Elliptic periods and primality proving. Journal of Number Theory, 133(1):343-368, 2013.

ELLIPTIC PERIODS AND PRIMALITY PROVING

TONY EZOME AND REYNALD LERCIER

Abstract. We construct extension rings with fast arithmetic using isogenies between elliptic curves. As an application, we give an elliptic version of the AKS primality criterion.

1. Introduction

Classical Kummer theory considers binomials of the form $x^d - \alpha$ where $d \geqslant 2$ is an integer and α is a unit in a (commutative and unitary) ring containing a primitive d-th root of unity ζ. The associated R-algebra $S = R[x]/(x^d - \alpha)$ has shown to be extremely useful, including in very recent algorithmic applications such as integer factoring and discrete logarithm computation [12], primality proving [1, 6], fast polynomial factorization and composition [14], low complexity normal basis [20, 11, 2] of field extensions and ring extensions [17].

Part of this computational relevance is due to the purely algebraic properties of S: a finite free étale R-algebra of rank d, endowed with an R-automorphism $\sigma : x \mapsto \zeta x$ such that R is the ring of invariants by σ in S (see Section 3.1). However, there are more geometric properties involved. For example, we can define the degree of a non-zero class in $R[x]/(x^d - \alpha)$ to be the smallest degree of non-zero polynomials in this class. This degree is subadditive and invariant by the automorphism σ. To understand this, it is sensible to introduce the multiplicative group $\mathbf{G}_m = \mathrm{Spec}(R[x, 1/x])$ over R and the multiplication by d isogeny $[d] : \mathbf{G}_m \to \mathbf{G}_m$. Then $x = \alpha$ defines a section A of $\mathbf{G}_m \to \mathrm{Spec}(R)$ and S can be seen as the residue ring at $\mathfrak{F}_A = [d]^{-1}(A)$. The kernel of $[d]$ is the disjoint union of d sections in $\mathbf{G}_m(R)$. Let T be the one defined by $x = \zeta$. Translation by T defines an automorphism of $\mathbf{G}_m$ that stabilizes $\mathfrak{F}_A$. One can then view elements in S as congruence classes of functions on $\mathbf{G}_m$ modulo $\mathfrak{F}_A$.

The main restriction of classical Kummer theory is that not every ring R has a primitive d-th root of unity. One may look for an auxiliary extension $R' \supset R$ that contains such a primitive root, but this may result in many complications and a great loss of efficiency. Another approach, already experimented in the context of normal bases [9] for finite fields extensions, consists in replacing the multiplicative group $\mathbf{G}_m$ by some well chosen elliptic curve E over R. We then look for a section $T \in E(R)$ of exact order d. Because elliptic curves are many, we increase our chances to find such a section. We call the resulting algebra S a ring of *elliptic periods* because of the strong analogy with classical Gauss periods.

The first half of the present work is devoted to the explicit study of Kummer theory of elliptic curves and, more specifically, to the algebraic and algorithmic description of the residue algebras constructed as sketched above. The resulting elliptic functions and equations are not quite as simple as binomials. Still they can be described very explicitly and quickly, e.g. in quasi-linear time in the degree d. The geometric situation is summarized by Theorem 1 and the R-algebra S of elliptic periods is described by Theorem 2. The second half of the paper

Date: January 10, 2015.

Research supported by the "Délégation Générale pour l'Armement" and by the "Agence Nationale de la Recherche" (project ALGOL).

proposes an elliptic version of the AKS primality criterion. A general, context free, primality criterion in the style of Berrizbeitia is first given in Theorem 3. This criterion involves an R-algebra S where $R = \mathbb{Z}/n\mathbb{Z}$ and n is the integer to be tested for primality. If we take S to be $R[x]/(x^d - \alpha)$, we recover results by Berrizbeitia and his followers. If we take S to be a ring of elliptic periods, we obtain the elliptic primality criterion of Corollary 2.

Similarly to the ECPP algorithm [15, 19], this algorithm is *Las Vegas probabilistic*. The behavior of a Las Vegas algorithm depends on the input of course, but also on the result of some random choices. It either stops with the correct result or informs that it failed. The running time is bounded from above by the same asymptotic bound as ECPP, *i.e.* $(\log n)^{3+o(1)}$ multiplications in $\mathbb{Z}/n\mathbb{Z}$. Nevertheless, the space requirement of our elliptic version of the AKS primality criterion is larger, $(\log n)^{3+o(1)}$ bits instead of $(\log n)^{2+o(1)}$ bits. This makes it at the time of writing less suitable than ECPP for proving the primality of large integers n.

While the proof of Corollary 2 uses the results in Section 2, much of Section 3 is independent of Section 2. Readers only interested in primality proving may skim through Section 2 and read Section 3, then come back to Section 2 for technical details.

Acknowledgments.

We wish to express our grateful acknowledgment to Jean-Marc Couveignes for his help and guidance. Among many other things, he explained to us how elliptic periods could yield a fast variant of the AKS primality criterion and without him, this work would genuinely not have been completed. We are heavily indebted to him.

2. Isogenies between elliptic curves

In this section, we use isogenies between elliptic curves to construct ring extensions. To this end, we extend the methods introduced by Couveignes and Lercier [9] in two different directions. Firstly, we provide efficient explicit expressions for the constants that appear in the multiplication tensor of the ring of elliptic periods. Thanks to these formulae, one can construct the ring of elliptic periods in quasi-linear time. Secondly, we explain how these methods, originally introduced in the context of finite fields, can be adapted to the more general context of rings.

We recall in Section 2.1 more or less classical formulae about elliptic curves and isogenies over fields. In Section 2.2, these formulae are proved to hold true over almost any base ring. In Section 2.3, we use isogenies to construct extension rings and we finally give a numerical example in Section 2.4.

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

2.1. Elliptic curves over fields.

In this section, $\mathbf{K}$ is a field with characteristic p and $E/\mathbf{K}$ is an elliptic curve given by a Weierstrass equation

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

We set

$$b_2 = a_1^2 + 4a_2\,,\ b_4 = a_1a_3 + 2a_4\,,\ b_6 = a_3^2 + 4a_6\,,$$
$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2\,.$$

We denote by $O = [0 : 1 : 0]$ the origin.

Following Vélu [25, 24] and Couveignes and Lercier [9], we state a few identities related to a degree d separable isogeny with cyclic kernel $I : E \to E'$. We exhibit in Section 2.1.3 a normal basis for the field extension $\mathbf{K}(E)/\mathbf{K}(E')$ consisting of degree 2 functions. We study in Section 2.1.4 the matrix of the trace form in this normal basis.

2.1.1. *Some simple elliptic functions.* If A is a point in $E(\overline{\mathbf{K}})$, we denote by $\tau_A : E \to E$ the translation by A. Following [9, Section 2], we set $x_A = x \circ \tau_{-A}$ and $y_A = y \circ \tau_{-A}$.

We check that

$$\begin{aligned} x_A \times (x - x(A))^2 &= (a_3 + 2y(A) + a_1x(A))\,y + x(A)x^2 + \\ &+ \left(a_4 + a_1^2x(A) + a_1a_3 + 2a_2x(A) + a_1y(A) + x(A)^2\right)x \\ &+ a_3^2 + a_1a_3x(A) + a_3y(A) + a_4x(A) + 2a_6\,. \end{aligned} \tag{1}$$

We do not give an explicit expression for y_A but we check that $y_A \times (x - x(A))^3$ can be written as a polynomial in $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x(A), y(A), x, y]$. We also check that

$$(x_A - x(A))(x_{-A} - x(A)) = -\frac{\psi_3(a_1, a_2, a_3, a_4, a_6, x(A))}{(x - x(A))^2} - \frac{\hat{\psi}_3(a_1, a_2, a_3, a_4, a_6, x(A))}{x - x(A)} \tag{2}$$

where $\psi_3(a_1, a_2, a_3, a_4, a_6, x)$ is the so-called 3-division polynomial:

$$\psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8\,,$$

and

$$\hat{\psi}_3 = \psi_3'/3 = 4x^3 + b_2x^2 + 2b_4x + b_6\,.$$

We also check that the resultant of ψ_3 and $\hat{\psi}_3$ in the variable x is

$$\mathrm{Res}_x(\psi_3, \hat{\psi}_3) = -\Delta^2 \tag{3}$$

where $\Delta \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$ is the discriminant of the elliptic curve E.

If A, B and C are three pairwise distinct points in $E(\overline{\mathbf{K}})$, we define $\Gamma(A, B, C)$ as in [9, Section 2],

$$\Gamma(A, B, C) = \frac{y(C - A) - y(A - B)}{x(C - A) - x(A - B)}\,. \tag{4}$$

Taking for C the generic point on E, we define a function $u_{A,B} \in \overline{\mathbf{K}}(E)$ by $u_{A,B}(C) = \Gamma(A, B, C)$. It has two simple poles: one at A and one at B. The following identities are proven in [9, Section 2].

$$\begin{aligned} \Gamma(A, B, C) &= \Gamma(B, C, A) = -\Gamma(B, A, C) - a_1\,, \\ &= -\Gamma(-A, -B, -C) - a_1\,, \\ u_{A,B} + u_{B,C} + u_{C,A} &= \Gamma(A, B, C) - a_1\,, \\ u_{A,B}u_{A,C} &= x_A + \Gamma(A, B, C)u_{A,C} + \Gamma(A, C, B)u_{A,B} \\ &\quad + a_2 + x_A(B) + x_A(C)\,, \end{aligned} \tag{5}$$

$$u_{A,B}^2 = x_A + x_B - a_1u_{A,B} + x_A(B) + a_2\,. \tag{6}$$

We further can prove in the same way

$$\begin{array}{rcl} x_C u_{A,B} &=& \Gamma(A,B,C) x_C + x_B(C) u_{C,B} - x_A(C) u_{C,A} + y_A(C) - y_B(C)\,, \\ x_A u_{A,B} &=& y_A + x_B(A) u_{A,B} - y_B(A)\,, \\ x_B u_{A,B} &=& -y_B - a_1 x_B - a_3 + x_B(A) u_{A,B} - y_B(A)\,. \end{array}$$

2.1.2. *Vélu's formulae.* Let $d \geqslant 3$ be an odd integer and let $T \in E(\mathbf{K})$ be a point of order d. For k an integer, we set $x_k = x_{kT}$, $y_k = y_{kT}$ and following Vélu [25], we define

$$x' = x + \sum_{1 \leqslant k \leqslant d-1} [x_k - x(kT)] \text{ and } y' = y + \sum_{1 \leqslant k \leqslant d-1} [y_k - y(kT)]\ . \tag{7}$$

We also set

$$\begin{array}{rcl} w_4 &=& \displaystyle\sum_{1 \leqslant k \leqslant (d-1)/2} 6\,x(kT)^2 + b_2\,x(kT) + b_4\,, \\ w_6 &=& \displaystyle\sum_{1 \leqslant k \leqslant (d-1)/2} 10\,x(kT)^3 + 2\,b_2\,x(kT)^2 + 3\,b_4\,x(kT) + b_6\,, \\ a'_4 &=& a_4 - 5w_4\,, \\ a'_6 &=& a_6 - b_2 w_4 - 7w_6\,, \end{array}$$

and

$$a'_1 = a_1,\ a'_2 = a_2,\ a'_3 = a_3\,. \tag{8}$$

Vélu proves the identity

$$(y')^2 + a'_1 x' y' + a'_3 y' = (x')^3 + a'_2 (x')^2 + a'_4 x' + a'_6\,.$$

So the map $(x, y) \mapsto (x', y')$ defines a degree d isogeny $I : E \to E'$ where E' is the elliptic curve given by the above Weierstrass equation.

2.1.3. *Elliptic normal basis.* Let

$$U_k = u_{kT,(k+1)T} \text{ and } u_k = \mathfrak{a} u_{kT,(k+1)T} + \mathfrak{b} \tag{9}$$

where $\mathfrak{a} \neq 0$ and $\mathfrak{b}$ are scalars in $\mathbf{K}$ chosen such that

$$\sum_{k \in \mathbb{Z}/d\mathbb{Z}} u_k = 1. \tag{10}$$

Such scalars always exist by [9, Lemma 4]. For k and l distinct and non-zero in $\mathbb{Z}/d\mathbb{Z}$, we set

$$\Gamma_{k,l} = \Gamma(O, kT, lT). \tag{11}$$

Recall

$$u_{O,kT} = \frac{y - y(-kT)}{x - x(kT)}\,. \tag{12}$$

We check that

$$U_k = u_{kT,(k+1)T} = u_{O,(k+1)T} - u_{O,kT} + \Gamma_{k,k+1}\,. \tag{13}$$

The system $(u_k)_{k \in \mathbb{Z}/d\mathbb{Z}}$ is a basis of $\mathbf{K}(E)$ over $\mathbf{K}(E')$. More precisely, we have the following lemma, that generalizes Lemma 5 of [9].

Lemma 1 (A normal basis)**.** *Let E be an elliptic curve over a field $\mathbf{K}$. Let $T \in E(\mathbf{K})$ be a point of odd order $d \geqslant 3$ and $I : E \to E'$ be the degree d separable isogeny defined from T by Vélu's formulae. Let $(u_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ be the functions in $\mathbf{K}(E)$ defined above. Then the system $(u_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ is a $\mathbf{K}(E')$-basis of $\mathbf{K}(E)$.*

Moreover, let $\mathbf{L} \supset \mathbf{K}$ be an extension of $\mathbf{K}$ and let $A \in E'(\mathbf{L})$ be a non-zero point. Let $B \in E(\overline{\mathbf{L}})$ be a point on E such that $I(B) = A$ and let

$$I^{(-1)}(A) = [B] + [B + T] + [B + 2T] + \cdots + [B + (d - 1)T]$$

be the fiber of I above A. Then the three following conditions are equivalent:

(i) The images of the $(u_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ in the residue ring at $I^{-1}(A)$ form an $\mathbf{L}$-basis of it;

(ii) The matrix $(u_k(B + lT))_{k,l\in\mathbb{Z}/d\mathbb{Z}}$ is invertible;

(iii) The point A is not in the kernel of the dual isogeny $I' : E' \to E$.

Proof. We preliminary base change E and E' to $\mathbf{L}$ and observe that the $(u_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ are $\mathbf{L}$-linearly independent and form a basis of the linear space $\mathcal{L}(I^{-1}(O'))$ where O' is the origin on E' and $I^{-1}(O') = [O] + [T] + [2T] + \cdots + [(d-1)T]$ is the kernel of I. Indeed, let $(\lambda_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ be scalars in $\mathbf{L}$ such that $f = \sum_{k\in\mathbb{Z}/d\mathbb{Z}} \lambda_k u_k$ is the zero function. Taylor expansions of f at poles of u_k (see [9, Section 2]) show that all λ_k are equal. Since the sum of the u_k is 1, we deduce that every λ_k is zero. So the $(u_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ are $\mathbf{L}$-independent. They form a basis of $\mathcal{L}(I^{-1}(O'))$ because $I^{-1}(O')$ is a degree d divisor (Riemann Roch theorem).

Now, let us prove the second part of the lemma.

To prove that (i) and (ii) are equivalent, we notice that a vector $(\lambda_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ is in the kernel of the matrix $(u_k(B + lT))_{k,l\in\mathbb{Z}/d\mathbb{Z}}$ if and only if $\sum_{k\in\mathbb{Z}/d\mathbb{Z}} \lambda_k u_k(B + lT)$ is zero for every $l \in \mathbb{Z}/d\mathbb{Z}$. This is equivalent to the vanishing of the function $\sum_{k\in\mathbb{Z}/d\mathbb{Z}} \lambda_k u_k$ on the fiber $I^{-1}(A)$. Incidentally, we notice that the matrix $(u_k(B + lT))_{k,l\in\mathbb{Z}/d\mathbb{Z}}$ is circulant.

To show that (iii) implies (i), let $(\lambda_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ be scalars in $\mathbf{L}$ such that $f = \sum_{k\in\mathbb{Z}/d\mathbb{Z}} \lambda_k u_k$ vanishes on the fiber $I^{(-1)}(A)$. If the λ_k are not all zero, then f is non-zero, and its divisor is $I^{(-1)}(A) - I^{(-1)}(O')$. We deduce that $\sum_{k\in\mathbb{Z}/d\mathbb{Z}}[B + kT] - [kT]$ is a principal divisor. Thus $\sum_{k\in\mathbb{Z}/d\mathbb{Z}}(B + kT - kT) = dB = I'(A) = O$, the origin on E. So A lies in the kernel of I'.

Conversely, if A lies in the kernel of I', then the divisor $I^{(-1)}(A) - I^{(-1)}(O')$ is principal. Let f be a non-zero function on E such that $(f) = I^{(-1)}(A) - I^{(-1)}(O')$. Since f lies in $\mathcal{L}(I^{-1}(O'))$, there exists a non-zero vector $(\lambda_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ in $\mathbf{L}^d$ such that $f = \sum_{k\in\mathbb{Z}/d\mathbb{Z}} \lambda_k u_k$. But f vanishes on the fiber $I^{(-1)}(A)$, by construction. So (i) implies (iii).

To finally prove the first part of the lemma, it is now enough to take for A the generic point of $E'/\mathbf{K}$. The generic point is not in the kernel of I' and thus the system $(u_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ is a $\mathbf{K}(E')$-basis of $\mathbf{K}(E)$. □

2.1.4. *The trace form.* Lemma 1 above provides a basis for the residue ring at a fiber $I^{-1}(A) = [B] + \ldots + [B + (d - 1)T]$ where $A \in E'(\mathbf{K})$. We need fast algorithms for multiplying two elements in this residue ring, given by their coordinates in our basis. A prerequisite is to determine the coordinates of $x(B)$ in the basis $(u_k(B))_{k\in\mathbb{Z}/d\mathbb{Z}}$. More generally, we are interested in the coordinates of x in the basis $(u_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ of the $\mathbf{K}(E')$-vector space $\mathbf{K}(E)$. The reason is that when multiplying u_k and u_l there appear some translates of x. See Eqs. (5) and (6). We will give explicit expressions for these coordinates and explain how to compute them efficiently. We shall make use of the trace form of $\mathbf{K}(E)/\mathbf{K}(E')$. Remind this is a non-degenerate quadratic form. For f a function on E, we denote by $\mathrm{Tr}(f)$ the sum $\sum_{k\in\mathbb{Z}/d\mathbb{Z}} f\circ\tau_{kT}$. It can be seen as a function on E'. Our goal is to compute $\mathrm{Tr}(u_{O,kT})$, $\mathrm{Tr}(u_k u_l)$ and $\mathrm{Tr}(u_k x)$ as linear combinations of 1, x' and y'. We then deduce an explicit formula for the determinant of the trace form.

2.1.4.1. Traces of $u_{O,kT}$. For $1\leqslant k\leqslant d-1$, we set $c_k=\mathrm{Tr}(u_{O,kT})$. It is proven in [9, Section 4.2] that

$$c_1=\mathrm{Tr}(u_{O,T})=\sum_{1\leqslant l\leqslant d-2}\Gamma_{l,l+1}-a_1\,. \tag{14}$$

Assume k, l and $k+l$ are non-zero in $\mathbb{Z}/d\mathbb{Z}$, then $\mathrm{Tr}(u_{O,(k+l)T})=\mathrm{Tr}(u_{O,kT})+\mathrm{Tr}(u_{O,lT})-d\Gamma_{k,k+l}$. Thus,

$$c_{k+l}=c_k+c_l-d\Gamma_{k,k+l}\,. \tag{15}$$

This formula enables us to compute all the c_k for $1\leqslant k\leqslant d-1$, at the expense of $O(d)$ operations in $\mathbf{K}$. Indeed, we first compute the coordinates $(x(kT),y(kT))$ for $1\leqslant k\leqslant d-1$. Then, using Eqs. (4) and (11), we compute $\Gamma_{k,k+1}$ for every $1\leqslant k\leqslant d-2$. We then use Eq. (14) to compute c_1. Finally, we use Eq. (15) repeatedly for $l=1$ and $1\leqslant k\leqslant d-2$, and we deduce the values of $c_2,\ldots,c_{d-1}$.

2.1.4.2. Traces of $u_k u_l$. Assume first that $k\notin\{-1,0,1\}$, so O, T, kT and $(k+1)T$ are pairwise distinct. Then

$$\begin{aligned}
U_0U_k &= u_{O,T}(u_{O,(k+1)T}-u_{O,kT}+\Gamma_{k,k+1})\,,\\
&= x+\Gamma_{1,k+1}u_{O,(k+1)T}-\Gamma_{1,k+1}u_{O,T}+x(T)+x((k+1)T)\\
&\quad -x-\Gamma_{1,k}u_{O,kT}+\Gamma_{1,k}u_{O,T}-x(T)-x(kT)+\Gamma_{k,k+1}u_{O,T}\,,\\
&= \Gamma_{1,k+1}(u_{O,(k+1)T}-u_{O,T})-\Gamma_{1,k}(u_{O,kT}-u_{O,T})\\
&\quad +x((k+1)T)-x(kT)+\Gamma_{k,k+1}u_{O,T}\,.
\end{aligned}$$

So

$$\mathrm{Tr}(U_0U_k)=\Gamma_{1,k+1}(c_{k+1}-c_1)-\Gamma_{1,k}(c_k-c_1)+d(x((k+1)T)-x(kT))+\Gamma_{k,k+1}c_1\,. \tag{16}$$

For $k=0$, we have $U_0^2=x+x_T-a_1u_{0,T}+x(T)+a_2$. And thus

$$\mathrm{Tr}(U_0^2)=2x'+d(x(T)+a_2)-a_1c_1+2\sum_{1\leqslant l\leqslant d-1}x(lT)\,. \tag{17}$$

For $k=-1$, we have

$$\begin{aligned}
U_0U_{-1} &= u_{O,T}u_{-T,O}=-u_{O,T}u_{O,-T}-a_1u_{O,T}\,,\\
&= -(x+\Gamma_{1,-1}u_{O,-T}-\Gamma_{1,-1}u_{O,T}+a_2+x(T)+x(-T))\,,\\
&= -x+\Gamma_{1,-1}(u_{-T,O}+a_1)+\Gamma_{1,-1}u_{O,T}-a_2-2x(T)\,.
\end{aligned}$$

And thus

$$\mathrm{Tr}(U_0U_{-1})=-x'+2\Gamma_{1,-1}c_1+d(a_1\Gamma_{1,-1}-a_2)-2dx(T)-\sum_{1\leqslant l\leqslant d-1}x(lT)\,. \tag{18}$$

Finally, for $k=1$, we have

$$\mathrm{Tr}(U_0U_1)=\mathrm{Tr}(U_{-1}U_0)=\mathrm{Tr}(U_0U_{-1})\,. \tag{19}$$

Now, for any k and l, we have

$$\mathrm{Tr}(u_k u_l) = \mathfrak{a}^2\,\mathrm{Tr}(U_k U_l) + \mathfrak{b}^2 d + 2\mathfrak{a}\mathfrak{b}c_1\,. \tag{20}$$

We set

$$\mathfrak{e}_k = \mathrm{Tr}(u_0 u_k)\,. \tag{21}$$

This is a polynomial in x' with degree one if $k \in \{-1,0,1\}$, and zero otherwise. We denote by $\overrightarrow{\mathfrak{e}}$ the vector $(\mathfrak{e}_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$.

Assume now we are given a non-zero point $A \in E'(\mathbf{K})$. For every k in $\mathbb{Z}/d\mathbb{Z}$, we write

$$e_k = \mathfrak{e}_k(A)\,. \tag{22}$$

We can compute the vector $\overrightarrow{e} = (e_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ at the expense of $O(d)$ operations in $\mathbf{K}$. We first compute the coordinates $(x(kT), y(kT))$ for $1 \leqslant k \leqslant d-1$, the coefficients $\Gamma_{k,k+1}$ for every $1 \leqslant k \leqslant d-2$ and the c_k for $1 \leqslant k \leqslant d-1$ as explained in Section 2.1.4.1. We then compute the $\Gamma_{1,k}$ for $2 \leqslant k \leqslant d-1$ using Eqs. (4) and (11). Then, we use Eqs. (16), (17), (18), and (19) to compute the values of the $\mathrm{Tr}(U_0U_k)$ at A. Finally, we use Eq. (20) to deduce $\overrightarrow{e}$.

2.1.4.3. Traces of xu_k. For $k \notin \{-1,0\}$, we have

$$\begin{aligned} xU_k &= x_O u_{kT,(k+1)T}\,, \\ &= \Gamma_{k,k+1}x + x((k+1)T)u_{O,(k+1)T} - x(kT)u_{O,kT} + \\ &\quad\; y((k+1)T) - y(kT) + a_1(x((k+1)T) - x(kT))\,. \end{aligned}$$

And thus,

$$\begin{aligned} \mathrm{Tr}(xU_k) &= \Gamma_{k,k+1}(x' + \sum_{1\leqslant l\leqslant d-1} x(lT)) + x((k+1)T)c_{k+1} - x(kT)c_k + \\ &\quad\; d(y((k+1)T) - y(kT) + a_1(x((k+1)T) - x(kT)))\,. \end{aligned} \tag{23}$$

For $k = 0$, we have

$$xU_0 = x_O u_{O,T} = y + x(T)u_{O,T} + y(T) + a_1x(T) + a_3\,.$$

And thus,

$$\mathrm{Tr}(xU_0) = y' + x(T)c_1 + d(y(T) + a_1x(T) + a_3) + \sum_{1\leqslant l\leqslant d-1} y(lT)\,. \tag{24}$$

For $k = -1$, we have

$$xU_{-1} = x_O u_{-T,O} = -y - a_1x + x(T)u_{-T,O} + y(T) + a_1x(T)\,.$$

And thus,

$$\mathrm{Tr}(xU_{-1}) = -y' - a_1x' + x(T)c_1 + d(y(T) + a_1x(T)) - \sum_{1\leqslant l\leqslant d-1} (y(lT) + a_1x(lT))\,. \tag{25}$$

We set

$$\mathfrak{u}_k = \mathrm{Tr}(xu_k) = \mathfrak{a}\,\mathrm{Tr}(xU_k) + \mathfrak{b}(x' + \sum_{1\leqslant l\leqslant d-1} x(lT))\,.$$

This is a polynomial in x' and y' with total degree at most 1. The vector $\overrightarrow{\mathfrak{u}} = (\mathfrak{u}_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ is the coordinate vector of x in the dual basis of $(u_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$. Remind we are interested in the coordinates of x in the basis $(u_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ itself. Call $\overrightarrow{\hat{\mathfrak{u}}} = (\hat{\mathfrak{u}}_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ these coordinates. We have

$$\overrightarrow{\mathfrak{u}} = \overrightarrow{\mathfrak{e}} \star \overrightarrow{\hat{\mathfrak{u}}}\,. \tag{26}$$

Assume now we are given a non-zero point $A \in E'(\mathbf{K})$. For every k in $\mathbb{Z}/d\mathbb{Z}$, we write

$$\iota_k = \mathfrak{u}_k(A) \text{ and } \hat{\iota}_k = \hat{\mathfrak{u}}_k(A).$$

We can compute the vector $\overrightarrow{\iota} = (\iota_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ at the expense of $O(d)$ operations in $\mathbf{K}$. Then, using Eq. (26), we can compute the vector $\overrightarrow{\hat{\iota}} = (\hat{\iota}_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ at the expense of one division in the degree d convolution algebra over $\mathbf{K}$. This boils down to $d(\log d)^2 \log\log d$ operations in $\mathbf{K}$.

2.1.4.4. The trace form. We now study the trace form in the basis $(u_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$.

The matrix $(\mathrm{Tr}(u_k u_l))_{k,l} = (\mathfrak{e}_{l-k})_{k,l}$ is circulant and its determinant is

$$D = |\mathrm{Tr}(u_k u_l)|_{k,l} = \prod_{k\in\mathbb{Z}/d\mathbb{Z}} \sum_{l\in\mathbb{Z}/d\mathbb{Z}} \zeta^{kl}\mathfrak{e}_l \tag{27}$$

where ζ is a primitive d-th root of unity (that is $\zeta^d = 1$ and $\zeta^k - 1$ is a unit for every $1 \leqslant k \leqslant d-1$).

We compute

$$\sum_{l\in\mathbb{Z}/d\mathbb{Z}} \mathfrak{e}_l = \sum_{l\in\mathbb{Z}/d\mathbb{Z}} \mathrm{Tr}(u_0 u_l) = \mathrm{Tr}(u_0 \sum_{l\in\mathbb{Z}/d\mathbb{Z}} u_l) = \mathrm{Tr}(u_0) = 1\,.$$

Using Eqs. (16), (17), (18) and (19), we deduce that D is a degree $\leqslant d-1$ polynomial in x' and the coefficient of $(x')^{d-1}$ is

$$\mathfrak{a}^{2d-2} \prod_{1\leqslant k\leqslant d-1} (2 - \zeta^k - \zeta^{-k}) = \mathfrak{a}^{2d-2} d^2\,.$$

Since $\mathfrak{e}_k = \mathfrak{e}_{-k}$ for every $k \in \mathbb{Z}/d\mathbb{Z}$, we deduce from Eq. (27) that D is a square.

We now assume that d and the characteristic of $\mathbf{K}$ are coprime. So the degree of $D(x')$ is $d-1$. From Lemma 1, we deduce that the roots of D are the abscissae of points in the kernel of the dual isogeny $I' : E' \to E$ and they all have multiplicity two. Using Eq. (7), we deduce

$$\psi_I^{2d}(x) D(x') = \mathfrak{a}^{2d-2} \psi_d^2(x)\,, \tag{28}$$

where

$$\psi_I(x) = \prod_{1\leqslant k\leqslant (d-1)/2} (x - x(kT)) \tag{29}$$

is the factor of $\psi_d(x)$ corresponding to points in the kernel of I.

2.1.4.5. Example. We detail on a simple example how to construct a ring of elliptic periods. Following [9], we consider the elliptic curve E of order 10 defined by

$$E/\mathbb{F}_7 : y^2 + xy + 5\,y = x^3 + 3\,x^2 + 3\,x + 2\,.$$

The point $T = (3, 1)$ generates a subgroup $T \subset E(\mathbb{F}_7)$ of order $d = 5$. The quotient elliptic curve $E' = E/T$ given by Vélu's formulae has equation

$$E'/\mathbb{F}_7 : y^2 + xy + 5\,y = x^3 + 3\,x^2 + 4\,x + 6\,,$$

and the quotient isogeny is

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

We focus first on $\mathrm{Tr}(u_{O,t})$. We have

$$(u_{O,kt})_{1\leqslant k\leqslant d-1} = \left(\frac{y+2}{x+4}, \frac{y+2}{x+3}, \frac{y}{x+3}, \frac{y+6}{x+4} \right) .$$

A direct but heavy calculation yields

$$c_1 = \frac{y+2}{x+4} + \frac{y+2\,x^2+5}{x^2+5} + \frac{5}{x+3} + \frac{6\,yx+3\,y+2\,x^3+3\,x}{(x^2+5)\,(x+4)} + \frac{6\,y+6\,x+4}{x+4} = 3\,.$$

Alternatively, if we first compute $\Gamma_{1,2} = 2\,,\ \Gamma_{2,3} = 0\,,\ \Gamma_{3,4} = 2$, we more easily come to $c_1 = 2+0+2-1 = 3$. From Eq. (15), we deduce $c_2 = 3\,,\ c_3 = 6\,,\ c_4 = 6$.

Let us now consider $\mathrm{Tr}(U_0^2)$. A direct calculation yields

$$\begin{aligned} \mathrm{Tr}(U_0^2) &= \frac{(y+2)^2}{(x+4)^2} + \frac{(y+2\,x^2+5)^2}{(x^2+5)^2} + \frac{5^2}{(x+3)^2} + \\ &\qquad \frac{(6\,y(x+3)+2\,x^3+3\,x)^2}{\left(x^2+5\right)^2(x+4)^2} + \frac{(6\,y+6\,x+4)^2}{(x+4)^2}\,, \\ &= \frac{2\,x^5+6\,x^4+x^2+3\,x+1}{x^4+3\,x^2+4}\,. \end{aligned}$$

But we can easily deduce from Eq. (17) that this is equal to

$$2\,x' + 5\,(3+3) - 1\,.\,3 + 2\,(3+4+4+3)\,.$$

If we now look more carefully at $\mathrm{Tr}(x\,U_0)$, we have

$$\begin{aligned} \mathrm{Tr}(x\,U_0) &= x\,.\,\frac{y+2}{x+4} + \frac{3\,y+3\,x^2+4\,x+2}{x^2+x+2}\,.\,\frac{y+2\,x^2+5}{x^2+5} + \\ &\quad \frac{2\,y+4\,x^2+3\,x+5}{x^2+6\,x+2}\,.\,\frac{5}{x+3} + \\ &\quad \frac{5\,y(x+1)+4\,x^3+6\,x^2+5\,x+6}{(x^2+6\,x+2)\,(x+3)}\,.\,\frac{6\,yx+3\,y+2\,x^3+3\,x}{(x^2+5)\,(x+4)} + \\ &\quad \frac{4\,y+3\,x^2+x+1}{x^2+x+2}\,.\,\frac{6\,y+6\,x+4}{x+4}\,, \\ &= \frac{y\,\left(x^6+4\,x^4+3\,x^3+6\,x^2+3\,x+4\right)+2\,x^6+3\,x^5+3\,x^4+x^3+6\,x^2+4\,x+6}{x^6+x^4+5\,x^2+6}\,. \end{aligned}$$

But, from Eq. (24), we find that this is equal to

$$y' + 3\,.\,3 + 5\,(1+1\,.\,3+5) + (1+0+5+5)\,.$$

Let us finally notice that since $c_1 = 3 \neq 0$, we can take $\mathfrak{a} = 1/c_1 = 3$ and $\mathfrak{b} = 0$ (see Section 2.1.3). Moreover, let now $A = (4,2) \in E'(\mathbb{F}_7)$. Take $B \in E(\overline{\mathbb{F}}_7)$ such that $I(B) = A$. We set $\tau = x(B) \in \overline{\mathbb{F}}_7$ and check that τ is a root of the irreducible $\mathbb{F}_7$-polynomial $(x^5 + 2\,x^2 + 5\,x + 6) - 4\,(x^4 + 3\,x^2 + 4) = x^5 + 3\,x^4 + 4\,x^2 + 5\,x + 4$. We find that

$$\overrightarrow{e} = (0, 4, 0, 0, 4)\,.$$

2.2. **Universal Weierstrass elliptic curves.** All identities stated in Section 2.1 still make sense and hold true for an elliptic curve over a commutative ring under some mild restrictions. Some (but not all) of these identities are proven in this general context in Vélu's thesis [24] and Katz and Mazur's book [13, Chapter 2]. In this section, we give an elementary proof for all the required identities. We consider in Section 2.2.2 a sort of universal ring for Weierstrass curves with torsion. This ring being an integral domain, the identities hold true in its fraction field. There only remains to check the integrality of all quantities involved. By inverting the determinant of Eq. (27), we define in Section 2.2.3 a localization of the universal ring where the system $(u_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ remains a basis for the function ring extension associated to the isogeny.

2.2.1. *Division polynomials.* Let A_1, A_2, A_3, A_4 and A_6 be indeterminates and set $B_2 = A_1^2 + 4A_2$, $B_4 = 2A_4 + A_1A_3$, $B_6 = A_3^2 + 4A_6$, $B_8 = A_1^2A_6 + 4A_2A_6 - A_1A_3A_4 + A_2A_3^2 - A_4^2$, and

$$\Delta = -B_2^2B_8 - 8B_4^3 - 27B_6^2 + 9B_2B_4B_6\,.$$

Set

$$\mathcal{A}_1 = \mathbb{Z}[A_1, A_2, A_3, A_4, A_6, \frac{1}{\Delta}]\,.$$

Let x and y be two more indeterminates. Set

$$\Lambda(A_1, A_2, A_3, A_4, A_6, x, y) = y^2 + A_1xy + A_3y - x^3 - A_2x^2 - A_4x - A_6 \in \mathcal{A}_1[x, y]\,.$$

Let E_{aff} be the affine smooth plane curve over $\mathcal{A}_1$ with equation $\Lambda(A_1, A_2, A_3, A_4, A_6, x, y) = 0$. Let E be the projective scheme over $\mathcal{A}_1$ with equation $Y^2Z + A_1XYZ + A_3YZ^2 = X^3 + A_2X^2Z + A_4XZ^2 + A_6Z^3$. We denote by O the section $[0, 1, 0]$. We have $E_{\mathrm{aff}} = E - O$ and E is an elliptic curve over (the spectrum of) $\mathcal{A}_1$ in the sense of [13].

For every integer $k \geqslant 0$, we denote by $\psi_k(A_1, A_2, A_3, A_4, A_6, x, y)$ the functions in $\mathcal{A}_1[x, y]/(\Lambda)$ defined recursively as in [10, Proposition 3.53]:

$$\begin{aligned}
&\psi_0 = 0,\ \psi_1 = 1,\ \psi_2 = 2y + A_1x + A_3,\\
&\psi_3 = 3x^4 + B_2x^3 + 3B_4x^2 + 3B_6x + B_8\,,\\
&\psi_4 = \psi_2\left(2x^6 + B_2x^5 + 5B_4x^4 + 10B_6x^3 + 10B_8x^2 + \right.\\
&\qquad\qquad \left.(B_2B_8 - B_4B_6)x + B_4B_8 - B_6^6\right)\,,\\
&\psi_{2k} = \frac{\psi_k}{\psi_2}\left(\psi_{k+2}\psi_{k-1}^2 - \psi_{k-2}\psi_{k+1}^2\right)\,,\\
&\psi_{2k+1} = \psi_{k+2}\psi_k^3 - \psi_{k-1}\psi_{k+1}^3\,.
\end{aligned}$$

These are in $\mathcal{A}_1[x, y]/(\Lambda)$ but we can see them as polynomials in $\mathcal{A}_1[x, y]$ with degree 0 or 1 in y. If k is odd, then ψ_k belongs to $\mathcal{A}_1[x]$ and, as a polynomial in x, we have $\psi_k = kx^{\frac{k^2-1}{2}} + O(x^{\frac{k^2-3}{2}})$. If k is even, then ψ_k/ψ_2 belongs to $\mathcal{A}_1[x]$. The ring $\mathcal{A}_1[x, y]/(\Lambda)$ is an integral domain. Following [10, Proposition 3.52, Proposition 3.55], we define the following elements of its field of fractions:

$$\begin{aligned} g_k &= x - \frac{\psi_{k+1}\psi_{k-1}}{\psi_k^2}, \\ h_k &= y + \frac{\psi_{k+2}\psi_{k-1}^2}{\psi_2\psi_k^3} + \left(3x^2 + 2A_2x + A_4 - A_1y\right)\frac{\psi_{k-1}\psi_{k+1}}{\psi_2\psi_k^2}. \end{aligned}$$

The following important relation holds true:

$$g_k - g_l = -\frac{\psi_{k+l}\psi_{k-l}}{\psi_k^2\psi_l^2} \text{ if } k > l \geqslant 1. \tag{30}$$

We recall that multiplication by k on $E - E[k]$ is given by $(x, y) \mapsto (g_k, h_k)$. Indeed, this is well known on the generic fiber of E and it extends to all E by (Zariski) continuity.

2.2.2. *Universal Vélu's isogenies.* Let $d \geqslant 3$ be an odd integer and let "$x(T)$" and "$y(T)$" be two more indeterminates. Let $\mathcal{S}$ be the multiplicative subset in $\mathcal{A}_1[x(T), y(T)]$ generated by all $\psi_k(x(T), y(T))$ for $1 \leqslant k \leqslant d-1$. Let $\mathcal{A}_d$ be the ring

$$\mathcal{A}_d = \mathcal{A}_1[x(T), y(T), \frac{1}{\mathcal{S}}, \frac{1}{d}]/(\psi_d(x(T)), \Lambda(A_1, A_2, A_3, A_4, A_6, x(T), y(T))).$$

This is an étale algebra over $\mathcal{A}_1[1/d, 1/\mathcal{S}]$. Since the later is a regular ring, $\mathcal{A}_d$ is regular too. This is also an integral domain. Indeed, the d-torsion of the generic Weierstrass curve is irreducible. We denote by $\mathcal{K}_d$ the field of fractions of $\mathcal{A}_d$. The point $T = (x(T), y(T))$ defines a section of E_{aff} over $\mathcal{A}_d$. The curve E, base changed to $\mathcal{A}_d$, may be seen as the universal Weierstrass elliptic curve with a point of exact order d over a ring where d is invertible.

For every integer k such that $1 \leqslant k \leqslant d-1$, the point kT defines a section of E over $\mathcal{A}_d$. We call $x(kT)$ and $y(kT)$ its coordinates and we have

$$\begin{aligned} x(kT) &= g_k(A_1, A_2, A_3, A_4, A_6, x(T), y(T)) \in \mathcal{A}_d, \\ y(kT) &= h_k(A_1, A_2, A_3, A_4, A_6, x(T), y(T)) \in \mathcal{A}_d. \end{aligned}$$

We note that due to Eq. (30), the difference $x(lT) - x(kT)$ is a *unit* in $\mathcal{A}_d$ for any k and l in $\mathbb{Z}/d\mathbb{Z}$ such that k, l, $k+l$ and $k-l$ are not zero. If we base change E to $\mathcal{K}_d$, we obtain an elliptic curve over a field and we can introduce all the scalars and functions of Section 2.1: the $\Gamma_{k,l}$, the x_k, y_k, U_k, x', y', w_4, w_6, c_k... The denominators arising in the definition of these scalars and functions are units in

$$\mathcal{A}_d\left[E - E[d]\right] = \mathcal{A}_d[\frac{1}{\psi_d(x)}, x, y]/(\Lambda(A_1, A_2, A_3, A_4, A_6, x, y)).$$

So all these scalars (resp. functions) are in $\mathcal{A}_d$ (resp. $\mathcal{A}_d\left[E - E[d]\right]$). Especially, we can now define the isogenous curve E' thanks to Eq. (8), then the isogenies I and I'.

There remains to choose $\mathfrak{a}$ and $\mathfrak{b}$. We just take $\mathfrak{a} = 1$ and $\mathfrak{b} = (1 - c_1)/d$. Then the functions $u_k = \mathfrak{a}U_k + \mathfrak{b}$ are in $\mathcal{A}_d\left[E - E[d]\right]$. All equations from Eq. (11) to Eq. (29) still hold true because they are true in $\mathcal{K}_d(E)$ and $\mathcal{A}_d\left[E - E[d]\right]$ embeds in the later field.

2.2.3. *A normal basis.* The open subset $E - E[d]$ is the spectrum of the ring $\mathcal{A}_d\left[E - E[d]\right]$. This is an integral domain and a regular ring (because it is smooth over $\mathcal{A}_d$). Therefore it is integrally closed. The open subset $E' - \operatorname{Ker} I'$ is the spectrum of the ring

$$\mathcal{A}_d\left[E' - \operatorname{Ker} I'\right] = \mathcal{A}_d[\frac{1}{D(x')}, x', y']/(\Lambda(A_1', A_2', A_3', A_4', A_6', x', y')).$$

This is again an integral domain and a regular ring (because it is smooth over $\mathcal{A}_d$). Therefore it is integrally closed too. Eqs. (1), (7), (28) and (29) show that $\mathcal{A}_d\,[E' - \operatorname{Ker} I']$ is included in $\mathcal{A}_d\,[E - E[d]]$. Eqs. (1) and (7) prove that x and y are integral over $\mathcal{A}_d\,[E' - \operatorname{Ker} I']$. We deduce that the translates $(x_k)_{1\leqslant k\leqslant d-1}$ and $(y_k)_{1\leqslant k\leqslant d-1}$ are integral over $\mathcal{A}_d\,[E' - \operatorname{Ker} I']$ too. Using Eq. (2), we deduce that the $1/(x - x(kT))$ are integral over $\mathcal{A}_d\,[E' - \operatorname{Ker} I']$. Note that in the special case $d = 3$, we also need Eq. (3). Now Eqs. (28) and (29) prove that $1/\psi_d(x)$ is integral over $\mathcal{A}_d\,[E' - \operatorname{Ker} I']$. Altogether $\mathcal{A}_d\,[E - E[d]]$ is the integral closure of $\mathcal{A}_d\,[E' - \operatorname{Ker} I']$ in $\mathcal{K}_d(E)$.

Using Eqs. (12) and (13) and the fact that the $1/(x - x(kT))$ are integral over $\mathcal{A}_d[E' - \operatorname{Ker} I']$, we show that the $(u_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ are integral over $\mathcal{A}_d\,[E' - \operatorname{Ker} I']$, therefore belong to $\mathcal{A}_d\,[E - E[d]]$. For every function f in $\mathcal{A}_d\,[E - E[d]]$, the products fu_k are integral over $\mathcal{A}_d\,[E' - \operatorname{Ker} I']$. Therefore their traces $\operatorname{Tr}(fu_k)$ belong to $\mathcal{A}_d\,[E' - \operatorname{Ker} I']$, since this ring is integrally closed. Now remember that the determinant of the trace form is

$$D(x') = |\operatorname{Tr}(u_k u_l)|_{k,l}\ ,$$

a unit in $\mathcal{A}_d\,[E' - \operatorname{Ker} I']$. We deduce that the coordinates of f in the basis $(u_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ are in $\mathcal{A}_d\,[E' - \operatorname{Ker} I']$. We thus have found a basis for the $\mathcal{A}_d\,[E' - \operatorname{Ker} I']$-module $\mathcal{A}_d\,[E - E[d]]$. This finite free module of rank d is also étale because the determinant $D(x')$ of the trace form is a unit.

Let σ be the $\mathcal{A}_d\,[E' - \operatorname{Ker} I']$-automorphism of $\mathcal{A}_d\,[E - E[d]]$ induced by the translation τ_{-T}. We have $\sigma(u_k) = u_{k+1}$ for every $k \in \mathbb{Z}/d\mathbb{Z}$.

Lemma 2 (A freeness result)**.** *The ring*

$$\mathcal{A}_d\,[E - E[d]] = \mathcal{A}_d[\frac{1}{\psi_d(x)}, x, y]/(\Lambda(A_1, A_2, A_3, A_4, A_6, x, y))$$

is a finite free étale algebra of rank d over

$$\mathcal{A}_d\,\left[E' - \operatorname{Ker} I'\right] = \mathcal{A}_d[\frac{1}{D(x')}, x', y']/(\Lambda(A_1', A_2', A_3', A_4', A_6', x', y'))$$

and $(u_k)_{1\leqslant k\leqslant d-1}$ is a basis for this free algebra. For every $k \in \mathbb{Z}/d\mathbb{Z}$, we have $\sigma(u_k) = u_{k+1}$ where σ is the $\mathcal{A}_d\,[E' - \operatorname{Ker} I']$-automorphism of $\mathcal{A}_d\,[E - E[d]]$ induced by the translation τ_{-T}.

The following theorem is proven by base change in Lemma 2.

Theorem 1 (Elliptic Kummer extension)**.** *Let $d \geqslant 3$ be an odd integer. Let R be a ring where d is invertible. Let a_1, a_2, a_3, a_4, a_6, $\mathfrak{x}$ and $\mathfrak{y}$ be elements in R such that*

- *$\Delta(a_1, a_2, a_3, a_4, a_6)$ is a unit in R,*
- *$\psi_d(a_1, a_2, a_3, a_4, a_6, \mathfrak{x}, \mathfrak{y}) = 0$,*
- *$\psi_k(a_1, a_2, a_3, a_4, a_6, \mathfrak{x}, \mathfrak{y})$ is a unit in R for any $1 \leqslant k \leqslant d - 1$.*

Then $T = (\mathfrak{x}, \mathfrak{y})$ is a point of exact order d on the Weierstrass elliptic curve given by the equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ over R.

Set $\mathfrak{a} = 1$ and $\mathfrak{b} = (1 - c_1)/d$ and $u_k = \mathfrak{a}U_k + \mathfrak{b}$. Then all equations from Eq. (11) to Eq. (29) still make sense and hold true in the ring

$$R\,[E - E[d]] = R[\frac{1}{\psi_d(x)}, x, y]/(\Lambda(a_1, a_2, a_3, a_4, a_6, x, y))$$

and this ring is a finite free étale algebra of rank d over

$$R\left[E' - \operatorname{Ker} I'\right] = R[\frac{1}{D(x')}, x', y']/(\Lambda(a_1', a_2', a_3', a_4', a_6', x', y'))$$

and $(u_l)_{1\leqslant l\leqslant d-1}$ is a basis for this free algebra.

For every $k \in \mathbb{Z}/d\mathbb{Z}$, we have $\sigma(u_k) = u_{k+1}$ where σ is the $R\left[E' - \operatorname{Ker} I'\right]$-automorphism of $R\left[E - E[d]\right]$ induced by the translation τ_{-T}.

2.3. **Rings of elliptic periods.** In this section, we give a recipe for constructing an extension of a ring R using an isogeny between two elliptic curves over R. The resulting ring will be called a *ring of elliptic periods*. It will be a finite free étale algebra over R. We just adapt the construction of [9, Section 4] to the case where the base ring is no longer a field. So in this section, R is a ring and $d \geqslant 3$ is an odd integer. We assume that d is invertible in R and that we are given an elliptic curve E over R by its Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ where $\Delta(a_1, a_2, a_3, a_4, a_6)$ is a unit in R. We also are given an R-point $T = (\mathfrak{x}, \mathfrak{y})$ on E with exact order d. We call $I : E \to E'$ the corresponding isogeny, given by Vélu's formulae. Let $D(x') = |\mathfrak{e}_{l-k}|_{k,l}$ be the polynomial in $R[x']$ defined by Eqs. (27), (28) and (21).

We further assume that we are given a section $A = (x'(A), y'(A)) \in E'(R)$ of $E'_{\text{aff}} \to \operatorname{Spec}(R)$. We assume that $D(x'(A))$ is a unit in R. Geometrically, this means that the section A does not intersect the kernel of the dual isogeny $I' : E' \to I$. This is equivalent to the circulant matrix $(\mathfrak{e}_{l-k}(A))_{k,l}$ being invertible. For every k in $\mathbb{Z}/d\mathbb{Z}$, we write $e_k = \mathfrak{e}_k(A)$. This is an element of R. Saying that the circulant matrix $(e_{l-k})_{k,l}$ is invertible means that the vector $\overrightarrow{e} = (e_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ is invertible for the convolution product $\star$ on R^d. We denote by $\overrightarrow{e}^{(-1)}$ the inverse of $\overrightarrow{e}$ for the convolution product. The ideal $(x' - x'(A), y' - y'(A))$ of $R\left[E - E[d]\right] = R[x, y, 1/\psi_d(x)]/(\Lambda(a_1, a_2, a_3, a_4, a_6, x, y))$ is denoted by $\mathfrak{F}_A$. We call

$$S = R[x, y, \frac{1}{\psi_d(x)}]/(\Lambda(a_1, a_2, a_3, a_4, a_6, x, y), \mathfrak{F}_A)\,,$$

the residue ring of $I^{-1}(A)$. We say that S is a ring of elliptic periods. If we specialize at A in Theorem 1, we find that S is a finite free étale R-algebra with basis $\Theta = (\theta_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ where

$$\theta_k = u_k \bmod \mathfrak{F}_A.$$

We call $\sigma : S \to S$ to be the R-automorphism induced on S by the translation τ_{-T},

$$\begin{array}{rrcl} \sigma: & S & \longrightarrow & S\,, \\ & f \bmod \mathfrak{F}_A & \longmapsto & f\circ\tau_{-T} \bmod \mathfrak{F}_A\,. \end{array}$$

It is clear that $\sigma(\theta_k) = \theta_{k+1}$ for all $k \in \mathbb{Z}/d\mathbb{Z}$. So, if $\alpha = \sum_{k\in\mathbb{Z}/d\mathbb{Z}} \alpha_k\theta_k$ is an element of S with coordinates $\overrightarrow{\alpha} = (\alpha_k)_{k\in\mathbb{Z}/d\mathbb{Z}} \in R^d$ in the basis Θ, then the coordinate vector of $\sigma(\alpha)$ is the cyclic shift $\sigma(\overrightarrow{\alpha}) = (\alpha_{k-1})_{k\in\mathbb{Z}/d\mathbb{Z}}$ of $\overrightarrow{\alpha}$. We see that the R-automorphism $\sigma : S \to S$ of the free R-algebra S takes a very simple form on the basis Θ.

We call $\mathcal{L} \subset R(E - E[d])$ the R-module generated by the u_k for $k \in \mathbb{Z}/d\mathbb{Z}$. We know that reduction modulo $\mathfrak{F}_A$ defines an isomorphism of R-modules:

$$\begin{array}{rrcl} \epsilon_A: & \mathcal{L} & \longrightarrow & S\,, \\ & f & \longmapsto & f \bmod \mathfrak{F}_A\,. \end{array}$$

So elements in S can be represented by elements in $\mathcal{L}$.

We now study the multiplication tensor in S. We shall find a simple expression for this tensor using interpolation at some auxiliary points, in the spirit of discrete Fourier transform. We first notice that if $k, l \in \mathbb{Z}/d\mathbb{Z}$ and $k \neq l, l+1, l-1 \bmod d$, then

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

This is proven using Eqs. (5), (9), and (13). Using Eqs. (5), (6), (9), and (13), we also show that

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

So if $(\alpha_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ and $(\beta_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ are two vectors in R^d, we have

$$\begin{aligned}(\sum_k \alpha_k u_k)(\sum_k \beta_k u_k) &= \mathfrak{a}^2 \sum_k \alpha_k\beta_k(x_k + x_{k+1}) - \mathfrak{a}^2 \sum_k \alpha_{k-1}\beta_k x_k - \mathfrak{a}^2 \sum_k \beta_{k-1}\alpha_k x_k \bmod \mathcal{L}\\ &= \mathfrak{a}^2 \sum_k (\alpha_k - \alpha_{k-1})(\beta_k - \beta_{k-1}) x_k \bmod \mathcal{L}. \end{aligned} \tag{31}$$

We now assume we are given an auxiliary section $M = (x(M), y(M))$ of $E_{\text{aff}} \to \operatorname{Spec}(R)$ such that the image $N = I(M)$ of M by I is a section $(x'(N), y'(N))$ of $E'_{\text{aff}} \to \operatorname{Spec}(R)$ and $D(x'(N))$ is a unit in R. So, the residue ring at $I^{-1}(N)$ is a free R-module of rank d and the evaluation map

$$\begin{array}{rccl}\epsilon_N: & \mathcal{L} & \longrightarrow & R^d\,,\\ & f & \longmapsto & (f(M+kT))_{k\in\mathbb{Z}/d\mathbb{Z}}\,.\end{array}$$

is a bijection. Also, the vector

$$\overrightarrow{u_N} = (u_0(M+kT))_{k\in\mathbb{Z}/d\mathbb{Z}} \tag{32}$$

is invertible for the convolution product in R^d. We call $\overrightarrow{u_N}^{(-1)}$ its inverse. We denote by $\overrightarrow{x_N}$ the vector

$$\overrightarrow{x_N} = \epsilon_N(x) = (x(M+kT))_{k\in\mathbb{Z}/d\mathbb{Z}}\,. \tag{33}$$

We note

$$\xi_k = x_k \bmod \mathfrak{F}_A$$

for every $k \in \mathbb{Z}/d\mathbb{Z}$. Since S is free over R and Θ is a basis for it, there exist scalars $(\hat{\imath}_k)_k$ in R such that

$$\xi_0 = \sum_{k\in\mathbb{Z}/d\mathbb{Z}} \hat{\imath}_k \theta_k.$$

So $\overrightarrow{\imath} = (\hat{\imath}_k)_k$ is the coordinate vector of ξ_0 in the basis Θ. In Section 2.1.4.3, we already explained how to compute these coordinates in quasi-linear time in the dimension d.

Let α, β and γ be three elements in S such that $\gamma = \alpha\beta$. Let $\overrightarrow{\alpha} = (\alpha_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ be the coordinate vector of α in the basis Θ. Define $\overrightarrow{\beta}$ and $\overrightarrow{\gamma}$ in a similar way. To compute the multiplication tensor, we use an argument similar to the one of [9, Section 4.3]. We define four functions in $\mathcal{A}_d\,[E - E[d]]$,

$$\begin{aligned} f_\alpha &= \sum_i \alpha_i u_i\,,\ f_\beta = \sum_i \beta_i u_i\,,\\ \mathcal{Q} &= \mathfrak{a}^2 \sum_i (\alpha_i - \alpha_{i-1})(\beta_i - \beta_{i-1}) x_i\,,\\ \mathcal{R} &= f_\alpha f_\beta - \mathcal{Q}\,. \end{aligned}$$

The product we want to compute is $f_\alpha f_\beta = \mathcal{Q} + \mathcal{R} \bmod \mathfrak{F}_A$. From Eq. (31), we deduce that $\mathcal{R}$ is in $\mathcal{L}$. From the definition of $\overrightarrow{\imath}$, we deduce that the coordinates in Θ of $\mathcal{Q} \bmod \mathfrak{F}_A$ are given by the vector

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

The evaluation of f_α at the points $(M+kT)_k$ is the vector $\epsilon_N(f_\alpha) = \overrightarrow{u_N} \star \overrightarrow{\alpha}$. The evaluation of $\mathcal{R}$ is $\epsilon_N(\mathcal{R}) = (\overrightarrow{u_N} \star \overrightarrow{\alpha}) \diamond (\overrightarrow{u_N} \star \overrightarrow{\beta}) - \overrightarrow{x_N} \star (\mathfrak{a}^2(\overrightarrow{\alpha} - \sigma(\overrightarrow{\alpha})) \diamond (\overrightarrow{\beta} - \sigma(\overrightarrow{\beta})))$. If we $\star$ multiply this last vector on the left by $\overrightarrow{u_N}^{(-1)}$, we obtain the coordinates of $\mathcal{R}$ in the basis $(u_0, \dots, u_{d-1})$. These are the coordinates of $\mathcal{R} \bmod \mathfrak{F}_A$ in the basis Θ too.

So the multiplication tensor in the R-basis Θ of the free R-algebra S is given by

$$\begin{aligned} \overrightarrow{\gamma} = (\mathfrak{a}^2 \overrightarrow{\imath}) \star \Big((\overrightarrow{\alpha} - \sigma(\overrightarrow{\alpha})) \diamond (\overrightarrow{\beta} - \sigma(\overrightarrow{\beta}))\Big) + \\ \overrightarrow{u_N}^{(-1)} \star \Big((\overrightarrow{u_N} \star \overrightarrow{\alpha}) \diamond (\overrightarrow{u_N} \star \overrightarrow{\beta}) - (\mathfrak{a}^2 \overrightarrow{x_N}) \star \Big((\overrightarrow{\alpha} - \sigma(\overrightarrow{\alpha})) \diamond (\overrightarrow{\beta} - \sigma(\overrightarrow{\beta}))\Big)\Big) \end{aligned} \tag{34}$$

This multiplication tensor consists of 5 convolution products, 2 component-wise products, 1 addition and 3 subtractions between vectors in R^d.

The following theorem summarizes the results in this section.

Theorem 2 (The ring of elliptic periods)**.** *Let $d \geqslant 3$ be an odd integer. Let R be a ring where d is invertible. Let a_1, a_2, a_3, a_4, a_6, $\mathfrak{x}$ and $\mathfrak{y}$ be elements in R such that $\Delta(a_1, a_2, a_3, a_4, a_6)$ is a unit in R and the point $T = (\mathfrak{x}, \mathfrak{y})$ is a point of exact order d on the Weierstrass elliptic curve over R given by the equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Let $I : E \to E'$ be Vélu's isogeny with kernel $\langle T \rangle$ and let $A = (x'(A), y'(A)) \in E'(R)$ be a section of $E'_{aff} \to \mathrm{Spec}(R)$ that does not intersect the kernel of the dual isogeny $I' : E' \to I$ (equivalently $D(x'(A))$ is a unit in R). Let $\mathfrak{F}_A = (x' - x'(A), y' - y'(A))$ be the corresponding ideal of $R[E - E[d]] = R[x, y, 1/\psi_d(x)]/(\Lambda(a_1, a_2, a_3, a_4, a_6, x, y))$. Let*

$$S = R[x, y, 1/\psi_d(x)]/(\Lambda(a_1, a_2, a_3, a_4, a_6, x, y), \mathfrak{F}_A) ,$$

be the residue ring of $I^{-1}(A)$. Then S is a finite free étale R-algebra of rank d. If we call $\sigma : S \to S$ the R-automorphism induced on S, by the translation τ_{-T}, then S is a free $R[\sigma]$-module of rank 1.

Using notations introduced from Eq. (11) to Eq. (29), we set $\mathfrak{a} = 1$, $\mathfrak{b} = (1 - c_1)/d$, $u_k = \mathfrak{a}U_k + \mathfrak{b}$ and $\theta_k = u_k \bmod \mathfrak{F}_A$. Then $\sigma(\theta_k) = \theta_{k+1}$, and $\Theta = (\theta_k)_{k \in \mathbb{Z}/d\mathbb{Z}}$ is an R-basis of S. If $M = (x(M), y(M)) \in E(R)$ is an auxiliary section that does not cross $E[d]$, then the multiplication tensor of S in the basis Θ is given by Eq. (34).

2.4. **Example.** Let R be the ring $\mathbb{Z}/101^2\mathbb{Z}$. We consider the elliptic curve E over R defined by the Weierstrass equation $E/(\mathbb{Z}/101^2\mathbb{Z}) : y^2 = x^3 + 55\,x + 91$. Let T be the point $(659, 8304) \in E/(\mathbb{Z}/101^2\mathbb{Z})$. This is a point with exact order $d = 7$.

We first compute $\Gamma_{1,2} = 5780$, $\Gamma_{2,3} = 4390$, $\Gamma_{3,4} = 3596$, $\Gamma_{4,5} = 4390$ and $\Gamma_{5,6} = 5780$. We then find $c_1 = 3534$, and from Eq. (15), we deduce $c_2 = 7412$, $c_3 = 618$, $c_4 = 9583$, $c_5 = 2789$ and $c_6 = 6667$. Moreover c_1 is a unit in R and we set $\mathfrak{a} = 1/c_1 = 6665$ and $\mathfrak{b} = 0$.

We compute the quotient elliptic curve $E' = E/\langle T \rangle$ thanks to Vélu's formulae. This yields the curve $E'/(\mathbb{Z}/101^2\mathbb{Z}) : y^2 = x^3 + 6725\,x + 6453$. Let A be the point $(1373, 1956) \in E'(\mathbb{Z}/101^2\mathbb{Z})$. This is a point with exact order 14.

We can efficiently compute traces of $u_k u_l$ evaluated at A with Eqs. (16), (17), (18), (19) and (20). We find

$$\overrightarrow{e} = (9428,\,6046,\,1946,\,2596,\,2596,\,1946,\,6046)\,.$$

This vector is invertible for the convolution product in R^d and its inverse is

$$\overrightarrow{e}^{(-1)} = (3392,\,3344,\,10\,161,\,101,\,101,\,10\,161,\,3344)\,.$$

We now compute traces of xu_k evaluated at A with Eqs. (23), (24), (25) and (26), and find

$$\overrightarrow{\iota} = (10\,063,\,4509,\,6660,\,4259,\,6660,\,4509,\,138)\,.$$

We finally obtain

$$\overrightarrow{i} = \overrightarrow{e}^{(-1)} \star \overrightarrow{\iota} = (7790,\,6555,\,2470,\,2741,\,4358,\,2047,\,636)\,.$$

Let us consider the additional evaluation point $M = (8903,\,4033) \in E(\mathbb{Z}/101^2\mathbb{Z})$. We check that $(\mathfrak{e}_k(N))_k$ where $N = I(M)$ is invertible for the convolution product in R^d. So N does not cross the kernel of the dual isogeny. Then Eq. (33) yields

$$\mathfrak{a}^2\overrightarrow{x_N} = (2742,\,2044,\,649,\,2348,\,7216,\,9732,\,7464)\,.$$

Similarly, Eq. (32) yields

$$\overrightarrow{u_N} = (1029,\,7201,\,10\,176,\,1807,\,4875,\,3261,\,2255)\,.$$

And therefore, $\overrightarrow{u_N}^{(-1)} = (7790,\,1761,\,3889,\,6998,\,5866,\,1090,\,3210)\,.$

Now, let us make use of these precomputations to, for instance, compute θ_0^2 with Eq. (34). We thus start from $\overrightarrow{\alpha} = (1,\,0,\,0,\,0,\,0,\,0,\,0)\,$, and we first compute

$$\overrightarrow{u_N} \star \overrightarrow{\alpha} = (1029,\,7201,\,10\,176,\,1807,\,4875,\,3261,\,2255)\,,$$

and

$$\mathfrak{a}^2\overrightarrow{x_N} \star ((\overrightarrow{\alpha} - \sigma(\overrightarrow{\alpha})) \diamond (\overrightarrow{\alpha} - \sigma(\overrightarrow{\alpha}))) = (5,\,4786,\,2693,\,2997,\,9564,\,6747,\,6995)\,.$$

Thus,

$$\overrightarrow{u_N}^{(-1)} \star \Big((\overrightarrow{u_N} \star \overrightarrow{\alpha}) \diamond (\overrightarrow{u_N} \star \overrightarrow{\beta}) - (\mathfrak{a}^2\overrightarrow{x_N}) \star \Big((\overrightarrow{\alpha} - \sigma(\overrightarrow{\alpha})) \diamond (\overrightarrow{\beta} - \sigma(\overrightarrow{\beta}))\Big)\Big) = (8133,\,8133,\,8133,\,8133,\,8133,\,8133,\,8133)\,.$$

It follows,

$$(\mathfrak{a}^2\,\overrightarrow{i}\,) \star \Big((\overrightarrow{\alpha} - \sigma(\overrightarrow{\alpha})) \diamond (\overrightarrow{\beta} - \sigma(\overrightarrow{\beta}))\Big) = (6406,\,4952,\,8520,\,969,\,8109,\,7516,\,7834)\,,$$

and finally

$$\overrightarrow{\gamma} = (4338,\,2884,\,6452,\,9102,\,6041,\,5448,\,5766)\,.$$

Algorithm 1: AKS primality test

Input : an integer $n > 1$

if $n = a^b$ for $a \in \mathbb{N}$ and $b > 1$ **then**
  return COMPOSITE

Find the smallest integer r such that the multiplicative order of n modulo r is $> \log_2^2 n$

if $1 < \gcd(a, n) < n$ for some $a \leqslant r$ **then**
  return COMPOSITE

if $n \leqslant r$ **then**
  return PRIME

for $a = 1$ **to** $\lfloor \sqrt{\varphi(r)} \log_2 n \rfloor$ **do**
  if $(x + a)^n \neq x^n + a \pmod{x^r - 1,\ n}$ **then**
    return COMPOSITE

return PRIME

3. An elliptic AKS criterion

Agrawal, Kayal and Saxena have proven [1] that primality of an integer n can be tested in deterministic polynomial time $(\log n)^{\frac{21}{2}+o(1)}$. Their test, often called the AKS test, relies on explicit computations in the multiplicative group of a well chosen free commutative R-algebra S of finite rank, where $R = \mathbb{Z}/n\mathbb{Z}$. More precisely, they take for S the cyclic algebra $R[x]/(x^r - 1)$ where r is a well chosen, and rather large, integer (see Algorithm 1).

Lenstra and Pomerance generalized this algorithm and obtained the better deterministic complexity $(\log n)^{6+o(1)}$ [16]. The main improvement in Lenstra and Pomerance's approach consists in using a more general construction for the free commutative algebra S. As a consequence, the dimension of S is much smaller for a given n, and this results in a faster algorithm. A nice survey [23] has been written by Schoof.

Berrizbeitia first [6], and then Cheng [8], have proven that there exists a probabilistic variant of these algorithms that works in time $(\log n)^{4+o(1)}$ provided $n - 1$ has a divisor d bigger than $(\log_2 n)^2$ and smaller than a constant times $(\log_2 n)^2$. Avanzi and Mihăilescu [4], and independently Bernstein [5], explain how to treat a general integer n using a divisor d of $n^f - 1$ instead, where f is a small integer. The initial idea consists in using R-automorphisms of S to speed up the calculations. In these variants, the free commutative R-algebra S has to be constructed in such a way that a non-trivial R-automorphism $\sigma : S \to S$ is effectively given, and can be efficiently applied to any element in S.

All the aforementioned algorithms construct S as a residue ring modulo n of a cyclotomic or Kummer extension of the ring $\mathbb{Z}$ of integers. In this section, we propose an AKS-like primality criterion that relies on Kummer theory of elliptic curves. The main advantage of this elliptic variant, compared to the Berrizbeitia-Cheng-Avanzi-Mihailescu-Bernstein one, is that it allows a much greater choice for the value of d, since there exist many elliptic curves modulo n. We are not restricted to divisors of $n - 1$. We can use any d that divides the order of any elliptic curve modulo n. In particular, we avoid the complication and the cost coming from the exponent f in $n^f - 1$. The algorithm remains almost quartic both in time and space. However, we heuristically save a factor $(\log \log n)^{O(\log \log \log \log n)}$ in the complexity.

From a practical viewpoint, it might be worth choosing for d a product of prime integers of the appropriate size, depending of ones implementation of fast Fourier transform.

Section 3.1 gathers prerequisites from commutative algebra. In Section 3.2, we describe a rather general variant of the AKS primality criterion: it makes uses of a free R-algebra S of rank d together with an R-automorphism $\sigma : S \to S$ of order d. We recall how this algebra can be constructed from multiplicative Kummer theory as in [6]. In Section 3.3, we state and prove a primality criterion involving rings of elliptic periods. The construction of such rings is detailed in Section 3.4.

3.1. **Étale cyclic extensions of a field.** Let $\mathbf{K}$ be a field and let $\mathbf{L} \supset \mathbf{K}$ be a commutative algebra over $\mathbf{K}$. We assume $\mathbf{L}$ is of finite dimension $d \geqslant 1$ over $\mathbf{K}$. We also assume there exist a $\mathbf{K}$-automorphism σ of $\mathbf{L}$ and a $\mathbf{K}$-basis $(\omega_i)_{i\in\mathbb{Z}/d\mathbb{Z}}$ of $\mathbf{L}$ such that $\sigma(\omega_i) = \omega_{i+1}$. So $\mathbf{L}$ is a rank 1 free $\mathbf{K}[\mathcal{G}]$-module, where $\mathcal{G} = \langle\sigma\rangle$ is the cyclic group generated by σ. And ω_0 is a basis of the $\mathbf{K}[\mathcal{G}]$-module $\mathbf{L}$. In this section, we recall a few elementary facts about the arithmetic of $\mathbf{L}$.

First, $\mathbf{L}$ is a noetherian ring, because it is of finite type over the field $\mathbf{K}$. Further $\mathbf{K}$ is the subring $\mathbf{L}^{\mathcal{G}}$ of elements in $\mathbf{L}$ that are invariant by σ. We deduce [7, Chapitre 5, paragraphe 1, numéro 9, Proposition 22] that $\mathbf{L}$ is integral over $\mathbf{K}$. Let $\mathfrak{p}$ be a prime ideal in $\mathbf{L}$. The intersection $\mathfrak{p} \cap \mathbf{K}$ is a prime ideal in $\mathbf{K}$, so it is equal to 0. Since 0 is maximal in $\mathbf{K}$, the ideal $\mathfrak{p}$ is maximal in $\mathbf{L}$ [7, Chapitre 5, paragraphe 2, numéro 1, Proposition 1]. Thus $\mathbf{L}$ is a ring of dimension 0. Since $\mathbf{L}$ is noetherian, it is an artinian ring [7, Chapitre 4, paragraphe 2, numéro 5, Proposition 9]. Its nilradical $\mathfrak{N}$, which is equal to its Jacobson radical, is nilpotent. The automorphism σ acts transitively on the set of prime ideals in $\mathbf{L}$ [7, Chapitre 5, paragraphe 2, numéro 2, Théorème 2]. We denote by $\mathcal{G}^Z$ (resp. $\mathcal{G}^T$) the decomposition group (resp. inertia group) of all these prime ideals. Let $e \geqslant 1$ be the order of the inertia group $\mathcal{G}^T$, and let f be the order of the quotient $\mathcal{G}^Z/\mathcal{G}^T$. We check that $d = efm$ where m is the number of prime ideals in $\mathbf{L}$. Let $\mathfrak{p}_0, \mathfrak{p}_1, \dots, \mathfrak{p}_{m-1}$ be all these prime ideals. They are pairwise relatively prime. The radical of $\mathbf{L}$ is

$$\mathfrak{N} = \bigcap_{0\leqslant i\leqslant m-1} \mathfrak{p}_i = \prod_{0\leqslant i\leqslant m-1} \mathfrak{p}_i.$$

The canonical map

$$\phi : \mathbf{L} \to \prod_{0\leqslant i\leqslant m-1} \mathbf{L}/\mathfrak{p}_i$$

is a ring epimorphism and its kernel is the radical $\mathfrak{N}$. For every i in $\{0, 1, \dots, m-1\}$, the quotient $\mathcal{G}^Z/\mathcal{G}^T$ is isomorphic to the group of $\mathbf{K}$-automorphisms of the residue field $\mathbf{M}_i = \mathbf{L}/\mathfrak{p}_i$ [7, Chapitre 5, paragraphe 2, numéro 2, Théorème 2]. The field extensions $\mathbf{M}_i$ of $\mathbf{K}$ are normal and their separable degree is f. Let r be their inseparable degree. The dimension of the $\mathbf{K}$-vector space $\mathbf{M}_i$ is rf. We deduce that the dimension of $\prod_{0\leqslant i\leqslant m-1} \mathbf{L}/\mathfrak{p}_i$ is rfm. And the dimension of the radical $\mathfrak{N}$ is

$$\dim_{\mathbf{K}}(\mathfrak{N}) = d - rfm = (e - r)fm. \tag{35}$$

The radical $\mathfrak{N}$ is nilpotent: there exists an integer k such that $\mathfrak{N}^k = 0$. The artinian ring $\mathbf{L}$ is isomorphic [3, Theorem 8.7] to the product of local artinian rings $\prod_{0\leqslant i\leqslant m-1} \mathbf{L}/\mathfrak{p}_i^k$.

One says that the algebra $\mathbf{L}$ is unramified over $\mathbf{K}$ [18, Chapter 4, Definition 3.17] if the residue fields $\mathbf{L}/\mathfrak{p}_i$ are separable extensions of $\mathbf{K}$ (that is $r = 1$) and the local factors $\mathbf{L}/\mathfrak{p}_i^k$ are fields (e.g. the nilradical is zero or equivalently $e - r = 0$). This is equivalent to $\mathbf{L}$ being étale over $\mathbf{K}$, e.g. the trace form being non-degenerate.

A sufficient condition for $\mathbf{L}$ to be unramified over $\mathbf{K}$ is that for every prime divisor ℓ of d there exists an element a_ℓ in $\mathbf{L}$ such that $\sigma^{D/\ell}(a_\ell) - a_\ell$ is a unit. Indeed this proves that $\sigma^{D/\ell}$ does not lie in $\mathcal{G}^T$. So $e = 1$. And $r = 1$ also, using Eq. (35).

Assume now $\mathbf{K}$ is a finite field and $\mathbf{L}$ is reduced (therefore étale over $\mathbf{K}$). Remember $\mathfrak{p}_0$, $\mathfrak{p}_1, \dots, \mathfrak{p}_{m-1}$ are the prime ideals in $\mathbf{L}$. The Frobenius automorphism Φ_i of $\mathbf{M}_i = \mathbf{L}/\mathfrak{p}_i$ is the reduction modulo $\mathfrak{p}_i$ of some power σ^{z_i} of σ lying in $\mathcal{G}^Z$. Especially, for every a in $\mathbf{L}$, one has $\sigma^{z_0}(a) = a^p \bmod \mathfrak{p}_0$ for some integer z_0. We let σ act on the above congruence and deduce that $z_0 = z_1 = \dots = z_{d-1}$ because σ acts transitively on the set of primes. So there exists an integer z such that for every element a in $\mathbf{L}$ we have

$$a^p = \sigma^z(a)\,. \tag{36}$$

Of course, z is a multiple of m.

3.2. **Ring extensions and primality proving.** Let $n \geqslant 2$ be an integer and set $R = \mathbb{Z}/n\mathbb{Z}$. In this section, we state a general AKS-like primality criterion in terms of the existence of some commutative free R-algebra S of finite rank fulfilling simple conditions.

Let $S \supset R$ be a finite free commutative R-algebra of rank $d \geqslant 1$. Then R can be identified with a subring of S. Let $\sigma : S \to S$ be an R-automorphism of S and assume that there exists an R basis $(\omega_i)_{i\in\mathbb{Z}/d\mathbb{Z}}$ of S such that $\sigma(\omega_i) = \omega_{i+1}$. Let p be a positive prime integer dividing n. Set $\mathbf{L} = S/pS$ and $\mathbf{K} = R/pR = \mathbb{Z}/p\mathbb{Z}$. Assume $\mathbf{L}$ is reduced. This is always the case when S is étale over R [18, Chapter 4, Definition 3.17, Lemma 3.20]. The R-automorphism $\sigma : S \to S$ induces a $\mathbf{K}$-automorphism of $\mathbf{L}$ that we call σ also. Let θ be a unit in S such that

$$\theta^n = \sigma(\theta)\,.$$

Reducing this identity modulo p and setting $a = \theta \bmod p \in \mathbf{L}$, we obtain

$$a^n = \sigma(a)\,. \tag{37}$$

Using Eqs. (37) and (36) repeatedly, we prove that there exists an integer z such that for $k, l \in \mathbb{N}$, we have

$$a^{n^k p^l} = \sigma^{k+zl}(a). \tag{38}$$

Let $\mathfrak{p}$ be a prime ideal in $\mathbf{L}$ and set $\mathbf{M} = \mathbf{L}/\mathfrak{p}$. Set $b = a \bmod \mathfrak{p} \in \mathbf{M}$. Let $G \subset \mathbf{L}^*$ be the group generated by a and let $H \subset \mathbf{M}$ be the group generated by b. We first show that the reduction modulo $\mathfrak{p}$ map $G \to H$ is a bijection. Indeed, let k be a positive integer such that $b^k = 1 \in \mathbf{M}$. Then $a^k = 1 \bmod \mathfrak{p}$. We raise both members in this congruence to the n-th power. Using Eq. (37), we find $a^{kn} = a^{nk} = \sigma(a)^k = \sigma(a^k) = 1 \bmod \mathfrak{p}$. So $a^k = 1 \bmod \sigma^{-1}(\mathfrak{p})$. We remind that σ acts transitively on the set of primes in $\mathbf{L}$. So a^k is congruent to 1 modulo all these primes. Since $\mathbf{L}$ is reduced, we deduce that $a^k = 1$.

The group H is a subgroup of $\mathbf{M}^*$. Therefore the order h of H (which is the order of G also) divides $p^f - 1$ where f is the dimension of $\mathbf{M}$ over $\mathbf{K}$. It is thus clear that p and $\#H$ are coprime. Iterating d times Eq. (37), we find that $a^{n^d} = a$. So n also is invertible modulo $h = \#G = \#H$. So Eq. (38) makes sense and holds true for k and l in $\mathbb{Z}$, provided the exponents are seen as residues modulo h.

We set $q = n/p$ and from Eqs. (37) and (36), we deduce that $a^q = \sigma^{1-z}(a)$. Moreover, there exist four integers i, i', j and j' in $\{0, 1, \dots, \lfloor\sqrt{d}\rfloor\}$ such that $(i, j) \neq (i', j')$ and $i(1-z) + jz$ is congruent to $i'(1-z) + j'z$ modulo d. Setting in Eq. (38), first $k = i$ and $l = j - i$, and then $k = i'$ and $l = j' - i'$, we find that exponentiations by $q^i p^j$ and $q^{i'} p^{j'}$ act similarly on a. We deduce that

$$q^i p^j = q^{i'} p^{j'} \bmod \#G. \tag{39}$$

We now observe that both integers $q^i p^j$ and $q^{i'} p^{j'}$ are bounded above by $n^{\lfloor \sqrt{d} \rfloor}$. If

$$n^{\lfloor \sqrt{d} \rfloor} \leqslant \#G\,,$$

then congruence (39) is an equality between integers and we deduce that n is a power of p.

Theorem 3 (AKS criterion)**.** *Let $n \geqslant 2$ be an integer and set $R = \mathbb{Z}/n\mathbb{Z}$. Let $S \supset R$ be a free algebra of rank d over R. Let σ be an R-automorphism of S. Let $\mathcal{G}$ be the group generated by σ. Assume S is a free $R[\mathcal{G}]$-module of rank 1: there exists an element ω in S such that $(\omega, \sigma(\omega), \ldots, \sigma^{d-1}(\omega))$ is an R basis of L. Let θ be a unit in S such that $\theta^n = \sigma(\theta)$. Let p be a prime divisor of n. Assume S/pS is reduced and $\theta \bmod p$ generates a subgroup of order at least $n^{\lfloor \sqrt{d} \rfloor}$ in $(S/pS)^*$. Then n is a power of p.*

The condition that S/pS is reduced is granted if S is étale over R. A sufficient condition for S to be étale over R is that for every prime divisor ℓ of d, there exists an element a_ℓ in S such that $\sigma^{D/\ell}(a_\ell) - a_\ell$ is a unit.

The condition on the size of the group generated by $\theta \bmod p$ is often obtained with the help of geometric arguments. In our case, these are degree considerations, which yield a lower bound for d.

Berrizbeitia, Cheng, Avanzi, Mihăilescu and Bernstein construct S as $R[x]/(x^d - \alpha)$ where $d \geqslant 2$ divides $n-1$ and α is a unit in R. We set $n - 1 = dm$ and $\zeta = \alpha^m$. Assume ζ has exact order d in R^*. This means that $\zeta^d = 1$ and $\zeta^k - 1$ is a unit for every $1 \leqslant k < d$. We define an R automorphism $\sigma : S \to S$ by setting $\sigma(x) = \zeta x$. We set $\omega = (\alpha - 1)/(x - 1) = 1 + x + x^2 + \cdots + x^{d-1} \bmod x^d - \alpha$ and we check that $(\omega, \sigma(\omega), \ldots, \sigma^{d-1}(\omega))$ is an R-basis of S. Indeed $(1, x, x^2, \ldots, x^{d-1})$ is a basis, and the matrix connecting the two systems is a Vandermonde matrix $V(1, \zeta, \ldots, \zeta^{d-1})$ which is invertible since ζ has exact order d. So S is a free $R[\sigma]$-module of rank 1.

We note that $x \bmod x^d - \alpha$ is a unit in S because α is a unit in R. For every integer $1 \leqslant k < d$, the difference $\sigma^k(x) - x = (\zeta^k - 1)x$ is a unit in S, because ζ has exact order d. So S is étale over R. The main computational step in Berrizbeitia test is to check, by explicit calculation, that the following congruence holds true in S,

$$(x-1)^n = \zeta x - 1 \bmod (n, x^d - \alpha)\,. \tag{40}$$

So, we set $\theta = x - 1 \bmod (n, x^d - a)$. This is a unit in S because $\alpha - 1$ is a unit in R. Letting σ repeatedly act on Eq. (40), we deduce that for any positive integer k, the class $\zeta^k x - 1 \bmod (n, x^d - \alpha)$ is a power of θ.

Let p be any prime divisor of n. We set $a = \theta \bmod p = x - 1 \bmod (p, x^d - \alpha) \in S/pS$. We show that the order of a in $(S/pS)^*$ is large. For every subset $\mathcal{S}$ of $\{0, 1, \ldots, d-1\}$, we denote by $a_{\mathcal{S}}$ the product

$$\prod_{k \in \mathcal{S}} (\zeta^k x - 1) \bmod (p, x^d - a) = \prod_{k \in \mathcal{S}} \sigma^k(a).$$

This is a power of a, because every $\sigma^k(a)$ is. Degree considerations similar to those in the original paper [1] show that if $\mathcal{S}_1$ and $\mathcal{S}_2$ are two strict distinct subsets of $\{0, 1, \ldots, d-1\}$, then $a_{\mathcal{S}_1}$ and $a_{\mathcal{S}_2}$ are distinct elements in S/pS. So the order of a in $(S/pS)^*$ is at least 2^d-1. This lower bound can be improved by several means (see for instance Voloch's work [26]).

If 2^d is bigger than $n^{\lfloor\sqrt{d}\rfloor}$, we deduce from Theorem 3 that n is a prime power.

Corollary 1 (Berrizbeitia criterion)**.** *Let $n \geqslant 3$ be an integer and set $R = \mathbb{Z}/n\mathbb{Z}$. Let $S = R[x]/(x^d-\alpha)$ where $d \geqslant 2$ divides $n-1$. Set $n-1 = dm$ and assume $\zeta = \alpha^m$ has exact order d in R^*. Assume Eq. (40) holds true in S. If 2^d is bigger than $n^{\lfloor\sqrt{d}\rfloor}$, then n is a prime power.*

In Section 3.3, we adapt this construction to the broader general context of Kummer theory of elliptic curves. This way, we get rid of the condition that d divides $n-1$.

3.3. **A primality criterion.** In this section, we state and prove a primality criterion involving elliptic periods. Assume we are given an integer $n \geqslant 2$. We set $R = \mathbb{Z}/n\mathbb{Z}$ and we assume we are in the situation of Theorem 2. We are given a Weierstrass elliptic curve E over R, a positive integer d relatively prime to $2n$ and a section $T \in E(R)$ of exact order d. The quotient by $\langle T\rangle$ isogeny $I : E \to E'$ is given by Vélu's formulae. We are given a section $A \in E'_{\mathrm{aff}}(R)$ and we call

$$\mathfrak{F}_A = (x' - x'(A), y' - y'(A))$$

the ideal of $I^{-1}(A)$ in $R[x, y, 1/\psi_d(x)]/(\Lambda(a_1, a_2, a_3, a_4, a_6, x, y))$. We assume that $D(x'(A))$ is a unit in R, where D is defined in Eqs. (27), (28) and (29). Let

$$S = R[x, y, 1/\psi_d(x)]/(x' - x'(A), y' - y'(A))$$

be the residue ring of $R[x, y, 1/\psi_d(x)]/(\Lambda(a_1, a_2, a_3, a_4, a_6, x, y))$ at $I^{-1}(A)$.

We call $\sigma : S \to S$ the automorphism induced on S by the translation τ_{-T}:

$$\begin{array}{rrcl}\sigma : & S & \longrightarrow & S\,, \\ & f \bmod \mathfrak{F}_A & \longmapsto & f\circ\tau_{-T} \bmod \mathfrak{F}_A\,.\end{array}$$

For $k \in \mathbb{Z}/d\mathbb{Z}$, we set $\theta_k = u_k \bmod \mathfrak{F}_A$. The $(\theta_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ form an R-basis of S and we have $\sigma(\theta_k) = \theta_{k+1}$. The algebra S is finite free étale of rank d over R because the determinant $D(x'(A))$ of the trace form is a unit. The main computational step now is to check, by explicit calculation, that the following congruence holds true in S,

$$\theta_0^n = \theta_1\,. \tag{41}$$

Letting σ repeatedly act on Eq. (41), we deduce that for any $k \in \mathbb{Z}/d\mathbb{Z}$, θ_k is a power of θ_0. In particular, all θ_k belong to the ideal generated by θ_0. Using Eq. (10), we deduce that $1 = \sum_{k\in\mathbb{Z}/d\mathbb{Z}}\theta_k$ belongs to the ideal generated by θ_0. So θ_0 is a unit.

Let p be any prime divisor of n. We set $a = \theta_0 \bmod p \in S/pS$. We show that the order of a in $(S/pS)^*$ is large. To every subset $\mathcal{S}$ of $\mathbb{Z}/d\mathbb{Z}$, we associate the product

$$u_{\mathcal{S}} = \prod_{k\in\mathcal{S}} u_k$$

We note that $u_{\mathcal{S}} \bmod (\mathfrak{F}_A, p) = \prod_{k\in\mathcal{S}}(\theta_k \bmod p)$ is a power of a. Let $\mathcal{S}_1$ and $\mathcal{S}_2$ be two subsets of

$$\{0, 2, 4, \ldots, d-3\} \subset \mathbb{Z}/d\mathbb{Z}.$$

Let l_1 and l_2 be two integers that are relatively prime to p. Then $l_1u_{\mathcal{S}_1} \neq l_2u_{\mathcal{S}_2} \bmod (\mathfrak{F}_A, p)$ unless $\mathcal{S}_1 = \mathcal{S}_2$ and $l_1 = l_2 \bmod p$. Indeed, if $l_1u_{\mathcal{S}_1} = l_2u_{\mathcal{S}_2} \bmod (\mathfrak{F}_A, p)$ then $l_1u_{\mathcal{S}_1} - l_2u_{\mathcal{S}_2} \bmod p$ is a function on $E \bmod p$ with divisor $\geqslant -\sum_{k\in\mathbb{Z}/d\mathbb{Z}}[kt]$ and it cancels on the degree d divisor

$I^{-1}(A) \bmod p$. So $l_1 u_{\mathcal{S}_1} = l_2 u_{\mathcal{S}_2} \bmod p$. Therefore these two functions have the same poles. We deduce first, that $\mathcal{S}_1 = \mathcal{S}_2$, and then, that $l_1 = l_2$.

There are $2^{\frac{d-1}{2}}$ subsets of $\{0, 2, 4, \ldots, d-3\}$. So, the order of a in $(S/pS)^*$ is at least $2^{\frac{d-1}{2}}$.

Using Theorem 3, we deduce the following primality criterion.

Corollary 2 (Elliptic AKS criterion)**.** *Let $n \geqslant 2$ be an integer and let E be a Weierstrass elliptic curve over $R = \mathbb{Z}/n\mathbb{Z}$. Let $T \in E(R)$ be a section of exact order d where d is an integer relatively prime to $2n$. Let E' be the quotient $E/\langle T\rangle$ given by Vélu's formulae. Let $A \in E'_{\mathit{aff}}(R)$ be a section such that the vector $\overrightarrow{e} = (\mathfrak{e}_k(A))_k$ defined by Eq. (22) is invertible for the convolution product $\star$ on R^d.*

Assume that

$$(\theta_0)^n = \theta_1 \tag{42}$$

holds true in the ring of elliptic periods $S = R[x, y, 1/\psi_d(x)]/(x' - x'(A), y' - y'(A))$.

Assume further that

$$2^{\frac{d-1}{2}} \geqslant n^{\sqrt{d}}. \tag{43}$$

Then n is a prime power.

We recall that the condition that the vector $\overrightarrow{e}$ be invertible means that the section A does not cross the kernel of the dual isogeny $I' : E' \to E$. Checking Eq. (42) requires $O(\log n)$ multiplications in the ring S. Any such multiplication requires $O(d \log d \log\log d)$ operations (additions, subtractions, multiplications) in $R = \mathbb{Z}/n\mathbb{Z}$. So the total cost is

$$O((\log n)^2 (\log\log n)^{1+o(1)} \times d \log d \log\log d)$$

elementary operations using fast arithmetic [21, 22]. In Section 3.4, we explain why one can hope to find a degree d that is $O((\log n)^2)$. With such a d, one can verify Eq. (42) in time

$$O((\log n)^4 (\log\log n)^{2+o(1)}).$$

Moreover, we explain how to construct the ring S in Corollary 2.

3.4. **Construction of a ring of elliptic periods.** In this section, we explain how to construct the ring of elliptic periods that is required to prove that a given integer $n \geqslant 2$ is prime using Corollary 2. So, we are given an integer $n \geqslant 2$ which is probably prime: it already passed many pseudo-primality tests. We want to construct a ring of elliptic periods modulo n with rank d for some d satisfying inequality (43). A sufficient condition is that $d \geqslant \mathrm{d_{min}}$ with

$$\mathrm{d_{min}} = \lceil 4(\log_2 n)^2 + 2 \rceil\,.$$

We assume that d is odd too. We like d to be as small as possible. We set $\mathrm{d_{max}} = \mathrm{d_{min}} \times O(1)$ and ask that $d \in [\mathrm{d_{min}}, \mathrm{d_{max}}]$. The construction is probabilistic and relies on several heuristics. Since n is probably prime, we shall allow ourselves to use algorithms that are only proven to work under the condition that n is prime. This is not an issue as far as we can check the result rigorously (and efficiently).

We set $R = \mathbb{Z}/n\mathbb{Z}$. We want to construct an elliptic curve E over R with a section $T \in E(R)$ of exact order d in the sense of [13, Chapter 1, 1.4]. We use complex multiplication theory.

The first step of the algorithm selects quadratic imaginary orders. We look over the maximal quadratic imaginary orders $\mathcal{O}$ for decreasing fundamental discriminants $-\Delta$. We start with

$-\Delta = -7$. For each order $\mathcal{O}$, we first look for a square root δ of $-\Delta$ modulo n using the algorithm of Legendre. Since n is expected to be prime, the algorithm will succeed in probabilistic time $(\log n)^2(\log\log n)^{1+o(1)}$. And of course we can check the result rigorously in time $(\log n)$ $(\log\log n)^{1+o(1)}$. For a given n, such a square root exists for one quadratic order over two. If we fail to find such a square root, we go to the next quadratic order.

Once we have found a square root δ of $-\Delta$ modulo n, we call $\mathfrak{n}$ the ideal $(n, \sqrt{-\Delta} - \delta)$ in $\mathcal{O}$ and we look for an element with norm n in $\mathfrak{n}$. We use fast Cornachia's algorithm. It runs in deterministic time $(\log n)(\log\log n)^{2+o(1)}$ and finds such an element $\phi \in \mathcal{O}$ when it exists.

We then set $t = \mathrm{Tr}(\phi)$ and look for an integer d that satisfies the following conditions:

- $d \in [\mathrm{d_{min}}, \mathrm{d_{max}}]$,
- d is relatively prime to $n(n-1)(n+1)$,
- there exists an $\epsilon \in \{1, -1\}$ such that d divides $n + 1 - \epsilon t$ and is relatively prime to $(n + 1 - \epsilon t)/d$.

In order to find such a d, we apply the elliptic curve factoring method to $n + 1 - t$ and $n + 1 + t$. Since the factors we are looking for are very small, we expect to find them in time $(\log n)^{1+o(1)}$. If we find no such integer d, we go to the next fundamental discriminant $-\Delta$.

We expect to succeed in finding an integer d for some $\Delta = (\log\log n)^{2+o(1)}$. Also the expected running time of this first step is $(\log n)^{2+o(1)}$. We note that the search for split discriminants can be accelerated using the same technique as in the J.O. Shallit fast-ECPP algorithm [15, 19].

The second step of the algorithm constructs the ring S from the pair $(-\Delta, d)$. Once we have found a quadratic order $\mathcal{O}$, we compute the associated Hilbert class polynomial. Computing $H_{\mathcal{O}}(X)$ requires quasi-linear time in the size of this polynomial. This polynomial has degree $\Delta^{1/2+o(1)}$ and height $\Delta^{1/2+o(1)}$, where $-\Delta$ is the discriminant of $\mathcal{O}$. So $H_{\mathcal{O}}(X)$ can be computed in time $\Delta^{1+o(1)}$. Finding a root j of $H_{\mathcal{O}}(X)$ modulo n is achieved in probabilistic time

$$\Delta^{1/2+o(1)}(\log n)^{2+o(1)}.$$

So the time for finding this root will be $(\log n)^{2+o(1)}$.

Once computed a root of the modular polynomial, we construct an elliptic curve E over $R = \mathbb{Z}/n\mathbb{Z}$ having modular invariant j. We then construct a random R-section P on E. We expect one and only one among $[n+1-t]P$ and $[n+1+t]P$ to be equal to the zero section O. If this is not the case, we pick another point P. Let $\epsilon \in \{-1, 1\}$ be such that d divides $n + 1 - \epsilon t$. If we have found a section P such that $[n + 1 - \epsilon t]P \neq O$, then we replace E by its quadratic twist. And we start again with this new curve. If we have found a point P such that $[n+1-\epsilon t]P = O$ and $[n+1+\epsilon t]P \neq O$, then we multiply P by $(n+1-t)/d$ and obtain a section T that, we hope, has exact order d. We can test that T has exact order d by checking that $\psi_k(x(T))$ is a unit in R for every strict divisor k of d. If this condition does not hold, we pick another section P on E.

Once we have found a T of exact order d, we consider the quotient isogeny $I : E \to E'$. We compute the coefficients in the Weierstrass equation of E' thanks to Eq. (8). We do not write down explicit equations for I. We look for an R-section A on E' having exact order d. We let S be the residue ring of $I^{-1}(A)$. Elements in S are represented by vectors in R^d. The automorphism σ is the cyclic shift of coordinates. There remains to describe the multiplication law. To this end, we pick an auxiliary R-section M of E such that $N = I(M)$

does not cross the kernel of the dual isogeny I'; or equivalently $D(x'(N))$ is a unit in R. We now can compute the multiplication tensor of the ring S. This tensor is given by Theorem 2. We just need to compute the vectors $\overrightarrow{\imath}$, $\overrightarrow{u_N}$, $\overrightarrow{x_N}$ using the method given in Section 2.1.4. This requires $O(d(\log d)^2 \log\log d)$ operations in R. This finishes the construction of the ring S.

The expected running time of this second step is $(\log n)^{1+o(1)}(\log n + d^{1+o(1)}) = (\log n)^{3+o(1)}$ operations in R.

3.5. **Example.** We consider here a primality test for $n = 1009$.

We first notice that $\mathrm{d_{min}} = \lceil 4(\log_2 n)^2 + 2\rceil = 401$, and a quick search among maximal quadratic imaginary orders $\mathcal{O}$ for decreasing fundamental discriminants yields $d = 479$ for $-\Delta = -148$ (and class number 2). In truth, we have $52^2 + 3^2\, 148 = 4\, n$, and the corresponding elliptic curve has got $n + 1 - 52$ $(= 2 \times 479)$ points.

The Hilbert class polynomial associated to $-\Delta = -148$ is

$$H_{-148}(X) = X^2 - 39\,660\,183\,801\,072\,000\, X - 7\,898\,242\,515\,936\,467\,904\,000\,000\,.$$

One of its roots mod n is $j_E = 353$, and one can check that the point $T = (296, 432)$ is of order d on the elliptic curve

$$E\ : y^2 + xy = x^3 + 364\, x + 907.$$

Similarly, we can check that the point $M = (726, 695)$ is of order 958. Vélu's formulae yield then the quotient elliptic curve,

$$E/\langle T\rangle\ : y^2 + xy = x^3 + 130\, x + 233\,.$$

We choose $A = (383, 201)$, a point of order d on $E/\langle T\rangle$. We can check also that the image of M by the isogeny is equal to $N = (321, 344)$, a point of order 2.

With this setting, we can now define, without any ambiguity, a normal elliptic basis $\Theta = (\theta_k)_{k\in\mathbb{Z}/d\mathbb{Z}}$ (see Section 2.3) and a final computation yields

$$\theta_0^{1009} = \theta_{91}\,.$$

We check that 91 is relatively prime to 479. So $T' = 91T$ is a point of exact order 479. Applying Corollary 2 with T' instead of T, we prove that 1009 is a prime.

References

[1] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. *Annals of Mathematics*, 160(2):781–793, 2004.

[2] David W. Ash, Ian F. Blake, and Scott A. Vanstone. Low complexity normal bases. *Discrete Applied Mathematics*, 25(3):191–210, 1989.

[3] M. Atiyah and I. G. McDonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Company, 1969.

[4] R. M. Avanzi and P. Mihăilescu. Efficient quasi-deterministic primality test improving AKS. Available at http://xwww.uni-math.gwdg.de/preda/, 2007.

[5] Daniel J. Bernstein. Proving primality in essentially quartic random time. *Mathematics of Computation*, 76(257):389–403, January 2007.

[6] Pedro Berrizbeitia. Sharpening "Primes is in P" for a large family of numbers. *Mathematics of Computation*, 74(252):2043–2059, October 2005.

[7] Nicolas Bourbaki. *Éléments de mathématiques. Algèbre commutative*. Springer, 2006. Chapitres 5 à 7.

[8] Qi Cheng. Primality proving via one round in ECPP and one iteration in AKS. *Journal of Cryptology*, 20(3):375–387, 2007.

[9] J.-M. Couveignes and R. Lercier. Elliptic periods for finite fields. *Finite Fields and their Applications*, 15(1):1–22, January 2009.
[10] Andreas Enge. *Elliptic Curves and Their Applications to Cryptography — An introduction*. Kluwer, 1999.
[11] S. Gao and H. W. Jr. Lenstra. Optimal normal basis. *Designs, Codes and Cryptography*, 2:315–323, 1992.
[12] A. Joux and R. Lercier. The Function Field Sieve in the Medium Prime Case. In S. Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 254–270. Springer Berlin / Heidelberg, May 2006.
[13] N. M. Katz and B. Mazur. *Arithmetic Moduli of Elliptic Curves*. Number 108 in Annals of mathematics studies. Princeton University Press, 1985.
[14] Kiran S. Kedlaya and Christopher Umans. Fast modular composition in any characteristic. In *Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science*, pages 146–155. IEEE Computer Society, 2008.
[15] Arjen K. Lenstra and Hendrik W. Lenstra Jr. Algorithms in number theory. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science, Volume A: Algorithms and Complexity (A)*, pages 673–716. North-Holland, 1990.
[16] H. W. Lenstra and C. Pomerance. Primality testing with gaussian periods. Dartmouth, 2009. Available at http://www.math.dartmouth.edu/~carlp/PDF/complexity12.pdf.
[17] R. Lercier and D Lubicz. Counting Points on Elliptic Curves over Finite Fields of Small Characteristic in Quasi Quadratic Time. In E. Biham, editor, *Advances in Cryptology - EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 360–373. Springer Berlin / Heidelberg, May 2003.
[18] Q. Liu. *Algebraic geometry and arithmetic curve*. Oxford science publications, 2006.
[19] F. Morain. Implementing the asymptotically fast version of the elliptic curve primality proving algorithm. *Mathematics of Computation*, 76(257):493–505, January 2007.
[20] R. C. Mullin, I. M. Onyszchuk, S. A. Vanstone, and R. M. Wilson. Optimal normal bases in $\mathrm{GF}(p^n)$. *Discrete Applied Mathematics*, 22(2):149–161, 1988–1989.
[21] A. Schönhage. Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2. *Acta Informatica*, 7:395–398, 1977.
[22] A. Schönhage and V. Strassen. Schnelle Multiplikation großer Zahlen. *Computing*, 7:281–292, 1971.
[23] R. Schoof. Four primality testing algorithms. In *Algorithmic number theory: lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ., Surveys in Number Theory*, pages 101–126. Cambridge Univ. Press, Cambridge, 2008.
[24] J. Vélu. Courbes elliptiques munies d'un sous-groupe $\mathbb{Z}/n\mathbb{Z} \times \mu_n$, 1978. Mémoires de la Société Mathématique de France.
[25] Jacques Vélu. Isogénies entre courbes elliptiques. *Comptes-Rendus de l'Académie des Sciences, Série I*, 273:238–241, July 1971.
[26] J. F. Voloch. On some subgroups of the multiplicative group of a finite ring. *Journal de théorie des nombres de Bordeaux*, 16:233–239, 2004.

Université des Sciences et Techniques de Masuku, Faculté des Sciences, Département de mathématiques et informatique, BP 943 Franceville, Gabon
E-mail address: latonyo2000@yahoo.fr

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

Institut de recherche mathématique de Rennes, Université de Rennes 1 et CNRS, Campus de Beaulieu, F-35042 Rennes Cedex, France.
E-mail address: reynald.lercier@m4x.org