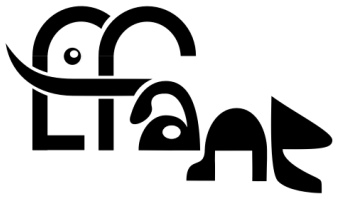
Class polynomials by Chinese remaindering

Andreas Enge

LFANT project-team
INRIA Bordeaux–Sud-Ouest
andreas.enge@inria.fr
http://www.math.u-bordeaux1.fr/~enge

ECC, 22/10/2010



INSTITUT NATIONAL
DE RECHERCHE
EN INFORMATIQUE
ET EN AUTOMATIQUE

Class polynomials by Chinese remaindering

1. Complex multiplication in a nutshell
2. Complex numbers, complexity and class invariants
   - Complex algorithm and its complexity
   - Class invariants, the complex case
   - Class invariants and ramification
3. Chinese remaindering
   - Class polynomials by CRT
   - Impossibility of class invariants by CRT
   - Unique roots
   - Trace trick
   - Fricke involution
4. Timings

Cardinality of elliptic curves

- Goal: Construct $E/\mathbb{F}_p$ with N points
- Applications
  - ECC
  - Primality proving
  - Pairing-based crypto

Cardinality of elliptic curves

- Goal: Construct $E/\mathbb{F}_p$ with N points
- Applications
  - ECC
  - Primality proving
  - Pairing-based crypto
- Deuring 1941
  - $\mathrm{End}(E/\mathbb{C})$ is either $\mathbb{Z}$ (boring) or imaginary-quadratic order $\mathcal{O}_D = \left[1, \frac{D+\sqrt{D}}{2}\right]_{\mathbb{Z}}$ with $D < 0$ (CM curve)
  - $E/\mathbb{F}_p$ is the reduction mod p of a CM curve over $\Omega_D \subseteq \mathbb{C}$
  - $N = p + 1 - t$, $t = \pi + \overline{\pi}$ with Frobenius $\pi = \frac{t+v\sqrt{D}}{2} \in \mathcal{O}_D$

Cardinality of elliptic curves

- Goal: Construct $E/\mathbb{F}_p$ with N points
- Applications
  - ECC
  - Primality proving
  - Pairing-based crypto
- Deuring 1941
  - $\mathrm{End}(E/\mathbb{C})$ is either $\mathbb{Z}$ (boring) or imaginary-quadratic order $\mathcal{O}_D = \left[1, \frac{D+\sqrt{D}}{2}\right]_{\mathbb{Z}}$ with $D < 0$ (CM curve)
  - $E/\mathbb{F}_p$ is the reduction mod p of a CM curve over $\Omega_D \subseteq \mathbb{C}$
  - $N = p + 1 - t$, $t = \pi + \overline{\pi}$ with Frobenius $\pi = \frac{t+v\sqrt{D}}{2} \in \mathcal{O}_D$
- CM algorithm (sketch)
  - Fix D and p such that $4p = t^2 - v^2 D$, $N = p + 1 - t$ convenient
  - Compute $j(E)$, where E/Ω_D has CM by $\mathcal{O}_D$
  - $j_1 = j(E) \bmod p$
  - $c = \frac{j_1}{1728 - j_1}$, $a = 3c$, $b = 2c$, $\overline{E} : Y^2 = X^3 + aX + b$

Complex multiplication over the complex numbers

What are the curves $/\mathbb{C}$ with CM by $\mathcal{O}_D$?

- Modular functions $\mathbb{C}_\Gamma$
  - $f : \mathbb{C} \to \mathbb{C}$ with $f\left(\frac{az+b}{cz+d}\right) = f(z)$ for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma = \mathrm{Sl}_2(\mathbb{Z})$
  - f meromorphic, in particular "at ∞":

$$q = e^{2\pi i z},\ f(z) = \sum_{\nu=\nu_0} c_\nu q^\nu$$

  - $\mathbb{C}_\Gamma = \mathbb{C}(j)$, where

$$j(z) = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots$$

- Answer
  - $\mathfrak{a} = (\alpha_1, \alpha_2)$ ideal of $\mathcal{O}_D$ with basis quotient $\tau = \frac{\alpha_2}{\alpha_1}$
  - $j(\mathfrak{a}) := j(\tau)$
    - ★ Depends only on $\mathfrak{a}$, not on the basis
    - ★ Depends only on the class of $\mathfrak{a}$ modulo principal ideals

Curve with j-invariant $j(\mathfrak{a})$ has CM by $\mathcal{O}_D$, there are $h_D = |\mathrm{Cl}(\mathcal{O}_D)|$.

First main theorem of complex multiplication

$$\begin{array}{c} \Omega_D \\ | \\ K = \mathbb{Q}(\sqrt{D}) \\ | \\ \mathbb{Q} \end{array}$$

$\Omega_D =$ ring class field of $\mathcal{O}_D$

$$\sigma : \mathrm{Cl}(\mathcal{O}_D) \xrightarrow{\sim} \mathrm{Gal}(\Omega_D/K)$$

$$\boxed{\Omega_D = K(j(\mathfrak{a}))}$$

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

Class polynomials by Chinese remaindering

1. Complex multiplication in a nutshell
2. Complex numbers, complexity and class invariants
   - Complex algorithm and its complexity
   - Class invariants, the complex case
   - Class invariants and ramification
3. Chinese remaindering
   - Class polynomials by CRT
   - Impossibility of class invariants by CRT
   - Unique roots
   - Trace trick
   - Fricke involution
4. Timings

Algorithm

- Fix D and p such that $4p = t^2 - v^2 D$, $N = p + 1 - t$ convenient
- Compute $j(E)$, where E/Ω_D has CM by $\mathcal{O}_D$

- $j_1 = j(E) \bmod p$

- $c = \frac{j_1}{1728 - j_1}$, $a = 3c$, $b = 2c$, $\overline{E} : Y^2 = X^3 + aX + b$

Algorithm

- Fix D and p such that $4p = t^2 - v^2 D$, $N = p + 1 - t$ convenient
- Enumerate the h_D ideal classes of $\mathcal{O}_D$:

$$\left(A_i, \frac{-B_i + \sqrt{D}}{2} \right)$$

- Compute over $\mathbb{C}$ the class polynomial (Weber 1908)

$$H_D(x) = \prod_{i=1}^{h_D} \left(x - j \left(\frac{-B_i + \sqrt{D}}{2A_i} \right) \right) \in \mathbb{Z}[x]$$

- Find a root j_1 of $H_D \bmod p$
- $c = \frac{j_1}{1728 - j_1}$, $a = 3c$, $b = 2c$, $\overline{E} : Y^2 = X^3 + aX + b$

Complexity

- Size of H_D
  - Degree $h \in O^{\sim}\left(\sqrt{|D|}\right)$ (GRH, Littlewood 1928)
  - Coefficients with $O^{\sim}\left(\sqrt{|D|}\right)$ digits (Schoof 1991, E. 2009)
  - Total size $O^{\sim}(|D|)$
- Evaluation of j: $O^{\sim}\left(\sqrt{|D|}\right)$
  - Multievaluation of the "polynomial" j (E. 2009)
  - Arithmetic-geometric mean (Dupont 2006)
- Total complexity (E. 2009)

$O^{\sim}(|D|)$ — quasi-linear in the output size!

`http://cm.multiprecision.org/`

Couveignes–Henocq 2002, Bröker–Stevenhagen 2004:
canonical p-adic lift in quasi-linear time

Class polynomials by Chinese remaindering

1. Complex multiplication in a nutshell
2. Complex numbers, complexity and class invariants
   - Complex algorithm and its complexity
   - Class invariants, the complex case
   - Class invariants and ramification
3. Chinese remaindering
   - Class polynomials by CRT
   - Impossibility of class invariants by CRT
   - Unique roots
   - Trace trick
   - Fricke involution
4. Timings

Class invariants

- Modular functions $\mathbb{C}_{\Gamma^0(N)}$
  - Invariant under matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $N \mid b$
- Class invariants (Weber 1908)
  - $f(\tau) \in \Omega_D$
  - Schertz 2002: All primes dividing N split in $K = \mathbb{Q}(\sqrt{D})$
    "$\Rightarrow$" class invariant
- Modular polynomial $\Psi_f(X, Y) \in \mathbb{Z}[X, Y]$ s.t. $\Psi(f, j) = 0$

Class invariants

- Modular functions $\mathbb{C}_{\Gamma^0(N)}$
  - Invariant under matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $N \mid b$
- Class invariants (Weber 1908)
  - $f(\tau) \in \Omega_D$
  - Schertz 2002: All primes dividing N split in $K = \mathbb{Q}(\sqrt{D})$
    "$\Rightarrow$" class invariant
- Modular polynomial $\Psi_f(X, Y) \in \mathbb{Z}[X, Y]$ s.t. $\Psi(f, j) = 0$
- Algorithm
  - Compute over $\mathbb{C}$ the class polynomial

$$H_D(x) = \prod_{i=1}^{h_D} \left(x - j\left(\frac{-B_i + \sqrt{D}}{2A_i} \right) \right) \in \mathbb{Z}[x]$$

  - Find root j_1 of $H_D \bmod p$
  - Write down curve $\bmod p$ with j-invariant j_1

Class invariants

- Modular functions $\mathbb{C}_{\Gamma^0(N)}$
  - Invariant under matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $N \mid b$
- Class invariants (Weber 1908)
  - $f(\tau) \in \Omega_D$
  - Schertz 2002: All primes dividing N split in $K = \mathbb{Q}(\sqrt{D})$
    "$\Rightarrow$" class invariant
- Modular polynomial $\Psi_f(X, Y) \in \mathbb{Z}[X, Y]$ s.t. $\Psi(f, j) = 0$
- Algorithm
  - Compute over $\mathbb{C}$ the class polynomial

$$H_D^f(x) = \prod_{i=1}^{h_D} \left(x - f\left(\frac{-B_i + \sqrt{D}}{2A_i} \right) \right) \in \mathbb{Z}[x]$$

  - Find root f_1 of $H_D^f \bmod p$
  - Write down curve $\bmod p$ with j-invariant j_1

Class invariants

- Modular functions $\mathbb{C}_{\Gamma^0(N)}$
  - Invariant under matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $N \mid b$
- Class invariants (Weber 1908)
  - $f(\tau) \in \Omega_D$
  - Schertz 2002: All primes dividing N split in $K = \mathbb{Q}(\sqrt{D})$
    "$\Rightarrow$" class invariant
- Modular polynomial $\Psi_f(X, Y) \in \mathbb{Z}[X, Y]$ s.t. $\Psi(f, j) = 0$
- Algorithm
  - Compute over $\mathbb{C}$ the class polynomial

$$H_D^f(x) = \prod_{i=1}^{h_D} \left(x - f\left(\frac{-B_i + \sqrt{D}}{2A_i} \right) \right) \in \mathbb{Z}[x]$$

  - Find root f_1 of $H_D^f \bmod p$
  - Find root j_1 of $\Psi_f(f_1, Y) \bmod p$
  - Write down curve $\bmod p$ with j-invariant j_1

Class invariants

- Problem: $f(\mathfrak{a})$ depends on the choice of basis!
  - Shimura reciprocity
  - N-systems (Schertz 2002)
- Advantage: Gain of a constant height factor $c(f) = \frac{\deg_X \Psi_f}{\deg_Y \Psi_f}$
- Popular class invariants

$\gamma_2 = \sqrt[3]{j}$	3	Weber 1908
$\mathfrak{f}^e \approx \left(\frac{\eta\left(\frac{z}{2}\right)}{\eta(z)}\right)^e$	$\frac{72}{e} \leqslant 72$	Weber 1908
$\mathfrak{w}_p^e = \left(\frac{\eta\left(\frac{z}{p}\right)}{\eta(z)}\right)^e$	$\frac{24(p+1)}{e(p-1)} \leqslant 48$	E.–Morain 2009
$\mathfrak{w}_{p_1,p_2}^e = \left(\frac{\eta\left(\frac{z}{p_1}\right)\eta\left(\frac{z}{p_2}\right)}{\eta\left(\frac{z}{p_1 p_2}\right)\eta(z)}\right)^e$	$\frac{12(p_1+1)(p_2+1)}{e(p_1-1)(p_2-1)} \leqslant 37$	E.–Schertz 2004
$\mathfrak{w}_{p_1,\ldots,p_k}^e = \cdots$	$\frac{48(p_1+1)\cdots(p_k+1)}{2^k\, e(p_1-1)\cdots(p_k-1)}$	E.–Schertz 2010
A_p : optimal on $X_0^+(p)$	$\frac{p+1}{\deg_Y \Psi_{A_p}}$	Morain 2009

Class invariants

- Sutherland (?)
  - $\mathfrak{w}_{2,5}^6$: 9
  - $\mathfrak{w}_{2,5}$: 54
- Morain 2009, E.–Sutherland 2010, Elkies 2010
  - A_{71}: 36
  - A_p with $p \equiv 11 \pmod{60}$: $30\frac{p+1}{p-11} \to 30$
  - A_p with $p \equiv -1 \pmod{60}$: 30
- E.–Schertz 2010
  - $\mathfrak{w}_{2,3,13}$: 42
  - $\mathfrak{w}_{2,3,p}$ with $p \equiv 1 \pmod{12}$: $36\frac{p+1}{p-1} \to 36$
  - $\mathfrak{w}_{2,3,5}^3$: 18
  - $\mathfrak{w}_{2,3,5}$ (??): 54
  - $\mathfrak{w}_{2,3,7}^2$: 24
  - $\mathfrak{w}_{2,3,7}$ (??): 48

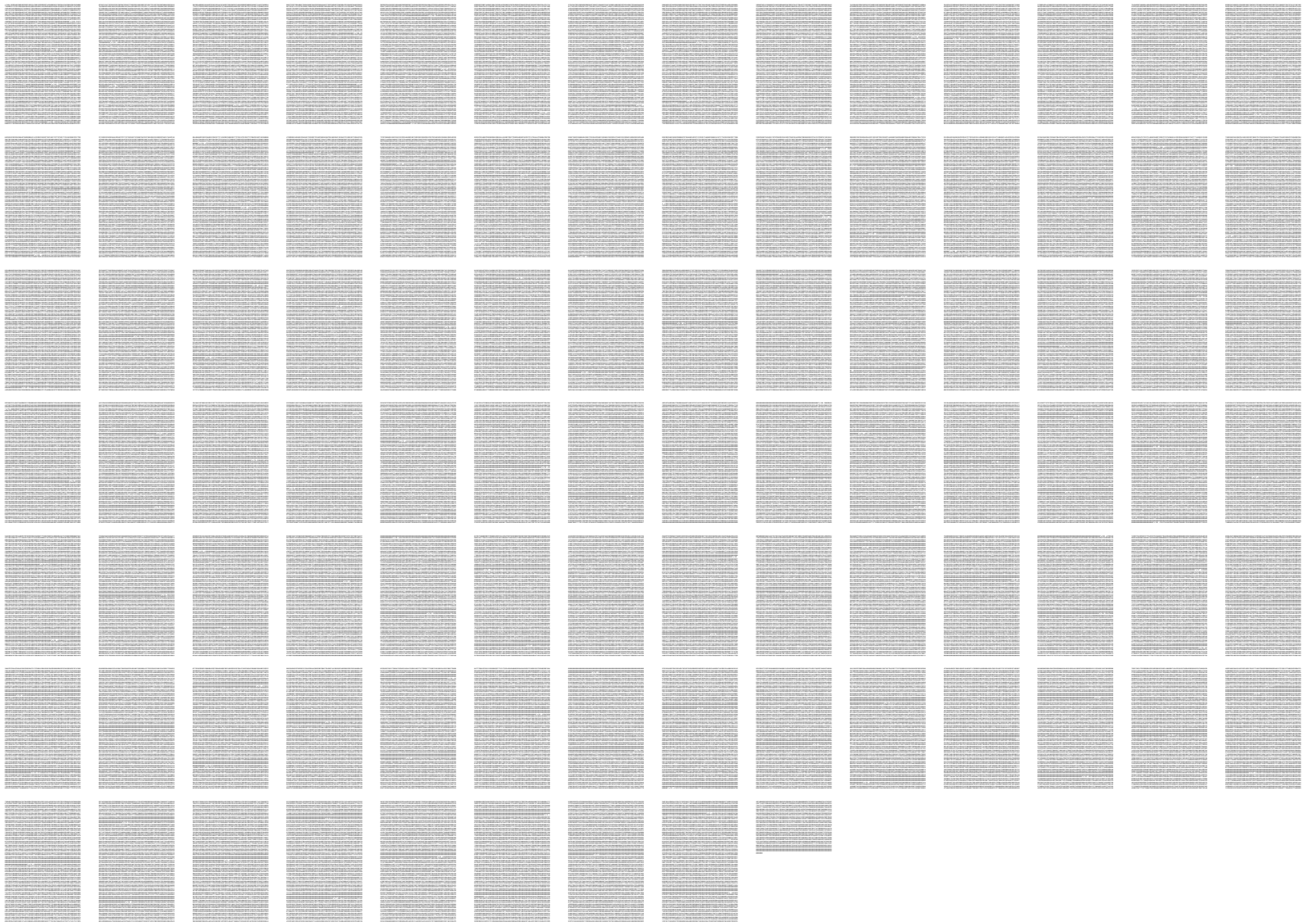
Corollary: For every D, there is an invariant f with $c(f) \geqslant 30$.

Size does matter

$$H_D$$

Visible universe

$D = -328020$, $h = 160$, height 11216 bits



Does size matter?

$$H_D$$

Visible universe

$H^{\mathfrak{w}_{2,3,13}}_{-328020}$, $h = 160$, height 290 bits

Class polynomials by Chinese remaindering

1. Complex multiplication in a nutshell
2. Complex numbers, complexity and class invariants
   - Complex algorithm and its complexity
   - Class invariants, the complex case
   - Class invariants and ramification
3. Chinese remaindering
   - Class polynomials by CRT
   - Impossibility of class invariants by CRT
   - Unique roots
   - Trace trick
   - Fricke involution
4. Timings

Direct construction of subfields of class fields

If $k' \leqslant k$ primes of a multiple eta quotient $\mathfrak{w}_{p_1,\ldots,p_k}$ divide D, then $H_D^{\mathfrak{w}_{p_1,\ldots,p_k}}$ is a $2^{k'-1}$-th power.

If p divides D, then $H_D^{A_p}$ is a square.

Source: Shimura reciprocity or Atkin–Lehner theory

E.–Pohst–Schertz 2005:
Verfahren zur Konstruktion elliptischer Kurven über endlichen Körpern, patent

E. 2007:
Courbes algébriques et cryptologie, habilitation, §1.6

E.–Schertz 2010:
Singular values of multiple eta-quotients for ramified primes

$\sqrt{H_{-328020}^{\mathfrak{w}_{2,3,13}}}$, $h' = 80$, height 144 bits

```
x^80 +2513913302*x^79 +108743202312028879805*x^78 +9514907308919833127374*x^77 +
736497124103211539025742*x^76-337121498099265358937969 50*x^75-878900057284354760
83782245*x^74 +4705458101993041519299689786*x^73 +9190655418900730775375 1564182*
x^72 +1053845476283819897082816524954*x^71 +96816809990369725575443434322 07*x^70
 +830420124533836743384 25159656514*x^69 +6946251065847976353002440331859 50*x^68
+542228219014556728125622752527 0526*x^67 +375820595248246783798380956129150 41*x^
66 +226629124381316587208016135465722870*x^65 +1190055302914206149911267700986 86
9171*x^64 +549522668950662651139786972765385006 8*x^63 +225853833427883509264090 5
6953676206822*x^62 +835908231159549753658995735394837668 12*x^61 +281464103045149
168438047733287244942996*x^60 +869631641893926796907710418002022870324*x^59 +248
264409697400408503060238731199438 1498*x^58 +658532851126119059091192635897777178
1420*x^57 +163023919223848227382378118606427076387 28*x^56 +377988821358019938655
979436056408534695 32*x^55 +823201828593301159147333075697015780795 74*x^54 +16879
067441589266552634680042878670643206 0*x^53 +326464813317539368745820762311235243
314388*x^52 +596555454699338175602457685971493666644604*x^51 +103121090756309969
849903499972041063954793 8*x^50 +168802099124179929015359274328036111643734 8*x^49
 +261882668648993261624820839032212603521 1325*x^48 +385325695163891385825165 6773
261530770565898*x^47 +537993532561927400738860367985415020759949 5*x^46 +71308617
951005720678644864384703011833466 18*x^45 +897576607817699992826061894302049773 99
34354*x^44 +107320066160543650230334738574126923063951 58*x^43 +121914825800421 77
706360501271299403588649865*x^42 +131600728693519597630582860221059492380917 82*x
^41 +134996232915256333758082135187990048772863 26*x^40 +131600728693519597630582
860221059492380917 82*x^39 +121914825800421777063605012712994035886498 65*x^38 +10
732006616054365023033473857412692306395158*x^37 +897576607817699992826061894302 0
497739934354*x^36 +713086179510057206786448643847030118334661 8*x^35 +53799353256
192740073886036798541502075994 95*x^34 +385325695163891385825165677326153077056 58
98*x^33 +261882668648993261624820839032212603521 1325*x^32 +168802099124179929015
359274328036111643734 8*x^31 +103121090756309969849903499972041063954793 8*x^30 +5
965554546993381756024576859714936666446 04*x^29 +326464813317539368745820762311 23
5243314388*x^28 +168790674415892665526346800428786706432060*x^27 +82320182859330
115914733307569701578079574*x^26 +377988821358019938655979436056408534695 32*x^25
 +163023919223848227382378118606427076387 28*x^24 +658532851126119059091192635897
7771781420*x^23 +248264409697400408503060238731199438 1498*x^22 +8696316418939267
969077104180020228703 24*x^21 +281464103045149168438047733287244942996*x^20 +8359
082311595497536589957353948376 6812*x^19 +225853833427883509264090569536762068 22*
x^18 +549522668950662651139786972765385006 8*x^17 +119005530291420614991126770098
6869171*x^16 +226629124381316587208016135465722870*x^15 +375820595248246783798 38
095612915041*x^14 +542228219014556728125622752527 0526*x^13 +694625106584797635300
0244033185950*x^12 +830420124533836743384 25159656514*x^11 +968168099903697255754
4343432207*x^10 +105384547628381989708 2816524954*x^9 +919065541890073077537515 64
182*x^8 +4705458101993041519299689786*x^7-878900057284354760837822 45*x^6-3371214
9809926535893796950*x^5 +736497124103211539025742*x^4 +951490730891983312737 4*x^
3 +108743202312028879805*x^2 +2513913302*x +1
```

$\sqrt[16]{H_{-328020}^{\mathfrak{w}_{2,3,5,7,11}}}$, $h' = 10$, height 31 bits

$$x^{10} - 8503232x^9 + 36794291x^8 + 24829894x^7 - 402996383x^6$$
$$-1303019142x^5 - 402996383x^4 + 24829894x^3 + 36794291x^2$$
$$-8503232x + 1$$

Class polynomials by Chinese remaindering

1. Complex multiplication in a nutshell
2. Complex numbers, complexity and class invariants
   - Complex algorithm and its complexity
   - Class invariants, the complex case
   - Class invariants and ramification
3. Chinese remaindering
   - Class polynomials by CRT
   - Impossibility of class invariants by CRT
   - Unique roots
   - Trace trick
   - Fricke involution
4. Timings

Agashe–Lauter–Venkatesan 2004

- Idea: compute $H_D(x) \bmod p$, lift to $\mathbb{Z}[x]$ by Chinese remaindering

Agashe–Lauter–Venkatesan 2004

- Idea: compute $H_D(x) \bmod p$, lift to $\mathbb{Z}[x]$ by Chinese remaindering
- Choose small primes p s.t. $4p = t^2 - v^2 D$,
  $$\prod p > 2 \max(\text{coeff. of } H_D)$$
- For each p:
  - Enumerate all $j_i \in \mathbb{F}_p$.
  - Write down a curve $E_i/\mathbb{F}_p$ with invariant j_i.
  - Verify whether $\mathrm{End}(E_i) = \mathcal{O}_D$, otherwise drop j_i:
    - Verify whether $\#E_i(\mathbb{F}_p) = p + 1 \pm t$
    - Compute $\mathcal{O}_{v^2 D} \subseteq \mathrm{End}(E_i) \subseteq \mathcal{O}_\Delta$ (Kohel 1996, Fouquet–Morain 2002)
  - $H_D \bmod p = \prod_{h \text{ values}} (x - j_i)$
- Chinese remaindering

Complexity

- Number of p
  - $n \in O^{\sim}\left(\sqrt{|D|}\right)$ precision in bits
  - $p \in O^{\sim}(|D|)$
  - $\Rightarrow \#p \in O^{\sim}\left(\sqrt{|D|}\right)$
- Time per p
  - $O^{\sim}(p) = O^{\sim}(|D|)$

$O^{\sim}\left(|D|^{3/2}\right)$, slower than the complex algorithm!

Belding–Bröker–Enge–Lauter 2008

- Choose small primes p s.t. $4p = t^2 - v^2 D$,
  $$\prod p > 2 \max(\text{coeff. of } H_D)$$
- For each p:
  - Find one $j_1 \in \mathbb{F}_p$ with $\mathrm{End}(E_1) = \mathcal{O}_D$.
  - Enumerate all other $j_i \in \mathbb{F}_p$ with $\mathrm{End}(E_i) = \mathcal{O}_D$ using isogenies:
    If $j_1 = j(\mathfrak{a}) \bmod p$ and $\mathfrak{l} \in \mathrm{Cl}(\mathcal{O}_D)$ of norm ℓ, then
    - ★ $j(\mathfrak{a}\mathfrak{l}^{-1})$ is a root of the modular polynomial $\Phi_\ell(j(\mathfrak{a}), Y)$
    - ★ $j_2 = j(\mathfrak{a}\mathfrak{l}^{-1}) \bmod p$ is a root of $\Phi_\ell(j_1, Y) \bmod p$

    Using several (small) generators $\mathfrak{l}$ of $\mathrm{Cl}(\mathcal{O}_D)$ yields all j_i.
  - $H_D \bmod p_k = \prod_{h \text{ values}} (x - j_i)$
- Chinese remaindering

Complexity

- Find one good j_1
  $\#$ good $j_1 = h$

$$\boxed{\frac{p}{h} = \frac{O^{\sim}(|D|)}{O^{\sim}\left(\sqrt{|D|}\right)} = O^{\sim}\left(\sqrt{|D|}\right)}$$

- GRH: $\ell \in O(\log^2 |D|) \subseteq O^{\sim}(1)$
- Time per p for all j_i: $O^{\sim}(h) = O^{\sim}\left(\sqrt{|D|}\right)$
- Total complexity for all p

$$\boxed{O^{\sim}(|D|)}$$

Example: $D = -823$, $h = 9$

- $p = 827$: $4p = 4^2 + 2^2 \cdot 823$
- $j_1 = 14$
- $\mathrm{Cl} = \langle \mathfrak{l} \rangle$, $\mathfrak{l}$ of norm 2
- $\mathrm{Cl} = \langle \mathfrak{l}_1, \mathfrak{l}_2 \rangle$, $\mathfrak{l}_1^3 \sim 1$ (norm 31), $\mathfrak{l}_2^{-3} \sim \mathfrak{l}_1$ (norm 53)

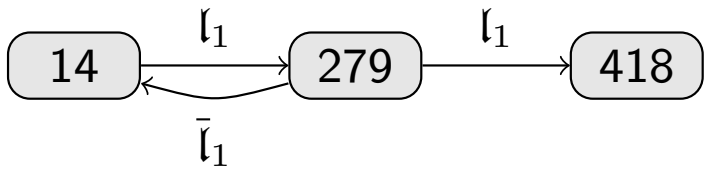
14

Example: $D = -823$, $h = 9$

- $p = 827$: $4p = 4^2 + 2^2 \cdot 823$
- $j_1 = 14$
- $\mathrm{Cl} = \langle \mathfrak{l} \rangle$, $\mathfrak{l}$ of norm 2
- $\mathrm{Cl} = \langle \mathfrak{l}_1, \mathfrak{l}_2 \rangle$, $\mathfrak{l}_1^3 \sim 1$ (norm 31), $\mathfrak{l}_2^{-3} \sim \mathfrak{l}_1$ (norm 53)

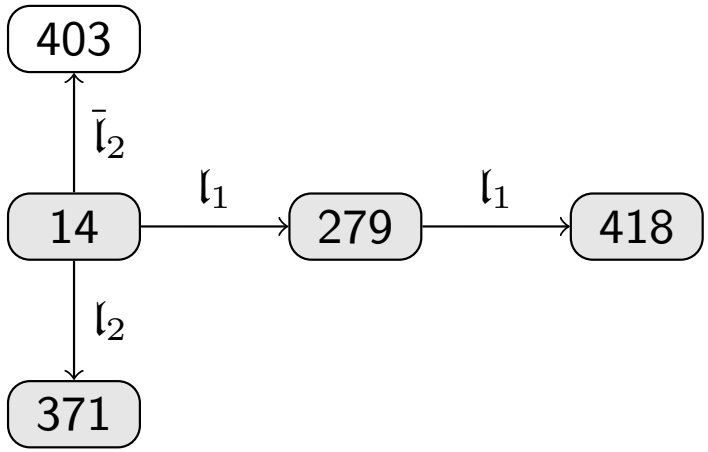
Example: $D = -823$, $h = 9$

- $p = 827$: $4p = 4^2 + 2^2 \cdot 823$
- $j_1 = 14$
- $\mathrm{Cl} = \langle \mathfrak{l} \rangle$, $\mathfrak{l}$ of norm 2
- $\mathrm{Cl} = \langle \mathfrak{l}_1, \mathfrak{l}_2 \rangle$, $\mathfrak{l}_1^3 \sim 1$ (norm 31), $\mathfrak{l}_2^{-3} \sim \mathfrak{l}_1$ (norm 53)



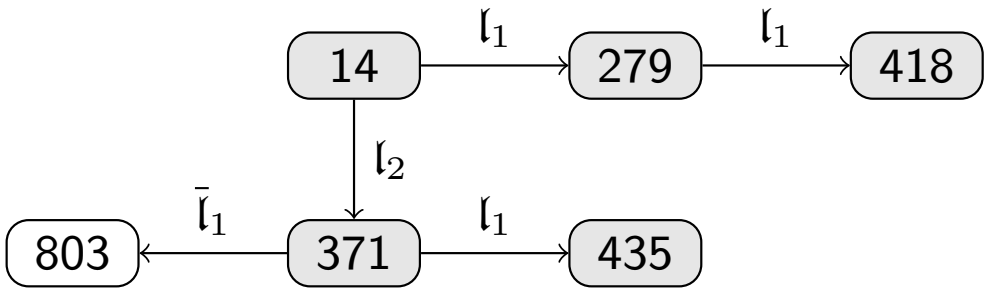
Example: $D = -823$, $h = 9$

- $p = 827$: $4p = 4^2 + 2^2 \cdot 823$
- $j_1 = 14$
- $\mathrm{Cl} = \langle \mathfrak{l} \rangle$, $\mathfrak{l}$ of norm 2
- $\mathrm{Cl} = \langle \mathfrak{l}_1, \mathfrak{l}_2 \rangle$, $\mathfrak{l}_1^3 \sim 1$ (norm 31), $\mathfrak{l}_2^{-3} \sim \mathfrak{l}_1$ (norm 53)



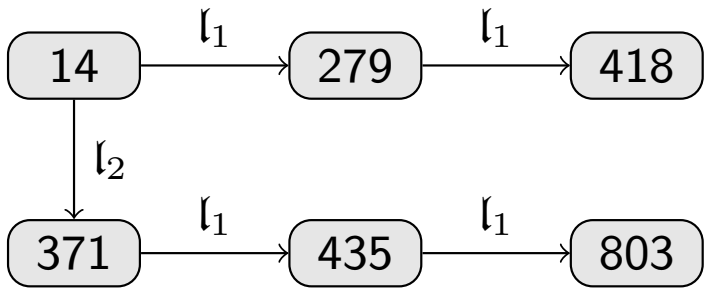
Example: $D = -823$, $h = 9$

- $p = 827$: $4p = 4^2 + 2^2 \cdot 823$
- $j_1 = 14$
- $\mathrm{Cl} = \langle \mathfrak{l} \rangle$, $\mathfrak{l}$ of norm 2
- $\mathrm{Cl} = \langle \mathfrak{l}_1, \mathfrak{l}_2 \rangle$, $\mathfrak{l}_1^3 \sim 1$ (norm 31), $\mathfrak{l}_2^{-3} \sim \mathfrak{l}_1$ (norm 53)



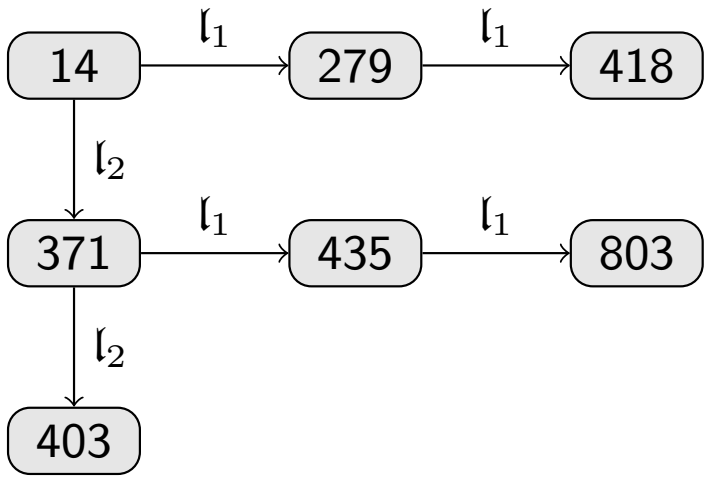
Example: $D = -823$, $h = 9$

- $p = 827$: $4p = 4^2 + 2^2 \cdot 823$
- $j_1 = 14$
- $\mathrm{Cl} = \langle \mathfrak{l} \rangle$, $\mathfrak{l}$ of norm 2
- $\mathrm{Cl} = \langle \mathfrak{l}_1, \mathfrak{l}_2 \rangle$, $\mathfrak{l}_1^3 \sim 1$ (norm 31), $\mathfrak{l}_2^{-3} \sim \mathfrak{l}_1$ (norm 53)



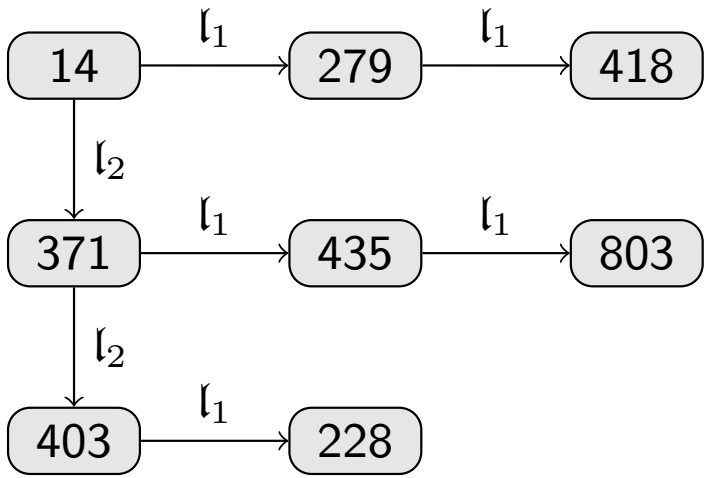
Example: $D = -823$, $h = 9$

- $p = 827$: $4p = 4^2 + 2^2 \cdot 823$
- $j_1 = 14$
- $\mathrm{Cl} = \langle \mathfrak{l} \rangle$, $\mathfrak{l}$ of norm 2
- $\mathrm{Cl} = \langle \mathfrak{l}_1, \mathfrak{l}_2 \rangle$, $\mathfrak{l}_1^3 \sim 1$ (norm 31), $\mathfrak{l}_2^{-3} \sim \mathfrak{l}_1$ (norm 53)



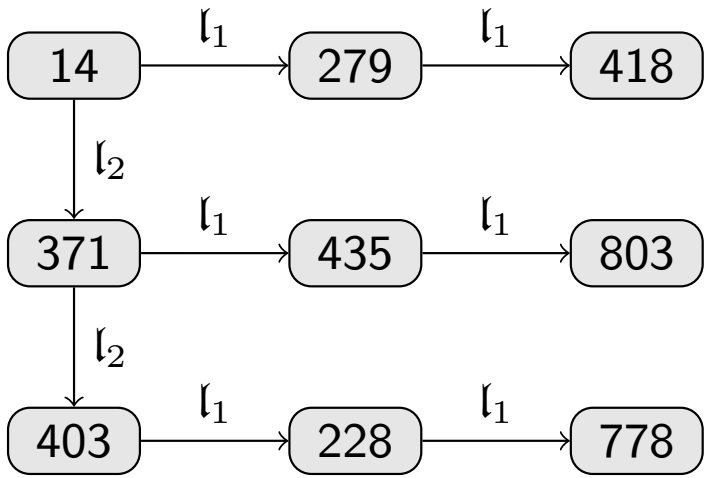
Example: $D = -823$, $h = 9$

- $p = 827$: $4p = 4^2 + 2^2 \cdot 823$
- $j_1 = 14$
- $\mathrm{Cl} = \langle \mathfrak{l} \rangle$, $\mathfrak{l}$ of norm 2
- $\mathrm{Cl} = \langle \mathfrak{l}_1, \mathfrak{l}_2 \rangle$, $\mathfrak{l}_1^3 \sim 1$ (norm 31), $\mathfrak{l}_2^{-3} \sim \mathfrak{l}_1$ (norm 53)



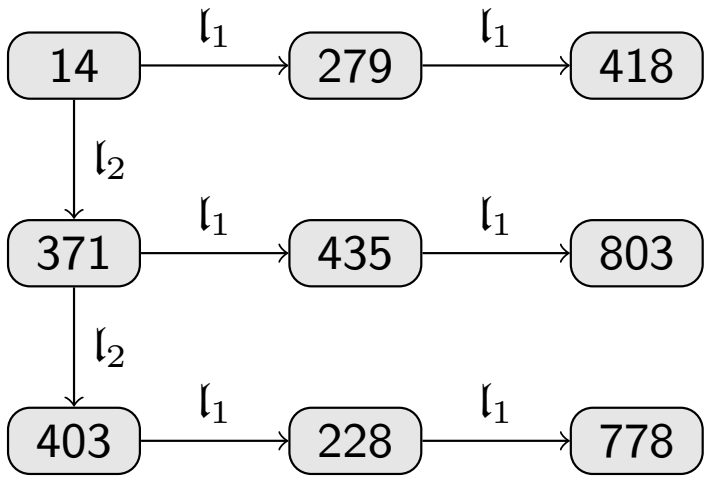
Example: $D = -823$, $h = 9$

- $p = 827$: $4p = 4^2 + 2^2 \cdot 823$
- $j_1 = 14$
- $\mathrm{Cl} = \langle \mathfrak{l} \rangle$, $\mathfrak{l}$ of norm 2
- $\mathrm{Cl} = \langle \mathfrak{l}_1, \mathfrak{l}_2 \rangle$, $\mathfrak{l}_1^3 \sim 1$ (norm 31), $\mathfrak{l}_2^{-3} \sim \mathfrak{l}_1$ (norm 53)



Example: $D = -823$, $h = 9$

- $p = 827$: $4p = 4^2 + 2^2 \cdot 823$
- $j_1 = 14$
- $\mathrm{Cl} = \langle \mathfrak{l} \rangle$, $\mathfrak{l}$ of norm 2
- $\mathrm{Cl} = \langle \mathfrak{l}_1, \mathfrak{l}_2 \rangle$, $\mathfrak{l}_1^3 \sim 1$ (norm 31), $\mathfrak{l}_2^{-3} \sim \mathfrak{l}_1$ (norm 53)



$H_{-823}(X) \bmod 827 =$
$x^9+406x^8+247x^7+738x^6+333x^5+486x^4+26x^3+391x^2+78x+243$

Implementations

- E. in Belding–Bröker–E.–Lauter 2008
  - Finding a curve talkes longer than the full complex algorithm...

Implementations

- E. in Belding–Bröker–E.–Lauter 2008
  - Finding a curve talkes longer than the full complex algorithm...
- Sutherland 2009
  - Big v — many curves with $\mathcal{O}_{v^2 D} \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_\Delta$
  - Families of curves with large known torsion – factor 15
  - Uses $\ell \mid v$ for enumeration
- Space complexity by "explicit CRT" (Sutherland 2009)

$$\tilde{O}\left(\sqrt{|D|}\log P\right) \text{ for } H_D \bmod P$$

Implementations

- E. in Belding–Bröker–E.–Lauter 2008
  - Finding a curve talkes longer than the full complex algorithm...
- Sutherland 2009
  - Big v — many curves with $\mathcal{O}_{v^2 D} \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_\Delta$
  - Families of curves with large known torsion – factor 15
  - Uses $\ell \mid v$ for enumeration
- Space complexity by "explicit CRT" (Sutherland 2009)

$$\tilde{O}\left(\sqrt{|D|}\log P\right) \text{ for } H_D \bmod P$$

- Record $\bmod P$
  - $D = -170\ 868\ 609\ 071$
  - $h = 1\ 000\ 000$
  - $1\ 970\ 000$ s $= 228$ d CPU time (Athlon 2.4 GHz)
  - 11.2 TB if computed over $\mathbb{Z}$
- Beats complex algorithm for $h \geqslant 100\ 000$

Class polynomials by Chinese remaindering

1. Complex multiplication in a nutshell
2. Complex numbers, complexity and class invariants
   - Complex algorithm and its complexity
   - Class invariants, the complex case
   - Class invariants and ramification
3. Chinese remaindering
   - Class polynomials by CRT
   - Impossibility of class invariants by CRT
   - Unique roots
   - Trace trick
   - Fricke involution
4. Timings

Concrete nonsense

- Modular functions f are not defined modulo p
  - $\mathbb{F}_p$?
  - $\mathbb{Q}_p$?
  - $\mathbb{C}_p$?

Abstract nonsense

- Concrete sense
  - $H_D^f(x) \in \mathbb{Z}[x]$ is defined mod p
  - H_D^f has h roots $f_1, \ldots, f_h \in \mathbb{F}_p$

Abstract nonsense

- Concrete sense
  - $H_D^f(x) \in \mathbb{Z}[x]$ is defined mod p
  - H_D^f has h roots $f_1, \ldots, f_h \in \mathbb{F}_p$
- Moduli spaces
  - j_i are j-invariants of elliptic curves with CM by $\mathcal{O}_D$
  - f_i give the moduli space of curves with torsion structure – so what?

Abstract nonsense

- Concrete sense
  - $H_D^f(x) \in \mathbb{Z}[x]$ is defined mod p
  - H_D^f has h roots $f_1, \ldots, f_h \in \mathbb{F}_p$
- Moduli spaces
  - j_i are j-invariants of elliptic curves with CM by $\mathcal{O}_D$
  - f_i give the moduli space of curves with torsion structure – so what?
- Concrete (non-)sense
  - f_i is a root of $\Psi_f(X, j_i) \bmod p$
  - Twofold combinatorial explosion
    - ★ Which root for any j_i?
    - ★ Which root across the p?

Abstract nonsense

- Concrete sense
  - $H_D^f(x) \in \mathbb{Z}[x]$ is defined mod p
  - H_D^f has h roots $f_1, \ldots, f_h \in \mathbb{F}_p$
- Moduli spaces
  - j_i are j-invariants of elliptic curves with CM by $\mathcal{O}_D$
  - f_i give the moduli space of curves with torsion structure – so what?
- Concrete (non-)sense
  - f_i is a root of $\Psi_f(X, j_i) \bmod p$
  - Twofold combinatorial explosion
    - ⋆ Which root for any j_i?
    - ⋆ Which root across the p?

Unmögliches wird sofort erledigt, Wunder dauern etwas länger.

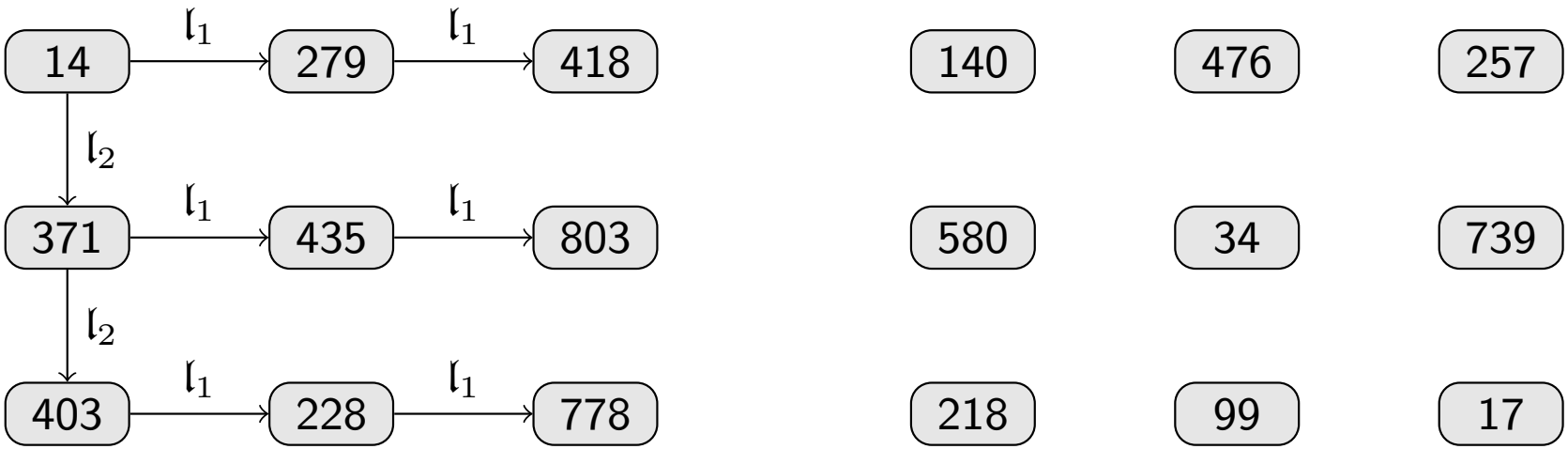
(joint work with A. Sutherland, ANTS-IX)

Class polynomials by Chinese remaindering

1. Complex multiplication in a nutshell
2. Complex numbers, complexity and class invariants
   - Complex algorithm and its complexity
   - Class invariants, the complex case
   - Class invariants and ramification
3. Chinese remaindering
   - Class polynomials by CRT
   - Impossibility of class invariants by CRT
   - Unique roots
   - Trace trick
   - Fricke involution
4. Timings

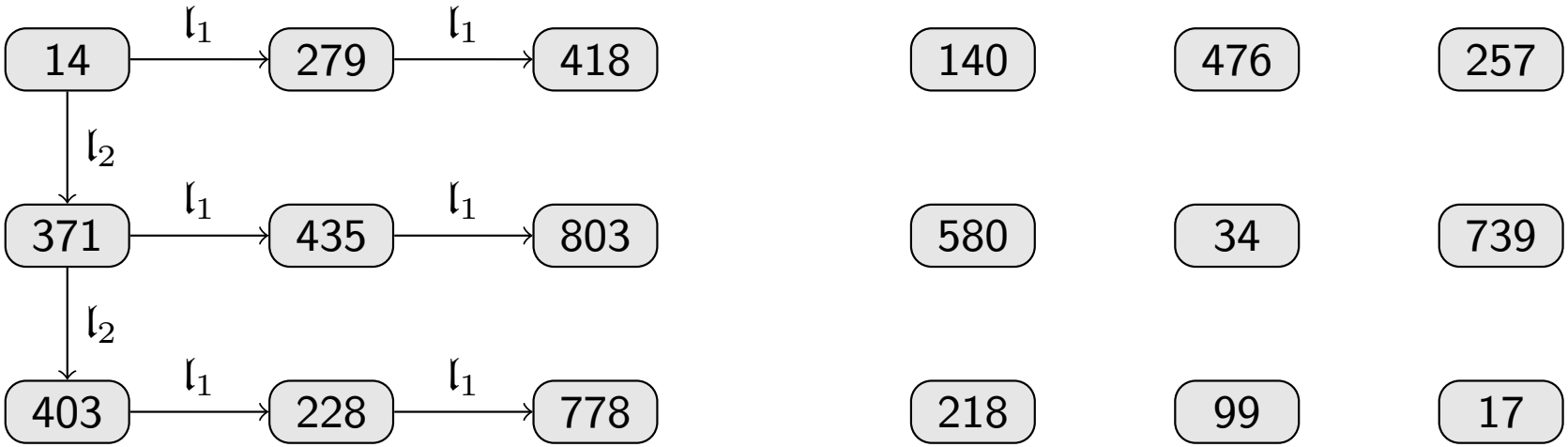
Forcing unicity of roots

- $\gamma_2 = \sqrt[3]{j}$, $\Psi_{\gamma_3} = X^3 - Y$
  - $p \equiv 2 \pmod 3 \Rightarrow f_i = \sqrt[3]{j_i} =$ root of $\Psi_f(X, j_i)$



Forcing unicity of roots

- $\gamma_2 = \sqrt[3]{j}$, $\Psi_{\gamma_3} = X^3 - Y$
  - $p \equiv 2 \pmod 3 \Rightarrow f_i = \sqrt[3]{j_i} =$ root of $\Psi_f(X, j_i)$



- Weber-$\mathfrak{f}$: $j = \left(\frac{\mathfrak{f}^{24}+16}{\mathfrak{f}^8}\right)^3$, $\Psi_{\mathfrak{f}} = X^{24}\,Y - (X^{24}+16)^3$
  - $\mathfrak{f}^2$ when $p \equiv 11 \pmod{12}$ and $\mathfrak{f}$ is class invariant
- Useful trick
  - f_1 from j_1
  - Direct enumeration: f_2 as root of relative modular polynomial $\Phi_\ell^f(f_1, Y)$
  - Exist for a finite number of functions ("Hauptmoduln")

Class polynomials by Chinese remaindering

1. Complex multiplication in a nutshell
2. Complex numbers, complexity and class invariants
   - Complex algorithm and its complexity
   - Class invariants, the complex case
   - Class invariants and ramification
3. Chinese remaindering
   - Class polynomials by CRT
   - Impossibility of class invariants by CRT
   - Unique roots
   - Trace trick
   - Fricke involution
4. Timings

Example: Weber-$\mathfrak{f}$ and $p \equiv 11 \pmod{12}$

$\Psi_{\mathfrak{f}} = X^{24}Y - (X^{24} + 16)^3$

- Two roots f_i and $f_i' = -f_i$
- 2^h combinations, but...
- Direct enumeration yields

$$H_D^f(x), H_D^{-f}(x) \bmod p$$

$$H_{-823}^{\pm\mathfrak{f}} \bmod 827 = x^9 \pm 29x^8 - 36^7 \pm 30x^6 - 33x^5 \pm 30x^4 - 12x^3 - x \pm 1$$

- If h odd and coefficient ± 1, choose sign $+1$ consistently for all p.
- Generalises to arbitrary numbers of roots
  - Take trace t (or other coefficient).
  - Compute elementary symmetric functions of t, $t', \ldots \bmod p$
  - Lift to $\mathbb{Z}$, fix $t \in \mathbb{Z}$

Class polynomials by Chinese remaindering

1. Complex multiplication in a nutshell
2. Complex numbers, complexity and class invariants
   - Complex algorithm and its complexity
   - Class invariants, the complex case
   - Class invariants and ramification
3. Chinese remaindering
   - Class polynomials by CRT
   - Impossibility of class invariants by CRT
   - Unique roots
   - Trace trick
   - Fricke involution
4. Timings

Fricke involution

Function for $\Gamma_0^+(N)$: invariant under $W_N : z \mapsto \frac{-N}{z}$

- A_p: $N = p$
- $\mathfrak{w}_{p_1,\ldots,p_k}$: $N = p_1 \cdots p_k$

Lemma:

- f for $\Gamma_0^+(N)$
- $\mathfrak{n}$ ideal of $\mathcal{O}_D$ of norm N
- $+$ technical conditions

Then

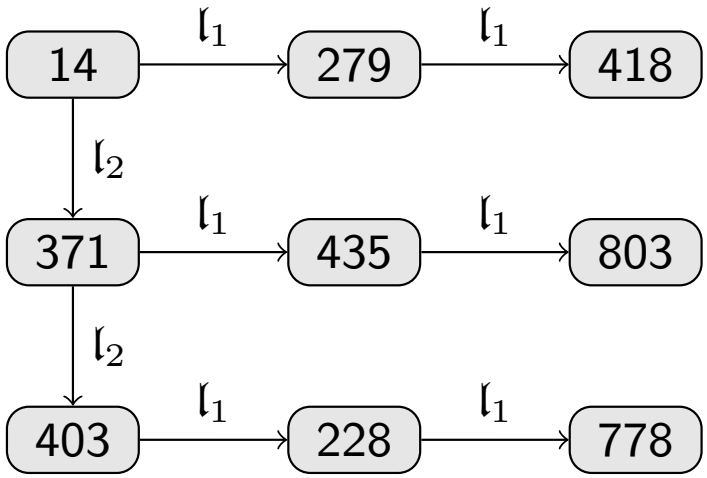
$$\Psi_f(f(\mathfrak{a}), j(\mathfrak{a})) = 0 \quad \text{and} \quad \Psi_f\left(f(\mathfrak{a}), j(\mathfrak{a})^{\sigma(\mathfrak{n})}\right) = 0$$

Mod p:

$$f_i \text{ is (unique?!) root of } \gcd\left(\Psi_f(X, j_i), \Psi_f\left(X, j_i^{\sigma(\mathfrak{n})}\right)\right)$$

Computing $j^{\sigma(\mathfrak{n})}$ — gobelins

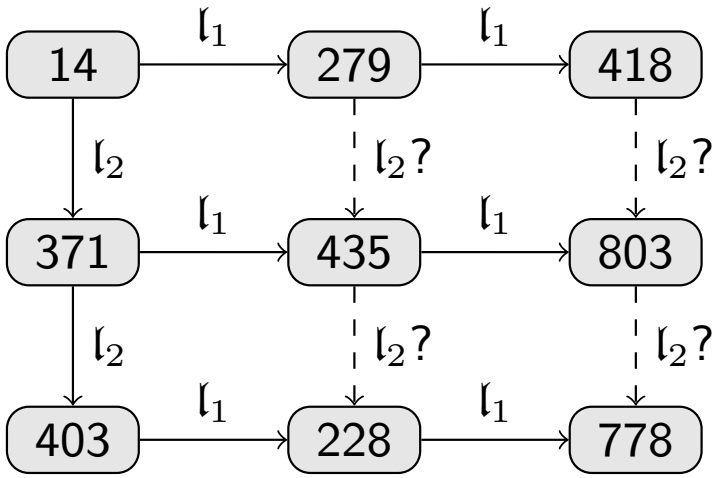
- $j^{\sigma(\mathfrak{n})}$ is N-isogenous to j
  - N may be large
  - N may be composite: 2^k possibilities
- Write $\mathfrak{n} = \mathfrak{l}_1^{e_1}\mathfrak{l}_2^{e_2}$



- Weave isolated threads into consistent tapestry

Computing $j^{\sigma(\mathfrak{n})}$ — gobelins

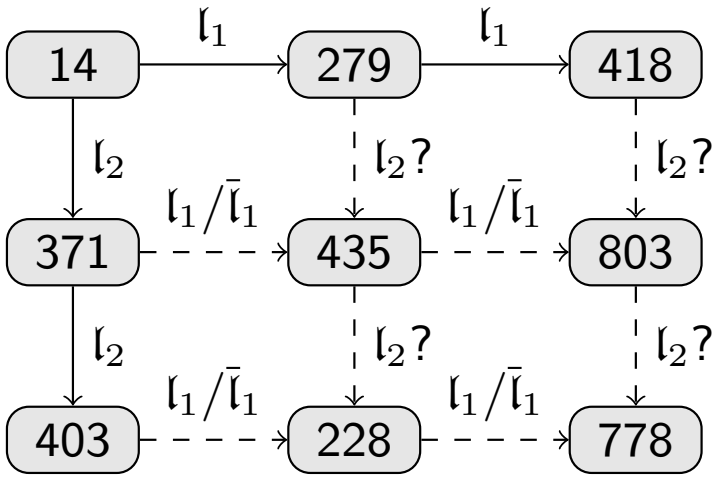
- $j^{\sigma(\mathfrak{n})}$ is N-isogenous to j
  - N may be large
  - N may be composite: 2^k possibilities
- Write $\mathfrak{n} = \mathfrak{l}_1^{e_1}\mathfrak{l}_2^{e_2}$



- Weave isolated threads into consistent tapestry

Computing $j^{\sigma(\mathfrak{n})}$ — gobelins

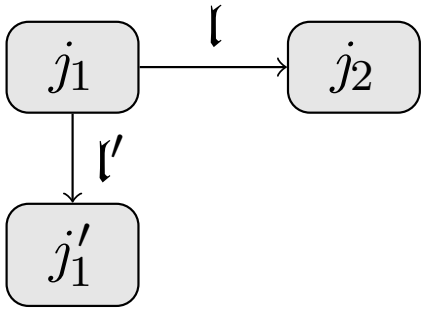
- $j^{\sigma(\mathfrak{n})}$ is N-isogenous to j
  - N may be large
  - N may be composite: 2^k possibilities
- Write $\mathfrak{n} = \mathfrak{l}_1^{e_1}\mathfrak{l}_2^{e_2}$



- Weave isolated threads into consistent tapestry

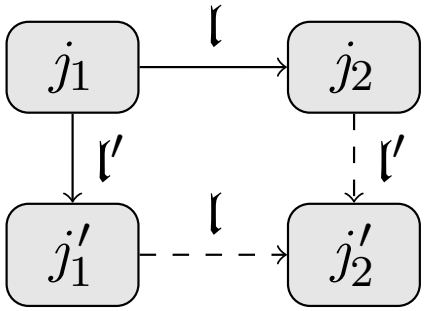
Computing $j^{\sigma(\mathfrak{n})}$ — gobelins

- Weave isolated threads into consistent tapestry



Computing $j^{\sigma(\mathfrak{n})}$ — gobelins

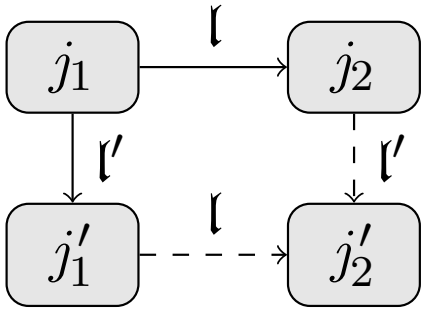
- Weave isolated threads into consistent tapestry



j_2' is (unique!) root of $\gcd\left(\Phi_\ell(j_1', Y), \Phi_{\ell'}(j_2, Y)\right)$

Computing $j^{\sigma(\mathfrak{n})}$ — gobelins

- Weave isolated threads into consistent tapestry

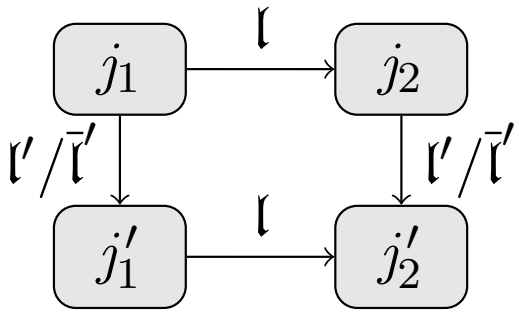


j_2' is (unique!) root of $\gcd\left(\Phi_\ell(j_1', Y), \Phi_{\ell'}(j_2, Y)\right)$

Gcds are faster than roots!

Computing $j^{\sigma(\mathfrak{n})}$ — signs

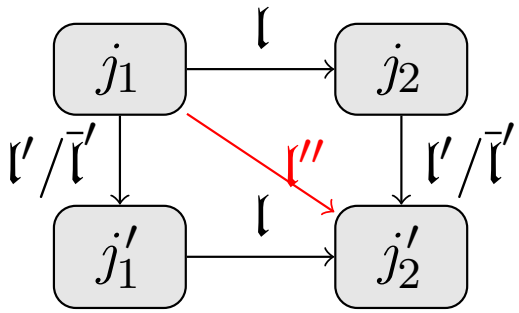
- Remaining problem: Distinguish $\mathfrak{l}'$ and $\bar{\mathfrak{l}}'$



- Solution: Elkies kernel polynomials as in SEA
- Fast solution:
  Choose $\mathfrak{l}'' \sim \mathfrak{l}\mathfrak{l}'$ and check whether $\Phi_{\ell''}(j_1, j_2') = 0$

Computing $j^{\sigma(\mathfrak{n})}$ — signs

- Remaining problem: Distinguish $\mathfrak{l}'$ and $\bar{\mathfrak{l}}'$



- Solution: Elkies kernel polynomials as in SEA
- Fast solution:
  Choose $\mathfrak{l}'' \sim \mathfrak{l}\mathfrak{l}'$ and check whether $\Phi_{\ell''}(j_1, j_2') = 0$

Class polynomials by Chinese remaindering

1. Complex multiplication in a nutshell
2. Complex numbers, complexity and class invariants
   - Complex algorithm and its complexity
   - Class invariants, the complex case
   - Class invariants and ramification
3. Chinese remaindering
   - Class polynomials by CRT
   - Impossibility of class invariants by CRT
   - Unique roots
   - Trace trick
   - Fricke involution
4. Timings

Trading roots for gcds

$\lvert D\rvert$	13569850003	12042704347
$h(D)$	20203	9788
height bound	2272564	1207412
$\ell_1^{e_1}, \ldots$	7^{20203}	$29^{2447}, 31^2, 43^2$
H_D time	19900	42400
H_D time (gcds)	15900	25300

Times in CPU seconds (3.0 GHz AMD Phenom II)

Class invariants

$\lvert D\rvert$	13569850003	12042704347
$h(D)$	20203	9788
height bound	2272564	1207412
$\ell_1^{e_1}, \ldots$	7^{20203}	$29^{2447}, 31^2, 43^2$
f	A_{71}	A_{59}
H_D time	19900	42400
H_D time (gcds)	15900	25300
H_D^f time	213	191
size factor	36	120^*
total speedup	**93**	**222**

Times in CPU seconds (3.0 GHz AMD Phenom II)

Chinese remaindering vs. floating point

		complex analytic		CRT		CRT mod P	
$\lvert D\rvert$	$h(D)$	$\mathfrak{w}_{3,13}$	$\mathfrak{f}$	$\mathfrak{w}_{3,13}$	$\mathfrak{f}$	$\mathfrak{w}_{3,13}$	$\mathfrak{f}$
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

- over $\mathbb{Z}$;
- modulo a 256-bit prime P.

Record class polynomial

We computed $\sqrt{H_D^{A_{71}}}$ using the discriminant D with

$$|D| = 1\ 000\ 000\ 013\ 079\ 299 > 10^{15}.$$

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 an imaginary quadratic order with class number

$$h(D) = 10\ 034\ 174 > 10^7.$$

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 10 000 000.*

   . . .

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

Not any more.