Courbes algébriques : de l'inutile à l'indispensable

Sylvain Duquesne

Habilitation à diriger des recherches

Soutenue le 27 novembre 2007 devant le jury composé de

J. C. Bajard	Professeur	Université Montpellier 2
H. Cohen	Professeur émérite	Université Bordeaux 1
J. M. Couveignes	Professeur	Université de Toulouse
G. Frey	Professeur	Universität Essen
M. Girault	Expert émérite	France Telecom R&D, Caen
P. Michel	Professeur	Université Montpellier 2
B. Vallée	Directrice de recherche	Université de Caen

après avis de

J. M. Couveignes	Professeur	Université de Toulouse
G. Frey	Professeur	Universität Essen
M. Girault	Expert émérite	France Telecom R&D, Caen

Table des matières

1 Animation de la recherche

1.1 Situation

Actuellement maître de conférences en mathématiques à l'université de Montpellier 2 au sein de l'I3M (Institut de Mathématiques et de Modélisation de Montpellier), je suis également chercheur associé au LIRMM (Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier). Je participe donc activement à la vie de deux équipes de recherche, d'une part l'équipe de théorie des nombres, dirigée par Philippe Michel (I3M) et d'autre part l'équipe ARITH d'arithmétique des ordinateurs dirigée par Arnaud Tisserand (LIRMM).

Par ailleurs, je suis responsable de la filière Mathématiques et Informatique du département de Mathématiques de Montpellier. En particulier, en tant que responsable du Parcours Mathématiques-Informatique du Master 2 Recherche, je reste en contact permanent avec les étudiants désirant faire de la recherche dans cette voie. J'ai donc pour responsabilité de les conseiller, de les orienter, de leur trouver des stages (aussi bien dans le monde académique que dans le monde industriel) et des financements pour poursuivre en doctorat.

1.2 Enseignements liés à la recherche

J'enseigne également dans ce M2 recherche un module de cryptographie théorique et appliquée depuis 2003 (15 puis 30 heures). J'y aborde tous les aspects de la cryptographie moderne (fonctions de hachage, cryptographie par flot, générateurs aléatoires) et ses applications (internet, téléphonie mobile, protection contre la copie, ...) avec bien sur une attention particulière portée sur les systèmes de chiffrement symétriques (DES, Blowfish, AES) et asymétriques (RSA, courbes elliptiques et hyperelliptiques). Ce module fait également partie du M2 recherche d'informatique de Montpellier.

D'autre part j'ai accepté de dispenser un cours en anglais dans le Master 2 SISA (Security of Integrated Systems Applications) de l'école des Mines de Saint-Etienne sur les chiffrements asymétriques.

1.3 Participation à la formation doctorale

Lors de l'école d'été de Cryptologie organisée en 2002 et destinée à promouvoir la recherche en cryptologie auprès des jeunes doctorants ou futurs

doctorants, j'ai donné une conférence sur le thème de l'utilisation des courbes hyperelliptiques en cryptographie et sur les avantages et les inconvénients que ces courbes apportaient.

Avec l'aide d'Emmanuel Royer et de Thomas Hausberger, j'ai organisé le colloque "Jeunes Chercheurs en théorie des nombres" qui s'est tenu à la Grande Motte en mars 2004, réunissant une soixantaine de jeunes chercheurs (essentiellement des doctorants). L'objectif de ce colloque était de permettre à ces doctorants de se réunir, de présenter leurs travaux lors d'exposés de vingt minutes et de rencontrer des chercheurs confirmés qui ont chacun donné un cours durant trois heures sur un sujet en développement.

Lors de l'école jeunes chercheurs en algorithmique et calcul formel de 2005, j'ai été sollicité pour présenter un cours sur les courbes elliptiques et leur utilisation en cryptographie.

1.4 Encadrement de travaux de recherche

Depuis mon arrivée à Montpellier, j'ai encadré plusieurs étudiants pour leur stage de recherche de première année de Master. Les sujets tournent autour de la théorie des nombres et de la cryptographie.

J'ai également encadré, chaque année, un étudiant pour son stage de deuxième année de Master (ou de DEA) :

- Nicolas Méloni en 2004 sur l'utilisation des couplages en cryptographie.
- Moana Tetiarahi en 2005 sur le comptage de points sur les courbes elliptiques en caractéristique 2.
- Nadia El Mrabet en 2006 sur les attaques sur carte à puces et contre mesures mathématiques.
- Julien Hoarau en 2007 sur la sécurité dans la téléphonie mobile (stage en entreprise).

Enfin, avec Jean Claude Bajard, professeur au LIRMM, je coencadre actuellement 2 doctorants en cryptographie dont les sujets sont détaillés dans la partie 3.

Nicolas Méloni va soutenir sa thèse le 26 novembre 2007. Il avait obtenu une allocation de recherche 50% Mathématique et 50% Informatique en 2004 grâce à ses bons résultats dans le DEA de Mathématiques de Montpellier. Ses recherches se sont concentrées sur les représentations alternatives per-

mettant d'accélérer ou de sécuriser les opérations cryptographiques basées sur les courbes elliptiques. Ses travaux ont pour l'instant donné lieu à 5 publications dans des conférences internationales à comité de lecture. Pour l'année 2007-2008, il a obtenu un demi poste d'ATER à l'université de Toulon.

Nadia El Mrabet a commencé sa thèse en octobre 2006. Titulaire de l'agrégation de mathématiques, elle a obtenue une bourse DPI cofinancée par la région et le CNRS. Son sujet de thèse porte sur l'utilisation des couplages, récemment apparus en cryptographie. Elle travaille plus précisément sur les algorithmes permettant de les calculer et sur leur résistance aux fuites. Ses travaux ont déjà donné lieu à une publication dans une conférence internationale à comité de lecture.

2 Travaux de recherche

Mon domaine de recherche est l'algorithmique en théorie des nombres et la cryptographie. Je me suis plus particulièrement intéressé à l'algorithmique des courbes elliptiques et des courbes hyperelliptiques de genre 2 ou 3 ainsi qu'à leurs applications en cryptographie.

Mes travaux s'articulent autour de deux idées directrices qui me tiennent à coeur et continueront à me guider dans les années à venir :

- Une démarche expérimentale, peu courante en recherche mathématique.
- L'utilisation d'outils théoriques et abstraits pour résoudre des problèmes très concrets rencontrés par les industriels.

Le domaine des courbes elliptiques (et des courbes algébriques en général) fait partie des grands axes de la théorie des nombres. Elles sont par exemple à la base de la démonstration du grand théorème de Fermat. Je parle bien sûr ici de mathématiques dites pures ou plus généralement de recherche fondamentale rimant trop souvent aux yeux du grand public avec inutilité voire même gaspillage de l'argent public. Il faut bien avouer que de savoir (et encore pire : d'avoir une preuve) que l'équation

$$x^n + y^n = z^n$$

n'a pas de solutions entières non triviales si n est un entier supérieur à 3 ne va pas aider à résoudre le problème du réchauffement climatique. Cela n'a

pas empêché des centaines de chercheurs du monde entier de s'attarder sur ce problème pendant 350 ans. Aucun de ces chercheurs ni des gouvernements ou mécènes qui les finançaient ne pensait que ces travaux finiraient un jour entre les mains de chacun d'entre nous. Et pourtant, les courbes elliptiques (et plus généralement les courbes algébriques) constituent, à n'en pas douter, l'avenir de la cryptographie moderne. Elles sont déjà utilisées dans certains produits de grande consommation (Blackberry, protection de HD-DVD et Blue-ray, serveurs de paiement en ligne) et leur récente recommandation par la NSA (National Security Agency, l'agence de sécurité américaine) leur promet un avenir radieux partout autour de nous (internet, cartes bancaires, téléphonie mobile, vote électronique, télévision payante, ...).

Pour ma part je me suis intéressé aux deux aspects des courbes algébriques, l'aspect "fondamental" et l'aspect "appliqué". Ces deux aspects ne sont bien sûr pas indépendants et les mêmes outils servent dans les deux cas. J'expliquerai en particulier dans la partie 2.3 comment la variété de Kummer, étudiée du point de vue théorique dans la partie 2.2, peut servir à sécuriser les algorithmes de chiffrement basés sur les courbes elliptiques et hyperelliptiques.

2.1 Étude algorithmique de familles de courbes algébriques

Les courbes algébriques sur lesquelles j'ai travaillé sont données par des équations de la forme

$$y^2 = f(x), \tag{1}$$

où f est un polynôme à coefficients dans $\mathbb{Q}$. Lorsque le degré de f vaut 3 ou 4, on a à faire aux courbes elliptiques et lorsque le degré est plus grand aux courbes hyperelliptiques. Ces courbes possèdent des propriétés très similaires du point de vue diophantien. D'une part Siegel a démontré en 1928 qu'une courbe elliptique ne pouvait posséder qu'un nombre fini de points entiers (c'est à dire de couples d'entiers (x,y) vérifiant l'équation (1)). D'autre part Faltings a démontré dans [Faltings 83] qu'une courbe hyperelliptique (sous-entendu non elliptique) ne pouvait posséder qu'un nombre fini de points rationnels.
Ces deux propriétés n'ont toutefois pas que leur énoncé comme ressemblance. Dans les deux cas, en effet, on ne connaît pas de méthode effective pour trouver ces points ni même pour connaître leur nombre.

Ces deux problèmes, très similaires, sont donc centraux dans la recherche actuelle en théorie des nombres et plus particulièrement pour les chercheurs intéressés par les équations diophantiennes. Dans cette section, je m'intéresse au premier problème en cherchant des points entiers sur des familles de courbes elliptiques. J'aborderai le second problème dans la section 2.2.

2.1.1 Les "simplest cubic fields"

Soit m un entier positif tel que

$$\Delta = m^2 + 3m + 9$$

soit sans facteur carré.
Le corps cubique $\mathbf{K}_m$ défini par le polynôme irréductible sur $\mathbb{Q}$,

$$f(X) = X^3 + mX^2 - (m+3)X + 1$$

a été introduit dans [Shanks 74] et est appelé un "simplest cubic field". Shanks a introduit cette classe de corps car les calculs sont particulièrement faciles à effectuer sur de tels corps, ce qui leur a valu leur nom. Ces corps ont été par la suite beaucoup étudiés car leur régulateur est explicite et petit. Ainsi leur nombre de classes a tendance à être particulièrement grand.

Je me suis pour ma part intéressé aux courbes elliptiques définies sur $\mathbb{Q}$ par les équations :

$$E_m \,:\, Y^2 = X^3 + mX^2 - (m+3)X + 1 \ , \tag{2}$$

pour un entier m définissant un "simplest cubic field".
Cette famille de courbes elliptiques a été introduite dans [Washington 87]. L'auteur y établit une relation entre le rang de la courbe elliptique E_m sur $\mathbb{Q}$ et le 2-rang du groupe des classes de $\mathbf{K}_m$. On peut ainsi espérer que le rang des courbes elliptiques de cette famille ne sera pas trop petit, du moins qu'il sera suffisamment grand pour que ces courbes contiennent des points entiers. C'est la raison pour laquelle je me suis intéressé au calcul de ces points sur les courbes de cette famille qui semblaient bien s'y prêter.

Dans un premier temps, j'ai utilisé une méthode permettant de calculer les points entiers sur une courbe elliptique lorsque son groupe de Mordell-Weil est connu. Cette méthode développée dans [Stroeker-Tzanakis 94], [Gebel-Pethö-Zimmer 94], et [Smart 94] entre autres, est basée sur les formes linéaires de logarithmes elliptiques.

Elle m'a permis de calculer tous les points entiers sur les courbes elliptiques E_m pour les valeurs du paramètre m inférieures à 1000 et définissant un "simplest cubic field". À partir de ces calculs, j'ai émis plusieurs conjectures concernant bien sûr les points entiers de ces courbes mais aussi la structure du groupe de Mordell-Weil $E(\mathbb{Q})$. J'ai finalement démontré ces conjectures dont la principale concerne le point $[0, 1]$ qui joue un rôle central dans ce travail. Les résultats les plus intéressants sont en effet :

- d'une part la preuve que le point $[0, 1]$ est un générateur du groupe de Mordell-Weil,

- d'autre part le calcul explicite de tous les multiples entiers de ce point.

J'ai démontré ces résultats pour un entier m quelconque définissant un "simplest cubic field". C'est le fait de travailler sur une famille infinie qui fait la difficulté de ces travaux. Ce type de calcul est en effet classique et bien connu sur une courbe donnée.

Il devient alors possible de déduire de ces deux résultats que, lorsque la courbe E_m est de rang 1, les points entiers de E_m sont exactement les points $[0, 1]$, $[0, -1]$ et leurs doubles si m est pair.

C'était la première fois que ce type de travail était réalisé sur une famille de courbes elliptiques et cela a donné lieu à la publication [Duquesne 01]. Ce premier travail a été pour moi la découverte de l'intérêt d'une démarche expérimentale (expérimentations, conjectures, preuves) en recherche mathématique et m'a encouragé à poursuivre dans cette voie.

Les preuves sont basées sur l'utilisation de la hauteur canonique sur les courbes elliptiques E_m et leur encadrement. Bien évidemment la méthode employée n'est pas généralisable à n'importe quelle famille (cela donnerait une version explicite du théorème de Siegel). Il est en effet nécessaire de pouvoir éliminer, grâce à une autre méthode ou à des astuces, les cas où une telle borne sur les hauteurs canoniques n'existe pas.
J'ai par la suite précisé les conditions pour qu'elle s'applique lors de mon étude des "simplest quartic fields" [Duquesne 07a].

En dehors de la problématique des points entiers, le fait de connaître explicitement le générateur d'une famille de courbes elliptiques ouvre de nouvelles perspectives. En effet la structure du groupe de Mordell-Weil d'une

courbe elliptique est l'outil de base pour une étude poussée de cette courbe. Avoir à sa disposition une famille de courbes dont on connaît la structure précise du groupe de Mordell-Weil permet ainsi de faire plus facilement des calculs et des statistiques sur un grand nombre de courbes. Avec Christophe Delaunay, nous avons ainsi étudié dans [Delaunay-Duquesne 03] les valeurs critiques des séries L associées aux courbes elliptiques de rang 1 définies par des "simplest cubic fields". D'après la conjecture de Birch et Swinnerton-Dyer, ces valeurs sont reliées à des invariants géométriques de la courbe elliptique tels la hauteur canonique du générateur et le groupe de Tate-Shafarevitch. La hauteur canonique du générateur étant connue grâce au travail précédent, on peut déduire des informations sur le groupe de Tate-Shafarevitch habituellement difficilement accessibles surtout sur une famille de courbes. Ce type de travail sur une famille de courbes elliptiques avait précédemment été réalisé ([Zagier-Kramarz 87]) dans le cas du rang 0 (où la structure du groupe de Mordell-Weil est particulièrement simple). Outre le fait d'étudier une autre famille pour valider ou moduler les constatations de [Zagier-Kramarz 87], le passage à une famille de courbes de rang 1 apporte d'autres nouveautés. Par exemple, il n'existe que peu d'exemples dans la littérature de courbes elliptiques de rang non nul et de groupe de Tate-Shafarevitch non trivial. Cela est dû à l'existence d'une infinité de points rationnels (contre un nombre fini en rang nul), il est donc plus difficile de trouver des points p-adiques ne correspondant pas à des points rationnels (c'est ce déséquilibre local/global que mesure le groupe de Tate-Shafarevitch). Ainsi déterminer l'ordre du groupe de Tate-Shafarevitch pour un grand nombre de courbes dans ces conditions revêt un intérêt particulier.

Nous avions, à l'époque, constaté (comme Zagier et Kramarz) une densité positive de courbes de rang strictement supérieur à 1, ce qui est contraire à l'opinion généralement admise sur le sujet. Des calculs plus avancés, réalisés dans [Watkins 07], sur la famille de courbes étudiée par Zagier et Kramarz d'une part et la théorie des matrices aléatoires d'autre part nous ont par la suite laissé penser que cette constatation était erronée et que nous n'avions pas poussé les calculs assez loin pour voir la courbe s'infléchir.

Par contre, concernant les fréquences d'apparition des différents ordres du groupe de Tate-Shafarevtich, nous avons constaté des densités non nulles, ce qui était cette fois en accord avec les heuristiques de [Delaunay 01].

Finalement nous avons utilisés nos calculs pour produire des exemples de courbes de rang 3 et 5 possédant des groupes de Tate-Shafarevitch non

triviaux qui sont extrêmement rares dans la littérature.

2.1.2 Les "simplest quartic fields"

Plus récemment dans [Duquesne 07a], j'ai continué l'étude des familles de courbes elliptiques en faisant un travail similaire à [Duquesne 01] sur une famille ne possédant pas les mêmes propriétés. J'ai ainsi étudié la famille, en apparence très similaire, des courbes elliptiques associés aux "simplest quartic fields". Les "simplest quartic fields" ont bien sûr la même origine que les "simplest cubic fields" et les courbes elliptiques qui leur sont associés sont de la forme

$$Q_t : \ Y^2 = X^4 - tX^3 - 6X^2 + tX + 1,$$

ou, en envoyant le point $[0, 1]$ à l'infini, de la forme (de Weierstrass)

$$C_t : \ y^2 = x^3 - (16 + t^2)x.$$

Certaines propriétés des courbes elliptiques associées aux "simplest cubic fields" et aux "simplest quartic fields" sont communes. Ainsi, dans les deux cas, il existe un point d'ordre infini (le point $[0, 1]$) et je démontre que ce point est de plus un générateur du groupe de Mordell-Weil. Cela laisse penser que la méthode utilisée dans [Duquesne 01] (utilisant les encadrements de hauteurs canoniques) peut être étendue à d'autres familles de courbes elliptiques. En fait, j'explique dans [Duquesne 07a] que si on dispose d'un point d'ordre infini et que celui ci est effectivement générateur, alors la méthode utilisée dans [Duquesne 01] permet de le démontrer.
Cette propriété est bien sûr fondamentale pour la suite puisqu'elle concerne la structure du groupe de Mordell-Weil qui doit être connue si on veut aller plus loin dans l'étude des propriétés arithmétiques des courbes elliptiques (par exemple si on veut connaître les points entiers).
Ainsi, comme c'était le cas pour les "simplest cubic fields", la structure du groupe de Mordell-Weil est complètement déterminée dans le cas des courbes de rang 1 associées aux "simplest quartic fields". La situation est toutefois différente pour les points entiers à cause de la présence d'un point de torsion, ce qui n'était pas le cas avec les courbes elliptiques associées aux "simplest cubic fields". Trouver exactement les points entiers sur la famille de courbes C_t de rang 1 devient alors impossible avec la méthode utilisée quand le paramètre t est pair. Toutefois une astuce m'a permis de contourner cette difficulté et de trouver quand même les points entiers sur la famille des courbes Q_t de rang 1, ce qui était le problème initial.

L'autre particularité de la famille des courbes elliptiques définies par des "simplest quartic fields" est la possibilité d'en extraire une sous-famille de courbes de rang 2 dont on connaît explicitement 2 points d'ordre infini. J'ai dû alors généraliser la méthode utilisée dans [Duquesne 01] pour démontrer que ces deux points sont indépendants et engendrent la partie libre du groupe de Mordell-Weil. Le passage à deux points est loin d'être aisé. Il utilise la méthode de descente infinie décrite dans [Siksek 95] et le régulateur. Le régulateur étant une différence de hauteurs canoniques, les bornes sur celles ci doivent être très précises sous peine de trouver de mauvaises bornes sur le régulateur.
Encore une fois la connaissance de la structure complète du groupe de Mordell-Weil (ici en rang 2) permet de s'attaquer à la détermination des points entiers. J'ai donc généralisé la méthode utilisée en rang 1 et obtenu exactement tous les points entiers sur la sous famille des courbes Q_t de rang 2 considérée. Pour des raisons similaires au cas du rang 1, je n'ai pas pu conclure sur la famille des C_t.

A ma connaissance, c'est la première fois que l'on a autant d'information sur la structure du groupe de Mordell-Weil et sur les points entiers pour une famille infinie de courbes de rang 2. Ce travail m'a également permis de mieux cerner les cas où les méthodes employées dans [Duquesne 01] peuvent être utilisées avec succès.

2.1.3 Pistes de futures recherches

Malgré l'orientation plus cryptographique de mes dernières recherches, j'ai plusieurs idées pour continuer mes travaux dans cette voie. La plus naturelle est de regarder ce qui se passe pour les "simplest quintic fields" ou les "simplest sextic fields". On quitte alors le monde des courbes elliptiques pour celui des courbes hyperelliptiques. Le reste de mes travaux concernant en grande partie les courbes hyperelliptiques, je connais bien les outils nécessaires à l'étude des courbes associées à ces corps et des résultats intéressants devraient pouvoir être obtenus.

D'autre part, très peu de travaux ont été réalisés dans le domaine de la vérification expérimentale de la conjecture de Birch et Swinnerton-Dyer pour les courbes hyperelliptiques. Des travaux du type de ceux entrepris dans [Delaunay-Duquesne 03] mais dans le cadre des courbes hyperelliptiques seraient particulièrement intéressants. Cette piste, ainsi que l'étude de familles de courbes elliptiques tordues quadratiques, fait partie de l'ANR

ALGOL dont je fais partie et qui démarre en 2007.

2.2 La Variété de Kummer d'une courbe algébrique

Dans cette partie, je m'intéresse à la variété de Kummer d'une courbe elliptique ou hyperelliptique. Du point de vue théorique, cet objet est simplement le quotient de la Jacobienne de la courbe par l'involution hyperelliptique. Cela signifie qu'il devient impossible de distinguer un diviseur de son opposé. Du point de vue pratique, cet objet présente l'avantage d'être plus simple à manipuler que la Jacobienne elle même. Il faut cependant, dans un premier temps, donner une description explicite de ce quotient et c'est ce qui va me préoccuper dans cette partie. Je donnerai aussi des applications de ce nouvel outil à des problèmes classiques sur les courbes algébriques comme la recherche de points rationnels.

Le fait qu'on ne puisse pas distinguer un élément de son opposé n'est à priori pas très restrictif. Par exemple dans le cas des courbes elliptiques, cela revient à ne conserver que l'abscisse des points qui contient l'essentiel de l'information puisque $y = \pm\sqrt{f(x)}$. Malheureusement, cela a des conséquences regrettables sur la loi de groupe. En effet il devient impossible d'additionner deux éléments A et B puisqu'il y a confusion pour le résultat entre $A + B$ et $A - B$. La loi de groupe de la Jacobienne, si fondamentale dans les applications, n'est donc plus valable dans la variété de Kummer. Cependant des traces de cette loi de groupe subsistent sur la variété de Kummer. Ainsi, un élément de 2-torsion est égal à son opposé, de sorte que l'addition par un élément de 2-torsion reste valable. De la même manière, il est possible d'ajouter un élément A avec lui-même puisque $A - A$ est l'élément neutre. Il est donc facilement reconnaissable et il ne peut pas y avoir de confusion avec $A + A$. Dans le cas des courbes de genre 2 (et en caractéristique impaire), Flynn a donné dans [Flynn 93] une version explicite de la variété de Kummer (qui est une surface dans $\mathbb{P}^3$ dans ce cas) et a donné des formules permettant de calculer rapidement ces traces de la loi de groupe. Il a également donné des formules pour les expressions de la forme

$$k_i(A + B)k_j(A - B) + k_j(A + B)k_i(A - B),$$

où $k_i(A)$ représente la i-ème coordonnée dans $\mathbb{P}^3$ de A. Ces formules sont bien définies sur la surface de Kummer (remplacer A ou B par son opposé ne les modifie pas) et permettent de faire explicitement la somme de A et de B sur la surface de Kummer si leur différence est connue.

Dans [Cassels-Flynn 96] Flynn reprend cette construction et décrit deux applications importantes de cette description complète des traces de la loi de groupe de la Jacobienne sur la surface de Kummer. La première est le développement d'une théorie explicite des hauteurs ([Flynn 95]) sur les Jacobiennes de courbes de genre 2 permettant d'effectuer une descente infinie [Flynn-Smart 97]. Cette descente infinie est la dernière étape du processus permettant de calculer les générateurs du groupe de Mordell-Weil. La seconde concerne la recherche des points rationnels d'une telle courbe.

2.2.1 Utilisation pour la recherche des points rationnels d'une courbe hyperelliptique

Le théorème de Faltings permet d'affirmer qu'il n'y a qu'un nombre fini de points rationnels sur une courbe de genre 2 sans toutefois donner d'angle d'attaque pour les déterminer. Une version plus explicite de ce résultat avait été donnée précédemment dans [Chabauty 41] mais à la condition que le rang de la Jacobienne soit strictement inférieur au genre de la courbe.

Dans [Flynn 97], la description de la surface de Kummer permet d'élaborer une méthode explicite pour appliquer le théorème de Chabauty à une courbe de genre 2 dont le rang de la jacobienne vaut 1 (le cas du rang 0 est résolu depuis longtemps puisqu'il ne s'agit que de calculer la torsion). Plus précisément, cette méthode permet de borner de façon fine le nombre de points rationnels et dans la plupart des cas, on peut ainsi connaître effectivement tous les points rationnels. Le principe simplifié de cette méthode est le suivant :

- On considère connue la structure du groupe de Mordell-Weil (c'est à dire sa torsion et un générateur G puisqu'on est en rang 1).
- Pour chaque élément de torsion T, on cherche un point rationnel sous la forme $T + nG$.
- On utilise la surface de Kummer pour assurer l'annulation d'une série formelle p-adique en n.
- On utilise le théorème de Strassman pour trouver une borne sur le nombre de valeurs de n annulant cette série formelle.
- En recollant toutes ces bornes, on obtient une borne sur le nombre de points rationnels.
- Si cette borne correspond aux nombre de points déjà connus, ce qui est souvent le cas, le problème de trouver tous les points rationnels est résolu.

Bien sûr, "souvent" ne veut pas dire "tout le temps" et les cas restants sont

sources de nouvelles idées et de nouvelles méthodes de résolution.

La plus prometteuse d'entre elle est la méthode dite de Chabauty elliptique. C'est fondamentalement la même méthode : au lieu de travailler sur une courbe de genre g dont le rang de la jacobienne est strictement inférieur à g, on travaille avec une courbe elliptique définie sur un corps de nombres de degré d et dont le rang r est strictement inférieur à d. En utilisant la loi de groupe formelle sur cette courbe elliptique, on se ramène également à une condition d'annulation de séries formelles.

Il existe plusieurs méthodes pour ramener le problème de la recherche de points rationnels sur une courbe hyperelliptique à celle d'un problème résoluble par la méthode de Chabauty elliptique et ces approches ont permis de résoudre bon nombre de cas où la méthode de Chabauty usuelle ne permettait pas de conclure ([Flynn-Wetherell 99], [Bruin 99],[Flynn-Wetherell 01], [Flynn 01], [Duquesne 03]).

Ces exemples restent cependant dans la même catégorie que la méthode de Chabauty pour les courbes de genre 2, à savoir que le rang de la courbe elliptique vaut 1 et qu'une seule série formelle en une seule variable doit s'annuler. Un nouveau problème se pose donc : que faire dans le cas où la courbe elliptique est de rang strictement supérieur à 1 (et bien sûr toujours strictement inférieur à d). La méthode (tout comme une éventuelle méthode de Chabauty basée sur la variété de Kummer d'une courbe dont la Jacobienne a un rang strictement supérieur à 1) conduit alors non pas à l'annulation d'une série formelle en une variable, mais à l'annulation simultanée de $d-1$ séries formelles en r variables (et on voit bien ici d'ailleurs pourquoi le rang doit être strictement inférieur au degré).

Dans [Duquesne 02a], j'ai utilisé le théorème de préparation de Weierstrass pour généraliser le théorème de Strassman au cas de plusieurs variables, j'en ai écrit une version explicite et déduit un algorithme permettant donc de borner effectivement et finement le nombre de solutions d'un système de séries formelles. Cela m'a permis de traiter le cas des points rationnels d'une courbe hyperelliptique de genre 4 dont le rang de la jacobienne vaut 4. Bien sûr cette courbe ne vérifie pas les conditions du théorème de Chabauty, mais le problème de trouver ses points rationnels se ramène au problème de Chabauty elliptique pour une courbe de rang 2 définie sur un corps de nombres de degré 3 (qui rentre dans le cadre de la méthode de résolution donnée dans [Duquesne 02a])

2.2.2 Cas des courbes de genre 3

La construction explicite de la variété de Kummer par Flynn a ainsi eu des applications variées et importantes quant à l'étude des propriétés arithmétiques et géométriques des courbes de genre 2. Il semble donc naturel d'essayer de les généraliser au cas des courbes hyperelliptiques de genre 3 en espérant que les applications pourront également se généraliser.

Dans [Stubbs 00], un doctorant de Flynn a commencé ce travail en décrivant la variété de Kummer d'un courbe hyperelliptique de genre 3 définie sur un corps de caractéristique impaire par une équation de la forme

$$y^2 = f(x) \text{ où } f \text{ est un polynôme de degré } 7.$$

Il donne ainsi un plongement de la variété de Kummer dans $\mathbb{P}^7$ ainsi que 27 équations polynômiales explicites reliant ses coordonnées dans $\mathbb{P}^7$. Dans le cas du genre 2, la variété de Kummer était une surface de $\mathbb{P}^3$, c'est à dire qu'une seule telle équation suffisait à la décrire. Les objets manipulés en genre 3 sont donc bien plus complexes qu'en genre 2 et les calculs sont bien plus lourds à réaliser.

Exactement comme dans le cas des courbes de genre 2, la structure de groupe de la jacobienne est perdue en passant dans la variété de Kummer mais les calculs s'en retrouvent considérablement simplifiés. Il reste cependant des traces de la loi de groupe qui sont d'ailleurs les mêmes que dans le cas des courbes de genre 2. L'objectif de [Duquesne 02b] était d'étudier ces traces de la loi de groupe. J'ai, dans un premier temps, calculé la matrice d'addition d'un élément de 2-torsion. Pour cela, j'ai suivi la méthode employée par Flynn moyennant quelques modifications techniques permettant d'accélérer les calculs qui auraient été trop lourds si une simple généralisation avait été effectuée. De plus, dans le cas du genre 2, une astuce est nécessaire à la fin du calcul pour remplir la dernière ligne de la matrice. Dans le cas du genre 3, ce sont les 4 dernières des 8 lignes qui doivent être déterminées et l'astuce utilisée par Flynn en genre 2 n'est plus suffisante.

L'addition d'un élément de 2-torsion n'est pas qu'une simple trace de la loi de groupe sans intérêt. Elle est à la base de la méthode utilisée par Flynn pour déterminer explicitement les formes biquadratiques B_{ij} telles que

$$k_i(A+B)k_j(A-B) + k_i(A-B)k_j(A+B) = B_{ij}(A,B).$$

En effet, le calcul direct de ces expressions aurait été irréalisable (comme on le verra dans la partie suivante) avec les moyens dont Flynn disposait

à l'époque et il est certainement toujours irréalisable pour les courbes de genre 3.

La méthode que Flynn emploie en genre 2 et que j'ai généralisée en genre 3 est très surprenante mais terriblement efficace ; elle consiste à calculer les B_{ij} en faisant l'hypothèse que B est un élément de 2-torsion mais sans l'exprimer dans ses coordonnées. Autrement dit on prend un élément B quelconque et on calcule les coordonnées de $A + B$ et de $A - B$ en utilisant la matrice d'addition d'un élément de 2-torsion précédemment calculée. Le résultat obtenu n'est alors, à priori, valable que pour les éléments de 2-torsion mais un argument d'indépendance des produits 2 à 2 des coordonnées formelles de A permet de conclure à leur validité pour un élément B quelconque. Cette méthode se généralise bien aux courbes hyperelliptiques de genre 3 sauf que l'argument d'indépendance ne peut être utilisé tel quel à cause des 27 relations définissant la variété de Kummer. Un argument du même type mais plus fin doit être utilisé.
Comme dans le cas du genre 2, ces résultats m'ont permis d'esquisser une théorie explicite des hauteurs pour les courbes hyperelliptiques de genre 3 définies par un polynôme de degré 7.

2.2.3 Cas des courbes de genre 2 en caractéristique 2

Dans tous ses travaux, Flynn se place en caractéristique impaire. Les différences avec la caractéristique 2 sont multiples puisque même l'équation de la courbe de départ n'a pas la même forme. Les outils utilisables sont très différents et la plupart des applications des travaux de Flynn sont en caractéristique nulle (et même sur $\mathbb{Q}$ à vrai dire). Il n'était donc pas nécessaire pour lui de se compliquer la tâche avec la caractéristique 2. Comme détaillé dans la section 2.3, j'ai pour ma part trouvé des applications de la variété de Kummer en cryptographie. Les corps finis de caractéristique 2 sont souvent utilisés en cryptographie si bien que le besoin d'une théorie analogue à celle de Flynn s'est vite fait ressentir en caractéristique 2.

Je me suis donc attelé à cette tâche dans [Duquesne 07b]. J'ai dû redéfinir le plongement dans $\mathbb{P}^3$ de la surface de Kummer ainsi que recalculer son équation, puis déterminer la matrice de l'addition d'un élément de 2-torsion. J'ai fait tout ceci avec des méthodes similaires à celles employées par Flynn en caractéristique impaire à ceci près que l'on tombe souvent sur des difficultés propres à la caractéristique 2. Il a fallu ensuite calculer les formes biquadratiques permettant d'additionner deux éléments de la surface de Kum-

mer si leur différence est connue. Comme je l'ai expliqué dans le paragraphe précédent, Flynn supposait pour cela que B était un élément de 2-torsion et utilisait la matrice d'addition d'un élément de 2-torsion bien définie sur la surface de Kummer. Malheureusement, ceci ne peut pas être appliqué en caractéristique 2 pour la simple et bonne raison que les expressions

$$k_i(A+B)k_j(A-B)+k_j(A+B)k_i(A-B),$$

sont toutes nulles si B est un élément de 2-torsion. Cette obstruction à une généralisation trop simpliste de la méthode de Flynn illustre d'ailleurs très bien le type de problèmes rencontrés en caractéristique 2.
J'ai donc dû m'attaquer directement au cas où A et B sont des éléments quelconques de la surface de Kummer. Les calculs deviennent alors vite très gourmands. En effet les éléments A et B sont définis par 8 variables reliées par 4 équations et ce travail nécessite des polynômes de degré supérieur à 10 en ces 8 variables, le tout sur un corps défini à l'aide de 10 variables (les coefficients de la courbe). Dans ces conditions une simple multiplication mal placée a vite fait de prendre toute une nuit de calcul ou d'utiliser toute la mémoire de la machine. J'ai donc dû utiliser des astuces pour alléger ces calculs et les rendre possibles. J'ai par exemple dû faire des essais sur des éléments B ayant certaines particularités ou même sur des exemples pour deviner la forme que devraient avoir les formes biquadratiques (ou même la forme des résultats intermédiaires). Cela a permis de diminuer les ressources informatiques nécessaires en rajoutant des contraintes sur le résultat. Comme dans le cas des familles de courbes elliptiques que j'ai étudiées et bien que dans un registre tout à fait différent, une démarche expérimentale m'a ainsi permis d'obtenir des résultats significatifs.

2.2.4 Pistes de futures recherches

Du point de vue de la construction de variétés de Kummer et applications arithmétiques, le cas du genre 3 ouvre de nombreuses portes. Il serait bien sûr intéressant de généraliser la construction de la variété de Kummer et la description explicite des traces de la loi de groupe aux courbes hyperelliptiques de genre 3 définies par un polynôme de degré 8 ou aux courbes de genre 3 non hyperelliptiques. Cependant, même dans le cas des courbes définie par un polynôme de degré 7, il reste beaucoup à faire. Je n'ai par exemple pas encore calculé les constantes permettant de borner la hauteur d'un élément car il est fort probable que leur taille les rende inexploitables en pratique (ce n'est déjà pas efficace en genre 2). Mes espoirs reposent sur une version équivalente de la méthode que Flynn emploie pour améliorer ces

constantes dans le cas des courbes de genre 2. Cela permettrait d'écrire un algorithme pour le calcul du sous-groupe de torsion de la jacobienne et pour la descente infinie qui sont deux des étapes majeures de la détermination de la structure du groupe de Mordell-Weil. Malheureusement la méthode de Flynn ne peut pas se généraliser telle quelle puisqu'elle utilise le fait que toutes les courbes de genre 2 sont hyperelliptiques, ce qui n'est plus le cas en genre 3. Une nouvelle approche est donc nécessaire.
A plus long terme, on peut espérer une méthode de Chabauty analogue à celle de Flynn pour les courbes de genre 3.

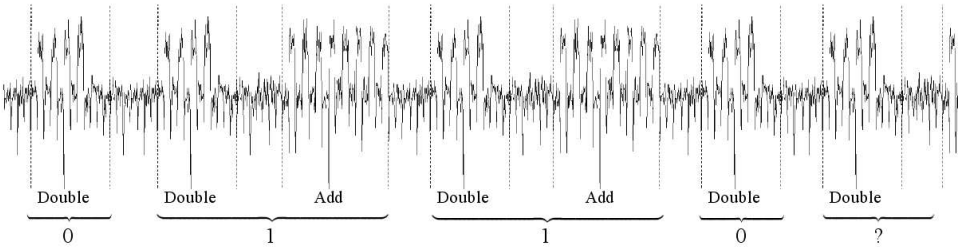
2.3 Application à la cryptographie : arithmétique résistante aux fuites sur les courbes algébriques

Une grande partie de mes travaux dans le domaine de la cryptographie tourne autour de la résistance aux fuites et c'est donc cet aspect que je vais détailler dans cette partie. Une première approche de la cryptographie consisterait à se satisfaire d'une primitive cryptographique mathématiquement robuste (comme RSA ou ECC) et à l'implémenter. Malheureusement, le monde réel n'est pas aussi idyllique que le monde abstrait des mathématiques. Ainsi, même si le problème mathématique sous-jacent est incassable, son implémentation peut facilement s'avérer désastreuse et révéler très rapidement des informations capitales sur les secrets à protéger, voire les secrets eux-mêmes. Les implémentations sur des systèmes embarqués, comme les cartes à puces, sont plus particulièrement sensibles à cette problématique puisque l'attaquant a accès à l'ensemble du système de chiffrement. Ce type d'attaques, couramment appelées attaques par canaux cachés, est basé sur l'observation d'informations fuyant de la carte à puce, comme ses temps d'exécution ([Kocher 96]), sa consommation ([Kocher-Jaffe-Jun 99]) ou son rayonnement électromagnétique ([Quisquater-Samyde 01]). Contrairement à ce qu'on pourrait penser, ce type d'information est accessible relativement facilement et pour un coût modeste (par rapport aux enjeux). Il faut enfin noter que ces attaques ne sont pas exclusivement orientées vers les systèmes embarqués ; il a par exemple été possible de réaliser une attaque par canaux cachés en analysant le bruit produit par un ordinateur à travers un mur.
Il existe deux types d'attaques par canaux cachés. D'une part, celles dites simples qui tirent les informations directement d'une seule opération spécifique et d'autre part celles dites différentielles qui utilisent des méthodes statistiques sur un grand nombre de réalisations d'une opération. D'après [Coron 99], il est toujours possible et relativement peu coûteux de se prémunir

contre les attaques différentielles. Je me suis donc plus particulièrement intéressé aux attaques simples.

Supposons par exemple qu'on sache analyser avec un oscilloscope la consommation d'une carte à puce sur laquelle est implémenté un algorithme simple de multiplication scalaire sur les courbes elliptiques : le double-and-add. Cette méthode, aussi appelée méthode du paysan russe ou square-and-multiply si on l'applique sur un groupe multiplicatif, est une simple application du schéma de Hörner et est à la base de toutes les méthodes de multiplication scalaire ou d'exponentiation.
La multiplication scalaire d'un entier k par un point de la courbe P est l'opération centrale dans le domaine de la cryptographie basée sur les courbes elliptiques. Dans la plupart des protocoles cryptographiques k est la clé secrète.

L'algorithme de double-and-add fonctionne de la façon suivante : pour chaque bit de la clé k, il effectue un doublement et si le bit vaut 1 il ajoute le point P. Une addition et un doublement étant obtenus avec des formules différentes sur une courbe elliptique, les opérations effectuées par la carte à puce sont différentes selon que le bit de la clé vaut 0 ou 1. En pratique, l'image obtenue sur l'oscilloscope ressemble à ceci.



On peut alors lire à l'œil nu l'enchaînement des bits de k et donc la clé k elle-même. Ainsi, il est possible de retrouver la clé utilisée sans avoir à casser un logarithme discret.

Pour parer ces attaques, il est donc nécessaire que les opérations effectuées sur la courbe elliptique ne dépendent plus des bits de la clé. Il existe plusieurs types de méthodes pour y parvenir.

- La plus simple est d'ajouter des opérations inutiles dans les calculs. On peut ainsi, dans l'exemple précédent, décider d'effectuer une addition

fantôme quand le bit de la clé vaut 0. Cette solution a l'avantage de la simplicité mais elle est coûteuse et surtout sensible aux attaques par injection de faute (si on force la puce à faire une faute au moment ou elle effectue une opération fantôme, cela n'a pas d'incidence sur le résultat final et on peut alors en déduire qu'au moment de l'injection de la faute, le bit de la clé valait 0).

- Une autre méthode consiste à utiliser des représentations des courbes elliptiques telles que le doublement d'un point et l'addition de deux points utilisent les mêmes formules. C'est la méthode des formules unifiées.
- La dernière possibilité est d'utiliser un algorithme exposé pour la première fois dans [Montgomery 87]. Cet algorithme consiste à ne considérer que l'abscisse d'un point sur une courbe elliptique. Il a la particularité d'utiliser à la fois un doublement et une addition pour chaque bit de la clé ce qui ne laisse donc pas de trace de la clé.

J'ai, pour ma part, apporté des améliorations ou des contributions à ces méthodes et surtout généralisé la troisième au cas des courbes hyperelliptiques de genre 2.

2.3.1 Formules unifiées : forme de Jacobi d'une courbe elliptique

Des formules unifiées pour l'addition et le doublement peuvent être obtenues de différentes façons. Elles sont décrites en détail dans [Cohen-et-al 06]. L'une d'entre elles utilise la forme de Jacobi d'une courbe elliptique ayant un point de 2-torsion ([Liardet-Smart 01]). D'après [Billet-Joye 03], ces formules nécessitent, pour chaque bit de l'exposant, 16 multiplications sur le corps de base et 14 sous certaines conditions. Jusqu'à mes améliorations, ces formules étaient les plus efficaces pour une courbe ayant un point de 2-torsion. J'ai en effet réussi dans [Duquesne 07b] à faire descendre cette complexité à 14 multiplications et 12 sous certaines conditions, par ailleurs moins contraignantes que celles de [Billet-Joye 03].

Un courbe elliptique sous forme de Jacobi est donnée par une équation

$$Y^2 = \varepsilon X^4 - 2\delta X^2 Z^2 + Z^4. \tag{3}$$

Un point est représenté par un triplet (X, Y, Z) satisfaisant cette équation et il est prouvé dans [Billet-Joye 03] que toute courbe elliptique définie sur un corps premier et ayant un point de 2-torsion peut se mettre sous cette forme. J'ai réussi à améliorer la complexité des formules fournies dans

[Billet-Joye 03] en changeant la représentation des points (je les ai représenté par un quadruplet (X^2, XZ, Z^2, Y)) et en adaptant les formules. Il faut toutefois noter qu'une transformation d'une représentation à l'autre doit être effectuée en début et en fin de calcul de la multiplication scalaire mais son coût est négligeable.

D'autre part, dans mes formules (comme dans celles de [Billet-Joye 03]) 2 multiplications par ε interviennent. Il est donc particulièrement intéressant d'essayer de se ramener au cas où ε est petit. Billet et Joye montrent que l'on peut souvent se ramener à ce cas à condition que la courbe elliptique possède 3 points de 2-torsion. J'ai également amélioré ce résultat en démontrant que non seulement la présence d'un seul point de 2-torsion était suffisante mais encore qu'on pouvait négliger les multiplications par ε dans de plus nombreux cas.

2.3.2 Utilisation de la surface de Kummer en genre 2

J'ai déjà mentionné le fait que Montgomery utilisait seulement l'abscisse d'un point sur une courbe elliptique pour décrire un algorithme de multiplication scalaire nécessitant, pour chaque bit de la clé, une addition et un doublement sur la courbe elliptique. Cet algorithme est donc naturellement protégé contre les attaques par canaux cachés simples et il a beaucoup de succès chez les développeurs sur carte à puce. Il n'est cependant pas applicable sur toutes les courbes elliptiques (et en particulier sur les courbes fournies dans les standards) sans les généralisations apparues plus récemment dans [Brier-Joye 02].

Dans le cadre des courbes elliptiques, ne conserver que l'abscisse des points est assez naturel puisque l'ordonnée ne porte que peu d'information et n'est même pas nécessaire dans tous les protocoles cryptographiques. L'inconvénient est qu'on ne peut plus distinguer un point de son opposé. Cela n'est bien sûr pas sans rappeler la variété de Kummer étudiée dans la partie 2.2. Les traces de la loi de groupe sur la variété de Kummer d'une courbe elliptique (doublement, formes biquadratiques) permettent aisément de retrouver, par un autre moyen que celui employé par Montgomery, les formules d'addition et de doublement données dans [Montgomery 87] et dans [Brier-Joye 02].

Il n'y a alors qu'un pas à franchir pour généraliser la méthode de Montgomery aux courbes hyperelliptiques de genre 2 puisque la plupart des outils

nécessaires ont été présentés dans la partie 2.2. Ces outils sont en effet d'une part le doublement qui reste bien défini sur la surface de Kummer et d'autre part les formes biquadratiques qui permettent d'additionner deux éléments si leur différence est connue.

J'ai pu transposer l'algorithme de multiplication scalaire donné par Montgomery au cas des courbes hyperelliptiques sans trop de difficulté. Son but est le calcul de kA où A est un élément de la Jacobienne (ou de la surface de Kummer) et k est un scalaire (dans les cas qui nous intéressent, k est censé rester secret). Étant donné qu'on ne sait additionner deux éléments que si leur différence est connue, le principe de base de cet algorithme est de garder à disposition, à chaque étape, le couple $(nA, (n+1)A)$ de sorte que leur différence est connue (et même constante égale à A). Si le bit de k à cette étape vaut 0, on calcule $(2nA, (2n+1)A)$ en effectuant un doublement (celui de nA) et une addition de deux éléments dont on connaît la différence (nA et $(n+1)A$) et si le bit vaut 1, on calcule $((2n+1)A, (2n+2)A)$ en effectuant un doublement (celui de $(n+1)A$) et une addition de deux éléments dont on connaît la différence (nA et $(n+1)A$). Il est alors facile de voir que lorsque tous les bits de k ont été décrits, le premier élément du couple est kA. Ainsi, pour chaque bit de la clé, on a bien effectué à la fois un doublement et une addition et on n'a utilisé que les traces de la loi de groupe sur la variété de Kummer.

Cependant les résultats obtenus par une retranscription basique des formules de [Flynn 93] sont décevants en terme d'efficacité. Il m'a donc fallu chercher à optimiser les formules pour réduire leur complexité globale. Le résultat, bien que bien meilleur, n'est toutefois toujours pas comparable avec les complexités obtenues dans [Montgomery 87]. Cela est tout à fait logique puisque Montgomery utilise des courbes elliptiques d'une forme particulière. J'ai donc dû, moi aussi, définir une forme particulière de courbes hyperelliptique de genre 2 bien adaptée à mes formules sans trop perdre en généralité comme l'avait fait Montgomery.

Finalement les formules que j'ai obtenues dans [Duquesne 05] sont compétitives avec les meilleures formules connues pour les courbes hyperelliptiques de genre 2 ([Lange 02]) et apportent en plus une protection contre les attaques par canaux cachés simples.

Pour finir, je me suis plus récemment intéressé à un autre type de protection contre les attaques par canaux cachés. La représentation RNS des

nombres procure en effet aux opérations sur le corps de base une protection contre les attaques par fuite. Il était donc intéressant d'essayer de combiner cette technique avec les techniques de protection au niveau de la courbe évoquées précédemment.

2.3.3 Représentation des nombres par restes modulaires appliquée aux courbes elliptiques

Pour finir, je me suis plus récemment intéressé à un autre type de protection contre les attaques par canaux cachés. La représentation RNS des nombres procure en effet aux opérations sur le corps de base une protection contre les attaques par fuite. Il était donc intéressant d'essayer de combiner cette technique avec les techniques de protection au niveau de la courbe évoquées précédemment.

Le système de représentation des nombres par restes modulaires (RNS) a été introduit dans [Garner 59] et [Szabo-Tanaka 67] et appliqué à la cryptographie dans [Bajard-Didier-Kornuerup 01]. Il présente de nombreux avantages :

- Il est facile à implémenter, notamment en hardware.
- Il est naturellement (et donc efficacement) parallélisable.
- Il procure une protection contre les attaques par canaux cachés sur le corps de base ([Bajard-Imbert-Liardet-Teglia 04]).
- Une même implémentation peut facilement être utilisée pour plusieurs corps de base.

C'est un système basé sur le théorème des restes chinois. Le principe est de représenter un élément de $\mathbb{F}_p$ par ses restes modulo suffisamment de nombres de petite taille. Son intérêt réside dans le fait que les opérations sur des grands nombres sont découpées en des opérations sur des petits nombres qu'on choisira de la taille d'un mot machine pour une efficacité optimale. Ainsi une multiplication de deux nombres de n mots s'effectue en seulement $2n$ multiplications de mots au lieu des n^2 habituelles (pour les tailles de nombres intéressantes en cryptographie elliptique et hyperelliptique). Les choses ne sont malheureusement pas aussi simples. En effet, pour que cette technique s'applique, il faudrait que p soit le produit de nombres de la taille d'un mot machine, or p est premier. Pour contourner cet obstacle on utilise un analogue de la méthode de réduction très utilisée de [Montgomery 85]. Cette méthode utilise une représentation spécifique des éléments de $\mathbb{F}_p$ pour transformer une réduction modulo p en une réduction modulo une puissance de 2 (une simple troncature, donc). Pour le RNS, on construit ainsi un M

supérieur à p, produit de nombres de la taille d'un mot machine, et on utilise la méthode de Montgomery en remplaçant la puissance de 2 par M. On remplace ainsi la réduction modulo p par une réduction modulo M.

En utilisant la représentation des nombres par restes modulaires, la multiplication devient donc de complexité linéaire alors que la réduction reste quadratique. Ainsi la réduction devient l'opération la plus coûteuse. Dans [Bajard-Duquesne-Ercegovac-Meloni 06] nous avons expliqué qu'il était donc intéressant de regrouper les expressions de la forme $AB + CD$ de façon à n'effectuer qu'une seule réduction au lieu de deux. Nous avons appliqué cela aux formules de [Brier-Joye 02]. Cependant, il est possible de faire mieux en optimisant les formules habituellement utilisées pour minimiser non pas le nombre de multiplications mais le nombre de réductions modulaires. Dans [Bajard-Duquesne-Ercegovac 07], nous avons fait ce travail pour toutes les formules sur les courbes elliptiques qui sont protégées contre les attaques par canaux cachés. Les résultats obtenus sont particulièrement intéressants dans le cas des formules de [Brier-Joye 02] utilisant l'algorithme de Montgomery (celui pour la multiplication scalaire sur les courbes elliptiques). En effet, en faisant une fois de plus appel aux outils de la surface de Kummer (plus précisément en n'utilisant pas les mêmes formes biquadratiques que celles qui permettent de retrouver les formules de [Brier-Joye 02]), nous avons obtenu des formules plus adaptées à la représentation RNS, c'est à dire faisant intervenir moins de réductions modulaires au détriment des multiplications. Dans ce même article, nous avons également diminué la complexité de la réduction en RNS par rapport aux travaux antérieurs en regroupant certaines opérations. Ces deux améliorations mises ensemble nous permettent d'obtenir des complexités globales compétitives avec les autres systèmes de représentation des nombres (et même meilleures pour des hauts niveau de sécurité). Étant donnés les avantages apportés par la représentation RNS décrits au début de ce paragraphe, l'utilisation du RNS en cryptographie basée sur les courbes elliptiques devient donc intéressante.

2.3.4 Pistes de futures recherches

Dans cette voie, plus que des pistes, j'ai de nombreux projets de recherche en cours dans la continuité des derniers travaux que j'ai effectués. Je compte ainsi essayer d'appliquer les formules pour la multiplication scalaire de Montgomery en genre 2 obtenues dans [Duquesne 05] à la représentation RNS. La difficulté consistera à réussir à minimiser le nombre de réductions sur des formules bien plus complexes que dans le cas des courbes ellip-

tiques. Dans un avenir très proche, j'ai également l'intention d'utiliser les résultats de [Duquesne 07b] pour développer une méthode de multiplication scalaire de Montgomery pour les courbes de genre 2 définies sur un corps de caractéristique 2. Afin d'améliorer l'efficacité de cet algorithme, je compte m'appuyer sur [Byramjee-Duquesne 04] afin de faire de bons choix de courbes sans trop perdre en généralité.

A plus long terme, un premier projet avec J.C. Bajard consisterait à améliorer la réduction RNS où les changements de base ont un poids déraisonnable et un autre projet utiliserait les résultats que j'ai obtenus sur les variétés de Kummer en genre 3 ainsi que d'éventuelles améliorations pour produire un algorithme de multiplication scalaire de Montgomery en genre 3.

3 Sujets de thèse des doctorants codirigés

Je coencadre 2 doctorants sur des sujets de cryptographie à la frontière entre les mathématiques et l'informatique. Dans les deux cas, Jean Claude Bajard est l'autre coencadrant.

3.1 Nicolas Méloni (2004-2007)

Le sujet de thèse de Nicolas Méloni porte sur l'arithmétique des courbes elliptiques pour la cryptographie. Nous lui avons plus précisément demandé de se concentrer sur les différentes représentations possibles autant au niveau du corps de base qu'au niveau de l'exposant ou de la courbe et d'en déduire de nouveaux algorithmes de multiplication scalaire ou des améliorations aux algorithmes existants.

Son travail le plus important a commencé par le développement de nouvelles formules d'addition sur les courbes elliptiques de deux points ayant la même coordonnée Z en coordonnées Jacobiennes. Ces formules ont l'avantage d'être beaucoup plus efficaces que les formules habituellement utilisées. En contrepartie, il n'est pas trivial de les mettre en oeuvre dans une multiplication scalaire. Il parait en effet hautement improbable que deux points pris au hasard aient la même coordonnée Z et ces formules ne s'appliquent donc jamais. Il remarque toutefois, qu'en effectuant l'opération $P_3 = P_1 + P_2$, il est possible de modifier légèrement ses formules pour qu'en sortie P_1 et P_3 (ou P_2 et P_3) aient la même coordonnée Z. De la sorte, il peut construire une chaîne d'addition où la coordonnée Z des 2 opérandes est la même à chaque étape. Le cas idéal pour une telle chaîne d'addition est le cas où le scalaire

utilisé est un nombre de Fibonacci. Ce n'est bien sûr pas toujours le cas, loin de là. Nicolas Méloni a donc dû utiliser les représentations de Zeckendorf (sommes de nombres de Fibonacci). L'algorithme obtenu marche très bien mais comprend malheureusement plus d'étapes (44% en plus) qu'une multiplication scalaire classique ce qui annule le gain d'efficacité obtenu via ses nouvelles formules. Il a donc dû aller plus loin et utiliser les chaines d'additions euclidiennes. Celles-ci sont une généralisation des chaînes obtenues par la représentation de Zeckendorff et permettent, à chaque étape, de choisir si on additionne P_3 avec P_1 ou avec P_2. Il existe plusieurs façons de représenter un entier en utilisant de telles chaînes et le but est bien sûr de trouver celles qui sont les plus courtes possibles afin de gagner en efficacité. Là encore, la tâche n'est pas aisée. En pratique, Nicolas Méloni obtient finalement un algorithme à peu près compétitif avec les meilleurs algorithmes connus. Il faut en outre noter que, comme seules des additions sont effectuées, cet algorithme est naturellement résistant aux attaques par canaux cachés. Il a également proposé une approche consistant à utiliser des chaînes différentielles et à les adapter à ces nouvelles formules et compte bien continuer dans cette voie pour améliorer son algorithme. Ce travail a donné lieu à plusieurs exposés et à deux publications

New Point Addition Formulae for ECC Applications WAIFI, Lecture Notes in Comput. Sci. **4547** (2007).

SPA resistant Elliptic Curve Cryptosystem using Addition Chains avec A. Byrne, F. Crowe, W. P. Marnane, A. Tisserand et E. M. Popovici, 4th International Conference on Information Technology (2007), pp. 995-1000.

Nicolas Méloni a également effectué plusieurs travaux sur la représentation des nombres par restes modulaires (RNS). J'ai déjà introduit cette technique dans la partie 2.3.3, je me contente donc ici de décrire brièvement les résultats auxquels il a participé. Il a ainsi participé à déterminer des bases de modules particulièrement bien adaptées au RNS en utilisant, pour les modules, des nombres inspirés des nombres premiers de Mersenne ou des pseudo-Mersenne. Il a également pris part à l'élaboration d'un algorithme d'inverse modulaire en RNS qui n'était jusque là pas satisfaisant. Enfin il a travaillé avec moi, entre autres, sur l'intérêt que peut apporter le RNS lorsque des expressions de la forme $\sum A_i B_i$ doivent être calculées. Ces travaux ont également donné lieu à des exposés et à trois publications.

Residue systems efficiency for modular products summation : Application

to Elliptic Curves Cryptography, avec J.-C. Bajard, S. Duquesne et M. Ercegovac, proc. SPIE **6313** (2006), 631304.

Study of modular inversion in RNS, avec J.-C. Bajard et T. Plantard, proc. SPIE **5910** (2005), 59100T.

Efficient RNS Bases for Cryptography avec J.-C. Bajard et T. Plantard, proc. IMACS'2005 World Congress.

3.2 Nadia El Mrabet (2006-2009)

Le sujet de thèse de Nadia El Mrabet est plus particulièrement orienté vers l'utilisation de couplages en cryptographie et des modifications qui pourraient être apportées pour améliorer les algorithmes où ils interviennent. Ces améliorations peuvent être de l'ordre de l'efficacité mais aussi de l'ordre de la robustesse des calculs.

Le couplage de Weil est un outil connu depuis longtemps par les théoriciens des nombres s'intéressant aux courbes elliptiques. Leur intérêt du point de vue de la cryptographie est qu'ils permettent de ramener le problème difficile du logarithme discret sur les courbes elliptiques au problème un peu moins difficile du logarithme discret sur le groupe multiplicatif d'un corps fini. Ils ont ainsi été utilisés pour la première fois en cryptographie au début des années 90 comme moyen d'attaque sur certaines courbes pour lesquelles le logarithme discret sur le corps fini est résoluble. Ce n'est que plus récemment (2000) qu'on s'est rendu compte qu'ils pouvaient aussi être utilisés pour construire de nouveaux protocoles cryptographiques, comme la cryptographie basée sur l'identité, impossibles à réaliser auparavant. Depuis, l'engouement pour ce nouvel outil n'a cessé de croître.

Les deux principaux couplages sont le couplage de Weil, déjà évoqué, et le couplage de Tate qui ont tous deux connu de nombreuses améliorations. Le premier (et pour l'instant unique puisqu'elle n'a fait qu'un an de thèse) travail de Nadia El Mrabet a consisté à comparer deux articles récents (l'un de Koblitz et Menezes et l'autre de Granger, Page et Smart) qui annoncent des résultats contradictoires quant à la supériorité d'un couplage sur l'autre. Elle a ainsi pu, dans un premier temps, se familiariser avec les améliorations les plus récentes sur les couplages. Elle a ensuite essayé d'appliquer les améliorations de l'un aux méthodes de l'autre pour enfin réaliser une comparaison la plus objective possible entre les deux. Son résultat est que le

couplage de Weil est plus intéressant que le couplage de Tate pour les hauts niveaux de sécurité. Elle fournit bien sûr des données chiffrées précises dans son article sur ce sujet.

Pairing in cryptography : an arithmetic point of view, avec J.C. Bajard, proc. SPIE **6697** (2007), 669724.

Elle connaît maintenant donc mieux les subtilités de l'implémentation des couplages et va pouvoir s'intéresser à des sujets plus pointus et encore peu explorés comme par exemple la résistance des algorithmes existants aux attaques par canaux cachés et bien sûr le développement de nouveaux algorithmes plus résistants.

Références

[Bajard-Didier-Kornuerup 01] J.C. Bajard, L.S. Didier, P. Kornerup, *Modular multiplication and base extension in residue number systems*, 15th IEEE Symposium on Computer Arithmetic, IEEE Computer Society Press (2001), pp. 59–65.

[Bajard-Duquesne-Ercegovac 07] J. C. Bajard, S. Duquesne, M. Ercegovac, *Combining leak-resistant arithmetic for elliptic curves defined over* $\mathbb{F}_p$ *and RNS representation*, preprint.

[Bajard-Duquesne-Ercegovac-Meloni 06] J. C. Bajard, S. Duquesne, M. Ercegovac, N. Meloni, *Residue systems efficiency for modular products summation : application to elliptic curves cryptography*, Proc. SPIE **6313** (2006), 631304.

[Bajard-Imbert-Liardet-Teglia 04] J.C. Bajard, L. Imbert, P.Y. Liardet, Y. Teglia, *Leak resistant arithmetic*, CHES 2004, Lecture Notes in Comput. Sci. **3156** (2004), pp. 59–65.

[Billet-Joye 03] O. Billet, M. Joye, *The Jacobi Model of an Elliptic Curve and Side-Channel Analysis*, Applied Algebra, Algorithms and Error-Correcting Codes, Lecture Notes in Comput. Sci. **2643** (2003), pp. 34–42.

[Brier-Joye 02] E. Brier, M. Joye,*Weierstrass Elliptic Curves and Side-Channel Attacks*, Public Key Cryptography, Lecture Notes in Comput. Sci. **2274** (2002).

[Brier-Joye 03] E. Brier, M. Joye, *Fast Point Multiplication on Elliptic Curves Trough Isogenies*, Applied Algebra, Algorithms and Error-Correcting Codes, Lecture Notes in Comput. Sci., **2643** (2003), pp. 43–50.

[Bruin 99] N. Bruin, *On Generalised Fermat Equations*, PhD Dissertation, Leiden (1999).

[Byramjee-Duquesne 04] B. Byramjee, S. Duquesne, *Classification of genus 2 curves over $\mathbb{F}_2^n$ and optimization of their arithmetic*, e-smart 2003 et Cryptology ePrint Archive, no. 107 (2004).

[Cassels-Flynn 96] J. W. S. Cassels, E. V. Flynn, *Prolegomena to a middlebrow Arithmetic of Curves of Genus 2*, LMS Lecture Note Series, **230**, Cambridge University Press (1996).

[Chabauty 41] C. Chabauty, *Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension*, C. R. A. S. Paris, **212** (1941), pp. 1022–1024.

[Cohen-et-al 06] H. Cohen et al. *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Math. Appl., Chapman & Hall/CRC (2006).

[Coron 99] J. S. Coron, *Resistance against differential power analysis for elliptic curve cryptosystems*, CHES'99, Lecture Notes in Comput. Sci. **1717** (1999), pp. 292–302.

[Delaunay 01] C. Delaunay, *Heuristics on Tate-Shafarevitch groups of elliptic curves defined over $\mathbb{Q}$*, Exp. Math. **10** (2001), no. 2, 191–196.

[Delaunay-Duquesne 03] C. Delaunay, S. Duquesne, *Numerical investigations related to the derivatives of the L-series of certain elliptic curves*, Experimental Mathematics **12 :3** (2003), pp. 311-317.

[Duquesne 01] S. Duquesne, *Integral points on elliptic curves defined by simplest cubic fields*, Experimental Mathematics **10 :1** (2001), pp. 91–102.

[Duquesne 02a] S. Duquesne, *Rational Points on Hyperelliptic Curves and an explicit Weierstrass Preparation Theorem*, Manuscripta Mathematica, **108** (2002), pp. 191–204.

[Duquesne 02b] S. Duquesne, *Hauteurs et descente infinie sur les courbes hyperelliptiques*, Publications Mathématiques de Besançon en théorie des nombres (2002), pp. 35–41.

[Duquesne 03] S. Duquesne, *Points rationnels et méthode de Chabauty elliptique*, Journ. Théor. Nombres Bordeaux **15 :1** (2003), pp. 99–113.

[Duquesne 05] S. Duquesne, *Montgomery scalar multiplication for genus 2 curves*, ANTS VI, Lecture Notes in Comput. Sci. **3076** (2004), pp. 153–168.

[Duquesne 07a] S. Duquesne, *Elliptic curves associated with simplest quartic fields*, Journ. Théor. Nombres Bordeaux, **19 :1** (2007), pp. 81–100.

[Duquesne 07b] S. Duquesne, *Improving the arithmetic of elliptic curves in the Jacobi model*, Information Processing Letters **104 :3** (2007), pp. 101–105.

[Duquesne 07b] S. Duquesne, *Traces of the group law on the Kummer surface of a curve of genus 2 in characteristic 2*, soumis.

[Faltings 83] G. Faltings, *Endlichtkeitssästze für abelsche Varietäten über Zahlenkörpen*, Inv. Math. **73** (1983), pp. 349–366.

[Flynn 93] E. V. Flynn, *The group law on the Jacobian of a curve of genus* 2, J. reine angew. Math., **439** (1993), pp. 45–69.

[Flynn 95] E. V. Flynn, *An explicit theory of heights*, Trans. Amer. Math. Soc., **347** (1995), pp. 3003–3015.

[Flynn 97] E. V. Flynn, *A flexible method for applying Chabauty's Thorem*, Compositio Math., **105** (1997), pp. 79–94.

[Flynn 01] E. V. Flynn, *On* $\mathbb{Q}$*-Derived Polynomials*, Proc. Edinburgh Math. Soc. **44 :1** (2001), pp. 103–110.

[Flynn-Smart 97] E. V. Flynn, N. P. Smart, *Canonical height on the Jacobians of curves of genus 2 and the infinite descent*, Acta Artih., **79 :4** (1997), pp. 333–352.

[Flynn-Wetherell 99] E. V. Flynn, J. L. Wetherell, *Finding rational points on bielliptic genus* 2 *curves*, Manuscripta Math., **100** (1999), pp. 519–533.

[Flynn-Wetherell 01] E. V. Flynn, J. L. Wetherell, *Covering Collections and a Challenge Problem of Serre*, Acta Arith., **98 :2** (2001), pp. 197–205.

[Garner 59] H.L. Garner, *The residue number system*, IRE Transactions on Electronic Computers, EL **8 :6** (1959), pp. 140–147.

[Gebel-Pethö-Zimmer 94] J. Gebel, A. Pethö, H. G. Zimmer, *Computing integral points on elliptic curves*, Acta Arith. **68 :2** (1994), pp. 171–192.

[Kocher 96] P. C. Kocher, *Timing attacks on implementations of DH, RSA, DSS and other systems*, CRYPTO'96, Lecture Notes in Comput. Sci. **1109** (1996), pp. 104–113.

[Kocher-Jaffe-Jun 99] P. C. Kocher, J. Jaffe, B. Jun, *Differential power analysis*, CRYPTO'99, Lecture Notes in Comput. Sci. **1666** (1999), pp. 388–397.

[Lange 02] T. Lange, *Weighted Coordinates on Genus 2 Hyperelliptic Curves*, Cryptology ePrint Archive, **153** (2002).

[Liardet-Smart 01] P. Y. Liardet, N. Smart, *Preventing SPA/DPA in ECC systems using the Jacobi form*, CHES 2001, Lecture Notes in Comput. Sci. **2162** (2001), pp. 391–401.

[Montgomery 85] P.L. Montgomery, *Modular multiplication without trial division*, Math. Comp. **44** (1985), pp. 519–521.

[Montgomery 87] P. L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization*, Math. Comp. **48** (1987), pp. 243–164.

[Quisquater-Samyde 01] J. J. Quisquater, D. Samyde, *ElectroMagnetic Analysis (EMA) : Measures and Countermeasures for Smart Cards*, e-smart 2001, Lecture Notes in Comput. Sci. **2140** (2001), pp. 200–210.

[Shanks 74] D. Shanks, *The simplest cubic fields*, Math. Comp. **28** (1974), pp. 1137–1152.

[Siksek 95] S. Siksek, *Infinite descent on elliptic curves*. Rocky Mountain J. Math. **25 :4** (1995), pp. 1501–1538.

[Smart 94] N. P. Smart, *S-integral points on elliptic curves*, Math. Proc. Cambridge Philos. Soc., **116 :3** (1994), pp.391–399.

[Stroeker-Tzanakis 94] R. J. Stroeker, N. Tzanakis, *Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms*, Acta Arith., **67 :2** (1994), pp. 177-196.

[Stubbs 00] A. Stubbs, *Hyperelliptic Curves*, Thesis, University of Liverpool (2000).

[Szabo-Tanaka 67] N.Z. Szabo, R.I. Tanaka, *Residue Arithmetic and its Applications to Computer Technology*, McGraw-Hill (1967).

[Washington 87] L. C. Washington, *Class Numbers of the Simplest Cubic Fields*, Math. Comp., **48 :177** (1987), pp. 371–384.

[Watkins 07] M. Watkins,*Rank distribution in a family of cubic twists*, in Ranks of Elliptic Curves and Random Matrix Theory, edited by J. B. Conrey, D. W. Farmer, F. Mezzadri, and N. C. Snaith, London Mathematical Society Lecture Note Series **341** (2007), pp. 237–246.

[Zagier-Kramarz 87] D. Zagier and G. Kramarz, *Numerical investigations related to the L–series of certain elliptic curves*, Journal of the Indian Math. Soc. **52** (1987), pp. 51–69.

Sélection des travaux les plus importants

1. *Integral Points on Elliptic Curves Defined by Simplest Cubic Fields*, Experimental Mathematics **10 :1** (2001), pp. 91-102.
2. *Rational Points on Hyperelliptic Curves and an explicit Weierstrass Preparation Theorem*, Manuscripta Mathematica, **108** (2002), pp. 191-204.
3. Numerical investigations related to the derivatives of the L-series of certain elliptic curves, avec C. Delaunay, Experimental Mathematics **12 :3** (2003), pp. 311-317.
4. *Classification of genus 2 curves over $\mathbb{F}_2^n$ and optimization of their arithmetic*, avec B. Byramjee, e-smart 2003 et Cryptology ePrint Archive, no. 107 (2004).
5. Montgomery scalar multiplication for genus 2 curves, ANTS VI, Lecture Notes in Comput. Sci. **3076** (2004), pp. 153-168.
6. *Elliptic curves associated with simplest quartic fields*, Journ. Théor. Nombres Bordeaux, **19 :1** (2007), pp. 81-100.
7. *Improving the Arithmetic of Elliptic Curves in the Jacobi Model*, Information Processing Letters **104 :3** (2007), pp. 101-105.
8. *Combining leak-resistant arithmetic for elliptic curves defined over $\mathbb{F}_p$ and RNS representation*, avec J. C. Bajard et M. Ercegovac, soumis.
9. *Traces of the group law on the Kummer surface of a curve of genus 2 in characteristic 2*, soumis.

Integral Points on Elliptic Curves Defined by Simplest Cubic Fields

Sylvain Duquesne

CONTENTS

Let f(X) be a cubic polynomial defining a simplest cubic field in the sense of Shanks. We study integral points on elliptic curves of the form $Y^2 = f(X)$. We compute the complete list of integral points on these curves for the values of the parameter below 1000. We prove that this list is exhaustive by using the methods of Tzanakis and de Weger, together with bounds on linear forms in elliptic logarithms due to S. David. Finally, we analyze this list and we prove in the general case the phenomena that we have observed. In particular, we find all integral points on the curve when the rank is equal to 1.

INTRODUCTION

Let m be a positive integer such that

$$\Delta := m^2 + 3m + 9$$

is squarefree. Denote by $\mathbb{K}_m$ the cubic field defined by the polynomial

$$f(X) = X^3 + mX^2 - (m{+}3)X + 1,$$

which is irreducible over $\mathbb{Q}$. The field $\mathbb{K}_m$ is said to be a *simplest cubic field* [Shanks 1974].

These fields have often been studied because their regulator is explicit and as small as possible, hence their class number is particularly large.

In this work, we are interested in elliptic curves defined by equation

$$E_m : Y^2 = X^3 + mX^2 - (m{+}3)X + 1 \qquad (0\text{–}1)$$

where m is an integer defining a simplest cubic field. We first want to find all the integral points on these curves for m below 1000. We then conjecture what should be true in general and finally we prove these conjectures. The main results are about the point $[0, 1]$: we prove that it is a generator of the Mordell–Weil group and we find all its integral multiples.

1058-6458/2001 $0.50 per page

1. ELLIPTIC CURVES DEFINED BY SIMPLEST CUBIC FIELDS

The discriminant of the curve E_m defined by (0–1) is $16\Delta^2$ (recall that $\Delta = m^2+3m+9$ is assumed squarefree). If m is even, the conductor is $16\Delta^2$; if $m \equiv 1 \pmod 4$, the conductor is $8\Delta^2$; and if $m \equiv 3 \pmod 4$, it is $4\Delta^2$. Since the discriminant is always positive, the curve $E(\mathbb{R})$ has two connected components. Denote by $E^0(\mathbb{R})$ the connected component of the identity and by $E_{gg}(\mathbb{R})$ (as in "egg") the compact part of $E(\mathbb{R})$.

We first state a theorem of L. Washington.

Let Cl be the ideal class group of the simplest cubic field $\mathbb{K}_m$ and set

$$\mathrm{Cl}_2 = \{x \in \mathrm{Cl} : x^2 = 1\}$$

. The 2-rank $\mathrm{rk}_2(\mathrm{Cl}_2)$ will denote its dimension as a $\mathbb{Z}/2\mathbb{Z}$-vector space. Note that since $\mathbb{K}_m$ is a cyclic cubic field, $\mathrm{rk}_2(\mathrm{Cl}_2)$ is even. Finally, let Ш_2 denote the 2-torsion of the Tate–Shafarevitch group of $E_m(\mathbb{Q})$.

Theorem 1.1 [Washington 1987]. *The rank* $\mathrm{rk}\, E_m(\mathbb{Q})$ *is at most* $1 + \mathrm{rk}_2\, \mathrm{Cl}_2$. *In fact, there is an exact sequence*

$$1 \to E_m^0(\mathbb{Q})/2E_m(\mathbb{Q}) \to \mathrm{Cl}_2 \to \text{Ш}_2 \to 1.$$

From this theorem, Washington deduces the following corollary.

Corollary 1.2. *Let m be a positive integer such that $m^2 + 3m + 9$ is squarefree, then the rank of the elliptic curve E_m is odd, assuming that the Tate–Shafarevitch group is finite.*

Theorem 1.1 tells us that the search for such curves having large rank is equivalent to the search for simplest cubic fields whose class group has a large 2-rank. Several people have tried to find quadratic fields with large 3-rank which is the corresponding problem in degree 2. Moreover, since the class number of K_m is expected to be large, if Ш_2 is small with respect to Cl_2, we can thus also expect the rank of E_m to be large.

Proposition 1.3. *If m is a positive integer such that m^2+3m+9 is squarefree, the group $E_m(\mathbb{Q})$ is torsionfree.*

Proof. Easy, using the well-known fact that $E_m(\mathbb{Q})_{\mathrm{tor}}$ can be embedded in $E_m(\mathbb{F}_p)$ when p is a prime of good reduction. □

We now give a method using elliptic logarithms for searching for integral points on elliptic curves. This method was suggested by Lang [1978, Chapter VI, § 8] and Zagier [1987] and was simultaneous developed by several researchers [Stroeker and Tzanakis 1994; Gebel et al. 1994; Smart 1994]. The algorithm requires the knowledge of a basis of the Mordell–Weil group, as calculated for example by `mwrank` [Cremona 1998], and of an explicit lower bound for linear forms in elliptic logarithms, as given in [David 1995]. For a general point of view and more details, see [Smart 1998].

2. LINEAR FORMS IN ELLIPTIC LOGARITHMS

Let E be an elliptic curve given by its Weierstrass equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

with $a_i \in \mathbb{Z}$. This curve is isomorphic over $\mathbb{Q}$ to curve of the form

$$Y^2 = 4X^3 - g_2X - g_3.$$

Let Λ be the lattice associated to E. We call ω_1 and ω_2 the periods of this lattice and $\wp$ the associated Weierstrass function. Note that we can always choose $\omega_1 \in \mathbb{R}$ and $\mathrm{Im}(\omega_1/\omega_2) > 0$.

We have the map φ from $\mathbb{C}/\Lambda$ to E defined by $\Phi(z) = \infty$ if $z \in \Lambda$ and $\varphi(z) = P = \big(x(z), y(z)\big)$ otherwise, with

$$x(z) = \wp(z) - \tfrac{1}{12}b_2, \quad y(z) = \tfrac{1}{2}(\wp'(z) - a_1x - a_3).$$

Let ψ be the inverse function of φ. It is given (modulo Λ) by

$$\psi(P) = \int_{\infty}^{x+b_2/12} \frac{dt}{\sqrt{4t^3 - g_2t - g_3}}.$$

This function is called the *elliptic logarithm* because it satisfies

$$\psi(P+Q) = \psi(P) + \psi(Q) \qquad (\mathrm{mod}\ \Lambda)$$

for all $P, Q \in E(\mathbb{Q})$. Henceforth, we take the fundamental region

$$\{a\omega_1 + b\omega_2 : a, b \in \mathbb{R},\ 0 < a \le 1,\ 0 \le b < 1\}.$$

To compute this function, we use the link between elliptic integrals and the AGM [Cohen 1993].

We now define the canonical height in order to fix notations.

If $P = (x, y) \in E(\mathbb{Q})$ and $x = p/q$ with $(p, q) = 1$, we define

$$h(P) = h(x(P)) = \log \max\{|p|, |q|\}.$$

This height can be modified to obtain the canonical height

$$\hat{h}(P) = \tfrac{1}{2} \lim_{N\to\infty} 4^{-N} h(2^N P).$$

It is possible to bound the difference between these heights:

Lemma 2.1 [Silverman 1990]. *There exist constants e_1 and e_2 such that*

$$-e_1 \le \hat{h}(P) - \tfrac{1}{2}h(P) \le e_2.$$

In our case, we can choose

$$e_2 = 1.57 + \frac{\log(m^2+3m+9)}{4} + \frac{\log m}{2} \text{ if } m \ge 9.$$

We now give a simplified version of S. David's result [1995] which allows us to give lower bounds for linear forms in elliptic logarithms.

Let E be an elliptic curve given by the equation

$$Y^2 = 4X^3 - g_2X - g_3$$

with invariant j and periods ω_1 and ω_2 such that $\omega_1 \in \mathbb{R}$ and $\mathrm{Im}(\omega_1/\omega_2) > 0$. Let $P_1, \ldots, P_n$ denote n points on E. We define the height

$$h_E = \max(1, h_2(1, g_2, g_3), h(j)),$$

of the elliptic curve, where h_2 denotes the absolute logarithmic height on $\mathbb{P}^2_{\mathbb{Q}}$; the constant

$$d_1 = \frac{3\pi}{|\omega_1|^2 \,\mathrm{Im}(\omega_1/\omega_2)};$$

the modified height

$$h_m(P_i) = \max\{2\hat{h}(P_i), h_E, d_1|\psi(P_i)|^2\};$$

and constants $d_2 = \max\{eh_E, h_m(P_1), \ldots, h_m(P_n)\}$,

$$d_3 = \min_{1\le i\le n}\left\{\frac{e\sqrt{h_m(P_i)}}{\sqrt{d_1}\,|\psi(P_i)|}\right\},$$

and

$$d_4 = 2.10^{8+7n}\left(\frac{2}{e}\right)^{2n^2} \times (n+1)^{4n^2+10n}(\log d_3)^{-2n-1}\prod_{i=1}^{n} h_m(P_i).$$

Theorem 2.2 [David 1995]. *Let $L(x) = \sum_{i=1}^n x_i\psi(P_i)$ with $x \in \mathbb{Z}^n$, and set $A = \max|x_i|$. If $L(x) \ne 0$ and $A \ge \exp(d_2)$, then*

$$\log|L(x)| > -d_4(\log A + \log d_3)(\log\log A + h_E + \log d_3)^{n+1}.$$

3. COMPUTATION OF INTEGRAL POINTS

Let E be an elliptic curve associated to a simplest cubic field. We assume that we have computed a basis $P_1, P_2, \ldots, P_n$ for the Mordell–Weil group. Since the sum of two points in $E^0(\mathbb{R})$ is still in $E^0(\mathbb{R})$, the sum of two points in $E_{gg}(\mathbb{R})$ is in $E^0(\mathbb{R})$ and $[0, 1] \in E_{gg}(\mathbb{R})$, we shall assume that P_1 and only P_1 belongs to $E_{gg}(\mathbb{R})$.

Let P be an integral point. Since $E(\mathbb{Q})$ is torsionfree, we have $P = p_1P_1 + \cdots + p_nP_n$ for some $p_i \in \mathbb{Z}$. It is easy to compute integral points in $E_{gg}(\mathbb{Q})$. Hence we now assume that the point P belongs to $E^0(\mathbb{R})$. Set

$$\begin{aligned} Q_1 &= 2P_1 \in E^0(\mathbb{R}),\\ q_1 &\in \mathbb{Z} \text{ such that } p_1 = 2q_1 + r, \text{ for } r = 0 \text{ or } 1,\\ Q_i &= P_i,\\ q_i &= p_i \text{ for } i \ne 1,\\ Q_{n+1} &= P_1, \end{aligned}$$

so that

$$P = q_1Q_1 + \cdots + q_nQ_n + rQ_{n+1}.$$

The points $P, Q_1, \ldots, Q_n$ being in $E^0(\mathbb{R})$, their sum also belongs to $E^0(\mathbb{R})$, hence $r = 0$.

Now set $H = \max|q_i|$. Our purpose is to find an upper bound for H. We first need to link H with the x-coordinate of P.

Proposition 3.1. *If $P = (x, y)$ is an integral point,*

$$\frac{1}{|x|} \le c_1 e^{-c_2H^2},$$

where $c_1 = \exp e_2$ (see Lemma 2.1) and c_2 is the smallest eigenvalue of the regulator matrix

$$[\hat{h}(Q_i + Q_j) - \hat{h}(Q_i) - \hat{h}(Q_j)]_{1\le i,j\le n}.$$

We now need to link the x-coordinate of P with its elliptic logarithm. As we have seen before, the curve E is isomorphic to a curve of the form

$$Y^2 = 4X^3 - g_2X - g_3 = g(X).$$

Let γ_1, γ_2, γ_3 denote the roots of $g(X)$. Set $c_4 = 2\max|\gamma_i|$.

Proposition 3.2. *If $P=(x,y)\in E^0(\mathbb{R})$ and $|x+b_2/12|>c_4$, then*

$$|\psi(P)|^2 \le \frac{c_5}{|x|}$$

with $c_5 = 8+|\omega_1^2|/12$.

Using the elliptic logarithm property and since iQ_i lies in $E^0(\mathbb{R})$ for all i, we have

$$\psi(P) - q_1\psi(Q_1) - \cdots - q_n\psi(Q_n) = m\omega_1$$

with $|m| \le nH+1$. We have $\omega_1 = \psi(\infty)$, hence $q_1\psi(Q_1)+\cdots+q_n\psi(Q_n)+m\omega_1$ is a linear form in elliptic logarithms. David's result allows us to obtain a lower bound for $\psi(P)$. Comparing this bound with the upper bound obtained by Propositions 3.1 and 3.2, we deduce a very large upper bound H_0 for H. We now seek to reduce this bound. For this, we consider the following problem: suppose we are given n real numbers $\alpha_1,\ldots,\alpha_n$, two positive real constants c_6 and c_7 and a linear form

$$L(x) = \sum_{i=1}^{n} x_i\alpha_i$$

where the x_i are integers bounded by nH_0+1.

We would like to deduce from the inequality

$$|L(x)| \le c_6 e^{-c_7 H^2}$$

a bound for H. In other words, we would like to show that the linear form cannot become too small if its coefficients are bounded.

This problem was studied by Baker and Davenport [1969] in the case $n=2$. There exist several ways to generalize their method. We give here the one most used in recent years.

The basic idea (due to de Weger) is to approximate the linear form by an approximation lattice and to find a reduced basis for this lattice. The first vector of this new basis gives an approximation to the smallest vector in the lattice. So it tells us when the linear form is small.

Consider the lattice Λ generated by the columns of the matrix

$$A = \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ 0 & & 1 & 0 \\ \lfloor C\alpha_1\rfloor & \cdots & \lfloor C\alpha_{n-1}\rfloor & \lfloor C\alpha_n\rfloor \end{pmatrix} \in \mathcal{M}_{n,n}(\mathbb{Z}).$$

We choose the constant C approximately equal to $(nH_0)^n$. Thus the determinant of A will be of the order of $(nH_0)^n$ and we hope that the first basis element in an LLL-reduced lattice will be of order nH_0.

Proposition 3.3. *Let $B=(b_1,\ldots,b_n)$ be a reduced basis for the lattice, B^* the associated Gram-Schmidt basis, $c_8 = \min\{\|b_i^*\| : 1\le i\le n\}$, $S=\sum_{i=1}^{n-1}X_i^2$ and $T=\frac{1}{2}\sum_{i=1}^{n}X_i$. If $c_8^2 \ge T^2+S$ and $x = {}^t(x_1,\ldots,x_n)\ne 0$ then*

$$H \le \sqrt{\left(\log(Cc_6) - \log\left(\sqrt{c_8^2-S}-T\right)\right)/c_7}.$$

Remark. If the bound for H exists, it is of the form $O\left(\sqrt{\log H_0}\right)$. If the method fails (i.e., if the condition on c_8 is not satisfied), we increase the constant C and repeat the algorithm.

Hence, this method allows us to reduce the bound to $O\left(\sqrt{\log H_0}\right)$. The new bound is generally small enough to enumerate all the possibilities for integral points. However, if this bound seems to large, we repeat the algorithm.

4. TABLES OF RESULTS

Tables 1–3 show results obtained by this method. For all $m\le 1000$ such that m^3+3m+9 is squarefree, we found the rank $\operatorname{rk} E_m(\mathbb{Q})$. Where possible, the basis of the Mordell–Weil group was computed using `mwrank` [Cremona 1998]. In some cases, distinguished in the tables by an underlined value of the parameter m, `mwrank` cannot conclude about the rank; we then computed the rank using the Birch and Swinnerton-Dyer conjecture.

The tables are separated by rank. Tables 2 and 3 list the x-coordinate of each integral point in $E_0(\mathbb{R})$. Examination shows that there are always integral points in $E_0(\mathbb{R})$ with a positive x-coordinate when m is odd and never when m is even.

When the rank is 1, the point $[0,1]$ seems to be a basis for the Mordell–Weil group and there does not exist any other integral point than $[0,1]$ and its double when m is odd. So Table 1 gives only the list of the values of the parameter m when the rank is 1. More generally, $[0,1]$ seems to always be a generator. (This last remark is valid only if the parameter m defines a simplest cubic field, as we have assumed;

000 +	1 2 4 7 8 10 13 14 16 19 20 22 28 31 32 34 35 37 38 40 43 46 47 49 50 52 53 56 58 61 62 65 68 70 73 74 76 77 79 80 82 86 88 89 91 92 94 97 98
100 +	4 6 7 9 10 12 15 16 19 21 22 24 25 28 31 34 40 45 48 55 58 60 61 64 67 $\underline{70}$ 72 73 75 78 82 $\underline{84}$ 85 90 93 96 97 99
200 +	0 2 3 5 6 8 9 11 12 14 15 17 21 24 26 32 33 38 39 41 44 45 47 51 53 54 56 57 59 60 $\underline{62}$ 65 66 68 72 78 $\underline{80}$ 81 $\underline{84}$ 89 $\underline{90}$ 93 95 96 98
300 +	$\underline{1}$ 2 4 10 13 14 16 17 19 20 22 23 25 26 28 31 $\underline{32}$ $\underline{34}$ 37 38 40 43 44 46 49 $\underline{52}$ 53 55 61 62 64 67 68 $\underline{70}$ 73 76 79 80 $\underline{82}$ 83 85 86 88 92 94
400 +	1 3 9 10 $\underline{12}$ 13 15 16 $\underline{18}$ 21 22 24 25 $\underline{27}$ 30 31 36 37 43 45 48 $\underline{49}$ 51 52 $\underline{54}$ 55 $\underline{60}$ 63 64 66 67 69 76 78 81 84 85 87 88 90 93 $\underline{96}$ 97
500 +	$\underline{2}$ $\underline{5}$ 6 8 9 $\underline{14}$ 18 20 21 $\underline{24}$ 26 27 29 30 36 39 41 $\underline{47}$ 50 51 53 54 $\underline{56}$ $\underline{60}$ 62 63 66 68 69 72 74 81 86 87 89 90 92 95 96 98 99
600 +	1 4 5 8 10 13 $\underline{14}$ 20 22 23 28 31 32 34 35 38 40 43 $\underline{46}$ 47 50 52 56 58 59 61 62 64 65 67 70 73 74 76 77 79 80 $\underline{82}$ 85 86 88 89 92 94 95 97
700 +	0 3 6 7 13 15 18 21 25 28 30 31 33 $\underline{34}$ 36 39 43 46 $\underline{48}$ 49 51 52 54 55 57 60 61 63 64 66 67 69 70 $\underline{72}$ 75 78 79 81 82 85 87 88 90 $\underline{94}$ 97 99
800 +	2 $\underline{5}$ 11 12 14 17 18 $\underline{20}$ 21 23 26 27 29 $\underline{32}$ 33 36 41 $\underline{42}$ 47 50 51 53 54 57 59 60 62 63 65 66 68 69 71 72 77 81 83 84 86 89 90 $\underline{92}$ 93 $\underline{95}$ 96 98
900 +	1 2 5 7 8 10 13 16 17 19 20 $\underline{22}$ 25 29 31 32 35 $\underline{37}$ 40 $\underline{44}$ 46 47 49 50 52 53 55 $\underline{62}$ $\underline{64}$ 65 67 68 $\underline{71}$ 73 74 76 79 80 86 88 94 97 98
1000	

TABLE 1. Values of $m \leq 1000$ such that $\mathbb{K}_m$ is a simplest cubic field and for which the rank of $E_m(\mathbb{Q})$ equals 1, as computed by `mwrank` [Cremona 1998], or, in the underlined cases, by the use of the Birch–Swinnerton-Dyer conjecture. Each row represents a range $100k \leq m < 100(k+1)$. In all these cases the point $[0,1]$ is a generator, so the integral points are given by Theorem 5.

it is false for $m = 5$, for instance.)

The remainder of this paper is devoted to proving these and other general results for the curves E_m defined by simplest cubic fields. In particular, we prove that $[0,1]$ is always a generator (Theorem 5.7 below) and that there are no other integral points on E_m that are positive multiples of $[0,1]$, apart from $2[0,1]$ when m is odd (Theorem 5.8).

5. GENERAL RESULTS ABOUT INTEGRAL POINTS ON THE ELLIPTIC CURVES $y^2 = x^3 + mx^2 - (m+3)x + 1$

Several papers have considered the problem of solving parametrized Diophantine equations. In particular for Thue equations see [Pethő 1991; Niklasch and Smart 1998]. In this paper, we obtain some interesting results on parametrized elliptic curves. All the curves in our family have the integral point $[0,1]$ however, and this is essential in the following. Hence it should be possible to extend our method to other parametrized curves having a fixed nontorsion point.

5A. Arithmetic Study of Integral Points

First we show that when the parameter m is even there is no integral point in the non-compact part of the curve E_m.

Lemma 5.1. *If m is even and if $[x,y]$ is an integral point, then $x \equiv 0 \pmod 8$.*

Proof. Set $m = 2k$, so that we have $y^2 = x^3 + 2kx^2 - (2k+3)x + 1$. Then, if x is even then y^2 is odd. The only odd square modulo 8 is 1, so $(2k+3)x \equiv 0 \pmod 8$. Since $2k+3$ is invertible modulo 8, we obtain $x \equiv 0 \pmod 8$. If x is odd, a similar argument leads to a contradiction. □

Lemma 5.2. *If m is odd and $[x,y]$ is an integral point, then 4 does not divide $|x-1|$.*

Proof. Similar to the previous proof. □

Theorem 5.3. *Let x be an integer. Set $a = x^2 - x$ and $b = x^3 - 3x + 1$. There exists m such that $am + b$ is a square if and only if every odd prime dividing $|x-1|$ is congruent to 1 modulo 4 and if in addition 4 does not divide $|x-1|$.*

Proof. Note that b is coprime to x and to $x-1$, hence to a. Thus, there exists m such that $am+b$ is a square if and only if b is a square modulo a; that is, if and only if for all prime divisor p of a, b is a square modulo $p^{v_p(a)}$ (where as usual $v_p(a)$ denotes the p-adic valuation of the nonzero integer a).

Using Hensel's lemma, if $p \neq 2$, we know that b is a square modulo p^n for every integer n if and only if b is a square modulo p.

143	−144, −124, −105, −81, −64, −33, −28, −4, −1, 0, 2, 6, 30, 90, 114, 182, 290, 846, 854, 4182, 5186, 17342, 414290
347	−345, −292, −225, −84, −64, −12, −4, 0, 6, 26, 98, 1190, 5070, 14930, 30278
419	−420, −280, −225, −196, −64, −33, −1, 0, 2, 6, 14, 366, 482, 594, 44102
439	−408, −276, −105, −9, 0, 42, 54, 222, 270, 966, 30090, 48402
473	−456, −364, −240, −60, −16, −4, 0, 27, 51, 107, 899, 2315, 56171
611	−612, −537, −324, −289, −280, −184, −9, −1, 0, 2, 74, 266, 546, 686, 1650, 8502, 93638, 1313274

TABLE 2. Parameter m and x-coordinate of integral points when the rank is 5, as determined by `mwrank`.

11	−12, −9, −4, −1, 0, 2, 6, 26, 30, 38, 3170, 7502
17	−12, −4, 0, 3, 35, 83
23	−24, −16, −9, −1, 0, 2, 14, 42, 146
25	−12, 0, 3, 51, 171
26	−24, −16, 0
29	−28, −4, 0, 11, 227
44	−40, −16, 0
55	−12, 0, 6, 126, 786
59	−60, −36, −25, −1, 0, 2, 42, 86, 902
64	−24, 0
67	−57, −9, 0, 6, 1158
71	−52, −4, 0, 14, 1298
83	−84, −49, −36, −1, 0, 2, 62, 114, 1766
85	−24, 0, 3, 1851
95	−84, −4, 0, 30, 2306
101	−40, 0, 3, 2603
113	−84, −4, 0, 35, 3251
118	−96, 0
127	−60, 0, 186, 4098
130	−72, 0
133	−24, 0, 4491
136	0
137	−40, 0, 3, 4763
142	−72, 0
146	−40, 0
149	−136, −16, 0, 11, 5627
151	0, 66, 5778
157	−84, −60, −12, 0, 3, 6243
163	−156, −36, 0, 6726
166	−24, 0
169	−168, −144, 0, 7227
176	−88, 0
179	−180, −100, −81, −1, 0, 2, 146, 222, 8102
181	−96, 0, 8283
187	−177, −9, 0, 18, 8838
191	−28, 0, 6, 9218
194	0
218	−88, 0
220	0
223	−33, 0, 6, 12546
227	−172, −4, 0, 66, 12998
229	0, 75, 13227
230	0
236	0
242	−64, 0
248	−88, 0
263	−264, −144, −121, −1, 0, 2, 222, 314, 17426
274	0
275	−12, 0, 26, 3770, 12630, 19046
277	−84, 0, 3, 19323
283	0, 174, 20166
287	−129, 0, 20738
292	−240, 0
305	−112, 0, 3, 23411
307	−57, 0, 6, 23718
308	0
311	−312, −169, −144, −1, 0, 2, 266, 366, 24338
329	0, 35, 627, 27227
341	−28, 0, 11, 29243
350	−24, 0
358	0
359	0, 114, 32402
365	−112, 0, 3, 33491
371	−24, 0, 14, 34598
377	−12, 0, 35, 35723
389	−376, −16, 0, 27, 38027
391	−84, 0, 34146, 38418
395	−60, 0, 1890, 39206
400	−192, 0
406	−168, 0
407	−385, −25, 0, 18, 41618
428	−24, 0
434	0
440	−40, 0
442	0
457	−240, 0, 52443
458	−40, 0
461	−12, 0, 35, 53363
470	0
472	0
475	−57, 0, 56646
479	−480, −256, −225, −1, 0, 2, 422, 546, 57602
491	−465, −25, 0, 18, 60518
494	−456, −16, 0
499	0, 30, 62502
500	0
503	−33, 0, 14, 63506
511	0, 102, 65538
512	0
517	−12, 0, 67083
523	−108, 0, 68646
532	−504, 0
533	−444, −4, 0, 147, 71291
535	0, 66, 71826
538	0
542	−280, 0
545	−40, 0, 74531
548	0
557	0, 555, 77843
559	−33, 0, 78402
571	−564, −36, 0, 81798
575	−444, −4, 0, 158, 82946
578	0
583	−105, 0, 6, 85266
584	0
616	−504, 0
617	−220, −52, 0, 3, 11, 95483
619	−96, 0, 6, 96102
625	0, 97971
626	−616, 0
637	−24, 0, 101763
641	−532, −4, 0, 147, 103043
644	−304, 0
649	0, 105627
653	−28, 0, 106931
655	−12, 0, 107586
668	−264, 0
671	−364, 0, 1470, 112898
683	−684, −361, −324, −1, 0, 2, 614, 762, 116966
698	−184, 0
701	−220, 0, 3, 123203
704	−688, −64, 0
709	0, 151, 126027
710	0
712	−24, 0
719	−633, −9, 0, 74, 129602
722	−304, 0
724	−288, 0
737	−72, 0, 11, 136163
745	−264, 0, 3, 139131
758	−240, 0
773	−348, 0, 149771
784	0
791	0, 156818
793	−156, 0, 3771, 157611
796	−336, 0
800	0, −112, 0
803	−744, −16, 0, 54, 161606
806	−480, 0
808	0
809	−628, −4, 0, 219, 164027
815	−145, 0, 6, 166466
824	0
830	−184, −40, 0
835	−792, 0, 174726
839	−840, −441, −400, 0, −1, 2, 762, 926, 176402
845	−72, 0, 11, 178931
848	−280, 0
856	−24, 0
875	−52, 0, 18, 10626, 191846
878	−168, 0
880	−240, 0
899	0, 202502
904	0
914	−376, 0
928	0
934	0
938	0
941	−732, −4, 0, 219, 221843
943	−660, −129, −24, 0, 42, 222786
956	0
958	−264, 0
959	−73, 0, 14, 230402
961	−12, 0, 75, 291, 231363
970	−792, 0
977	0, 203, 10131, 239123
982	−840, 0
983	−33, 0, 242066
989	−168, 0, 245027
991	−156, 0, 6, 246018
995	−52, 0, 18, 248006

TABLE 3. Parameter m and x-coordinate of integral points when the rank is 3 (as determined by `mwrank` or, for underlined values of m, using the Birch–Swinnerton-Dyer conjecture.)

Thus, let p be an odd prime divisor of a. Then either p divides x, so

$$\left(\frac{b}{p}\right) = \left(\frac{1}{p}\right) = 1,$$

so b is a square modulo p; or p divides $x-1$, hence

$$\left(\frac{b}{p}\right) = \left(\frac{(x^2-2)(x-1)-1}{p}\right) = \left(\frac{-1}{p}\right).$$

It follows that b is a square if and only if $p \equiv 1 \pmod 4$.

Assume now that a is even, so that b is odd. Then, when $a \equiv 2 \pmod 4$, b is always a square modulo 2. When $a \equiv 4 \pmod 8$, we have $x^2 - x \equiv 0 \pmod 4$ so either x is even, hence $b \equiv 1 \pmod 4$, so b is a square modulo 4. Or x is odd, hence $x \equiv 3 \pmod 4$, so $x^2 - x \equiv 2 \pmod 4$ which is a contradiction. When $a \equiv 0 \pmod 8$, b is odd and it is trivial to prove by induction that for all n, b is a square modulo 2^n if and only if $b \equiv 1 \pmod 8$. Thus, when $x \equiv 0 \pmod 4$ then $b \equiv 1 \pmod 8$, so b is a square modulo 2^n. The case $x \equiv 1 \pmod 4$ is not possible by hypothesis. Finally, if $x \equiv 2$ or $3 \pmod 4$, then $a \equiv x^2 - x \equiv 2 \pmod 4$, which is a contradiction. □

Corollary 5.4. *Let $P = [x, y]$ be an integral point on the curve E_m. Then, if $x > 1$ we have $x \equiv 2 \pmod 4$ or $x \equiv 3 \pmod 8$, while if $x < 1$ we have $x \equiv 0 \pmod 4$ or $x \equiv 7 \pmod 8$.*

Proof. Assume first that $x > 1$. If $[x, y]$ is an integral point, $x^3 + mx^2 - (m+3)x + 1$ is a square. Theorem 5.3 implies that every odd prime dividing $x - 1$ is congruent to 1 modulo 4. If x is even, we deduce that $x - 1$ is congruent to 1 modulo 4. If x is odd, we know that 4 does not divide $|x-1|$ by Lemma 5.2 and so

$$x - 1 = 2 \prod_{\substack{p \mid x-1 \\ p \neq 2}} p \equiv 2 \pmod 8.$$

The proof is similar when $x < 1$. □

Corollary 5.5. *If m is even, there is no integral point on $E_m^0(\mathbb{Q})$ (i.e., with a positive x-coordinate).*

Proof. The point $[1, y]$ is never on the curve. If $x > 1$, there is a contradiction between the previous corollary and Lemma 5.1. □

These corollaries can be summarized as follows:

Proposition 5.6. *There exists m (not necessary defining a simplest cubic field) such that the point $[x, y]$ is on $E_m(\mathbb{Z})$ if and only if the following conditions are satisfied:*

1. *$y \equiv \pm 1 \pmod{q^{v_q(x)}}$ for every odd prime q dividing x;*
2. *$y \equiv \pm\sqrt{-1} \pmod{p^{v_p(x)}}$ for every odd prime p dividing $x-1$;*
3. *y is odd;*
4. *if $x < 1$ and $x \equiv 0 \pmod 8$, then*

$$y \equiv \pm 1 \pmod{2^{v_2(x)-1}}.$$

This proposition allows us to do a "faster" systematic search for integral points. Before proving the announced results, we look for some parametrized solutions of equation (0–1).

5B. Parametrized Solutions of $y^2 = x^3 + mx^2 - (m+3)x + 1$

In this section, we consider the equation (0–1) as an affine surface in $\mathbb{R}^3$. We set $x = u+1$. Since $(0, 1, m)$ is always on the surface, we can set $y - 1 = (t-1)x$. Thanks to the linearity in m of the equation, we obtain a rational parametrization of our surface:

$$\begin{aligned} x &= u + 1, \\ y &= tu + t - u, \\ m &= t^2 - 2t - u - 1 + \frac{t^2+1}{u}. \end{aligned}$$

In order to find parametrized integral solutions of our equation, we set

$$k = \frac{t^2+1}{u},$$

and we denote by $P(k)$ the parametrized solution thus obtained. For example:

$$P(1) = \begin{cases} x = t^2 + 2, \\ y = -t^3 - 2t - t^2 - 1, \\ m = 2t - 1 \end{cases}$$

The solution obtained is the point $2\,[0, 1]$ when m is odd. This remark has already been made.

The equations for $P(-1)$ give an integral point when $m = 2t^2 + 2t - 1$. In this case the points $P_0 = [-1, 2t+1]$, $P_1 = [0, 1]$ and $P_2 = [2, 2t+1]$ are independent on $E_m(\mathbb{Q}(t))$ (this can be shown using the Néron–Tate height pairing [Shioda 1990]). Moreover $2P_1$, $P_0 + P_1$, $P_0 - P_1$, $P_2 + P_1$, $P_0 + P_2$ and $P_2 - P_1$ are integral points. Note that this last one

is the point given by $P(-1)$. So finally in this case, we obtain at least 9 integral points on the curve E_m. The numerical data suggest this phenomenon.

Similar considerations with $k = -5$ give (after replacing t by $-\frac{5}{2}t+2$) an integral point for $m = 5t^2-3t+3$ and we find on this curve 3 independent integral points.

We can hope to find some m such that E_m has high rank if m satisfy both of the two previous equations, in other words if

$$m = 2t_1^2+2t_1-1 = 5t_2^2-3t_2+3.$$

Set $T_1 = 2t_1+1$ and $T_2 = 10t_2-3$, we have to solve $T_2^2-10T_1^2 = -81$ with the conditions T_1 odd, $T_2 \equiv -3 \pmod{10}$, T_1 and T_2 not multiples of 3. An easy argument in the field $\mathbb{Q}(\sqrt{10})$ shows that the general solution is

$$T_2+T_1\sqrt{10} = (-1)^{k+1}(3+\sqrt{10})^{2k+1}(11+2\sqrt{10}).$$

with $k \in \mathbb{Z}$. If $k = 0$, we obtain $m = 11$ which is the smallest value of m for rank 3. If $k = -1$, we obtain $m = 143$ which is the smallest value for rank 5. If $k = 1$, we obtain $m = 14963$ and E_m is of rank at least 7 (the points $[0,1]$, $[-1,173]$, $[2,173]$, $[-4,547]$, $[-11884,659563]$ are given by our parametrization and the additional generators

$$[-64,7873] \quad \text{and } [90,10981]$$

are found by a systematic search. All these points are independent). Note that this is not the smallest rank 7 curve in our family, since E_m is of rank 7 also for $m = 12563$, which may well be the smallest m.

We now prove results concerning the point $[0,1]$. For this purpose, we must find approximations for the height of a point on E_m. For this, we need in particular to know the asymptotic behavior of the periods associated to the curve E_m in terms of the parameter m.

5C. Approximating the periods ω_1 and ω_2

The curve E_m defined by (0–1) is isomorphic to the curve

$$y^2 = 4f(x)$$

with

$$f(x) = x^3-\left(\tfrac{1}{3}m^2+m+3\right)x+\tfrac{2}{27}m^3+\tfrac{1}{3}m^2+m+1.$$

Let $e_1 \le e_2 \le e_3$ be the real roots of f (the discriminant is always positive). The periods ω_1 and ω_2 are given by

$$\omega_1 = \int_{e_1}^{e_2}\frac{dx}{\sqrt{f(x)}} \quad \text{and} \quad \omega_2 = -\int_{e_2}^{e_3}\frac{dx}{\sqrt{f(x)}}.$$

A straightforward study of the function f gives the inequalities:

$$-\frac{2m}{3}-1-\frac{2}{m} \le e_1 \le -\frac{2m}{3}-1-\frac{1}{m} \quad \text{if } m \ge 2,$$
$$\frac{m}{3} \le e_2 \le \frac{m}{3}+\frac{1}{m},$$
$$\frac{m}{3}+1 \le e_3 \le \frac{m}{3}+1+\frac{1}{m}.$$

We start with an approximation for ω_2 given by

$$\omega_2 = i\int_{e_2}^{e_3}\frac{dx}{\sqrt{(x-e_1)(x-e_2)(e_3-x)}} \in i\mathbb{R}.$$

If $x \in [e_2,e_3]$, then $m+1+1/m \le x-e_1 \le m+2+3/m$, so

$$\frac{1}{\sqrt{m+2+3/m}} \le \frac{1}{\sqrt{x-e_1}} \le \frac{1}{\sqrt{m+1+1/m}}$$

and

$$\frac{I}{\sqrt{m+2+3/m}} \le \frac{\omega_2}{i} \le \frac{I}{\sqrt{m+1+1/m}}$$

with

$$I = \int_{e_2}^{e_3}\frac{dx}{\sqrt{(x-e_2)(e_3-x)}} = \int_{-1}^{1}\frac{dt}{\sqrt{1-t^2}} = \pi.$$

Finally, we have

$$\frac{\pi}{\sqrt{m+2+3/m}} \le \frac{\omega_2}{i} \le \frac{\pi}{\sqrt{m+1+1/m}}.$$

So $\omega_2 \sim i\pi/\sqrt{m}$ and $\omega_2/i \ge 3.13/\sqrt{m}$ if $m \ge 500$.

We now consider the case of ω_1.

We split the integral into two parts: $\omega_1 = \omega_1^+ + \omega_1^-$, with

$$\omega_1^- = \int_{e_1}^{0}\frac{dx}{\sqrt{f(x)}} \quad \text{and} \quad \omega_1^+ = \int_{0}^{e_2}\frac{dx}{\sqrt{f(x)}}.$$

For ω_1^-, the roots e_2 and e_3 are far from the endpoints of the domain of integration. We thus have, for $x \in [e_1,0]$:

$$m/3 \le e_2-x \le m+1+3/m,$$
$$m/3+1 \le e_3-x \le m+2+3/m.$$

So

$$\omega_1^- \geq \frac{1}{\sqrt{(m+1+3/m)(m+2+3/m)}} \int_{e_1}^{0} \frac{dx}{\sqrt{x-e_1}},$$

$$\omega_1^- \leq \frac{1}{\sqrt{(m/3)(m/3+1)}} \int_{e_1}^{0} \frac{dx}{\sqrt{x-e_1}},$$

$$\omega_1^- \geq \frac{2\sqrt{-e_1}}{\sqrt{(m+1+3/m)(m+2+3/m)}},$$

$$\omega_1^- \leq \frac{2\sqrt{-e_1}}{\sqrt{(m/3)(m/3+1)}},$$

$$\omega_1^- \geq \frac{2\sqrt{2m/3+1+1/m}}{\sqrt{(m+1+3/m)(m+2+3/m)}},$$

$$\omega_1^- \leq \frac{2\sqrt{2m/3+1+2/m}}{\sqrt{(m/3)(m/3+1)}}.$$

We deduce the inequalities $\omega_1^- \leq 4.9/\sqrt{m}$ and $\omega_1^- \geq 1.63/\sqrt{m}$ if $m \geq 500$.

Now consider the case of ω_1^+. Here only e_1 is sufficiently far from the domain of integration. For $x \in [0, e_2]$,

$$\frac{2m}{3} + 1 + \frac{1}{m} \leq x - e_1 \leq m + 1 + \frac{3}{m},$$

so

$$\frac{I}{\sqrt{m+1+3/m}} \leq \omega_1^+ \leq \frac{I}{\sqrt{2m/3+1+1/m}}$$

with

$$I = \int_0^{e_2} \frac{dx}{\sqrt{(x-e_2)(x-e_3)}} = \log \frac{\sqrt{e_3}+\sqrt{e_2}}{\sqrt{e_3}-\sqrt{e_2}}$$

and

$$\frac{4m/3}{1+1/m} \leq \frac{\sqrt{e_3}+\sqrt{e_2}}{\sqrt{e_3}-\sqrt{e_2}} \leq \frac{4\,(m/3+1+1/m)}{1-1/m}.$$

We can thus write

$$\omega_1^+ \geq \frac{1}{\sqrt{m+1+3/m}} \log \frac{4m}{3\,(1+1/m)},$$

$$\omega_1^+ \leq \frac{1}{\sqrt{2m/3+1+1/m}} \log \frac{4(m+3+3/m)}{3(1-1/m)},$$

$$\omega_1^+ \geq \frac{\log \dfrac{4}{3\,(1+1/m)}}{\sqrt{m+1+3/m}} + \frac{\log m}{\sqrt{m+1+3/m}},$$

$$\omega_1^+ \leq \frac{\log \dfrac{4}{3\,(1-1/m)}}{\sqrt{2m/3+1+1/m}} + \frac{\log\,(m+3+3/m)}{\sqrt{2m/3+1+1/m}}.$$

Finally, we have, for $m \geq 500$,

$$\frac{0.28}{\sqrt{m}} + \frac{0.99\log m}{\sqrt{m}} \leq \omega_1^+ \leq \frac{5.26}{\sqrt{m}} + \frac{1.23\log m}{\sqrt{m}},$$

$$\frac{1.91}{\sqrt{m}} + \frac{0.99\log m}{\sqrt{m}} \leq \omega_1 \leq \frac{5.26}{\sqrt{m}} + \frac{1.23\log m}{\sqrt{m}}.$$

Remark. In fact we can easily prove that

$$\omega_1 = \frac{\log m + 4\log 2 + o(1)}{\sqrt{m}},$$

but we do not need this.

5D. Approximating the Canonical Height

First, we find an upper bound for the canonical height of an integral point P on E_m. By Lemma 2.1,

$$\hat{h}(P) - \tfrac{1}{2}h(P) \leq 1.57 + \tfrac{1}{4}\log(m^2+3m+9) + \tfrac{1}{2}\log m.$$

Since P is integral, $h(P) = \log\max\{1, |x_P|\}$. So

$$\hat{h}(P) \leq \tfrac{32}{25}\log m + \tfrac{1}{2}\log\max\{1, |x_P|\} \quad \text{if } m \geq 500. \tag{5–1}$$

To find a lower bound for the canonical height of a rational point on E, we write it as the sum of local contributions.

Let $P = \left[\alpha/d^2, \beta/d^3\right] \in E_m(\mathbb{Q})$ with $(\alpha, d) = (\beta, d) = 1$. We first compute the non-Archimedean contribution. We use the algorithm described in [Silverman 1988; Cohen 1993, Section 7.5.2]. We have $\beta^2 = \alpha^3 + md^2\alpha^2 - (m+3)d^4\alpha + 1$. So $\beta \equiv \alpha + 1 \pmod 2$ and d cannot be even. A similar argument shows that d is not a multiple of 3. Set

- $\Delta = m^2+3m+9$;
- $A = 3\alpha^2 + 2md^2\alpha - (m+3)d^4$ (the numerator of $3\alpha^2/d^4 + 2m\alpha/d^2 - (m+3)$);
- $B = 2\beta$ (the numerator of $2\beta/d^3$);
- $C = 3\alpha^4 + 4m\alpha^3d^2 - (6m+18)\alpha^2d^4 + 12\alpha d^6 - \Delta d^8$ (the numerator of $3\alpha^4/d^8 + 4m\alpha^3/d^6 - (6m+18) \times \alpha^2/d^4 + 12\alpha/d^2 - \Delta$); and
- $D = \gcd(A, B)$.

We prove that the only prime giving any local contribution is 2. Let p be an odd prime dividing D. Because

$$4A^2 = (9\alpha+3d^2m)B^2 + 4\Delta d^4(\alpha^2-d^2\alpha+d^4),$$

p^2 divides $4\Delta d^4(\alpha^2-d^2\alpha+d^4)$. On the other hand p does not divide d (because p divides β) and Δ

is squarefree, so p divides $(\alpha^2-d^2\alpha+d^4)$. Next, because

$$B^2 = 4(\alpha+d^2(m+1))(\alpha^2-d^2\alpha+d^4) - 4d^4(3\alpha+d^2m),$$

p divides $3\alpha+d^2m$. Moreover the resultant of A and B is $d^{12}\Delta^2$, so p divides Δ and hence p divides $(3\alpha+d^2m-3d^4\Delta)$. Because

$$27B^2 = 4(3\alpha+d^2m-3d^4\Delta)(3\alpha+d^2m)+4d^6(2m+3)\Delta,$$

p^2 divides $d^6(2m+3)\Delta$, so p divides $2m+3$. And since $4\Delta = (2m+3)^2+27$, we conclude that $p=3$; but then 3 divides m and Δ is not squarefree. We have thus proved 2 is the only prime dividing D.

We now compute the local contribution $C_2 = C_l$ at $l=2$. We have $v_2(B)=1$ and $C \equiv -(2m+2) \pmod 8$, so we obtain:

- If m is even, $C_2 = \log d$.
- If $m \equiv 1 \pmod 4$, $C_2 = \log d - \frac{1}{4}\log 2$.
- If $m \equiv 3 \pmod 4$, $C_2 = \log d - \frac{1}{3}\log 2$.

In all cases, $C_2 \geq \log d - \frac{1}{3}\log 2$.

We consider now the Archimedean contribution C_∞ of the point P. Denote by z the elliptic logarithm of P. Set $\lambda = 2\pi/\omega_1$, $t = \lambda \operatorname{Re} z$, $q = \exp(2i\pi\omega_2/\omega_1)$ and

$$\theta = \sum_{n=0}^{\infty} \sin((2n+1)t)(-1)^n q^{n(n+1)/2}.$$

Then the Archimedean contribution is

$$C_\infty = \tfrac{1}{32}\log\left|16\Delta^2/q\right| - \tfrac{1}{4}\log|\theta| + \tfrac{1}{8}\log\left(\frac{(\alpha/d^2)^3+m(\alpha/d^2)^2-(m+3)\alpha/d^2+1}{\lambda}\right).$$

The discriminant $16\Delta^2$ of the curve is greater than $16m^4$. On the other hand,

$$|\theta| \leq \sum_{n=0}^{\infty} q^{n(n+1)/2} \leq \frac{1}{1-q}.$$

To find a lower bound for C_∞, we need an upper bound for q. Using approximations to the periods, we deduce

$$2i\pi\frac{\omega_2}{\omega_1} \leq \frac{-3.13\ 2\pi}{5.26+1.23\log m} \leq -\frac{9.47}{\log m}$$

if $m \geq 500$, so

$$q \leq \exp\left(-\frac{9.47}{\log m}\right) \leq 1 - \frac{4.86}{\log m}$$

if $m \geq 500$.

We are now able to minimize each part of C_∞ for $m \geq 500$:

$$\tfrac{1}{32}\log\left|16\Delta^2\right| \geq \tfrac{1}{8}\log m + \tfrac{1}{8}\log 2,$$

$$\tfrac{1}{32}\log|1/q| \geq \tfrac{1}{32}\log\exp\frac{9.47}{\log m} \geq \frac{9.47}{32\log m},$$

$$-\tfrac{1}{4}\log|\theta| \geq -\tfrac{1}{4}\log\frac{1}{1-q} \geq -\tfrac{1}{4}\log\frac{\log m}{4.86} \geq \tfrac{1}{4}\log 4.86 - \tfrac{1}{4}\log\log m.$$

As for $-\frac{1}{8}\log\lambda = \frac{1}{8}\log(\omega_1/2\pi)$, it is greater than or equal to

$$-\tfrac{1}{8}\log(2\pi) + \tfrac{1}{8}\log\frac{1.91+0.99\log m}{\sqrt{m}}$$
$$\geq \tfrac{1}{8}\log\frac{1}{\sqrt{m}} - \tfrac{1}{8}\log(2\pi) + \tfrac{1}{8}\log(1.91+0.99\log m)$$
$$\geq -\tfrac{1}{16}\log m - \tfrac{1}{8}\log(2\pi) + \tfrac{1}{8}\log\left(0.99+\frac{1.91}{\log m}\right) + \tfrac{1}{8}\log\log m,$$

Moreover

$$\frac{\log 2}{8} - \frac{8}{\log(2\pi)} + \frac{\log 4.86}{4} \geq 0.252.$$

Finally, we obtain the following lower bound for C_∞:

$$\tfrac{1}{16}\log m + \frac{9.47}{32\log m} + \tfrac{1}{4}\log(\beta/d^3) + \tfrac{1}{8}\log(0.99+1.91/\log m) - \tfrac{1}{8}\log\log m + 0.252.$$

Adding the non-Archimedean contribution, we obtain

$$\hat{h}(P) \geq \tfrac{1}{16}\log m + \frac{9.47}{32\log m} + \tfrac{1}{4}\log(\beta/d^3) + \tfrac{1}{8}\log(0.99+1.91/\log m) - \tfrac{1}{8}\log\log m + \log d - \tfrac{1}{3}\log 2 + 0.252.$$

Hence, we obtain a lower bound for $\hat{h}(P)$:

$$\hat{h}(P) \geq \tfrac{1}{16}\log m + \frac{9.47}{32\log m} + \tfrac{1}{4}\log(\beta d) + \tfrac{1}{8}\log(0.99+1.91/\log m) - \tfrac{1}{8}\log\log m + 0.02. \quad (5\text{–}2)$$

5E. About the Special Point $[0,1]$

Theorem 5.7. *The point* $[0,1]$ *is always a generator.*

Proof. If $m \leq 500$, we have computed the Mordell–Weil group and all the integral points (see Tables on pages 95 and 96) and the assertion of the theorem is satisfied. If $m \geq 500$, we use the above

approximations. Let P be a point (with positive y-coordinate) on E such that $[0,1] = nP$. Since the sum of two points in $E_0(\mathbb{Q})$ is still in $E_0(\mathbb{Q})$, P belongs to $E_{gg}(\mathbb{Q})$. We assume first that P is integral and not equal to $[0,1]$. The y-coordinate of such a point is greater than $\sqrt{2m+3}$, so by (5–2)

$$\begin{aligned}
\hat{h}(P) &\geq \tfrac{1}{16}\log m + \tfrac{1}{4}\log\sqrt{2m} + \tfrac{1}{8}\log 0.99 - \tfrac{1}{8}\log\log m \\
&\qquad + 0.02, \\
\hat{h}(P) &\geq \tfrac{3}{16}\log m - \tfrac{1}{8}\log\log m + 0.1, \\
\hat{h}(P) &\geq \tfrac{1}{6}\log m.
\end{aligned}$$

On the other hand, $\hat{h}([0,1]) \leq \frac{32}{25}\log m$ by (5–1), so

$$n^2 = \frac{\hat{h}([0,1])}{\hat{h}(P)} \leq 6\ \tfrac{32}{25} \leq 8.$$

Moreover $2P \in E_0(\mathbb{Q})$ and hence P cannot exist.

We now assume that $P = [\alpha/d^2, \beta/d^3]$ is not integral. We have seen that d is odd and not a multiple of 3, so $\beta d \geq 5$. We have by (5–2)

$$\begin{aligned}
\hat{h}(P) &\geq \tfrac{1}{16}\log m + \tfrac{1}{8}\log 0.99 - \tfrac{1}{8}\log\log m + \tfrac{1}{4}\log 5, \\
\hat{h}(P) &\geq \tfrac{1}{17}\log m.
\end{aligned}$$

As in the previous case, we obtain

$$n^2 \leq 17\ \tfrac{32}{25} \leq 22.$$

The points $2P$ and $4P$ are in $E_0(\mathbb{Q})$. By an explicit computation, it is easy to show that d^2 divides the denominator of the x-coordinate of $3P$. Hence $[0,1]$ is a generator. □

Theorem 5.8. *The only integral points on E_m which are positive multiples of the point $[0,1]$ are:*

- $[0,1]$ *if m is even.*
- $[0,1]$ *and* $2[0,1]$ *if m is odd.*

Proof. If $m \leq 500$, the assertion of the theorem is satisfied (see Section 4). If $m \geq 500$ we use the previous approximations. We first prove three lemmas. We only consider positive multiples.

Lemma 5.9. *The odd multiples of the point $[0,1]$ are never integral, except of course for $[0,1]$ itself.*

Proof. Let $P = (2n+1)[0,1]$ be an integral point. Since $[0,1] \in E_{gg}(\mathbb{Q})$, $P \in E_{gg}(\mathbb{Q})$. We then have $|x_P| \leq m+1$ and, by (5–1) and (5–2),

$$\begin{aligned}
\hat{h}(P) &\leq \tfrac{32}{25}\log m + \tfrac{1}{2}\log(m+1), \\
\hat{h}(P) &\leq \tfrac{45}{25}\log m, \\
\hat{h}([0,1]) &\geq \tfrac{1}{16}\log m + \tfrac{1}{8}\log\left(0.99 + 1.91/\log m\right) \\
&\qquad + \frac{9.47}{32\log m} - \tfrac{1}{8}\log\log m + 0.02, \\
\hat{h}([0,1]) &\geq \tfrac{1}{25}\log m.
\end{aligned}$$

Remark. $\hat{h}([0,1])$ is experimentally equal to

$$\tfrac{1}{4}\log m + C_2 + o(1),$$

where C_2 is as above with $d = 1$. This should not be difficult to prove.

Finally, if $m \geq 500$, we have

$$(2n+1)^2 \leq 45.$$

To complete the proof, we have to look at the points $3[0,1]$ and $5[0,1]$. We have

$$x(3[0,1]) = -\frac{8m^3 + 40m^2 + 120m + 152}{m^4 + 4m^3 + 22m^2 + 36m + 81},$$

$|x(3[0,1])| < 1$ when $m \geq 8$, so $3[0,1]$ is not integral. The same reasoning with $m \geq 29$ implies that $5[0,1]$ is not integral. □

Lemma 5.10. *The point $4[0,1]$ is never integral.*

Proof. We have the following expression for $x(4[0,1])$:

$$\frac{m^8+8m^7+60m^6+280m^5+1158m^4+3320m^3+7868m^2+11368m+12033}{(4m^3+20m^2+60m+76)^2}$$

If m is even, the numerator is odd whereas the denominator is even, so that $4[0,1]$ is not integral in this case.

If $m \equiv 1 \pmod 4$, we set $m = 4k+1$ and replace in $x(4[0,1])$; the same reasoning then implies that $4[0,1]$ is not integral.

If $m \equiv 3 \pmod 4$, we set $m = 4k+3$, expand, and eliminate common factors of 2, writing

$$x(4[0,1]) = \frac{p(k)}{q(k)^2}.$$

Then $p(k)$ and $q(k)$ are coprime for all values of k; in fact, we have $u(k)p(k)+v(k)q(k) = 1$ with $u(k) = 16k^2+8k-16$ and $v(k) = -128k^7-640k^6-1408k^5-1584k^4-648k^3+596k^2+908k+401$. It follows that $4[0,1]$ is never integral as claimed. □

Lemma 5.11. $P \notin E(\mathbb{Z}) \Longrightarrow 2P \notin E(\mathbb{Z})$.

Proof. Let $P = [a/d^2, b/d^3]$, with $(a,d) = (b,d) = 1$. Using the duplication formula we obtain

$$x_{2P} = \frac{a^4 - 2(m+3)a^2d^4 - 8ad^6 + (m^2+2m+9)d^8}{4b^2d^2}.$$

Since a and d are coprime, d^2 divides the denominator of x_{2P}. □

Remark. In general if P is not integral them $[m]P$ is not integral for any integer m. This follows from standard facts about the p-adic filtration of an elliptic curve over $\mathbb{Q}_p$ [Husemoller 1987].

We now complete the proof of the theorem. We have

$$x(2\,[0,1]) = \left(\frac{m+1}{2}\right)^2 + 2,$$

so the point $2\,[0,1]$ is integral if and only if m is odd.

Let $P = 2^p m[0,1]$ with m odd and $p \geq 0$. If $m = 1$, then either $p = 0$ (and $P = [0,1]$ is integral), or $p = 1$ (and $P = 2\,[0,1]$ is integral if and only if m is odd), or $p \geq 2$ and then P is not integral by Lemmas 5.10 and 5.11. If $m > 1$, $m[0,1]$ is not integral by Lemma 5.9, so P is not integral by Lemma 5.11. □

Corollary 5.12. *When the rank is* 1, *these theorems give us all integral points on the curve.*

REFERENCES

[Baker and Davenport 1969] A. Baker and H. Davenport, "The equations $3x^2-2=y^2$ and $8x^2-7=z^2$", *Quart. J. Math. Oxford Ser.* (2) **20** (1969), 129–137.

[Cohen 1993] H. Cohen, *A course in computational algebraic number theory*, Springer, Berlin, 1993.

[Cremona 1998] J. E. Cremona, "`mwrank`, a program for 2-descent on elliptic curves over $\mathbb{Q}$", last major update 1998. See http://www.maths.nottingham.ac.uk/personal/jec/ftp/progs.

[David 1995] S. David, *Minorations de formes linéaires de logarithmes elliptiques*, Mém. Soc. Math. France (N.S.) **62**, Soc. math. France, Paris, 1995.

[Gebel et al. 1994] J. Gebel, A. Pethő, and H. G. Zimmer, "Computing integral points on elliptic curves", *Acta Arith.* **68**:2 (1994), 171–192.

[Husemoller 1987] D. Husemoller, *Elliptic curves*, Graduate Texts in Math. **111**, Springer, New York, 1987.

[Lang 1978] S. Lang, *Elliptic curves: Diophantine analysis*, Grundlehren der math. Wissenschaften **231**, Springer, Berlin, 1978.

[Niklasch and Smart 1998] G. Niklasch and N. P. Smart, "Exceptional units in a family of quartic number fields", *Math. Comp.* **67**:222 (1998), 759–772.

[Pethő 1991] A. Pethő, "Complete solutions to families of quartic Thue equations", *Math. Comp.* **57**:196 (1991), 777–798.

[Shanks 1974] D. Shanks, "The simplest cubic fields", *Math. Comp.* **28** (1974), 1137–1152.

[Shioda 1990] T. Shioda, "On the Mordell-Weil lattices", *Comment. Math. Univ. St. Paul.* **39**:2 (1990), 211–240.

[Silverman 1988] J. H. Silverman, "Computing heights on elliptic curves", *Math. Comp.* **51**:183 (1988), 339–358.

[Silverman 1990] J. H. Silverman, "The difference between the Weil height and the canonical height on elliptic curves", *Math. Comp.* **55**:192 (1990), 723–743.

[Smart 1994] N. P. Smart, "S-integral points on elliptic curves", *Math. Proc. Cambridge Philos. Soc.* **116**:3 (1994), 391–399.

[Smart 1998] N. P. Smart, *The algorithmic resolution of Diophantine equations*, London Math. Soc. student texts **41**, Cambridge University Press, Cambridge, 1998.

[Stroeker and Tzanakis 1994] R. J. Stroeker and N. Tzanakis, "Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms", *Acta Arith.* **67**:2 (1994), 177–196.

[Washington 1987] L. C. Washington, "Class numbers of the simplest cubic fields", *Math. Comp.* **48**:177 (1987), 371–384.

[Zagier 1987] D. Zagier, "Large integral points on elliptic curves", *Math. Comp.* **48**:177 (1987), 425–436. Addendum in **51** (1988), 375.

Sylvain Duquesne, Université Bordeaux I, Laboratoire A2X, 351 Cours de la Libération, 33405 Talence, France (duquesne@math.u-bordeaux.fr)

Received July 9, 1999; accepted in revised form April 3, 2000

manuscripta math. 108, 191–204 (2002)

S. Duquesne

Rational points on hyperelliptic curves and an explicit Weierstrass preparation theorem

Received: 2 January 2001

Abstract. By using the so-called elliptic curve Chabauty method, N. Bruin [1], V. Flynn and J. Wetherell [6] have extended Chabauty's method to some cases where the rank of the Jacobian may not be less than the genus. The main tool in these methods is a theorem of Strassman on p-adic zeros of power series in one variable, and is applicable only if certain Jacobians are of rank less than or equal to 1. In the present paper, we give an explicit generalization of Strassman's theorem to several variables, enabling us to treat cases where the rank is greater than 1. We apply this to find all the rational points on a hyperelliptic curve of rank and genus equal to 4.

1. Introduction

One of the most important problems about curves of genus greater or equal to 2 is the computation of their rational points. It is now well-known that by using a method of Chabauty ([3], [4], [5]), if the rank of the Jacobian of a hyperelliptic curve is strictly less than the genus, we can bound the number of rational points on the curve. In many cases it is thus possible to compute all the rational points on the curve.

When the rank of the Jacobian is greater than or equal to the genus of the curve, a few methods are known for computing rational points (see [1], [7], [13]).

One of these methods (the elliptic curve Chabauty method, explained in [1] and [6]) consists in reducing the problem to finding rational points with a $\mathbb{Q}$-rational x-coordinate on an elliptic curve over some number field. In all the examples given in the paper of Flynn and Wetherell, the elliptic curves which occur are of rank at most equal to 1, hence one only needs to bound the number of p-adic zeros of a power series in one variable, which is done using Strassman's theorem.

When the rank of the elliptic curve is larger than 1, it is possible to obtain systems of power series in several variables. Bruin treated some examples in this case in [1]. In the general case, Strassman's theorem does not apply and we need a generalization of this theorem to power series in several variables.

Flynn and Wetherell suggest to use instead the Weierstrass preparation theorem. The goal of the present paper is to make this suggestion explicit.

S. Duquesne: Laboratoire A2X, Université Bordeaux I, 351 Cours de la Libération, 33405 Talence Cedex, France. e-mail: duquesne@math.u-bordeaux.fr

Mathematics Subject Classification (2000): 11G30, 11Y50

As an illustration, we give the following example.

Theorem 1. *Let $\mathcal{C}$ denote the hyperelliptic curve defined by*

$$y^2 = x^9 - 6x^8 + 31x^7 - 81x^6 + 177x^5 - 176x^4 - 9x^3 + 107x^2 + 19x + 1 \ .$$

Then $\mathcal{C}(\mathbb{Q}) = \{\infty, (1, \pm 8), (0, \pm 1)\}$.

Remark 1. The curve $\mathcal{C}$ is a hyperelliptic curve of genus 4. Using a `magma` program of M. Stoll [11] included in `magma 2.7` and above, we compute that the rank of its Jacobian is equal to 4. Since the rank is greater than or equal to the genus, we cannot apply Chabauty's theorem. Hence, we will try to apply the elliptic curve Chabauty method developed in [1] and [6]. In other words, we will look for an elliptic curve defined over some number field such that every rational point on $\mathcal{C}$ gives rise to a point on the elliptic curve with a $\mathbb{Q}$-rational x-coordinate.

Let $\mathbf{K}$ denote the number field $\mathbb{Q}(\beta)$, where β is a root of $x^3 + 2x + 1$. The curve $\mathcal{C}$ has been chosen so that we can factorize its defining polynomial f over $\mathbf{K}$. More precisely, we have

$$f(x) = f_1(x) f_2(x) \ ,$$

where

$$\begin{aligned} f_1(x) &= x^3 - 2x^2 + (-4\beta^2 - \beta + 1)x + 1 \ . \\ f_2(x) &= x^6 - 4x^5 + (4\beta^2 + \beta + 22)x^4 + (-8\beta^2 - 2\beta - 34)x^3 \\ &\quad + (37\beta^2 - 15\beta + 83)x^2 + (4\beta^2 + \beta + 18)x + 1 \ . \end{aligned}$$

Let (x, y) be any rational point in $\mathcal{C}(\mathbb{Q})$. Since $\mathbf{K}$ has class number 1, there exist $y_1, y_2, \alpha \in \mathbf{K}$ such that

$$\begin{aligned} \alpha y_1^2 &= f_1(x) \ , \\ \alpha y_2^2 &= f_2(x) \ . \end{aligned}$$

Note that there is no solution with $y = 0$, and that solutions with $y = \infty$ correspond to $x = \infty$. On the other hand, the resultant of $f_1(x)$ and $f_2(x)$ is equal to $(-4 + 3\beta - 2\beta^2)^3(-16 + \beta + 4\beta^2)^3$ so that, if $y \neq 0, \infty$, without loss of generality we can choose α belonging to a system of representatives of $\{2, (-4 + 3\beta - 2\beta^2), (-16 + \beta + 4\beta^2)\}$-units in $\mathbf{K}$ modulo squares. Moreover, these units are generated by $-1, \beta, 1 + \beta, 1 + \beta + \beta^2, -4 + 3\beta - 2\beta^2$, and $-16 + \beta + 4\beta^2$. It follows that up to squares there are 64 $\{2, (-4+3\beta-2\beta^2), (-16+\beta+4\beta^2)\}$-units in $\mathbf{K}$ and we can compute them explicitly.

We have now to search for which of these $\{2, (-4+3\beta-2\beta^2), (-16+\beta+4\beta^2)\}$-units α there exists an x in $\mathbb{Q}$ such that $\alpha f_1(x)$ and $\alpha f_2(x)$ are simultaneously squares. We can first look for those α which satisfy this property everywhere locally. Modulo 32, we find that this only happens for $\alpha = 1$.

We have thus proved that $\alpha = 1$ is the only value to consider. Thus, if $(x, y) \in \mathcal{C}(\mathbb{Q})$, there exist $y_1, y_2 \in \mathbf{K}$ such that

$$\begin{aligned} y_1^2 &= f_1(x) \ , \\ y_2^2 &= f_2(x) \ . \end{aligned}$$

In particular, if (x, y) is a rational point on the curve $\mathcal{C}$, then (x, y_1) is a $\mathbf{K}$-rational point on the elliptic curve

$$\mathcal{E} \ : \ y^2 = f_1(x) = x^3 - 2x^2 + (-4\beta^2 - \beta + 1)x + 1 \ ,$$

with a $\mathbb{Q}$-rational x-coordinate.

We are thus interested in the $x \in \mathbb{Q}$ which are the x-coordinates of points on the curve $\mathcal{E}$ over $\mathbf{K}$. For this purpose, we want to apply the elliptic curve Chabauty method explained in [1] and [6].

When the rank of the elliptic curve is one, this method reduces to bounding the number of p-adic zeros of a power series in one variable, which is done by using Strassman's theorem. In our case, the rank of $\mathcal{E}$ over K is equal to 2. Thus, if we follow the elliptic curve Chabauty method, we will need to bound the number of p-adic solutions of systems of power series in two variables. In [6], Flynn and Wetherell suggest to use the Weierstrass preparation theorem in several variables, since Strassman's theorem is equivalent to the Weierstrass preparation theorem in one variable. We now follow this suggestion.

2. The Weierstrass preparation theorem in two variables

In this section we rewrite for the case $n = 2$ the Weierstrass preparation theorem in n variables of Sugatani [12].

As in [12], we denote by $\mathbb{Z}_p \langle n_1, n_2 \rangle$ the set of power series in two variables n_1 and n_2 with coefficients in $\mathbb{Z}_p$ which can be written in the form

$$f = \sum_{(i,j)=(0,0)}^{\infty} f_{(i,j)} n_1^i n_2^j \ ,$$

where the coefficients $f_{(i,j)}$ are in $\mathbb{Z}_p$ and $\left| f_{(i,j)} \right|_p \to 0$ as $i + j \to \infty$.

We define a norm on $\mathbb{Z}_p \langle n_1, n_2 \rangle$ by $||f|| = \max \left\{ |f_{(i,j)}|_p \right\}$.

Moreover, we define $\mathbb{Z}_p \langle n_2 \rangle$ and $\mathbb{Z}_p \langle n_2 \rangle \langle n_1 \rangle$ in the same way and we identify $\mathbb{Z}_p \langle n_2 \rangle \langle n_1 \rangle$ with $\mathbb{Z}_p \langle n_1, n_2 \rangle$ so that each element f of $\mathbb{Z}_p \langle n_1, n_2 \rangle$ has an expression $\sum_{i=0}^{\infty} f_i n_1^i$, where $f_i \in \mathbb{Z}_p \langle n_2 \rangle$ and $||f_i|| \to 0$ as $i \to \infty$.

Let us first characterize units in $\mathbb{Z}_p \langle n_2 \rangle$ and $\mathbb{Z}_p \langle n_1, n_2 \rangle$.

- $f = \sum_{j=0}^{\infty} f_j n_2^j \in \mathbb{Z}_p \langle n_2 \rangle$ is a unit of $\mathbb{Z}_p \langle n_2 \rangle$ if and only if $|f_0|_p = 1$ and $|f_j|_p < 1$ for each $j \neq 0$.
- $f = \sum_{(i,j)=(0,0)}^{\infty} f_{(i,j)} n_1^i n_2^j \in \mathbb{Z}_p \langle n_1, n_2 \rangle$ is a unit of $\mathbb{Z}_p \langle n_1, n_2 \rangle$ if and only if $|f_{(0,0)}|_p = 1$ and $|f_{(i,j)}|_p < 1$ for each $(i, j) \neq (0, 0)$.

Finally, we say that $f = \sum f_i n_1^i \in \mathbb{Z}_p \langle n_2 \rangle \langle n_1 \rangle$ is *general in* n_1 *of order* s if f_s is a unit element of $\mathbb{Z}_p \langle n_2 \rangle$ and if $||f_i|| < 1$ for all $i > s$.

We can now state the following theorem which is a special case of Theorem 3.1 of Sugatani [12]:

Theorem 2 (Sugatani). *Let $f \in \mathbb{Z}_p \langle n_1, n_2 \rangle$ be general in n_1 of order $s \geq 0$. Then there exist unique $h, g_0, \ldots, g_{s-1}$ and g_s satisfying the following conditions:*

- *h is a unit element of $\mathbb{Z}_p \langle n_1, n_2 \rangle$ and $h_0(n_2) = 1$.*
- *$g_0, \ldots, g_{s-1}$ are in $\mathbb{Z}_p \langle n_2 \rangle$ and g_s is a unit element of $\mathbb{Z}_p \langle n_2 \rangle$.*
- *$f(n_1, n_2) = h(n_1, n_2)(g_s(n_2)n_1^s + g_{s-1}(n_2)n_1^{s-1} + \cdots + g_1(n_2)n_1 + g_0(n_2))$.*

Remark 2. We can recognize the Weierstrass preparation theorem which says the same thing for power series in one variable (see for example [2] p. 108). In order to bound the number of zeros of systems of two power series in two variables, we need to apply explicitly the Weierstrass preparation theorem to one of the power series, and so we need to know how to compute the functions g_i and h_i of the theorem.

3. An explicit Weierstrass preparation theorem

In this section, we give a method for computing the functions occurring in the previous theorem (2).
We have

$$f(n_1, n_2) = \sum_{(i,j)=0}^{\infty} f_{(i,j)} n_1^i n_2^j \quad \in \mathbb{Z}_p \langle n_1, n_2 \rangle \ ,$$

where $f_{(i,j)}$ converges to 0 in $\mathbb{Z}_p$ as $i + j \to \infty$. In order to apply the Weierstrass preparation theorem, we consider f as a power series in n_1 with coefficients in $\mathbb{Z}_p \langle n_2 \rangle$ denoted by $f_i(n_2)$. Moreover f is general in n_1 of order s, hence the coefficient $f_s(n_2)$ of n_1^s is invertible in $\mathbb{Z}_p \langle n_2 \rangle$ and $||f_i(n_2)|| < 1$ for all $i \geq s+1$.

Let us denote by $g(n_1, n_2)$ the polynomial $g_0(n_2) + g_1(n_2)n_1 + \cdots + g_s(n_2)n_1^s$ and $h(n_1, n_2) = 1 + \sum_1^\infty h_i(n_2)n_1^i$ the functions of Theorem 2. Our goal is to compute these functions. The equation $f(n_1, n_2) = g(n_1, n_2)h(n_1, n_2)$ gives

$$h_n \ g_0 + h_{n-1} \ g_1 + \cdots + h_{n-s} \ g_s = f_n \quad \text{for all } n \geq 0 \ , \tag{1}$$

with the notation $h_0(n_2) = 1$ and $h_n(n_2) = 0$ if $n < 0$.

Since h is a unit in $\mathbb{Z}_p \langle n_1, n_2 \rangle$, we have $||h_i(n_2)|| < 1$ for all $i \geq 1$. Hence, since $f_s(n_2)$ is invertible, Equation (1) for $n = s$ implies that $g_s(n_2)$ is also invertible in $\mathbb{Z}_p \langle n_2 \rangle$.

Proposition 1. *The functions h_i can be written in terms of $g_0, g_1, \ldots, g_s$ by the following formula:*

$$h_n = \sum_{k=0}^{\infty} \frac{(-1)^k}{g_s^{k+1}} \sum_{i_0+i_1+\cdots+i_{s-1}=k} \binom{k}{i_0, i_1, \ldots, i_{s-1}} f_{ind(n,k,s,\mathbf{i})} \prod_{\ell=0}^{s-1} g_\ell^{i_\ell} \ , \tag{2}$$

where

- $\mathbf{i} = (i_0, i_1, \ldots, i_{s-1})$,
- $ind(n, k, s, \mathbf{i}) = n + s + \sum_{j=0}^{s-1} (s - j) i_j$,

– *and* $\binom{k}{i_0, i_1, \ldots, i_{s-1}} = \dfrac{k!}{i_0! i_1! \cdots i_{s-1}!}$ *is a multinomial coefficient.*

Proof. Thanks to Theorem 2, we must simply show that these functions satisfy Equation (1). For this purpose, denote by $h_{n,k}$ the k-th summand occurring in Equation (2). Thus, we must show that $h_n = \sum_{k=0}^{\infty} h_{n,k}$ satisfy Equation (1) or, equivalently, that

$$\sum_{k=0}^{\infty} (h_{n,k}\, g_0 + h_{n-1,k}\, g_1 + \cdots + h_{n-s,k}\, g_s) = f_n \ .$$

Let us consider the first term of this sum ($k = 0$) :

$$h_{n,0} g_0 + h_{n-1,0} g_1 + \cdots + h_{n-s+1,0} g_{s-1} + h_{n-s,0} g_s \ ,$$

the last term, $h_{n-s,0}$, is equal to f_n and it is easy to prove that the other terms are canceled by the last term for $k = 1$ ($h_{n-s,1}\, g_s$). In the same way, for any given $k \geq 0$ it is easy to prove that the term $h_{n,k}\, g_0 + h_{n-1,k}\, g_1 + \cdots + h_{n-s+1,k}\, g_{s-1}$ is canceled by the term $h_{n-s,k+1}\, g_s$, proving the proposition. □

In order to obtain an explicit Weierstrass preparation theorem, thanks to this proposition, we only need to compute the functions $g_0, \ldots, g_s$. Since $h_0 = 1$ and $h_n = 0$ for all $n \leq 0$, Equation (1) allows us to write

$$g_0 = f_0 \text{ and } g_i = f_i - \sum_{j=1}^{i} h_j g_{i-j} \quad 1 \leq i \leq s \ . \tag{3}$$

At this stage, it is possible to obtain formulas for g_i by recursive substitution using Formula (2), but the computation is very costly. We give here a method which computes the g_i's and the h_i's for any given precision in $\mathbb{Q}_p$ if the f_i's are given with this precision.

Assume that we have computed the functions g_i and h_i modulo p^k. We can then compute the inverse of g_s modulo p^k. Since by definition, p divides f_i for all $i \geq s + 1$, Equations (2) for $n = 0, \ldots, s$ allow us to compute the functions $h_0, \ldots, h_s$ modulo p^{k+1} (we can even compute the following h_i's, but we do not need them to compute the g_i's). In fact, in the formula of Proposition 1, the index of the functions f_i is greater than $s + 1$.

Hence, using Formula (3) for $i = 0, \ldots, s$ we can compute the functions $g_0, \ldots, g_s$ modulo p^{k+1}. In fact, the h_i's are now known modulo p^{k+1} and divisible by p. In this way, we can compute the g_i's and even the h_i's with the same precision as the f_i's.

Our main problem is to solve systems of two formal equations in two variables. For this purpose, we consider one of the two equations as an element of $\mathbb{Z}_p \langle n_1, n_2 \rangle$ (Flynn and Wetherell show in [6] that these equations are in $Z_p \langle n_1, n_2 \rangle$). We apply the Weierstrass preparation theorem to this equation which reduces to a formula of the form

$$g_0 + g_1 n_1 + \cdots + g_s n_1^s = 0 \ .$$

In fact, in Theorem 2 the function h cannot be identically 0 because $h_{(0,0)} = 1$, hence the solution of our first equation must be a zero of a polynomial of degree s. In this way, we can hope to eliminate the variable n_1 of the equations of our system. In order to apply this method to the curve of the introduction, let us compute the power series associated to it following the "elliptic curve Chabauty" method described in [6]. For this, we first need to compute the Mordell-Weil group $\mathcal{E}(\mathbf{K})$.

4. Computing $\mathcal{E}(\mathbf{K})$

We first compute the rank of the curve with the program of D. Simon [10]. The curve $\mathcal{E}(\mathbf{K})$ has rank 2. It is torsion-free and generators for $\mathcal{E}(\mathbf{K})/2\mathcal{E}(\mathbf{K})$ are $G_1 = (0, 1)$ and $G_2 = (1, 1 - \beta^2)$.

We have now to find a basis for the full Mordell-Weill group $\mathcal{E}(\mathbf{K})$. For this we perform an infinite descent as described by Siksek in [8].

Proposition 2. *G_1 and G_2 are generators for the full Mordell-Weill group.*

Proof. The first step is to bound the difference between the naive height and the canonical height on $\mathcal{E}$. The method developed by Siksek allows us to prove that for any point P in $\mathcal{E}(\mathbf{K})$, we have

$$h(P) - \hat{h}(P) \leq 0.217 \ .$$

The second step is to prove that there are no point in $\mathcal{E}(\mathbf{K})$ with canonical height less than 0.5. If P is such a point, its naive height must be less than 0.717 thanks to the first step. We have now to test which elements of $\mathbf{K}$ with logarithmic height less than 0.717 are corresponding to points in $\mathcal{E}(\mathbf{K})$ with canonical height less than 0.5. Such elements are represented by polynomials with integral coefficients of degree less than 3 and with Mahler mesure less than 8.6. There are only finitely many such polynomials and we can compute all of them. By this way, we prove that 0 and 1 are the only elements of $\mathbf{K}$ which are the x-coordinate of any point in $\mathcal{E}(\mathbf{K})$ with naive height less than 0.717. The canonical height of these points (G_1 and G_2) are respectively 0.8054... and 0.9715.... Hence we proved that there are no point in $\mathcal{E}(\mathbf{K})$ with canonical height less than 0.5.

For the last step we use the following standard fact:

If $\mathcal{E}(\mathbf{K})$ contains no point of infinite order with canonical height less than λ and G_1, G_2 generate a sublattice of $\mathcal{E}(\mathbf{K})$ of full rank 2, then the index of the span of G_1, G_2 in $\mathcal{E}(\mathbf{K})$ satisfies

$$n \leq R(G_1, G_2)^{1/2} \frac{\gamma_2}{\lambda} \ ,$$

where $\gamma_2 = 2/\sqrt{3}$ and $R(G_1, G_2) \leq 0.718$ is the determinant of the height pairing matrix.

We proved in the second step that we can choose $\lambda = 1/2$, so that $n \leq 1.96$. This means that n must be equal to 1 and then that G_1 and G_2 are generators for $\mathcal{E}(\mathbf{K})$. $\square$

5. Elliptic curve Chabauty for $\mathcal{C}$

In this section, we follow the method explain in [6].

We then choose a prime p satisfying the six conditions given in [6]: the prime 3 satisfies these conditions. The order of $\widetilde{G_1}$ is 11 and the order of $\widetilde{G_2}$ is 33, where hereafter, $\widetilde{}$ denotes the reduction modulo 3. If we define $G_3 = G_1 - 3G_2$, (G_2, G_3) is still a basis for $\mathcal{E}(\mathbf{K})$ and the order of $\widetilde{G_3}$ is 1, so we define:

- $m_1 = 1$ and $m_2 = 33$,
- $Q_1 = G_3$ and $Q_2 = 33G_2$,
- $\mathcal{S} = \{\infty, \pm iG_2,\ 1 \leq i \leq 16\}$,

so that every $P \in \mathcal{E}(\mathbf{K})$ can be written as $P = S + n_1Q_1 + n_2Q_2$ for some $S \in \mathcal{S}, n_1, n_2 \in \mathbb{Z}$.

We first want to reduce the size of the set $\mathcal{S}$.

Since by construction Q_1 and Q_2 are in the kernel of reduction modulo 3, $\widetilde{P} = \widetilde{S}$. Hence if P has a $\mathbb{Q}$-rational x-coordinate then $\widetilde{S}$ must have an $\mathbb{F}_3$-rational x-coordinate. Computing the elements of $\mathcal{S}$ mod 3, we find that this is true for $S = \infty, \pm G_2, \pm 3G_2, \pm 14G_2$, and so these are the only $S \in \mathcal{S}$ that we need to consider.

Moreover, since n_1 and n_2 are in $\mathbb{Z}$, it is of course not necessary to consider $-G_2, -3G_2$ and $-14G_2$.

In fact, $-G_2 + n_1Q_1 + n_2Q_2 = -(G_2 - n_1Q_1 - n_2Q_2)$. Since we are interested in the x-coordinate of such a point, we have only to consider the points in $\mathcal{E}(\mathbf{K})$ which can be written as $S + n_1Q_1 + n_2Q_2$ for some $S \in \mathcal{S}', n_1, n_2 \in \mathbb{Z}$ if $\mathcal{S}'$ denotes the set $\{\infty, G_2, 3G_2, 14G_2\}$.

For each point $Q_i = (x_i, y_i)$, define the z-coordinate of Q_i as $z_i = -x_i/y_i$, and let $g_3 = 1$, $g_2 = -2$, $g_1 = 1 - \beta - 4\beta^2$ and $g_0 = 1$ be the coefficients of our elliptic curve.

We will now compute the z-coordinate of an arbitrary $P \in \mathcal{E}(\mathbf{K})$ in terms of n_1 and n_2. For this, we use the formal group law on elliptic curves and the formal logarithm and exponential (see [9] for details).

Note that, in our cases, it will be sufficient to work mod 3^5.

Thanks to the fact that $k!$ times the coefficient of t^k in $\log(t)$ or $\exp(t)$ belongs to $\mathbb{Z}[g_0, g_1, g_2, g_3]$ and the standard estimate $|k!|_p \geq p^{-(k-1)/(p-1)}$, the terms in $O(t^9)$ can be ignored in the formulas.

Let $\theta_\infty(n_1, n_2)$ denote the inverse of the x-coordinate of $n_1Q_1 + n_2Q_2$ and $\theta_S(n_1, n_2)$ denote the x-coordinate of $S + n_1Q_1 + n_2Q_2$ if $S \neq \infty$. We can split θ_S into its components:

$$\theta_S(n_1, n_2) = \theta_S^{(0)}(n_1, n_2) + \theta_S^{(1)}(n_1, n_2)\beta + \theta_S^{(2)}(n_1, n_2)\beta^2 \ .$$

If the x-coordinate of P is $\mathbb{Q}$-rational, then $\theta_S^{(1)}(n_1, n_2)$ and $\theta_S^{(2)}(n_1, n_2)$ must be equal to 0, giving our system of two power series in two variables. In other words, we have to determine which (n_1, n_2) satisfies $\theta_S^{(1)}(n_1, n_2) = \theta_S^{(2)}(n_1, n_2) = 0$ in order to obtain a bound for points on $\mathcal{E}(\mathbf{K})$ with a $\mathbb{Q}$-rational x-coordinate.

We first compute the z-coordinate of Q_i and its formal logarithm modulo 3^5:

$$\begin{aligned} z_1 &\equiv 240 + 84\beta + 57\beta^2 \pmod{3^5}\ , \\ z_2 &\equiv 60 + 99\beta + 195\beta^2 \pmod{3^5}\ , \\ \log(z_1) &\equiv 42 + 48\beta + 39\beta^2 \pmod{3^5}\ , \\ \log(z_2) &\equiv 15 + 117\beta + 15\beta^2 \pmod{3^5}\ . \end{aligned}$$

We now substitute $n_1 \log(z_1) + n_2 \log(z_2)$ in the expression of the formal exponential and we obtain:

$$\begin{aligned} z\text{-coord of } n_1 Q_1 + n_2 Q_2 \equiv\ & ((162n_2^2 + 18)n_1^3 + (162n_2^3 + 216n_2)n_1^2 \\ & +(81n_2^4 + 81n_2^2 + 39)n_1 + (63n_2^3 + 132n_2))\beta^2 \\ & +(81n_1^5 + (162n_2^2 + 198)n_1^3 + (81n_2^3 + 189n_2)n_1^2 \\ & +(162n_2^4+216n_2^2+48)n_1+(162n_2^5+63n_2^3+117n_2))\beta \\ & +162n_1^5 + 162n_2n_1^4 + 36n_1^3 + (81n_2^3 + 162n_2)n_1^2 \\ & +(162n_2^2 + 42)n_1 + (45n_2^3 + 15n_2) \pmod{3^5}\ . \end{aligned}$$

Hence, we have $\theta_\infty(n_1, n_2)$ as a power series in two variables and:

$$\begin{aligned} \theta_\infty(n_1, n_2) \equiv\ & (27n_1^4 + 81n_2^3n_1^3 + (81n_2^2 + 207)n_1^2 + (27n_2^3 + 117n_2)n_1 \\ & +(189n_2^4 + 198n_2^2)) + [54n_1^4 + (162n_2^3 + 162n_2)n_1^3 + 126n_1^2 \\ & +(189n_2^3 + 144n_2)n_1 + (189n_2^4 + 126n_2^2)]\beta + [189n_1^4 \\ & +(81n_2^3 + 54n_2)n_1^3 + (162n_2^2 + 108)n_1^2 + (162n_2^3 + 225n_2)n_1 \\ & +(189n_2^4 + 54n_2^2)]\beta^2 \pmod{3^5}\ . \end{aligned}$$

$$\begin{aligned} \text{and so } \theta_\infty^{(1)}(n_1, n_2) \equiv\ & 54n_1^4 + (162n_2^3 + 162n_2)n_1^3 + 126n_1^2 + (189n_2^3 + 144n_2)n_1 \\ & +(189n_2^4 + 126n_2^2) \pmod{3^5}\ . \\ \theta_\infty^{(2)}(n_1, n_2) \equiv\ & 189n_1^4 + (81n_2^3 + 54n_2)n_1^3 + (162n_2^2 + 108)n_1^2 \\ & +(162n_2^3 + 225n_2)n_1 + (189n_2^4 + 54n_2^2) \pmod{3^5}\ . \end{aligned}$$

In the same way, we show that:

$$\begin{aligned} \theta_{G_2}^{(1)}(n_1, n_2) \equiv\ & 162n_1^4 + (81n_2^2 + 162n_2 + 9)n_1^3 \\ & +(81n_2^3 + 162n_2^2 + 108n_2 + 234)n_1^2 \\ & +(162n_2^4 + 189n_2^3 + 198n_2 + 123)n_1 \\ & +(189n_2^4 + 18n_2^3 + 162n_2^2 + 237n_2) \pmod{3^5}\ . \end{aligned}$$

$$\begin{aligned} \theta_{G_2}^{(2)}(n_1, n_2) \equiv\ & 162n_1^5 + (162n_2 + 54)n_1^4 + (162n_2^3 + 108n_2 + 36)n_1^3 \\ & +(81n_2^3 + 153)n_1^2 + (27n_2^3 + 162n_2^2 + 216n_2 + 150)n_1 \\ & +(45n_2^3 + 33n_2) \pmod{3^5}\ . \end{aligned}$$

$$\begin{aligned}\theta^{(1)}_{3G_2}(n_1,n_2) \equiv\ & 162n_1^5 + 135n_1^4 + (162n_2^3 + 81n_2^2 + 81n_2 + 207)n_1^3 \\ & +(162n_2^3 + 162n_2^2 + 216n_2 + 225)n_1^2 \\ & +(81n_2^4 + 54n_2^3 + 27n_2^2 + 153n_2 + 105)n_1 \\ & +(81n_2^6+81n_2^5+54n_2^4+99n_2^3+18n_2^2+27n_2+138) \pmod{3^5}\ .\end{aligned}$$

$$\begin{aligned}\theta^{(2)}_{3G_2}(n_1,n_2) \equiv\ & 81n_1^6+(81n_2^2+162n_2+9)n_1^3+(81n_2^3+162n_2^2+108n_2 + 234)n_1^2 \\ & +(162n_2^4 + 27n_2^3 + 81n_2^2 + 225n_2 + 69)n_1 \\ & +(162n_2^6 + 27n_2^4 + 126n_2^3 + 216n_2^2 + 12n_2 + 93) \pmod{3^5}\ .\end{aligned}$$

$$\begin{aligned}\theta^{(1)}_{14G_2}(n_1,n_2) \equiv\ & (162n_2 + 108)n_1^4 + (81n_2^3 + 81n_2 + 135)n_1^3 \\ & +(162n_2^2+54n_2+189)n_1^2+(81n_2^4+162n_2^3+54n_2^2+108n_2+60)n_1 \\ & +(162n_2^5 + 81n_2^4 + 45n_2^3 + 36n_2^2 + 171n_2 + 189) \pmod{3^5}\ .\end{aligned}$$

$$\begin{aligned}\theta^{(2)}_{14G_2}(n_1,n_2) \equiv\ & 162n_1^5 + (81n_2 + 108)n_1^4 + (81n_2^3 + 81n_2^2 + 135n_2 + 126)n_1^3 \\ & +(162n_2^3 + 81n_2^2 + 81n_2 + 99)n_1^2 \\ & +(189n_2^3 + 54n_2^2 + 18n_2 + 162)n_1 \\ & +(162n_2^5+54n_2^4+108n_2^3+135n_2^2+207n_2+150) \pmod{3^5}\ .\end{aligned}$$

In all these cases, we have to solve a system of two power series in two variables. We already know solutions to these systems, for example $(0, 0)$ for the first one. Thanks to the Weierstrass preparation theorem, we will now try to bound the number of solutions and hope that the bound will correspond to the number of known solutions.

6. Application of the Weierstrass preparation theorem in two variables to the curve $\mathcal{C}$

We have shown that the only rational points on the curve $\mathcal{C}$ which are apt to have a $\mathbb{Q} - rational$ x-coordinate can be written $\pm S + n_1Q_1 + n_2Q_2$ with $S = \infty, G_2, 3G_2$ or $14G_2$. Moreover, for each of these S, n_1 and n_2 satisfy a system of two equations. Let us first consider the case $S = G_2$.

6.1. The linear Weierstrass preparation theorem ($s = 1$) and θ_{G_2}

We have

$$\begin{aligned}\theta^{(1)}_{G_2}(n_1,n_2) \equiv\ & 162n_1^4 + (81n_2^2 + 162n_2 + 9)n_1^3 \\ & +(81n_2^3 + 162n_2^2 + 108n_2 + 234)n_1^2 \\ & +(162n_2^4 + 189n_2^3 + 198n_2 + 123)n_1 \\ & +(189n_2^4 + 18n_2^3 + 162n_2^2 + 237n_2) \pmod{3^5}\ .\end{aligned}$$

$$\begin{aligned}\theta^{(2)}_{G_2}(n_1,n_2) \equiv\ & 162n_1^5 + (162n_2+54)n_1^4 + (162n_2^3+108n_2+36)n_1^3 \\ & +(81n_2^3+153)n_1^2 + (27n_2^3+162n_2^2+216n_2+150)n_1 \\ & +(45n_2^3+33n_2) \pmod{3^5}\ .\end{aligned}$$

We want to apply the Weierstrass preparation theorem to $\theta^{(1)}_{G_2}(n_1,n_2)$. In our case $p=3$, let us consider

$$\begin{aligned}f(n_1,n_2) = \frac{1}{3}\theta^{(1)}_{G_2}(n_1,n_2) \equiv\ & 54n_1^4 + (27n_2^2+54n_2+3)n_1^3 \\ & +(27n_2^3+54n_2^2+36n_2+78)n_1^2 \\ & +(54n_2^4+63n_2^3+66n_2+41)n_1 \\ & +(63n_2^4+6n_2^3+54n_2^2+79n_2) \pmod{3^4}\ .\end{aligned}$$

Since by construction $f_{(i,j)}$ converges to 0 as $i+j \to \infty$ (see [6]), $f \in \mathbb{Z}_3\langle n_1,n_2\rangle$. Moreover $f_1(n_2)$ is a unit element of $\mathbb{Z}_3\langle n_2\rangle$ (because $f_1(n_2) \equiv 2 \pmod 3$) and 3 divides $f_i(n_2)$ for all $i \geq 2$. It follows that f is general in n_1 of order 1.

Applying the method described in Section 3, we have

$$h_1 = \sum_{k=0}^{\infty} \frac{(-1)^k}{g_1^{k+1}} f_{k+2}\, g_0^k\ , \tag{4}$$

$$g_0 = f_0\ , \tag{5}$$

$$g_1 = f_1 - g_0\, h_1\ , \tag{6}$$

We know f_0 and f_1 modulo 3^4, hence we know g_0 modulo 3^4, and we want to compute g_1 modulo 3^4.

We know that $h_1 \equiv 0 \pmod 3$, hence $g_0 \equiv f_0 \equiv n_2 \pmod 3$ and $g_1 \equiv f_1 \equiv 2 \pmod 3$.

Let us follow the method described in Section 3 in order to compute g_1 modulo 9. The inverse of g_1 modulo 3 is equal to 2. Since the f_i's are known modulo 9, are divisible by 3, and known to be $0 \pmod 9$ for all i greater than 4, we can compute h_1 modulo 9 using Equation (4):

$$h_1(n_2) \equiv -3n_2 + 3 \pmod 9.$$

Hence, we can compute g_1 modulo 9 using Formula (6):

$$g_1(n_2) \equiv 3n_2^2 + 5 \pmod 9.$$

All the functions are now known modulo 9 and we can reapply this method. Finally we compute g_0 and g_1 modulo 3^4 and obtain

$$g_0(n_2) \equiv 63n_2^4 + 6n_2^3 + 54n_2^2 + 79n_2 \pmod{3^4}\ , \tag{7}$$

$$g_1(n_2) \equiv 27n_2^5 + 9n_2^3 + 30n_2^2 + 54n_2 + 41 \pmod{3^4}\ . \tag{8}$$

Hence we have, using Theorem 2

$$\frac{\theta^{(1)}_{G_2}(n_1,n_2)}{3} = (g_0(n_2) + g_1(n_2)n_1)(1 + \sum_{i=1}^{\infty} h_i(n_2)n_1^i)\ ,$$

with $||h_i(n_2)|| < 1$ for all $i > 0$.

It follows that the condition $\theta^{(1)}_{G_2}(n_1, n_2) = 0$ implies that $g_0(n_2) + g_1(n_2)n_1$ must be 0, and so for any given n_2 there is at most one solution in n_1 to our equation, and moreover the above theorem gives us an explicit solution $\phi(n_2) = -g_0(n_2)/g_1(n_2)$ in $\mathbb{Z}_3\langle n_2\rangle$, so that

$$n_1 = \phi(n_2) \equiv 54n_2^5 + 45n_2^4 + 72n_2^3 + 27n_2^2 + 4n_2 \pmod{3^4} .$$

We can now compute $\theta^{(2)}_{G_2}(\phi(n_2), n_2)$. Since $\theta^{(2)}_{G_2} \in \mathbb{Z}_3\langle n_1, n_2\rangle$, we obtain a power series $\psi \in \mathbb{Z}_3\langle n_2\rangle$ and we have

$$\psi(n_2) \equiv 54n_2^4 + 27n_2^3 + 72n_2^2 + 66n_2 \pmod{3^4} .$$

We can now apply Strassman's theorem (i.e., the Weierstrass preparation theorem in one variable) to this power series and we obtain at most one solution for n_2. We know that $n_2 = 0$ is a solution, so this is the only one.

Finally, we have shown that $(0, 0)$ is the unique solution to

$$\theta^{(1)}_{G_2}(n_1, n_2) = \theta^{(2)}_{G_2}(n_1, n_2) = 0 ,$$

as required.

Of course it was not really necessary to work modulo 3^5, but we did this in order to explain the computations. We note that this method can always be applied when $s = 1$.

Let us now consider the case $S = \infty$.

6.2. The quadratic weierstrass preparation theorem ($s = 2$) and θ_∞

We have

$$\begin{aligned}\theta^{(1)}_\infty(n_1, n_2) \equiv{}& 54n_1^4 + (162n_2^3 + 162n_2)n_1^3 + 126n_1^2 + (189n_2^3 + 144n_2)n_1 \\ &+(189n_2^4 + 126n_2^2) \pmod{3^5} .\end{aligned}$$

$$\begin{aligned}\theta^{(2)}_\infty(n_1, n_2) \equiv{}& 189n_1^4 + (81n_2^3 + 54n_2)n_1^3 + (162n_2^2 + 108)n_1^2 \\ &+(162n_2^3 + 225n_2)n_1 + (189n_2^4 + 54n_2^2) \pmod{3^5} .\end{aligned}$$

We want to apply the Weierstrass preparation theorem to $\theta^{(1)}_\infty(n_1, n_2)$. In our case p is equal to 3, and let us consider the function f of $\mathbb{Z}_p\langle n_1, n_2\rangle$ given by

$$\begin{aligned}f(n_1, n_2) &= \frac{1}{9}\theta^{(1)}_\infty(n_1, n_2) , \\ &\equiv 6n_1^4 + (18n_2^3 + 18n_2)n_1^3 + 14n_1^2 + \\ &\quad (21n_2^3 + 16n_2)n_1 + (21n_2^4 + 14n_2^2) \pmod{3^3} .\end{aligned}$$

$f_2(n_2)$ is a unit of $\mathbb{Z}_3\langle n_2\rangle$ (because is it equal to 2 modulo 3) and 3 divides $f_i(n_2)$ for all $i \geq 3$. Hence f is general in n_1 of order 2.

Using our method, we can compute g_0, g_1 and g_2 modulo 3^3. We obtain:

$$\begin{aligned} g_0(n_2) &\equiv 21n_2^4 + 14n_2^2 \pmod{3^3} , \\ g_1(n_2) &\equiv 18n_2^5 + 6n_2^3 + 16n_2 \pmod{3^3} , \\ g_2(n_2) &\equiv 14 \pmod{3^3} . \end{aligned}$$

Hence we have

$$\frac{\theta_\infty^{(1)}(n_1, n_2)}{9} = (g_0(n_2) + g_1(n_2)n_1 + g_2(n_2)n_1^2)(1 + \sum_{i=0}^{\infty} h_i(n_2)n_1^i) ,$$

with $||h_i(n_2)|| < 1$ for all $i > 0$.

Thus, the condition $\theta_\infty^{(1)}(n_1, n_2) = 0$ implies that $g_0(n_2)+g_1(n_2)n_1+g_2(n_2)n_1^2 = 0$. Hence, for any given n_2 there are at most two solutions in n_1 to our equation. Moreover, $g_2(n_2)$ is invertible in $\mathbb{Z}_3\langle n_2\rangle$, hence there exist power series ϕ_0 and ϕ_1 in $\mathbb{Z}_3\langle n_2\rangle$ such that

$$n_1^2 = \phi_0(n_2) + \phi_1(n_2)n_1 .$$

Let us substitute recursively n_1^2 by $\phi_0(n_2) + \phi_1(n_2)n_1$ in the equation $\frac{\theta_\infty^{(2)}(n_1,n_2)}{9} = 0$. We deduce that there exist power series ψ_0 and ψ_1 in $\mathbb{Z}_3\langle n_2\rangle$ such that

$$\psi_0(n_2) + \psi_1(n_2)n_1 = 0 . \tag{9}$$

In our case, we have

$$\begin{aligned} \psi_0(n_2) &\equiv 9n_2^6 + 24n_2^4 + 21n_2^2 \pmod{3^3} , \\ \psi_1(n_2) &\equiv 18n_2^5 + 24n_2^3 + 19n_2 \pmod{3^3} . \end{aligned}$$

Thanks to the fact that 19 is invertible modulo 3^3, we deduce from (9) that there exists a power series $\Psi = -\frac{\psi_0}{\psi_1}$ in $\mathbb{Z}_3\langle n_2\rangle$ such that $n_1 = \Psi(n_2)$. In our case, we have

$$\Psi(n_2) \equiv 21n_2^3 + 6n_2 \pmod{3^3} .$$

We can now compute $f(\Psi(n_2), n_2) \in \mathbb{Z}_3\langle n_2\rangle$ and we can apply Strassman's theorem to this power series. In our case, we have

$$f(\Psi(n_2)) \equiv 15n_2^4 + 20n_2^2 \pmod{3^3} .$$

Applying Strassman's theorem to $\frac{f(\Psi(n_2))}{n_2^2}$ allows us to conclude that $n_2 = 0$ is the only solution to $f(\Psi(n_2), n_2) = 0$ and finally that $n_1 = n_2 = 0$ is the only solution to our problem.

Finally, we have shown that $(0, 0)$ is the only solution to

$$\theta_\infty^{(1)}(n_1, n_2) = \theta_\infty^{(2)}(n_1, n_2) = 0 ,$$

as required.

7. Conclusion

As for θ_{G_2}, we can show that $n_1 = 1, n_2 = 0$ is the unique solution to $\theta^{(1)}_{3G_2}(n_1, n_2) = \theta^{(2)}_{3G_2}(n_1, n_2) = 0$. In order to prove that $\theta^{(1)}_{14G_2}(n_1, n_2) = \theta^{(2)}_{14G_2}(n_1, n_2) = 0$ has no solution, we only need to apply Strassman's theorem to $\theta^{(2)}_{14}(n_1, n_2)$ with respect to one of the variables (the term having largest 3-adic norm is the constant term).

This shows that the only **K**-rational points on the curve $\mathcal{E}$ with $\mathbb{Q}$-rational x-coordinates are ∞, $\pm G_2$ and $\pm(3G_2 + Q_1) = \pm G_1$. It follows that the only possible x-coordinates for a $\mathbb{Q}$-rational point on $\mathcal{C}$ are $\{\infty,\ 0,\ 1\}$, thus proving Theorem 1.

There is a more general method to apply the Weierstrass preparation theorem: we can compute the functions g_i for each of the power series. By this way we obtain 2 polynomials P_1 and P_2 in n_1 with coefficients in $\mathbb{Z}_p < n_2 >$. Our goal is to bound the number of solutions (n_1, n_2) of $P_1 = P_2 = 0$. It is then natural to compute the resultant of P_1 and P_2 which is a power series in $\mathbb{Z}_p < n_2 >$. Then applying Strassman's theorem allows to bound the number of solutions.

I write a Maple program which compute the function g_i and h_i as explained in section 3 and apply this method in order to bound the number of p-adics solutions of systems of two power series in two variables. This program is available by ftp:
`ftp://megrez.math.u-bordeaux.fr/pub/duquesne`
or on my home page on the web:
`http://www.math.u-bordeaux.fr/~duquesne/programs`.

To conclude, we see that the use of the Weierstrass preparation theorem in two variables allows us to extend the elliptic curve Chabauty method to elliptic curves of rank 2 over number fields. In the same way, by writing explicitly the Weierstrass preparation theorem in n variables it is easy to extend the method to elliptic curves of rank n over number fields of degree strictly larger than n.

References

[1] Bruin, N.: Chabauty methods and covering techniques applied to generalized Fermat equation, PhD Dissertation, Leiden University, (1999)

[2] Cassels, J.W.S.: Local fields, London Math. Soc. Student Texts **3**, Cambridge University Press, (1986)

[3] Chabauty, C.: Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension, C.R.A.S. Paris **212**, 1022–1024 (1941)

[4] Coleman, R.F.: Effective Chabauty, Duke Math. J. **52**, 765–780 (1985)

[5] Flynn, E.V.: A flexible method for applying Chabauty's theorem, Compositio Mathematica **105**, 79–94 (1997)

[6] Flynn, E.V., Wetherell, J.L.: Finding rational points on bielliptic genus 2 curves, Manuscripta Math. **100**, 519–533 (1999)

[7] Flynn, E.V.: On $\mathbb{Q}$-derived polynomials, Manuscript (2000), to appear in Proc. Edinburgh Math. Soc.

[8] Siksek, S.: Infinite descent on elliptic curves, Rocky Mountain Journal of Mathematics **25**(4), 1501–1538 (1995)

[9] Silverman, J.: The arithmetic of elliptic curves, Springer, (1986)

[10] Simon, D.: Computing the rank of elliptic curves over number fields, Manuscript (2000), to appear in LMS J. Comput. Math.

[11] Stoll, M.: Implementing 2-descent for Jacobians of hyperelliptic curves, Acta Arith. **98**(3), 245–277 (2001)
[12] Sugatani, T.: Rings of convergent power series and Weierstrass preparation theorem, Nagoya Math. J. **81**, 73–78 (1981)
[13] Wetherell, J.L.: Bounding the number of rational points on certain curves of high rank, PhD Dissertation, University of California at Berkeley, (1997)

Numerical investigations related to the derivatives of the L–series of certain elliptic curves

C. Delaunay, S. Duquesne

September 23, 2003

Abstract

In [Zagier and Kramarz 1987], the authors computed the critical value of the L-series of the family of elliptic curves $x^3+y^3=m$ and they pointed out some numerical phenomena concerning the frequency of curves with a positive rank and the frequency of occurrences of the Tate-Shafarevitch groups Ш in the rank 0 case (assuming the Birch and Swinnerton-Dyer conjecture). In this paper, we give a similar study for the family of elliptic curves associated to simplest cubic fields. These curves have a nonzero rank and we discuss about the density of curves of rank 3 that occurs. We also remark a possible positive density of nontrivial Tate–Shafarevitch groups in the rank 1 case. Finally, we give examples of curves of rank 3 and 5 for which the group Ш is nontrivial.

1 Introduction and Motivations

Let E be an elliptic curve defined over $\mathbb{Q}$. From the work of [Wiles 1995], [Taylor and Wiles 1995] and [Breuil et al. 2001], E is known to be modular. This implies that its L-function $L(E,s)$ can be analytically continued to the whole complex plane. Furthermore, if N is the conductor of E, then the following functional equation holds:

$$\Lambda(E,2-s)=\varepsilon\Lambda(E,s) \quad , \tag{1}$$

where $\varepsilon=\pm 1$ is the sign of the functional equation and:

$$\Lambda(E,s)=\left(\frac{\sqrt{N}}{2\pi}\right)^s\Gamma(s)L(E,s) \quad .$$

In this paper, we are interested in computing the analytic order of the Tate–Shafarevich group Ш of certain elliptic curves E defined over $\mathbb{Q}$ using the Birch and Swinnerton-Dyer (BSD) conjecture:

Conjecture 1 (Birch and Swinnerton-Dyer) *Let r denote the rank of the Mordell-Weil group $E(\mathbb{Q})$. We have:*

$$\lim_{s\to 1}\frac{L(E,s)}{(s-1)^r}=\frac{c\,\Omega\,R}{|E(\mathbb{Q})_{tors}|^2}|Ш| \quad , \tag{2}$$

where c denotes the product of the Tamagawa numbers, Ω the real period and R the regulator of E.

In [Zagier and Kramarz 1987], Kramarz and Zagier carried out some numerical computations related to the family of elliptic curves given by equations $x^3 + y^3 = m$ (the so-called Sylvester cubics). They computed the critical value of the L-functions of the curves having an even functional equation (i.e. $\varepsilon = 1$) for $m \leq 70000$ and they pointed out some numerical phenomena concerning the frequency of curves with a positive rank and the frequencies of occurrences of $|Ш|$ in the rank 0 case (with formula (2)). More precisely, concerning the rank, their numerical data suggest a possible positive density of curves with positive rank. In [Watkins], Watkins extended the computations to $m = 10^7$, the results being that the density of positive rank is finally decreasing and probably tends to zero like $x^{5/6}\log(x)^C$ (with some constant $C \approx 3/5$). The behaviour $x^{5/6}$ was already mentioned in [Zagier and Kramarz 1987], and stronger models using random matrix theory as in [Conrey et al. 2000] should give $x^{5/6}\log(x)^C$ for some constant C.
Watkins computations confirm the remark on Kramarz and Zagier that the frequency of occurrences of $|Ш| = 1$, $|Ш| = 4$, etc. among rank 0 curves is decreasing. Heuristics in [Delaunay 2001] predict that these frequencies should be 0 (but note that these heuristics predict a general behaviour for all elliptic curves and that we are only concerned here with very specific families). Furthermore, the numerical results of Watkins about the question of how often a given prime p divides $|Ш|$ seem to be not too much discordant with the predictions in [Delaunay 2001] (at least for $p \neq 3$).

In this paper, we make a similar experimental study but in the case of a family of elliptic curves with positive rank. It is quite natural and interesting to wonder if the same phenomena will occur or not and, in fact, as far as we know there is no such study in the literature. In the case of positive rank, heuristics in [Delaunay 2001] predict that there is a positive density of curves with nontrivial Tate–Shafarevich group but, in practice, they are quite sparsely observed. For example, the tables of Cremona ([Cremona data]) found only 196 such curves among all elliptic curves of conductor less than 20000, furthermore all these 196 curves have rank one and most of them have $Ш = 4$. Indeed, there are infinitely many rational points on such curves, so that it is more difficult to find p-adic points not corresponding to rational points. In fact, nontrivial Tate–Shafarevich groups appear for large conductors.
The problem of computing $|Ш|$ using formula (2) when the rank is positive is much more complicated because on the one hand we have to determine the regulator R (in the rank-zero case, the regulator is simply $R = 1$) and on the other hand we have to deal with quite large conductors to be able to detect nontrivial Ш.
Here, we are concerned with the family of elliptic curves associated to the simplest cubic fields (see below) which were introduced by Shanks in [Shanks 1974] and were studied by Washington ([Washington 1987]) and more recently in

[Duquesne 2001]. This family has properties interesting for our purpose. Each of these curves has an odd rank and an explicit generator so that the regulator is easily computable when the rank is one. The conductor grows fast so that we can hope finding nontrivial Tate-Shafarevich groups. We compute, using the GP-Pari software ([PARI]), values of $L'(E,1)$ for many of these curves and deduce from them and from formula (2) analytic orders of Tate–Shafarevich groups for the rank-one case. The method we used are well known since we have to evaluate a rapidly converging series (see formula (6)), and are explained in [Cohen 1993] and in [Cremona 1997]. Furthermore, several GP-programs are available, for example a program by Cremona and Womack ([Cremona and Womack], which computes the derivatives of L-functions of elliptic curves) or by Dokchitser ([Dokchitser], this program deals with general L-function having a classical functional equation).

According to our numerical data, we first observe an experimental positive-like density of curves with high ranks. In regard to the above Zagier-Kramarz extension by Watkins, we must be careful; indeed, the fact that the growth of the regulator can be well estimate allows to use the same argument-principle as in the case of the Sylvester cubics and it suggests the density of curves with ranks ≥ 3 may tend to 0. We also discuss about the density of occurrences of $|Ш|$ when the rank is one (with the same reticence as above). Finally, we find example of nontrivial Tate–Shafarevich groups for some curves of rank 3 and 5 by computing $L^{(3)}(E,1)$ and $L^{(5)}(E,1)$.

2 Elliptic curves associated to simplest cubic fields

In the sequel, m will always denotes a positive integer such that the number $\Delta = m^2 + 3m + 9$ is squarefree. Let E be the elliptic curve:

$$E \,:\, Y^2 = X^3 + mX^2 - (m+3)X + 1 \quad . \tag{3}$$

The field defined by the polynomial of the right hand side of (3) is said to be a simplest cubic field. These fields were introduced by Shanks in [Shanks 1974].

In [Washington 1987], Washington studied these fields and deduced some properties of the related elliptic curves (3) including the following result:

Theorem 2 (Washington) *The rank of the elliptic curve E is odd, assuming that the Tate–Shafarevitch group is finite.*

In [Duquesne 2001], the second author studies the structure of the Mordell–Weil group of these curves, and in particular proves:

Theorem 3 *The Mordell–Weil group $E(\mathbb{Q})$ is torsion-free and the point $(0,1)$ can always be taken as an element of a system of generators for $E(\mathbb{Q})$. In particular, if the rank of E is one, the point $(0,1)$ generates $E(\mathbb{Q})$.*

Let us now write down the classical invariants attached to these curves. The discriminant of E is $16\Delta^2$, its j-invariant is 256Δ. Note that $16\Delta^2$ is the discriminant of (3) and is the minimal discriminant of E whereas equation (3) does not give the minimal Weierstrass model. In fact, the minimal model is given by a slightly more complicated equation:

$$Y^2 = X^3+\varepsilon X^2-\big(3(k^2+k+1)+(2k+1)\varepsilon\big)\,X+(2k+1)(k^2+k+1)+k(k+1)\varepsilon \ ,$$

where $m = 3k+\varepsilon$ with $\varepsilon = \pm 1$ (if $\varepsilon = 0$, m does not define a simplest cubic field). Moreover, Tate's algorithm also allows us to compute the conductor and the Tamagawa numbers :

	$m \equiv 0 \pmod 2$	$m \equiv 1 \pmod 4$	$m \equiv 3 \pmod 4$
N	$16\Delta^2$	$8\Delta^2$	$4\Delta^2$
c	1	2	3

The table above gives N is about m^4 and grows sufficiently quickly as mentioned in the introduction.
In our case, the BSD conjecture predicts that:

$$L'(E,1) = c\ \Omega\ \widehat{h}\,((0,1))\ \ S \quad , \tag{4}$$

where $\widehat{h}$ is the canonical height on E and is computed using GP-Pari, Ω is the real period of E (which is easily computable using the AGM method) and:

$$S = \begin{cases} 0 & \text{if} \quad \text{rank}(E) > 1, \\ |Ш| & \text{if} \quad \text{rank}(E) = 1. \end{cases}$$

From the work of [Duquesne 2001], one can see that $\widehat{h}\,((0,1))$ behaves like $\log(m)$ and that $\Omega \simeq m^{-1/2}\log(m)$. Since, under GRH, $L'(E,1) = O(m^{\varepsilon})$, using formula (4), we obtain :

$$S = O(m^{1/2+\varepsilon}) \ . \tag{5}$$

Furthermore, the value of $L'(E,1)$ is computed by:

$$L'(E,1) = 2\sum_{n\geq 1}\frac{a_n}{n}\int_{\frac{2\pi n}{\sqrt{N}}}^{\infty} e^{-t}\frac{dt}{t} \quad , \tag{6}$$

where $L(E,s) = \sum_{n\geq 1} a_n n^{-s}$.
Thus, we compute S using (4). From the well-known work of Gross and Zagier ([Gross and Zagier 1986]) S is known to be a rational number. All the values that we find in our numerical calculations are near to perfect squares of integers as required by the BSD conjecture. This gives a check of our numerical computations.

3 Numerical results

We computed S for all integers m less than 14000 defining simplest cubic fields. For this, we need about $O(\sqrt{N})$ coefficients in the right hand side of formula (6) to obtain a reasonable accuracy for $L'(E,1)$. Since the conductor grows as m^4, we were led to consider sums with about m^2 terms (and so sums with about 2×10^8 terms for the largest values of m we considered). For this, the strategy that we use to get a sufficiently good approximation for $L'(E,1)$ is the following (the same sort of strategy is used in [Zagier and Kramarz 1987]) :

- We compute and store the values of the coefficients a_n for n less than some bound B of the order of $\sqrt{N}$ ($B = 1.67 \times 10^7$ for large values of m).
- We compute the partial sum in (6) using these first coefficients.
- Beyond B, we compute on the fly the coefficients a_n (if $n = n_1 n_2$ with $n_1, n_2 \leq B$, we can deduce a_n from a_{n_1} and a_{n_2}) and add their contributions to the sum. At each step, we add 10^6 new terms in the partial sum.
- We repeat the last step until two successive sums Σ_1 and Σ_2 satisfy:

$$|\Sigma_1 - \Sigma_2| < 0.02 \text{ and } |\Sigma_2 - s^2| < 0.02 \text{ for some } s \in \mathbb{Z}.$$

Note that for each prime p dividing the conductor we have $p^2|N$. Thus from Atkin–Lehner theory ([Atkin and Lehner 1970]), $(n,N) \neq 1 \Rightarrow a_n = 0$, and in particular $a_n = 0$ if n is even. This remark is helpful for computations.

For large values of the parameter (say $m \geq 8000$), the computation of $L'(E,1)$ requires a lot of time and memory. We needed several months of CPU on a Pentium III @ 1GHz to deal with the values of m less than 14000.
In order to give the numerical data that we obtained, we set:

$$\begin{aligned} N(x) &= \sharp\left\{m \leq x \mid m^2 + 3m + 9 \text{ is squarefree}\right\} \quad , \\ N_s(x) &= \sharp\left\{m \leq x \mid m^2 + 3m + 9 \text{ is squarefree and } S_m = s\right\} \quad . \end{aligned}$$

The results are summarized in the following table:

x	2000	4000	6000	8000	10000	12000	14000
$N(x)$	1246	2492	3739	4986	6234	7477	8722
$N_0(x)$	363	700	1031	1347	1681	2026	2328
$N_1(x)$	728	1384	2025	2677	3267	3828	4402
$N_4(x)$	101	235	389	522	703	868	1035
$N_9(x)$	45	141	227	326	427	540	674
$N_{16}(x)$	5	19	42	67	91	116	150
$N_{25}(x)$	3	11	17	32	46	72	97
$N_{36}(x)$	1	2	7	13	13	15	21
$N_{49}(x)$			1	1	3	7	9
$N_{64}(x)$					1	2	3
$N_{81}(x)$				1	2	3	3

3.1 Density of high rank curves

The discussion we give here is founded on the experimental data and several interpretations are possible so we must be careful all the more that the behaviour of the curves for $m \leq 14000$ may not mirror the general one when m tends to ∞ (as it is the case for the Zagier-Kramarz computations). A first approach concerning the frequency of occurrences of curves with $L'(E,1) = 0$ (and so of curves with rank ≥ 3) suggests that there is a positive density of such curves. Indeed, as it can be seen on figure (1), the ratio $N_0(x)/N(x)$ is fairly nearly constant (the constant being ≈ 0.27).

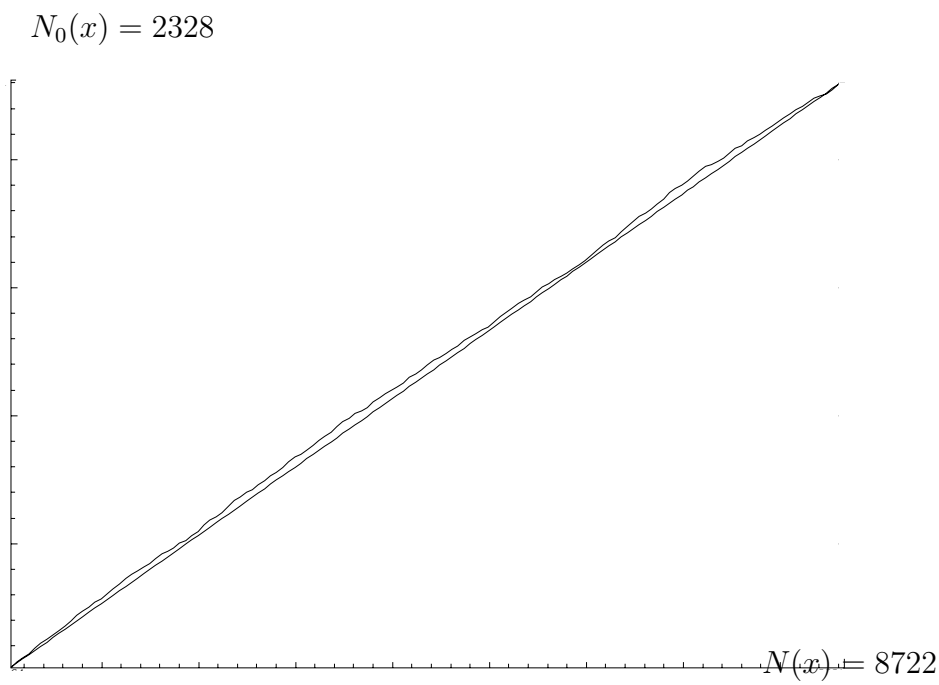


Figure 1: The points $(N(x), N_0(x))$ (and joined)

Such an observation should provide, as asked in [Zagier and Kramarz 1987] an example of a family of curves with an expected positive density of curves with high rank. Note that in the case of the simplest cubic fields, and contrary to the Fermat cubics, the curves are not isomorphic over any number field (their j-invariant is not constant). We should compare this 27% of extra-rank curves we obtained with the large table of Stein and Watkins in [Stein and Watkins 2002] extending the Brumer-McGuiness one ([Brumer and McGuinness 1990]) and for which 92.5% of their curves with odd functional equation have rank one (their database contains million of curves, and their conductors do not exceed 10^{10}). In

fact, one of the current opinion about the rank of elliptic curves is that asymptotically, the rank is the lowest one compatible with the sign of the functional equation ([Brumer and McGuinness 1990]). So, it would be very surprising if a positive density really occurs for our family.
Thanks to the estimate of formula (5), we can adapt the argument of Zagier and Kramarz : assuming S is, in fact, a random perfect square between 0 and $\sqrt{m}$ for each value of m, then the number of curves with $m \leq x$ that have rank greater than 1 should be about $x^{3/4}$. Moreover a naive extension of the conjecture [Conrey et al. 2000] to our case should provide the more precise estimate $x^{3/4}\log(x)^C$ for some constant C. However, it does not seem obvious how to extend the work of [Conrey et al. 2000] to the derivatives of L-functions even if, as in our case, the regulator can be well estimated. The interpretation above is corroborated by taking the best linear fit to a log-log graph of figure (1). We obtain by this way that the number of curves with $m < x$ that have rank greater than 1 appear to grow like $x^{0.967}$, which is enough close to $x^{3/4}\log(x)^{0.91}$ when $x \leq 14000$.

3.2 Frequency of occurrences of S

We also compute the frequency of occurrences of each analytic order of Tate–Shafarevich groups among curves of (analytic) rank 1. The figure 2 illustrates the results that we obtain.

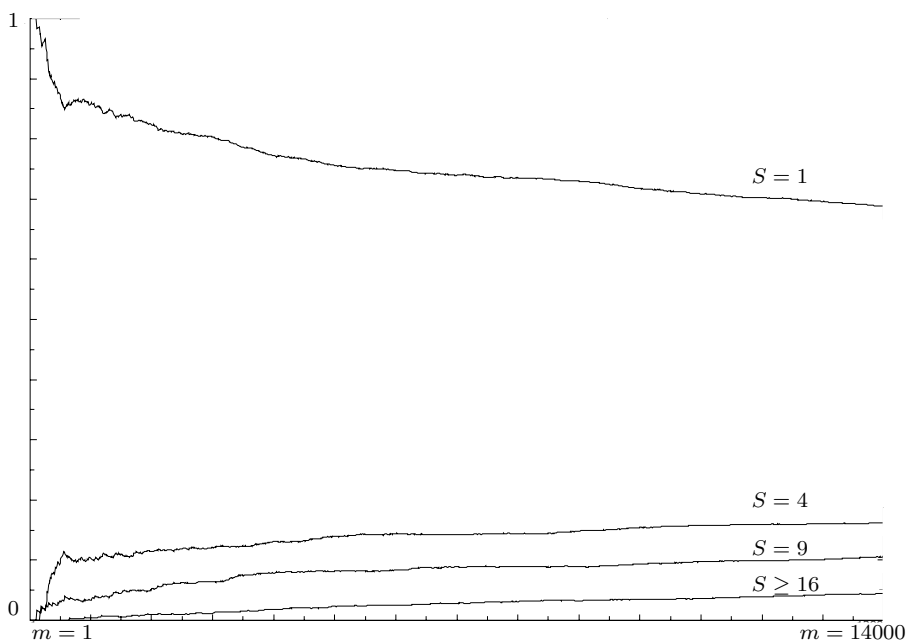


Figure 2: Frequencies of occurrence of S

Although we cannot produce sufficient data, we seem to have a positive density for each order. This is in accordance with the heuristics in [Delaunay 2001]. However the densities could differ from the predicted ones since we only consider a specific family of elliptic curves. For instance, 68.8% (resp. 18.9%, 10.9%) of rank 1 curves with $m \leq 14000$ have trivial Ш (resp. have 2 dividing S, have 3 dividing S) whereas [Delaunay 2001] would predict 54.9% (resp. 31.1%, resp. 12.3%).
Furthermore, the same heuristic argument as for $S = 0$ could be also used here and predicts that $N_S(x)/(N(x) - N_0(x))$ should tend to zero like $x^{3/4}$ and so clashes with the heuristics and seems to be discordant with our numerical data.

Arithmetic effects on m could also modify the frequencies we considered. In view of the invariants of E, it is natural to fit m into three cases : m even, $m \equiv 1 \mod 4$ and $m \equiv 3 \mod 4$ (in fact, other cases were considered as Δ prime for example, but gave the nearly the same results as in the general case). We sum up the results for all curves with $m \leq 14000$ in the following table :

	$\sharp\{S = 0\}$	$\sharp\{S = 1\}$	$\sharp\{S = 4\}$	$\sharp\{S = 9\}$	$\sharp\{S \geq 16\}$
$m \equiv 0 \mod 2$	964	2040	628	490	239
$m \equiv 1 \mod 4$	649	1133	256	110	32
$m \equiv 3 \mod 4$	715	1229	151	74	12

It follows from the data that the densities are, as in the general case, nearly constant for $m \leq 14000$ but depend on the class of m.
For $m \equiv 0 \mod 2$ (resp. $m \equiv 1 \mod 4$, $m \equiv 3 \mod 4$), there are about 22.1% (resp. 29.7%, 32.7%) of elliptic curves with $S = 0$. This difference could be explained by the fact that formula (4) and the invariant c force S to be smaller when m is odd, and so S is more often equal to 0 or 1 in this case. We also remark that all parametrization of [Duquesne 2001] in order to have elliptic curves with large rank give odd values of m.

4 Nontrivial Tate–Shafarevich groups of curves with rank 3 and 5

Among the 27% of our curves of rank 3 or more, we find some curves of analytic rank 3 with nontrivial Tate–Shafarevich group. For this, we use conjecture (2) and we compute $L'''(E, 1)$ by the method of Buhler, Gross and Zagier ([Buhler, Gross and Zagier 1985]).

The first example of rank greater than 1 for which the program `mwrank` of Cremona ([Cremona]) is not able to determine the rank completely is obtained with $m = 157$. As `mwrank` uses a 2-descent, this suggests a non trivial 2-part in the Tate–Shafarevich group. In order to compute the regulator, we check that the

points

$$P_1 = [-12, 151],\ P_2 = [0, 1] \text{ and } P_3 = [3, 31]$$

form a basis for $E(\mathbb{Q})$ using Siksek's method ([Siksek 1995]). Finally, we get $|Ш| = 4$, thus providing a nontrivial Tate–Shafarevich group for an elliptic curve of rank 3 (assuming BSD). Other such examples are given for examples by $m = 617, 830, 856, 943, 961$.

We can also obtain similar results for rank 5. In this case, the first value for which the `mwrank` program does not seem to determine the rank completely is $m = 3461$. Thus, this suggests a nontrivial 2-part. Indeed, we can check that the points:

$$[0, 1], [-4, 263], [-40, 2369], [-124, 7193] \text{ and } \left[\frac{-12}{169}, \frac{35725}{2197}\right]$$

give a basis for $E(\mathbb{Q})$ and so that $|Ш| = 4$ (under BSD).

Aknowledgements. We are very grateful to the anonymous referees for their comments and suggestions which improved this paper. We are very pleased to thank them here.

References

[Atkin and Lehner 1970] A. O. L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(N)$, Math. Ann. **185** (1970), 134–160.

[PARI] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, `pari-gp`, available at http://www.math.u-psud.fr/~belabas/pari/

[Buhler, Gross and Zagier 1985] J. Buhler, B. Gross and D. Zagier, *On the Conjecture of Birch and Swinnerton-Dyer for an Elliptic Curve of Rank 3*, Math. Comp. **44** (1985), no. 170, 473–481.

[Breuil et al. 2001] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over* $\mathbb{Q}$ *: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic).

[Brumer and McGuinness 1990] A. Brumer and O. McGuinness, *The behaviour of the Mordell-Weil group of elliptic curves*, Bull. Amer. Soc. **23** (1990), no. 2, 375–382.

[Cohen 1993] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Math. **138**, Springer-Verlag, New-York, 4-th corrected printing (2000).

[Conrey et al. 2000] J. Conrey, J. Keating, M. Rubinstein and N. Snaith, *On the frequency of vanishing of quadratic twists of modular L-functions*, Number theory for the millennium, I (Urbana, IL, 2000), 301–315, A. K. Peters, Natick, MA, 2002.

[Cremona 1997] J. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, (1997) second edition.

[Cremona] J. Cremona, `mwrank`, program available at http://www.maths.nott.ac.uk/personal/jec/.

[Cremona data] J. Cremona, *Elliptic curve data for conductors up to 20000* available at http://www.maths.nott.ac.uk/personal/jec/

[Cremona and Womack] J. Cremona and T. Womack, program available at http://www.maths.nott.ac.uk/personal/pmxtow/BG.gp

[Delaunay 2001] C. Delaunay, *Heuristics on Tate-Shafarevitch groups of elliptic curves defined over* $\mathbb{Q}$, Exp. Math. **10** (2001), no. 2, 191–196.

[Dokchitser] T. Dokchitser program available at http://maths.dur.ac.uk/~dma0td/computel/

[Duquesne 2001] S. Duquesne, *Integral points on elliptic curves defined by simplest cubic fields*, Exp. Math. **10** (2001), no. 1, 91–102.

[Gross and Zagier 1986] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84**, (1986), 225–320.

[Shanks 1974] D. Shanks, *The simplest cubic fields*, Math. Comp. **28** (1974), 1137–1152.

[Siksek 1995] S. Siksek, *Infinite descent on elliptic curves*, Rocky Mountain Journal of Math. **25** (1995), no. 4, 1501–1538.

[Stein and Watkins 2002] W. Stein and M. Watkins, *A database of elliptic curves – first report*, ANTS-V, LNCS **2369**, Springer-Verlag, 267–275.

[Taylor and Wiles 1995] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2)**141** (1995), no. 3, 553–572.

[Washington 1987] L. C. Washington, *Class numbers of the simplest cubic fields*, Math. Comp. **48:177** (1987), 371–384.

[Watkins] M. Watkins, *Rank distribution of cubic twists*, preprint, available at www.math.psu.edu/watkins/zk.dvi

[Wiles 1995] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no.3, 443–551.

[Zagier and Kramarz 1987] D. Zagier and G. Kramarz, *Numerical investigations related to the L–series of certain elliptic curves*, Journal of the Indian Math. Soc.**52** (1987), 51–69.

Christophe Delaunay, École Polytechnique Fédérale de Lausanne, Faculté des sciences de Base, CSAG, 1015 Lausanne, Switzerland.
e-mail : `christophe.delaunay@epfl.ch`

Sylvain Duquesne, Département des Sciences Mathématiques, Université Montpellier II - Case Courrier 051, Place Eugène Bataillon, 34095 Montpellier cedex 5, France.
e-mail : `duquesne@math.univ-montp2.fr`

Classification of genus 2 curves over $\mathbb{F}_{2^n}$ and optimization of their arithmetic

Bertrand Byramjee[1] and Sylvain Duquesne[2]

[1] Oberthur Card Systems,
25, rue Auguste Blanche, 92800 Puteaux, France,
b.byramjee@oberthurcs.com
[2] Université de Montpellier II, Laboratoire I3M, UMR CNRS 5149
CC 051, place Eugene Bataillon, 34095 Montpellier Cedex 5, France,
duquesne@math.univ-montp2.fr

Abstract

To obtain efficient cryptosystems based on hyperelliptic curves, we studied genus 2 isomorphism classes of hyperelliptic curves in characteristic 2. We found general and optimal form for these curves, just as the short Weierstrass form for elliptic curves. We studied the security and the arithmetic on their jacobian. We also rewrote and optimized the formulas of Lange in characteristic 2, and we introduced a new system of coordinate. Therefore, we deduced the best form of hyperelliptic curves of genus 2 in characteristic 2 to use in cryptography.

Key words. hyperelliptic curve cryptography, genus 2, characteristic 2, explicit formulas, security, isomorphism classes, standardization of curves.

1 Introduction

There is no sub-exponential time algorithm to solve the discrete problem based on abelian generic group. Elliptic curves provide the simplest example with no better algorithm than for generic group. In 1985, Elliptic curves cryptosystems were introduced independently by Miller [13] and Koblitz [6]. In 1989, Koblitz [7] suggested using the jacobian of hyperelliptic curves as a source of finite abelian groups. The main advantage is to use smaller ground field for the same level of security. For example, a hyperelliptic curve

of genus 2 over $\mathbb{F}_{2^{80}}$ can be used in order to have the same level of security as an elliptic curve defined over $\mathbb{F}_{2^{160}}$.

This paper deals with hyperelliptic curves of genus 2 in characteristic 2. It is organized as follows. In section 2, we recall the basic notions of hyperelliptic curves. We refer the reader to [8] for further details and in section 3 we proceed as in [2] and [16] to classify hyperelliptic curves. In the case of elliptic curves ($g = 1$), one can prove that every non supersingular curve can be transformed into a curve of the type:

$$y^2 + xy = x^3 + a_2x^2 + a_6.$$

At this point, there is no analogous in higher genus. Such a representation is very important to define a standard for hyperelliptic curves. Some work has already been done in this field, at least in genus 2 in [2]. Nevertheless we can improve it. We suggest two types of curves suitable for cryptography which are general and optimal in a sense that we will precise later.

In section 4, we analyze the security of the different classes of curves defined in the previous section. In section 5, we rewrite and optimize characteristic 2 formulas of Lange, but we count multiplications of all the coefficients. Moreover we suggest a new system of coordinates which allows faster scalar multiplications on jacobians. All these formulas are given in appendix. Thanks to the results of the last two sections, we suggest a form for equations for hyperelliptic curves of genus 2 in characteristic 2 for future standards in cryptography.

2 Background on Hyperelliptic curves

Let $\overline{\mathbb{F}}_{2^n}$ be an algebraic closure of the field $\mathbb{F}_{2^n}$. A hyperelliptic curve C of genus $g \geq 1$ on $\mathbb{F}_{2^n}$ is given by the general equation :

$$C : y^2 + h(x)y = f(x) \tag{G}$$

where $h \in \mathbb{F}_{2^n}[X]$, is a polynomial of degree at most g, $f \in \mathbb{F}_{2^n}[X]$ is a monic polynomial of degree $2g + 1$ and there is no singular points $(x, y) \in \overline{\mathbb{F}}_{2^n} \times \overline{\mathbb{F}}_{2^n}$. These are the solutions satisfying simultaneously equation (G) and the partial derivative equations $h(x) = 0$ and $h'(x)y + f'(x) = 0$.

Now, we concentrate in the genus 2 case. Let us define some objects on these curves.

A divisor D is a formal sum of points on the hyperelliptic curve C. The

jacobian J is the group of degree 0 divisors modulo principal divisors. In practice, we use the Mumford representation : each divisor is represented by a pair of polynomials $[u, v]$ such that u is a monic polynomial of degree 2, $\deg v < \deg u$ and $u | f - hv - v^2$ (these types of divisors are called reduced).

Cantor described a general algorithm (working in every genera) to add divisors on J, see [1] for more definitions on hyperelliptic curves and details on this algorithm. Nevertheless, his algorithm is too slow, mainly because using gcd algorithms, and uses up too much memory for restricted environments like smart cards.

To improve it in the genus 2 case, Lange following Harley [5], suggests several explicit formulas in affine, projective and weighted projective, in [9], [10] & [11]. Nevertheless she doesn't count multiplications by the coefficients of h, as with the Koblitz curves. Therefore her formulas are not general. That's why we suggest here to rewrite her formulas in the general case and in the different types we define in section 2. In so doing, we optimize these formulas. The best optimizations we obtained, are in the doubling case which is the most important in scalar multiplication.

3 Classification of genus 2 hyperelliptic curves over $\mathbb{F}_{2^n}$

For the genus 2 case, we use the following equation

$$y^2 + (h_2x^2 + h_1x + h_0)y = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0.$$

We divide the hyperelliptic curves into three types depending on the leading coefficient of h, following the notation of [2]:

- type I: $h_2 \neq 0$.
- type II: $h_2 = 0$, $h_1 \neq 0$.
- type III: $h_2 = h_1 = 0$, $h_0 \neq 0$.

Moreover, Choie and Yun prove in [2] that type I has asymptotically between $2q^3$ and $4q^3$ isomorphism classes ($q = 2^n$), type II about $2q^2$ and type III between $2q$ and $32q$. Nevertheless, from these 3 types, only 2 are interesting for a cryptosystem based on the Discrete Logarithm problem, as Galbraith proves in [4] the following result.

Proposition 1. *A characteristic 2 hyperelliptic curve is of type III if and only if it is supersingular.*

Let us first give results concerning the resolution of some simple equation in $\mathbb{F}_{2^n}$.

Proposition 2. *Let $a, b \in \mathbb{F}_{2^n}$,*

1. *The equation $x^{2^k} = b$ has always a solution in $\mathbb{F}_{2^n}$ for $k \geq 1$.*
2. *The equation $x^3 = b$ has always a solution in $\mathbb{F}_{2^n}$ if n is odd.*
3. *For $a \neq 0$, $x^2 + ax + b = 0$ has a solution in $\mathbb{F}_{2^n}$ iff $Tr(a^{-2}b) = 0$.*
4. *If $Tr(a^{-2}b) = 1$, the equation $x^2 + ax + b = ta^2$ has a solution in $\mathbb{F}_{2^n}$ where t is an element of trace 1.*

Remark:

- Here the Trace function is defined by $\mathrm{Tr}(x) = \sum_{i=0}^{n-1} x^{2^i}$.
- In 4, if n is odd, t can be chosen equal to 1 and if n is even, t is a power of π in polynomial basis representation (i.e. $\mathbb{F}_{2^n} \simeq \mathbb{F}_2[\pi]$). In all cases, multiplication by t is free.

Sketch of the proof:

1. $x^2 = b$ has always the solution $x = b^{2^{n-1}}$. This proves the first point.
2. $x^3 = b$ has a solution in $\mathbb{F}_{2^n}$ iff $b^{\frac{2^n-1}{d}} = 1$ where $d = gcd(2^n - 1, 3)$. If n is odd, $d = 1$ so $x^3 = b$ has a solution.
3. This is an application of the additive form of Hilbert's "Satz 90".
4. Please note that $\mathrm{Tr}(a^{-2}(b + ta^2)) = 0$. $\square$

We will now write equation for type I and type II in a minimal form, in the sense that if the coefficients of the equation describe the base field, the expected number of curves is obtained (say $2q^3$ for type I and $2q^2$ for type II). In the following, t denotes an element of trace 1 ($t = 1$ if n is odd) as explained in the previous proposition and ε an element of $\mathbb{F}_2$.

Theorem 1. *A characteristic 2 hyperelliptic curve of type I can always be transformed into one of the following equations:*

$$\begin{aligned} \textit{type Ia} &: \quad y^2 + (x^2 + h_1 x + t h_1^2)y = x^5 + t\varepsilon x^4 + f_1 x + f_0, \\ \textit{type Ib} &: \quad y^2 + x(x + h_1)y = x^5 + t\varepsilon x^4 + f_1 x + f_0. \end{aligned}$$

Remark:

- It is possible to define only one type, but we chose to separate the case where the polynomial h is irreducible (type Ia) and the case where it can be factorized (type Ib) because they are mathematically different. For example, the order of the jacobian of a type Ia curve will always be divisible by two, (since there exists a divisor of order 2) whereas it is divisible by 4 (since there exists two divisors of order 2) in type Ib case.
  This kind of observation is of course very important in cryptography and must be taken into account if one wants to construct good curves for future standards.

- In both cases, we obtain in this way at most $2q^3$ isomorphism classes of curves of type I, which was the expected number as proved in [2].

Sketch of the proof: specializing Lockhart's formula (see [12] for details),

$$\begin{cases} x = & h_2^2 x + \lambda \\ y = & h_2^5 y + h_2^4 \alpha x^2 + h_2^2 \beta x + \gamma \end{cases}$$

with

- λ a root of $h_2 X^2 + h_1 X + h_0$, if $\mathrm{Tr}(h_0 h_2 h_1^{-2}) = 0$ and we obtain a curve of type Ib.
- λ a root of $h_2 X^2 + h_1 X + h_0 + t h_1^2 h_2^{-1}$, if $\mathrm{Tr}(h_0 h_2 h_1^{-2}) = 1$ and we obtain a curve of type Ia.
- α a root of $X^2 + h_2 X + f_4 + \lambda + \varepsilon t h_2^2$ with $\varepsilon = \mathrm{Tr}((f_4 + \lambda) h_2^2)$.
- $\beta = (f_3 + h_1 \alpha) h_2^{-1}$.
- $\gamma = (\beta^2 + h_1 \beta + \alpha(h_2 \lambda^2 + h_1 \lambda + h_0) + f_3 \lambda + f_2) h_2^{-1}$. $\square$

Theorem 2. *If n is odd, a hyperelliptic curve of type II defined over $\mathbb{F}_{2^n}$ can be transformed into the following equation :*

$$y^2 + xy = x^5 + f_3 x^3 + \varepsilon x^2 + f_0.$$

Sketch of the proof: with Lockhart's formula:

$$\begin{cases} x = & \mu^2 x + \lambda \\ y = & \mu^5 y + \mu^4 \alpha x^2 + \mu^2 \beta x + \gamma \end{cases}$$

with

- μ such as $\mu^3 = h_1$,
- $\lambda = h_0 h_1^{-1}$,
- $\alpha = \sqrt{\lambda + f_4}$,
- β is a root of $X^2 + h_1 X + f_2 + \varepsilon h_1^2$ with $\varepsilon = \mathrm{Tr}(f_2 h_1^{-2})$,
- $\gamma = \left((h_0 + h_1\lambda)\beta + \lambda^2 f_3 + \lambda^4 + f_1\right) h_1^{-1}$. $\square$

Theorem 2'. *If n is even, a hyperelliptic curve of type II defined over $\mathbb{F}_{2^n}$ can be transformed into the following equation :*

$$y^2 + h_1 xy = x^5 + \varepsilon' x^3 + t\varepsilon h_1^2 x^2 + f_0.$$

Remark:

- To prove theorem 2', one just have to choose μ so that $\mu^4 = f_3 + h_1\alpha$.
- In theorem 2, we could have erased f_3 instead of h_0, choosing λ before α and so would have had the following form:

  $$y^2 + (x + h_0)y = x^5 + \varepsilon x^2 + f_0.$$

  This form can be useful if someone wants to implement a general form of a hyperelliptic curve as there is no f_3 term in type I or type II. Nevertheless we didn't choose this form as we lose performance by keeping h_0 in the explicit formulas.
- To avoid the Weil-descent attack, n must be chosen prime, which means that only the theorem 2 is of interest for cryptographic purposes.
- If n is odd (resp. even), we obtain in this way at the most $2q^2$ (resp. $4q^2$) isomorphism classes of curves of type II, which was the expected number as proved in [2].

If one wants to use pairings, we provide the following result for the last type of hyperelliptic curves.

Theorem 3. *A characteristic 2 hyperelliptic curve of type III can be transformed into the following equation :*

$$y^2 + y = x^5 + f_3 x^3 + f_1 x + t\varepsilon.$$

Sketch of the proof: with Lockhart's formula:

$$\begin{cases} x = & \mu^2 x \\ y = & \mu^5 y + \mu^4 \alpha x^2 + \mu^2 \beta x + \gamma \end{cases}$$

with

- μ such as $\mu^5 = h_0$,
- $\alpha = \sqrt{f_4}$,
- $\beta = \sqrt{f_2 + f_4}$,
- γ is a root of $X^2 + h_0 X + f_0 + \varepsilon h_0^2$ with $\varepsilon = \mathrm{Tr}(f_0 h_0^{-2})$. $\square$

Remark:
This is not the optimal form as there are between $2q$ and $32q$ curves of type III. Nevertheless, we believe that the correct choice is to take $f_1 = 0$, but we can't prove it in a general way.

4 Analysis of the security of different types of curves

In the previous section, we have classified the curves of genus 2 define over $\mathbb{F}_{2^n}$. In order to use these curves in cryptography, it is very interesting to check the security of each type of curve and to compare them. For example, in proposition 1, we have already seen that all curves of type III are supersingular, which means that they are weak for cryptographic use.

To compare the behavior of different curves, we computed the cardinality of at least 10 000 curves of each type and each value of ε. We use the implementation of Kedlaya's algorithm to compute the cardinality of the jacobian of a curve of genus 2 [15]. We thank F. Vercauteren for allowing us to use his implementation and for answering kindly all our questions.

We have chosen $\mathbb{F}_{2^{89}}$ as ground field so that all the curves are resistant to Weil descent attacks, see Rück in [14] for details.

We call *good curves* those suitable for cryptography, i.e. where there is a divisor of prime order greater than 2^{160} and *nice curves* those with minimal cofactor. In characteristic 2, as in the case of elliptic curves, the cardinality cannot be prime, but we want the cofactor to be minimal (we denote it by f). For example a nice curve with cofactor 2 means that the cardinality of the jacobian is two times a prime.

For each type of curve, we computed the rate of good curves and the rate of nice curves. Moreover, proposition 1 states that curves of type III are the only supersingular curves. However, this didn't prove that curves of type I or II are resistant to Frey-Rück attack [3] (using transfer via the Tate-Lichtenbaum pairing) but it seems to be true in practice. In fact all the curves we tested are resistant.

	good curves	nice curves	minimal f	curves tested
Type Ia, $\varepsilon = 0$	10.4 %	0.56 %	2	10 000
$\varepsilon = 1$	10 %	0.53 %	2	11 446
Type Ib, $\varepsilon = 0$	8.9 %	0.33 %	4	10 000
$\varepsilon = 1$	9.6 %	0.6 %	4	11 445
Type II, $\varepsilon = 0$	9.6 %	0.6 %	4	20 917
$\varepsilon = 1$	10.9 %	1.23 %	2	16 724

We note with these computations, that there are some differences between different types of curves. We already stated that the order of the jacobian is always divisible by 2 for type Ia and by 4 for type Ib, therefore one could hope to find more good curves of type Ia than Ib. This is in fact the case. We can conclude that if one wants to use curves of type I, it is better to choose type Ia because there are more good curves and moreover the minimal cofactor is 2 instead of 4. Nevertheless, we will see in the next section that formulas for doubling and adding in the jacobian are slightly faster in the case of type Ib.

Concerning curves of type II, even if it was not obvious at first sight, we have the following properties on the cardinality of the jacobian:

Proposition 3. *Let C be a type II hyperelliptic curve of genus 2 defined over $\mathbb{F}_{2^n}$ by the equation*

$$y^2 + xy = x^5 + f_3x^3 + \varepsilon x^2 + f_0$$

The minimal cofactor is 4 if $\varepsilon = 0$ and 2 if $\varepsilon = 1$.

Sketch of the proof:
The divisor $\left(0, \sqrt{f_0}\right) + \infty$ is the only one divisor of order 2 and it exists a divisor D such that $2D = \left(0, \sqrt{f_0}\right) + \infty$ (i.e. a divisor of order 4) if and only if $\varepsilon = 0$. This proves that the cardinality of the jacobian is congruent to zero modulo 4 if $\varepsilon = 0$ and to 2 if $\varepsilon = 1$. $\square$

In this last case, we find many of both good curves and nice curves. From these results, it appears that, among hyperelliptic curves of genus 2 in

characteristic 2, the curves of type II with $\varepsilon = 1$ are the best from a security point of view.

5 Application to jacobian scalar multiplication

We use this classification of hyperelliptic curve of genus 2, to rewrite and even optimize formulas of Lange for mixed addition and doubling on their jacobian. Lange uses three types of coordinates, affine [9], projective [10] and weighted projective [11]. In these papers Lange chose the coefficients of h in $\mathbb{F}_2$. In the last sections, we proved that we can't always assume that. That is why contrary to Lange we count multiplications by h_0 and h_1.

These formulas can be found in the appendix for curves of type II which is the most efficient. In fact the mixed addition formulas are just those of Lange rewritten in characteristic 2. We did not rewrite formulas for classical addition as they are also the same as Lange one's. Nevertheless, for doubling, our formulas are slightly different and optimized for each type of curve. Formulas for general cases and curves of type I can be found on the web page of the author.

Besides, we also introduced a new system of coordinates called *Modified Projective Coordinates*. Based on Projective representation, we add two coordinates Z_0, Z_1. So the septuple $[U_1, U_0, V_1, V_0, Z_0, Z_1, Z]$ stand for $[x^2 + U_1/Z + U_0/Z, x^2 + V_1/Z + V_0/Z]$ and $Z_0 = h_0 Z$, $Z_1 = h_1 Z$. The formulas for addition are the same as for projective one's but we gain some multiplications in doubling. The complexities we obtained are listed in the following table.

	General case	**type I**		**type II**
Affine				
Addition	25M + I	25M + I		24M + I
Doubling	27M + I	26M + I		18M + I
Projective		(Ia)	(Ib)	
Mixed Addition	45M	45M	44M	42M
Doubling	45M	44M	41M	31M
Modified Projective				
Mixed Addition	45M	45M	44M	42M
Doubling	43M	42M	40M	31M
Weighted Projective				
Mixed Addition	42M	42M	41M	40M
Doubling	46M	45M	42M	27M

We see we gain at least one multiplication in each system of coordinates for doubling, and of course more for each type of curve. The best performance was produced using type II.

We also noticed the weighted projective coordinates are only interesting for additions in the general case and type I. Thus, the use of projective and modified projective coordinates is more interesting if we use scalar multiplication methods such as sliding window (since it uses much more doubling than adding). Nevertheless, weighted projective coordinates are still competitive in type II or if one has to use doubling and adding at each step, for instance to resist against power analysis in restricted environments like smart cards. It can also be used with algorithms like BGMW, where doublings are pre-computed.
For example in type I, what we gain in addition by using weighted projective coordinates instead of modified projective, we lose in doubling.

Besides, one has to keep in mind that weighted projective coordinates uses up more memory, which has to be taken into account by anyone who wants to implement in restricted environments.

6 Conclusion

We studied genus 2 isomorphism classes of curves in characteristic 2. They are classified in three types. Type III curves are supersingular. We focused our effort on type I and type II and found optimal forms for these curves, just as the short Weierstrass form. For these types of curves we studied the security and the arithmetic on their jacobian.

In addition, we rewrote and optimized formulas of Lange in characteristic 2, and we introduced a new system of coordinate.

We noticed that both from the arithmetic and the security point of view, curves of the form

$$y^2 + xy = x^5 + f_3x^3 + x^2 + f_0$$

are the best for cryptographic use.
Hence we recommend this type for future standards.

Appendix: formulas for hyperelliptic curves over $\mathbb{F}_{2^n}$ of type II: $y^2 + xy = x^5 + f_3x^3 + \varepsilon x^2 + f_0$

Affine case

Affine Doubling with type II: $y^2 + xy = x^5 + f_3x^3 + \varepsilon x^2 + f_0$ with $\varepsilon \in \mathbb{F}_2$	
Input	$D = [u_1, u_0, v_1, v_0]$
Output	$2D = [u'_1, u'_0, v'_1, v'_0]$

Step	Operations	Cost
1	resultant r: $r = u_0$	
2	compute almost inverse: $1 = inv_1$, $u_1 = inv_0$	
3	compute k: $k_1 = u_1^2 + f_3$ $k_0 = u_1k_1 + v_1^2 + v_1 + \varepsilon$	2S, 1M
4	compute $s = kinv \bmod u$: Karatsuba is useless now $s_1 = k_0 + u_1k_1$ $s_0 = k_1u_0$ for $s_1 \neq 0$	1M
5	precomputation $t_0 = (u_0s_1)^{-1}$, $t_1 = u_0t_0$, $t_2 = s_1^2t_0$, $t_3 = u_0t_1$, $s_0 = s_0t_1$	1I, 1S, 5M
6	compute l $l_2 = u_1 + s_0$, $l_1 = u_1s_0 + u_0$, $l_0 = u_0s_0$	2M
7	compute u' $u'_0 = s_0^2 + t_3$ $u'_1 = t_3^2$	2S
8	compute v' $t_0 = u'_1(l_2 + u'_1) + u'_0 + l_1$ $v'_1 = t_2t_0 + v_1 + 1$ $t_0 = u'_0(l_2 + u'_1) + l_0$ $v'_0 = t_2t_0 + v_0$	4M
total		1I, 5S, 13M

Projective case

Projective Doubling with type II: $y^2 + xy = x^5 + f_3x^3 + \varepsilon x^2 + f_0$ with $\varepsilon \in \mathbb{F}_2$	
Input	$D = [U_1, U_0, V_1, V_0, Z]$
Output	$2D = [U_1', U_0', V_1', V_0', Z']$

Step	Operations	Cost
1	precomputation and resultant r: $t_0 = Z^2$, $t_1 = U_1^2$ $r = U_0 Z$	2S, 1M
2	compute almost inverse: useless $inv_0 = U_1 Z$, $inv_1 = Z$	
3	compute k: $k_1 = f_3 t_0 + t_1$, $k_0 = U_1 k_1 + Z(\varepsilon t_0 + V_1(Z + V_1))$	4M
4	compute $s = kinv \bmod u$: Karatsuba is useless now $t_2 = k_0 U_1$ $s_1 = k_0 Z$ $s_0 = k_1 r + t_2$ for $s_1 \neq 0$	3M
5	precomputation and compute l $t_0 = t_0 r$, $r = t_0 s_1$, $t_1 = s_1 k_0$, $t_3 = U_0 k_0$ $l_2 = s_1 t_2$, $l_0 = s_0 t_3$, $l_1 = (t_2 + t_3)(s_0 + s_1) + l_2 + l_0$	7M
6	compute U' $U_0' = s_0^2 + r$ $U_1' = t_0^2$	2S
7	precomputation: $l_2 = l_2 + s_0 s_1 + U_1'$, $s_1 = s_1^2$, $t_2 = r t_1$ $t_0 = U_0' l_2 + l_0 s_1$, $t_1 = U_1' l_2 + s_1(U_0' + l_1)$	1S, 6M
8	adjust: $Z' = s_1 r$, $U_1' = U_1' r$, $U_0' = U_0' r$	3M
9	compute V' $V_0' = t_0 + t_2 V_0$ $V_1' = t_1 + t_2 V_1 + Z'$	2M
total		5S, 26M

Modified projective coordinates, are obviously useless in this case.

Weighted projective case

Weighted projective Mixed Addition with type II: $y^2 + xy = x^5 + f_3x^3 + \varepsilon x^2 + f_0$ with $\varepsilon \in \mathbb{F}_2$		
Input	$D_1 = [u_{11}, u_{10}, v_{11}, v_{10}]$, $D_2 = [U_{21}, U_{20}, V_{21}, V_{20}, Z_{20}, Z_{21}, z_{20}, z_{21}, z_{22}, z_{23}]$	
Output	$D_1 + D_2 = [U'_1, U'_0, V'_1, V'_0, Z'_0, Z'_1, z'_0, z'_1, z'_2, z'_3]$	
Step	Operations	Cost
1	precomputation and resultant r: $t_1 = u_{11}z_{20} + U_{21}$, $t_2 = u_{10}z_{20} + U_{20}$, $t_0 = u_{11}t_1 + t_2$ $r = u_{10}t_1^2 + t_2t_0$, $t_3 = rz_{22}$, $Z'_1 = t_3Z_{20}$	1S, 7M
2	compute almost inverse: nothing to do $t_1 = inv_1$, $t_0 = inv_0$	
3	compute almost s: $t_4 = V_{10}z_{23} + V_{20}$, $t_5 = V_{11}z_{23} + V_{21}$, $s_0 = (t_2t_0) + u_{10}(t_3t_1)$ $s_1 = (t_0 + t_1)(t_4 + t_5) + (t_2t_0) + (t_3t_1)(1 + u_{11})$ for $s_1 \neq 0$	7M
4	precomputation: $Z'_0 = s_1Z_{20}$, $t_0 = rs_1$, $t_3 = t_3^2$, $t_4 = s_0Z_{20}$, $s_0 = s_0s_1$, $s_1 = s_1^2$, $z'_0 = {Z'_0}^2$, $z'_1 = {Z'_1}^2$, $z'_2 = Z'_0Z'_1$, $z'_3 = z'_0z'_2$	4S, 6M
5	compute l $l_2 = s_1u_{21}$, $l_0 = s_0u_{20}$, $l_1 = (s_0 + s_1)(u_{21} + u_{20}) + l_0 + l_2$	3M
6	compute U' $t_5 = t_1s_1$ $U'_0 = t_4^2 + u_{11}t_5 + s_1t_2 + z'_2 + t_1t_3$ $U'_1 = t_5 + z'_1$	1S, 3M
7	compute V' $t_1 = l_2 + Z'_0t_4 + U'_1$, $t_2 = t_1U'_0$, $t_3 = t_1U'_1$ $V'_1 = t_3 + z'_0(l_1 + t_0V_{21} + U'_0 + z'_2)$ $V'_0 = t_2 + z'_0(l_1 + t_0V_{20})$	8M
total		6S, 34M

Weighted projective Doubling with type II: $y^2 + xy = x^5 + f_3x^3 + \varepsilon x^2 + f_0$ with $\varepsilon \in \mathbb{F}_2$	
Input	$D = [U_1, U_0, V_1, V_0, Z_0, Z_1, z_0, z_1, z_2, z_3]$
Output	$2D = [U'_1, U'_0, V'_1, V'_0, Z'_0, Z'_1, z'_0, z'_1, z'_2, z'_3]$

Step	Operations	Cost
1	<u>resultant r</u>: $r = z_0U_0$, $t_0 = rz_2$, $Z'_1 = t_0z_2$	3M
2	<u>compute almost inverse</u>: useless $z_0 = inv_1$, $z_0U_1 = inv_0$	
3	<u>compute k</u>: $t_0 = (\sqrt{f_3}z_0 + U_1)^2$ with precomputation of $\sqrt{f_3}$ $k_1 = t_0z_1$ $k_0 = U_1k_1 + V_1(V_1 + z_3) + \varepsilon z_3^2$	2S, 4M
4	<u>compute $s = kinv \bmod u$</u>: Karatsuba is useless now $s_1 = k_0$ $s_0 = s_1U_1 + k_1r$ for $s_1 \neq 0$	2M
5	<u>precomputation</u> $Z'_0 = s_1$, $t_0 = t_1Z'_0$, $r = s_0^2$, $s_0 = s_0Z'_0$ $z'_0 = {Z'_0}^2$, $z'_1 = {Z'_1}^2$, $z'_2 = Z'_0Z'_1$, $z'_3 = z'_0z'_2$	3S, 4M
6	<u>compute l</u> $l_2 = U_1z'_0$, $l_0 = U_0s_0$, $l_1 = (s_0 + z'_0)(U_1 + U_0) + l_0 + l_2$ $l_2 = l_2 + s_0$	3M
7	<u>compute U'</u> $U'_0 = r + z'_2$ $U'_1 = z'_1$	
8	<u>compute V'</u> $t_1 = (l_2 + U'_1)U'_0$ $V'_0 = t_1 + z'_0(l_0 + t_0V_0)$ $t_1 = (l_2 + U'_1)U'_1$ $V'_1 = t_1 + z'_0(l_1 + t_0V_1 + U'_0) + z'_3$	6M
total		5S, 22M

Remark: for the general case we choose the following form:

$$y^2 + (h_2x^2 + h_1x + h_0)y = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0 \text{ with } h_2, f_4, f_3, f_2 \in \mathbb{F}_2$$

as for type I, there is no f_2 or f_3 and $f_4 \in \mathbb{F}_2$, and for type II $f_2 \in \mathbb{F}_2$, there is no f_4 and following the remark of theorem 2 we can also erase f_3.
The formulas are mostly the same of T. Lange [9], [10], [11], but can be found in the web page of the author.

References

[1] D.G. Cantor. *Computing on the Jacobian of a hyperelliptic curve* Math. Comp., vol. 48, pp. 95-101, 1987.

[2] Y. Choie and D. Yun. *Isomorphism classes of hyperelliptic curves of genus 2 over* $\mathbb{F}_{11}$, in ACISP 2002. LNCS, vol. 2384, pp. 190-202, 2002.

[3] G. Frey and H. Rück. *A remark concerning m-divisibility and the dicrete logarithm in the divisor class group of curves,* Math. Comp., vol. 62, pp. 865-874, 1994.

[4] S. Galbraith. *Supersingular curves in cryptography,* in Advances in Cryptology Asiacrypt 2001, LNCS, vol. 2248, pp. 495-513, 2001.

[5] R. Harley. *Fast arithmetic on genus 2 curves.* available at `http://cristal.inria.fr/ harley/hyper`, 2000.

[6] N. Koblitz. *Elliptic Curves cryptosystem* Math. Comp., vol. 48, pp. 203-209, 1987.

[7] N. Koblitz. *Hyperelliptic cryptosystem* J. Crypto, vol. 1, pp. 139-150, 1989.

[8] N. Koblitz. *Algebraic aspects of cryptosystem* Springer, 1998.

[9] T. Lange. *Efficient Arithmetic on Genus 2 Hyperelliptic Curves over Finite Fields via Explicit Formulae.* Cryptology ePrint Archive, Report 2002/121, 2002. `http://eprint.iacr.org/`

[10] T. Lange. *Inversion-Free Arithmetic on Genus 2 Hyperelliptic Curves.* Cryptology ePrint Archive, Report 2002/147, 2002.

[11] T. Lange. *Weighted Coordinates on Genus 2 Hyperelliptic Curves.* Cryptology ePrint Archive, Report 2002/153, 2002.

[12] P. Lockhart. *On the discriminant of a hyperelliptic curve,* Trans. Ame. Math. Soc. 342, pp. 729-752, 1994.

[13] V. Miller. *Uses of Elliptic Curves in cryptography,* in Advances in Cryptology CRYPTO'85, LNCS, vol. 218, pp. 417-426, 1986.

[14] H.G. Rück. *On the discrete logarithms in the divisor of class group of curves,* Math. Comp., vol. 68, pp. 805-806, 1999.

[15] F. Vercauteren. *Computing Zeta Functions of Hyperelliptic Curves over Finite Fields of Characteristic 2,* in Advances in Cryptology CRYPTO'02, LNCS, vol. 2248, pp. 369-384, 2002.

[16] F. Zhang, S. Liu and K. Kim. *Compact representation of domain parameters of hyperelliptic curve cryptosystems,* in ACISP 2002. LNCS, vol. 2384, pp. 203-213, 2002.

Montgomery Scalar Multiplication for Genus 2 Curves

Sylvain Duquesne

Université Montpellier II, Laboratoire I3S, UMR CNRS 5149
Place Eugène Bataillon CC 051, 34005 Montpellier Cedex, France
duquesne@math.univ-montp2.fr

Abstract. Using powerful tools on genus 2 curves like the Kummer variety, we generalize the Montgomery method for scalar multiplication to the jacobian of these curves. Previously this method was only known for elliptic curves. We obtain an algorithm that is competitive compared to the usual methods of scalar multiplication and that has additional properties such as resistance to timings attacks. This algorithm has very important applications in cryptography using hyperelliptic curves and more particularly for people interested in cryptography on smart cards.

1 Introduction

In this paper we are dealing with the scalar multiplication on the jacobian of curves defined over a field of large characteristic. One of the motivations is that this operation is the main part in cryptography based on the jacobian of curves which is becoming more and more popular. For elliptic curves, Montgomery [24] developed a method for certain curves (which are said to be in the Montgomery form) which allows faster scalar multiplication than the usual methods of exponentiation for groups. This method has the extra advantage that it is resistant to side-channel attacks which is very interesting for people who want to use elliptic curves in cryptography on smart cards. The aim of this paper is the generalization of this method to genus 2 curves. In the following, $\mathbf{K}$ will denote a field of characteristic $k \geq 7$. For cryptographic application, the base field we have in mind is $\mathbb{F}_p$ where p is prime.

2 The Montgomery Method for Scalar Multiplication on Elliptic Curves

Let E be an elliptic curve defined over $\mathbf{K}$ by the equation

$$y^2 = x^3 + a_4 x + a_6 \ .$$

Every elliptic curve defined over $\mathbf{K}$ is isomorphic to a curve given by such an equation which is called the short Weierstrass form. The set $E(\mathbf{K})$ of the points $P = (x, y)$ verifying this equation with x and y in $\mathbf{K}$, forms (together with the point at infinity) a group which will be denoted additively. The problem we are interested in is the following :

Scalar multiplication

Given a point $P \in E(\mathbf{K})$ and an integer n, compute nP as fast as possible.

Of course there are a lot of very old methods to do this, such as the classical double and add algorithm and its variants (like the sliding window method). To improve these algorithms one can choose other systems of coordinates (i.e. other means to represent points on the curve) [4]. For example, the best-known coordinates are projective ones. They are obtained by introducing a new coordinate, usually called Z, which is the lcm of the denominators of x and y. Of course, x and y are replaced by X and Y such that $x = X/Z$ and $y = Y/Z$. This choice of coordinates allows to avoid inversions, which are very costly operations. In the following, we will work with projective coordinates for reasons of efficiency. Nevertheless, the same work can be done with other systems of coordinates. The algorithm we will present here is slightly different from the usual exponentiation algorithms in the sense that the purpose is not to minimize the number of operations but rather the cost of each operation.

2.1 The Algorithm

The original idea of Montgomery [24] was to avoid the computation of the y-coordinate, so that one can hope that basic operations (doubling and adding) are easier to compute. Since for any x-coordinate, there are two corresponding points on the curve (x, y) and $(x, -y)$, this restriction is equivalent to identifying a point on the curve and its opposite. When trying to add two points $\pm P$ and $\pm Q$, one cannot decide if the result obtained is $\pm(P + Q)$ as required or $\pm(P - Q)$. Nevertheless, some operations remain possible like doubling since it is not difficult to decide if the result is $\pm 2P$ or the point at infinity. Unfortunately, doubling is not sufficient for a complete scalar multiplication: one really needs to perform some additions. In fact additions are possible if the difference $P - Q$ is known. The principle of the computation of nP is to use pairs of consecutive powers of P, so that the difference between the two components of the pair is always known and equals to P. The algorithm for scalar multiplication is as follows:

Algorithm 1. *Montgomery scalar multiplication algorithm on elliptic curves*
Input : $P \in E(\mathbf{K})$ *and* $n \in \mathbb{Z}$.
Output : x *and* z*-coordinate of* nP.

Step 1. Initialize $Q = (Q_1, Q_2) = (\mathcal{O}, P)$ *where* $\mathcal{O}$ *is the point at infinity.*

Step 2. If the bit of n *is 0,* $Q = (2Q_1, Q_1 + Q_2)$.

Step 3. If the bit of n *is 1,* $Q = (Q_1 + Q_2, 2Q_2)$.

Step 4. After doing that for each bit of n*, return* Q_1.

In fact, at each step, $Q = (kP, (k + 1)P)$ for some k and we compute either $(2kP, (2k + 1)P)$ or $((2k + 1)P, (2k + 2)P)$ in the following step, so that we always have $Q_2 - Q_1 = P$.
Let us note that contrary to double and add or sliding window methods, both

an addition and a doubling are done for each bit of the exponent. It is the price to be paid to avoid the computation of the y-coordinate but we hope that the gain obtained thanks to this restriction will be sufficient to compensate for the large number of operations. That is the reason why the Montgomery form for elliptic curves has been introduced. The interested reader will find more details for this section in [24] or [26].

2.2 The Montgomery Form

An elliptic curve E is transformable into the Montgomery form if it is isomorphic to a curve given by an equation of the type

$$E_m : By^2 = x^3 + Ax^2 + x \ .$$

It is easy to prove ([26]) that E is transformable in the Montgomery form if and only if

- the polynomial $x^3 + a_4x + a_6$ has at least one root α in $\mathbf{K}$,
- the number $3\alpha^2 + a_4$ is a square in $\mathbf{K}$.

Thus all elliptic curves are not transformable into the Montgomery form. Nevertheless, since the two coefficients can be chosen arbitrarily in $\mathbf{K}$, the number of curves in such a form is of the same order as for general elliptic curves (for example $O(p^2)$ if $\mathbf{K} = \mathbb{F}_p$).
Please note that the first condition means that there is at least one 2-torsion point on the curve E, so that the cardinality of the curve is even.

2.3 Formulas for Doubling and Adding

Let us now describe the arithmetic of curves in the Montgomery form.

Proposition 1. *Let $\mathbf{K}$ be a field of characteristic $k \neq 2, 3$ and let E_m be an elliptic curve defined over $\mathbf{K}$ in the Montgomery form. Let $P = (X_p, Y_p, Z_p)$ and $Q = (X_q, Y_q, Z_q) \in E_m(\mathbf{K})$ be given in projective coordinates. Assume that the difference $P - Q = (x, y)$ is known in affine coordinates. Then we obtain the X and Z-coordinates for $P + Q$ and $2P$ by the following formulas :*

$$\begin{aligned} X_{p+q} &= ((X_p - Z_p)(X_q + Z_q) + (X_p + Z_p)(X_q - Z_q))^2 \ , \\ Z_{p+q} &= x\,((X_p - Z_p)(X_q + Z_q) - (X_p + Z_p)(X_q - Z_q))^2 \ , \end{aligned}$$

$$\begin{aligned} 4X_pZ_p &= (X_p + Z_p)^2 - (X_p - Z_p)^2 \ , \\ X_{2p} &= (X_p + Z_p)^2(X_p - Z_p)^2 \ , \\ Z_{2p} &= 4X_pZ_p\left((X_p - Z_p)^2 + \frac{A+2}{4}4X_pZ_p\right) \ . \end{aligned}$$

In this way, both an addition and a doubling take 3 multiplications and 2 squares each so that the cost of this algorithm is about $10|n|_2$ multiplications where $|n|_2$ denotes the number of bits of n.
In the best case with usual scalar multiplication, one needs 4 multiplications and 4 squaring just for doubling and more for adding. Thus, for curves in the Montgomery form, this method is interesting. In practice, the gain obtained is about 10 percent (compared in [6] for 192 bits with a sliding window method of size 4 after a Koyama-Tsuruoka recoding [18] and using mixed jacobian modified coordinates [4]).

2.4 General Case

We are now interested in a Montgomery method for scalar multiplication for elliptic curves which cannot be transformed into the Montgomery form. In fact the method for scalar multiplication is the same, we just need to have formulas for doubling and adding. These formulas can be found in [1], [10] or [13]. Let us recall them.

Proposition 2. *Let* $\mathbf{K}$ *be a field of characteristic* $k \neq 2, 3$ *and let* E *be an elliptic curve defined over* $\mathbf{K}$ *as described in Sect. 2. Let* $P = (X_p, Y_p, Z_p)$ *and* $Q = (X_q, Y_q, Z_q) \in E(\mathbf{K})$ *be given in projective coordinates. Assume that the difference* $P - Q = (x, y)$ *is known in affine coordinates. Then we obtain the* X *and* Z*-coordinates for* $P + Q$ *and* $2P$ *by the following formulas :*

$$\begin{aligned} X_{p+q} &= -4a_6 Z_p Z_q (X_p Z_q + X_q Z_p) + (X_p X_q - a_4 Z_p Z_q)^2 \ , \\ Z_{p+q} &= x(X_p Z_q - X_q Z_p) \ , \\ X_{2p} &= \left(X_p^2 - a_4 Z_p^2\right)^2 - 8a_6 X_p Z_p^3 \ , \\ Z_{2p} &= 4Z_p \left(X_p^3 + a_4 X_p Z_p^2 + a_6 Z_p^3\right) \ . \end{aligned}$$

Addition can be evaluated in 10 multiplications and doubling in 9. Thus, in this way, the scalar multiplication can be performed in about $19|n|_2$ multiplications in the base field. This method can even be optimized in most cases to $17|n|_2$ multiplications [7]. Of course, in this case, the algorithm is not interesting any more compared with the usual methods. However, it can be useful in some situations as we will see in the next section.

2.5 Use and Interest in Cryptography

In this section, we are dealing with elliptic curve cryptography. Elliptic curve cryptosystems were simultaneously introduced by Koblitz [14] and Miller [23]. They are becoming more and more popular because the key length can be chosen smaller than with RSA cryptosystems for the same level of security. This small key size is especially attractive for small cryptographic devices like smart cards. In all schemes (such as encryption/decryption or signature generation/verification) the dominant operation is the scalar multiplication of some

point on the elliptic curve. Hence, the efficiency of this scalar multiplication is central in elliptic curve cryptography, and more generally in cryptography based on the discrete logarithm problem. In the case where the curve is in the Montgomery form, we saw in the previous sections that the Montgomery scalar multiplication method allows to compute the multiple of any given point on the curve faster than with the usual scalar multiplication algorithms. Unfortunately, we also saw that some elliptic curves cannot be transformed into the Montgomery form. This is for example the case for most of the standards. The reason is really simple: any curve which can be transformed in the Montgomery form has a 2-torsion point so that its cardinality is divisible by 2 and this is not ideal for cryptographic use since we prefer to use curves with prime order.

In the general case, the Montgomery method can also be applied but is much more time-consuming. Indeed, we need to perform both an addition and a doubling for each bit of the exponent. This is not the case for example in the classical double and add algorithm where we only have to perform an addition every two bits on average (and even fewer with the sliding window method). Nevertheless, this particularity allows to resist to side-channel attacks on smart cards which is not the case with other algorithms.

This kind of attacks uses observations like timings [16], power consumption [17] or electromagnetic radiation [28]. They are based on the fact that addition and doubling are two different operations. In this situation, it is easy to decide, for each bit of the exponent, if the algorithm (double and add for example) is performing either a doubling (if the bit is 0) or a doubling and an addition (if the bit is 1). Hence, it is easy to recover the whole exponent (which was the secret key). Of course, various countermeasures have been proposed to secure the elliptic curve scalar multiplication against side-channel attacks [5]. For example, if one wants to protect a double and add algorithm, one can perform extra, useless, additions when the bit of the exponent is 0. In this way, for each bit of the exponent we perform both an addition and a doubling so that bits of the exponent are indistinguishable, but this is of course time consuming.

With the Montgomery scalar multiplication method, we always have to perform both an addition and a doubling for each bit of the exponent, so that this method is resistant against side-channel attacks. Therefore it is always interesting even with 19 multiplications at each step for general curves.

Of course elliptic curves in the Montgomery form are very attractive for people interested in elliptic curve cryptosystems on smart cards since, on the one hand, the scalar multiplication method is the most efficient one known to date and, on the other hand, it is resistant to side-channel attacks. That is one of the reasons why we want to generalize this method to hyperelliptic curves of genus 2.

Finally, for some cryptosystems, the x-coordinate of nP is sufficient but others, like the elliptic curve signature scheme ECDSA, require the y-coordinates. To recover it, we use the following result from [27] in the case of a curve in the Montgomery form.

Proposition 3. *Suppose that $R = P + Q$ with $P = (x_1, y_1)$, $Q = (x', y')$ and $R = (x^+, y^+)$. Then, if $y_1 \neq 0$, one has*

$$y^+ = \frac{(x'x_1 + 1)(x' + x_1 + 2A) - 2A - (x' - x_1)^2 x^+}{2By_1} \quad .$$

For general curves, it is also possible to recover the y-coordinate ([1]).

In order to generalize this method to genus 2 curves, let us first recall some lowbrow background on these curves.

3 Background on Genus 2 Curves

First, let us note that every genus 2 curve is hyperelliptic, so that, in the following we will not state that the curves we are interested in are hyperelliptic. Moreover, we will concentrate on imaginary hyperelliptic curves. Since the characteristic of the field $\mathbf{K}$ has been chosen different from 2 and 5, the hyperelliptic curves we are interested in are given by an equation of the form

$$\mathcal{C} : y^2 = f(x) = x^5 + f_3x^3 + f_2x^2 + f_1x + f_0 \text{ with } f_0, f_1, f_2, f_3 \in \mathbf{K} \ . \qquad (1)$$

Contrary to elliptic curves, the set of points on genus 2 curves does not form a group. Thus, one can define the jacobian of $\mathcal{C}$, denoted $\mathcal{J}(\mathcal{C})$ which is the quotient of the group of divisors of degree 0 by the principal divisors. In the case of elliptic curves, this jacobian is isomorphic to the curve itself. More details on the definition of the jacobian can be found in [15]. Our purpose in this paper is to give an algorithm for scalar multiplication in this jacobian. There are mainly two means to represent elements in the jacobian. The first one is a consequence of the Riemann-Roch theorem and says that a divisor class can be represented by a couple of points ($P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$) on the curve which are conjugated over some quadratic extension of the base field $\mathbf{K}$. The second one makes explicit the correspondence of ideal classes and divisor classes and was introduced by Mumford [25]:

Theorem 1. *Let the function field be given via the irreducible polynomial $y^2 = f(x)$ where $f \in \mathbf{K}[x]$ and deg(f)=5. Each non trivial ideal class over $\mathbf{K}$ can be represented via a unique ideal generated by $u(x)$ and $y - v(x)$, $u, v \in \mathbf{K}[x]$, where u is monic, deg(v) <deg(u) ≤ 2 and $u|(v^2 - f)$.*

The correspondence between these representations is that $u(x) = (x - x_1)(x - x_2)$ and $v(x_i) = y_i$ with appropriate multiplicities. This Mumford representation was used by Cantor to develop his algorithm to compute the group law on jacobians of curves [2]. Several researchers such as Harley [12], or more recently Lange [19], [20], [21] made explicit the steps of Cantor's Algorithm and list the operations one really needs to perform. They obtained explicit formulas for the group law on the jacobian.

The basic objects are now defined and we can give an analog for genus 2 curves of the Montgomery form for elliptic curves.

4 A Montgomery-like Form for Genus 2 Curves

4.1 Definition

In the following, we will say that a curve $\mathcal{C}$ is transformable into Montgomery-like form if it is isomorphic to a curve given by an equation of the type

$$By^2 = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + x \ . \tag{2}$$

It is easy to prove that a curve $\mathcal{C}$ as defined in Sect. 3 is transformable into Montgomery-like form if and only if

- the polynomial $f(x)$ has at least one root α in $\mathbf{K}$.
- the number $f'(\alpha)$ is a fourth power in $\mathbf{K}$.

Thus, as in the case of elliptic curves, not all the curves are transformable into the Montgomery-like form. Nevertheless, since the four coefficients can be chosen arbitrarily in $\mathbf{K}$, the number of such curves is about the same as for general genus 2 curves ($O(p^4)$ if $\mathbf{K} = \mathbb{F}_p$).
Please note that the first condition means that there is at least one 2-torsion element in the jacobian variety of the curve $\mathcal{C}$, so that the cardinality of the jacobian is even.

4.2 The Kummer Surface

With elliptic curves, the main idea of the Montgomery method was to avoid the computation of the y-coordinate. At first sight an analog for genus 2 curves would be to avoid the computation of the polynomial v in the Mumford representation and keep only u. But this is not satisfying since it has no mathematical sense. In fact, with elliptic curves, working only with the x-coordinate means that we identify a point and its opposite. The analog for genus 2 curves is called the Kummer surface, where a divisor and its opposite are identified. The Kummer surface is a quartic surface in $\mathbb{P}^3$. We give here the definition of the Kummer surface and its properties without demonstrations for curves in Montgomery-like form. They were obtained using the same method as that in the book of Cassels and Flynn on genus 2 curves ([3] or [8]). The Kummer surface is the image of the map

$$\begin{aligned} \kappa : J(\mathbf{K}) &\longrightarrow \mathbb{P}^3(\mathbf{K}) \\ \{(x_1, y_1), (x_2, y_2)\} &\longmapsto \left(1, x_1 + x_2, x_1x_2, \frac{F_0(x_1, x_2) - 2By_1y_2}{(x_1 - x_2)^2}\right) \ , \end{aligned}$$

with

$$F_0(x_1, x_2) = (x_1 + x_2) + 2f_2x_1x_2 + f_3(x_1 + x_2)x_1x_2 + 2f_4x_1^2x_2^2 + (x_1 + x_2)x_1^2x_2^2 \ .$$

In the following, for any divisor $\mathcal{A} \in \mathcal{J}(\mathcal{C}))$, we will denote

$$\kappa(\mathcal{A}) = (k_1(\mathcal{A}), k_2(\mathcal{A}), k_3(\mathcal{A}), k_4(\mathcal{A})) \ .$$

More precisely, the Kummer surface is the projective locus given by an equation K of degree four in the first three variables and of degree two in the last one. The exact equation can be found online [9]. In passing from the jacobian to the Kummer surface, we have lost the group structure (as was already the case with elliptic curves) but traces of it remain. For example, it is possible to double on the Kummer surface.
Nevertheless, for general divisors $\mathcal{A}$ and $\mathcal{B}$, we cannot determine the values of the $k_i(\mathcal{A}+\mathcal{B})$ from the values of the $k_i(\mathcal{A})$ and $k_i(\mathcal{B})$ since the latter do not distinguish between $\pm\mathcal{A}$ and $\pm\mathcal{B}$, and so not between $\mathcal{A}\pm\mathcal{B}$. However the values of the $k_i(\mathcal{A}+\mathcal{B})k_j(\mathcal{A}-\mathcal{B})+k_i(\mathcal{A}-\mathcal{B})k_j(\mathcal{A}+\mathcal{B})$ are well determined. We have

Theorem 2. *There are explicit polynomials φ_{ij} biquadratic in the $k_i(\mathcal{A}), k_i(\mathcal{B})$ such that projectively*

$$k_i(\mathcal{A}+\mathcal{B})k_j(\mathcal{A}-\mathcal{B})+k_i(\mathcal{A}-\mathcal{B})k_j(\mathcal{A}+\mathcal{B})=\varphi_{ij}(\mathcal{A},\mathcal{B}) \ . \tag{3}$$

Using these biquadratic forms, we can easily compute the $k_i(\mathcal{A}+\mathcal{B})$ if the $k_i(\mathcal{A}-\mathcal{B})$ are known. We can also compute the $k_i(2\mathcal{A})$ by puting $\mathcal{A}=\mathcal{B}$.

4.3 Formulas for Adding

Proposition 4. *Let $\mathbf{K}$ be a field of characteristic $k\neq 2,3$ and let $\mathcal{C}$ be a curve of genus 2 defined over $\mathbf{K}$ in the Montgomery form as defined in Sect. 4. Let $\mathcal{K}$ denote the Kummer surface of $\mathcal{C}$. Let $\mathcal{A}$ and $\mathcal{B}$ be two divisors on the jacobian of $\mathcal{C}$, $\kappa(\mathcal{A})=(k_1(\mathcal{A}),k_2(\mathcal{A}),k_3(\mathcal{A}),k_4(\mathcal{A}))$ and $\kappa(\mathcal{B})=(k_1(\mathcal{B}),k_2(\mathcal{B}),k_3(\mathcal{B}),k_4(\mathcal{B}))$ their images in the Kummer surface. Assume that the difference $\mathcal{A}-\mathcal{B}$ is known and that the last coordinate of its image in the Kummer surface is one (remember we are in $\mathbb{P}^3(\mathbf{K})$). Then we obtain the Kummer coordinates for $\mathcal{A}+\mathcal{B}$ by the following formulas :*

$$\begin{aligned}
k_1(\mathcal{A}+\mathcal{B}) &= \varphi_{11}(\mathcal{A},\mathcal{B}) \ ,\\
k_2(\mathcal{A}+\mathcal{B}) &= 2\left(\varphi_{12}(\mathcal{A},\mathcal{B})-k_1(\mathcal{A}+\mathcal{B})k_2(\mathcal{A}-\mathcal{B})\right) \ ,\\
k_3(\mathcal{A}+\mathcal{B}) &= k_1(\mathcal{A}-\mathcal{B})\varphi_{33}(\mathcal{A},\mathcal{B}) \ ,\\
k_4(\mathcal{A}+\mathcal{B}) &= 2(\varphi_{14}(\mathcal{A},\mathcal{B})-k_1(\mathcal{A}+\mathcal{B})k_4(\mathcal{A}-\mathcal{B})) \ ,
\end{aligned}$$

where the φ_{ij} are the biquadratic forms described in Sect. 4.2.

The expressions of the $\varphi_{ij}(\mathcal{A}+\mathcal{B})$ are available by anonymous ftp [9] but require a large number of operations in the base field to be computed. The main difficulty is to find expressions which require the least possible multiplications in $\mathbf{K}$. We now give more precisely these expressions for the φ_{ij} we are interested in. For clarity we will denote $\kappa(\mathcal{A})=(k_1,k_2,k_3,k_4)$ and $\kappa(\mathcal{B})=(l_1,l_2,l_3,l_4)$.

$$\begin{aligned}
\varphi_{11}(\mathcal{A},\mathcal{B}) &= ((k_4l_1-k_1l_4)+(k_2l_3-k_3l_2))^2 \ ,\\
\varphi_{12}(\mathcal{A},\mathcal{B}) &= ((k_2l_3+k_3l_2)+(k_1l_4+k_4l_1))(f_3(k_1l_3+k_3l_1)+(k_2l_4+k_4l_2))+\\
&\quad 2(k_1l_3+k_3l_1)(f_2(k_1l_3+k_3l_1)+(k_1l_2+k_2l_1)-(k_3l_4+k_4l_3))+
\end{aligned}$$

$$
\begin{aligned}
& 2f_4(k_1l_4+k_4l_1)(k_2l_3+k_3l_2) \ , \\
\varphi_{33}(\mathcal{A},\mathcal{B}) &= ((k_3l_4-k_4l_3)+(k_1l_2-k_2l_1))^2 \ , \\
\varphi_{14}(\mathcal{A},\mathcal{B}) &= (k_1l_1-k_3l_3)(f_3((k_1l_4+k_4l_1)-(k_2l_3+k_3l_2))+ \\
& \qquad 2((k_1l_2+k_2l_1)-(k_3l_4+k_4l_3))+ \\
& \qquad f_2(k_4l_4+k_2l_2)+2f_4(k_1l_1-k_3l_3))+ \\
& (k_2l_2-k_4l_4)((k_2l_3+k_3l_2)-(k_1l_4+k_4l_1)-f_2(k_1l_1+k_3l_3)) \ .
\end{aligned}
$$

4.4 Formulas for Doubling

Proposition 5. *Let* $\mathbf{K}$ *be a field of characteristic* $k \neq 2,3$ *and let* $\mathcal{C}$ *be a curve of genus 2 defined over* $\mathbf{K}$ *in the Montgomery form as defined in Sect. 4. Let* $\mathcal{K}$ *denote the Kummer surface of* $\mathcal{C}$*. Let also* $\mathcal{A}$ *be a divisor on the jacobian of* $\mathcal{C}$ *and* $\kappa(\mathcal{A}) = (k_1,k_2,k_3,k_4)$ *its image in the Kummer surface. Then we obtain the Kummer coordinates for* $2\mathcal{A}$ *(*$\kappa(2\mathcal{A}) = \delta_1,\delta_2,\delta_3,\delta_4$*) by the following formulas :*

$$
\begin{aligned}
\delta_1 &= 2\varphi_{14}(\mathcal{A},\mathcal{A}) \ , \\
\delta_2 &= 2\varphi_{24}(\mathcal{A},\mathcal{A}) + 2f_3K(\mathcal{A}) \ , \\
\delta_3 &= 2\varphi_{34}(\mathcal{A},\mathcal{A}) \ , \\
\delta_4 &= \varphi_{44}(\mathcal{A},\mathcal{A}) + 2K(\mathcal{A}) \ ,
\end{aligned}
$$

where the φ_{ij} *are the biquadratic forms described in Sect. 4.2 and* K *is the equation of the Kummer surface also described in Sect. 4.2 and such that* $K(\mathcal{A}) = 0$.

This is just a consequence of Theorem 2. Let us note that in δ_2 and δ_4 we added a multiple of the equation of the Kummer surface in order to simplify the expressions as much as possible. We give now more precisely these expressions for the δ_i.

$$
\begin{aligned}
\delta_1 &= 8(k_1^2-k_3^2)(f_4(k_1^2-k_3^2)+2(k_1k_2-k_3k_4))+ \\
& \quad 8(k_1k_4-k_2k_3)(k_4^2-k_2^2+f_2(k_1k_4-k_2k_3)+f_3(k_1^2-k_3^2)) \ , \\
\delta_2 &= 8(k_1^2+k_3^2-f_3k_1k_3-3k_2k_4)(k_2^2+k_4^2-f_3(k_1^2+k_3^2)+4k_1k_3)+ \\
& \quad 16(k_2k_4+f_3k_1kl_3)(f_4(k_1k_2+k_3k_4)+2(k_2^2+k_4^2)+f_2(k_1k_4+k_2k_3))+ \\
& \quad 32k_1k_3(4k_2k_4+f_2(k_1k_2+k_3k_4)+(f_2^2+f_4^2)k_1k_3+8f_4(k_1k_4+k_2k_3)) \ , \\
\delta_3 &= 8(k_1^2-k_3^2)(f_2(k_1^2-k_3^2)+2(k_1k_4-k_2k_3)+f_3(k_1k_2-k_3k_4))+ \\
& \quad 8(k_3k_4-k_1k_2)(k_4^2-k_2^2+f_4(k_3k_4-k_1k_2)) \ , \\
\delta_4 &= (k_2^2+k_4^2)((k_2^2+k_4^2)-2f_3(k_1^2+k_3^2)-8k_1k_3)+ \\
& \quad (k_1^2+k_3^2)(f_3k_1k_3+f_4(k_1k_4+k_2k_3)+2k_2k_4+f_2(k_1k_2+k_3k_4)+ \\
& \qquad (f_3^2-4f_2f_4)(k_1^2+k_3^2))-8f_2f_4(k_1k_3)^2 \ .
\end{aligned}
$$

5 The Montgomery Scalar Multiplication on Genus 2 Curves in Montgomery-like Form

5.1 Algorithm

We give here an analog for genus 2 curves of the Montgomery method for scalar multiplication on elliptic curves described in Sect. 2.1. In the case of elliptic curves, Montgomery's method [24] avoids the computation of the y-coordinate. We saw that an equivalent method in genus 2 was to work on the Kummer surface. Of course we have the same restriction in the case of genus 2 curves, namely that it is not possible to add two divisors except if their difference is known. If $\mathcal{D}$ is some divisor, recalling that our goal is the computation of $n\mathcal{D}$ for some integer n, the principle is, as it was already the case for elliptic curves, to use pairs of consecutive powers of $\mathcal{D}$, so that the difference between the two components of the pair is always known and equal to $\mathcal{D}$. The algorithm for scalar multiplication is as follows:

Algorithm 2. *Montgomery scalar multiplication algorithm for genus 2 curves*
Input : $\mathcal{D} \in \mathcal{J}(\mathbf{K})$ *and* $n \in \mathbb{Z}$.
Output : $\kappa(n\mathcal{D})$*, the image in the Kummer surface of* $n\mathcal{D}$.

Step 1. Initialize $(\mathcal{A}, \mathcal{B}) = ((0,0,0,1), \kappa(\mathcal{D}))$ *where* $(0,0,0,1)$ *is the image in the Kummer surface of the neutral element on* $\mathcal{J}(\mathcal{C})$.

Step 2. If the bit of n *is 0,* $(\mathcal{A}, \mathcal{B}) = (2\mathcal{A}, \mathcal{A} + \mathcal{B})$.

Step 3. If the bit of n *is 1,* $(\mathcal{A}, \mathcal{B}) = (\mathcal{A} + \mathcal{B}, 2\mathcal{B})$.

Step 4. After doing that for each bit of n*, return* $\mathcal{A}$.

Note that, at each step, we always have $\mathcal{B} - \mathcal{A} = \kappa(\mathcal{D})$ so that the addition of $\mathcal{A}$ and $\mathcal{B}$ is possible.

5.2 Number of Operations

At each step of the algorithm, we perform both an addition and a doubling, hence we just have to count the number of operations required for each of them. In the following, M will denote a multiplication in $\mathbf{K}$ and S a squaring.

Table 1. Addition of $\mathcal{A}$ and $\mathcal{B}$ in $\mathcal{K}(\mathcal{C})$ if $\mathcal{A} - \mathcal{B}$ is known

expressions	operations
precomputations $\{k_i l_j\}_{i,j=1..4}$	$16M$
$\varphi_{11}(\mathcal{A}, \mathcal{B})$	S
$\varphi_{12}(\mathcal{A}, \mathcal{B})$	$6M$
$\varphi_{33}(\mathcal{A}, \mathcal{B})$	S
$\varphi_{14}(\mathcal{A}, \mathcal{B})$	$6M$
$\kappa(\mathcal{A} + \mathcal{B})$	$3M$
total	$31M + 2S$

Remark 1. The 31 multiplications include 7 multiplications by coefficients of the curve.

Table 2. Doubling of $\mathcal{A}$ in $\mathcal{K}(\mathcal{C})$

expressions	operations
precomputations $\{k_i k_j\}_{i,j=1..4}$	$6M + 4S$
$\delta_1(\mathcal{A}, \mathcal{B})$	$5M$
$\delta_2(\mathcal{A}, \mathcal{B})$	$11M$
$\delta_3(\mathcal{A}, \mathcal{B})$	$5M$
$\delta_4(\mathcal{A}, \mathcal{B})$	$5M$
total	$31M + 5S$

Remark 2. The 31 multiplications include 16 multiplications by coefficients of the curve. Moreover the multiplications $f_3 k_1 k_3$, $f_3(k_1^2 + k_3^2)$, $f_4(k_1 k_4 + k_2 k_3)$ and $f_2(k_1 k_2 + k_3 k_4)$ are not counted in δ_4 since they were already computed in δ_2. Finally, we of course assumed that $f_2 f_4$, $f_3^2 - 4 f_2 f_4$ and $f_2^2 + f_4^2$ were precomputed.

Hence, on a curve in the Montgomery form as in (2), the scalar multiplication using the Montgomery method requires $69|n|_2$ base field multiplications (assuming that a squaring is a multiplication), where $|n|_2$ is the number of bits of n.

5.3 Comparison with Usual Algorithms for Scalar Multiplication

To date, the best algorithms for scalar multiplication on genus 2 curves defined over a field of odd characteristic are obtained by using mixed weighted projective coordinates [21]. In this case, Lange needs 41 multiplications both for a mixed addition and for a doubling. Hence our formulas requires fewer base field operations. But, in the Montgomery algorithm, we must perform both an addition and a doubling for each bit of the exponent whereas one can use efficient algorithms (like the sliding window method) with Lange's formulas. Nevertheless, this algorithm is still interesting for many reasons.

- As was the case for elliptic curves and as explained in Sect. 2.5, the Montgomery algorithm is resistant to side-channel attacks, contrary to other algorithms for scalar multiplications. For this reason it will be of interest to people who need to implement hyperelliptic curves protocols on smart cards or systems sensitive to side-channel attacks. For example, if one wants to make safe algorithms using mixed weighted projective coordinates, one needs to perform an extra addition when the bit of the exponent is one. In this case, for each bit of the exponent, 82 base field operations are required and with only 69, our algorithm allows a gain of 16 percent, which is significant.
- This algorithm is very easy to implement, there are no precomputations (as in the sliding window method) and an element on the Kummer surface requires only 4 base field elements whereas weighted projective coordinates require 8 of them so that it is also interesting in terms of memory usage.

This last remark will be an advantage for constrained environments like smart cards.

– It is very dependent of the coefficients of the curve. Indeed there are 23 multiplications by these coefficients but only 2 in Lange's formulas. Hence a good choice of the coefficients of the curve certainly allows better timings. This is the subject of the following section.

5.4 Some Special Cases

In order to decrease the number of base field operations for our algorithm, certain choices of coefficients of the curve are better to use. For example there are 6 multiplications by f_3 in the formulas given in Sects. 4.3 and 4.4 so that, if one chooses $f_3 = 0$ or 1, the total amount of multiplications necessary for each bit of the exponent is 63 instead of 69. In the following table, we summarize the gain obtained in each operation. Let us note that there is no gain for the calculation of φ_{11}, φ_{33} and precomputations.

Table 3. Gain obtained if ...

	$f_2 = 0$	f_2 small	$f_3 = 0$ or small	$f_4 = 0$	f_4 small
φ_{12}	1	1	1	2	1
φ_{14}	2	2	1	1	1
δ_1	1	1	1	1	1
δ_2	2	2	2	2	2
δ_3	1	1	1	1	1
δ_4	2	1	0	2	1
total	9	8	6	9	7

Remark 3. If two of these conditions on the coefficients are satisfied the gain obtained is just the sum of the gains.

Of course this kind of restriction implies that fewer curves are taken into account. For example, if $\mathbf{K} = \mathbb{F}_p$ and $f_3 = 0$, one can only choose three coefficients in $\mathbb{F}_p$ (namely f_2, f_4 and B) so that the number of such curves is $O(p^3)$. Thus we lose in generality. However, in cryptography, one only needs to find a curve such that the order of its jacobian is divisible by a huge prime number. For this, one needs enough choices of curves in order to be able to find a curve with this property and $O(p^3)$ choices are of course widely sufficient.
Let us now examine more precisely a particular case and compare our algorithm to usual ones. Let $\mathcal{C}$ be a genus 2 curve defined over $\mathbf{K}$ by an equation of the form

$$By^2 = x^5 + f_3x^3 + \varepsilon x^2 + x \text{ with } \varepsilon = 0 \text{ or } \pm 1 \text{ and } B \text{ and } f_3 \in \mathbf{K} \ . \quad (4)$$

There are $O(p^2)$ curves in this form (which is sufficient to find one of these with nice properties for use in cryptography). Here, our algorithm of scalar multiplication requires 52 multiplications for each bit of the exponent whereas with mixed weighted projective coordinates,

– a sliding window method with window size equal to 4 requires in average 48 multiplications,
– a classical double and add requires 61 multiplications on average,
– a side-channel attack resistant double and add requires 81 multiplications.

Thus, our algorithm is 15 percent faster than a double and add, not so far from the sliding window method (around 7 percent) and much more efficient if one wants the operation to be resistant to side-channel attacks. Indeed, in this case, we obtain a gain of 36 percent. Of course one can even be faster than the sliding window method by choosing a small coefficient f_3 but the number of such curves becomes small.

Remark 4. Another means to accelerate this algorithm would be to choose f_2, f_3 and f_4 one word long. For example, on a 32 bits processor, if we are working on some finite field of cryptographic size for genus 2 curves, a multiplication of a coefficient of the curve and an element of the base field is about three times faster than the usual multiplication in the base field. Hence, as there are 23 multiplications by coefficients of the curve, our algorithm will require the equivalent of 53 multiplications, which is not so bad.

5.5 Examples

In this section, the base field is the prime field $\mathbb{F}_{2^{80}+13}$ (so that cryptosystems based on genus 2 curves defined over this field have the same security level than those based on elliptic curves defined over some 160 bits prime field). Let $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{C}_3$ be the genus 2 curves respectively defined by the equations

$$\begin{aligned}
442946377804223815965 77\, y^2 &= x^5 + 271937476575616687835 34\, x^4 \\
&\quad + 297559220985752192390 37\, x^3 \\
&\quad + 760478620401411267378 26\, x^2 + x \ , \\
1037793104745672252229 2\, y^2 &= x^5 + 773041988679881578656 77\, x^3 + x^2 + x \ , \\
6941883706844249386422 0\, y^2 &= x^5 + x^3 + x \ .
\end{aligned}$$

We compared our algorithm on these curves with a sliding window of size 4, a classical double and add and a double and always add (used to resist against side-channel attacks). For these three algorithms, we of course always used the weighted projective coordinates as in [21] which are the more efficient ones. In the following table, we provide the timings obtained using GMP 4.1.2 on a Pentium IV 3.06 GHz. We carried out 1000 scalar multiplications in each case with various divisors and 160 bits exponents.

Table 4. Timings

	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_3$
Sliding window	13.4 ms	13.3 ms	12.9 ms
Double and add	16 ms	16 ms	15.5 ms
Double and always add	21.5 ms	21.5 ms	21 ms
Montgomery method	18.3 ms	13.6 ms	11.9 ms

6 Conclusion and Prospects

Thanks to the theory of the Kummer surface of a hyperelliptic curve of genus 2, we have generalized to genus 2 curves the method of Montgomery for scalar multiplication on elliptic curves. As Montgomery does for elliptic curves, we restrict to curves transformable into Montgomery-like form. However, there are no theoretical obstructions to generalize this method to all genus 2 curves. Indeed Propositions 4.3 and 4.4 remain valid but the total amount of multiplications to compute the biquadratic forms is really huge so that this method is not competitive with the classical ones. This is not so surprising since it was already the case for elliptic curves.

In fact, for people interested in cryptography, this restriction is not very important since the number of choices of curves remains largely the same. The only significant restriction is that the order of the jacobian of such curves is even and then cannot be prime. But working with a jacobian whose order is twice a prime is not less efficient than working with a prime order.

For elliptic curves, the standards are not transformable into the Montgomery form because of this restriction and it's really a shame because the Montgomery method for scalar multiplication is the most interesting one (the fastest, easy to implement, resistant to side-channel attacks). Up to now, there are no standards for genus 2 curves. If such standards exist one day, it would be useful to take the method that we developed into account.

Moreover, we have seen that, with some restrictions, we obtain very interesting timings for the scalar multiplication on the jacobian of genus 2 curves. It would be nice to verify (even if there is no reason for this) that these restrictions are not awkward for finding jacobians suitable for cryptography (i.e. with a large prime dividing the order). Unfortunately, algorithms for finding the order of the jacobian over $\mathbb{F}_p$ are still under development ([11], [22]).

Finally, it would be very interesting to study the case of the characteristic 2, since it is in that case that this method is the most efficient for elliptic curves. For this, all the necessary mathematical objects, such as the Kummer surface, remain to be defined.

References

1. Brier, E., Joye, M.: Weierstrass Elliptic Curves and Side-Channel Attacks, Public Key Cryptography, Lecture Notes in Computer Science, **2274** (2002)
2. Cantor, D. G.: Computing on the Jacobian of a hyperelliptic curve. Math. Comp., **48** (1987) 95–101
3. Cassel, J. W. S., Flynn, E. V.: Prolegomena to a middlebrow arithmetic of curves of genus 2, London Mathematical Society Lecture Note Series, **230** (1996)
4. Cohen, H., Miyaji, A., Ono, T.: Efficient elliptic curve exponentiation using mixed coordinates, Asiacrypt'98, Lecture Notes in Computer Science, **1514** (1998) 51–65
5. Coron, J. S.: Resistance against differential power analysis for elliptic curve cryptosystems, CHES'99, Lecture Notes in Computer Science, **1717** (1999) 292–302

6. Doche, C., Duquesne, S.: Manual for the elliptic curve library, Arehcc report (2003)
7. Duquesne, S.: Improvement of the Montgomery method for general elliptic curves defined over $\mathbb{F}_p$, preprint (2003)
8. Flynn, E. V.: The group law on the Jacobian of a curve of genus 2, J. reine angew. Math., **439** (1993), 45–69
9. Flynn, E. V.: ftp site, ftp://ftp.liv.ac.uk/pub/genus2/kummer
10. Fischer, W., Giraud, C., Knudsen, E. W., Seifert, J. P.: Parallel scalar multiplication on general elliptic curves over $\mathbb{F}_p$ hedged against Non-Differential Side-Channel Attacks, preprint
11. Gaudry, P., Schost, E.: Construction of secure random curves of genus 2 over prime fields, Eurocrypt'04, Lecture Notes in Computer Science (2004)
12. Harley, R.: Fast arithmetic on genus 2 curves, available at http://cristal.inria.fr/∼harley/hyper (2000)
13. Izu, T., Takagi, T.: A fast Elliptic Curve Multiplication Resistant against Side Channel Attacks, preprint
14. Koblitz, N.: Elliptic curve cryptosystems, Math. Comp., **48** (1987) 203–209
15. Koblitz, N.: Algebraic aspects of cryptography, Algorithms and Computation in Mathematics, **3** (1998)
16. Kocher, P. C.: Timing attacks on implementations of DH, RSA, DSS and other systems, CRYPTO'96, Lecture Notes in Computer Science, **1109** (1996), 104–113
17. Kocher, P. C., Jaffe, J., Jun, B.: Differential power analysis, CRYPTO'99, Lecture Notes in Computer Science, **1666** (1999) 388-397
18. Koyama, K., Tsuruoka, Y.: Speeding up elliptic cryptosystems by using a signed binary window method, Crypto'92, Lecture Notes in Computer Science, **740** (1993) 345–357
19. Lange, T.: Efficient Arithmetic on Genus 2 Hyperelliptic Curves over Finite Fields via Explicit Formulae, Cryptology ePrint Archive, **121** (2002)
20. Lange, T.: Inversion-Free Arithmetic on Genus 2 Hyperelliptic Curves, Cryptology ePrint Archive, **147** (2002)
21. Lange, T.: Weighted Coordinates on Genus 2 Hyperelliptic Curves, Cryptology ePrint Archive, **153** (2002)
22. Matsuo, K. Chao, J. Tsujii, S.: An improved baby step giant step algorithm for point counting of hyperelliptic curves over finite fields, ANTS-V, Lecture Notes in Computer Science, **2369** (2002) 461–474
23. Miller, V. S.: Use of elliptic curves in cryptography, Crypto'85, Lecture Notes in Computer Science, **218** (1986) 417–426
24. Montgomery, P. L.: Speeding the Pollard and elliptic curve methods of factorization, Math. Comp., **48** (1987) 243–164
25. Mumford, D.: Tata lectures on Theta II, Birkhuser (1984)
26. Okeya, K., Kurumatani, H., Sakurai, K.: Elliptic curves with the Montgomery-form and their cryptographic applications, Public Key Cryptography, Lecture Notes in Computer Science, **1751** (2000) 238–257
27. Okeya, O., Sakurai, K.: Efficient Elliptic Curve Cryptosystems from a Scalar Multiplication Algorithm with Recovery of the y-Coordinate on a Montgomery-Form Elliptic Curve, Cryptographic Hardware and Embedded Systems, Lecture Notes in Computer Science, **2162** (2001) 126–141
28. Quisquater, J. J., Samyde, D.: ElectroMagnetic Analysis (EMA): Measures and Countermeasures for Smart Cards, e-smart 2001, Lecture Notes in Computer Science, **2140**, (2001), 200–210

Journal de Théorie des Nombres
de Bordeaux **19** (2007), 81–100

Elliptic curves associated with simplest quartic fields

par Sylvain DUQUESNE

Résumé. Nous étudions la famille infinie des courbes elliptiques associées aux "simplest quartic fields". Si le rang de telles courbes vaut 1, nous déterminons la structure complète du groupe de Mordell-Weil et nous trouvons tous les points entiers sur le modèle original de la courbe. Notons toutefois que nous ne sommes pas capables de les trouver sur le modèle de Weierstrass quand le paramètre est pair. Nous obtenons également des résultats similaires pour une sous-famille infinie de courbes de rang 2. A notre connaissance, c'est la première fois que l'on a autant d'information sur la structure du groupe de Mordell-Weil et sur les points entiers pour une famille infinie de courbes de rang 2. Le principal outils que nous avons utilisé pour cette étude est la hauteur canonique.

Abstract. We are studying the infinite family of elliptic curves associated with simplest cubic fields. If the rank of such curves is 1, we determine the whole structure of the Mordell-Weil group and find all integral points on the original model of the curve. Note however, that we are not able to find them on the Weierstrass model if the parameter is even. We have also obtained similar results for an infinite subfamily of curves of rank 2. To our knowledge, this is the first time that so much information has been obtained both on the structure of the Mordell-Weil group and on integral points for an infinite family of curves of rank 2. The canonical height is the main tool we used for that study.

1. Introduction

In [4], we studied elliptic curves associated with simplest cubic fields. In the case of curves of rank 1, we determined both the structure of the Mordell-Weil group and all integral points. Several questions remained unanswered at the end of this study. Is it possible to do the same work with other families of rank 1 curves? Is it possible to generalize to families of curves of higher ranks? Xavier Roblot and Franck Leprevost suggested

Manuscrit reçu le 28 décembre 2005.

that I should work on elliptic curves associated with simplest quartic fields. This family has several interesting properties.

- There is an explicit point on every curve of the family, which is a necessary condition for the kind of study we are interested in.
- Contrary to simplest cubic fields, the curves are not torsion-free. Hence we can check if the method used in [4] is also valid when there are torsion points.
- It is possible to extract a subfamily of curves of rank at least 2 with two explicit points.

In this paper, we will first see that the method used for simplest cubic fields to determine the structure of the Mordell-Weil group can also be used for simplest quartic fields. It can also be generalized to higher ranks and probably to other families. However, we will see that this is not the case for integral points, even though a technical trick enabled us to conclude in our case.

Finally recent papers ([2], [3]), not known when this paper was written, would be helpful in simplifying some of the calculations. They provide better bounds than those used in this paper and then will probably eliminate some cases which are done by hand in the following.

2. Simplest quartic fields

The term "simplest" has been used to describe certain number fields defined by a one-parameter family of polynomials. The regulator of these simplest fields is small in an asymptotic sense, so their class number tends to be large. This is why they have generated so much interest. In degree 4, simplest quartic fields are defined by adjoining to $\mathbb{Q}$ a root of the polynomials

$$X^4 - tX^3 - 6X^2 + tX + 1,$$

where $16+t^2$ is not divisible by an odd square (which ensures the irreducibility of the polynomial). These fields were studied, among other things, by Gras, who proved that this family is infinite [5]. Later, Lazarus studied their class number [8, 9]. More recently, they were studied by Louboutin [10], Kim [7] and Olajos [11].

3. Elliptic curves associated with simplest quartic fields

In the following, we are interested in the infinite family of elliptic curves Q_t given by the equation

$$Y^2 = X^4 - tX^3 - 6X^2 + tX + 1,$$

where $16 + t^2$ is not divisible by an odd square. The discriminant is $\Delta_t = 2^6(16 + t^2)^3$.

Let us first put the curve into the Weierstrass form

$$C_t : \ y^2 = x^3 - (16 + t^2)x$$

by sending the point $[0, 1]$ to infinity using the transformation φ

$$x = \frac{2Y - 2X^2 + tX + 2}{X^2},$$
$$y = \frac{\left(Y + X^2 + 1\right)\left(2Y - 2X^2 + tX + 2\right)}{X^3}.$$

Such curves are special cases of curves defined by equations of the form $y^2 = x^3 + Dx$ which often appear in the literature. For instance they are studied in the book of Silverman [14] where several general results are proved, one of which is given below

Proposition 3.1. *Let D be a fourth-power-free integer. Let E_D be the elliptic curve defined over $\mathbb{Q}$ by the equation*

$$y^2 = x^3 + Dx.$$

If $D \neq 4$ and $-D$ is not a perfect square, then

$$E_D(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z}.$$

This result can be applied to our family.

Corollary 3.2. *Let t be an integer defining a simplest quartic field. The only torsion points on $C_t(\mathbb{Q})$ are the point at infinity and the 2-torsion point $[0, 0]$. The torsion points on $Q_t(\mathbb{Q})$ can be obtained using the inverse map of φ.*

As usual with elliptic curves, we are interested in the following two Diophantine problems.

(1) Determination of the structure of the Mordell-Weil group $Q_t(\mathbb{Q})$ (or equivalently $C_t(\mathbb{Q})$). This means that we want to compute the torsion subgroup (already done thanks to Proposition 3.1), the rank and a set of generators for the free part.
(2) Determination of all integral points on both Q_t and C_t, since a famous theorem of Siegel states that there are only finitely many such points.

Concerning the second problem, it is important to note that the integral points are dependent on the model. In the case of elliptic curves associated with simplest quartic fields, both models (Q_t and C_t) given above are interesting. Nevertheless they are linked thanks to the following property.

Proposition 3.3. *Let t be an integer defining a simplest quartic field and $[X, Y]$ be an integral point on the quartic model. Then $\varphi([X, Y]) + [0, 0]$ is an integral point on the cubic model.*

Proof. It is easy to formally compute $\varphi([X,Y])+[0,0]$ using the group law on $C_t(\mathbb{Q})$:

$$\varphi([X,Y])+[0,0]=[2Y+2X^2-tX-2,-(Y+X^2+1)(2Y+2X^2-tX-2)]$$

which proves the proposition. □

This means that it is sufficient to find all integral points on C_t in order to find those of Q_t. On the other hand, the structure of the Mordell-Weil group does not depend on the model, so we will work on C_t in the following.

4. Experimental approach

Using the `magma` algebra system, we performed a large number of computations both of the structure of the Mordell-Weil group and of the integral points. Here we do not present the results we obtained, but we give the most important observations we deduced from these computations.

(1) The rank is never 0.
(2) The rank parity only depends on the congruence class of t modulo 16.
(3) The point $[-4,2t]$ can always be in a system of generators of $C_t(\mathbb{Q})$.
(4) In the case of rank 1, the only integral points on C_t are $[0,0]$, $[-4,\pm 2t]$ and $\left[\frac{t^2}{4}+4,\pm\left(\frac{t^3}{8}+2t\right)\right]$ if t is even.
(5) In the case of rank 1, $[0,\pm 1]$ are the only integral points on Q_t.
(6) In higher ranks, there are very few integral points on Q_t apart from a point with a x-coordinate equal to -3.

The first observation is trivial to prove. Indeed, $[-4,2t]$ is always a point on $C_t(\mathbb{Q})$. Moreover, we already proved that $[0,0]$ and the point at infinity are the only torsion points. So $[-4,2t]$ has an infinite order and $C_t(\mathbb{Q})$ has a rank of at least one.

5. The sign of the functional equation

We will now prove the second observation assuming the conjecture of Birch and Swinnerton-Dyer.

Theorem 5.1. *Let t be an integer defining a simplest quartic field. Assuming the Birch and Swinnerton-Dyer conjecture, the Mordell-Weil rank of $C_t(\mathbb{Q})$ is even if and only if*

$$t\equiv 0,\pm 1,\pm 7 \bmod 16.$$

Proof. We use the sign of the functional equation which is 1 if and only if the rank is even assuming the conjecture of Birch and Swinnerton-Dyer.

This sign can be computed as a product of local signs :

$$\varepsilon=\varepsilon_\infty\prod_{p \text{ prime}}\varepsilon_p.$$

The value of the sign at the Archimedean place is always $\varepsilon_\infty = -1$. Concerning finite places, the local sign depends on the type of curve reduction. It can be computed using the tables given by Rizzo in [12]. The places 2 and 3 must be treated separately. The first remark is that $16 + t^2$ is never divisible by 3, so 3 is always a prime of good reduction and $\varepsilon_3 = 1$. Now let p be a prime number greater than or equal to 5. Hereafter in this paper, $v_p(x)$ will denote the p-adic valuation of x.

If $p \nmid \Delta_t$, then $\varepsilon_p = 1$.

If $p|\Delta_t$, we have that $v_p(\Delta_t) = 3$ since $16 + t^2$ is not divisible by an odd square. In this case, Rizzo's tables give $\varepsilon_p = \left(\frac{-2}{p}\right)$, so

$$\varepsilon_p = \begin{cases} (-1)^{\frac{p-1}{4}} & \text{if} \quad p \equiv 1 \bmod 4 \\ -(-1)^{\frac{p+1}{4}} & \text{if} \quad p \equiv -1 \bmod 4\,. \end{cases}$$

We want now to compute the product of all these local signs.

Let $\delta_t = 16 + t^2$ and $\delta'_t = \frac{\delta_t}{2^{v_2(\delta_t)}}$. Since t defines a simplest quartic field, there are k different prime numbers $p_1, \ldots, p_k$ which are congruent to 1 modulo 4 and r different prime numbers $p_{k+1}, \ldots, p_{k+r}$ which are congruent to -1 modulo 4, such that

$$\delta'_t = p_1 \ldots p_k p_{k+1} \ldots p_{k+r}.$$

Moreover, it is easy to prove that δ'_t equals 1 modulo 4, so r must be even. Let $q_i = \frac{p_i - 1}{4}$ if $i \leq k$ and $q_i = \frac{p_i+1}{4}$ if $i \geq k+1$. We have

$$\begin{aligned} \delta'_t &= (1 + 4q_1) \ldots (1 + 4q_k)(-1 + 4q_{k+1}) \ldots (-1 + 4q_{k+r}) \\ &\equiv 1 + 4q_1 + \cdots + 4q_{k+r} \bmod 8. \end{aligned}$$

On the other hand,

$$\begin{aligned} \prod_{p \neq 2} \varepsilon_p &= (-1)^{q_1} \ldots (-1)^{q_k} (-1)^r (-1)^{q_{k+1}} \ldots (-1)^{q_{k+r}} \\ &= (-1)^{q_1 + \cdots + q_{k+r}}. \end{aligned}$$

So

$$\prod_{p \neq 2} \varepsilon_p = (-1)^{\frac{\delta'_t - 1}{4}}.$$

It is easy to deduce that

$$\prod_{p \neq 2} \varepsilon_p = 1 \Longleftrightarrow t \text{ odd or } t \equiv 0 \bmod 16 \text{ or } t \equiv \pm 4 \bmod 32.$$

We will now compute the local sign ε_2. For this, we again use the tables of Rizzo. For each value of t modulo 32, the 2-adic valuations of both Δ_t and the usual invariant $c_4 = 3.2^4(16 + t^2)$ give the value of ε_2. We have

$$\varepsilon_2 = 1 \Longleftrightarrow t \equiv \pm 3 \bmod 8 \text{ or } t \equiv \pm 4 \bmod 32.$$

We just have to multiply ε_∞, $\prod_{p\neq 2}\varepsilon_p$ and ε_2 to achieve the proof of the theorem. $\square$

Remark. We chose to use the tables of Rizzo instead of those of Halberstadt [6] because the minimality of the model is not required. In fact, the model is minimal if t is not divisible by 4. When t is divisible by 4, the minimal model is $y^2 = x^3 - (1+t^2)x$.

We now want to prove the observations 3, 4 and 5. For this, we use a method similar to that we used for elliptic curves associated with simplest cubic fields in [4]. The central part of this method is a good estimate of the canonical height. Let us briefly review this canonical height.

6. Canonical height on elliptic curves

Even though it is possible to work on number fields, we will restrict our study to $\mathbb{Q}$ since this is the case we are interested in. Let E be an elliptic curve defined over $\mathbb{Q}$ and $P = [x, y]$ be a point on $E(\mathbb{Q})$. If $x = n/d$ with $\gcd(n, d) = 1$ the naïve height of point P is defined as

$$h(P) = \max(\log|n|, \log|d|).$$

This height function is the main tool for the proof of the Mordell-Weil theorem which states that $E(\mathbb{Q})$ is finitely generated. The naïve height has some nice properties but we need a more regular function. This function is the canonical height and is defined as follows

$$\hat{h}(P) = \lim_{k\to\infty}\frac{h(kP)}{k^2} = \lim_{n\to\infty}\frac{h(2^nP)}{4^n}.$$

Remark. The canonical height is sometimes defined as half of this value, so one must be very careful which definition is used for results from different origins.

The canonical height has a lot of interesting properties. We will just mention here those that we will use later in this work.

(1) We have
$$\hat{h}(P) = 0 \Longleftrightarrow P \in E(\mathbb{Q})_{\text{tors}}.$$

(2) Function $\hat{h}$ is a quadratic form on $E(\mathbb{Q})$.

(3) Let
$$\langle P, Q\rangle = \frac{\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)}{2},$$
denote the scalar product associated with $\hat{h}$. If $P_1, \ldots, P_n$ are n points in the free part of $E(\mathbb{Q})$, let us define the elliptic regulator of points P_i by
$$R(P_1, \ldots, P_n) = \det(\langle P_i, P_j\rangle)_{1\le i,j\le n}.$$

Then, points $P_1, \ldots, P_n$ are linearly independent if and only if their elliptic regulator is not equal to zero.

The naïve height is much easier to compute than the canonical height, so it is interesting to have explicit bounds for the difference between both of them. Such bounds are given by Silverman in [16].

Theorem 6.1 (Silverman)**.** *Let E be an elliptic curve defined over $\mathbb{Q}$. Let Δ be the discriminant of E and j its j-invariant. Then for any P in $E(\mathbb{Q})$ we have*

$$-\frac{h(j)}{4} - \frac{h(\Delta)}{6} - 1.946 \leq \hat{h}(P) - h(P) \leq \frac{h(j)}{6} + \frac{h(\Delta)}{6} + 2.14.$$

However, better bounds on the canonical heights are required for our purpose. For instance, if the naïve height of P is small, the lower bound given by Silverman does not give any information since $\hat{h}(P)$ is always non-negative. We will now briefly recall two ways to compute the canonical height. Both will be used hereafter in this work to improve Silverman's bounds for the curves we are interested in.

7. Computation of the canonical height

The two ways of computation we will present here consist of expressing the canonical height as a sum of local functions. The finite part of the height equals 0 for all primes of good reduction. For primes of bad reduction, it can be computed using a technical but simple algorithm given in [1]. The main part of the computation is focused on the Archimedean contribution which we will denote $\hat{h}_\infty$. This can be done by two ways. The first one uses q-expansions and consists of evaluation of the following formula

$$\hat{h}_\infty(P) = \frac{1}{16}\log\left|\frac{\Delta}{q}\right| + \frac{1}{4}\log\left(\frac{y(P)^2}{\lambda}\right) - \frac{1}{2}\log\theta,$$

where, if ω_1 and ω_2 denote the periods of the curve, and $z(P)$ is the elliptic logarithm of the point P

$$\begin{aligned}
\lambda &= \frac{2\pi}{\omega_1},\\
q &= e^{2\imath\pi\frac{\omega_1}{\omega_2}},\\
\theta &= \sum_{n=0}^{\infty}(-1)^n q^{\frac{n(n+1)}{2}}\sin((2n+1)\lambda\Re e(z(P))).
\end{aligned}$$

If the curve is explicitly given, this method is very efficient since the series θ converges rapidly. However, we are dealing with a family of elliptic curves and, in this context, computation of the terms of the series θ seems

difficult. We can still give an upper bound for this series. It is indeed trivial that

$$|\theta| \leq \frac{1}{1-|q|}.$$

This will provide a lower bound for the canonical height which is more useful than that given by Theorem 6.1. Such a lower bound combined with Silverman's upper bound was successfully used for simplest cubic fields in [4]. Concerning simplest quartic fields, these bounds can also be used when the rank of $C_t(\mathbb{Q})$ is 1. However, they are not sharp enough when the rank is 2. The second way of computing the Archimedean contribution will provide these better bounds. This other way is slower but more appropriate for specific cases we are studying. It was developed by Tate and was improved by Silverman in [15]. It consists of computing the simple series

$$\hat{h}_\infty(P) = \log|x(P)| + \frac{1}{4}\sum_{n=0}^{\infty}\frac{c_n}{4^n}$$

where c_i are easily computable and bounded. The main advantage is that the computation of the c_i of a specific point can be done even for our family whereas computation of the terms of the series θ seems difficult for a family. Moreover, Silverman gives bounds for the error term if only N terms are used in the series. Let $H = \max(4, 2|a|, 4|b|, a^2)$, then

$$\hat{h}_\infty(P) = \log|x(P)| + \frac{1}{4}\sum_{n=0}^{N-1}\frac{c_n}{4^n} + R(N),$$

with

$$\frac{1}{3.4^N}\log\left(\frac{\Delta^2}{2^{60}H^8}\right) \leq R(N) \leq \frac{1}{3.4^N}\log\left(2^{11}H\right). \tag{1}$$

Thus, Tate's method will provide better bounds for the canonical height of specific points, such as $[-4, 2t]$. However, we first need bounds which are valid for any point in $C_t(\mathbb{Q})$, so we use Silverman's theorem and q-expansions.

8. Approximation of the canonical height of any point on $C_t(\mathbb{Q})$

As explained above, an upper bound of the canonical height is given by Silverman's theorem:

$$\hat{h}(P) - h(P) \leq \frac{h(j)}{6} + \frac{h(\Delta)}{6} + 2.14.$$

Applying this bound to our family gives the following proposition.

Proposition 8.1. *Let t be an integer defining a simplest quartic field. Let P be a point in $C_t(\mathbb{Q})$, then*

$$\hat{h}(P) \leq h(P) + \frac{1}{2}\log(16+t^2) + 4.08.$$

We will now use the decomposition of the canonical height as a sum of local functions to obtain a lower bound.

The first step involves the computation of the finite part of the canonical height of a point $P = \left[\frac{a}{d^2}, \frac{b}{d^3}\right]$. For this, we follow the algorithm given in [1]. If p is an odd prime number, it is easy to prove that the local contribution at p is $2\log\left(p^{v_p(d)}\right) - \frac{1}{2}\log(p)$ if p divides a, b and $16+t^2$ and 0 otherwise. The contribution at 2 is more difficult to find since there are several cases depending on the 2-adic valuation of t and a. We summarize the result in the following table.

condition	contribution at 2
d even	$2\log\left(2^{v_2(d)}\right)$
t odd and a odd	$-\frac{1}{2}\log(2)$
t even and a odd or a even and t odd	0
$v_2(a)=1$ and $v_2(t)=1$	$-\frac{3}{2}\log(2)$
$v_2(a)=1$ and $v_2(t)\geq 2$ or $v_2(t)=1$ and $v_2(a)\geq 2$	$-\log(2)$
$v_2(a)=2$ and $v_2(t)=2$ or $v_2(a)\geq 3$ and $v_2(t)\geq 3$	$-2\log(2)$
$v_2(a)=2$ and $v_2(t)\geq 3$ or $v_2(t)=2$ and $v_2(a)\geq 3$	$-\frac{5}{2}\log(2)$

Finally, the local contribution at non-Archimedean places to the canonical height of any point P is given by

$$\hat{h}_f(P) = 2\log(d) - \frac{1}{2}\log\left(\prod_{p_i\neq 2, p_i \mid a,b,16+t^2} p_i\right) + \hat{h}_2(P), \tag{2}$$

where $\hat{h}_2(P)$ is equal to zero if d is even and to the contribution at 2, given in the previous table, if d is odd. The second step is the computation of the Archimedean contribution. As explained above, we will use q-expansions since we want a lower bound that is valid for any point on the curve. We first need approximations for the periods ω_1 and ω_2.

Lemma 8.2. *Let t be an integer defining a simplest quartic field and C_t be the associated elliptic curve. Let ω_1 and ω_2 be the periods of C_t such that ω_1 and $\imath\omega_2$ are positive, then*

$$\omega_1 = \imath\omega_2 \quad \textit{and} \quad \frac{\pi}{\sqrt{2}(16+t^2)^{\frac{1}{4}}} \leq \omega_1 \leq \frac{\pi}{(16+t^2)^{\frac{1}{4}}}$$

Proof. Let $\delta = \sqrt{16+t^2}$. The C_t equation is

$$y^2 = x^3 - \left(16+t^2\right)x = x(x-\delta)(x+\delta).$$

Thus, with the convention we chose for the periods, ω_1 and ω_2 are given by the integrals

$$\omega_1 = \int_{-\delta}^{0} \frac{1}{\sqrt{x\,(x-\delta)\,(x+\delta)}},$$
$$\omega_2 = \int_{0}^{\delta} \frac{1}{\sqrt{x\,(x-\delta)\,(x+\delta)}}.$$

A trivial change of variable shows that $\omega_1 = \imath\omega_2$. Concerning ω_1, within the integration range, we have $-2\delta \leq x-\delta \leq -\delta$, so that

$$\frac{1}{\sqrt{2}(16+t^2)^{\frac{1}{4}}}\int_{-\delta}^{0}\frac{1}{\sqrt{x(x+\delta)}} \leq \omega_1 \leq \frac{1}{(16+t^2)^{\frac{1}{4}}}\int_{-\delta}^{0}\frac{1}{\sqrt{x(x+\delta)}}.$$

The result follows thanks to an easy change of variables. □

So, thanks to this lemma, we can give a lower bound for the Archimedean contribution to the canonical height of any point $P = \left[\frac{a}{d^2}, \frac{b}{d^3}\right]$ in the free part of $C_t(\mathbb{Q})$.

$$\hat{h}_\infty\left([P]\right) \geq 0.38 + \frac{1}{8}\log(16+t^2) + \frac{1}{2}\log\left(\frac{b}{d^3}\right).$$

Thus, combining this lower bound with the non-Archimedean contributions, we have

$$\hat{h}(P) \geq 0.38 - \frac{5}{2}\log(2) + \frac{1}{8}\log(16+t^2) + \frac{1}{2}\log(d) + \frac{1}{2}\log\left(\frac{b}{\prod\limits_{p_i\neq 2, p_i | a,b,16+t^2} p_i}\right).$$

The last two terms are always positive, so this provides an explicit lower bound. However, these terms can be used to reduce the constant $0.38 - \frac{5}{2}\log(2)$. Let g be the gcd of a, b and $16+t^2$ divided by its higher power of 2. Let $A = \frac{a}{g}$ and $B = \frac{b}{g}$. With these notations, the sum of the last two terms of the lower bound equals $\frac{1}{2}\log(Bd)$, so a lower bound for Bd will improve the lower bound for $\hat{h}(P)$. Based on the fact that $\left[\frac{a}{d^2}, \frac{b}{d^3}\right]$ is a point on the curve, we prove that g must satisfy the equation

$$A^3g^2 - B^2g - A(16+t^2)d^4 = 0.$$

Since g is an integer, the discriminant of this degree 2 polynomial must be the square of an integer, say C, such that

$$B^4 + 64A^4d^4 = \left(C - 2A^2td^2\right)\left(C + 2A^2td^2\right).$$

It is easy to deduce that, if such a C exists, then

$$t \leq \frac{B^4 + 64A^4d^4 - 1}{4A^2d^2}.$$

Let us assume that the local contribution at 2 is negative, i. e. d is odd and t and a are together even or odd. In this case, we have $4|B$ and $A \leq B^2$. If $B = 4$ and $d = 1$, the above condition becomes $t \leq 4160$. For all $t \leq 4160$ and $A \leq 16$, we can check if the discriminant of the degree 2 polynomial is a square. This never occurs if $t > 256$. Thus, if $t > 256$, it is not possible to have $B = 4$ and $d = 1$, so either $B \geq 4$ and $d \geq 3$ or $B \geq 8$ and $d = 1$. In any case, $Bd \geq 8$. We can now give a lower bound for the canonical height.

Proposition 8.3. *Let t be an integer greater than 256 defining a simplest quartic field. Let P be any point in the free part of $C_t(\mathbb{Q})$. We have*

$$\hat{h}(P) \geq 0.38 + \frac{1}{8}\log(16 + t^2) \qquad \textit{if } t \textit{ is odd,}$$

$$\hat{h}(P) \geq 0.38 + \frac{1}{8}\log(16 + t^2) - \log(2) \qquad \textit{in any case.}$$

Proof. If t is odd and $\hat{h}_2(P) = 0$ then $Bd \geq 1$ is sufficient to give the required lower bound for $\hat{h}(P)$. If t is odd and $\hat{h}_2(P) < 0$, this contribution is $-\frac{1}{2}\log(2)$ and we proved that $Bd \geq 8$. This provides a better lower bound than required. Finally, if t is even and $\hat{h}_2(P) < 0$, this contribution is greater than or equal to $-\frac{5}{2}\log(2)$ and we proved that $Bd \geq 8$. Again, this is sufficient to conclude. □

9. Estimates of the canonical height of a specific point: $[-4, 2t]$

The previous bounds are valid for any non-torsion point on $C_t(\mathbb{Q})$, so they provide bounds for the points $G_1 = [-4, 2t]$. However, we need a more precise approximation for $\hat{h}(G_1)$. So we will use Tate's series to compute $\hat{h}(G_1)$ in terms of t. For our purpose, it is sufficient to compute the first four terms of the series:

$$\hat{h}_\infty(G_1) = \log(4) + \frac{1}{4}\left(c_0 + \frac{c_1}{4} + \frac{c_2}{16} + \frac{c_3}{64}\right) + R(4).$$

We are using the algorithm given in [15] to formally compute c_0, c_1, c_2 and c_3. In fact, the only significant contribution comes from c_0. Thus we only give approximations for the others.

$$c_0 = 2\log\left(16 + t^2\right) - 8\log(2) \text{ and } 0 \leq c_1, c_2, c_3 \leq \log(4).$$

Let us now estimate the error term $R(4)$. In the case of elliptic curves defined by simplest quartic fields, the constant H involved in the approximation of the rest (1) equals $\left(16 + t^2\right)^2$ so

$$\frac{1}{3.4^4}\log\left(\frac{2^{12}\left(16+t^2\right)^6}{2^{60}\left(16+t^2\right)^{16}}\right) \leq R(4) \leq \frac{1}{3.4^4}\log\left(2^{11}\left(16+t^2\right)^2\right),$$

$$-\frac{48\log(2)+10\log\left(16+t^2\right)}{768} \leq R(4) \leq \frac{11\log(2)+2\log\left(16+t^2\right)}{768}.$$

Concerning non-Archimedean contributions, the only non-zero one comes from 2. The previous table can be used to estimate the contribution at 2

$$\begin{cases} \hat{h}_2(G_1)=0 & \text{if } t \text{ is odd,} \\ -\frac{5}{2}\log(2) \leq \hat{h}_2(G_1) \leq -\log(2) & \text{otherwise.} \end{cases}$$

Finally, combining these estimates we obtain an estimate for the canonical height of the point $[-4,2t]$

$$\begin{aligned} \hat{h}([-4,2t]) &\geq \tfrac{187}{384}\log\left(16+t^2\right)-\tfrac{1}{16}\log(2) && \text{if } t \text{ is odd,} \\ \hat{h}([-4,2t]) &\geq \tfrac{187}{384}\log\left(16+t^2\right)-\tfrac{41}{16}\log(2) && \text{in any case,} \\ \hat{h}([-4,2t]) &\leq \tfrac{193}{384}\log\left(16+t^2\right)+\tfrac{137}{768}\log(2) && \text{in any case.} \end{aligned}$$

We now have sufficiently good estimates to prove some of our observations when the rank is 1.

10. Solving Diophantine problems in rank 1

In this section, we will prove most of our observations concerning the structure of $C_t(\mathbb{Q})$ and the integral points both on C_t and Q_t.

Theorem 10.1. *Let t be an integer defining a simplest quartic field, and C_t be the associated elliptic curve. Then the point $[-4,2t]$ can always be in a system of generators. In particular, if the rank of C_t is one,*

$$C_t(\mathbb{Q}) = \langle [0,0],[-4,2t]\rangle.$$

Proof. Assume that $G_1=[-4,2t]$ cannot be in a system of generators. This means that there exist $P \in C_t(\mathbb{Q})$, $\varepsilon \in \{0,1\}$ and $n \in \mathbb{Z}$ such that

$$G_1 = nP + \varepsilon[0,0].$$

So the canonical height of G_1 equals the canonical height of nP and

$$n^2 = \frac{\hat{h}(G_1)}{\hat{h}(P)}.$$

The estimates obtained above can now be used to bound n^2. If $t \geq 257$

$$n^2 \leq \frac{\frac{193}{384}\log\left(16+t^2\right)+\frac{137}{768}\log(2)}{\frac{1}{8}\log\left(16+t^2\right)+0.38-\log(2)}.$$

Since this function decreases with t, it is easy to prove that

$$n^2 \leq 5.31 \text{ if } t \geq 257.$$

The remaining cases, namely $n = 2$ or $t \leq 256$, can be computed by hand. □

Let us now concentrate on integral points. When the rank is one, the structure of the Mordell-Weil group is known, so we are using it to find integral points on C_t. If P is an integral point then there exist $\varepsilon \in \{0, 1\}$ and $n \in \mathbb{Z}$ such that

$$P = nG_1 + \varepsilon[0, 0].$$

The strategy is the same as above, namely we are using the bounds on canonical heights to deduce an upper bound on n. But, in this case, we need an upper bound for the canonical height of any integral point. Using Silverman's bounds, this means that we need an upper bound for the naïve height of any integral point. This is of course not possible unless we have an explicit version of Siegel's theorem. In the case of simplest cubic fields, we proved by an other means that there are no integral points in the connected component of the point at inifinity of the curve. This cannot be done for simplest quartic fields for any t. However, it can be done if t is odd. For this, we will use the following lemma.

Lemma 10.2. *Let E be an elliptic curve defined over $\mathbb{Q}$ and P be a point on $E(\mathbb{Q})$ which is not integral. Then none of the multiples of P are integral.*

Proof. We just give the idea of the proof. Let p be a prime number dividing the denominator of the coordinates of P. The reduction of P modulo p is the point at infinity on the reduced curve. So all multiples of P are also the point at infinity on the reduced curve. Thus their denominators are also divisible by p. □

Theorem 10.3. *Let t be an odd number defining a simplest quartic field. Assume that the elliptic curve C_t has rank 1, then the only integral points on C_t are $[0, 0]$ and $[-4, \pm 2t]$.*

Proof. Let P be an integral point on C_t. Then, there exist $\varepsilon \in \{0, 1\}$ and $n \in \mathbb{Z}$ such that

$$P = nG_1 + \varepsilon[0, 0].$$

Three cases can occur

- n is even and $\varepsilon = 0$. In this case, P is a multiple of $2[-4, 2t]$ which is never an integral point if $t \neq 4, 8$. Lemma 10.2 then ensures that P is not an integral point.
- n is odd and $\varepsilon = 1$. Again P is a multiple of $[-4, 2t] + [0, 0]$ which is not an integral point and we use Lemma 10.2.

- n is odd and $\varepsilon = 0$ or n is even and $\varepsilon = 1$. In this case, P is not in the connected component of the point at infinity of $C_t(\mathbb{R})$ so its x-coordinate is bounded
$$-\sqrt{16+t^2} \leq x(P) \leq 0.$$
The method using canonical heights can then be applied. Thanks to Proposition 8.1, the canonical height of such a point is bounded as follows
$$\hat{h}(P) \leq h(P) + \frac{1}{2}\log(16+t^2) + 4.08 \leq \log(16+t^2) + 4.08.$$
Using the lower bound for the canonical height of $[-4, 2t]$ obtained in section 9, we deduce that
$$n^2 \leq \frac{\log(16+t^2) + 4.08}{\frac{187}{384}\log\left(16+t^2\right) - \frac{1}{16}\log(2)}.$$
Again, the function is decreasing and
$$n^2 \leq 3.9 \text{ if } t \geq 10.$$

So only $n = 0, 1$ or -1 can provide integral points. □

Remark. The second case cannot be treated if t is even because $[-4, 2t] + [0, 0]$ is an integral point.

We deduce the following corollary from this theorem and Proposition 3.3

Corollary 10.4. *Let t be an odd number defining a simplest quartic field such that Q_t has rank 1, then the only integral points on Q_t are $[0, \pm 1]$.*

In fact, we can prove this also when t is even thanks to the following lemma.

Lemma 10.5. *Let t be an odd number defining a simplest quartic field. Let $P = [X, Y]$ be an integral point on Q_t such that $Y \leq 0$. Then $\varphi(P) + [0, 0]$ is an integral point on C_t whose x-coordinate is bounded by t^2.*

Proof. The x-coordinate of $\varphi(P) + [0, 0]$ equals $2Y + 2X^2 - tX - 2$ and $Y = -\sqrt{X^4 - tX^3 - 6X^2 + tX + 1}$. Thus, it is sufficient to prove that
$$\left(2X^2 - tX - 2 - t^2\right)^2 - 4\left(X^4 - tX^3 - 6X^2 + tX + 1\right) \leq 0.$$
This polynomial is a degree 2 polynomial and it is easy to prove that it is negative outside of $\left]-\frac{n}{3} - 1, n + 1\right[$. Within this range, $2X^2 - tX - 2 - t^2$ is always negative which achieves the proof. □

We can now prove the following theorem

Theorem 10.6. *Let t be an integer defining a simplest quartic field such that Q_t has rank 1, then the only integral points on Q_t are $[0, \pm 1]$.*

Proof. Thanks to Lemma 10.5, it is sufficient to find all integral points on C_t whose naïve height is less than or equal to t^2. Let P be such an integral point. Proposition 8.1 provides an upper bound for its canonical height.

$$\hat{h}(P) \leq h(P) + \frac{1}{2}\log(16+t^2) + 4.08 \leq \frac{3}{2}\log(16+t^2) + 4.08.$$

If $P = n[-4, 2t] + \varepsilon[0,0]$, then

$$n^2 \leq \frac{\frac{3}{2}\log(16+t^2) + 4.08}{\frac{187}{384}\log\left(16+t^2\right) - \frac{41}{16}\log(2)}.$$

As in the previous cases, the function is decreasing and we deduce that

$$n^2 \leq 8.92 \text{ if } t \geq 33.$$

The remaining cases, namely $n = 2$ or $t \leq 32$, can easily be done by hand. □

We are now interested in the last observation in section 4 which will provide a subfamily with a rank of at least 2.

11. A subfamily with a rank at least 2

During our numerical experiments, we noticed that -3 is sometimes the x-coordinate of an integral point on Q_t. It is in fact not difficult to prove that

$$[-3, \dots] \in Q_t(\mathbb{Z}) \Longleftrightarrow t = 6k^2 + 2k - 1 \text{ with } k \in \mathbb{Z}.$$

In this case, there are new integral points on $C_t(\mathbb{Q})$. One of them is of course given by $\varphi([-3, 2+12k]) + [0,0]$. These new points are the following and their opposites.

$$\begin{aligned} G_2 &= \left[-2k^2 + 2k - 1, 4(k+1)\left(2k^2 - 2k + 1\right)\right], \\ G_2 + [0,0] &= \left[18k^2 + 30k + 17, 4(k+1)\left(18k^2 + 30k + 17\right)\right], \\ G_1 + G_2 &= \left[9\left(2k^2 - 2k + 1\right), 12(3k-2)\left(2k^2 - 2k + 1\right)\right]. \end{aligned}$$

Since t is odd and G_2 is an integral point, Theorem 10.3 ensures that the rank is at least 2. The aim of the rest of this paper is to generalize the results obtained in rank 1 to the case of rank 2 using this subfamily. Let us first consider the structure of the Mordell-Weil group.

12. Case of rank 2: generators

The infinite descent generalizes to higher ranks the method we used to prove that G_1 can always be in a system of generators. Let us first recall the principle of this method.

Suppose that $P_1 \dots P_r$ generate a subgroup of the free part of the Mordell-Weil group of full rank and denote by n the index of this subgroup. If $n = 1$, this provides a basis. Let R be the regulator of the curve (i. e. the elliptic

regulator of a basis B of the free part of the Mordell-Weil group), then we have

$$n^2 R = R(P_1 \dots P_r).$$

Since the regulator is roughly of the same order of magnitude as the product of the canonical heights of the basis B, it can be bounded using Proposition 8.3. So that n can be bounded. In [13], Siksek specifies this idea by the following theorem (written here only in the case of rank 2 and base field $\mathbb{Q}$).

Theorem 12.1 (Siksek)**.** *Let E be an elliptic curve defined over $\mathbb{Q}$ of rank 2. Suppose that $E(\mathbb{Q})$ contains no point of infinite order with a canonical height less than some positive real number λ. Suppose that P_1 and P_2 generate a subgroup of the free part of the Mordell-Weil group of full rank and denote by n the index of this subgroup. Then we have*

$$n \leq \frac{2}{\sqrt{3}} \frac{R(G_1, G_2)^{\frac{1}{2}}}{\lambda}.$$

As explained above, the infinite descent is based on canonical heights. Thus, we need to approximate the canonical heights of the points involved in our problem.

Proposition 12.2. *Let k be an integer such that $t = 6k^2 + 2k - 1$ defines a simplest quartic field and such that $|k| \geq 27$, then we have*

$$\begin{array}{lcl} 0.96\log(t) \leq & \hat{h}(G_1) & \leq 1.02\log(t) \\ 0.47\log(t) \leq & \hat{h}(G_2) & \leq 0.56\log(t) \\ 0.47\log(t) \leq & \hat{h}(G_1+G_2) & \leq 0.54\log(t). \end{array}$$

Proof. The first estimate is a direct consequence of the estimates given in section 9. Estimates for the canonical height of G_2 and G_1+G_2 are obtained in the same way, namely using the first four terms of the Tate series for the Archimedean contribution. Non-Archimedean contributions are given by formula (2), knowing that t is odd and that the gcd of a, b and $16 + t^2$ is exactly $2k^2 - 2k + 1$ both for G_2 and $G_1 + G_2$. □

We can now prove the following theorem

Theorem 12.3. *Let k be an integer such that $t = 6k^2 + 2k - 1$ defines a simplest quartic field. Then the points $G_1 = [-4, 2t]$ and $G_2 = \left[-2k^2 + 2k - 1, 4(k+1)\left(2k^2 - 2k + 1\right)\right]$ can always be in a system of generators. In particular, if the rank of C_t is exactly 2, we have*

$$C_t(\mathbb{Q}) = \langle G_1, G_2, [0, 0] \rangle.$$

Proof. In order to apply Siksek's theorem, we need an estimate of

$$R(G_1, G_2) = \hat{h}(G_1)\hat{h}(G_2) - \langle G_1, G_2 \rangle^2$$

with $\langle G_1, G_2\rangle = \frac{1}{2}\Big(\hat{h}(G_1+G_2) - \hat{h}(G_1) - h(G_2)\Big)$. Proposition 12.2 provides these estimates

$$\begin{aligned} -0.56\log(t) \leq \ \langle G_1, G_2\rangle \ &\leq -0.44\log(t) \\ R(G_1, G_2) &\leq 0.39\,(\log(t))^2 \end{aligned}$$

Siksek's theorem then ensures that if G_1 and G_2 generate a subgroup of index n of the free part of the Mordell-Weil group, then

$$n \leq \frac{2}{\sqrt{3}}\frac{R(G_1, G_2)^{\frac{1}{2}}}{\lambda},$$

with $\hat{h}(P) \geq \lambda$ for any point P in the free part of the Mordell-Weil group. The estimates obtained in Propositions 12.2 and 8.3 imply that, for any k such that $|k| \geq 27$,

$$n \leq \frac{2}{\sqrt{3}}\frac{\sqrt{0.39}\log(t)}{0.38 + \frac{1}{8}\log(16+t^2)} \leq \frac{2}{\sqrt{3}}\frac{\sqrt{0.39}\log(t)}{\frac{1}{4}\log(t)} \leq 2.9.$$

The case $n = 2$ must be treated by hand. For this, it is sufficient to prove that there are no point $Q \in C_t(\mathbb{Q})$ and integers ε_1 and ε_2 in $\{0, 1\}$ such that

$$\varepsilon_1 G_1 + \varepsilon_2 G_2 = 2Q.$$

This is not difficult because G_1, G_2 and $G_1 + G_2$ are integral points, so Q must be an integral point because of Lemma 10.2. Looking at the numerator and denominator of the double of any integral point modulo 8 shows that such a double is not an integral point. Finally, the cases with $k \leq 26$ can be treated by hand (i. e. using `magma`). □

The structure of the Mordell-Weil rank is now completely determined and can be used to find integral points.

13. Case of rank 2: integral points

The situation is the same as in rank one, namely we do not have any bound for the naïve height for integral points on $C_t(\mathbb{Q})$, so it is not possible, with our method, to determine all integral points on C_t. However, we can use the same trick to determine all integral points on Q_t.

Theorem 13.1. *Let k be an integer such that $t = 6k^2 + 2k - 1$ defines a simplest quartic field. Suppose that Q_t has rank 2, then the only integral points on Q_t are $[0, \pm 1]$ and $[-3, \pm(2 + 12k)]$.*

Proof. Thanks to Lemma 10.5, it is sufficient to find all integral points on C_t whose naïve height is less than or equal to t^2. Let P be such an

integral point. We have an upper bound for its canonical height provided by Proposition 8.1.

$$\hat{h}(P) \leq \frac{3}{2}\log(16+t^2)+4.08.$$

Theorem 12.3 implies that there are integers n_1 and n_2 and $\varepsilon \in \{0,1\}$ such that

$$P = n_1G_1 + n_2G_2 + \varepsilon[0,0].$$

Using the properties of the canonical height, we deduce that

$$\hat{h}(P) = n_1^2\hat{h}(G_1) + n_2^2\hat{h}(G_2) + 2n_1n_2\langle G_1, G_2\rangle.$$

We know, thanks to Proposition 12.2, that $\langle G_1, G_2\rangle$ is negative and that $\hat{h}(G_1) \geq \hat{h}(G_2)$. Hence it is easy to conclude if n_1n_2 is non-positive. Indeed, we have

$$\hat{h}(P) \geq (n_1^2+n_2^2)\hat{h}(G_2).$$

So, if $|k| \geq 27$, we have

$$\begin{aligned} n_1^2+n_2^2 &\leq \frac{\frac{3}{2}\log(16+t^2)+4.08}{0.47\log(t)} \\ &\leq 7.5 \end{aligned}$$

This proves that both $|n_1|$ and $|n_2|$ are less than or equal to 2, but not at the same time.If n_1n_2 is positive, it is more subtle. In this case we especially need precise approximations of Proposition 12.2. If $|k| \geq 27$, we have

$$\begin{aligned} \hat{h}(P) &\geq 0.96\log(t)n_1^2 + 0.47\log(t)n_2^2 - 1.11\log(t)n_1n_2 \\ &\geq 0.47(2.04n_1^2 + n_2^2 + 2.38n_1n_2)\log(t) \\ &\geq 0.47\left(0.62n_1^2 + (1.19n_1 - n_2)^2\right)\log(t)\,. \end{aligned}$$

Using the upper bound on $\hat{h}(P)$ given by Silverman, we deduce

$$\begin{aligned} \left(0.62n_1^2 + (1.19n_1^2 - n_2)^2\right) &\leq \frac{\frac{3}{2}\log(16+t^2)+4.08}{0.47\log(t)} \\ &\leq 7.5 \end{aligned}$$

We assume, without loss of generality, that n_1 and n_2 are both positive. It is easy to deduce that n_1 must be less than or equal to 3 and that

$$\begin{aligned} n_1 = 1 &\implies n_2 \leq 3 \\ n_1 = 2 &\implies n_2 \leq 4 \\ n_1 = 3 &\implies n_2 = 3 \text{ or } 4. \end{aligned}$$

The remaining cases must be done by hand; for $|k| < 27$ we used `magma`. For small values of n_1 and n_2, we are again using canonical heights. Let

us treat, for instance, the case $n_1 = 2$ and $n_2 = -1$. The bounds given in Proposition 12.2 ensure that

$$\hat{h}(G_1 - 2G_2) \geq 4.34 \log(t).$$

If $G_1 - 2G_2$ is an integral point, its naïve height equals the logarithm of its x-coordinate, so, using Proposition 8.1, we have

$$\hat{h}(G_1 - 2G_2) \leq \log(x(P)) + \frac{1}{2}\log(16 + t^2) + 4.08$$

with

$$x(P) = -4\left(\frac{24k^5 + 60k^4 + 24k^3 - 48k^2 - 54k - 13}{20k^4 + 56k^3 + 88k^2 + 76k + 29}\right)^2.$$

These two bounds are incompatible so $G_1 - 2G_2$ is never an integral point. In some cases, Silverman's bounds are not precise enough and thus we used bounds obtained by Tate's series.Finally, this proves that the only integral points having their x-coordinate less than or equal to t^2 on C_t are $[0,0]$, G_1, G_2, $G_1 + G_2$, $G_2 + [0,0]$ and $G_1 + 2G_2$ if $k \equiv -1 \bmod 5$ and their opposites. Using the reciprocal map of φ, it is easy to find all integral points on Q_t. □

14. Conclusion

As in the case of simplest cubic fields, we succeeded in proving that the point $[-4, 2t]$ can always be in a system of generators of $C_t(\mathbb{Q})$. We also succeeded in generalizing this to the rank 2 case. This is not surprising since it is based on the infinite descent method. Moreover, it is almost sure that it will also work with other families or with higher ranks assuming, of course, that explicit generators exist and are known.

On the contrary, we encountered difficulties in solving the problem of integral points on C_t, even in rank 1. This is due to the fact that we do not know any bound on the naïve height of integral points. This difficulty can be overcome in some specific situations, as in the case of simplest cubic fields or of simplest quartic fields when the parameter is odd. In fact, we noticed that the method used for simplest cubic fields in rank 1 will be successful for any family of torsion-free curves of rank 1.

However, we were able to give exactly all integral points on the original model of the curve both in the case of rank 1 and in the case of a subfamily of curves of rank 2.

References

[1] H. Cohen, *A Course in Computational Algebraic Number Theory.* Graduate Texts in Math. **138**, Springer-Verlag, 1993.

[2] J. Cremona, M. Prickett, S. Siksek, *Height difference bounds for elliptic curves over number fields.* Journal of Number Theory **116** (2006), 42–68.

[3] J. Cremona, S. Siksek, *Computing a Lower Bound for the Canonical Height on Elliptic Curves over* $\mathbb{Q}$. Algorithmic Number Theory, 7th International Symposium, ANTS-VII, LNCS **4076** (2006), 275–286.

[4] S. Duquesne, *Integral points on elliptic curves defined by simplest cubic fields.* Exp. Math. **10:1** (2001), 91–102.

[5] M. N. Gras, *Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré 4 de* $\mathbb{Q}$. Publ. Math. Fac. Sci. Besancon, fasc **2** (1977/1978).

[6] E. Halberstadt, *Signes locaux des courbes elliptiques en 2 et 3.* C. R. Acad. Sci. Paris Sér. I Math. **326:9** (1998), 1047–1052.

[7] H. K. Kim, *Evaluation of zeta functions at* $s = -1$ *of the simplest quartic fields.* Proceedings of the 2003 Nagoya Conference "Yokoi-Chowla Conjecture and Related Problems", Saga Univ., Saga, 2004, 63–73.

[8] A. J. Lazarus, *Class numbers of simplest quartic fields.* Number theory (Banff, AB, 1988), de Gruyter, Berlin, 1990, 313–323.

[9] A. J. Lazarus, *On the class number and unit index of simplest quartic fields.* Nagoya Math. J. **121** (1991), 1–13.

[10] S. Louboutin, *The simplest quartic fields with ideal class groups of exponents less than or equal to 2.* J. Math. Soc. Japan **56:3** (2004), 717–727.

[11] P. Olajos, *Power integral bases in the family of simplest quartic fields.* Experiment. Math. **14:2** (2005), 129–132.

[12] O. Rizzo, *Average root numbers for a nonconstant family of elliptic curves.* Compositio Math. **136:1** (2003), 1–23.

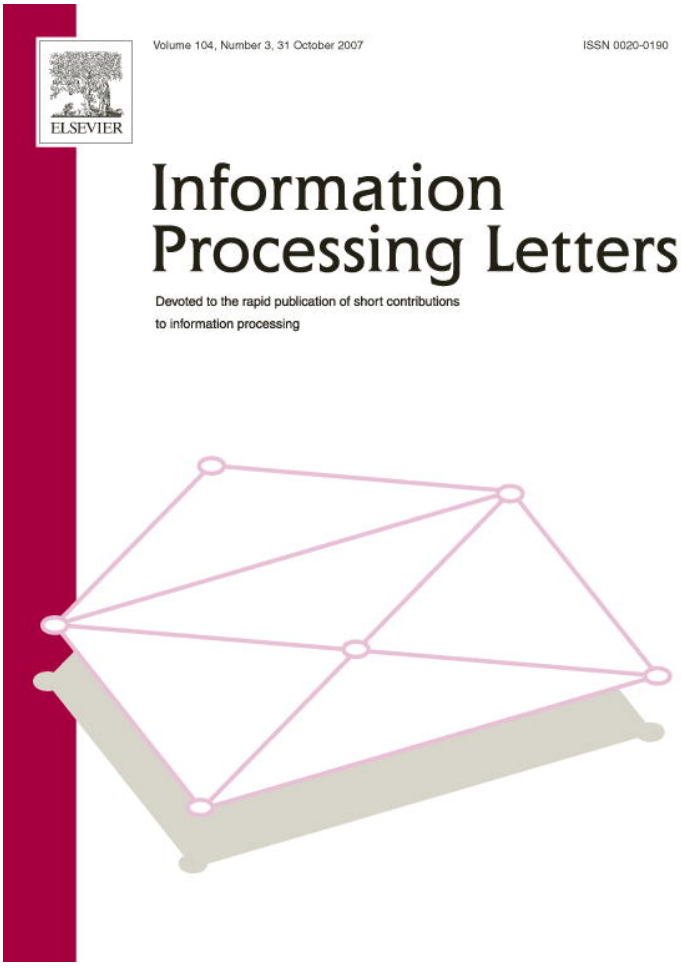
[13] S. Siksek, *Infinite descent on elliptic curves.* Rocky Mountain J. Math. **25:4** (1995), 1501–1538.

[14] J. H. Silverman, *The arithmetic of elliptic curves.* Graduate Texts in Mathematics **106**, Springer-Verlag, 1986.

[15] J. H. Silverman, *Computing heights on elliptic curves.* Math. Comp. **51** (1988), 339–358.

[16] J. H. Silverman, *The difference between the Weil height and the canonical height on elliptic curves.* Math. Comp. **55** (1990), 723–743.

Sylvain Duquesne
Université Montpellier II
Laboratoire I3M (UMR 5149) et LIRMM (UMR 5506)
CC 051, Place Eugène Bataillon
34005 Montpellier Cedex, France
E-mail : `duquesne@math.univ-montp2.fr`



Available online at www.sciencedirect.com
ScienceDirect
Information Processing Letters 104 (2007) 101–105
Information Processing Letters
www.elsevier.com/locate/ipl

Improving the arithmetic of elliptic curves in the Jacobi model

Sylvain Duquesne

I3M (UMR CNRS 5149) and LIRMM (UMR CNRS 5506), Université Montpellier II, CC 051, Place Eugène Bataillon, 34095 Montpellier Cedex 5, France

Received 25 April 2007; accepted 17 May 2007

Available online 5 June 2007

Communicated by D. Pointcheval

Abstract

The use of elliptic curve cryptosystems on embedded systems has been becoming widespread for some years. Therefore the resistance of such cryptosystems to side-channel attacks is becoming crucial. Several techniques have recently been developed. One of these consists in finding a representation of the elliptic curve such that formulae for doubling and addition are the same. Until now, one of the best results has been obtained by using the Jacobi model. In this Letter, we improve the arithmetic of elliptic curves in the Jacobi model and we relax some conditions required to work efficiently on this model. We thus obtained the fastest unified addition formulae for elliptic curve cryptography (assuming that the curve has a 2-torsion point).

Keywords: Cryptography; Elliptic curves; Side-channel attacks; Unified addition formulae

1. Introduction

Because of their short key length and their long-term strength, elliptic curve cryptosystems have become very popular. They have recently been recommended by NSA. This small key size is especially attractive for devices with limited capacities, like smart cards. However, such devices are sensitive to side-channel attacks. In the following, we focus on simple attacks since it is always possible to introduce countermeasures against differential attacks [6]. Such simple attacks are based on the difference of complexity between doubling and addition operations on an elliptic curve. They can be achieved by analysing information like timing [8], power consumption [9], electromagnetic radiation [11] or any other side-channel information.

Several methods have been developed to obtain an arithmetic which is resistant to side-channel attacks, and most of them can be found in [5]. Some of these methods consist in rewriting the addition formulae so that it can be used for doubling a point. In this way, the doubling of a point and the addition of two distinct points become indistinguishable and simple side-channel attacks are staved off. The most efficient unified formulae have been obtained with the Hessian model (12 field multiplications) for curves having a 3-torsion point [7]. Until now, the most efficient unified addition formulae for elliptic curves with a 2-torsion point have been obtained by using the Jacobi form [2]. Based on curve representation, the authors present formulae requiring 14 field multiplications if some additional conditions are satisfied, and 16 unconditionally.

In this Letter, we will improve these formulae. The result of this enhancement is that the unified addition

E-mail address: duquesne@math.univ-montp2.fr.

0020-0190/$ – see front matter
doi:10.1016/j.ipl.2007.05.012

requires only 12 field multiplications under conditions and 14 unconditionally. Moreover, we relax the conditions evoked above. Thus, we obtain the most efficient unified addition for an elliptic curve containing a 2-torsion point (which means that the order of the curve is even).

The paper is organized as follows. In Section 2 we review the Jacobi form of an elliptic curve and the unconditional unified addition formulae obtained in [2]. In Section 3, we give our improved unconditional formulae and discuss the differences with the previous ones. Then, in Section 4, we explain how these formulae can again be improved under some conditions and how we are relaxing the conditions given in [2]. Finally, we conclude in Section 5.

2. Elliptic curves in Jacobi form

In this Letter, the base field is a finite prime field $\mathbb{F}_p$ where p is a large prime number. In fact, it is easy to generalize the results to any finite field of characteristic greater than or equal to 5, but this is of no interest for cryptography in real life.

Let E be an elliptic curve defined over such a field. It is well known that E can be represented by the set of points (x, y) in $\mathbb{F}_p^2$ satisfying an equation of the form

$$E : y^2 = x^3 + a_4 x + a_6,$$

together with a point at infinity (denoted $\mathcal{O}$ in the following) [12]. Constants a_4 and a_6 are elements of $\mathbb{F}_p$ such that $4a_4^3 + 27a_6^2 \neq 0$. Following [4], Liardet and Smart explain in [10] how the embedding of an elliptic curve as the intersection of two quadrics in $\mathbb{P}^3$ can be used to produce unified addition formulae. In [2], Billet and Joye generalize and improve this idea by considering the (extended) Jacobi quartics given by equations of the form

$$Y^2 = \varepsilon X^4 - 2\delta X^2 Z^2 + Z^4. \tag{1}$$

With this equation, a point is represented by a triplet (X, Y, Z) satisfying Eq. (1). Let us note that two triplets (X_1, Y_1, Z_1) and (X_2, Y_2, Z_2) represent the same point if and only if there is an element k in $\mathbb{F}_p^*$ such that $X_1 = kX_2$, $Y_1 = k^2 Y_2$ and $Z_1 = kZ_2$.

It is proved in [2] that any elliptic curve defined over $\mathbb{F}_p$ having a 2-torsion point is birationally equivalent to such a quartic.

Let $(\theta, 0)$ be such a 2-torsion point (i.e., θ is a root of the polynomial $x^3 + a_4 x + a_6$), then constants ε and δ are defined by

$$\varepsilon = -\frac{3\theta^2 + 4a_4}{16}, \qquad \delta = \frac{3}{4}\theta,$$

and the birational transformations are given by

$$\psi : \begin{cases} (\theta, 0) \to (0, -1, 1), \\ \mathcal{O} \to (0, 1, 1), \\ (x, y) \to \big(2(x-\theta), (2x+\theta)(x-\theta)^2 - y^2, y\big), \end{cases}$$

and

$$\psi^{-1} : \begin{cases} (0, 1, 0) \to \mathcal{O}, \\ (0, -1, 0) \to (\theta, 0), \\ (X, Y, Z) \to \big(\frac{2(Y+Z^2)}{X^2} - \frac{\theta}{2}, Z\frac{4(Y+Z^2)-3\theta^2}{X^3}\big). \end{cases}$$

Of course, this means that all the curves cannot be transformed into an extended Jacobi quartic. In particular, the cardinality of a curve transformable into such a form is even. However, this is more general than the intersection of two quadrics [10] or the Montgomery form [5] whose cardinality is a multiple of 4. Let us now give the formulae for the addition

$$(X_1, Y_1, Z_1) + (X_2, Y_2, Z_2) = (X_3, Y_3, Z_3).$$

We have

$$\begin{cases} X_3 = X_1 Z_1 Y_2 + Y_1 X_2 Z_2, \\ Y_3 = \big(Z_1^2 Z_2^2 + \varepsilon X_1^2 X_2^2 ht\big)(Y_1 Y_2 - 2\delta X_1 X_2 Z_1 Z_2) \\ \qquad + 2\varepsilon X_1 X_2 Z_1 Z_2 \big(X_1^2 Z_2^2 + Z_1^2 X_2^2\big), \\ Z_3 = Z_1^2 Z_2^2 - \varepsilon X_1^2 X_2^2. \end{cases} \tag{2}$$

The main interest of these formulae is that they remain valid if $(X_1, Y_1, Z_1) = (X_2, Y_2, Z_2)$. They are also valid if one of the points is the neutral element. According to [2], these formulae require 13 *multiplications* and 3 *multiplications by constants*, which has provided the best unified formulae until now for curves of even order. They also require 14 *modular reductions* and 8 *temporary variables*. Note that we give both the number of multiplications (which is standard) and the number of modular reductions because the latter is the most important operation in RNS representation, which can be used for performing a safe arithmetic on elliptic curves, as explained in [1]. This complexity can be reduced by eliminating 2 multiplications by constants if ε is small, which is possible under some conditions. Before explaining these conditions and relaxing them in comparison with [2], let us explain how to reduce the number of multiplications and modular reductions.

3. Improved addition formulae

Let φ be the map

$$\varphi : \mathbb{F}_p^3 \to \mathbb{F}_p^4,$$
$$(X, Y, Z) \mapsto \big(X^2, XZ, Z^2, Y\big)$$

Let (X, Y, Z) be a point on the extended Jacobi quartic. To reduce the number of field multiplications, we will use $\varphi(X, Y, Z)$ instead of (X, Y, Z). Of course this increases the memory required compared to [2]. This is a drawback for small devices, but we will see that in practice only 9 temporary variables are necessary instead of 8 in [2], so the memory extra cost is not very high (we do not count the registers for storing ε and δ in the memory requirements).

We thus use the formulae (2) and give, in Table 1, the operations necessary to add two points (X_1, Y_1, Z_1) and (X_2, Y_2, Z_2) represented by $\varphi(X_1, Y_1, Z_1) = (U_1, V_1, W_1, Y_1)$ and $\varphi(X_2, Y_2, Z_2) = (U_2, V_2, W_2, Y_2)$. If the sum of these points is (X_3, Y_3, Z_3), the operations described can either return (X_3, Y_3, Z_3) or return $\varphi(X_3, Y_3, Z_3) = (U_3, V_3, W_3, Y_3)$.

Assuming that the input and output are represented using φ, executing operations of Table 1 requires only 11 *multiplications* and 3 *multiplications by constants*. They also require 12 *modular reductions* and 9 *temporary variables*. Compared to [2], this is a gain of 14% and even 17% if ε is assumed to be small (as discussed in the next section). Thus, this provides the best unified addition for an elliptic curve with a 2-torsion point. Let us now describe in detail how this new system of coordinates can be used to perform a scalar multiplication which is resistant to side-channel attacks.

Let E be an elliptic curve defined over $\mathbb{F}_p$ containing a 2-torsion point and let P be a point in $E(\mathbb{F}_p)$ and n an integer. The computation of nP is crucial in elliptic curve cryptography since this operation is used in almost all cryptosystems and is the most time-consuming operation. We can proceed as follows:

(1) Compute constants θ, ε and δ to obtain the equation of the (extended) Jacobi quartic (of the form (1)).
(2) Send the point P to the (extended) Jacobi quartic model using the rational transformation ψ.
(3) Compute the new coordinates (U, V, W, Y) of $\psi(P)$ using the map φ.
(4) Use the full Table 1 and your favorite exponentiation algorithm to compute $n(U, V, W, Y)$.
(5) Remember to use only the first part of Table 1 for the last operation of the exponentiation, so that the result of the exponentiation is a point on the (extended) Jacobi quartic with standard coordinates (X, Y, Z).
(6) Send this point back to the original elliptic curve via the reverse rational transformation ψ^{-1}.

Of course, steps (1), (2) and (6) are not necessary if the curve is originally given in (extended) Jacobi quartic form. Moreover, note that, since addition and doubling are indistinguishable, any of the many exponentiation algorithms (double-and-add, w-NAF, addition chains, fixed base point methods) can be used without jeopardizing the security against simple side-channel attacks.

Table 1
Unified addition on a Jacobi quartic using φ

Operation	Value of the variable
$T_1 \leftarrow U_1$	X_1^2
$T_2 \leftarrow U_2$	X_2^2
$T_3 \leftarrow V_1$	$X_1 Z_1$
$T_4 \leftarrow V_2$	$X_2 Z_2$
$T_5 \leftarrow W_1$	Z_1^2
$T_6 \leftarrow W_2$	Z_2^2
$T_7 \leftarrow Y_1$	Y_1
$T_8 \leftarrow Y_2$	Y_2
$T_9 \leftarrow T_7 T_8$	$Y_1 Y_2$
$T_7 \leftarrow T_7 + T_3$	$X_1 Z_1 + Y_1$
$T_8 \leftarrow T_8 + T_4$	$X_2 Z_2 + Y_2$
$T_3 \leftarrow T_3 T_4$	$X_1 X_2 Z_1 Z_2$
$T_7 \leftarrow T_7 T_8$	$(X_1 Z_1 + Y_1)(X_2 Z_2 + Y_2)$
$T_7 \leftarrow T_7 - T_9$	$X_1 Z_1 Y_2 + X_2 Z_2 Y_1 + X_1 Z_1 X_2 Z_2$
$T_7 \leftarrow T_7 - T_3$	$\mathbf{X}_3$
$T_4 \leftarrow T_1 T_2$	$X_1^2 X_2^2$
$T_8 \leftarrow T_5 T_6$	$Z_1^2 Z_2^2$
$T_1 \leftarrow T_1 + T_5$	$X_1^2 + Z_1^2$
$T_2 \leftarrow T_2 + T_6$	$X_2^2 + Z_2^2$
$T_5 \leftarrow T_1 T_2$	$(X_1^2 + Z_1^2)(X_2^2 + Z_2^2)$
$T_5 \leftarrow T_5 - T_4$	$X_1^2 Z_2^2 + X_2^2 Z_1^2 + Z_1^2 Z_2^2$
$T_5 \leftarrow T_5 - T_8$	$X_1^2 Z_2^2 + X_2^2 Z_1^2$
$T_4 \leftarrow \varepsilon T_4$	$\varepsilon X_1^2 X_2^2$
$T_1 \leftarrow T_8 - T_4$	$\mathbf{Z}_3$
$T_2 \leftarrow T_8 + T_4$	$Z_1^2 Z_2^2 + \varepsilon X_1^2 X_2^2$
$T_6 \leftarrow 2\delta T_3$	$2\delta X_1 X_2 Z_1 Z_2$
$T_6 \leftarrow T_9 - T_6$	$Y_1 Y_2 - 2\delta X_1 X_2 Z_1 Z_2$
$T_6 \leftarrow T_6 T_2$	$(Z_1^2 Z_2^2 + \varepsilon X_1^2 X_2^2)(Y_1 Y_2 - 2\delta X_1 X_2 Z_1 Z_2)$
$T_3 \leftarrow 2\varepsilon T_3$	$2\varepsilon X_1 X_2 Z_1 Z_2$
$T_3 \leftarrow T_5 T_3$	$2\varepsilon X_1 X_2 Z_1 Z_2 (X_1^2 Z_2^2 + X_2^2 Z_1^2)$
$T_8 \leftarrow T_6 + T_3$	$\mathbf{Y}_3$
$T_2 \leftarrow T_7^2$	$\mathbf{U}_3$ $(= X_3^2)$
$T_4 \leftarrow T_1 T_7$	$\mathbf{V}_3$ $(= X_3 Z_3)$
$T_6 \leftarrow T_1^2$	$\mathbf{W}_3$ $(= Z_3^2)$

4. The case of small coefficients

In formulae (2), there are two multiplications by ε, so it is very interesting to assume that ε is small. In [2], the authors explained that this is possible for most elliptic curves with *three* points of order 2. More precisely they

prove that ε can always be rescaled to 1 if $p \equiv 3 \bmod 4$ and with a probability 7/8 if $p \equiv 1 \bmod 4$. In this part, we explain how to relax the condition on the number of 2-torsion points. Indeed, it is not necessary to make additional assumptions to obtain this result and it is even possible to conclude in more cases.

Thus, we only assume in the following that the elliptic curve E has **one** 2-torsion point (which is a necessary condition to transform the curve into a Jacobi quartic). Let $(\theta, 0)$ be this 2-torsion point on E, and recall that

$$\varepsilon = -\frac{3\theta^2 + 4a_4}{16}.$$

Let $\alpha \in \mathbb{F}_p^*$. We will consider the change of variables

$$x = \frac{X}{\alpha^2}, \qquad y = \frac{Y}{\alpha^3}$$

which makes the elliptic curve E isomorphic to the elliptic curve

$$E' : Y^2 = X^3 + a_4' X + a_6',$$

with $a_4' = a_4\alpha^4$ and $a_6' = b\alpha^6$. This curve has, of course, a 2-torsion point $(\theta', 0)$ with $\theta' = \theta\alpha^2$, so if one wants to transforms E' into a Jacobi quartic, the new value of ε is

$$\varepsilon' = \varepsilon\alpha^4.$$

We therefore have to find an α such that $\varepsilon\alpha^4$ is a small number. For this, let μ denote the smallest integer (greater than or equal to -1) which is not a square modulo p. Using the multiplicativity of the Legendre symbol, one can prove that four cases can occur (with the same probability):

(i) ε is a fourth power in $\mathbb{F}_p$ and we can choose α such that $\varepsilon' = 1$.
(ii) ε is not a square in $\mathbb{F}_p$ and $\sqrt{\varepsilon/\mu}$ is a square. In this case, ε/μ is a fourth power and we can choose α such that $\varepsilon' = \mu$.
(iii) ε is a square in $\mathbb{F}_p$ but not $\sqrt{\varepsilon}$. In this case, ε/μ^2 is a fourth power and we can choose α such that $\varepsilon' = \mu^2$.
(iv) Neither ε nor $\sqrt{\varepsilon/\mu}$ are squares in $\mathbb{F}_p$. In this case, ε/μ^3 is a fourth power and we can choose α such that $\varepsilon' = \mu^3$.

The simplest case to treat is $p \equiv 3 \bmod 4$. Indeed, we can choose $\mu = -1$ so that we can always rescale ε to 1 or -1. Note that this is the most current case in cryptographic applications (pseudo-Mersenne primes or generalized Mersenne primes). If $p \equiv 1 \bmod 4$, we have to check that μ is sufficiently small. It is easy to prove (again using the properties of the Legendre symbol) that the proportion of prime fields such that the n first prime numbers are squares is only $1/2^n$. Thus, in most cases it is possible to rescale ε to a small number.

Anyway, if μ is too large to assume that the multiplication by ε' can be neglected (for instance, if we are in cases (iii) or (iv)), there is another way to rescale ε to a small value. This method is explained in [3]. The principle is to find an isogeny of small degree between the elliptic curve E and a new elliptic curve, say E'', having the same cardinality. One can then hope that the method explained above (i.e. via isomorphisms) will give a better result on E'' than on E (for instance, if we are in cases (i) or (ii)).

Basically, this is the same idea as the previous isomorphism between E and E' (an isomorphism is an isogeny of degree 1), but the composition of the isogeny and its dual is not the identity on E, so the scalar multiplication must be modified to give a good result. This operation is of negligible cost compared to full scalar multiplication, as explained in detail in [3].

5. Conclusion

In this Letter, we provide better unified addition formulae for elliptic curves having a 2-torsion point by introducing a new system of coordinates on the (extended) Jacobi quartic model. Moreover, we prove that, in most cases, it is not necessary to assume that the elliptic curve has three 2-torsion points to further improve the performance. In particular, we prove that, if $p \equiv 3 \bmod 4$, ε can be rescaled to 1 or -1 without any additional assumption on the curve.

Finally, we obtain unified addition formulae (on elliptic curves with a 2-torsion point) requiring only 12 multiplications on the base field in most cases, which represents a gain of 17% compared to the best known formulae until now [2]. This formulae will allow more efficient scalar multiplication, which is resistant to side-channel attacks, on elliptic curves whose order is even.

References

[1] J.C. Bajard, S. Duquesne, M. Ercegovac, N. Meloni, Residue systems efficiency for modular products summation: application to elliptic curves cryptography, Proc. SPIE 6313 (2006) 631304.
[2] O. Billet, M. Joye, The Jacobi model of an elliptic curve and side-channel analysis, in: Applied Algebra, Algorithms and Error-Correcting Codes, Lecture Notes in Comput. Sci., vol. 2643, Springer, Berlin, 2003, pp. 34–42.
[3] E. Brier, M. Joye, Fast point multiplication on elliptic curves trough isogenies, in: Applied Algebra, Algorithms and Error-

Correcting Codes, in: Lecture Notes in Comput. Sci., vol. 2643, Springer, Berlin, 2003, pp. 43–50.

[4] D.V. Chudnovsky, G.V. Chudnovsky, Sequences of numbers generated by addition in formal groups and new primality and factorization tests, Adv. in Appl. Math. 7 (1986) 385–434.

[5] H. Cohen, G. Frey, Handbook of Elliptic and Hyperelliptic Curve Cryptography, Discrete Math. Appl., Chapman & Hall/CRC, 2006.

[6] J.S. Coron, Resistance against differential power analysis for elliptic curve cryptosystems, in: CHES'99, in: Lecture Notes in Comput. Sci., vol. 1717, Springer, Berlin, 1999, pp. 292–302.

[7] M. Joye, J.J. Quisquater, Hessian elliptic curves and side-channel attacks, in: CHES 2001, in: Lecture Notes in Comput. Sci., vol. 2162, Springer, Berlin, 2001, pp. 402–410.

[8] P.C. Kocher, Timing attacks on implementations of DH, RSA, DSS and other systems, in: CRYPTO'96, in: Lecture Notes in Comput. Sci., vol. 1109, Springer, Berlin, 1996, pp. 104–113.

[9] P.C. Kocher, J. Jaffe, B. Jun, in: Differential power analysis, CRYPTO'99, in: Lecture Notes in Comput. Sci., vol. 1666, Springer, Berlin, 1999, pp. 388–397.

[10] P.Y. Liardet, N. Smart, in: Preventing SPA/DPA in ECC Systems Using the Jacobi Form, CHES 2001, in: Lecture Notes in Comput. Sci., vol. 2162, Springer, Berlin, 2001, pp. 391–401.

[11] J.J. Quisquater, D. Samyde, in: ElectroMagnetic Analysis (EMA): Measures and Countermeasures for Smart Cards, e-smart 2001, in: Lecture Notes in Comput. Sci., vol. 2140, Springer, Berlin, 2001, pp. 200–210.

[12] J.H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, vol. 106, Springer, Berlin, 1986.

Combining leak–resistant arithmetic for elliptic curves defined over $\mathbb{F}_p$ and RNS representation

JC Bajard[a], S. Duquesne[b], M Ercegovac[c]
[a] ARITH-LIRMM, CNRS Université Montpellier2, France;
[b] I3M, CNRS Université Montpellier2, France;
[c] UCLA, Computer Science Dep., Los Angeles, US

September 24, 2007

Contents

Abstract

In this paper we combine the RNS representation and the leak-resistant arithmetic on elliptic curves. These two techniques are relevant for implementation of elliptic curve cryptography on embedded devices since they have leak-resistance properties. We improve the reduction step of the RNS modular product and we optimize formulae for the basic operations

arising in leak-resistant arithmetic on elliptic curves (unified addition, Montgomery ladder) in order to minimize the number of modular reduction. Finally, we obtain a competitive and secure implementation. We also explain the advantages of the RNS representation, especially in hardware and for embedded devices, and show that, contrary to other approaches, ours takes optimal advantage of a dedicated parallel architecture.

Keywords: Elliptic curves, Montgomery, Leak-resistance, RNS, Modular multiplication.

1 Introduction

Elliptic curve cryptosystems, because of their small key length, has become popular to such a point that they have recently been recommended by the NSA. Their small key size is especially attractive for small cryptographic devices like smart cards. However, such devices are sensitive to side channel attacks. These attacks consist in analyzing side channel informations like timings [22], power consumptions [23] or electromagnetic radiations [30] of a device. They have become such a threat that protecting ECC against them has become itself a whole research area giving rise to various countermeasures [14].

The weakness comes from the difference of complexity between the addition and the doubling on elliptic curves. There are two ways to resolve this. The first one is to use representations of the curve for which the two operations are obtained with the same formulae as in [24], [20] or [8]. The second one is to use an algorithm for the scalar multiplication due to Montgomery [26] for a family of curves defined over $\mathbb{F}_p$ and generalized in [16], [8] and [19]. This algorithm has many advantages for constrained environments: it is leak-resistant, very simple to implement, careful in memory and does not required precomputations. On the other hand the RNS representation of numbers in $\mathbb{F}_p$ has interesting leak-resistance properties for the arithmetic on the base field, it is easily parallelizable in hardware [4] and it is scalable.

The aim of this paper is to combine these two techniques, especially in the case of curves in Weierstrass form, to obtain an implementation of ECC which is leak-resistant, both at the level of the curve and at the level of the field, and which can be easily and efficiently parallelized in hardware.
In the following, $\mathbf{K}$ denotes a field of characteristic $\neq 2, 3$ (which is a prime field $\mathbb{F}_p$ in practice) and $|n|_2$ denotes the bit-length of n.

2 Background properties of the different representations and algorithms

2.1 Modular multiplication

Elliptic curve arithmetic over $\mathbb{F}_p$ mainly involves modular multiplications modulo p. Such a modular multiplication can be decomposed into one classic multiplication followed by a modular reduction. Because of the small size of the numbers used with ECC (192 to 512 bits, i.e., 6 to 16 32-bit words), the multiplication is performed by the so called schoolbook method. Let us consider A and B two n-word integers given in radix representation (i.e., $X = \sum_{i=0}^{n} x_i \beta^i$ with $0 \leq a_i < \beta$), then $A \times B$ can be computed by a succession of word multiplications and additions (which will be considered in the following as basic word operations). We can summarize it by the equation

$$A \times B = b_0 A + \beta(b_1 A + \beta(b_2 A \cdots + \beta b_n A) \dots).$$

We get a complexity of n^2 word operations.

The reduction of an integer k modulo another integer p consists in finding the remainder of the euclidean division of k by p. This operation is costly. It can be substantially speeded up by using the Montgomery reduction (we will recall now this method as it is in RNS) or by using special modulo.

Montgomery general reduction algorithm:

In [25] Montgomery proposed to substitute the reduction modulo p by a division by a power of the radix β (a simple shift). The result is not exactly $k \mod p$ but $k\beta^{-n} \mod p$. Using Montgomery representation allows overcoming of this problem.

Algorithm 1: Montgomery$_p(R)$

Data: $R = A \times B < \beta^{2n}$ and $\beta^{n-1} \leq p < \beta^n$
and a precomputed value $(-p^{-1} \bmod \beta^n)$;
Result: (q, r) such that $r = R\beta^{-n} \pmod p < 2p$;
$q \leftarrow -R \times p^{-1} \bmod \beta^n$;
$r \leftarrow (R + qp)/\beta^n$;

The complexity of this reduction is $n^2 + n$ word operations [7]. As all the computations can be done in Montgomery representation, we ignore the cost of the conversion from Montgomery to classic representation.

Reduction using special modulo:

When using ECC, one can choose the underlying field without restriction. In this case, the cost of a modular reduction can be reduced to some additions. Compared to the cost of a general reduction, it can be considered as almost free. As an example, if the field $\mathbb{F}_p$ is such that p is a Mersenne number (ie

$p = 2^k - 1$), then the reduction of a $2n$-word integer R modulo p requires only $2n$ word additions. Just write $R = R_1 2^k + R_0$, then $R \pmod p = R_1 + R_2$, if $R_1 + R_2 \geq p$ then $R \pmod p = R_1 + R_2 - p$. Prime Mersenne numbers are rare. This is why the generalized Mersenne number class has been introduced [33, 11] (integer of the form $P(2^k)$ where $P(X) = X^n - C(X)$ and C is a polynomial with coefficients equal to $-1, 0$ or 1 and $\deg(C) \leq \frac{n}{2}$) . Modular reduction is still a question of additions, so it is almost free. However, one can not find generalized Mersenne numbers for all the number length. Moreover, the main drawback is that a dedicated architecture to a particular p cannot be used for other values. Consequently, it is not realistic in either a context of software or hardware implementation.

2.2 Leak-resistant arithmetic in elliptic curve cryptography

In all elliptic curves based schemes (such as encryption/decryption or signature generation/verification) the dominant operation is the scalar multiplication of points on the curve. Hence, the efficiency of this operation is central in elliptic curve cryptography. This is usually done by using standards scalar multiplication methods such as double and add or sliding window methods combined with recoding of the exponent.

However, these methods are not leak-resistant because of the difference of complexity between the addition and the doubling operations. There exists some methods to protect these algorithms, for example, if one wants to protect a double and add algorithm against side-channel attacks, one can perform extra (useless) additions [14]. By this way, for each bit of the exponent we perform both an addition and a doubling so that bits of the exponent are indistinguishable. Unfortunately this protection is not only expensive but vulnerable to fault attacks too.

Currently there are essentially two means to perform leak-resistant arithmetic on elliptic curves. The first one is the use of unified addition formulae. This means that we use a representation of the curve for which the addition and the doubling can be performed using the same formulae. In the following, we will present unified formulae for three representations of the curve, namely, the Hessian form, the Jacobi form (leading to the most efficient formulae but not applicable to all elliptic curves) and the short Weierstrass form (which is the general case). The second one is to use the Montgomery ladder where both an addition and a doubling are necessary to perform at each step of the scalar multiplication algorithm. Again, in this case, the arithmetic is more efficient on restrictive models of the curve and we will present both the restrictive and the general model.

Unified addition formulae

The use of the Hessian form for a leak-resistant arithmetic has been introduce in [20]. An elliptic curve over $\mathbb{F}_p$ is said to be in Hessian form if it is given by

an equation of the form

$$X^3 + Y^3 + Z^3 = 3dXYZ$$

where $d \in \mathbb{F}_p$ and is not a third root of unity. Such curves have a point of 3-torsion (which means that there cardinality is divisible by 3) so that all elliptic curve cannot be given in this form. In [20], Joye and Quisquater described the formulae for the addtion of two points (X_1, Y_1, Z_1) and (X_2, Y_2, Z_2) for the elliptic curve in such a representation.

$$\left\{ \begin{array}{rcl} X_3 & = & Y_1^2 X_2 Z_2 - Y_2^2 X_1 Z_1, \\ Y_3 & = & X_1^2 Y_2 Z_2 - X_2^2 Y_1 Z_1, \\ Z_3 & = & Z_1^2 X_2 Y_2 - Z_2^2 X_1 Y_1. \end{array} \right.$$

These formulae require 12 field multiplications and can be used for the addition and the doubling since we have

$$2(X, Y, Z) = (Z, X, Y) + (Y, Z, X).$$

At the same time, the use of the Jacobi model was introduced by Liardet and Smart in [24]. It is improved in [6] and, more recently, in [15]. It is easy to prove that any elliptic curve containing a 2-torsion point is birationally equivalent to the Jacobi quartic given by an equation of the form

$$Y^2 = \varepsilon X^4 - 2\delta X^2 Z^2 + Z^4,$$

where ε and δ are constants in $\mathbb{F}_p$. In this case, the formulae for the addition of two points (X_1, Y_1, Z_1) and (X_2, Y_2, Z_2) are also valid if the two points are the same.

$$\left\{ \begin{array}{rcl} X_3 & = & X_1 Z_1 Y_2 + Y_1 X_2 Z_2, \\ Y_3 & = & \left(Z_1^2 Z_2^2 + \varepsilon X_1^2 X_2^2\right)(Y_1 Y_2 - 2\delta X_1 X_2 Z_1 Z_2) \\ & & +2\varepsilon X_1 X_2 Z_1 Z_2 \left(X_1^2 Z_2^2 + Z_1^2 X_2^2\right), \\ Z_3 & = & Z_1^2 Z_2^2 - \varepsilon X_1^2 X_2^2. \end{array} \right.$$

In most cases, ε can be rescaled to a small value so that it is not too restrictive to neglect multiplication by ε. Thus these formuale are also requiring 12 multiplication as explained in [15]. However this method cannot be applied to any elliptic curve since the cardinality of a Jacobi quartic is even.

In [8] Brier and Joye are giving unified formulae for a curve given in short Weierstrass form (which is not restrictive over $\mathbb{F}_p$ where p is a large prime number)

$$Y^2 Z = X^3 + aXZ^2 + bZ^3.$$

Again, the formulae given for the addition of two points (X_1, Y_1, Z_1) and (X_2, Y_2, Z_2) are also valid if the two points are the same.

$$\left\{ \begin{array}{rcl} X_3 & = & 2\lambda_d \left(\lambda_n^2 - (X_1 Z_2 + X_2 Z_1)(Y_1 Z_2 + Y_2 Z_1)\lambda_d\right), \\ Y_3 & = & \lambda_n \left(3(X_1 Z_2 + X_2 Z_1)(Y_1 Z_2 + Y_2 Z_1)\lambda_d - 2\lambda_n^2\right) - \left((Y_1 Z_2 + Y_2 Z_1)\lambda_d\right)^2, \\ Z_3 & = & 2\lambda_d^3, \end{array} \right.$$

where

$$\begin{aligned}\lambda_n &= (X_1Z_2 + X_2Z_1)^2 - X_1X_2Z_1Z_2 + aZ_1^2Z_2^2,\\ \lambda_d &= (Y_1Z_2 + Y_2Z_1)Z_1Z_2.\end{aligned}$$

These formulae are valid for all elliptic curve but are less efficient since they are requiring 18 field multiplications. Note that, by using an isomorphism or an isogeny, it is possible, in most cases, to rescale a to a small value. We will explain this in details in Section 4.3 within the context of Montgomery arithmetic.

The Montgomery scalar multiplication

Montgomery proposed in [26] to work only with the x-coordinate. Of course, the group law is lost but traces remain. So doubling is still possible and the addition of two points P and Q is possible if $P-Q$ is known. Montgomery gives the formulae for those operations when the curve is in Montgomery form, that is defined by an equation of the type

$$By^2 = x^3 + Ax^2 + x.$$

Proposition 1 *Let E be an elliptic curve defined over $\mathbb{F}_p$ in Montgomery form. Let also $P = (X_p, Y_p, Z_p)$ and $Q = (X_q, Y_q, Z_q) \in E(\mathbf{K})$ given in projective coordinates. Assume that $P - Q = (x, y)$ is known in affine coordinates. Then the X and Z-coordinates for $P + Q$ and $2P$ are given by*

$$\begin{aligned}X_{p+q} &= ((X_p - Z_p)(X_q + Z_q) + (X_p + Z_p)(X_q - Z_q))^2,\\ Z_{p+q} &= x\left((X_p - Z_p)(X_q + Z_q) - (X_p + Z_p)(X_q - Z_q)\right)^2,\\ 4X_pZ_p &= \left((X_p + Z_p)^2 - (X_p - Z_p)^2\right),\\ X_{2p} &= (X_p + Z_p)^2(X_p - Z_p)^2,\\ Z_{2p} &= 4X_pZ_p\left((X_p - Z_p)^2 + \tfrac{A+2}{4}4X_pZ_p\right).\end{aligned}$$

By this way, both an addition and a doubling takes only 3 multiplications and 2 squares which is much faster than usual operations ([13]). The fact that the difference $P-Q$ must be known to compute $P+Q$ implies that a new algorithm must be used to compute the scalar multiplication of a point G by an integer k. The solution is to use pairs of consecutive multiples of P, so that the difference between the two components of the pair is always known and equal to G. The algorithm for scalar multiplication is as follows:

Algorithm 2: Montgomery_Scalar()

Data: $G \in E(\mathbb{F}_p)$ and $k \in \mathbb{Z}$
Result: x and z-coordinate of kG

1 Initialize $Q = (P, Q) = (\mathcal{O}, G)$ where $\mathcal{O}$ is the point at infinity;
2 If the bit of k is 0, $Q = (2P, P + Q)$;
3 If the bit of k is 1, $Q = (P + Q, 2Q)$;
4 After doing that for each bit of k, return P;

Both an addition and a doubling are done for each bit of the exponent. So the cost of this algorithm is about $10|k|_2$ multiplications for a curve in Montgomery form which is better than other available algorithms.
Moreover, the operations we have to perform do not depend on the bits of the exponent so that this method has interesting leak-resistance properties.
Finally, the x-coordinate of kG is usually sufficient but some cryptosystems, like ECDSA, require the y-coordinates. It can easily be recovered, as explain in [27].

Unfortunately, in odd characteristic, all the elliptic curves cannot be transformed into Montgomery form. This is, for example, the case for most of the standards. The reason is that any curve which can be transformed into Montgomery form has a 2-torsion point so that its cardinality is not prime (it is divisible by 2).

In general, namely when the curve is defined by an equation of the form

$$y^2 = x^3 + ax + b, \tag{1}$$

this method can also be applied but is more time consuming ([8],[16] and [19]).

Proposition 2 *Let E be an elliptic curve defined over $\mathbb{F}_p$ by (1). Let also $P = (X_p, Y_p, Z_p)$ and $Q = (X_q, Y_q, Z_q) \in E(\mathbb{F}_p)$ given in projective coordinates. Assume that $P - Q = (x, y)$ is known in affine coordinates. Then we obtain the X and Z-coordinates for $P + Q$ and $2P$ by the following formulae :*

$$\begin{aligned}
X_{p+q} &= -4bZ_pZ_q(X_pZ_q + X_qZ_p) + (X_pX_q - aZ_pZ_q)^2, \\
Z_{p+q} &= x(X_pZ_q - X_qZ_p)^2, \\
X_{2p} &= \left(X_p^2 - aZ_p^2\right)^2 - 8bX_pZ_p^3, \\
Z_{2p} &= 4Z_p\left(X_p^3 + aX_pZ_p^2 + bZ_p^3\right).
\end{aligned}$$

Addition can be performed in 10 multiplications and doubling in 9. Hence, the scalar multiplication can be performed in about $19|n|_2$ multiplications on $\mathbb{F}_p$ which is not interesting in terms of performance but it is interesting in terms of leak-resistance. Note that the y-coordinate can also be recovered in this case ([8]).

Proposition 3 *Suppose that $Q = P + G$ with $G = (x, y)$, $P = (x_p, y_p)$ and $Q = (x_q, y_q)$. Then, if $y \neq 0$, one has*

$$y_p = -\frac{2b + (a + xx_p)(x + x_p) - x_q(x - x_p)^2}{2y}$$

With the Montgomery scalar multiplication method, we always have to perform both an addition and a doubling for each bit of the exponent, so that this method is resistant against side-channel attacks and that is the reason why this method is always interesting even with 19 multiplications int each step.

In this paper, we will use the Residue Number Systems (RNS) for the arithmetic on the base field. The consequence is that the cost of the multiplication

becomes negligible compared to the cost of the modular reduction. Thus, it is necessary to rewrite the formulae given above in order to minimize the number of modular reductions. Let us now briefly review this system of representation.

3 Residue Number Systems

3.1 Presentation

The Residue Number Systems (RNS) are based on the well-known Chinese Remainder Theorem (CRT). It was introduced in computer science in [18] and [34]. A good presentation can be found in [21].

These systems are based on the fact that a number x can be represented by its residues $(x_1, x_2, \ldots, x_n)$ modulo a set of coprime numbers $(m_1, m_2, \ldots, m_n)$, called RNS basis. We generally assume that $0 \leq x < M = \prod_{i=1}^{n} m_i$. The elements x_i are called RNS-digits, or simply digits if there is no ambiguity. The biggest interest of a such system, is to distribute integer operations on the residues values. Large integer operations are made on the residues, in other words on small numbers independently. We consider in this part a RNS base $(m_1, ..., m_n)$ with elements such that, $m_i = \beta - c_i$ where c_i is small (with few non null digits). This property ensure that the reduction part on each m_i can be neglected [5]. We assume that $M = \prod_{i=1}^{n} m_i$ is such that $p < M$. In this system two numbers a, and b can be represented by their remainders modulo the m_i, $i = 1, \ldots, n$.

$$a = (a_1, \ldots, a_n) \quad \text{and} \quad b = (b_1, \ldots, b_n)$$

A multiplication is reduced to n digit modular digit-products. A modular digit-product is equivalent to a classical digit product following by few additions (which are due to the number of ones in the binary representation of c_i, see [5]). Thus this modular digit-operation can be done in one clock cycle on an hardware composed of n arithmetic cells. This operation is done in n independent products on words.

$$r = (a_1 \times b_1 \pmod{m_1}, \ldots, a_n \times b_n \pmod{m_n}) \tag{2}$$

It is clear that if a product is followed by an addition, the cost is just increased of one addition on each modulo, and so, can be done in the same cycle.

$$r = (a_1 \times b_1 + d_1 \pmod{m_1}, \ldots, a_n \times b_n + d_n \pmod{m_n}) \tag{3}$$

We now focus our attention on the multiplication modulo p using the algorithm presented in [1]. This algorithm for two numbers a and b given in RNS, evaluates in fact $r = abM^{-1} \mod p$. To obtain the right result we need to use it again with r and $M^2 \mod p$ as operands. To prevent this fact, we convert the values in a Montgomery representation where $a' = a \times M \mod p$ which is stable for Montgomery product and addition. Thus, this conversion is done one

time at the beginning by calling Montgomery product with a and $M^2 \mod p$ as operands, and one time at the end of the complete cryptographic computing with 1, as second operand. Hence, this transformation will be neglected in the following. Moreover, as the RNS is not redundant, this representation is well suited for cryptography without any conversion.

3.2 RNS Montgomery reduction

This algorithm is a direct transposition of the classical Montgomery method. The main difference is due to the representation system. When Montgomery is applied in a classical radix β representation, the value β^n occurs for reduction, division and Montgomery factor. In RNS this value is replaced by M. Thus an auxiliary RNS Bases is need to handle the inverse of M. Hence some operation as the initial product will be done on the two bases, which will cost $2n$ words-products ($2n+1$ if we consider the extra modulo m_{2n+1}, but as its value is of the order of n, the cost due to this modulo can be neglected).

Algorithm 3 presents the RNS Montgomery reduction (c can be considered as the result of an RNS product on the two bases), where all the operations considered are in RNS. We clarify on which basis (and auxiliary modulo) they are done.

Algorithm 3: MontgR_RNS(c, p)

Data:

- Two RNS bases $\mathcal{B} = (m_1, \ldots, m_n)$, and $\mathcal{B}' = (m_{n+1}, \ldots, m_{2n})$, such that $M = \prod_{i=1}^{n} m_i < M' = \prod_{i=1}^{n} m_{n+i}$ and $\gcd(M, M') = 1$;
- a redundant modulus m_{2n+1}, $\gcd(m_{2n+1}, m_i) = 1 \; \forall i = 1...2n$;
- a positive integer p represented in RNS in both bases such that $0 < (n+2)^2 p < M$ and $\gcd(p, M) = 1$ (p is prime);
- a positive integers c represented in RNS in both bases, with $c < Mp$.

Result:

- A positive integer $r \equiv cM^{-1} \pmod p$ represented in RNS in both bases, with $r < (n+2)p$.

begin

1 $q \leftarrow (c) \times (-p^{-1})$ in $\mathcal{B}$;
2 $[q$ in $\mathcal{B}] \longrightarrow [\hat{q}$ in $\mathcal{B}'$ and $m_{2n+1}]$ *First base extension*;
3 $r \leftarrow (c + \hat{q} \times p) \times M^{-1}$ in $\mathcal{B}'$ and m_{2n+1};
4 $[r$ in $\mathcal{B}$ and $m_{2n+1}] \longleftarrow [r$ in $\mathcal{B}']$ *Second base extension*;

end

Instructions 1 and 3 of the Algorithm 3 deal with RNS operations as presented in the previous section, which are made independently one each element

of the basis, so they are very efficient. These two instructions are linear (or constant number of words-operations on a n cells architecture) Instructions 2 and 4 represent RNS bases extensions which are quadratic (or linear on an n-cell architecture) are costly. To reduce this cost, we can use two different full RNS extensions as shown in [1]. The extension to base $\mathcal{B}'$ of q (instruction 2), obtained in its RNS form $(q_1, \ldots, q_n)$ in the base $\mathcal{B}$, is done by evaluating first:

$$\sigma_i = \left|q_i \left|M_i^{-1}\right|_{m_i}\right|_{m_i}, \tag{4}$$

and then,

$$\hat{q}_j = \Big|\sum_{i=1}^{n} \left|M_i\right|_{m_j} \sigma_i\Big|_{m_j}, \quad \forall j = n+1 \ldots 2n \quad \text{and} \quad m_{2n+1} \tag{5}$$

we have $\hat{q} = q + \alpha M$ with $\alpha < n$.

Then we compute in the base $\mathcal{B}'$ the value

$$r = (ab + \hat{q}p)M^{-1} = (ab + qp)M^{-1} + \alpha p < M'. \tag{6}$$

After instruction 3, we get r such that $r \equiv abM^{-1} \pmod{p}$. The conditions $\alpha < n$, $q < M$ and $ab < Mp$ gives $\hat{q} < (n+1)M$ and thus $r < (n+2)p < M'$.

In order to use this algorithm within a cryptographic protocol, we must be able to compute $x^2 \mod p$, where x is the output of a former evaluation verifying $x < (n+2)p$. The condition $ab < Mp$ then implies $(n+2)^2p^2 < Mp$ which rewrites:

$$(n+2)^2 p < M. \tag{7}$$

The second extension of r from $\mathcal{B}'$ to $\mathcal{B}$ is a classical Shenoy-Kumaresan scheme [31] using the extra modulus m_{2n+1} for the computing of the factor α (this is depicted in Algorithm 4), which gives a result smaller than $(n+2)p$. This transformation has no consequence on the conditions.

Reduction of the number of operations:

To reduce the number of operations some pre-computing is helpful. For that, we develop the previous algorithm 3, giving in Algorithm 4 the details of the bases extensions. Then we introduce a new combination of the operations in Algorithm 5, which is faster than the previous versions.

Algorithm 4: MontgR2_RNS(c, p)

Data:

- Two RNS bases $\mathcal{B} = (m_1, \ldots, m_n)$, and $\mathcal{B}' = (m_{n+1}, \ldots, m_{2n})$, such that $M = \prod_{i=1}^{n} m_i < M' = \prod_{i=1}^{n} m_{n+i}$ and $\gcd(M, M') = 1$;
- a redundant modulus m_{2n+1}, $\gcd(m_{2n+1}, m_i) = 1 \; \forall i = 1...2n$;
- a positive integer p represented in RNS in both bases such that $0 < (n+2)^2 p < M$ and $\gcd(p, M) = 1$ (p is prime);
- a positive integers c represented in RNS in both bases, with $c < Mp$.

Result:

- A positive integer $r \equiv cM^{-1} \pmod{p}$ represented in RNS in both bases, with $r < (n+2)p$.

begin

1 $\quad q_i \leftarrow \left| c_i \times \left| -p \right|_{m_i}^{-1} \right|_{m_i}$ in $\mathcal{B}$;

$\boxed{[q \text{ in } \mathcal{B}] \longrightarrow [\hat{q} \text{ in } \mathcal{B}' \text{ and } m_{2n+1}] \quad \textit{First base extension} \text{ (lines 2 and 3)}}$;

2 $\quad \sigma_i \leftarrow \left| q_i \left| M_i^{-1} \right|_{m_i} \right|_{m_i}$ in $\mathcal{B}$;

3 $\quad \hat{q}_j \leftarrow \left| \sum_{i=1}^{n} \left| M_i \right|_{m_j} \sigma_i \right|_{m_j}$, in $\mathcal{B}'$ and m_{2n+1};

4 $\quad r_j \leftarrow \left| (c_j + \hat{q}_j \times p_j) \times \left| M \right|_{m_j}^{-1} \right|_{m_j}$ in $\mathcal{B}'$ and m_{2n+1};

$\boxed{[r \text{ in } \mathcal{B} \text{ and } m_{2n+1}] \longleftarrow [r \text{ in } \mathcal{B}'] \quad \textit{Second base extension} \text{ (lines 5 to 8)}}$;

5 $\quad \mu_j \leftarrow \left| r_j \times \left| M'_j \right|_{m_j}^{-1} \right|_{m_j}$, in $\mathcal{B}'$;

6 $\quad \xi_i \leftarrow \left| \sum_{j=n+1}^{2n} \mu_j \times \left| M'_j \right|_{m_i} \right|_{m_i}$, in $\mathcal{B}$ and m_{2n+1} ;

7 $\quad \alpha \leftarrow \left| (\xi_{2n+1} - r_{2n+1}) \times \left| M' \right|_{m_{2n+1}}^{-1} \right|_{m_{2n+1}}$;

8 $\quad r_j \leftarrow \left| (\xi_i - \alpha \times \left| M' \right|_{m_i}) \right|_{m_i}$ in $\mathcal{B}$;

end

We remark that most of the operations are done with constant values. To minimize their number, we try to regroup these multiplications by a constant value. Instruction 1 can be merged with the first step (instruction 2) of the first extension given equation (4), then we obtain the following transformation :

$$\begin{cases} 1 - . \;\; q_i \leftarrow \left| c_i \times \left| -p \right|_{m_i}^{-1} \right|_{m_i} & \text{in } \mathcal{B} \\ 2 - . \;\; \sigma_i \leftarrow \left| q_i \left| M_i^{-1} \right|_{m_i} \right|_{m_i} & \text{in } \mathcal{B} \end{cases} \tag{8}$$

becomes the instruction 1 of Algorithm 5

$$1-.\ \ \sigma_i \leftarrow |c_i \times \tau_i|_{m_i}\ ,\ \text{with } \tau_i = \left|\left|-p\right|_{m_i}^{-1}\left|M_i\right|_{m_i}^{-1}\right|_{m_i}\ ,\ \text{in } \mathcal{B} \tag{9}$$

Then we merge the next three instructions (lines 3, 4 and 5 of Algorithm 4) , for obtaining new expressions where new constants occur.

$$\begin{cases} 3-.\ \ \hat{q}_j \leftarrow \left|\sum_{i=1}^{n} \left|M_i\right|_{m_j} \sigma_i\right|_{m_j}, & \text{in } \mathcal{B}' \text{ and } m_{2n+1} \\ 4-.\ \ r_j \leftarrow \left|(c_j + \hat{q}_j \times p_j) \times \left|M\right|_{m_j}^{-1}\right|_{m_j} & \text{in } \mathcal{B}' \text{ and } m_{2n+1} \\ 5-.\ \ \mu_j \leftarrow \left|r_j \times \left|M'_j\right|_{m_j}^{-1}\right|_{m_j} & \text{in } \mathcal{B}' \end{cases} \tag{10}$$

These three instructions can be rewritten as follow:

$$\begin{cases} r_{2n+1} \leftarrow \left|c_{2n+1} + \sum_{i=1}^{n} \sigma_i \times \left|M_i\right|_{m_{2n+1}} \times p_{2n+1}) \times \left|M\right|_{m_{2n+1}}^{-1}\right|_{m_{2n+1}} \\ \mu_j \leftarrow \left|(c_j + \sum_{i=1}^{n} \sigma_i \times \left|M_i\right|_{m_j} \times p_j) \times \left|M\right|_{m_j}^{-1} \times \left|M'_j\right|_{m_j}^{-1}\right|_{m_j} \end{cases} \quad \text{in } \mathcal{B}' \tag{11}$$

Thus we obtain the instructions 3 and 4 of Algorithm 5:

$$3-.\ \ \gamma_j \leftarrow \left|c_j + \sum_{i=1}^{n} \rho_i \sigma_i\right|_{m_j}\ ,\ \text{with } \rho_i = \left|\left|M_i\right|_{m_j} \left|p\right|_{m_j}\right|_{m_j} \quad \text{in } \mathcal{B}' \tag{12}$$

$$4-.\ \ \mu_j \leftarrow \left|\gamma_j \times \nu_j\right|_{m_j} \text{ with } \nu_j = \left|\left|M\right|_{m_j}^{-1} \times \left|M'_j\right|_{m_j}^{-1}\right|_{m_j} \quad \text{in } \mathcal{B}' \tag{13}$$

We remark that we can apply this rewriting to the complete evaluation of α from the last instructions.

$$\begin{cases} 6-.\ \ \xi_i \leftarrow \left|\sum_{j=n+1}^{2n} \mu_j \times \left|M'_j\right|_{m_i}\right|_{m_i} & \text{in } \mathcal{B} \text{ and } m_{2n+1} \\ 7-.\ \alpha \leftarrow \left|(\xi_{2n+1} - r_{2n+1}) \times \left|M'\right|_{m_{2n+1}}^{-1}\right|_{m_{2n+1}} \\ 8-.\ \ r_j \leftarrow \left|(\xi_i - \alpha \times \left|M'\right|_{m_i})\right|_{m_i} & \text{in } \mathcal{B} \end{cases} \tag{14}$$

Then we obtain for the evaluation modulo m_{2n+1}, the instructions 6, 2 and 7 of Algorithm 5:

$$\begin{cases} 6-.\ \ \xi'_{2n+1} \leftarrow \left|\sum_{j=n+1}^{2n} \mu_j \times \left|M'_j\right|_{m_{2n+1}} \times \left|M'\right|_{m_{2n+1}}^{-1}\right|_{m_{2n+1}} \\ 2-.\ \ r'_{2n+1} \leftarrow \left|c_{2n+1} + \sum_{i=1}^{n} \sigma_i \times \left|M_i\right|_{m_{2n+1}} \times p_{2n+1}) \times \left|M\right|_{m_{2n+1}}^{-1} \times \left|M'\right|_{m_{2n+1}}^{-1}\right|_{m_{2n+1}} \\ 7-.\ \alpha \leftarrow \left|\xi'_{2n+1} - r'_{2n+1}\right|_{m_{2n+1}} \end{cases} \tag{15}$$

Hence the algorithm becomes:

Algorithm 5: MontgR_RNSbis(c, p)

Data:

- Two RNS bases $\mathcal{B} = (m_1, \ldots, m_n)$, and $\mathcal{B}' = (m_{n+1}, \ldots, m_{2n})$, such that $M = \prod_{i=1}^{n} m_i < M' = \prod_{j=1+n}^{2n} m_j$ and $\gcd(M, M') = 1$;
  with $M_i = M/m_i$ and $M'_j = M'/m_j$
- a redundant modulus m_{2n+1}, coprime to all the m_i for $i = 1...2n$
- a positive integer p represented in RNS in both bases such that $0 < (n+2)^2 p < M$ and $\gcd(p, M) = 1$ (p is prime);
- $\tau_i = \left| -p^{-1} \right|_{m_i} \times \left| M_i \right|_{m_i}^{-1} \Big|_{m_i}$, $\forall i = 1...n$;
- $\rho_{i,j} = \left| \left| M_i \right|_{m_j} \times \left| p \right|_{m_j} \right|_{m_j}$, $\forall i = 1...n$ and $\forall j = n+1...2n+1$,
- $\nu_j = \left| \left| M \right|_{m_j}^{-1} \times \left| M'_j \right|_{m_j}^{-1} \right|_{m_j}$, in $\mathcal{B}'$.

Input: A positive integer c represented in RNS in in $\mathcal{B}$ in $\mathcal{B}'$ and m_{2n+1}, with $c < Mp$

Result: A positive integer $r \equiv abM^{-1} \pmod{p}$ represented in RNS in both bases, with $r < (n+2)p$.

1 $\sigma_i \leftarrow \left| c_i \times \tau_i \right|_{m_i}$, in $\mathcal{B}$;

2 $r'_{2n+1} \leftarrow \left| (c_{2n+1} + \sum_{i=1}^{n} \sigma_i \times \rho_{i,2n+1}) \times (\left| M \right|_{m_{2n+1}}^{-1} \left| M' \right|_{m_{2n+1}}^{-1}) \right|_{m_{2n+1}}$;

3 $\gamma_j \leftarrow \left| c_j + \sum_{i=1}^{n} \rho_{i,j} \times \sigma_i \right|_{m_j}$, in $\mathcal{B}'$;

4 $\mu_j \leftarrow \left| \gamma_j \times \nu_j \right|_{m_j}$, in $\mathcal{B}'$, ;

5 $\xi_i \leftarrow \left| \sum_{j=n+1}^{2n} \mu_j \times \left| M'_j \right|_{m_i} \right|_{m_i}$, in $\mathcal{B}$;

6 $\xi'_{2n+1} \leftarrow \left| \sum_{j=n+1}^{2n} \mu_j \times (\left| M'_j \right|_{m_{2n+1}} \left| M' \right|_{m_{2n+1}}^{-1}) \right|_{m_{2n+1}}$;

7 $\alpha \leftarrow \left| \xi'_{2n+1} - r'_{2n+1} \right|_{m_{2n+1}}$;

8 $r_j \leftarrow \left| \xi_i - \alpha \times \left| M' \right|_{m_i} \right|_{m_i}$ in $\mathcal{B}$;

We summarize now the cost of this algorithm. The evaluations in bases $\mathcal{B}$ and $\mathcal{B}'$ (lines 1, 3, 4, 5 and 8), represent $2n^2 + 3n$ products. The evaluations on the extra modulus m_{2n+1} (instructions 6, 2 and 7) use $2n + 1$ multiplications. Thus, the total cost of these reduction is $2n^2 + 5n + 1$ words-operations (on a $n+1$ arithmetic cells, that represents, due to the dependencies, $2n+3$ product-cycles). Now, we remind that m_{2n+1} is small, it can be chosen as the smaller

power of two greater than n. So, this part of the calculus can be neglected. Hence, we can consider that the total cost of the reduction represents $2n^2 + 3n$ words-products

3.3 Discussion about the advantages

Even if the number of operations needed is somewhat higher than in a classical representation ($2n^2 + n$ words products for the classical Montgomery), RNS has some important advantages. It is easy to implement, particularly in hardware, and it provides a reduced cost for multiplication and addition and a competitive modular reduction. Furthermore, RNS allows, due to the independence of the modular operations, to perform computations in a random way and to parallelize the architecture.

Moreover, it is shown that RNS can be used as a leak-resistant arithmetic [12, 4], by selecting randomly $\mathcal{B}$ and $\mathcal{B}'$ in a set of $2n$ coprime numbers. It is shown that we got $\binom{2n}{n}$ ways to do the same calculus. Hence, DPA attacks are very difficult to operate. Against SPA it can be possible to exchange the bases during the evaluation.

The parallelization of the architecture, with n basic operators (the extra modulus m_r can be included inside [3]), gives a time complexity of 2 modular digit-operation for the multiplication (or multiplication-addition) and $2n+3$ for the modular reduction. According to this point we see that if we accumulate some operations (i.e., sum of products) before reduction we obtain an efficient implementation ([2]). We develop this approach in the next section with ECC.

Last advantage of the RNS is the natural scalability of the architecture. With a given structure of n modular digit operators, it is possible to handle many values of p whose verify (7): $(n+2)^2 \times p < M$. If we refer to Algorithm 5, we remark that the only values depending of p are: τ_i and $\rho_{i,j}$. Thus by reinitializing these pre-computed values the system can be adapted for a new value of p. If p is relatively smaller than M, we can adjust the RNS basis by reducing it of some m_i. In this case we will use partial RNS bases $(m_1, ..., m_{\tilde{n}})$ and $(m_{n+1}, ..., m_{n+\tilde{n}})$ with $\tilde{n} < n$. In this case, with a control part which takes into account of $\tilde{n}$, we can assume that the performances of the system depends of the size of p.

Hence, the architecture proposed in this paper offer different level of adaptability, scalability and security proper to the RNS.

4 Leak-resistant arithmetic on elliptic curves optimized for the RNS representation

The aim of this section is to rewrite or modify the formulae given in section 2.2 in order to minimize the number of modular reduction since this is the most expensive operation in RNS representation. Thus we have to group together several multiplications and perform only one reduction.

4.1 Unified addition formulae

This can be very well illustrated by the formulae for Hessian elliptic curves. We give here the steps that must be done to compute the sum of two points (X_1, Y_1, Z_1) and (X_2, Y_2, Z_2). The costs are given by the number of modular reductions.

step	operations	cost
computation of intermediate products	$A = X_2Y_1, \quad B = Y_1Z_2, \quad C = X_1Y_2$ $D = Y_2Z_1, \quad E = X_1Z_2, \quad F = X_2Z_1$	3 3
computation of X_3	$AB - CD$	1
computation of Y_3	$EC - FA$	1
computation of Z_3	$EB - FD$	1

Thus the total cost in RNS representation is 9 modular reductions which has to be compared to the 12 base field multiplication in standard representation.

Concerning the Jacobi quartic the cost in term of modular reductions (and the formulae) is given in [15] and is equal to 10 whereas 12 multiplications are necessary.

Finally, we give the details of the steps for computing the sum of two points using unified addition formulae for a curve given in short Weierstrass form

step	operations	cost
computation of λ_n	$A = X_2Z_1, \quad B = X_1Z_2,$ $C = Z_1Z_2, \quad D = aC$ $\lambda_n = (A+B)^2 - AB + CD$	2 2 1
computation of λ_d	$E = Y_1Z_2 + Y_2Z_1$ $\lambda_d = EC$	1 1
intermediary computations	$F = E\lambda_d, \quad G = \lambda_n^2$ $H = F(A+B)$	2 1
computation of X_3	$2\lambda_d(G - H)$	1
computation of Y_3	$\lambda_n(3H - 2G) - F^2$	1
computation of Z_3	$2\lambda_d^3$	2

In this case, the total cost in RNS is 14 modular reduction whereas 18 multiplication must be performed.

Thus, for all known unified formulae, the computation of the addition requires less reductions than multiplications. This means that, even if the cost of the RNS modular multiplication is higher than the cost of the standard modular multiplication (as shown in Section 3.2), using the RNS representation of numbers can become interesting in term of performance. In addition, it has all the advantages described in Section 3.3. We give in Section 5 a detailled comparison.

4.2 Montgomery formulae

The situation is even more exciting in this case. In fact it is not exciting at all for curves which can be transformed into Montgomery form since both 10 multiplications and modular reduction are required. Moreover, because of the degree of the formulae, it is easy to see that it is not possible to have a better result. The case of Montgomery formulae in the general Weierstrass form is much more interesting. Indeed one can do better than re-using the formulae described in Section 2.2. Following the strategy used for the unified addition formulae leads to 16 modular reductions and 19 multiplications. Slightly rewriting the formulae given in Section 2.2 already allows to perform only 15 modular reductions. These formulae are given in [2]. It is in fact possible to reduce again this complexity by resuming from the beginning the Montomery ladder with a more theoretical point of view.

The Montgomery ladder is based on the fact that the y-coordinate brings only minor information. Indeed, it only allows to distinguish a point and its opposite (or equivalently a point and its image under the hyperelliptic involution). Thus the Montgomery ladder is only dealing with the x-coordinate. From a theoretical point of view, this means that we are working on the quotient of the curve by the hyperelliptic involution : the Kummer surface. Of course, taking such a quotient implies that it is not possible to add two different points (since $P+Q$ and $P-Q$ are not equal in the Kummer surface. However the doubling is still possible (it is easy to discern $P+P$ and $P-P$) and if $P-Q$ is known it will be possible to discern $P+Q$ and $P-Q$. More precisely, it is proved in [17] that there exists biquadratic forms M_x, M_z and M_{xz} such that for any points $P=(X_p,Z_p)$ and $Q=(X_q,Z_q)$ on the Kummer surface

$$\begin{array}{lcl} 2X_{p+q}X_{p-q} & = & M_x \\ X_{p+q}Z_{p-q}+X_{p-q}Z_{p+q} & = & M_{xz} \\ 2Z_{p+q}Z_{p-q} & = & M_z \end{array}$$

with

$$\begin{array}{rcl} M_x & = & (X_pX_q-aZ_pZ_q)^2-4bZ_pZ_q(Z_pX_q+X_pZ_q), \\ M_{xz} & = & X_pX_q(Z_pX_q+X_pZ_q)+Z_pZ_q(a(Z_pX_q+X_pZ_q)+2bZ_pZ_q) \\ M_z & = & (Z_pX_q-X_pZ_q)^2 \end{array}$$

If $P-Q$ is known, one can easily deduce from these biquadratic forms the formulae to compute X_{p+q} and Z_{p+q}. In fact, only two of the biquadratic forms are necessary. For instance, the formulae obtained (by an other way) by Brier and Joye in [8] and given in Proposition 2 can be easily deduced from M_x and M_z. Here, in order to minimize the number of modular reductions, we will use M_{xz} and M_z. In the context of the Montgomery ladder (Algorithm 2), the difference between the two points we want to add is always the base point $G=(x,y)$ which is given in affine coordinate so that $Z_{p-q}=1$ and $X_{p+q}=x$.

Thus we obtain

$$\begin{aligned} X_{p+q} &= 2(M_{xz} - xZ_{p+q}) \\ Z_{p+q} &= M_z \end{aligned}$$

Let us note that the theory of Kummer surfaces also provides formulae for the doubling but there are always leading to the same formulae than in Proposition 2. Therefore, we have the following theorem.

Theorem 1 *Let p be a prime number and E be an elliptic curve defined over $\mathbb{F}_p$ by (1). Let also $P = (X_p, Y_p, Z_p)$ and $Q = (X_q, Y_q, Z_q) \in E(\mathbb{F}_p)$ given in projective coordinates. Assume that $P - Q = (x, y)$ is known in affine coordinates. Then we obtain the X and Z-coordinates for $P + Q$ and $2P$ in terms of the X and Z-coordinates for P and Q by the following formulae :*

$$\begin{aligned} X_{p+q} &= 2\left(X_pX_q(Z_pX_q + X_pZ_q) + Z_pZ_q(a(Z_pX_q + X_pZ_q) + 2bZ_pZ_q) - xZ_{p+q}\right), \\ Z_{p+q} &= (X_pZ_q + X_qZ_p)^2 - 4X_pX_qZ_pZ_q, \\ X_{2p} &= \left(X_p^2 - aZ_p^2\right)^2 - 8bX_pZ_p^3, \\ Z_{2p} &= 4X_pZ_p\left(X_p^2 + aZ_p^2\right) + 4bZ_p^4. \end{aligned}$$

Finally, we give the details of the steps for computing the sum of two points and the doubling of a point

step	operations	cost
preliminary computations	$A = Z_pX_q + X_pZ_q$	1
	$B = 2X_pX_q, \quad C = 2Z_pZ_q$	2
computation of Z_{p+q}	$A^2 - BC$	1
computation of X_{p+q}	$D = aA + bC$	1
	$BA + CD + 2xZ_{p+q}$	1
preliminary computations	$A = 2X_pZ_p$	1
	$B = X_p^2, \quad C = Z_p^2$	2
	$D = -4bA, \quad E = aA$	2
computation of X_{2p}	$BD + (C - E)^2$	1
computation of Z_{2p}	$2B(C + E) - AD$	1

In this case, the total cost in RNS representation is 13 modular reduction (and 20 almost for free multiplications) whereas 19 base field multiplications must be performed in a standard representation.
It is interesting to notice that, contrary to the case of the standard representation, the extra cost for curves in short Weierstrass form compared to (more specific) curves in Montgomery form is not too large (33% in RNS representation compared to 90% in standard representation).
Lastly, if a (or b) is a small number, the cost becomes 12 modular reductions whereas 17 base field multiplications must be performed in a standard representation. Let us now show that we can almost always assume that either a or b is small.

4.3 Rescaling the constant to a small value

This section is not specific to the RNS representation and can be applied in other contexts. It takes source in the fact that there are 2 multiplications by a in the general formulae for the Montgomery ladder. Thus if a can be rescaled to a small value, the gain will be attractive.
The standard way to perform such a rescaling is the use of an isomorphism

$$\begin{array}{rcl} \psi : E(\mathbb{F}_p) & \longrightarrow & E'(\mathbb{F}_p) \\ (x,y) & \mapsto & \left(\dfrac{x}{u^2}, \dfrac{y}{u^3}\right) \end{array}$$

where $u \in \mathbb{F}_p^*$ and E' is the elliptic curve given by the equation

$$y^2 = x^3 + \frac{a}{u^4}x + \frac{b}{u^6}.$$

Thus if we want to rescale a to a small value, say k, we have to find an element u such that $u^4 = \frac{a}{k}$. In other words, rescaling a to the smallest possible value is equivalent to find the smallest k such that $\frac{a}{k}$ is a fourth power in $\mathbb{F}_p$. For instance a can be rescaled to 1 if it is a fourth power. The probability for an element of $\mathbb{F}_p$ to be a fourth power is $\frac{1}{4}$. In fact, one can obtain a better result in the context of the Montgomery ladder. Indeed y is not used in this representation so that only u^2 will be used and it is in fact sufficient that $\frac{a}{k}$ is a square in $\mathbb{F}_p$. This allows to relax the constraints. Of course it is not possible to use an isomorphism over $\mathbb{F}_p$ anymore. We can use an isomorphism defined over $\overline{\mathbb{F}_p}$ but it is easier to use a change of variables.

Theorem 2 *Let E be an elliptic curve defined over $\mathbb{F}_p$ by (1) and k be a small integer such that $\frac{a}{k}$ is a square in $\mathbb{F}_p$. Let also $P = (X_p, Y_p, Z_p)$ and $Q = (X_q, Y_q, Z_q) \in E(\mathbb{F}_p)$ given in projective coordinates. Assume that $P - Q = (x, y)$ is known in affine coordinates. Put $Z' = \sqrt{\frac{a}{k}}Z$. Then we obtain the X and Z'-coordinates for $P + Q$ and $2P$ in terms of the X and Z'-coordinates for P and Q by the following formulae :*

$$\begin{array}{rcl} X_{p+q} & = & -4\frac{b}{\frac{a}{k}\sqrt{\frac{a}{k}}} Z'_p Z'_q (X_p Z'_q + X_q Z'_p) + (X_p X_q - k Z'_p Z'_q)^2, \\ Z'_{p+q} & = & \frac{x}{\sqrt{\frac{a}{k}}}(X_p Z'_q - X_q Z'_p), \\ X_{2p} & = & \left(X_p^2 - k Z_p'^2\right)^2 - 8\frac{b}{\frac{a}{k}\sqrt{\frac{a}{k}}} X_p Z_p'^3, \\ Z'_{2p} & = & 4Z'_p\left(X_p^3 + k X_p Z_p'^2 + \frac{b}{\frac{a}{k}\sqrt{\frac{a}{k}}} Z_p'^3\right). \end{array}$$

Of course, $\frac{b}{a\sqrt{a}}$ and $\frac{x}{\sqrt{a}}$ must be precomputed. In this case, addition can be performed in 9 multiplications and doubling in 8. The same idea can be applied to formulae optimized for the RNS representation given in Section 4.2.
However, is it always possible to find such a small k ?
The first remark is that a is a square with probability $\frac{1}{2}$ (which is better than

the probabilty of $\frac{1}{4}$ that a is a fourth power). In this case, we can choose $k = 1$. Otherwise, if a is not a square, the simplest case to treat is the case $p \equiv 3 \bmod 4$. Indeed, in this case, -1 is not a square in $\mathbb{F}_p$ so that $-a$ is a square (thanks to the multiplicativity of the Legendre symbol) and we can choose $k = -1$. If $p \equiv 1 \bmod 4$, we have to check that k is sufficiently small. It is easy to prove (using again the properties of the Legendre symbol) that the proportion of prime fields such that the n first prime numbers are squares is only $\frac{1}{2^n}$. Thus, in most cases, it is possible to rescale a to a small number.

Anyway, if k is too large to assume that the multiplication by k can be neglected, there is another way to rescale a to a small value. This method is explained in [9]. The principle is to find an isogeny of small degree between the elliptic curve E and an new elliptic curve, say E'' having the same cardinality. One can then hope that the method explained above will give a better result on E'' than on E.
Basically, it is the same idea that the previous isomorphism between E and E' (an isomorphism is an isogeny of degree 1) but the composition of the isogeny and its dual is not the identity on E so that the scalar multiplication must be modified to give the right result. This operation has a negligible cost compared to the full scalar multiplication and is explained in detail in [9].

Finally, the method explained for rescaling a to a small value can also be applied to b if there exists a small k such that $\frac{4b}{k}$ is a cube in $\mathbb{F}_p$ which leads to the same gain (2 multiplications).

As a conclusion, the probability that neither a nor b can be rescaled (by using Z' or isogenies) to a small value is very low in the Montgomery ladder context.

5 Comparisons of performance

In this section, we will compare the complexity of our approach to those using Montgomery modular multiplication or Mersenne numbers.
First we summarize the complexities in Table 1: obtained for the base field

Operation	RNS	Montgomery	Mersenne
Multiplication	$2n$	n^2	n^2
Reduction	$2n^2 + 3n$	$n^2 + n$	0

Table 1: Number of word operations in RNS, Montgomery and Mersenne approach for two n-word integers

operations. Table 2 shows the number of operations required for each bit of the exponent and for the different representations of the curve we chose to deal with

in this paper.

Curve representation	RNS representation	Standard representation
Hessian form	9 red. and 12 mul.	12 mul. and 9 red.
Jacobi form	10 red. and 12 mul.	12 mul. and 10 red.
unified Weierstrass form	14 red. and 18 mul.	18 mul. and 14 red.
Montgomery ladder	13 red. and 20 mul.	19 mul. and 16 red.
Montgomery ladder (a small)	12 red. and 18 mul.	17 mul. and 14 red.

Table 2: Optimal number of operations in RNS and standard representation for a basic step of the scalar multiplication

It is then easy to deduce the global complexity in each case. For instance, one step of Montgomery exponentiation algorithm using the formulae given in Section 2.2 (for Montgomery and Mersenne approach) or section 4.2 (for our approach) when a is small requires $17n^2+14(n^2+n)$ operations with Montgomery modular multiplication, $17n^2$ with Mersenne numbers and $18(2n)+12(2n^2+3n)$ in RNS. We summarize inTable 3 the word complexity for each representation of the curve we considered in this paper (i.e., those having leak-resistance properties). We also give these complexities for usual ECC sizes for a 32-bit architecture. All these complexities are given for one basic step of the scalar multiplication.

As expected, Mersenne numbers based arithmetic is unbeatable in term of performance. Nevertheless, we have seen that RNS arithmetic has other advantages such as leak-resistance properties and scalable architecture. On the other hand, it is interesting to remark that the complexities we obtain in RNS are assymptotically always better than in Montgommery representation despite the fact that Montgomery arithmetic on the base field has a better complexity. This is due to the fact that we optimised formulae on elliptic curves in order to minimize the number of reduction. Unfortunately, such a better complexity is not sufficient when n is small as it is the case for 192 or 256 bits elliptic curves. Our method becomes competitive for larger sizes such as 512 bits elliptic curves (or equivalently 256 bits elliptic curves on a 16 bits architecture) when unified formulae are used. Concerning the Montgomery ladder, the results are better since our method is competitive for 256 bits elliptic curves. This is because we discovered new formulae which are well adapted to the RNS representation of numbers. Anyway, RNS arithmetic shows all its advantages when a parallel architecture is used.

Indeed, if we assume that we dispose of an architecture equivalent to n word-operators on a single word-bus, we get in table 4 the complexities of the different approaches in number of word operations. Note that we only give these complexities in the case of the Montgomery ladder with a small in order to simplify the paper. The complexities for the other curves representations can

Curve representation	size in bit	RNS	Montgomery	Mersenne
Hessian form	$32n$	$18n^2 + 51n$	$21n^2 + 9n$	$12n^2$
	192	954	810	432
	256	1560	1416	768
	512	5424	5520	3072
Jacobi form	32n	$20n^2 + 54n$	$22n^2 + 10n$	$12n^2$
	192	1044	852	432
	256	1712	1488	768
	512	5984	5792	3072
unified Weierstrass form	32n	$28n^2 + 78n$	$32n^2 + 14n$	$18n^2$
	192	1476	1236	648
	256	2416	2160	1152
	512	8416	8416	4608
Montgomery ladder	32n	$26n^2 + 79n$	$35n^2 + 16n$	$19n^2$
	192	1410	1356	684
	256	2296	2368	1216
	512	7920	9216	4864
Montg. ladder (a small)	32n	$24n^2 + 72n$	$31n^2 + 14n$	$17n^2$
	192	1296	1200	612
	256	2112	2096	1088
	512	7296	8160	4352

Table 3: Cost of one iteration of scalar multiplication

be easily deduced from Table 3.

Operation	RNS	Montgomery	Mersenne
Multiplication	2	$n \dots 2n$	$n \dots 2n$
Reduction	$2n + 3$	$2n \dots 3n$	0
One iteration of algorithm 2	$24n + 72$	$44n \dots 75n$	$17n \dots 34n$

Table 4: Number of cycles with parallel implementations on a n word-operators structure (18M+12R for RNS and Montgomery and 17M+14R for Mersenne).

The estimation of the cost for the multiplication and for Montgomery parallel product are based on systolic implementations [28] or on parallel implementations [10, 32] where the given architecture are respectively in $O(n^2/log(n)^2)$ and $O(n^2)$ for the area and $O(\log(n))$ for the time. As we did not find an explicit complexity for multiplication using a $O(n)$ area architecture, we give two values for the complexity. The first one is minimal but certainly not realistic. The second one, which is not necessarily optimal, takes into account that

- each product of a number by a digit will produce two numbers (the high and the low part),

- a carry-save adder will need an extra register for storing the carry and a final adder for absorbing those carries,
- 32-bit words look-up tables are not reasonable.

Then, to get an idea with ECC key size, we compare three different implementations in table 5 for the number of operations required for one step of the Montgomery scalar multiplication on an elliptic curve in Weierstrass form with a small.

$\lvert p\rvert_2$	word	RNS	Montgomery	Mersenne
192	6	216	264 ... 450	102... 204
256	8	264	352... 600	136... 272
512	16	456	704... 1200	272... 544

Table 5: Comparison of parallel implementations

In this configuration, the RNS becomes very interesting compared to Montgomery arithmetic in terms of efficiency for a leak-resistant implementation of elliptic curve cryptosystems even if we use the non-realistic lower bound for the comparison.

Implementations based on generalized Mersenne primes are still slighlty better in term of efficiency but one has to keep in mind that an architecture using such prime numbers has some disadvantages compared to RNS. In particular, it is not highly scalable.

6 Conclusion

We combined two leak-resistance techniques to obtain an efficient and secure implementation of elliptic curves cryptosystems on embedded devices.
Since the expensive operation in RNS is the reduction, we had to rewrite formulae for elliptic curve leak-resistant arithmetic in order to minimize the number of reductions even if the number of multiplications is increasing. In the case of the Montgomery ladder on elliptic curves in Weierstrass form, we obtained new formulae which are better adapted to RNS representation of numbers and we explain why multiplications by one of the coefficients of the curve can be neglected in most cases.
We also give a deep analysis of the complexity of the Montgomery reduction. Doing this, we realize that some improvements could be done leading to a final complexity of $2n^2 + 3n$ for a n-word number.
Combining this improvement of the RNS reduction and the revisited formulae for elliptic curves leads to a competitive leak-resistant arithmetic for high security levels in particular in the case of the Montgomery ladder on elliptic curves in Weierstrass form.

Our approach is particularly interesting from the hardware point of view since the RNS representation of numbers has many advantages (leak-resistance, easy to implement and to parallelize, scalability). It is also very attractive in the case of a dedicated parallel architecture.

References

[1] Bajard, J.C., Didier, L.S., Kornerup, P.: Modular multiplication and base extension in residue number systems. 15th IEEE Symposium on Computer Arithmetic, IEEE Computer Society Press (2001) 59–65

[2] Bajard, J.C., Duquesne, S., Ercegovac M. and Meloni N.: Residue systems efficiency for modular products summation: Application to Elliptic Curves Cryptography, in Advanced Signal Processing Algorithms, Architectures, and Implementations XVI, part of the SPIE Optics & Photonics 2006 Symposium. August 2006 San Diego, USA.

[3] Bajard, J.C., Imbert, L.: A full RNS implementation of RSA. IEEE Transactions on Computers **53:6** (2004) 769–774

[4] Bajard, J.C., Imbert, L., Liardet, P.Y., Teglia, Y.: Leak resistant arithmetic. CHES 2004, LNCS **3156** 59–65

[5] Bajard, J.C., Meloni, N., Plantard, T.: Efficient RNS bases for Cryptography IMACS'05, Applied Mathematics and Simulation, (2005) ???–???

[6] Billet, O., Joye, M.: The Jacobi Model of an Elliptic Curve and Side-Channel Analysis. Applied Algebra, Algorithms and Error-Correcting Codes, LNCS **2643** (2003) 34–42.

[7] Bosselaers, A., Govaerts, R., Vandewalle. J.: Comparison of the three modular reduction functions LNCS **773** (1994) 175–186

[8] Brier, E., Joye, M.: Weierstrass Elliptic Curves and Side-Channel Attacks. Public Key Cryptography, LNCS **2274** (2002) 335–345

[9] E. Brier, M. Joye, Fast Point Multiplication on Elliptic Curves Trough Isogenies, Applied Algebra, Algorithms and Error-Correcting Codes, Lecture Notes in Comput. Sci., vol.2643, Springer, Berlin, 2003, pp. 43–50.

[10] Bunimov, V., Schimmler, M.: Efficient Parallel Multiplication Algorithm for Large Integers Euro-Par 2003, International Conference on Parallel and Distributed Computing (2003) 923–928

[11] Chung, J., Hasan, A.: More generalized mersenne numbers. SAC 2003, LNCS **3006** (2003) 335–347

[12] Ciet, M., Neve, M., Peeters, E., Quisquater, J.J.: Parallel FPGA implementation of RSA with residue number systems– can side-channel threats be avoided? 46th IEEE International Midwest Symposium on Circuits and Systems (2003)

[13] Cohen, H., Frey, G.: Handbook of elliptic and hyperelliptic curve cryptography. Discrete Math. Appl., Chapman & Hall/CRC (2006)

[14] Coron, J.S.: Resistance against differential power analysis for elliptic curve cryptosystems. CHES'99, LNCS **1717** (1999) 292–302

[15] Duquesne, S.: Improving the Arithmetic of Elliptic Curve in Jacobi Model. Information Processing Letters **104:3** (2007) 101–105.

[16] Fischer, W., Giraud, C., Knudsen, E.W., Seifert, J. P.: Parallel scalar multiplication on general elliptic curves over $\mathbb{F}_p$ hedged against Non-Differential Side-Channel Attacks. Preprint

[17] Flynn, E.V.: An explicit theory of heights. Trans. Amer. Math. Soc. **347:8** (1995) 3003–3015.

[18] Garner, H.L.: The residue number system. IRE Transactions on Electronic Computers, EL **8:6** (1959) 140–147

[19] Izu, T., Takagi, T.: A Fast Parallel Elliptic Curve Multiplication Resistant against Side Channel Attacks. Public Key Cryptography, LNCS **2274** (2002) 280–296

[20] Joye, M., Quisquater, J.J.: Hessian Elliptic Curves and Side-Channel Attacks. CHES 2001, LNCS **2162** 402–410.

[21] Knuth, D.: Seminumerical Algorithms. The Art of Computer Programming, vol. 2. Addison-Wesley (1981)

[22] Kocher, P.C.: Timing attacks on implementations of DH, RSA, DSS and other systems. CRYPTO'96, LNCS **1109** (1996) 104–113

[23] Kocher, P.C., Jaffe, J., Jun, B.: Differential power analysis. CRYPTO'99, LNCS **1666** (1999) 388–397

[24] Liardet, P. Y., Smart, N.: Preventing SPA/DPA in ECC systems using the Jacobi form. CHESS 2001, LNCS **2162** 391–401.

[25] Montgomery, P.L.: Modular multiplication without trial division. Math. Comp. **44:170** (1985) 519–521

[26] Montgomery, P.L.: Speeding the Pollard and elliptic curve methods of factorization. Math. Comp. **48:177** (1987) 243–164

[27] Okeya, O., Sakurai, K.: Efficient Elliptic Curve Cryptosystems from a Scalar Multiplication Algorithm with Recovery of the y-Coordinate on a Montgomery-Form Elliptic Curve. Cryptographic Hardware and Embedded Systems, LNCS **2162** (2001) 126–141

[28] G. Orlando and C. Paar. A scalable GF(p) elliptic curve processor architecture for programmable hardware. In Proceedings of Workshop on Cryptograpic Hardware and Embedded Systems (CHES 2001)

[29] Posch, K.C., Posch, R.: Modulo reduction in residue number systems. IEEE Transaction on Parallel and Distributed Systems **6:5** (1995) 449–454

[30] Quisquater, J.J., Samyde, D.: ElectroMagnetic Analysis (EMA): Measures and Countermeasures for Smart Cards. e-smart 2001, LNCS **2140** (2001) 200–210

[31] Shenoy, A.P., Kumaresan, R.: Fast base extension using a redundant modulus in RNS. IEEE Transactions on Computer **38:2** (1989) 292–296

[32] Sanu, M.O., Swartzlander, E.E., Chase, C.M.: Parallel Montgomery Multipliers. 15th IEEE International Conference on Application-Specific Systems, Architectures and Processors (ASAP'04) (2004) 63–72

[33] Solinas, J.: Generalized Mersenne numbers. Research Report CORR-99-39, Center for Applied Cryptographic Research, University of Waterloo (1999)

[34] Szabo, N.S., Tanaka, R.I.: Residue Arithmetic and its Applications to Computer Technology. McGraw-Hill (1967)

Traces of the group law on the Kummer surface of a curve of genus 2 in characteristic 2

Sylvain Duquesne

Universités Montpellier II,
Laboratoires I3M, UMR CNRS 5149 et LIRMM, UMR CNRS 5506
CC 051, Place Eugène Bataillon, 34005 Montpellier Cedex, France.
duquesne@math.univ-montp2.fr

Abstract

In the beginning of the 90's, Flynn gave an explicit description of the Jacobian of a genus 2 hyperelliptic curve allowing to perform efficient arithmetic on these objects. In this paper, we give a generalization of the work done by Flynn when the ground field has characteristic 2. More precisely we give an explicit description of both the Jacobian and the Kummer surface. We also give (and explain how we found them) explicit formulas for the structure of the group law on the Jacobian that is preserved on the Kummer surface.

Contents

Introduction

During the 90's, Victor Flynn provides many tools for the explicit arithmetic on Jacobians of genus 2 hyperelliptic curves which are gathered in [Cas-Fly 96]. He first gave in [Fly 90] an explicit description of such Jacobians as a $\mathbb{P}^{15}$ embedding and therefore brings to the community a new tool to perform computations on such curves. However, this explicit description was heavy to manipulate in practice. Flynn solved this problem in [Fly 93] by introducing the Kummer surface as an embedding in $\mathbb{P}^3$. This description is, of course, simpler but the group structure is lost in passing from the Jacobian to the Kummer surface. Fortunately, traces of this group law remain and Flynn computed them. He deduced several applications of this work as in [Fly 95], [Fly-Sma 97] or [Fly 97]. All this applications were on fields of characteristic 0 (and even on $\mathbb{Q}$ or number fields) so that he never needs to consider the case of characteristic 2. In [Sma-Sik 99] and [Duq 05], applications of this Kummer surface to cryptography are given. As the characteristic 2 is often used in cryptography, it is interesting to generalize the work of Flynn to characteristic 2. Of course other applications could be find, but this one was our first motivation.

All the formulas obtained in this paper are available in `Maple` or `Magma` format on my web site `http://www.math.univ-montp2.fr/~duquesne`.

1 The Kummer surface in genus 2 and odd characteristic

In this section, we suppose that the characteristic of the ground field k is not 2 and consider curves $\mathcal{C}$ of genus 2 in the form

$$\mathcal{C} : y^2 = f(x),$$

where

$$f(x) = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0 \in k[x]$$

has no multiple factors. Every curve of genus 2 defined over k is birationally equivalent over k to such a curve.

1.1 Description of the Jacobian

The Jacobian, denoted by $\mathcal{J}$ in the following, is an algebraic variety whose points correspond to the elements of Pic^2, the group of the divisor classes of degree 2 divisors modulo principal divisors. This means that an element of the Jacobian can be identified with a pair of points on the curve. Such an element is defined over k if the two points are in k or if they are conjugate over a quadratic extension of k.

In [Fly 90] and [Cas-Fly 96], Flynn explains how to realize an embedding of the Jacobian in $\mathbb{P}^{15}(k)$. He uses a theorem of Lefschetz ([Lan 82], p. 105) setting up that a basis of $\mathcal{L}\left(2(\Theta^+ + \Theta^-)\right)$[1] gives such a projective embedding of the Jacobian. $\mathcal{L}\left(2(\Theta^+ + \Theta^-)\right)$ is equivalent to the space of symmetric functions on $\mathcal{C} \times \mathcal{C}$ which have at most a double pole at infinity, a pole of any order at the neutral element $\mathcal{O}$, and are regular elsewhere. Such functions form a vector space of dimension 16 thanks to the Riemman-Roch theorem. Therefore, Flynn describes the Jacobian by exhibiting 16 independent functions in $\mathcal{L}\left(2(\Theta^+ + \Theta^-)\right)$ that we will not reproduce here.

Afterward, Flynn studies the behaviour of these 16 basis element in the neighbourhood of $\mathcal{O}$. He deduces from this study a basis for the quadratic relations between the 16 functions. There are 72 such relations (available on the ftp site of Flynn) and they form a set of defining equations for the Jacobian.

[1] Θ^+ and Θ^- are the images of the curve $\mathcal{C}$ in the Jacobian via the embedding $P \mapsto P - \infty^+$ and $P \mapsto P - \infty^-$, where ∞^+ and ∞^- are the two branches of the singularity of $\mathcal{C}$ at infinity.

1.2 Description of the Kummer surface

Among the 16 functions defining the Jacobian in $\mathbb{P}^{15}$, 10 are even, in the sense that the negation on the Jacobian leaves them unchanged.
Of these 10 even functions, there are 4 functions which give a basis for the vector space $\mathcal{L}((\Theta^+ + \Theta^-))$. These functions are providing a basis in $\mathbb{P}^3$ for the Kummer surface. More precisely, if an element of the Jacobian is represented by the two points on the curve (x_1, y_1) and (x_2, y_2), these 4 functions are

$$\begin{aligned}
k_1 &= 1 \\
k_2 &= x_1 + x_2 \\
k_3 &= x_1 x_2 \\
k_4 &= \frac{1}{(x_1 - x_2)^2} [2f_6(x_1x_2)^3 + f_5(x_1 + x_2)(x_1x_2)^2 + 2f_4(x_1x_2)^2 + \\
&\qquad f_3(x_1 + x_2)x_1x_2 + 2f_2x_1x_2 + f_1(x_1 + x_2) + 2f_0 - 2y_1y_2]
\end{aligned}$$

We let κ the projection from the Jacobian to $\mathbb{P}^3$ defined by the choice of these 4 functions among the 16 defining the Jacobian. The image of this projection is the Kummer surface $\mathcal{K}$. The map κ identifies $\pm$. Elements of order 2 are injected into $\mathcal{K}$ and all other elements $\kappa(A)$ have precisely $\pm A$ as pre-images. Moreover, Flynn proves that these 4 functions are satisfying an explicit homogeneous quartic equation of total degree 4 and of degree at most 2 in k_4. This quartic is defined over $\mathbb{Z}[f_0, \ldots, f_6]$ and is given in [Fly 93] and on the ftp site of Flynn.

It is of course preferable to work with the simpler Kummer surface in $\mathbb{P}^3$ rather than with the Jacobian in $\mathbb{P}^{15}$. It is however not always possible because the group law on the Jacobian is not preserved in the Kummer surfaces. Fortunately, traces of this group law remain on the Kummer surface.

1.3 Traces of the group law

The obstruction for the group law to be preserved on the Kummer surface is that one cannot distinguish an element B and its opposite $-B$. Hence, if we want to add an element A and B, there are 4 possibilities for the result namely $A + B$, $-A - B$, $A - B$ or $-A + B$. There is no ambiguity between $A + B$ and $-A - B$ (and between $A - B$ and $-A + B$) because they map to the same element in the Kummer surface. On the contrary, there is an ambiguity between $A+B$ and $A-B$ which are not equal in the Kummer surface.

The simplest case to treat is the addition of an element B of order 2. Indeed, in this case, $A + B = A - B$ so that this operation is well defined on the Kummer surface. It is in fact a linear map on $\mathbb{P}^3$ and is given by a 4×4 matrix. Flynn computes this matrix in [Fly 93] by formally adding an arbitrary element and an element of order 2.

A second useful piece of structure on the Kummer surface is the addition of two elements if their difference is known. Indeed, there is no ambiguity between $A+B$ and $A-B$ if $A-B$ is already known. More precisely, Flynn proves that there exist biquadratic forms φ_{ij} defined over $\mathbb{Z}[f_0, \ldots, f_6]$ such that projectively

$$\varphi_{ij}(\kappa(A), \kappa(B)) = k_i(A+B)k_j(A-B) + k_i(A-B)k_j(A+B).$$

Moreover, he gives these biquadratic forms explicitly in [Fly 93]. The way Flynn computes them is very clever. Instead of performing a direct algebraic manipulation with 2 generic elements of the Jacobian, he first assumes that B is an element of order 2 but keep its coordinates in the generic form. Thus, he can use the matrix of the addition of an element of order 2 to compute the biquadratic forms φ_{ij}. Of course, these forms are only valid, a priori, if B is an element of order 2, but Flynn proves that the formulas he obtains are in fact valid for any element B.

Finally, Flynn deduces formulas for the multiplication-by-2 map from these biquadratic forms. This map is of course well defined on the Kummer surface as there is no ambiguity between $A + A$ and $A - A = \mathcal{O}$.
Using an easy induction argument, it follows that the multiplication-by-n map can also be defined on the Kummer surface and is explicit.

1.4 Applications

Flynn provides several applications of these traces of the group law. In [Fly 95], he determines explicit height constants for Jacobians of hyperelliptic curves. These constants are necessary to perform the last step of the computation of the generators of the Jacobian (which is finitely generated if the base field is a number field). This step is called the infinite descent and is detailed in [Fly-Sma 97].
Last but not least, he deduces in [Fly 97] an explicit and efficient algorithm to compute the rational points on the curve when the rank of the Jacobian is 1 (i.e. when the condition of application of the Chabauty's theorem is

satisfied).

More recently, I used the Kummer surface and the traces of the group for cryptographic purposes. The multiplication-by-n map is the central tool in cryptography based on algebraic curves. Flynn already noticed that this map was well defined on the Kummer surface but gave an inefficient algorithm for its computation. I give in [Duq 05] a new algorithm which is on the one hand more efficient and on the other hand well adapted for cryptographic applications in the real life.

All the applications given by Flynn are on a ground field of characteristic 0 (and even on $\mathbb{Q}$ or on a number field). Thus Flynn did not need to complicate its computations by considering the case of the characteristic 2. However, in cryptography, fields of characteristic 2 are often used, so that a generalization of the work done by Flynn to the characteristic 2 is interesting. Of course, this does not exclude other applications in the future.

2 Description of the Jacobian as a $\mathbb{P}^{15}$ embedding in characteristic 2

The situation in characteristic 2 is very different of the odd characteristic. In fact a genus 2 hyperelliptic curve in characteristic 2 is not defined by an equation of the form

$$\mathcal{C} : y^2 = f(x),$$

but by an equation of the form

$$\mathcal{C}_2 : y^2 + h(x)y = f(x),$$

where

$$\begin{aligned} h(x) &= h_2x^2 + h_1x + h_0 \text{ and} \\ f(x) &= f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0 \end{aligned}$$

are polynomials in $k[x]$ satisfying some conditions ensuring the regularity of the curve. That is one of the reason why Flynn preferred to exclude this case.

An element of the Jacobian can still be represented by two points on the curve and we will always use this representation in the following. The opposite of an element is given by

$$-\{(x_1, y_1), (x_2, y_2)\} = \{(x_1, y_1 + h(x_1)), (x_2, y_2 + h(x_2))\}$$

The methodology used by Flynn in [Fly 90] and [Cas-Fly 96] to realize an embedding of the Jacobian in $\mathbb{P}^{15}(k)$ is valid for any ground field k. Thus, a projective embedding of the Jacobian is given by the vector space of symmetric functions on $\mathcal{C} \times \mathcal{C}$ which have at most a double pole at infinity (ie large at worst like $x_1^2 x_2^2$ at infinity), a pole of any order at the neutral element $\mathcal{O}$, and are regular elsewhere. The dimension of this vector space is 16 (by the Riemann-Roch theorem) and we exhibit 16 independent functions. These 16 functions form a basis so that they entirely describe the Jacobian as a $\mathbb{P}^{15}$ embedding.

As in odd characteristic, it is easy to find functions which are regular at $\mathcal{O}$ and those which have a simple pole. The situation is more complicated for functions having a pole of higher order. Indeed, the derivation cannot be used in characteristic 2 to find such order.

All the functions we will construct have $(x_1 + x_2)^n$ as a denominator. Thus, remembering that the neutral element is represented by a pair of points on the curve of the form $\{(x_1, y_1), (x_1, y_1 + h(x_1))\}$, it is sufficient (and easy) to prove that their numerator does not vanish on such pairs of points to prove that they have a pole of order n at $\mathcal{O}$. However, we have to prove that they have no other pole. Because the denominators are a power of $(x_1 + x_2)$, we just have to prove that $\{(x_1, y_1), (x_1, y_1)\}$ is not a pole. Then, we have to prove that the numerators have a zero of order n at $\{(x_1, y_1), (x_1, y_1)\}$. For this, we introduce the ideal M of $k[x_1, y_1, x_2, y_2]/(P_1, P_2)$ (where $P_i = y_i^2 + h(x_i)y_i + f(x_i)$) generated by $(x_1 + x_2)$ and $(y_1 + y_2)$. By this way, a polynomial has a zero of order n at $\{(x_1, y_1), (x_1, y_1)\}$ if and only if it lies in M^n. The ideal M is in fact principal, generated by $(x_1 + x_2)$. Moreover, $(y_1 + y_2)$ can be written as a multiple of $(x_1 + x_2)$ in any M^n (by induction) thanks to a relation deduced from the defining equation of the curve and given here :

$$h(x_2)(y_1 + y_2) = (y_1 + y_2)^2 + f_6(x_1 + x_2)^6 + f_5(x_1 + x_2)^5 + f_4(x_1 + x_2)^4 + (f_3 + f_5 x_1 x_2)(x_1 + x_2)^3 + (f_2 + f_6 x_1^2 x_2^2 + h_2 y_1)(x_1 + x_2)^2 + (f_1 + f_3 x_1 x_2 + f_5 x_1^2 x_2^2 + h_1 y_1)(x_1 + x_2) \quad (*)$$

Using these tools, we can find all the symmetric functions on $\mathcal{C}_2 \times \mathcal{C}_2$ which are large at worst like $x_1^2 x_2^2$ at infinity, have a pole of any order at the neutral element $\mathcal{O}$, and are regular elsewhere. We use for this a computer algebra package such as `Maple` or `Magma` and we obtain the following theorem

Theorem 1. *The vector space of symmetric functions on $\mathcal{C}_2 \times \mathcal{C}_2$ which have*

at most a double pole at infinity, a pole of any order at the neutral element $\mathcal{O}$, and are regular elsewhere is generated by the following 16 independent functions :

Double zero at $\mathcal{O}$

$$s_2 = (x_1 + x_2)^2$$

Simple zero at $\mathcal{O}$

$$s = x_1 + x_2$$

Regular non-zero at $\mathcal{O}$

$$\begin{aligned} u &= 1 \\ p &= x_1 x_2 \\ p_2 &= x_1^2 x_2^2 \end{aligned}$$

Simple pole at $\mathcal{O}$

$$\begin{aligned} \alpha_0 &= \frac{y_1 + y_2}{x_1 + x_2} \\ \alpha_1 &= \frac{x_2 y_1 + x_1 y_2}{x_1 + x_2} \\ \alpha_2 &= \frac{x_2^2 y_1 + x_1^2 y_2}{x_1 + x_2} \\ \alpha_3 &= \frac{x_2^3 y_1 + x_1^3 y_2}{x_1 + x_2} \end{aligned}$$

Double pole at $\mathcal{O}$

$$\begin{aligned} \beta_0 &= \frac{(x_1 + x_2)\left(f_5 x_1^2 x_2^2 + f_3 x_1 x_2 + f_1\right) + h(x_2) y_1 + h(x_1) y_2}{(x_1 + x_2)^2} \\ \beta_1 &= \frac{(x_1+x_2)\left(f_6 x_1^3 x_2^3 + f_4 x_1^2 x_2^2 + f_2 x_1 x_2 + f_0 + y_1 y_2\right) + x_1 h(x_1) y_2 + x_2 h(x_2) y_1}{(x_1+x_2)^2} \\ \beta_2 &= x_1 x_2 \beta_0 \end{aligned}$$

Triple pole at $\mathcal{O}$

$$\gamma_1 = \alpha_0 \beta_0 + f_6 (x_1 + x_2)\left(h_2 x_1^2 x_2^2 + h_1 x_1 x_2 (x_1 + x_2) + h_0 (x_1 + x_2)^2\right) + f_5 x_1 x_2 \alpha_1$$

$$\gamma_2 = \alpha_0\beta_1 + \left(x_1^2 + x_2^2 + x_1x_2\right)(f_5\alpha_2 + f_6\alpha_3) + (f_4 + f_5(x_1+x_2))\alpha_1x_1x_2 + f_6x_1x_2\left(h_2x_1^2x_2^2 + h_1(x_1+x_2)x_1x_2 + h_0(x_1+x_2)^2\right)$$

Quadruple pole at $\mathcal{O}$

$$\delta = \beta_0^2$$

The most complicated cases are γ_0 and γ_1. We notice that even if a term of degree 3 in x_1 appears in the expressions given above, these functions are not larger than $x_1^2x_2^2$ at infinity because some simplifications hold when we expand formulas. However, we prefer to give them in this form because it is much more simple than the expanded form.

These functions are difficult to find because we have to describe all the possibilities for symmetric functions on $\mathcal{C}_2 \times \mathcal{C}_2$ which have $(x_1+x_2)^3$ as a denominator and are large at worst like $x_1^2x_2^2$ at infinity. Then we have to use that they have a pole of order 3 at $\mathcal{O}$, and are regular elsewhere to get sufficiently many constraints on the functions. It is however much more easy to verify that the functions we provide are satisfying the required conditions. Indeed, one just have to check that their numerator is in M^3.

Of course, it is also easy to check that the 14 other functions given are satisfying the required conditions. Afterwards, we verify by algebraic computation that these 16 functions are independent to complete the proof of the theorem.

Finally, these 16 functions are defining an embedding of the Jacobian in $\mathbb{P}^{15}(k)$. Moreover, using the same method than Flynn (the local behaviour of these functions in the neighbourhood of $\mathcal{O}$), it is possible to determine a basis for the quadratic relations between these 16 functions and the Jacobian is given by these quadratic relations.

3 Description of the Kummer surface as a $\mathbb{P}^3$ embedding in characteristic 2

By analogy with the terminology used by Flynn, we call "even" a function which is invariant under the map

$$\begin{array}{ccc} k[x_1,y_1,x_2,y_2]/(P_1,P_2) & \longrightarrow & k[x_1,y_1,x_2,y_2]/(P_1,P_2) \\ (x_1,y_1,x_2,y_2) & \longmapsto & (x_1, y_1+h(x_1), x_2, y_2+h(x_2)) \end{array}$$

Among the 16 functions describing the Jacobian and given in Theorem 1, 9 are even and only 4 of them are large at worst like x_1x_2 at infinity, (namely u, s, p and β_0) and then provide a basis in $\mathbb{P}^3$ for the Kummer surface. For convenience, we introduce a new labelling so that

$$\begin{aligned} k_1 &= 1 \\ k_2 &= x_1 + x_2 \\ k_3 &= x_1x_2 \\ k_4 &= \frac{(x_1+x_2)\left(f_5x_1^2x_2^2 + f_3x_1x_2 + f_1\right) + h(x_2)y_1 + h(x_1)y_2}{(x_1+x_2)^2} \end{aligned}$$

The Kummer surface $\mathcal{K}_2(k)$ is then the image of the projection from the Jacobian to $\mathbb{P}^3(k)$ defined by the choice of these 4 functions among the 16 defining the Jacobian.

Proposition 1. *Let the map*

$$\begin{array}{rccc} \kappa_2 : & \mathcal{J}_2(k) & \longrightarrow & \mathcal{K}_2(k) \\ & \{(x_1,y_1),(x_2,y_2)\} & \longmapsto & [k_1,k_2,k_3,k_4] \end{array}$$

- *This map identifies an element and its opposite.*
- *The elements of order 2 are injected into $\mathcal{K}_2$ and all other elements $\kappa_2(A)$ in $\mathcal{K}_2$ have precisely A and $-A$ as pre-images.*
- *The functions k_1, k_2, k_3 and k_4 satisfy an explicit homogeneous quartic K of total degree 4 and of degree at most 2 in k_4. The Kummer surface is defined by $K(k_1,k_2,k_3,k_4) = 0$.*

The first assumption is trivial, because the 4 functions k_1, k_2, k_3 and k_4 have been chosen among even functions.

Concerning the second assumption, it is trivial that k_2 and k_3 are completely determining x_1 and x_2. Thus, there are only 4 possibilities for the pre-images namely

- $A = \{(x_1,y_1),(x_2,y_2)\}$ itself,
- $\{(x_1,y_1+h(x_1)),(x_2,y_2)\}$,
- $\{(x_1,y_1),(x_2,y_2+h(x_2))\}$ and
- $-A = \{(x_1,y_1+h(x_1)),(x_2,y_2+h(x_2))\}$.

If $\{(x_1, y_1+h(x_1)), (x_2, y_2)\}$ is a pre-image, it must have the same k_4 than A. This implies that either $h(x_1)$ or $h(x_2)$ equals 0. The situation is of course the same if $\{(x_1, y_1), (x_2, y_2 + h(x_2))\}$ is a pre-image. Hence, if $h(x_1)$ and $h(x_2)$ are both non-zero, the only possibilities for pre-images are A and $-A$. If either $h(x_1)$ or $h(x_2)$ equals 0, then only 2 of the 4 possibilities for the pre-images are different and this yields again to A and $-A$ as pre-images. Finally, the elements of order 2 are exactly those such that $h(x_1) = h(x_2) = 0$ and there is, in this case, only one pre-image.

The third assumption is proved using a formal computation of k_4^2. We obtain an equation of the form

$$K_2 k_4^2 + K_1 k_4 + K_0 = 0.$$

where K_0, K_1 and K_2 are symmetric expressions in x_1 and x_2

$$\begin{aligned}
K_2 &= (x_1 + x_2)^2 \\
K_1 &= h(x_1)h(x_2) \\
K_0 &= \frac{h(x_1)h(x_2)(x_1+x_2)(f_5x_1^2x_2^2+f_3x_1x_2+f_1)+h(x_2)f(x_1)+h(x_1)f(x_2)}{(x_1+x_2)^2}+ \\
&\qquad (f_5x_1^2x_2^2 + f_3x_1x_2 + f_1)^2
\end{aligned}$$

Despite the appearance, the term K_0 is a symmetric polynomial. Thus, we can write K_0, K_1 and K_2 as polynomials in terms of k_1, k_2 and k_3.

$$\begin{aligned}
K_2 &= k_2^2 \\
K_1 &= h_0^2k_1^3 + h_1^2k_3k_1^2 + h_0h_1k_2k_1^2 + h_2^2k_3^2k_1 + h_2h_1k_2k_3k_1 + h_0h_2k_2^2k_1 \\
K_0 &= \left(f_1^2 + h_1^2f_0 + h_0^2f_2 + h_1h_0f_1\right)k_1^4 + (h_0^2f_3 + h_2h_0f_1)k_2k_1^3 + (h_2h_1f_1 + \\
&\quad h_1h_0f_3)k_3k_1^3 + (h_2^2f_0 + h_0^2f_4)k_2^2k_1^2 + (h_2h_0f_3 + h_0^2f_5 + h_2^2f_1)k_2k_3k_1^2 + \\
&\quad (f_3^2 + h_2^2f_2 + h_1^2f_4 + h_0h_1f_5 + h_1h_2f_3 + h_0^2f_6)k_3^2k_1^2 + h_0^2f_5k_2^3k_1 + (h_1^2f_5 + \\
&\quad h_2h_0f_5)k_3^2k_2k_1 + h_2h_1f_5k_3^3k_1 + h_0^2f_6k_2^4 + h_1^2f_6k_3^2k_2^2 + (f_5^2 + h_2^2f_6)k_3^4
\end{aligned}$$

4 Traces of the group law in characteristic 2

We will now consider the structure of the Jacobian which is preserved by the map κ_2 into the Kummer surface.

4.1 Addition of an element of order 2

Let B be an element of order 2 on the Jacobian represented by the couple of points $\{(x_1, y_1), (x_2, y_2)\}$. Such an element is invariant under the map which send an element to its opposite so that both x_1 and x_2 are roots of

h. We have already seen that the addition of B with an arbitrary element A was defined on the Kummer surface because $A + B = A - B$. As this operation is linear, it can be represented by a 4×4 matrix. To compute this matrix, we use the same method than Flynn, namely we performe a direct algebraic manipulation using the geometric description of the group law on the Jacobian. We do not give details of this computation here because we will give them in the next section in a more general case. Anyway, it is easy to obtain the 3 first lines of the matrix. To obtain the fourth, we use the fact that the addition by an element of order 2 is an involution so that the square of the matrix must be the identity of $\mathbb{P}^3$. Finally, we have that

$$k_i(A+B) = \sum_{j=1}^{4} w_{ij} k_j(A) \qquad (i = 1, 2, 3, 4)$$

where the w_{ij} are given in Appendix A. Let us note that they are given in term of the coefficients of the curve and in term of x_1, x_2, y_1 and y_2. It is possible, as Flynn, to give them only in terms of the coefficients of the curve but this involves square roots of these coefficients. The expressions obtained are more complicated so that we do not give them.

4.2 Biquadratic forms

In odd characteristic, Flynn deduced the biquadratic forms φ_{ij} such that projectively

$$\varphi_{ij}(\kappa(A), \kappa(B)) = k_i(A+B)k_j(A-B) + k_i(A-B)k_j(A+B)$$

from the matrix of the addition of an element of order 2. This cannot be applied in characteristic 2. Indeed, if B is an element of order 2, these expressions are all zero. This is a good illustration of the difficulties we encounter for the generalization of Flynn's works to characteristic 2. Therefore, we have to find the biquadratic forms by using a direct algebraic manipulation which is much more demanding in term of computing resources. We notice at this step, that these expressions are also zero if $i = j$, so that, in this case, we will be interested by $k_i(A+B)k_i(A-B)$ only.

Let us first describe generically the group law on the Jacobian. Let A and B be two generic elements defined over k of the Jacobian represented by the couples of points $\{(x_1, y_1), (x_2, y_2)\}$ and $\{(x_3, y_3), (x_4, y_4)\}$. Then, there is a unique polynomial $m(x)$ defined over k of degree 3 such that $y = m(x)$

passes through the four points $(x_1, y_1), (x_2, y_2), (x_3, y_3)$ and (x_4, y_4). The complete intersection of this cubic with $\mathcal{C}_2$ is given by

$$\left\{ \begin{array}{rcl} m(x)^2 + m(x)h(x) & = & f(x) \\ y & = & m(x) \end{array} \right.$$

This intersection provide two new points (x_5, y_5) and (x_6, y_6) representing a new element C on $\mathcal{J}_2(k)$ such that

$$A + B + C = \mathcal{O}.$$

Thus, the opposite of C is the sum of A and B.

To compute the biquadratic forms, we will first formally compute the coordinates of $A+B$ in the Kummer, and then express the $k_i(A+B)k_j(A-B) + k_i(A-B)k_j(A+B)$ in terms of the coordinates of A and B in the Kummer.

The first step is to compute the cubic m and does not pose any particular problem. The second step is the computation of $m(x)^2 + m(x)h(x) + f(x)$ which must vanish. This leads to the vanishing of a polynomial of degree 6 having $(x+x_1)(x+x_2)(x+x_3)(x+x_4)$ as a factor because (x_1, y_1), (x_2, y_2), (x_3, y_3) and (x_4, y_4) are satisfying $m(x)^2 + m(x)h(x) + f(x) = 0$. After performing this exact division, it remains a polynomial of degree 2 whose coefficients are giving $x_5 + x_6$ and x_5x_6. Putting their common denominator in $k_1(A+B)$, the corresponding numerators are then giving $k_2(A+B)$ and $k_3(A+B)$. So it is not so difficult to obtain projectively the 3 first coordinates in the Kummer surface of the sum of A and B. These are given as polynomials symmetric in the $(x_i, y_i)_{i=1..4}$ of degree 5 in x_i and 1 in y_i.

It is much more difficult to obtain a simple expression for the fourth coordinate. For convenience, we will use in the following $[k_i(A+B)]_{i=1..4}$ to denote the projective coordinates of $A+B$ in the Kummer surface and $[1, s, p, \beta_0]$ to specify the affine case so that we have

$$\begin{array}{rclcl} s & = & \frac{k_2(A+B)}{k_1(A+B)} & = & x_5 + x_6 \\ p & = & \frac{k_3(A+B)}{k_1(A+B)} & = & x_5x_6 \\ \beta_0 & = & \frac{k_4(A+B)}{k_1(A+B)} & = & \frac{(x_5+x_6)\left(f_5x_5^2x_6^2+f_3x_5x_6+f_1\right)+h(x_6)y_5+h(x_5)y_6}{(x_5+x_6)^2} \end{array}$$

The numerator of β_0 can be obtained as a symmetric expression of degree 3 in x_5 and x_6 using the relations

$$y_5 = m(x_5) \text{ and } y_6 = m(x_6).$$

Then we can write this numerator as a function in $k_1(A+B), k_2(A+B)$ and $k_3(A+B)$. This function is not a polynomial because x_5+x_6 (resp. x_5x_6) must be replaced by $k_2(A+B)/k_1(A+B)$ (resp. $k_3(A+B)/k_1(A+B)$) so that $k_1(A+B)^3$ appears as a denominator. On the other hand, the denominator of β_0 is $(x_5+x_6)^2$ so that, the denominator of β_0 (written as a function of $k_1(A+B), k_2(A+B)$ and $k_3(A+B)$) is $k_2(A+B)^2k_1(A+B)$. Thus, we have to multiply the original $k_1(A+B), k_2(A+B)$ and $k_3(A+B)$ by $k_2(A+B)^2$ if we want a result without denominators. This leads to very large expressions of degree 15 in the x_i. This is not reasonable (remember that there are 18 variables, namely the x_i, the y_i and the coefficients of the curve and that we want to compute $k_i(A+B)k_j(A-B)$).

As $y_5 = m(x_5)$, $y_6 = m(x_6)$ and β_0 is regular at $\{(x_5, y_5), (x_5, y_5)\}$, β_0 must in fact be a polynomial. This will eliminate the term $(x_5+x_6)^2$ in the denominator so that we can hope a simpler result. Indeed, using the relation (*), we have

$$\beta_0 = f_6(x_5+x_6)^4 + f_5(x_5+x_6)^3 + f_4(x_5+x_6)^2 + (f_3+f_5x_6x_5)(x_5+x_6) + h_2(m(x_5)+m(x_6)) + (f_2+f_6x_5^2x_6^2) + (m_3((x_5+x_6)^2+x_5x_6)+m_2(x_5+x_6)+m_1)^2 + h_1(m_3((x_5+x_6)^2+x_5x_6)+m_2(x_5+x_6)+m_1)$$

where $m(x) = m_3x^3+m_2x^2+m_1x+m_0$ is the cubic polynomial introduced in the beginning of this section. This is the most natural way to eliminate denominators in $k_4(A+B)$. Unfortunately, this is worst than the previous situation because this symmetric polynomial has degree 4 so that the denominator of β_0 (written as a function of $k_1(A+B), k_2(A+B)$ and $k_3(A+B)$) is $k_1(A+B)^4$ and we have to multiply the original $k_1(A+B), k_2(A+B)$ and $k_3(A+B)$ by $k_1(A+B)^3$ if we want a result without denominators.

We choose an intermediate solution which consists in only simplifying β_0 by x_5+x_6. This is simpler than the previous case since we do not need the relation (*). We have that

$\beta_0 = \frac{B_0}{x_5+x_6}$ with

$$B_0 = f_5x_5^2x_6^2 + f_3x_5x_6 + f_1 + m_3(h_2x_5^2x_6^2 + h_1x_5x_6(x_5+x_6) + h_0(x_5^2+x_5x_6+x_6^2)) + m_2(h_1x_5x_6 + h_0(x_5+x_6)) + m_1(h_2x_5x_6+h_0) + m_0(h_2(x_5+x_6)+h_1)$$

In this case, the symmetric polynomials in x_5 and x_6 appear only in degree 2 in B_0 so that the denominator of β_0 (written as a function of $k_1(A+$

$B), k_2(A+B)$ and $k_3(A+B))$ is $k_1(A+B)k_2(A+B)$ and we have only to multiply the original $k_1(A+B), k_2(A+B)$ and $k_3(A+B)$ by $k_2(A+B)$ if we want a result without denominators. This is better than the two previous cases but still not satisfying. Indeed, for the reasons explained above, the expression obtained by this way for B_0 must be divisible by $k_2(A+B)$. However this property of divisibility holds only in

$$\mathbb{F}_{2hf}[x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4]/(P_1, P_2, P_3, P_4)$$

where $\mathbb{F}_{2hf} = \mathbb{F}_2[h_0, h_1, h_2, f_0, f_1, f_2, f_3, f_4, f_5, f_6]$ and $P_i = y_i^2 + h(x_i)y_i + f(x_i)$. A direct computation of the quotient of B_0 by $k_2(A+B)$ in this ring is not possible even with modern computer algebra package as `Magma`. Thus, We choose to compute it by myself using a specific way. The idea is to discover and use specific properties of the quotient to reduce the complexity of the computation.

In order to be able to exploit such specific properties, we have to proceed by identification. The general strategy of the identification method is as follows :

- the polynomials B_0 and $k_2(A+B)$ have degree 10 and 5 in each x_i (and of course 1 in each y_i) so that we construct a formal polynomial Q of degree 5 in each x_i (and of course 1 in each y_i),
- we then formally compute $Qk_2(A+B)$ and identify the coefficients with those of B_0,
- this provides a (sparse) linear system of equations whose variables are the coefficients of Q,
- finally, the coefficients of the quotient are recovered by linear algebra.

Of course there exist much better algorithms for computing a quotient but they cannot conclude with B_0 and $k_2(A+B)$ as input and we cannot speed them up if we have specific properties for the quotient. On the contrary, if we proceed by identification, it is easy to take such new properties into account.

Let us now find those specific properties. First, we can exploit the fact that our polynomials are symmetrical in the couples (x_i, y_i) so that

- the term in degree 0 in the y_i is a symmetric polynomial in the x_i,
- the term in y_1 is a symmetric polynomial in x_2, x_3 and x_4,

- the term in y_i can be deduced from the term in y_1 by exchanging x_i and x_1,
- the term in y_1y_2 is a symmetric polynomial in x_3 and x_4,
- the term in y_iy_j can be deduced from the term in y_1y_2 by exchanging x_i and x_1 on the one hand and x_j and x_2 on the other hand,
- the same properties holds for products of 3 and 4 y_i but we do not need them.

These properties allow to reduce the number of variables but more than 600 variables are necessary to formally describe Q and is it always too complicated to perform linear algebra in this case (remember that the matrix obtained has its coefficients in $\mathbb{F}_2[h_0, h_1, h_2, f_0, f_1, f_2, f_3, f_4, f_5, f_6]$). Fortunately, we can do better using an experimental approach. Our idea, in order to find specific properties of the quotient, is to compute this quotient in various simpler cases. For example, evaluating most of the 18 variables yields to a simpler ring where the computation of the quotient can be performed. Putting together the results obtained, we deduce properties which hold in all examples and then assume that they hold in the general case. The properties we obtain by this way are

- the term in degree 0 in the y_i is divisible by $\prod_{i\neq j}(x_i + x_j)$,
- the term in y_1 is divisible by $(x_2+x_3)(x_2+x_4)(x_3+x_4)$ and its degree in x_1 is bounded by 2 (instead of 5),
- the term in y_1y_2 equals $h(x_3)h(x_4)(x_1 + x_2)^2(x_3 + x_4)^2$,
- there are no terms of total degree greater than or equal to 3 in the y_i.

These properties are in fact very constraining for the quotient so that, finally, only 75 variables are required to formally describe Q. The linear algebra step can now be performed in some seconds on `Magma`. Of course, this computation is done under assumptions, but it is very easy to verify that the result obtained multiplied by $k_2(A + B)$ equals B_0.

Finally, we put this quotient in $k_4(A + B)$ so that $[k_1(A + B), k_2(A + B), k_3(A + B), k_4(A + B)]$ are the coordinates in the Kummer of $A + B$. These are given as polynomials symmetric in the $(x_i, y_i)_{i=1..4}$ of degree only 5 in x_i and 1 in y_i.

Of course, the addition is not defined on the Kummer surface so that we cannot write $k_i(A+B)$ in terms of the $k_i(A)$ and the $k_i(B)$ but we can do it for the expressions of the form $k_i(A+B)k_j(A-B)+\varepsilon_{ij}k_i(A-B)k_j(A+B)$ (where $\varepsilon_{ij}=1$ if $i\neq j$ and 0 if $i=j$). This is not difficult to do so that we do not give the details. However, at first glance, the formulas obtained are not biquadratic in the $k_i(A)$ and the $k_i(B)$. They are, in fact, all divisible by $k_2(A)^2k_2(B)^2$ when $i\neq j$ and the quotients are biquadratic which is encouraging. This is not the case if $i=j$ but we succeed in bypassing this problem using a trick. Indeed, for each i, it is possible to found an appropriate linear combination of $K(A)$ and $K(B)$ (K is the defining equation of the Kummer surface so that such a linear combination is in fact equal to zero) such that adding this linear combination to the formula for $i=j$ ensure that the modified formula is also divisible by $k_2(A)^2k_2(B)^2$.

We notice that this approach is close of the approach used by Flynn in odd characteristic since he also used a particular case to deduce the general case.

The above discussion and the computations we have done with `Maple` and `Magma` may be summarized by the following theorem

Theorem 2. *Let A, B in $\mathcal{J}_2(k)$ and $\kappa_2(A)$, $\kappa_2(B)$ their image in $\mathcal{K}_2(k)$. Then, for $i,j\in\{1,\ldots,4\}$, there exist explicit biquadratic forms φ_{ij} defined over $\mathbb{F}_2[h_0,h_1,h_2,f_0,f_1,f_2,f_3,f_4,f_5,f_6]$ such that the 4×4 symmetric matrix $(\varphi_{ij}(\kappa_2(A),\kappa_2(B)))$ is projectively equal to*

$$(k_i(A+B)k_j(A-B)+\varepsilon_{ij}k_i(A-B)k_j(A+B))$$

where $\varepsilon_{ij}=1$ if $i\neq j$ and 0 if $i=j$. These biquadratic forms are explicitly given in Appendix B.

4.3 Multiplication-by-2 map

The last trace of the group law we are interested in is the multiplication-by-2 map and more generally, the multiplication-by-n map. We have already seen that the multiplication-by-2 map was well defined on the Kummer surface. Of course, we can compute formulas by using a direct algebraic manipulation, but they can in fact be deduced from the biquadratic forms. Indeed, as the coordinates of $\mathcal{O}$ in the Kummer are $[0,0,0,1]$, we have that, projectively

$$\varphi_{i4}(\kappa_2(A),\kappa_2(A)) \quad = \quad k_i(2A)$$

The explicit formulas are given in Appendix B.

As in the case of odd characteristic, using an easy induction argument, we prove that the multiplication-by-n map can be defined on the Kummer surface and is explicit. This argument gives an algorithm that computes the multiplication-by-n map with a complexity in $O(n)$ whereas algorithms in $O(\log(n))$ exist as explained in [Duq 05].

Conclusion

Despite many technical problems due to the passing from the odd characteristic to the characteristic 2, we succeed in giving a generalization of the work done by Victor Flynn in the beginning of the 90's. Indeed, we give an explicit description of Jacobians of genus 2 hyperelliptic curves in characteristic 2 as a $\mathbb{P}^{15}$ embedding. We also describe the Kummer surface as a $\mathbb{P}^3$ embedding (more suitable for computations) and provide the traces of the group law on the Kummer surface (addition of an element of order 2, biquadratic forms enabling the addition of 2 elements if their difference is known, multiplication-by-2 map). In this way, we bring new tools to people interested in the explicit arithmetic of curves of genus 2 in characteritic 2. In particular, the formulas we provide can be used to perform a multiplication-by-n map for cryptographic applications. However a detailed study of these formulas is necessary to obtain a competitive algorithm in this domain, but we are sure that it can be done.

Appendix A

Let B be an element of order 2 on the Jacobian represented by the couple of points $\{(x_1, y_1), (x_2, y_2)\}$. The addition by B in the Kummer surface is

given by the matrix W whose coefficients are

$$
\begin{array}{rcl}
w_{11} & = & f_1 h_2^2 + f_3 h_0 h_2 + f_5 h_0^2 \\
w_{12} & = & f_5 h_1 h_0 \\
w_{13} & = & f_5 h_1^2 \\
w_{14} & = & h_1 h_2 \\
w_{21} & = & h_2(y_1 x_2^2 + x_1^2 y_2) + h_0 h_1 f_3 \\
w_{22} & = & h_2(y_1 x_2 + x_1 y_2) + f_1 h_2^2 + f_3 h_0 h_2 + f_5 h_0^2 \\
w_{23} & = & h_2(y_1 + y_2) + h_2 h_1 f_3 \\
w_{24} & = & h_1^2 \\
w_{31} & = & h_2(y_1 x_2^3 + x_1^3 y_2) + h_1^2 f_1 \\
w_{32} & = & h_2(y_1 x_2^2 + x_1^2 y_2) + h_2 h_1 f_1 \\
w_{33} & = & h_2(y_1 x_2 + x_1 y_2) + f_1 h_2^2 + f_3 h_0 h_2 + f_5 h_0^2 \\
w_{34} & = & h_1 h_0 \\
w_{41} & = & h_2 f_1(y_1 + y_2) + h_2 f_3(y_1 x_2^2 + x_1^2 y_2) + h_1 f_3 f_1 h_2 \\
w_{42} & = & h_2 f_5(y_1 x_2^3 + x_1^3 y_2) + h_1^2 f_5 f_1 \\
w_{43} & = & h_2 f_5(y_1 x_2^2 + x_1^2 y_2) + f_5 h_0 h_1 f_3 \\
w_{44} & = & f_1 h_2^2 + f_3 h_0 h_2 + f_5 h_0^2
\end{array}
$$

Appendix B

We give here the formulas for the biquadratic forms and for the multiplication-by-2 map on the Kummer surface. For clarity we change the notations and use

- $[k_1, k_2, k_3, k_4]$ instead of $[k_1(A), k_2(A), k_3(A), k_4(A)]$,
- $[l_1, l_2, l_3, l_4]$ instead of $[k_1(B), k_2(B), k_3(B), k_4(B)]$,
- φ_{ij} instead of $\varphi_{ij}(\kappa_2(A), \kappa_2(B))$,
- $[\delta_1, \delta_2, \delta_3, \delta_4]$ instead of $[k_1(2A), k_2(2A), k_3(2A), k_4(2A)]$.

All these formulas are available on my web site at

`http://www.math.univ-montp2.fr/~duquesne`.

$\varphi_{11} = f_6h_0^2k_1^2l_2^2 + f_6h_1^2k_1^2l_3^2 + k_1^2l_4^2 + f_6h_0^2k_2^2l_1^2 + (f_5^2 + f_6h_2^2)k_2^2l_3^2 + f_6h_1^2k_3^2l_1^2 + (f_5^2 + f_6h_2^2)k_3^2l_2^2 + k_4^2l_1^2$

$\varphi_{12} = f_5h_0^2k_1^2l_2^2 + h_0h_2k_1^2l_2l_4 + f_5h_1^2k_1^2l_3^2 + h_1h_2k_1^2l_3l_4 + h_0h_2k_1k_2l_1l_4 + f_5h_0h_2k_1k_2l_2l_3 + f_5h_1h_2k_1k_2l_3^2 + h_2^2k_1k_2l_3l_4 + h_1h_2k_1k_3l_1l_4 + f_5h_0h_2k_1k_3l_2^2 + f_5h_1h_2k_1k_3l_2l_3 + h_2^2k_1k_3l_2l_4 + h_0h_2k_1k_4l_1l_2 + h_1h_2k_1k_4l_1l_3 + f_5h_0^2k_2^2l_1^2 + f_5h_0h_2k_2^2l_1l_3 + f_5h_0h_2k_2k_3l_1l_2 + f_5h_1h_2k_2k_3l_1l_3 + h_0h_2k_2k_4l_1^2 + h_2^2k_2k_4l_1l_3 + f_5h_1^2k_3^2l_1^2 + f_5h_1h_2k_3^2l_1l_2 + h_1h_2k_3k_4l_1^2 + h_2^2k_3k_4l_1l_2$

$\varphi_{13} = (f_1h_0h_2 + f_3h_0^2)k_1^2l_1l_2 + (f_1h_1h_2 + f_3h_0h_1)k_1^2l_1l_3 + h_0^2k_1^2l_1l_4 + f_5h_0^2k_1^2l_2l_3 + f_5h_0h_1k_1^2l_3^2 + h_0h_2k_1^2l_3l_4 + (f_1h_0h_2 + f_3h_0^2)k_1k_2l_1^2 + (f_1h_2^2 + f_3h_0h_2)k_1k_2l_1l_3 + h_0h_1k_1k_2l_1l_4 + f_5h_0^2k_1k_2l_2^2 + f_5h_0h_1k_1k_2l_2l_3 + h_0h_2k_1k_2l_2l_4 + (f_1h_1h_2 + f_3h_0h_1)k_1k_3l_1^2 + (f_1h_2^2 + f_3h_0h_2)k_1k_3l_1l_2 + (h_0h_2 + h_1^2)k_1k_3l_1l_4 + f_5h_0h_1k_1k_3l_2^2 + (f_5h_0h_2 + f_5h_1^2)k_1k_3l_2l_3 + h_1h_2k_1k_3l_2l_4 + f_5h_1h_2k_1k_3l_3^2 + h_2^2k_1k_3l_3l_4 + h_0^2k_1k_4l_1^2 + h_0h_1k_1k_4l_1l_2 + (h_0h_2 + h_1^2)k_1k_4l_1l_3 + f_5h_0^2k_2^2l_1l_2 + f_5h_0h_1k_2^2l_1l_3 + f_5h_0^2k_2k_3l_1^2 + f_5h_0h_1k_2k_3l_1l_2 + (f_5h_0h_2 + f_5h_1^2)k_2k_3l_1l_3 + h_0h_2k_2k_4l_1l_2 + h_1h_2k_2k_4l_1l_3 + f_5h_0h_1k_3^2l_1^2 + f_5h_1h_2k_3^2l_1l_3 + h_0h_2k_3k_4l_1^2 + h_2^2k_3k_4l_1l_3$

$\varphi_{14} = (f_1^2h_2^2 + f_3^2h_0^2 + f_6h_0^4)k_1^2l_1^2 + f_6h_0^3h_1k_1^2l_1l_2 + f_6h_0^2h_1^2k_1^2l_1l_3 + (f_1h_1h_2 + f_3h_0h_1)k_1^2l_1l_4 + f_6h_0^3h_2k_1^2l_2^2 + f_6h_0^2h_1h_2k_1^2l_2l_3 + f_5h_0^2k_1^2l_2l_4 + (f_5^2h_0^2 + f_6h_0^2h_2^2)k_1^2l_3^2 + f_6h_0^3h_1k_1k_2l_1^2 + f_6h_0^2h_1^2k_1k_2l_1l_2 + (f_1f_5h_1h_2 + f_3f_5h_0h_1 + f_6h_0h_1^3)k_1k_2l_1l_3 + f_5h_0^2k_1k_2l_1l_4 + f_6h_0^2h_1h_2k_1k_2l_2^2 + (f_5^2h_0^2 + f_6h_0h_1^2h_2)k_1k_2l_2l_3 + f_5h_0h_1k_1k_2l_2l_4 + f_6h_0h_1h_2^2k_1k_2l_3^2 + f_5h_0h_2k_1k_2l_3l_4 +$

$f_6h_0^2h_1^2k_1k_3l_1^2 + (f_1f_5h_1h_2 + f_3f_5h_0h_1 + f_6h_0h_1^3)k_1k_3l_1l_2 + f_6h_1^4k_1k_3l_1l_3 + (f_5^2h_0^2 + f_6h_0h_1^2h_2)k_1k_3l_2^2 + f_6h_1^3h_2k_1k_3l_2l_3 + (f_5h_0h_2 + f_5h_1^2)k_1k_3l_2l_4 + f_6h_1^2h_2^2k_1k_3l_3^2 + f_5h_1h_2k_1k_3l_3l_4 + (f_1h_1h_2 + f_3h_0h_1)k_1k_4l_1^2 + f_5h_0^2k_1k_4l_1l_2 + h_1^2k_1k_4l_1l_4 + f_6h_0^3h_2k_2^2l_1^2 + f_6h_0^2h_1h_2k_2^2l_1l_2 + (f_5^2h_0^2 + f_6h_0h_1^2h_2)k_2^2l_1l_3 + (f_5^2h_0^2 + f_6h_0^2h_2^2)k_2^2l_2^2 + (f_5^2h_0h_1 + f_6h_0h_1h_2^2)k_2^2l_2l_3 + (f_5^2h_0h_2 + f_6h_0h_2^3)k_2^2l_3^2 + f_6h_0^2h_1h_2k_2k_3l_1^2 + (f_5^2h_0^2 + f_6h_0h_1^2h_2)k_2k_3l_1l_2 + f_6h_1^3h_2k_2k_3l_1l_3 + (f_5^2h_0h_1 + f_6h_0h_1h_2^2)k_2k_3l_2^2 + (f_5^2h_1^2 + f_6h_1^2h_2^2)k_2k_3l_2l_3 + (f_5^2h_1h_2 + f_6h_1h_2^3)k_2k_3l_3^2 + f_5h_0^2k_2k_4l_1^2 + f_5h_0h_1k_2k_4l_1l_2 + (f_5h_0h_2 + f_5h_1^2)k_2k_4l_1l_3 + (f_5^2h_0^2 + f_6h_0^2h_2^2)k_3^2l_1^2 + f_6h_0h_1h_2^2k_3^2l_1l_2 + f_6h_1^2h_2^2k_3^2l_1l_3 + (f_5^2h_0h_2 + f_6h_0h_2^3)k_3^2l_2^2 + (f_5^2h_1h_2 + f_6h_1h_2^3)k_3^2l_2l_3 + (f_5^2h_2^2 + f_6h_2^4)k_3^2l_3^2 + f_5h_0h_2k_3k_4l_1l_2 + f_5h_1h_2k_3k_4l_1l_3$

$\varphi_{22} = (f_1h_0h_2 + f_3h_0^2)k_1^2l_1l_2 + (f_1h_1h_2 + f_3h_0h_1)k_1^2l_1l_3 + h_0^2k_1^2l_1l_4 + (f_0h_2^2 + f_4h_0^2)k_1^2l_2^2 + (f_1h_2^2 + f_3h_0h_2 + f_5h_0^2)k_1^2l_2l_3 + h_0h_1k_1^2l_2l_4 + (f_2h_2^2 + f_3^2 + f_3h_1h_2 + f_4h_1^2 + f_5h_0h_1 + f_6h_0^2)k_1^2l_3^2 + h_1^2k_1^2l_3l_4 + (f_1h_0h_2 + f_3h_0^2)k_1k_2l_1^2 + f_5h_0^2k_1k_2l_2^2 + (f_5h_0h_2 + f_5h_1^2)k_1k_2l_3^2 + h_1h_2k_1k_2l_3l_4 + (f_1h_1h_2 + f_3h_0h_1)k_1k_3l_1^2 + h_1h_2k_1k_3l_2l_4 + f_5h_1h_2k_1k_3l_3^2 + h_0^2k_1k_4l_1^2 + h_0h_2k_1k_4l_2^2 + h_1h_2k_1k_4l_2l_3 + h_2^2k_1k_4l_3^2 + (f_0h_2^2 + f_4h_0^2)k_2^2l_1^2 + f_5h_0^2k_2^2l_1l_2 + h_0h_2k_2^2l_1l_4 + f_6h_1^2k_2^2l_3^2 + k_2^2l_4^2 + (f_1h_2^2 + f_3h_0h_2 + f_5h_0^2)k_2k_3l_1^2 + h_1h_2k_2k_3l_1l_4 + h_0h_1k_2k_4l_1^2 + h_1h_2k_2k_4l_1l_3 + (f_2h_2^2 + f_3^2 + f_3h_1h_2 + f_4h_1^2 + f_5h_0h_1 + f_6h_0^2)k_3^2l_1^2 + (f_5h_0h_2 + f_5h_1^2)k_3^2l_1l_2 + f_5h_1h_2k_3^2l_1l_3 + h_2^2k_3^2l_1l_4 + f_6h_1^2k_3^2l_2^2 + h_1^2k_3k_4l_1^2 + h_1h_2k_3k_4l_1l_2 + k_4^2l_2^2$

$\varphi_{23} = (f_1h_0h_2 + f_3h_0^2)k_1^2l_2^2 + (f_1h_1h_2 + f_3h_0h_1)k_1^2l_2l_3 + h_0^2k_1^2l_2l_4 + (f_1h_2^2 + f_3h_0h_2 + f_5h_0^2)k_1^2l_3^2 + (f_1h_1h_2 + f_3h_0h_1)k_1k_2l_1l_3 + h_0^2k_1k_2l_1l_4 + f_5h_0^2k_1k_2l_2l_3 + h_0h_1k_1k_2l_2l_4 + h_0h_2k_1k_2l_3l_4 + (f_1h_1h_2 + f_3h_0h_1)k_1k_3l_1l_2 + f_5h_0^2k_1k_3l_2^2 + (h_0h_2 + h_1^2)k_1k_3l_2l_4 + h_1h_2k_1k_3l_3l_4 + h_0^2k_1k_4l_1l_2 + h_0h_1k_1k_4l_2^2 + h_1^2k_1k_4l_2l_3 + h_1h_2k_1k_4l_3^2 + (f_1h_0h_2 + f_3h_0^2)k_2^2l_1^2 + f_5h_0^2k_2^2l_1l_3 + h_0h_1k_2^2l_1l_4 + (f_1h_1h_2 + f_3h_0h_1)k_2k_3l_1^2 + f_5h_0^2k_2k_3l_1l_2 + h_1^2k_2k_3l_1l_4 + h_0^2k_2k_4l_1^2 + h_0h_1k_2k_4l_1l_2 + (h_0h_2 + h_1^2)k_2k_4l_1l_3 + (f_1h_2^2 + f_3h_0h_2 + f_5h_0^2)k_3^2l_1^2 + h_1h_2k_3^2l_1l_4 + h_0h_2k_3k_4l_1l_2 + h_1h_2k_3k_4l_1l_3$

$\varphi_{24} = (f_0h_1^3h_2 + f_1^2h_1h_2 + f_1h_0^2h_2^2 + f_1h_0h_1^2h_2 + f_2h_0^2h_1h_2 + f_3h_0^3h_2 + f_5h_0^4)k_1^2l_1^2 + (f_0h_0h_2^3 + f_0h_1^2h_2^2 + f_1h_0h_1h_2^2 + f_2h_0^2h_2^2 + f_3^2h_0^2 + f_4h_0^3h_2 + f_5h_0^3h_1 + f_6h_0^4)k_1^2l_1l_2 + (f_0h_1h_2^3 + f_1h_0h_2^3 + f_3h_0^2h_2^2 + f_4h_0^2h_1h_2 + f_5h_0^3h_2 + f_5h_0^2h_1^2)k_1^2l_1l_3 + f_6h_0^3h_1k_1^2l_2^2 + f_6h_0^2h_1^2k_1^2l_2l_3 + (f_1h_1h_2 + f_3h_0h_1)k_1^2l_2l_4 + (f_1f_5h_1h_2 + f_3f_5h_0h_1 + f_6h_0^2h_1h_2)k_1^2l_3^2 + (f_0h_0h_2^3 + f_0h_1^2h_2^2 + f_1h_0h_1h_2^2 + f_2h_0^2h_2^2 + f_3^2h_0^2 + f_4h_0^3h_2 + f_5h_0^3h_1 + f_6h_0^4)k_1k_2l_1^2 + (f_0h_1h_2^3 + f_1h_0h_2^3 + f_3h_0^2h_2^2 + f_4h_0^2h_1h_2 + f_5h_0^3h_2 + f_5h_0^2h_1^2)k_1k_2l_1l_2 + (f_0h_2^4 + f_2h_0h_2^3 + f_3^2h_0h_2 + f_3h_0h_1h_2^2 + f_4h_0^2h_2^2 + f_4h_0h_1^2h_2 + f_5h_0h_1^3 + f_6h_0^3h_2 + f_6h_0^2h_1^2)k_1k_2l_1l_3 + (f_1h_1h_2 + f_3h_0h_1)k_1k_2l_1l_4 + (f_1f_5h_0h_2 + f_3f_5h_0^2 + f_6h_0^2h_1^2)k_1k_2l_2^2 + (f_1f_5h_1h_2 + f_3f_5h_0h_1 + f_6h_0h_1^3)k_1k_2l_2l_3 + (f_1h_2^2 + f_3h_0h_2)k_1k_2l_2l_4 + f_6h_0h_1^2h_2k_1k_2l_3^2 + (f_0h_1h_2^3 + f_1h_0h_2^3 + f_3h_0^2h_2^2 + f_4h_0^2h_1h_2 +$

$f_5h_0^3h_2 + f_5h_0^2h_1^2)k_1k_3l_1^2 + (f_0h_2^4 + f_2h_0h_2^3 + f_3^2h_0h_2 + f_3h_0h_1h_2^2 + f_4h_0^2h_2^2 + f_4h_0h_1^2h_2 + f_5h_0h_1^3 + f_6h_0^3h_2 + f_6h_0^2h_1^2)k_1k_3l_1l_2 + (f_1h_2^4 + f_2h_1h_2^3 + f_3^2h_1h_2 + f_3h_0h_2^3 + f_3h_1^2h_2^2 + f_4h_1^3h_2 + f_5h_0^2h_2^2 + f_5h_0h_1^2h_2 + f_5h_1^4 + f_6h_0^2h_1h_2)k_1k_3l_1l_3 + f_6h_0h_1^3k_1k_3l_2^2 + f_6h_1^4k_1k_3l_2l_3 + f_6h_1^3h_2k_1k_3l_3^2 + (f_1h_1h_2 + f_3h_0h_1)k_1k_4l_1l_2 + f_5h_0^2k_1k_4l_2^2 + (h_0h_2 + h_1^2)k_1k_4l_2l_4 + h_1h_2k_1k_4l_3l_4 + f_6h_0^3h_1k_2^2l_1^2 + (f_1f_5h_0h_2 + f_3f_5h_0^2 + f_6h_0^2h_1^2)k_2^2l_1l_2 + f_6h_0h_1^3k_2^2l_1l_3 + f_5h_0^2k_2^2l_1l_4 + f_6h_0^2h_1h_2k_2^2l_2^2 + (f_5^2h_0^2 + f_6h_0h_1^2h_2)k_2^2l_2l_3 + f_5h_0h_1k_2^2l_2l_4 + f_6h_0h_1h_2^2k_2^2l_3^2 + f_5h_0h_2k_2^2l_3l_4 + f_6h_0^2h_1^2k_2k_3l_1^2 + (f_1f_5h_1h_2 + f_3f_5h_0h_1 + f_6h_0h_1^3)k_2k_3l_1l_2 + f_6h_1^4k_2k_3l_1l_3 + (f_5^2h_0^2 + f_6h_0h_1^2h_2)k_2k_3l_2^2 + f_6h_1^3h_2k_2k_3l_2l_3 + (f_5h_0h_2 + f_5h_1^2)k_2k_3l_2l_4 + f_6h_1^2h_2^2k_2k_3l_3^2 + f_5h_1h_2k_2k_3l_3l_4 + (f_1h_1h_2 + f_3h_0h_1)k_2k_4l_1^2 + (f_1h_2^2 + f_3h_0h_2)k_2k_4l_1l_2 + (h_0h_2 + h_1^2)k_2k_4l_1l_4 + f_5h_0h_1k_2k_4l_2^2 + (f_5h_0h_2 + f_5h_1^2)k_2k_4l_2l_3 + h_1h_2k_2k_4l_2l_4 + f_5h_1h_2k_2k_4l_3^2 + h_2^2k_2k_4l_3l_4 + (f_1f_5h_1h_2 + f_3f_5h_0h_1 + f_6h_0^2h_1h_2)k_3^2l_1^2 + f_6h_0h_1^2h_2k_3^2l_1l_2 + f_6h_1^3h_2k_3^2l_1l_3 + f_6h_0h_1h_2^2k_3^2l_2^2 + f_6h_1^2h_2^2k_3^2l_2l_3 + f_5h_1h_2k_3^2l_2l_4 + (f_5^2h_1h_2 + f_6h_1h_2^3)k_3^2l_3^2 + h_1h_2k_3k_4l_1l_4 + f_5h_0h_2k_3k_4l_2^2 + f_5h_1h_2k_3k_4l_2l_3 + h_2^2k_3k_4l_2l_4$

$\varphi_{33} = (f_0h_1^2 + f_1^2 + f_1h_0h_1 + f_2h_0^2)k_1^2l_2^2 + (f_1h_0h_2 + f_3h_0^2)k_1^2l_2l_3 + (f_0h_2^2 + f_4h_0^2)k_1^2l_3^2 + h_0^2k_1^2l_3l_4 + (f_1h_0h_2 + f_3h_0^2)k_1k_2l_1l_3 + h_0^2k_1k_2l_2l_4 + f_5h_0^2k_1k_2l_3^2 + (f_1h_0h_2 + f_3h_0^2)k_1k_3l_1l_2 + h_0^2k_1k_3l_1l_4 + f_5h_0^2k_1k_3l_2l_3 + h_0h_1k_1k_3l_2l_4 + h_0h_2k_1k_3l_3l_4 + h_0^2k_1k_4l_1l_3 + h_0^2k_1k_4l_2^2 + h_0h_1k_1k_4l_2l_3 + h_0h_2k_1k_4l_3^2 + (f_0h_1^2 + f_1^2 + f_1h_0h_1 + f_2h_0^2)k_2^2l_1^2 + h_0^2k_2^2l_1l_4 + f_6h_0^2k_2^2l_3^2 + (f_1h_0h_2 + f_3h_0^2)k_2k_3l_1^2 + f_5h_0^2k_2k_3l_1l_3 + h_0h_1k_2k_3l_1l_4 + h_0^2k_2k_4l_1l_2 + h_0h_1k_2k_4l_1l_3 + (f_0h_2^2 + f_4h_0^2)k_3^2l_1^2 + f_5h_0^2k_3^2l_1l_2 + h_0h_2k_3^2l_1l_4 + f_6h_0^2k_3^2l_2^2 + k_3^2l_4^2 + h_0^2k_3k_4l_1^2 + h_0h_2k_3k_4l_1l_3 + k_4^2l_3^2$

$\varphi_{34} = (f_0h_0^2h_2^2 + f_0h_0h_1^2h_2 + f_0h_1^4 + f_1^2h_0h_2 + f_1^2h_1^2 + f_1h_0h_1^3 + f_2h_0^3h_2 + f_2h_0^2h_1^2 + f_3h_0^3h_1 + f_4h_0^4)k_1^2l_1^2 + (f_0h_1^3h_2 + f_1^2h_1h_2 + f_1h_0^2h_2^2 + f_1h_0h_1^2h_2 + f_2h_0^2h_1h_2 + f_3h_0^3h_2 + f_5h_0^4)k_1^2l_1l_2 + (f_0h_0h_2^3 + f_0h_1^2h_2^2 + f_1h_0h_1h_2^2 + f_2h_0^2h_2^2 + f_3^2h_0^2 + f_4h_0^3h_2 + f_5h_0^3h_1 + f_6h_0^4)k_1^2l_1l_3 + f_6h_0^4k_1^2l_2^2 + f_6h_0^3h_1k_1^2l_2l_3 + (f_1h_0h_2 + f_3h_0^2)k_1^2l_2l_4 + (f_1f_5h_0h_2 + f_3f_5h_0^2 + f_6h_0^3h_2)k_1^2l_3^2 + (f_0h_1^3h_2 + f_1^2h_1h_2 + f_1h_0^2h_2^2 + f_1h_0h_1^2h_2 + f_2h_0^2h_1h_2 + f_3h_0^3h_2 + f_5h_0^4)k_1k_2l_1^2 + (f_0h_0h_2^3 + f_0h_1^2h_2^2 + f_1^2h_2^2 + f_1h_0h_1h_2^2 + f_2h_0^2h_2^2 + f_4h_0^3h_2 + f_5h_0^3h_1 + f_6h_0^4)k_1k_2l_1l_2 + (f_0h_1h_2^3 + f_1h_0h_2^3 + f_3h_0^2h_2^2 + f_4h_0^2h_1h_2 + f_5h_0^3h_2 + f_5h_0^2h_1^2)k_1k_2l_1l_3 + f_6h_0^3h_1k_1k_2l_2^2 + f_6h_0^2h_1^2k_1k_2l_2l_3 + f_6h_0^2h_1h_2k_1k_2l_3^2 + (f_0h_0h_2^3 + f_0h_1^2h_2^2 + f_1h_0h_1h_2^2 + f_2h_0^2h_2^2 + f_3^2h_0^2 + f_4h_0^3h_2 + f_5h_0^3h_1 + f_6h_0^4)k_1k_3l_1^2 + (f_0h_1h_2^3 + f_1h_0h_2^3 + f_3h_0^2h_2^2 + f_4h_0^2h_1h_2 + f_5h_0^3h_2 + f_5h_0^2h_1^2)k_1k_3l_1l_2 + (f_0h_2^4 + f_2h_0h_2^3 + f_3^2h_0h_2 + f_3h_0h_1h_2^2 + f_4h_0^2h_2^2 + f_4h_0h_1^2h_2 + f_5h_0h_1^3 + f_6h_0^3h_2 + f_6h_0^2h_1^2)k_1k_3l_1l_3 + (f_1h_1h_2 + f_3h_0h_1)k_1k_3l_1l_4 + (f_1f_5h_0h_2 + f_3f_5h_0^2 + f_6h_0^2h_1^2)k_1k_3l_2^2 + (f_1f_5h_1h_2 + f_3f_5h_0h_1 + f_6h_0h_1^3)k_1k_3l_2l_3 + (f_1h_2^2 + f_3h_0h_2)k_1k_3l_2l_4 + f_6h_0h_1^2h_2k_1k_3l_3^2 + (f_1h_1h_2 + f_3h_0h_1)k_1k_4l_1l_3 + h_0^2k_1k_4l_1l_4 + f_5h_0^2k_1k_4l_2l_3 + h_0h_1k_1k_4l_2l_4 + h_0h_2k_1k_4l_3l_4 + f_6h_0^4k_2^2l_1^2 + f_6h_0^3h_1k_2^2l_1l_2 + (f_1f_5h_0h_2 + f_3f_5h_0^2 + f_6h_0^2h_1^2)k_2^2l_1l_3 + f_6h_0^3h_2k_2^2l_2^2 + f_6h_0^2h_1h_2k_2^2l_2l_3 +$

$f_5h_0^2k_2^2l_2l_4 + (f_5^2h_0^2 + f_6h_0^2h_2^2)k_2^2l_3^2 + f_6h_0^3h_1k_2k_3l_1^2 + f_6h_0^2h_1^2k_2k_3l_1l_2 + (f_1f_5h_1h_2 + f_3f_5h_0h_1 + f_6h_0h_1^3)k_2k_3l_1l_3 + f_5h_0^2k_2k_3l_1l_4 + f_6h_0^2h_1h_2k_2k_3l_2^2 + (f_5^2h_0^2 + f_6h_0h_1^2h_2)k_2k_3l_2l_3 + f_5h_0h_1k_2k_3l_2l_4 + f_6h_0h_1h_2^2k_2k_3l_3^2 + f_5h_0h_2k_2k_3l_3l_4 + (f_1h_0h_2 + f_3h_0^2)k_2k_4l_1^2 + (f_1h_2^2 + f_3h_0h_2)k_2k_4l_1l_3 + h_0h_1k_2k_4l_1l_4 + f_5h_0^2k_2k_4l_2^2 + f_5h_0h_1k_2k_4l_2l_3 + h_0h_2k_2k_4l_2l_4 + (f_1f_5h_0h_2 + f_3f_5h_0^2 + f_6h_0^3h_2)k_3^2l_1^2 + f_6h_0^2h_1h_2k_3^2l_1l_2 + f_6h_0h_1^2h_2k_3^2l_1l_3 + (f_5^2h_0^2 + f_6h_0^2h_2^2)k_3^2l_2^2 + f_6h_0h_1h_2^2k_3^2l_2l_3 + (f_5^2h_0h_2 + f_5^2h_1^2 + f_6h_0h_2^3)k_3^2l_3^2 + f_5h_1h_2k_3^2l_3l_4 + h_0h_2k_3k_4l_1l_4 + f_5h_0h_2k_3k_4l_2l_3 + f_5h_1h_2k_3k_4l_3^2 + h_2^2k_3k_4l_3l_4$

$\varphi_{44} = (f_0^2h_2^4 + f_0f_1h_1h_2^3 + f_0f_2h_1^2h_2^2 + f_0f_3^2h_1^2 + f_0f_3h_0h_1h_2^2 + f_0f_3h_1^3h_2 + f_0f_4h_1^4 + f_0f_5h_0h_1^3 + f_0f_6h_0^2h_1^2 + f_1^2f_2h_2^2 + f_1^2f_3^2 + f_1^2f_3h_1h_2 + f_1^2f_4h_1^2 + f_1^2f_5h_0h_1 + f_1^2f_6h_0^2 + f_1^2h_0h_2^3 + f_1f_2h_0h_1h_2^2 + f_1f_3^2h_0h_1 + f_1f_3h_0h_1^2h_2 + f_1f_4h_0^2h_1h_2 + f_1f_4h_0h_1^3 + f_1f_5h_0^3h_2 + f_1f_5h_0^2h_1^2 + f_1f_6h_0^3h_1 + f_2^2h_0^2h_2^2 + f_2f_3^2h_0^2 + f_2f_3h_0^2h_1h_2 + f_2f_4h_0^2h_1^2 + f_2f_5h_0^3h_1 + f_2f_6h_0^4 + f_3^2h_0^3h_2 + f_3f_4h_0^3h_1 + f_3f_5h_0^4 + f_4^2h_0^4)k_1^2l_1^2 + (f_0f_5h_0^2h_2^2 + f_0f_5h_0h_1^2h_2 + f_0f_5h_1^4 + f_1^2f_5h_0h_2 + f_1^2f_5h_1^2 + f_1f_5h_0h_1^3 + f_1f_6h_0^3h_2 + f_2f_5h_0^3h_2 + f_2f_5h_0^2h_1^2 + f_3f_5h_0^3h_1 + f_3f_6h_0^4 + f_4f_5h_0^4)k_1^2l_1l_2 + (f_0f_5h_1^3h_2 + f_1^2f_5h_1h_2 + f_1f_5h_0^2h_2^2 + f_1f_5h_0h_1^2h_2 + f_1f_6h_0^2h_1h_2 + f_2f_5h_0^2h_1h_2 + f_3f_5h_0^3h_2 + f_3f_6h_0^3h_1 + f_5^2h_0^4)k_1^2l_1l_3 + (f_1^2h_2^2 + f_3^2h_0^2)k_1^2l_1l_4 + (f_0f_6h_0^2h_2^2 + f_0f_6h_1^4 + f_1^2f_6h_1^2 + f_1f_6h_0^2h_1h_2 + f_1f_6h_0h_1^3 + f_2f_6h_0^2h_1^2 + f_3f_6h_0^3h_1 + f_4f_6h_0^4)k_1^2l_2^2 + (f_1f_6h_0^2h_2^2 + f_3f_6h_0^3h_2 + f_5f_6h_0^4)k_1^2l_2l_3 + (f_0f_6h_1^2h_2^2 + f_1f_6h_0h_1h_2^2 + f_2f_6h_0^2h_2^2 + f_3^2f_6h_0^2 + f_6^2h_0^4)k_1^2l_3^2 + (f_0f_5h_0^2h_2^2 + f_0f_5h_0h_1^2h_2 + f_0f_5h_1^4 + f_1^2f_5h_0h_2 + f_1^2f_5h_1^2 + f_1f_5h_0h_1^3 + f_1f_6h_0^3h_2 + f_2f_5h_0^3h_2 + f_2f_5h_0^2h_1^2 + f_3f_5h_0^3h_1 + f_3f_6h_0^4 + f_4f_5h_0^4)k_1k_2l_1^2 + (f_0f_5h_1^3h_2 + f_1^2f_5h_1h_2 + f_1f_5h_0^2h_2^2 + f_1f_5h_0h_1^2h_2 + f_1f_6h_0^2h_1h_2 + f_2f_5h_0^2h_1h_2 + f_3f_5h_0^3h_2 + f_3f_6h_0^3h_1 + f_5^2h_0^4)k_1k_2l_1l_2 + (f_0f_5h_0h_2^3 + f_0f_5h_1^2h_2^2 + f_1f_5h_0h_1h_2^2 + f_1f_6h_0h_1^2h_2 + f_2f_5h_0^2h_2^2 + f_3^2f_5h_0^2 + f_3f_6h_0^3h_1 + f_4f_5h_0^3h_2 + f_5^2h_0^3h_1 + f_5f_6h_0^4)k_1k_2l_1l_3 + (f_1f_6h_0^2h_2^2 + f_3f_6h_0^3h_2 + f_5f_6h_0^4)k_1k_2l_2^2 + (f_1f_6h_0h_1h_2^2 + f_3f_6h_0^2h_1h_2 + f_5f_6h_0^3h_1)k_1k_2l_2l_3 + (f_1f_5h_0h_2 + f_3f_5h_0^2)k_1k_2l_2l_4 + (f_1f_5^2h_0h_2 + f_1f_6h_0h_2^3 + f_3f_5^2h_0^2 + f_3f_6h_0^2h_2^2 + f_5f_6h_0^3h_2)k_1k_2l_3^2 + (f_0f_5h_1^3h_2 + f_1^2f_5h_1h_2 + f_1f_5h_0^2h_2^2 + f_1f_5h_0h_1^2h_2 + f_1f_6h_0^2h_1h_2 + f_2f_5h_0^2h_1h_2 + f_3f_5h_0^3h_2 + f_3f_6h_0^3h_1 + f_5^2h_0^4)k_1k_3l_1^2 + (f_0f_5h_0h_2^3 + f_0f_5h_1^2h_2^2 + f_1f_5h_0h_1h_2^2 + f_1f_6h_0h_1^2h_2 + f_2f_5h_0^2h_2^2 + f_3^2f_5h_0^2 + f_3f_6h_0^2h_1^2 + f_4f_5h_0^3h_2 + f_5^2h_0^3h_1 + f_5f_6h_0^4)k_1k_3l_1l_2 + (f_0f_5h_1h_2^3 + f_1f_5h_0h_2^3 + f_1f_6h_1^3h_2 + f_3f_5h_0^2h_2^2 + f_3f_6h_0h_1^3 + f_4f_5h_0^2h_1h_2 + f_5^2h_0^3h_2 + f_5^2h_0^2h_1^2)k_1k_3l_1l_3 + (f_1f_6h_0h_1h_2^2 + f_3f_6h_0^2h_1h_2 + f_5f_6h_0^3h_1)k_1k_3l_2^2 + (f_1f_6h_1^2h_2^2 + f_3f_6h_0h_1^2h_2 + f_5f_6h_0^2h_1^2)k_1k_3l_2l_3 + (f_1f_5h_1h_2 + f_3f_5h_0h_1)k_1k_3l_2l_4 + (f_1f_5^2h_1h_2 + f_1f_6h_1h_2^3 + f_3f_5^2h_0h_1 + f_3f_6h_0h_1h_2^2 + f_5f_6h_0^2h_1h_2)k_1k_3l_3^2 + (f_1^2h_2^2 + f_3^2h_0^2)k_1k_4l_1^2 + (f_1h_1h_2 + f_3h_0h_1)k_1k_4l_1l_4 + f_5h_0^2k_1k_4l_2l_4 + f_5^2h_0^2k_1k_4l_3^2 + (f_0f_6h_0^2h_2^2 + f_0f_6h_1^4 + f_1^2f_6h_1^2 + f_1f_6h_0^2h_1h_2 + f_1f_6h_0h_1^3 + f_2f_6h_0^2h_1^2 + f_3f_6h_0^3h_1 + f_4f_6h_0^4)k_2^2l_1^2 + (f_1f_6h_0^2h_2^2 + f_3f_6h_0^3h_2 + f_5f_6h_0^4)k_2^2l_1l_2 + (f_1f_6h_0h_1h_2^2 + f_3f_6h_0^2h_1h_2 + f_5f_6h_0^3h_1)k_2^2l_1l_3 + (f_0f_5^2h_1^2 + f_0f_6h_1^2h_2^2 + f_1^2f_5^2 + f_1^2f_6h_2^2 + f_1f_5^2h_0h_1 + f_1f_6h_0h_1h_2^2 + f_2f_5^2h_0^2 +$

$f_2f_6h_0^2h_2^2 + f_6^2h_0^4)k_2^2l_2^2 + (f_1f_5^2h_0h_2 + f_1f_6h_0h_2^3 + f_3f_5^2h_0^2 + f_3f_6h_0^2h_2^2 + f_5f_6h_0^3h_2)k_2^2l_2l_3 + (f_0f_5^2h_2^2 + f_0f_6h_2^4 + f_4f_5^2h_0^2 + f_4f_6h_0^2h_2^2 + f_5f_6h_0^2h_1h_2 + f_6^2h_0^2h_1^2)k_2^2l_3^2 + f_5^2h_0^2k_2^2l_3l_4 + (f_1f_6h_0^2h_2^2 + f_3f_6h_0^3h_2 + f_5f_6h_0^4)k_2k_3l_1^2 + (f_1f_6h_0h_1h_2^2 + f_3f_6h_0^2h_1h_2 + f_5f_6h_0^3h_1)k_2k_3l_1l_2 + (f_1f_6h_1^2h_2^2 + f_3f_6h_0h_1^2h_2 + f_5f_6h_0^2h_1^2)k_2k_3l_1l_3 + (f_1f_5^2h_0h_2 + f_1f_6h_0h_2^3 + f_3f_5^2h_0^2 + f_3f_6h_0^2h_2^2 + f_5f_6h_0^3h_2)k_2k_3l_2^2 + (f_1f_5^2h_1h_2 + f_1f_6h_1h_2^3 + f_3f_5^2h_0h_1 + f_3f_6h_0h_1h_2^2 + f_5f_6h_0^2h_1h_2)k_2k_3l_2l_3 + f_5^2h_0^2k_2k_3l_2l_4 + (f_1f_5^2h_2^2 + f_1f_6h_2^4 + f_3f_5^2h_0h_2 + f_3f_6h_0h_2^3 + f_5^3h_0^2 + f_5f_6h_0^2h_2^2)k_2k_3l_3^2 + (f_1f_5h_0h_2 + f_3f_5h_0^2)k_2k_4l_1l_2 + (f_1f_5h_1h_2+f_3f_5h_0h_1)k_2k_4l_1l_3+f_5h_0^2k_2k_4l_1l_4+f_5^2h_0^2k_2k_4l_2l_3+f_5^2h_0h_1k_2k_4l_3^2+f_5h_0h_2k_2k_4l_3l_4+(f_0f_6h_1^2h_2^2+f_1f_6h_0h_1h_2^2+f_2f_6h_0^2h_2^2+f_3^2f_6h_0^2+f_6^2h_0^4)k_3^2l_1^2+(f_1f_5^2h_0h_2+f_1f_6h_0h_2^3+f_3f_5^2h_0^2+f_3f_6h_0^2h_2^2+f_5f_6h_0^3h_2)k_3^2l_1l_2+(f_1f_5^2h_1h_2+f_1f_6h_1h_2^3+f_3f_5^2h_0h_1+f_3f_6h_0h_1h_2^2+f_5f_6h_0^2h_1h_2)k_3^2l_1l_3+f_5^2h_0^2k_3^2l_1l_4+(f_0f_5^2h_2^2+f_0f_6h_2^4+f_4f_5^2h_0^2+f_4f_6h_0^2h_2^2+f_5f_6h_0^2h_1h_2+f_6^2h_0^2h_1^2)k_3^2l_2^2+(f_1f_5^2h_2^2+f_1f_6h_2^4+f_3f_5^2h_0h_2+f_3f_6h_0h_2^3+f_5^3h_0^2+f_5f_6h_0^2h_2^2)k_3^2l_2l_3+f_5^2h_0h_1k_3^2l_2l_4+(f_2f_5^2h_2^2+f_2f_6h_2^4+f_3^2f_5^2+f_3^2f_6h_2^2+f_3f_5^2h_1h_2+f_3f_6h_1h_2^3+f_4f_5^2h_1^2+f_4f_6h_1^2h_2^2+f_5^3h_0h_1+f_5^2f_6h_0^2+f_5f_6h_0h_1h_2^2+f_5f_6h_1^3h_2+f_6^2h_0^2h_2^2+f_6^2h_1^4)k_3^2l_3^2+f_5^2h_1^2k_3^2l_3l_4+f_5^2h_0^2k_3k_4l_2^2+f_5h_0h_2k_3k_4l_2l_4+f_5^2h_1^2k_3k_4l_3^2+f_5h_1h_2k_3k_4l_3l_4+k_4^2l_4^2$

Let us give now the formulas for the multiplication-by-2 map.

$\delta_1 = (f_1^2h_2^2 + f_3^2h_0^2 + f_6h_0^4)k_1^4 + f_6h_0^2h_1^2k_1^2k_2^2 + f_6h_1^4k_1^2k_3^2 + h_1^2k_1^2k_4^2 + (f_5^2h_0^2 + f_6h_0^2h_2^2)k_2^4 + (f_5^2h_1^2 + f_6h_1^2h_2^2)k_2^2k_3^2 + (f_5^2h_2^2 + f_6h_2^4)k_3^4$

$\delta_2 = (f_0h_1^3h_2+f_1^2h_1h_2+f_1h_0^2h_2^2+f_1h_0h_1^2h_2+f_2h_0^2h_1h_2+f_3h_0^3h_2+f_5h_0^4)k_1^4+(f_0h_1h_2^3 + f_1h_0h_2^3 + f_3h_0^2h_2^2 + f_4h_0^2h_1h_2 + f_5h_0^3h_2 + f_5h_0^2h_1^2)k_1^2k_2^2 + (f_1h_2^4 + f_2h_1h_2^3 + f_3^2h_1h_2 + f_3h_0h_2^3 + f_3h_1^2h_2^2 + f_4h_1^3h_2 + f_5h_0^2h_2^2 + f_5h_0h_1^2h_2 + f_5h_1^4 + f_6h_0^2h_1h_2)k_1^2k_3^2+f_6h_0^2h_1h_2k_2^4+f_6h_1^3h_2k_2^2k_3^2+h_1h_2k_2^2k_4^2+(f_5^2h_1h_2+f_6h_1h_2^3)k_3^4$

$\delta_3 = (f_0h_0^2h_2^2 + f_0h_0h_1^2h_2 + f_0h_1^4 + f_1^2h_0h_2 + f_1^2h_1^2 + f_1h_0h_1^3 + f_2h_0^3h_2 + f_2h_0^2h_1^2 + f_3h_0^3h_1 + f_4h_0^4)k_1^4 + (f_0h_0h_2^3 + f_0h_1^2h_2^2 + f_1^2h_2^2 + f_1h_0h_1h_2^2 + f_2h_0^2h_2^2 + f_4h_0^3h_2 + f_5h_0^3h_1 + f_6h_0^4)k_1^2k_2^2 + (f_0h_2^4 + f_2h_0h_2^3 + f_3^2h_0h_2 + f_3h_0h_1h_2^2 + f_4h_0^2h_2^2 + f_4h_0h_1^2h_2 + f_5h_0h_1^3 + f_6h_0^3h_2 + f_6h_0^2h_1^2)k_1^2k_3^2 + h_0^2k_1^2k_4^2 + f_6h_0^3h_2k_2^4 + (f_5^2h_0^2 + f_6h_0h_1^2h_2)k_2^2k_3^2 + h_0h_2k_2^2k_4^2 + (f_5^2h_0h_2 + f_5^2h_1^2 + f_6h_0h_2^3)k_3^4 + h_2^2k_3^2k_4^2$

$\delta_4 = (f_0^2h_2^4+f_0f_1h_1h_2^3+f_0f_2h_1^2h_2^2+f_0f_3^2h_1^2+f_0f_3h_0h_1h_2^2+f_0f_3h_1^3h_2+f_0f_4h_1^4+f_0f_5h_0h_1^3 + f_0f_6h_0^2h_1^2 + f_1^2f_2h_2^2 + f_1^2f_3^2 + f_1^2f_3h_1h_2 + f_1^2f_4h_1^2 + f_1^2f_5h_0h_1 + f_1^2f_6h_0^2 + f_1^2h_0h_2^3 + f_1f_2h_0h_1h_2^2 + f_1f_3^2h_0h_1 + f_1f_3h_0h_1^2h_2 + f_1f_4h_0^2h_1h_2 + f_1f_4h_0h_1^3+f_1f_5h_0^3h_2+f_1f_5h_0^2h_1^2+f_1f_6h_0^3h_1+f_2^2h_0^2h_2^2+f_2f_3^2h_0^2+f_2f_3h_0^2h_1h_2+f_2f_4h_0^2h_1^2 + f_2f_5h_0^3h_1 + f_2f_6h_0^4 + f_3^2h_0^3h_2 + f_3f_4h_0^3h_1 + f_3f_5h_0^4 + f_4^2h_0^4)k_1^4 + (f_0f_5h_1^3h_2+f_1^2f_5h_1h_2+f_1f_5h_0^2h_2^2+f_1f_5h_0h_1^2h_2+f_1f_6h_0^2h_1h_2+f_2f_5h_0^2h_1h_2+f_3f_5h_0^3h_2 + f_3f_6h_0^3h_1 + f_5^2h_0^4)k_1^2k_2^2 + (f_0f_5h_1h_2^3 + f_1f_5h_0h_2^3 + f_1f_6h_1^3h_2+$

$f_3f_5h_0^2h_2^2 + f_3f_6h_0h_1^3 + f_4f_5h_0^2h_1h_2 + f_5^2h_0^3h_2 + f_5^2h_0^2h_1^2)k_1^2k_3^2 + (f_1h_1h_2 + f_3h_0h_1)k_1^2k_4^2 + (f_0f_5^2h_1^2 + f_0f_6h_1^2h_2^2 + f_1^2f_5^2 + f_1^2f_6h_2^2 + f_1f_5^2h_0h_1 + f_1f_6h_0h_1h_2^2 + f_2f_5^2h_0^2 + f_2f_6h_0^2h_2^2 + f_6^2h_0^4)k_2^4 + (f_1f_5^2h_1h_2 + f_1f_6h_1h_2^3 + f_3f_5^2h_0h_1 + f_3f_6h_0h_1h_2^2 + f_5f_6h_0^2h_1h_2)k_2^2k_3^2 + (f_2f_5^2h_2^2 + f_2f_6h_2^4 + f_3^2f_5^2 + f_3^2f_6h_2^2 + f_3f_5^2h_1h_2 + f_3f_6h_1h_2^3 + f_4f_5^2h_1^2 + f_4f_6h_1^2h_2^2 + f_5^3h_0h_1 + f_5^2f_6h_0^2 + f_5f_6h_0h_1h_2^2 + f_5f_6h_1^3h_2 + f_6^2h_0^2h_2^2 + f_6^2h_1^4)k_3^4 + f_5h_1h_2k_3^2k_4^2 + k_4^4$

References

[Cas-Fly 96] J. W. S. Cassels, E. V. Flynn, *Prolegomena to a middlebrow Arithmetic of Curves of Genus 2*, LMS Lecture Note Series, **230**, Cambridge University Press (1996).

[Duq 05] S. Duquesne, *Montgomery scalar multiplication for genus 2 curves*, ANTS VI, Lecture Notes in Comput. Sci. **3076** (2004), pp. 153–168.

[Fly 90] E. V. Flynn, *The Jacobian and formal group of a curve of genus 2 over an arbitrary groud field*, Math. Proc. Camb. Phil. Soc., **107** (1990), pp. 425–441.

[Fly 93] E. V. Flynn, *The group law on the Jacobian of a curve of genus* 2, J. reine angew. Math., **439** (1993), pp. 45–69.

[Fly 95] E. V. Flynn, *An explicit theory of heights*, Trans. Amer. Math. Soc., **347** (1995), pp. 3003–3015.

[Fly 97] E. V. Flynn, *A flexible method for applying Chabauty's Thorem*, Compositio Math., **105** (1997), pp. 79–94.

[Fly-Sma 97] E. V. Flynn, N. P. Smart, *Canonical height on the Jacobians of curves of genus 2 and the infinite descent*, Acta Artih., **79:4** (1997), pp. 333–352.

[Lan 82] S. Lang, *Introduction to Algebraic and Abelian Functions*, 2nd edition, Graduate Texts in Math., **89** (1982).

[Sma-Sik 99] N. Smart, S. Siksek, *A fast Diffie-Hellman protocol in genus 2*, Journal of Cryptology, **12** (1999), pp. 67–73.