Galois invariant smoothness basis

Jean-Marc Couveignes, Reynald Lercier

Galois invariant smoothness basis*

Jean-Marc Couveignes† and Reynald Lercier‡

August 18, 2011

Abstract

This text answers a question raised by Joux and the second author about the computation of discrete logarithms in the multiplicative group of finite fields. Given a finite residue field $\mathbf{K}$, one looks for a smoothness basis for $\mathbf{K}^*$ that is left invariant by automorphisms of $\mathbf{K}$. For a broad class of finite fields, we manage to construct models that allow such a smoothness basis. This work aims at accelerating discrete logarithm computations in such fields. We treat the cases of codimension one (the linear sieve) and codimension two (the function field sieve).

To Gilles Lachaud, on the occasion of his 60th birthday

1 Motivation

We look for finite fields that admit Galois invariant smoothness basis. It is known that such basis accelerate the calculation of discrete logarithms. We first recall this observation by Joux and Lercier in section 2 and we give a first example of this situation in section 3. We recall in section 4 the rudiments of Kummer and Artin-Schreier theories. These theories produce the known examples of such smoothness basis. We then show in section 5 that the only extensions admitting Galois invariant flags of linear spaces are given by those two theories. In section 6, we consider a more general setting: specialization of isogenies between algebraic groups. We deduce a first non trivial example of Galois invariant smoothness basis in section 7. In the next section 8, we show that elliptic curves produce a range of such invariant basis, provided the degree of the field is not too large.

In section 9, we recall the principles of fast sieving algorithms (the number field sieve and the function field sieve). We show in section 10 that our approach can be adapted to these algorithms. A detailed example is given in section 11. We finish with a few remarks and questions about the relevance of our method.

*Research supported by the French Délégation Générale pour l'Armement, Centre d'Électronique de l'Armement and by the Fonds National pour la Science (ACI NIM).

†Institut de Mathématiques de Toulouse, Université de Toulouse et CNRS.

‡Centre d'Électronique de l'Armement, 35170 Bruz, France.

2 A remark by Joux and Lercier

We recall in this section the principle of a simple algorithm for computing discrete logarithms in the multiplicative group of a finite field $\mathbb{F}_q$ where $q = p^d$ and $d \geq 2$. See [7] for a survey on discrete logarithm computation.

The finite field $\mathbb{F}_q$ is seen as a residue field $\mathbb{F}_p[X]/(A(X))$ where $A(X) \in \mathbb{F}_p[X]$ is a degree d unitary irreducible polynomial. We set $x = X \bmod A(X)$. Let k be an integer such that $0 \leq k \leq d-1$ and let $V_k \subset \mathbb{F}_q$ be the $\mathbb{F}_p$-vector space generated by $1, x, \ldots, x^k$. So $V_0 = \mathbb{F}_p \subset V_1 \subset \ldots \subset V_{d-1} = \mathbb{F}_q$ and $V_k \times V_l \subset V_{k+l}$ if $k + l \leq d-1$.

One looks for multiplicative relations between elements of V_κ for some integer κ. For example, if one takes $\kappa = 1$, the relations we are looking for take the form

$$\prod_i (a_i + b_i x)^{e_i} = 1 \in \mathbb{F}_q \tag{1}$$

where the a_i and b_i lie in $\mathbb{F}_p$. We collect such relations until we obtain a basis of the $\mathbb{Z}$-module of relations between elements in V_κ.

How do we find relations like relation (1) ? Assume again $\kappa = 1$. The simplest form of the sieving algorithm picks random triplets (a_i, b_i, e_i) and computes the remainder $r(X)$ of the Euclidean division of $\prod_i (a_i + b_i X)^{e_i}$ by $A(X)$. So

$$r(X) \equiv \prod_i (a_i + b_i X)^{e_i} \bmod A(X)$$

where $r(X)$ is a more or less random polynomial in $\mathbb{F}_p[X]$ with degree $\leq d-1$.

We hope $r(X)$ decomposes as a product of polynomials with degree smaller than or equal to $\kappa = 1$. If this is the case, we find $r(X) = \prod_j (a'_j + b'_j X)^{e'_j}$ and we obtain a relation

$$\prod_i (a_i + b_i x)^{e_i} \prod_j (a'_j + b'_j x)^{-e'_j} = 1$$

of the expected form. One says that V_κ is the smoothness basis.

Joux and Lercier notice in [3] that, if there exists an automorphism $\mathfrak{a}$ of $\mathbb{F}_q$ such that $\mathfrak{a}(x) = ux + v$ with $u, v \in \mathbb{F}_p$, then the action of $\mathfrak{a}$ on equation (1) produces another equation of the same kind. Since the efficiency of discrete logarithm algorithms depends on the number of such equations one can produce in a given amount of time, one wishes to know when such useful automorphisms exist. We also wonder how to generalize this observation.

We stress that $\mathfrak{a}$ acts both on equations and factors of the form $a_i + b_i x$. Rather than increasing the number of equations, such an action may be used to lower the number of factors involved in them. If $\mathfrak{a}$ is the n-th power of the Frobenius automorphism, we obtain for free

$$\mathfrak{a}(a + bx) = (a + bx)^{p^n} = v + a + ubx$$

So we can remove $v + a + ubx$ out of the smoothness basis and replace it everywhere by $(a + bx)^{p^n}$. This way, we only keep one element in every orbit of the Galois group acting on V_κ. As a

consequence, the size of the linear system we must solve is divided by the order of the group generated by $\mathfrak{a}$. If $\mathfrak{a}$ generates the full Galois group of $\mathbb{F}_q/\mathbb{F}_p$, then the number of unknowns is divided by d, the degree of the finite field $\mathbb{F}_q$.

Our concern in this text is to find models for finite fields for which the automorphisms respect the special form of certain elements. For example, if the finite field is given as above, the elements are given as polynomials in x. Any element z of the finite field has a degree: This is the smallest integer k such that $z \in V_k$. The degree of $a_0 + a_1 x + \cdots + a_k x^k$ is thus k provided $0 \leq k < d$ and $a_k \neq 0$ (and by convention, $\deg 0 = 0$). The degree is sub-additive, $\deg(w \times z) \leq \deg(w) + \deg(z)$.

The question raised boils down to asking if this degree function is preserved by the automorphisms of $\mathbb{F}_q$. It is worth noticing that the interest of the degree function in this context comes from the following properties.

- The degree is sub-additive (and often even additive): The degree of the product of two non zero elements is the sum of the degrees of either elements provided this sum is $< d$.
- The degree sorts nicely the elements of $\mathbb{F}_q$: There are q^n elements of degree $< n$ if $1 \leq n \leq d$.
- There exists a factoring algorithm that decomposes some elements in $\mathbb{F}_q$ as products of elements with smaller degrees (*e.g.* with degree $\leq \kappa$). The density of such κ-smooth elements is not too small.

In this article, we look for such degree functions on finite fields having the extra property that they are Galois invariant: Two conjugate elements have the same degree.

3 A first example

Here is an example provided by Joux and Lercier. Take $p = 43$ and $d = 6$, so $q = 43^6$, and set $A(X) = X^6 - 3$ which is an irreducible polynomial in $\mathbb{F}_{43}[X]$. So $\mathbb{F}_q$ is seen as the residue field $\mathbb{F}_{43}[X]/(X^6 - 3)$.

One checks that $p = 43$ is congruent to 1 modulo $d = 6$, so $\phi(x) = x^{43} = (x^6)^7 \times x = 3^7 x = \zeta_6 x$ where $\zeta_6 = 3^7 = 37 \bmod 43$ is a primitive sixth root of unity. Since the Frobenius ϕ generates the Galois group, one can divide by 6 the size of the smoothness basis.

In the second example provided by Joux and Lercier (and coming from XTR of type T30) one takes $p = 370801$ and $d = 30$ with $A(X) = X^{30} - 17$. This time, p is congruent to 1 modulo $d = 30$ and $\phi(x) = x^p = x^{30 \times 12360} \times x = \zeta_{30} x$ where $\zeta_{30} = 17^{12360} \bmod p = 172960 \bmod p$. As a consequence, one can divide by 30 the size of the smoothness basis.

We are here in the context of Kummer theory. In the next section we recall the basics of this theory, that classifies cyclic extensions of $\mathbb{F}_p$ with degree d dividing $p - 1$. Artin-Schreier theory is the counterpart for cyclic p-extensions in characteristic p and we sketch it as well. Both theories are of very limited interest for our purpose. We shall need to consider the more general situation of an algebraic group with rational torsion.

4 Kummer and Artin-Schreier theories

The purpose here is to classify cyclic extensions of degree $d \geq 2$ of a field $\mathbf{K}$ with characteristic p in two simple cases.

- Kummer case: p is prime to d and $\mathbf{K}$ contains a primitive d-th root of unity;
- Artin-Schreier case: $d = p$.

Kummer theory. We follow Bourbaki [1, A V.84]. According to Kummer theory, if p is prime to d and $\mathbf{K}$ contains a primitive d-th root of unity, then every degree d cyclic extension of $\mathbf{K}$ is generated by a radical.

Assume $\mathbf{K}$ is embedded in some algebraic closure $\bar{\mathbf{K}}$. To every a in $\mathbf{K}^*/(\mathbf{K}^*)^d$ (which we may regard as an element in $\mathbf{K}^*$), we associate the field $\mathbf{L} = \mathbf{K}(a^{\frac{1}{d}})$ where $a^{\frac{1}{d}}$ is any root of $X^d - a$ in $\bar{\mathbf{K}}$.

The map $x \mapsto x^d$ is an epimorphism from the multiplicative group $\bar{\mathbf{K}}^*$ onto itself. The kernel of this epimorphism is the group of d-th roots of unity. The roots of $X^d - a$ lie in the inverse image of d by this epimorphism.

The field $\mathbf{K}(a^{\frac{1}{d}})$ may not be isomorphic to $\mathbf{K}[X]/(X^d - a)$. It is when a has order d in the group $\mathbf{K}^*/(\mathbf{K}^*)^d$. On the other hand, if a lies in $(\mathbf{K}^*)^d$ then $\mathbf{K}[X]/(X^d - a)$ is the product of d copies of $\mathbf{K}$.

Let's come back to the case when a has order d in $\mathbf{K}^*/(\mathbf{K}^*)^d$. The degree d extension $\mathbf{L}/\mathbf{K}$ is Galois since, if we set $b = a^{\frac{1}{d}}$, we have

$$X^d - a = (X - b)(X - b\zeta_d)(X - b\zeta_d^2)\dots(X - b\zeta_d^{d-1})$$

where ζ_d is a primitive d-th root of unity. The Galois group of $\mathbf{L}/\mathbf{K}$ is made of transformations $\mathfrak{a}_n : x \mapsto x\zeta_d^n$ and the map $n \mapsto \mathfrak{a}_n$ is an isomorphism from the group $\mathbb{Z}/d\mathbb{Z}$ onto $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$.

To avoid distinguishing too many cases, one follows Bourbaki [1, A V.84]. Rather than a single element in $\mathbf{K}^*/(\mathbf{K}^*)^d$ one picks a subgroup H of $\mathbf{K}^*$ containing $(\mathbf{K}^*)^d$ and one forms the extension $\mathbf{K}(H^{\frac{1}{d}})$ by adding to $\mathbf{K}$ all d-th roots of all elements in H. To every automorphism $\mathfrak{a}$ in $\mathrm{Gal}(\mathbf{K}(H^{\frac{1}{d}})/\mathbf{K})$, one associates an homomorphism $\psi(\mathfrak{a})$ from $H/(\mathbf{K}^*)^d$ to the group $\mu_d(\mathbf{K})$ of d-th roots of unity. The homomorphism $\psi(\mathfrak{a})$ is defined by

$$\psi(\mathfrak{a}) : \theta \mapsto \frac{\mathfrak{a}(\theta^{\frac{1}{d}})}{\theta^{\frac{1}{d}}}$$

where $\theta^{\frac{1}{d}}$ is one of the d-th roots of θ. The map $\mathfrak{a} \mapsto \psi(\mathfrak{a})$ is an isomorphism from the $\mathrm{Gal}(\mathbf{K}(H^{\frac{1}{d}})/\mathbf{K})$ onto $\mathrm{Hom}(H/(\mathbf{K}^*)^d, \mu_d(\mathbf{K}))$. This presentation of Kummer theory constructs abelian extensions of $\mathbf{K}$ with exponent dividing d.

In the case we are interested in, the field $\mathbf{K} = \mathbb{F}_q$ is finite. Any subgroup H of $\mathbf{K}^*$ is cyclic. In order to have μ_d in $\mathbf{K}$, one assumes that d divides $q-1$. We set $q - 1 = md$. The group $(\mathbf{K}^*)^d$ has order m. The quotient $\mathbf{K}^*/(\mathbf{K}^*)^d$ is cyclic of order d. It is natural to take $H = \mathbf{K}^*$. We find

the unique degree d cyclic extension $\mathbf{L}$ of $\mathbf{K}$. It is generated by a d-th root of a generator a of $\mathbf{K}^*$.

Set $b = a^{\frac{1}{d}}$ and $\mathbf{L} = \mathbf{K}(b)$. The Galois group $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$ is generated by the Frobenius ϕ and the action of ϕ on b is given by $\phi(b) = b^q$, so

$$\zeta = \frac{\phi(b)}{b} = b^{q-1} = a^m$$

is a d-th root of unity that depends on a. The map $a \mapsto \zeta$ is an isomorphism of $\mathbf{K}^*/(\mathbf{K}^*)^d$ onto $\mu_d(\mathbf{K})$ which is nothing but exponentiation by m.

The limitations of this construction are clear: It requires primitive d-th roots of unity in $\mathbf{K}$. Otherwise, one may jump to some auxiliary extension $\mathbf{K}' = \mathbf{K}(\zeta_d)$ of $\mathbf{K}$, that may be quite large. One applies Kummer theory to this bigger extension and one obtains a degree d cyclic extension $\mathbf{L}'/\mathbf{K}'$. Descent can be performed using resolvants (see [6, Chapter III.4]) at a serious computational expense. We shall not follow this track.

Example. Coming back to the first example one finds $q = p = 43$, $p - 1 = 42$, $d = 6$, $m = 7$, $a = 3$ and $\phi(b)/b = a^m = 3^7 \bmod 43$.

Artin-Schreier theory. We follow Bourbaki [1, A V.88]. If p is the characteristic of $\mathbf{K}$, then any cyclic degree p extension of $\mathbf{K}$ is generated by the roots of a polynomial of the form

$$X^p - X - a = \wp(X) - a = 0$$

where $a \in \mathbf{K}$ and the expression $\wp(X) = X^p - X$ plays a similar role to X^d in Kummer theory. The map $x \mapsto \wp(x)$ defines an epimorphism from the additive group $\bar{\mathbf{K}}$ onto itself. The kernel of this epimorphism is the additive group of the prime field $\mathbb{F}_p \subset \bar{\mathbf{K}}$.

Let a be an element of $\mathbf{K}/\wp(\mathbf{K})$ (that we may see as an element of $\mathbf{K}$ in this class). One associates to it the extension field $\mathbf{L} = \mathbf{K}(b)$ where $b \in \wp^{-1}(a)$. If a has order p in $\mathbf{K}/\wp(\mathbf{K})$, the extension $\mathbf{L}/\mathbf{K}$ has degree p and is Galois since we have

$$X^p - X - a = (X - b)(X - b - 1)(X - b - 2)\dots(X - b - (p - 1)).$$

The Galois group is made of transformations of the form $\mathfrak{a}_n : x \mapsto x + n$ and the map $n \mapsto \mathfrak{a}_n$ is an isomorphism from the group $\mathbb{Z}/p\mathbb{Z}$ onto $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$.

Again, if one wishes to construct all abelian extensions of $\mathbf{K}$ with exponent p one follows Bourbaki [1, A V.88]. One takes a subgroup H of $(\mathbf{K}, +)$ containing $\wp(\mathbf{K})$ and one forms the extension $\mathbf{K}(\wp^{-1}(H))$. To every automorphism $\mathfrak{a}$ in $\mathrm{Gal}(\mathbf{K}(\wp^{-1}(H))/\mathbf{K})$, one associates an homomorphism $\psi(\mathfrak{a})$ from $H/\wp(\mathbf{K})$ onto the additive group $\mathbb{F}_p$ of the prime field. The homomorphism $\psi(\mathfrak{a})$ is defined by

$$\psi(\mathfrak{a}) : \theta \mapsto \mathfrak{a}(c) - c$$

where c belongs to $\wp^{-1}(\theta)$, the fiber of $\wp$ above θ.

The map $\mathfrak{a} \mapsto \psi(\mathfrak{a})$ is an isomorphism from the Galois group $\mathrm{Gal}(\mathbf{K}(\wp^{-1}(H))/\mathbf{K})$ onto $\mathrm{Hom}(H/\wp(\mathbf{K}), \mathbb{F}_p)$.

In our case, the field $\mathbf{K} = \mathbb{F}_q$ is finite of characteristic p. We set $q = p^f$. The morphism $\wp : \mathbb{F}_q \to \mathbb{F}_q$ has kernel $\mathbb{F}_p$ and the quotient $\mathbb{F}_q/\wp(\mathbb{F}_q)$ has order p. The unique degree p extension $\mathbf{L}$ of $\mathbb{F}_q$ is generated by $b \in \wp^{-1}(a)$ where $a \in \mathbb{F}_q - \wp(\mathbb{F}_q)$. The Galois group $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$ is generated by the Frobenius ϕ and $\phi(b) - b$ belongs to $\mathbb{F}_p$. The map $a \mapsto \phi(b) - b$ is an isomorphism from $\mathbf{K}/\wp(\mathbf{K})$ onto $\mathbb{F}_p$.

Let us make this isomorphism more explicit. We have $\phi(b) = b^q$ where $q = p^f$ is the order of $\mathbf{K} = \mathbb{F}_q$. One computes

$$\phi(b) - b = b^q - b = (b^p)^{p^{f-1}} - b = (b + a)^{p^{f-1}} - b \text{ since } \wp(b) = b^p - b = a.$$

So $b^{p^f} - b = b^{p^{f-1}} - b + a^{p^{f-1}}$. Iterating, we obtain

$$\phi(b) - b = b^{p^f} - b = a + a^p + a^{p^2} + \cdots + a^{p^{f-1}}.$$

The isomorphism from $\mathbf{K}/\wp(\mathbf{K})$ onto the additive group $\mathbb{F}_p$ is nothing but the absolute trace.

Example. Take $p = 7$ and $f = 1$, so $q = 7$. The absolute trace of 1 is 1, so we set $\mathbf{K} = \mathbb{F}_7$ and $A(X) = X^7 - X - 1$ and we set $\mathbf{L} = \mathbb{F}_{7^7} = \mathbb{F}_7[X]/(A(X))$. Setting $x = X \bmod A(X)$, one has $\phi(x) = x + 1$.

5 Invariant linear spaces of a cyclic extension

Let us recall that the question raised in section 2 concerns the existence of automorphisms that stabilize a given smoothness basis. We saw that smoothness basis are usually made using flags of linear spaces. Therefore, one wonders if, for a given cyclic extension $\mathbf{L}/\mathbf{K}$, there exists $\mathbf{K}$-vector subspaces of $\mathbf{L}$ that are left invariant by the Galois group of $\mathbf{L}/\mathbf{K}$.

Let $d \geq 2$ be an integer and $\mathbf{L} = \mathbf{K}[X]/(X^d - r)$ a Kummer extension. For any integer k between 0 and $d - 1$, let $L_k = \mathbf{K} \oplus \mathbf{K}x \oplus \cdots \oplus \mathbf{K}x^k$ be the $\mathbf{K}$-vector subspace generated by the $k + 1$ first powers of $x = X \bmod X^d - r$. The L_k are invariant under Galois action since for $\mathfrak{a}$, a $\mathbf{K}$-automorphism of $\mathbf{L}$, there exists a d-th root of unity $\zeta \in \mathbf{K}$ such that

$$\mathfrak{a}(x) = \zeta x$$

and $\mathfrak{a}(x^k) = \zeta^k x^k$. One has a flag of $\mathbf{K}$-vector spaces, $V_0 = \mathbf{K} \subset V_1 \subset \cdots \subset V_{d-1} = \mathbf{L}$, respected by Galois action. So the "degree" function is invariant under this action. This is exactly what happens in the two examples of section 2. If the smoothness basis is made of irreducible polynomials of degree $\leq \kappa$, then it is acted on by the Galois group.

If now $\mathbf{L} = \mathbf{K}[X]/(X^p - X - a)$ is an Artin-Schreier extension, for every integer k between 0 and $p - 1$, we call $V_k = \mathbf{K} \oplus \mathbf{K}x \oplus \cdots \oplus \mathbf{K}x^k$ the $\mathbf{K}$-vector space generated by the $k + 1$ first powers of $x = X \bmod X^p - X - a$. The V_k are globally invariant under Galois action. Indeed, if $\mathfrak{a}$ is a $\mathbf{K}$-automorphism of $\mathbf{L}$, then there is a $n \in \mathbb{F}_p$ such that $\mathfrak{a}(x) = x + n$, so

$$\mathfrak{a}(x^k) = (x + n)^k = \sum_{0 \leq \ell \leq k} \binom{k}{\ell} n^{k-\ell} x^\ell.$$

We find again a flag of $\mathbf{K}$-vector spaces, $V_0 = \mathbf{K} \subset V_1 \subset \cdots \subset V_{p-1} = \mathbf{L}$, that is fixed by Galois action. This time, the Galois action is no longer diagonal but triangular. For cyclic extensions of degree a power of p, Witt-Artin-Schreier theory also produces a flag of Galois invariant vector spaces. See the beginning of Lara Thomas's thesis [8] for an introduction with references.

One may wonder if Galois invariant flags of vector spaces exist for other cyclic field extensions. Assume $\mathbf{L}/\mathbf{K}$ is a degree d cyclic extension where d is prime to the characteristic p. Let ϕ be a generator of the Galois group $C =< \phi >= \mathrm{Gal}(\mathbf{L}/\mathbf{K})$. According to the normal basis theorem [4, Theorem 13.1.], there exists a w in $\mathbf{L}$ such that

$$(w, \phi(w), \phi^2(w), \ldots, \phi^{d-1}(w))$$

is a $\mathbf{K}$-basis of $\mathbf{L}$. Therefore $\mathbf{L}$, as a $\mathbf{K}[C]$-module, is isomorphic to the regular representation. The order d of C being prime to the characteristic, the ring $\mathbf{K}[C]$ is semi-simple according to Maschke theorem [4, Theorem 1.2.]. The characteristic polynomial of ϕ acting on the $\mathbf{K}$-vector space $\mathbf{L}$ is $X^d - 1$. This is a separable polynomial in $\mathbf{K}[X]$.

To every $\mathbf{K}$-irreducible factor $f(X) \in \mathbf{K}[X]$ of $X^n - 1$, there corresponds a unique irreducible characteristic subspace $V_f \subset \mathbf{L}$, invariant by ϕ. The characteristic polynomial of ϕ restricted to V_f is f. According to Schur's lemma [4, Proposition 1.1.], any $\mathbf{K}[C]$-submodule of $\mathbf{L}$ is a direct sum of some V_f.

Assume there exists a complete flag of $\mathbf{K}$-vector spaces, each invariant by ϕ, $V_0 = \mathbf{K} \subset V_1 \subset \cdots \subset V_{d-1} = \mathbf{L}$, where V_k has dimension k. Then all irreducible factors of $X^d - 1$ must have degree 1. So $\mathbf{K}$ contains primitive roots of unity and we are in the context of Kummer theory. To every Galois invariant flag, there corresponds an order on d-th roots of unity (or equivalently on the associated characteristic spaces in $\mathbf{L}$). There are $d!$ such flags.

The flags produced by Kummer theory are of the following form:

$$V_1 \subset V_1 \oplus V_\zeta \subset V_1 \oplus V_\zeta \oplus V_{\zeta^2} \subset \ldots \\ \subset V_1 \oplus V_\zeta \oplus V_{\zeta^2} \oplus \cdots \oplus V_{\zeta^{d-2}} \subset V_1 \oplus V_\zeta \oplus V_{\zeta^2} \oplus \cdots \oplus V_{\zeta^{d-2}} \oplus V_{\zeta^{d-1}}$$

where ζ is a primitive d-th root of unity and V_ζ is $V_{X-\zeta}$, the eigenspace associated to ζ.

Among the $d!$ flags that are ϕ-invariants, only $\varphi(d)$ come from Kummer theory. They correspond to the $\varphi(d)$ primitive roots of unity. These flags enjoy a multiplicative property: If $k \geq 0$ and $l \geq 0$ and $k + l \leq d - 1$, then $V_k \times V_l \subset V_{k+l}$.

The conclusion of this section is thus rather negative. If we want to go further than Kummer theory, we cannot ask for Galois invariant flags of vector subspaces.

6 Specializing isogenies between commutative algebraic groups

Kummer and Artin-Schreier theories are two special cases of a general situation that we now describe. Our aim is to produce nice models for a broader variety of finite fields.

Let $\mathbf{K}$ be a field and $\mathbf{G}$ a commutative algebraic group over $\mathbf{K}$. Let $T \subset \mathbf{G}(\mathbf{K})$ be a non trivial finite group of $\mathbf{K}$-rational points in $\mathbf{G}$ and let

$$I : \mathbf{G} \to \mathbf{H}$$

be the quotient isogeny of $\mathbf{G}$ by T. Let $d \geq 2$ be the cardinality of T which is also the degree of I. Assume there exists a $\mathbf{K}$-rational point a on $\mathbf{H}$ such that $I^{-1}(a)$ is irreducible over $\mathbf{K}$. Then every point $b \in \mathbf{G}(\bar{\mathbf{K}})$ such that $I(b) = a$ defines a cyclic degree d extension $\mathbf{L}$ of $\mathbf{K}$: We set $\mathbf{L} = \mathbf{K}(b)$ and we notice that the geometric origin of this extension results in a nice description of $\mathbf{K}$-automorphisms of $\mathbf{L}$.

Let t be a point in T and let $\oplus_{\mathbf{G}}$ stand for the addition law in the algebraic group $\mathbf{G}$. Let $\oplus_{\mathbf{H}}$ stand for the addition law in $\mathbf{H}$. We denote by $0_{\mathbf{G}}$ the unit element in $\mathbf{G}$ and $0_{\mathbf{H}}$ the one in $\mathbf{H}$. The point $t \oplus_{\mathbf{G}} b$ verifies

$$I(t \oplus_{\mathbf{G}} b) = I(t) \oplus_{\mathbf{H}} I(b) = 0_{\mathbf{H}} \oplus_{\mathbf{H}} a = a.$$

So $t \oplus_{\mathbf{G}} b$ is Galois conjugated to b and all conjugates are obtained that way from all points t in T. So we have an isomorphism between T and $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$, which associates to every $t \in T$ the residual automorphism

$$b \in I^{-1}(a) \mapsto b \oplus_{\mathbf{G}} t.$$

Now, assuming the geometric formulae that describe the translation $P \mapsto P \oplus_{\mathbf{G}} t$ in $\mathbf{G}$ are simple enough, we obtain a nice description of the Galois group of $\mathbf{L}$ over $\mathbf{K}$.

Kummer and Artin-Schreier theories provide two illustrations of this general geometric situation.

The algebraic group underlying Kummer theory is the multiplicative group $\mathbf{G}_m$ over the base field $\mathbf{K}$. The isogeny I is the multiplication by d:

$$I = [d] : \mathbf{G}_m \to \mathbf{G}_m.$$

One can see the group $\mathbf{G}_m$ as a sub-variety of the affine line $\mathbb{A}^1$ with z-coordinate. The inequality $z \neq 0$ defines the open subset $\mathbf{G} \subset \mathbb{A}^1$. The origin $0_{\mathbf{G}}$ has coordinate $z(0_{\mathbf{G}}) = 1$. The group law is given by

$$z(P_1 \oplus_{\mathbf{G}_m} P_2) = z(P_1) \times z(P_2).$$

Here we have $\mathbf{H} = \mathbf{G} = \mathbf{G}_m$ and the isogeny I can be given in terms of the z-coordinates by

$$z(I(P)) = z(P)^d.$$

Points in the kernel of I have for z-coordinates the d-th roots of unity. The inverse image by I of a point P in $\mathbf{G}$ is made of d geometric points having for z-coordinates the d-th roots of $z(P)$. Translation by an element t of the kernel of I, $P \mapsto P \oplus_{\mathbf{G}_m} t$, can be expressed in terms of z-coordinates by

$$z(P \oplus_{\mathbf{G}_m} t) = z(P) \times \zeta$$

where $\zeta = z(t)$ is the d-th root of unity associated by z to the d-torsion point t.

As far as Artin-Schreier theory is concerned, the underlying algebraic group is the additive group $\mathbf{G}_a$ over the base field $\mathbf{K}$, identified with the affine line $\mathbb{A}^1$ over $\mathbf{K}$. A point P on $\mathbf{G}_a$ is given by its z-coordinate. The origin $0_{\mathbf{G}}$ has coordinate $z(0_{\mathbf{G}}) = 0$ and the group law is given by

$$z(P_1 \oplus_{\mathbf{G}_a} P_2) = z(P_1) + z(P_2).$$

The degree p isogeny I is $\wp : \mathbf{G}_a \to \mathbf{G}_a$, given in terms of z-coordinates by

$$z(\wp(P)) = z(P)^p - z(P).$$

Here again $\mathbf{H} = \mathbf{G}$. The z-coordinates of points in the kernel of $\wp$ are the elements of the prime field $\mathbb{F}_p$. The inverse image by I of a point P in $\mathbf{G}$ is made of p geometric points whose z-coordinates are the p roots of the equation $X^p - X = z(P)$. Translation by an element t in the kernel of I, $P \mapsto P \oplus_{\mathbf{G}_a} t$, can be expressed in terms of z-coordinates by

$$z(P \oplus_{\mathbf{G}_a} t) = z(P) + \tau \text{ where } \tau = z(t) \in \mathbb{F}_p \ .$$

7 A different example

We plan to apply the generalities in the previous section to various algebraic groups. We guess every commutative algebraic group may bring its contribution to the construction of Galois invariant smoothness basis. Since we look for simple translation formulae, we expect the simplest algebraic groups to be the most useful. We start with the most familiar algebraic groups (after $\mathbf{G}_m$ and $\mathbf{G}_a$): These are the dimension 1 tori. Let $\mathbf{K}$ be a field with characteristic different from 2 and let D be a non zero element in $\mathbf{K}$. Let $\mathbb{P}^1$ be the projective line with projective coordinates $[U, V]$. Let $u = \frac{U}{V}$ be the associated affine coordinate. We denote by $\mathbf{G}$ the open subset of $\mathbb{P}^1$ defined by the inequality

$$U^2 - DV^2 \neq 0.$$

To every point P of $\mathbf{G}$, we associate its u-coordinate, possibly infinite but distinct from $\sqrt{D}$ and $-\sqrt{D}$. The unit element in $\mathbf{G}$ is the point $0_{\mathbf{G}}$ with projective coordinates $[1, 0]$ and u-coordinate ∞. For $P_1 \neq 0_{\mathbf{G}}$ and $P_2 \neq 0_{\mathbf{G}}$, the addition law is given by

$$u(P_1 \oplus_{\mathbf{G}} P_2) = \frac{u(P_1)u(P_2) + D}{u(P_1) + u(P_2)} \text{ and } u(\ominus_{\mathbf{G}} P_1) = -u(P_1).$$

We now assume that $\mathbf{K} = \mathbb{F}_q$ is a finite field and $D \in \mathbb{F}_q^*$ is not a square in $\mathbb{F}_q$. The group $\mathbf{G}(\mathbb{F}_q)$ has order $q + 1$ and the corresponding values of u lie in $\mathbb{F}_q \cup \{\infty\}$. The Frobenius endomorphism, $\phi : \mathbf{G} \to \mathbf{G}$, $[U, V] \to [U^q, V^q]$, is nothing but multiplication by $-q$. Indeed, let P be a point with projective coordinates $[U, V]$. The projective coordinates of $R = [q]P$ are the coordinates in $(1, \sqrt{D})$ of

$$(U + V\sqrt{D})^q = U^q - \sqrt{D}V^q$$

because D is not a square in $\mathbb{F}_q$. So R has coordinates $[U^q, -V^q]$ and it is the inverse of $\phi(P)$.

We pick an integer $d \geq 2$ such that the d-torsion $\mathbf{G}[d]$ is $\mathbb{F}_q$-rational. This is equivalent to the condition that d divides $q+1$. We set $q+1 = md$. Let I be the multiplication by d isogeny, $I = [d] : \mathbf{G} \to \mathbf{G}$, with kernel the cyclic group $\mathbf{G}[d]$ of order d. The quotient $\mathbf{G}(\mathbb{F}_q)/I(\mathbf{G}(\mathbb{F}_q)) = \mathbf{G}(\mathbb{F}_q)/\mathbf{G}(\mathbb{F}_q)^d$ is cyclic of order d.

Let a be a generator of $\mathbf{G}(\mathbb{F}_q)$ and b a geometric point in the fiber of I above a. Let $u(b)$ be the u-coordinate of b and set $\mathbf{L} = \mathbf{K}(u(b))$. This is a degree d extension of $\mathbf{K} = \mathbb{F}_q$. So $\mathbf{L} = \mathbb{F}_{q^d}$.

The Galois group of $\mathbb{F}_{q^d}/\mathbb{F}_q$ is isomorphic to $\mathbf{G}[d]$: For any $\mathfrak{a} \in \mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$, the difference $\mathfrak{a}(b) \ominus_{\mathbf{G}} b$ is in $\mathbf{G}[d]$ and the pairing

$$(\mathfrak{a}, a) \mapsto \mathfrak{a}(b) \ominus_{\mathbf{G}} b$$

defines an isomorphism of $\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ onto $\mathrm{Hom}(\mathbf{G}(\mathbb{F}_q)/(\mathbf{G}(\mathbb{F}_q))^d, \mathbf{G}[d])$.

Here $\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ is cyclic of order d generated by the Frobenius ϕ. The pairing (ϕ, a) equals $\phi(b) \ominus_{\mathbf{G}} b$. Remember that $\phi(b) = [-q]b$ in $\mathbf{G}$. So

$$(\phi, a) = [-q-1]b = [-m]a. \tag{2}$$

We obtain an exact description of Galois action on $I^{-1}(a)$. It is given by translations of the form $P \mapsto P \oplus_{\mathbf{G}} t$ with $t \in \mathbf{G}[d]$. If we denote by τ the affine coordinate of t and by u the coordinate of P then the action is given by

$$u \mapsto \frac{\tau u + D}{u + \tau},$$

which is rather nice since it is a rational linear transform.

We form the polynomial

$$A(X) = \prod_{b \in I^{-1}(a)} (X - u(b))$$

annihilating the u-coordinates of points in the inverse image of a by I. This is a degree d polynomial with coefficients in $\mathbf{K} = \mathbb{F}_q$. It is irreducible in $\mathbb{F}_q[X]$ because a generates $\mathbf{G}(\mathbb{F}_q)$. We have $\mathbf{L} = \mathbf{K}[X]/(A(X)) = \mathbb{F}_{q^d}$.

The exponentiation formulae in $\mathbf{G}$ give the explicit form of $A(X)$. One has

$$(U + \sqrt{D}V)^d = \sum_{0 \leq 2k \leq d} \binom{d}{2k} U^{d-2k} V^{2k} D^k + \sqrt{D} \sum_{1 \leq 2k+1 \leq d} \binom{d}{2k+1} U^{d-2k-1} V^{2k+1} D^k.$$

So,

$$u([d]P) = \frac{\sum_{0 \leq 2k \leq d} u(P)^{d-2k} \binom{d}{2k} D^k}{\sum_{1 \leq 2k+1 \leq d} u(P)^{d-2k-1} \binom{d}{2k+1} D^k}.$$

And

$$A(X) = \sum_{0 \leq 2k \leq d} X^{d-2k} \binom{d}{2k} D^k - u(a) \sum_{1 \leq 2k+1 \leq d} X^{d-2k-1} \binom{d}{2k+1} D^k.$$

We set $x = X \bmod A(X)$. Since every $\mathbb{F}_q$-automorphism of $\mathbb{F}_{q^d}$ transforms x into a linear rational fraction of x, it is natural to define for every integer k such that $k \geq 0$ and $k < d$ the subset

$$V_k = \{\frac{u_0 + u_1 x + u_2 x^2 + \cdots + u_k x^k}{v_0 + v_1 x + v_2 x^2 + \cdots + v_k x^k} \mid (u_0, u_1, \ldots, u_k, v_0, v_1, \ldots, v_k) \in \mathbf{K}^{2k+2}\} .$$

One has $\mathbb{F}_q = V_0 \subset V_1 \subset \cdots \subset V_{d-1} = \mathbb{F}_{q^d}$ and the V_k are Galois invariant. Further, it is clear that $V_k \times V_l \subset V_{k+l}$ provided $k+l \leq d-1$. Again we find a flag of Galois invariant subsets of $\mathbf{L} = \mathbb{F}_{q^d}$. But these subsets are no longer vector spaces.

If we define the degree of an element of $\mathbf{L}$ to be the smallest integer k such that V_k contains this element, then the degree is Galois invariant and sub-additive, $\deg(wz) \leq \deg(w) + \deg(z)$. The degree this times takes values between 0 and $\lceil \frac{d-1}{2} \rceil$. It is a slightly less informative function than in the Kummer or Artin-Schreier cases (it takes twice less values).

Example. Take $p = q = 13$ and $d = 7$. So $m = 2$. Let $D = 2$ which is not a square in $\mathbb{F}_{13}$. We look for some $a = U + \sqrt{2}V$ such that $U^2 - 2V^2 = 1$ and a has order $p+1 = 14$ in $\mathbb{F}_{13}(\sqrt{2})^*$. For example $U = 3$ and $V = 2$ are fine. The u-coordinate of $3 + 2\sqrt{2}$ is $u(a) = \frac{3}{2} = 8$. One can write the polynomial

$$A(X) = X^7 + 3X^5 + 10X^3 + 4X - 8(7X^6 + 5X^4 + 6X^2 + 8).$$

Formula (2) predicts the Frobenius action. We set $t = [-m]a = [-2]a$ so $u(t) = 4$ and Frobenius operates by translation by t, so $X^p = \frac{4X+2}{X+4} \bmod A(X)$.

So we have made a small progress: We can now treat extensions of $\mathbb{F}_q$ of degree dividing $q+1$. Unfortunately this condition is just as restrictive (though different) as the one imposed by Kummer theory. What do we do if the degree does not divide $q+1$ nor $q-1$?

We must diversify the algebraic groups we use. The next family to consider is made of elliptic curves.

8 Residue fields of divisors on elliptic curves

We now specialize the computations in section 6 to the case where $\mathbf{G}$ is an elliptic curve. Take $\mathbf{K} = \mathbb{F}_q$ a finite field for which we want to construct a degree $d \geq 2$ extension where d is prime to the characteristic p of $\mathbb{F}_q$. Here $\mathbf{G} = E$ is an ordinary elliptic curve over $\mathbb{F}_q$. We denote by ϕ the Frobenius endomorphism of E. Let $\mathfrak{i}$ be an invertible ideal in the endomorphism ring $\mathrm{End}(E)$ of E. Assume $\mathfrak{i}$ divides $\phi - 1$ and $\mathrm{End}(E)/\mathfrak{i}$ is cyclic of order $d \geq 2$. So $E(\mathbb{F}_q)$ contains a cyclic subgroup $T = \mathrm{Ker}\,\mathfrak{i}$ of order d.

Let $I : E \to F$ be the degree d cyclic isogeny with kernel T. The quotient $F(\mathbb{F}_q)/I(E(\mathbb{F}_q))$ is isomorphic to T. Take a in $F(\mathbb{F}_q)$ such that $a \bmod I(E(\mathbb{F}_q))$ generates this quotient. The fiber $I^{-1}(a)$ is an irreducible divisor. This means that the d geometric points above a are defined on a degree d extension $\mathbf{L}$ of $\mathbf{K}$ and permuted by Galois action. We denote by $B = I^{-1}(a)$ the corresponding prime divisor.

Since $\mathbf{L}$ is the residue extension of E at B, we can represent elements of $\mathbf{L}$ in the following way: If f is a function on E with polar divisor disjoint to B, we denote by $f \bmod B \in \mathbf{L}$ the residue of f at B.

For f a function in $\mathbb{F}_q(E)$, the degree of f is the number of poles of f counted with multiplicities. For every $k \geq 0$ we call $\mathcal{F}_k$ the set of degree $\leq k$ functions in $\mathbb{F}_q(E)$, having no pole at B. We denote by V_k the corresponding set of residues in $\mathbf{L}$,

$$V_k = \{f \bmod B | f \in \mathcal{F}_k\}.$$

We have $V_0 = V_1 = \mathbf{K} \subset V_2 \subset \cdots \subset V_d = \mathbf{L}$ (Riemann-Roch) and $V_k \times V_l \subset V_{k+l}$. It is clear also that $\mathcal{F}_k$ is Galois invariant since composition by a translation from T does not affect the degree of a function. Therefore V_k is invariant under the action of $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$.

If we want to test whether an element z of $\mathbf{L}$ is in V_k, we look for a function f in $\mathcal{F}_k$ such that $f = z \pmod B$. This is an interpolation problem which is hardly more difficult than in the two previous cases (polynomials for Kummer and rational fractions for the torus). We look for f as a quotient of two homogeneous forms of degree $\lceil \frac{k+1}{3} \rceil$, which can be done with linear algebra.

One can choose a smoothness basis consisting of all elements $f \bmod B$ in V_κ for a given κ. Factoring an element $z = f \bmod B$ of $\mathbf{L}$ boils down to factoring the divisor of f as a sum of prime divisors of degree $\leq \kappa$.

What conditions are sufficient for an elliptic curve to exist with all the required properties ? Since the number of $\mathbb{F}_q$-rational points on the elliptic curve is divisible by d, the size q of the field cannot be too small, that is

$$q + 2\sqrt{q} + 1 > d.$$

Assume d is odd and there exists a squarefree multiple D of d such that $D \not\equiv 1 \bmod p$ and

$$q + 1 - 2\sqrt{q} < D < q + 1 + 2\sqrt{q}.$$

There exists an ordinary elliptic curve E over $\mathbb{F}_q$ having D rational points over $\mathbb{F}_q$ and trace $t = q + 1 - D$. The ring $\mathbb{Z}[\phi]$ is integrally closed locally at every odd prime dividing D. The larger ring $\mathrm{End}(E)$ has the same property. The ideal $(\phi - 1)$ of $\mathrm{End}(E)$ has a unique degree d factor $\mathfrak{i}$. The quotient $\mathrm{End}(E)/\mathfrak{i}$ is cyclic and $\mathfrak{i}$ is invertible in $\mathrm{End}(E)$.

Given q and ϕ (a quadratic integer) as above, one can find an elliptic curve $E/\mathbb{F}_q$ by exhaustive search or using complex multiplication theory.

Example. Let $p = q = 11$, and $d = D = 7$, so $t = 5$ and $\phi^2 - 5\phi + 11 = 0$. The elliptic curve E with equation $y^2 + xy = x^3 + 2x + 8$ has complex multiplication by $\mathbb{Z}[\frac{\sqrt{-19}+1}{2}]$. The discriminant of $\mathbb{Z}[\phi]$ is -19, so $\mathrm{End}(E) = \mathbb{Z}[\phi]$. The ideal $\mathfrak{i} = (\phi - 1)$ is invertible and its kernel T is the full group of $\mathbb{F}_q$-rational points on E. The kernel of the degree 7 isogeny $I : E \to F$ is the group of rational points on E and for any non zero $a \in F(\mathbb{F}_{11})$, the fiber $B = I^{-1}(a)$ is irreducible.

9 Sieving algorithms and surfaces

There exists a family of algorithms for factoring integers and computing discrete logarithms that rely on intersection theory on algebraic or arithmetic surfaces. These algorithms are known as *the number field sieve*, *the function field sieve*, etc. The core of these algorithms is illustrated on the front page of the book [5]. In this section, we present the ideas underlying this family of algorithms in a rather general setting. This will help us to describe our construction in the next section 10. The sieving algorithm invented by Joux and Lercier in [2] for computing discrete logarithms will serve as a nice illustration for these ideas.

Let $\mathbb{F}_p$ be the field with p elements where p is prime. Let $\mathcal{S}$ be a smooth projective reduced, absolutely irreducible surface over $\mathbb{F}_p$. Let $\mathcal{A}$ and $\mathcal{B}$ be two absolutely irreducible curves on $\mathcal{S}$. Let $\mathcal{I}$ be an irreducible sub-variety of the intersection $\mathcal{A} \cap \mathcal{B}$. We assume that $\mathcal{A}$ and $\mathcal{B}$ meet transversely at $\mathcal{I}$ and we denote by d the degree of $\mathcal{I}$. The residue field of $\mathcal{I}$ is $\mathbb{F}_p(\mathcal{I}) = \mathbb{F}_q$ with $q = p^d$.

We need a pencil (linear or at least algebraic and connected) of effective divisors on $\mathcal{S}$. We denote it by $(D_\lambda)_{\lambda \in \Lambda}$ where Λ is the parameter space.

We fix an integer κ and we look (at random) for divisors D_λ in the pencil, such that both intersection divisors $D \cap \mathcal{A}$ and $D \cap \mathcal{B}$ are disjoint to $\mathcal{I}$ and κ-smooth (they split as sums of effective $\mathbb{F}_q$-divisors of degree $\leq \kappa$).

We define an equivalence relation $\equiv_{\mathcal{I}}$ on the set of divisors on $\mathcal{S}$ not meeting $\mathcal{I}$: We say $D \equiv_{\mathcal{I}} 0$ if and only if D is the divisor of a function f and f is constant modulo $\mathcal{I}$. The equivalence classes for this relation are parameterized by points in some algebraic group denoted $\mathrm{Pic}(\mathcal{S}, \mathcal{I})$. This algebraic group is an extension of $\mathrm{Pic}(\mathcal{S})$ by a torus $T_{\mathcal{I}}$ of dimension $d - 1$.

One similarly defines the algebraic groups $\mathrm{Pic}(\mathcal{A}, \mathcal{I})$ and $\mathrm{Pic}(\mathcal{B}, \mathcal{I})$. These are generalized jacobians of $\mathcal{A}$ and $\mathcal{B}$ respectively. The natural (restriction) morphisms $\mathrm{Pic}(\mathcal{S}, \mathcal{I}) \to \mathrm{Pic}(\mathcal{A}, \mathcal{I})$ and $\mathrm{Pic}(\mathcal{S}, \mathcal{I}) \to \mathrm{Pic}(\mathcal{B}, \mathcal{I})$ induce the identity on the torus $T_{\mathcal{I}}$.

Let N be an integer that kills the three groups $\mathrm{Pic}^0(\mathcal{S})(\mathbb{F}_p)$, $\mathrm{Pic}^0(\mathcal{A})(\mathbb{F}_p)$, and $\mathrm{Pic}^0(\mathcal{B})(\mathbb{F}_p)$. Let λ and μ be two parameters in Λ corresponding to the divisors D_λ and D_μ in our pencil. We assume that $D_\lambda \cap \mathcal{A}$, $D_\mu \cap \mathcal{A}$, $D_\lambda \cap \mathcal{B}$, and $D_\mu \cap \mathcal{B}$ are smooth and disjoint to $\mathcal{I}$.

Let $D_\lambda \cap \mathcal{A} = \sum \mathfrak{a}_i$, $D_\mu \cap \mathcal{A} = \sum \mathfrak{b}_j$, $D_\lambda \cap \mathcal{B} = \sum \mathfrak{c}_k$ and $D_\mu \cap \mathcal{B} = \sum \mathfrak{d}_l$ be decompositions as sums of effective divisors on $\mathcal{A}$ and $\mathcal{B}$ with degree $\leq \kappa$. The divisor $D_\lambda - D_\mu$ is algebraically equivalent to zero and $N(D_\lambda - D_\mu)$ is principal.

Let f be a function on $\mathcal{S}$ with divisor $N(D_\lambda - D_\mu)$. We fix a smooth divisor X on $\mathcal{A}$ (resp. Y on $\mathcal{B}$) with degree 1. For every i and j, let α_i and β_j be functions on $\mathcal{A}$ with divisors $N(\mathfrak{a}_i - \deg(\mathfrak{a}_i)X)$ and $N(\mathfrak{b}_j - \deg(\mathfrak{b}_j)X)$. Similarly, for every k and l, let γ_k and δ_l be functions on $\mathcal{B}$ with divisors $N(\mathfrak{c}_k - \deg(\mathfrak{c}_k)Y)$ and $N(\mathfrak{d}_l - \deg(\mathfrak{d}_l)Y)$. There exist two multiplicative constant c and c' in $\mathbb{F}_p^*$ such that

$$f \equiv c.\frac{\prod_i \alpha_i}{\prod_j \beta_j} \equiv c'.\frac{\prod_k \gamma_k}{\prod_l \delta_l} \bmod \mathcal{I}.$$

This congruence can be regarded as a relation in the group $T_{\mathcal{I}}(\mathbb{F}_p) = \mathbb{F}_q^*/\mathbb{F}_p^*$. The factors in the first fraction belong to the smoothness basis on the $\mathcal{A}$ side: They are residues modulo $\mathcal{I}$

of functions on $\mathcal{A}$ with degree $\leq \kappa$. Similarly, the factors in the second fraction belong to the smoothness basis on the $\mathcal{B}$ side: They are residue modulo $\mathcal{I}$ of functions on $\mathcal{B}$ with degree $\leq \kappa$.

Joux and Lercier take $\mathcal{S}/\mathbb{F}_p$ to be $\mathcal{S} = \mathbb{P}^1 \times \mathbb{P}^1$ the product of $\mathbb{P}^1$ with itself over $\mathbb{F}_p$. To avoid any confusion we call $\mathcal{C}_1 = \mathbb{P}^1/\mathbb{F}_p$ the first factor and $\mathcal{C}_2 = \mathbb{P}^1/\mathbb{F}_p$ the second factor. Let O_1 be a rational point on $\mathcal{C}_1$ and $\mathcal{U}_1 = \mathcal{C}_1 - O_1$. Let x be an affine coordinate on $\mathcal{U}_1 \sim \mathbb{A}^1$. We similarly choose $O_2, \mathcal{U}_2$ and y an affine coordinate on $\mathcal{U}_2$.

They choose $\mathcal{A}$ to be the Zariski closure in $\mathcal{S}$ of the curve in $\mathcal{U}_1 \times \mathcal{U}_2$ with equation $y = f(x)$ where f is a polynomial with degree d_f in $\mathbb{F}_p[x]$. As for $\mathcal{B}$, they choose the Zariski closure in $\mathcal{S}$ of the curve with equation $x = g(y)$ where g is a polynomial with degree d_g in $\mathbb{F}_p[y]$.

The Néron-Severi group of a product of two smooth algebraically irreducible projective curves is $\mathbb{Z}$ times $\mathbb{Z}$ times the group of homomorphisms between the jacobians of the two curves. See [9, Mumford's appendix to Chapter VI]. The Hurwitz formula for the intersection of two classes is also given in this appendix.

Here the Néron-Severi group of $\mathcal{S}$ is $\mathbb{Z} \times \mathbb{Z}$. The algebraic equivalence class of a divisor D is given as its bidegree $(d_x(D), d_y(D))$ where $d_x(D) = D.(\mathcal{C}_1 \times O_2)$ and $d_y(D) = D.(O_1 \times \mathcal{C}_2)$. The intersection form is given by the formula

$$D.E = d_x(E)d_y(D) + d_x(D)d_y(E).$$

The bidegree of $\mathcal{A}$ is $(d_f, 1)$ and the bidegree of $\mathcal{B}$ is $(1, d_g)$. So $\mathcal{A}.\mathcal{B} = 1 + d_f d_g$ and the intersection of $\mathcal{A}$ and $\mathcal{B}$ is made of the point $O_1 \times O_2$ and the $d_f d_g$ points of the form $(\alpha, f(\alpha))$ where α is one of the $d_f d_g$ roots of $g(f(x)) - x$.

Let $h(x)$ be a simple irreducible factor of the later polynomial and let d be its degree. We take $\mathcal{I}$ to be the zero dimensional and degree d corresponding variety. The residue field $\mathbb{F}_p(\mathcal{I})$ is finite of order q where $q = p^d$.

To finish with, we need a pencil of effective divisors $(D_\lambda)_{\lambda \in \Lambda}$ on $\mathcal{S}$. It is standard to take for Λ the set of polynomials λ in $\mathbb{F}_p[x, y]$ with given bidegree (u_x, u_y) where u_x and u_y are chosen according to p and q. The corresponding divisor D_λ to λ is the Zariski closure of the zero set of λ. It has bidegree (u_x, u_y) too.

We fix an integer κ and look for divisors D_λ such that the two intersection divisors $D_\lambda \cap \mathcal{A}$ and $D_\lambda \cap \mathcal{B}$ are disjoint to $\mathcal{I}$ and κ-smooth. For example, if $\lambda(x, y)$ is a polynomial in x and y, the intersection of D_λ and $\mathcal{A}$ has degree $d_f u_y + u_x$. Its affine part is given by the roots of the polynomial $\lambda(x, f(x)) = 0$. Similarly, the intersection of D_λ and $\mathcal{B}$ has degree $u_y + u_x d_g$. Its affine part is given by the roots of the polynomial $\lambda(g(y), y)) = 0$. Joux and Lercier explain how to choose u_x, u_y and κ according to p and d.

10 Finite residue fields on elliptic squares

In this section we try to conciliate the generic construction in section 9 and the ideas developed in section 8. We would like the automorphisms of $\mathbb{F}_p(\mathcal{I})$ to be induced by automorphisms of the surface $\mathcal{S}$. So let E be an ordinary elliptic curve over $\mathbb{F}_p$ and let $\mathfrak{i}$ be an invertible ideal in the endomorphism ring $\mathrm{End}(E)$. We assume that $\mathfrak{i}$ divides $\phi - 1$ and $\mathrm{End}(E)/\mathfrak{i}$ is cyclic of order

$d \geq 2$. So $E(\mathbb{F}_q)$ contains a cyclic subgroup $T = \mathrm{Ker}\,\mathfrak{i}$ of order d. Let $I : E \to F$ be the quotient by $\mathrm{Ker}\,\mathfrak{i}$ isogeny and let $J : F \to E$ be such that $\phi - 1 = J \circ I$.

We take for $\mathcal{S}$ the product $E \times E$ and to avoid any confusion, we call E_1 the first factor and E_2 the second factor. Let O_1 be the origin on E_1 and O_2 the origin on E_2.

We use again the description of the Néron-Severi group of a product of two curves as given in [9, Appendix to Chapter VI]. This time, the Néron-Severi group of $\mathcal{S}$ is $\mathbb{Z} \times \mathbb{Z} \times \mathrm{End}(E)$. The class (d_1, d_2, ξ) of a divisor D consists of the bidegree and the induced isogeny. More precisely, d_1 is the intersection degree of D and $E_1 \times O_2$, d_2 is the intersection degree of D and $O_1 \times E_2$, and ξ is the homomorphism from E_1 to E_2 induced by the correspondence associated with D.

Let α and β be two endomorphisms of E and let a and b be two $\mathbb{F}_p$-rational points on E. We take $\mathcal{A}$ to be the inverse image of a by the morphism from $E \times E$ to E that maps (P, Q) onto $\alpha(P) - Q$. Let $\mathcal{B}$ be the inverse image of b by the morphism from $E \times E$ onto E that sends (P, Q) onto $P - \beta(Q)$.

Assume $1 - \beta\alpha = \phi - 1$. The intersection of $\mathcal{A}$ and $\mathcal{B}$ consists of points (P, Q) such that $(\phi - 1)(P) = b - \beta(a)$ and $Q = \alpha(P) - a$.

We choose a and b such that there exists a point c in $F(\mathbb{F}_p)$ generating $F(\mathbb{F}_p)/I(E(\mathbb{F}_p))$ and satisfying $J(c) = b - \beta(a)$. Then the intersection between $\mathcal{A}$ and $\mathcal{B}$ contains an irreducible component $\mathcal{I}$ of degree d.

The class of $\mathcal{A}$ is $(\alpha\bar{\alpha}, 1, \alpha)$. Indeed, the first coordinate of this triple is the degree of the projection $\mathcal{A} \to E_2$ onto the second component, that is the number of solutions in P to $\alpha(P) = Q + a$ for generic Q. This is the degree $\alpha\bar{\alpha}$ of α. The second coordinate of this triple is the degree of the projection $\mathcal{A} \to E_1$ onto the first component, that is the number of solutions in Q to $Q = \alpha(P) - a$ for generic P. This is 1. The third coordinate is the morphism in $\mathrm{Hom}(E_1, E_2)$ induced by the correspondence $\mathcal{A}$. This is clearly α. In the same way, we prove that the class of $\mathcal{B}$ is $(1, \beta\bar{\beta}, \bar{\beta})$.

Now let D be a divisor on $\mathcal{S}$ and (d_1, d_2, ξ) its class in the Néron-Severi group. The intersection degree of D and $\mathcal{A}$ is thus

$$D.\mathcal{A} = d_1 + d_2\alpha\bar{\alpha} - \xi\bar{\alpha} - \bar{\xi}\alpha \tag{3}$$

and similarly

$$D.\mathcal{B} = d_1\beta\bar{\beta} + d_2 - \xi\bar{\beta} - \bar{\xi}\beta. \tag{4}$$

We are particularly interested in the case where α and β have norms of essentially the same size (that is the square root of the norm of $\phi - 2$). We then obtain a similar behavior as the algorithm in section 9 with an extra advantage: The smoothness bases on both $\mathcal{A}$ and $\mathcal{B}$ are Galois invariant.

Indeed, let $f_{\mathcal{A}}$ be a function with degree $\leq \kappa$ on $\mathcal{A}$. A point on $\mathcal{A}$ is a couple (P, Q) with $Q = \alpha(P) - a$. So the projection on the first component $\Pi_1 : E_1 \times E_2 \to E_1$ is an isomorphism. There is a unique function f_1 on E_1 such that $f_{\mathcal{A}} = f_1 \circ \Pi_1$. Assume now that (P, Q) is in $\mathcal{I} \subset \mathcal{A}$. Then $f_\alpha(P, Q) = f_1(P)$ is an element of the smoothness basis on $\mathcal{A}$. We observe that $f_1(P)^p = f_1(\phi(P)) = f_1(P + t)$ where t is in the kernel T of $\mathfrak{i}$. So $f_1(P)^p$ is the value at P of $f_1 \circ \tau_t$ where $\tau_t : E_1 \to E_1$ is the translation by t. Since $f_1 \circ \tau_t$ and f_1 have the same degree, the value of $f_1 \circ \tau_t$ at P is again an element in the smoothness basis.

That way, one can divide by d the size of either smoothness basis on $\mathcal{A}$ and $\mathcal{B}$.

As in section 9 we need a pencil of divisors on $\mathcal{S}$ with small class in the Néron-Severi group. We choose small values for (d_1, d_2, ξ) that minimize the expressions in Eq. (3) and Eq. (4) under the three contraints $d_1 \geq 1$, $d_2 \geq 1$ and

$$d_1 d_2 \geq \xi\bar{\xi} + 1. \tag{5}$$

We look for effective divisors in the algebraic equivalence class $\mathfrak{c} = (d_1, d_2, \xi)$. Recall O_1 is the origin on E_1 and O_2 the origin on E_2. The graph $\mathcal{G} = \{(P, Q) | Q = -\xi(P)\}$ of $-\xi : E_1 \to E_2$ is a divisor in the class $(\xi\bar{\xi}, 1, -\xi)$. The divisor $\mathcal{H} = -\mathcal{G} + (d_1 + \xi\bar{\xi})O_1 \times E_2 + (d_2 + 1)E_1 \times O_2$ is in $\mathfrak{c}$. We compute the linear space

$$\mathcal{L}(-\mathcal{G} + (d_1 + \xi\bar{\xi})O_1 \times E_2 + (d_2 + 1)E_1 \times O_2)$$

using the (restriction) exact sequence

$$0 \to \mathcal{L}_S(-\mathcal{G} + (d_1 + \xi\bar{\xi})O_1 \times E_2 + (d_2 + 1)E_1 \times O_2) \\ \to \mathcal{L}_{E_1}((d_1 + \xi\bar{\xi})O_1) \otimes \mathcal{L}_{E_2}((d_2 + 1)O_2) \to \mathcal{L}_{\mathcal{G}}(\Delta)$$

where Δ is the divisor on $\mathcal{G}$ given by the intersection with

$$(d_1 + \xi\bar{\xi})O_1 \times E_2 + (d_2 + 1)E_1 \times O_2.$$

This divisor has degree $d_1 + \xi\bar{\xi} + (d_2 + 1)\xi\bar{\xi}$, so the dimension of the right hand term in the sequence above is equal to this number.

On the other hand, the middle term has dimension $(d_1+\xi\bar{\xi})(d_2+1)$, that is strictly bigger than the dimension of the right hand term, because of Inequality (5). So the linear space on the left is non zero and the divisor class is effective. Inequality (5) is a sufficient condition for effectivity.

In practice, one computes a basis for $\mathcal{L}_{E_1}((d_1 + \xi\bar{\xi})O_1)$ and a basis for $\mathcal{L}_{E_2}((d_2 + 1)O_2)$ and one multiplies the two basis (one takes all products of one element in the first basis with one element in the second basis.) This produces a basis for $\mathcal{L}_{E_1}((d_1 + \xi\bar{\xi})O_1) \otimes \mathcal{L}_{E_2}((d_2 + 1)O_2)$.

One selects enough (more than $d_1 + \xi\bar{\xi} + (d_2 + 1)\xi\bar{\xi}$) points $(A_i)_i$ on $\mathcal{G}$ and one evaluates all functions in the above basis at all these points. A linear algebra calculation produces a basis for the subspace of $\mathcal{L}_{E_1}((d_1 + \xi\bar{\xi})O_1) \otimes \mathcal{L}_{E_2}((d_2 + 1)O_2)$ consisting of functions that vanish along $\mathcal{G}$. For every function ϕ in the later subspace, the divisor of zeroes of ϕ contains $\mathcal{G}$ and the difference $(\phi)_0 - \mathcal{G}$ is an effective divisor in the linear equivalence class of $\mathcal{H}$.

We have thus constructed a complete linear equivalence class inside $\mathfrak{c}$. To find the other linear classes in $\mathfrak{c}$, we remind that $E \times E$ is isomorphic to its Picard variety. So it suffices to replace $\mathcal{H}$ in the above calculation by $\mathcal{H} + E_1 \times Z_2 - E_1 \times O_2 + Z_1 \times E_2 - O_1 \times E_2$ where Z_1 and Z_2 run over $E_1(\mathbb{F}_p)$ and $E_2(\mathbb{F}_p)$ respectively.

11 Experiments

In this section, we give a practical example of the geometric construction of section 10. We perform a discrete logarithm computation in $\mathbb{F}_{61^{19}}$. In such a field, Joux and Lercier algorithm

would handle a factor basis of irreducible polynomials of degree 2 over $\mathbb{F}_{61}$, in two variables. Such a factor basis would have about 3600 elements. It turns out that in this case we can reduce the factor basis to only 198 elements using the ideas given in the previous section.

Initialization phase. We set $p = 61$ and consider the plane projective elliptic curve E over $\mathbb{F}_p$ with equation $Y^2Z = X^3 + 20XZ^2 + 21Z^3$. It is ordinary with trace $t = -14$. The ring generated by the Frobenius ϕ has discriminant -48. The full endomorphism ring of E is the maximal order in the field $\mathbb{Q}(\sqrt{-3})$.

Let β be the degree 3 endomorphism of E given by

$$\begin{array}{rccl} \beta : & E & \to & E\,, \\ (x\ :y\ :1) & \mapsto & (\frac{20\,x^3+36\,x^2+35\,x+40}{(x+7)^2}\ :y\frac{58\,x^3+59\,x^2+12\,x+21}{(x+7)^3}\ :1)\,. \end{array}$$

We check $\beta^2 = -3$ and we fix an isomorphism between $\mathrm{End}(E) \otimes \mathbb{Q}$ and $\mathbb{Q}(\sqrt{-3}) \subset \mathbb{C}$ by setting $\beta = \sqrt{-3}$. The Frobenius endomorphism is $\phi = -7 + 2\sqrt{-3}$.

Let α be the degree 4 endomorphism defined by $\alpha = 1 + \beta = 1 + \sqrt{-3}$. It can be given explicitly by

$$\begin{array}{rccl} \alpha : & E & \to & E\,, \\ (x\ :y\ :1) & \mapsto & (\frac{49\,x^4+28\,x^3+55\,x^2+53\,x+27}{(x+25)(x+27)^2}\ :y\frac{38\,x^5+37\,x^4+30\,x^3+49\,x^2+9\,x+46}{(x+25)^2(x+27)^3}\ :1)\,. \end{array}$$

The endomorphism $I = 1 - \beta\alpha$ has degree 19 and divides $\phi - 1$. The kernel of I consists of the following 19 rational points,

$$\begin{aligned} \mathrm{Ker}\, I = \{&(0:1:0), (11:\pm 13:1), (14:\pm 19:1), (21:\pm 8:1), (35:\pm 15:1), \\ &(40:\pm 10:1), (41:\pm 10:1), (45:\pm 27:1), (48:\pm 2:1), (51:\pm 23:1)\}\,. \end{aligned}$$

Let $\mathcal{S} = E \times E$. We call $E_1 = E$ the first factor and $E_2 = E$ the second one. If P and Q are independent generic points on E, then (P, Q) is a generic point on $\mathcal{S}$. Let a on E be the point with coordinates $(52 : 24 : 1)$. Let $\mathcal{A} \subset \mathcal{S}$ be the curve with equation $\alpha(P) - Q = a$. Let b on E be the point with coordinates $(1 : 46 : 1)$. Let $\mathcal{B} \subset \mathcal{S}$ be the curve with equation $P - \beta(Q) = b$. The numerical class of $\mathcal{A}$ is $(4, 1, 1 + \sqrt{-3})$ and the numerical class of $\mathcal{B}$ is $(1, 3, -\sqrt{-3})$. Note that $b - \beta(a) = (57 : 11 : 1)$ is of order 38 and generates $E(\mathbb{F}_p)$ modulo the image of I.

Call $\mathcal{I}$ the intersection $\mathcal{A} \cap \mathcal{B}$. It consists of points (P, Q) such that $(1 - \beta\alpha)(P) = b - \beta(a)$, $Q = \alpha(P) - a$ and thus $(\alpha\beta - 1)(Q) = a - \alpha(b)$. In terms of the affine coordinates (x_1, y_1) of P and (x_2, y_2) of Q, this reads

$$\begin{aligned} x_1 = \frac{\left(44\,{x_2}^4 + 12\,{x_2}^3 + 9\,{x_2}^2 + 46\,x_2 + 40\right) y_2}{{x_2}^6 + 34\,{x_2}^5 + 41\,{x_2}^4 + 47\,{x_2}^3 + 7\,{x_2}^2 + 14\,x_2 + 58} + \\ \frac{{x_2}^6 + 26\,{x_2}^5 + 25\,{x_2}^3 + 41\,{x_2}^2 + 19\,x_2 + 6}{{x_2}^6 + 34\,{x_2}^5 + 41\,{x_2}^4 + 47\,{x_2}^3 + 7\,{x_2}^2 + 14\,x_2 + 58}, \end{aligned} \quad (6)$$

$$\begin{aligned} y_1 = \frac{\left(11\,{x_2}^7 + 2\,{x_2}^6 + 50\,{x_2}^5 + 59\,{x_2}^4 + 57\,{x_2}^3 + 30\,{x_2}^2 + 4\,x_2 + 14\right) y_2}{{x_2}^9 + 51\,{x_2}^8 + 7\,{x_2}^7 + 32\,{x_2}^6 + 56\,{x_2}^5 + 48\,{x_2}^4 + 26\,{x_2}^3 + 49\,{x_2}^2 + 18\,x_2 + 41} + \\ \frac{46\,{x_2}^9 + 54\,{x_2}^8 + 2\,{x_2}^7 + 4\,{x_2}^6 + 52\,{x_2}^5 + 17\,{x_2}^4 + 60\,{x_2}^3 + 41\,{x_2}^2 + 48\,x_2 + 21}{{x_2}^9 + 51\,{x_2}^8 + 7\,{x_2}^7 + 32\,{x_2}^6 + 56\,{x_2}^5 + 48\,{x_2}^4 + 26\,{x_2}^3 + 49\,{x_2}^2 + 18\,x_2 + 41}, \end{aligned} \quad (7)$$

or alternatively, x_2, y_2 can be given as functions of degree 8 and degree 12 in x_1, y_1.

The projection of $\mathcal{I}$ on E_1 (resp. E_2) yields a place $\mathcal{P}$ (resp. $\mathcal{Q}$) of degree 19 defined in the affine coordinates (x, y) by the equations

$$\begin{aligned}\mathcal{P} = (&{x_1}^{19} + 60\,{x_1}^{18} + 25\,{x_1}^{17} + 21\,{x_1}^{16} + 23\,{x_1}^{15} + 22\,{x_1}^{14} + 49\,{x_1}^{13} + 38\,{x_1}^{12} + 30\,{x_1}^{11} + 57\,{x_1}^{10} + \\ &3\,{x_1}^{9} + 15\,{x_1}^{8} + 26\,{x_1}^{7} + 17\,{x_1}^{6} + 45\,{x_1}^{5} + 30\,{x_1}^{4} + 48\,{x_1}^{3} + 55\,{x_1}^{2} + 18\,x_1 + 35, \\ &y_1 + 12\,{x_1}^{18} + 38\,{x_1}^{17} + 5\,{x_1}^{16} + {x_1}^{15} + 45\,{x_1}^{14} + 42\,{x_1}^{13} + 18\,{x_1}^{12} + 34\,{x_1}^{11} + 39\,{x_1}^{10} + \\ &59\,{x_1}^{9} + 16\,{x_1}^{8} + 18\,{x_1}^{7} + 16\,{x_1}^{6} + 36\,{x_1}^{5} + 11\,{x_1}^{4} + 9\,{x_1}^{3} + 48\,{x_1}^{2} + 59\,x_1 + 8)\,,\end{aligned}$$

$$\begin{aligned}\mathcal{Q} = (&{x_2}^{19} + 25\,{x_2}^{18} + 34\,{x_2}^{17} + 46\,{x_2}^{16} + 16\,{x_2}^{15} + 14\,{x_2}^{14} + 58\,{x_2}^{13} + 52\,{x_2}^{12} + 39\,{x_2}^{11} + 48\,{x_2}^{10} + \\ &18\,{x_2}^{9} + 56\,{x_2}^{8} + 41\,{x_2}^{7} + 40\,{x_2}^{6} + 11\,{x_2}^{5} + 33\,{x_2}^{4} + 55\,{x_2}^{3} + 14\,{x_2}^{2} + 5\,x_2 + 56, \\ &y_2 + 42\,{x_2}^{18} + 40\,{x_2}^{17} + 23\,{x_2}^{16} + 41\,{x_2}^{15} + 14\,{x_2}^{14} + 12\,{x_2}^{13} + 30\,{x_2}^{12} + 50\,{x_2}^{11} + 33\,{x_2}^{10} + \\ &33\,{x_2}^{9} + 60\,{x_2}^{8} + 15\,{x_2}^{7} + 54\,{x_2}^{6} + 13\,{x_2}^{5} + 17\,{x_2}^{4} + 31\,{x_2}^{3} + 50\,{x_2}^{2} + 52\,x_2 + 3)\,.\end{aligned}$$

The residue fields of these two places are isomorphic (both being degree 19 extensions of $\mathbb{F}_{61}$). We fix an isomorphism between these two residue fields by setting

$$\begin{aligned}x_2 \mapsto\ &2\,{x_1}^{18} + 57\,{x_1}^{17} + 21\,{x_1}^{16} + 10\,{x_1}^{15} + 54\,{x_1}^{14} + 35\,{x_1}^{13} + 45\,{x_1}^{12} + 27\,{x_1}^{11} + 41\,{x_1}^{10} + \\ &55\,{x_1}^{9} + 27\,{x_1}^{8} + 36\,{x_1}^{7} + 29\,{x_1}^{6} + 50\,{x_1}^{5} + 44\,{x_1}^{4} + 18\,{x_1}^{3} + 38\,{x_1}^{2} + 51\,x_1 + 18\,. \quad (8)\end{aligned}$$

Fixing this isomorphism is equivalent to choosing a geometric point in $\mathcal{I}$.

Sieving phase. We are now going to look for "smooth" functions on $\mathcal{S}$. We first explain what we mean by smooth in this context. Let $\varepsilon(x_1, y_1, x_2, y_2)$ be a function on $\mathcal{S}$. We assume ε does not vanish at $\mathcal{I}$. Let $\Pi_1 : \mathcal{S} = E_1 \times E_2 \to E_1$ be the projection on the first factor. The restriction of Π_1 to $\mathcal{A}$ is a bijection. So we can define a point on $\mathcal{A}$ by its coordinates (x_1, y_1). Let $\Pi_2 : \mathcal{S} = E_1 \times E_2 \to E_2$ be the projection on the second factor. The restriction of Π_2 to $\mathcal{B}$ is a bijection. So we can define a point on $\mathcal{B}$ by its coordinates (x_2, y_2).

Let $\varepsilon_1(x_1, y_1)$ (resp. $\varepsilon_2(x_2, y_2)$) be the restriction of ε to $\mathcal{A}$ (resp. $\mathcal{B}$). For example $\varepsilon_2(x_2, y_2)$ is obtained by substituting x_1, y_1 as functions in x_2, y_2 in ε thanks to Eq. (6) and Eq. (7).

The function ε is said to be smooth if the divisors of ε_1 and ε_2 both contain only places of small degree κ. In our example, we choose $\kappa = 2$. Let us remark at this point that thanks to the isomorphism given by Eq. (8), the reduction modulo $\mathcal{P}$ of ε_1 is equal to the reduction modulo $\mathcal{Q}$ of ε_2, and this yields an equality in $\mathbb{F}_{61^{19}}$.

To every non-zero function on $\mathcal{S}$, one can associate a linear pencil of divisors. We define the linear (resp. numerical) class of the function to be the linear (resp. numerical) class of the divisor of its zeroes (or poles).

We shall be firstly interested in functions ε with numerical class $(1, 0, 0)$. An effective divisor in these classes is $c \times E_2$ where c is a place of degree 1 on E_1 and it is not difficult to see that the intersection degrees of such a divisor with $\mathcal{A}$ and $\mathcal{B}$ are 1 and 3. Functions with numerical class $(2, 0, 0)$ are obtained in the same way.

We found similarly functions ε in the class $(0, 1, 0)$, derived from divisors $E_1 \times c$. The intersection degrees are now 4 and 1. Functions with numerical class $(0, 2, 0)$ are obtained in

the same way too. More interesting, the class $(1,1,1)$ containing the divisors with equation $P = Q + c$, yields intersection degrees 3 and 4.

We finally consider the class $(2,2,1)$ which is, by far, much larger than the previous classes. The intersection degrees are 8 and 8. To enumerate functions in this class, we first build a basis for the linear space associated to divisors of degree 3 on both E_1 and E_2. For instance, let us consider $\mathcal{L}_{E_1}(3\,O_1)$ and $\mathcal{L}_{E_2}(3\,O_2)$, basis of which are given by $\{1, x_1, y_1\}$ and $\{1, x_2, y_2\}$. We then determinate that a basis for the subspace of $\mathcal{L}_{E_1}(3\,O_1) \otimes \mathcal{L}_{E_2}(3\,O_2)$, consisting of functions that vanish along the graph $\mathcal{G} = \{(P, Q), Q = -P\}$, is given by $\{y_1\,x_2 + x_1\,y_2, y_1 + y_2, x_1 - x_2\}$. An exhaustive enumeration of functions of the form $y_1\,x_2 + x_1\,y_2 + \lambda(y_1 + y_2) + \mu(x_1 - x_2)$, with $\lambda, \mu \in \mathbb{F}_p$ yields useful equations.

We give examples of such relations in Tab. 1.

Linear algebra phase. With our smoothness choice, the factor basis is derived from places of degree one and two. Since we prefer functions to divisors, the factor basis will contain the reduction modulo $\mathcal{P}$, resp. $\mathcal{Q}$, of functions the divisors of which are equal to $76(x_1 + \alpha, y_1 + \beta) - 76(1/x_1, y_1/x_1^2)$, resp. $76(x_2 + \alpha, y_2 + \beta) - 76(1/x_2, y_2/x_2^2)$ (remember that in our example $\#E(\mathbb{F}_p) = 76$). In this setting, the evaluation at $\mathcal{P}$ or $\mathcal{Q}$ of any smooth function can be easily written as a product of elements of the factor basis.

It is worth recalling that the action of the Frobenius ϕ on the reduction of a function modulo $\mathcal{P}$ or $\mathcal{Q}$ is equal to the reduction of a function, the poles and the zeros of which are translated by one specific point of $\mathrm{Ker}\, I$. In our example, this point is $F_1 = (11 : 48 : 1)$ for the reduction modulo $\mathcal{P}$ and $F_2 = (45 : 34 : 1)$ for the reduction modulo $\mathcal{Q}$. For instance, let us consider a function g_0 the divisor of which is equal to $76(x_1 + 41, y_1 + 8) - 76(1/x_1, y_1/x_1^2)$. Let us now consider a function g_6 which corresponds to $(-41 : -8 : 1) + 6F_1$, that is a function with divisor equal to $76(x_1 + 45, y_1 + 17) - 76(1/x_1, y_1/x_1^2)$. We have then $\overline{g_6} = c.\overline{g_0}^{p^6}\overline{f}^{1+p+p^2+p^3+p^4+p^5}$ for some $c \in \mathbb{F}_p$, where f is a function the divisor of which is equal to $76\,F_1 - 76(1/x_1, y_1/x_1^2)$.

Thanks to this observation, we can thus divide by 19 the size of the factor basis, at the expense in the linear algebra phase of entries equal to sums of powers of p. We finally have 4 meaningful places of degree 1 and 92 meaningful places of degree 2 on each side, that is a total of 196 entries in our factor basis. Of course, under the Galois conjugations, most of the relations obtained in the sieving phase are redundant, but it does not really matter since it is not difficult to reduce the sieving phase to the only meaningful relations.

We have

$$61^{19} - 1 = 2^2 \cdot 3 \cdot 5 \cdot 229 \cdot 607127818287731321660577427051.$$

We performed the linear algebra modulo the largest factor of $61^{19} - 1$, that is the 99-bit integer $607127818287731321660577427051$. This gives us the discrete logarithm in basis $f \bmod \mathcal{I}$ of any element in the smoothness basis. For instance, if g is any function such that div $g = 76\,(x_1^2 + 37\,x_1 + 54, y_1 + 41\,x_1 + 16) - 152(1/x_1, y_1/x_1^2)$, we find that

$$g^{2^2 \cdot 3 \cdot 5 \cdot 229} = (f^{2^2 \cdot 3 \cdot 5 \cdot 229})^{471821537021905592692223848756}.$$

Class	div ε_1	div ε_2
$(1,0,0)$	$(x_1+43, y_1+33)-(x_1+13, y_1+59)$	$(x_2^2+x_2+52, y_2+10\,x_2+37)+(x_2+12, y_2+35)-(x_2+2, y_2+20)-(x_2^2+26\,x_2+39, y_2+5\,x_2+27)$
$(2,0,0)$	$(x_1^2+56\,x_1+34, y_1+22\,x_1+52)-2\,(x_1+13, y_1+59)$	$(x_2^2+37\,x_2+53, y_2+42\,x_2+58)+(x_2^2+12\,x_2+19, y_2+52\,x_2+43)+(x_2^2+41\,x_2+29, y_2+33\,x_2+41)-2\,(x_2+2, y_2+20)-2\,(x_2^2+26\,x_2+39, y_2+5\,x_2+27)$
$(0,1,0)$	$(x_1^2+4\,x_1+12, y_1+55\,x_1+47)+(x_1^2+45\,x_1+31, y_1+19\,x_1+23)-(x_1+42, y_1+60)-(x_1+36, y_1+15)-(x_1^2+60\,x_1+25, y_1+36\,x_1+26)$	$(x_2+43, y_2+33)-(x_2+13, y_2+59)$
$(0,2,0)$	$(x_1^2+26\,x_1+12, y_1+12\,x_1+32)+(x_1^2+48\,x_1+6, y_1+59)+(x_1^2+53\,x_1+56, y_1+42\,x_1+56)+(x_1^2+3\,x_1+38, y_1+17\,x_1+36)-2\,(x_1+42, y_1+60)-2\,(x_1+36, y_1+15)-2\,(x_1^2+60\,x_1+25, y_1+36\,x_1+26)$	$(x_2^2+24\,x_2+39, y_2+37\,x_2+27)-2\,(x_2+13, y_2+59)$
$(1,1,1)$	$(x_1+2, y_1+41)+(x_1^2+26\,x_1+39, y_1+56\,x_1+34)-(x_1^2+48\,x_1+6, y_1+2)-(x_1+52, y_1+25)$	$(x_2+17, y_2+21)+(x_2^2+57\,x_2+11, y_2+33\,x_2)+(x_2+55, y_2+33)-(x_2^2+49\,x_2+42, y_2+26)-(x_2^2+3\,x_2+4, y_2+30\,x_2+20)$
$(2,2,2)$	$(x_1^2+25\,x_1+42, y_1+5\,x_1+13)+(x_1^2+30\,x_1+19, y_1+52\,x_1+42)+(x_1^2+59\,x_1+30, y_1+28\,x_1+22)-2\,(x_1^2+48\,x_1+6, y_1+2)-2\,(x_1+52, y_1+25)$	$(x_2^2+30\,x_2+21, y_2+50\,x_2+52)+(x_2^2+41\,x_2+8, y_2+54\,x_2+58)+(x_2^2+32\,x_2+20, y_2+34\,x_2+28)+(x_2^2+42\,x_2+49, y_2+29\,x_2+51)-2\,(x_2^2+49\,x_2+42, y_2+26)-2\,(x_2^2+3\,x_2+4, y_2+30\,x_2+20)$
$(2,2,1)$	$(x_1+24, y_1+33)+(x_1+25, y_1)+(x_1+35, y_1)+(x_1+60, y_1+46)+(x_1^2+33\,x_1+43, y_1+3\,x_1+34)+(x_1^2+53\,x_1+53, y_1+24\,x_1+33)-(x_1+1, y_1)-(x_1+54, y_1+4)-(x_1^2+17\,x_1+19, y_1+41\,x_1+21)-(x_1^2+51\,x_1+53, y_1+44\,x_1+31)-(x_1^2+55\,x_1+38, y_1+38\,x_1+58)$	$(x_2+3, y_2+42)+(x_2^2+7\,x_2+20, y_2+33\,x_2+46)+(x_2^2+38\,x_2+12, y_2+58\,x_2+6)+(x_2^2+42\,x_2+35, y_2+7\,x_2+41)-(x_2+1, y_2)-(x_2+11, y_2+42)-(x_2+16, y_2+34)-(x_2^2+26\,x_2+12, y_2+49\,x_2+29)-(x_2^2+47\,x_2+5, y_2+7\,x_2+14)$
$(2,2,1)$	$(x_1+10, y_1+23)+(x_1+20, y_1+x_1+30)+(x_1+29, y_1+1)+(x_1+41, y_1+x_1+33)+(x_1^2+6\,x_1+17, y_1+25\,x_1+16)+(x_1^2+25\,x_1+12, y_1+25\,x_1+47)-(x_1+1, y_1)-(x_1+54, y_1+4)-(x_1^2+17\,x_1+19, y_1+41\,x_1+21)-(x_1^2+51\,x_1+53, y_1+44\,x_1+31)-(x_1^2+55\,x_1+38, y_1+38\,x_1+58)$	$(x_2+29, y_2+60)+(x_2+36, y_2+15)+(x_2^2+15\,x_2+58, y_2+41\,x_2+39)+(x_2^2+23\,x_2+2, y_2+33\,x_2+7)+(x_2^2+44\,x_2+33, y_2+35\,x_2+28)-(x_2+1, y_2)-(x_2+11, y_2+42)-(x_2+16, y_2+34)-(x_2+50, y_2+13)-(x_2^2+26\,x_2+12, y_2+49\,x_2+29)-(x_2^2+47\,x_2+5, y_2+7\,x+14)$

Table 1: Some relations collected in the sieving phase.

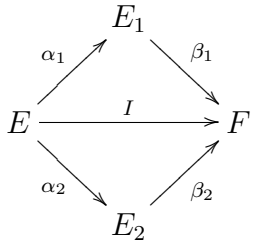
12 Generalization and limitations

The construction in section 10 can and should be generalized.

Let E be again an ordinary elliptic curve over $\mathbb{F}_p$ and let $\mathfrak{i}$ be an invertible ideal in the endomorphism ring $\mathrm{End}(E)$. We assume that $\mathfrak{i}$ divides $\phi - 1$ and $\mathrm{End}(E)/\mathfrak{i}$ is cyclic of order $d \geq 2$. Let F be the quotient of E by the kernel T of $\mathfrak{i}$ and $I : E \to F$ the quotient isogeny.

The integer d belongs to the ideal $\mathfrak{i}$. Let u and v be two elements in $\mathfrak{i}$ such that $d = u + v$ and $(u) = \mathfrak{i}\mathfrak{a}_1\mathfrak{b}_1$ and $(v) = \mathfrak{i}\mathfrak{a}_2\mathfrak{b}_2$ where $\mathfrak{a}_1$, $\mathfrak{b}_1$, $\mathfrak{a}_2$, $\mathfrak{b}_2$ are invertible ideals in $\mathrm{End}(E)$. We deduce the existence of two elliptic curves E_1 and E_2 and four isogenies α_1, β_1, α_2, β_2, such that $\beta_1\alpha_1 + \beta_2\alpha_2 = I$.

We represent all these isogenies on the (non commutative) diagram below.



We set $\mathcal{S} = E_1 \times E_2$. As for $\mathcal{A}$ we choose the image of $(\alpha_1, \alpha_2) : E \to \mathcal{S}$. And $\mathcal{B}$ is the inverse image of f by $\beta_1 + \beta_2 : \mathcal{S} \to F$ where f generates the quotient $F(\mathbb{F}_p)/I(E(\mathbb{F}_p))$. The intersection of $\mathcal{A}$ and $\mathcal{B}$ is the image by (α_1, α_2) of $I^{-1}(f) \subset E$. We choose u and v such that $\mathfrak{a}_1$, $\mathfrak{b}_1$, $\mathfrak{a}_2$, and $\mathfrak{b}_2$, have norms close to the square root of d.

This construction is useful when the norm of $\mathfrak{i}$ is much smaller than the norm of $\phi - 1$. So we managed to construct Galois invariant smoothness basis for a range of finite fields. Our constructions go beyond the classical Kummer case. They are efficient when the degree d is either below $4\sqrt{q}$ or in the interval $]q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}[$.

References

[1] N. Bourbaki. *Algèbre, chapitre V*. Masson, 1981.

[2] A. Joux and R. Lercier. The function field sieve is quite special. *Lecture Notes in Comput. Sci.*, 2369:431–445, 2002.

[3] A. Joux and R. Lercier. The function field sieve in the medium prime case. *Lecture Notes in Comput. Sci.*, 4004:254–270, 2006.

[4] S. Lang. *Algebra*. Addison-Wesley, 1984.

[5] A.K. Lenstra and H.W. Lenstra. *The development of the number field sieve*. Number 1554 in Lecture Notes in Mathematics. Springer, 1993.

[6] G. Malle and B.H. Matzat. *Inverse Galois Theory*. Springer, 1999.

[7] A. M. Odlyzko. Discrete logarithms: The past and the future. *Designs, Codes, and Cryptography*, 19:129–145, 2000.

[8] L. Thomas. *Arithmétique des extensions d'Artin-Schreier-Witt*. Thèse de l'Université Toulouse 2, 2006.

[9] P. Zariski. *Algebraic surfaces, supplemented edition*. Springer, 1971.