Constructing elliptic curves with known number of points over a prime field *

Amod Agashe
Max Planck Institut, Bonn
and University of Texas, Austin

October 2, 2002

*These slides can be obtained from http://www.ma.utexas.edu/users/amod/mymath.html

Abstract: In applications of elliptic curves to cryptography, one often needs to construct elliptic curves with known number of points over a prime field $\mathbf{F}_n$, where n is a prime. Atkin suggested the use of complex multiplication to construct such curves. One of the steps in this method is the calculation of a certain Hilbert class polynomial $H_D(X)$ modulo n for a certain fundamental discriminant D. The usual way of doing this is to compute $H_D(X)$ over the integers and then reduce modulo n. We suggest the use of a modified version of the Chinese remainder theorem to compute $H_D(X)$ modulo n directly from the knowledge of $H_D(X)$ modulo enough small primes. This is joint work with K. Lauter and R. Venkatesan.

Complex multiplication method

Given a prime n, we want an elliptic curve over $\mathbf{F}_n$ with known number of points (over $\mathbf{F}_n$).

Step 1: Find a negative fundamental discriminant D such that there are integers x and y such that $4n = x^2 - Dy^2$.

Def: The *Hilbert class polynomial* $H_D(X)$ is

$$H_D(X) = \prod \left(X - j\left(\frac{-b + \sqrt{D}}{2a} \right) \right),$$

where the product ranges over the set of $(a, b) \in \mathbf{Z} \times \mathbf{Z}$ such that $ax^2 + bxy + cy^2$ is a primitive, reduced, positive definite binary quadratic form of discriminant D for some $c \in \mathbf{Z}$, and j denotes the modular invariant. It is known that $H_D(X)$ has integer coefficients.

Step 2: Find a root j of $H_D(X) \bmod n$, and write down an elliptic curve E with j-invariant j. Then $\#E(\mathbf{F}_n) = 1 + n + x$ or $\#E(\mathbf{F}_n) = 1 + n - x$.

Computing $H_D(X)$

An upper bound for the size of the coefficients of $H_D(X)$ is

$$B = \binom{h}{\lfloor h/2 \rfloor} \exp\left(\pi\sqrt{-D}\sum \frac{1}{a}\right),$$

where h is the class number of $\mathbf{Q}(\sqrt{D})$.

Atkin-Morain method:
Compute $H_D(X)$ with complex coefficients with sufficient accuracy, and round it to the nearest integer polynomial.

Chinese remainder theorem (CRT) method (Chao-Nakamura-Sobotaka-Tsujii):
Compute $H_D(X)$ modulo sufficiently many "small" primes and lift it to $H_D(X)$ using CRT.

Computing $H_D(X)$ mod a small prime

Let $\mathcal{O}$ be the ring of integers of $\mathbf{Q}(\sqrt{D})$ and let $\mathrm{Ell}(D)$ denote the set of isomorphism classes of elliptic curves over $\mathbf{C}$ with complex multiplication by $\mathcal{O}$. Then

$$H_D(X) = \prod_{[E] \in \mathrm{Ell}(D)} (X - j(E)).$$

Let p be a prime such that $4p = t^2 - D$ for some integer t. Let $\mathrm{Ell}'(D)$ denote the set of isomorphism classes (over $\overline{\mathbf{F}}_p$) of elliptic curves over $\mathbf{F}_p$ with endomorphism ring (over $\overline{\mathbf{F}}_p$) isomorphic to $\mathcal{O}$.

Proposition 1.

$$H_D(X) \bmod p = \prod_{[E'] \in \mathrm{Ell}'(D)} (X - j(E')).$$

Proposition 2. *Let E' be an elliptic curve over $\mathbf{F}_p$. Then $\mathrm{End}_{\overline{\mathbf{F}}_p} E' \cong \mathcal{O}$ if and only if $\#E'(\mathbf{F}_p)$ is either $p+1-t$ or $p+1+t$.*

CRT method

Suppose $D \not\equiv 1 \bmod 8$.

Step 1: Start with the prime 2 and consider successive primes; if a prime p satisfies $4p = t^2 - D$ for some integer t, then we put it in the collection S (which is empty to begin with) and keep doing this till $\prod_{p \in S} p > B$ (assume this is possible).

Step 2: Compute $H_D(X) \bmod p$ for each $p \in S$ (this can be done using point counting).

Step 3: Lift using CRT to $H_D(X)$.

Find a root of $H_D(X) \bmod n$...

Our idea: With the knowledge of $H_D(X) \bmod p$ for each $p \in S$ compute $H_D(X) \bmod n$ directly using a modified version of CRT.

Modified CRT

Following Couveignes, Montgomery-Silverman.

GIVEN:
A collection of pairwise coprime positive integers m_i for $i = 1, 2, \ldots, \ell$.
For each i, an integer x_i with $0 \le x_i < m_i$.
A small positive real number ϵ.
There is an integer x s.t. $|x| < (1/2 - \epsilon) \prod_i m_i$,
and $x \equiv x_i \bmod m_i$ for each i.

TASK:
Compute $x \bmod n$,
for a given positive integer n.

Let $M = \prod_i m_i$, $M_i = M/m_i$, $a_i = 1/M_i \bmod m_i$.
Then $z = \sum_i a_i M_i x_i \equiv x \bmod M$.

If $r = \left\lfloor \frac{z}{M} + \frac{1}{2} \right\rfloor$, then $x = z - rM$.
So $x \bmod n = z \bmod n - (r \bmod n)(M \bmod n)$.

Easy check: $\frac{z}{M} + \frac{1}{2}$ is not within ϵ of an integer.
So, compute $\frac{z}{M} + \frac{1}{2}$ to precision ϵ, and round off to get r.

Complexity analysis

This part should be taken with a grain of salt!

Let $d = | D |$. Then $B = \mathrm{O}(\sqrt{d}(\log d)^2)$.
Atkin-Morain method for computing $H_D(X)$ takes time $\mathrm{O}(d^2(\log d)^4)$.

Statement 3. *If* $d \not\equiv 7 \bmod 8$, *then the set* S *is finite, the size of the set is* $\mathrm{O}(\frac{\log B}{\log \log B})$, *and each* $p \in S$ *is* $\mathrm{O}((\log B)^2)$.

Statement 3 is true with high probability; for what follows, assume Statement 3.

Computing $H_D(X) \bmod p$ for $p \in S$ takes time $\mathrm{O}(d^{3/2}(\log d)^{10})$.

The CRT method to lift to $H_D(X)$ takes time $\mathrm{O}(d(\log d)^2 \log n + d^{3/2}(\log d)^4)$.

Our method to compute $H_D(X) \bmod n$ takes time $\mathrm{O}(d(\log d)^2 \log n + \sqrt{d}(\log n)^2 + d(\log d)^4)$.

So our method would be an improvement only when d is "very large" (say $d > (\log n)^2$).