Advances in the CM method for elliptic curves

F. Morain

Laboratoire d'Informatique de l'École polytechnique

logoX CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE logoINRIA logoUW

Fields Institute – Toronto, May 13, 2009

Contents

I. Motivations

Context: use elliptic curves of known cardinality when Schoof's algorithm is inedaquate.

Fundamental theorem: (Hasse, Deuring, ...) if $4p = U^2 - DV^2$, there exists an elliptic curve $E/\mathbb{F}_p$ of cardinality $m = p + 1 - U$.

A short list of applications:

- Primality proving: ECPP (Atkin 1986, M.); EAKS (Couveignes/Ezome/Lercier);
- Building cyclic elliptic curves (M. 1991);
- E of given cardinality (but varying p – Bröker/Stevenhagen);
- Pairing friendly curves (see Freeman/Scott/Teske taxonomy paper).

Rem. For ease of presentation, stick to $\mathbb{F}_p$ with p (large) prime; results generalize to any finite field.

ECPP in one slide

function ECPP(N)

- if N is small enough, prove its primality directly.
- **repeat**
  find $D \in \mathscr{D}$ s.t. $4N = U^2 - DV^2$ (Cornacchia)
  until $m = N + 1 - U = cN'$ with $c > 1$ small, N' probable prime;
- use the CM method to build E and find P of order m;
- return ECPP(N').

Variants differ in the choice of $\mathscr{D}$; fastest leads to heuristic $\tilde{O}((\log N)^4)$; record still at $20,000$ dd.

Two slightly different contexts

- **ECPP:**
  - probable prime $N \approx 2^{30000}$;
  - N to be proven prime, so more checks are necessary and some tricks cannot be used (Montgomery form only if Bernstein in some cases?);
  - numerous D's available, happy with $3 \mid D$;
  - $\#E$ proven by the succesful termination of the algorithm on subsequent numbers;
  - (very) few verifications of the certificate?
- **Cryptography:**
  - prime $p \approx 2^{200}$;
  - any parametrization of E possible;
  - few D's available, perhaps $D \equiv 5 \bmod 8$, and perhaps no point of order 4 at all...;
  - $\#E$ often prime or almost prime;
  - many verifications of the certificate?

In both cases, potentially large D's or h's (see later for large in ECPP; pairing friendly curves have large requirements).

II. Defining the CM methods

Notations: $D = m^2 D_K$ where D_K is the discriminant of an imaginary quadratic field $\mathbf{K}$; D is the discriminant of $\mathscr{O} = [1, m\omega]$ where $\mathbb{Z}_K = [1, \omega]$; $h(\mathscr{O}) = \#Cl(\mathscr{O})$.

Ex. $D = -1^2 \cdot 4$, $\mathbf{K} = \mathbb{Q}(i)$, $\mathbb{Z}_K = [1, i]$, $h = 1$, $Cl = \{(1,0,1)\}$.

Thm. $4p = U^2 - DV^2$ iff p splits in the ring class field $\mathbf{K}_D$ ($m = 1$ corresponds to the Hilbert Class Field of $\mathbf{K}$).

Thm. $\mathbf{K}_D = \mathbf{K}(j(m\omega))$ where j is the modular invariant

$$j(z) = \frac{1}{q} + 744 + \sum_{n>0} c_n q^n$$

with $q = \exp(2i\pi z)$.

Algebraic theory

Write $\mathfrak{a} = [\alpha_1, \alpha_2]$ and $\alpha = \alpha_1/\alpha_2$; define $j(\mathfrak{a}) = j(\alpha)$.

Thm. K_D/K is Galois, with group $\sim Cl(\mathscr{O})$ and therefore $[K_D : K] = h(\mathscr{O})$. Moreover:

$$j(\mathfrak{a})^{\sigma(\mathfrak{i})} = j(\mathfrak{i}^{-1}\mathfrak{a}).$$

Thm. $H_D(X) = \prod_{\mathfrak{i} \in Cl(\mathscr{O})} (X - j(\mathfrak{i})) \in \mathbb{Z}[X]$.

Fundamental Thm. $4p = U^2 - DV^2$ iff $(D/p) = +1$ and $H_D(X)$ has $h(\mathscr{O})$ roots modulo p.

Ex. $4p = U^2 + 4V^2$ if and only if $p = 2$ or $p \equiv 1 \bmod 4$.

References: LNM 21, Serre, Cox.

“Computing” K_D

Computation of $H_D(X)$: write each class of $Cl(\mathcal{O})$ as $\mathfrak{i} = [\alpha_1, \alpha_2]$ and evaluate $j(\alpha_1/\alpha_2)$ as a multiprecision number.

Ex. $H_{-3}(X) = X$, $H_{-4}(X) = X - 1728$;

$$H_{-23}(X) = X^3 + 3491750X^2 - 5151296875X + 12771880859375;$$

$$H_{-3\times 5^2}(X) = X^2 + 654403829760X + 5209253090426880.$$

$\Rightarrow p = x^2 + y^2$ iff $(-4/p) = +1$;

$4p = x^2 + 3 \times 5^2 y^2$ iff $(-75/p) = +1$ and $H_{-3\times 5^2}(X)$ factors modulo p.

More on this later!

The CM method

INPUT:

- p (or $q = p^n$);
- $D < 0$ (fundamental or not);
- U and V in $\mathbb{Z}$ s.t. $p = (U^2 - DV^2)/4$.

OUTPUT:

- $E/\mathbb{F}_p$ s.t. $m = \#E(\mathbb{F}_p) = p + 1 - U$;
- a proof of correctness.

Rem.

- if U and V are not known, compute them using Cornacchia's algorithm;
- proof of correctness: might involve factoring m and exhibiting generators of $E/\mathbb{F}_p$; soft proof could be P s.t. $[m]P = O_E$ but $[m']P = O_E$ ($m' = p + 1 + U$ is the cardinality of a twist E' of E); in ECPP, proof is recursive.

The CM method

INPUT:

- p (or $q = p^n$);
- $D < 0$ (fundamental or not);
- U and V in $\mathbb{Z}$ s.t. $p = (U^2 - DV^2)/4$.

OUTPUT:

- $E/\mathbb{F}_p$ s.t. $m = \#E(\mathbb{F}_p) = p + 1 - U$;
- a proof of correctness.

Rem.

- if U and V are not known, compute them using Cornacchia's algorithm;
- proof of correctness: might involve factoring m and exhibiting generators of $E/\mathbb{F}_p$; soft proof could be P s.t. $[m]P = O_E$ but $[m']P = O_E$ ($m' = p + 1 + U$ is the cardinality of a twist E' of E); in ECPP, proof is recursive.

The CM method (more precise)

INPUT:

- p (or $q = p^n$);
- $D < 0$ (fundamental or not);
- U and V in $\mathbb{Z}$ s.t. $p = (U^2 - DV^2)/4$.

OUTPUT:

- E having CM by the order of discriminant D; as a consequence $E/\mathbb{F}_p$ s.t. $m = \#E(\mathbb{F}_p) = p + 1 - U$;
- a proof of correctness.

Rem. The proof of correctness could involve volcanoes.

Let's open drawers

function CM(p, D, U, V)

1. Compute $H_D[j](X)$.

2. Find a root j_0 of $H_D[j](X) \bmod p$.

3. Find E of invariant j_0:

$$E_c : Y^2 = X^3 + \frac{3j_0}{1728 - j_0} c^2 X + \frac{2j_0}{1728 - j_0} c^3$$

where c accounts for twists of E.

4. Prove that E has cardinality $m = p + 1 - U$.

Let's open drawers

function CM(p, D, U, V)

1. Compute $H_D[j](X)$.
$\Rightarrow$ three methods for this! all in $O(D^{1+\varepsilon})$: complex, p-adic, CRT.

2. Find a root j_0 of $H_D[j](X) \bmod p$.
$\Rightarrow$ use Galois theory + classical tricks from computer algebra

3. Find E of invariant j_0:

$$E_c : Y^2 = X^3 + \frac{3j_0}{1728 - j_0} c^2 X + \frac{2j_0}{1728 - j_0} c^3$$

where c accounts for twists of E.
$\Rightarrow$ Try to try only one curve (see recent Rubin/Silverberg, cf. part IV.)

4. Prove that E has cardinality $m = p + 1 - U$.
$\Rightarrow$ Use adequate parametrizations to check $[m]P = O_E$, sometimes Edwards/Montgomery curves – see `http://arxiv.org/abs/0904.2243`.

III. Replacing j: class invariants

Q. How do we find smaller defining polynomials for K_D?

Two cases:

- construct K_D;
- build a CM curve (need some relation between f and j).

From $j(\sqrt{-2}) = 8000$, one solves

$$(*) \quad j = \frac{(X+16)^3}{X}$$

to get $X = 2^6$.

Key remark: equation $(*)$ is a modular equation for $X_0(2) \Rightarrow$ generalize to $X_0(N)$ or $X^0(N)$ for any $N > 1$.

$\Longleftrightarrow$ replace $j(\alpha)$ by class invariants $f(\alpha)$ for some modular function f.

Rem. The classical Weber functions are $\mathfrak{f}$, $\mathfrak{f}_1$, $\mathfrak{f}_2$ s.t. $-\mathfrak{f}(\alpha)^{24}$, $\mathfrak{f}_1(\alpha)^{24}$ and $\mathfrak{f}_2(\alpha)^{24}$ are roots of $(*)$.

A) Modular functions for $\Gamma^0(N)$

$$\Gamma^0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & 0 \\ * & * \end{pmatrix} \bmod N \right\}$$

$$\psi(N) = [\Gamma : \Gamma^0(N)] = N \prod_{p|N} (1 + 1/p)$$

Def. f on $\mathbb{H}^*$ is a modular function for $\Gamma^0(N)$ if and only if

$$\forall M \in \Gamma^0(N), z \in \mathbb{H}^*, (f \circ M)(z) = f(Mz) = f(z)$$

(+ some technical conditions).

Thm. Let f be a function for $\Gamma^0(N)$, $\Gamma/\Gamma^0(N) = \{\gamma_v\}_{1 \le v \le \psi(N)}$. Put

$$\Phi[f](X) = \prod_{v=1}^{\psi(N)} (X - f \circ \gamma_v) = \sum_{v=0}^{\psi(N)} R_v(J) X^v$$

where $R_v(J) \in \mathbb{C}(J)$. Then $\Phi[f](X, J) = 0$ is called a modular equation for $\Gamma^0(N)$.

Why do class invariants exist?

Thm. If $f = \sum a_n q^n$ has integer coefficients, $\Phi[f](X,J) \in \mathbb{Z}[X,J]$.

Coro. If $j(\tau)$ is an algebraic integer, so is $f(\tau)$.

$\Rightarrow$ if $f(z) \in K_D$ and we know its conjugates, we are done!

Shimura's reciprocity law tells us when $f(z)$ is in $\mathbf{K}_D$.

Use Schertz's simplified formulation that also gives conjugates of $f(z)$.

What is a small invariant?

Def. $\mathscr{H}(P = \sum(a_i + b_i\omega)X^i) = \log(\max\{|a_i|, |b_i|\})$.

Prop. (Hindry & Silverman)

$$\frac{\mathscr{H}(f(z))}{\mathscr{H}(j(z))} = \frac{\deg_J(\Phi[f])}{\deg_X(\Phi[f])}(1 + o(1)) = c(f)(1 + o(1)).$$

$\Rightarrow$ we have a measure for the size of $f(z)$ w.r.t. $j(z)$.

$\Rightarrow$ favor invariants with small $\deg_J \Phi[f]$, e.g., $\deg_J = 1$ (i.e., $g(X^0(N)) = 0$); $\deg_X \Phi = \psi(N)$.

B) Finding functions on $\Gamma^0(N)$: Newman's lemma

Lemma. If $N > 1$ and (r_d) is a sequence of integers such that

$$\sum_{d|N} r_d = 0,$$

$$\sum_{d|N} d r_d \equiv 0 \bmod 24, \quad \sum_{d|N} \frac{N}{d} \quad r_d \equiv 0 \bmod 24,$$

$$\prod_{d|N} d^{r_d} = t^2$$

with $t \in \mathbb{Q}^*$, then the function

$$g(z) = \prod_{d|N} \eta(z/d)^{r_d}$$

is a modular function on $\Gamma^0(N)$.

$$\eta(z) = q^{1/24} \prod_{m \geq 1} (1 - q^m).$$

Some studied (sub)families

Enge/Schertz:

$$\mathfrak{w}_{p_1,p_2}(z)^{\sigma} = \left(\frac{\eta\left(\frac{z}{p_1}\right)\eta\left(\frac{z}{p_2}\right)}{\eta\left(\frac{z}{p_1 p_2}\right)\eta(z)} \right)^{\sigma},$$

where $\sigma = \frac{24}{\gcd(24,(p_1-1)(p_2-1))}$.

Generalized Weber functions (Enge+M.):

$$\mathfrak{w}_N(z)^s = \left(\frac{\eta(z/N)}{\eta(z)} \right)^s$$

where $t = 24/\gcd(24, N-1)$, $s = 2t$ if t is odd and not a square, $s = t$ otherwise; $N = 2$ classical, $\mathfrak{w}_2 = \mathfrak{f}_1$, $N = 3$ by A. Gee.

The genus 0 case

$\mathcal{N}_N = q^{1/N}(1+\ldots)$ and $\deg_J = 1$, $c(\mathcal{N}_N) = 1/\psi(N)$.

Two cases:

- use generalized Weber for $N-1 \mid 24$:

$$\Phi[\mathfrak{w}_2^{24}](X,J) = (X+16)^3 - JX,$$

$$\Phi[\mathfrak{w}_3^{12}](X,J) = (X+27)(X+3)^2 - JX,$$

$$\Phi[\mathfrak{w}_4^{8}](X,J) = (X^2+16X+16)^3 - JX(X+16),$$

- Klein, Fricke (with $\eta_K = \eta(z/K)$):

N	$\mathcal{N}_N$	$c(\mathcal{N}_N)$
6	$\eta_6^5\eta_3^{-1}\eta_2\eta_1^{-5}$	$1/12$
8	$\eta_8^4\eta_4^{-2}\eta_2^2\eta_1^{-4}$	$1/12$
10	$\eta_{10}^3\eta_5^{-1}\eta_2\eta_1^{-3}$	$1/18$
12	$\eta_{12}^3\eta_6^{-2}\eta_4^{-1}\eta_3\eta_2^2\eta_1^{-3}$	$1/24$
16	$\eta_{16}^2\eta_8^{-1}\eta_2\eta_1^{-2}$	$1/24$
18	$\eta_{18}^2\eta_9^{-1}\eta_6^{-1}\eta_3\eta_2\eta_1^{-2}$	$1/36$

Generalized Weber functions (Enge + M.)

Thm. If f is a Newman function for $\Gamma^0(N)$ and $B^2 \equiv D \bmod (4N)$, then $f((-B+\sqrt{D})/2)$ is a class invariant. Its conjugates are given by a N-system à la Schertz.

A glimpse at our winter work: find all cases where $\zeta_{24}^k \mathfrak{w}_N^e$ is a class invariant for $e \mid s$. Needs: classification of $N \bmod 12$ + extension of Schertz's results.

Prop. (a) If $N \equiv 5 \bmod 12$ and $3 \nmid D$, then $\mathfrak{w}_N^2$ is a class invariant.
(b) If $N \equiv 7 \bmod 12$ and $2 \nmid D$, then $\mathfrak{w}_N^2$ is a class invariant.
(c) If $N \equiv 7 \bmod 12$ and $D \equiv 88 \bmod 112$, then $\zeta_4 \mathfrak{w}_N^2$ is a class invariant.

$$H_{-24}[\zeta_4 \mathfrak{w}_7^2] = X^2 + (\omega - 1)X - 2\omega - 5;$$

Generalized Weber functions (2/2)

$N = 3$ (compare Gee): use $\mathfrak{w}_3^e$ for

B	D mod 36	e
0:1	$0, 12$	12
0:1	$9, 21$	6
1:3	24	4
2:3	$4, 16, 28$	4
1:3	33	2
2:3	$1, 13, 25$	2

$N = 4$: if $D \equiv 1 \bmod 8$, use $\mathfrak{w}_4$ ($c = 1/48$).

$N = 25$: for D a square mod 20, use $\mathfrak{w}_{25}$ ($c = 1/30$).

Much more results in our preprint.

Comparing the invariants

f	$c(f)$	$\deg_J$
$\mathfrak{w}_\ell^e$	$\frac{e(\ell-1)}{24(\ell+1)}$	$\frac{s(N-1)}{24}$
$\mathfrak{w}_{\ell^2}^e$	$\frac{e(\ell-1)}{24\ell}$	$\frac{\ell^2-1}{24}$ if $\ell > 3$
$\mathfrak{w}_{p_1p_2}^e$	$\frac{e(p_2-1)}{24(p_2+1)}$	$\frac{s(p_2-1)(p_1-1)}{24}$
$\mathfrak{w}_N^e$	$\frac{e(N-1+S(N))}{24\psi(N)}$	$\frac{s(N-1+S(N))}{24}$
$\mathfrak{w}_{\ell,\ell}^e$	$\frac{e(\ell-1)^2}{12\ell(\ell+1)}$	$\frac{\sigma(\ell-1)^2}{12}$
$\mathfrak{w}_{p_1,p_2}^e$	$\frac{e(p_1-1)(p_2-1)}{12(p_1+1)(p_2+1)}$	$\frac{\sigma(p_1-1)(p_2-1)}{12}$

Rem. $\mathfrak{w}_{\ell^2}^1$ for prime $\ell > 3$ is often better than $\mathfrak{w}_\ell^e$.

What is the smallest invariant?

Extension of Enge+M. of ANTSV:

$$\underset{96,?}{?} > \underset{72,1}{\mathfrak{w}_2} > \underset{48,1}{\mathfrak{w}_4} > \underset{37,6}{\mathfrak{w}_{2,73}} > \underset{147/4,8}{\mathfrak{w}_{2,97}} > \underset{36,1}{\mathfrak{w}_9} = \underset{36,1}{t}$$

$$= \underset{36,1}{\mathscr{A}_{71}} = \underset{36,1}{\mathfrak{w}_2^2} = \underset{36,1}{\mathscr{N}_{18}} > \underset{32,6}{\mathfrak{w}_{16}} > \underset{30,1}{\mathfrak{w}_{25}} > \underset{28,2}{\mathfrak{w}_{3,13}} = \underset{28,2}{\mathfrak{w}_{49}}$$

$$> \underset{27,12}{\mathfrak{w}_{81}} > \underset{132/5,5}{\mathfrak{w}_{112}} > \underset{26,7}{\mathfrak{w}_{132}} > \underset{51/2,12}{\mathfrak{w}_{172}} > \underset{76/3,6}{\mathfrak{w}_{3,37}} = \underset{76/3,15}{\mathfrak{w}_{192}} > \underset{124/5,10}{\mathfrak{w}_{3,61}}$$

$$> \underset{24,2}{\mathfrak{w}_{5,7}} = \underset{24,1}{\mathfrak{w}_2^3} = \underset{24,6}{\mathfrak{w}_6^2} = \underset{24,1}{\mathfrak{w}_4^2} = \underset{24,1}{\mathfrak{w}_3^2} \cdots$$

$$\cdots > \underset{3,1}{\gamma_2} > \underset{2,1}{\gamma_3} > \underset{1,1}{j}$$

$$j = \gamma_2^3 = \gamma_3^2 + 1728.$$

t: Ramanujan (Konstantinou/Kontogeorgis 08, Enge 08) for $D \equiv 1 \bmod 12$.

Looking for $1/96$

Selberg+Abramovich+Bröker/Stevenhagen: for all f for $\Gamma^0(N)$, $c(f) \geq 1/96$.

Generalized Weber:

$$c(\mathfrak{w}_N^s) = \frac{s}{24}\,\frac{N-1+S(N)}{\psi(N)}.$$

Best value so far: $1/72$ obtained with $c(\mathfrak{w}_N) = c(\mathfrak{w}_N^s)^{1/s}$ for $N=2$, $s=24$.

Enge/Schertz:

$$c(\mathfrak{w}_{p_1,p_2}^s) = \frac{s}{12}\,\frac{(p_1-1)(p_2-1)}{(p_1+1)(p_2+1)}.$$

Rem. $g(X_0(N)) \approx \psi(N)/12$ and $\deg_J \geq g(X_0(N))+1$, so that $c(f) \approx \frac{1}{12}$.

Looking for $1/96$ (cont'd)

For prime $N = \ell$:

$$g(X_0(\ell)/w_\ell) = \frac{g(X_0(\ell)) + 1}{2} - \frac{a(\ell)}{4}, \quad a(\ell) = O(\sqrt{\ell})$$

$\Rightarrow c(f) \approx 1/12$, since $\deg_J \geq 2(g(X_0^*(\ell) + 1)$.

Best values for Atkin's minimal functions for $X_0^*(\ell)$ (for $\ell \leq 2000$):

ℓ	71	131	191
$c(f)$	$1/36$	$1/33$	$1/32$
$\deg_J$	2	4	6
g	0	2	3

$\mathscr{A}_{71} = (\Theta_{2,1,9} - \Theta_{4,3,5})/\eta\eta_{71}$ (also obtainable by Atkin's laundry method). Usable as soon as $(D/71) \neq -1$.

Going further: use composite values of N (work in progress).

Using class invariants

procedure BUILDCMCURVE(p, D)

0. Compute $H_D[u](X)$ and $\Phi[u](X,J)$ (precomputation).
1. Compute a root u_0 of $H_D[u](X) \equiv 0 \bmod p$.
2. Compute the set $\mathscr{J}$ of all roots of $\Phi[u](u_0,J) \equiv 0 \bmod p$ and find one elliptic curve having j-invariant in $\mathscr{J}$ which has cardinality $p+1-U$.

Rem.

- Most favorable case when $X_0(N)$ is of genus 0.
- Some j can be discarded if we know that $j-1728$ must be a square, or j a cube.
- No need to compute $\Phi[\mathfrak{w}_{25}]$, use $\Phi[\mathfrak{w}_5^6]$ together with resultants.

IV. Finding the correct twist

Pb. Given $p = (U^2 - DV^2)/4$, j, find an equation of

$$E_c : Y^2 = X^3 + \frac{3j}{1728-j}c^2X + \frac{2j}{1728-j}c^3$$

s.t. $\#E_c(\mathbb{F}_p) = p + 1 - U$.

The actual Frobenius of the curve is $\pi = (\tilde{U} + \tilde{V}\sqrt{D})/2$, and w.l.o.g. $|U| = |\tilde{U}|$, so we need fix the sign.

Why bother? find a point P, check $[m]P = O_E$ (or even $[\pi - 1]P$ using rational CM formulas to get some speedup) and if not try the twist.

- 1.5 curves tried on average; can be tricky to distinguish E from E' (cf. Mestre's algorithm).
- If solving the problem can be done at no cost, do it! And it involves nice mathematics (character sums, etc.).

A short history

- $D = -4$, $D = -3$: many variants, starting with Gauss (of course!).
- $h = 1$: Rajwade *et alii*, Joux+M., Leprévost + M., Padma+Venkataraman, Ishii, etc.
- **Stark** (1996): $\gcd(D, 6) = 1$, but needs γ_2 and γ_3.
- **M.** (2007): use small torsion points; e.g., use $\mathfrak{w}_3$ to get a 3-torsion point P_3 and compute action of π on P_3.
- **Rubin & Silverberg** (2009): all cases for D fundamental, but use costly invariants (j or $\gamma_3\sqrt{D}$); ok for small $|D|$'s (precomputations), probably not for large $|D|$'s and on the fly computations.

Rubin/Silverberg: the case $|D|/4 \equiv 1 \bmod 4$

With $d = |D|/4$, write

$$H_D[j](X) = f_1(X) + \sqrt{d}\, f_2(X)$$

where $\deg(f_1) = \deg(f_2) = h/2$. This is possible since $4 \,||\, D$ implies $D = (-4)q_1 \cdots q_r(-q_{r+1}) \cdots (-q_t)$ and $\sqrt{d} = \sqrt{-D}/\sqrt{-1}/2 \in \mathbf{K}_H$.

Algorithm: fix $\delta = \sqrt{d} \bmod p$ and proceed with easy formulas (cost $\approx$ one modular exponentiation over $\mathbb{F}_p$).

To make this more efficient:

- replace j with any real invariant (using complex invariants does not seem straightforward);
- factor $H_D[u]$ over $\mathbf{K}_g^+ = \mathbb{Q}(\sqrt{|q_i|})_{1 \le i \le t}$;
- use Galois theory over $\mathbf{K}_g^+$.

Rubin/Silverberg: other cases

Solve the problem completely using minimal polynomial of $\sqrt{\pm D}\gamma_3$ (remember that $\gamma_3(\alpha)^2 = j(\alpha) - 1728$).

A particular case: in some cases, $\sqrt{D}\mathfrak{w}_N^{s/2}$ is a real class invariant. Then use $w_3 = \mathfrak{w}_3(\alpha)^6$ or $w_7 = \mathfrak{w}_7(\alpha)^2$, since

$$\gamma_3(\alpha) = \frac{w_3^4 + 18w_3^2 - 27}{w_3} = \frac{w_7^8 + 14w_7^6 + 67w_7^4 + 70w_7^2 - 7}{w_7}$$

see Weber; these are the only equations with $\mathfrak{w}_N$ and γ_3 only.
Now rewrite

$$\sqrt{D}\gamma_3(\alpha) = D\frac{\cdots}{\sqrt{D}\mathfrak{w}_N^{s/2}}.$$

Rem. The case $\sqrt{|D|}\gamma_3$ seems more difficult.

V. Benchmarks

$N_1 = 2072644824759 \cdot 2^{33333} + 5$ $N_2 = 59056921173 \cdot 2^{34030} + 7$,
$N_3 = \zeta(-4305)/\zeta(-1)$, $N_4 = Cyclo_{23912}(10)$

N	N_1	N_2	N_3	N_4
$\#dd$	10047	10255	10342	10081
#steps	921	960	937	917
time (d)	$86+32$	$44+16$	$49+15$	$49+13$
m mod 4	(376+247)/286	(395+258)/288	(401+230)/288	(401+209)/284
D, h	3997096072 | 12080	954271591 | 14272 2657033560 | 12512 2060139016 | 12448 1928523316 | 13840	3715931860 | 13280 679224920 | 14656	339174836 | 14400 1908601428 | 13920 3610127752 | 12896
new inv.	91 $\mathfrak{w}_{3,13}$ 69 $\mathfrak{f}_1^2/\sqrt{2}$ 63 $\mathfrak{w}_{3,37}$ 39 $\mathfrak{f}(-4D)$ 38 $\mathfrak{w}_{5,7}$ 25 $\mathfrak{w}_{3,61}$ 19 $\mathfrak{f}^2/\sqrt{2}$	75 $\mathfrak{w}_{3,13}$ 81 $\mathfrak{w}_{25}$ 48 $\mathfrak{w}_{49}$ 41 $\mathfrak{f}(-4D)$ 37 N_{18} 34 $\mathfrak{f}_1^2/\sqrt{2}$ 29 $\mathfrak{w}_{3,37}$	78 $\mathfrak{w}_{25}$ 66 $\mathfrak{w}_{3,13}$ 59 N_{18} 45 $\mathfrak{w}_{49}$ 40 $\mathfrak{f}(-4D)$ 38 $\mathfrak{w}_{3,37}$ 36 $\mathfrak{f}_1^2/\sqrt{2}$	80 $\mathfrak{w}_{25}$ 58 $\mathfrak{w}_{3,13}$ 56 $\mathfrak{w}_{49}$ 50 N_{18} 43 $\mathfrak{f}(-4D)$ 36 $\mathfrak{w}_{3,37}$ 25 $\mathfrak{w}_9$

$D = 679224920$: $\mathcal{N}_{18}$ + Galois needed 8869 s;
2+2+2+2+2+2+229 roots mod p_{33480b} took 51097 s; $[m]P$ 300 s.

More statistics

N_1: Luhn; N_2: Jordan; N_3: Broadhurst; N_4: Broadhurst2.

what	N_1	N_2	N_3	N_4
# steps	921	960	937	917
$\sqrt{D}$	25.5	15.5	15.9	14.8
find (D,h)	5.0	4.3	6.0	5.2
Cornacchia	3.2	1.3	2.5	1.8
FKW	9.1	4.4	5.2	5.9
PRP	43.1	25.5	26.6	22.9
H_D	0.8	0.6	0.7	0.7
root H_D	27.9	14.0	13.0	11.5
Step 1	85.9	50.2	56.4	48.8
Step 2	31.8	16.1	15.2	13.4
Check	0.8	0.5	0.6	0.6

Timings are in cumulated days on some AMD Athlon(tm) 64 Processor 3400+ (2.4 GHz).

Conclusions

- ECPP vs. crypto-CM: the present talk was biased towards ECPP; different optimizations are claimed for by crypto-CM.
- New invariants are being used in practice. Some more to come (1/96??). Wait for CRT method to be operational for all of these.
- **Some unsolved problems in ECPP:** compute $h(D)$ for a batch of $D \in \mathscr{D}$; even more faster root finding?
- **My programs:** in the process of cleaning, new 13.8.7 arriving soon (SAGE?) $\longleftrightarrow$ yet another attempt at having them survive without me (?).

Rem. More references on my web page.