Équations modulaires algorithmes et applications

F. Morain

Laboratoire d'Informatique de l'École polytechnique

Journées C2, April 5, 2011

Contents

I. Introduction and motivation

Elliptic integrals:

$$K(k) = \int_0^{\frac{\pi}{2}} \frac{d\phi}{\sqrt{1 - k^2 \sin^2 \phi}}.$$

$0 < k < 1$ is the modulus of K, $k' = \sqrt{1 - k^2}$ is the complementary modulus, $K' = K(k')$.

Thm. (J. Landen – 1771, 1775)

$$k = \frac{2\sqrt{\ell}}{1 + \ell} \Rightarrow K(k) = (1 + \ell) K(\ell).$$

Modular equation: $k^2(1 + \ell)^2 = 4\ell$.

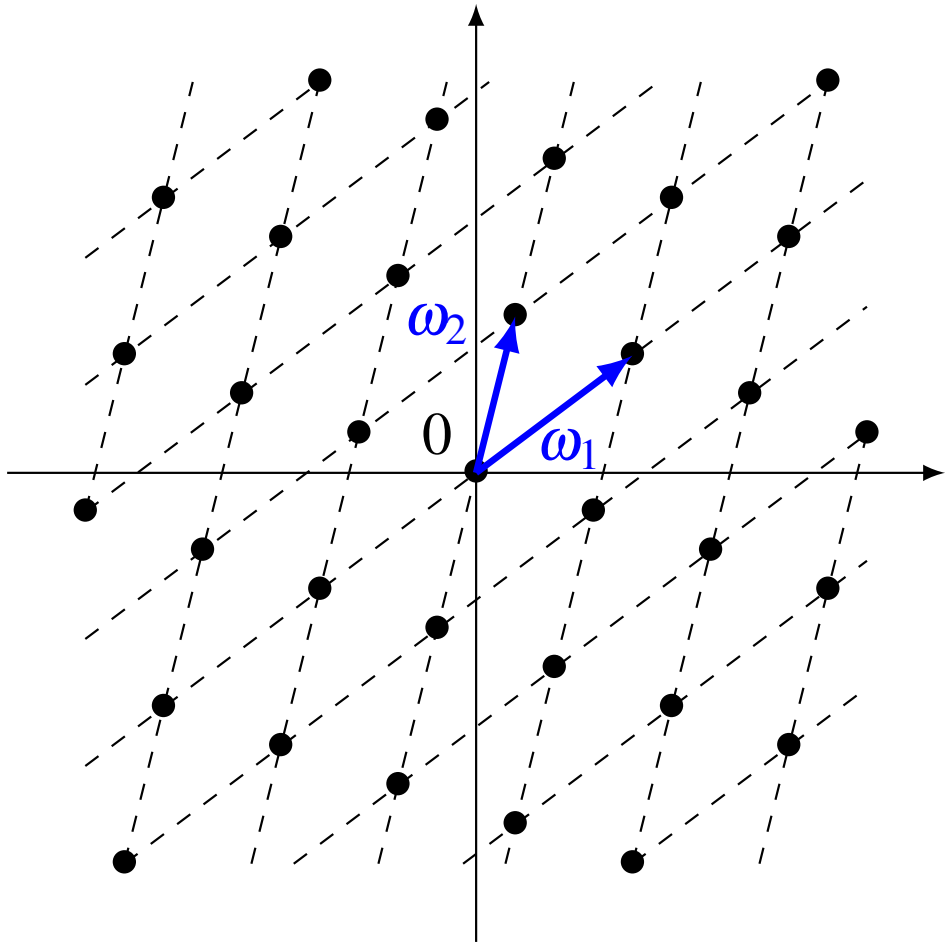
- Subsequent work by Legendre, Jacobi, etc.
- Switch to the use of J in the late XIX-th century (see later).

Bibliography

- Borwein and Borwein: π *and the AGM*, etc.;
- Berndt (*Ramanujan's notebooks*), etc.
- $+$ Zillions of articles, books, etc.

II. The classical theory

Lattice: $\mathscr{L} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2, \quad \tau = \omega_2/\omega_1 \in \mathbb{H} = \{z \in \mathbb{C}, \Im(z) > 0\}$



$\Rightarrow$ What are the periodic functions over $\mathscr{L}$?

Weierstrass's function

Def. f is an elliptic function iff

- f is doubly periodic: $f(z+\omega_i) = f(z)$;
- f is analytic (except at poles), with no finite singularities (except at poles)

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \mathscr{L}, \omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

Thm. $\wp$ is differentiable and:

$$\wp'(z) = -2 \sum_{\omega \in \mathscr{L}} \frac{1}{(z-\omega)^3}.$$

Prop. $\wp'$ and $\wp$ are periodic on $\mathscr{L}$.

Expansion of $\wp$ near the origin

$$\frac{1}{(z-\omega)^2} = \frac{1}{\omega^2(1-\frac{z}{\omega})^2} = \frac{1}{\omega^2} + \frac{2z}{\omega^3} + \cdots + \frac{kz^{k-1}}{\omega^{k+1}} + \cdots$$

Eisenstein series ($k \geq 2$):

$$G_k(\mathscr{L}) = \sum_{\omega \in \mathscr{L},\, \omega \neq 0} \frac{1}{\omega^k}$$

$$\wp(z) = \frac{1}{z^2} + 3z^2 G_4 + 5z^4 G_6 + \cdots$$

Rem. Fast expansion of $\wp$ in BoMoSaSc08.

Link with elliptic curves

$$g_2 = 60\,G_4, \quad g_3 = 140\,G_6$$

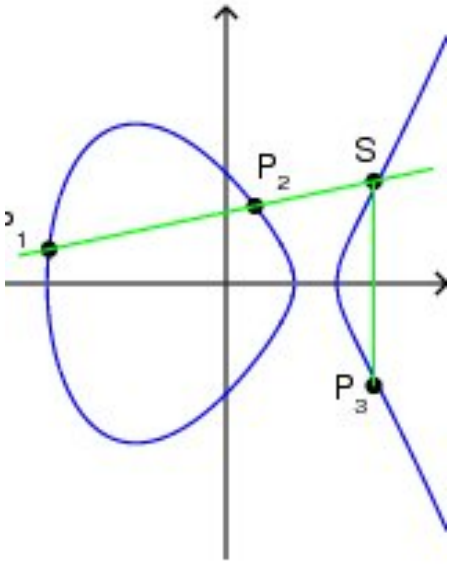
$$\forall\, z \in \mathbb{C} - \mathscr{L},\ \wp'^2(z) = 4\,\wp(z)^3 - g_2\,\wp(z) - g_3$$

We get a parametrization

$$\begin{array}{ccc} \mathbb{C} - \mathscr{L} & \to & E \\ z & \mapsto & (\wp(z), \wp'(z)) \end{array}$$

(and we send $\mathscr{L}$ to O_E.)

Group law



On $E : y^2 = x^3 + ax + b$, to find

$$(x_3, y_3) = (x_1, y_1) \oplus (x_2, y_2),$$

relate $\wp(z_1 + z_2)$ to $\wp(z_1)$ and $\wp(z_2)$.

$$P_1P_2 : y = \lambda x + \mu, \quad x_1 + x_2 + x_3 = -\lambda^2$$

with

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P_2 \neq P_1 \\ \dfrac{3x_1^2 + a}{2y_1} & \text{if } P_2 = P_1 \end{cases}$$

$\Rightarrow$ algebraic formulas; ditto for $[k]P = \underbrace{P \oplus \cdots \oplus P}_{k \text{ times}}$.

The j-invariant

$$\Delta(\tau) = g_2^3(\tau) - 27\, g_3^2(\tau) = q \prod_{n \geq 1} (1 - q^n)^{24} = \eta(q)^{24}$$

$$j(\tau) = 1728\, \frac{g_2^3(\tau)}{\Delta(\tau)}$$

$$j(q) = \frac{1}{q} + 744 + \sum_{n \geq 1} c_n\, q^n, c_n \in \mathbb{N}$$

where $q = \exp(2i\pi\tau)$.

Def. $\mathscr{L}'$ and $\mathscr{L}$ are isomorphic iff there exists P in $SL_2(\mathbb{Z})$ s.t.

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = P \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}.$$

Thm. $\mathscr{L}$ and $\mathscr{L}'$ are isomorphic iff $j(\mathscr{L}) = j(\mathscr{L}')$.

Isogenous lattices

Def. $\mathscr{L}$ and $\mathscr{M}$ are isogenous iff $\exists \alpha \in \mathbb{C}, \alpha\mathscr{L} \subset \mathscr{M}$.

Most interesting case: $\mathscr{M}$ is a sublattice of $\mathscr{L}$ s.t. $\mathscr{L}/\mathscr{M}$ is cyclic of finite index. In other words:

$$\mathscr{M} = (a\omega_1 + b\omega_2)\mathbb{Z} + (c\omega_1 + d\omega_2)\mathbb{Z}$$

and $ad - bc = m$ with $\gcd(a,b,c,d) = 1$.

Fundamental theorem (modular polynomial):
$\exists \alpha \in \mathbb{C}$ s.t. $\alpha\mathscr{M} \subset \mathscr{L}$ iff $\exists m$ s.t. $\Phi_m(j(\mathscr{M}), j(\mathscr{L})) = 0$ where

$$\Phi_m(X,\tau) = \prod_{A \in \mathscr{S}_m} (X - j(A\tau)) = \sum_{k=0}^{\mu_0(m)} C_k(\tau) X^k,$$

$$\mathscr{S}_m = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, ad = m, \gcd(a,b,d) = 1, a > 0, d > b \geq 0 \right\}$$

of cardinality $\mu_0(m) = m\prod_{p|m}(1 + 1/p)$.

Translation old-new

Define $\lambda(t) = k(t)^2$ which parametrizes the Legendre form of an elliptic curve $y^2 = x(x-1)(x-\lambda)$.

Def. Klein absolute invariant

$$J(t) = j(t)/1728 = \frac{4}{27}\frac{(1-\lambda(t)+\lambda(t)^2)^3}{\lambda(t)^2(1-\lambda(t))^2}.$$

Computing resultants with $j(k)$, $j'(\ell)$ and $k^2(1+\ell)^2 = 4\ell$ yields $\Phi_2(j,j')$

Rem. Theta functions are lurking. . . !

The curve $X_0(N)$

More abstract definition:

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

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

Thm. $X_0(N) = \widehat{\mathbb{H}^*/\Gamma_0(N)}$ is a curve, called *modular curve* of completely explicit genus $g_0(N)$.

Thm. An equation for $X_0(N)$ is $\Phi_N(X, Y) = 0$.

Def. $X_0(N)(\mathbf{K}) =$ reduction of $X_0(N)$.

Modular interpretation: $X_0(N)$ parametrizes pairs (E, C) where C is a rational cyclic subgroup of E of order N.

Some applications in number theory

- Shimura/Taniyama/Weil/Wiles/etc.: All elliptic curves are modular. There exists $\varphi : X_0(N) \to E$ where N is the conductor of E ($N \mid \Delta(E)$). Computing φ is already a problem of its own.
- CM constructions:
  - Production of class invariants, that is "small" generators.
  - Fast construction of class polynomials (Sutherland et al).
- Basis of the Elkies/Atkin improvements to Schoof's algorithm (SEA).
- Crypo applications: Frey et al use some $X_0(N)(\mathbb{F}_p)$ of genus $g \geq 4$ using Hecke operators; complexity in $O(p)$. But DLP turned out to be easier...
- ...

III. Computing modular equations

Thm.

- $\Phi_m(X,Y) \in \mathbb{Z}[X,Y]$;
- $\Phi_m(Y,X) = \Phi_m(X,Y)$;
- if m is squarefree, then the coefficient of highest degree of $\Phi_m(X,X)$ is ± 1.

Prop. ("Cyclotomic" properties)
(a) If $(m_1,m_2) = 1$, then

$$\Phi_{m_1 m_2}(X,J) = \mathrm{Resultant}_Z(\Phi_{m_1}(X,Z), \Phi_{m_2}(Z,J)).$$

(b) If $m = \ell^e$ with $e > 1$, then

$$\Phi_{\ell^e}(X,J) = \mathrm{Resultant}_Z(\Phi_\ell(X,Z), \Phi_{\ell^{e-1}}(Z,J))/\Phi_{\ell^{e-2}}(Z,J)^\ell.$$

Thm. (Kronecker) If ℓ is prime, then

$$\Phi_\ell(X,Y) \equiv (X^\ell - Y)(Y^\ell - X) \bmod \ell.$$

A) Algorithms

Remember that

$$j(q) = \frac{1}{q} + 744 + \sum_{n \geq 1} c_n q^n.$$

Then $\Phi_\ell(X, Y)$ is such that $\Phi_\ell(j(q), j(q^\ell))$ vanishes identically.

Naive method: indeterminate coefficients (over $\mathbb{Q}$ or small p's); at least $\tilde{O}((\ell^2)^\omega)$ operations over $\mathbb{Q}$.

Ex.

$$\Phi_2(X, Y) = X^3 + X^2\left(-Y^2 + 1488\,Y - 162000\right)$$

$$+X\left(1488\,Y^2 + 40773375\,Y + 8748000000\right)$$

$$+Y^3 - 162000\,Y^2 + 8748000000\,Y - 157464000000000.$$

Height

Thm. (P. Cohen)
$H(\Phi_m) = 6\mu_0(m)(\log m - 2\sum_{p|m}(\log p)/p + O(1))$.

ℓ	101	211	503	1009	2003
$H(\Phi_\ell)$	3985	9256	24736	53820	115125
PCohen	2768	6743	18736	41832	91320

$\Rightarrow$ Φ_ℓ has $O(\ell^2)$ coefficients of size $\ell \log \ell$, or a $\tilde{O}(\ell^3)$-bit object.

Computing modular polynomials (cont'd)

Enneper (1890) use q-expansion of j and $j(q^\ell)$ with $O(\ell^2)$ terms; Atkin used this modulo CRT primes. $\tilde{O}(\ell^3 \mathsf{M}(p))$

Charles+Lauter (2005): compute Φ_ℓ modulo p using supersingular invariants mod p, Mestre *méthode des graphes*, ℓ torsion points defined over $\mathbb{F}_{p^{O(\ell)}}$ and interpolation. $\tilde{O}(\ell^4 \mathsf{M}(p))$

Enge (2004); Dupont (2004): use complex floating point evaluation and interpolation. $\tilde{O}(\ell^3)$

Bröker, Lauter, Sutherland (2010): Under the Generalized Riemann Hypothesis (GRH), expected running time of $O(\ell^3 (\log \ell)^3 \log\log \ell)$, and compute $\Phi_\ell \bmod p$ using $O(\ell^2 (\log \ell)^2 + \ell^2 \log p)$ space.

B) Real life: choosing other modular polynomials

Why? Always good to have the smallest polynomial so as not to fill the disks too rapidly... For small ℓ, Φ_ℓ is not a desperate choice.

Key point: any function on $\Gamma_0(\ell)$ (or $\Gamma_0(\ell)/\langle w_\ell \rangle$) will do. In particular, if

$$f(q) = q^{-v} + \cdots$$

then there will exist a polynomial $\Phi_\ell[f](X,Y)$ s.t.

$$\Phi_\ell[f](j(q), f(q)) \equiv 0.$$

This polynomial will have $(v+1)(\ell+1)$ coefficients, and height $O(v \log \ell)$.

Choosing f

Atkin proposed several choices:

- canonical choice $f(q)$ using some power of $\eta(q)/\eta(q^\ell)$ where:
$$\eta(q) = q^{1/24}\prod_{n\geq 1}(1-q^n).$$
$\Rightarrow$ family of curves.
- a difficult method (the laundry method) for finding (conjecturally) the f with smallest v (that he is now able to rewrite as θ-functions with characters).

Alternatively, one may use some linear algebra on functions obtained via Hecke operators.

Examples

ℓ	r	H	$\deg(J)$	eval(s)	interp(s)	tot (d)	Mb gz
3011	5	7560	200				368
3079	97	9018	254	7790	640	23	547
3527	13	9894	268	799	1440	3	746
3517	97	10746	290	12400	1110	42	850
4003	13	11408	308	1130	2320	4	1127
5009	5	13349	334	880	3110	3	1819
6029	5	16418	402	1550	6370	7	3251
7001	5	19473	466	2440	11700	13	5182
8009	5	22515	534	3500	20000	22	7905
9029	5	25507	602	5030	33100	35	11460
10079	5	28825	672	7690	56300	61	16152

C) Special values of N

For each G, there is a finite number of N with $g_0(N) = G$

$\Rightarrow$ tables for fixed genus, classification (hyperelliptic, bi-elliptic, etc.).

$\Rightarrow$ finding an equation with j (for ECPP, crypto);

or a "minimal" normalized equation for $X_0(N)$.

Rem. We can use computer algebra to find rational parametrizations (e.g., `algcurves[parametrization]` in MAPLE). For $\Phi_2(X, Y)$, we get

$$Y = \frac{(T+16)^3}{T}, \quad X = \frac{(T+256)^3}{T^2}.$$

The genus 0 case

$\mathscr{N}_N = q^{1/N}(1+\ldots)$ and $\deg_J = 1$; $\mathfrak{w}_N = \eta(z/N)/\eta(z)$.

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	$\mathscr{N}_N$	$1/c(\mathscr{N}_N)$
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

Elkies's computation of modular towers (1/3)

$X_0(\ell^n)$ has something to do with cyclic isogenies of degree ℓ^n between elliptic curves

$$E_0 \to E_1 \to \cdots \to E_n$$

and we get a tower of maps:

$$X_0(\ell^n) \to X_0(\ell^{n-1}) \to \cdots \to X_0(\ell^2) \to X_0(\ell)$$

where all maps are of degree ℓ.

Trick: one may compute this tower from $X_0(\ell^2) \to X_0(\ell)$ and Atkin-Lehner involutions, using dual isogenies

$$\begin{array}{ccccccc} E_0 & \to & E_1 & \to & \cdots & \to & E_n \\ & & \downarrow & & \vdots & & \downarrow \\ & & E_0 & & & & E_{n-1} \end{array}$$

Elkies (2/3)

Example: $X_0(2)$ can be parametrized by $h_2 = \left(\frac{\eta(\tau)}{\eta(2\tau)}\right)^{24}$ and $X_0(4)$ can be parametrized by

$$\xi = 1 + \frac{1}{8}\left(\frac{\eta(\tau)}{\eta(4\tau)}\right)^8$$

such that

$$h_2 = 8\frac{(\xi+1)^2}{\xi - 1}.$$

Remember that $\Phi[h_2](X,J) = (X+16)^3 - JX$.

Elkies (3/3)

Thm. $x_j = \xi(2^{j-1}\tau)$, $0 < j < n$; then $(x_1, \ldots, x_{n-1})$ identifies $X_0(2^n)$ with $(\mathbf{P^1})^{n-1}$ via

$$(x_j^2 - 1)(z_{j+1}^2 - 1) = 1, \quad j = 1, \ldots, n-2,$$

$$z_j = (x_j + 3)/(x_j - 1).$$

In characteristic 2: $y_j = 1 - x_j^{-1}$ and

$$y_{j+1}^2 = y_j^3 + y_j^2 + y_j$$

and this is Garcia/Stichtenoth.

For $X_0(3^n)$:

$$(x_j^3 - 1)(z_{j+1}^3 - 1) = 1, j = 1, \ldots, n-2,$$

$$z_j = (x_j + 2)/(x_j - 1).$$

V. Application to coding theory

The main construction for AG-codes:
Let $\mathscr{X}$ be an absolutely irreducible smooth projective curve of genus g over $\mathbb{F}_q$;

$P_1, P_2, \ldots, P_n$ $\mathbb{F}_q$-rational points on $\mathscr{X}$;

$D = P_1 + P_2 + \ldots + P_n$;

divisor G on $\mathscr{X}$ with rational support not containing the P_i's $\Rightarrow$ no P_i is a pole of any $f \in L(G)$.

Linear code: $C(D,G)$ is the image of

$$\alpha : L(G) \to \mathbb{F}_q^n$$

where $\alpha(f) = (f(P_1), f(P_2), \ldots, f(P_n))$.

Theory (con't)

Thm. If $2g-2 < \deg(G) < n$, the $C(D,G)$ has parameters $[n,k,d]$ where

$$\begin{aligned} n &= \deg(D) \\ k &= \deg(G) - g + 1 \\ d &\geq \delta_1 = n - \deg(G). \end{aligned}$$

(Proof: use Riemann-Roch)

$\Rightarrow$ the higher n, the better; somewhat constrained by Hasse-Weil.

Generating matrix: if $(f_i)_{1\leq i\leq k} \in L(G)$, then the matrix is $(f_i(P_j))$.
$\Rightarrow$ how do we build the f_i's in general?

Easy examples

(From Hiramatsu and Köhler)

$\mathscr{X} = \mathbf{P}^1$, $g = 0$, $\#\mathscr{X} = q+1$.

Points: $(x:1)$ for $x \in \mathbb{F}_q$ and $O_{\mathscr{X}} = (1:0)$.

Alternatively: $P_i = (\alpha^i : 1)$ for primitive α.

$D = \sum_{i=0}^{q-2} P_i$, $G = (k-1)O_{\mathscr{X}}$ for some $k < q-1$.

Basis of $L(G) = \{1, x, x^2, \ldots, x^{k-1}\}$ and $C(D,G)$ is a Reed-Solomon code.

Using elliptic curves

$\mathscr{X}$ = elliptic curve over $\mathbb{F}_q$ with $g = 1$ and n points.

$$D = P_1 + P_2 + \cdots + P_n, G = mO_{\mathscr{X}},$$

for $0 < m < n$. The code $C(D,G)$ has parameters $[n,m,d]$ with $d \geq n - m$.

Hasse-Weil. $q + 1 - 2\sqrt{q} \leq n \leq q + 1 + 2\sqrt{q}$.

When $q = p^{2n}$, maximal curves exist with $n = (p^n + 1)^2$ points. These curves are supersingular and are easily constructible.

When $q \neq \square$, put $r = \lfloor 2\sqrt{q} \rfloor \leq 2\sqrt{q} < r + 1$ so that

$$0 \leq 4q - r^2 = D < 2r + 1 = O(\sqrt{q}).$$

If $D = f^2 D_K$ with small D_K, we can construct $\mathscr{X}$ using the CM method.

How modular curves enter the game

Thm. (Tsfasman, Vlăduţ, Zink) Let $X_0(N)$ be a modular curve of genus $g_0(N)$. Then, for $q = p^2$,

$$\lim_{N \to +\infty} \frac{g_0(N)}{\#X_0(N)(\mathbb{F}_q)} = \frac{1}{\sqrt{q} - 1}$$

where N runs over a set of primes different from p.

follows from

Thm. $g_0(N) \approx N/12$.

Thm. $\#X_0(N)(\mathbb{F}_{p^2}) = (p-1)g_0(N) + O(1)$.
Proof: consequence of Hasse-Weil.

In “practice”: everything can be constructed in polynomial time.

A numerical example (1/2)

$$\mathscr{X} = X_0(27) : Y^2 - Y = X^3 - 7, \quad g = 1$$

$$\#\mathscr{X}(\mathbb{F}_2) = 2 + 1 - 0 = 3,$$
$$\#\mathscr{X}(\mathbb{F}_{2^n}) = 2^n + 1 - (\alpha_1^n + \overline{\alpha}_1^n), \quad \alpha_1 = \sqrt{-2},$$

Rem. For the Hermitian friends, this curve is birationally equivalent to $X^3 + Y^3 + Z^3 = 0$.

$$\#\mathscr{X}(\mathbb{F}_{2^2}) = 4 + 1 - ((-2) + (-2)) = 9 = 3^2.$$

$$\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1) = \{0, 1, \alpha, \alpha^2\}.$$

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	$O_{\mathscr{X}}$
x	0	0	1	1	α	α	α^2	α^2	0
y	α	α^2	0	1	0	1	0	1	1
z	1	1	1	1	1	1	1	1	0

A numerical example (2/2)

$$D = \sum_{i=1}^{8} P_i, \quad G = 2O_{\mathscr{X}}$$

$\Rightarrow C(D,G)$ has parameters $[8,2,\geq 6]$. $L(G) = \{1,u\}$, so that

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha & \alpha^2 & \alpha^2 \end{pmatrix}$$

is of rank 2 and the minimal distance is actually 6.

$L(4O_{\mathscr{X}}) = \{1,u,u^2,v\}$, code $[8,4,4]$ (auto-dual).

Conclusions

- **New input for towers?** quotients of $X_0(N)$ by a subgroup of the Atkin-Lehner involutions.
- **More crypto applications?** study more carefully modular elliptic curves to understand if they are weak or not.
- **Big open path:** the genus 1 case is quite well known. Theory exists for other genera. In practice? Most probably, theta-functions are the key.

Borwein and Borwein I

$a_{n+1} = (a_n + b_n)/2, \quad b_{n+1} = \sqrt{a_n b_n}$ converge towards $M(a,b)$ which is such that $M(a,b) = M((a+b)/2, \sqrt{ab})$.

$M(1,b) = (1+b)/2M(1, \frac{2\sqrt{b}}{1+b})$.

$K(k) = \frac{\pi}{2M(1,k')}$.

$M(1,k') = \theta(q)^{-2}$ where q is the unique solution in $(0,1)$ to $K(k) = \frac{\pi}{2}\theta(q)^2$.

À la Cayley I

$$\frac{M(\ell,k)dy}{\sqrt{(1-y^2)(1-\ell^2y^2)}} = \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}}.$$

$M(\ell,k)$ is a *multiplier*.

$n=3$: $k^2 = \frac{t^3(2+t)}{2t+1}$, $\ell^2 = \frac{t(2+t)^3}{(2t+1)^3}$. $M = 1/(2t+1)$.

$\lambda(t) = k(t)^2 = (\theta_2(q)/\theta_3(q))^2$ $q = \exp(i\pi t)$ is a λ-modular function.

$$J(t) = \frac{4}{27}\frac{(1-\lambda(t)+\lambda(t)^2)^3}{\lambda(t)^2(1-\lambda(t))^2}.$$

More stuff I

More generally: Suppose K, K', L, L' are integrals of modulus k, k', ℓ, ℓ'; suppose also that

$$n\frac{K'}{K} = \frac{L'}{L}$$

for some positive integer n. Then a modular equation of degree n is a relation between k and ℓ.