Schoof-Elkies-Atkin Algorithm for Point Counting on an Elliptic Curve over a Finite Field

Joanna Gaski

December 10, 2010

1 Introduction

Let E be an elliptic curve given by the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where the a_i are integers. If we consider E as a curve over $\mathbb{Q}$, then for any finite field $\mathbb{F}_q$, the number of points (x, y) in $\mathbb{F}_q$ x $\mathbb{F}_q$ which satisfy the elliptic curve equation (when taken for all finite fields) characterizes the isogeny class of the curve E. If instead we take E as a curve over some finite field $\mathbb{F}_q$ from the beginning, then the number of points of $E/\mathbb{F}_q$ can help to solve the discrete logarithm problem for two points P and Q on E.

The value $\#E(\mathbb{F}_q)$, the cardinality of E over $\mathbb{F}_q$, can be determined by several means. As the most straightforward solution, we could take all points in $\mathbb{F}_q$ x $\mathbb{F}_q$, and see if they satisfy the equation, which would take $O(q^2)$ operations. We could also express the curve as $f = y^2 - x^3 + Ax + B$ (ignoring the case where the characteristic of $\mathbb{F}_q$ is two), and use the relationship

$$\#E(\mathbb{F}_q) = q + 1 - a_q \text{ and}$$
$$a_q = \sum_{x \in \mathbb{F}_q} \left(\frac{f(x)}{q} \right)$$

where $\left(\frac{f(x)}{q} \right)$ is the Legendre symbol. In this way, we would need to compute $f(x)$ for all $x \in \mathbb{F}_q$, which would be $O(q)$ computations.

Other techniques to compute $E(\mathbb{F}_q)$ include baby-step / giant-step, which is also exponential time $O(q^{1/4})$.

2 Schoof's algorithm

In 1985, René Schoof published a paper describing an algorithm to compute the cardinality of $E(\mathbb{F}_q)$ for such a curve. If $q = p^e$ where p is a large prime, and $f = y^2 = x^3 + Ax + B$ is the equation for E, then Hasse's theorem state that $|a_q| \leq 2\sqrt{q}$. We can use this short form of the Weierstrass equation for E because the characteristic of $\mathbb{F}_q$ is not 2 or 3. Thus, if we can calculate a_q modulo l for a set S of small primes l such that

$$\prod_{l \in S} l > 4\sqrt{q},$$

then a_q can be reconstructed using the Chinese Remainder Theorem.

When $l = 2$ the determination of a_q modulo l is straightforward. We know that $E[2]$ contains $\mathcal{O}$, the unique point at infinity, and by Hasse's theorem that $\#E(\mathbb{F}_q) = q + 1 - a_q$. Since $q + 1$ is even, this gives $\#E(\mathbb{F}_q) \equiv a_q \bmod 2$. If $f = x^3 + Ax + B$ has no root in $\mathbb{F}_q$, then $E(\mathbb{F}_q)$ has no 2-torsion points, and so a_q is odd. If $x^3 + Ax + B$ has a root $(e, 0)$ in $E(\mathbb{F}_q)$, then the fact that $E[n] \simeq \mathbb{Z}/2\mathbb{Z}$ x $\mathbb{Z}/2\mathbb{Z}$ forces $\#E(\mathbb{F}_q)$ to be even.

Instead of checking all points in $\mathbb{F}_q$ to find if $x^3 + Ax + B$ has a root, we use the fact that the points in $\mathbb{F}_q$ are exactly the points satisfying $x^q - x = 0$. Thus, $\gcd(x^q - x, x^3 + Ax + B) = 1 \iff f$ has no root in $\mathbb{F}_q$.

3 The trace of Frobenius

For $l > 2$ an odd prime, another method is used to determine a_q modulo l. The q-power Frobenius endomorphism on E

$$\tau : E(\bar{\mathbb{F}}_q) \longrightarrow E(\bar{\mathbb{F}}_q)$$

$$\tau : x \longmapsto x^q$$

$$\tau : \mathcal{O} \longmapsto \mathcal{O}$$

satisfies its characteristic polynomial

$$x^2 - a_q x + q = 0,$$

where a_q is the trace of the Frobenius element. If $P = (x, y) \in E(\mathbb{F}_q)$, this becomes

$$(x^{q^2}, y^{q^2}) + q(x, y) = a_q(x^q, y^q).$$

When l is an odd prime for which $\gcd(q, l) = 1$, and $P \in E[l]$ is an l-torsion point of E, then

$$(x^{q^2}, y^{q^2}) + [q](x, y) \equiv [a_q](x^q, y^q) \text{ modulo } l.$$

Thus the set S of residues a_q modulo l can be obtained by restricting our attention to the l-torsion points of E for each l. Using those points only, the above comparison will yield each residue $[a_q]$ modulo l.

4 Torsion polynomials

In order to work with all points in $E[l]$ simultaneously, Schoof saw that the comparison could be carried out in a particular quotient ring $R_l = \mathbb{F}_q[x, y]/(f - y^2, f_l)$ of $\mathbb{F}_q[x, y]/(f - y^2)$. The torsion polynomials (equivalently called division polynomials), given by

$$\begin{aligned}
\psi_1 &= 1, \\
\psi_2 &= 2y, \\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2, \\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3), \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, && \text{for } m \geq 2, \\
\psi_{2m} &= \left(\frac{\psi_m}{2y}\right) \cdot \left(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2\right), && \text{for } m \geq 3.
\end{aligned}$$

are useful for this application because they satisfy the following properties. Let

$$f_m(x, y) = \begin{cases} \psi_m(x, y), & \text{if } m \text{ is odd;} \\ \psi_m(x, y)/2y, & \text{if } m \text{ is even.} \end{cases}$$

- For all positive integers m, the polynomial ψ_m is contained in the polynomial ring $\mathbb{Z}[A, B, x, y]$. Furthermore, the polynomial f_m depends only on x.

- A point $P = (x, y) \in \mathbb{F}_q$ x $\mathbb{F}_q$ is a root of the torsion polynomial ψ_m if and only if P is a non-zero m-torsion point of E over $\mathbb{F}_q$. Similarly, x is a root of f_m if and only if x is the x-coefficient of such a point P.

- The multiplication by m map needed to compute a_q can be expressed as a rational map in the ψ_i. In particular

$$[m]P = \left(x - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2}, \frac{\psi_{2m}}{2\psi_m^4} \right).$$

- For l odd, the order of ψ_l or f_l is $\frac{1}{2}(l^2 - 1)$.

5 The quotient ring $R_l = \mathbb{F}_q[x, y]/(f - y^2, f_l)$

Because the roots of ψ_l in $\mathbb{F}_q$ are the l-torsion points of $E(\mathbb{F}_q)$, when working with the l-torsion points of E, we can perform the comparison

$$(x^{q^2}, y^{q^2}) + [q](x, y) \equiv [a_q](x^q, y^q) \text{ modulo } l$$

in the smaller ring R_l. So Schoof's algorithm interates over the integer residues modulo l, and checks for the equality

$$(x^{q^2}, y^{q^2}) + [q \bmod l](x, y) \equiv [a_q \bmod l](x^q, y^q) \text{ in } R_l.$$

Because we are working modulo $f - y^2$, all powers of y greater than or equal to 2 can be reduced to power 0 or 1 in R_l. Because the order of ψ_l is $\frac{1}{2}(l^2 - 1)$, powers of x can be similar reduced so that multiplications and comparisons are done with polynomials of x degree less than or equal to $\frac{1}{2}(l^2 - 1)$, and y degree less than 2.

6 Schoof's algorithm – outline of the steps

We are given a prime power order of a finite field, $q = p^e$, and an elliptic curve E: f $= y^2 = x^3 + Ax + B$ over that field. We want to find $\#E(\mathbb{F}_q) = q + 1 - a_q$.

1. Choose a smallest set of the first n prime S such that each prime l is coprime to q, and $\prod_{l \in S} l > 4\sqrt{q}$.

2. For $l = 2$, calculate $\gcd(x^q - x, f)$. If the gcd is 1, set $a_q \equiv 0$ modulo 2, else $a_q \equiv 1$ modulo 2.

3. For each odd prime $l \in S$:
    (a) Calculate the x coordinate of $(x^{q^2}, y^{q^2}) + [q](x, y)$ in R_l where $[q]$ is q modulo l.
    (b) For each residue n_l modulo l:
        i. Calculate the x coordinate of $[n_l](x^q, y^q)$ in R_l.
        ii. Compare the x coordinates of $(x^{q^2}, y^{q^2}) + [q](x, y)$ and $[n_l](x^q, y^q)$ in R_l.
        iii. If they are equal:
            A. Calculate the y coordinate of $(x^{q^2}, y^{q^2}) + [q](x, y)$ modulo R_l
            B. Calculate the y coordinate of $[n_l](x^q, y^q)$ in R_l.
            C. Compare the y coordinates of $(x^{q^2}, y^{q^2}) + [q](x, y)$ and $[n_l](x^q, y^q)$ in R_l.
            D. If they are equal, set $a_q \equiv n_l$ modulo l. Else $a_q \equiv -n_l$ modulo l.
            E. Move to next prime l until S exhausted. This prime l is done.
        iv. Else, continue to next residue n_l modulo l.
    (c) If all residues modulo l are exhausted, and there was no x coordinate match, check if q is a square modulo l.
        i. If not, then set $a_q \equiv 0$ modulo l.
        ii. If so, choose w so that $w^2 \equiv q$ modulo l.
            A. Calculate the x coordinate of $(x^q, y^q) - [w](x, y)$.
            B. If gcd(numerator of x-coordinate, ψ_l) $= 1$, set $a_q \equiv 0$ modulo l.
            C. Otherwise, calculate the y coordinate. If gcd(numerator of (y-coordinate)$/y, \psi_l$) $\neq 1$, set $a_q \equiv 2w$ modulo l. Else set $a_q \equiv -2w$ modulo l.
4. When all residues of a_q modulo prime in S are computed, compute a_q such that a_q is the unique integer satisfying those congruences, and in the range $-2\sqrt{q} \leq a_q \leq 2\sqrt{q}$.

7 Elkies & Atkin improvements

For the Elkies & Atkins improvements to Schoof's original algorithm, we let E be an elliptic curve defined over $\mathbb{F}_p$ where p is a large prime. We also require that E is not supersingular, meaning that $E[p]$ is not trivial. This is not a severe restriction because in the case that $E/\mathbb{F}_p$ was supersingular, we would have $\#E(\mathbb{F}_p) = p + 1$. We also require that $j(E)$, the j-invariant of E, is not zero or 1728.

The improvements follow from the determination of whether l is an Elkies or Atkin prime, for each prime $l \in S$ as in Schoof's. This equates to whether the reduced characteristic polynomial of the Frobenius endomorphism,

$$\chi_l(x) = x^2 - [a_p]x + [p]$$

splits in $\mathbb{F}_p$, where $[a_p]$ and $[p]$ are a_p and p modulo l respectively, with τ the p-power Frobenius endomorphism and a_p the trace of the Frobenius as in the q case. This in turn equates to the question of whether the Frobenius discriminant $\Delta_{\chi_l} = [a_p]^2 - 4[p]$ is a square in $\mathbb{F}_l$.

As a_q is the quantity to be determined by the algorithm, this cannot be computed at the outset, but is determined from the behaviour of the l-th modular polynomial $\Phi_l(x, j(E))$ on E, described in the next section.

The basis for the performance improvements of Elkies' & Atkin's contributions to Schoof's algorithm are several-fold. For Elkies primes, arithmetic can be carried out in a smaller quotient ring R'_l, and the search for $[a_p]$ modulo l is simplified. The ring will be $R'_l = \mathbb{F}_q[x, y]/(f - y^2, F_l)$ where F_l is a degree $(l-1)/2$ polynomial, versus the degree $(l^2 - 1)/2$ degree polynomial f_l. For Atkin primes, we will need to work with elements in the extension $\mathbb{F}_{l^2}$ of $\mathbb{F}_l$. But the search for the residue $[a_p]$ modulo l will only have to consider operations on the primitive r-th roots of unity in $\mathbb{F}_{l^2}$ where r is the degree of the Frobenius endomorphism acting on $E[l]$.

8 Background to define the modular polynomial

To define the modular polynomial $\Phi_l(x, j(E))$ and explain its use in SEA, we define the j-invariant $j(E)$ of an elliptic curve E, the Weierstrass $\wp$ function, and explain the relationship between an elliptic curve $E/\mathbb{C}$ and the associated lattice $\Lambda \subset \mathbb{C}$. We try to keep this minimal and focus on the methods of the algorithms.

Briefly, there is a bijective relationship between isomorphism classes of elliptic curves over $\bar{K}$, and the values of the j-invariant $j(E)$, so that $E_1/\bar{K} \simeq E_2/\bar{K} \iff$

$j(E_1) = j(E_2)$. The j-invariant can be defined as $j(E) = 1728(\frac{4A^3}{4A^3+27B^2})$. Additionally, each isomorphism class of elliptic curves over $\mathbb{C}$ is associated with a particular lattice (fully identified by $\tau = \omega_1/\omega_2 \in \mathcal{H}$ the upper half plane, with (ω_1, ω_2) a homogeneous basis so that $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \mathbb{Z} + \tau\mathbb{Z})$ Λ of $\mathbb{C}$. With E in short Weierstrass form, there is a bijective correspondence between E and $\mathbb{C}/\Lambda$ given by the map

$$\begin{aligned} \mathbb{C}/\Lambda &\longrightarrow E \\ z + \Lambda &\longmapsto \begin{cases} (\wp(z), (\wp'(z)/2), & \text{for } z \notin \Lambda; \\ \mathcal{O}, & \text{for } z \in \Lambda. \end{cases} \end{aligned}$$

Here, $\wp$ is the Weierstrass $\wp$ function, relative to Λ, given by the series

$$\wp(z; \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}.$$

When the lattice Λ is fixed, as when dealing with a particular elliptic curve, we write $\wp(z)$. Furthermore, because of the correspondence between j-invariants of isomorphism classes of elliptic curves over $\mathbb{C}$, and lattices in the complex plane, the j-invariant function can be given in terms of the lattice Λ in the complex plane, independent of any specific elliptic curve.

Schoof [3] creates the following formal power series in $\mathbb{Z}[[q]]$ and uses a relation of Jacobi to express j as a function of $q = e^{2\pi i \tau}$.

$$E_4(q) = 1 + 240 \sum_{n=1}^{\infty} \frac{n^3 q^n}{1 - q^n} \equiv -48A \text{ modulo } \mathfrak{B}$$

$$E_6(q) = 1 - 504 \sum_{n=1}^{\infty} \frac{n^5 q^n}{1 - q^n} \equiv 864B \text{ modulo } \mathfrak{B}$$

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

Here $\mathfrak{B}$ is a prime ideal of $\mathcal{O}_k$ for a number field K in which $E_4(q)$ and $E_6(q)$ are integers, and the residue field $\mathcal{O}_k/\mathfrak{B} \simeq \mathbb{F}_p$. With j expressed in terms of the complex variable $\tau \in \mathcal{H}$, we can define the modular polynomial.

9 The modular polynomial $\Phi_l(x, j(E))$

For $n \in \mathbb{Z}_{>0}$, let

$$S_n^* = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \text{ such that } a,\, b, \text{ and } d \in \mathbb{Z},\ 0 \leq b < d,\ ad = n, \text{ and } \gcd(a, b, d) = 1. \right\}$$

Define $j \circ \alpha$ by $j \circ \alpha(\tau) = j(\frac{a\tau+b}{d})$.

Definition 1 (Modular polynomial)**.** *Let $l \in \mathbb{Z}_{>0}$. Then the l-th modular polynomial $\Phi_l(x, j)$ is given by*

$$\Phi_l(x, j) = \prod_{\alpha \in S_n^*} (x - j \circ \alpha).$$

This $\Phi_l(x, j)$ has the property that if j_{E_1} and j_{E_2} are the j-invariants of two elliptic curves E_1 and E_2 defined over $\mathbb{C}$, then $\Phi_l(j_{E_1}, j_{E_2}) = 0$ if and only if there is no isogeny of degree l from E_1 to E_2.

Let E be an elliptic curve defined over the finite field $\mathbb{F}_p$ and l be a prime coprime to p. Recall that $E[l] \simeq \mathbb{Z}/l\mathbb{Z} \text{ x } \mathbb{Z}/l\mathbb{Z}$, and that therefore $E[l]$ has $l+1$ cyclic subgroups of order l. In this situation, the zeroes $\tilde{j}$ of $\Phi_l(x, j(E)) = 0$ are the j-invariants of the isogenous curves $\tilde{E} = E/C$ where C is one of those order l subgroups.

10 Distinguishing Atkin & Elkies primes

Recall that a prime l was an Elkies prime for an elliptic curve E defined over $\mathbb{F}_p$ if the characteristic polynomial of the reduced p-power Frobenius endomorphism $x^2 - [a_p]x + p = 0$ splits into linear factors over $\mathbb{F}_l$, and an Atkin prime otherwise. The modular polynomial provides a way to determine if this polynomial splits without knowing a_p.

The comparison turns out to be straightforward. If the degree of $\gcd(\Phi_l(x, j(E)), x^p - x) = 0$, then l is an Atkin prime. Otherwise, l is an Elkies prime. Recall that the roots of $x^p - x$ are the elements of $\mathbb{F}_p$, so that the above gcd will be 1 if and only if $\Phi_l(x, j(E))$ has no root in $\mathbb{F}_p$. In this case, the degree is zero.

The correspondence follows from a theorem of Atkin [3] classifying the possible factorizations of $\Phi_l(x, j(E))$ in $\mathbb{F}_p[x]$. In summary, when $E/\mathbb{F}_p$ is ordinary with $j \neq$

$0, 1728$, and $\Phi_l(x, j(E)) = h_1 h_2 ... h_s$ is the factorization of $\Phi_l(x, j(E))$, then the h_i have degree either

1. $(1, 1, \ldots 1)$ or $(1, l)$. In these cases, $[a_q]^2 - 4p \equiv 0$ modulo l and so is a square.
2. $(1, 1, r, \ldots r)$. In this case $[a_q]^2 - 4p$ is a square modulo l.
3. $(r, r, \ldots r)$. In this case, $[a_q]^2 - 4p$ is not a square modulo l.

11 Elkies primes

When Δ_{χ_l} is a square modulo l, and $\chi_l(x) = x^2 - [a_p]x + [p] = (x - \lambda)(x - \mu)$ splits in $\mathbb{F}_l$, we can find a factor F_l of division polynomial f_l with linear degree $(l+1)/2$. This new polynomial can be used to create a smaller quotient ring R_l' in which to find $[a_p]$ modulo l such that $(x^{q^2}, y^{q^2}) + [p](x, y) = [a_p](x^q, y^q)$ as in Schoof's original algorithm.

To construct the polynomial F_l, first a root of the modular polynomial $\Phi_l(x, j(E)) \in \mathbb{F}_p[x]$ is found, giving an isogenous curve $\tilde{E}$ to E. (In practice, polynomials which have smaller coefficients than the modular polynomials, but have similar properties, such as Müller's modular polynomial $G_l(x, y)$ [1].) Rarely, this curve may not provide the necessary isogeny and another curve may need to be used, if $(j, \tilde{j})$ is a singular point of $\Phi_l(x, y)$.

From the Weierstrass equations of E and $\tilde{E}$, the coefficients a_i of

$$F_l(x) = x^{(l-1)/2)} + a_{(l-3)/2} x^{(l-3)/2} + \ldots + a_0$$

can be computed, using the Laurent series of $\wp$ as described in [3].

Furthermore, since $\chi_l(x)$ splits in $\mathbb{F}_p$, we know that $[a_p] = \lambda + \mu = \lambda + \frac{[p]}{\lambda}$ for some $\lambda, \mu \in \mathbb{F}_p$, so it suffices to find λ. A theorem of Atkin (treated briefly in next section) categorizes the possible cases for Elkies primes. Both λ and μ are the eigenvalues of the Frobenius τ, so that there is a point $P \in E[l] \setminus \mathcal{O}$ with $\tau(P) = [\lambda]P$. Expanding the multiplication by λ map, we have that the x-coefficient of P must satisfy

$$x^p = x - \frac{\psi_{\lambda-1}\psi_{\lambda+1}}{\psi_\lambda^2}.$$

Since P is an l-torsion point, this means that P satisfies both $F_l(P) = 0$ and $\psi_\lambda^2(x^- x) + \psi_{\lambda-1}\psi_{\lambda+1} = 0$. So the computation of $[a_p]$ modulo l is reduced to finding $\lambda \in \mathbb{F}_l$ such that

$$\gcd(\psi_\lambda^2(x^- x) + \psi_{\lambda-1}\psi_{\lambda+1}, F_l) \neq 1.$$

12 Atkin primes

In the case that $\chi_l(x) = x^2 - [a_p]x + p$ does not split in $\mathbb{F}_p$, ie where $\Phi_l(x, j(E))$ is irreducible in $\mathbb{F}_p[x]$, we use another technique. We find the degree r of the smallest extension field $\mathbb{F}_{p^r}$ of $\mathbb{F}_p$ containing the roots of$\Phi_l(x, j(E))$. From Atkin's theorem [3], r will be the smallest integer such that

$$\gcd(\Phi_l(x, j(E)), x^{p^r} - x) = \Phi_l(x, j(E)).$$

Atkin's earlier theorem on the factorization of $\Phi_l(x, j(E))$ restricts the values that must be checked, as r must satisfy $r|(l+1)$ and $(-1)^{(l+1)/r} = (\frac{p}{l})$. Further, this r will equal the degree of the Frobenius endomorphism acting on $E[l]$.

Since $\mathbb{F}_{l^2}$ contains a primitive r-th roots of unity for $\mathbb{F}_l$, it turns out that $\chi_l(x) = (x-\lambda)(x-\mu)$ splits in $\mathbb{F}_{l^2}$, which is isomorphic to $\mathbb{F}_l[\sqrt{d}]$ for some non-square $d \in \mathbb{F}_l$, and that λ/μ must be such a primitive r-th root. If g is a generator of $\mathbb{F}_{l^2}^*$, then $\gamma = g^{(l^2-1)/2)}$ is a primitive r-th root, and powers (all powers n coprime to r) give the other primitive r-th roots.

Since $\lambda\mu = [p] \in \mathbb{F}_l$ and $\lambda + \mu = [a_p] \in \mathbb{F}_l$, we know that $\lambda = a_1 + a_2\sqrt{d}$ and $\mu = a_1 - a_2\sqrt{d}$ for some $a_1, a_2 \in \mathbb{F}_l$, and d non-square as above. After fixing such a d, Atkin's technique checks for each of the $\gamma^n = g_{n_1} + g_{n_2}\sqrt{d}$ whether $p(g_{n_1} + 1)/2$ is a square in $\mathbb{F}_l$. If not, that γ^n can be discarded because it cannot possibly satisfy

$$\gamma^n = g_{n_1} + g_{n_2}\sqrt{d} = \frac{\lambda}{\mu} = \frac{\lambda^2}{\lambda\mu} = \frac{a_1^2 + da_2^2 + 2a_1a_2\sqrt{d}}{p}$$
$$= \frac{a_1^2 + da_2^2}{p} + \frac{2a_1a_2}{p}\sqrt{d}.$$

For a particular γ^n to satisfy the above ($\gamma^n = \lambda/\mu$), since $p = a_1^2 - da_2^2$ and $pg_{n_1} = a_1^2 + da_2^2$ we would have $a_1^2 = p(g_{n_1} + 1)/2$. For the non-discarded γ^n, each $\pm 2a_1$ is added to the possible a_p since $a_p = \lambda + \mu = 2x_1$. In this technique, a (small) set of possible residues $[a_p]$ modulo l is collected, instead of a single value as with Schoof's original algorithm and Elkies primes.

13 SEA algorithm – outline of the steps

We are given a prime order of a finite field, p, and an Elliptic curve E: $\mathrm{f} = y^2 = x^3 + Ax + B$ over that field. We want to find $\#E(\mathbb{F}_p) = p + 1 - a_p$. For each Elkies prime, we will keep a residue $E_l \equiv a_p$ modulo l. For each Atkin prime, we will keep a set A_l of possible residues of a_p modulo l.

1. Compute the j-invariant $j = j(E)$.
2. Loop over primes l while a_p is not fully determined. For each prime l:
   (a) Compute $\gcd(\Phi_l(x, j), x^p - x)$.
   (b) If the degree of the gcd is 0, this is an Atkin prime.
      i. Find degree r of p-power Frobenius τ acting on $E[l]$.
      ii. Choose a non-square element d of $\mathbb{F}_l$.
      iii. Find a generator g of $\mathbb{F}^*_{l^2}$.
      iv. Create $T = \{g^n\colon \gcd(n, r) = 1,\, n \in \mathbb{F}_l\}$.
      v. For each $\gamma \in T$:
         A. Express γ as $g_1 + g_2\sqrt{d}$.
         B. Check if $p(g_1+1)/2$ is a square in $\mathbb{F}_l$. If not, move to next element of T. If so, calculate a_1 such that $a_1^2 = p(g_1+1)/2$ and add $\{\pm 2a_1\}$ to the set A_l, possible residues a_p mod l.
   (c) Otherwise, this is an Elkies prime.
      i. Find polynomial $\mathbb{F}_l$ factor of f_l.
      ii. Find $\lambda \in \mathbb{F}_l$ such that $\gcd(\psi_\lambda^2(x^- x) + \psi_{\lambda-1}\psi_{\lambda+1}, F_l) \neq 1$.
      iii. Save $[a_p] = \lambda + p/\lambda$ as E_l.
3. Recover a_q from the A_l and E_l residues, as the unique integer satisfying those congruences in the range $-2\sqrt{q} \leq a_q \leq 2\sqrt{q}$.

14 Complexity of the algorithms and a few benchmarks

Schoof's original algorithm is not implemented in practice, because its $O(\log^8 q)$ complexity is prohibitive. Using SEA, it may be necessary to work with a larger set of primes than in Schoof's algorithm, due to the set of possible residues $[a_p]$ modulo l when l is an Atkin prime. However, in SEA the modular polynomials can be precomputed, and with Elkies primes, it is much faster to compute in the smaller quotient ring R'_l.

The following table is of the algorithm complexities for baby-step / giant step, Schoof's algorithm, and SEA.

	Algorithm		
	BSGS	Schoof's	SEA
Largest prime		$O(\log q)$	$O(\log q)$
Outer loop on l		$O(\log q)$	$O(\log q)$
Inner loop over n_l		$O(\log^6 q)$ bit ops in R_l	$O(\log^4 q)$ bit ops in R'_l
Total	$O(q^{1/4})$	$O(\log^8 q)$	$O(\log^6 q)$

SEA is implemented in the PARI number theory software package, which is included with the open source Sage software system. Another common but commercial implementation of SEA is in the Magma computer algebra system. The following rough benchmarks were done in Sage 4.6 (with PARI 2.4.3) and in Magma version 2.17-1 via an online calculator. In each case, the cardinality of $E : y^2 = x^3 + x + 1$ was found over $\mathbb{F}_p$ where p was the first prime with n digits.

	Algorithm & Implementation		
Number of digits of p	BSGS, Sage	SEA, Sage	SEA, Magma
15	1.02 s	4.43 ms	340 ms
20	23.4 s	38.6 ms	370 ms
80	-	7.79 s	8.429 s
90	-	14.9 s	14.720 s
100	-	20.1 s	19.339 s
110	-	24.8 s	26.600 s
120	-	54.2 s	48.649 s
130	-	fail	59.659 s
140	-	fail	$>$ 60 s, so could not complete

Because these tests were run on different computers, with different hardware configurations and different operating systems, they cannot be taken as a fine-grained comparison. However, they clearly highlight the improvement that Schoof's algorithm (and SEA in particular) were to previous algorithms.

References

[1] Ian Blake, Gadiel Seroussi & Nigel Smart, *Elliptic curves in cryptograhy*, volume 265 of London Mathematical Society Lecture Note Series, Cambridge University Press, (2002)

[2] Ben Galin *Schoof-Elkies-Atkin Algorithm*, Senior Thesis, Department of Mathematics, Stanford University, Stanford, CA, (December 2007).

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

[4] Daniel Shumow, *Isogenies of Elliptic Curves: A Computational Approach*, Masters Thesis, Department of Mathematics, University of Seattle, Seattle, WA, (June 2009).

[5] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd Edition, Springer-Verlag, Graduate Texts in Mathematics, (2009).

[6] Lawrence C. Washington, *Elliptic Curves: Number theory and cryptography*, 2nd Edition, Chapman & Hall, (2008).