Elliptic curves with a given number of points

Reinier Bröker and Peter Stevenhagen

Mathematisch Instituut, Universiteit Leiden,
Postbus 9512, 2300 RA Leiden, The Netherlands
reinier@math.leidenuniv.nl psh@math.leidenuniv.nl

Abstract. We present a non-archimedean method to construct, given an integer $N \geq 1$, a finite field $\mathbf{F}_q$ and an elliptic curve $E/\mathbf{F}_q$ such that $E(\mathbf{F}_q)$ has order N.

1 Introduction

A classical theorem of Hasse from 1934 states that for an elliptic curve E defined over the finite field $\mathbf{F}_q$ of q elements, the order of the group $E(\mathbf{F}_q)$ of $\mathbf{F}_q$-rational points is an integer in the *Hasse interval*

$$\mathcal{H}_q = [q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$$

around q. If E is given in some standard way, say by a Weierstrass equation over $\mathbf{F}_q$, there are several algorithms that compute the order of $E(\mathbf{F}_q)$. The 1985 algorithm by Schoof [8, 9] runs in time polynomial in $\log q$, and in small characteristic p there are even faster p-adic algorithms due to Satoh [7] and Kedlaya [5].

The situation is rather different in the case of the following problem, which can be seen as an 'inverse problem' to the point counting problem.

Problem 1. Given an integer $N \geq 1$, find a a finite field $\mathbf{F}_q$ and an elliptic curve $E/\mathbf{F}_q$ for which the number of $\mathbf{F}_q$-rational points equals N.

As with other inverse problems, such as in Galois theory, this is mathematically a natural question to ask. In this particular case, an efficient solution to the problem would also be desirable in view of the need in current applications to construct elliptic curves having point groups satisfying various smoothness requirements with respect to their order. It is one of the reasons why we focus on the order N, and do not specify the finite field $\mathbf{F}_q$ as being part of the input. In addition, we will use the freedom with respect to the choice of a base field $\mathbf{F}_q$ to our advantage.

A necessary condition for our problem to be solvable for given N is clearly that N is contained in *some* Hasse interval $\mathcal{H}_q$, so we would like the union $\bigcup_q \mathcal{H}_q$ over all prime powers q to contain *all* positive integers. It is easy to see that the contribution to the union coming from the 'true' prime powers q that are not primes is negligible: it is contained in a zero density subset of $\mathbf{Z}_{\geq 1}$. For this reason, we may and will restrict in the sequel to the case where the base field $\mathbf{F}_q$

is the prime field coming from a prime number q. In this particular case, all integers in $\mathcal{H}_q$ actually do occur as the group order of $E(\mathbf{F}_q)$ for some elliptic curve E, so $N \in \mathcal{H}_q$ is sufficient to guarantee the existence of a solution. (For arbitrary prime powers q there are often not enough supersingular curves to realize all orders congruent to 1 modulo the characteristic.)

For the equality $\mathbf{Z}_{\geq 1} = \bigcup_{q \text{ prime}} \mathcal{H}_q$ we need to show that the primes are not too far apart, i.e., that the gap between consecutive primes q and q' is roughly bounded by $4\sqrt{q}$ for large q. This is more than what is currently known to be true: even under assumption of the Riemann hypothesis the gap between consecutive primes can only shown to be of order $O(\sqrt{q}(\log q)^2)$. However, from a practical, algorithmic point of view there are always *lots* of primes q for which a large integer N is contained in $\mathcal{H}_q$. Indeed, by the prime number theorem, we expect 1 out of every $\log N$ integers around N to be prime, so for large N the set of primes q having $N \in \mathcal{H}_q$ is on average of size $4\sqrt{N}/\log N$, and finding such q is never a problem in practice.

Once we have found a prime $q > 3$ for which we have $N \in \mathcal{H}_q$ (we now require $N > 1$), there is the following *naive algorithm* to find an elliptic curve having exactly N rational points over $\mathbf{F}_q$. Suppose that we are not in the easy cases where we have $N = q + 1$ (then any supersingular curve over $\mathbf{F}_q$ will do) or where one of the few curves with j-invariant 0 or 1728 has the right number of points. Then we try

$$E_a : y^2 = x^3 + ax - a \qquad (a \in \mathbf{F}_q^* \setminus \{-27/4\})$$

for random a as the Weierstrass equation of the desired curve until we find a curve having N points. More precisely, we write $N = q+1-t$ and check whether for our a the point $(1, 1) \in E_a(\mathbf{F}_q)$ is annihilated by $N = q+1-t$ or $q+1+t$. If it is, we check whether the number of $\mathbf{F}_q$-rational points is indeed $q + 1 \pm t$. For order $N = q+1-t$ we are done, for order $q+1+t$ not E_a itself but its quadratic twist has N points. Even though the distribution of the group orders of elliptic curves over $\mathbf{F}_q$ is not quite uniform, we expect to examine $O(\sqrt{q}) = O(\sqrt{N})$ curves E_a before we hit a curve having exactly N points. As the amount of time spent per a is usually very small, and certainly polynomial in $\log N$, this yields a probabilistic algorithm with expected running time $O(N^{\frac{1}{2}+o(1)})$. It is quite practical for small values of N, but becomes unwieldy for $N \gg 10^{15}$.

In the next section we briefly describe a classical deterministic algorithm based on complex multiplication methods which, although not asymptotically faster than the naive algorithm, can be improved in various ways. Our first improvement is a p-adic approach to complex multiplication based on the recent work of Couveignes and Henocq [3]. It is described in section 3, and illustrated by the explicit computation in section 4 of an 'ANTS 6 curve' having 2004061320040618 rational points. Our second improvement, in section 5, consists of using 'small' modular functions in this p-adic context to push the limits of what is feasible by p-adic methods. Although the resulting algorithm is still far from polynomial, its power is illustrated in section 6 by the computation of an elliptic curve having 10^{30} rational points.

2 Complex multiplication

A deterministic algorithm to produce an elliptic curve E over the prime field $\mathbf{F}_q$ having $N \in \mathcal{H}_q$ points is provided by the theory of complex multiplication. One writes $N = q+1-t$ and observes that the Frobenius endomorphism $F_q : E \to E$ on the desired curve $E/\mathbf{F}_q$ satisfies the quadratic relation $F_q^2 - tF_q + q = 0$ of discriminant $\Delta = t^2 - 4q < 0$ in $\mathrm{End}(E) = \mathrm{End}_{\overline{\mathbf{F}}_q}(E)$. Assume we are not in the supersingular case $t = 0$. Then our observation gives rise to an embedding

$$\begin{aligned} \mathrm{End}(E) &\longrightarrow K = \mathbf{Q}(\sqrt{\Delta}) \\ F_q &\longmapsto \pi_q = (t + \sqrt{\Delta})/2 \end{aligned}$$

that maps F_q to a prime element π_q of trace t and norm q in the quadratic order $\mathcal{O}_\Delta = \mathbf{Z}[(\Delta + \sqrt{\Delta})/2] \subset K$ of discriminant Δ. By the *Deuring lifting theorem*, there exist a number field $H \supset K$ and an elliptic curve $\tilde{E}/H$ such that

1. there exists $\phi_q \in \mathrm{End}(\tilde{E})$ satisfying $\phi_q^2 - t\phi_q + q = 0$;
2. the prime q splits completely in $H/\mathbf{Q}$, and for every prime $\mathfrak{q}|q$ in H the reduced curve $\tilde{E} \bmod \mathfrak{q}$ is an elliptic curve having $q + 1 - t$ points.

In fact, the reduction of the endomorphism $\phi_q \in \mathrm{End}(\tilde{E})$ above modulo a prime $\mathfrak{q}|q$ in H yields the Frobenius endomorphism of the curve $\tilde{E} \bmod \mathfrak{q}$ over $\mathbf{F}_q$.

The smallest field $H \supset K$ over which a curve $\tilde{E}$ satisfying 1 and 2 can be defined is the Hilbert class field of K. More explicitly, from a list of reduced binary quadratic forms $[a, b, c]$ of discriminant $D = \mathrm{disc}(K)$, which can be viewed as a list of elements of the *class group* $\mathrm{Cl}(D)$ of discriminant D, we can form the *class polynomial*

$$F_D = \prod_{[a,b,c]\in \mathrm{Cl}(D)} \left(X - j\Big(\frac{-b + \sqrt{D}}{2a}\Big) \right) \in \mathbf{Z}[X]$$

of discriminant D. Here $j : \mathbf{H} \to \mathbf{C}$ denotes the well-known elliptic modular function on the complex upper half plane. Using sufficiently accurate complex approximations of the zeroes $j(\frac{-b+\sqrt{D}}{2a})$ of F_D, one may *exactly* determine F_D as it has integral coefficients. Once we have F_D, we are essentially done. Indeed, any zero of the irreducible polynomial $F_D \in \mathbf{Z}[X]$ generates the Hilbert class field H of K over K, and modulo q the polynomial $\bar{F}_D \in \mathbf{F}_q[X]$ splits into linear factors. (In fact, this property of F_D is an excellent check for the correctness of any algorithm to compute F_D.) The zeroes of $\bar{F}_D$ in $\mathbf{F}_q$ are the j-invariants of the elliptic curves over $\mathbf{F}_q$ having endomorphism ring isomorphic to the ring of integers $\mathcal{O}_D$ of K. If $\bar{j} \in \mathbf{F}_q$ is one of these zeroes, we write down a curve with this j-invariant, and check whether it has $q + 1 - t$ points. If it hasn't, we have found a curve with $q + 1 + t$ points, and (for $j \neq 0, 1728$) its quadratic twist has $N = q + 1 - t$ points.

This deterministic algorithm, although relatively simple, is not much faster than the naive algorithm, as for large D the class polynomial F_D is of degree

$h(D) = O(D^{\frac{1}{2}+o(1)})$ and has coefficients of size $O(D^{\frac{1}{2}+o(1)})$, making the total running time of order $O(D^{1+o(1)})$. However, if we have the freedom to pick q on input N, it is often possible to find primes q for which the associated discriminant $\Delta = \Delta(q) = (q-1-N)^2 - 4N$ is not only of size $N^{\frac{1}{2}+o(1)}$ (this is simply done by picking $q \in [N+1-2\sqrt{N}, N+1+2\sqrt{N}]$ close to the end points of the interval), but moreover has a large square factor. This leads to a field discriminant D of K which is quite a bit smaller than Δ, and makes the method feasible in cases where the naive method would take too long. As we currently cannot even *prove* the existence of a single prime in $q \in [N+1-2\sqrt{N}, N+1+2\sqrt{N}]$, we certainly cannot prove the existence of q for which $\Delta(q)$ has large square factors and D is of order substantially smaller than $O(N^{\frac{1}{2}+o(1)})$.

3 A non-archimedean approach

The key feature of the complex multiplication method in the previous section is the computation of the class polynomial $F_D \in \mathbf{Z}[X]$ of the order $\mathcal{O}_D$ for suitable D. As the zeroes modulo q of F_D are j-invariants of curves $E/\mathbf{F}_q$ for which either E or its quadratic twist has exactly N points, this immediately solves our problem. In this section we achieve the computation of F_D in an other way, using p-adic instead of complex approximations of the zeroes of F_D. Working in a non-archimedean setting has the advantage that we no longer have to cope with the problem of rounding errors that arises in the complex case. It does require a p-adic substitute for the complex analytic method to evaluate j in CM-points of $\mathbf{H}$ using Fourier expansions, and this is provided by the recent work of Couveignes and Henocq [3] explained in this section.

Let $N = q+1-t$ and $\Delta = t^2 - 4q$ be as in the previous section, and $D < -4$ the discriminant of $\mathbf{Q}(\sqrt{\Delta})$. We first construct an elliptic curve E over a finite field $\mathbf{F}_p$ which has CM with $\mathcal{O}_D$. As we want p to be as small as possible, we let s be the smallest positive integer of the same parity as D for which $p = (s^2 - D)/4$ is prime. For $D \equiv 1 \bmod 8$ such p does not exist for parity reasons unless $D = -7$, and we pick the smallest positive s for which $p = (s^2 - 4D)/4$ is prime instead. In practice we expect s to be small, at most a power of $\log|D|$, such that p is of the same order of magnitude as D. Unfortunately, even under GRH proven upper bounds [3] for s are much weaker.

As there is a prime element $\pi_p = (s + \sqrt{D})/2$ (or $\pi_p = (s + 2\sqrt{D})/2$) of norm p and trace $s > 0$ in the order $\mathcal{O}_D = \mathbf{Z}[\pi_p]$ (or $\mathcal{O}_{4D} = \mathbf{Z}[\pi_p]$), there exists an ordinary elliptic curve over $\mathbf{F}_p$ having CM by $\mathbf{Z}[\pi_p]$ and $p + 1 \pm s$ points over $\mathbf{F}_p$. We can find such a curve $E/\mathbf{F}_p$ by applying the naive algorithm, as we saw in section 2 that $|D|$ is much smaller than N. We have $\mathrm{End}(E) = \mathcal{O}_D$ for $D \not\equiv 1 \bmod 8$. For $D \equiv 1 \bmod 8$ the ring $\mathrm{End}(E)$ is either equal to $\mathbf{Z}[\pi_p] = \mathcal{O}_{4D}$ or to $\mathcal{O}_D \supsetneq \mathbf{Z}[\pi_p]$. We are in the second case if all 2-torsion of E is $\mathbf{F}_p$-rational, and in the first if it isn't. As for $D \equiv 1 \bmod 8$ the class polynomials F_D and F_{4D} have the same degree and both generate the Hilbert class field H of K, they are both fine for our purposes. Alternatively, in case we have $\mathrm{End}(E) = \mathcal{O}_{4D}$ there is a unique point P of order 2 in $E(\mathbf{F}_p)$, and we can replace E by the 2-isogenous curve $E/\langle P\rangle$ to achieve $\mathrm{End}(E) = \mathcal{O}_D$. We assume that we have $\mathrm{End}(E) = \mathcal{O}_D$ in the sequel. Note that D is by definition fundamental.

By the Deuring lifting theorem, there exists a curve $\tilde{E}/H$ and a prime $\mathfrak{p}|p$ such that $\tilde{E}$ reduces modulo $\mathfrak{p}$ to E and such that we have $\mathrm{End}(\tilde{E}) \cong \mathrm{End}(E)$. As p splits completely in $H/\mathbf{Q}$ the curve $\tilde{E}$ is actually defined over $\mathbf{Q}_p$. In fact, $\tilde{E}$ is the *unique* elliptic curve over $\mathbf{Q}_p$ with reduction E and endomorphism ring $\mathrm{End}(\tilde{E}) \cong \mathrm{End}(E) \cong \mathcal{O}_D$. It is this *canonical lift* $\tilde{E}$ of E that we want to compute, as its j-invariant is a zero of our class polynomial.

Let $\mathrm{Ell}_D(\mathbf{F}_p)$ be the set of $\overline{\mathbf{F}}_p$-isomorphism classes of elliptic curves over $\mathbf{F}_p$ with endomorphism ring $\mathcal{O}_D$. The j-invariants of the elements in $\mathrm{Ell}_D(\mathbf{F}_p)$ are the zeroes of $(F_D \bmod p)$, so $\mathrm{Ell}_D(\mathbf{F}_p)$ is finite of order $h(D) = \#\mathrm{Cl}(D)$. It can be identified with the similarly defined set $\mathrm{Ell}_D(\mathbf{Q}_p)$ of $\overline{\mathbf{Q}}_p$-isomorphism classes of elliptic curves over $\mathbf{Q}_p$ with endomorphism ring $\mathcal{O}_D$. The j-invariants of the elements in $\mathrm{Ell}_D(\mathbf{Q}_p)$ are the zeroes of F_D. Let $\mathbf{C}_p$ be the completion of an algebraic closure of $\mathbf{Q}_p$, and write $X_D(\mathbf{C}_p)$ for the set of isomorphism classes of elliptic curves over $\mathbf{C}_p$ with the property that their reduction is an element of $\mathrm{Ell}_D(\mathbf{F}_p)$. Then $X_D(\mathbf{C}_p)$ is a p-adic analytic space, as the j-invariant identifies it with a subset of $\mathbf{C}_p$. It consists of $h(D)$ discs of p-adic radius 1. Each disc contains exactly one element of $\mathrm{Ell}_D(\mathbf{Q}_p)$, and this is the subset of $\mathbf{C}_p$ we want to compute. It consists of the (j-invariants of the) isomorphism classes of elliptic curves in $X_D(\mathbf{C}_p)$ having CM with $\mathcal{O}_D$.

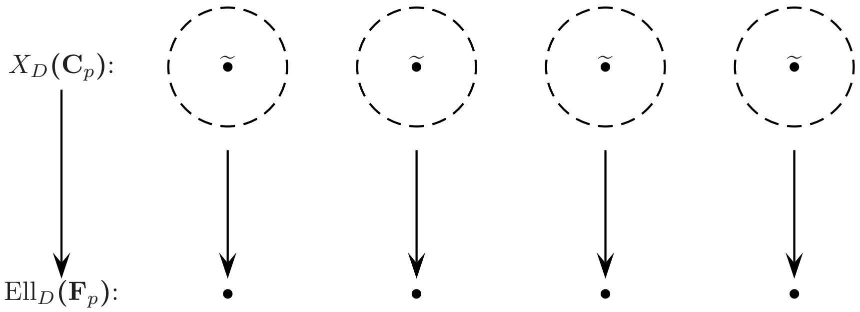
Let $I \subset \mathcal{O}_D$ be an $\mathcal{O}_D$-ideal prime to p and $E/\mathbf{F}_p$ an elliptic curve in $\mathrm{Ell}_D(\mathbf{F}_p)$. Then there is a separable isogeny $E \to E_I$ which has the subgroup $E[I]$ of I-torsion points of E as its kernel. In this way, we obtain a bijection $\bar{\rho}_I : \mathrm{Ell}_D(\mathbf{F}_p) \to \mathrm{Ell}_D(\mathbf{F}_p)$ that sends the isomorphism class of E to that of E_I. We obtain an action of the group $I(p)$ of $\mathcal{O}_K$-ideals prime to p on $\mathrm{Ell}_D(\mathbf{F}_p)$, and since principal $\mathcal{O}_K$-ideals act trivially, this action factors via the quotient map $I(p) \twoheadrightarrow \mathrm{Cl}(D)$. This makes $\mathrm{Ell}_D(\mathbf{F}_p)$ into a principal homogeneous $\mathrm{Cl}(D)$-space.

The fundamental idea in [3] is that the action of $I(p)$ on $\mathrm{Ell}_D(\mathbf{F}_p)$ admits a natural lift to an action of $I(p)$ on $X_D(\mathbf{C}_p)$. More precisely, for $I \in I(p)$ the map $\rho_I : X_D(\mathbf{C}_p) \to X_D(\mathbf{C}_p)$ is a p-adic analytic map that lifts $\bar{\rho}_I$ in the sense that on $\mathrm{Ell}_D(\mathbf{Q}_p) \subset X_D(\mathbf{C}_p)$, the restriction of ρ_I is the standard Galois action that factors via $\mathrm{Cl}(D)$. If $I = (\alpha)$ is principal with $\alpha \in \mathcal{O}_D \setminus \mathbf{Z}$, then $\rho_\alpha = \rho_I$ stabilizes each disk around a CM-point in $\mathrm{Ell}_D(\mathbf{Q}_p)$, and has the CM-point in the disk as its unique fixed point.

It is shown in [3] that the derivative of the map ρ_α in a point of $\mathrm{Ell}_D(\mathbf{Q}_p)$ equals $\alpha/\bar{\alpha}$, and this can be used to compute the j-invariant of a CM-point in $\mathrm{Ell}_D(\mathbf{Q}_p)$ starting from an arbitrary point in the disk using a Newton iteration process. If E_1 is any lift of E to $\mathbf{C}_p$, we put

$$j(E_{k+1}) = j(E_k) - \frac{j(\rho_\alpha(E_k)) - j(E_k)}{(\alpha/\bar{\alpha}) - 1} \qquad \text{for } k \in \mathbf{Z}_{\geq 1}. \tag{1}$$

If α is small with respect to p, then $(\alpha/\bar{\alpha}) - 1$ is a unit in $\mathbf{Z}_p$ and the sequence (1) converges to the j-invariant of the canonical lift $\tilde{E}$. In each step, the p-adic precision of the approximation is doubled.



For the definition of ρ_I on the isomorphism class of E' in $X_D(\mathbf{C}_p)$, we note that the subgroup $E[I]$ of I-torsion points of the reduction $E/\mathbf{F}_p$ of E' lifts canonically to a subgroup $E'[I]$ of E', and we put $\rho_I(E') = E'_I$, with $E \to E'_I$ the isogeny with kernel $E'[I]$. This provides a lift of $E[I]$ to a *group scheme* over the p-adic disk in $X_D(\mathbf{C}_p)$ lying over $[E] \in \mathrm{Ell}_D(\mathbf{F}_p)$. More algorithmically, if E is given by a Weierstrass model, the subgroup $E[I]$ can be described by a separable polynomial $\bar{f}_I \in \mathbf{F}_p[X]$ having the x-coordinates of the affine points in $E[I]$ as its zeroes. If I has norm n, then $p \nmid n$ and $\bar{f}_I$ divides the n-th division polynomial of E in $\mathbf{F}_p[X]$. Choosing a Weierstrass model for E' reducing to that for E, we can lift $\bar{f}_I$ uniquely by Hensel's lemma to a factor f_I of the n-th division polynomial of E', and this factor describes the subgroup $E'[I]$. Note that ρ_I is the identity on $X_D(\mathbf{C}_p)$ if I is generated by an integer, and that, consequently, $\rho_{\bar{I}}$ is the inverse of ρ_I.

For the explicit computation of $\rho_\alpha(E')$, we take an element $\alpha = a + b\pi_p$ in $\mathcal{O}_D \setminus \mathbf{Z}$ that is sufficiently smooth, i.e., a product of $\mathcal{O}_D$-ideals $L = (\ell, a + b\pi_p)$ of small prime norm $\ell \neq p$. Such an element is found by sieving in the set

$$\{a + b\pi_p : a, b \in \mathbf{Z}, b \neq 0, (a, b) = 1\}.$$

Again, the smoothness properties are in practice much better than what can be rigorously proved [3]. For the computation of $\rho_L(E')$, we first compute the action of $\bar{\rho}_L$ on the reduction $E = \bar{E}' \in \mathrm{Ell}_D(\mathbf{F}_p)$, i.e., the j-invariant of $E_L = \bar{E}'_L$. The kernel $E[L]$ of the isogeny $E \to E_L$ is a cyclic subgroup of order ℓ of $E[\ell]$ that is an eigenspace of the Frobenius morphism with eigenvalue $-b/a \in \mathbf{F}_\ell$. The corresponding polynomial $\bar{f}_L \in \mathbf{F}_p[X]$ can be computed by the techniques used by Atkin and Elkies to improve Schoof's original point counting algorithm, see [9]. These techniques also yield a Weierstrass model for E_L; we only need the j-invariant $j(E_L) \in \mathbf{F}_p$ of $E_L = \bar{\rho}_L(E)$. From the decomposition of ρ_α into 'prime degree' maps ρ_L, we obtain a *cycle* of isogenies

$$E \xrightarrow{\bar{\rho}_{L_1}} E_{L_1} \xrightarrow{\bar{\rho}_{L_2}} E_{L_1 L_2} \longrightarrow \ldots \xrightarrow{\bar{\rho}_{L_t}} E_{(\alpha)} = E. \tag{2}$$

To compute the action of L on the lift E' of E, we do *not* lift $\bar{f}_L$ to some precision to a divisor of the ℓ-th division polynomial of E', and then find a

Weierstrass model and the j-invariant for E_L using Vélu's formulas. As the division polynomial has degree $(\ell^2-1)/2$ for $\ell > 2$, this would be rather time-consuming. Instead, we exploit the ℓ-th modular polynomial $\Phi_\ell(X,Y) \in \mathbf{Z}[X,Y]$, which is of degree $\ell+1$ in each of the variables, and which we can precompute for a number of small primes ℓ. As there is an isogeny $E' \to E'_L$ of degree ℓ, we know that $j(E'_L)$ is a zero of $\Phi_\ell(j(E'),Y) \in \mathbf{Z}_p[Y]$. Since we know the j-invariant of the reduction of E'_L, we also know which root to approximate in $\mathbf{Z}_p$, and this reduces the lifting process to a simple Hensel lift of a zero of a polynomial of degree $\ell+1$.

For our Newton process in (1), we start from $E \in \mathrm{Ell}_D(\mathbf{F}_p)$, and compute the cycle of $\mathbf{F}_p$-isogenies in (2). We then lift E arbitrarily to a curve E_1 over $\mathbf{Q}_p$, the '1 digit precision' approximation of the canonical lift. Now we compute lifts over $\mathbf{Q}_p$ of our $\mathbf{F}_p$-isogenies in 2 digit precision, using the modular polynomials, and use the value of $\rho_\alpha(E_1)$ obtained to update E_1 as in (1) to a 2 digit precision approximation E_2 of the canonical lift. We continue this process of making (not really closed) cycles over $\mathbf{Q}_p$, doubling the precision of the computation at each step, until we have the canonical lift with high enough accuracy (see [2] for an estimate of the required accuracy).

If we know the canonical lift $\tilde{E}$, we compute its Galois conjugates again via the modular polynomials. For this, we need small primes L that generate the class group. Under GRH, this can be done using primes L not exceeding the Bach bound $6\log^2(|D|)$, see [2]. In practice, this is never a problem. If we have all the conjugates to the required precision, we find by simple expansion of the product below the class polynomial

$$F_D = \prod_{[I]\in \mathrm{Cl}(D)} (X - j(\tilde{E}_I)) \in \mathbf{Z}[X].$$

4 An elliptic curve for ANTS 6

We illustrate the working of our p-adic method by computing a tailor made elliptic curve for ANTS 6 having exactly $N = 2004061320040618$ points.

First we look for a small discriminant, so we write $N = q+1-t$ for various primes q and search for a large square dividing $\Delta = t^2-4q$. In this example, the choice

$$N = 2004061230508291 + 1 + 89532326$$

yields $\Delta = -2^3 \cdot 3 \cdot 619^2 \cdot 22567$, so we take $D = -2^3 \cdot 3 \cdot 22567 = -541608$ in this section. The corresponding class group $\mathrm{Cl}(D)$ has order 132.

Our goal is to compute the class polynomial F_D. We will do this p-adically, so we first find an elliptic curve over some $\mathbf{F}_p$ which has CM with $\mathcal{O}_D$. The smallest integer $s > 0$ for which $(s^2-D)/4$ is prime is $s = 2$, so we have $D = 2^2 - 4p$ with $p = 135403$. We fix this value of p for the rest of this section.

We now apply the naive method to find a curve $E_a:\ y^2 = x^3 + ax - a$ over $\mathbf{F}_p$ with trace of Frobenius 2. We find that E_{1737} has trace 2 and take this as our base curve $E/\mathbf{F}_p$.

Next we determine which element $\alpha \in \mathcal{O}_D \setminus \mathbf{Z}$ we will use for the map ρ_α. The ideal $(\alpha) = (22539 + 4\pi_p)$ of norm $510353281 = 19^2 \cdot 29^2 \cdot 41^2$ factors as

$$(\alpha) = L_{19}^2 \cdot L_{29}^2 \cdot L_{41}^2 = (19, \pi_p + 6)^2 \cdot (29, \pi_p - 13)^2 \cdot (41, \pi_p - 13)^2.$$

We compute the action for the prime ideal L_{19}. The eigenvalue of the action of Frobenius on the 19-torsion is $-6 \in \mathbf{F}_{19}$. If we evaluate the modular polynomial $\Phi_{19}(X,Y)$ in $X = j(E) = 41556 \in \mathbf{F}_p$, we get a polynomial which has two roots over $\mathbf{F}_p$, namely 19533 and 54827. From this we deduce that L_{19} sends $j(E)$ to one of these two roots; we don't know which one yet.

We just *guess* that the correct j-invariant is $54827 \in \mathbf{F}_p$. Following Elkies, we now compute the eigenspace S of the 19-torsion corresponding to this isogeny. We get the x-coordinates of the points on E in S as zeroes of

$$\begin{aligned}\bar{f}_{L_{19}} = X^9 &+ 29873X^8 + 49874X^7 + 131130X^6 + 49222X^5 + 46538X^4 + \\ &111513X^3 + 68602X^2 + 126444X + 20947 \in \mathbf{F}_p[X]\end{aligned}$$

Since we know that the eigenvalue for L_{19} is -6, we can now just check whether

$$(X^p, Y^p) = -6 \cdot (X, Y)$$

holds for points in S, i.e., we compute both (X^p, Y^p) and $-6 \cdot (X,Y)$ in the ring

$$\mathbf{F}_p[X,Y]/(\bar{f}_{L_{19}}(X), Y^2 - X^3 + 1737X - 1737).$$

Note that the $\cdot$ means adding *on the curve*! In this example, it turns out that (X^p, Y^p) and $-6 \cdot (X,Y)$ are not the same. It follows that the correct j-invariant of the L_{19}-isogenous curve is the other value $19533 \in \mathbf{F}_p$.

The action of L_{19} on the curve with j-invariant 19533 is now easier to compute: the modular polynomial has again two roots, but one of the roots has to be $j(E)$. This root corresponds to the action of $\bar{L}_{19}$, so we pick the other root. If we compute the entire cycle corresponding to L, we get:

$$41556 \xrightarrow{L_{19}} 19533 \xrightarrow{L_{19}} 100121 \xrightarrow{L_{29}} 86491 \xrightarrow{L_{29}} 40349 \xrightarrow{L_{41}} 32517 \xrightarrow{L_{41}} 41556.$$

We now lift $E/\mathbf{F}_p$ to $E_1/\mathbf{Q}_p$ by lifting the coefficients of the Weierstrass equation arbitrarily. The polynomial $\Phi_{19}(j(E_1), Y) \in \mathbf{Z}_p[Y]$ has exactly two roots, one of which reduces to 19533 modulo p. We compute this root, which is the value of the L_{19}-action on $j(E_1)$, to two p-adic digits of precision. We continue to lift the whole cycle to two p-adic digits of precision, and update $j(E_1)$ according to formula (1) to obtain $j(E_2)$. Starting from $j(E_2)$, we now lift the cycle to four p-adic digits of precision, compute $j(E_3)$ from this, and so on. We obtain

$$\begin{aligned}j(\tilde{E}) &= 41556 + O(p) \\ &= 41556 - 17953p + O(p^2) \\ &= 41556 - 17953p - 51143p^2 - 17793p^3 + O(p^4) \\ &= 41556 - 17953p - 51143p^2 - 17793p^3 + 45123p^4 + 52596p^5 + 18237p^6 \\ &\quad +42211p^7 + O(p^8) \\ &= 41556 - 17953p - 51143p^2 - 17793p^3 + 45123p^4 + 52596p^5 + 18237p^6 \\ &\quad +42211p^7 + 45716p^8 + 58788p^9 + 18836p^{10} - 4101p^{11} - 60004p^{12} \\ &\quad -24668p^{13} + 27527p^{14} - 58942p^{15} + O(p^{16}).\end{aligned}$$

From the estimate in [2], we know that we need approximately 3000 decimals of accuracy. As we have $10^{3000} \approx p^{585}$, we compute $j(\tilde{E})$ up to 585 p-adic digits. The class group $\mathrm{Cl}(D) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/66\mathbf{Z}$ is generated by a prime of norm 2 and a prime of norm 29, so we find all 132 conjugates of $j(\tilde{E})$ under $\mathrm{Gal}(H/K)$ up to 585 p-adic digits using the modular polynomials Φ_2 and Φ_{29}. In the end, we expand the polynomial of degree 132 to find the class polynomial

$$F_D = \prod_{[I] \in \mathrm{Cl}(D)} (X - j(\tilde{E}_I)) \in \mathbf{Z}[X]$$

We now compute a root of $F_D \in \mathbf{F}_q$, and note that we can check our computations so far by testing whether F_D splits completely in $\mathbf{F}_q[X]$. One of the 132 roots is $j = 5215470850369 \in \mathbf{F}_q$, and an elliptic curve with this j-invariant is $E_a :\ y^2 = x^3 + ax - a$ with $a = 27j/(4(1728 - j)) = 1460967812073632 \in \mathbf{F}_q$. We know that E_a has CM with $\mathcal{O}_D$ and that its trace of Frobenius equals $\pm t$. To test whether it actually equals t, we look at the order of $P = (1, 1) \in E_a(\mathbf{F}_q)$. We see that $(q + 1 + t)P \neq O = (q + 1 - t)P$, so E_a must have trace equal to t. We conclude that the curve defined by

$$y^2 = x^3 + 1460967812073632x + 543093418434659$$

over $\mathbf{F}_{2004061230508291}$ has exactly 2004061320040618 rational points.

5 Using class invariants

A serious drawback of the complex multiplication method is that it requires the computation of the class polynomial F_D, which grows rapidly in size with D, and is already sizable for moderately small discriminants. Around 1900, Weber [11] computed generating polynomials for Hilbert class fields using the values at CM-points of modular functions of higher level instead of the j-function. These techniques have become important again in an algorithmic context, and many complications from Weber's days are now well understood [4, 10]. The classical theory of class invariants is firmly rooted in complex analytic arguments, but much of it can be made to work in our non-archimedean setting. This section gives an indication of what can be done, leaving a fuller treatment to [1].

The complex multiplication method to compute the class polynomial F_D is based on the fact that its zeroes are the j-invariants of the elliptic curves in characteristic zero having complex multiplication with $\mathcal{O}_D$. In the complex analytic setting, we simply list the complex lattices (up to scaling) giving rise to such curves and compute their j-invariants to sufficient accuracy using the q-expansion of j. In the p-adic setting, we first compute one such curve in the finite set $\mathrm{Ell}_D(\mathbf{F}_p)$. Then we lift the action on $\mathrm{Ell}_D(\mathbf{F}_p)$ of the group $I(p)$ of $\mathcal{O}_D$-ideals prime to p to an action on the set $X(\mathbf{C}_p)$ of their $\mathbf{C}_p$-lifts in such a way that the induced action on the subset $\mathrm{Ell}_D(\mathbf{Q}_p)$ of canonical lifts is the standard Galois action coming from $\mathrm{Cl}(D)$. This enables us to compute the finite subset $\mathrm{Ell}_D(\mathbf{Q}_p) \subset X(\mathbf{C}_p) \xrightarrow{j} \mathbf{C}_p$ in $\mathbf{C}_p$ consisting of the zeroes of F_D. We use a

Newton type lift of our curve in $\mathrm{Ell}_D(\mathbf{F}_p)$ to $\mathrm{Ell}_D(\mathbf{Q}_p)$ together with the explicit Galois action of $\mathrm{Cl}(D)$ on $\mathrm{Ell}_D(\mathbf{Q}_p)$, which we handle by exploiting modular polynomials.

We now want to replace j by modular functions of higher level. These are elements of the modular function field $\mathcal{F} = \bigcup_{n\geq 1} \mathcal{F}_n$ as defined in [6, Chapter 6, Section 3]. Here $\mathcal{F}_n$ denotes the field of modular functions of level n over $\mathbf{Q}$. It can be viewed as the function field of the modular curve $X(n)$ over the cyclotomic field $\mathbf{Q}(\zeta_n)$. Over $\mathcal{F}_1 = \mathbf{Q}(j)$, it is generated by the Fricke functions of level n, which are normalized x-coordinates of n-torsion points on an elliptic curve with j-invariant j.

The modular functions f we use are *integral* over $\mathbf{Z}[j]$, so they are given as the zero of some irreducible polynomial $\Psi_f(X, j) \in \mathbf{Z}[j, X]$. If we specialize j to be the j-invariant of a curve $\tilde{E} \in \mathrm{Ell}_D(\mathbf{Q}_p)$, then the roots of the polynomial $\Psi_f(X, j(\tilde{E})) \in H[X]$, which has integral coefficients, lie in the ray class field H_n of conductor n of $K = \mathbf{Q}(\sqrt{D})$, with n the level of f. It is known that for many choices of 'small' f, one or more of these roots are *class invariants* that actually lie in the Hilbert class field $H = H_1 \subset H_n$ of K. If we can determine which roots end up in H, and compute the explicit Galois action of $\mathrm{Cl}(D)$ on such a root, we can compute its irreducible polynomial over K or $\mathbf{Q}$ just like we did this for j. In the complex analytic setting the tool to perform these tasks is Shimura's reciprocity law [4, 10]. It tells us in which points $\tau \in K \subset \mathbf{H}$ a function f should be evaluated to obtain a class invariant, and describes the conjugates of $f(\tau)$ over K as the values of conjugates of f over $\mathbf{Q}(j)$ in certain other points $\tau' \in K$. These values can be approximated in $\mathbf{C}$ using the q-expansions of f and its conjugates. Once we have computed the irreducible polynomial of $f(\tau)$ over K or $\mathbf{Q}$, one can use the relation $\Psi_f(f(\tau), j(\tau)) = 0$ to obtain information on $j(\tau)$ itself.

In a p-adic setting, we cannot deal with j and f as functions on the complex upper half plane, and the expansion of modular functions as Fourier series in $q = e^{2\pi i\tau}$ has no non-archimedean analogue when dealing as we do with CM-curves, which have integral j-invariants. What we do have is an action from class field theory of the $\mathcal{O}_D$-ideals coprime to n on the roots of $\Psi_f(X, j(\tilde{E})) \in H[X]$ in H_n associated to $j(\tilde{E})$. This action factors via the class group $\mathrm{Cl}(n^2 D)$ of the order of discriminant $n^2 D$, which is a non-maximal order for $n > 1$.

Example 1. The modular function $j : \mathbf{H} \to \mathbf{C}$ has a holomorphic cube root $\gamma_2 : \mathbf{H} \to \mathbf{C}$ that is modular of level 3 and has $\Psi_{\gamma_2}(X, j) = X^3 - j$. It is the unique root of $X^3 - j$ having a rational q-expansion. If D is not divisible by 3 and we write $\mathcal{O}_D = \mathbf{Z}[\tau]$ with $\tau + \bar{\tau} = 0 \bmod 3$, then $\gamma_2(\tau)$ is a class invariant, and its 'size' is only one third of that of $j(\tau)$.

If $\tilde{E} : y^2 = x^3 + ax + b$ is in $\mathrm{Ell}_D(\mathbf{Q}_p)$ and $c_1, \ldots, c_4$ are the 4 roots of its 3-division polynomial, then

$$\frac{-48a}{2a - 3(c_1 c_2 + c_3 c_4)} \tag{3}$$

is a cube root of $j(\tilde{E})$. As there are 3 ways to divide the roots $c_1, \ldots, c_4$ in two sets of two roots each, formula (3) yields 3 distinct cube roots of j. Note that there is no obvious way to single out an expression in (3) as being 'the function' corresponding to γ_2.

If I is an $\mathcal{O}_D$-ideal prime to $3p$, the isogeny $\tilde{E} \to \tilde{E}_I$ induces an isomorphism $\tilde{E}[3] \xrightarrow{\sim} \tilde{E}_I[3]$ on the 3-torsion subgroups, and maps each possible cube root of $j(\tilde{E})$ in (3) to some well-defined cube root of $j(\tilde{E}_I)$. This is the Galois action of the Artin symbol of I, which maps $j(\tilde{E})$ to $j(\tilde{E}_I)$, on these cube roots. It provides an extension of the map $\rho_I : \mathrm{Ell}_D(\mathbf{Q}_p) \to \mathrm{Ell}_D(\mathbf{Q}_p)$ to the set of the cube roots of (the j-invariants of) the elements in $\mathrm{Ell}_D(\mathbf{Q}_p)$. As all these cube roots are p-adically integral, reduction of this map provides an extension of $\bar{\rho}_I : \mathrm{Ell}_D(\mathbf{F}_p) \to \mathrm{Ell}_D(\mathbf{F}_p)$ to the set of cube roots in $\bar{\mathbf{F}}_p$, provided we have $p \neq 3$. In a similar way, we have an extension of the map $\rho_I : X_D(\mathbf{C}_p) \to X_D(\mathbf{C}_p)$ to the set of cube roots.

Example 1 nicely illustrates that the cube roots of j are functions on the modular curve $X(3)$, the points of which can be viewed as isomorphism classes of elliptic curves with complete 3-level structure: in order to have a well defined value not only the j-invariant of the curve but also some 'ordering' of 3-torsion points is required.

As the field $\mathcal{F}_n$ is generated over $\mathbf{Q}(j)$ by Fricke functions, a modular function f of level n is always a rational expression in j and the roots of the n-th division polynomial of a curve with j-invariant j. As in Example 1, the action ρ_I of an $\mathcal{O}_D$-ideal I coprime to pn on $X_D(\mathbf{C}_p)$ naturally maps the roots of $\Psi_f(X, j)$ for $j \in X_D(\mathbf{C}_p)$ to the roots of $\Psi_f(X, \rho_I(j))$. This observation suffices to treat modular functions providing class invariants by p-adic methods similar to that in section 3.

Suppose f is an integral modular function of level n that is known to provide class invariants for $\mathcal{O}_D$ at certain CM-points for $\mathcal{O}_D$ in $\mathbf{H}$. Then we know that for every curve $\tilde{E} \in \mathrm{Ell}_D(\mathbf{Q}_p)$, certain roots of $\Psi_f(X, j(\tilde{E})) \in \mathbf{Q}_p[X]$ are class invariants, so they lie in $\mathbf{Q}_p$. If $E \in \mathrm{Ell}_D(\mathbf{F}_p)$ is the reduction of $\tilde{E}$, then $\Psi_f(X, j(E)) \in \mathbf{F}_p[X]$ will have roots in $\mathbf{F}_p$, and we want to know which roots in $\mathbf{F}_p$ arise as the reduction of class invariants. Let β be a root, and assume for simplicity that $\Psi_f(X, j(E))$ is separable. (This is usually the case in practice as p is not too small, of size $O(D^{1+\varepsilon})$.) The roots of $\Psi_f(X, j(\tilde{E})) \in \mathbf{Q}_p[X]$ all lie in H_n, and they are class invariants exactly when they are fixed by the Galois group

$$\mathrm{Gal}(H_n/H) \cong (\mathcal{O}_D/n\mathcal{O}_D)^*/\mathcal{O}_D^* = \ker[\mathrm{Cl}(n^2D) \to \mathrm{Cl}(D)].$$

It follows that β arises as the reduction of a class invariant if it is fixed by the maps $\bar{\rho}_x : \mathrm{Ell}_D(\mathbf{F}_p) \to \mathrm{Ell}_D(\mathbf{F}_p)$ for a set of generators x of $(\mathcal{O}_D/n\mathcal{O}_D)^*/\mathcal{O}_D^*$. We can compute $\bar{\rho}_x(j(E))$ as before when x is sufficiently smooth, and we need the extension of the action to the roots of $\Psi_f(X, j(E))$. In theory this can be done by working with explicit Weierstrass models and an explicit description of f in terms of n-torsion points as in Example 1. In practice we work with *modular polynomials* for prime degree ℓ isogenies relating the roots of $\Psi_f(X, j_1)$ to that of $\Psi_f(X, j_2)$ when j_1 and j_2 are j-invariants of ℓ-isogenous curves. Such modular polynomials are in many ways similar to the modular polynomials $\Phi_\ell(X,Y)$ arising for the j-function, and they may be found using complex analytic methods involving q-expansions.

Suppose we find that a certain root $\beta \in \mathbf{F}_p$ of $\Psi_f(X, j(E))$ is the reduction of a class invariant $\tilde{\beta}$. Then we lift the *pair* (E,β) to the pair $(\tilde{E},\tilde{\beta})$ consisting of the canonical lift $\tilde{E}/\mathbf{Q}_p$ and the class invariant $\tilde{\beta}$. In theory this can be done by lifting $j(E)$ as in section 3, using cycles of smooth isogenies, and then compute the Hensel lift of β to the root $\tilde{\beta}$. This method makes use of the modular polynomials Φ_ℓ for j, which are big. In many cases the corresponding polynomials Φ_ℓ^f for f are much more pleasant to work with, so it is better to lift isogeny cycles not in terms of j-invariants but in terms of a root of $\Psi_f(X,j)$, and find the resulting j-invariant from its corresponding root.

All that remains is computing the conjugates of the pairs $(\tilde{E},\tilde{\beta})$ under $\mathrm{Cl}(D)$. This is done in exactly the same manner as before, using small primes that generate $\mathrm{Cl}(D)$. We are only interested in the conjugates of $\tilde{\beta}$, so we use the modular polynomials Φ_ℓ^f to compute these conjugates. In the end we expand the polynomial

$$F_D^f = \prod_{[I]\in \mathrm{Cl}(D)} (X - \tilde{\beta}^I) \in \mathbf{Z}[X] \quad (\text{or } \mathcal{O}_D[X].)$$

This polynomial splits again completely in $\mathbf{F}_q[X]$, and from a root in $\mathbf{F}_q$ we compute the corresponding j-value in $\mathbf{F}_q$.

Example 2. We take for f the Weber function $\mathfrak{f}$, which is classically defined on $\mathbf{H}$ in terms of the Dedekind η-function as $\mathfrak{f}(\tau) = \zeta_{48}^{-1}\eta(\frac{\tau+1}{2})/\eta(\tau)$. It is a modular function of level 48 of degree 72 over $\mathbf{Q}(j)$ with

$$\Psi_\mathfrak{f}(X,j) = (X^{24}-16)^3 - jX^{24} \in \mathbf{Z}[j,X].$$

For discriminants $D \equiv 1 \bmod 8$ with $3 \nmid D$, it yields class invariants when evaluated at appropriate points $\tau \in \mathbf{H}$. In other cases small powers of $\mathfrak{f}$ often have the same property [4].

In principle we can express $\mathfrak{f}$ in terms of x-coordinates of 48-torsion points, but there is no need to do this. It suffices to find, for $E/\mathbf{F}_p$ a curve having CM with $\mathcal{O}_D$, first a root $\beta \in \mathbf{F}_p$ of $\Psi_f(X, j(E))$ that is the reduction of a class invariant $\tilde{\beta}$, then a good approximation of the root $\tilde{\beta}$ of $\Psi_\mathfrak{f}(j(\tilde{E}), X)$ in $\mathbf{Q}_p$, and finally good approximations in $\mathbf{Q}_p$ of the conjugates of $\tilde{\beta}$ under $\mathrm{Cl}(D)$. These questions ultimately reduce to computing the action of an ideal L of prime norm $\ell \nmid pn$ on pairs (E',β'), with E' in $X_D(\mathbf{C}_p)$ or $\mathrm{Ell}_D(\mathbf{F}_p)$ and β' a root of $\Psi_f(X, j(E')$ in $\mathbf{Q}_p$ or $\mathbf{F}_p$. For E' we know how to compute $j(\tilde{E}'_L)$, for $(\beta')^L$ we use the fact that it is a zero of the modular polynomial $\Phi_\ell^\mathfrak{f}(\beta', X)$ *and* of $\Psi_\mathfrak{f}(X, j(E'_L))$. Usually there are only two roots $\Phi_\ell^\mathfrak{f}(\beta', X)$ that we need to consider, the correct one and the image under the action of $\bar{L}$. It is of great help that the modular polynomials $\Phi_\ell^\mathfrak{f}$ are quite a bit smaller than the classical modular polynomials for j. For small ℓ they are really small, like

$$\Phi_5^\mathfrak{f}(X,Y) = (X^5 - Y)(X - Y^5) + 5XY$$
$$\Phi_7^\mathfrak{f}(X,Y) = (X^7 - Y)(X - Y^7) + 7(XY - X^4Y^4).$$

For $\ell = 13$ it takes at least two of these pages to write down Φ_ℓ, but we have

$$\begin{aligned}\Phi_{13}^{\mathfrak{f}}(X,Y) = {} & (X^{13}-Y)(X-Y^{13}) + 5\cdot 13XY \\ & +13(X^2Y^{12} + X^{12}Y^2 + 4X^{10}Y^4 + 4X^{10}Y^4 + 6X^6Y^8 + 6X^8Y^6).\end{aligned}$$

6 An elliptic curve having 10^{30} points.

We illustrate the power of the method presented in the previous section by constructing an elliptic curve having exactly $N = 10^{30}$ rational points.

Just as in section 4, we first look for a suitable discriminant. We write $N = q + 1 - t$, and by looking at $|t|$ slightly less than $2\sqrt{N} = 2 \cdot 10^{15}$, we find that for trace $t = 1999999999167682$ the number $q = 10^{30} + t - 1$ is prime and

$$\Delta = t^2 - 4q = -2^{12} \cdot 3^2 \cdot 5^2 \cdot 17^2 \cdot 367^2 \cdot 3943 \cdot 23537$$

has a large square factor leading to $D = -92806391$. The corresponding class group $\mathrm{Cl}(D)$ has order 15610. Computing the Hilbert class polynomial for our D would require an accuracy of 313618 decimals, which is clearly not practical.

Instead, we notice that we have $D \equiv 1 \bmod 8$ and $D \not\equiv 0 \bmod 3$, so we can use the classical Weber function $\mathfrak{f}$ to compute a class polynomial for $H(K)$. We first compute an elliptic curve in $\mathrm{Ell}_D(\mathbf{F}_p)$ for a 'small' prime p. We have $D \equiv 1 \bmod 8$, and the smallest $s \in \mathbf{Z}_{>0}$ with $p = (s^2 - 4D)/4$ prime is $s = 132$, leading to $p = 92810747$. The first curve $E_a/\mathbf{F}_p$ of trace 132 we encounter is $E_{1086} : y^2 = x^3 + 1086x - 1086$ of j-invariant 37202456. As E has all three of its two-torsion points defined over $\mathbf{F}_p$, its endomorphism ring is $\mathcal{O}_D$, not $\mathcal{O}_{4D}$.

We now have to determine which root β of the polynomial $\Psi_{\mathfrak{f}}(X, j(E)) = (X^{24} - 16)^3 - j(E)X^{24} \in \mathbf{F}_p[X]$ is the reduction of a *class invariant* $\tilde{\beta} \in \mathbf{Z}_p$. We are lucky since ± 21677132 are the only two roots in $\mathbf{F}_p$. Since $-\tilde{\beta}$ is also a class invariant, it does not matter which root we pick. We take $\beta = 21677132$.

For the smooth ideal inducing ρ_α we pick $(\alpha) = (-420 + \pi_p)$, which factors as

$$(11, 8 + 2\pi_p) \cdot (17, 4 + 2\pi_p)^2 \cdot (23, 16 + 2\pi_p)^2 \cdot (31, 13 + 2\pi_p) \cdot (41, 30 + 2\pi_p).$$

Just as in section 4, we compute the cycle in $\mathbf{F}_p$ for the *j-invariants*:

$$37202456 \xrightarrow{L_{11}} 4967239 \xrightarrow{L_{17}} \cdots \xrightarrow{L_{31}} 21402782 \xrightarrow{L_{41}} 37202456.$$

Using this cycle, we can also compute the cycle for β. For instance, the modular polynomial $\Phi_{11}^{\mathfrak{f}}(\beta, Y) \in \mathbf{F}_p[Y]$ has two roots: 32604444 and 60476019. In order to determine which root to take, we note that β is a root of $\Psi_{\mathfrak{f}}(X, j(E_{L_{11}})) = (X^{24} - 16)^3 - j(E_{L_{11}})X^{24} \in \mathbf{F}_p[X]$. We find that 60476019 is the root we need. Continuing like this, we get the following cycle for β in $\mathbf{F}_p$:

$$21677132 \xrightarrow{L_{11}} 60476019 \xrightarrow{L_{17}} \cdots \xrightarrow{L_{31}} 53004472 \xrightarrow{L_{41}} 21677132.$$

Just as in section 4, we lift $E/\mathbf{F}_p$ to $E_1/\mathbf{Q}_p$ by lifting the coefficients of its Weierstrass equation. We could now compute the canonical lift $\tilde{E}$ in two p-adic digits just like we did in section 4, and use that information to compute $\tilde{\beta} \in \mathbf{Z}_p$ in two p-adic digits accuracy. Indeed, $\tilde{\beta}$ is a root of $\Psi_{\mathfrak{f}}(X, j(\tilde{E})) \in \mathbf{Z}_p[X]$, and since we have $(\tilde{\beta} \bmod p) = \beta$, this root is just a Hensel lift of β. This approach has the disadvantage that we have to use modular polynomials for the j-function.

Instead, we lift β to a root β_1 of $\Psi_{\mathfrak{f}}(X, j(E_1)) \in \mathbf{Z}_p[X]$. Now we lift the cycle that we had for $\beta \in \mathbf{F}_p$ to a cycle for $\beta_1 \in \mathbf{Z}_p$ by applying the small modular polynomials for $\mathfrak{f}$ once more. Since we know that $\beta_1^{(\alpha)}$ is a root of $\Psi_{\mathfrak{f}}(X, j(E_1^{(\alpha)}))$, we can compute

$$j(E_1^{(\alpha)}) = \frac{((\beta_1^{(\alpha)})^{24} - 16)^3}{(\beta_1^{(\alpha)})^{24}}$$

and use this value to update $j(E_1)$ as in formula (1) to a value of the j-invariant of the canonical lift $\tilde{E}$ that is accurate to two p-adic digits. Knowing $j(\tilde{E}) \bmod p^2$, we can lift $\beta \in \mathbf{F}_p$ to a root of $\Psi_{\mathfrak{f}}(X, j(\tilde{E}))$ in $\mathbf{Z}_p$ that is accurate to two p-adic digits. We continue this process of doubling the precision until we have $\tilde{\beta}$ with sufficient accuracy. The first four cycles yield:

$$\begin{aligned}
\tilde{\beta} &= 21677132 + O(p) \\
&= 21677132 + 28966941p + O(p^2) \\
&= 21677132 + 28966941p + 7010373p^2 + 31182954p^3 + O(p^4) \\
&= 21677132 + 28966941p + 7010373p^2 + 31182954p^3 - 33808617p^4 \\
&\quad + 27519307p^5 - 31601027p^6 - 36195013p^7 + O(p^8) \\
&= 21677132 + 28966941p + 7010373p^2 + 31182954p^3 - 33808617p^4 \\
&\quad + 27519307p^5 - 31601027p^6 - 36195013p^7 - 8331811p^8 \\
&\quad - 33957007p^9 - 18191700p^{10} + 5895954p^{11} - 42670221p^{12} \\
&\quad + 23637278p^{13} - 40784695p^{14} + 7754196p^{15} + O(p^{16}).
\end{aligned}$$

We expect to need $\lceil 313618/72 \rceil = 4356$ decimals of accuracy, so we compute $\tilde{\beta}$ upto 550 p-adic digits. The class group $\mathrm{Cl}(D)$, which is cyclic of order 15610, is generated by a prime of norm 11. We can thus compute all the conjugates of $\tilde{\beta}$ under $\mathrm{Gal}(H/K)$ to 550 p-adic digits using the modular polynomial $\Phi_{11}^{\mathfrak{f}}$. In the end, we expand the polynomial of degree 15610 to find the class polynomial

$$F_D^{\mathfrak{f}} = \prod_{[I] \in \mathrm{Cl}(D)} (X - \tilde{\beta}^I) \in \mathbf{Z}[X],$$

which we reduce modulo q to compute a root $\gamma \in \mathbf{F}_q$. From γ, we compute the corresponding j-value and write down a curve $\bar{E}$ with that j-invariant. We then know that $\bar{E}$ has CM with $\mathcal{O}_D$, but we still need to check whether the trace really equals t. This turns out not to be the case, so we conclude that the quadratic twist of $\bar{E}$, given by

$$y^2 = x^3 + 669397215131271955483581235905x + 363369366443977510319399421188$$

over $\mathbf{F}_q$, with $q = 10^{30} + 1999999999167681$, has exactly 10^{30} rational points. Checking that this curve indeed has the required number of points is an easy matter for the current point counting algorithms.

References

[1] Bröker, R.: Thesis, Universiteit Leiden, in preparation.
[2] Cohen, H.: A course in computational algebraic number theory, Springer Lecture Notes in Mathematics 138, (1993)
[3] Couveignes, J.-M. and Henocq, T.: Action of modular correspondences around CM points, Algorithmic Number Theory Symposium V. (2002)
[4] Gee, A.: Class invariants by Shimura's reciprocity law, Journal de Théorie des Nombres de Bordeaux **11**, (1999), 45–72
[5] Kedlaya, K.: Counting Points on Hyperelliptic Curves using Monsky-Washnitzer Cohomology, Journal Ramanujan Mathematical Society **16**, (2002) 323–338
[6] Lang, S.: Elliptic functions, 2nd edition Springer Lecture Notes in Mathematics 112, (1987)
[7] Satoh, T.: The canonical lift of an ordinary elliptic curve over a finite field and its point counting, Journal Ramanujan Mathematical Society **15**, (2000) 247-270
[8] Schoof, R.: Elliptic Curves over Finite Fields and the Computation of Square Roots mod p, Mathematics of Computation **44**, (1985) 483–494
[9] Schoof, R.: Counting points on elliptic curves over finite fields, Journal de Théorie des Nombres de Bordeaux **7**, (1995) 219–254
[10] Stevenhagen, P.: Hilbert's 12th problem, complex multiplication and Shimura reciprocity Class field theory—its centenary and prospect (Tokyo, 1998) Adv. Stud. Pure Math., **30**, Math. Soc. Japan, (2001) 161–176
[11] Weber, H.: Lehrbuch der Algebra, Vol. III. Chelsea reprint, original edition 1908