Elliptic periods for finite fields. Finite Fields and their Applications, 15(1):1-22, January 2009.

Elliptic periods for finite fields*

Jean-Marc Couveignes[†] and Reynald Lercier[‡§]

Abstract

We construct two new families of basis for finite field extensions. Bases in the first family, the so-called *elliptic bases*, are not quite normal bases, but they allow very fast Frobenius exponentiation while preserving sparse multiplication formulas. Bases in the second family, the so-called *normal elliptic bases* are normal bases and allow fast (quasi-linear) arithmetic. We prove that all extensions admit models of this kind.

1 Introduction

The main computational advantage of normal basis for a finite field extension $\mathbb{F}_{q^d}/\mathbb{F}_q$ is that they allow fast exponentiation by q since it corresponds to a cyclic shift of coordinates, and it can be computed in time $O(d)$. There is a concern however about how difficult is multiplication in this context.

Let α and β be two elements in $\mathbb{F}_{q^d}$ with coordinates $\vec{\alpha} = (\alpha_i)_{0\leqslant i\leqslant d-1}$ and $\vec{\beta} = (\beta_i)_{0\leqslant i\leqslant d-1}$ in the given normal basis. Let $(\gamma_i)_{0\leqslant i\leqslant d-1}$ be the coordinates of the product $\alpha\times\beta$. Each γ_i is a bilinear form in $\vec{\alpha}$ and $\vec{\beta}$. The number of non-zero terms in γ_i does not depend on i because the d corresponding tensors are cyclic shifts of each others. This number of terms is called the *complexity* $\mathcal{C}$ of the normal basis. Multiplication with the straightforward algorithm can be done with $2d\mathcal{C}$ operations ($d\mathcal{C}$ when coefficients of the bilinear forms γ_i are all ± 1). It was shown by Mullin, Onyszchuk, Vanstone and Wilson [15] that the complexity $\mathcal{C}$ is at least $2d-1$. This bound is reached by the so-called optimal normal bases. But such optimal normal bases only exist for very special extensions. As a general fact, normal bases with bounded complexity are not known to exist, unless the degree d takes very special and sparse values.

*January 10, 2015— Research supported by the French Délégation Générale pour l'Armement, Centre d'Électronique de l'Armement and by the Agence Nationale de la Recherche (projet blanc ALGOL).

†Institut de Mathématiques de Toulouse, Université de Toulouse et CNRS, Département de Mathématiques et Informatique, Université Toulouse 2, 5 allées Antonio Machado, 31058 Toulouse cédex 9.

‡DGA/CÉLAR, La Roche Marguerite, F-35174 Bruz.

§IRMAR, Université de Rennes 1, Campus de Beaulieu, F-35042 Rennes.

Normal bases with low complexity usually are constructed using *Gauss periods* as in work by Ash, Blake and Vanstone [2] or Gao and Lenstra [11]. The construction uses r-th roots of unity where $r = kd + 1$ is prime. It requires that q generates the unique quotient of order d of $(\mathbb{Z}/r\mathbb{Z})^*$. The parameter k is very important and should be kept as small as possible, because the complexity of the normal basis is bounded by $(d-1)k + d$ and is not expected to be much smaller [10, Theorem 4.1.4]. Optimal normal bases occur when $k = 1$ or $k = 2$. This corresponds to very sparse values of d. In general, for q a prime, assuming the Extended Riemann Hypothesis, it has been shown by Adleman and Lenstra [1] that there exists a k and a r as above with $r = O(d^4(\log(dq))^2)$. This is unfortunately of no use when bounding the complexity. In some cases, there is no k at all [22, Satz 3.3.4]. We shall not survey all the variants and improvements for this method. We just quote works by Christopoulou, Garefalakis, Panario and Thomson [7] where traces of optimal normal bases are shown to have a reasonable complexity in some special cases. Wan and Zhou show [21] that the dual of type I optimal normal bases have good complexity too.

Gao, von zur Gathen and Panario show [12] that fast multiplication methods (like FFT) can be adapted to normal bases constructed with Gauss periods. They give a multiplication algorithm in such a normal basis with complexity $O(dk\log(dk)\log|\log(dk)|)$. This is a considerable progress for Gauss normal bases with bounded k. But in the general case, k being only upperbounded by $O(d^3(\log(dq))^2)$, this is just too large.

In his thesis [10] Gao presented a new way of constructing normal bases with low complexity. In Gao's construction, the Lucas torus and its isogenies play an important, though implicit, role. Gao thus constructs more normal bases with low complexity. In our work, we consider the remaining algebraic groups of dimension one: elliptic curves. Since there are many elliptic curves, we can enlarge significantly the number of cases where a normal basis with fast multiplication exists.

In order to state our results, we shall need the following definition where v_ℓ stands for the valuation associated to the prime ℓ.

Definition 1 *Let p be a prime and q a power of p. Let $d \geqslant 2$ be an integer.*
We denote by d_q the unique positive integer such that for every prime ℓ

- $v_\ell(d_q) = v_\ell(d)$ *if ℓ is prime to $q-1$,*
- $v_\ell(d_q) = 0$ *if $v_\ell(d) = 0$,*
- $v_\ell(d_q) = \max(2v_\ell(q-1)+1, 2v_\ell(d))$ *if ℓ divides both $q-1$ and d.*

For example, if $d = 14$ and $q = 654323$ then $q - 1 = 2.19.67.257$ and $d_q = 2^3.7$.

Note that $d_q = d$ whenever d is prime to $q - 1$.

We now can state our first result.

Theorem 1 *To every couple (q, d) with q a prime power and $d \geqslant 2$ an integer and $d_q \leqslant q^{\frac{1}{2}}$, one can associate a normal basis $\Theta(q, d)$ of the degree d extension of $\mathbb{F}_q$ such that the following holds:*

- *There exist a positive constant K and an algorithm that multiplies two elements given in the basis $\Theta(q,d)$ at the expense of $5d^2+2d$ multiplications and $5d^2+4d$ additions/subtractions in $\mathbb{F}_q$. The amount of necessary memory is $\leqslant Kd\log q$ bits.*

There is also a fast arithmetic version of Theorem 1.

Theorem 2 *To every couple (q,d) with q a prime power and $d \geq 2$ an integer and $d_q \leqslant q^{\frac{1}{2}}$, one can associate a normal basis $\Theta(q,d)$ of the degree d extension of $\mathbb{F}_q$ such that the following holds:*

- *There exist a positive constant K and an algorithm that multiplies two elements given in the basis $\Theta(q,d)$ at the expense of $Kd\log d \log|\log d|$ operations in $\mathbb{F}_q$.*
- *There exists an algorithm that divides two elements given in the basis $\Theta(q,d)$ at the expense of*

$$Kd(\log d)^2 \log|\log d|$$

operations in $\mathbb{F}_q$.

The basis $\Theta(q,d)$ that appears in Theorem 1 and Theorem 2 has a multiplication tensor that mainly consists of 5 convolution products. We also construct a basis $\Omega(q,d)$ having a sparse multiplication tensor. Sparsity is useful when using such constrained devices as circuits. Further, this basis $\Omega(q,d)$ allows a faster elementary multiplication algorithm than $\Theta(q,d)$. It is not quite a normal basis but exponentiation by q is still done in linear time.

Theorem 3 *To every couple (q,d) with q a prime power and $d \geq 2$ an integer and $d_q \leqslant 2q^{\frac{1}{2}}$, one can associate a basis $\Omega(q,d)$ of the degree d extension of $\mathbb{F}_q$ such that the following holds:*

- *There exist a positive constant K and an algorithm that computes the q-th power of an element given in basis $\Omega(q,d)$ at the expense of $d-1$ multiplications and $2d-3$ additions in $\mathbb{F}_q$. The amount of necessary memory is $\leqslant Kd\log q$ bits.*
- *There exists an algorithm that multiplies two elements given in basis $\Omega(q,d)$ at the expense of $(31d^2+6d)/12$ multiplications, $d^2/12$ inverses and $(37d^2+30d)/12$ additions/subtractions in $\mathbb{F}_q$. The amount of necessary memory is $\leqslant Kd\log q$ bits.*

The following result is valid without any restriction.

Theorem 4 *To every couple (q,d), one can associate a model $\Xi(q,d)$ of the degree d extension of $\mathbb{F}_q$ such that the following holds :*

There exists a positive constant K such that the following is true :

- *Elements in $\mathbb{F}_{q^d}$ are represented by vectors with less than $Kd(\log d)^2(\log(\log d))^2$ components in $\mathbb{F}_q$.*

- *Addition (resp. substraction) of two elements in* $\mathbb{F}_{q^d}$ *requires less than*

$$Kd(\log d)^2(\log(\log d))^2$$

  additions (resp. substractions) in $\mathbb{F}_q$.
- *Exponentiation by* q *consists in a circular shift of the the coordinates.*
- *There exists an algorithm that multiplies two elements at the expense of*

$$Kd(\log d)^3|\log(\log d)|^3$$

  multiplications/additions/substractions in $\mathbb{F}_q$.
- *There exists an algorithm that divides two elements at the expense of*

$$Kd(\log d)^4|\log(\log d)|^3$$

  multiplications/additions/substractions in $\mathbb{F}_q$.

So, for every finite field extension, there exists a model that allows both fast multiplication and fast application of the Frobenius automorphism.

In Section 2, we recall simple relations between low degree elliptic functions. We show in Section 3 that evaluation of such functions at a well chosen divisor produces an almost normal basis for the residue field. Relations between elliptic functions result in nice multiplication formulas in this basis. Such bases have similar properties to those constructed by Gao in his thesis: they have low complexity. This is shown in Subsection 3.3. In Section 4, we construct normal bases allowing fast (quasi-linear) multiplication. We show in Section 5 that an elliptic basis exists for any degree d extension of $\mathbb{F}_q$ provided d is not too large. We explain in Subsection 5.2 what to do when d is large. In Subsection 5.4, we introduce a polynomial basis that can be related efficiently to the elliptic (normal) basis. We deduce a fast inversion algorithm for elliptic normal bases.

We further support our claims with extensive experiments using the computational algebra system MAGMA [4]. We developed for this task a package, named ELLBASIS, the sources of which are available on the web page of the second author.

Acknowledgments: We thank Cécile Dartyge, Guillaume Hanrot, Gerald Tenenbaum and Jie Wu for pointing Iwaniec's result on Jacobsthal's problem to us.

2 Linear and quadratic relations among elliptic functions

In this section, we study the simplest elliptic functions: those with degree 2. We prove simple linear and quadratic relations between these functions. The monography [19] by J. Silverman contains all the necessary background about elliptic curves.

Let $\mathbf{K}$ be a field and let E be an elliptic curve over $\mathbf{K}$. We assume E is given by some Weierstrass equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \,.$$

We set $x = X/Z$, $y = Y/Z$ and $z = -x/y = -X/Y$, and we find

$$\begin{aligned} x &= \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3z + O(z^2)\,, \\ y &= -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + O(z)\,. \end{aligned}$$

The involution $P = (x, y) \mapsto -P = (x, -y - a_1x - a_3)$ transforms z into

$$z(-P) = \frac{x}{y + a_1x + a_3} = -z - a_1z^2 - a_1^2z^3 - (a_1^3 + a_3)z^4 + O(z^5)\,.$$

If A is a geometric point on E, we denote by τ_A the translation by A. We denote by $z_A = z\circ\tau_{-A}$ the composition of z with the translation by $-A$. We define x_A and y_A in a similar way. The composition of z_A with the involution fixing A is $-z_A - a_1z_A^2 - a_1^2z_A^3 - (a_1^3 + a_3)z_A^4 + O(z_A^5)$. The composition of $1/z_A$ with the involution fixing A is $-1/z_A + a_1 + a_3z_A^2 + O(z_A^3)$.

If A and B are two distinct geometric points on E, we denote by $u_{A,B}$ the function on E defined as

$$u_{A,B} = \frac{y_A - y(A - B)}{x_A - x(A - B)}\,.$$

It has polar divisor $-[A] - [B]$. It is invariant by the involution exchanging A and B,

$$u_{A,B}(A + B - P) = u_{A,B}(P)\,.$$

Its Taylor expansion at A is $u_{A,B} = -1/z_A - x_A(B)z_A + (y_A(B) + a_3){z_A}^2 + O(z_A^3)\,.$

If C is any third geometric point, we set $\Gamma(A, B, C) = u_{A,B}(C)$. This is the slope of the secant (resp. tangent) to E going through $C - A$ and $A - B$. It is well defined for any three points A, B, C such that $\#\{A, B, C\} \geqslant 2$. It is finite if and only if $\#\{A, B, C\} = 3$. We check

$$\Gamma(-A, -B, -C) = -\Gamma(A, B, C) - a_1. \tag{1}$$

The Taylor expansions of $u_{A,B}$ at A and B are

$$\begin{aligned} u_{A,B} &= -\frac{1}{z_A} - x_A(B)z_A + (y_A(B) + a_3)z_A^2 + O(z_A^3) \\ &= \frac{1}{z_B} - a_1 + x_A(B)z_B + (y_A(B) + a_1x_A(B))z_B^2 + O(z_B^3). \end{aligned}$$

As a consequence $u_{B,A} = -u_{A,B} - a_1$, $x_B(A) = x_A(B)$ and $y_B(A) = -y_A(B) - a_1 x_A(B) - a_3$ and examination of Taylor expansions at A, B and C shows that

$$u_{A,B} + u_{B,C} + u_{C,A} = \Gamma(A, B, C) - a_1 \tag{2}$$

and

$$\Gamma(A, B, C) = u_{B,C}(A) = u_{C,A}(B) = u_{A,B}(C) = -u_{B,A}(C) - a_1. \tag{3}$$

We deduce

$$u_{B,C} = u_{B,C}(A) - (x_A(C) - x_A(B))z_A + (y_A(C) - y_A(B))z_A^2 + O(z_A^3).$$

By comparison of Taylor expansions at A, B and C we prove

$$u_{A,B}u_{A,C} = x_A + u_{B,C}(A)u_{B,C} - u_{B,C}^2(A) - a_1 u_{A,B} + x_A(B) + x_A(C) + a_2$$

or, derived from Equation (2),

$$u_{A,B}u_{A,C} = x_A + \Gamma(A, B, C)u_{A,C} + \Gamma(A, C, B)u_{A,B} + a_2 + x_A(B) + x_A(C). \tag{4}$$

Indeed,

$$\begin{aligned}(-\frac{1}{z_A} - x_A(B)z_A + (y_A(B) + a_3)z_A^2)(-\frac{1}{z_A} - x_A(C)z_A + (y_A(C) + a_3)z_A^2) + O(z_A^2) \\ = \frac{1}{z_A^2} + x_A(B) + x_A(C) - (y_A(B) + y_A(C) + 2a_3)z_A + O(z_A^2).\end{aligned}$$

So, $u_{A,B}u_{A,C} - x_A + a_1 u_{A,B} - x_A(B) - x_A(C) - a_2$ cancels at A and its polar divisor is $-[B] - [C]$. Its residue at B is $-u_{A,B}(C)$. This proves Equation (4).

In the same vein, we prove

$$u_{A,B}^2 = x_A + x_B - a_1 u_{A,B} + x_A(B) + a_2\,. \tag{5}$$

Indeed,

$$\begin{aligned}u_{A,B}^2 = (-\frac{1}{z_A} - x_A(B)z_A + (y_A(B) + a_3)z_A^2)^2 + O(z_A^2) \\ = \frac{1}{z_A^2} + 2x_A(B) - 2(y_A(B) + a_3)z_A + O(z_A^2)\end{aligned}$$

and similarly

$$u_{A,B}^2 = (\frac{1}{z_B} - a_1 + x_A(B)z_B + (y_A(B) + a_1 x_A(B))z_B^2)^2 + O(z_B^2)$$
$$= \frac{1}{z_B^2} - \frac{2a_1}{z_B} + a_1^2 + 2x_A(B) + 2y_A(B)z_B + O(z_B^2)\,.$$

So $u_{A,B}^2 - x_A - x_B + a_1 u_{A,B} = x_A(B) + a_2$.

Here are more explicit formulas. For A and B distinct,

$$u_{A,B} = \begin{cases} -u_{O,A} - a_1 & \text{if } B = O\,, \\ \frac{y + y(B) + a_1\, x(B) + a_3}{x - x(B)} & \text{if } A = O, \\ \frac{a_1\, y(A) - 3\, x(A)^2 - 2\, a_2\, x(A) - a_4}{2\, y(A) + a_1\, x(A) + a_3} - \frac{a_1 x + a_3 + 2\, y(A)}{x - x(A)} & \text{if } B = -A\,, \\ \frac{y(B) + y(A) + a_1\, x(A) + a_3}{x(B) - x(A)} & \\ \quad + \frac{(x(B) - x(A))(y + a_1 x + a_3) + (y(B) - y(A))x + y(A)x(B) - y(B)x(A)}{(x - x(A))(x - x(B))} & \text{otherwise.} \end{cases}$$

Especially, when $A = O$, provided B and C are distinct and non-zero, we have

$$\Gamma(O, B, C) = \begin{cases} -\frac{3\, x(B)^2 + a_1\, (y(B) + a_1 x(B) + a_3) + 2\, a_2\, x(B) + a_4}{2\, y(B) + a_1\, x(B) + a_3} & \text{if } C = -B\,, \\ \frac{y(C) + y(B) + a_1 x(B) + a_3}{x(C) - x(B)} & \text{otherwise.} \end{cases} \qquad (6)$$

These formulae can be derived from the definition of $\Gamma(A, B, C)$ as a slope, using the explicit form of the addition law on elliptic curves.

3 Elliptic bases for finite fields extensions

In this section, we use elliptic functions to construct interesting bases for many finite field extensions.

Assume E is an elliptic curve over a finite field $\mathbf{K} = \mathbb{F}_q$ and let $d \geqslant 2$ be an integer. Let $t \in E(\mathbb{F}_q)[d]$ be a rational point of order d. We call T the group generated by t. Let $\phi : E \to E$ be the Frobenius endomorphism. Let $b \in E(\bar{\mathbf{K}})$ be a point such that $\phi(b) = b + t$. So b belongs to $E(\mathbf{L})$ where $\mathbf{L}$ is the degree d extension of $\mathbf{K}$. We denote by E' the quotient E/T and by $I : E \to E'$ the quotient isogeny. We also assume $db \neq O \in E$. We set $a = I(b)$ and check $a \in E'(\mathbb{F}_q)$. For another use of Kummer theory of elliptic curves in order to construct efficient representations for finite fields, see [9].

3.1 The elliptic basis Ω

We denote by Ω the system $(\omega_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ defined as

$$\omega_0 = 1 \text{ and } \omega_k = u_{O,kt}(b) \in \mathbf{L} \text{ for } k \neq 0 \bmod d\,.$$

Lemma 1 *With the above notation, the system $\Omega = (\omega_0, \omega_1, \ldots, \omega_{d-1})$ is a $\mathbf{K}$ basis of $\mathbf{L}$.*

Proof. Indeed, let the λ_k for $k \in \mathbb{Z}/d\mathbb{Z}$ be scalars in $\mathbf{K}$ such that $\sum_{k\in\mathbb{Z}/d\mathbb{Z}} \lambda_k\omega_k = 0$. The function $f = \lambda_0 + \sum_{0\neq k\in\mathbb{Z}/d\mathbb{Z}} \lambda_k u_{O,kt}$ cancels at b and also at all its d conjugates over $\mathbf{K}$ (because f is defined over $\mathbf{K}$). But f has no more than d poles (the points in T). If f is non-zero, its divisor is $(f)_0 - (f)_\infty$ with $(f)_0 = \sum_{t\in T}[b+t]$ and $(f)_\infty = \sum_{t\in T}[t]$. We deduce $d \times b$ is zero in E. But this is impossible by hypothesis. Examination of poles shows that all λ_k are zero.

□

We call such a basis as Ω an *elliptic basis*. It enjoys nice properties as we shall see.

We set

$$\Gamma_{k,l} = \Gamma(O, kt, lt) \in \mathbf{K}$$

for any distinct non-zero $k, l \in \mathbb{Z}/d\mathbb{Z}$. For any $k \in \mathbb{Z}/d\mathbb{Z}$, we set furthermore $\xi_k = x_{kt}(b) \in \mathbf{L}$. If $k \neq 0 \bmod d$, we set $\nu_k = x_O(kt) \in \mathbf{K}$ and $\rho_k = y_O(kt) \in \mathbf{K}$ too.

Let now $\Phi : \bar{\mathbb{F}}_q \to \bar{\mathbb{F}}_q$ be the q-Frobenius automorphism. We have $x_O(b) = \xi_0$ and $\Phi(\xi_0) = x_O(\phi(b)) = x_O(b+t) = x_{-t}(b) = \xi_{-1}$. There exist d scalars $(\kappa_k)_{0\leqslant k\leqslant d-1}$ in $\mathbf{K}$ such that

$$\xi_0 = \sum_{0\leqslant k\leqslant d-1} \kappa_k\omega_k. \tag{7}$$

We have for $k \neq 0, 1 \bmod d$,

$$\begin{aligned}\Phi(\omega_k) = u_{O,kt}(\phi(b)) &= u_{O,kt}(b+t) = u_{-t,(k-1)t}(b)\\ &= u_{O,(k-1)t}(b) - u_{O,-t}(b) + \Gamma(0,-t,(k-1)t)\\ &= \omega_{k-1} - \omega_{-1} + \Gamma_{-1,k-1}\end{aligned} \tag{8}$$

using Equation (2). Similarly

$$\Phi(\omega_1) = u_{O,t}(b+t) = u_{-t,O}(b) = -\omega_{-1} - a_1 \text{ and } \Phi(\omega_0) = \omega_0\,. \tag{9}$$

Equations (8) and (9) show that the action of Frobenius is expressed very easily in an elliptic basis.

As far as multiplication is concerned, we set $A = O$, $B = kt$ and $C = lt$ in Equation (4), and we evaluate at b. We find, for k and l distinct and non-zero in $\mathbb{Z}/d\mathbb{Z}$,

$$\omega_k\omega_l = \xi_0 + \Gamma_{-k,-l}\omega_k + \Gamma_{k,l}\omega_l + \nu_k + \nu_l + a_2\,. \tag{10}$$

In the same vein, from Equation (5), we obtain for any non-zero k in $\mathbb{Z}/d\mathbb{Z}$,

$$\omega_k^2 = \xi_0 - a_1\omega_k + \xi_k + \nu_k + a_2\,. \tag{11}$$

So, if we multiply two $\mathbf{K}$-linear combinations of the ω's, we quickly get a linear combination of the ω's and ξ's using Equations (10) and (11). We then reduce (eliminate all the ξ_k) using the expression of ξ_0 in the basis Ω given by Equation (7). We also use Equation (8) to deduce the expressions of all ξ_k's in the basis Ω.

We don't need to store all constants $\Gamma_{k,l}$. Equation (6) allows to recalculate all these d^2 quantities from the ν_k and ρ_k. Moreover, we use in the following that only a small amount of these coefficients has to be computed due to symmetry relations (3) and (1) and invariance by translation.

Example. Let $\mathbf{K} = \mathbb{F}_7$ and $d = 5$, we first consider the elliptic curve E of order 10 defined by $y^2 + xy + 5\,y = x^3 + 3\,x^2 + 3\,x + 2$. The point $t = (3, 1)$ generates a subgroup $T \subset E$ of order 5, and with $E' = E/T$ defined by $y^2 + xy + 5\,y = x^3 + 3\,x^2 + 4\,x + 6$, we find

$$I : (x, y) \mapsto \left(\frac{x^5 + 2\,x^2 + 5\,x + 6}{x^4 + 3\,x^2 + 4},\right.$$
$$\left.\frac{(x^6 + 4\,x^4 + 3\,x^3 + 6\,x^2 + 3\,x + 4)\,y + 3\,x^5 + x^4 + x^3 + 3\,x^2 + 4\,x + 1}{x^6 + x^4 + 5\,x^2 + 6}\right)\,.$$

Let now $a = (4, 2)$, we define $\mathbf{L}$ with the irreducible polynomial $(\tau^5 + 2\,\tau^2 + 5\,\tau + 6) - 4\,(\tau^4 + 3\,\tau^2 + 4) = \tau^5 + 3\,\tau^4 + 4\,\tau^2 + 5\,\tau + 4$, and we set $b = (\tau : \tau^{4756})$.

We find

$$(u_{O,kt})_{k\in\mathbb{Z}/d\mathbb{Z}} = \left(1, \frac{y+2}{x+4}, \frac{y+2}{x+3}, \frac{y}{x+3}, \frac{y+6}{x+4}\right)\,,$$

so that,

$$\Omega = (1, \tau^{10884}, \tau^{11164}, \tau^{9837}, \tau^{15166})\,.$$

3.2 A cell decomposition of the torus

Equations (1) and (3) show that the quantity $\Gamma(A, B, C)$ is covariant for the symmetric group $\mathcal{S}_3$ and even for $\mathcal{S}_3 \times \{1, -1\}$. It is also invariant by translation,

$$\Gamma(A + P, B + P, C + P) = \Gamma(A, B, C).$$

Altogether, Γ is covariant for the group $E(\bar{\mathbf{K}}) \rtimes (\mathcal{S}_3 \times \{1,-1\})$.

These covariance properties are useful when computing the $\Gamma_{k,l}$: we divide by 12 the amount of work. Since in that case, $A = 0$, $B = kt$ and $C = lt$ lie in the group $T =< t >$, a cyclic group or order d, it makes sense to study the action of $(\mathbb{Z}/d\mathbb{Z}) \rtimes (\mathcal{S}_3 \times \{1,-1\})$ on the group $(\mathbb{Z}/d\mathbb{Z})^3$. In particular, we are interested in fundamental domains for this action. It turns out that it is more natural to study first the action of $\mathbb{R}^3 \rtimes (\mathcal{S}_3 \times \{1,-1\})$ on $\mathbb{R}^3$. In this subsection we justify the choice of fundamental domain that is made in Subsection 3.3.

Let $\psi : \mathbb{R}^3 \to \mathbb{C}$ be the map that sends the triplet (a,b,c) onto $a + b\rho + c\rho^2$ where $\rho = \exp(2i\pi/3)$. This is a group homomorphism. Its kernel is the diagonal subgroup of $\mathbb{R}^3$. The group $\mathcal{S}_3 \times \{1,-1\}$ acts on $\mathbb{R}^3$ and we have the following covariance formulas

$$\begin{aligned}\psi(a,c,b) &= \overline{\psi(a,b,c)}\,,\\ \psi(c,a,b) &= \rho\psi(a,b,c)\,,\\ \psi(-a,-b,-c) &= -\psi(a,b,c)\,.\end{aligned}$$

So the map ψ induces a bijection between the quotient of $\mathbb{R}^3$ by $\mathbb{R} \rtimes (\mathcal{S}_3 \times \{1,-1\})$ and the quotient of $\mathbb{C}$ by $\mu_6 \times \{1, \mathrm{conj}\}$ where μ_6 is the group of sixth roots of unity and conj is complex conjugation.

The image of $\mathbb{Z}^3 \subset \mathbb{R}^3$ by ψ is the ring of Gaussian integers. Since $\mathbb{Z}^3$ is normalized by $\mathcal{S}_3 \times \{1,-1\}$, the map ψ induces a morphism $\tilde{\psi} : \mathbb{U}^3 \to T_0$ where $\mathbb{U} = \mathbb{R}/\mathbb{Z}$ is the unit circle and $T_0 = \mathbb{C}/(\mathbb{Z} + \rho\mathbb{Z})$ the complex torus with zero modular invariant. This map $\tilde{\psi}$ is covariant. We denote by Λ the lattice $\mathbb{Z} + \rho\mathbb{Z}$. For any $d \geqslant 2$ an integer, we denote by $\mathbb{U}[d]$ the d-torsion group of $\mathbb{U}$ and $T_0[d]$ the one of T_0. We denote by ψ_d the map from $\mathbb{U}[d]^3$ to $T_0[d]$ induced by $\tilde{\psi}$.

Let k and l be two elements in $\mathbb{U}$ and let $z = k\rho + l\rho^2 \in T_0$ the image of $(0,k,l)$ by $\tilde{\psi}$. We compute the stabilizer of z in $\mu_6 \times \{1, \mathrm{conj}\}$. It is clear that $z = \bar{z} \bmod \Lambda$ if and only if $k = l \bmod 1$. The set of fixed points by complex conjugation is the circle made of real points in T_0. In the same manner we show that $-\rho\bar{z} = z \bmod \Lambda$ if and only if z lies on the circle with equation $k = 2l \bmod 1$. Similarly $\rho^2\bar{z} = z \bmod \Lambda$ if and only if $l = 0 \bmod 1$. And $-\bar{z} = z \bmod \Lambda$ if and only if $k = -l \bmod 1$. And $\rho\bar{z} = z \bmod \Lambda$ if and only if $k = 0 \bmod 1$. At last $-\rho^2\bar{z} = z \bmod \Lambda$ if and only if $2k = l \bmod 1$.

The only fixed point of $z \bmod \Lambda \mapsto -\rho z \bmod \Lambda$ is 0. The same is true for $z \bmod \Lambda \mapsto -\rho^2 z \bmod \Lambda$.

The map $z \bmod \Lambda \mapsto \rho z \bmod \Lambda$ has three fixed points, namely 0, $(\rho - \rho^2)/3$ and its opposite. These are the fixed points of $z \bmod \Lambda \mapsto \rho^2 z \bmod \Lambda$ also. Altogether, these three points form the intersection of the three circles with equations $k = 2l \bmod 1$, $l = 2k \bmod 1$ and $l = -k \bmod 1$.

The complementary set of the six circles above consists of 12 triangles. Each of these triangles (with its boundary) is a fundamental domain for the action of $\mu_6 \times \{1, \mathrm{conj}\}$ on the torus. The intersection of such a triangle with $T_0[d]$ gives a fundamental domain for

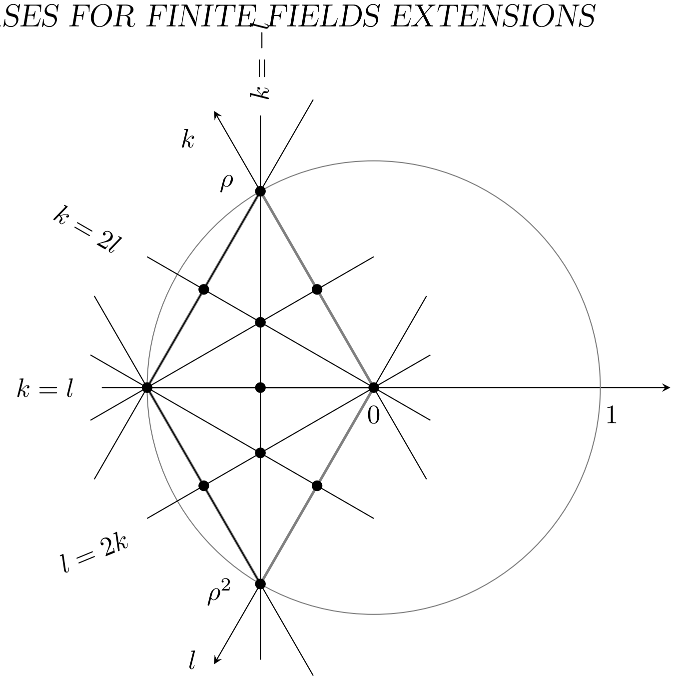

Figure 1: Cell decomposition of the torus

the action of $\mu_6 \times \{1, \mathrm{conj}\}$ on $T_0[d]$. This is also a fundamental domain for the action of $(\mathbb{Z}/d\mathbb{Z}) \rtimes (\mathcal{S}_3 \times \{1, -1\})$ on $(\mathbb{Z}/d\mathbb{Z})^3$.

3.3 Complexities

Given an elliptic basis $\Omega = (\omega_k)_{k \in \mathbb{Z}/d\mathbb{Z}}$, we now focus on the complexity of algorithms for computing the Frobenius or the multiplication of two elements. To be as efficient as possible, and since operands of the algorithms are already of size $d \log q$, we assume that any precomputation, the storage of which does not exceed $O(d \log q)$, is possible.

We first have the following result.

Lemma 2 *Let* $\alpha = \sum_{i=0}^{d-1} \alpha_i \omega_i \in \mathbf{L}$. *Then there exists algorithms that compute* $\Phi(\alpha)$ *and* $\Phi^{-1}(\alpha)$ *at the expense of* $d-1$ *multiplications and* $2d-3$ *additions in* $\mathbf{K}$*, among which are one multiplication and one addition because of the coefficient* a_1.

Proof. Plugging Equation (8) and Equation (9) in $\sum_{i=0}^{d-1} \alpha_i \Phi(\omega_i)$ or $\sum_{i=0}^{d-1} \alpha_i \Phi^{-1}(\omega_i)$ proves the correctness of Algorithm 3.1 and Algorithm 3.2. And, once precomputed the $\Gamma_{d-1,j}$'s and $\Gamma_{j,d-1}$'s, the complexity is obvious.

□

Multiplying two elements in such a basis can be done with good complexity too.

Algorithm 3.1 EllipticFrobenius

Frobenius of an element given in an elliptic basis.

INPUT : $\vec{\alpha} = (\alpha_i)_{0 \leqslant i \leqslant d-1}$ such that $\alpha = \sum_{i=0}^{d-1} \alpha_i \omega_i \in \mathbf{L}$.
OUTPUT : $\vec{\gamma} = (\gamma_i)_{0 \leqslant i \leqslant d-1}$ such that $\gamma = \sum_{i=0}^{d-1} \gamma_i \omega_i = \Phi(\alpha) \in \mathbf{L}$.

return $(\alpha_0 - a_1\alpha_1 + \sum_{j=2}^{d-1} \alpha_j \Gamma_{d-1,j-1}, \alpha_2, \ldots, \alpha_{d-1}, -\sum_{j=1}^{d-1} \alpha_j)$

Algorithm 3.2 EllipticFrobeniusInverse

Inverse Frobenius of an element given in an elliptic basis.

INPUT : $\vec{\alpha} = (\alpha_i)_{0 \leqslant i \leqslant d-1}$ such that $\alpha = \sum_{i=0}^{d-1} \alpha_i \omega_i \in \mathbf{L}$.
OUTPUT : $\vec{\gamma} = (\gamma_i)_{0 \leqslant i \leqslant d-1}$ such that $\gamma = \sum_{i=0}^{d-1} \gamma_i \omega_i = \Phi^{-1}(\alpha) \in \mathbf{L}$.

return $(\alpha_0 + \sum_{j=1}^{d-2} \alpha_j \Gamma_{j,d-1} - a_1\alpha_{d-1}, -\sum_{j=1}^{d-1} \alpha_j, \alpha_1, \ldots, \alpha_{d-2})$

Lemma 3 *Let $\alpha = \sum_{i=0}^{d-1} \alpha_i \omega_i \in \mathbf{L}$ and $\beta = \sum_{i=0}^{d-1} \beta_i \omega_i \in \mathbf{L}$. Then there exists an algorithm that computes the product $\alpha \times \beta$ at the expense of*

- $(37\,d^2 + 30\,d - 7\varepsilon - 60)/12$ *additions,* $(32\,d^2 + 42\,d - 2\varepsilon - 48)/12$ *multiplications and* $(d^2 - \varepsilon)/12$ *inversions in* $\mathbf{K}$*,*

where $\varepsilon = 12, 1, 4, 9, 4, 1$ *respectively for* $d = 0, \ldots, 5 \bmod 6$*, among which are* $(d^2 + 12d - \varepsilon - 24)/12$ *additions and* $(d^2 + 36\,d - \varepsilon - 48)/12$ *multiplications because of the coefficient* a_1*,* $(d^2 - \varepsilon)/12$ *additions because of the coefficient* a_3*.*

Proof. We prove the correctness of Algorithm 3.3 and establish its complexity.

Correctness. Equations (4) and (5), for $k \leqslant l$, yield

$$\omega_k\,\omega_l = \omega_l\,\omega_k = \begin{cases} \omega_l & \text{if } k = 0\,, \\ \xi_0 + a_2 - a_1\omega_k + \Phi^{-k}(\xi_0) + \nu_k\,\omega_0 & \text{if } l = k \text{ and } k > 0\,, \\ \xi_0 + a_2 - a_1\omega_k + \Gamma_{k,l}\,(\omega_l - \omega_k) + (\nu_k + \nu_l)\,\omega_0 & \text{otherwise}\,. \end{cases}$$

Algorithm 3.3 ELLIPTICMULTIPLICATION

Product of two elements given in an elliptic basis.

INPUT : $\vec{\alpha} = (\alpha_i)_{0 \leqslant i \leqslant d-1}$ and $\vec{\beta} = (\beta_i)_{0 \leqslant i \leqslant d-1}$ such that $\alpha = \sum_{i=0}^{d-1} \alpha_i \omega_i$, $\beta = \sum_{i=0}^{d-1} \beta_i \omega_i \in \mathbf{L}$.
OUTPUT : $\vec{\gamma} = (\gamma_i)_{0 \leqslant i \leqslant d-1}$ such that $\gamma = \sum_{i=0}^{d-1} \gamma_i \omega_i = \alpha \times \beta \in \mathbf{L}$.

$s_a := 0\,;\ s_b := \beta_1\,;\ \gamma_0 := 0\,;\ \gamma_1 := -a_1 s_b \alpha_1\,;$
for $k := 2$ **to** $d-1$ **do** $s_a {+}{:=} \alpha_{k-1}\,;\ s_b {+}{:=} \beta_k\,;\ \gamma_k := -a_1(s_b\alpha_k + s_a\beta_k)\,;$
$s_a {+}{:=} \alpha_{d-1}\,;\ (\gamma_0, \ldots, \gamma_{d-1}) {+}{:=} s_a s_b\,(\kappa_0 + a_2, \kappa_1, \ldots \kappa_{d-1})\,;$
$s'_a := \sum_{i=1}^{d-1} \alpha_i \nu_i\,;\ s'_b := \sum_{i=1}^{d-1} \beta_i \nu_i\,;\ \gamma_0 \mathrel{+}:= s_a s'_b + s'_a s_b\,;$
for $k := 1$ **to** $d-1$ **do**
    $\delta := \alpha_k \beta_k\,;\ \gamma_0 {+}{:=} \delta\,((\Phi^{-k}(\xi_0))_0 - \nu_k)\,;\ \gamma_k {-}{:=} \delta\, \sum_{l=1}^{d-1} \kappa_l;$
    for $l := 1$ **to** $k-1$ **do** $\gamma_l {+}{:=} \delta\, \kappa_{(d-k+l) \bmod d};$
    for $l := k+1$ **to** $d-1$ **do** $\gamma_l {+}{:=} \delta\, \kappa_{(d-k+l) \bmod d};$
$(\gamma_0, \ldots, \gamma_{d-1}) \mathrel{+}:= (\alpha_0\beta_0, \alpha_1\beta_0 + \alpha_0\beta_1, \ldots, \alpha_{d-1}\beta_0 + \alpha_0\beta_{d-1})\,;$
if $d \bmod 3 = 0$ **then**
    $g := -(3\,\nu_{2d/3}^2 + 2a_2\nu_{2d/3} + a_4)/(2\rho_{2d/3} + a_1\nu_{2d/3} + a_3) - a_1\,;$
    $\delta := g\,(\alpha_{2d/3}\beta_{d/3} + \alpha_{d/3}\beta_{2d/3})\,;\ \gamma_{2d/3} \mathrel{-}:= \delta\,;\ \gamma_{d/3} \mathrel{+}:= \delta\,;$
for $k := 2$ **to** $\lfloor (2d-1)/3 \rfloor$ **by** 2 **do**
    $l := k/2\,;\ g := (\rho_l + \rho_k + a_1\nu_k + a_3)/(\nu_l - \nu_k)\,;$
    $i_1, i_2 := 2\,l, d-l\,;\ j_1, j_2 := d - 2\,l, l\,;$
    $\delta_{12} := g\,(\alpha_{i_1}\,\beta_{j_2} + \alpha_{j_2}\,\beta_{i_1})\,;\ \delta_{21} := g\,(\alpha_{i_2}\,\beta_{j_1} + \alpha_{j_1}\,\beta_{i_2})\,;\ \delta_{22} := g\,(\alpha_{i_2}\,\beta_{j_2} + \alpha_{j_2}\,\beta_{i_2})\,;$
    $\gamma_{i_1} \mathrel{-}:= \delta_{12}\,;\ \gamma_{i_2} \mathrel{-}:= \delta_{21} + \delta_{22}\,;\ \gamma_{j_1} \mathrel{+}:= \delta_{21}\,;\ \gamma_{j_2} \mathrel{+}:= \delta_{12} + \delta_{22}\,;$
for $k := \lfloor 1 + d/2 \rfloor$ **to** $\lfloor (2d-1)/3 \rfloor$ **do**
    $l := 2k \bmod d\,;\ g := (\rho_l + \rho_k + a_1\nu_k + a_3)/(\nu_l - \nu_k)\,;$
    $i_1, i_2 := k, (2d-2k) \bmod d\,;\ j_1, j_2 := (2k) \bmod d, d-k;$
    $\delta_{11} := g\,(\alpha_{i_1}\,\beta_{j_1} + \alpha_{j_1}\,\beta_{i_1})\,;\ \delta_{22} := g\,(\alpha_{i_2}\,\beta_{j_2} + \alpha_{j_2}\,\beta_{i_2})\,;\ \delta_{12} := g\,(\alpha_{i_1}\,\beta_{j_2} + \alpha_{j_2}\,\beta_{i_1})\,;$
    $\gamma_{i_1} \mathrel{-}:= \delta_{11} + \delta_{12}\,;\ \gamma_{i_2} \mathrel{-}:= \delta_{22}\,;\ \gamma_{j_1} \mathrel{+}:= \delta_{11}\,;\ \gamma_{j_2} \mathrel{+}:= \delta_{22} + \delta_{12}\,;$
for $k := 3$ **to** $\lfloor (2d-1)/3 \rfloor$ **do**
    for $l := \max(1, 2k-d+1)$ **to** $\lfloor (k-1)/2 \rfloor$ **do**
        $g := (\rho_l + \rho_k + a_1\nu_k + a_3)/(\nu_l - \nu_k)\,;$
        $i_1, i_2, i_3 := k, d-l, d-k+l\,;\ j_1, j_2, j_3 := d-k, l, k-l;$
        $\delta_{12} := g\,(\alpha_{i_1}\,\beta_{j_2} + \alpha_{j_2}\,\beta_{i_1})\,;\ \delta_{13} := g\,(\alpha_{i_1}\,\beta_{j_3} + \alpha_{j_3}\,\beta_{i_1})\,;\ \delta_{21} := g\,(\alpha_{i_2}\,\beta_{j_1} + \alpha_{j_1}\,\beta_{i_2})\,;$
        $\delta_{23} := g\,(\alpha_{i_2}\,\beta_{j_3} + \alpha_{j_3}\,\beta_{i_2})\,;\ \delta_{31} := g\,(\alpha_{i_3}\,\beta_{j_1} + \alpha_{j_1}\,\beta_{i_3})\,;\ \delta_{32} := g\,(\alpha_{i_3}\,\beta_{j_2} + \alpha_{j_2}\,\beta_{i_3})\,;$
        $\gamma_{i_1} \mathrel{-}:= \delta_{12} + \delta_{13}\,;\ \gamma_{i_2} \mathrel{-}:= \delta_{21} + \delta_{23}\,;\ \gamma_{i_3} \mathrel{-}:= \delta_{31} + \delta_{32}\,;$
        $\gamma_{j_1} \mathrel{+}:= \delta_{21} + \delta_{31}\,;\ \gamma_{j_2} \mathrel{+}:= \delta_{12} + \delta_{32}\,;\ \gamma_{j_3} \mathrel{+}:= \delta_{13} + \delta_{23}\,;$
return $(\gamma_i)_{0 \leqslant i \leqslant d-1}$

And we have,

$$
\begin{aligned}
\alpha \times \beta = \sum_{k=0}^{d-1}\sum_{l=0}^{d-1} \alpha_k\beta_l\omega_k\omega_l = (\sum_{k=1}^{d-1}\alpha_k)(\sum_{l=1}^{d-1}\beta_l)(\xi_0 + a_2) \\
+ \left((\sum_{k=1}^{d-1}\alpha_k)(\sum_{l=1}^{d-1}\beta_l\nu_l) + (\sum_{k=1}^{d-1}\alpha_k\nu_k)(\sum_{l=1}^{d-1}\beta_l) \right)\omega_0 \\
+ \alpha_0\beta_0\omega_0 + \sum_{k=1}^{d-1}\alpha_k\,\beta_k\,(\Phi^{-k}(\xi_0) - \nu_k\,\omega_0) + \sum_{k=1}^{d-1}(\alpha_k\beta_0 + \beta_k\alpha_0)\omega_k \\
- a_1 \sum_{0<k,l<d} \alpha_k\beta_l\omega_k + \sum_{\substack{0<k,l<d\\ k\neq l}} \Gamma_{k,l}\alpha_k\beta_l(\omega_l - \omega_k)\,. \quad (12)
\end{aligned}
$$

The first two terms of this sum are computed at steps 3. and 4. of the algorithm. The three next terms are computed in steps 5. to 9. Especially, steps 5. to 8. correspond to the action of Φ^{-k} on ξ_0 (the quantity $(\Phi^{-k}(\xi_0))_0$, at step 4., is the first coordinate of $\Phi^{-k}(\xi_0)$ written in basis Ω).

The constants $\Gamma_{k,l}$ satisfied 12 symmetry relations and we take advantage of them to compute the two last terms of the sum. More precisely, for k and l distinct and non-zero in $\mathbb{Z}/d\mathbb{Z}$, we have

$$
\begin{cases} \Gamma_{k,l} = \Gamma_{-l,-k} = \Gamma_{k,k-l} = \Gamma_{l-k,-k} = \Gamma_{l-k,l} = \Gamma_{-l,k-l}\,, \\ \Gamma_{l,k} = \Gamma_{-k,-l} = \Gamma_{k-l,k} = \Gamma_{-k,l-k} = \Gamma_{l,l-k} = \Gamma_{k-l,-l}\,, \end{cases} \quad \text{and } \Gamma_{k,l} = -\Gamma_{l,k} - a_1\,.
$$

All of these relations can be proved thanks to Equation (3) and Equation (1). For instance, to check that $\Gamma_{k,l} = \Gamma_{l-k,-k}$, we start from $\Gamma(O, kt, lt) = u_{O,kt}(b+kt)+u_{kt,lt}(b+kt)+u_{lt,O}(b+kt)$, and we find $\Gamma(O, kt, lt) = u_{-kt,O}(b) + u_{O,(l-k)t}(b) + u_{(l-k)t,-kt}(b) = \Gamma(O,(l-k)t, -kt)\,.$

We use first that $\Gamma_{k,l} = -\Gamma_{l,k} - a_1$ and we rewrite the last two terms of Equation (12) as follows,

$$
-a_1 \sum_{k=1}^{d-1}(\beta_k \sum_{l=1}^{k-1}\alpha_l + \alpha_k \sum_{l=1}^{k}\beta_l)\omega_k + \sum_{0<l<k<d} \Gamma_{k,l}(\alpha_k\beta_l + \alpha_l\beta_k)(\omega_l - \omega_k)\,.
$$

The first term of this sum is computed at at steps 1. and 2. of the algorithm. To compute the last term, we consider in turn each orbit of the action defined by the symmetries on the coefficients $\Gamma_{k,l}$. We choose as a fundamental domain for this action the triangle delimited by the circles $l = 1$, $k = 2\,l \bmod d$ and $l = 2\,k \mod d$ (cf. Figure 2). It is cumbersome, but not difficult, to check that any point of this domain, outside the two circles $k = 2\,l \bmod d$ and $l = 2\,k \mod d$, has an orbit of exactly 12 points: we compute only once the constant $\Gamma_{k,l}$ corresponding to these 12 points and we calculate accordingly their contribution to the product $\alpha \times \beta$. These are steps 23. to 30. of the algorithm.

Points on the line $k = 2\,l \bmod d$ have orbits of only 6 points. We precisely have $\Gamma_{2\,l,l} = \Gamma_{-l,-2\,l} = \Gamma_{-l,l} = -\Gamma_{l,2\,l} - a_1 = -\Gamma_{-2\,l,-l} - a_1 = -\Gamma_{l,-l} - a_1$, and this yield steps 13. to 17.

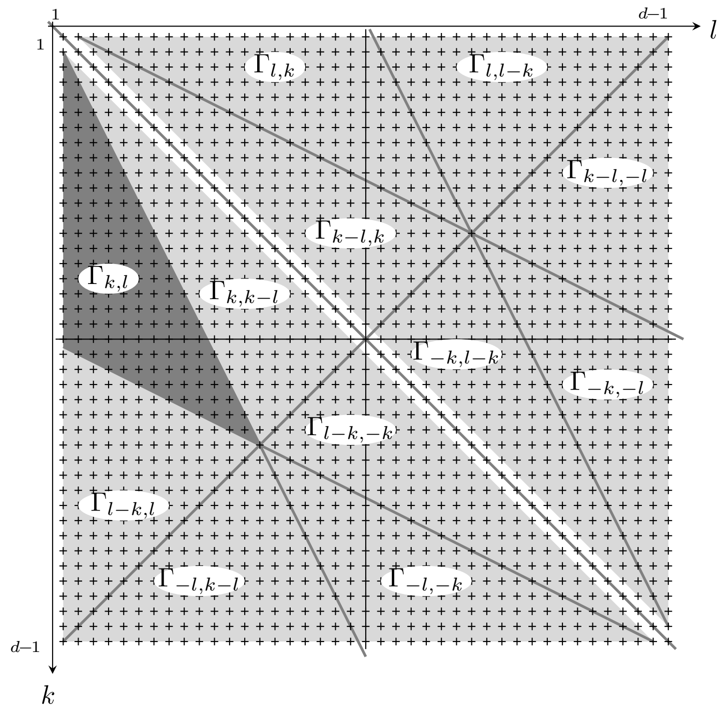

Figure 2: Symmetry relations on the coefficients $\Gamma_{k,l}$ ($d = 42$)

of the algorithm. Similarly, points on the line $l = 2\,k \bmod d$ have orbits of only 6 points too. We have $\Gamma_{k,2\,k} = \Gamma_{-2\,k,-k} = \Gamma_{k,-k} = -\Gamma_{2\,k,k} - a_1 = -\Gamma_{-k,-2\,k} - a_1 = -\Gamma_{-k,k} - a_1$ and this yield steps 18. to 22. of the algorithm.

Finally, when d is divisible by 3, the two circles $k = 2\,l \bmod d$ and $l = 2\,k \bmod d$ meet at the exceptional point $(2d/3, d/3)$, which is on the $k + l = 0 \bmod d$ line too. This point has an orbit of only 2 points, *i.e.* $\Gamma_{2d/3,d/3} = -\Gamma_{d/3,2d/3} - a_1$. This yields steps 10. to 12. of the algorithm.

Complexity. We precompute the d constants ν_k and ρ_k, the constant $\Gamma_{2d/3,d/3}$ if $d \bmod 3 = 0$, the d coordinates in the basis Ω of ξ_0, their sum $\sum_{l=1}^{d-1} \kappa_l$, $\kappa_0 + a_2$ and the ω_0-coordinates of all $\Phi^k(\xi_0) - \nu_k$ for $0 \leqslant k \leqslant d-1$.

Then, Steps 1.-2. need $3d-7$ additions and $3d-4$ multiplications in $\mathbf{K}$ (among which are $d-2$ additions and $3d-4$ multiplications because of a_1), Step 3. needs $d+1$ additions and $d+1$ multiplications in $\mathbf{K}$, Step 6. needs $d-1$ additions and $2d-2$ multiplications in $\mathbf{K}$, Steps 7.-8. need d^2-2d+1 additions and d^2-2d+1 multiplications in $\mathbf{K}$, Step 9. needs $2d-1$ additions and $2d-1$ multiplications in $\mathbf{K}$, Steps 11.-12. need 3 additions and 3 multiplications in $\mathbf{K}$ if d is a multiple of 3 (and cost nothing otherwise), Steps 13.-17. consist in $\lfloor (d-1)/3 \rfloor$ iterations and Steps 18.-22. consist in $\lfloor (d-5+6\varepsilon')/6 \rfloor$ (where $\varepsilon' = 0$ if $d \bmod 6 = 0$ and $\varepsilon' = 1$ otherwise), each of them needs 16 additions, 11 multiplications and 1 inversion in $\mathbf{K}$ (among which are 1 addition, 1 multiplication because of a_1 and 1 addition because of a_3), and finally, Steps 23.-30. consist in $\lfloor d^2/12 \rfloor - \lfloor d/2 \rfloor + \varepsilon''$ iterations (where $\varepsilon'' = 0$ if $d \bmod 6 = 1, 5$ and $\varepsilon'' = 1$ otherwise), each of them needs 25 additions, 12 multiplications and 1 inversion in $\mathbf{K}$ (among which are 1 addition, 1 multiplication because of a_1 and 1 addition because of a_3).

Adding all these complexities yields the complexity announced.

□

Depending on the characteristic of $\mathbf{K}$, it is classical to consider the reduced Weierstrass Model to define elliptic curves. We give in Table 3 precise complexities for these cases, all obtained with Lemma 3.

Condition		Model	Add.	Mult.	Inv.
$\mathrm{Char}(\mathbf{K}) \neq 2, 3$		$Y^2 = X^3 + a_4 X + a_6$	$\frac{35\,d^2 + 18\,d - 5\,\varepsilon - 36}{12}$	$\frac{31\,d^2 + 6\,d - \varepsilon}{12}$	$\frac{d^2 - \varepsilon}{12}$
$\mathrm{Char}(\mathbf{K}) = 3,$	$j_E \neq 0$	$Y^2 = X^3 + a_2 X^2 + a_6$			
	$j_E = 0$	$Y^2 = X^3 + a_4 X + a_6$			
$\mathrm{Char}(\mathbf{K}) = 2$	$j_E \neq 0$	$Y^2 + XY = X^3 + a_2 X^2 + a_6$	$\frac{6\,d^2 + 5\,d - \varepsilon - 10}{2}$		
	$j_E = 0$	$Y^2 + a_3 Y = X^3 + a_4 X + a_6$	$\frac{6\,d^2 + 3\,d - \varepsilon - 6}{2}$		

Figure 3: Elliptic multiplication complexities

4 Elliptic normal bases

In this section, we assume that we are in the situation of Section 3. So E is an elliptic curve over a finite field $\mathbf{K} = \mathbb{F}_q$ and $d \geqslant 2$ is an integer. Let $t \in E(\mathbb{F}_q)[d]$ be a rational point of order d. We call T the group generated by t. Let $\phi : E \to E$ be the Frobenius endomorphism. Let $b \in E(\bar{\mathbf{K}})$ be a point such that $\phi(b) = b + t$. So, b belongs to $E(\mathbf{L})$ where $\mathbf{L}$ is the degree d extension of $\mathbf{K}$. We denote by E' the quotient E/T and by $I : E \to E'$ the quotient isogeny. We also assume $db \neq O \in E$. We set $a = I(b)$ and check $a \in E'(\mathbb{F}_q)$. We further assume there exists one point R in $E(\mathbb{F}_q)$ such that $dR \neq 0$.

We construct a normal basis for $\mathbf{L}$, the degree $d = \#T$ extension of $\mathbf{K}$. In this basis, the product of two elements can be computed at the expense of 5 convolution products between vectors of dimension d. Such bases may be preferred to the ones constructed in Section 3 when d is large enough, depending on the implementation context.

4.1 The elliptic normal basis Θ

We start with a lemma concerning the sum $\sum_{k\in\mathbb{Z}/d\mathbb{Z}} u_{kt,(k+1)t}$.

Lemma 4 *The sum $\sum_{k\in\mathbb{Z}/d\mathbb{Z}} u_{kt,(k+1)t}$ is a constant $\mathfrak{c}\in\mathbf{K}$. If the characteristic p of $\mathbf{K}$ divides the degree d, then $\mathfrak{c}\neq 0$.*

Proof. The sum $\sum_{k\in\mathbb{Z}/d\mathbb{Z}} u_{kt,(k+1)t}$ is invariant by translations in T. So it can be seen as a function on $E'=E/T$. As such, it has no more than one pole. Therefore it is constant.

Assume now p divides d and $\sum_{k\in\mathbb{Z}/d\mathbb{Z}} u_{kt,(k+1)t}=0$. The sum $\sum_{k\in\mathbb{Z}/d\mathbb{Z}} ku_{kt,(k+1)t}$ is thus invariant by translations in T. So it can be seen as a function on $E'=E/T$. As such, it has no more than one pole. Therefore it is constant. However, seen as a function on E, this sum $\sum_{k\in\mathbb{Z}/d\mathbb{Z}} ku_{kt,(k+1)t}$ has a pole at O. A contradiction.

□

So at least one of the two following conditions holds: either d is prime to p or $\mathfrak{c}\neq 0$. In any case, there exist two scalars $\mathfrak{a}\neq 0$ and $\mathfrak{b}$ in $\mathbf{K}$ such that $\mathfrak{a}\mathfrak{c}+d\mathfrak{b}=1$. For $k\in\mathbb{Z}/d\mathbb{Z}$ we set $u_k=\mathfrak{a}u_{kt,(k+1)t}+\mathfrak{b}$ and $x_k=x_{kt}$.

We denote by Θ the system $(\theta_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ defined as $\theta_k=u_k(b)$. We have $\sum_{k\in\mathbb{Z}/d\mathbb{Z}}\theta_k=1\in\mathbf{K}$. and $\Phi(\theta_k)=\theta_{k-1}$.

Lemma 5 *With the above notation, the system $(u_0,u_1,\ldots,u_{d-1})$ is a basis of*

$$\mathcal{L}=\mathcal{L}(\sum_{k\in\mathbb{Z}/d\mathbb{Z}}[kt]).$$

The system $\Theta=(\theta_0,\theta_1,\ldots,\theta_{d-1})$ is a $\mathbf{K}$ basis of $\mathbf{L}$.

Proof. Indeed, let the λ_k for $k\in\mathbb{Z}/d\mathbb{Z}$ be scalars in $\mathbf{K}$ such that $\sum_{k\in\mathbb{Z}/d\mathbb{Z}}\lambda_k\theta_k=0$. The function $f=\sum_{k\in\mathbb{Z}/d\mathbb{Z}}\lambda_k u_k$ cancels at b and also at all its d conjugates over $\mathbf{K}$ (because f is defined over $\mathbf{K}$). But f has no more than d poles (the points in T). If f is non-zero, its divisor is $(f)_0-(f)_\infty$ with $(f)_0=\sum_{t\in T}[b+t]$ and $(f)_\infty=\sum_{t\in T}[t]$. We deduce $d\times b$ is zero in E. But this is impossible by hypothesis. So f is constant equal to zero. This implies all λ_k's are equal (look at poles). Since the sum of all θ_k's is non-zero, this implies that all λ_k's are null.

□

We call such a basis as Θ an *elliptic normal basis*.

If $k,l\in\mathbb{Z}/d\mathbb{Z}$ and $k\neq l,l+1,l-1 \bmod d$, then

$$u_k u_l\in\mathcal{L}$$

where $\mathcal{L}=\mathcal{L}(\sum_{k\in\mathbb{Z}/d\mathbb{Z}}[kt])$ is the $\mathbf{K}$-vector space generated by all u_m for $m\in\mathbb{Z}/d\mathbb{Z}$. Further

$$u_{k-1}u_k+\mathfrak{a}^2x_k\in\mathcal{L} \text{ and } u_k^2-\mathfrak{a}^2x_k-\mathfrak{a}^2x_{k+1}\in\mathcal{L}\,.$$

So if $(\alpha_k)_{0\leqslant k\leqslant d-1}$ and $(\beta_k)_{0\leqslant k\leqslant d-1}$ are two vectors in $\mathbf{K}^d$, we have

$$\begin{aligned}(\sum_k \alpha_k u_k)(\sum_k \beta_k u_k) &= \mathfrak{a}^2 \sum_k \alpha_k\beta_k(x_k + x_{k+1}) - \mathfrak{a}^2 \sum_k \alpha_{k-1}\beta_k x_k - \mathfrak{a}^2 \sum_k \beta_{k-1}\alpha_k x_k \bmod \mathcal{L} \\ &= \mathfrak{a}^2 \sum_k (\alpha_k - \alpha_{k-1})(\beta_k - \beta_{k-1}) x_k \bmod \mathcal{L}. \qquad (13)\end{aligned}$$

Example. Let us continue the example of section 3, *i.e.* $\mathbf{K} = \mathbb{F}_7$ and $d = 5$. We find

$$(u_{kt,(k+1)t})_k = \left(\frac{5\,y+3}{x+4}, \frac{5\,y+3\,x^2+4}{x^2+5}, \frac{4}{x+3}, \frac{y\,(2\,x+8)+3\,x^3+15\,x}{(x^2+5)\,(x+4)}, \frac{2\,y+2\,x+6}{x+4}\right),$$

so that $\mathfrak{c} = 3$, $\mathfrak{a} = 5$, $\mathfrak{b} = 0$, and

$$\Theta = \left(\tau^{8083}, \tau^{13159}, \tau^{16285}, \tau^{9529}, \tau^{6163}\right).$$

4.2 Change of coordinates

Thanks to Equation (2), the θ's can be given in the basis $(\omega_k)_k$ as

$$\theta_k = \begin{cases} \mathfrak{a}\omega_1 + \mathfrak{b}\omega_0 & \text{if } k = 0, \\ -\mathfrak{a}\omega_{-1} - a_1\mathfrak{a}\omega_0 + \mathfrak{b}\omega_0 & \text{if } k = d-1, \\ \mathfrak{a}\omega_{k+1} - \mathfrak{a}\omega_k + \mathfrak{a}\Gamma_{k,k+1}\,\omega_0 + \mathfrak{b}\omega_0 & \text{otherwise.} \end{cases}$$

Inversely, we set $\lambda_k = \sum_{i=1}^{k} \Gamma_{i,i+1}$ and we observe that $\mathfrak{c} = \lambda_{d-2} - a_1$. We obtain

$$\omega_k = \begin{cases} \displaystyle\sum_{i=0}^{d-1} \theta_i & \text{if } k = 0, \\ \mathfrak{a}^{-1}\theta_0 - \mathfrak{b}\mathfrak{a}^{-1} \sum_{i=0}^{d-1} \theta_i & \text{if } k = 1, \\ \displaystyle -\mathfrak{a}^{-1}\theta_{-1} + (\mathfrak{b}\mathfrak{a}^{-1} - a_1) \sum_{i=0}^{d-1} \theta_i & \text{if } k = -1, \\ \displaystyle \mathfrak{a}^{-1} \sum_{i=0}^{k-1} \theta_i - (k\mathfrak{b}\mathfrak{a}^{-1} + \lambda_{k-1}) \sum_{i=0}^{d-1} \theta_i & \text{otherwise.} \end{cases}$$

This shows that one can compute the change of variable from Ω to Θ, and back, at the expense of $O(d)$ operations in $\mathbf{K}$.

4.3 Complexities

We exhibit an algorithm with quasi-linear complexity to multiply two elements given in an elliptic normal basis. As often with FFT-like algorithms, it consists in evaluations and interpolations.

Notation. If $\vec{\alpha} = (\alpha_i)_{0 \leqslant i \leqslant d-1}$ and $\vec{\beta} = (\beta_i)_{0 \leqslant i \leqslant d-1}$ are two vectors of length d we denote by $\vec{\alpha} \star_j \vec{\beta} = \sum_i \alpha_i \beta_{j-i}$ the j-th component of the convolution product. We denote by $\sigma(\vec{\alpha}) = (\alpha_{i-1})_i$ the cyclic shift of $\vec{\alpha}$. We denote by $\vec{\alpha} \diamond \vec{\beta} = (\alpha_i \beta_i)_i$ the component-wise product and by $\vec{\alpha} \star \vec{\beta} = (\vec{\alpha} \star_i \vec{\beta})_i$ the convolution product.

4.3.1 Reduction

Given a linear combination of the ξ's we may want to reduce it: express it as a linear combination of the θ's.

Let $\vec{\iota} = (\iota_i)_{0 \leqslant i \leqslant d-1}$ be the vector in $\mathbf{K}^d$ such that $\xi_0 = \sum_{0 \leqslant k \leqslant d-1} \iota_k \theta_k$.

$$\xi_i = \Phi^{-i}(\xi_0) = \sum_{0 \leqslant k \leqslant d-1} \iota_k \Phi^{-i}(\theta_k) = \sum_{0 \leqslant k \leqslant d-1} \iota_k \theta_{k+i} = \sum_{0 \leqslant k \leqslant d-1} \iota_{k-i} \theta_k.$$

Let $\vec{\alpha} = (\alpha_i)_{0 \leqslant i \leqslant d-1}$ and $\vec{\beta} = (\beta_j)_{0 \leqslant j \leqslant d-1}$ be vectors in $\mathbf{K}^d$ such that

$$\sum_{0 \leqslant i \leqslant d-1} \alpha_i \xi_i = \sum_{0 \leqslant j \leqslant d-1} \beta_j \theta_j.$$

We want to express the β_j's as linear expressions in the α_i's.

$$\begin{aligned} \sum_{0 \leqslant i \leqslant d-1} \alpha_i \xi_i &= \sum_{0 \leqslant i \leqslant d-1} \alpha_i \sum_{0 \leqslant k \leqslant d-1} \iota_{k-i} \theta_k \\ &= \sum_k \theta_k \sum_i \alpha_i \iota_{k-i} = \sum_k (\vec{\iota} \star_k \vec{\alpha}) \theta_k. \end{aligned} \tag{14}$$

We deduce $\vec{\beta} = \vec{\iota} \star \vec{\alpha}$. So $\vec{\beta}$ is the convolution product of $\vec{\iota}$ and $\vec{\alpha}$.

4.3.2 Evaluation

Let $(\alpha_i)_{0 \leqslant i \leqslant d-1}$ be scalars in $\mathbf{K}$. Let $R \in E(\mathbf{K}) - E[d]$ be a $\mathbf{K}$-rational point on E such that $dR \neq 0$.

We want to evaluate $f = \sum_{0 \leqslant i \leqslant d-1} \alpha_i x_i$ at all $R + jt$ for $0 \leqslant j \leqslant d-1$. We set $\beta_j = f(R + jt)$. We have

$$\beta_j = \sum_{0 \leqslant i \leqslant d-1} \alpha_i x_i(R + jt) = \sum_{0 \leqslant i \leqslant d-1} \alpha_i x_0(R + (j-i)t) = \vec{\alpha} \star_j \vec{x}_R$$

where $\vec{x}_R = (x_0(R + kt))_{0 \leqslant k \leqslant d-1}$. So,

$$\vec{\beta} = \vec{x}_R \star \vec{\alpha}.$$

Similarly, we want to evaluate $f = \sum_{0\leqslant i\leqslant d-1} \alpha_i u_i$ at all $R + jt$ for $0 \leqslant j \leqslant d-1$. We set $\beta_j = f(R+jt)$. We have

$$\beta_j = \sum_{0\leqslant i\leqslant d-1} \alpha_i u_i(R+jt) = \sum_{0\leqslant i\leqslant d-1} \alpha_i u_0(R+(j-i)t) = \vec{\alpha} \star_j \vec{u}_R$$

where $\vec{u}_R = (u_0(R+kt))_{0\leqslant k\leqslant d-1}$. So,

$$\vec{\beta} = \vec{u}_R \star \vec{\alpha}. \tag{15}$$

4.3.3 Interpolation

Let $R \in E(\mathbf{K}) - E[d]$ be a $\mathbf{K}$-rational point on E such that $dR \neq 0$. The evaluation map $f \mapsto (f(R+jt))_{0\leqslant j\leqslant d-1}$ is a bijection from $\mathcal{L}$ onto $\mathbf{K}^d$.

Given the $\beta_j = f(R+jt)$ we want to compute the α_i such that $f = \sum_{0\leqslant i\leqslant d-1} \alpha_i u_i$. Since $\vec{\beta} = \vec{u}_R \star \vec{\alpha}$ we just need to compute once for all the inverse $\overrightarrow{u_R}^{(-1)}$ of $\vec{u}_R$ for the convolution product. This inverse exists because the evaluation map is bijective.

4.3.4 Multiplication

Let $\vec{\alpha} = (\alpha_i)_{0\leqslant i\leqslant d-1}$ and $\vec{\beta} = (\beta_i)_{0\leqslant i\leqslant d-1}$ be two vectors in $\mathbf{K}^d$. We want to multiply $\sum_i \alpha_i\theta_i$ and $\sum_i \beta_i\theta_i$.

We define four functions on E,

$$\begin{aligned} A &= \sum_i \alpha_i u_i\,,\ B = \sum_i \beta_i u_i\,, \\ C &= \mathfrak{a}^2 \sum_i (\alpha_i - \alpha_{i-1})(\beta_i - \beta_{i-1}) x_i\,, \\ D &= AB - C\,. \end{aligned}$$

The product we want to compute is $A(b)B(b) = C(b) + D(b)$.

>From Equation (13), we deduce that D is in $\mathcal{L}$. >From Equation (14), we deduce that the coordinates in Θ of $C(b)$ are given by the vector

$$\vec{\iota} \star \left(\mathfrak{a}^2(\vec{\alpha} - \sigma(\vec{\alpha})) \diamond (\vec{\beta} - \sigma(\vec{\beta})) \right).$$

According to Equation (15), the evaluation of A at the points $(R+jt)_j$ is given by the vector $\vec{u}_R \star \vec{\alpha}$. The evaluation at these points of D is $(\vec{u}_R \star \vec{\alpha}) \diamond (\vec{u}_R \star \vec{\beta}) - \vec{x}_R \star (\mathfrak{a}^2(\vec{\alpha} - \sigma(\vec{\alpha})) \diamond (\vec{\beta} - \sigma(\vec{\beta})))$. If we $\star$ multiply this late vector on the left by $\overrightarrow{u_R}^{(-1)}$ we obtain the coordinates of D in the basis $(u_0, \ldots, u_{d-1})$. These are also the coordinates of $D(b)$ in the basis Θ.

Altogether, we have proved what follows.

Lemma 6 *The multiplication tensor for normal elliptic bases of type* Θ *is*

$$(\mathfrak{a}^2\vec{\iota}) \star \Big((\vec{\alpha} - \sigma(\vec{\alpha})) \diamond (\vec{\beta} - \sigma(\vec{\beta}))\Big) + \\ \overrightarrow{u_R}^{(-1)} \star \Big((\vec{u}_R \star \vec{\alpha}) \diamond (\vec{u}_R \star \vec{\beta}) - (\mathfrak{a}^2\vec{x}_R) \star \Big((\vec{\alpha} - \sigma(\vec{\alpha})) \diamond (\vec{\beta} - \sigma(\vec{\beta}))\Big)\Big)$$

It consists in 5 *convolution products,* 2 *component-wise products,* 1 *addition and* 3 *subtractions between vectors of size* d*, the degree of the extension.*

Note that convolution products can be computed at the expense of $O(d \log d \log |\log d|)$ operations in $\mathbf{K}$ using algorithms due to Schönhage and Strassen [17], Schönhage [16], and Cantor and Kaltofen [5].

Note also that it is standard to use elliptic curves (and even curves of higher genera) to bound the bilinear complexity of multiplication. One should mention in particular work by Chudnowsky [8], Shokrollahi [18], Ballet [3], Chaumine [6]. The tensor we produce here is not competitive with theirs from the point of view of bilinear complexity. But this tensor is symmetric enough to allow fast application of the Frobenius automorphism.

Example. In the setting of the examples of Section 3 and Section 4, *i.e.* $\mathbf{K} = \mathbb{F}_7$ and $d = 5$, we first precompute, with $R = (1, 2)$ a point of order 10 on E,

$$\vec{\iota} = (0, 5, 5, 1, 0),\ \vec{u}_R = (4, 1, 5, 1, 4),\ \overrightarrow{u_R}^{(-1)} = (2, 2, 0, 4, 0) \text{ and } \vec{x}_R = (1, 5, 5, 1, 2)\,.$$

Now, we are going to multiply $\sum_i \alpha_i\theta_i$ and $\sum_i \beta_i\theta_i$ with $\vec{\alpha} = (6, 3, 6, 1, 2)$ and $\vec{\beta} = (2, 6, 6, 4, 2)$. We first easily find $\vec{\alpha} - \sigma(\vec{\alpha}) = (4, 4, 3, 2, 1)$, $\vec{\beta} - \sigma(\vec{\beta}) = (0, 4, 0, 5, 5)$ and thus $(\vec{\alpha} - \sigma(\vec{\alpha})) \diamond (\vec{\beta} - \sigma(\vec{\beta})) = (0, 2, 0, 3, 5)$.

Therefore,

$$\begin{aligned} (\mathfrak{a}^2\vec{\iota}) \star \Big((\vec{\alpha} - \sigma(\vec{\alpha})) \diamond (\vec{\beta} - \sigma(\vec{\beta}))\Big) &= (6, 0, 4, 5, 5)\,, \\ (\vec{u}_R \star \vec{\alpha}) \diamond (\vec{u}_R \star \vec{\beta}) &= (0, 4, 0, 3, 0)\,, \\ (\mathfrak{a}^2\vec{x}_R) \star \Big((\vec{\alpha} - \sigma(\vec{\alpha})) \diamond (\vec{\beta} - \sigma(\vec{\beta}))\Big) &= (1, 1, 0, 1, 4)\,. \end{aligned}$$

It remains to compute

$$\overrightarrow{u_R}^{(-1)} \star ((\vec{u}_R \star \vec{\alpha}) \diamond (\vec{u}_R \star \vec{\beta}) - (\mathfrak{a}^2\vec{x}_R) \star ((\vec{\alpha} - \sigma(\vec{\alpha})) \diamond (\vec{\beta} - \sigma(\vec{\beta})))) = (4, 5, 4, 0, 1)\,,$$

and finally, we obtain

$$(\sum_i \alpha_i\theta_i) \times (\sum_i \beta_i\theta_i) = 3\,\theta_0 + 5\,\theta_1 + 1\,\theta_2 + 5\,\theta_3 + 6\,\theta_4\,.$$

5 Beyond Gauss periods

Complexity estimates in Subsection 3.3 and Subsection 4.3.4 suggest that an elliptic basis may be preferred to standard normal basis.

In this section we first show that the main condition for the existence of an elliptic basis is that the degree should not be too large. This is explained in Subsection 5.1. If this condition is not fulfilled, we may translate the field extension along a small auxiliary base change. This is explained in Subsection 5.2. We recall in Subsection 5.3 that fast inversion using Lagrange's theorem and addition chains is possible in the context of elliptic normal bases. In Subsection 5.4 we associate a well chosen polynomial basis to any elliptic basis. We explain how to fast change coordinates between either bases. This gives a quasi-linear division algorithm for elliptic bases.

5.1 Existence conditions for elliptic bases

Let q be a power of a prime p. Given a finite field $\mathbb{F}_q$ and an integer $d \geqslant 2$, we want to construct an elliptic basis for the degree d extension of $\mathbb{F}_q$.

We first need some easy properties of the d_q (cf. Definition 1).

Lemma 7 *Let p be a prime and q a power of p. Let $d \geqslant 2$ be an integer.*

- *If d is prime to $q-1$ then $d_q = d$.*
- *If $q-1$ is squarefree then $d_q \leqslant d^3$.*
- *In any case $d_q \leqslant d^2(q-1)^2$.*
- *If $f \geqslant 1$ is an integer prime to $d\varphi(d)$ then $d_{q^f} = d_q$.*

We can now give a sufficient condition for the existence of an elliptic basis. The necessary background about elliptic curves over finite fields can be found in chapter 5 of Silverman's book [19].

Lemma 8 *Let p be a prime and q a power of p. Let $d \geq 2$ be an integer. We assume that*

$$d_q \leqslant 2\sqrt{q}\,.$$

Then, there exists an elliptic curve E over $\mathbb{F}_q$, a point t of order d in $E(\mathbb{F}_q)$ and a point b in $E(\bar{\mathbb{F}}_q)$ such that $\phi(b) = b + t$ and the order of b is a multiple of d^2. In particular $db \neq 0$.

Proof. There are at least too consecutive multiples of d_q in the interval $[q+1-2\sqrt{q}, q+1+2\sqrt{q}]$. One of them is not congruent to 1 modulo p. We call $M = \lambda d_q$ this integer and we set $\mathfrak{t} = q + 1 - M$ and $\Delta = \mathfrak{t}^2 - 4q$. Let $\mathcal{O}$ be the maximal order in $\mathbb{Q}(\sqrt{\Delta})$. There exists an ordinary elliptic curve E over $\mathbb{F}_q$ such that E has M points over $\mathbb{F}_q$ and $\mathrm{End}(E) = \mathcal{O}$. Let ℓ be a prime divisor of d. We set $e_\ell = v_\ell(d)$.

Assume first that ℓ is prime to $q-1$.

It cannot divide both $q+1-\mathfrak{t}$ and $\mathfrak{t}^2-4q$. So ℓ is prime to $\mathfrak{t}^2-4q$ and is unramified in $\mathbb{Z}[\phi]$ and in $\mathrm{End}(E)$. If ℓ were inert, it would divide both $\phi-1$ and its conjugate $\bar{\phi}-1$ and also the trace $\mathrm{Tr}(\phi-1)=\mathfrak{t}-2$. Since ℓ divides $q+1-\mathfrak{t}$ this would imply that ℓ divides $q-1$, a contradiction. So ℓ splits in $\mathbb{Z}[\phi]$. Let $\mathfrak{l}=(\ell,\phi-1)$ be the ideal in $\mathrm{End}(E)$ above ℓ and containing $\phi-1$. This prime ideal divides $\phi-1$ exactly e times, where $e\geq e_\ell$ is the valuation of M at ℓ. Let λ be the unique root of $(X+1)^2-\mathfrak{t}(X+1)+q$ in $\mathbb{Z}_\ell$ that is congruent to 0 modulo ℓ. The ℓ-adic valuation of λ is e. The kernel of $\mathfrak{l}^{e+e_\ell}$ is cyclic of order ℓ^{e+e_ℓ}. The Frobenius ϕ acts on this group as multiplication by $1+\lambda$. Let b_ℓ be a generator of this group. We set $t_\ell=\phi(b_\ell)-b_\ell$ and we check that t_ℓ has order ℓ^{e_ℓ} and is $\mathbb{F}_q$-rational. Indeed t_ℓ is left invariant by ϕ because $e\geqslant e_\ell$.

Assume now ℓ divides $q-1$.

So $v_\ell(M)\geq v_\ell(d_q)>2v_\ell(q-1)$. We check

$$\mathfrak{t}^2-4q=(q-1)^2+M^2-2M(q+1)=(q-1)^2+O(\ell^s)$$

where $s=v_\ell(M)>2v_\ell(q-1)$ if ℓ is odd, and $s=v_\ell(M)+2>2v_\ell(q-1)+2$ if $\ell=2$.

We deduce $\mathfrak{t}^2-4q$ is a square in $\mathbb{Z}_\ell$ and ℓ splits in $\mathrm{End}(E)$. Let λ_1 and λ_2 be the two roots of $(X+1)^2-\mathfrak{t}(X+1)+q$ in $\mathbb{Z}_\ell$. Since $\lambda_1\lambda_2=q+1-\mathfrak{t}=M$, one of these two roots has ℓ-adic valuation $\geqslant e_\ell$. Assume for example $v_\ell(\lambda_1)=e_1\geqslant e_\ell$. The $\ell^{e_1+e_\ell}$-torsion group $E[\ell^{e_1+e_\ell}]$ has a cyclic subgroup V_1 of order $\ell^{e_1+e_\ell}$ where ϕ acts as multiplication by $1+\lambda_1$.

Let b_ℓ be a point of order $\ell^{e_1+e_\ell}$ in V_1. We set $t_\ell=\phi(b_\ell)-b_\ell=\lambda_1 b_\ell$. This is a point of order ℓ^{e_ℓ}. It is left invariant by ϕ because $e_1\geqslant e_\ell$. So again t_ℓ is in $E[\ell^{e_\ell}](\mathbb{F}_q)$.

We now patch all these points together.

We set $t=\sum_\ell t_\ell$ and $b=\sum_\ell b_\ell$. We have $\phi(b)-b=t$ and t has order d. The order of the point b is a multiple of $\prod_\ell \ell^{2e_\ell}=d^2$. In particular $db\neq 0$.

□

Lemma 9 *Let p be a prime and q a power of p. Let $d\geq 2$ be an integer. We assume that*

$$d_q\leqslant\sqrt{q}\,.$$

Then, there exists an elliptic curve E over $\mathbb{F}_q$, a point t of order d in $E(\mathbb{F}_q)$ and a point b in $E(\bar{\mathbb{F}}_q)$ such that $\phi(b)=b+t$ and the order of b is a multiple of d^2. In particular $db\neq 0$. There is also a point R in $E(\mathbb{F}_q)$ that such that $dR\neq 0$.

Proof. We apply lemma 8 above to p, q and $d'=2d\leqslant 2\sqrt{q}$. We obtain an elliptic curve E, a point t' of order $d'=2d$ in $E(\mathbb{F}_q)$ and a point b' such that $\phi(b')=b'+t'$. We set $t=2t'$, $b=2b'$ and $R=t$ and we are done.

□

5.2 Base change

Let q be a prime power and let d be an integer. If d is too large we may not be able to construct an elliptic basis for the degree d extension of $\mathbb{F}_q$. We try to embed $\mathbb{F}_q$ into some small degree auxiliary extension $\mathbf{K} = \mathbb{F}_Q$ with $Q = q^f$ then construct an elliptic basis for the degree d extension $\mathbf{L}$ of $\mathbf{K}$. We shall need the following lemma.

Lemma 10 (Iwaniec) *There exists a constant* $K_{\mathrm{Iw}} \geqslant 1$ *such that the following is true.*

Let $k \geqslant 2$ *be an integer and let* $p_1, p_2, \ldots, p_k$ *be distinct prime integers. Let* μ_i *and* μ_s *be two integers with* $\mu_s - \mu_i \geqslant K_{\mathrm{Iw}} k^2 (\log k)^2$*. Let* I *be the interval* $[\mu_i, \mu_s]$*. There is an integer* n *in* I *that is prime to every* p_i *for* $i \in \{1, 2, \ldots, k\}$*.*

This lemma is proven by Iwaniec in [14].

The number of prime divisors of d is $O(\log d)$. We look for some integer f such that

- f is prime to $d\varphi(d)$,
- $d_{q^f} = d_q \leqslant q^{\frac{f}{2}}$.

>From Lemma 10, we find some f that is

$$O(\log_q d_q + (\log d)^2 (\log(\log d))^2) = O((\log d)^2 (\log(\log d))^2).$$

In this context, we call $\Phi_q : \bar{\mathbb{F}}_q \to \bar{\mathbb{F}}_q$ the absolute Frobenius of $\mathbb{F}_q$ and $\Phi_Q = \Phi_q^f$ the Frobenius of $\mathbf{K}$. Once given an elliptic basis for $\mathbf{L}/\mathbf{K}$, we can compute efficiently the action of Φ_Q. Let F be an integer such that $1 \leqslant F \leqslant d-1$ and $fF = 1 \bmod d$. The restriction of Φ_Q^F to $\mathbb{F}_{q^d}$ is $\Phi_q : \mathbb{F}_{q^d} \to \mathbb{F}_{q^d}$. We thus can compute efficiently the Frobenius action on $\mathbb{F}_{q^d}$ using the elliptic basis for $\mathbf{L}/\mathbf{K}$.

Elements in $\mathbb{F}_{q^d}$ being represented and treated as elements in $\mathbf{L}$, we have a slight loss of efficiency: the size is multiplied by f. An element in $\mathbb{F}_{q^d}$ is represented by $d \log Q$ bits instead of $d \log q$.

5.3 Inversion using Lagrange's theorem

We have constructed models for finite fields where addition, multiplication and Frobenius action can be quickly computed. We should worry now about inversion.

The inverse of $\alpha \in \mathbb{F}_{q^d}$ can be computed as α^{q^d-2} because of Lagrange Theorem. This exponentiation can be done at the expense of $O(\log q + \log d)$ multiplications in $\mathbb{F}_{q^d}$ using an addition chain for $d-1$ and another addition chain for $q-2$. This is [13, Theorem 2] of Itoh and Tsujii generalized in [20, Corollary 30] by von zur Gathen and Nöcker. The computation also requires $O(\log d)$ exponentiations by powers of q.

5.4 Moving to a polynomial basis and quasi-linear inversion

Using Lagrange's theorem for inversion is one of the possible motivations for using normal bases but it brings an extra $\log q$ factor in the complexity. This may harm if $\log q$ is bigger than any polynomial in $\log d$. So it makes sense to look for an inversion algorithm that uses less than e.g. $Kd(\log d)^2 \log|\log d|$ operations in $\mathbb{F}_q$ where K does not depend on d nor on q.

In this subsection we show that to any elliptic basis one can associate a polynomial r basis such that changing coordinates between either bases can be done in quasi-linear time. This gives another algorithm for fast multiplication in elliptic bases. More importantly, this allows fast division in elliptic bases.

Let $\mathbf{K} = \mathbb{F}_q$, d, $\mathbf{L}$, E, t and b be as in the beginning of Section 4. We further assume $2db \neq 0$. This is guaranteed if we use Lemma 9 and if $d \geqslant 3$. The unitary polynomial

$$\Pi(x) = (x - x(b))(x - x(b+t)) \cdots (x - x(b + (d-1)t)) \in \mathbf{K}[x]$$

is then irreducible.

In order to simplify the presentation, we shall assume in the following that d is odd. There exist a degree $(d+1)/2$ unitary polynomial $Y_1 \in \mathbf{K}[x]$ and a degree $\leqslant (d-3)/2$ polynomial $Y_0 \in \mathbf{K}[x]$ such that the function $Y_1(x) - yY_0(x)$ cancels at b, $b+t$,..., $b + (d-1)t$. Besides Y_1 and Y_0 are coprime and $Y_1(x) - yY_0(x)$ also cancels at $-db$. We precompute these two polynomials.

We denote by $\mathcal{R} \subset \mathbf{K}(E)$ the ring of functions having no pole outside $\{O, t, 2t, \ldots, (d-1)t\}$. The ideal $\mathfrak{b} \subset \mathcal{R}$ of the closed subset $\{b, b+t, b+2t, \ldots, b+(d-1)t\}$ is generated by $\Pi(x)$ and $Y_1(x) - yY_0(x)$.

The system $(1, u_{O,t}, \ldots, u_{O,(d-1)t})$ is a $\mathbf{K}$-basis of $\mathcal{L}_1 = \mathcal{L}(O + t + 2t + \cdots + (d-1)t)$ and reduction modulo $\mathfrak{b}$ (evaluation at b) defines a bijection $\epsilon_1 : \mathcal{L}_1 \to \mathbf{K}(b) = \mathbf{L}$. The system $(1, u_{O,t}(b), \ldots, u_{O,(d-1)t}(b))$ is the elliptic basis Ω.

The system $(1, x, x^2, \ldots, x^{d-1})$ is free and generates a subspace $\mathcal{L}_2$ of $\mathcal{L}((2d-2)O)$. Reduction modulo $\mathfrak{b}$ (evaluation at b) defines a bijection $\epsilon_2 : \mathcal{L}_2 \to \mathbf{K}(b) = \mathbf{L}$. The system $\Psi = (1, x(b), x(b)^2, \ldots, x(b)^{d-1})$ is a $\mathbf{K}$-basis of $\mathbf{L}$. This is a polynomial basis.

In order to change coordinates from Ω to Ψ and back[1], we now explain how to quickly evaluate the bijections $\epsilon_2^{-1} \circ \epsilon_1$ and $\epsilon_1^{-1} \circ \epsilon_2$.

<u>*From Ω to Ψ*</u>.

Recall we have set $\nu_k = x(kt)$ for $k \in \mathbb{Z}/d\mathbb{Z}$. Equation (6) shows that there exist constants $s_k = a_1 x(kt) + a_3 + y(kt)$ in $\mathbf{K}$ such that for $1 \leqslant k \leqslant d-1$

$$u_{O,kt} = \frac{y + s_k}{x - \nu_k}.$$

[1]Recall that changing coordinates from Ω to Θ and back is done in linear time as explained in praragraph 4.2.

Any function f in $\mathcal{L}_1$ is a combination

$$f = \alpha_0 + \sum_{1 \leqslant k \leqslant d-1} \alpha_k \frac{y + s_k}{x - \nu_k}$$

with $\alpha_k \in \mathbb{F}_q$ for $0 \leqslant k \leqslant d-1$. We set

$$D(x) = \prod_{1 \leqslant k \leqslant (d-1)/2} (x - \nu_k).$$

We can rewrite f as $(U(x) + yV(x))/D(x)$ where $U(x)$ and $V(x)$ are polynomials in $\mathbf{K}[x]$ with degree $\leqslant \frac{d-3}{2}$.

The numerator $U(x) + yV(x)$ can be computed at the expense of $O(d(\log d)^2 \log|\log d|)$ operations in $\mathbb{F}_q$ using a divide and conquer algorithm.

Now the function f is congruent modulo $\mathfrak{b}$ to $(U(x) + M(x)V(x))/D(x)$. There exists a polynomial $W(x) \in \mathbf{K}[x]$ with degree $\leqslant d-1$ that is congruent to the later fraction modulo $\Pi(x)$. We compute it at the expense of $O(d(\log d)^2 \log|\log d|)$ operations in $\mathbb{F}_q$ using standard fast modular multiplication and inversion algorithms. This polynomial $W(x)$ is nothing but $\epsilon_2^{-1}(\epsilon_1(f))$.

From Ψ to Ω.

Conversely, let $W(x) \in \mathcal{L}_2$ be a polynomial in $\mathbf{K}[x]$ with degree $\leqslant d-1$. We look for a function $f = \alpha_0 + \sum_{1 \leqslant k \leqslant d-1} \alpha_k (y + s_k)/(x - \nu_k)$ in $\mathcal{L}_1$ that is congruent to $W(x)$ modulo $\mathfrak{b}$.

For $k \neq 0$ in $\mathbb{Z}/d\mathbb{Z}$ we set

$$D_k(x) = \prod_{1 \leqslant l \leqslant (d-1)/2,\ l \not\equiv \pm k \bmod d} (x - \nu_l) = D(x)/(x - \nu_k).$$

We assume we have precomputed the $D_k(\nu_k)$ for $1 \leqslant k \leqslant (d-1)/2$ using fast multipoint evaluation of the derivative $D'(x)$ at the expense of $O(d(\log d)^2 \log|\log d|)$ operations in $\mathbb{F}_q$.

We first compute a degree $\leqslant d-1$ polynomial $N(x)$ that is congruent to $W(x)D(x)Y_0(x)$ modulo $\Pi(x)$. This is done at the expense of $O(d(\log d)^2 \log|\log d|)$ operations in $\mathbb{F}_q$ using a standard fast modular multiplication and reduction algorithm.

We have

$$N(x) \equiv D(x)Y_0(x)f \equiv \alpha_0 D(x)Y_0(x) + \sum_{1 \leqslant k \leqslant d-1} \alpha_k D_k(x)(Y_1(x) + s_k Y_0(x)) \bmod \mathfrak{b}.$$

The leftmost and rightmost terms in the above congruence are polynomials in x with degree $\leqslant d-1$. Therefore they are equal. Since $D_k = D_{-k}$, we obtain

$$N(x) = \alpha_0 D(x)Y_0(x) + \sum_{1 \leqslant k \leqslant (d-1)/2} (\alpha_k(Y_1(x) + s_k Y_0(x)) + \alpha_{-k}(Y_1(x) + s_{-k}Y_0(x)))D_k(x).$$

We set

$$A_0(x) = \sum_{1\leqslant k\leqslant (d-1)/2} (\alpha_k s_k + \alpha_{-k} s_{-k}) D_k \quad \text{and} \quad A_1(x) = \sum_{1\leqslant k\leqslant (d-1)/2} (\alpha_k + \alpha_{-k}) D_k \qquad (16)$$

and we obtain

$$N(x) = \alpha_0 D(x) Y_0(x) + A_0(x) Y_0(x) + A_1(x) Y_1(x).$$

We now reduce this identity modulo $Y_1(x)$. Let $\hat{N}(x) \in \mathbf{K}[x]$ be a polynomial with degree $\leqslant (d-1)/2$ that is congruent to $N(x)/Y_0(x)$ modulo $Y_1(x)$. We have $A_0(x) = \hat{N}(x) - \alpha_0 D(x)$ where α_0 is the only constant in $\mathbf{K}$ such that $\hat{N}(x) - \alpha_0 D(x)$ has degree $\leqslant (d-3)/2$. Once we know α_0 and $A_0(x)$ we set $A_1(x) = (N(x) - \alpha_0 D(x) Y_0(x) - A_0(x) Y_0(x))/Y_1(x)$.

>From equations (16) we deduce

$$\begin{aligned} \alpha_k s_k + \alpha_{-k} s_{-k} &= A_0(\nu_k)/D_k(\nu_k), \\ \alpha_k + \alpha_{-k} &= A_1(\nu_k)/D_k(\nu_k). \end{aligned}$$

These pairs of equations allow us to compute all the α_k from the $A_0(\nu_k)$, $A_1(\nu_k)$, and $D_k(\nu_k)$ at the expense of $O(d)$ operations in $\mathbf{K}$. The $A_0(\nu_k)$ and $A_1(\nu_k)$ are computed using a fast multipoint evaluation algorithm at the expense of $O(d(\log d)^2 \log|\log d|)$ operations in $\mathbb{F}_q$.

References

[1] L.M. Adleman and H.W. Lenstra. Finding irreducible polynomials over finite fields. *Proceedings of the 18th Annual ACM Symposium on the Theory of Computing*, pages 350–355, 1986.

[2] D.W. Ash, I.F. Blake, and S.A. Vanstone. Low complexity normal basis. *Discrete Applied Mathematics*, pages 191–200, 1989.

[3] S. Ballet. An improvement of the construction of the D.V. and G.V. Chudnovsky algorithm for multiplication in finite fields. *Theoretical Computer Science*, 352:293–305, 2006.

[4] J. Canon, W. Bosma, C. Fieker, and A. Steel. *Handbook of Magma Functions*. Sydney, May 2008. Version 2.14.

[5] D.G. Cantor and E. Kaltofen. On fast multiplication of polynomials over arbitrary algebras. *Acta Inform.*, 28:693–701, 1991.

[6] J. Chaumine. Complexité bilinéaire de la multiplication dans des petits corps finis. *C.R. Acad. Sci. Paris, Ser. I*, 343, 2006.

[7] M. Christopoulou, T. Garefalakis, D. Panario, and D. Thomson. The trace of an optimal normal element and low complexity normal bases. *Designs, Codes and Cryptography*, 2008.

[8] D.V. Chudnovsky and G.V. Chudnovsky. Algebraic Complexities and Algebraic Curves over Finite Fields. *J. Complexity*, 4:285–316, 1988.

[9] J.-M. Couveignes and R. Lercier. Galois invariant smoothness basis. *Series on number theory and its application*, 5:154–179, 2008.

[10] S. Gao. *Normal basis over finite fields.* PhD Thesis, Waterloo University, 1993.

[11] S. Gao and H.W. Lenstra. Optimal normal basis. *Designs, Codes and Cryptography*, 2:315–323, 1992.

[12] S. Gao, J. von zur Gathen, D. Panario, and V. Shoup. Algorithms for exponentiation in finite fields. *J. Symbolic Comput.*, 29(6):879–889, 2000.

[13] T. Itoh and S. Tsujii. A fast algorithm for computing multiplicative inverses in $GF(2^m)$ using normal basis. *Information and Computation*, 78:171–177, 1988.

[14] H. Iwaniec. On the problem of Jacobsthal. *Demonstratio Math.*, 11:225–231, 1978.

[15] R.C. Mullin, I.M. Onyszchuk, S.A. Vanstone, and R.M. Wilson. Optimal normal basis in $GF(p^n)$. *Discrete Applied Math.*, 22:149–161, 1989.

[16] A. Schönhage. Schnelle Multiplikation von Polynomen über Körpen der Characteristik 2. *Acta Inform.*, 7:395–398, 1977.

[17] A. Schönhage and V. Strassen. Schnelle Multiplikation grosser Zahlen. *Computing*, 7:281–292, 1971.

[18] M.A. Shokrollahi. Optimal Algorithms for Multiplication in Certain Finite Fields using Algebraic Curves. *SIAM J. Comp.*, 21(6):1193–1198, 1992.

[19] J. Silverman. *The Arithmetic of Elliptic Curves.* Springer, 1986.

[20] J. von zur Gathen and M. Nöcker. Computing special powers in finite fields. *Math. Comp.*, 73(247):1499–1523, 2004.

[21] Zhe-Xian Wan and Kai Zhou. On the complexity of the dual basis of a type i optimal normal basis. *Finite Fields and their Applications*, 13:411–417, 2007.

[22] A. Wassermann. Zur Arithmetik in endlichen Körpern. *Bayreuther Math. Schriften*, 44:147–251, 1993.