Fast construction of irreducible polynomials over finite fields *

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

September 30, 2009

Abstract

We present a randomized algorithm that on input a finite field $\mathbf{K}$ with q elements and a positive integer d outputs a degree d irreducible polynomial in $\mathbf{K}[x]$. The running time is $d^{1+o(1)} \times (\log q)^{5+o(1)}$ elementary operations. The $o(1)$ in $d^{1+o(1)}$ is a function of d that tends to zero when d tends to infinity. And the $o(1)$ in $(\log q)^{5+o(1)}$ is a function of q that tends to zero when q tends to infinity. In particular, the complexity is quasi-linear in the degree d.

1 Introduction

This article deals with the following problem: given a prime p, a power $q = p^w$ of p, a finite field $\mathbf{K}$ with q elements, and a positive integer d, find a degree d irreducible polynomial in $\mathbf{K}[x]$. We assume that the finite field $\mathbf{K}$ is given as a quotient $(\mathbb{Z}/p\mathbb{Z})[z]/h(z)$ where $h(z)$ is a degree w unitary irreducible polynomial in $(\mathbb{Z}/p\mathbb{Z})[z]$. The complexity of algorithms will be evaluated in terms of the number of necessary elementary operations. Additions, subtractions and comparisons in $\mathbf{K}$ require $O(\log q)$ elementary operations. Multiplication and division require $(\log q) \times (\log \log q)^{1+o(1)}$ elementary operations[1].

A classical approach to finding irreducible polynomials consists in first choosing a random polynomial of degree d and then testing for its irreducibility. The probability that a polynomial of degree d be irreducible is $\geq 1/(2d)$. See Lidl and Niederreiter [11, Ex. 3.26 and 3.27, page 142] and Lemma 4 of Section 7.3 below. In order to check whether a polynomial $f(x)$ is irreducible, we may use Ben-Or's irreducibility test [2]. This test has maximal complexity $(\log q)^{2+o(1)} \times d^{2+o(1)}$ elementary operations while its average complexity is $(\log q)^{2+o(1)} \times d^{1+o(1)}$ elementary operations according to Panario and Richmond [12]. The average complexity of finding an irreducible polynomial with this method is thus $d^{2+o(1)} \times (\log q)^{2+o(1)}$ elementary operations. All the known algorithms have a quadratic factor at least in d. A survey can be found in the work of Shoup [14, section 1.2]. It seems difficult to improve on these existing methods as long as we use an irreducibility test.

So we are driven to consider very particular polynomials. For example, Adleman and Lenstra [1] construct irreducible polynomials in this way. Their method is deterministic polynomial time, under

*Research supported by the "Agence Nationale de la Recherche" through project ALGOL (ANR-07-BLAN-0248) and by the French "Délégation Générale pour l'Armement".

[†]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.

[1]In this paper, an $o(1)$ arising in the exponent of a quantity x stands for a function of x alone, tending to 0 when x tends to infinity.

the Riemann Hypothesis. It uses Gauss Periods. In Section 2 we recall how efficient such methods can be for very special values of the degree d. We reach quasi-linear complexity in d when $d = \ell^\delta$ is a power of a prime divisor ℓ of $p(q-1)$. Section 3 explains how to construct a degree $d_1 d_2$ irreducible polynomial once given two irreducible polynomials of coprime degrees d_1 and d_2. We explain in Sections 4 and 5 how to construct irreducible polynomials using isogenies between elliptic curves. Thanks to this new construction, we reach quasi-linear complexity in d when $d = \ell^\delta$ is a power of a prime ℓ and ℓ does not divide $p(q-1)$. Putting everything together, we obtain a probabilistic algorithm that finds a degree d irreducible polynomial in $\mathbf{K}[x]$ at the expense of $d^{1+o(1)} \times (\log q)^{5+o(1)}$ elementary operations, without any restriction on d nor q. Our constructions are summarized in Section 6 and Theorem 1. In Section 7 we state several useful preliminary results about finite fields, polynomials and elliptic curves.

Remark: One may wonder if the algorithms and complexity estimates in this paper are still valid when the base field is not presented as a quotient $(\mathbb{Z}/p\mathbb{Z})[z]/(h(z))$. Assume for example that elements in $\mathbf{K}$ are represented as vectors in $(\mathbb{Z}/p\mathbb{Z})^w$. Assume we are given the vector corresponding to the unit element 1. Assume also we are given a black box or an algorithm that computes multiplications and divisions of elements in $\mathbf{K}$. In this situation, before applying the algorithms presented in this paper, we should first construct an isomorphism between the given $\mathbf{K}$ and a quotient ring of the form $(\mathbb{Z}/p\mathbb{Z})[z]/(h(z))$. To this end, we first look for a generator τ of the $(\mathbb{Z}/p\mathbb{Z})$-algebra $\mathbf{K}$. We pick a random element τ in $\mathbf{K}$. The probability that τ generates $\mathbf{K}$ over $\mathbb{Z}/p\mathbb{Z}$ is at least $1/2$ according to lemma 4 of Section 7.3. We compute the powers τ^k for $0 \leqslant k \leqslant w$. These are $w+1$ vectors of length w. We compute the kernel of the corresponding matrix in $\mathcal{M}_{w\times(w+1)}(\mathbb{Z}/p\mathbb{Z})$. If the dimension of this kernel is bigger than 1 then τ is not a generator, so we pick a different τ and start again. If the kernel has dimension 1 we obtain the minimal polynomial $h(z) \in (\mathbb{Z}/p\mathbb{Z})[z]$ of τ, and an explicit isomorphism κ from $\tilde{\mathbf{K}} = (\mathbb{Z}/p\mathbb{Z})[z]/(h(z))$ onto $\mathbf{K}$. All this requires $O(w)$ operations in $\mathbf{K}$ and $O(w^3)$ operations in $\mathbb{Z}/p\mathbb{Z}$. Given any degree d irreducible polynomial $\tilde{f}(x)$ in $\tilde{\mathbf{K}}[x]$ we deduce an irreducible polynomial in $\mathbf{K}[x]$ by applying the isomorphism κ to every coefficient in $\tilde{f}(x)$. This requires dw^2 operations in $\mathbb{Z}/p\mathbb{Z}$. So our algorithms and complexity estimates remain valid in that case, as long as elementary operations in $\mathbf{K}$ can be computed in time $(\log q)^{4+o(1)}$ elementary operations. This includes all the reasonable known models for finite fields, including normal bases and towers of extensions.

Notation: if $\mathbf{K}$ is a field with characteristic p and q is a power of p, we note $\Phi_q : \mathbf{K} \to \mathbf{K}$ the morphism which raises to the q-th power. If $\mathbf{G}$ is an algebraic group over $\mathbf{K}$ we note $\varphi_q : \mathbf{G} \to \mathbf{G}^{(q)}$ the Frobenius morphism.

Acknowledgements: we thank K. Kedlaya for pointing his joint work with Umans [9] to us, and H. Lenstra for explaining to us how to save a $\log q$ factor in the complexity using [7].

2 Basic constructions

In this section $\mathbf{K}$ is a finite field with $q = p^w$ elements and Ω is an algebraic closure of $\mathbf{K}$. For every positive integer k, we denote by $\mathbb{F}_{p^k}$ the unique subfield of Ω with p^k elements. We explain how to quickly construct a degree d irreducible polynomial when d is a prime power ℓ^δ and ℓ divides $p(q-1)$. All the constructions in this section are known, but deserve to be quickly surveyed. Section 2.1 deals with the case $\ell = p$. Section 2.2 deals with the case when ℓ is a prime divisor of $(q-1)$. Section 2.3 is concerned with the special case $\ell = 2$ and q odd. In Section 2.4 we detail on a simple example how Gauss periods can be useful in some cases. Although the results in Section 2.4 are not necessary to

prove Theorem 1, several ideas at work in this section play a decisive role later in the slightly more advanced context of Section 5.

2.1 Artin-Schreier towers

In this section we are given a p-th power $d = p^\delta$ and we want to construct a degree d irreducible polynomial in $\mathbf{K}[x]$. We use a construction of Lenstra and de Smit [6] in that case. If k and l are two positive integers such that k divides l we define the polynomial $T_{l,k}(x) = x+x^{p^l}+x^{p^{2l}}+\cdots+x^{p^{(\frac{k}{l}-1)l}}$. For every positive integer k we denote by $\mathcal{A}_k \subset \Omega$ the subset consisting of all scalars $a \in \Omega$ such that the three following conditions hold true:

1. a generates $\mathbb{F}_{p^k}$ over $\mathbb{F}_p$ i.e. $\mathbb{F}_p(a) = \mathbb{F}_{p^k}$,
2. a has non-zero absolute trace: $T_{1,k}(a) \neq 0$,
3. a^{-1} has non-zero absolute trace: $T_{1,k}(a^{-1}) \neq 0$.

We set $I(X) = \frac{X^p-1}{\sum_{1\leqslant i\leqslant p-1} X^i}$. This rational fraction induces an unramified covering

$$I : \Omega - \mathbb{F}_p \to \Omega - \{0\}.$$

We check that $I^{-1}(\mathcal{A}_k) \subset \mathcal{A}_{pk}$ for every $k \geq 1$. Indeed, if $a \in \mathcal{A}_k$ and if $I(b) = a$ then $b \neq 1$ and

$$\frac{1}{(1-b)^p} - \frac{1}{1-b} = \frac{b^p - b}{(b-1)^{p+1}} = \frac{b+\cdots+b^{p-1}}{b^p-1} = a^{-1}.$$

So $1/(1-b)$ is a root of the separable polynomial $x^p - x = a^{-1}$. This polynomial is irreducible over $\mathbb{F}_{p^k}[x]$ because the absolute trace of a^{-1} is non-zero. So $\mathbb{F}_p(b) = \mathbb{F}_{p^{pk}}$. Further b is a root of the polynomial $x^p - a(x^{p-1}+\cdots+x) - 1$. So the trace $T_{k,pk}(b)$ of b relative to the extension $\mathbb{F}_{p^{pk}}/\mathbb{F}_{p^k}$ is a. As a consequence the absolute trace of b is $T_{1,pk}(b) = T_{1,k}(T_{k,pk}(b)) = T_{1,k}(a)$ the absolute trace of a; and it is non-zero. Now b^{-1} is a root of the reversed polynomial $x^p + a(x^{p-1}+\cdots+x) - 1$. So the trace of b^{-1} relative to the extension $\mathbb{F}_{p^{pk}}/\mathbb{F}_{p^k}$ is $-a$. As a consequence the absolute trace of b^{-1} is the opposite of the absolute trace of a; and it is non-zero.

Since $\mathcal{A}_1 = \mathbb{F}_p - \{0\}$ we deduce that $\#\mathcal{A}_{p^k} \geq (p-1)p^k$. In particular the fiber above 1 of the iterated rational fraction $I^{(\delta)}$ is irreducible over $\mathbb{F}_p$. If w is prime to p then this fiber remains irreducible over $\mathbf{K} = \mathbb{F}_q$. In general, we factor the degree w of $\mathbb{F}_q/\mathbb{F}_p$ as $w = p^e w'$ where w' is prime to p. We first look for an element $a \in \mathcal{A}_{p^e} \subset \mathbb{F}_q$. Using the remarks above we can find such an a by solving e Artin-Schreier equations with coefficients in $\mathbb{F}_q$. To this end, we write down the matrix of the $\mathbb{F}_p$-linear map $x \mapsto x^p - x$ in the $\mathbb{F}_p$-basis $(1, z, \ldots, z^{w-1})$ of $\mathbf{K} = (\mathbb{Z}/p\mathbb{Z})[z]/(h(z))$. We then solve the e corresponding $\mathbb{F}_p$-linear systems of dimension w. Altogether, finding a requires $O(w \times \log p)$ operations in $\mathbf{K}$ and $O(ew^3)$ operations in $\mathbb{F}_p$. Since $w = O(\log q)$ and $e = O(\log w) = O(\log\log q)$ we end up with a complexity of $(\log q)^{4+o(1)}$ elementary operations.

The fiber $I^{-\delta}(a)$ is a degree p^δ irreducible divisor over $\mathbb{F}_{p^{p^e}}$. It remains irreducible over $\mathbf{K} = \mathbb{F}_q$. There remains to compute the annihilating polynomial of this fiber. We compute the iterated rational fraction $I^\delta(x) = \frac{N(x)}{D(x)}$. Composition of polynomials and power series can be computed in quasi-linear time i.e. $d^{1+o(1)} \times (\log q)^{1+o(1)}$ elementary operations, using recent results by Umans and Kedlaya [15, 9]. See Corollary 2 in Section 7.5 below. An older algorithm due to Brent and Kung has exponent $\frac{\omega+1}{2} + o(1)$ where ω is the exponent in matrix multiplication. So we can compute $N(x)$ and

$D(x)$ at the expense of $p^{\delta+o(1)} \times (\log q)^{1+o(1)} = d^{1+o(1)} \times (\log q)^{1+o(1)}$ elementary operations. The polynomial $f(x) = N(x) - aD(x)$ is an irreducible degree d polynomial in $\mathbf{K}[x]$.

An example: We take $p = 2$, $q = 4$, $\delta = 2$ and $d = 4$. We assume $\mathbf{K} = \mathbb{F}_2[z]/(z^2 + z + 1)$. So $e = 1$. We know that $1 \in \mathcal{A}_1$. We set $a = z \bmod z^2 + z + 1$ and check that $I(a) = 1$. So $a \in \mathcal{A}_2$. We compute $I(I(x)) = \frac{x^4+x^2+1}{x^3+x}$ and set $f(x) = x^4 + x^2 + 1 - a(x^3 + x)$. This is an irreducible polynomial in $\mathbf{K}[x]$.

2.2 Radicial extensions

In this section ℓ is a prime dividing $q - 1$. Let $d = \ell^\delta$ for some positive integer δ. In the special case $\ell = 2$ we further ask that $\ell^2 = 4$ divide $q - 1$. We want to construct a degree d irreducible polynomial in $\mathbf{K}[x]$. This is a very classical case. We write $q - 1 = \ell^e \ell'$ where ℓ' is prime to ℓ. We first look for a generator a of the ℓ-Sylow subgroup of $\mathbb{F}_q^*$. To find such a generator, we pick a random element in $\mathbb{F}_q^*$ and raise it to the power ℓ'. Call a the result. Check that $a^{\ell^{e-1}} \neq 1$. If this is not the case, start again. The probability of success is $1 - 1/\ell$. The average complexity of finding such an a is $O(\log q)$ operations in $\mathbb{F}_q$. The polynomial $f(x) = x^d - a$ is irreducible in $\mathbb{F}_q[x]$. This is well know but we try to prove it in a way that will be easily adapted to a more general context later.

The $\ell^{\delta+e}$-torsion $\mathbf{G}_m[\ell^{\delta+e}]$ of the multiplicative group $\mathbf{G}_m$ is isomorphic to $(\mathbb{Z}/\ell^{\delta+e}\mathbb{Z}, +)$ and the Frobenius endomorphism $\varphi_q : \mathbf{G}_m \to \mathbf{G}_m$ acts on it as multiplication by q. The order of $q = 1 + \ell'\ell^e$ in $(\mathbb{Z}/\ell^{e+\delta}\mathbb{Z})^*$ is $\ell^\delta = d$. So the Frobenius Φ_q acts transitively on the roots of $f(x)$.

An example: We take $p = 5$, $q = 5$, $\ell = 2$, $\delta = 3$ and $d = 8$. We check that 4 divides $p - 1$. In particular $e = 2$ and $\ell' = 1$. The class $a = 2 \bmod 5$ generates the 2-Sylow subgroup of $(\mathbb{Z}/5\mathbb{Z})^*$. Indeed $2^4 = 1 \bmod 5$ and $2^2 = -1 \bmod 5$. We set $f(x) = x^8 - 2$.

2.3 A special case

In this section we assume that p is odd, $\ell = 2$ and $d = 2^\delta$ for some positive δ. We need to adapt the methods of Section 2.2 in that special case because the group of units in $\mathbb{Z}/d\mathbb{Z}$ that are congruent to 1 modulo ℓ is no longer cyclic when $\ell = 2$ and $\delta > 2$. We want to construct a degree d irreducible polynomial in $\mathbf{K}[x]$. This time we assume that 2^2 does not divide $q-1$. So q is congruent to 3 modulo 4. We set $Q = q^2$ and observe that 4 divides $Q - 1$.

We first look for a generator c of $\mathbb{F}_Q$ over $\mathbf{K} = \mathbb{F}_q$. For example we take c a root of the polynomial $y^2 - r$ where r is not a square in $\mathbf{K}$. If $\delta = 1$ we are done. Assume now $\delta \geq 2$. We write $Q - 1 = 2^e \ell'$ where ℓ' is prime to 2. We find a generator a of the 2-Sylow subgroup of $\mathbb{F}_Q^*$. The polynomial $F(x) = x^{d/2} - a$ is irreducible in $\mathbb{F}_Q[x]$. There remains to derive from $F(x)$ an irreducible polynomial $f(x)$ of degree d in $\mathbf{K}[x]$. We call $\bar{a} = \Phi_q(a) = a^q$ the conjugate of a over $\mathbb{F}_q$. We can compute it at the expense of $O(\log q)$ operations in $\mathbf{K}$. It is clear that $\bar{a} \neq a$ because the order of a is divisible by 4 and there is no point of order 4 in $\mathbf{G}_m(\mathbb{F}_q)$. The polynomial $f(x) = (x^{d/2} - a)(x^{d/2} + \bar{a})$ has coefficients in $\mathbf{K}$. It is irreducible over $\mathbf{K}$. Indeed, any root b of $x^{d/2} - a$ is also a root of $f(x)$. The field $\mathbb{F}_q(b)$ generated by b over $\mathbb{F}_q$ contains a and it has degree $d/2$ over $\mathbb{F}_q(a) = \mathbb{F}_Q$ because $F(x)$ is irreducible in $\mathbb{F}_Q[x]$. So $f(x)$ is irreducible in $\mathbf{K}[x]$.

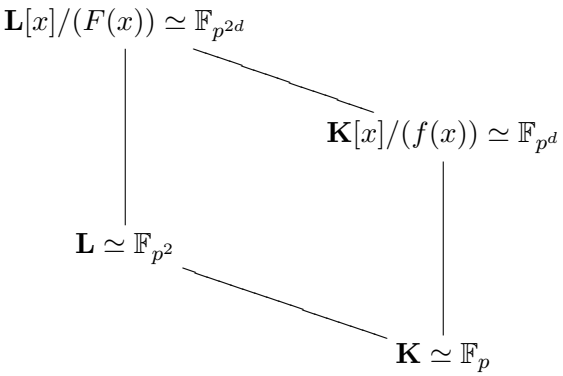
An example: We take $p = 7$, $q = 7$, $\ell = 2$, $\delta = 3$ and $d = 8$. Since 4 does not divide $q - 1$ we set $Q = q^2 = 49$. We factor $49 - 1 = 2^4 \times 3$ so $e = 4$ and $\ell' = 3$. We check that $r = 3 \bmod 7$ is not a square in $\mathbb{F}_7$. So we set $c = y \bmod y^2 - 3 \in \mathbb{F}_7[y]/(y^2 - 3)$. We set $a = (1 + c)^3 = 3 - c$ and check $a^{16} = 1$ and $a^8 = -1$. We set $F(x) = x^4 - a$. We compute $\bar{a} = a^7 = 3 + c$. We set $f(x) = (x^4 - a)(x^4 - \bar{a}) = x^8 + x^4 - 1$. This is an irreducible polynomial in $\mathbb{F}_7[x]$.

2.4 Gauss periods

In this section we assume $\ell = 3$ and $d = 3^\delta$ and $p = q \neq 3$. We assume that 3 does not divide $q - 1$. So q is congruent to 2 modulo 3, and we cannot apply the method in Section 2.2. We experiment in this simple context an idea that will be decisive in Section 5. We base change to a small auxiliary extension. We set $Q = q^2$ and observe that 3 divides $Q - 1$. We shall deal with the field $\mathbb{F}_Q$ with Q elements. We note that this idea is valid for any prime ℓ, but the degree of the auxiliary extension $\mathbb{F}_Q/\mathbb{F}_q$ might be quite large (up to $\ell - 1$) for a general ℓ. This is the reason why we shall later need to adapt this construction to the context of Kummer theory of elliptic curve.

We first need to build a computational model for this field. For example we pick a degree 2 irreducible polynomial $y^2 - r_1 y + r_2$ in $\mathbf{K}[x]$ and set $\mathbf{L} = \mathbf{K}[y]/(y^2 - r_1 y + r_2)$. We set $c = y \bmod y^2 - r_1 y + r_2$. We write $Q - 1 = 3^e \ell'$ where ℓ' is prime to 3. We find a generator a of the 3-Sylow subgroup of $\mathbf{L}^*$. The polynomial $F(x) = x^d - a$ is irreducible in $\mathbf{L}[x]$. There remains to derive from $F(x)$ an irreducible polynomial $f(x)$ of degree d in $\mathbf{K}[x]$.

Let $b = x \bmod F(x)$. This is a root of $F(x)$ in $\mathbf{L}[x]/(F(x))$. The later field has q^{2d} elements. Recall Φ_q is the application which raises to the q-th power. We have $\Phi_Q = \Phi_q^2$. For any $\alpha \in \mathbf{L}[x]/F((x))$ we set $\Sigma_1(\alpha) = \alpha + \Phi_q^d(\alpha)$ and $\Sigma_2(\alpha) = \alpha \times \Phi_q^d(\alpha)$.



Since d is a *prime power*, at least one among $\Sigma_1(b)$ and $\Sigma_2(b)$ generates an extension of degree d of $\mathbb{F}_q$. Otherwise $\Sigma_1(b)$ and $\Sigma_2(b)$ would both belong to the unique extension of degree $d/3$ of $\mathbf{K}$ inside $\mathbf{L}[x]/F((x))$; and b would then belong to the degree $d/3$ extension of $\mathbf{L}$ inside $\mathbf{L}[x]/(F(x))$, a contradiction. See also Lemma 1 of Section 7.1.

In other words, there exists a $k \in \{1, 2\}$ such that the polynomial

$$f(x) = \prod_{0 \leqslant l \leqslant d-1} (x - \Phi_q^l(\Sigma_k(b)))$$

is irreducible of degree d in $\mathbf{K}[x]$.

Three questions now worry us:

1. How to compute $\Sigma_k(b)$ for $k \in \{1, 2\}$?
2. How to find the good integer k ?
3. How to compute $f(x)$ starting from $F(x)$?

- Question 1 boils down to asking how to compute $\Phi_q^d(b)$. A first method would be to compute $\Phi_q^d(b)$ as b^{q^d} at the expense of $O(d \log q)$ operations in $\mathbf{L}[x]/(F(x))$. This would require $O(\log q) \times d^{2+o(1)}$ operations in $\mathbf{K}$. This is too much for us.

Instead of that, we should remind of the geometric origin of the polynomial $F(x)$. Indeed, b lies in $\mathbf{G}_m[3^{e+\delta}]$. We write $q^d = R \bmod 3^{e+\delta}$ where $0 \leqslant R < 3^{e+\delta} \leqslant Qd$. Then $\Phi_q^d(b) = b^R$ can be computed at the expense of $O(\log R) = O(\log q + \log d)$ operations in $\mathbf{L}[x]/(F(x))$. This requires $O(\log q) \times d^{1+o(1)}$ operations in $\mathbf{K}$.

- Question 2 can be solved by comparing $\Sigma_1(b)$ and its conjugate by $\Phi_q^{3^{\delta-1}}$ namely

$$\Phi_q^{3^{\delta-1}}(\Sigma_1(b)) = \Sigma_1(\Phi_q^{3^{\delta-1}}(b)) = \Phi_q^{3^{\delta-1}}(b) + \Phi_q^{3^\delta+3^{\delta-1}}(b).$$

Each of the two terms in the above sum can be computed as explained in the paragraph above.

- Question 3 is related to the following problem: we are given $\Sigma_k(b)$ for $k \in \{1, 2\}$. We know that $\Sigma_k(b)$ belongs to the degree d extension of $\mathbf{K}$ inside $\mathbf{L}[x]/(F(x))$. We want to compute its minimal polynomial $f(x)$ as a polynomial in $\mathbf{K}[x] \subset \mathbf{L}[x]$. One can apply a general algorithm for this task, such as the one given by Kedlaya and Umans [15, 9]. See also Theorem 4 in Section 7.5 below. They show that it is possible to compute this minimal polynomial at the expense of $d^{1+o(1)} \times (\log Q)^{1+o(1)}$ elementary operations. Thus the complexity is quasi-linear in d.

An example: We take $p = q = 5$, $\ell = 3$, $\delta = 2$, $d = 9$. So $Q = 25$, $Q - 1 = 3 \times 8$, $e = 1$ and $\ell' = 8$. We check that $r = 2 \bmod 5$ is not a square. We set $c = y \bmod y^2 - 2 \in \mathbb{F}_5[y]/(y^2 - 2)$. We compute $a = (1 + c)^8 = 2 + 3c$. We check $a^3 = 1$ and $a \neq 1$. We set $F(x) = x^9 - a$ and $b = x \bmod F(x)$. We need to compute the conjugate of b above $\mathbb{F}_{5^9}$. This is b^{5^9}. Remind b lies in $\mathbf{G}_m[27]$. So we don't raise b to the power 5^9 brutally. We rather compute $5^9 = 1953125 = -1 \bmod 27$. So $\Phi_{5^9}(b) = 1/b = 2(y + 1)x^8 \bmod (x^9 - 2 - 3y, y^2 - 2, 5)$. The product $\Sigma_2(b) = 1$ is not the good candidate. So we compute the characteristic polynomial of $\Sigma_1(b) = b + 1/b$ and find $f(x) = x^9 + x^7 + 2x^5 + 4x + 1 \in \mathbb{F}_5[x]$.

3 Compositum

In this section $\mathbf{K}$ is a finite field with $q = p^w$ elements and Ω is an algebraic closure of $\mathbf{K}$. For every positive integer k, we denote by $\mathbb{F}_{p^k}$ the unique subfield of Ω with p^k elements. We have seen in Section 2 how to construct an irreducible polynomial of degree d in $\mathbf{K}[x]$ when d is a prime power ℓ^δ and ℓ divides $p(q - 1)$. In Sections 5 and 4 we shall treat the case when d is a prime power ℓ^δ and ℓ is prime to $p(q - 1)$.

The last problem to be considered is thus the following one: given two irreducible polynomials $f_1(x)$ and $f_2(x)$ in $\mathbf{K}[x]$ with coprime degrees d_1 and d_2, construct a degree $d_1 d_2$ irreducible polynomial.

Let $\alpha_1 \in \Omega$ be a root of $f_1(x)$. Let $\alpha_2 \in \Omega$ be a root of $f_2(x)$. We first show that $\alpha_1 + \alpha_2$ generates an extension of degree $d_1 d_2$ of $\mathbb{F}_q$. Indeed, let $\Phi \in \mathrm{Gal}(\Omega/\mathbb{F}_q)$ be an automorphism that fixes $\alpha_1 + \alpha_2$:

$$\Phi(\alpha_1 + \alpha_2) = \alpha_1 + \alpha_2\,. \tag{1}$$

One deduces that $\Phi(\alpha_1) - \alpha_1 = \alpha_2 - \Phi(\alpha_2)$ is an element γ of the intersection $\mathbb{F}_q$ of $\mathbb{F}_{q^{d_1}}$ and $\mathbb{F}_{q^{d_2}}$. The order of Φ acting on $\mathbb{F}_{q^{d_1}}$ divides d_1. So $\Phi^{d_1}(\alpha_1) - \alpha_1 = d_1\gamma = 0$. We prove in the same way that $d_2\gamma = 0$. Since d_1 and d_2 are coprime we deduce that $\gamma = 0$. Thus Φ acts trivially on $\mathbb{F}_{q^{d_1}} = \mathbb{F}_q(\alpha_1)$ and on $\mathbb{F}_{q^{d_2}} = \mathbb{F}_q(\alpha_2)$, therefore also on their compositum $\mathbb{F}_{q^{d_1 d_2}}$. So $\alpha_1 + \alpha_2$ generates this compositum.

The same argument proves that $\alpha_1\alpha_2$ generates $\mathbb{F}_{q^{d_1 d_2}}$.

It is thus enough to compute the minimal polynomial of the sum or the product of α_1 and α_2. For this task, one may follow work by Bostan, Flajolet, Salvy and Schost [3], based on algorithms for symmetric power sums due to Kaltofen and Pan [5] and Schönhage [13]. See also [4]. This yields an algorithm with a quasi-linear time complexity in $d_1 d_2$.

4 Isogeny fibers

In this section we show how to construct irreducible polynomials using elliptic curves. Let $\mathbf{K}$ be a field and let Ω be an algebraic closure of $\mathbf{K}$. Let $E/\mathbf{K}$ be an elliptic curve given by the Weierstrass equation

$$E/\mathbf{K} \ : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \, .$$

We denote by $O_E = [0 : 1 : 0]$ the origin of E and by $x = X/Z$, $y = Y/Z$ the affine coordinates associated with the projective coordinates $[X : Y : Z]$.

Let $E'/\mathbf{K}$ be another elliptic curve in Weierstrass form. We define X', Y', Z', a'_1, a'_2, a'_3, a'_4, a'_6, x', y', O' similarly. Let $\iota/\mathbf{K} : E/\mathbf{K} \to E'/\mathbf{K}$ be a degree d separable isogeny. We assume that d is a positive odd number and the kernel $\operatorname{Ker}\iota$ is cyclic. Let $T \in E(\Omega)$ be a generator of $\operatorname{Ker}\iota$. Let $\psi_\iota(x) \in \mathbf{K}[x]$ be the degree $(d-1)/2$ polynomial

$$\psi_\iota(x) = \prod_{1 \leqslant k \leqslant (d-1)/2} (x - x(kT)) \, . \tag{2}$$

There exists a degree d polynomial $\phi_\iota(x) \in \mathbf{K}[x]$ and a polynomial $\omega_\iota(x,y) = \omega_0(x) + y\omega_1(x) \in \mathbf{K}[x,y]$ with degree 1 in y such that the image of the point (x,y) by ι is (x',y') where $x' = \frac{\phi_\iota(x)}{\psi_\iota^2(x)}$ and $y' = \frac{\omega_\iota(x,y)}{\psi_\iota^3(x)}$. We call $I(x) \in \mathbf{K}(x)$ the rational fraction $I(x) = \frac{\phi_\iota(x)}{\psi_\iota^2(x)}$.

Now let A be a $\mathbf{K}$-rational point on E' such that $2A \neq O'$ and let $B \in E(\Omega)$ be a point on E such that $I(B) = A$. We define the polynomial

$$f_{\iota,A}(x) = \phi_\iota(x) - x'(A)\psi_\iota^2(x) \in \mathbf{K}[x].$$

This is a separable polynomial. Its roots are the $x(B + kT)$ for $0 \leqslant k < d$.

The map $x : E(\Omega) - O \to \Omega$ induces a Galois equivariant bijection between the fiber $\iota^{-1}(A)$ and the roots of $f_{\iota,A}(x)$. In particular, $f_{\iota,A}(x)$ is irreducible if and only if the fiber $\iota^{-1}(A)$ is.

The residue ring of $I^{-1}(A)$ is $\mathbf{K}[x]/(f_{\iota,A}(x))$ and the class of y in this ring is given by equation:

$$y = \frac{y'(A)\psi_\iota^3(x) - \omega_0(x)}{\omega_1(x)} \bmod f_{\iota,A}(x). \tag{3}$$

The two questions that worry us are the following ones.

- Can we compute $f_{\iota,A}(x)$ quickly, *e.g.* in quasi-linear time in d ?
- Under which conditions is $f_{\iota,A}(x)$ irreducible ?

These two questions are successively addressed in Sections 4.1 and 4.2. In Section 4.3 we deduce a fast algorithm that constructs a degree d irreducible polynomial in $\mathbf{K}[x]$ when $\mathbf{K}$ is a finite field with $q = p^w$ elements and $d = \ell^\delta$ is a power of a prime ℓ such that ℓ is prime to $p(q-1)$ and $4\ell \leqslant q^{\frac{1}{4}}$.

4.1 Calculation of the polynomial $f_{\iota,A}(x)$

For any geometrical point $P \in E(\Omega)$, we denote by $\tau_P : E \to E$ the translation by P. Let x_P be the function $x \circ \tau_{-P}$ and similarly let y_P be the function $y \circ \tau_{-P}$. If $P = kT$, we moreover define $x_k = x_{kT}$ and $y_k = y_{kT}$. Recall d is assumed to be odd. In this section we present methods for fast construction of isogenies. Section 4.1.1 concerns isogenies with split cyclic kernel. We just recall Vélu's formulae in that case. Section 4.1.2 recalls how one can take advantage of the decomposition of an isogeny into several ones with smaller degrees. This is particularly useful when $E/\mathbf{K}$ has complex multiplication and the isogeny in question is the kernel isogeny associated to some power of an invertible prime ideal in the endomorphism ring of E. This idea is detailed in Section 4.1.3.

4.1.1 Vélu's isogenies

In this paragraph, we assume that T is a $\mathbf{K}$-rational point and ι is the isogeny given by Vélu's formulae [16]:

$$\left\{ \begin{array}{rcl} x' & = & x + \displaystyle\sum_{0<k<d} \left[x_k - x(kT) \right] , \\ y' & = & y + \displaystyle\sum_{0<k<d} \left[y_k - y(kT) \right] . \end{array} \right. \tag{4}$$

We put some order in Eq. (4). We first express x_k in terms of x and y,

$$\begin{array}{rcl} x_{kT} \times (x - x(kT))^2 & = & x(kT)x^2 + (a_3 + 2y(kT) + a_1 x(kT))\, y \\ & + & \left(a_4 + a_1^2 x(kT) + a_1 a_3 + 2a_2 x(kT) + a_1 y(kT) + x(kT)^2 \right) x? \\ & + & a_3^2 + a_1 a_3 x(kT) + a_3 y(kT) + a_4 x(kT) + 2a_6. \end{array} \tag{5}$$

We deduce that $x_{kT} + x_{-kT} - 2x(kT)$ is equal to

$$\frac{(6x(kT)^2 + (a_1^2 + 4a_2)x(kT) + a_1 a_3 + 2a_4)x? - 2x(kT)^3 + (a_1 a_3 + 2a_4)x(kT) + a_3^2 + 4a_6}{(x - x(kT))^2} . \tag{6}$$

One computes the rational fraction $x' = \frac{\phi_\iota(x)}{\psi_\iota^2(x)}$ using Eqs. (4) and (6) by gathering the terms relative to k and $-k$, with the help of a *divide and conquer* strategy. Complexity is quasi-linear in d.

A similar calculation gives us the explicit form of $y' = \frac{\omega_\iota(x,y)}{\psi_\iota^3(x)}$.

4.1.2 Composition of isogenies

Assume d factors as $d_1 d_2$. Then the degree d isogeny $\iota : E \to E'$ decomposes as $\iota = \iota_2 \circ \iota_1$ where $\iota_1 : E \to F$ is a degree d_1 isogeny and $\iota_2 : F \to E_2$ is a degree d_2 isogeny. The kernel of ι_1 is generated by $d_2 T$ and the kernel of ι_2 is generated by $\iota_1(T)$. Let $I(x)$ be the degree d rational fraction associated with ι. Define similarly $I_1(x)$ and $I_2(x)$. Then $I(x) = I_2(I_1(x))$. We may then compute $I(x)$ in three steps: first compute $I_1(x)$, then compute $I_2(x)$, and finally compute the composition $I = I_2 \circ I_1$ using work by Umans and Kedlaya [15, 9]. See Corollary 2 in Section 7.5.

4.1.3 A special simple case

We now assume that $\mathbf{K}$ is a finite field with $q = p^w$ elements. Let $\varphi_q : E \to E$ be the Frobenius endomorphism of E and by t its trace. Let $\mathcal{O}$ be the quotient ring $\mathbb{Z}[X]/(X^2 - tX + q)$ and let α

be the class of X in $\mathcal{O}$. We call $\epsilon : \mathcal{O} \to \mathrm{End}(E)$ the ring monomorphism that sends α onto φ_q. For every subset S of $\mathcal{O}$ we define the *kernel* of S in E to be the intersection of all the kernels of the endomorphisms $\epsilon(s)$ for $s \in S$. This is a subgroup scheme of E. We denote it by $E[S]$. Let ℓ be a prime not dividing $p(q-1)$. We assume that ℓ divides the order $q+1-t$ of $E(\mathbf{K})$. As a consequence ℓ is coprime to t^2-4q.

We have

$$X^2 - tX + q = (X-1)(X-q) \bmod \ell\,,$$

because $1-t+q$ is divisible by ℓ and the product of the roots of X^2-tX+q equals q. Furthermore, the roots $1 \bmod \ell$ and $q \bmod \ell$ are distinct because ℓ does not divide $q-1$.

Let $\mathfrak{l} = (\ell, \alpha - 1)$ be the prime ideal in $\mathcal{O}$ above ℓ and containing $\alpha - 1$. This is an invertible ideal. It's kernel in E is $E[\ell](\mathbf{K})$ the rational part of the ℓ-torsion of E.

Let m be a positive integer. According to Hensel's lemma, there exist two integers λ_m and μ_m in $[0, \ell^m[$ such that $\lambda_m = 1 \bmod \ell$, $\mu_m = q \bmod \ell$ and

$$X^2 - tX + q = (X-\lambda_m)(X-\mu_m) \bmod \ell^m.$$

The ideal $\mathfrak{l}^m$ of $\mathcal{O}$ is generated by ℓ^m and $\alpha - \lambda_m$. The kernel of $\mathfrak{l}^m$ in E is a cyclic group of order ℓ^m inside $E(\Omega)$. We denote by $\iota_m : E \to E_m$ the quotient isogeny by $E[\mathfrak{l}^m]$. The elliptic curve E_m is defined over $\mathbf{K}$, a finite field with q elements. Let $\epsilon_m : \mathcal{O} \to \mathrm{End}(E_m)$ be the ring homomorphism that sends α onto the q-Frobenius endomorphism of E_m. The two homomorphisms ϵ and ϵ_m are compatible with the isogeny ι_m in the sense that for every s in $\mathcal{O}$ one has $\epsilon_m(s) = \iota_m \circ \epsilon(s) \circ \iota_m^{-1}$. For every subset S of $\mathcal{O}$ we define the *kernel* of S in E_m to be the intersection of all the kernels of the endomorphisms $\epsilon_m(s)$ for $s \in S$. This is a subgroup scheme of E_m. We denote it by $E_m[S]$.

Using Lemma 2 of Section 7.2 we see that $\iota_{m+1} : E \to E_{m+1}$ decomposes as $\jmath_{m+1} \circ \iota_m$ where $\jmath_{m+1} : E_m \to E_{m+1}$ is a degree ℓ isogeny with kernel $E_m[\mathfrak{l}] = E_m[\ell](\mathbf{K})$.

We denote by $I_m(x) \in \mathbf{K}(x)$ the degree ℓ^m rational fraction associated with ι_m. We denote by $J_m \in \mathbf{K}(x)$ the degree ℓ rational fraction associated with $\jmath_m$. We have $\jmath_1 = \iota_1$. So $I_1 = J_1$ and $I_m = J_m \circ \cdots J_2 \circ J_1$. Every rational fraction J_k can be computed using the method of Paragraph 4.1.1. The composition I_m can be computed using the method in Paragraph 4.1.2.

4.2 Irreducibility conditions

We assume that we still are in the situation of Paragraph 4.1.3. We have a finite field $\mathbf{K}$ with q elements. We denote by p its characteristic. We have an elliptic curve E over $\mathbf{K}$. We denote by $\varphi_q : E \to E$ the Frobenius endomorphism of E and by t its trace. Let ℓ be a prime not dividing $p(q-1)$. In particular ℓ is odd. We assume that ℓ divides the order $q+1-t$ of $E(\mathbf{K})$. We want to construct an irreducible polynomial $f(x) \in \mathbf{K}[x]$ with degree $d = \ell^\delta$. We factor $q+1-t$ as $q+1-t = \ell^e \ell'$ where ℓ' is prime to ℓ. We use the notation introduced in Paragraph 4.1.3.

There exist two integers $\lambda_{e+\delta}$ and $\mu_{e+\delta}$ such that

$$\begin{aligned} \lambda_{e+\delta} = 1 \bmod \ell^e \quad &, \quad \mu_{e+\delta} = q \bmod \ell^e\,, \\ X^2 - tX + q \quad &= \quad (X - \lambda_{e+\delta})(X - \mu_{e+\delta}) \bmod \ell^{e+\delta}\,. \end{aligned}$$

We write $\lambda_{e+\delta} = 1 + \ell^e \ell''$ with ℓ'' prime to ℓ. In the sequel we set $\lambda = \lambda_{e+\delta}$ and $\mu = \mu_{e+\delta}$. Let now

$$\mathfrak{d} = (d, \alpha - \lambda) = (\ell, \alpha - \lambda)^\delta = \mathfrak{l}^\delta.$$

This is an invertible ideal. Its kernel $E[\mathfrak{d}]$ in E is the kernel of the isogeny $\iota_\delta : E \to E_\delta$. The ℓ-Sylow subgroup of $E_\delta(\mathbf{K})$ is the kernel of $\mathfrak{l}^e = (\ell^e, \alpha - 1)$ in E_δ and it is cyclic. Let A be a generator of it. Let $B \in E(\Omega)$ such that $\iota_\delta(B) = A$. Then B generates the kernel of $\mathfrak{l}^{e+\delta} = (\ell^{e+\delta}, \varphi_q - \lambda)$ in E. Especially,

$$\varphi_q(B) = \lambda B, \tag{7}$$

and the order of $\lambda = 1 + \ell^e \ell''$ in $(\mathbb{Z}/\ell^{e+\delta}\mathbb{Z})^*$ is $d = \ell^\delta$. Thus, the Galois orbit of B has cardinality d and the polynomial $f_{\iota,A}(X)$ is irreducible.

4.3 Existence conditions

Assume we are given a finite field $\mathbf{K}$ with characteristic p and cardinality q and an integer $d = \ell^\delta$ such that ℓ is prime to $p(q-1)$. We look for a degree d irreducible polynomial in $\mathbf{K}[x]$. The construction in Section 4.2 requires an elliptic curve over $\mathbf{K}$ such that ℓ divides the cardinality $q + 1 - t$ of $E(\mathbf{K})$. Is there any such elliptic curve ? How can we find it ?

If $\ell \leqslant 2\sqrt{q}$ then there are at least two consecutive integer multiples of ℓ in the interval $[q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$. At least one of them is not congruent to 1 modulo p. So there exists at least one elliptic curve with cardinality divisible by the prime ℓ.

We want to bound from below the number of such elliptic curves. We use the results of Lenstra [10] extended by Howe [7]. >From Theorem 2 and Corollary 1 of Section 7.4 we deduce that the proportion of Weierstrass elliptic curves over a finite field $\mathbf{K}$ with q element having order divisible by ℓ is $\frac{1}{\ell-1}$ up to an error term bounded in absolute value by $\frac{8\ell}{\sqrt{q}}$. We deduce that if

$$4\ell \leqslant q^{\frac{1}{4}} \tag{8}$$

then this proportion is at least $\frac{1}{2\ell}$.

In that case, we can find such an elliptic curve in the following way: we pick a random Weierstrass elliptic curve over $\mathbf{K}$. We compute its cardinality using Schoof's algorithm at the expense of $(\log q)^{5+o(1)}$ elementary operations. If this cardinality is divisible by ℓ we are done. Otherwise we try again. The average number of trials is $O(\ell)$. The expected time to find the needed curve E is $O(\ell(\log q)^{4+o(1)})$ operations in $\mathbf{K}$ provided condition (8) holds true.

The conclusion of this section is that we have a fast algorithm that constructs a degree d irreducible polynomial in $\mathbf{K}[x]$ when $\mathbf{K}$ is a finite field with $q = p^w$ elements and $d = \ell^\delta$ is a power of a prime ℓ such that ℓ is prime to $p(q-1)$ and $4\ell \leqslant q^{\frac{1}{4}}$.

4.4 An Example

We take $p = 7$, $q = 7$ and $d = 5$. The elliptic curve

$$E/\mathbb{F}_7 \ : y^2 = x^3 + x + 4$$

has got ten $\mathbb{F}_7$-rational points. The point $T = (6, 4)$ has order $\ell = 5$. The group generated by T is

$$\langle T \rangle = \{O_E,\ (6,4),\ (4,4),\ (4,3),\ (6,3)\}\ .$$

The quotient by $\langle T \rangle$ isogenous curve E' is given by Vélu's formulae

$$E' \ : y^2 = x^3 + 3\,x + 4.$$

Moreover, Eq. (4) yields

$$x' = x + \frac{y + 6\,x^2 + 2\,x}{(x+1)^2} - 6 + \frac{y + 4\,x^2 + 3\,x + 5}{(x+3)^2} - 4 + \\ \frac{6\,y + 4\,x^2 + 3\,x + 5}{(x+3)^2} - 4 + \frac{6\,y + 6\,x^2 + 2\,x}{(x+1)^2} - 6\,.$$

Using Eq. (6), we find an expression for x' in terms of x alone:

$$x' = x + \frac{x+2}{(x+1)^2} + \frac{1}{(x+3)^2} = \frac{x^5 + x^4 + 2\,x^3 + 5\,x^2 + 4\,x + 5}{(x+3)^2\,(x+1)^2}\,.$$

There remains to choose a point A of order 5 in $E'(\mathbb{F}_7)$, for instance $A = (1, 1)$, and we finally obtain,

$$f_{\iota,A}(x) = x^5 + x^4 + 2\,x^3 + 5\,x^2 + 4\,x + 5 - (x+3)^2\,(x+1)^2 = x^5 + x^3 + 4\,x^2 + x + 3\,.$$

5 Base change

In this section $\mathbf{K} = (\mathbb{Z}/p\mathbb{Z})[z]/(h(z))$ is a finite field with $q = p^w$ elements. We still assume here that $d = \ell^\delta$ is a power of a prime ℓ where ℓ is prime to $p(q-1)$. We look for a degree d irreducible polynomial in $\mathbf{K}[x]$. However, we no longer assume that $4\ell \leqslant q^{\frac{1}{4}}$.

We adapt the main idea in Section 2.4 to the context of elliptic curves: we base change to a small auxiliary extension.

Let n be the smallest integer coprime with $\ell(\ell-1)$ such that $Q = q^n$ satisfies $4\ell \leqslant Q^{\frac{1}{4}}$. According to Iwaniec's result about Jacobsthal's problem [8] we have $n = (\log \ell)^{2+o(1)}$. Let us remark that d is then coprime with $Q - 1$ too.

Using e.g. the methods in Shoup [14] we find a degree n irreducible polynomial $g(y) \in \mathbf{K}[y]$. We set $\mathbf{L} = \mathbf{K}[y]/(g(y))$. A basis of this $(\mathbb{Z}/p\mathbb{Z})$-vector space is given by the $z^j y^i$ for $0 \leqslant i < n$ and $0 \leqslant j < w$. Using the method explained in the introduction we find a generator τ of the $(\mathbb{Z}/p\mathbb{Z})$-algebra $\mathbf{L}$. We compute also the minimal polynomial $h(u) \in (\mathbb{Z}/p\mathbb{Z})[u]$ of τ. We set $\tilde{\mathbf{L}} = (\mathbb{Z}/p\mathbb{Z})[u]/(h(u))$. A basis of this $(\mathbb{Z}/p\mathbb{Z})$-vector space is given by the u^k for $0 \leqslant k < nw$. We compute and store the matrix of the isomorphism $\kappa : \tilde{\mathbf{L}} \to \mathbf{L}$ that sends $u \bmod h(u)$ onto τ. This is a $nw \times nw$ matrix with entries in $\mathbb{Z}/p\mathbb{Z}$. We also compute and store the inverse of this matrix. The image $\tilde{\mathbf{K}} = \kappa^{-1}(\mathbf{K})$ of $\mathbf{K}$ by κ^{-1} is the unique subfield with q elements inside $\tilde{\mathbf{L}}$.

The reason for introducing these two different models of the field with q^n elements is that, on the one hand, this field should be constructed as an extension of $\mathbf{K}$ because we shall have to descend to $\mathbf{K}$ later on; but on the other hand, the field with q^n elements should be also presented as a monogenous extension of $\mathbb{Z}/p\mathbb{Z}$, because all the algorithms described and used so far (an in particular the algorithms due to Umans and Kedlaya) require that the base field be presented as a monogenous extension of $\mathbb{Z}/p\mathbb{Z}$.

One can now apply the construction of Section 4 to $\tilde{\mathbf{L}}$ and obtain an irreducible polynomial $F_{\iota,A}(x)$ of degree d in $\tilde{\mathbf{L}}[x]$, in time

$$(\log Q)^{5+o(1)} d^{1+o(1)} = (\log q)^{5+o(1)} d^{1+o(1)}$$

elementary operations.

Remind $F_{\iota,A}(x)$ is the minimal polynomial of $x(B)$ where B is a geometric point of order $\ell^{e+\delta} \leqslant 4Qd$ on an elliptic curve E over $\tilde{\mathbf{L}}$. We also are given an integer λ such that $0 \leqslant \lambda < \ell^{e+\delta}$ and

$$\varphi_Q(B) = \lambda B. \tag{9}$$

It remains to derive from $F_{\iota,A}(x)$ an irreducible polynomial $f(x)$ of degree d over $\mathbf{K}$.

We set $\alpha = x(B) \in \tilde{\mathbf{L}}[x]/(F_{\iota,A}(x))$. This is a root of $F_{\iota,A}(x)$. Recall Φ_q is the application which raises to the q-th power. We have $\Phi_Q = \Phi_q^n$. The field $\tilde{\mathbf{L}}[x]/(F_{\iota,A}(x)) = \tilde{\mathbf{L}}(\alpha)$ is an extension of degree d of $\tilde{\mathbf{L}}$. For any integer k between 1 and n, one denotes by $\Sigma_k(\alpha)$ the k-th symmetric function of the conjugates of α over the subfield with q^d elements:

$$\alpha,\ \Phi_q^d(\alpha),\ \Phi_q^{2d}(\alpha),\ \ldots,\ \Phi_q^{(n-1)d}(\alpha)\,.$$

Since d is a *prime power*, we deduce from Lemma 1 of Section 7.1 that at least one among these n symmetric functions generates the extension of degree d of $\tilde{\mathbf{K}}$. In other words, there exists a k between 1 and n such that the polynomial

$$\tilde{f}(x) = \prod_{0 \leqslant l < d} (x - \Phi_q^l(\Sigma_k(\alpha)))$$

is irreducible of degree d in $\tilde{\mathbf{K}}[x] \subset \tilde{\mathbf{L}}[x]$.

Three questions now worry us.

- How to compute $\Sigma_k(\alpha)$ and its conjugates ?
- How to find the good integer k ?
- How to compute $\tilde{f}(x) \in \tilde{\mathbf{K}}[x]$ starting from $F_{\iota,A}(x) \in \tilde{\mathbf{L}}[x]$?

5.1 How to compute $\Sigma_k(\alpha)$ and its conjugates ?

First, let us note $\alpha_l = \Phi_q^l(\alpha)$ for every integer l and let us see how to compute one of these conjugates.We first need to compute $\beta = y(B)$ as an element in the residue ring $\tilde{\mathbf{L}}[x]/(F_{\iota,A}(x))$. For this, we use Eq. (3).

Let now l be an integer between 0 and $dn - 1$. We want to compute $\alpha_l = \Phi_q^l(\alpha)$. We write $l = r + ns$ with $0 \leqslant r < n$ and $0 \leqslant s < d$. Then,

$$\alpha_l = \Phi_q^l(\alpha) = \Phi_q^r(\Phi_Q^s(\alpha))\,.$$

We first compute $\Phi_Q^s(\alpha) = x(\varphi_Q^s(B)) = x(\lambda^s B)$ using Eq. (9). To this end, we write $\lambda^s = R \bmod \ell^{e+\delta}$ where $0 \leqslant R < \ell^{e+\delta}$ and we multiply the $\ell^{\delta+e}$-torsion point $B \in E(\tilde{\mathbf{L}}[x]/(F_{\iota,A}(x)))$ by R using fast exponentiation. This is done at the expense of $O(\log Q + \log d)$ operations in $\tilde{\mathbf{L}}[x]/(F_{\iota,A}(x))$.

One then raises $\Phi_Q^s(\alpha)$ to the q^r-th power at the expense of at most $n \log q$ operations modulo $F_{\iota,A}(x)$. Thus, each conjugate is computed at the expense of

$$d^{1+o(1)}(\log q)^{2+o(1)}\,.$$

elementary operations.

To compute all the $(\Sigma_k(\alpha))_{0<k\leqslant n}$, one computes the n conjugates $\alpha, \Phi_q^d(\alpha), \Phi_q^{2d}(\alpha), \ldots, \Phi_q^{(n-1)d}(\alpha)$ and one forms the corresponding polynomial of degree n. Altogether, the computation of the symmetric functions $(\Sigma_k(\alpha))_{0<k\leqslant n}$ requires

$$d^{1+o(1)}(\log q)^{2+o(1)},$$

elementary operations.

5.2 How to find the integer k ?

One seeks an integer k between 1 and n such that $\Sigma_k(\alpha)$ generates an extension of degree d of $\tilde{\mathbf{K}}$.We know that there is at least one such integer. So we successively test all the k between 1 and n. As n is small, this is not a problem. We know that $\Sigma_k(\alpha)$ generates the degree d extension of $\tilde{\mathbf{K}}$ if and only if

$$\Phi_q^{\ell^{\delta-1}}(\Sigma_k(\alpha)) \neq \Sigma_k(\alpha)\,,$$

where $\ell^{\delta-1}$ is the unique maximal divisor of d. This condition is equivalent to

$$\Sigma_k(\Phi_q^{\ell^{\delta-1}}(\alpha)) \neq \Sigma_k(\alpha),$$

or

$$\Sigma_k(\alpha_{\ell^{\delta-1}}) \neq \Sigma_k(\alpha).$$

One computes the $\Sigma_k(\alpha_{\ell^{\delta-1}})$'s in the same way as the $\Sigma_k(\alpha)$'s, following Section 5.1. It is then easy to compare $\Sigma_k(\alpha_{\ell^{\delta-1}})$ and $\Sigma_k(\alpha)$.

One can thus find k in

$$d^{1+o(1)}(\log q)^{2+o(1)}$$

elementary operations.

5.3 How to compute the characteristic polynomial $f(x)$?

We now have an element $\Sigma_k(\alpha)$ of $\tilde{\mathbf{L}}[x]/(F_{\iota,A}(x))$ and we know that it actually belongs to the degree d extension of $\tilde{\mathbf{K}}$. But this is not really visible because $\Sigma_k(\alpha)$ is given in the basis $1, x, \ldots, x^{d-1}$ of $\tilde{\mathbf{L}}[x]/(F_{\iota,A}(x))$. Still, the characteristic polynomial $\tilde{f}(x)$ of $\Sigma_k(\alpha)$ has coefficients in $\tilde{\mathbf{K}} \subset \tilde{\mathbf{L}}$. We compute this characteristic polynomial. We use a general algorithm for this task, such as the one appearing in recent work by Umans and Kedlaya [15, 9]. See Theorem 4 in Section 7.5. This algorithm requires $d^{1+o(1)} \times (\log Q)^{1+o(1)}$ elementary operations. Finally, we apply the isomorphism $\kappa : \tilde{\mathbf{L}} \to \mathbf{L}$ to every coefficient in $\tilde{f}(x)$ and we find a polynomial $f(x)$ with coefficients in $\mathbf{K} \subset \mathbf{L}$. This polynomial is irreducible in $\mathbf{K}[x]$.

6 Summary

The following theorem summarizes our work in this paper.

Theorem 1 *There exists a probabilistic (Las Vegas) algorithm that on input a finite field $\mathbf{K}$ with characteristic p and cardinality $q = p^w$, and a positive integer d, returns a degree d irreducible polynomial in $\mathbf{K}[x]$. The algorithm requires $d^{1+o(1)} \times (\log q)^{5+o(1)}$ elementary operations.*

The statement above assumes that the finite field $\mathbf{K}$ is given in a reasonable way as explained in the introduction. The algorithms runs as follows.

We first factor the degree d as $d = \prod_i \ell_i^{\delta_i}$. This requires $O(d)$ elementary operations. Section 3 shows that it suffices to find an irreducible polynomial of degree $\ell_i^{\delta_i}$ for every i.

So we may assume that $d = \ell^\delta$ is a prime power.

If $\ell = p$ we use the construction in Section 2.1.

If ℓ divides $q-1$ we use the construction in Sections 2.2 and 2.3.

Assume now ℓ is prime to $p(q-1)$. We find the smallest integer n such that n is coprime with $\ell(\ell-1)$ and $Q=q^n$ satisfies

$$4\ell \leqslant Q^{\frac{1}{4}}.$$

Using e.g. the methods in Shoup [14] we find a degree n irreducible polynomial $g(y) \in \mathbf{K}[y]$. We set $\mathbf{L}=\mathbf{K}[y]/(g(y))$. We find a generator τ of the $(\mathbb{Z}/p\mathbb{Z})$-algebra $\mathbf{L}$. We compute the minimal polynomial $h(u) \in (\mathbb{Z}/p\mathbb{Z})[u]$ of τ. We set $\tilde{\mathbf{L}}=(\mathbb{Z}/p\mathbb{Z})[u]/(h(u))$. We compute and store the matrix of the isomorphism $\kappa : \tilde{\mathbf{L}} \to \mathbf{L}$, and also its inverse.

We pick random elliptic curves over $\tilde{\mathbf{L}}$ and compute their cardinalities until we find one with cardinality divisible by ℓ. Let E be such a curve. Let t be its trace.

We look for a point of order ℓ in $E(\tilde{\mathbf{L}})$. To this end, we pick a random point in $E(\tilde{\mathbf{L}})$ and multiply it by $(Q+1-t)/\ell$. If the result is non-zero we are done. Otherwise we start again.

Once we have found a point of order ℓ in $E(\tilde{\mathbf{L}})$, we compute the associated degree ℓ quotient isogeny $E \to E_1$ using Vélu's formulae in Paragraph 4.1.1.

We iterate the construction above and obtain a chain of δ degree ℓ isogenies

$$E \to E_1 \to \cdots \to E_\delta.$$

We find a generator A of the ℓ-Sylow subgroup of $E_\delta(\tilde{\mathbf{L}})$. We compute the polynomial $f_{\iota,A}(x) \in \tilde{\mathbf{L}}[x]$ associated with the isogeny $\iota : E \to E_\delta$ and the point A. To this end, we use the methods given in Paragraphs 4.1.2 and 4.1.1. This polynomial is irreducible in $\tilde{\mathbf{L}}[x]$.

We use the method in Section 5 to deduce an irreducible polynomial of degree ℓ^δ in $\mathbf{K}[x]$.

7 Appendix

In this section we state several known and useful facts about fields, polynomials and elliptic curves.

7.1 Generator of a subextension

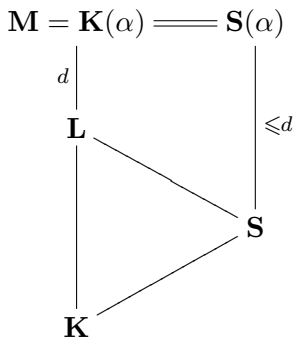
Let $\mathbf{M}$ be a field and let $\mathbf{K}$ be a subfield of $\mathbf{M}$. Assume $\mathbf{M}=\mathbf{K}(\alpha)$ is a monogenous extension of $\mathbf{K}$. Let $\mathbf{L}$ be a subfield of $\mathbf{M}$ containing $\mathbf{K}$. In this section, we use α to construct a generator of $\mathbf{L}$ over $\mathbf{K}$.

The extension $\mathbf{M}/\mathbf{L}$ is assumed to be cyclic of finite degree d. We also assume that there exists a strict subfield $\mathbf{S}$ of $\mathbf{L}$ containing $\mathbf{K}$, such that every strict subfield of $\mathbf{L}$ containing $\mathbf{K}$ is included in $\mathbf{S}$.

Let $(\Sigma_k)_{1\leqslant k\leqslant d}$ be the d symmetric functions of α over $\mathbf{L}$. These are the coefficients of the characteristic polynomial of α, seen as an element in the $\mathbf{L}$-algebra $\mathbf{M}$.

We claim that at least one of these symmetric functions generates $\mathbf{L}$ over $\mathbf{K}$.

Otherwise, all these functions would be contained in $\mathbf{S}$. The field $\mathbf{S}(\alpha)$ would then be a degree $\leqslant d$ algebraic extension of $\mathbf{S}$. But $\mathbf{S}(\alpha)$ contains $\mathbf{K}(\alpha)$ so $\mathbf{S}(\alpha)$ is $\mathbf{M}$. So $\mathbf{M}$ is a finite extension of $\mathbf{S}$; and $\mathbf{L}$ also since $\mathbf{S} \subset \mathbf{L} \subset \mathbf{M}$. But the degree of $\mathbf{M}$ over $\mathbf{L}$ is d; and this is greater than or equal to the degree of $\mathbf{M}$ over $\mathbf{S}$. So $\mathbf{L}=\mathbf{S}$. A contradiction.



We notice that the existence of a unique maximum strict subextension $\mathbf{S}$ of $\mathbf{L}/\mathbf{K}$ is granted if $\mathbf{L}/\mathbf{K}$ is finite, Galois and cyclic of degree a prime power.

We deduce the following lemma.

Lemma 1 (Subfield generated by a symmetric function) *Let $\mathbf{M}$ be a finite field and let $\mathbf{K}$ be a subfield of $\mathbf{M}$. We assume that the degree of $\mathbf{M}$ over $\mathbf{K}$ is a prime power. Let α be a generator of $\mathbf{M}$ over $\mathbf{K}$. Let $\mathbf{L}$ be a subfield of $\mathbf{M}$ containing $\mathbf{K}$. Let d be the degree of $\mathbf{M}$ over $\mathbf{L}$. Let $(\Sigma_k)_{1\leqslant k\leqslant d}$ be the d symmetric functions of α above $\mathbf{L}$. Then at least one among these d symmetric functions generates $\mathbf{L}$ over $\mathbf{K}$.*

7.2 Some kernel isogenies

Let $\mathbf{K}$ be a finite field of characteristic p and cardinality q. Let E be an elliptic curve over $\mathbf{K}$. We denote by $\varphi_E : E \to E$ the degree q Frobenius endomorphism of E. Let t be the trace of φ_E. Let $\mathcal{O}$ be the quotient ring $\mathbb{Z}[X]/(X^2 - tX + q)$ and let α be the class of X in $\mathcal{O}$. Let $\epsilon_E : \mathcal{O} \to \mathrm{End}(E)$ be the ring homomorphism that maps α onto φ_E. We say that ϵ_E is the *standard labeling* of E.

Let S be a subset of $\mathcal{O}$ containing a prime to p integer. We define the *kernel* of S in E to be the intersection of the kernels of all endomorphisms $\epsilon_E(s)$ for $s \in S$. This a finite étale subgroup of E. So it is characterized by its set of geometric points.

Now let F be another elliptic curve over $\mathbf{K}$ and let $\iota : E \to F$ be an isogeny defined over $\mathbf{K}$. Let $\epsilon_F : \mathcal{O} \to \mathrm{End}(F)$ be the morphism of free $\mathbb{Z}$-modules that sends 1 onto the identity and α onto φ_F. For any element s in $\mathcal{O}$ we have

$$\iota \circ \epsilon_E(s) = \epsilon_F(s) \circ \iota. \tag{10}$$

Indeed, the identity above is true for $s = \alpha$ because ι is defined over $\mathbf{K}$. It is evidently true also for $s = 1$. Therefore it is true for all s in $\mathcal{O}$ by linearity.

We deduce from identity (10) that ϵ_F is a ring homomorphism, just as ϵ_E.

Now let G be a third elliptic curve over $\mathbf{K}$. Let $\jmath : F \to G$ be an isogeny defined over $\mathbf{K}$. We define $\epsilon_G : \mathcal{O} \to \mathrm{End}(G)$ as before.

Assume $\iota : E \to F$ is separable with kernel $E[S]$ where S is a subset of $\mathcal{O}$ containing a prime to p integer. Assume $\jmath : F \to G$ is separable with kernel $F[T]$ where T is a subset of $\mathcal{O}$ containing a prime to p integer. Then the kernel of $\jmath \circ \iota$ is $E[ST]$.

$$E \xrightarrow{\iota} F \xrightarrow{\jmath} G.$$

Indeed, both the kernel of $\jmath \circ \iota$ and $E[ST]$ are étale; so they are characterized by their geometric points.

Now let x be a point in the kernel of $\jmath \circ \iota$. Its image $\iota(x)$ by ι lies in the kernel of $\jmath$. Therefore it is killed by T: for any element t of T one has $\epsilon_F(t)(\iota(x)) = 0_F$. So $\iota(\epsilon_E(t)(x)) = 0_F$ and $\epsilon_E(t)(x)$ belongs in the kernel of ι. Thus it is killed by S: for any s in S we have $\epsilon_E(s)(\epsilon_E(t)(x)) = 0_E$ or equivalently $\epsilon_E(st)(x) = 0$. Therefore x lies in $E[ST]$.

Conversely, let x be a point in $E[ST]$. Let t be an element in T. We observe that $\epsilon_E(t)(x)$ is killed by S, so it belongs to the kernel of ι. Thus $\iota(\epsilon_E(t)(x)) = \epsilon_F(t)(\iota(x)) = 0_F$. So $\iota(x)$ is killed by T; therefore it belongs to the kernel of $\jmath$. Thus $\jmath(\iota(x)) = 0_G$.

Following Waterhouse [17] we say that an isogeny $\iota : E \to F$ whose kernel takes the form $E[S]$, is a *kernel isogeny*.

Lemma 2 (Composition of kernel isogenies) *Let $\mathbf{K}$ be a finite field with characteristic p. Let E be an elliptic curve over $\mathbf{K}$. Let t be the trace of the Frobenius endomorphism of E. Let $\mathcal{O}$ be the quotient ring $\mathbb{Z}[X]/(X^2 - tX + q)$ and let $\epsilon_E : \mathcal{O} \to \mathrm{End}(E)$ be the standard labeling. Let S be a subset of $\mathcal{O}$ containing a prime to p integer and let $\iota : E \to F$ be the quotient by $E[S]$ isogeny. Let T be a subset of $\mathcal{O}$ containing a prime to p integer and let $\jmath : F \to G$ be the quotient by $F[T]$ isogeny.*

Then the kernel of $\jmath \circ \iota$ is $E[ST]$.

7.3 The number of irreducible polynomials

Let $\mathbf{K}$ be a finite field with cardinality q and characteristic p. Let $d \geq 2$ be an integer. We are interested in the number of degree d irreducible unitary polynomials in $\mathbf{K}[x]$. We recall and prove a very classical lower bound [11, Ex. 3.26 and 3.27, page 142].

Let Ω be an algebraic closure of $\mathbf{K}$ and let $\mathbf{L}$ be the unique degree d extension of $\mathbf{K}$ inside Ω. Call $\mathcal{G}_d$ the set of generators of the $\mathbf{K}$-algebra $\mathbf{L}$. This is the set of all α in $\mathbf{L}$ such that $\mathbf{K}(\alpha) = \mathbf{L}$. Let $\mathcal{I}_d$ be the set of degree d unitary irreducible polynomials in $\mathbf{K}[x]$. Let $\rho : \mathcal{G}_d \to \mathcal{I}_d$ be the map that to every generator α associates its minimal polynomial. Every polynomial $P(x)$ in $\mathcal{I}_d$ has exactly d preimages by ρ, namely its d roots.

To enumerate the degree d unitary irreducible polynomials, we just count the generators of $\mathbf{L}$ over $\mathbf{K}$. Let α be an element in $\mathbf{L}$. If α does not generate $\mathbf{L}$, then it belongs to a smaller extension of $\mathbf{K}$ inside $\mathbf{L}$. Therefore the complementary set of $\mathcal{G}_d$ in $\mathbf{L}$ is the union of all strict subfields of $\mathbf{L}$ containing $\mathbf{K}$. These subfields are in correspondence with the strict divisors of d. To any such divisor D we associate the unique extension of $\mathbf{K}$ with degree D. It has q^D elements. The set of strict divisors of d is a subset of $\{1, 2, 3, 4, \ldots, \lfloor \frac{d}{2} \rfloor\}$. So the number of elements in $\mathbf{L}$ that do not generate it over $\mathbf{K}$ is upper bounded by

$$q + q^2 + q^3 + q^4 + \cdots + q^{\lfloor \frac{d}{2} \rfloor} = q \frac{q^{\lfloor \frac{d}{2} \rfloor} - 1}{q - 1} \leqslant \frac{q}{q-1}(q^{d/2} - 1).$$

The cardinality of $\mathcal{G}_d$ is thus $\geq q^d - \frac{q}{q-1}(q^{d/2} - 1)$ and the cardinality of $\mathcal{I}_d$ is

$$\geq \frac{q^d}{d} - \frac{q}{d(q-1)}(q^{d/2} - 1).$$

We deduce the following lemma [11, Ex. 3.26 and 3.27, page 142].

Lemma 3 *Let* $\mathbf{K}$ *be a finite field with* q *elements. Let* $d \geq 2$ *be an integer. The density of irreducible polynomials among the degree* d *unitary polynomials is*

$$\geq \frac{1}{d}(1 - \frac{q}{q-1}(q^{-\frac{d}{2}} - q^{-d})).$$

Let $\mathbf{L}$ *be a degree* d *extension of* $\mathbf{K}$. *The density of generators of the* $\mathbf{K}$*-algebra* $\mathbf{L}$ *is* $\geq 1 - \frac{q}{q-1}(q^{-\frac{d}{2}} - q^{-d})$.

If $d \geq 2$ we deduce that the later density is $\geq 1 - \frac{1}{q-1} = \frac{q-2}{q-1}$. So $\geq \frac{1}{2}$ si $q \geq 3$.
If $q = 2$ and $d \geq 4$ then this density is $\geq 1 - 2 \times 2^{-2} = \frac{1}{2}$.
If $q = 2$ and d equals 2 (resp. 3) then this density is $\frac{1}{2}$ (resp. $\frac{3}{4}$).
If $d = 1$ then this density is 1.
We deduce the following lemma.

Lemma 4 (Density of generators) *Let* $\mathbf{K}$ *be a finite field with* q *elements. Let* $d \geq 1$ *be an integer. The density of irreducible polynomials among the degree* d *unitary polynomials is* $\geq \frac{1}{2d}$.

Let $\mathbf{L}$ *be a degree* d *extension of* $\mathbf{K}$. *The density of generators in the* $\mathbf{K}$*-algebra* $\mathbf{L}$ *is* $\geq \frac{1}{2}$.

7.4 Density of elliptic curves with an ℓ-torsion point

Let $\mathbf{K}$ be a finite field with q elements and let ℓ be a prime integer. Lenstra [10] and Howe [7] give estimates for the density of elliptic curves over $\mathbf{K}$ whose number of $\mathbf{K}$-rational points is divisible by ℓ. In this section, we recall what these authors mean by density and we explain why this density fits with the uniform density on Weierstrass curves.

We call $\mathcal{E}(\mathbf{K})$ the set of $\mathbf{K}$-isomorphism classes of elliptic curves over $\mathbf{K}$. The $\mathbf{K}$-isomorphism class of a curve $E/\mathbf{K}$ is denoted $[E]$. One defines a measure on the finite set $\mathcal{E}(\mathbf{K})$ in the following way: the measure of a class $[E]$ is the inverse of the group of $\mathbf{K}$-automorphisms of E. So the measure of a subset S of $\mathcal{E}(\mathbf{K})$

$$\mu_{\mathcal{E}}(S) = \sum_{[E] \in S} \frac{1}{\#\operatorname{Aut}_{\mathbf{K}}(E)}. \tag{11}$$

Lenstra and Howe prove that the measure of the full set $\mathcal{E}(\mathbf{K})$ is q.

Now let $\mathcal{W}(\mathbf{K})$ be the set of Weierstrass elliptic curves over $\mathbf{K}$. We denote by $\mu_{\mathcal{W}}$ the uniform measure on this set: the $\mu_{\mathcal{W}}$-measure of a subset of $\mathcal{W}(\mathbf{K})$ is defined to be its cardinality. This is a very convenient measure. In order to pick a random Weierstrass curve according to this measure, we just choose each coefficient a_1, a_2, a_3, a_4, a_6 at random with the uniform probability in $\mathbf{K}$ and we check that the discriminant is non-zero (if it is zero we start again).

Let $\gamma : \mathcal{W}(\mathbf{K}) \to \mathcal{E}(\mathbf{K})$ be the map that to every curve E associates its isomorphism class $[E]$. This is a surjection : every elliptic curve over $\mathbf{K}$ has a Weierstrass model over $\mathbf{K}$.

Let $\mathbf{A}(\mathbf{K})$ be the group of projective transforms of the form

$$(X : Y : Z) \mapsto (u^2X + rZ : u^3Y + su^2X + tZ : Z)$$

where $u \in \mathbf{K}^*$ and $r, s, t \in \mathbf{K}$. This group acts on the set $\mathcal{W}(\mathbf{K})$ of Weierstrass elliptic curves over $\mathbf{K}$. Two Weierstrass elliptic curves over $\mathbf{K}$ are isomorphic over $\mathbf{K}$ if and only if they lay in the same orbit for the action of $\mathcal{A}(\mathbf{K})$. Further the group of $\mathbf{K}$-automorphisms of a Weierstrass elliptic curve is isomorphic to the stabilizer of E in $\mathbf{A}(\mathbf{K})$.

So the orbit of a Weierstrass curve $E/\mathbf{K}$ under the action of $\mathbf{A}(\mathbf{K})$ is the fiber $\gamma^{-1}([E])$ and the cardinality of this fiber is the quotient

$$\frac{\#\mathbf{A}(\mathbf{K})}{\#\operatorname{Aut}_{\mathbf{K}}(E)}.$$

Therefore if S is a subset of $\mathcal{E}(\mathbf{K})$ and if T is its preimage by γ, then the measures of S and T are proportional

$$\mu_{\mathcal{W}}(T) = \#\mathbf{A}(\mathbf{K}) \times \mu_{\mathcal{E}}(S)$$

where

$$\#\mathbf{A}(\mathbf{K}) = (q-1)q^3.$$

In particular, if we want to pick a random $\mathbf{K}$-isomorphism class of elliptic curve according to the measure $\mu_{\mathcal{E}}$, it suffices to pick a random Weierstrass elliptic curve according to the uniform measure $\mu_{\mathcal{W}}$.

We now can state a special case of the main result in Howe's paper [7].

Theorem 2 (Howe) *Let q be a prime power and let $\mathbf{K}$ a field with q elements. Let $\mathcal{E}(\mathbf{K})$ be the set of $\mathbf{K}$-isomorphism classes of elliptic curves over $\mathbf{K}$. Let $\mu_{\mathcal{E}}$ be the measure on this set defined by Eq. (11). Let ℓ be a prime integer not dividing $q-1$. The isomorphism classes in $\mathcal{E}(\mathbf{K})$ of elliptic curves having a $\mathbf{K}$-rational point of order ℓ form a subset of density*

$$\frac{1}{\ell - 1}$$

plus an error term bounded in absolute value by

$$\frac{4\ell(\ell+1)}{(\ell-1)\sqrt{q}}.$$

We deduce the following corollary.

Corollary 1 (Density of elliptic curves with an ℓ-torsion point) *Let q be a prime power and let $\mathbf{K}$ a field with $\mathbf{K}$ elements. Let $\mathcal{W}(\mathbf{K})$ be the set of Weierstrass elliptic curves over $\mathbf{K}$. Let $\mu_{\mathcal{W}}$ be the uniform measure on this set. Let ℓ be a prime integer not dividing $q-1$. The density of Weierstrass curves having a $\mathbf{K}$-rational point of order ℓ is*

$$\frac{1}{\ell - 1}$$

plus an error term bounded in absolute value by

$$\frac{4\ell(\ell+1)}{(\ell-1)\sqrt{q}}.$$

7.5 Fast composition

The following theorems were recently proven by Umans and Kedlaya [9].

Theorem 3 (Kedlaya and Umans) *There exists a deterministic algorithm that on input a finite field* $\mathbf{K} = (\mathbb{Z}/p\mathbb{Z})[y]/(a(y))$ *with* q *elements and three polynomials* $f(x)$, $g(x)$ *and* $h(x)$ *in* $\mathbf{K}[x]$ *with degrees bounded by* d, *outputs the remainder* $f(g(x)) \bmod h(x)$ *at the expense of* $d^{1+o(1)}(\log q)^{1+o(1)}$ *elementary operations.*

Theorem 4 (Kedlaya and Umans) *There exists a deterministic algorithm that on input a finite field* $\mathbf{K} = (\mathbb{Z}/p\mathbb{Z})[y]/(a(y))$ *with* q *elements, a degree* d *irreducible unitary polynomial* $f(x)$ *in* $\mathbf{K}[x]$, *and a degree* $\leqslant d-1$ *polynomial* $g(x)$ *in* $\mathbf{K}[x]$ *such that the class* γ *of* $g(x)$ *modulo* $f(x)$, *generates the* $\mathbf{K}$ *algebra* $\mathbf{K}[x]/(f(x))$, *outputs the minimal polynomial* $h(x) \in \mathbf{K}[x]$ *of* γ *at the expense of* $d^{1+o(1)}(\log q)^{1+o(1)}$ *elementary operations*[2]

The following corollary of Theorem 3 is particularly useful.

Corollary 2 *There exists a deterministic algorithm that on input a finite field* $\mathbf{K} = (\mathbb{Z}/p\mathbb{Z})[y]/(a(y))$ *with* q *elements and two rational fractions* $F(x)$ *and* $G(x)$ *in* $\mathbf{K}(x)$ *with respective degrees* d_F *and* d_G, *outputs the composition* $F(G(x)) = u(x)/v(x)$ *where* $u(x)$ *and* $v(x)$ *are coprime polynomials, at the expense of* $(d_F d_G)^{1+o(1)}(\log q)^{1+o(1)}$ *elementary operations.*

We first notice that the problem is trivial if one of the two fractions has degree 1. Composing F and G with rational linear fractions we may assume that $F(0) = G(0) = 0$. We compute the Taylor expansions at 0 of either fractions and we compose them using the algorithm in Theorem 3. We recover the numerator $u(x)$ and denominator $v(x)$ of the corresponding fraction using fast extended Euclid algorithm.

References

[1] L. M. Adleman and Jr. H. W. Lenstra. Finding irreducible polynomials over finite fields. *Proc. 18th Symp. on Theory of Comp.*, pages 350–355, 1986.

[2] M. Ben-Or. Probabilistic algorithms in finite fields. *22nd Annual Symposium on Foundations of Computer Science*, 11:394–398, 1981.

[3] A. Bostan, Ph. Flajolet, B. Salvy, and É. Schost. Fast computation of special resultants. *Journal of Symbolic Computation*, 41(1):1–29, January 2006.

[4] A. Bostan, L. González-Vega, H. Perdry, É. Schost. From Newton sums to coefficients: complexity issues in characteristic p. *Proceedings MEGA'05*, 2005.

[5] E. Kaltofen and V. Y. Pan. Parallel solution of Toeplitz and Toeplitz-like linear systems over fields of small positive characteristic. In *PASCO 94. Vol. 5 of Lecture Notes Ser. Comput.* World Sci. Publishing, pp. 225-233.

[6] Jr. H. W. Lenstra and B. de Smit. Standard models for finite fields: the definition. *http://www.math.leidenuniv.nl/∼desmit*, pages 1–4, 2008.

[2] Remember that in this paper, an $o(1)$ arising in the exponent of a quantity x stands for a function of x alone, tending to 0 when x tends to infinity.

[7] E. W. Howe. On the group orders of elliptic curves over finite fields. *Compositio Mathematica*, 85:229–247, 1993.

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

[9] K.S. Kedlaya and C. Umans. Modular composition in any characteristic. *Foundations of Computer Science, FOCS*, 2008.

[10] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Annals of Mathematics*, 126:649–673, 1987.

[11] R. Lidl and Niederreiter H. *Finite Fields*. Addison-Wesley, 1983.

[12] D. Panario and B. Richmond. Analysis of Ben-Or's polynomial irreducibility test. *Random Structures and Algorithms*, 13:439–456, 1998.

[13] A. Schönhage. Fast parallel computation of characteristic polynomials by Leverrier's power sum method adapted to fields of finite characteristic. In *Automata, languages and programming (Lund, 1993)*. Vol. 700 of LNCS. Springer, pp. 410-417.

[14] V. Shoup. Fast construction of irreducible polynomials over finite fields. In *Proceedings of the 4th Annual ACM-SIAM Symposium on Discrete Algorithms, SODA'93 (Austin, Texas, January 25-27, 1993)*, pages 484–492, New York; SIAM: Philadelphia, 1993. ACM.

[15] Ch. Umans. Fast polynomial factorization and modular composition in small characteristic. In Richard E. Ladner and Cynthia Dwork, editors, *STOC, Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008*, pages 481–490. ACM, 2008.

[16] J. Vélu. Isogénies entre courbes elliptiques. *Comptes-Rendus de l'Académie des Sciences, Série I*, 273:238–241, juillet 1971.

[17] W. C. Waterhouse. Abelian varieties over finite fields. *Annales scientifiques de l'École Normale Supérieure, Sér. 4, 2 no. 4 (1969), p. 521-560.*