Counting points on elliptic curves over $\mathbf{F}_q$

Christiane Peters

DIAMANT-Summer School on
Elliptic and Hyperelliptic Curve Cryptography

September 17, 2008

Motivation

Given an elliptic curve E over a finite field $\mathbf{F}_q$.

Is the Discrete Logarithm Problem hard on E?

One criterion for hardness: Group order $\#E(\mathbf{F}_q)$ divisible by a large prime factor.

Short introductory notes

Schoof (1983): first polynomial-time algorithm for point counting.

late 80s/early 90s: Elkies and Atkin come up with speed-ups; leads to SEA (Schoof-Elkies-Atkin) algorithm.

mid-90s: lots of speed-ups, characteristic-2 algorithms

note: basic Schoof algorithm also applicable for hyperelliptic curves;
see Eric Schost's talk next week at ECC

1. Introduction

2. Schoof's algorithm

3. Computing in the torsion group

4. Improvements by Elkies

Elliptic curves over $\mathbf{F}_q$

Let $q = p^r$ for a prime $p \geq 5$.

Given $A, B \in \mathbf{F}_q$ with $4A^3 + 27B^2 \neq 0$. The zero set of

$$Y^2 = X^3 + AX + B$$

with the point $\mathcal{P}_\infty$ at infinity forms an elliptic curve.

Multiplication map

Let $m \in \mathbf{Z}$.

If $m > 0$:

$$[m](P) = \underbrace{P + \cdots + P}_{m \text{ times}},$$

If $m < 0$:

$$[m]\,(P) = [-m](-P).$$

$[0] : E \to E$, $[0](P) = \mathcal{P}_\infty$ is the constant map and $[1]$ the identity.

The m-torsion group contains all points of order divisible by m:

$$E[m] = \{P \in E \ : \ [m](P) = \mathcal{P}_\infty\}.$$

Frobenius Endomorphism

The map

$$\pi : E \longrightarrow E, \qquad (x, y) \mapsto (x^q, y^q)$$

is called Frobenius endomorphism.

We call a point (x, y) on E $\mathbf{F}_q$-rational if and only if

$$\pi(x, y) = (x, y).$$

We denote the rational points of E by $E(\mathbf{F}_q)$.

In particular

$$E(\mathbf{F}_q) = \ker([1] - \pi).$$

The number of rational points

Denote the number of rational points of E by $\#E(\mathbf{F}_q)$.

Trivial bound $\#E(\mathbf{F}_q) \leq 2q + 1$:
check for all $x \in \mathbf{F}_q$ whether $x^3 + Ax + B$ is a square in $\mathbf{F}_q$.

Recall Legendre symbol:

$$\left(\frac{a}{q}\right) = \begin{cases} -1 & \text{if } a \text{ is a non-square in } \mathbf{F}_q, \\ 0 & \text{if } a = 0 \text{ in } \mathbf{F}_q, \\ 1 & \text{if } a \text{ is a square in } \mathbf{F}_q. \end{cases}$$

We get

$$\#E(\mathbf{F}_q) = 1 + \sum_{x \in \mathbf{F}_q} \left(1 + \left(\frac{x^3 + Ax + B}{q}\right)\right).$$

Hasse's bound

The Frobenius endomorphism satisfies the following characteristic equation over $\mathbf{Z}$.

$$\pi^2 - t\ \pi + q = 0.$$

The integer t is called the trace of the Frobenius endomorphism. It satisfies

- $$\#E(\mathbf{F}_q) = 1 + q - t.$$
- $$|t| \leq 2\sqrt{q}.$$

1. Introduction

2. Schoof's algorithm

3. Computing in the torsion group

4. Improvements by Elkies

The idea

Hasse: $\#E(\mathbf{F}_q) = q + 1 - t$ with $|t| \leq 2\sqrt{q}$.

Let L be minimimal among all primes which satisfy

$$\prod_{\substack{\ell \text{ prime} \\ 2 \leq \ell \leq L}} \ell > 4\sqrt{q}.$$

Then the Chinese Remainder Theorem gives a unique t satisfying

$$t \mod \prod \ell \in [-2\sqrt{q},\ 2\sqrt{q}\,].$$

Prime number theorem: Need only $\mathcal{O}(\log q)$ primes ℓ.

Determine t mod ℓ

The restriction of the Frobenius endomorphism π to $E[\ell]$ satisfies

$$\pi^2 - t'\,\pi + q' = 0$$

where $t' = t \mod \ell$ and $q' = q \mod \ell$ are uniquely determined.

Let $P \in E[\ell]$.

1. Compute $R = \pi(P)$ and $Q = \pi^2(P) + [q']P$ in $E[\ell]$.
2. Check which $t' \in \{0, 1, \ldots, \ell - 1\}$ satisfies

$$Q = [t']R.$$

1. Introduction

2. Schoof's algorithm

3. Computing in the torsion group

4. Improvements by Elkies

Division polynomials

Torsion group $E[m] = \{P \in E \; : \; [m](P) = \mathcal{P}_\infty\}$.
If $\gcd(q, m) = 1$ we have

$$E[m] \cong (\mathbf{Z}/m\mathbf{Z}) \times (\mathbf{Z}/m\mathbf{Z}).$$

Let $m \geq 1$. The ℓth division polynomial $\psi_\ell \in \mathbf{F}_q[X, Y]$ vanishes in all ℓ-torsion points, i.e.,

for $P = (x, y)$ in $E(\bar{\mathbf{F}}_q)$, $P \notin E[2]$

$$\ell\, P = \mathcal{P}_\infty \;\Leftrightarrow\; \psi_\ell(x, y) = 0.$$

Recursion for $\psi_m(X, Y)$

Given $E : Y^2 = X^3 + AX + B$ over $\mathbf{F}_q$.

$$
\begin{aligned}
\psi_1 &= 1, \\
\psi_2 &= 2\,Y, \\
\psi_3 &= 3\,X^4 + 6A\,X^2 + 12B\,X - A^2, \\
\psi_4 &= 4\,Y(X^6 + 5A\,X^4 + 20B\,X^3 - 5A^2\,X^2 - 4AB\,X - 8B^2 - A^3)
\end{aligned}
$$

and

$$
\begin{aligned}
\psi_{2m+1} &= \psi_{m+2}\,\psi_m^3 - \psi_{m+1}^3\,\psi_{m-1} && \text{if } m \geq 2, \\
2Y\psi_{2m} &= \psi_m\,(\psi_{m+2}\,\psi_{m-1}^2 - \psi_{m-2}\,\psi_{m+1}^2) && \text{if } m \geq 3.
\end{aligned}
$$

Let $\gcd(m, q) = 1$.

- For odd m we have $\psi_m \in \mathbf{F}_q[X]$ with $\deg_X(\psi_m) = (m^2 - 1)/2$.
- For even m we have $\psi_m \in Y\,\mathbf{F}_q[X]$ with $\deg_X(\psi_m) = (m^2 - 4)/2$. (replace all powers of Y by the curve equation.)

Multiplication map revisited

Theorem

For $m \geq 3$

$$[m](x, y) = \left(x - \frac{\psi_{m-1}\, \psi_{m+1}}{\psi_m^2},\ \frac{\psi_{m+2}\, \psi_{m-1}^2 - \psi_{m-2}\, \psi_{m+1}^2}{4y\, \psi_m^3} \right).$$

Note: this shows that $[m]$ is a rational map.

Compute in a polynomial ring

Check equality $\pi^2(P) + [q](P) = [t](P)$ in $E[\ell]$ by looking at the polynomials corresponding to the x-coordinates of the point on the left and right side, resp.

We compute the trace t modulo ℓ in the ring

$$\mathcal{R}_\ell = \mathbf{F}_q[X,Y]/(Y^2 - X^3 - AX - B, \psi_\ell(X))$$

If we want to check if $p_1(X) = p_2(X)$ in $\mathcal{R}_\ell$ for two polynomials $p_1(X), p_2(X)$ we check whether

$$\gcd(p_1 - p_2, \psi_\ell) \neq 1.$$

Exercise Given a point (x, y) on a curve in Weierstrass form. You can write y^q as $h(x)y$ in $\mathcal{R}_\ell$. Determine $h(x) \in \mathbf{F}_q[x]$.

Example

Consider the curve $E : Y^2 = X^3 + 31X - 12$ in $\mathbf{F}_q$ with $q = 97$.

Determine the trace of π modulo $\ell = 5$.

The 5th division polynomial ψ_5 is given by $5\,x^{12} - 18\,x^{10} - x^9 - 25\,x^8 - 40\,x^7 - 39\,x^6 + 7\,x^5 + 3\,x^4 - 14\,x^3 + 26\,x^2 + 40\,x + 47$

Given a point $P = (x, y)$ in $E[5]$ we work in $\mathcal{R}_5 = \mathbf{F}_{97}[x, y]/(y^2 - x^3 - 31x + 12, \psi_5(x))$.

Computing in $\mathcal{R}_5$

$\pi(x,y) =$
$[47\,x^{11} + 11\,x^{10} - 16\,x^9 + 8\,x^8 + 44\,x^7 + 8\,x^6 + 10\,x^5 + 12\,x^4 -$
$40\,x^3 + 42\,x^2 + 11\,x + 26,$
$(6\,x^{11} + 45\,x^{10} + 34\,x^9 + 28\,x^8 - 11\,x^7 + 3\,x^6 - 3\,x^5 + 2\,x^4 - 39\,x^3 -$
$48\,x^2 - x - 9)y].$

$\pi^2(x,y) =$
$[-17\,x^{11} + 2\,x^{10} - 25\,x^9 - x^8 + 28\,x^7 + 31\,x^6 + 25\,x^5 - 32\,x^4 +$
$45\,x^3 + 26\,x^2 + 36\,x + 34,$
$(34\,x^{11} + 35\,x^{10} - 8\,x^9 - 11\,x^8 - 48\,x^7 + 34\,x^6 - 8\,x^5 - 37\,x^4 -$
$21\,x^3 + 40\,x^2 + 11\,x + 48)y].$

$[q \mod 5](x,y) = [2](x,y) =$
$[22\,x^{11} + 17\,x^{10} + 18\,x^9 + 40\,x^8 + 41\,x^7 - 13\,x^6 + 30\,x^5 + 11\,x^4 -$
$38\,x^3 + 7\,x^2 + 20\,x + 17,$
$(-11\,x^{10} - 17\,x^9 - 48\,x^8 - 12\,x^7 + 17\,x^6 + 44\,x^5 - 10\,x^4 + 8\,x^3 +$
$38\,x^2 + 25\,x + 24)y]$

Find t such that $\pi^2(x,y) + [2](x,y) = [t]\pi(x,y)$

$\pi^2(x,y) + [2]P =$
$[-14\,x^{14} + 15\,x^{13} - 20\,x^{12} - 43\,x^{11} - 10\,x^{10} - 27\,x^9 + 5\,x^7 + 11\,x^6 + 45\,x^5 - 17\,x^4 + 30\,x^3 - 2\,x^2 + 35\,x - 46,$
$(-11\,x^{14} - 35\,x^{13} - 26\,x^{12} - 21\,x^{11} + 25\,x^{10} + 23\,x^9 + 4\,x^8 - 24\,x^7 + 9\,x^6 + 43\,x^5 - 47\,x^4 + 26\,x^3 + 19\,x^2 - 40\,x - 32)y]$.

For $t = 1$ the point $[t]\pi(x,y) = \pi(x,y)$ has a non-trivial gcd with $\pi^2(x,y) + [2](x,y)$ in both its x- and y-coordinate.

Thus, $t \equiv 1 \mod 5$.

In fact, $t = -14$ and therefore
$\#E(\mathbf{F}_{97}) = 97 + 1 - (-14) = 112 = 2^4 \cdot 7$.

Complexity - very rough operation count

Each prime ℓ is about $\mathcal{O}(\log q)$.

Fix ℓ.

Elements of $\mathcal{R}_\ell = \mathbf{F}_q[X,Y]/(Y^2 - X^3 - AX - B, \psi_\ell)(X)$ have size $\mathcal{O}(\ell^2 \log q) = \mathcal{O}(\log^3 q)$, since $\deg \psi_\ell = (\ell^2 - 1)/2$.

Computing the Frobenius endomorphism in $\mathcal{R}_\ell$ takes $\mathcal{O}(\log^7 q)$ bit operations.

Prime number theorem: need $\mathcal{O}(\log q)$ primes ℓ.

Total cost: $\mathcal{O}(\log^8 q)$.

Summary Schoof's algorithm

Determine the trace t of the Frobenius endomorphism π modulo small primes ℓ, in order to compute $\#E(\mathbf{F}_q) = q + 1 - t$.

Compute t mod ℓ in $\mathcal{R}_\ell = \mathbf{F}_q[X,Y]/(Y^2 - X^3 - AX - B, \psi_\ell(X))$ whose size is determined by the degree of ψ_ℓ which is $(\ell^2 - 1)/2)$.

Improvement:
Try to determine the trace modulo ℓ in a subgroup of $E[\ell]$ and therefore determine a linear factor of the ℓth division polynomial ψ_ℓ.

1. Introduction

2. Schoof's algorithm

3. Computing in the torsion group

4. Improvements by Elkies

Characteristic polynomial revisited

The Frobenius endomorphism π is a linear operator on the vector space $E[\ell] \cong \mathbf{F}_\ell^2$.

Its characteristic polynomial splits over $\bar{\mathbf{F}}_\ell$

$$T^2 - tT + q = (T - \lambda_1)(T - \lambda_2).$$

If $\lambda_1, \lambda_2 \in \mathbf{F}_\ell$, we found two eigenvalues of π. We call ℓ an Elkies prime.

Then there exist two points $P_1, P_2 \in E[\ell]$ such that $\pi(P_1) = [\lambda_1]P_1$ and $\pi(P_2) = [\lambda_2]P_2$.

The points P_1, P_2 generate each a π-invariant subgroup of order ℓ of $E[\ell]$.

Compute the trace of the Frobenius in a subgroup of $E[\ell]$

Characteristic equation $T^2 - tT + q = (T - \lambda_1)(T - \lambda_2)$.

For $\lambda_1, \lambda_2 \in \mathbf{F}_\ell$ we get $q = \lambda_1 \cdot \lambda_2$ and thus

$$t = \lambda_1 + \lambda_2 = \lambda_1 + q/\lambda_1.$$

Determining t in a subgroup means finding an eigenvalue of the Frobenius in $\mathbf{F}_\ell$.

New 'check equation'. Find $\lambda \in \{0, 1, \ldots, \ell - 1\}$ such that

$$\pi(P) = [\lambda](P)$$

for a non-trivial point of a subgroup of $E[\ell]$.

Determine whether ℓ is an Elkies prime

Let E have a subgroup $\mathcal{C}$ of prime order ℓ. Then there exists an elliptic curve E' and an isogeny $\phi : E \to E'$ with kernel $\mathcal{C}$.

The ℓth modular polynomial Φ_ℓ is a polynomial of degree $\ell + 1$ in $\mathbf{F}_q[X, Y]$. Its roots are exactly the j-invariants of all ℓ-isogeneous elliptic curves.

Theorem

Let E be an elliptic curve over $\mathbf{F}_q$, not supersingular with j-invariant j not equal to 0 or 1728.
Then E has a π-invariant subgroup $\mathcal{C}$ of order ℓ if and only if the polynomial $\Phi_\ell(j, T)$ has a root $\tilde{j}$ in $\mathbf{F}_q$.

Note: $\tilde{j}$ is the j-invariant of an ℓ-isogeneous elliptic curve E' which is isomorphic to $E/\mathcal{C}$.

Representing a ℓ-group $\mathcal{C}$

Determine factor F_ℓ of ψ_ℓ in $\mathbf{F}_q[X]$ such that

$$(x, y) \in \mathcal{C} \;\Leftrightarrow\; F_\ell(x) = 0.$$

Construct F_ℓ by finding an degree-ℓ isogeny ϕ with kernel $\mathcal{C}$.

We get

$$F_\ell(X) = \prod_{\substack{\pm P \in \mathcal{C} \\ P \neq \mathcal{P}_\infty}} (X - P_x).$$

Degree: $\deg_X F_\ell = (\ell - 1)/2$.

Complexity for the Elkies procedure

Compute the Frobenius and $[\lambda]P$ in the ring $\mathbf{F}_q[X,Y]/(Y^2 - X^3 - AX - B, F_\ell(X))$ which has size $\mathcal{O}(\ell \log q) = \mathcal{O}(\log^2 q)$.

Overall complexity $\mathcal{O}(\log^5 q)$ bit operations.

Atkin and SEA

If ℓ is not an Elkies prime we can use Atkin's method to compute t mod ℓ:
Determine the rth power of the Frobenius such that there is a π^r-invariant subgroup of $E[\ell]$. Then $t \mod \ell$ satisfies

$$t^2 \equiv (\zeta_r + 2 + \zeta_r^{-1})q$$

for an rth root of unity.

Schoof-Elkies-Atkin algorithm

- Compute the trace t modulo small primes ℓ until $\prod \ell > 4\sqrt{q}$.
- For each ℓ use the modular polynomial Φ_ℓ to decide whether to use Elkies' or Atkin's procedure.
- Determine the trace t in the Hasse interval using the Chinese Remainder theorem.

Complexity of SEA: $\mathcal{O}(\log^6 q)$.

Thank you!