Decomposing class polynomials with the CRT method

Andrew V. Sutherland

Massachusetts Institute of Technology

April 15, 2010

http://math.mit.edu/~drew/

Constructing elliptic curves with dice

1. Write down a random curve $y^2 = x^3 + ax + b$ over $\mathbb{F}_q$.
2. Compute $N = \#E(\mathbb{F}_q)$.
3. Repeat steps 1 and 2 until you get an answer you like.

If you are picky, this might take a while...

Constructing elliptic curves with the CM method

Pick the values of q and N, with $t = q + 1 - N \not\equiv 0$ (in $\mathbb{F}_q$).
Let $D < 0$ be a discriminant satisfying $4q = t^2 - v^2 D$.

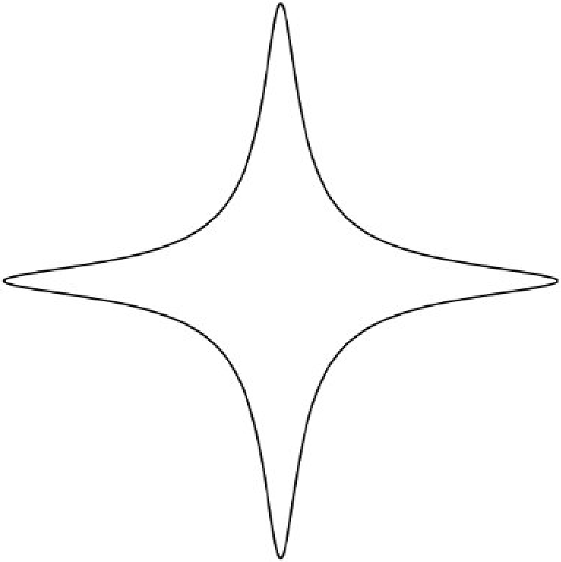
1. Compute the Hilbert class polynomial H_D.
2. Find a root j of H_D in $\mathbb{F}_q$.

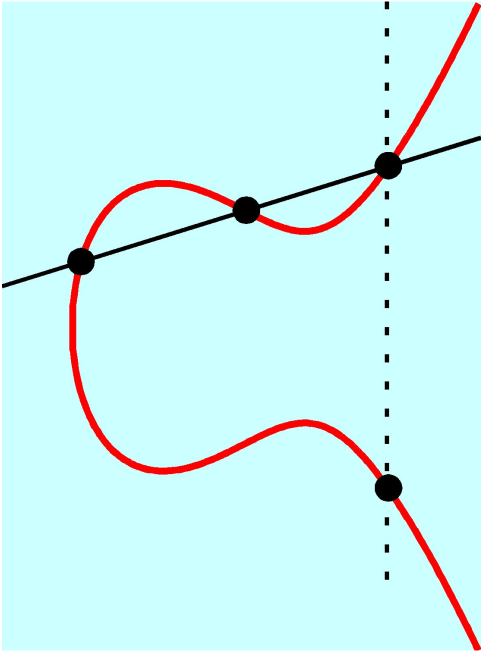
This yields the j-invariant of a curve $E/\mathbb{F}_q$ with N points.

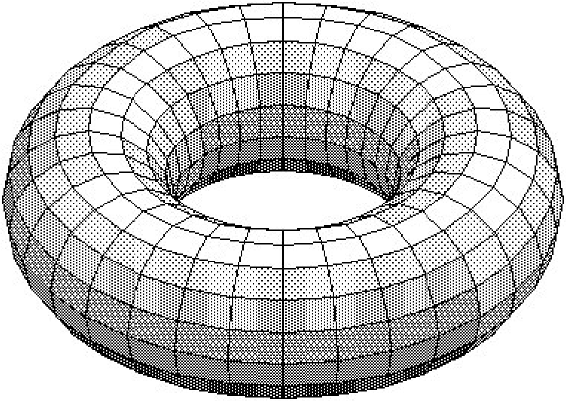
Assuming $j \neq 0, 1728$, we set $k = j/(1728 - j)$ and use either

$$y^2 = x^3 + 3kx + 2k$$

or its quadratic twist.







Complex multiplication (CM) in its simplest setting

Let Λ be a 2-d lattice in $\mathbb{C}$.
The torus $\mathbb{C}/\Lambda$ corresponds to an elliptic curve $E/\mathbb{C}$.
If $\alpha \in \mathbb{C}$ is nonzero, then $\mathbb{C}/\Lambda \cong \mathbb{C}/(\alpha\Lambda)$.

$$\mathrm{End}(E/\mathbb{C}) \cong \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}.$$

So $\mathbb{Z} \in \mathrm{End}(E/\mathbb{C})$, and if Λ is an imaginary quadratic order $\mathcal{O}$ (a 2-d subring of $\mathcal{O}_K$), or any ideal in $\mathcal{O}$, then $\mathrm{End}(E/\mathbb{C}) \cong \mathcal{O}$.

Every ordinary elliptic curve $E/\mathbb{F}_p$ is the reduction of some $E'/\mathbb{C}$ with CM by an imaginary quadratic order $\mathcal{O}$ [Deuring].

Elliptic curves with CM by $\mathcal{O}$.

Let $\mathcal{O}$ be an imaginary quadratic order with discriminant D.
Let $\mathrm{Ell}(\mathcal{O}) = \{j(E) : \mathrm{End}(E) \cong \mathcal{O}\}$.

1. $\mathrm{Ell}(\mathcal{O}) \cong \mathrm{cl}(\mathcal{O})$ is a finite set with $h(D)$ elements.
2. These are precisely the roots of $H_D(X)$.

To obtain H_D we enumerate $\mathrm{Ell}(\mathcal{O})$ and compute

$$H_D(X) = \prod_{j \in \mathrm{Ell}(\mathcal{O})} (X - j).$$

We can do this in $\mathbb{C}$, or in $\mathbb{F}_p$, if H_D splits completely in $\mathbb{F}_p[X]$.
Any prime p of the form $4p = t^2 - v^2 D$ will suffice.

The Hilbert class polynomial H_D

Good news: The coefficients of H_D are integers!

Bad news: They are really big integers!

The total size of H_D is $O(|D| \log^{1+\epsilon} |D|)$ bits.

$$H_D(x)$$

Visible Universe

Computing H_D with the CRT

Compute $H_D \bmod p$ for many "small" primes p, use the CRT to obtain H_D [CNST '98], or $H_D \bmod q$ via the explicit CRT [ALV '06].

Compute H_D in $O(|D| \log^{7+\epsilon} |D|)$ time (GRH) [BBEL '08].

Compute $H_D \bmod q$ in $O(|D|^{1/2+\epsilon} \log q)$ space and $O(|D| \log^{5+\epsilon} |D|)$ time (GRH), (up to 100x speedup) [S '09].

Alternative class invariants (up to 200x speedup) [ES '10].

State of the art (as of Jan 2010): $|D| \approx 10^{15}$ and $h(D) \approx 10^7$.

But stay tuned for more...

Decomposing class polynomials [HM 2001, EM 2003]

Let $\mathcal{O}$ have fraction field K and ring class field M. Let $G = \mathrm{cl}(\mathcal{O}) \cong \mathrm{Gal}(M/K)$ have subgroup $H = \mathrm{Gal}(M/L)$.

$$\mathbb{Q} \subset K \subset L \subset M$$

Let $\beta_1, \ldots, \beta_m$ be the elements of H.
Let $\alpha_1 H \ldots, \alpha_n H$ be the cosets of H in G.
For i from 1 to n define the values $\theta_{ij} \in L$ via

$$\sum_{j=0}^{m} \theta_{ij} X^j = \prod_{j=1}^{m} (X - [\alpha_i \beta_j] j_0),$$

where j_0 is a root of H_D with Galois conjugates $[\alpha_i \beta_j] j_0$.

Decomposing class polynomials (continued)

Let $t_i = \theta_{i,m-1}$ and define

$$V(Y) = \prod_{i=1}^{n}(Y - t_i)$$

and

$$W_j(Y) = \sum_{i=1}^{n}\theta_{ij}\frac{V(Y)}{Y - t_i}$$

so that $W_j(t_i) = \theta_{ij}V'(t_i)$. Finally, let

$$U(X,Y) = \frac{1}{V'(Y)}\sum_{j=0}^{m}W_j(Y)X^j.$$

The coefficients of V and W_j are integers in $\mathbb{Q}$ (not just K).

Modified CM method (version 1)

If r is a root of V then the roots of $U(X,r)$ are roots of H_D.
Modified CM method:

1. Compute V and the W_j mod q (using explicit CRT).
2. Find a root r of V and j of $U(X,r)$ in $\mathbb{F}_q$.

Suppose $m \approx n$. Step 2 is much improved. What about Step 1?

The cost of computing V and the W_j modulo each CRT prime p is reduced by a factor of up to 4 (typically about 2).

The number of CRT primes is reduced by a factor of about 2.
The space required is unchanged.

We can do better, assuming q is prime.

Modified CM method (version 2, q prime)

Recall that $W_j(Y) = \sum_{i=1}^n \theta_{ij} \frac{V(Y)}{Y-t_i}$.
We don't need to compute W_j in order to evaluate it!

1. Compute V (using explicit CRT mod q).
2. Find a root r of $V \bmod q$ and "lift" it to $\mathbb{Z}$.
3. Evaluate $W_j(r)$ (using explicit CRT mod q).
4. Construct $U(X,r) \bmod q$ and find a root j in $\mathbb{F}_q$.

The number of $\mathbb{F}_p$-operations to compute the θ_{ij} is

$$O\big((h/m)\mathsf{M}(m)\log m\big)$$

When $m \approx \log^2 h$ this is $O\big(h(\log\log h)^{2+\epsilon}\big)$, versus $O(h\log^{2+\epsilon} h)$.
Evaluating all the $W_j(r)$ costs $O(h)$ versus $O(h\log^{2+\epsilon} h)$.

Asmptotic results

Assume q is prime.

Theorem (Heuristic)

For any $\delta < 1$ there is a set of discriminants D with density δ for which version 2 of the modified CM method runs in time $O(|D| \log^{5/2+o(1)} |D|)$, provided $\log q = O(\log^{5/2} |D|)$.

Theorem (GRH)

The space required by version 2 of the modified CM method is $O((m+n)\log q + h \log h)$ bits, where $h(D) = h = mn$.

Using the CM method is easier than computing $H_D \bmod q$!

Practical results

Tests were run on a cluster of 8 quad-core AMD Phenom IIs.
Timings for 256-bit prime fields (1024-bit essentially the same).

Previous record $|D| \approx 10^{15}$ and $h \approx 10^7$ used 200 cpu-days (about a week). Now under 50 cpu-days (about 36 hours).

New record $|D| \approx 10^{15}$ and $h \approx 2 \cdot 10^7$ used 170 cpu-days.

New record $|D| \approx 5 \cdot 10^{14}$ and $h \approx 5 \cdot 10^7$ used 200 cpu-days.
Space: $H_D \approx$ 30PB, $H_D \bmod q \approx$ 1.6GB, $U, V \bmod q \approx$ 3MB

$|D| > 10^{16}$ and $h > 10^8$ are certainly within reach.

ECC Brainpool Standard

Taken from page 5 of `www.ecc-brainpool.org/download/Domain-parameters.pdf`.

3.2 Security Requirements.

. . .

3. *The class number of the maximal order of the endomorphism ring of E is larger than 10000000.*

   . . .

   This condition excludes curves that are generated by the well-known CM-method.

Not anymore.

Challenges

Challenge to number-theorists: Barreto and Naehrig have proposed pairing-friendly curve parameterizations that require 80-bit or 100-bit CM discriminants. Can we get there?

Challenge to cryptographers: Assume you can use 50-bit CM discriminants. What can you do with this?

A parameterization with $q \approx |D|^4$ would be interesting.

Decomposing class polynomials with the CRT method

Andrew V. Sutherland

Massachusetts Institute of Technology

April 15, 2010

http://math.mit.edu/~drew/