An Improvement of Schoof's Algorithm

Federico Pintore

Università di Trento

Trento, 22 Maggio 2013

Elliptic curves

Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$ by the Weierstrass equation:

$$y^2 = x^3 + Ax + B \qquad \textit{with} \qquad A, B \in \mathbb{F}_q$$

If $\mathbb{F}$ is an extension of $\mathbb{F}_q$, we put:

$$E(\mathbb{F}) = \{(x, y) \in \mathbb{A}^2(\mathbb{F}) \mid y^2 = x^3 + Ax + B\} \cup \{\infty\}$$

Group Structure

It is possible to define a group operation over $E(\mathbb{F})$ with the point at infinity as the zero element.

Given two points $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, their sum $P_3 = (x_3, y_3)$ is:

$$P_3 := \begin{cases} (m^2 - x_1 - x_2, m(x_1 - x_3) - y_1) & \text{if } x_1 \neq x_2 \\ \infty & \text{if } x_1 = x_2 \text{ and } y_1 \neq y_2 \\ (m^2 - 2x_1, m(x_1 - x_3) - y_1) & \text{if } P_1 = P_2 \text{ and } y_1 \neq 0 \\ \infty & \text{if } P_1 = P_2 \text{ and } y_1 = 0 \end{cases}$$

where m is the shape of the line through P_1 end P_2.

Point counting

Hasse Theorem

$$\#E(\mathbb{F}_q) = q + 1 + a \qquad | a | \leq 2\sqrt{q}$$

Theorem

Given the Frobenius Endomorphism:

$$\begin{array}{rccc} \phi_q : & E(\overline{\mathbb{F}_q}) & \rightarrow & E(\overline{\mathbb{F}_q}) \\ & (x, y) & \mapsto & (x^q, y^q) \end{array}$$

we have:

$$(\phi_q)^2 - a\phi_q + q = 0$$

Schoof's Algorithm

Consider a set of primes $S = \{2, 3, \ldots, L\}$ such that

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

If we know the congruences

$$a_l \equiv a \mod l \qquad (l \in S)$$

by the Chinese Remainder Theorem we can find a.

Schoof's Algorithm

Theorem

Exists a family of polynomials $\{f_n(x) \in \mathbb{F}_q[x]\}_{n\in\mathbb{N}}$ *such that:*

$$nP = \begin{cases} \left(\frac{x(x^3+Ax+B)f_n^2 - f_{n+1}f_{n-1}}{(x^3+Ax+B)f_n^2}, \frac{f_{n+2}f_{n-1}^2 - f_{n-2}f_{n+1}^2}{4y(x^3+Ax+b)f_n^3}\right) & n \text{ even} \\ \left(\frac{xf_n^2 - (x^3+Ax+B)f_{n+1}f_{n-1}}{f_n^2}, \frac{(x^3+Ax+B)[f_{n+2}f_{n-1}^2 - f_{n-2}]}{4yf_n^3}\right) & n \text{ odd} \end{cases}$$

Furthermore

$$nP = n(x,y) = \infty \iff f_n(x) = 0$$

How to proceed

Fixed a prime $l \in S$ we have:

$$\phi_q^2(P) + q(P) = a_l(\phi_q(P)) \qquad \forall P \in E[l]$$

where $a_l \equiv a$ modulo l.

Case 1

If $\phi_q^2(P) \neq \pm qP$ for some non zero $P \in E[l]$, for these kind of points the sum (x', y') of $\phi_q^2(P)$ and qP is such that:

$$x' - x_j = \frac{r_1(x)}{r_2(x)} \qquad j \in \{-2\sqrt{q}, \ldots, 2\sqrt{q}\} \in \mathbb{Z}$$

We find j such that $x' - x_j \equiv 0$ modulo $f_l(x)$.

Case 2

If $\phi_q^2(P) = qP$ for all non zero $P \in E[l]$, exists an integer w such that

$$w^2 \equiv q \qquad \textit{modulo } l$$

Then we have $a \equiv -2w$ or $a \equiv 2w$ modulo l.

Case 3

If exists a non zero point $P = (x, y) \in E[l]$ such that

$$\phi_q^2(P) = -q_l P$$

then $a \equiv 0$ modulo l.

Computational Complexity

The Schoof's Algorithm has a $O((log(q))^9)$ deterministic computational complexity.

Atkin - Elkies

Atkin and Elkies sought to improve the efficiency by first analyzing the roots of the restricted characteristic polynomial of the Frobenius endomorphism:

$$\chi_l(T) = T^2 - aT + q \quad \in \mathbb{Z}_l[T]$$

Definition

A prime $l \in \mathbb{Z}$ is an Elkies prime if $a^2 - 4q$ is a square modulo l; is an Atkin prime otherwise.

Atkin and Elkies Primes

Since a is unknown, one has to use indirect techniques to determine if l is an Atkin or a Elkies prime.

The splitting type of the l-th modular polynomial $\Phi_l(x, j)$ over $\mathbb{Z}_l$ (j is the j-invariant of E) determine if $a^2 - 4q$ is a square in $\mathbb{Z}_l$ or not.

Elkies Primes

Since $E[l] \simeq \mathbb{Z}_l \oplus \mathbb{Z}_l$, it is a bidimensional $\mathbb{Z}_l$ vector space.
We have:

$$(\phi_q)_l = \begin{pmatrix} s & t \\ u & v \end{pmatrix}$$

with $tr((\phi_q)_l) \equiv a$ and $det((\phi_q)_l)) \equiv q$ modulo l.

Remark

$\chi_l(T)$ *is the characteristic polynomial of* $(\phi_q)_l$.

If $l \in S$ is an Elkies Primes, χ_l has two roots in $\mathbb{Z}_l$: λ and μ.

Elkies Primes

- For $\mu = \lambda = 0$ we have $a \equiv \pm 2\sqrt{q}$ modulo l.
- For $\lambda \neq \mu$ we have $a \equiv \lambda + \frac{q}{\lambda}$ modulo l. Hence it suffices to find a non zero eigenvalue. Modular polynomials allow for a construction of a polynomial:

$$F_l(x) = \prod_{\pm P \in C} (x - (P)_x) \quad \Rightarrow \quad deg(F_l) = \frac{l-1}{2}$$

We can use $F_l(x)$ to compute λ such that:

$$(x^q, y^q) = \lambda(x, y) \qquad \forall \quad P \in C$$

Atkin Primes

If l is an Atkin Primes, we determine a set of possible values of a modulo l, of cardinality $\varphi(r)$ (with $r \leq l + 1$).

SEA Algorithm

Combining the procedures for Elkies and Atkin primes we find a.

The Elkies procedure has a polynomial complexity $O(l^6)$; the Atkin procedures has a exponential complexity with base $logq$.

Thanks for your attention