Elliptic curves with complex multiplication: history and computations

F. Morain

Laboratoire d'Informatique de l'École polytechnique

ÉCOLE POLYTECHNIQUE ParisTech CNRS INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE INRIA centre de recherche SACLAY - ÎLE-DE-FRANCE

ECC2010 – Redmond (WA), October 18, 2010

Corrected and improved after the talk (2010/10/26 version)

Contents

I. History.

II. A review of classical theory.

III. Using CM.

IV. Modular curves and class invariants.

I. History

Gauß, Abel, Eisentein, Kronecker, Klein, Weber, Watson, Fueter, Takagi, Hasse, Deuring, Weil, Shimura, etc.

See *Kronecker's Jugendtraum and modular functions*, by S. G. Vlăduţ.

A new era

Schoof (1985):

- gives the first polynomial time deterministic algorithm for computing $\#E(\mathbb{F}_q)$, using $O((\log p)^8)$ bit operations;
- for marketing reasons, he applies it to a known case, thereby obtaining the striking result that $\sqrt{-1} \bmod p$ can be computed in the same time.
- The same article contains this marvelous algorithm and everything you need to understand CM theory!

A new era (cont'd)

The same year:

- H. W. Lenstra, Jr. invents ECM (soon implemented with great successes);
- Bosma introduces elliptic Mersenne primes (for $\mathbb{Z}[i]$, $\mathbb{Z}[\rho]$);
- Chudnovsky & Chudnovsky write an IBM report investigating many aspects of elliptic curves over finite fields.

1986:

- Primality proving: two independent threads
  - Atkin proposes to use CM curves to get a usable primality proving algorithm, tried with success on Cunningham prp's not proven by Cohen/Lenstra.
  - Goldwasser & Kilian are close to proving **isPrime?** is in RP (this is eventually done by Adleman & Huang using hyperelliptic curves).
- Miller, Koblitz invent (independently) elliptic curve cryptography.

A fundamental dichotomy

If you want to do ECC, then you need a curve. . . !

Two choices:

- look for a random curve $E/\mathbb{F}_p$ and compute its cardinality (or other properties) using Schoof's algorithms (and its improvements); rather slow.
- build E as the reduction of some CM curve defined over some K_D; faster. You get $\#E$, but do these CM properties endanger the corresponding cryptosystems?

II. A review of the classical theory

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

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

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

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

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 $\sim Cl(\mathcal{O})$ and therefore $[K_D : K] = h(\mathcal{O})$. Moreover:

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

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

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

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

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

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

$\Rightarrow p = x^2 + y^2$ 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!

Elliptic curves with CM

Def. $E/\mathbb{C}$ has complex multiplication iff its ring of endomorphisms is greater than $\mathbb{Z}$ (all $[n]$ belong to $\mathrm{End}(E)$).

Thm. $E/\mathbb{C}$ has CM iff $\mathrm{End}(E) \sim \mathcal{O}$, an order in some imaginary quadratic K.

Ex. $E : Y^2 = X^3 + X$ has CM by $\mathbb{Z}[i]$.

Thm. $E/\mathbb{C}$ has CM iff $j(E)$ is a root of $H_D(X)$ for some D.

Elliptic curves over finite fields

Thm. $E/\mathbb{F}_p$ has always CM (due to the Frobenius: $(X, Y) \mapsto (X^p, Y^p)$).

Thm. (Hasse) $\#E(\mathbb{F}_p) = p + 1 - t$, $|t| \leq 2\sqrt{p}$.

Thm. (Deuring) given $|t|$, there exists $E/\mathbb{F}_p$ s.t. $\#E = p + 1 - t$, obtainable as the reduction of $\mathcal{E}/\mathbf{K}_D$ modulo a factor of (p) in K_D, where $D = t^2 - 4p = mD_K$.

But:

- no general formula for $\#E$ except in some special cases (small CM, E obtained by reduction).
- no efficient way for finding E given t except in some special cases (CM again).

Rem. (Partially) generalizable to $q = p^n$.

III. Using CM

A) A tribute to the pioneer

Thm. (Schoof) $\sqrt{-1} \bmod p$ can be computed in deterministic polynomial time $O((\log p)^8)$ (resp. $\tilde{O}((\log p)^5)$).

Proof: compute the cardinality of $E : Y^2 = X^3 + X$, which we know is $p + 1 - 2u$ where $p = u^2 + v^2$. Deduce v and $-1 \equiv (u/v)^2 \bmod p$. $\square$

Claim: we can improve this to $O((\log p)^6)$ or $\tilde{O}((\log p)^4)$.

Improving Schoof's squareroot algorithm (1/2)

For $E : Y^2 = X^3 + X$, the splitting of the division polynomial f_ℓ is given by CM theory:

- if $\ell \equiv 3 \bmod 4$: f_ℓ is irreducible over $\mathbb{Q}(i)$.
- if $\ell \equiv 1 \bmod 4$: f_ℓ has two eigenfactors of degree $(\ell - 1)/2$ over $\mathbb{Q}(i)$. Ex:

$$f_5(X) = 5\ \left(X^2 + 1/5 + 2/5\, i\right) \left(X^2 + 1/5 - 2/5\, i\right)$$
$$\times \left(X^8 + 12\, X^6 - 26\, X^4 - 52\, X^2 + 1\right).$$

Over $\mathbb{F}_p[T]/(T^2 + 1)$: use $f_\lambda(X) = X^2 + 1/5 + 2/5\, i$ and look for the eigenvalue $1 \leq \lambda < \ell$

$$(X^p, Y^p) = [\lambda](X, Y)$$

in $B_\ell = \mathbb{F}_p[X, Y, T]/(Y^2 - (X^3 + AX + B)), f_\lambda(X, T), T^2 + 1)$.

It has the flavor of Elkies's algorithm... and a better complexity (no modular polynomials needed).

Improving Schoof's squareroot algorithm (2/2)

How do we compute f_λ? write $f_\lambda(X) = f_{2+i}(X)$ and use Satoh's generalized division polynomials, computable using generalized recurrences ($f_{2u+1\pm\omega}$, etc.).

Equality test: $\gcd(a_i(T) - b_i(T), T^2 + 1)$ for $a(X, T) = \sum_i a_i(T)X^i$, $b(X, T) = \sum_i b_i(T)X^i$.

Ex. $p = 241$, $\ell = 5$, $E : Y^2 = X^3 + X$:

$$f_\lambda(X, T) = X^2 + 193 + 145T,$$

$$X^p \equiv -X, Y^p \equiv 177Y$$

$$[2](X, Y, 1) = (-X, -YT, 1)$$

and $\gcd(T^2 + 1, -T - 177) = T + 177$ (actually guessable from the value of Y^p).

This behaviour is very very very frequent: hard to find an example where we must really compute t.

B) Primality proving

[...] I conceived and programmed the method (with me this is one thing - I don't "implement" myself anymore than I would subcontract my algebra or analysis) in 3 months in the spring of 1986.

ECPP in one slide

Idea: (Selfridge's) DOWNRUN using CM elliptic curves.

One of the important parameters: a set $\mathcal{D}$ of (fundamental) discriminants.

```
function ECPP($N$, $\mathcal{D}$)
  • if $N$ is small enough, prove its primality directly.
  • repeat
      find $D \in \mathcal{D}$ s.t. $4N = U^2 - DV^2$
    until $m = N + 1 - U = cN'$ with $c > 1$ small, $N'$ probable prime;
  • build $E$ as the reduction of an elliptic curve having CM over $\overline{\mathbb{Q}}$, and find $P$ of order $m$;
  • return ECPP($N'$, $\mathcal{D}$).
```

ECPP (cont'd)

Complexity: (Lenstra & Lenstra, 1990) for $\mathcal{D} = \{|D| = O((\log N)^2)\}$, one gets a heuristic complexity

$$\tilde{O}(\underbrace{(\log N)}_{\text{number of steps}}\underbrace{(\log N)^2}_{\#\mathcal{D}}\underbrace{(\log N)^2}_{\sqrt{D} \bmod N}).$$

All other steps are in $\tilde{O}((\log N)^4)$.

Output: a generalized Pratt certificate of size $O((\log N)^2)$ requiring $\tilde{O}((\log N)^3)$ deterministic time to be checked.

A short history of ECPP

- First program of Atkin: up to 243 decimal digits (the largest PRP in the Cunningham tables at that time).
- Original M. implementation (1987–1988): up to 500 dd (cofactor of F_{11}).
- Distribution of computations (1989): 1000dd.
- Problems: class polynomials ⇒ new smaller invariants
- Competition with PRIMO.
- AKS (and Dan Bernstein – 2003) caused renewed interest in a faster version (J. Shallit, see LeLe90), never implemented so far, using $\mathcal{D} = \{q_{i_1}^* q_{i_2}^* \cdots q_{i_r}^*, 1 \leq i_u \leq t\}$ for $t = O(\log N)$.

  ⇒ complexities of all phases are now (heuristically) $\tilde{O}((\log N)^4)$.

  ⇒ $10,000$ dd reached (Franke/Kleinjung/Wirth, 2003)

  ⇒ $15,000$ dd reached (Franke/Kleinjung/M./Wirth, 2004)

  ⇒ $20,000$ dd reached (M., 2006).

One step further

$N = 6753^{5122} + 5122^{6753}$ (taken from P. Leyland's tables) is a 25050-digit prime; gzipped certificate of 2024 steps has 55 Mb.

Calendar time: 2010/09/01 – 2010/10/15.

Machines: network of bi-core i7 quad-core; using open MPI.

what	CPU days
$\sqrt{D}$	281
find (D, h)	199
Cornacchia	172
FKW	37
PRP	1005
H_D	5
root H_D	253
Step 1	1696
Step 2	282
Check	4.4

C) The independent life of the CM method

The sentence

• build E as the reduction of an elliptic curve having CM over $\overline{\mathbb{Q}}$, and find P of order m;

has nothing to do with primality proving and can serve as a building block in cryptography related things.

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

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;
  - 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).

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 $[m']P \neq O_E$ ($m' = p + 1 + U$ 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 $H_D[j](X)$.
⇒ three methods for this! all in $O(D^{1+\varepsilon})$: complex, p-adic, CRT. See AEnge's talk

2. Find a root j_0 of $H_D[j](X) \bmod p$.
⇒ use Galois theory + classical algorithms 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.
⇒ Try only one curve (see Rubin/Silverberg when using j).

4. Prove that E has cardinality $m = p + 1 - U$.
⇒ Use adequate parametrizations to check $[m]P = O_E$.

IV. Modular curves and class invariants

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

Two cases:

- construct K_D: just need one minimal polynomial (Hajir, etc.);
- build a CM curve: need some relation between f and j $\Longleftrightarrow$ modular curves and replace $j(\alpha)$ by class invariants $f(\alpha)$ for some modular function f.

Ex. $(X+16)^3 - Xj = 0$ is a modular equation for $X_0(2)$; its roots are the classical Weber functions $-\mathfrak{f}(\alpha)^{24}$, $\mathfrak{f}_1(\alpha)^{24}$ and $\mathfrak{f}_2(\alpha)^{24}$. For $j(\sqrt{-2}) = 8000$, one finds a root $X = 2^6 = \mathfrak{f}_1(\sqrt{-2})^{24}$ which is smaller.

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

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

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

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 $\Gamma^0(N)$, $\Gamma/\Gamma^0(N) = \{\gamma_\nu\}_{1 \le \nu \le \mu^0(N)}$. Put

$$\Phi[f](X) = \prod_{\nu=1}^{\mu^0(N)} (X - f \circ \gamma_\nu) = \sum_{\nu=0}^{\mu^0(N)} R_\nu(J) X^\nu$$

where $R_\nu(J) \in \mathbb{C}(J)$. 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. $\mathcal{H}(P = \sum (a_i + b_i\omega) X^i) = \log(\max\{|a_i|, |b_i|\})$.

Prop. (Hindry & Silverman)

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

$\Rightarrow$ 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., $g(X^0(N)) = 0$); $\deg_X \Phi = \mu^0(N)$.

Asymptotically, $c(f) \to 1/12$, since $\deg_J \approx g \approx \mu^0(N)/12$.

B) Finding functions on $\Gamma^0(N)$

B. Birch, Antwerp I.

To find differentials, there are various methods available:

(i) *luck;*

(ii) *theta functions;*

(iii) *Eichler's trace formula;*

(iv) *direct computation of the eigenvalues of the Hecke operators, acting on the 1-dimensional homology of $\mathcal{H}/G$.*

The luck part:

- Families (η-quotients: Enge/Schertz; Enge/M.; etc.);
- Elkies: $X_0(\ell^n)$ for many ℓ's.

Newman's lemma

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

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

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

$$\prod_{d|N} d^{r_d} = t^2, \quad t \in \mathbb{Q}^*$$

then the function

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

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

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

Coro. Any Newman function yields a class invariant.

The genus 0 case

$\mathcal{N}_N = q^{1/N}(1 + \ldots)$ and $\deg_J = 1$, $c(\mathcal{N}_N) = 1/\mu^0(N)$.

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

What is the smallest invariant?

Extension of Enge+M. of ANTSV:

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

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

$$> \substack{\mathfrak{w}_{81} \\ 27,12} > \substack{\mathfrak{w}_{11^2} \\ 132/5,5} > \substack{\mathfrak{w}_{13^2} \\ 26,7} > \substack{\mathfrak{w}_{17^2} \\ 51/2,12} > \substack{\mathfrak{w}_{3,37} \\ 76/3,6} = \substack{\mathfrak{w}_{19^2} \\ 76/3,15} > \substack{\mathfrak{w}_{3,61} \\ 124/5,10}$$

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

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

96: conjectured upper bound (Selberg+Abramovich+Bröker/Stevenhagen)

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

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

C) Using quotients of modular curves

(joint work in progress with É. Brier)

Goal: instead of using general families, look at each case and find an optimal function/equation for these.

Natural candidates: quotients of $X_0(N)$ by a subgroup of $\mathrm{Aut}(X_0(N))$ which is almost always $= \mathcal{W}_N$, the group of Atkin-Lehner involutions.

Def. $X_0^*(N) = X_0(N)/\mathcal{W}_N$.

Prop. the "natural" modular equation for $X_0^*(N)$ will have degree $2^{\omega(N)}(g_0^*(N)+1)$ (and a similar formula for any intermediate quotient).

Caveat: for our purpose, we need some way of computing j from the equation. We cannot be satisfied with equations for modular curves coming out of the blue (in a lot of papers).

The prime case $N = \ell$

Fricke: all prime cases of genus 0.

Atkin's functions for $X_0^*(\ell)$: the laundry method yields (conjectured) minimal functions on $X_0^*(\ell)$.

We can turn these into class invariants and look at magical constants:

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

Atkin's legacy

B. Birch: *As everyone knows, it has since been Oliver's way to make his work known by bush telegraph, via e-mail, or as quoted by others; [...].*

Atkin was able to recognize his functions as quotients of "known" functions (private email).

Ex. $\mathcal{A}_{71} = (\Theta_{2,1,9} - \Theta_{4,3,5})/\eta\eta_{71}$.

$$\Theta(a,b,c,\gamma) = \sum_{m,n} \varepsilon_\gamma(m,n) x^{(am^2+bmn+cn^2)/K}$$

for some "code" γ ($\varepsilon_\gamma = 1$, $K = 1$ when $\ell \equiv 23 \bmod 24$).

Shouldn't we gather to webify some "Collected emails of A. O. L. Atkin"?
Check my web page soon for the history of ECPP.

Gonzalez & Lario (1/2)

- Table of all quotients of small genera;
- give methods for computing the "final step" when X' has genus g' and some w is s.t. $X'/\langle w\rangle$ has small genus (including 0);
- identify intermediate quadratic subfields predicted by Galois theory.

Gonzalez & Lario (2/2)

$N = p \cdot q$	g	w_p	w_q	w_{pq}
$6 = 2 \cdot 3$	0	0	0	0
$10 = 2 \cdot 5$	0	0	0	0
$14 = 2 \cdot 7$	1	1	0	0
$\dots$				
$94 = 2 \cdot 47$	11	6	1	4
$95 = 5 \cdot 19$	9	5	3	1
$119 = 7 \cdot 17$	11	6	4	1

$N = p \cdot q \cdot r$	g	p, q	p, r	q, r	p, qr	q, pr	pq, pr	pqr
$30 = 2 \cdot 3 \cdot 5$	3	1	1	0	0	1	0	0
$42 = 2 \cdot 3 \cdot 7$	5	1	1	1	1	0	1	0
$66 = 2 \cdot 3 \cdot 11$	9	2	1	1	1	2	0	2
$70 = 2 \cdot 5 \cdot 7$	9	2	2	1	1	1	2	0
$78 = 2 \cdot 3 \cdot 13$	11	3	2	1	1	1	3	0
$105 = 3 \cdot 5 \cdot 7$	13	3	3	1	1	1	3	1
$110 = 2 \cdot 5 \cdot 11$	15	4	3	1	1	3	1	2

Magical constants

N	c
6	$12/4 = 3$
	$\dots$
87	$120/4 = 30$
94	$144/4 = 36$
95	$120/4 = 30$
119	$144/4 = 36$

N	c
30	$72/8 = 9$
42	$32/8 = 4$
66	$40/8 = 5$
70	$40/8 = 5$
78	$40/8 = 5$
105	$192/8 = 24$
110	$216/8 = 27$

$N = 94$

$X_0^*(47)$ has genus 0 and

$$A^{48} + (696 - J)A^{47} + \dots + J^2 + 2^{16}J + 2^{30} = 0.$$

$$t_{47} = \frac{\Theta(1,1,12) - \Theta(3,1,4)}{\eta\eta_{47}} \Rightarrow c(t_{47}) = 24$$

$$r = t_{47}(\tau) + t_{47}(2\tau), \quad s = t_{47}(\tau)t_{47}(2\tau)$$

$$t_{94}(\tau) = \frac{s-1}{r-1} = x^{-1} + x + x^3 + x^4 + x^5 + x^6 + \dots$$

$$j_1 + j_2 + j_{47} + j_{94} = T^{94} - 94T^{92} + \dots - 32327680T + 2528000$$

$$j_1 j_2 j_{47} j_{94} = (T^{48} + 248T^{47} + 4324T^{46} + \dots - 12615680T + 774400)^3$$

$$c(t_{94}) = 144/4 = 36$$

$N = 30$ (from Gonzalez)

$$\begin{tikzcd}
X_0(30) \arrow[d] & \mathbb{Q}(r)(j)\, j^2 - \frac{P_1(r)}{(r-1)^{30}(r+1)^{10}r^5}j + \frac{P_2(r)}{(r-1)^{32}(r+1)^{16}r^8} = 0 & \\
X_0(30)/\langle w_{15}\rangle \arrow[d] & \mathbb{Q}(r) & r = \frac{\eta_1\eta_6^2\eta_{10}^2\eta_{15}}{\eta_2^2\eta_3\eta_5\eta_{30}^2} \\
X_0(30)/\langle w_3, w_{15}\rangle \arrow[d] & \mathbb{Q}(s) & s = r - 1/r = \frac{\eta_1\eta_3\eta_5\eta_{15}}{\eta_2\eta_6\eta_{10}\eta_{30}} \\
X_0^*(30) & \mathbb{Q}(t) & t = s + 4/s
\end{tikzcd}$$

$$r|w_{15} = r$$

$$r|w_3 = -1/r \Rightarrow (s = r - 1/r)|w_3 = s$$

$$s|w_{30} = 4/s \Rightarrow (t = s + 4/s)|w_{30} = t$$

$\mathbb{Q}(t,j)$ is the composition of three quadratic extensions of $\mathbb{Q}(t)$: $\mathbb{Q}(t)(\sqrt{t^2-16})$, $\mathbb{Q}(t)(\sqrt{t(t+4)})$, $\mathbb{Q}(\sqrt{(t+5)(t+1)})$.

95 and 119

Note that

$$t_{23} = \frac{2\Theta(2,1,3)-1}{\eta\eta_{23}},$$
$$t_{47} = \frac{\Theta(1,1,12)-\Theta(3,1,4)}{\eta\eta_{47}},$$
$$t_{71} = \frac{\Theta_{2,1,9}-\Theta_{4,3,5}}{\eta\eta_{71}}$$

are Hauptmoduln for the corresponding $X_0^*(\ell)$.

We can generalize Atkin's approach for $X_0^*(95)$ and $X_0^*(119)$:

$$t_{95} = \frac{\Theta(4,1,6)-\Theta(3,1,8)}{2\eta\eta_{95}},$$

$$t_{119} = \frac{\Theta(4,3,8)-\Theta(5,1,6)}{2\eta\eta_{119}}.$$

Summary of results

- We now have the best (conjectured) constants for all (quotients of) modular curves of genus 0, plus some of genus 1.
- We still need to identify optimal functions as quotients of known functions, in case we need evaluate them.
- For $\omega(N)=\nu$, there are cases where $H_D(X)=G(X)^\nu$, when $N \mid D$, $N \neq D$ (see AEnge's talk for other examples and theorems). E.g.,

$$H_{420}[t_{30}](X) = (X-9)^8, \quad H_{660}[t_{110}](X) = (X+2)^8.$$

- Open problem: is there an algorithm that computes $\Theta(a,b,c)$ rapidly (as for the classical θ's)?

Conclusions

- CM is everywhere and has many applications
  - after 200 years of studies in genus 1, computations lead to beautiful numbers, equations, etc.
  - a lot of work is needed for the higher genus case, though the theory exists. Since modular equations are difficult to compute, trying to find class invariants is not as easily doable yet.
- I haven't told you everything on the subject, but stay tuned for the other talks on these subjects!