Final Report: A Brief Introduction to the Scoof-Elkies-Atkins(SEA) Algorithm

This is a modification to the basic Schoof's Algorithm which improves the computational efficiency. Throughout the notes, we assume $E : y^2 = x^3 + Ax + B$ is a non-supersingular elliptic curve defined over a finite field F_q with characteristic p not equal to 2 or 3 and j-invariant $j(E) \neq 0, 1728$. l are prime numbers such that $\prod l > 4\sqrt{q}$ as in the basic Schoof's algorithm.

Recall the characteristic equation of the Frobenius map φ modulo a prime l,

$$\mathcal{F}_l = u^2 - t_l u + q_l.$$

If the discriminant $\Delta_t = t^2 - 4q$ is a quadratic residue in $\mathbb{F}_l$, we say l is an Elkies prime; otherwise, an Atkin prime. By the proposition we will see below, whether l is an Elkies or Atkin prime can be determined by the splitting type of $\Phi_l(x, j)$, where $\Phi_l(x, y)$ is the lth modular polynomial and $j = j(E)$ is the j-invariant of E. Recall that the case of Φ_3 was introduced in class. In general, all roots of $\Phi_l(x, j)$ are given by the j-invariants of all the $l + 1$ l-isogenies of E.

Proposition 1 (Atkin) *Let E be a non-supersingular elliptic curve over $\mathbb{F}_q$ with j-invariant $j \neq 0, 1728$. Let $\Phi_l(x, j) = h_1 h_2 \cdots h_s$ be the factorization of $\Phi_l(x, j) \in \mathbb{F}_q[x]$ as a product of irreducible polynomials. Then there are the following possibilities for the degrees of h_1, h_2, $\cdots$, h_s.*

(i) either 1 and l (in which case we set $r = l$) or 1,1,$\cdots$,1 (in which case we set $r = 1$) - in either situation l divides the discriminant $\Delta_t = t^2 - 4q$;

(ii) 1,1,r,r,$\cdots$,r - in this case Δ_t is a square mod l, r divides $l - 1$ and φ acts on $E[l]$ as a matrix

$$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$$

with $\lambda, \mu \in \mathbb{F}_l^*$;

(iii) r, r, $\cdots$, r for some $r > 1$ - in this case $t^2 - 4q$ is not a square modulo l, r divides $l + 1$ and φ acts on $E[l]$ as a 2×2 matrix whose characteristic polynomial is $\mathcal{F}_l$, which is irreducible over $\mathbb{F}_l$.

In all three cases r is the order of φ in $PGL_2(\mathbb{F}_l)$ and the trace t of φ satisfies the equation

$$t^2 = q(\zeta + 2 + \zeta^{-1})$$

over $\mathbb{F}_l$, for some primitive rth root of unity $\zeta \in \overline{\mathbb{F}_l}$.

By noting that the roots of $x^q - x$ are exactly the elements of $\mathbb{F}_q$, the degree of

$$\gcd(x^q - x, \Phi_l(x, j))$$

is 0, 1, 2 or $l + 1$, where degree 1, 2 and $l + 1$ correspond to an Elkies prime(where 1 and $l + 1$ correspond to the double root case which we will mention later) and degree 0 corresponds to an Atkin Prime. Therefore we don't need to have the factorization of the modular polynomial to determine the type of the prime l. However, the coefficients of the modular polynomials $\Phi_l(x, y)$ can grow extremely large (although they are used modulo prime p, their computation is done over $\mathbb{C}$), making the computation really hard(maybe infeasible for large p). This difficulty can be resolved by using variants of the modular polynomials, e.g., Müller's modular polynomials, which have the same splitting type as the corresponding ordinary modular polynomials, but whose coefficients are smaller.

Elkies Primes. If l is an Elkies prime, then the discriminant Δ_t is a square in $\mathbb{F}_q$ and the characteristic polynomial $\mathcal{F}_l$ of φ has two roots, say λ and μ, which are eigenvalues of the Frobenius map modulo l. Assume for convenience that $\lambda \neq \mu$(the case of double root, i.e.,$\lambda = \mu$,

corresponds to $t \equiv \pm 2\sqrt{q} (\text{mod } l)$). The set of l-torsion points $E[l]$ has two of its $l+1$ subgroups, say C_1 and C_2, that are stable under the action of φ, i.e., $\varphi(P_1) = \lambda P_1$ for all $P_1 \in C_1$ and $\varphi(P_2) = \mu P_2$ for all $P_2 \in C_2$. Therefor we have

$$\mathcal{F}_l(u) = u^2 - t_l u + q_l = (u - \lambda)(u - \mu)$$

over $\mathbb{F}_l$. If we can determine one of the roots, say λ, then

$$t \equiv \lambda + \frac{q}{\lambda} (\text{mod } l).$$

To find such an eigenvalue we could test for a point $P = (x, y) \in C_i$ and a value $\lambda \in \{1, 2, \cdots, l-1\}$ such that

$$(x^q, y^q) = [\lambda](x, y)$$

Note that we don't need to try all values of λ by Proposition 1. Let C be one of the C_1 and C_2 above and set

$$F_l(x) = \prod_{\pm P_i \in C \setminus \{\mathcal{O}\}} (x - (P_i)_X)$$

Then F_l is defined over $\mathbb{F}_q$, since C is stable under the action of φ. Note that F_l has degree $(l-1)/2$ and it is a factor of the lth division polynomial $\psi_l(x)$ as is used in the basic Schoof's algorithm. There is a complicated result on how to obtain such $F_l(x)$ efficiently and this is beyond the scope of this presentation. The idea is: with the help of one root of the modular equation we find an elliptic curve, say E_1, isogenous to E such that the kernel of the isogeny is C and such that sufficient information about C is obtained to give all coefficients of the polynomial F_l. And we can get the desired F_l by working with the Müller modular polynomials. When F_l is computed, we set

$$h(x) := ((x^p - x)\psi_\lambda^2(x, y) + \psi_{\lambda-1}(x, y)\psi_{\lambda+1}(x, y)) (\text{mod } F_l(x), y^2 - x^3 - Ax - B)$$

This is a function of x only, due to the fact that ψ_n is a polynomial in $\mathbb{Z}[x, y^2, A, B]$ when n is odd, and a polynomial in $2y\mathbb{Z}[x, y^2, A, B]$ when n is even. Then we start computing $H(x) = \gcd(h(x), F_l(x))$. If $H(x)$=1 then λ is not an eigenvalue and if $H(x) \neq 1$ then the y-coordinates are checked.

Atkin Primes. If l is an Atkin prime, then the characteristic polynomial of φ has two roots $\lambda, \mu \in \mathbb{F}_{l^2} - \mathbb{F}_l$. The element $\lambda/\mu = \gamma_r$ is then an element of order exactly r in $\mathbb{F}_{l^2}$ and it comes from a set of order $\phi(r)$ by Proposition 1. All elements of order r in $\mathbb{F}_{l^2}$ can be determined by first finding a generator g for $\mathbb{F}_{l^2}^*$, and then computing $\gamma_r = g^{i(l^2-1)/r}$, where $i \in \{1, \cdots, r-1\}$ is coprime to r. Enumerating all possibilities for γ_r we obtain a set T of possible values for t (mod l) by the following equations

$$t = \lambda + \mu (\text{mod } l), q = \lambda\mu (\text{mod } l), \gamma_r = \lambda/\mu.$$

Computation of the trace t. There are suggestions that we only use the Elkies primes; but then we have to deal with higher degree modular polynomials. So the best compromise is to use the Elkies primes and the Atkin primes giving small sets T. Then the exact value of t can be found using the CRT, BSGS and a probabilistic random point checking method. However, we will skip the details here.

We summarize the SEA algorithm as follows:
INPUT: An elliptic curve E over a finite field $\mathbb{F}_q$.
OUTPUT: The order of $E(\mathbb{F}_q)$.

1. Set $M = 1$, $l = 2$, $A = \{\}$ and $El = \{\}$.
2. While $M < 4\sqrt{q}$ do:
3. Decide whether l is an Atkin or Elkies prime by finding the splitting type of the modular polynomial.
4. if l is an Elkies prime, do
5. Determine the polynomial $F_l(x)$.
6. Find an eigenvalue, λ, mod l.
7. $t = \lambda + q/\lambda (\text{mod } l)$.
8. $El = El \cup \{(t, l)\}$.
9. Else do:
10. Determine a (small) set T such that t (mod l)$\in T$.
11. $A = A \cup \{(T, l)\}$.
12. $M = M \times l$.
13. $l =$nextprime(l)
14. Recover t using the sets A and El, the CRT and BSGS.
15. Return $q + 1 - t$.

The bottleneck of this algorithm is the computation of x^q and y^q modulo $F_l(x)$ and the curve equation for E, which takes $O(l^{3+\epsilon})$ with fast arithmetic. The complexity of constructing $F_l(x)$ is bounded by $O(l^{2+\epsilon})$ using fast arithmetic. Since the number of Elkies primes processed will be $O(\log q)$, the overall complexity of the Elkies portion of the algorithm is $O(\log^{4+\epsilon})$ for fast arithmetic. It is clear that the the Atkin portion of the algorithm is of exponential asymptotic complexity. However we can still take advantage from them by choosing carefully a subset of Atkin primes to process.

SEA is the preferred point counting algorithm for $\mathbb{F}_p$, large p.