Journal de Théorie des Nombres
de Bordeaux **7** *(1995), 219–254*

Counting points on elliptic curves over finite fields

par René SCHOOF

Abstract. –We describe three algorithms to count the number of points on an elliptic curve over a finite field. The first one is very practical when the finite field is not too large; it is based on Shanks's baby-step-giant-step strategy. The second algorithm is very efficient when the endomorphism ring of the curve is known. It exploits the natural lattice structure of this ring. The third algorithm is based on calculations with the torsion points of the elliptic curve [18]. This deterministic polynomial time algorithm was impractical in its original form. We discuss several practical improvements by Atkin and Elkies.

1. Introduction.

Let p be a large prime and let E be an elliptic curve over $\mathbf{F}_p$ given by a Weierstraß equation

$$Y^2 = X^3 + AX + B$$

for some A, $B \in \mathbf{F}_p$. Since the curve is not singular we have that $4A^3 + 27B^2 \not\equiv 0 \pmod{p}$. We describe several methods to count the rational points on E, i.e., methods to determine the number of points (x, y) on E with $x, y \in \mathbf{F}_p$. Most of what we say applies to elliptic curves over any finite base field. An exception is the algorithm in section 8.

In this paper we merely report on work by others; these results have not been and will not be published by the authors themselves. We discuss an algorithm due to J.-F. Mestre, an exposition of Cornacchia's algorithm due to H.W. Lenstra and recent work by A.O.L. Atkin and N.D. Elkies.

Let $E(\mathbf{F}_p)$ denote the set of rational points of E. It is easy to see that the number of points in $E(\mathbf{F}_p)$ with given X-coordinate $x \in \mathbf{F}_p$ is 0, 1 or 2. More precisely, there are

$$1 + \left(\frac{x^3 + Ax + B}{p}\right)$$

Manuscrit reçu le le 21 mars 1994.

rational points on E with X-coordinate equal to x. Here $\left(\frac{\cdot}{p}\right)$ denotes the quadratic residue symbol. Including the point at infinity, the set of rational points $E(\mathbf{F}_p)$ of E therefore has cardinality

$$1+\sum_{x\in\mathbf{F}_p}\left(1+\left(\frac{x^3+Ax+B}{p}\right)\right)=1+p+\sum_{x\in\mathbf{F}_p}\left(\frac{x^3+Ax+B}{p}\right).$$

This implies that evaluating the sum

$$\sum_{x\in\mathbf{F}_p}\left(\frac{x^3+Ax+B}{p}\right)$$

is the same problem as computing $\#E(\mathbf{F}_p)$.

For very small primes ($p<200$ say) a straightforward evaluation of this sum is an efficient way to compute $\#E(\mathbf{F}_p)$. In practice it is convenient to make first a table of squares modulo p and then count how often x^3+Ax+B is a square for $x=0, 1, \ldots, p-1$. The running time of this algorithm is $O(p^{1+\varepsilon})$ for every $\varepsilon>0$.

For larger p, there are better algorithms. In section 2 we discuss an algorithm based on Shanks's baby-step-giant-step strategy. Its running time is $O(p^{1/4+\varepsilon})$ for every $\varepsilon>0$. This algorithm is practical for somewhat larger primes; it becomes impractical when p has more than, say, 20 decimal digits. In section 3 we explain a clever trick due to J.-F.Mestre [6, Alg.7.4.12] which simplifies certain group theoretical computations in the baby-step-giant-step algorithm. This version has been implemented in the PARI computer algebra package [4].

In section 4 we discuss an algorithm to count the number of points on an elliptic curve E over $\mathbf{F}_p$, when the endomorphism ring of E is known. It is based on the usual reduction algorithm for lattices in $\mathbf{R}^2$. We discuss Cornacchia's related algorithm [7] and H.W. Lenstra's proof [15] of its correctness.

In section 5 we discuss a deterministic polynomial time algorithm to count the number of points on an elliptic curve over a finite field [18]. It is based on calculations with torsion points. The running time is $O(\log^8 p)$, but the algorithm is not very efficient in practice. In sections 6, 7 and 8 we explain practical improvements by A.O.L. Atkin [1, 2] and N.D. Elkies [10]. These enabled Atkin in 1992 to compute the number of points on the curve

$$Y^2=X^3+105X+78153$$

modulo the the smallest 200 digit prime:

10000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000153.

The result is

10000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000
06789750288004224118080314365460277641928049641888
39991591392960032210630561760029050858613689631753.

The curve is "random" in the sense that it was inspired by the address of the INRIA institute: Domaine de Voluceau – Rocquencourt, B.P. 105, 78153 Le Chesnay cedex. See the papers by Morain and Couveignes [8,17] and by Lehmann et al. [13] for even larger examples.

There are several unsolved computational problems concerning elliptic curves over finite fields. There is, for instance, no efficient algorithm known to find the Weierstraß equation of an elliptic curve over $\mathbf{F}_p$ with a given number of rational points. The problem of efficiently computing the *structure* of the group of points over a finite field, or, more generally, the problem of determining the endomorphism ring of a given elliptic curve, is also very interesting.

Finally, Elkies's improvement, explained in sections 7 and 8, applies only to half the primes l: those for which the Frobenius endomorphism acting on the l-torsion points, has its eigenvalues in $\mathbf{F}_l$. It would be very interesting to extend his ideas to the remaining l.

Recently the methods of section 8 have been extended by J.-M. Couveignes [9] to large finite fields of small characteristic, in particular to large finite fields of characteristic 2. This problem first came up in cryptography [16]. Couveignes exploits the formal group associated to the elliptic curve.

I would like to thank J.-M. Couveignes, D. Kohel and H.W. Lenstra for their comments on earlier versions of this paper.

2. Baby steps and giant steps.

In this section we explain the baby-step-giant-step algorithm to compute the number of points on an elliptic curve E over $\mathbf{F}_p$ given by $Y^2 = X^3 + AX + B$. The most important ingredient is the fact that the set of points $E(\mathbf{F}_p)$ forms an additive group with the well-known chord and tangent method:

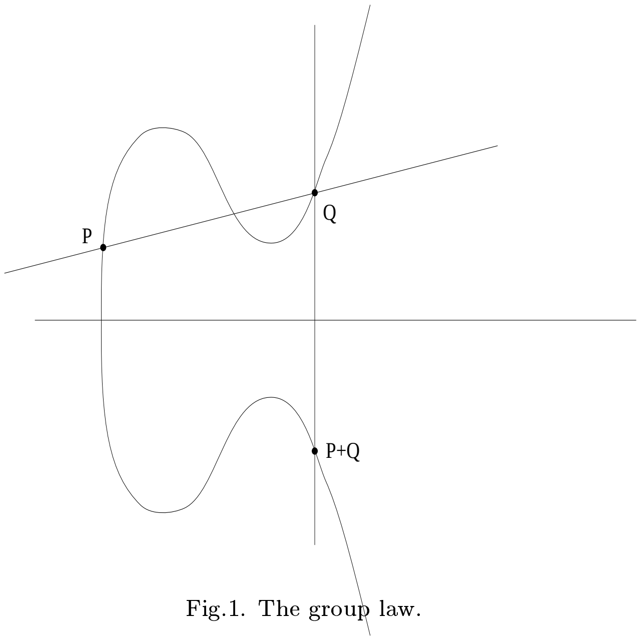

Fig.1. The group law.

The point at infinity $(0:1:0)$ is the neutral element of this group. The opposite of a point $P = (x_1, y_1)$ is the point $(x_1, -y_1)$. It is very easy to derive explicit formulas for the addition of points: if $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are two points with $Q \neq -P$, then their sum is (x_3, y_3) where

$$x_3 = -x_1 - x_2 + \lambda^2,$$
$$y_3 = \lambda(x_1 - x_3) - y_1.$$

Here λ is the slope of the line through P and Q. We have $\lambda = (y_2 - y_1)/(x_2 - x_1)$ if $P \neq Q$ and $\lambda = (3x_1^2 + A)/2y_1$ otherwise.

The following result, the analogue of the Riemann Hypothesis, gives an estimate for the order of the group $\#E(\mathbf{F}_p)$.

Theorem 2.1. *(H. Hasse, 1933) Let p be a prime and let E be an elliptic curve over $\mathbf{F}_p$. Then*

$$|p+1-\#E(\mathbf{F}_p)| < 2\sqrt{p}.$$

Proof. See [21].

The groups $E(\mathbf{F}_p)$ "tend" to be cyclic. Not only can they be generated by at most two points, but for any prime l, the proportion of curves E over $\mathbf{F}_p$ with the l-part of $E(\mathbf{F}_p)$ not cyclic does, roughly speaking, not exceed $1/l(l^2-1)$.

The idea of the algorithm is to pick a random point $P \in E(\mathbf{F}_p)$ and to compute an integer m in the interval $(p+1-2\sqrt{p}, p+1+2\sqrt{p})$ such that $mP = 0$. If m is the *only* such number in the interval, it follows from Theorem 2.1 that $m = \#E(\mathbf{F}_p)$.

To pick the point $P = (x, y)$ in $E(\mathbf{F}_p)$ one just selects random values of x until $x^3 + Ax + B$ is a square in $\mathbf{F}_p$. Then compute a square root y of $x^3 + Ax + B$. See [20] and [6, Alg.1.5.1] for efficient practical methods to compute square roots mod p.

The number m is computed by means of the so-called baby-step-giant-step strategy due to D. Shanks [19]; see also [6, Alg.5.4.1]. His method proceeds as follows. First make the *baby steps:* make a list of the first $s \approx \sqrt[4]{p}$ multiples $P, 2P, 3P, \ldots, sP$ of the point P. Note that, since the inverse of a point is obtained by inverting the sign of its Y-coordinate, one actually knows the coordinates of the $2s+1$ points: $0, \pm P, \pm 2P, \ldots, \pm sP$.

Next compute $Q = (2s+1)P$ and compute, using the binary expansion of $p+1$, the point $R = (p+1)P$. Finally make the *giant steps:* by repeatedly adding and subtracting the point Q compute $R, R \pm Q, R \pm 2Q, \ldots, R \pm tQ$. Here $t = [2\sqrt{p}/(2s+1)]$, which is approximately equal to $\sqrt[4]{p}$. By Theorem 2.1, the point $R + iQ$ is, for some integer $i = 0, \pm 1, \pm 2, \ldots, \pm t$ equal to one of the points in our list of baby steps: for this i one has that

$$R + iQ = jP \qquad \text{for some } j \in \{0, \pm 1, \pm 2, \ldots, \pm s\}.$$

Putting $m = p + 1 + (2s+1)i - j$, we have $mP = 0$. This completes the description of the algorithm.

It is important that one can efficiently search among the points in the list of baby steps; one should sort this list or use some kind of hash coding. It is not difficult to see that the running time of this algorithm is $O(p^{1/4+\varepsilon})$

for every $\varepsilon > 0$. The algorithm fails if there are two distinct integers m, m' in the interval $(p+1-2\sqrt{p}, p+1+2\sqrt{p})$ with $mP = m'P = 0$. This rarely happens in practice. If it does, then $(m-m')P = 0$ and one knows, in fact, the order d of P. Usually it suffices to repeat the algorithm with a second random point. The fact that, this time, one knows that d divides $\#E(\mathbf{F}_p)$ usually speeds up the second computation considerably.

Very rarely the algorithm is doomed to fail because there is for every point P more than one m in the interval $(p+1-2\sqrt{p}, p+1+2\sqrt{p})$ for which $mP = 0$. This happens when the exponent of the group $E(\mathbf{F}_p)$ is very small. Although writing a program that covers these rare exceptional cases is somewhat painful, these are not very serious problems; one can compute independent generators for the group, ... etc. In the next section we discuss Mestre's elegant trick to avoid these complications.

3. Mestre's algorithm.

We explain an idea of J.-F. Mestre to avoid the group theoretical complications that were mentioned at the end of section 2. It employs the *quadratic twist* of E. If the elliptic curve E is given by the Weierstraß-equation $Y^2 = X^3 + AX + B$, then the twisted curve E' is given by $gY^2 = X^3 + AX + B$ for some non-square $g \in \mathbf{F}_p^*$. The isomorphism class of this curve does not depend on the choice of g. It is easy to see that

$$Y^2 = X^3 + Ag^2X + Bg^3.$$

is a Weierstraß-equation of the curve E'. It follows from the formula given in the introduction that $\#E'(\mathbf{F}_p) + \#E(\mathbf{F}_p) = 2(p+1)$. Therefore, in order to compute $\#E(\mathbf{F}_p)$ one may as well compute $\#E'(\mathbf{F}_p)$. It follows from Theorems 3.1 and 3.2 below that if $E(\mathbf{F}_p)$ has a very small exponent, then the group of points on its quadratic twist E' does not. One can use this observation as follows: if for a curve E, the baby-step-giant-step strategy has failed for a number of points P because each time more than one value of m was found for which $mP = 0$, then replace E by its quadratic twist E' and try again. By the discussion at the end of section 3, it is very likely that this time the algorithm will succeed.

Before formulating Theorems 3.1 and 3.2 we introduce a few more concepts: the *j-invariant* of an elliptic curve E which is given by the equation $Y^2 = X^3 + AX + B$, is defined by

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}.$$

It is easy to see that E and its quadratic twist E' have the same j-invariants. For most j-invariants $j \in \mathbf{F}_p$ there are, up to isomorphism, precisely two elliptic curves E over $\mathbf{F}_p$ with $j(E) = j$: a curve E and its quadratic twist. There are two well known exceptions: $j = 0$ when $p \equiv 1 \pmod 3$ and $j = 1728$ when $p \equiv 1 \pmod 4$. In the first case there are six curves and in the second case there are four.

The morphisms $f : E \longrightarrow E$ that preserve the point at infinity form the *ring* $\mathrm{End}(E)$ *of* $\mathbf{F}_p$*-endomorphisms of* E. It is isomorphic to a complex quadratic order. If $\Delta \in \mathbf{Z}_{<0}$ denotes the discriminant of the order we have

$$\mathrm{End}(E) \cong \mathbf{Z}[\delta] = \mathbf{Z} + \delta\mathbf{Z}$$

where $\delta = \frac{\sqrt{\Delta}}{2}$ or $\delta = \frac{1+\sqrt{\Delta}}{2}$ depending on whether Δ is even or odd. An elliptic curve and its quadratic twist have isomorphic endomorphism rings. If $p \equiv 1 \pmod 3$, the six curves with $j = 0$ all have their endomorphism ring isomorphic to $\mathbf{Z}[(1+\sqrt{-3})/2]$ and if $p \equiv 1 \pmod 4$, the four curves E with $j = 1728$ all have $\mathrm{End}(E)$ isomorphic to the ring of Gaussian integers $\mathbf{Z}[i]$.

The *Frobenius endomorphism* $\varphi \in \mathrm{End}(E)$ is the endomorphism given by

$$\varphi(x, y) = (x^p, y^p).$$

It satisfies the quadratic relation

$$\varphi^2 - t\varphi + p = 0$$

in the endomorphism ring of E. Here t is an integer which is related to the number of $\mathbf{F}_p$-points on E by

$$\#E(\mathbf{F}_p) = p + 1 - t.$$

The group $E(\mathbf{F}_p)$ is precisely the kernel of the homomorphism $\varphi - 1$ acting on the group of points over an algebraic closure of $\mathbf{F}_p$. Therefore the exponent of the group $E(\mathbf{F}_p)$ is $(p+1-t)/n$, where n is the largest integer such $E(\mathbf{F}_p)$ admits a subgroup isomorphic to $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$. Equivalently, n is the largest integer for which $\varphi \equiv 1 \pmod n$ in $\mathrm{End}(E)$.

Theorem 3.1. *(J.-F. Mestre) Let $p > 457$ be a prime and let E be an elliptic curve over $\mathbf{F}_p$. Then either E or its quadratic twist E' admits an $\mathbf{F}_p$-rational point of order at least $4\sqrt{p}$.*

Proof. The endomorphism rings of E and E' are both isomorphic to the same quadratic order O of discriminant Δ. Let $\varphi \in O$ denote the Frobenius endomorphism of E. Let n be the largest integer such that $\varphi \equiv 1 \pmod{n}$ in $\mathrm{End}(E)$ and let $N = (p+1-t)/n$ denote the exponent of $E(\mathbf{F}_p)$. We have that

$$\mathbf{Z}[\varphi] \subset \mathbf{Z}[\frac{\varphi - 1}{n}] \subset O$$

which implies that n divides the index $[O : \mathbf{Z}[\varphi]]$. Since $[O : \mathbf{Z}[\varphi]]^2$ is equal to the quotient of the discriminants of the orders O and $\mathbf{Z}[\varphi]$, we see that n^2 divides $(t^2 - 4p)/\Delta$.

Similarly, let m be the largest integer such that $-\varphi \equiv 1 \pmod{m}$ in $\mathrm{End}(E)$ and let $M = (p+1+t)/m$ denote the exponent of $E'(\mathbf{F}_p)$. Then

$$\mathbf{Z}[\varphi] \subset \mathbf{Z}[\frac{\varphi + 1}{m}] \subset O.$$

Therefore m^2 also divides $(t^2 - 4p)/\Delta$. Since n divides $\varphi - 1$ and m divides $\varphi + 1$, we see that $\gcd(n, m)$ divides $\gcd(\varphi - 1, \varphi + 1)$ which divides 2. Therefore

$$n^2 m^2 \quad \text{divides} \quad 4\frac{t^2 - 4p}{\Delta}$$

Since $|\Delta| \geq 3$ this implies that $(nm)^2 \leq 4\frac{4p - t^2}{3}$. If *both* exponents N and M are less than $4\sqrt{p}$, we have that

$$\left((p+1)^2 - t^2\right)^2 = (nNmM)^2 < (4\sqrt{p})^4 4\frac{4p - t^2}{3}$$

and therefore

$$p^4 + 4p^3 < (p+1)^4 < \frac{4^6}{3}p^3 - t^4 - \left(\frac{4^5}{3}p^2 - 2(p+1)^2\right) t^2 \leq \frac{4^6}{3}p^3,$$

which implies that $p < 1362$.

A straightforward case-by-case calculation shows that the theorem also holds for the primes p with $457 < p < 1362$. This completes the proof.

For $p = 457$ the theorem is not valid: consider the curve given by

$$Y^2 = X^3 - 1.$$

Its j-invariant is 0 and the ring of endomorphisms is $\mathbf{Z}[\delta]$, where $\delta = (1 + \sqrt{-3})/2$ is the endomorphism given by $(x, y) \mapsto (133x, -y)$. The Frobenius endomorphism is given by $\varphi = -17 + 24\delta$ which has trace -10. The group of points over $\mathbf{F}_{457}$ has cardinality 468 and since $\varphi = 1 - 6(3 - 4\delta)$, it is isomorphic to $\mathbf{Z}/78\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$. The quadratic twist $Y^2 = X^3 - 125$ has Frobenius $17 - 24\delta = 1 + 8(2 - 3\delta)$. The group of rational points has cardinality 468 and is isomorphic to $\mathbf{Z}/56\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$. Both groups have an exponent not exceeding $4\sqrt{457} \approx 85.51023$.

Note that the result mentioned in [6, Prop.7.4.11] is not correct.

To make sure that the baby-step-giant-step algorithm as explained above, works for an elliptic curve over E, one does not really need to find a rational point on E of order at least $4\sqrt{p}$. What one needs is a point P as described in the following theorem.

Theorem 3.2. *Let $p > 229$ be a prime and let E be an elliptic curve over $\mathbf{F}_p$. Then either E or its quadratic twist E' admits an $\mathbf{F}_p$-rational point P with the property that the only integer $m \in (p+1-2\sqrt{p}, p+1+2\sqrt{p})$ for which $mP = 0$ is the order of the group of points.*

Proof. By the proof of Mestre's result, the theorem is true for $p > 457$. A case-by-case calculation shows that it is actually true for $p > 229$.

For $p = 229$ the theorem is not valid: consider the curve given by

$$Y^2 = X^3 - 1.$$

Its ring of endomorphisms is again $\mathbf{Z}[\delta]$. The Frobenius endomorphism is given by $\varphi = -17 + 12\delta$ which has trace -22. Since $\varphi = 1 + 6(-3 + 2\delta)$ the group of points over $\mathbf{F}_{229}$ has cardinality 252 and is isomorphic to $\mathbf{Z}/42\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$. The quadratic twist $Y^2 = X^3 - 8$ has Frobenius $17 + 12\delta = 1 - 4(4 - 3\delta)$. The group of rational points has cardinality 208 and is isomorphic to $\mathbf{Z}/52\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$. Every rational point on the curve $Y^2 = X^3 - 1$ is killed by the order of the group 252, but also by $252 - 42 = 210$. Every rational point on the twisted curve $Y^2 = X^3 - 8$ is killed by both 208 and by $260 = 208 + 52$.

The interval $(p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$ contains the integers 200, 201, …, 259, 260.

Many of the curves E for which Theorem 3.2. fails, have their j-invariants equal to 0 or 1728 and therefore their endomorphism rings are isomorphic to $\mathbf{Z}[(1 + \sqrt{-3})/2]$ or $\mathbf{Z}[i]$ respectively. However, if one knows the endomorphism ring of E, it is extremely easy to compute $\#E(\mathbf{F}_p)$, even when p is very large. This is a consequence of Theorem 4.1 of the next section. When one excludes the curves with j-invariant 0, then Theorem 3.1 is correct for $p > 193$ and Theorem 3.2 is correct for $p > 53$.

4. Cornacchia's algorithm.

In this section we explain how to count the number of points on an elliptic curve E, when the endomorphism ring of E is known. In this case there is an extremely efficient practical algorithm. It forms the basis of the primality test of Atkin and Morain [3].

As usual, p is a large prime and E is an elliptic curve over $\mathbf{F}_p$ given by a Weierstraß-equation $Y^2 = X^3 + AX + B$. Let Δ denote the discriminant of the endomorphism ring $\mathrm{End}(E)$ of E. Recall that $\mathrm{End}(E)$ is isomorphic to a subring of $\mathbf{C}$:

$$\begin{aligned}\mathrm{End}(E) &\cong \{\frac{u+v\sqrt{\Delta}}{2} : u, v \in \mathbf{Z} \text{ and } u \equiv v \pmod{2}\},\\ &\cong \{u + v\delta : u, v \in \mathbf{Z}\} = \mathbf{Z} + \delta\mathbf{Z}.\end{aligned}$$

where $\delta = \frac{\sqrt{\Delta}}{2}$ or $\frac{1+\sqrt{\Delta}}{2}$ depending on whether Δ is even or odd.

The Frobenius endomorphism $\varphi \in \mathrm{End}(E)$ satisfies $\varphi^2 - t\varphi + p = 0$ where t is an integer satisfying $t^2 < 4p$. It is related to $\#E(\mathbf{F}_p)$ by the formula $\#E(\mathbf{F}_p) = p + 1 - t$. If p divides Δ, then $t = 0$ and $\#E(\mathbf{F}_p) = p + 1$. Therefore we assume from now on that p does not divide Δ. In order to compute $\#E(\mathbf{F}_p)$, it suffices to compute $\varphi \in \mathrm{End}(E) \cong \mathbf{Z}[\delta] \subset \mathbf{C}$. First we observe that $p = \varphi\overline{\varphi}$. This shows that the prime p splits in $\mathrm{End}(E)$ into a product of the two *principal* prime ideals (φ) and $(\overline{\varphi})$ of index p.

The idea of the algorithm is to compute a generator of a prime divisor $\mathfrak{p}$ of p in $\mathbf{Z}[\delta]$. If $\Delta \neq -3$ or -4, a generator is unique up to sign and hence we obtain φ (or its conjugate) and therefore t up to sign. This leaves only two possibilities for $\#E(\mathbf{F}_p)$. It is not difficult to decide which of the two possible values is the correct one. One either picks a random point $Q \in E(\mathbf{F}_p)$ and checks whether $(p + 1 \pm t)Q = 0$ or one considers the action of φ on the 3-torsion points. When $\Delta = -3$ or -4, there are 6 and 4 possibilities respectively for the value of t. These cases can be handled in a similar, efficient way [14, p.112].

To compute a generator of the prime ideal $\mathfrak{p} \subset \mathbf{Z}[\delta]$ we first compute a square root b of Δ modulo p. Replacing b by $p - b$ if necessary, we may assume that $|b| < p$ and $b \equiv \Delta \pmod{2}$. Then $\mathfrak{p} = ((b + \sqrt{\Delta})/2, p)$ is a prime ideal of index p. It divides p. Since $\mathfrak{p}$ is principal, the fractional ideal

$$\mathbf{Z} + \frac{b+\sqrt{\Delta}}{2p}\mathbf{Z}$$

is equal to an ideal of the form $(\mathbf{Z}+\delta\mathbf{Z})\alpha$ for some $\alpha \in \mathbf{Z}[\delta]$. In other words, there is a matrix $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$ such that

Inspection of the imaginary parts, shows that $(r+s\delta)(r+s\overline{\delta}) = p$. Therefore $r+s\delta$ is a generator of either the ideal $\mathfrak{p}$ or its conjugate.

To find the matrix $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$, we consider the usual action of the group $\mathrm{SL}_2(\mathbf{Z})$ on the upper half plane $\{z \in \mathbf{C} : \mathrm{Im}\, z > 0\}$. Both $(b+\sqrt{\Delta})/2$ and δ are in the same $\mathrm{SL}_2(\mathbf{Z})$-orbit and δ is contained in the standard fundamental domain.

By successive applications of the matrices $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$ one transforms $z = \frac{b+\sqrt{\Delta}}{2p}$ to δ. The matrix $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$ is then the product of all the matrices involved.

This algorithm is well known. It is a reformulation of the usual algorithm for reducing positive definite quadratic forms. It is very efficient [6, Alg.5.4.2]. We do not give all the details because the following theorem [7] gives an even simpler solution our problem.

Theorem 4.1. *(G. Cornacchia, 1908) Let O be a complex quadratic order of discriminant Δ and let p be an odd prime number for which Δ is a non-zero square modulo p. Let x be an integer with $x^2 \equiv \Delta \pmod p$, $x \equiv \Delta \pmod 2$ and $0 < x < 2p$. Define the finite sequence of non-negative integers $x_0, x_1, \ldots, x_t = 0$ as follows*

$$\begin{aligned} x_0 &= 2p, \\ x_1 &= x, \\ x_{i+1} &= \text{the remainder of } x_{i-1} \text{ after division by } x_i. \end{aligned}$$

Let i be the smallest index for which $x_i < 2\sqrt{p}$. If Δ divides $x_i^2 - 4p$ and the quotient is a square v^2, then

$$\frac{x_i + v\sqrt{\Delta}}{2}$$

is a generator of a prime ideal $\mathfrak{p}$ of O dividing p. If not, then the prime ideals $\mathfrak{p}$ of O that divide p are not principal.

Proof. (H.W. Lenstra [15]) The ideal $\mathfrak{p} = ((x - \sqrt{\Delta})/2, p)$ of O is a prime divisor of p. We view $\mathfrak{p}$ as a lattice L in $\mathbf{C}$. We define a finite sequence of elements $z_0, z_1, \ldots, z_t \in L$ by $z_0 = p$, $z_1 = (x - \sqrt{\Delta})/2$ and

$$z_{i+1} = z_i - qz_{i+1} \qquad \text{for } i \geq 1$$

where $q \in \mathbf{Z}_{>0}$ is the integral part of $\mathrm{Re}\, z_i / \mathrm{Re}\, z_{i-1}$. Since the sequence $\mathrm{Re}\, z_i$ is strictly decreasing, the last z_t has real part equal to 0. The traces $z_i + \overline{z_i}$ are precisely the x_i in Cornacchia's algorithm. The imaginary parts of the z_i form an alternating sequence and $(-1)^i \mathrm{Im} z_i$ is increasing. Any two consecutive z_i form a basis for L over $\mathbf{Z}$.

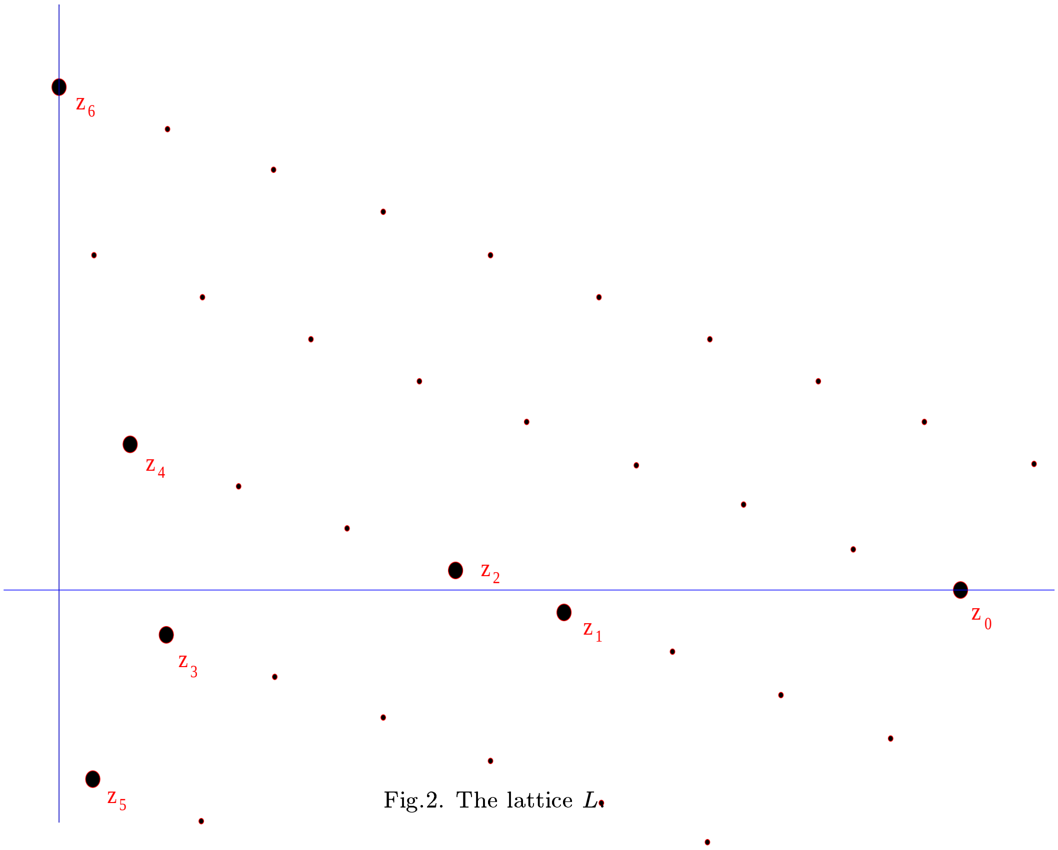

Fig.2. The lattice L.

A *minimal* element of the lattice L is a non-zero vector $z \in L$ with the property that the rectangular box with center 0 and corner z, contains no lattice points except on its corners. In other words, every $w \in L$ with

$$|\mathrm{Re}\, w| \leq |\mathrm{Re}\, z| \quad \text{and} \quad |\mathrm{Im}\, w| \leq |\mathrm{Im}\, z|$$

satisfies $|\mathrm{Re}\, w| = |\mathrm{Re}\, z|$ and $|\mathrm{Im}\, w| = |\mathrm{Im}\, z|$. It is easy to see that all the vectors z_i are minimal. There is only one small exception to this: when the real part of z_1 exceeds $\mathrm{Re}\, z_0/2 = p/2$, then $\mathrm{Im}\, z_2 = -\mathrm{Im}\, z_1$, but $|\mathrm{Re}\, z_1| \neq |\mathrm{Re}\, z_2|$, so z_1 is not minimal in this case.

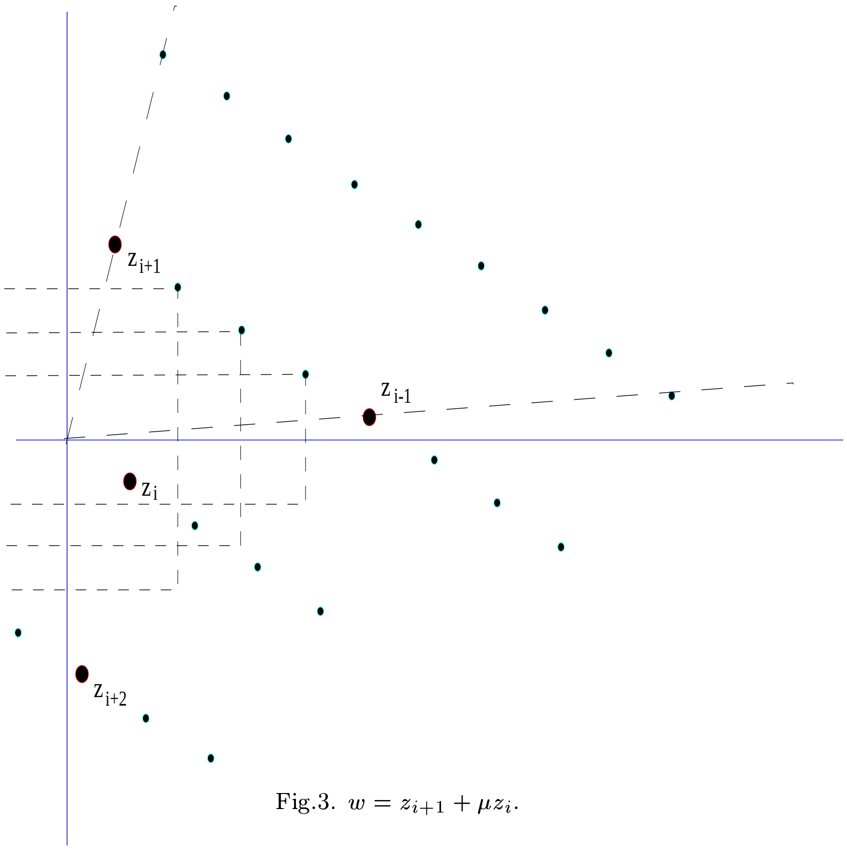

Fig.3. $w = z_{i+1} + \mu z_i$.

Apart from this exception, the vectors $\pm z_i$ are precisely *all* minimal vectors of L. We briefly explain this general fact: let $w \in L$ be a minimal vector with $\mathrm{Re}\, w \geq 0$. Then, putting $z_{t+1} = -z_t$, one can either "see" w from the origin between z_{i-1} and z_{i+1} for some $i = 1, 2, \ldots, t$ or one can "see" w between z_0 and z_1. In the latter case $\mathrm{Im}\, w = \mathrm{Im}\, z_1$ or $\mathrm{Im}\, w =$

$\operatorname{Im} z_0 = 0$ which, by the minimality of w, implies that $w = z_0$ or $w = z_1$. In the other cases let q denote the integral part of $\operatorname{Re} z_i / \operatorname{Re} z_{i-1}$. Then $z_{i+1} = z_{i-1} - q z_i$ and

$$w = \lambda z_{i+1} + \mu z_i, \qquad \text{for some } \lambda, \mu \in \mathbf{Z} \text{ with } \lambda \geq 0 \text{ and } 0 \leq \mu \leq q\lambda.$$

If $\lambda \geq 2$ then either z_{i+1} or z_{i-1} would be contained in the interior of the rectangular box with center 0 and corner w. Since w is minimal, this is impossible and we have that

$$w = z_i \quad \text{or} \quad w = z_{i+1} + \mu z_i \quad \text{for some } \mu \text{ satisfying } 0 \leq \mu \leq q\lambda.$$

The point z_i is contained in the box with center 0 and corner $z_{i+1} + \mu z_i$ whenever $0 < \mu < q$. It is usually contained in the interior, in which case we conclude, by minimality of w, that $\mu = 0$ or $\mu = q$. The exceptional case occurs when $z_{i+1} + \mu z_i = \overline{z_i}$. In this case $\mu = 1$, $t = 2$ and $w = (z_0 + z_2)/2$. Since p does not divide x, this case does not occur for our lattice L.

If $\mathfrak{p}$ is principal, every generator is evidently minimal. Therefore one of the z_i is a generator of $\mathfrak{p}$. Consider the one with maximal real part. Since $|z_i| = \sqrt{p}$, its trace $x_i = z_i + \overline{z_i}$ is less than $2\sqrt{p}$. We must show that $\operatorname{Re} z_{i-1} > \sqrt{p}$. Since z_{i-1} is in $\mathfrak{p} = (z_i)$ and since the real part of z_i is maximal, z_{i-1} is not a generator of $\mathfrak{p}$ and we have that $|z_{i-1}|^2 \geq 2|z_i|^2$. Therefore

$$(\operatorname{Re} z_{i-1})^2 = |z_{i-1}|^2 - (\operatorname{Im} z_{i-1})^2 \geq 2|z_i|^2 - (\operatorname{Im} z_i)^2 \geq |z_i|^2 = p$$

which shows that $\operatorname{Re} z_{i-1} > \sqrt{p}$.

This completes the proof.

When Δ is even, both initial values x_0 and x_1 are even. Therefore all x_i are even and one can simplify Cornacchia's algorithm a little bit by dividing everything by 2: let $x_0 = p$ and $x_1^2 \equiv \Delta/4 \pmod{p}$ and stop the Euclidean algorithm when $x_i < \sqrt{p}$. See [6, Alg.1.5.2].

The running time of both these algorithms to compute $E(\mathbf{F}_p)$ when the endomorphism ring is given, is dominated by the calculation of the square root of Δ modulo p. Using the method explained in [20] or [6, Alg.1.5.1] and assuming the generalized Riemann Hypothesis, the running time is $O(\log^4 p)$.

5. A polynomial time algorithm.

In this section we briefly explain a deterministic polynomial time algorithm [18] to count the number of points on an elliptic curve E over $\mathbf{F}_p$. We suppose that E is given by a Weierstraß equation $Y^2 = X^3 + AX + B$.

It is easy to compute $\#E(\mathbf{F}_p)$ modulo 2: the cardinality of the group $E(\mathbf{F}_p)$ is even if and only if it contains a point of order 2. Since the points of order 2 have the form $(x, 0)$, this means precisely that the polynomial $X^3 + AX + B$ has a zero in $\mathbf{F}_p$. This, in turn, is equivalent to

$$\gcd(X^p - X, X^3 + AX + B) \neq 1 \qquad \text{in the ring } \mathbf{F}_p[X].$$

This can be tested efficiently; the bulk of the computation is the calculation of X^p in the ring $\mathbf{F}_p[X]/(X^3 + AX + B)$, which can be done by repeated squarings and multiplications, using the binary presentation of the exponent p. The amount of work involved is $O(\log^3 p)$.

Now we generalize this calculation to other primes l. We compute $\#E(\mathbf{F}_p)$ modulo the first few small primes $l = 3, 5, 7, \ldots$. Since, by Hasse's Theorem

$$p + 1 - 2\sqrt{p} < \#E(\mathbf{F}_p) < p + 1 + 2\sqrt{p}$$

it suffices that

$$\prod_l l > 4\sqrt{p}$$

in order to determine the cardinality uniquely by means of the Chinese Remainder Theorem. A weak form of the prime number theorem shows that this can be achieved with at most $O(\log p)$ primes l, each of size at most $O(\log p)$. Since p is large, the primes l are very small with respect to p. In particular, $l \neq p$.

As in the case where $l = 2$, we use the subgroup $E[l]$ of l-torsion points of $E(\overline{\mathbf{F}}_p)$:

$$E[l] = \{P \in E(\overline{\mathbf{F}}_p) : l \cdot P = 0\}.$$

The group $E[l]$ is isomorphic to $\mathbf{Z}/l\mathbf{Z} \times \mathbf{Z}/l\mathbf{Z}$. There exist polynomials, the socalled *division polynomials*

$$\Psi_l(X) \in \mathbf{F}_p[X],$$

that vanish precisely in the l-torsion points. For example

$$\begin{aligned}\Psi_3(X) =& 3X^4 + 6AX^2 + 12BX - A^2,\\ \Psi_5(X) =& 5X^{12} + 62AX^{10} + 380BX^9 - 105A^2X^8 + 240BAX^7\\ &+ (-300A^3 - 240B^2)X^6 - 696BA^2X^5 + (-125A^4\\ &- 1920B^2A)X^4 + (-80BA^3 - 1600B^3)X^3 + (-50A^5\\ &- 240B^2A^2)X^2 + (-100BA^4 - 640B^3A)X\\ &+ (A^6 - 32B^2A^3 - 256B^4).\end{aligned}$$

The division polynomials can be calculated recursively by means of the addition formulas [5, 18]. Their degree is $(l^2-1)/2$. The amount of work involved in calculating them is dominated by the rest of the computation, so we don't bother estimating it.

The Frobenius endomorphism $\varphi : E \longrightarrow E$ satisfies the quadratic relation

$$\varphi^2 - t\varphi + p = 0,$$

where t is an integer satisfying $\#E(\mathbf{F}_p) = p + 1 - t$. In the algorithm we check which of the relations

$$\varphi^2 - t'\varphi + p = 0 \qquad t' = 0, 1, 2, \ldots, l-1$$

holds *on the group* $E[l]$ *of* l*-torsion points.* It is easily seen that the relation can only hold for $t' \equiv t \pmod{l}$ and in this way we obtain the value of t modulo l.

The point is that the relations can be expressed by means of polynomials and that they can be checked efficiently: we have that

$$\varphi^2(x,y) + p(x,y) = t'\varphi(x,y) \qquad \text{for all } (x,y) \in E[l]$$

if and only if

$$(X^{p^2}, Y^{p^2}) + p'(X,Y) \equiv t'(X^p, Y^p)$$

modulo the polynomials $\Psi_l(X)$ and $Y^2 - X^3 - AX - B$. Here p' denotes the integer congruent to $p \pmod{l}$ that satisfies $0 \le p' < l$. Note that the "+" that occurs in the formula is the addition on the elliptic curve and that the multiplications are repeated additions.

The bulk of the computation is, first, the computation of the powers X^p, X^{p^2}, etc. in the ring

$$\mathbf{F}_p[X,Y]/(\Psi_l(X), Y^2 - X^3 - AX - B)$$

and then, l times, the addition of the point (X^p, Y^p), which boils down to a few additions and multiplications in the same ring. Since the elements of the ring have size $l^2 \log p$, the amount of work involved is $O(\log p (l^2 \log p)^2)$ and $O(l(l^2 \log p)^2)$ respectively. Here we assume that the usual multiplication algorithms are being used, so that multiplying two elements of length n takes time proportional to n^2.

Keeping in mind that $l = O(\log p)$ and that we have to do this calculation for each l, we conclude that the amount of work involved in the entire calculation is

$$O(\log^8 p).$$

So, this is a deterministic polynomial time algorithm, i.e. it is asymptotically very fast. In practice it behaves, unfortunately, rather poorly because of the huge degrees of the division polynomials involved. For instance, the computations for the example with $p \approx 10^{200}$ mentioned in the introduction would involve primes $l > 250$. For such l, representing one element in the ring $\mathbf{F}_p[X,Y]/(\Psi_l(X), Y^2 - X^3 - AX - B)$ requires more than 1.5 megabytes of memory.

In the following sections we explain practical improvements of this algorithm due to Atkin and Elkies.

6. The action of Frobenius on the l-torsion points.

As in the previous sections, let p be a large prime and let E be an elliptic curve over $\mathbf{F}_p$ given by a Weierstraß-equation. In this section l is a prime different from p and we study the action of the Frobenius endomorphism on the group $E[l]$ of l-torsion points on an elliptic curve. As an application we describe Atkin's algorithm [1,2] to compute the order of the image of the Frobenius endomorphism in the group $\mathrm{PGL}_2(\mathbf{F}_l)$. We explain how this can be used to count the number of points on an elliptic curve over $\mathbf{F}_p$.

For every prime l we introduce the so-called *modular equation.* This a symmetric polynomial $\Phi_l(S,T) \in \mathbf{Z}[S,T]$, which is equal to to $S^{l+1} - S^l T^l + T^{l+1}$ plus terms of the form $S^i T^j$ with $i,j \leq l$ and $i + j < 2l$. By the famous *Kronecker congruence relation,* one has that $\Phi_l(S,T) \equiv (S^l - T)(T - S^l) \pmod{l}$. The polynomial has the property that for any field F of $\mathrm{char}(F) \neq l$ and for every j-invariant $j \in F$, the $l+1$ zeroes $\tilde{\jmath} \in \overline{F}$ of the polynomial $\Phi_l(j,T) = 0$ are precisely the j-invariants of the *isogenous* curves E/C. Here E is an elliptic curve with j-invariant j and C runs through the $l+1$ cyclic subgroups of $E[l]$. See [21] for the construction of the curves E/C.

The polynomial $\Phi_l(S,T)$ describes a singular model for the modular curve $X_0(l)$ in $\mathbf{P}^1\times\mathbf{P}^1$ over $\mathbf{Z}$. As an example we give the modular equation for $l=3$:

$$\begin{aligned}\Phi_3(T,S) =&S^4 - S^3T^3 + T^4 + 2232(S^3T^2 + T^3S^2) - 1069956(S^3T + T^3S)\\ &+ 36864000(S^3 + T^3) + 2587918086S^2T^2\\ &+ 8900222976000(S^2T + T^2S)\\ &+ 452984832000000(S^2 + T^2) - 770845966336000000ST\\ &+ 1855425871872000000000(S + T).\end{aligned}$$

An elliptic curve E over a finite field of characteristic p is called *supersingular* if it possesses no points of order p, not even over an algebraic closure $\overline{\mathbf{F}}_p$. Equivalently, some power of the Frobenius endomorphism of E is an integer. Since the property of being supersingular only depends on the curve E over $\overline{\mathbf{F}}_p$, it only depends on the j-invariant of E. Therefore we can speak of *supersingular j-invariants.* Supersingular curves are rare. Their j-invariants are always contained in $\mathbf{F}_{p^2}$ and the number of supersingular j-invariants in $\mathbf{F}_p$ is approximately $O(\sqrt{p})$. See [21].

For an elliptic curve E, an isogeny $E \longrightarrow E/C$ is usually defined over the field that contains the j-invariants of E and E/C, but this need not be true if the j-invariant of E is supersingular or equal to 0 or 1728. The following proposition is sufficient for our purposes.

Proposition 6.1. *Let E be an elliptic curve over $\mathbf{F}_p$. Suppose that its j-invariant j is not supersingular and that $j \neq 0$ or 1728. Then*

(i) the polynomial $\Phi_l(j,T)$ has a zero $\tilde{\jmath} \in \mathbf{F}_{p^r}$ if and only if the kernel C of the corresponding isogeny

$$E \longrightarrow E/C$$

is a 1-dimensional eigenspace of φ^r in $E[l]$. Here φ denotes the Frobenius endomorphism of E.

(ii) The polynomial $\Phi_l(j,T)$ splits completely in $\mathbf{F}_{p^r}[T]$ if and only if φ^r acts as a scalar matrix on $E[l]$.

Proof. *(i)* If C is an eigenspace of φ^r, it is stable under the action of the Galois group generated by φ^r. Therefore the isogeny $E \longrightarrow E/C$ is defined over $\mathbf{F}_{p^r}$ and the j-invariant $\tilde{\jmath}$ of E/C is contained in $\mathbf{F}_{p^r}$.

Conversely, if $\Phi_l(j,\tilde{\jmath}) = 0$, then there is a cyclic subgroup C of $E[l]$ such that the j-invariant of E/C is equal to $\tilde{\jmath} \in \mathbf{F}_{p^r}$. Let E' be an elliptic curve over $\mathbf{F}_{p^r}$ with j-invariant equal to $\tilde{\jmath}$. Let $E/C \longrightarrow E'$ be an $\overline{\mathbf{F}}_p$-isomorphism and let $f : E \longrightarrow E/C \longrightarrow E'$ be the composite isogeny. It has kernel C.

The group $\mathrm{Hom}_{\mathbf{F}_{p^r}}(E, E')$ of isogenies $E \longrightarrow E'$ that are defined over $\mathbf{F}_{p^r}$ is a subgroup of the group of all isogenies $\mathrm{Hom}_{\overline{\mathbf{F}}_p}(E, E')$. Since E is not supersingular, $\mathrm{Hom}_{\overline{\mathbf{F}}_p}(E, E')$ is free of rank 2. The subgroup $\mathrm{Hom}_{\mathbf{F}_{p^r}}(E, E')$ is either trivial or equal to $\mathrm{Hom}_{\overline{\mathbf{F}}_p}(E, E')$. Therefore f is defined over $\mathbf{F}_{p^r}$ as soon as there exists an isogeny $E \longrightarrow E'$ which is defined over $\mathbf{F}_{p^r}$. This means that C is an eigenspace of φ^r, as soon as curves E and E' are $\mathbf{F}_{p^r}$-isogenous or, equivalently, when their Frobenius endomorphisms over $\mathbf{F}_{p^r}$ satisfy the same characteristic equation [21, Chpt.III, Thm. 7.7].

We will show that E' can be chosen to be $\mathbf{F}_{p^r}$-isogenous to E. Since E and E' are isogenous over $\overline{\mathbf{F}}_p$, the quotient fields of their endomorphism rings are isomorphic to the same complex quadratic field K. Let ψ and ψ' denote the Frobenius endomorphisms over $\mathbf{F}_{p^r}$ of E and E' respectively. We have that $\psi = \varphi^r$. In K we have, up to complex conjugation, the relation

$$\psi^s = \psi'^s \qquad \text{for some positive integer } s.$$

If $\psi = \psi'$, the curves E and E' are $\mathbf{F}_{p^r}$-isogenous. If $\psi = -\psi'$, then we replace E' by its quadratic twist, which has Frobenius endomorphism $-\psi'$. Again the curves E and E' are $\mathbf{F}_{p^r}$-isogenous.

From now on we suppose that $\psi \neq \pm\psi'$. Then $\psi/\psi' \in K$ is a root of unity of order at least 3 and either $K = \mathbf{Q}(i)$ and $\psi' = \pm i\psi$ or $K = \mathbf{Q}(\zeta)$ and $\psi' = \pm\zeta\psi$ or $\pm\zeta^{-1}\psi$. Here ζ denotes a primitive cube root of unity. The endomorphism rings of E and E' are orders of conductor f and f' respectively in K. We have the following:

- f and f' are coprime. We only give the easy proof for $K = \mathbf{Q}(i)$; the other case is similar. Let $\psi = a + bi$ for some $a, b \in \mathbf{Z}$, then $\psi' = \pm b \pm ai$ and f divides b while f' divides a. Since a and b are coprime integers, so are f and f'.
- The quotient f/f' is equal to l, 1 or $1/l$. To see this, let $R_C \subset \mathrm{End}(E)$ be the subring defined by

  $$R_C = \{f \in \mathrm{End}(E) : f(C) \subset C\}.$$

  The index of this ring in $\mathrm{End}(E)$ divides l and the natural map $R_C \longrightarrow \mathrm{End}(E')$ given by $g \mapsto g$ is a well defined injective ring homomorphism. Therefore f' divides the conductor of R_C which in turn divides lf. Using the dual isogeny of f, we find in a similar way that f divides lf'. If f would not divide f' and f' would not divide f, then $\mathrm{ord}_l(f) = \mathrm{ord}_l(f')+1$ and $\mathrm{ord}_l(f') = \mathrm{ord}_l(f)+1$ which is absurd. Therefore either f divides f' or f' divides f and we conclude that either f'/f divides l or f/f' divides l.

It follows easily that either f or f' is equal to 1. Since $j \neq 0$ or 1728, the conductor f cannot be 1. Therefore $f' = 1$ and the j-invariant $\tilde{\jmath}$ of E' is 1728 or 0 respectively. In the first case $K = \mathbf{Q}(i)$ and, since E is not supersingular, $p \equiv 1 \pmod 4$ and there are, up to isomorphisms, four curves over $\mathbf{F}_p$ with $j = 1728$. Their Frobenius endomorphisms are given by $\pm\psi$, $\pm i\psi$. Therefore one of these curves is $\mathbf{F}_{p^r}$-isogenous to E and we replace E' by this $\overline{\mathbf{F}}_p$-isomorphic curve. In the second case $\tilde{\jmath} = 0$ and $p \equiv 1 \pmod 3$; there are six curves $\mathbf{F}_p$ with j-invariant equal to 0, one of which is isogenous to E. We replace E' by this curve. In both cases we conclude that the isogeny f and its kernel C are defined over $\mathbf{F}_{p^r}$. This proves *(i)*.

(ii) If all zeroes $\tilde{\jmath}$ of $\Phi_l(j,T)$ are contained in $\mathbf{F}_{p^r}$, then by *(i)*, all 1-dimensional subspaces of $E[l]$ are eigenspaces of φ^r. This implies that φ^r is a scalar matrix.

This proves the proposition.

The conditions of the proposition are necessary. For instance, let E be the elliptic curve over $\mathbf{F}_7$ given by the equation $Y^2 = X^3 - 1$. It has j-invariant 0. Let $l = 3$. The 3-division polynomial is equal to $\Psi_3(X) = X(X^3-4)$ and the modular equation with $S = j = 0$ becomes $\Phi_3(j,T) = T(T-3)^3 \pmod 7$. The zero $X = 0$ of $\Psi_3(X)$ gives rise to the subgroup $C = \{\infty, (0, \pm i)\}$ where $i \in \mathbf{F}_{49}$ satisfies $i^2 = -1$. The group C is the kernel of the endomorphism $1 - \delta$ where δ is given by $\delta(x,y) = (2x,y)$. Therefore $E/C \cong E$ and E/C has j-invariant equal to $\tilde{\jmath} = 0$. This explains the zero $\tilde{\jmath} = 0$ of $\Phi_3(j,T)$. The other (triple) zero $\tilde{\jmath} = 3$ is the j-invariant of E/C where C is any of the other three subgroups of order 3. The six non-trivial points in these groups are given by $(\pm 2i, \sqrt[3]{4})$. Since the Frobenius endomorphism φ acts transitively on these six points, we conclude that the only eigenspace of φ is the kernel of $1 - \delta$. There are no eigenspaces corresponding to the the zero $\tilde{\jmath} = 3$ of $\Phi_3(j,T)$.

For supersingular curves E Prop.6.1 is, in general, also false. For instance, let $p = 13$ and consider the curve E given by $Y^2 = X^3 - 3X - 6$ over $\mathbf{F}_{13}$. The j-invariant of E is equal to 5 and E has 14 points over $\mathbf{F}_{13}$. Therefore the trace of the Frobenius endomorphism φ is zero and φ satisfies $\varphi^2 + 13 = 0$. This means that $\varphi^2 \in \mathbf{Z}$ and hence that E is supersingular. All supersingular curves over $\overline{\mathbf{F}}_{13}$ have j-invariant equal to 5. Therefore, for every prime l, the modular equation $\Phi_l(j,T)$ is congruent to $(T-5)^{l+1} \pmod{13}$. All its zeroes are in $\mathbf{F}_{13}$, but when l is a prime modulo which -13 is not a square, the characteristic equation $\varphi^2+13=0$ of the Frobenius endomorphism φ is irreducible modulo l. Therefore φ has no 1-dimensional eigenspaces in $E[l]$.

In general, if j is a supersingular j-invariant, all irreducible factors of the polynomial $\Phi_l(j,T) \in \mathbf{F}_p[T]$ have degree 1 or 2. The following two propositions are in [2].

Proposition 6.2. *Let E be a non-supersingular elliptic curve over $\mathbf{F}_p$ with j-invariant $j \neq 0$ or 1728. Let $\Phi_l(j,T) = f_1 f_2 \cdots f_s$ be the factorization of $\Phi_l(j,T) \in \mathbf{F}_p[T]$ as a product of irreducible polynomials. Then there are the following possibilities for the degrees of $f_1, f_2, \ldots, f_s$:*

(i)

$$1 \text{ and } l;$$

in other words, $\Phi_l(j,T)$ factors as a product of a linear factor and an irreducible factor of degree l. In this case l divides the discriminant t^2-4p. We put $r=l$ in this case.

(ii)

$$1, 1, r, r, \ldots, r;$$

in this case t^2-4p is a square modulo l, the degree r divides $l-1$ and φ acts on $E[l]$ as a matrix $\left(\begin{smallmatrix}\lambda & 0\\ 0 & \mu\end{smallmatrix}\right)$ with $\lambda, \mu \in \mathbf{F}_l^*$.

(iii)

$$r, r, r, \ldots, r \qquad \text{for some } r > 1;$$

in this case t^2-4p is not a square modulo l, the degree r divides $l+1$ and φ acts on $E[l]$ as a 2×2-matrix that has a characteristic polynomial which is irreducible modulo l.

In all cases, r is the order of φ in the group $\mathrm{PGL}_2(\mathbf{F}_l)$ and the trace t of φ satisfies

$$t^2 = (\zeta+\zeta^{-1})^2 p \pmod{l} \qquad \text{for some primitive } r\text{-th root of unity } \zeta \in \overline{\mathbf{F}}_l.$$

Proof. This follows from the previous proposition. The Frobenius endomorphism φ acts on $E[l]$ via a 2×2-matrix with characteristic equation $\varphi^2 - t\varphi + p = 0$. If the matrix has a double eigenvalue and is not diagonalizable, then there is only one 1-dimensional eigenspace of φ and the matrix φ^l is scalar. This is case *(i)*.

If the matrix has two eigenvalues in $\mathbf{F}_l$ and is diagonalizable, then the discriminant $t^2 - 4p$ is a square modulo l and $E[l]$ is the direct product of two 1-dimensional φ-eigenspaces. This accounts for the two factors of degree 1 of $\Phi_l(j,T)$. The remaining factors have degree r, where r is the smallest positive integer such that φ^r is a scalar matrix. This is case *(ii)*.

If the matrix has two conjugate eigenvalues $\lambda, \mu \in \mathbf{F}_{l^2} - \mathbf{F}_l$, then there are no 1-dimensional eigenspaces and all irreducible factors of $\Phi_l(j,T)$ have degree r where r is the smallest exponent such that $\lambda^r \in \mathbf{F}_l^*$. It is easy to see that this is also the smallest exponent such that φ^r is scalar. This covers case *(iii)*

To prove the last statement, we note that the matrix φ^r acts on $E[l]$ as a scalar matrix. This implies that the eigenvalues λ and μ of φ satisfy $\lambda^r = \mu^r$. Since $\lambda\mu = p$, we have $\lambda^{2r} = p^r$ and hence $\lambda^2 = \zeta p$ for some primitive r-th root of unity ζ. This implies that $t^2 = (\lambda + p/\lambda)^2 = (\zeta + \zeta^{-1})^2 p \pmod{l}$ as required. Here one should take $\zeta = 1$ in case *(i)* where $r = l$.

The following proposition puts a further restriction on the possible value of r.

Proposition 6.3. *Suppose E is a non-supersingular curve over $\mathbf{F}_p$ with j-invariant $j \neq 0$ or 1728. Let l be an odd prime and let s denote the number of irreducible factors in the factorization of $\Phi_l(j,T) \in \mathbf{F}_p[T]$. Then*

$$(-1)^s = \left(\frac{p}{l}\right)$$

Proof. If l divides $t^2 - 4p$ and φ has order l we are in case *(i)* of Prop.6.2 and the result is true. Suppose therefore that $t^2 - 4p \not\equiv 0 \pmod{l}$, i.e., that we are in case *(ii)* or *(iii)* and let $T \subset \mathrm{PGL}_2(\mathbf{F}_l)$ be a maximal torus containing φ. In other words, we take $T = \{\left(\begin{smallmatrix}\alpha & 0\\ 0 & \beta\end{smallmatrix}\right) : \alpha, \beta \in \mathbf{F}_l^*\}$ split in case *(ii)* and we take T non-split, i.e., isomorphic to $\mathbf{F}_{l^2}^*$ in case *(iii)*. Let $\overline{T}$ denote the image of T in $\mathrm{PGL}_2(\mathbf{F}_l)$. The group $\overline{T}$ is cyclic of order $l-1$ in case *(ii)* and of order $l+1$ in case *(iii)*. The determinant induces an isomorphism $\det : \overline{T}/\overline{T}^2 \longrightarrow \mathbf{F}_l^*/(\mathbf{F}_l^*)^2$. Since the characteristic equation of φ is $\varphi^2 - t\varphi + p = 0$, the action of φ is via $\det(\varphi) = p$ and we obtain an isomorphism

$$\det : \overline{T}/\langle \overline{T}^2, \varphi\rangle \longrightarrow \mathbf{F}_l^*/\langle (\mathbf{F}_l^*)^2, p\rangle.$$

This shows that the index $[\overline{T} : \varphi]$ is odd if and only if p is not a square mod l. Since the number s of irreducible factors of $\Phi_l(j,T)$ over $\mathbf{F}_p$ is equal to $s = (l \pm 1)/r = [\overline{T} : \langle\varphi\rangle]$, the proposition follows.

Propositions 6.2 and 6.3 can be employed to obtain information about the trace t. The restriction to elliptic curves that are not supersingular and have $j \neq 0$ or 1728 is not very serious. For curves with j-invariant equal to 0 or 1728, the algorithm of section 4 is much more efficient, while supersingular curves always have $t = 0$ and hence $p+1$ points over $\mathbf{F}_p$. The chance that a "random" elliptic curve like in the introduction, is supersingular, is very small; the probability is bounded by $O(p^{-1/2})$. In practice this case is recognized easily because for each prime l, the polynomial $\Phi_l(j,T)$ has only irreducible factors of degree 1 and 2.

Rather than doing the computations modulo the division polynomial $\Psi_l(X)$ of degree $(l^2-1)/2$ that were introduced in section 5, Atkin does computations modulo the polynomial $\Phi_l(j,T)$ of degree $l+1$. This is much more efficient, but one obtains less information: instead of computing $t \pmod{l}$, Atkin only obtains certain restrictions on the value of $t \pmod{l}$.

Atkin's algorithm. Let E be an elliptic curve over $\mathbf{F}_p$ given by a Weierstraß-equation. Let $j \in \mathbf{F}_p$ denote its j-invariant. Let l be a prime number.

Atkin first determines how many zeroes the polynomial $\Phi_l(j,T)$ has in $\mathbf{F}_p$. This is done by computing

$$\gcd(T^p - T, \Phi_l(j,T)).$$

Then one can see which case of Prop.6.2 applies to the prime l. The bulk of the calculation is the computation of T^p in the ring $\mathbf{F}_p[T]/(\Phi_l(j,T))$; since the degree of $\Phi_l(j,T)$ is $l+1$, the amount of work is proportional to $O(l^2 \log^3 p)$.

To compute the exact order r of the Frobenius endomorphism in $\mathrm{PGL}_2(\mathbf{F}_l)$, Atkin computes in addition

$$\gcd(T^{p^i} - T, \Phi_l(j,T))$$

for $i = 2, 3, \ldots$. For $i = r$ one finds that the gcd is equal to $\Phi_l(j,T)$ and this is the smallest index i with this property. One knows by Prop.6.2 that r divides $l \pm 1$ and by Prop.6.3 one knows the parity of $(l \pm 1)/r$. This information can be used to speed up the computations.

By the last statement of Prop.6.2, the knowledge of r severely restricts the possibilities for $t \pmod{l}$. For instance, when $r = 1, 2, 3, 4$ one has that $t^2 \equiv 4p$, $4p$, p and $0 \pmod{l}$ respectively. For $r > 2$ the number of possibilities for t are at least cut in half: there are, a priori, $(l+1)/2$

possibilities for $t^2 \pmod l$. Since $l \pm 1$ is even and r divides $l \pm 1$, there are at most $\varphi(l \pm 1) \leq (l+1)/2$ primitive r-th roots of unity modulo l. By symmetry there are therefore at most $(l+1)/4$ possibilities for t^2 and hence at most $(l+1)/2$ for $t \pmod l$.

To find the correct value of t, Atkin [2] performs these calculations for several small primes l and then searches by means of a sophisticated baby-step-giant-step algorithm among the possible residue classes modulo the product of the primes l. We do not give the details of his method here.

In practice Atkin does not use j-invariants and the modular equation $\Phi_l(X, Y) = 0$, but related modular functions that satisfy an equation with fewer and smaller coefficients [1, 2, 17]. The resulting algorithm is practical for moderately large values of p. The computations with the modular polynomials can be done in polynomial time, but the final baby-step-giant-step search is not a polynomial time algorithm.

7. An equation for the isogenous curve.

In this section and the next we explain Elkies's algorithm to compute the trace t of the Frobenius endomorphism φ modulo small primes l of an elliptic curve E over $\mathbf{F}_p$, which is given by a Weierstraß-equation $Y^2 = X^3 + AX + B$. The main idea is to do this with computations similar to those in section 5, but employing a divisor $F(X)$ of small degree of the l-division polynomial $\Psi_l(X)$ rather than the division polynomial itself. See [2, 5, 10].

Elkies's algorithm. If the Frobenius endomorphism φ acts on the l-torsion points $E[l]$ as a 2×2-matrix with eigenvalues in $\mathbf{F}_l$, then there is an eigenspace C of order l, which is respected by the action of the Galois group. Using Proposition 6.2 of the previous section, this can be tested efficiently. Corresponding to the eigenspace C, there is a divisor $F(X) \in \mathbf{F}_p[X]$ of degree $(l-1)/2$ of the division polynomial $\Psi_l(X)$, whose zeroes are the $(l-1)/2$ distinct X-coordinates of the points in C. Elkies computes the eigenvalue λ corresponding to the eigenspace C. Since the product of the eigenvalues is equal to p, this implies that

$$t \equiv \lambda + p/\lambda \pmod l.$$

To compute λ, Elkies checks which of the relations

$$\varphi(X, Y) = (X^p, Y^p) = \lambda' \cdot (X, Y) \qquad \lambda' = 1, \ldots, l-1$$

hold on C, i.e., modulo $F(X)$. One has that $\lambda \equiv \lambda' \pmod{l}$. The bulk of the calculation is the computation of X^p and Y^p in the ring

$$\mathbf{F}_p[X,Y]/(F(X), Y^2 - X^3 - AX - B).$$

Since $F(X)$ has degree $(l-1)/2$ rather than $(l^2-1)/2$, these computations take only $O(l^2 \log^3 p + l^3 \log^2 p) = O(\log^5 p)$ operations. This is a crucial improvement over the running time $O(\log^7 p)$ of the corresponding part of the algorithm in section 5.

Elkies's idea *only* works for the primes l, for which φ has its eigenvalues in $\mathbf{F}_l$. That is, for about half the primes l: those that split in the field $\mathbf{Q}(\sqrt{t^2-4p})$. In order to apply it, one needs to compute the coefficients of the polynomial $F(X) \in \mathbf{F}_p[X]$. Fortunately this can be done in a very efficient way.

The algorithm proceeds in two steps. In this section we explain how to compute *an equation for the isogenous curve E/C*. This involves once more the modular equation $\Phi_l(X,Y) = 0$. In the process we also compute the *first* coefficient of $F(X)$: the sum of its roots. In section 8, we use the results of section 7 to compute *all the coefficients* of the polynomial $F(X)$. In both sections we follow Atkin's approach [2]. We assume throughout that E is not supersingular and that the j-invariant of E is not 0 or 1728. This is not a serious restriction: when $j = 0$ or 1728, the algorithms of section 4 are much more efficient and when E is supersingular it has $p+1$ rational points.

We introduce the following power series in $\mathbf{Z}[[q]]$:

Definition.

$$E_2(q) = 1 - 24 \sum_{n=1}^{\infty} \frac{nq^n}{1-q^n},$$

$$E_4(q) = 1 + 240 \sum_{n=1}^{\infty} \frac{n^3 q^n}{1-q^n},$$

$$E_6(q) = 1 - 504 \sum_{n=1}^{\infty} \frac{n^5 q^n}{1-q^n}$$

and

$$\Delta(q) = q \prod_{n=1}^{\infty} (1-q^n)^{24}.$$

There is the following well known relation due to Jacobi:

$$\Delta(q) = \frac{E_4(q)^3 - E_6(q)^2}{1728}.$$

Finally we introduce the j-function:

$$j(q) = \frac{E_4(q)^3}{\Delta(q)} = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \ldots$$

Clearly we have that $E_4^3 = j\Delta$ and $E_6^2 = (j - 1728)\Delta$. For any Laurent series $f(q) = \sum_n a_n q^n$ we let $f'(q)$ denote the Laurent series $q df/dq = \sum_n n a_n q^n$. The following proposition is well known.

Proposition 7.1. *The following equalities hold in* $\mathbf{Z}[[q]]$*:*

(i)

$$\frac{j'}{j} = -\frac{E_6}{E_4}, \qquad \frac{j'}{j-1728} = -\frac{E_4^2}{E_6};$$

(ii)

$$3\frac{E_4'}{E_4} = E_2 - \frac{E_6}{E_4}, \qquad 2\frac{E_6'}{E_6} = E_2 - \frac{E_4^2}{E_6};$$

(iii)

$$\frac{j''}{j'} = \frac{1}{6}E_2 - \frac{1}{2}\frac{E_4^2}{E_6} - \frac{2}{3}\frac{E_6}{E_4}.$$

Proof. To prove these relations we interpret q as $\exp(2\pi i\tau)$ with $\tau \in \mathbf{C}$, $\operatorname{Im}\tau > 0$ and we view the power series above as the Fourier expansions of some well known modular forms for the group $\mathrm{SL}_2(\mathbf{Z})$. The differential operator $f \mapsto q df/dq$ is just the usual differentiation of $f(q)$ with respect to the variable $2\pi i\tau$.

The logarithmic derivative j'/j of the modular j-function is modular of weight 2. So is E_6/E_4. Since both these forms have a simple pole at $j = 0$, they agree up to a constant which one easily checks to be equal to -1. Similarly, $j'/(j - 1728)$ and E_4^2/E_6 each have a simple pole at $j = 1728$ and therefore they agree up to a constant, which appears to be -1. This proves *(i)*.

Clearly the logarithmic derivative of Δ is equal to E_2. Taking the logarithmic derivative of the relations $E_4^3 = j\Delta$ and $E_6^2 = (j - 1728)\Delta$ gives the formulas in *(ii)*. Finally, combining the relations in part *(ii)* with the logarithmic derivative of the relation $j' = -jE_6/E_4$ of part *(i)* proves *(iii)*.

This completes the proof of the proposition.

Next we introduce the following power series in $\mathbf{Z}[\zeta, \frac{1}{\zeta(1-\zeta)}][[q]]$

$$x(\zeta; q) = \frac{1}{12} - 2\sum_{n=1}^{\infty} \frac{q^n}{(1-q^n)^2} + \sum_{n\in\mathbf{Z}} \frac{\zeta q^n}{(1-\zeta q^n)^2},$$
$$y(\zeta; q) = \frac{1}{2}\sum_{n\in\mathbf{Z}} \frac{\zeta q^n(1+\zeta q^n)}{(1-\zeta q^n)^3}.$$

These are really power series in q. For example,

$$\sum_{n\in\mathbf{Z}} \frac{\zeta q^n}{(1-\zeta q^n)^2} = \frac{\zeta}{(1-\zeta)^2} + \sum_{n=1}^{\infty}\left(\frac{\zeta q^n}{(1-\zeta q^n)^2} + \frac{\zeta^{-1}q^n}{(1-\zeta^{-1}q^n)^2}\right).$$

Proposition 7.2. *We have the following equalities of power series:*

(i)

$$y^2 = x^3 - \frac{E_4(q)}{48}x + \frac{E_6(q)}{864}.$$

Here $y = y(\zeta; q)$ and $x = x(\zeta; q)$.

(ii)

$$\sum_{\zeta\in\mu_l, \zeta\neq 1} x(\zeta; q) = \frac{1}{12} l\left(E_2(q) - lE_2(q^l)\right)$$

Proof. If we interpret q as $e^{2\pi i\tau}$ for some $\tau \in \mathbf{C}$ with $\operatorname{Im}\tau > 0$, and $\zeta = e^{2\pi i z}$, then $x(\zeta; q)$ is just $(2\pi i)^2\wp(z;\tau)$ and $y(\zeta; q) = (2\pi i)^3\wp'(z;\tau)/2$ (see [12, Chpt.4]) Part *(i)* then follows from the usual properties of the Weierstraß $\wp$-function. To obtain the equality in *(ii)*, use the series expansions and the elementary fact that

$$\sum_{\zeta\in\mu_l, \zeta\neq 1} \frac{\zeta}{(1-\zeta)^2} = \frac{1-l^2}{12}$$

and

$$\sum_{\zeta\in\mu_l} \frac{\zeta X}{(1-\zeta X)^2} = \frac{l^2 X^l}{(1-X^l)^2}.$$

We leave the calculations to the reader.

Theorem 7.3. *Let $\Phi_l(X,Y) \in \mathbf{Z}[X,Y]$ denote the modular equation for $X_0(l)$. Let l be a prime and let $\tilde{\jmath}$ denote the Laurent series $j(q^l)$.*

(i) Then

$$\Phi_l(j,\tilde{\jmath}) = 0.$$

(ii) We have the following identity of Laurent series

$$j'\Phi_X(j,\tilde{\jmath}) + l\tilde{\jmath}'\Phi_Y(j,\tilde{\jmath}) = 0.$$

Here Φ_X denote the partial derivative $\partial\Phi_l/\partial X$ and similarly, $\Phi_Y = \partial\Phi_l/\partial Y$.

(iii) We have the following identity of power series

$$\frac{j''}{j'} - l\frac{\tilde{\jmath}''}{\tilde{\jmath}'} = -\frac{j'^2\Phi_{XX}(j,\tilde{\jmath}) + 2lj'\tilde{\jmath}'\Phi_{XY}(j,\tilde{\jmath}) + l^2\tilde{\jmath}'^2\Phi_{YY}(j,\tilde{\jmath})}{j'\Phi_X(j,\tilde{\jmath})}.$$

Here the notation is as in part (ii). For instance, Φ_{XX} denotes $\partial^2\Phi_l/\partial X^2$, etc.

Proof. Interpret q as $\exp(2\pi i\tau)$ with $\tau \in \mathbf{C}$, $\mathrm{Im}\tau > 0$. The "Tate" curve

$$\mathbf{C}/2\pi i(\mathbf{Z} + \tau\mathbf{Z}) \underset{\cong}{\xrightarrow{\exp}} \mathbf{C}^*/q^{\mathbf{Z}}$$

has j-invariant equal to $j(q)$ and the curve $\mathbf{C}^*/q^{l\mathbf{Z}}$ has j-invariant equal to $\tilde{\jmath} = j(q^l)$. The map $z \mapsto z^l$ induces an isogeny of degree l with kernel the group of l-th roots of unity μ_l:

$$0 \longrightarrow \mu_l \longrightarrow \mathbf{C}^*/q^{\mathbf{Z}} \longrightarrow \mathbf{C}^*/q^{l\mathbf{Z}} \longrightarrow 0.$$

Therefore the relation in *(i)* holds. Differentiating the identity in *(i)*, we obtain the identity in *(ii)*. Differentiating once more and dividing this relation by $j'\Phi_X(j,\tilde{\jmath}) = -l\tilde{\jmath}'\Phi_Y(j,\tilde{\jmath})$, we obtain the relation in *(iii)*.

This proves the theorem.

Now we can explain Elkies's algorithm.

Equation for the isogenous curve. Let E be an non-supersingular elliptic curve over $\mathbf{F}_p$ given by the usual equation $Y^2 = X^3 + AX + B$ and let $j \in \mathbf{F}_p$ be its j-invariant. Let $\Phi_l(X,Y)$ denote the modular equation of level l. We first compute

$$\gcd(T^p - T, \Phi_l(j,T))$$

in the ring $\mathbf{F}_p[T]$, just as we did in Atkin's algorithm in section 6. If the gcd is 1, the algorithm does not apply. If the gcd is non-trivial, then it has all its roots (usually two) in $\mathbf{F}_p$ and we compute one such root $\tilde{\jmath}$. By Prop.6.1, $E[l]$ admits a one dimensional eigenspace C for the action of φ such that $\tilde{\jmath}$ is the j-invariant of the isogenous curve E/C.

A Weierstraß equation

$$Y^2 = X^3 + \tilde{A}X + \tilde{B}$$

for the isogenous curve $\tilde{E} = E/C$ is given by:

$$\tilde{A} = -\frac{1}{48}\,\frac{\tilde{\jmath}'^2}{\tilde{\jmath}(\tilde{\jmath}-1728)},$$
$$\tilde{B} = -\frac{1}{864}\,\frac{\tilde{\jmath}'^3}{\tilde{\jmath}^2(\tilde{\jmath}-1728)},$$

where $\tilde{\jmath}' \in \mathbf{F}_p$ is given by

$$\tilde{\jmath}' = -\frac{18}{l}\,\frac{B}{A}\,\frac{\Phi_X(j,\tilde{\jmath})}{\Phi_Y(j,\tilde{\jmath})}j.$$

To justify this, we invoke Deuring's Lifting Theorem [12, Chpt. 13] and we lift the isogeny $E \longrightarrow E/C$ to characteristic 0. More precisely, there exists $q = \exp(2\pi i\tau) \in \mathbf{C}$ such that $E_4(q)$, $E_6(q)$, are integers in some number field, and there is a prime ideal $\mathfrak{P}$ with residue field $\mathbf{F}_p$ of the ring of integers of this number field such that the reduction modulo $\mathfrak{P}$ of the isogeny

$$0 \longrightarrow \mu_l \longrightarrow \mathbf{C}^*/q^{\mathbf{Z}} \longrightarrow \mathbf{C}^*/q^{l\mathbf{Z}} \longrightarrow 0.$$

gives the isogeny

$$0 \longrightarrow C \longrightarrow E \longrightarrow E/C \longrightarrow 0$$

over $\mathbf{F}_p$. The curve $\mathbf{C}^*/q^{\mathbf{Z}}$ admits a Weierstraß-equation

$$Y^2 = X^3 - \frac{E_4(q)}{48}X + \frac{E_6(q)}{864}$$

with $A \equiv -E_4(q)/48 \pmod{\mathfrak{P}}$ and $B \equiv -E_6(q)/864 \pmod{\mathfrak{P}}$. Similarly $\mathbf{C}^*/q^{l\mathbf{Z}}$ admits an equation

$$Y^2 = X^3 - \frac{E_4(q^l)}{48}X + \frac{E_6(q^l)}{864}$$

with $\tilde{A} \equiv -E_4(q^l)/48 \pmod{\mathfrak{P}}$ and $\tilde{B} \equiv -E_6(q^l)/864 \pmod{\mathfrak{P}}$. Its j-invariant satisfies $j(q^l) \equiv \tilde{\jmath} \pmod{\mathfrak{P}}$.

This enables us to compute the Weierstraß-equation of the isogenous curve: we know E_4, E_6, j and $\tilde{\jmath}$ modulo $\mathfrak{P}$; using Prop.7.1*(i)* and Theorem 7.3*(ii)* we calculate $\tilde{\jmath}' \pmod{\mathfrak{P}}$. Applying the formulas of Prop. 7.1 to $\tilde{\jmath}$ and $\tilde{\jmath}'$ we find $E_4(q^l) \pmod{\mathfrak{P}}$ and $E_6(q^l) \pmod{\mathfrak{P}}$. This gives us $\tilde{A}, \tilde{B} \in \mathbf{F}_p$.

Finally we compute the sum $p_1 \in \mathbf{F}_p$ of the X-coordinates of the points in the kernel C of the isogeny. The value of p_1 is needed in section 8. To this end we use the fact that the map $\zeta \mapsto (x(\zeta;q), y(\zeta;q))$ gives an isomorphism between $\mathbf{C}^*/q^{\mathbf{Z}}$ and the $\mathbf{C}$-valued points of $Y^2 = X^3 - E_4(q)/48X + E_6(q)/864$. The points in C are precisely the ones that correspond to $\zeta \in \mu_l$. The value of $p_1 \pmod{\mathfrak{P}}$ can now be computed by combining Prop. 7.1*(iii)*, Prop. 7.2*(ii)* and Theorem 7.3*(iii)*.

Note that, even though we used the analytic theory to justify the computations, all calculations take place in $\mathbf{F}_p$.

This approach does not work if $\Phi_X(j,\tilde{\jmath}) = \Phi_Y(j,\tilde{\jmath}) = 0$, since in this case the relation of Thm.7.3*(ii)* vanishes. This happens precisely when $(j,\tilde{\jmath})$ is a singular point of the modular curve $\Phi_l(X,Y) = 0$ over $\mathbf{F}_p$. We claim that in that case the point $(j,\tilde{\jmath})$ is the reduction of a singular point over $\mathbf{C}$. Indeed if this would not be the case, then there would be a Zariski open neighborhood U of $(j,\tilde{\jmath}) \pmod{p}$ in the curve $\Phi_l(X,Y) = 0$ in $\mathbf{P}^1 \times \mathbf{P}^1$ over $\mathbf{Z}$ which is regular in codimension 1. It then follows from a slight generalization of [11, Chpt.II, Prop.8.23] that the curve given by $\Phi_l(X,Y) = 0$ is normal over $\mathbf{F}_p$. However, its normalization is the modular curve $X_0(l)$ and this curve is well known to be smooth in characteristic p. Therefore the point $(j,\tilde{\jmath})$ is the reduction of a singular point over $\mathbf{C}$. I thank Bas Edixhoven for explaining this to me.

By the Kronecker congruence relation $\Phi_l(X,Y) \equiv (X^l - Y)(X - Y^l) \pmod{l}$ over $\overline{\mathbf{F}}_l$. Therefore all singular points of the curve modulo l are ordinary double points and hence the same is true over $\mathbf{C}$. This implies there are two isogenies $f, g : E \longrightarrow \tilde{E}$ over $\mathbf{C}$ of degree l which are not equal, not even up to an automorphism. This in turn implies that the isogeny $\check{g}f : E \longrightarrow E$ of degree l^2 is not equal to l times an automorphism. Here $\check{g}$ denotes the dual isogeny of g. We conclude that E admits an endomorphism of degree l^2 which has a cyclic kernel. This implies that the discriminant Δ of the endomorphism ring of the lifted complex curve E satisfies $|\Delta| \leq 4l^2$. Since the curve E over $\mathbf{F}_p$ is not supersingular, Δ is also the discriminant of

$\mathrm{End}_{\mathbf{F}_p}(E)$. Since $l = O(\log p)$, the prime l and the discriminant Δ are very small with respect to p. There are very few possibilities for Δ. Therefore it is very easy to compute $\#E(\mathbf{F}_p)$ using the methods of section 4.

The discriminant of an endomorphism ring of a "random" curve as in the introduction usually has the same order of magnitude as $-4p$. For such curves the above phenomenon can only occur when E is supersingular. As has been pointed out before, the chance that a "random" elliptic curve is supersingular is very small; the probability is bounded by $O(p^{-1/2})$.

In practice one does not work with the modular equations $\Phi_l(X, Y)$. These equations have many huge coefficients. Atkin [2] and Morain [17] use different modular functions to generate the function field of the curve $X_0(l)$. Their functions are more convenient to work with, since they give rise to equations which have fewer and smaller coefficients.

8. The kernel of the isogeny.

Let E be the elliptic curve given by $Y^2 = X^3 + AX + B$ over $\mathbf{F}_p$. We use the notation of the previous section: C is a subgroup of $E[l]$ of order l, which is respected by the action of the Galois group. The corresponding isogeny $f : E \longrightarrow E/C$ is defined over $\mathbf{F}_p$. Let $\tilde{A}$ and $\tilde{B}$ denote the coefficients of a Weierstraß-equation for E/C and let p_1 denote the sum of the X-coordinates of the points in C.

In this section we explain how, given the two Weierstraß-equations and p_1, to obtain the polynomial $F(X) \in \mathbf{F}_p[X]$ of degree $(l-1)/2$ that vanishes precisely on the X-coordinates of the points in C. As in the previous section we use the analytic theory to justify our method, but all calculations are done modulo p. In this section we use the Taylor series expansion of the Weierstraß $\wp$-function rather than its Fourier series expansion.

As explained in the previous section, there is an elliptic curve over a number field K, complex analytically isomorphic to $\mathbf{C}$ modulo a lattice $\omega_1\mathbf{Z} + \omega_2\mathbf{Z}$, such that the isogeny

$$\mathbf{C}/(\omega_1\mathbf{Z} + \omega_2\mathbf{Z}) \longrightarrow \mathbf{C}/(\omega_1\mathbf{Z} + l\omega_2\mathbf{Z})$$

given by $z \mapsto lz$, modulo a prime ideal $\mathfrak{P}$ of K with residue field $\mathbf{F}_p$ is the l-isogeny $E \longrightarrow E/C$. We also write $Y^2 = X^3 + AX + B$ for the Weierstraß-equation of the curve over $\mathbf{C}$ which reduces to E modulo $\mathfrak{P}$ and $Y^2 = X^3 + \tilde{A}X + \tilde{B}$ for the isogenous curve, which reduces to E/C modulo $\mathfrak{P}$.

It is convenient to work with the isogeny

$$\mathbf{C}/(\omega_1\mathbf{Z}+\omega_2\mathbf{Z}) \longrightarrow \mathbf{C}/(\frac{1}{l}\omega_1\mathbf{Z}+\omega_2\mathbf{Z})$$

given by $z \mapsto z$. The kernel of this isogeny is equal to the kernel of the isogeny above, but the Weierstraß-equation of this isogenous curve is given by

$$Y^2 = X^3 + \frac{\tilde{A}}{l^4}X + \frac{\tilde{B}}{l^6}.$$

Let $\wp(z)$ be the Weierstraß function associated to the lattice $L = \omega_1\mathbf{Z}+\omega_2\mathbf{Z}$ and let

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega\in L\\ \omega\neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right) = \frac{1}{z^2} + \sum_{k=1}^{\infty} c_k z^{2k}$$

be the Laurent series of the Weierstraß $\wp$-function at infinity. One has

$$c_1 = -\frac{A}{5}, \qquad c_2 = -\frac{B}{7},$$
$$c_k = \frac{3}{(k-2)(2k+3)}\sum_{j=1}^{k-2} c_j c_{k-1-j}, \qquad \text{for } k \geq 3.$$

Similarly, let $\tilde{\wp}(z)$ be the Weierstraß function associated to the lattice $\frac{\omega_1}{l}\mathbf{Z}+\omega_2\mathbf{Z}$:

$$\tilde{\wp}(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} \tilde{c}_k z^{2k}.$$

One has

$$\tilde{c}_1 = -\frac{1}{5}\,\frac{\tilde{A}}{l^4}, \qquad \tilde{c}_2 = -\frac{1}{7}\,\frac{\tilde{B}}{l^6},$$
$$\tilde{c}_k = \frac{3}{(k-2)(2k+3)}\sum_{j=1}^{k-2} \tilde{c}_j \tilde{c}_{k-1-j}, \qquad \text{for } k \geq 3.$$

Note that all the c_k and $\tilde{c}_k$ are contained in the number field K. The denominators of the c_k and $\tilde{c}_k$ are only divisible by primes less than $2k+4$. We introduce the Weierstraß ζ-function; it is the Laurent series given by

$$\zeta(z) = \frac{1}{z} - \sum_{k=1}^{\infty} \frac{c_k}{2k+1} z^{2k+1}.$$

We have that $\zeta'(z) = -\wp(z)$. The function $\tilde{\zeta}$ is defined in a similar way:

$$\tilde{\zeta}(z) = \frac{1}{z} - \sum_{k=1}^{\infty} \frac{\tilde{c}_k}{2k+1} z^{2k+1}.$$

Lemma 8.1. *For every $a \in \mathbf{C}$ one has that*

$$\zeta(z+a) + \zeta(z-a) - 2\zeta(z) = \frac{\wp'(z)}{\wp(z) - \wp(a)}$$

as meromorphic functions.

Proof. We interpret the series as meromorphic functions on $\mathbf{C}$. Take the difference of the left hand side and the right hand side and differentiate. This gives a meromorphic function on the torus $\mathbf{C}/(\omega_1\mathbf{Z}+\omega_2\mathbf{Z})$. Inspection of the pole divisors of the summands easily shows that the function has no poles and is hence constant. Letting z tend to 0, one sees that the constant is 0. Therefore the function itself is also constant. Since $\zeta(z)$ is an odd function, one sees that it tends to zero as z tends to 0. This proves the lemma.

Lemma 8.2. *One has*

(i)

$$\tilde{\wp}(z) = \sum_{i=1}^{l-1} \wp(z + \frac{i}{l}\omega_1) - \sum_{i=1}^{l-1} \wp(\frac{i}{l}\omega_1),$$

(ii)

$$\sum_{-l/2<i<l/2} \zeta(z + \frac{i}{l}\omega_1) = \tilde{\zeta}(z) - z\sum_{i=1}^{l-1} \wp(\frac{i}{l}\omega_1)$$

as meromorphic functions.

Proof. *(i)* The function $\tilde{\wp}(z) = \sum_{i=0}^{l-1} \wp(z + \frac{i}{l}\omega_1)$ is periodic modulo the lattice $\mathbf{C}/(\frac{\omega_1}{l}\mathbf{Z} + \omega_2\mathbf{Z})$. It is easy to see that it has no poles. Therefore the function is constant and letting z tend to 0, one sees that this constant is, in fact, equal to $\sum_{i=0}^{l-1} \wp(\frac{i}{l}\omega_1)$.

(ii) Differentiating $-\tilde{\zeta}(z) + \sum_{-l/2<i<l/2} \zeta(z + \frac{i}{l}\omega_1)$ one obtains the function

$$\tilde{\wp}(z) \;-\; \sum_{-l/2<i<l/2} \wp(z + \frac{i}{l}\omega_1)$$

which, by *(i)* is equal to $-\sum_{i=0}^{l-1}\wp(\frac{i}{l}\omega_1)$. Integrating, we see that the function

$$-\tilde{\zeta}(z) + \sum_{-l/2<i<l/2} \zeta(z+\frac{i}{l}\omega_1) + z\sum_{i=1}^{l-1}\wp(\frac{i}{l}\omega_1)$$

is constant. Letting z tend to 0 and using the fact that $\zeta(z)$ is an odd function, one finds that the constant is 0. This proves the lemma.

Theorem 8.3. *Let l be prime and let $F(X)$ be the polynomial that vanishes on the X-coordinates of the points in the kernel of the isogeny*

$$\mathbf{C}/(\omega_1\mathbf{Z}+\omega_2\mathbf{Z}) \longrightarrow \mathbf{C}/(\frac{\omega_1}{l}\mathbf{Z}+\omega_2\mathbf{Z}).$$

Then

$$z^{l-1}F(\wp(z)) = \exp\left(-\frac{1}{2}p_1z^2 - \sum_{k=1}^{\infty}\frac{\tilde{c}_k - lc_k}{(2k+1)(2k+2)}z^{2k+2}\right).$$

Proof. By Lemma 8.1 we have, for $i = 1,2,\dots,(l-1)/2$,

$$\zeta(z+\frac{i}{l}\omega_1) + \zeta(z-\frac{i}{l}\omega_1) - 2\zeta(z) = \frac{\wp'(z)}{\wp(z)-\wp(\frac{i}{l}\omega_1)}.$$

Adding these equations gives

$$-l\zeta(z) + \sum_{-l/2<i<l/2}\zeta(z+\frac{i}{l}\omega_1) = \sum_{i=1}^{(l-1)/2}\frac{\wp'(z)}{\wp(z)-\wp(\frac{i}{l}\omega_1)}.$$

By Lemma 8.2 this becomes

$$-l\zeta(z) + \tilde{\zeta}(z) - p_1z = \sum_{i=1}^{(l-1)/2}\frac{\wp'(z)}{\wp(z)-\wp(\frac{i}{l}\omega_1)}.$$

By inverting the process of differentiating logarithmically, we find

$$z^{1-l}\exp\left(-\frac{1}{2}p_1z^2 - \sum_{k=1}^{\infty}\frac{\tilde{c}_k - lc_k}{(2k+1)(2k+2)}z^{2k+2}\right) = \alpha\prod_{i=1}^{(l-1)/2}(\wp(z)-\wp(\frac{i}{l}\omega_1))$$

for some $\alpha \in \mathbf{C}^*$. Inspection of the coefficient of z^{1-l} gives that $\alpha = 1$ as required.

Theorem 8.3 enables one to compute $F(X) = X^{(l-1)/2} + a_{\frac{l-3}{2}} X^{(l-3)/2} + \ldots + a_0$ in an efficient way. The first few coefficients of F are given by

$$\begin{aligned}
a_{\frac{l-3}{2}} &= -\frac{p_1}{2}, \\
a_{\frac{l-5}{2}} &= \frac{1}{8}p_1^2 - \frac{\tilde{c}_1 - lc_1}{12} - \frac{l-1}{2}c_1, \\
a_{\frac{l-7}{2}} &= -\frac{1}{48}p_1^3 - \frac{\tilde{c}_2 - lc_2}{30} + p_1\frac{\tilde{c}_1 - lc_1}{24} - \frac{l-1}{2}c_2 + \frac{l-3}{4}c_1 p_1, \\
&\vdots
\end{aligned}$$

To obtain the coefficients of the polynomial $F(X) \in \mathbf{F}_p[X]$, we inductively compute the coefficients c_k and $\tilde{c}_k$ from A, B and $\tilde{A}$,$\tilde{B}$ respectively. Finally we use Theorem 8.3 and the value of p_1 computed in section 7, to compute the coefficients a_k (mod $\mathfrak{P}$). By the analytic theory, the resulting polynomial vanishes on the X-coordinates of the points in C on the curve E over $\mathbf{F}_p$.

Note that even though we have used the complex analytic theory to justify the computations, the entire calculation can be done with numbers in $\mathbf{F}_p$. The formulas for the c_k and the a_k involve denominators having only small prime divisors. This is harmless since p is very large. This phenomenon creates problems when one tries to extend the algorithms of section 7 and 8 to large finite fields of small characteristic [9, 16].

Bibliography

[1] Atkin, A.O.L.: The Number of Points an an Elliptic Curve Modulo a Prime, manuscript, Chicago IL, January 1, 1988.

[2] Atkin, A.O.L.: Several public email messages, 1990-1992.

[3] Atkin, A.O.L and Morain, F.: Elliptic curves and primality proving, *Math. Comp.* **61** (1993), 29–67.

[4] Batut, C., Bernardi, D., Cohen, H. and Olivier, M.: *User's Guide to PARI-GP*, version 1.30, Bordeaux February 1, 1990.

[5] Charlap, L.S., Coley, R. and Robbins, D.P.: Enumeration of rational Points on Elliptic Curves over Finite Fields, manuscript, Princeton 1992.

[6] Cohen, H.: *A course in computational number theory*, Graduate Texts in Math. **138**, Springer-Verlag, Berlin Heidelberg New York 1993.

[7] Cornacchia, G.: Su di un metodo per la risoluzione in numeri interi dell'equazione $\sum_{h=0}^{n} C_h x^{n-h} y^h = P$. *Giornale di Mat. di Battaglini* **46** (1908), 33–90.

[8] Couveignes, J.-M. and Morain, F.: Schoof's algorithm and isogeny cycles, *Proceedings of the ANTS conference, Ithaca 1994*, Lecture Notes in Computer Science 1994.

[9] Couveignes, J.-M.: Computing isogenies in low characteristic, Thesis Bordeaux 1994. To appear.

[10] Elkies, N.D.: Explicit Isogenies, manuscript, Boston MA, 1992.

[11] Hartshorne, R.: *Algebraic Geometry*, Graduate Texts in Math. **52**, Springer-Verlag, Berlin Heidelberg New York 1977.

[12] Lang, S.: *Elliptic Functions*, Addison-Wesley, Reading MA 1973.

[13] Lehmann, F., Maurer, M., Müller, V. and Shoup, V.: Counting the number of points on elliptic curves over finite fields of characteristic greater than three. Preprint 1994.

[14] Lenstra, H.W.: Elliptic curves and number-theoretical algorithms, *Proc. of the International Congress of Math.*, Berkeley 1986, 99–120.

[15] Lenstra, H.W.: Letter to H. Cohen, August 16, 1990.

[16] Menezes, A.J., Vanstone, S.A. and Zuccherato, R.J.: Counting points on elliptic curves over $\mathbf{F}_{2^m}$, *Math. Comp.* **60** (1993), 407–420.

[17] Morain, F.: Calcul du nombre de points sur une courbe elliptique dans un corps fini: aspects algorithmiques, Proceedings of the Journées Arithmétiques, Bordeaux 1993.

[18] Schoof, R.: Elliptic curves over finite fields and the computation of square roots mod p, *Math. Comp.* **44** (1985), 483–494.

[19] Shanks, D.: Class Number, a Theory of Factorization, and Genera, *1969 Number Theory Institute*, Proc. of Symp. in Pure Math. **20**, AMS, Providence RI 1971.

[20] Shanks, D.: Five number theoretical algorithms, *Proc. 2nd Manitoba conference on numerical math., (Congressus Numerantium VII, Univ. Manitoba Winnipeg)*, (1972), 51–70.

[21] Silverman, J.: *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, Berlin Heidelberg New York 1986.

René SCHOOF
Dipartimento di Matematica
2ª Università di Roma "Tor Vergata"
I-00133 Roma ITALY
e-mail : schoof@volterra.science.unitn.it