LMS Durham Symposium on Computational Number Theory

24 July - 3 August 2000

Modular curves and class invariants

(Corrected version)

F. Morain

morain@lix.polytechnique.fr

http://www.lix.polytechnique.fr/Labo/Francois.Morain

Contents

I. Classical motivation.

II. Modular functions for $\Gamma_0(N)$.

III. Generalized Weber functions and applications.

IV. When do class invariants exist?

I. Classical motivation

Pb: When can we represent the prime p as $4p = x^2 + Dy^2$ for $D > 0$?

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

Thm. p is representable iff p splits in the ring class field $\mathbf{K}_m$.

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

Thm. There is a unique modular function j of weight 0 s.t. $j(Mz) = j(z)$ for all $M \in \Gamma = \mathrm{SL}_2(\mathbb{Z})$ and

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

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

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

Thm. The extension $K[\mathfrak{i}] = \mathbb{Q}(\alpha, j(\alpha))$ is Galois over $\mathbb{Q}(j(\alpha))$. The only non-trivial automorphism of this group is denoted by λ and the action of λ is given by:

$$j(\mathfrak{a})^{\lambda(\mathfrak{b})} = j(\mathfrak{a}^{-1}\mathfrak{b}^2).$$

Fundamental Thm. Define

$$H_{D_K m^2}(X) = \prod_{\mathfrak{i} \in Cl(\mathcal{O})} (X - j(\mathfrak{i})).$$

Then $4p = x^2 + D_K m^2 y^2$ iff $(-D_K/p) = +1$ and $H_{D_K m^2}(X)$ has h roots modulo p.

Biblio: LNM 21, Serre, Cox.

Building K_m

Def. η function:

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

$$= q^{1/24}(1 + \sum_{n\geq 1} (-1)^n (q^{n(3n-1)/2} + q^{n(3n+1)/2})).$$

Prop. With $\zeta_n = \exp(2i\pi/n)$

$$\eta(z+1) = \zeta_{24}\eta(z), \quad \eta(-1/z) = \sqrt{z/i}\eta(z).$$

Def. Weber functions:

$$\mathfrak{f}(z) = \zeta_{48}^{-1} \frac{\eta((z+1)/2)}{\eta(z)},$$

$$\mathfrak{f}_1(z) = \frac{\eta(z/2)}{\eta(z)}, \quad \mathfrak{f}_2(z) = \sqrt{2}\,\frac{\eta(2z)}{\eta(z)}$$

$$\gamma_2 = \frac{\mathfrak{f}^{24}-16}{\mathfrak{f}^8}, \gamma_3 = \frac{(\mathfrak{f}^{24}+8)(\mathfrak{f}_1^8 - \mathfrak{f}_2^8)}{\mathfrak{f}^8}.$$

Thm.

$$j(z) = \frac{(-\mathfrak{f}(z)^{24}+16)^3}{-\mathfrak{f}(z)^{24}} = \frac{(\mathfrak{f}_1(z)^{24}+16)^3}{\mathfrak{f}_1(z)^{24}} = \frac{(\mathfrak{f}_2(z)^{24}+16)^3}{\mathfrak{f}_2(z)^{24}}$$

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

Computation of $H_{D_K m^2}(X)$: 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 using η.

Ex. $H_3(X) = X, H_4(X) = X - 1728;$

$$H_{39}(X) = X^4 + 331531596\,X^3 - 429878960946\,X^2$$

$$+109873509788637459\,X + 20919104368024767633,$$

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

From this: $p = x^2 + y^2$ 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.

Application: primality proving (ECPP).

Question: How to find small defining polynomials for K_m?

First answer: use powers of Weber functions. For instance: from $j(\sqrt{-2}) = 8000$, one solves

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

to get $\mathfrak{f}_1(\sqrt{-2})^{24} = 2^6$ and (optimally with more work) $\mathfrak{f}_1(\sqrt{-2})^4 = 2$.

Other answer: Schertz, Cohen.

But in general, does not work well when $3 \mid D_K$.

In this talk: equation $(*)$ is a modular equation for $X_0(2) \Rightarrow$ generalize to $X_0(N)$.

II. Modular functions for $\Gamma_0(N)$

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N \right\}$$

$$\mu_0(N) = [\Gamma : \Gamma_0(N)] = N \prod_{p|N} (1 + 1/p)$$

Def. $\mathcal{H}^*/\Gamma_0(N) = \{< z >\}$ where

$$< z > = \{Mz, M \in \Gamma_0(N)\}$$

Thm. $\mathcal{H}^*/\Gamma_0(N)$ is a Riemann surface $X_0(N)$.

Rem. $X_0(1)$ is the Riemann sphere.

Prop. $g(N) = 0$ iff
$N \in \{2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\}$.

$g(N) = 1$ iff
$N \in \{11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49\}$.

$g(N) = 2$ iff $N \in \{22, 23, 26, 28, 29, 31, 37, 50\}$.

Thm. (Ogg) $X_0(N)$ hyperelliptic and $g \geq 3$ iff $(N, g) \in \{(30, 3), (33, 3), (35, 3), (39, 3), (40, 3), (41, 3), (46, 5), (47, 4), (48, 3), (59, 5), (71, 6)\}$.

Rem. Equations given by Murabayashi ($g = 2$) and Rovira; Hibino & Murabayashi; $2 \leq g \leq 6$ by M. Shimura.

Functions on subgroups

Def. f on $\mathcal{H}^*$ is a modular function for $\Gamma_0(N)$ iff

1. f is meromorphic on $\mathcal{H}$;
2. $\forall M \in \Gamma_0(N)$, $z \in \mathcal{H}^*$, one has $f(Mz) = f(z)$;
3. at a cusp $-d/c$, $(d, c) = 1$:

$$f(z) = \sum_{v \geq v_0} c_v e^{\frac{2\pi i}{\kappa_1} A(z) v}$$

with

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$$

and $\kappa_1 \in \mathbb{N}^*$ (true for $\Im(z)$ large enough).

Prop. If f is a function for $\Gamma_0(N)$ and $M \in \Gamma$, then
$f|M : \mathcal{H}^* \to \hat{\mathbb{C}}$, $z \mapsto f(M(z))$ is a function for $M^{-1}\Gamma_0(N)M$.

Def. Fricke-Atkin-Lehner involution:

$$W_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}.$$

Prop. $W_N \Gamma_0(N) W_N^{-1} = \Gamma_0(N)$.

Cor. if f is a function on $\Gamma_0(N)$, so is $f|W_N$.

Finding functions: Newman's Lemma

Use the η function:

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

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

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

is a modular function on $\Gamma_0(N)$. Moreover:

$$g^* = g|W_N = \frac{1}{t}\hat{g}$$

where $\hat{g}(z) = \prod_{d|N} \eta(dz)^{r_{N/d}}$.

Ex. Given N, let $s = 12/\gcd(12, N-1)$. Then $g_N(z) = (\eta(z)/\eta(Nz))^{2s}$ is a function for $\Gamma_0(N)$ and $g_N|W_N = N^s/g_N$.

The cases where $X_0(N)$ has genus 0

$N - 1 \mid 24$: put $s = 12/(N-1)$ and then $g_N(z) = (\eta(z)/\eta(Nz))^{2s}$, $g_N|W_N = N^s/g_N$ (take care to $N \in \{9, 25\}$).

Other cases: Klein (Fricke).

N	g_N	$g_N\|W_N$
6	$\eta_1^5\eta_2^{-1}\eta_3\eta_6^{-5}$	$72/g_6$
8	$\eta_1^4\eta_2^{-2}\eta_4^2\eta_8^{-4}$	$32/g_8$
10	$\eta_1^3\eta_2^{-1}\eta_5\eta_{10}^{-3}$	$20/g_{10}$
12	$\eta_1^3\eta_2^{-2}\eta_3^{-1}\eta_4\eta_6^2\eta_{12}^{-3}$	$12/g_{12}$
16	$\eta_1^2\eta_2^{-1}\eta_8\eta_{16}^{-2}$	$8/g_{16}$
18	$\eta_1^2\eta_2^{-1}\eta_3^{-1}\eta_6\eta_9\eta_{18}^{-2}$	$6/g_{18}$

Modular equations

$$\Gamma/\Gamma_0(N) = \{\gamma_v\}_{1 \le v \le \mu_0(N)}, \quad \Gamma = \bigcup_{v=1}^{\mu_0(N)} \Gamma_0(N)\gamma_v$$

Thm. Let f be a function for $\Gamma_0(N)$. Put

$$G(X) = \prod_{v=1}^{\mu_0(N)} (X - f|\gamma_v) = \sum_{v=0}^{\mu_0(N)} R_v(J) X^v$$

where $R_v(J) \in \mathbb{C}(J)$. Then $G(X,J) = 0$ is called a modular equation for $\Gamma_0(N)$.

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

Rem. For technical reasons, one prefers to find the modular equation for $f|W_N$:

$$G(X,J) = (X - (f|W_N))(X - f(z/N)) \cdots$$

Ex. $j(z)$ is a function on $\Gamma_0(N)$; the modular polynomial is

$$\Phi_N(X,J) = \prod_{v=1}^{\mu_0(N)} (X - j|\gamma_v).$$

For instance:

$$\Phi_2(X,Y) = X^3 + Y^3 - X^2Y^2 - 162000\,(X^2+Y^2)$$
$$+8748000000\,(X+Y) + 40773375\,XY$$
$$+1488\,(X^2Y + XY^2) - 157464000000000.$$

All cases where $X_0(N)$ has genus 0: $J = \mathcal{R}_N(F)$

Cases where $N - 1 \mid 24$

N	$\mathcal{R}_N$
2	$\frac{(F+16)^3}{F}$
3	$\frac{(F+27)(F+3)^3}{F}$
4	$\frac{(F^2+16F+16)^3}{F(F+16)}$
5	$\frac{(F^2+10F+5)^3}{F}$
7	$\frac{(F^2+13F+49)(F^2+5F+1)^3}{F}$
9	$\frac{(F+3)^3(F^3+9F^2+27F+3)^3}{F(F^2+9F+27)}$
13	$\frac{(F^2+5F+13)(F^4+7F^3+20F^2+19F+1)^3}{F}$
25	$\frac{(F^{10}+10F^9+55F^8+200F^7+525F^6+1010F^5+1425F^4+1400F^3+875F^2+250F+5)^3}{F(F^4+5F^3+15F^2+25F+25)}$

Other cases

N	$\mathcal{R}_N$
6	$\frac{(F+6)^3\left(F^3+18\,F^2+84\,F+24\right)^3}{F(F+9)^2(F+8)^3}$
8	$\frac{\left(F^4+16\,F^3+80\,F^2+128\,F+16\right)^3}{F(F+8)(F+4)^2}$
10	$\frac{\left(F^6+20\,F^5+160\,F^4+640\,F^3+1280\,F^2+1040\,F+80\right)^3}{F(F+5)^2(F+4)^5}$
12	$\frac{\left(F^2+6\,F+6\right)^3\left(F^6+18\,F^5+126\,F^4+432\,F^3+732\,F^2+504\,F+24\right)^3}{F(F+6)(F+4)^3(F+2)^3(F+3)^4}$
16	$\frac{\left(F^8+16\,F^7+112\,F^6+448\,F^5+1104\,F^4+1664\,F^3+1408\,F^2+512\,F+16\right)^3}{F(F+4)(F^2+4\,F+8)(F+2)^4}$
18	$\frac{\left(F^3+6\,F^2+12\,F+6\right)^3\left(F^9+18\,F^8+144\,F^7+666\,F^6+1944\,F^5+3672\,F^4+4404\,F^3+3096\,F^2+1008\,F+24\right)^3}{F(F^2+6\,F+12)(F+3)^2(F^2+3\,F+3)^2(F+2)^9}$

Rem. Does not yield a “minimal” model for $X_0(N)$.

III. Generalized Weber functions and applications

A) Historical use of modular equations

Starting from $j(i) = 1728$:

$$\Phi_2(X, 1728) = (X - 1728)\,(X - 287496)^2$$

and $j(2i) = 287496 = 66^3$;

$$\Phi_2(X, 287496) = (X - 1728)P_4$$

where

$$P_4(X) = X^2 - 82226316240\,X - 7367066619912$$

so that $j(4i)$ belongs to $\mathbb{Q}(\sqrt{2})$. Again:

$$\begin{aligned}\mathrm{Res}_Y(\Phi_2(X,Y), P_4(Y)) = \big(&Y^4 - 6761166974781862161312\,Y^3\\ &-1826592673506207200904172752\,Y^2\\ &+2692562339666300831137589096678 4\,Y\\ &-1064410681181869521037208505239142408)\\ &(Y-287496)^2\end{aligned}$$

and $j(8i)$ eventually belongs to $\mathbb{Q}(\sqrt[4]{2})$.

Rem. This trend was used by Mathews, Russel, Greenhill, Watson, Berwick, etc. to compute singular moduli.

Thm. (H. Cohn) If $p \equiv 1 \bmod 4$, then $p = x^2 + 4^{t+1}y^2$ is solvalble iff a sequence of integers $r_1, r_2, \ldots, r_t$ is definable modulo p under the recursion $r_1^2 \equiv 9/8 \bmod p$, $r_{s+1}^2 \equiv (r_s+3)^2/(8(r_s+1)) \bmod p$.

B) Generalized Weber functions

Notations: for $A\alpha^2 + B\alpha + C = 0$ with $(A, B, C) = 1$, put $\Delta(\alpha) = B^2 - 4AC$.

Thm. $j(z)$ and $j(Nz)$ are functions on $\Gamma_0(N)$. Conversely, every modular function on $\Gamma_0(N)$ is a rational function of $j(z)$ and $j(Nz)$.

Idea of the Proof: let f be a function on $\Gamma_0(N)$ and define:

$$G(X, z) = \Phi_N(X, j(z)) \sum_{A \in \mathcal{S}_N} \frac{f(Az)}{X - j(N(Az))}.$$

$$= \sum_{A} f(Az) \prod_{B \neq A} (X - j(N(Bz))).$$

Every coefficient of $G(X, z)$ is a modular function, hence is a rational function of J.

$$G(j(Nz), j(z)) = f(z) \frac{\partial \Phi_N}{\partial X}(j(Nz), j(z)). \square$$

Def. $\mathcal{C}(N, \alpha)$ is the property that $x^2 + |\Delta(\alpha)| y^2 = 4N^2$ has the only trivial solution $(\pm 2N, 0)$ in integers x and y.

Thm. If f is a function on $\Gamma_0(N)$ and $\mathcal{C}(N, \alpha)$ holds, then $f(\alpha) \in \mathbb{Q}(j(\alpha), j(N\alpha))$.

Proof: Condition $\mathcal{C}(N, \alpha)$ says that $\frac{\partial \Phi_N}{\partial X}(j(N\alpha), j(\alpha)) \neq 0$. $\square$

A general theorem

Thm. Let f a function on $\Gamma_0(N)$. If $A\alpha^2 + B\alpha + C = 0$ with $(A, N) = 1$, $B \equiv C \equiv 0 \bmod N$, and $\mathcal{C}(N, \alpha)$ holds, then $\mathbb{Q}(f(\alpha/N)) \subset \mathbb{Q}(j(\alpha))$. If $X_0(N)$ has genus 0 or $h(\Delta(\alpha)) = 1$, then $\mathbb{Q}(f(\alpha/N)) = \mathbb{Q}(j(\alpha))$.

Proof: à la Schertz 1976.

- $f(\alpha/N)$ is an algebraic integer, since $j(\alpha)$ is;
- $f(\alpha/N) \in \mathbb{Q}(j(\alpha/N), \mathbb{Q}(j(\alpha)))$ by the preceding Theorem;
- $j(\alpha/N) \in \mathbb{Q}(\alpha, j(\alpha))$, since $\Delta(\alpha/N) \mid \Delta(\alpha)$;
- using Galois action, $j(\alpha/N) \in \mathbb{Q}(j(\alpha))$, implying that $f(\alpha/N)$ does;
- if $X_0(N)$ has genus 0, then $j(\alpha) = \mathcal{R}_N(f(\alpha/N))$, and $\mathbb{Q}(j(\alpha)) \subset \mathbb{Q}(f(\alpha/N))$. $\square$

Thm. If $A \equiv 0 \bmod N$, $B \equiv 0 \bmod N$, and $(C, N) = 1$, then $\mathbb{Q}(f^*(\alpha)) \subset \mathbb{Q}(j(\alpha))$.

Proof: $\beta = -1/\alpha$ is a root of $Cx^2 - Bx + A = 0$ and $f(\beta/N) = f(-1/(\alpha N)) = f^*(\alpha)$. Then $\mathbb{Q}(f(\beta/N)) \subset \mathbb{Q}(j(\beta)) = \mathbb{Q}(j(\alpha))$. $\square$

Application to the case $N-1 \mid 24$

Remember that

$$s = 12/(N-1), g_N(z) = (\eta(z)/\eta(Nz))^{2s}.$$

Define

$$\mathfrak{v}_N(z) = \sqrt{N}\frac{\eta(Nz)}{\eta(z)}, \quad \mathfrak{w}_N(z) = \frac{\eta(z/N)}{\eta(z)}$$

and note that:

$$\mathfrak{w}_N(z)^{2s} = g_N(z/N).$$

Rem. Case $N = 2$ yields Weber's functions: $\mathfrak{w}_2 = \mathfrak{f}_1$, $\mathfrak{v}_2 = \mathfrak{f}_2$, and these two functions are dual.

Thm. Suppose that $N \mid \Delta(\alpha)$, $(A, N) = 1$, $B \equiv 0 \bmod N$ and that condition $\mathcal{C}(N, \alpha)$ holds. Then $\mathbb{Q}(\mathfrak{w}_N(\alpha)^{2s}) = \mathbb{Q}(j(\alpha))$.

Thm. Suppose that $N \mid \Delta(\alpha)$, $(C, N) = 1$, $B \equiv 0 \bmod N$ and that condition $\mathcal{C}(N, \alpha)$ holds. Then $\mathbb{Q}(\mathfrak{v}_N(\alpha)^{2s}) = \mathbb{Q}(j(\alpha))$.

Numerical examples

$$\mathfrak{w}_2(\sqrt{-2}) = 64, j(\sqrt{-2}) = 8000;$$
$$\mathfrak{w}_3((-3+\sqrt{-3})/2)^{12} = -27;$$
$$H_{15}[\mathfrak{w}_3^{12}](X) = X^2 + 81X + 729$$

vs.

$$H_{15}[j](X) = X^2 + 191025X - 121287375;$$
$$H_{35}[\mathfrak{w}_5^6](X) = X^2 + 50X + 125;$$
$$H_{35}[\mathfrak{w}_7^4](X) = X^2 + 21X + 49;$$
$$H_{3\times 5^2}[\mathfrak{w}_{25}](X) = X^2 + 5\,X + 5$$

vs.

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

Rem. In some cases smaller powers; might be divisible by some integer.

Conj. Suppose that $\Delta(\alpha) \equiv -3 \bmod 9$ and $(A, 3) = 1$, $B \equiv 0 \bmod 9$, $C \equiv 0 \bmod 3$. Then $\mathfrak{w}_3(\alpha)^4$ is a class invariant.

Ex. For $D = 39$, $M[\mathfrak{w}_3^4] = X^4 + 9\,X^3 + 9\,X^2 + 81\,X + 81$.
Better: $M[\mathfrak{w}_3^4/3] = X^4 + 3\,X^3 + X^2 + 3\,X + 1$.

More examples

A) Canonical invariants

For any N, use $g_N(z) = (\eta(z)/\eta(Nz))^{2s}$,
$s = 12/\gcd(12, N-1)$.

Thm. Suppose that $N \mid \Delta(\alpha)$, $(A, N) = 1$, $N \mid B$ and that $\mathcal{C}(N, \alpha)$ holds. Then $\mathbb{Q}(\mathfrak{w}_N(\alpha)^{2s}) \subset \mathbb{Q}(j(\alpha))$.

$$\mathfrak{w}_{11}((-11+\sqrt{-11})/2)^{12} = -11^3,$$
$$\mathfrak{w}_{19}((-19+\sqrt{-19})/2)^{4} = -19,$$
$$\mathfrak{w}_{43}((-43+\sqrt{-43})/2)^{4} = -43,$$
$$\mathfrak{w}_{67}((-67+\sqrt{-67})/2)^{4} = -67,$$
$$\mathfrak{w}_{163}((-163+\sqrt{-163})/2)^{4} = -163.$$
$$H_{44}[\mathfrak{w}_{11}^{12}](X) = (X + 11^3)^3$$
$$H_{44}[j](X) = X^3 - 1122662608\,X^2 + 270413882112\,X - 653249011576832.$$
$$H_{55}[\mathfrak{w}_{11}^{12}](X) = X^4 + 131769\,X^3 - 139953319\,X^2 + 233436821409\,X + 3138428376721$$

and the cube root of X has minimum polynomial:

$$X^4 + 33\,X^3 - 847\,X^2 + 3993\,X + 14641$$

B) $X_0(\ell)^+$

A function for $\Gamma_0(11)^+$ is

$$\left(\frac{\theta_{1,1,3}(z)}{\eta(z)\eta(11z)}\right)^2 - 1 = q^{-1} + 5 + 17q + 46q^2 + 116q^3 + \cdots.$$

where

$$\theta_{a,b,c}(z) = \sum_{m,n} q^{am^2+bmn+cn^2}.$$

$$\Phi_{11}^{+}(F,J) = F^{12} + F^{11}(-J+684) + F^{10}(55J+157410)$$
$$+F^9(-1188J+12515580) + F^8(12716J+75763215)$$
$$+F^7(-69630J+76077144) + F^6(177408J-207606564)$$
$$+F^5(-133056J-34321320) + F^4(-132066J+418524975)$$
$$+F^3(187407J-477130500) + F^2(-40095J+270641250)$$
$$+F(-24300J-82012500) + J^2 + 6750J + 11390625.$$

For $D = 11$, Φ_{11}^{+} has root -1.

For $D = 44$, Φ_{11}^{+} has a factor $F^3 - 17F^2 + 19F - 7$.

An application

Let $E[j]$ denote the elliptic curve

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

of invariant $j \notin \{0, 1728\}$.

Lemma. Let v be any root of

$$(X+27)(X+3)^3 - Xj = 0.$$

Then

$$x_3 = -\frac{(v+27)(v+3)}{v^2+18v-27}$$

is the abscissa of a 3-division point on $E[j]$.

Computing the cardinality of CM-curves with $\mathfrak{w}_3$:

Let $4p = U^2 + DV^2$ with $3 \mid D, D > 3$. This implies $U \equiv \pm 1 \bmod 3$. We fix U and V and we want to characterize the coefficients of the curve E of Frobenius $\pi = (U + V\sqrt{D})/2$, or equivalently with cardinality $p + 1 - U$.

Prop. Suppose there exists a 3-torsion point $P = (x_3, y_3)$ for which x_3 is rational. Let $z = x_3^3 + ax_3 + b \bmod p$. The Frobenius $\pi = (U + V\sqrt{D})/2$ of E is completely determined by $U \equiv -(z/p) \bmod 3$.

Proof: If $y_3 \in \mathbb{F}_p$, then $\pi(P_3) = (x_3^p, y_3^p) = (x_3, y_3) = P_3$ and therefore $U \equiv -1 \bmod 3$. If y_3 is in $\mathbb{F}_{p^2} - \mathbb{F}_p$, then $\pi(P_3) = (x_3, -y_3) = -P_3$ and $U \equiv 1 \bmod 3$. □

In practice: use $\mathfrak{w}_3$ to build j and $E[j]$ and use the 3-torsion point.

IV. When do class invariants exist?

Thm. Let ℓ be a prime number and put

$$P_\ell(X, \alpha) = \Phi_\ell(X, j(\alpha))$$

for α of discriminant $-D$. Then:

(i) if $(D/\ell) = 0$, $P_\ell(X, \alpha) = (X - \theta)Q_1$ where $Q_1(X) \in K_\alpha[X], \theta \in K_\alpha = \mathbb{Q}(\alpha, j(\alpha))$.

(ii) if $(D/\ell) = +1$, $P_\ell(X, \alpha) = (X - \theta)(X - \theta')Q_1Q_2$ where θ and θ' are in K_α and conjugate over $\mathbb{Q}(\sqrt{-D})$, $Q_i(X) \in K_\alpha(\zeta_\ell)[X]$ of degree $(\ell - 1)/2$;

(iii) if $(D/\ell) = -1$, $P_\ell(X, \alpha)$ is irreducible over $K_\alpha(\zeta_\ell)$.

Rem. Such a theorem is reminiscent of point counting on elliptic curves over finite fields.

Ex. For $N = 3$, $D = 8$, with Φ_3^c:

$$P_3(X) = (X + 23 + 5\sqrt{-8})(X + 23 - 5\sqrt{-8})(X^2 - 10X + 1)$$

and $X^2 - 10X + 1$ factors over $\mathbb{Q}(\sqrt{-8}, \zeta_3)$.

For $N = 5$, $D = 11$:

$$P_5(X) = (X + 9 - 2\sqrt{-11})(X + 9 + 2\sqrt{-11})Q_1Q_2$$

$$Q_1(X) = X^2 + (-8\zeta_5^3 - 8\zeta_5^2 + 2)X + +8\zeta_5^3 + 8\zeta_5^2 + 13.$$

Solving a mystery

Let $P_\alpha(X) = (X+27)(X+3)^3 - Xj(\alpha)$. Use Skolem's approach to find the roots of

$$P(X) = X^4 + a_1X^3 + a_2X^2 + a_3X + a_4.$$

We use the four roots x_i of P to define

$$\left\{\begin{array}{lcl} z_1 & = & x_1+x_2-x_3-x_4, \\ z_2 & = & x_1-x_2+x_3-x_4, \\ z_3 & = & x_1-x_2-x_3+x_4. \end{array}\right. \tag{1}$$

Writing $y_i = z_i^2$, the y_i's are roots of

$$R(y) = y^3 + b_1y^2 + b_2y + b_3 \tag{2}$$

in which

$$\left\{\begin{array}{lcl} b_1 & = & 8a_2 - 3a_1^2, \\ b_2 & = & 3a_1^4 - 16a_1^2a_2 + 16a_1a_3 + 16a_2^2 - 64a_4, \\ b_3 & = & -(a_1^3 - 4a_1a_2 + 8a_3)^2. \end{array}\right. \tag{3}$$

Conversely, if the y_i's are the roots of R and

$$-z_1z_2z_3 = a_1^3 - 4a_1a_2 + 8a_3,$$

then the x_i's defined by (1) (together with $x_1+x_2+x_3+x_4 = -a_1$) are the roots of P.

Here:

$$R(Y) = Y^3 - 1728Y^2 - 576(j(\alpha)-1728)Y - 64(j(\alpha)-1728)^2$$

and the compatibility relation is $z_1z_2z_3 = 8(j(\alpha)-1728)$.

If $3 \nmid \Delta(\alpha)$, $3 \nmid A$ and $3 \mid B$, then $\gamma_2(\alpha)$ is a class invariant and the roots of $R(Y)$ are:

$$4(\zeta_3^i\gamma_2(\alpha)^2 + 12\zeta_3^i\gamma_2(\alpha) + 144)$$

for $i = 0, 1, 2$.

The mystery is solved! if g is a prescribed root of

$$g(\alpha)^6 - 27g(\alpha)^{-6} = \gamma_2(\alpha) + 6,$$

put

$$\mathcal{A} = \sqrt{\gamma_2^2 + 12\gamma_2 + 144} = 2g^6 - \gamma_2 - 6 = g^6 + 27g^{-6},$$

$$\mathcal{A}_i = g_i^6 + 26g_i^{-6}$$

where $g_i^6 - 27g_i^{-6} = \zeta_3^{2i}\gamma_2 + 6$, g_i^2 being the conjugate of g^2.

Thm. (Birch) If $\Delta(\alpha) \equiv 1 \bmod 3$, then $\mathcal{A}(\alpha) \in \mathbf{K}_\alpha$ and $\mathcal{A}_i \in \mathbf{K}_\alpha(\zeta_3)$. Moreover, $g(\alpha)^2 \in \mathbf{K}_\alpha$. If $\Delta(\alpha) \equiv -1 \bmod 3$, then $\sqrt{-3}\mathcal{A}(\alpha) \in \mathbf{K}_\alpha$, but $\mathcal{A}(\alpha) \notin \mathbf{K}_\alpha$ and $\mathcal{A}_i \notin \mathbf{K}_\alpha(\zeta_3)$.

Concluding remarks

- A wealth of class invariants, sometimes better than Schertz's.

- Additional work required to finish to prove the conjectures (use Shimura's reciprocity law *à la* A. Gee).