Class invariants by the CRT method

Andreas Enge

INRIA Bordeaux-Sud-Ouest

Andrew V. Sutherland

Massachusetts Institute of Technology

ANTS IX

Constructing an elliptic curve $E/\mathbb{F}_q$ with N points

Set $t = q + 1 - N$, assuming $t \neq 0$ and $|t| < 2\sqrt{q}$.
Write $4q = t^2 - v^2 D$ with $D < 0$, and then

1. Compute the Hilbert class polynomial $H_D(X)$.
2. Find a root j_0 of H_D in $\mathbb{F}_q$.

Now set $k = j_0/(1728 - j_0)$. Either the elliptic curve

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

or its quadratic twist has exactly N points over $\mathbb{F}_q$.

This is the CM method.

The Hilbert class polynomial

The discriminant D uniquely determines an imaginary quadratic order $\mathcal{O} = \mathbb{Z}[\tau]$. The curve E has CM by $\mathcal{O}$, i.e., $\mathrm{End}(E) \cong \mathcal{O}$.

- $j(\tau)$ is an algebraic integer.
- $H_D(X)$ is its minimal polynomial over $K = \mathbb{Q}(\sqrt{D})$.

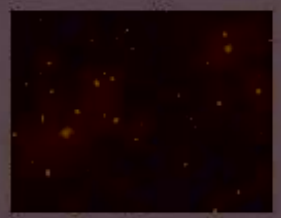
Good news: the coefficients of H_D are integers.

Bad news: they are really big integers!

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

C'est grand...

$$H_D(x)$$



Visible Universe

Approximate size of H_D

$\lvert D\rvert$	$h(D)$	height bound (bits)	$\approx$ total size
$10^5 + 4$	152	7983	150 KB
$10^6 + 104$	472	28154	1.7 MB
$10^7 + 47$	1512	117947	22 MB
$10^8 + 20$	5056	376700	240 MB
$10^9 + 15$	15216	1431844	2.7 GB
$10^{10} + 47$	48720	5152491	31 GB
$10^{11} + 4$	150192	17154622	320 GB
$10^{12} + 135$	476524	59259782	3.5 TB
$10^{13} + 15$	1522770	202225102	38 TB
$10^{14} + 4$	4927264	721773307	440 TB
$10^{15} + 15$	15209152	2337598720	4.4 PB

These are typical examples ($|D|^{1/2}/h(D) \approx 0.46\ldots$)

A tale of two ANTS

ANTS VIII 

- $O(|D|^{1+\epsilon})$ time H_D using CRT [BBEL]
  (matches complexity of p-adic and complex analytic)
- CRT method practically slow, restricted to j
- CM record: $|D| > 10^{10}$ using complex analytic [E]

ANTS IX 

- $O(|D|^{1/2+\epsilon} \log q)$ space H_D mod q using CRT [S]
  (surpasses p-adic and complex analytic)
- CRT method practically fast, not restricted to j
- CM record: $|D| > 10^{15}$ using CRT [ES]

Both CM records use class invariants other than j.

Class invariants

Let f be a modular function satisfying $\Psi(f, j) = 0$
for some integer polynomial $\Psi(F, J)$.

If $f(\tau) \in K(j(\tau))$ then $f(\tau)$ is a *class invariant*.
Its minimal polynomial $H_D[f](X)$ is a *class polynomial*.
We shall assume $H_D[f]$ has integer coefficients.

If f_0 is a root of $H_D[f]$ then we may obtain a root j_0 of H_D
as a root of $\Psi(f_0, J)$.

$H_D[f]$ is smaller than H_D by a factor of
$c(f) = \deg_F(\Psi)/\deg_J(\Psi)$.

Some particularly useful class invariants

- Weber $\mathfrak{f}$-function
- Double η-quotients $\mathfrak{w}^s_{p_1,p_2}$, with p_1 and p_2 prime
- Atkin functions A_N with N prime

function	level	$\deg_F(\Psi)$	$\deg_J(\Psi)$	$c(f)$	ρ
$\mathfrak{f}$	48	72	1	72	0.17
$\mathfrak{w}_{3,13}$	39	42	2	28	0.36
$\mathfrak{w}_{5,7}$	35	48	2	24	0.34
A_{71}	71	72	2	36	0.51
A_{59}	59	60	2	30	0.51
A_{47}	47	48	2	24	0.51

ρ is the proportion of fundamental D that yield class invariants.

Computing H_D with the CRT

For sufficiently many suitable primes p:

1. Find one root j_1 of H_D mod p. (test "random" curves)
2. Find all roots $j_1, \ldots, j_h$ of H_D mod p. (using isogenies)
3. $H_D(X) = (X - j_1) \cdots (X - j_h)$ mod p. (via a product tree)

Apply the CRT to obtain $H_D \in \mathbb{Z}[X]$ or (better) H_D mod q.

Sufficiently many means $O(|D|^{1/2+\epsilon})$.
Suitable means p is of the form $4p = t^2 - v^2 D$ and not very big.

See *Computing Hilbert class polynomials with the CRT* [S] for more details.

Realizing the Galois action via isogenies

The class group of $\mathcal{O}$ acts on the roots of H_D.
If $[\mathfrak{l}] \in \mathrm{cl}(\mathcal{O})$ has prime norm ℓ and j_1 is a root of H_D then

$$\Phi_\ell(j_1, [\mathfrak{l}]j_1) = 0,$$

where $\Phi_\ell(X, Y)$ is the classical modular polynomial.
Typically $[\mathfrak{l}]j_1$ and $[\bar{\mathfrak{l}}]j_1$ are the only roots of $\Phi_\ell(j_1, X)$ in $\mathbb{F}_p$.

We use ideals $\mathfrak{l}_1, \ldots, \mathfrak{l}_k$, with prime norms $\ell_1, \ldots, \ell_k$, such that every $[\mathfrak{a}] \in \mathrm{cl}(\mathcal{O})$ may be written uniquely as

$$[\mathfrak{a}] = [\mathfrak{l}_1^{e_1}] \cdots [\mathfrak{l}_k^{e_k}] \qquad (0 \le e_i < r_i).$$

for some positive integers $r_1, \ldots, r_k$.

Enumerating the roots of H_D mod p

Given a root j_1 of H_D mod p, all the roots of H_D mod p may be enumerated with the recursive algorithm below.

ENUMERATE$(j_1, \ell_1, \ldots, \ell_k)$:

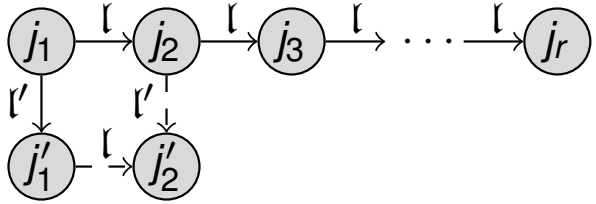
1. Arbitrarily choose a root j_2 of $\Phi_{\ell_k}(j_1, X)$ in $\mathbb{F}_p$.
2. For i from 3 to r_k:
   Let j_i be the root of $\Phi_{\ell_k}(j_{i-1}, X)/(X - j_{i-2})$ in $\mathbb{F}_p$.
3. If $k = 1$ then output $j_1, \ldots, j_{r_k}$ and return.
4. ENUMERATE$(j_i, \ell_1, \ldots, \ell_{k-1})$ for i from 1 to r_k.

Strategy 1: Convert j_1 to f_1 and enumerate $f_1, \ldots, f_h$.
This requires modular polynomials Φ_ℓ^f.

Strategy 2: Convert $j_1, \ldots, j_h$ to $f_1, \ldots, f_h$.
This requires us to choose directions *consistently*.

Choosing directions consistently

Having walked one path of ℓ-isogenies, we can ensure that all parallel paths are oriented in the same direction.



Instead of picking j'_2 arbitrarily, we compute the polynomial

$$\phi(X) = \gcd\big(\Phi_\ell(j'_1, X), \Phi_{\ell'}(j_2, X)\big)$$

and let j'_2 be its unique root (if $4\ell^2\ell'^2 < |D|$ then $\deg\phi = 1$).

We can compute $j'_3, \ldots, j'_r$ in the same way.

Computing GCDs is easier than finding roots!

CRT class polynomial computations: $H_D[f]$ vs. H_D

	Example 1	Example 2	Example 3	Example 4
$\lvert D\rvert$	13569850003	11039933587	12901800539	12042704347
function f	A_{71}	A_{47}	A_{71}	A_{59}
H_D time	19900	23700	52200	42400
H_D time (gcds)	15900	15500	44700	25300
$H_D[f]$ time	213	305	629	191
size factor	36	24	36	120*
total speedup	93	78	83	222

Times in CPU seconds (3.0 GHz AMD Phenom II)

These examples computed H_D or $H_D[f]$ modulo a cryptographic-size prime q. They were used to construct pairing-friendly curves of prime order.

Invariants with ramified level

For the Atkin functions and the double η-quotients, when the primes dividing the level ramify in $\mathbb{Q}(\sqrt{D})$, the class polynomial $H_D[f]$ is a perfect square.

In this case we can simply compute $\sqrt{H_D[f]}$, which reduces both the degree and the coefficient size by a factor of 2.

If 71 divides D, for example, the polynomial $\sqrt{H_D[A_{71}]}$ is approximately $2 \cdot 2 \cdot 36 = 144$ times smaller than H_D.

This beats Weber $\mathfrak{f}$ with $c(\mathfrak{f}) = 72$.

CRT vs Complex Analytic

		complex analytic		CRT		CRT mod q	
$\lvert D\rvert$	$h(D)$	$\mathfrak{w}_{3,13}$	$\mathfrak{f}$	$\mathfrak{w}_{3,13}$	$\mathfrak{f}$	$\mathfrak{w}_{3,13}$	$\mathfrak{f}$
6961631	5000	15	5.4	2.2	1.0	2.1	1.0
23512271	10000	106	33	10	4.1	9.8	4.0
98016239	20000	819	262	52	22	47	22
357116231	40000	6210	1900	248	101	213	94
2093236031	100000	91000	27900	2200	870	1800	770

Times in CPU seconds (3.0 GHz AMD Phenom II)

For the CRT timings, $H_D[f]$ was computed both over $\mathbb{Z}$ and modulo a 256-bit prime q.

A record CM construction

We computed the square-root of the class polynomial $H_D[A_{71}]$ using the discriminant D with

$$|D| = 1000000013079299 > 10^{15}.$$

We then used the CM method to construct an elliptic curve E of prime order over a 256-bit prime field $\mathbb{F}_q$.

The endomorphism ring of E is isomorphic to an imaginary quadratic order with class number

$$h(D) = 10034174 > 10^7.$$

ECC Brainpool Standard

`http://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."

This is no longer true.

Class invariants by the CRT method

Andreas Enge

INRIA Bordeaux-Sud-Ouest

Andrew V. Sutherland

Massachusetts Institute of Technology

ANTS IX