AN EXPOSITION OF THE SEA ALGORITHM

JÁNOS A. CSIRIK

Abstract. The Schoof–Elkies–Atkin algorithm is an efficient way to count the number of points on an elliptic curve defined over a large prime field. This expository paper describes the algorithm in sufficient detail to allow a reader not familiar with arithmetic geometry to implement the algorithm. The mathematical background for the technique is then given.

1. Introduction

Let p be a large (odd) prime and let

$$E: \qquad y^2 = x^3 + a_4 x + a_6$$

be an elliptic curve, where a_4 and a_6 are given fixed integers. In the case where p does not divide $4a_4^3 + 27a_6^2$, E can be reduced to an elliptic curve over $\mathbb{F}_p$. The number of points of E over $\mathbb{F}_p$, denoted by $\#E(\mathbb{F}_p)$, is of cryptographic interest, since the properties of this number determine the security of elliptic curve cryptosystems based on E against various known attacks.

The first polynomial time algorithm for determining the number of rational points on an elliptic curve defined over a finite field is due to Schoof. He used calculations with torsion points on the curve to arrive at the number of points. At first Schoof's algorithm was considered impractical, but Elkies suggested the use of "good" primes (now known as Elkies primes), where isogenies and modular curves can be involved to speed up the calculation. Atkin also made a number of important contributions to the algorithm, which then became known as the Schoof–Elkies–Atkin (SEA) algorithm. Further improvements were later proposed by Dewaghe and Couveignes–Dewaghe–Morain. The SEA algorithm was implemented by Morain, Müller, and Izu et al.

Schoof's seminal paper [18] describes the original algorithm. He later also published a paper [19] that is a lovely overview of the developments in the subject up to 1995. Elkies' paper [9] describes the ideas of his original manuscript [8] and contains many other theoretical insights and illuminating examples. The implementations of Morain and Müller are described in [15] and [16]. The implementation of Izu, Kogure, Noro and Yokoyama, which focuses on speeding up the algorithm as much as possible, is described in [13]. Dewaghe's improvement is published in [7], see also Section 3.13. The improvement by Couveignes–Dewaghe–Morain is published in [5], see also Section 4.3. Atkin never formally published his contributions described in [1], but they are discussed extensively in [9, 19].

This paper, which is not aimed at the experts in the area, describes in detail a reasonably fast implementation of the SEA algorithm that is closely modeled upon Morain's. The algorithm considered below is probabilistic and, for a 200-bit prime p, succeeds with a probability of about 3/4 (which can be brought arbitrarily close to 1 by enlarging the set A of auxiliary primes below). The algorithm implemented

on a typical personal computer takes several minutes to find the number of points on a typical curve over $\mathbb{F}_p$, where p has 200 bits.

It is known that

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

where t is an integer which satisfies the Hasse bound

$$-2\sqrt{p} \leq t \leq 2\sqrt{p}.$$

The algorithm works by calculating t modulo several small auxiliary primes ℓ. When the product of the auxiliary primes exceeds $4\sqrt{p}$, the Chinese Remainder Theorem is used to recover the exact value of t, and hence that of $\#E(\mathbb{F}_p)$.

The algorithm works its way though a fixed list of 40 candidates for auxiliary primes given below. For each candidate ℓ, a calculation has to be carried out to generate a certain polynomial Ψ_ℓ that is necessary for further calculations with this ℓ. These polynomials Ψ_ℓ do not depend on the curve E under consideration and hence might be precomputed and stored if memory allows. Then for any elliptic curve E we can quickly decide if our algorithm applies (the probability that the algorithm applies for a specific E and ℓ is $1/2$). For those curves where the algorithm applies, we can determine t modulo ℓ.

When we finished with all our candidates for the auxiliary primes, we can look at the elliptic curve and check whether the product of auxiliary primes that worked exceeds $4\sqrt{p}$ or not. In the former case, we succeeded in determining t.

A typical application for this point counting would be to take a random prime p and a random elliptic curve E over $\mathbb{F}_p$, with the intention of finding an E with $\#E(\mathbb{F}_p) = xr$, where r is a prime and x is small. Given such a curve, a point P of order r can be located easily and the pair (E, P) could be used for a number of cryptographic algorithms, such as Diffie-Hellman key exchange, El Gamal encryption, etc. If we use 200-bit primes for p and require $x \leq 32$, then the probability that $\#E = xr$ is about 2.5%, so we expect to have to run our algorithm on about 55 curves.[1]

Section 2 describes the algorithm in detail. Section 3 presents the mathematical background of the algorithm. Section 4 presents ideas by which the algorithm could be improved. Section 5 contains certain tables of data that need to be hardwired into a program implementing this algorithm.

2. The Algorithm

2.1. **Overview.** The set A of potential auxiliary primes is the union of the set A_s of small primes and the set A_l of larger primes. For each $\ell \in A$, we need to determine a polynomial $\Psi_\ell(F, J) \in \mathbb{Z}[F, J]$. For $\ell \in A_\mathrm{s}$, this is stored in the program. For $\ell \in A_\mathrm{l}$, Ψ_ℓ must be calculated by determining a number of coefficients of a certain q-series $f(q) \in \mathbb{Z}[[q]]$ and carrying out certain algebraic operations on it. The polynomials Ψ_ℓ do not depend on the elliptic curve under consideration and therefore may be pre-calculated and stored if there is enough space for them (they require just under a half megabyte to store).

We start out with a given prime p and an elliptic curve

$$E: \qquad y^2 = x^3 + a_4 x + a_6.$$

[1] The chance that a randomly selected integer of similar size is of the form xr as above is about 3%. For more details, see [12, 10]

We need to check a few simple things and calculate the j-invariant $j = j(E) = 6912a_4^3/(4a_4^3 + 27a_6^2) \in \mathbb{F}_p$.

Working over $\mathbb{F}_p$, we plug in $J = j \in \mathbb{F}_p$ into $\Psi_\ell(F, J)$ and find all roots $f \in \mathbb{F}_p$ that satisfy

$$\Psi_\ell(f, j) = 0.$$

For each of these f, we need to find all $\tilde{j}$ such that

$$\Psi_\ell(f, \tilde{j}) = 0.$$

For all possible pairs $(f, \tilde{j})$, we do various operations involving Ψ_ℓ and its partial derivatives to obtain the quantities $\tilde{a}_4, \tilde{a}_6, p_1$. For any quintuplet $(a_4, a_6, \tilde{a}_4, \tilde{a}_6, p_1)$, we can determine whether it is "valid", and if so, we can generate a "kernel polynomial" $h(X) \in \mathbb{F}_p[X]$ of degree $d = (\ell - 1)/2$. Given a kernel polynomial $h(X)$, we can determine the "eigenvalue" $e \in \mathbb{F}_p$ and conclude that $t \equiv e + p/e \pmod{\ell}$.

An application of the Chinese Remainder Theorem completes the calculation.

The remaining subsections of Section 2 explain the details of the steps described above.

2.2. **Determination of Ψ_ℓ for $\ell \in A_{\mathrm{s}}$.** Set $A_{\mathrm{s}} = \{3, 5, 7, 11, 13, 17, 19, 23\}$. For $\ell \in A_{\mathrm{s}}$, the polynomial Ψ_ℓ is to be found in the table of Section 5.3.

2.3. **Determination of f for $\ell \in A_{\mathrm{l}}$.** Let A_{l} be the set of prime numbers from 29 through 197, except for 37, 43, 67 and 163. We need to calculate using q-series (power series in the variable q, possibly with a finite number of negative powers of q). Let $\sigma_k(n)$ denote the sum of kth powers of the positive divisors of n. The following q-series will be needed.

$$\begin{aligned}
E_4(q) &= 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n = 1 + 240q + 2160q^2 + 6720q^3 + \cdots \\
E_6(q) &= 1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n = 1 - 504q - 16632q^2 - 122976q^3 - \cdots \\
j(q) &= 1728E_4(q)^3/(E_4(q)^3 - E_6(q)^2) = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots \\
\bar{\eta}(q) &= \prod_{n=1}^{\infty}(1 - q^n) = \sum_{k=-\infty}^{\infty}(-1)^k q^{(3k^2+k)/2} = 1 - q - q^2 + q^5 + \cdots
\end{aligned}$$

For each ℓ, we need to look up the suitable polynomial P_ℓ from the table in Section 5.1. Let v denote the degree of P_ℓ. Calculate the coefficients $a_k \in \mathbb{F}_\ell$ such that

$$P_\ell(j(q))\bar{\eta}(q)\bar{\eta}(q^\ell) \equiv \sum_{k=-v}^{2\ell v - v} a_k q^k + O(q^{2\ell v - v + 1}) \pmod{\ell}.$$

(This can be done by multiplying out the product on the left hand side modulo ℓ and reading off the coefficients.) For each a_k, let b_k be the least absolute remainder of a_k mod ℓ (the integer with the smallest possible absolute value that reduces to a_k modulo ℓ). Now the f we are searching for is the q-series

$$\left(\sum_{k=-v}^{2\ell v - v} b_k q^k + O(q^{2\ell v - v + 1})\right) / (\bar{\eta}(q)\bar{\eta}(q^\ell)).$$

This will enable us to determine the coefficients of q^k in $f(q)$ for all $k \leq 2v\ell - v$.

2.4. **Determination of Ψ_ℓ for $\ell \in A_1$.** This calculation involves manipulation of q-series. To simplify notation, we write all q-series as though all the coefficients were known, but in fact we need to calculate only as many coefficients as our knowledge of f from the previous step will allow. The previous step calculated just enough coefficients in f for this step to work correctly (see Section 3.14 for details).

For the calculation that follows, we shall need the q-expansions of $f, f^2, \ldots, f^\ell$. Let

$$(f(q))^k = \sum_n a(n,k)q^n.$$

For each $1 \le k \le \ell$, let

$$s_k(q) = \sum_n \ell a(\ell n, k)q^n.$$

For each $1 \le k \le \ell$, let

$$c_k(q) = -\left(s_k(q) + \sum_{r=1}^{k-1} c_{k-r}(q)s_r(q)\right)/k.$$

Finally, let $C_1(q) = -f + c_1(q)$, $C_{\ell+1}(q) = -fc_\ell(q)$ and for each $2 \le k \le \ell$,

$$C_k(q) = -fc_{k-1}(q) + c_k(q).$$

It turns out that for each $1 \le k \le \ell + 1$, there is a polynomial G_k such that

$$G_k(j(q)) \equiv C_k(q) \pmod{p}.$$

Since the q-expansion of j starts with $q^{-1} + \cdots$, the coefficients of G_k are easy to determine. Indeed, let d be the order of the pole of C_k at $q = 0$, so that $C_k(q) = aq^{-d} + \cdots$, where a is some non-zero constant. Then $C_k(q) = aj(q)^d + C'_k(q)$, where $C'_k(q) = C_k(q) - aj(q)^d$ is a polynomial in $j(q)$, with a pole of order strictly less than d. Iterating this procedure, we obtain all the coefficients of G_k.

Once we determined all the G_k, we can write down Ψ_ℓ as

$$\Psi_\ell(F, J) = F^{\ell+1} + \sum_{i=1}^{\ell} G_i(J)F^{\ell+1-i}.$$

2.5. **Initialization.** The prime p is intended to be large: indeed, we need to check that $\ell < p$ for all $\ell \in A$ for the algorithm to work at all.

We also need to confirm that p does not divide $4a_4^3 + 27a_6^2$, otherwise E is not an elliptic curve when reduced modulo p.

Finally, calculate and store the j-invariant $j = j(E) = 6912a_4^3/(4a_4^3 + 27a_6^2) \in \mathbb{F}_p$.

We discard E if its j-invariant equals 0 or 1728. This condition would only be satisfied for a very small number of curves. Also later in the calculation, we shall abandon the branch of the calculation where an elliptic curve with j-invariant 0 or 1728 arises.

We also discard E if it is *supersingular*. Supersingular curves are the ones for which $\#E(\mathbb{F}_p) = p+1$. We can check E for supersingularity by taking a few random points on it and checking if $p+1$ annihilates them. If not, then the curve is definitely not supersingular and we can go on. If yes, then E is probably supersingular so we throw it away. Once again, we only throw away a few E this way. Furthermore, this check needs to be carried out only for our original E and not for any other curves that arise during the calculations later on.

2.6. **Determination of the Possible Pairs $(f, \tilde{\jmath})$.** Since we are working with a single ℓ here, let us denote Ψ_ℓ by Ψ. Let Ψ_1 denote the first partial derivative of Ψ, let Ψ_{12} denote the second partial derivative of Ψ_1, and so on.

If we plug in $J = j$ into $\Psi(F, J)$, we obtain a univariate polynomial $\Psi(F, j)$ in the variable F. The roots $f \in \mathbb{F}_p$ of this polynomial are our candiates for f. If Ψ_1 or Ψ_2 vanishes at (f, j), then that f must be discarded from our list. This will happen very rarely but must be caught to avoid a division by zero later on.[2]

For each one of our remaining candidates $f \in \mathbb{F}_p$, we should find all the roots $\tilde{\jmath} \in \mathbb{F}_p$ of the polynomial $\Psi(f, J)$. These are our candidates for $\tilde{\jmath}$ with the given f. If Ψ_1 or Ψ_2 vanishes at $(f, \tilde{\jmath})$, then this pair $(f, \tilde{\jmath})$ must be dropped from our list. This will happen very rarely but must be caught to avoid a division by zero later on.

Also discard all the pairs $(f, \tilde{\jmath})$ where $\tilde{\jmath} = 0$ or $\tilde{\jmath} = 1728$.

2.7. **Determination of $\tilde{a}_4$, $\tilde{a}_6$, p_1, Given $(f, \tilde{\jmath})$.** We need to calculate the following quantities, which are elements of $\mathbb{F}_p$. Let $E_4 = -48a_4$, $E_6 = 864a_6$ and

$$f' = \frac{E_6}{E_4} j \frac{\Psi_2(f,j)}{\Psi_1(f,j)}, \qquad Q = \frac{f'}{\tilde{\jmath}} \frac{1}{\ell} \frac{\Psi_1(f,\tilde{\jmath})}{\Psi_2(f,\tilde{\jmath})}, \qquad \tilde{E}_4 = \frac{\tilde{\jmath}}{\tilde{\jmath} - 1728} Q^2.$$

Let $\tilde{E}_6 = \tilde{E}_4 Q$ and

$$\begin{aligned} t_1 &= \frac{1}{\Psi_1(f,j)} \left(-f'\Psi_{11}(f,j) + 2j\Psi_{12}(f,j)\frac{E_6}{E_4} - \frac{E_6^2}{f' E_4^2}(j\Psi_2(f,j) + j^2\Psi_{22}(f,j)) \right), \\ t_2 &= \frac{1}{\Psi_1(f,\tilde{\jmath})} \left(-f'\Psi_{11}(f,\tilde{\jmath}) + 2\ell\tilde{\jmath}\Psi_{12}(f,\tilde{\jmath})\frac{\tilde{E}_6}{\tilde{E}_4} - \ell^2\frac{\tilde{E}_6^2}{f'\tilde{E}_4^2}(\tilde{\jmath}\Psi_2(f,\tilde{\jmath}) + \tilde{\jmath}^2\Psi_{22}(f,\tilde{\jmath})) \right). \end{aligned}$$

Let

$$t_3 = \frac{E_6}{3E_4} - \frac{E_4^2}{2E_6}, \qquad t_4 = \ell\left(\frac{\tilde{E}_6}{3\tilde{E}_4} - \frac{\tilde{E}_4^2}{2\tilde{E}_6}\right).$$

Finally, let $p_1 = \ell(t_2 + t_4 - t_1 - t_3)/4$, $\tilde{a}_4 = -\ell^4\tilde{E}_4/48$ and $\tilde{a}_6 = \ell^6\tilde{E}_6/864$.

All of the intermediate results, except for $\tilde{a}_4$, $\tilde{a}_6$ and p_1, can be discarded before moving on.

2.8. **Determination of the Kernel Polynomial $h(X)$ given $\tilde{a}_4$, $\tilde{a}_6$ and p_1.** Recall our notation $d = (\ell - 1)/2$. Here we are aiming to produce a polynomial $h(X)$ of degree d. We need to pick an integer S, which is a small positive integer determining the number of "extra" terms we carry for a certain calculation. These extra terms will have to vanish at the end to assure us that the triple $(\tilde{a}_4, \tilde{a}_6, p_1)$ we started with is "valid". The choice $S = 3$ works fine.

First we set

$$\begin{aligned} p_0 &= d, \\ p_2 &= ((1 - 10d)a_4 - \tilde{a}_4)/30, \\ p_3 &= ((1 - 28d)a_6 - 42p_1a_4 - \tilde{a}_6)/70. \end{aligned}$$

[2]If one, but not both, of Ψ_1 and Ψ_2 vanishes at (f, j) then our formulae can be rewritten to make sense and avoid division by zero. However, even writing this footnote seems like excessive effort in the face of an eventuality this unlikely.

Recall that p_1 was already given as part of our data. Then set

$$\begin{aligned} c_1 &= 6p_2 + 2a_4 d, \\ c_2 &= 10p_3 + 6a_4 p_1 + 4a_6 d, \end{aligned}$$

and for each $2 \leq r \leq d - 1 + S$, let

$$c_{r+1} = \frac{3\sum_{n=1}^{r-1} c_n c_{r-n} - (2r-1)(r-1)a_4 c_{r-1} - (2r-2)(r-2)a_6 c_{r-2}}{(r-1)(2r+5)}.$$

Next, for each $3 \leq n \leq d - 1 + S$, let

$$p_{n+1} = \frac{1}{4n+2}\left(c_n - (4n-2)a_4 p_{n-1} - (4n-4)a_6 p_{n-2}\right).$$

The quantity p_i is the sum of the ith powers of the roots of $h(X)$. From here, we can obtain the coefficients in the usual manner (see [4, Prop. 4.3.3.]). Specifically, set $s_0 = 1$, and for all $1 \leq i \leq d + S$, let

$$s_i = \frac{-1}{i}\sum_{k=1}^{i}(-1)^k p_k s_{i-k}.$$

We need to check if $s_{d+1} = s_{d+2} = \cdots = s_{d+S} = 0$. If not, we conclude that our triplet $(\tilde{a}_4, \tilde{a}_6, p_1)$ was not valid, and we go on to the next $(f, \tilde{\jmath})$ pair.

If our triplet was deemed to be valid, then

$$h(X) = \sum_{i=0}^{d}(-1)^i s_i X^{d-i}.$$

If the triplet $(\tilde{a}_4, \tilde{a}_6, p_1)$ is not valid, then we can go on to the next pair $(f, \tilde{\jmath})$ to get our next triplet $(\tilde{a}_4, \tilde{a}_6, p_1)$, and so on. If no valid triplet $(\tilde{a}_4, \tilde{a}_6, p_1)$ can be found, then the algorithm does not apply to the elliptic curve under consideration and this ℓ, so we find out nothing about t modulo ℓ.

2.9. **Determination of the Eigenvalue e Given the Kernel Polynomial $h(X)$.** First of all, factor $h(X)$ and replace it by any one of its (non-trivial) factors. From now on, $h(X)$ will denote the factor that we chose. Note that in this step, the algorithm can be speeded up appreciably by rearranging the order in which some steps are carried out. For details, see Section 4.1.

Use the table in Section 5.2 to pick an integer s based on the value of ℓ. For any ℓ, we get an $s \leq 11$. Given this s, we need four polynomials, $a_s(X)$, $b_s(X)$, $c_s(X)$ and $d_s(X)$. The way to obtain these is explained in Section 2.10.

The procedure we need to follow here is slightly different for the cases where the degree of h is even or odd. Let us assume for now that $\deg(h)$ is even.

Start by calculating and storing $Q_1(X) = X^p \bmod h(X)$ and $Q_2(X) = (X^3 + a_4 X + a_6)^{(p-1)/2} \bmod h(X)$.

Throughout this calculation, we need to maintain a pair of polynomials $(P_1(X), P_2(X))$ and an integer e. Initially, $(P_1(X), P_2(X)) = (X \bmod h(X), 1)$ and $e = 1$.

If at some stage $(P_1(X), P_2(X)) = (Q_1(X), \pm Q_2(X))$ then we may stop. If $P_2(X) = Q_2(X)$ then the current value of e is the eigenvalue we are aiming to calculate. If $P_2(X) = -Q_2(X)$ then the eigenvalue is $-e$.

Otherwise, do the following replacements *simultaneously* (in other words, the values of P_1 and P_2 to be used on the right hand side are the *old* ones):

$$\begin{aligned} P_1(X) &\leftarrow \frac{a_s(P_1(X))}{b_s(P_1(X))} \bmod h(X), \\ P_2(X) &\leftarrow P_2(X)\frac{c_s(P_1(X))}{d_s(P_1(X))} \bmod h(X), \\ e &\leftarrow es \bmod \ell \end{aligned}$$

Iterate this until the condition $(P_1(X), P_2(X)) = (Q_1(X), \pm Q_2(X))$ is satisfied. This should occur after no more than $(\ell - 1)/2$ steps.

In the case where $\deg(h)$ is odd, the calculation is the same except that we do not have to calculate Q_2 or P_2. Whenever $P_1(X) = Q_1(X)$ is achieved, the correct value of the eigenvalue is

$$e^{s(e)} \left(\frac{r}{\ell}\right) e,$$

where r is the resultant of $h(X)$ and $w(X) = X^3 + a_4X + a_6$, and $s(x)$ is the *semi-order* of x modulo ℓ, i.e., the smallest positive n such that $x^n \equiv \pm 1 \pmod{\ell}$.

2.10. **Determination of the Polynomials $a_s(X)$, $b_s(X)$, $c_s(X)$ and $d_s(X)$.** The polynomials we will obtain depend on E, but not on ℓ. Since they are of relatively low degree, it is probably a good idea to calculate and store them once for each E and just look up the right ones for each ℓ.

Choose an integer R such that we need to calculate the polynomials $a_s(X)$, $b_s(X)$, $c_s(X)$ and $d_s(X)$ for $s \le R$. For example, $R = 11$ will do with the set of ℓ that are used in this algorithm. (But $R = 5$ will suffice with the modification described in Section 4.2.)

We need to calculate a number of polynomials with coefficients in $\mathbb{F}_p$.

$$\begin{aligned} w(X) &= X^3 + a_4X + a_6, \\ f_1(X) &= 1, \\ f_2(X) &= 2, \\ f_3(X) &= 3X^4 + 6a_4X^2 + 12a_6X - a_4^2, \\ f_4(X) &= 4X^6 + 20a_4X^4 + 80a_6X^3 - 20a_4^2X^2 - 16a_4a_6X - 4a_4^3 - 32a_6^2. \end{aligned}$$

We can now determine the desired polynomials for $s = 2$ as

$$\begin{aligned} a_2(X) &= 4Xw(X) - f_3(X), \\ b_2(X) &= 4w(X), \\ c_2(X) &= f_4(X)/4, \\ d_2(X) &= 8w(X)^2. \end{aligned}$$

For each $5 \le n \le R + 2$, we need to calculate the polynomial $f_n(X)$. If $n = 2m$, let

$$f_n = f_m(f_{m+2}f_{m-1}^2 - f_{m-2}f_{m+1}^2)/2.$$

If $n = 2m + 1$ with m even, let

$$f_n = w^2 f_{m+2}f_m^3 - f_{m-1}f_{m+1}^3.$$

If $n = 2m + 1$ with m odd, let

$$f_n = f_{m+2}f_m^3 - w^2 f_{m-1}f_{m+1}^3.$$

Now for any *odd*[3] s in the range $2 < s \leq R$, we can write down

$$\begin{aligned} a_s(X) &= Xf_s(X)^2 - w(X)f_{s-1}(X)f_{s+1}(X), \\ b_s(X) &= f_s(X)^2, \\ c_s(X) &= f_{s+2}(X)f_{s-1}(X)^2 - f_{s-2}(X)f_{s+1}(X)^2, \\ d_s(X) &= 4f_s(X)^3. \end{aligned}$$

2.11. **The Last Step.** For each elliptic curve E we end up knowing the important integer t modulo various small primes ℓ. Since the absolute value of t is bounded by $2\sqrt{p}$, we can use the Chinese Remainder Theorem to deduce t once the product of the moduli exceeds $4\sqrt{p}$.

For any specific curve E, once we have narrowed down the possibilities for t to a manageable number, we can use another method to arrive at the correct value of t faster. For details, consult Section 4.5.

3. Mathematical Background

3.1. **A Few Unusual Curves.** The theory is a lot cleaner if we assume that for any elliptic curve E that occurs later, $j(E)$ is not 0 or 1728, and E is not supersingular (recall that this means $\#E(\mathbb{F}_p) = p + 1$). The first condition assures that E does not have too many automorphisms, the second one assures that the endomorphism ring of E has rank 2 over $\mathbb{Z}$ (as opposed to rank 4 for supersingular curves).

Since each point on a supersingular curve is annihilated by $p + 1$ in the group law, whereas most points on most non-supersingular curves are not annihilated by $p + 1$, supersingularity can be effectively checked by multiplying a few points on the curve by $p + 1$. For details, see Section 2.5.

The curves just mentioned are in fact known to have a discrete logarithm problem that is easier than usual to solve, and hence their exclusion only does good to our intended applications in cryptography.

3.2. **Reducing Point-Counting to Considering Isogenies.** The idea of the algorithm is that since our elliptic curve E is defined over $\mathbb{F}_p$, the Frobenius map $F : (x, y) \mapsto (x^p, y^p)$ acts on it. In fact, it satisfies

$$F^2 - tF + p = 0.$$

The same relation is also valid for the action of F on the set of ℓ-torsion points of E, denoted by $E[\ell]$. We could therefore obtain $t' = t \bmod \ell$ by checking which $0 \leq t' \leq \ell - 1$ satisfies $(F^2 + p)Q = t'FQ$ for all $Q \in E[l]$. This is the original idea of Schoof's algorithm in [18].

Carrying out this plan quickly leads to arithmetic with polynomials of degree $(\ell^2 - 1)/2$ over $\mathbb{F}_p$. Therefore, in practice it is better to use an idea of Elkies, which works only for half the primes ℓ, but then only requires the use of polynomials of degree $(\ell - 1)/2$ over $\mathbb{F}_p$.

The method works if $t^2 - 4p$ is a square modulo ℓ. This condition is satisfied for (asymptotically) half of all prime numbers ℓ. In this case, the action of F on $E[\ell]$ splits into (usually) two eigenspaces. If we somehow knew a subgroup B of $E[\ell]$

[3]Similar formulae exist for even $s > 2$, but those will not be needed in this algorithm.

where F acts as a scalar, then we could check which $0 \leq e \leq \ell - 1$ has the property that

$$eQ = FQ$$

for all $Q \in B$. Then we could use the congruence $t' \equiv e + p/e \pmod{\ell}$ to get t'. Such a subgroup B can be described by a degree $(\ell - 1)/2$ polynomial $h(X)$ that vanishes exactly at the x coordinates of points in B. Indeed, given $h(X)$ what we need to check is whether

$$e(X, Y) \equiv (X^p, Y^p) \pmod{h(X), Y^2 - X^3 - a_4X - a_6}.$$

(Here the left hand side means $(X, Y) \oplus \cdots \oplus (X, Y)$ (e times), where $\oplus$ denotes addition according to the group law of E.)

Any subgroup B of size ℓ in E determines a degree ℓ isogeny (to be referred as an ℓ-isogeny) $E \to E/B$. The group B being (in) an eigenspace of F is equivalent to this isogeny being defined over $\mathbb{F}_p$. So we have reduced our problem to finding an explicitly described ℓ-isogeny $E \to E_1$ defined over $\mathbb{F}_p$, if such a thing exists. (This happens exactly if $t^2 - 4p$ is a square modulo ℓ, but we do not know $t^2 - 4p$ yet!)

3.3. **Parametrizing ℓ-isogenies.** Let us think about ℓ-isogenies of elliptic curves defined over $\mathbb{C}$ first. Section 3.10 shall indicate how these considerations can be made to apply to elliptic curves defined over $\mathbb{F}_p$.

Any elliptic curve E over $\mathbb{C}$ can be regarded as a quotient of $\mathbb{C}$ by a rank 2 lattice L. Multiplying all elements of the lattice by a complex constant does not change the isomorphism class of the curve, so we may assume that the lattice L is spanned by 1 and $\tau \in \mathbb{C}$, with τ in the upper half plane. Hence

$$E \cong \mathbb{C}/(\mathbb{Z} \oplus \tau\mathbb{Z}).$$

However, for our purposes it is useful to choose another uniformization of E, that obtained via the map $z \mapsto \exp(2\pi iz)$. It is clear that this gives an isomorphism

$$E \cong \mathbb{C}^*/q^{\mathbb{Z}},$$

where $q = \exp(2\pi iz)$ and $q^{\mathbb{Z}} = \{q^n : n \in \mathbb{Z}\}$. Any compact Riemann surface (such as $\mathbb{C}^*/q^{\mathbb{Z}}$) is a projective algebraic variety (c.f. [11, B, Theorem 3.1]), and it turns out that $\mathbb{C}^*/q^{\mathbb{Z}}$ is (isomorphic to) the elliptic curve

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

where $E_4(q)$ and $E_6(q)$ are the q-series mentioned in Section 2.3. This E is in fact ℓ-isogenous to $E_1 = \mathbb{C}^*/q^{\ell\mathbb{Z}}$, via the map $z \mapsto z^\ell$. We can once again use q-series to describe the equation of E_1: indeed,

$$E_1: \qquad Y^2 = X^3 - \frac{E_4(q^\ell)}{48} + \frac{E_6(q^\ell)}{864}.$$

We also need the kernel polynomial $h(X)$, which vanishes exactly at the x coordinates of points in the kernel of our isogeny (these points are just the images of the ℓth roots of 1 in $\mathbb{C}^*/q^{\mathbb{Z}}$). In fact, as explained in Section 3.9, it suffices to calculate here the first coefficient p_1 of $h(X)$, because the rest of the coefficients can be obtained from p_1 and the data we already have. As for p_1, it turns out that

$$p_1 = \frac{\ell}{24}\left(E_2(q) - \ell E_2(q^\ell)\right),$$

where

$$E_2(q) = 1 - 24\sum_{n=1}^{\infty}\sigma_1(n)q^n = 1 - 24q - 72q^2 - 96q^3 - \cdots$$

Hence, if we are given an elliptic curve

$$E: \qquad Y^2 = X^3 + a_4X + a_6,$$

we can find ℓ-isogenies by locating various q such that $E \cong \mathbb{C}^*/q^{\mathbb{Z}}$. For each such q, we can find the equation of $E_1 \cong \mathbb{C}^*/q^{\ell\mathbb{Z}}$ as well as the kernel of the isogeny.

3.4. **Locating the Parameters that Belong to a Certain Isogeny.** The method suggested in Section 3.3 is impractical in the sense that infinitely many different choices of q give the same elliptic curve $\mathbb{C}^*/q^{\mathbb{Z}}$ (up to isomorphism). Two elliptic curves are isomorphic if and only if they have the same j-invariant. The j-invariant of $\mathbb{C}^*/q^{\mathbb{Z}}$ turns out to be the q-series $j(q) = 1728E_4(q)^3/(E_4(q)^3 - E_6(q)^2)$ (the same $j(q)$ that occurs in Section 2.3). Any complex number can occur as the j-invariant of an elliptic curve, and the q-series $j(q)$ can actually take any value as we vary q. Therefore, we could just pick a q for each possible j-invariant and restrict our attention to just those q, since all other ones would just clutter our calculations without yielding new elliptic curves.

In fact, we can do a little better. Instead of restricting attention to those q that give us all the isomorphism classes of elliptic curves E as $\mathbb{C}^*/q^{\mathbb{Z}}$, we take a bigger set of q so that the corresponding ℓ-isogenies $\mathbb{C}^*/q^{\mathbb{Z}} \to \mathbb{C}^*/q^{\ell\mathbb{Z}}$ give us all isomorphism classes of ℓ-isogenies $E \to E_1$. It turns out this set can be given the structure of an algebraic curve called $Y_0(\ell)$. The addition of two extra points (called the cusps) compactifies the curve, and we obtain a smooth projective curve $X_0(\ell)$. The curve $X_0(\ell)$ is a *modular curve*, so called since its points are moduli (parameters) for ℓ-isogenies of elliptic curves.

The fact that $X_0(\ell)$ has geometric structure is a powerful tool. For example, the q-series $j(q)$ is just a (rational) function on $X_0(\ell)$, for each point giving us the j-invariant of the "source" curve of the isogeny parametrized by that point. Similarly, $j(q^l)$ is a rational function on $X_0(\ell)$ that gives the the j invariant of the target. Also, given an ℓ-isogeny $\phi : E \to E_1$, we can take the dual isogeny $\phi^\vee : E_1 \to E$. This operation is reflected on $X_0(\ell)$ by a *morphism* $w : X_0(\ell) \to X_0(\ell)$. If Q is the point that parametrizes ϕ, then wQ parametrizes $\phi^\vee$. Since $(\phi^\vee)^\vee = \phi$, we conclude that the morphism $w \circ w$ is just the identity. The morphism w is called the *Atkin-Lehner involution*. (It swaps the two cusps.)

Now we can get rid of another unwieldy feature of the process suggested in Section 3.3: that of determining q from $E_4(q)$ and $E_6(q)$ and using this value to evaluate other q-series. That would be a very tedious task which can be sidestepped as follows. The functions $j(q)$ and $j(q^\ell)$ are known to satisfy a polynomial relation, the *Kronecker relation*:

$$\Phi(j(q), j(q^l)) = 0,$$

for a certain $\Phi = \Phi_\ell \in \mathbb{Z}[X, Y]$ that can be determined explicitly. The polynomial Φ has degree $\ell + 1$ in each variable.

To explain how to use the Kronecker relation, we need some notation. For any q-series g, denote the q-series $g(q^l)$ by $\tilde{g}$. Furthermore, for any q-series $g(q)$, let $g'(q) = q(\mathrm{d}g/\mathrm{d}q)$. In fact $g'(q) = (1/2\pi i)(\mathrm{d}g/\mathrm{d}\tau)$ (recall that $q = \exp(2\pi i\tau)$), so this $g'(q)$ can be used as a usual derivative of g. When both $'$ and $\tilde{}$ are involved,

the $\tilde{}$ is to be taken *last*, so $\tilde{g}'$ is intended to mean $\widetilde{(g')}$. This is an important point, since $(\tilde{g})' = \ell\widetilde{(g')}$.

The q-series j, E_4 and E_6 enjoy a number of identities, for example

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

Therefore, if we know the values of $j(q)$, $E_4(q)$ and $E_6(q)$ (but *not* that of q), we can still find the value of $j'(q)$.

Now we can put the Kronecker relation to good use. Assume that we know the values of $E_4(q)$ and $E_6(q)$ and we want to describe the isogeny $\mathbb{C}^*/q^{\mathbb{Z}} \to \mathbb{C}^*/q^{\ell\mathbb{Z}}$. We can immediately determine $j(q) = 1728E_4(q)^3/(E_4(q)^3 - E_6(q)^2)$, and by the identities above, also the value of $j'(q)$. Plugging the value of $j(q)$ into the Kronecker relation, we obtain a polynomial whose $\ell+1$ roots are the possible values of $j(q^\ell) = \tilde{\jmath}$. Differentiating the Kronecker relation (using the notation for partial derivatives introduced in Section 2.6), we obtain

$$j'\Phi_1(j,\tilde{\jmath}) + \ell\tilde{\jmath}'\Phi_2(j,\tilde{\jmath}) = 0.$$

For each candidate for $\tilde{\jmath}$, this allows us to deduce the value of $\tilde{\jmath}'$, and hence that of $\tilde{E}_4$ and $\tilde{E}_6$ by the identities above (which of course remain valid if we plug in q^ℓ instead of q). We can also get the value of $E_2 - \ell\tilde{E}_2$ for p_1 by looking at the second derivative of the Kronecker relation and then utilizing some more complicated identities to get at E_2, but we won't do that since there is an even better way. The aspect of this method that needs improving is its use of Φ_ℓ: that equation has extremely large coefficients (which would actually be fine with us since we are only trying to compute it modulo p in the end), and determining it requires that we calculate using approximately $2\ell^2$ coefficients of a certain power series. The improved method cuts that $2\ell^2$ to about $2\ell v$, where v is less than $\ell/24+1$.

What one should do instead is to choose a suitable q-series f that is a function on $X_0(\ell)$. We also require that f be invariant under the Atkin-Lehner involution w. For technical reasons (that will be explained in Section 3.5), we pick f to have poles only at the cusps, and we want those poles to have relatively low order. Then we find by the process of Section 3.5 a polynomial relation

$$\Psi_\ell(f,j) = 0.$$

By the w-invariance of f, we also have

$$\Psi_\ell(f,\tilde{\jmath}) = 0.$$

Hence given j, we can find all possible values of f, and for each possible value of f, we can get all values of $\tilde{\jmath}$. We can take partial derivatives of the above two relations and gradually deduce all the information we need to describe our isogeny.

It is possible for distinct pairs $(j_1,\tilde{\jmath}_1)$ and $(j_2,\tilde{\jmath}_2)$ to correspond to the same value of f. Therefore, starting from j_1, we might get this f and end up with $\tilde{\jmath}_2$. However, the $p_1, p_2, \ldots$ of Section 2.8 obtained from $(j_1, f, \tilde{\jmath}_2)$ will not be power sums of the roots of a degree d polynomial, and hence will be deemed invalid because $s_{d+i} \neq 0$ for some small i. Readers not satisfied with this test are referred to Section 3.11.

The calculations needed are explained in Morain's [15, 3.2.2]. (The second formula on page 273 contains a typo: a denominator should have a 6 instead of a 2. However, it is evident that the correct version was used as input for the subsequent calculations. Also, the numerical example on top of page 274 is of course for $\ell = 31$, not 23.) Morain's notation is similar to ours, the following conversion rules apply:

Morain	here	Morain	here	Morain	here
F	f	∂_{FF}	$\Psi_{11}(f,j)$	∂_{FF*}	$\Psi_{11}(f,\tilde{j})$
J	j	∂_{FJ}	$\Psi_{12}(f,j)$	∂_{FJ*}	$\Psi_{12}(f,\tilde{j})$
$\tilde{J}$	$\tilde{j}$	∂_{JJ}	$\Psi_{22}(f,j)$	∂_{JJ*}	$\Psi_{22}(f,\tilde{j})$
∂_F	$\Psi_1(f,j)$	∂_{F*}	$\Psi_1(f,\tilde{j})$		
∂_J	$\Psi_2(f,j)$	∂_{J*}	$\Psi_2(f,\tilde{j})$		

The polynomials Φ_ℓ and Ψ_ℓ are not the only ones that can be used here (although Ψ_ℓ is the optimal one in a certain sense). For an analysis of these and related polynomials and algorithms for computing them, see [2].

3.5. **Obtaining Ψ_ℓ from f.** Using the terminology of Section 3.4, we introduce another modular curve. It is $X(1)$, and it parametrizes isomorphism classes of elliptic curves. As a Riemann surface, $X(1)$ is just the complex numbers plus a cusp that is considered to lie "at infinity": each finite number corresponds to the elliptic curve with that j-invariant. (The cusp does not parametrize an elliptic curve, it is just there to make our object compact and geometrically nice.) If we agree that $j = \infty$ at the cusp, then j gives an isomorphism between $X(1)$ and the complex projective line.

There is a "degeneracy" morphism $\phi : X_0(\ell) \to X(1)$. It sends the point parametrizing $E \to E_1$ to the point parametrizing E (and sends both cusps of $X_0(\ell)$ to the unique cusp of $X(1)$). The map ϕ is a ramified Galois covering. Using the coordinate τ on $X_0(\ell)$ (recall that $q = \exp(2\pi i\tau)$), for any value of τ, the set $\{\tau, -1/\tau, -1/(\tau+1), \dots, -1/(\tau+\ell-1)\}$ is invariant under the deck transformation group of ϕ. So if g is any function on $X_0(\ell)$, then any elementary symmetric polynomial s in $\{g(\tau), g(-1/\tau), g(-1/(\tau+1)), \dots, g(-1/(\tau+\ell-1))\}$ is actually a pullback of a function on $X(1)$. Therefore s "is" a rational function in j.

Since $w\tau = -1/\ell\tau$, if f is a w-invariant function on $X_0(\ell)$ then all the coefficients of the polynomial

$$\begin{aligned}\Psi(F) &= (F - f(\tau)) \prod_{k=0}^{\ell-1} \left(F - f\left(\frac{-1}{\tau+k}\right)\right) \\ &= (F - f(\tau)) \prod_{k=0}^{\ell-1} \left(F - f\left(\frac{\tau+k}{\ell}\right)\right)\end{aligned}$$

are rational functions in $j(\tau)$. Additionally, if f has poles only at the cusps, then the coefficients of $\Psi(F)$ must be *polynomials* in $j(q)$. Hence if we calculate the q-expansions of the coefficients of $\Psi(F)$, we can read off what those polynomials in $j(q)$ must be. Thereby we obtain a polynomial relation

$$\Psi_\ell(F, J) = 0$$

which is satisfied by $F = f(q)$ and $J = j(q)$.

It remains to calculate the q-expansions of the coefficients of $\Psi(F)$, given the q-expansion of f. (The question of picking a suitable f with a known q-expansion will be addressed in Section 3.6.) Let $\zeta = exp(2\pi i/\ell)$ and

$$f^r(q) = \sum_n a(n,r) q^n.$$

Then

$$f\left(\frac{\tau+k}{\ell}\right)^r = f^r(q^{1/\ell}\zeta^k) = \sum_n a(n,r)q^{n/\ell}\zeta^{kn}$$

Summing the above from $k=0$ to $k=\ell-1$, the roots of unity cause the fractional powers of q to cancel each other out, and we are left with

$$s_r(q) = \sum_{k=0}^{\ell-1} f\left(\frac{\tau+k}{\ell}\right)^r = \ell\sum_n a(\ell n, r)q^n.$$

These $s_r(q)$ are exactly the power sums of the roots of the polynomial $\prod_{k=0}^{\ell-1}\left(F - f\left(\frac{\tau+k}{\ell}\right)\right)$. From there we can obtain its coefficients $c_r(q)$ in the usual manner, from which the coefficients $C_r(q)$ of $\Psi(F)$ come out. The details are given in Section 2.4.

3.6. **Finding a good $f(q)$ using hands-on methods.** Let $X_0^+(\ell)$ denote the smooth curve that is the quotient of $X_0(\ell)$ by the Atkin-Lehner involution w. The requirements of Section 3.4 and 3.5 then translate simply to finding (a lot of initial coefficients of) the q-expansion of a certain non-constant function f on $X_0^+(\ell)$. This f is required to have a pole only at the (unique) cusp of $X_0^+(\ell)$, and the order v of this pole should be as small as possible. Denote the genus of $X_0^+(\ell)$ by $g_0^+(\ell)$, and the genus of $X_0(\ell)$ by $g_0(\ell)$. A simple application of the Riemann–Roch theorem tells us that we can always find such a function f with $v \le g_0^+(\ell)+1$. By [15, Thm. 2.1] and the fact that $g_0(\ell)$ is about $\ell/12$, we confirm that we can always get a v no bigger than about $\ell/24$. (For each ℓ, the geometric properties of $X_0^+(\ell)$ determine what the smallest v is. The definition of the cusp being a *Weierstrass point* of the curve is that $v < g_0^+(\ell)+1$ can be achieved.

In fact, if ℓ is very small then finding an f is straightforward. In this case Ψ_ℓ also has very small coefficients, so we may as well just determine it from the f in advance, and hardwire the polynomial Ψ_ℓ into our program.

For instance, if $\ell \in \{3,5,7,13\}$, the curve $X_0(\ell)$ is rational, isomorphic to the projective line via

$$h(q) = \left(\frac{\eta(q)}{\eta(q^\ell)}\right)^{24/(\ell-1)}.$$

(Here we use $\eta(q) = q^{1/24}\bar\eta(q)$, c.f. [9, *The rational case* in Section 4].) This h has a single pole at $q=0$. Since $(w^*h)h = l^{12/(\ell-1)}$, we conclude that

$$f(q) = h(q) + \ell^{12/(\ell-1)}/h(q)$$

is a degree-1 function on $X_0(\ell)$ that is invariant under the action of w. Therefore it is a function on the rational curve $X_0^+(\ell)$, with a single pole at the cusp. The q-expansion of f is easily calculated to any reasonable precision by using the explicit definition of $h(q)$. For example, for $\ell=3$ we get

$$f(q) = q^{-1} - 12 + 783q + 8672q^2 + 65367q^3 + \cdots$$

For $\ell \in \{11,17,19,23\}$, we use ad hoc methods to produce our function f.

The case $\ell=11$ is treated explicitly in [15, Section 2.3.1]. A suitable f is given as

$$f(q) = \left(\frac{\theta([2,1;1,6],q)}{\eta(q)\eta(q^{11})}\right)^2 - 1 = q^{-1} + 5 + 17q + 46q^2 + \cdots$$

(For information on θ-series and our notation, refer to [14, Section 4.9, especially Corollary 4.9.5.(3)].)

Now consider the case $\ell = 17$. First we write down the q-series

$$\begin{aligned} f_1(q) &= (17E_2(q^{17}) - E_2(q))/24, \\ f_2(q) &= 17^2 E_4(q^{17}) + E_4(q), \\ f_3(q) &= \theta([12,1,0,3;1,2,2,1;0,2,8,3;3,1,3,4], q). \end{aligned}$$

All three of these functions are modular forms with respect to the group $\Gamma_0(17)$. The forms f_1, f_2, f_3 have weight $2, 4, 2$ respectively. The functions f_1, f_3 are anti-invariant under the action of the Atkin-Lehner involution, whereas f_2 is invariant. Therefore the q-series

$$\begin{aligned} a(q) &= f_3^2/f_2 = 1/290 + (46/4205)q + \cdots, \\ b(q) &= f_1/f_3 = 2/3 - (1/3)q + \cdots \end{aligned}$$

are functions on $X_0^+(17)$. They satisfy the equation

$$(b^3 - \frac{19}{3}b^2 + \frac{15}{4}b - \frac{1}{4})a + (\frac{1}{360}b - \frac{1}{1080}) = 0.$$

The above equation can be considered a singular equation of the curve $X_0^+(17)$. Therefore its normalization (desingularization) is isomorphic to $X_0^+(17)$. The given equation is only singular at the point at infinity in the direction $b = 0$, where it has an ordinary triple point. By blowing up the singularity, we see that the normalization is a space curve that lies on a nonsingular the quadric surface in $\mathbb{P}^3$. The normalization itself is a (1,3)-curve on the surface. (For details of the blowing up process and the naming convention for curves on the nonsingular quadric surface, refer to [11, Section I.4 and (II, Ex. 5.6)].) In the end it turns out that b gives an isomorphism between $X_0^+(17)$ and the projective line. The cusp $q = 0$ corresponds to $b = 2/3$. Since we want a pole at the cusp, we set

$$f = \frac{-1/3}{b - 2/3} = q^{-1} + 3 + 7q + 14q^2 + 29q^3 + \cdots$$

The cases $\ell = 19$ and $\ell = 23$ may be handled in a similar way.

3.7. **Finding a good $f(q)$ by lifting it from characteristic ℓ.** The difficulty in finding a good f is essentially that we have to know about some complicated geometric properties of the curve $X_0^+(\ell)$. An idea of Atkin is very useful in this context. Instead of trying to find the coefficients in the q-expansion of f, we try to find them modulo some prime number and use those values to guess the original coefficients in f. With any luck, the reductions of the coefficients of f will have to do with a simpler curve and will therefore be simpler to calculate.

We shall reduce $X_0^+(\ell)$ modulo ℓ. Formally, this amounts to taking the model $\mathcal{X}_0^+(\ell)$ that Deligne and Rapoport define over $\mathbb{Z}_\ell$, and considering its special fiber $X_0^+(\ell)_{/\mathbb{F}_\ell}$. The curve thus obtained is not smooth, but it is very simple: it is isomorphic to the projective j-line over $\mathbb{F}_\ell$ with a certain number of simple double points. (For details, see [6, Thm. 6.9].)

The double points result from the identification of the points x and x^ℓ for each of $x \in S$, for a certain set S. To define S, we need to talk about *supersingular j-invariants*. Let K be any field of characteristic ℓ. In this more general setting, there is still a notion of whether an elliptic curve defined over K is ordinary or supersingular. For example, we may say that a curve E is supersingular if $E[\ell] = 0$,

otherwise it is ordinary. This is consistent with our previous definition of supersingular in the case where $K = \mathbb{F}_\ell$ (for $\ell \geq 5$), since for E defined over such an $\mathbb{F}_\ell$, $E[\ell] = 0$ occurs if and only if[4] $\#E(\mathbb{F}_\ell) = \ell + 1$. (Recall that the notation $E[\ell]$ stands for the points of order ℓ on E defined over the algebraic closure of the base field.) It is an interesting fact that for any field K of characteristic ℓ and any elliptic curve E defined over that field, the curve is supersingular if and only if $j(E) \in T$, for a certain finite set $T \subseteq \mathbb{F}_{\ell^2}$. Then S is just the set of those elements of T that are not in $\mathbb{F}_\ell$. We shall discuss how to find the set S explicitly in Section 3.8.

Therefore, a function f on $X_0^+(\ell)_{/\mathbb{F}_\ell}$ that has its only pole at the cusp is nothing but a polynomial function $P(j)$ in j with the property that $P(x) = P(x^\ell)$ for each $x \in S$.

Assume now that we have already found a suitable function f on $X_0^+(\ell)$. Then its reduction modulo ℓ is just a function $P(j)$ on $X_0^+(\ell)_{/\mathbb{F}_\ell}$. From what was described above (and with our explicit knowledge of the set S), we can determine the non-constant P of lowest degree v that can occur in this way. Then we could just evaluate

$$P(j(q)) \bmod \ell$$

and lift the coefficients back to characteristic 0 to obtain our original f.

So far, so good, but there are two difficulties that we need to address.

Firstly, we need some explicit bounds on the coefficients of f to make sure that our lifting is unique. However, we expect the coefficients of f to increase exponentially, and therefore there is no chance that we could lift the (at least) hundreds of coefficients that we need. *Atkin's laundering process* solves this problem. If $(\ell + 1)/24 > v$, then we can look at the function

$$g(q) = f(q)\eta(q)\eta(q^\ell).$$

It is a *cusp form* of weight 1, level ℓ (and some character), and therefore its nth coefficient is only $O(n^\varepsilon)$. Furthermore, if $g(q)$ is also a newform then we have an explicit bound: the nth coefficent is no more than the sum of divisors of n. In fact, if $g(q)$ is a linear combination (with small coefficients) of newforms, then we still have a good explicit bound on the size of the coefficients, enabling us to reconstruct a lot of them from their mod ℓ reductions, which we obtain by calculating

$$P(j(q))\eta(q)\eta(q^\ell) \bmod \ell.$$

A suggestion of Atkin on how to make $g(q)$ a linear combination of newforms with small coefficients is to choose P in such a way that the coefficient of $q^{(\ell+1)/24}$ in $P(j(q))\eta(q)\eta(q^\ell) \bmod \ell$ is 0. This amounts to modifying the constant term of $P(X)$.

A second problem has to do with the possibility that the q-expansion of f might start with some terms that are divisible by ℓ and therefore would be visible in the mod ℓ picture. This does not seem to occur for any of the ℓs in use. Atkin, Elkies and yours truly have calculated a number of examples and confirmed that this phenomenon did not occur there.

Of course, once we have a lot of coefficients of $g(q)$, we can find a lot of coefficients of

$$f(q) = g(q)/(\eta(q)\eta(q^\ell)).$$

[4]For $\ell = 2, 3$, we might also have $\#E(\mathbb{F}_\ell) = 1$ or $\#E(\mathbb{F}_\ell) = 2\ell + 1$.

The above process works only if the condition $(\ell+1)/24 > v$ is satisfied. This is the case if $\ell \geq 29$, with the exceptions $\ell = 37, 43, 67, 163$.

Finally, we remark that a suitable g can also be found either as a combination of suitably chosen theta-series (see [1]) or by considering the action of a certain Hecke operator on the modular form $\eta(q)\eta(q^\ell)$ (as in [16]).

3.8. **Finding functions on $X_0^+(\ell)_{/\mathbb{F}_\ell}$.** Let $H_\ell(X) \in \mathbb{F}_\ell[X]$ denote the polynomial whose roots are exactly the set T of supersingular j-invariants in characteristic ℓ. This polynomial is easily calculated in a number of ways, for example by using [15, Thm. 2.2].

Since all elements of T are contained in $\mathbb{F}_{\ell^2}$, the polynomial $H_\ell(X)$ splits completely into linear and quadratic factors. Let $H_\ell^*(X)$ denote the product of the quadratic factors (which is easily calculated once $H_\ell(X)$ is known). The roots of $H_\ell^*(X)$ are exactly the elements of the set S mentioned in Section 3.7.

We are aiming to find a non-constant polynomial $P \in \mathbb{F}_\ell[X]$ of the lowest possible degree that satisfies

$$P(x) = P(x^\ell)$$

for all $x \in S$. This is equivalent to saying that

$$P(X^\ell) - P(X) \equiv 0 \pmod{H_\ell^*(X)}.$$

Indeed, this is the same as saying that $P(X)$ is in the kernel of the Berlekamp matrix associated to $H_\ell^*(X)$. Therefore, we merely need to find a vanishing linear combination of the quantities $X^\ell - X \bmod H_\ell^*(X), X^{2\ell} - X^2 \bmod H_\ell^*(X), X^{3\ell} - X^3 \bmod H_\ell^*(X), \ldots$, and the corresponding linear combination of $X, X^2, X^3, \ldots$ will give us $P(X)$.

Finally, we also need to adjust the constant term of $P(X)$ as indicated in Section 3.7.

3.9. **Obtaining the rest of the coefficients of $h(X)$.** In [9], in the subsection titled *The kernel of the isogeny* in Section 3, Elkies carefully explains how plugging the q-expansions for the x and y coordinates on $E_1 = \mathbb{C}^*/q^{\ell\mathbb{Z}}$ into the derivative of the Weierstrass equation of that curve gives a recursion on the coefficients of $h(X)$ that enables one to find all coefficients once $a_4, a_6, p_1, \tilde{a}_4, \tilde{a}_6$ are known. The actual formulae deduced from there are listed in Section 2.7.

3.10. **Isogenies of elliptic curves over $\mathbb{F}_p$.** Although in the previous sections we worked over $\mathbb{C}$, exactly the same formulae work over $\mathbb{F}_p$. We can justify this using Deuring's lifting theorem: for any isogeny $E \to E_1$ over $\mathbb{F}_p$, we can just lift the coefficients to a number field and reduce them again to when we worked out all the data we needed. For details, consult [19, §7]. We could also appeal to the algebraic definition of modular forms as sections of certain sheaves and arrive at their q-expansions that way.

Secondly, for an ordinary elliptic curve defined over $\mathbb{F}_p$ with j-invariant not equal to 0 or 1728, an isogeny is defined over $\mathbb{F}_p$ if and only if $j, f, \tilde{j} \in \mathbb{F}_p$ (see [19, Prop. 6.1a]).

3.11. **Checking the correctness of $h(X)$.** Note that once a proposed $h(X)$ is determined, it is easy for the suspicious user to check (without using any methods based on modular curves) that it has the claimed properties.

Firstly, calculating $\ell(X,Y) \pmod{h(X), Y^2 - a_4X - a_6}$, we can confirm that it is neutral element of the elliptic curve, and thereby show that $h(X)$ is indeed the polynomial associated to some order ℓ subgroup B of E. Secondly, the existence of some e such that $e(X,Y) \equiv (X^p, Y^p) \pmod{h(X), Y^2 - a_4X - a_6}$ shows that this subgroup B is invariant under the action of the Frobenius morphism.

3.12. **Determining e given $h(X)$.** We have now described a subgroup B of $E[\ell]$ where Frobenius acts by multiplication by e. Determining the e for which

$$e(X,Y) \equiv (X^p, Y^p) \pmod{h(X), Y^2 - X^3 - a_4X - a_6}$$

amounts to determining e such that $eQ = FQ$ for all $Q \in B$. But since B is cyclic of prime order, it suffices to check $eQ = FQ$ for *any one* nonzero $Q \in B$. Therefore we may replace h by any nontrivial factor h' of h in our calculations, since this just amounts to checking $eQ = FQ$ for just those (at least one nonzero) $Q \in B$ where h' vanishes on the x-coordinate.

It is evident that $h(X)$ has no double roots. It is also true that $h(X)$ will split into factors each of which have degree $s(e)$, where $s(x)$, the *semi-order* of x, is the smallest positive integer n such that $x^n \equiv \pm 1 \pmod{\ell}$. Indeed, let $Q = (x_0, y_0)$ be any particular element of B. Then $e(x_0, y_0) = (x_0^p, y_0^p)$ and therefore $(x_m, y_m) := e^m(x_0, y_0) = (x_0^{p^m}, y_0^{p^m})$. Therefore $x_0^{p^m} = x_m = x_0$ if and only if $e^m \equiv \pm 1 \pmod{\ell}$. By definition, the smallest m for which this occurs is $s(e)$, so the minimal polynomial of x_0 has degree $s(e)$ as claimed.

To calculate the e for which $e(X,Y) \equiv (X^p, Y^p)$ holds, we just take some number s with the property that the coordinates sP are easy to calculate from the coordinates of P, for any point P on the curve. For example, for $s = 2$ we have the duplication formulas. This s will also have to have the property that s^k hits all possible residue classes modulo ℓ. Actually, since P and $-P$ have the same x coordinates and opposite y coordinates, so it is sufficient for s^k to hit either a residue class or its negative. A number with such a property may be called a *semiprimitive root* for ℓ. Determining a good small s for each ℓ is trivial. For this algorithm, $s \leq 11$ will suffice (see Section 5.2).

As for the calculation, observe that all can be done in the ring $\mathbb{F}_p[X]/(h(X))$. We represent each point that occurs as $(P_1(X), YP_2(X))$. The appropriate formulas for taking s times a point are easily derived from the formulas on page 105 in [20].

Note that finding e (given $h(X)$) can be carried out faster by using a baby step–giant step or similar method, with the arithmetic carried out as in [3, Chapter IV].

3.13. **Dewaghe's improvement.** L. Dewaghe proposed a method that makes finding e significantly faster when $\deg(h)$ is odd. This condition is bound to occur when $\ell \equiv 3 \pmod 4$, since $\deg(h)$ divides $(\ell - 1)/2$ which is odd in this case. Of course $\deg(h)$ might happen to be odd also when $\ell \equiv 1 \pmod 4$.

According to [7, Theorem 1 of Section 3.2], if $\deg(h)$ is odd and the x-coordinates of $\lambda(X,Y)$ and (X^p, Y^p) match, then

$$e = \lambda^{s(\lambda)} \left(\frac{r}{p}\right) \lambda.$$

Here r is the resultant of $h(X)$ and $w(X) = X^3 + a_4X + a_6$.

3.14. **The accuracy to which $f(q)$ needs to be calculated.** We will demonstrate that it is sufficient to evaluate the coefficients of $f(q)$ up to and including that of $q^{2\ell v - v}$.

Let $g(q)$ be any q-series that is only evaluated to finite precision. Let $v(g)$ be the order of the pole at $q = 0$ and let $t(g)$ be the smallest integer such that the coefficient of $q^{t(g)}$ is not known. Mnemonically,

$$g(q) = cq^{-v(g)} + \cdots + O(q^{t(g)}),$$

where c is a nonzero constant. We know that $v(f) = v$. Assume now that $t(f) = 2\ell v - v + 1$. Using the notation of Section 2.4, we shall prove that $t(C_k) > 0$ for $0 \le k \le \ell + 1$, and therefore that Ψ_ℓ can indeed be determined from the coefficients of f that are known.

For any $1 \le k \le \ell$, evidently $v(f^k) = kv(f) = kv$, and

$$t(f^k) = 2\ell v - v + 1 - (k-1)v = v(2\ell - k) + 1.$$

Let $\lfloor x \rfloor$ denote the largest integer not exceeding x. By the definition of s_k, for all $1 \le k \le \ell$, we conclude that

$$\begin{aligned} v(s_k) &\le \lfloor kv/\ell \rfloor \\ t(s_k) &= \lfloor v(2\ell - k)/\ell \rfloor + 1. \end{aligned}$$

The inequality sign above reflects the fact that a "randomly picked" coefficient in g^k might happen to be zero, in which case s_k might have a pole of lower order than might have been supposed at first.

Now looking at the definition of c_k and using the elementary fact that for any pair a, b of integers, we always have $\lfloor a/\ell \rfloor + \lfloor b/\ell \rfloor \le \lfloor (a+b)/\ell \rfloor$, we conclude that

$$v(c_k) \le \lfloor kv/\ell \rfloor.$$

(This can be proved by induction on k, starting with $k = 1$.)

We can also show by induction that

$$t(c_k) \ge t(s_k) = \lfloor v(2\ell - k)/\ell \rfloor + 1.$$

Indeed, the base case $k = 1$ is obvious. Then by the same elementary fact,

$$t(c_{k-r}s_r) = \min(t(c_{k-r}) - v(s_r), t(s_r) - v(c_{k-r})) \ge t(s_k),$$

and the rest is clear.

Looking at the definition of C_k, we see that if suffices to show that for all $1 \le k \le \ell$,

$$t(fc_k) = \min(t(f) - v(c_k), t(c_k) - v(f)) \ge 1.$$

This is equivalent to two inequalities, the first one of which is immediate. The second one comes down to

$$\lfloor v(2\ell - k)/\ell \rfloor + 1 \ge v + 1,$$

which follows from $k \le \ell$.

4. Possible Improvements

4.1. **Factoring $h(X)$.** The following considerations can be used to speed up the determination of e given $h(X)$. As mentioned in Section 2.9, we might replace $h(X)$ by any of its factors $h'(X)$. This has the advantage that the lower the degree of $h'(X)$ we use, the faster the process in the rest of Section 2.9 runs. Dewaghe's method gives an additional boost of speed if $\deg(h')$ is odd.

However, factoring $h(X)$ to obtain $h'(X)$ might take a long time. Therefore, an alternative strategy might be to not factor $h(X)$, set $h'(X) = h(X)$, and hope that we gain more time on factoring than we lose later.

In a test implementation, these two methods were about equally fast. Here is a method that is faster than either of the above. Recall that $h(X)$ splits into irreducible factors of equal degree. For each ℓ, choose integers o_ℓ and e_ℓ.

The method is this. For each odd divisor $N \leq o_\ell$ of $\deg(h) = (\ell-1)/2$, check if $h(X)$ has a factor $h'(X)$ of degree N. If not, for each even divisor $N \leq e_\ell$ of $\deg(h) = (\ell-1)/2$, check if $h(X)$ has a factor $h'(X)$ of degree N. If still no divisor h' is found, set $h' = h$.

The constants o_ℓ and e_ℓ need to be chosen based on how long the particular implementation at hand can find factors of degree N of $h(X)$ for various N, and the speed the rest of Section 2.9 takes as a function of the degree of h.

4.2. **Doing with $s \leq 5$.** A simple calculation shows that for $s \geq 3$ odd,

$$\begin{aligned} \deg(a_s) &= s^2, \\ \deg(b_s) &= s^2 - 1, \\ \deg(c_s) &= 3(s^2-1)/2, \\ \deg(d_s) &= 3(s^2-1)/2. \end{aligned}$$

Hence carrying out the step in Section 2.9 will require plugging polynomials into other polynomials of degree up to 180. (Degree 180 occurs for $\ell = 109$, $s = 11$.) However, we can get along with using $s \leq 5$, in which case we have to plug into polynomials of degree no more than 36. This is because whenever $s > 5$ occurs ($\ell = 41, 109$), it turns out that 6 is a semiprimitive root modulo ℓ. We could use $s = 6$ here, but also we can just break down multiplication by 6 to a multiplication by 2 followed by a multiplication by 3, and therefore we can always restrict ourselves to $s \in \{2, 3, 5\}$.

4.3. **Isogeny cycles.** If ℓ is a good auxiliary prime, we can often continue by finding a chain of isogenies from E to E_1 to E_2 to $\ldots$ to E_k etc. Then we can get a degree $\ell^{k-1}(\ell-1)/2$ kernel polynomial in basically no time and we can determine t modulo ℓ^k. For example, when this works for $\ell = 11$, we can find the eigenvalue modulo 121, which takes relatively long (about as long as for $\ell = 127$), but at least Ψ_{11} does not have to be calculated. Note that here the arguments in Section 3.12 about factoring $h(X)$ do not apply. Therefore we must either not factor $h(X)$ or be very careful.

4.4. **Atkin primes.** The algorithm can be made to use slightly fewer auxiliary primes (resulting in a reduction of both running time and memory use) by using an idea of Atkin. Even if $\Psi_\ell(F, j)$ has no roots in $\mathbb{F}_p$, we can get some restrictions on $t^2 \bmod \ell$ by looking at the factorization of $\Psi_\ell(F, j)$. It will usually split into factors which all have the same degree r. The knowledge of r will usually eliminate about

half the possibilities for $t \bmod \ell$, but can even determine $\pm t \bmod \ell$ if r is less than 5 (which is not that common). For details, consult [1] and [19, Proposition 6.2].

4.5. **Catching kangaroos.** Running our algorithm for many (but not all) auxiliary primes, we arrive at a stage where there are only a relatively small number of possible t (and they form an arithmetic sequence). Since $\#E(\mathbb{F}_p) = p + 1 - t$, for the correct t the number $p + 1 - t$ annihilates all points on E (under the group law of E). A t for which $p + 1 - t$ annihilates several random points on E is then probably the correct one. (We use the fact that $E(\mathbb{F}_p)$ "tends" to be cyclic for more certainty, we could also check the quadratic twist E' of E, which has $p+1+t$ points. For details, see [19, Section 3, especially Theorem 3.2].)

For a random point P on E, we can use either Shanks' baby step–giant step method or Pollard's lambda (kangaroo trap) method to determine for which of the possible ts will $p + 1 - t$ annihilate P.

A more significant reduction in running time would result from not dropping quite as many auxiliary primes as our kangaroo trap would allow. Then the probability of the algorithm succeeding would go up, and therefore we wouldn't have to try quite as many curves to get one with the properties described in Section 1.

5. Tables

5.1. **Table of the $P_\ell(J)$.** Note that the primes above 197 do not appear in the sets A_s or A_l. They are provided here for the reader's convenience in implementing the algorithm for use with primes p with more than 200 bits.

ℓ	$P_\ell(J)$
29	$J + 11$
31	$J + 1$
41	$J - 5$
47	$J + 9$
53	$J^2 - 3J + 26$
59	$J + 24$
61	$J^2 - 23J - 1$
71	$J - 33$
73	$J^3 + 32J^2 - 30J + 1$
79	$J^2 + 14J - 1$
83	$J^2 + 7J - 2$
89	$J^2 + 26J - 17$
97	$J^4 + 32J^3 + 42J^2 - 24J - 2$
101	$J^2 + 27J - 13$
103	$J^3 + 34J^2 - 7J - 2$
107	$J^3 + 16J^2 - 32J + 11$
109	$J^3 - 51J^2 + 52J$
113	$J^4 - 37J^3 + 24J^2 - 3J - 36$
127	$J^4 - 54J^3 - 41J^2 - 32J - 2$
131	$J^2 - 47J - 51$
137	$J^5 - 20J^4 - 23J^3 + 53J^2 + 65J + 52$
139	$J^4 - 56J^3 - 18J^2 + 40J + 1$
149	$J^4 + 5J^3 - 61J^2 + 48J - 57$
151	$J^3 + 34J^2 - 7J - 1$

ℓ	$P_\ell(J)$
157	$J^6 - 67J^5 - 48J^4 - 70J^3 + 30J^2 - 5J + 2$
167	$J^3 - 60J^2 + 3J - 14$
173	$J^4 - 34J^3 - 60J^2 - 74J - 22$
179	$J^3 - 83J^2 + 18J - 62$
181	$J^6 + 62J^5 + 12J^4 + 82J^3 - 10J^2 + 51J - 1$
191	$J^3 + 60J^2 - 25J + 56$
193	$J^6 - 24J^5 - 15J^4 - 70J^3 - 53J^2 + 58J + 1$
197	$J^6 + 68J^5 + 14J^4 - 66J^3 + 3J^2 - 59J + 59$
199	$J^5 + 62J^4 + 19J^3 + 46J^2 + 87J + 1$
211	$J^7 + 68J^6 + 88J^5 + 77J^4 + 67J^3 - 10J^2 - 82J + 2$
223	$J^7 - 78J^6 + 108J^5 - 41J^4 + 92J^3 + 78J^2 - 17J + 1$
227	$J^5 - 88J^4 + 45J^3 + 62J^2 + 84J - 73$
229	$J^7 + 60J^6 + 39J^5 - 37J^4 - 114J^3 - 42J^2 + 59J + 1$
233	$J^7 - 81J^6 + 91J^5 + 30J^4 + 115J^3 + 105J^2 + 96J + 30$
239	$J^4 - 107J^3 - 39J^2 - 9J - 28$
241	$J^6 + 115J^5 - 54J^4 - 105J^3 + 40J^2 + 85J + 1$
251	$J^4 + 36J^3 + 87J^2 - 8J + 62$
257	$J^6 - 94J^5 - 112J^4 - 51J^3 - 124J^2 + 42J - 122$
263	$J^5 - 37J^4 - 94J^3 - 40J^2 - 78J + 74$
269	$J^6 + 109J^5 - 38J^4 - 7J^3 + 62J^2 + 4J - 120$
271	$J^6 - 127J^5 - 69J^4 + 132J^3 + 46J^2 - 63J - 2$
277	$J^9 - 48J^8 - 70J^7 + 3J^6 - 87J^5 + 25J^4 + 105J^3 + 39J^2 + 24J + 1$
281	$J^7 + 131J^6 - 34J^5 - 36J^4 + 101J^3 + 114J^2 + 115J + 53$

5.2. **Table of the s for each $\ell \in A$.**

ℓ	s
$3, 5, 7, 11, 13, 19, 23, 29, 47, 53, 59, 61, 71, 79, 83, 101$	2
$103, 107, 131, 139, 149, 167, 173, 179, 181, 191, 197$	2
$17, 31, 89, 113, 127, 137$	3
$73, 97, 151, 157, 193$	5
41	7
109	11

5.3. **Table of the Ψ_ℓ for each $\ell \in A_{\mathrm{s}}$.**

$$\begin{aligned}\Psi_3(F,J) &= F^4 + (-J+792)F^3 + (-36J+221400)F^2 \\ &\quad + (1916J + 24690528)F + (J^2 + 50976J + 803894544)\end{aligned}$$

$$\begin{aligned}\Psi_5(F,J) &= F^6 + (-J+780)F^5 + (-30J+218940)F^4 \\ &\quad + (310J + 25968800)F^3 + (13700J + 1177897200)F^2 \\ &\quad + (38424J + 22576632000)F + (J^2 - 614000J + 155720872000)\end{aligned}$$

$$\begin{aligned}\Psi_7(F,J) &= F^8+(-J+776)F^7+(-28J+217756)F^6\\ &+(21J+26195512)F^5+(6328J+1276406726)F^4\\ &+(39361J+31050881848)F^3+(-240492J+404938789276)F^2\\ &+(-2176581J+2721214073864)F\\ &+(J^2-1711008J+7427483226241)\end{aligned}$$

$$\begin{aligned}\Psi_{11}(F,J) &= F^{12}+(-J+684)F^{11}+(55J+157410)F^{10}\\ &+(-1188J+12515580)F^9+(12716J+75763215)F^8\\ &+(-69630J+76077144)F^7+(177408J-207606564)F^6\\ &+(-133056J-34321320)F^5+(-132066J+418524975)F^4\\ &+(187407J-477130500)F^3+(-40095J+270641250)F^2\\ &+(-24300J-82012500)F+(J^2+6750J+11390625)\end{aligned}$$

$$\begin{aligned}\Psi_{13}(F,J) &= F^{14}+(-J+772)F^{13}+(-26J+216424)F^{12}\\ &+(-156J+26333528)F^{11}+(1508J+1359640022)F^{10}\\ &+(21658J+39120460496)F^9+(39624J+716780223796)F^8\\ &+(-612742J+8956723925032)F^7\\ &+(-3355976J+79070093432161)F^6\\ &+(454779J+500196729175884)F^5\\ &+(43741490J+2260671730897788)F^4\\ &+(95939974J+7142292018579744)F^3\\ &+(-41335164J+15009662255513328)F^2\\ &+(-291162600J+1887420148839648 0)F\\ &+(J^2-174668400J+10755802087387200)\end{aligned}$$

$$\begin{aligned}\Psi_{17}(F,J) &= F^{18}+(-J+690)F^{17}+(51J+160191)F^{16}\\ &+(-1105J+12849212)F^{15}+(13243J+77940903)F^{14}\\ &+(-95659J-24306702)F^{13}+(424065J-489756655)F^{12}\\ &+(-1110355J+856070496)F^{11}+(1454945J+247945272)F^{10}\\ &+(-73746J-4127455840)F^9+(-2450210J+10326614640)F^8\\ &+(3131026J-15993234432)F^7\\ &+(-1104830J+18158824448)F^6\\ &+(-1073992J-15889021440)F^5\\ &+(1392232J+10788499200)F^4\\ &+(-557600J-5622784000)F^3\\ &+(-2720J+2154240000)F^2\\ &+(67200J-537600000)F+(J^2-16000J+64000000)\end{aligned}$$

$$\begin{aligned}\Psi_{19}(F,J) &= F^{20}+(-J+664)F^{19}+(76J+143260)F^{18}\\ &\quad+(-2622J+9204360)F^{17}+(54454J-176115066)F^{16}\\ &\quad+(-761425J+1108178952)F^{15}+(7598556J-1742337316)F^{14}\\ &\quad+(-55989713J-13420942600)F^{13}\\ &\quad+(310967414J+79673435585)F^{12}\\ &\quad+(-1317638334J-133492721376)F^{11}\\ &\quad+(4284347658J-271425795648)F^{10}\\ &\quad+(-10696404825J+1738318231104)F^{9}\\ &\quad+(20413753140J-3257912161280)F^{8}\\ &\quad+(-29485216120J+528231178240)F^{7}\\ &\quad+(31694225470J+10718241992704)F^{6}\\ &\quad+(-24698209440J-26958821326848)F^{5}\\ &\quad+(13397395520J+36334713176064)F^{4}\\ &\quad+(-4738229120J-31060143636480)F^{3}\\ &\quad+(973578240J+16944463872000)F^{2}\\ &\quad+(-91238400J-5430382166016)F\\ &\quad+(J^{2}+1769472J+782757789696)\end{aligned}$$

$$\begin{aligned}\Psi_{23}(F,J) &= F^{24}+(-J+720)F^{23}+(23J+179952)F^{22}\\ &\quad+(-161J+17282016)F^{21}+441081120F^{20}\\ &\quad+(3864J+5678198784)F^{19}+(-5681J+45492865088)F^{18}\\ &\quad+(-46644J+252605710080)F^{17}\\ &\quad+(53084J+1038071734272)F^{16}\\ &\quad+(393024J+3294356631552)F^{15}\\ &\quad+(19136J+8309302456320)F^{14}\\ &\quad+(-1978368J+16991995871232)F^{13}\\ &\quad+(-2689666J+28563290271744)F^{12}\\ &\quad+(2882544J+39839110889472)F^{11}\\ &\quad+(11625488J+46370418130944)F^{10}\\ &\quad+(11002464J+45154515419136)F^{9}\\ &\quad+(-3833824J+36762400456704)F^{8}\\ &\quad+(-19783680J+24919460020224)F^{7}\\ &\quad+(-21906304J+13946021740544)F^{6}\\ &\quad+(-11787776J+6353857806336)F^{5}\\ &\quad+(-1554432J+2304837156864)F^{4}\\ &\quad+(2213888J+642483486720)F^{3}\\ &\quad+(1648640J+129654325248)F^{2}\\ &\quad+(516096J+16911433728)F\\ &\quad+(J^{2}+65536J+1073741824)\end{aligned}$$

References

[1] A. O. L. Atkin. Several public email messages. unpublished, 1991–1992.

[2] Ian F. Blake, János A. Csirik, Michael Rubinstein, and Gadiel Seroussi. On the computation of modular polynomials. preprint, 1999.

[3] Ian F. Blake, Gadiel Seroussi, and Nigel Smart. *Elliptic Curves in Cryptography*, volume 265 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, 1999.

[4] Henri Cohen. *A Course in Computational Algebraic Number Theory*, volume 138 of *Graduate Texts in Mathematics*. Springer, 1993.

[5] J.-M. Couveignes and François Morain. Schoof's algorithm and isogeny cycles. In Leonard M. Adleman and Ming-Deh Huang, editors, *Algorithmic number theory, Proceedings of the First International Symposium (ANTS-I) held at Cornell University, Ithaca, New York, May 6–9, 1994*, number 877 in Lecture Notes in Computer Science, pages 43–58. Springer, Berlin, 1994.

[6] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In P. Deligne and W. Kuyk, editors, *Modular Functions of One Variable II*, volume 349 of *Lecture Notes in Mathematics*, pages 143–316. Springer, 1972.

[7] L. Dewaghe. Remarks on the Schoof-Elkies-Atkin algorithm. *Mathematics of Computation*, 67(223):1247–1252, 1998.

[8] Noam D. Elkies. Explicit isogenies. manuscript, Boston, MA, 1992.

[9] Noam D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In D. A. Buell and J. T. Teitelbaum, editors, *Computational Perspectives in Number Theory: Proceedings of a Conference in Honor of A. O. L. Atkin, (Chicago, IL, 1995)*, pages 21–76. AMS, 1998.

[10] Steven Galbraith and James McKee. The probability that the number of points on an elliptic curve over a finite field is prime. preprint CORR 99–51, University of Waterloo, Centre for Applied Cryptographic Research, 1999.

[11] Robin Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. springer, 1977.

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

[13] T. Izu, J. Kogure, M. Noro, and K. Yokoyama. Efficient implementation of Schoof's algorithm. In Kazuo Ohta and Dingyi Pei, editors, *Proceedings of ASIACRYPT '98*, volume 1514 of *Lecture Notes in Computer Science*, pages 66–79. Springer, 1998.

[14] Toshitsune Miyake. *Modular Forms*. Springer, 1989.

[15] François Morain. Calcul du nombre de points sur une courbe elliptique dans un cops fini: aspects algorithmiques. *Journal de Théorie des Nombres de Bordeaux*, 7:255–282, 1995.

[16] Volker Müller. *Ein Algorithmus zur Bestimmung der Punktzahl elliptischer Kurven über endlichen Körpern der Charakteristik größer drei*. PhD thesis, Universität des Saarlandes, 1995.

[17] J.-M. Pollard. Monte Carlo methods for index computation (*modp*). *Mathematics of Computation*, 32(143):918–924, July 1978.

[18] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, 44:483–494, 1985.

[19] René Schoof. Counting points on elliptic curves over finite fields. *Journal de Théorie des Nombres de Bordeaux*, 7:219–254, 1995.

[20] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, 1986.

AT&T Shannon Lab, 180 Park Ave, Florham Park NJ 07932-0971

E-mail address: janos@research.att.com