Schoof-Elkies-Atkin Algorithm

Rong-Jaye Chen

Department of Computer Science, National Chiao Tung University

ECC 2008
Outline

1. Backgrounds

2. Basic Schoof’s Algorithm

3. Schoof-Elkies-Atkin Algorithm
   - Elkies primes and Atkin primes
   - Modular Polynomial
   - Elkies primes
   - Compute $F_1(x)$
   - Atkin primes
   - Schoof-Elkies-Atkin Procedure
   - Complexity Analysis
The $l$-torsion group, denoted by $E[l]$.

$$E[l] = \{ P \in E(F_q) | lP = \infty \}$$

If $\gcd(l, p) = 1$,

$$E[l] \cong \mathbb{Z}_l \oplus \mathbb{Z}_l$$

We can see it as a two dimension vector space, with basis $\{P_1, P_2\}$.

It has $l + 1$ subgroups of order $l$.

$$\langle P_1 \rangle, \langle P_2 + kP_1 \rangle, k = 0, 1, .., l - 1$$
Frobenius endomorphism

- The *Frobenius endomorphism* (map) $\phi_q$

  $$\phi_q(x, y) = (x^q, y^q)$$

- For all $a \in \mathbb{F}_q$, $a^q = a$.

  $$\phi(P) = P, \quad \forall P \in E(\mathbb{F}_q)$$

- $\phi_q^2 - t\phi_q + q = 0$ is a *zero* map of $E$

- The characteristic polynomial of $\phi_q$ is

  $$x^2 - tx + q = 0$$
Schoof’s Algorithm

**Theorem (Hasse’s Theorem)**

Let $E$ be an elliptic curve over finite field $F_q$

\[ |t| = |q + 1 - \#E(F_q)| \leq 2\sqrt{q} \]

- Pick the small primes $l \neq p(q = p^k)$, such that $\prod l > 4\sqrt{q}$
- Use Frobenius map to calculate on each $l$-torsion points to find each $t_l \equiv t \pmod{l}$
- Use CRT to compute the unique $t$ satisfying Hasse’s Theorem
Details of the steps of Basic Schoof’s Algorithm

- Consider the \( l \)-torsion group \( E[l] \), and find the \( t_l \) where

\[
(x^{q^2}, y^{q^2}) + q_l(x, y) = t_l(x^q, y^q)
\]

- For \( l = 2 \), use the following rules:
  - For odd characteristic, \( t \equiv \#E(\mathbb{F}_q) \pmod{2} \).

\[
t \pmod{2} \equiv \begin{cases} 
1, & \gcd(X^3 + aX + b, X^q - X) = 1 \\
0, & \text{otherwise}
\end{cases}
\]

  - For characteristic 2, since the curve is non-supersingular, \( t \equiv 1 \pmod{2} \)

- All the \( x \)-coordinate of the points in \( E[l] \) are roots of \( f_l \), where

\[
f_l = \begin{cases} 
\psi_m, & m \text{ odd}, \\
\psi_m/\psi_2, & m \text{ even}.
\end{cases}
\]

So, we compute the \( (x^{q^2}, y^{q^2}) + q_l(x, y) \), and \( t_l(x^q, y^q) \) modulus \( f_l \), where \( \deg(f_l) = O(l^2) \), and the equation of \( E \)
Complexity Analysis of Basic Schoof’s Algorithm

- **INPUT**: An elliptic curve $E$ over a finite field $\mathbb{F}_q$.
- **OUTPUT**: The order of $E(\mathbb{F}_q)$

1. $M \leftarrow 2$, $l \leftarrow 3$, $S \leftarrow (t \pmod{2}, 2)$
2. while $M < 4\sqrt{q}$ do:
   \[ \Leftarrow O(\log q) \]
   3. For $\tau = 0, \ldots, \frac{l-1}{2}$ do:
   \[ \Leftarrow O(\log^7 q) \]
   4. Using the formula to find $\tau$.
5. $S \leftarrow S \cup \{ (\tau, l) \}$.
6. $M \leftarrow M \times l$.
7. $l \leftarrow \text{next prime}(l)$.
8. Recover $t$ using the set $S$ and the CRT.
9. Return $q + 1 - t$
Elkies primes and Atkin primes

- The Frobenius map $\phi_q$ induces a matrix $(\phi_q)_l$ that describes the action of $\phi_q$ on $E[l]$
- The characteristic polynomial of the Frobenius map modulo $l$

$$\mathcal{F}_l(u) = u^2 - t_l x + q_l = 0$$

is the characteristic polynomial of $(\phi_q)_l$
- The discriminant of $\mathcal{F}_l(u)$

$$\Delta_l = t_l^2 - 4q_l$$

- Legendre symbol \( \left( \frac{\Delta_l}{l} \right) = \begin{cases} 1 & , l \text{ is an Elkies prime} \\ -1 & , l \text{ is an Atkin prime} \end{cases} \)
- But, $t_l$ is unknown. (Using Modular Polynomial)
Modular Polynomial - (1)

\[ q(\tau) = e^{2\pi i \tau}, \quad v = \frac{l - 1}{\gcd(12, l - 1)} \in \mathbb{N} \]

\[ \eta(\tau) = q^{\frac{1}{24}} \left( 1 + \sum_{n=1}^{\infty} \left( q^{\frac{n(3n-1)}{2}} + q^{\frac{n(3n+1)}{2}} \right) \right) \]

\[ \Delta(\tau) = (\eta(\tau))^{24}, \quad h(\tau) = \frac{\Delta(2\tau)}{\Delta(\tau)} \]

\[ j(\tau) = 16777216h(\tau)^2 + 196608h(\tau) + 768 + \frac{1}{h(\tau)} \]
Modular Polynomial - (2)

- Matrix acts on $\tau$
  \[
  \alpha = \begin{pmatrix}
  a & b \\
  c & d
  \end{pmatrix}, \det(\alpha) > 0, \quad \text{define } j(\alpha(\tau)) = j\left(\frac{a\tau + b}{c\tau + d}\right)
  \]

- \[
  S_i^* = \left\{ \begin{pmatrix}
  a & b \\
  0 & d
  \end{pmatrix} \middle| a, b, d \in \mathbb{Z}, ad = l, \gcd(a, b, d) = 1, 0 \leq b < d \right\}
  \]

- Definition of the modular polynomial
  \[
  \Phi_l(x, j(\tau)) = \prod_{\alpha \in S_i^*} (x - j(\alpha(\tau)))
  \]
Since $ad = l$ is a prime,

$a = 1, d = l$ : $b = \{0, 1, \ldots, l - 1\}$, \hspace{1cm} $j(\alpha(\tau)) = j\left(\frac{\tau + k}{l}\right), k \in \{0, \ldots, l - 1\}$

$a = l, d = 1$ : $b = 0$, \hspace{1cm} $j(\alpha(\tau)) = j(l \tau)$

So,

$$\Phi_l = (x - j(l \tau)) \prod_{k=0}^{l-1} (x - j\left(\frac{\tau + k}{l}\right))$$

Let $y = j(\tau)$, then $\Phi_n(x, y) \in \mathbb{Z}[x, y]$

There is an isogeny of degree $l$, from $E_1$ to $E_2$, if and only if\n
$$\Phi_l(j(E_1), j(E_2)) = 0$$
Consider the modular polynomial $\Phi_l(x, j(E))$ as $\Phi_l(x)$.

We can factor the $\Phi_l(x)$ over $F_q$

$$\Phi_l(x) = f_1 f_2 \ldots f_s$$

all $f_i$’s are irreducible.

Case 1. If the degree of $f_i$’s are 1 and $l$, or 1,1,...,1

$$t^2_l - 4ql \equiv 0 \pmod{l}$$

Case 2. If the degree of $f_i$’s are 1,1,$r$,$r$,...,$r$

$$\left( \frac{t^2_l - 4ql}{l} \right) = 1$$

and $r \mid l - 1$, moreover, $\phi_q$ acts on $E[l]$ as a matrix

$$\left( \begin{array}{cc} \lambda & 0 \\ 0 & \mu \end{array} \right), \quad \lambda, \mu \in F^*_q$$
Case 3. If the degree of $f_i$’s are $r, r, \ldots, r$

$$\left( \frac{t_i^2 - 4ql}{l} \right) = -1$$

and $r \mid l + 1$, moreover, $\phi_q$ acts on $E[l]$ as a $2 \times 2$ matrix whose characteristic polynomial is $\mathbb{F}_l$, which is irreducible over $F_q$, and the $\frac{\lambda}{\mu}$ is an element of order exactly $r$ in $\mathbb{F}_{l^2}$

In all three cases $r$ is the order of $\phi$ and the tract $t$ of $\phi$ satisfies

$$t^2 = q(\xi + 2 + \xi^{-1}) \text{over} \mathbb{F}_l$$

, for some primitive $r$-th root of unity $\xi \in \overline{\mathbb{F}_l}$

So, we can use each $\Phi_l(x)$ to determine $l$ is either Elkies prime or Atkin prime
Modular polynomial - (6)

\[ s = \frac{12}{\gcd(l - 1, 12)}, \quad v = \frac{l - 1}{\gcd(l - 1, 12)} \]

\[ f(\tau) = \left( \frac{\eta(\tau)}{\eta(l\tau)} \right)^{2s} \]

There exist coefficients \( a_{r,k} \in \mathbb{Z} \) such that

\[ \sum_{r=0}^{l-1} \sum_{k=0}^{v} a_{r,k} f(\tau)^r j(l\tau)^k = 0 \]

Define the polynomial

\[ G_l(x,y) = \sum_{r=0}^{l-1} \sum_{k=0}^{v} a_{r,k} x^r y^k \in \mathbb{Z}[x,y] \]

\( G_l(x, j(E)) \) has the same **splitting type** as \( \Phi_l(x, j(E)) \)
Elkies primes

1. The characteristic polynomial of \((\phi_q)_l\) has two roots \(\lambda, \mu\).

- If \(\lambda = \mu\), test \(\phi(P) = \omega_0 P\), where \(\omega_0^2 \equiv q \pmod{l}\), then

\[ t_l \equiv 2\omega_0 \pmod{l} \]

2. If \(\lambda \neq \mu\), \(E[l]\) has two subgroups \(C_1, C_2\) that are stable under \(\phi_q\).

- Find the \(F_l(x)\) whose roots are the \(x\)-coordinate of the subgroup \(C\).
  (one of \(C_1\) or \(C_2\))
- \(\text{deg}(F_l) = \frac{l-1}{2}\)
- Find \(\lambda\) such that

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

- Compute \((x^q, y^q)\) and \(\lambda(x, y)\) modulus \(F_l\), and the equation of \(E\)
- Here, the computation complexity is down to \(O(\log^4 q)\) corresponding to \(O(\log^6 q)\) part of original Schoof’s Algorithm.
Elkies prime procedure

- Find $\lambda$ such that $(x^q, y^q) = \lambda (x, y)$

1. For $\lambda$, compute

$$h(x, y) = ((x^q - x)\psi_\lambda^2(x, y) + \psi_{\lambda-1}(x, y)\psi_{\lambda+1}(x, y))$$

$$(\mod F_l(x), y^2 - x^3 - ax - b) = a(x) + yb(x)$$

2. If $\gcd(a(x), b(x), F_l(x)) \neq 1$, check the $y$-coordinate to determine the $\lambda$

3. Finally, we get

$$t \equiv \lambda + \frac{q}{\lambda} \pmod l$$
Compute $\tilde{a}, \tilde{b},$ and $p_1$ - (1)

- First, compute a root, $g$, of the polynomial $G_l(x, j(E))$.
- Set
  $$E_4 = -\frac{a}{3}, \quad E_6 = -\frac{b}{2}, \quad \Delta = \frac{E_4^3 - E_6^2}{1728}$$
- Compute $j = j(E)$
  $$D_g = g \left( \frac{\partial}{\partial x} G_l(x, y) \right) (g, j), \quad D_j = j \left( \frac{\partial}{\partial y} G_l(x, y) \right) (g, j)$$
- The coefficient of the isogenous curve will be given by $\sim a, \tilde{b}$ and have the associated invariants $E_4^{(l)}$, $E_6^{(l)}$, $\Delta^{(l)}$
  $$\Delta^{(l)} = l^{-12} g^{\gcd(12, l-1)}$$
Compute $\tilde{a}$, $\tilde{b}$, and $p_1$ - (2)

- If $D_j = 0$,

$$\overline{E_4^{(l)}} = l^{-2}E_4, \quad \tilde{a} = -3l\overline{E_4^{(l)}}, \quad j^{(l)} = \frac{\left(\overline{E_4^{(l)}}\right)^3}{\Delta^{(l)}}$$

$$\tilde{b} = \pm 2l^6 \sqrt{(j^{(l)} - 1728)\Delta^{(l)}}, \quad p_1 = 0$$

- Now assume $D_j \neq 0$

$$s = \frac{12}{\gcd(12, l - 1)}, \quad \overline{E_2^*} = \frac{-12\overline{E_6}D_j}{s\overline{E_4D_g}}, \quad g' = -\frac{s}{12}\overline{E_2^*}g$$

$$j' = -\overline{E_4^2\overline{E_6}\Delta^{-1}}, \quad \overline{E_0} = \overline{E_6(\overline{E_4E_2^*})^{-1}}$$
Compute $\tilde{a}$, $\tilde{b}$, and $p_1$ - (3)

Then, we need to compute the quantities

$$D'_g = g' \left( \frac{\partial}{\partial x} G_l(x, y) \right) (g, j) + g \left[ g' \left( \frac{\partial^2}{\partial x^2} G_l(x, y) \right) (g, j) + j' \left( \frac{\partial^2}{\partial x \partial y} G_l(x, y) \right) (g, j) \right]$$

$$D'_j = j' \left( \frac{\partial}{\partial y} G_l(x, y) \right) (g, j) + j \left[ j' \left( \frac{\partial^2}{\partial y^2} G_l(x, y) \right) (g, j) + g' \left( \frac{\partial^2}{\partial y \partial x} G_l(x, y) \right) (g, j) \right]$$

Now, we can determine

$$\overline{E_0'} = \frac{1}{D_j} \left( \frac{-s}{12} D'_g - \overline{E_0} D'_j \right)$$
Compute $\tilde{a}$, $\tilde{b}$, and $p_1$ - (4)

- So, we have

$$E_4^{(l)} = \frac{1}{l^2} \left( \frac{E_4 - E_2^*}{E_0} \left[ 12 \frac{E_0'}{E_0} + 6 \frac{E_4^2}{E_6} - 4 \frac{E_6}{E_4} \right] + E_2^* \right)$$

- The $j$-invariant of the isogenous curve

$$j^{(l)} = \frac{E_4^{(l)^3}}{\Delta^{(l)}}$$

- Setting $f = l^s g^{-1}$, $f' = E_2^* f / \gcd(12, l - 1)$

$$D_g^* = \left( \frac{\partial}{\partial x} G_l(x, y) \right) (f, j^{(l)}), \quad D_j^* = \left( \frac{\partial}{\partial y} G_l(x, y) \right) (f, j^{(l)})$$
Compute $\tilde{a}$, $\tilde{b}$, and $p_1$ - (5)

- Finally, we compute
  
  \[
  j^{(l)'} = -\frac{f'D^*_g}{lD^*_j}, \quad E_6^{(l)} = -\frac{E_4^{(l)}j^{(l)'}}{j^{(l)}}
  \]

- Thus, we have three desired quantities as
  
  \[
  \tilde{a} = -3lE_4^{(l)}, \quad \tilde{b} = -2l^6E_6^{(l)}, \quad p_1 = -\frac{lE_2^*}{2}
  \]
Compute $F_l(x)$ - (1)

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

where coefficients $c_k$ are obtained from the following

$$c_1 = -\frac{a}{5}, \quad c_2 = -\frac{b}{7}, \quad c_k = \frac{3}{(k-2)(2k+3)} \sum_{j=1}^{k-2} c_j c_{k-1-j}$$

The $\tilde{\varrho}(z)$ is the similar as above. We obtain

$$\tilde{c} = -\frac{1}{5} \frac{\tilde{a}}{l^4}, \quad \tilde{\varrho} = -\frac{1}{7} \frac{\tilde{b}}{l^6}, \quad \tilde{\kappa} = \frac{3}{(k-2)(2k+3)} \sum_{j=1}^{k-2} \tilde{\varrho} \tilde{\kappa}^{-1-j}$$
Compute $F_l(x)$ - (2)

- $F_l(x)$ satisfies the equation

$$z^{l-1} F_l(\varphi(z)) = \exp \left( -\frac{1}{2} p_1 z^2 - \sum_{k=1}^{\infty} \frac{\tilde{\xi} - lc_k}{(2k+1)(2k+2)} z^{2k+2} \right)$$

- Let $\omega = z^2$,

$$A(\omega) = \exp \left( -\frac{1}{2} p_1 \omega - \sum_{k=1}^{\infty} \frac{\tilde{\xi} - lc_k}{(2k+1)(2k+2)} \omega^{k+1} \right)$$

- Let $C(\omega) = \varphi(z) - \omega^{-1} = \sum_{k=1}^{\infty} c_k \omega^k$, and denote the coefficient of the $\omega^i$ of $B(\omega)$ by $[B(\omega)]_i$.

- Compare the coefficients of $\omega^i$ to find $F_l(x)$
Compute $F_l(x)$ - (3)

- $F_{l,d} = 1$, and

$$F_{l,d-i} = [A(\omega)]_i - \sum_{k=1}^{i} \left( \sum_{j=0}^{k} \binom{d-i+k}{k-j} [C(\omega)^{k-j}]_j \right) F_{l,d-i+k}$$

- Expand $A(\omega)$ by using Taylor Series

- Compute $C(\omega)^i$ and obtain the coefficients for $[C(\omega)^i]_j$ from $j = 0$ to $d - i$
Atkin primes - (1)

- Since

\[ t^2 = q(\xi + 2 + \xi^{-1}) \text{over } \mathbb{F}_l \]

, each pair \((\xi, \xi^{-1})\) determines one value of \(t^2\), or at most two values of \(t\).
- The number of the possible values of \(t_l\) is \(\phi_{Eul}(r)\), and \(r \leq l + 1\)
- \(\frac{\lambda}{\mu}\) is an element of order exactly \(r\) in \(\mathbb{F}_{l^2}\)

1. Find \(r\), the smallest \(d\) such that \(gcd(x^{q^d} - x, \Phi(x)) \neq 1\)
2. Find a generator \(g\) of \(\mathbb{F}_{l^2}^*\), and \(\gamma_i = \frac{\lambda}{\mu} = g\left(\frac{i(l^2-1)}{r}\right)\), where \(gcd(i, r) = 1\).
3. Choose a QNR \(d\), and write \(\gamma_i = g_1 + \sqrt{d}g_2\)
4. \(x_1^2 = \frac{q(g_1+1)}{2}\)
5. \(t \equiv 2x_1 \pmod{l}\)
Atkin primes - (2)

- Suppose $\lambda = x_1 + \sqrt{d}x_2$, then $\mu = x_1 - \sqrt{d}x_2$

\[
g_1 + \sqrt{d}g_2 = \gamma_i = \frac{\lambda}{\mu} = \frac{\lambda^2}{\mu\lambda}
\]

\[
\frac{1}{q} \left( x_1^2 + dx_2^2 + 2x_1x_2\sqrt{d} \right)
\]

- Hence,

\[
qg_1 \equiv x_1^2 + dx_2^2 \pmod{l}
\]

\[
qg_2 \equiv 2x_1x_2 \pmod{l}
\]

\[
q = x_1^2 - dx_2^2 \pmod{l}
\]

- $x_1^2 = \frac{q(g_1+1)}{2}$
Schoof-Elkies-Atkin Algorithm

- INPUT: An elliptic curve $E$ over finite field $\mathbb{F}_q$
- OUTPUT: The order of $E(\mathbb{F}_q)$

1. $M \leftarrow 1$, $l \leftarrow 2$, $A \leftarrow \{\}$, and $E \leftarrow \{\}$
2. while $M < 4\sqrt{q}$ do:
   - Decide whether $l$ is an Atkin or Elkies prime.
   - If $l$ is an Elkies prime, do: \( \leftarrow O(\log^4 q) \)
      - Find an eigenvalue, $\lambda$, and $t \leftarrow \lambda + \frac{q}{\lambda} \pmod{l}$
      - $E \leftarrow E \cup \{(t, l)\}$
   - Else do:
      - Determine a set $T$ for all possibilities of trace
      - $A \leftarrow A \cup \{(T, l)\}$
      - $M \leftarrow M \times l$, $l \leftarrow \text{next prime}(l)$.
5. Recover $t$ using the sets $A$ and $E$, the CRT and BSGS.
6. Return $q + 1 - t$
Combine Elkies and Atkin primes - (1)

- Combine Elkies via CRT to determine
  \[ t \equiv t_3 \pmod{m_3} \]

- Divide Atkin primes to two sets such that each set gives roughly the same numbers.
  \[ t \equiv t_1 \pmod{m_1} \]
  \[ t \equiv t_2 \pmod{m_2} \]
  Hence, \( m_1 m_2 m_3 > 4\sqrt{q} \).

- Now let \( M_1 \equiv \frac{1}{m_2 m_3} \pmod{m_1}, M_2 \equiv \frac{1}{m_1 m_3} \pmod{m_2}, M_3 \equiv \frac{1}{m_1 m_2} \pmod{m_3} \)
Combine Elkies and Atkin primes - (2)

- From *Chinese Remainder Theorem*, we obtain

\[ m_1 m_2 M_3 + m_1 m_3 M_2 + m_2 m_3 M_1 \equiv 1 \pmod{m_1 m_2 m_3} \]

\[ t \equiv t_1 m_2 m_3 M_1 + t_2 m_1 m_3 M_2 + t_3 m_1 m_2 M_3 \pmod{m_1 m_2 m_3} \]

- Let \( r_1 \equiv \frac{t_1 - t_3}{m_2 m_3} (\text{mod } m_1) \), \( r_2 \equiv \frac{t_2 - t_3}{m_1 m_3} (\text{mod } m_2) \). Then,

\[ t \equiv t_1 m_2 m_3 M_1 + t_2 m_1 m_3 M_2 + t_3 (1 - m_1 m_3 M_2 - m_2 m_3 M_1) \]

\[ \equiv t_3 + m_3 (m_1 r_2 + m_2 r_1) \pmod{m_1 m_2 m_3} \]

- Write \( t = t_3 + m_3 (m_1 r_2 + m_2 r_1) \)

\[ [q + 1]P = [t]P = [t_3 + m_3 (m_1 r_2 + m_2 r_1)]P \]

\[ [q + 1 - t_3]P - [r_1 m_2 m_3]P = [r_2 m_1 m_3]P \]
Now, we process baby steps. For every possible \( t_1 \pmod{m_1} \), take \( r_1, |r_1| < \left\lfloor \frac{m_1}{2} \right\rfloor \)

\[
Q_{r_1} = [q + 1 - t_3]P - [r_1 m_2 m_3]P
\]

Giant step. For every possible \( t_2 \pmod{m_2} \), take two \( r_2 \)'s

\[
R_{t_2} = [r_2 m_1 m_3]P
\]

If \( Q_{t_1} = R_{t_2} \), then the corresponding \( r_1, r_2 \) have to satisfy \( |t| < 2\sqrt{q} \)

Each matching \((r_1, r_2)\) pair determines a possible \( t \), this group order can then checked by random curve points.
Complexity Analysis of Schoof-Elkies-Atkin Algorithm

- If an Elkies prime occurs, the complexity is down.
- The algorithm of Atkin primes transpire that this is actually of exponential asymptotic complexity.
- So, an idea is to drop Atkin primes.
- However, this implies having to deal with modular polynomials of higher degree, which in itself a problem.
- Best practical compromise is obtained by judicious use of the Atkin procedure, where only the ‘best’ Atkin primes are retained, and the overall size of the set of potential traces is bounded.