PARI workshop – Grenoble 2020

Computing modular equations

Razvan Barbulescu
IMB (CNRS, INP, Inria, Univ Bordeaux)

Plan of the lecture

- Motivation
- Fricke (Weber) functions

Motivation : Pollard's $p - 1$ algorithm

Pollard's $p - 1$ algorithm

Input

- a non-prime power odd integer N
- a parameter B

Output the product of prime powers p^e of N such that $\varphi(p^e)$ is B-smooth

$a \leftarrow$ random value in $\mathbb{Z}/N\mathbb{Z}$
$M \leftarrow (B!)^{\lfloor \log_2 B \rfloor}$
$a_M \leftarrow a^M \bmod N$
return $\gcd(a_M - 1, N)$

Motivation : Pollard's $p-1$ algorithm

Pollard's $p-1$ algorithm

Input

- a non-prime power odd integer N
- a parameter B

Output the product of prime powers p^e of N such that $\varphi(p^e)$ is B-smooth

$a \leftarrow$ random value in $\mathbb{Z}/N\mathbb{Z}$
$M \leftarrow (B!)^{\lfloor \log_2 B \rfloor}$
$a_M \leftarrow a^M \bmod N$
return $\gcd(a_M - 1, N)$

$\boxed{\text{Drawback: if it fails one cannot start again.}}$

The elliptic curve method of factorization (ECM)

H. Lenstra's ECM algorithm (modern variant)

Input

- a non-prime power odd integer N
- a parameter B

Output a non-trivial factor of N

repeat

E elliptic curve with rational coeffs and $P \in E(\mathbb{Q})$

$M \leftarrow (B!)^{\lfloor \log_2 B \rfloor}$

$(x_M : y_M : z_M) \leftarrow [M](x : y : 1)$ on $E(\mathbb{Z}/N\mathbb{Z})$

return $g = \gcd(z_M, N)$

until $1 < g < N$

The elliptic curve method of factorization (ECM)

H. Lenstra's ECM algorithm (modern variant)

Input

- a non-prime power odd integer N
- a parameter B

Output a non-trivial factor of N

repeat

Select E depending on N.

E elliptic curve with rational coeffs and $P \in E(\mathbb{Q})$

$M \leftarrow (B!)^{\lfloor \log_2 B \rfloor}$

$(x_M : y_M : z_M) \leftarrow [M](x : y : 1)$ on $E(\mathbb{Z}/N\mathbb{Z})$

return $g = \gcd(z_M, N)$

until $1 < g < N$

Drawback : one does not use the form of N even if $N = a^2 + b^2$.

ECM-friendly elliptic curves

Definition

The Galois representation of E and an integer N is

$$\begin{array}{rcl} \rho: \ \mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q}) & \to & \mathrm{Aut}(E[N]) \simeq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \\ \sigma & \mapsto & (P(x:y:z) \mapsto (\sigma(x):\sigma(y):\sigma(z)). \end{array}$$

ECM-friendly means $\exists N, H \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that $\mathrm{Im}_{E,N} \subset H$

#	Family	label in our tables	comment	$\subset$
1	Section 10.3.1 of [Mon92] Section 2.1 of [BL09]	X_{13}	Montgomery form twisted Edwards	1
2	Section 1.1 of [BL09]	X_{13f}	$a = -\square$ twisted Edwards	1
3	Section 2.1 of [BL09]	X_{13h}	$E(\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$ Edwards curves $a = \square$ twisted Edwards	1
4	Section 2 of [HMR16]	$3\mathrm{B}^0$-$3a$	isogenous to a curve with a point of order 3	
5	Section 10.3.2 of [Mon85] and [Suy85]	X_{13}, $3\mathrm{B}^0$-$3a\mathrm{T}2$	Suyama	1,4
6	Section 3.2 of [AM93]	$5\mathrm{D}^0$-$5b\mathrm{T}1$	$E(\mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z}$	
7	Section 3.3 of [AM93]	$7\mathrm{E}^0$-$7b\mathrm{T}1$	$E(\mathbb{Q}) \simeq \mathbb{Z}/7\mathbb{Z}$	
$\vdots$	$\vdots$	$\vdots$	$\vdots$	
œ 23	Section 3.4.1 of [BBBKM12], $e = \frac{g^2-1}{2g}$	X_{189d}	exceptional Galois	1,3,12,16

Table: Literature families and $\rho_{E,N}$ they parametrize.

Mazur's program B

Theorem (Fricke and Weber in IXX$^{\text{th}}$ century then Shimura in 1971)

Let $H \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be such that $-I \in H$ and $\det(H) = (\mathbb{Z}/N\mathbb{Z})^*$, Then there exists a plane curve $C(j,t) = 0$ such that
$\mathrm{Im}\rho_{E,N} \subset H$ (up to conjugacy) if and only if $\exists t \in \mathbb{Q}$ such that $C(j,t) = 0$.

Mazur's program B

Given a number field K, all N and $N \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, parametrize the set of (isomorphism classes) of elliptic curves over K such that $\rho_{E,N}$ is contained in H.
Serre's uniformity conjecture states that the set of pairs (N, H) is finite for each K.

Theorem (B. and Shinde 2019)

There are 1525 possible images of non CM elliptic curves over $\mathbb{Q}$ in $\prod \mathrm{GL}_2(\mathbb{Z}_\ell)$.

Goal : For the NFS algorithm, compute rapidly many parametrizations.

Fricke forms

Definition

- The Weierstrass $\wp$-function relative to Λ is given by $\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\omega\in\Lambda\setminus\{0\}}(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2})$ for $z \in \mathbb{C}$.
- The Weber form of $\vec{v} = (a,b) \in (\mathbb{Z}/N)^2$ is $\wp(\frac{az+b}{N}; \langle 1, z\rangle)$ belongs to $\mathcal{E}_2(\Gamma(N)) \subset \mathcal{M}_2(\Gamma(N))$.
- The Fricke function of $\vec{v}$,

$$f_{\vec{v}}(z) = \frac{9}{\pi^2}\frac{E_4(z)E_6(z)}{\Delta}\wp_z(\frac{az+b}{N}),$$

belongs to $\mathcal{M}_0(\Gamma(N))$.

Direct properties

- For a given $z \in \mathbb{C}$, let E be such that $j(E) = j(z)$. Then $\{\wp_z(\frac{az+b}{N}) \mid 0 \le a, b \le N, \gcd(a,b,N) = 1\}$ are the x-coords of the points of order N.
- For $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and $v = (v_1, v2)$, $f_{\alpha\cdot v}(z) = f_v(\frac{az+b}{cz+d})$.
- $\mathcal{F}_N = \mathbb{Q}(\zeta_N, \{f_v\}_v)$ and $\mathrm{Gal}(\mathcal{F}_N/\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\pm I$.

Fricke forms : more properties

q-expansion of the Fricke functions

$\mathcal{F}_N = \{f \in \mathcal{M}_0(\Gamma(N)) \mid$ coeffs at ∞ belong to $\mathbb{Q}(\zeta_N)\}$.
We note ζ_N an N^{th} root of unity and we recall the q-expansion:

$$f_{\vec{v}} = 1 + \frac{6}{\frac{\zeta^d+\zeta^{-d}}{2} - 1} + 12 \sum_{m=1}^{\infty} \Big(1_{m\equiv 0 \bmod N} \cdot \sigma\Big(\frac{m}{N}\Big) + \sum_{\substack{r \mid m \\ \frac{m}{r} \equiv c \bmod N}} r\zeta^{dr} + \sum_{\substack{r \mid m \\ \frac{m}{r} \equiv -c \bmod N}} r\zeta^{-dr}\Big) q^{\frac{m}{N}}.$$

Properties

- $\sum_v f_v = 0$ the sum being all order-N points v modulo $-I$.
- $\dim_{\mathbb{Q}(\zeta_N)} \mathrm{Span}(\{f_v\}_v) = \#\{f_v\}_v - 1$.
- Let $H \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and let Γ be such that $\mathrm{GL}_2(\mathbb{Z})/\Gamma(N) \simeq H$, Then

$$\dim_{\mathbb{Q}(\zeta_N)} \mathcal{E}_2(\Gamma) = n_\infty(\Gamma \bigcap \mathrm{SL}_2(\mathbb{Z})) - 1.$$

- Numerical evaluation : linear convergence.
- poles on the cusps, zeros can be computed in poly(N) time.

Computing equations : main idea

Method

- Step 1: compute $g = \sum c_v f_v$ such that $\mathcal{F}_N^H = \mathbb{Q}(\zeta, j, g)$

$$
\begin{tikzcd}
 & \mathcal{F}_N \supset \mathrm{Span}_{\mathbb{Q}(\zeta_N)}(\{f_v\}_v) \arrow[d, dash] \\
\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\pm I & \mathcal{F}_N^\Gamma = \mathbb{Q}(\zeta, j, g) \text{ where } g = \sum_v c_v f_v \arrow[d, dash, "\mathrm{H}"'] \\
 & \mathbb{Q}(\zeta, j)
\end{tikzcd}
$$

- Step 2: compute the characteristic polynomial of g over $\mathbb{Q}(\zeta, j)$

Computing equations : main idea

Method

- Step 1: compute $g = \sum c_v f_v$ such that $\mathcal{F}_N^H = \mathbb{Q}(\zeta, j, g)$

$\mathcal{F}_N \supset \mathrm{Span}_{\mathbb{Q}(\zeta_N)}(\{f_v\}_v)$ $\quad n_\infty(\Gamma(N)) = 1$

$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\pm I$

$\mathcal{F}_N^H \cancel{= \mathbb{Q}(\zeta, j, g) \text{ where } g = \sum_v c_v f_v}$ $\quad n_\infty(\langle \Gamma(N), H \rangle) = 1$

$\mathcal{F}_N^{H_1} = \mathbb{Q}(\zeta, j, g_1)$ where $g_1 = \sum_v c_v f_v$ $\quad n_\infty(\langle \Gamma(N), H_1 \rangle) > 1$

H_1

$\mathbb{Q}(\zeta, j)$

- Step 2: compute the characteristic polynomial of g over $\mathbb{Q}(\zeta, j)$

Computing g : algorithm

Compute σ_1, ..., σ_t such that $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) = \bigcup H\sigma_t$ and a set of generators $\tau_1, \ldots, \tau_{t'}$ of $H \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

Example

- $N = 3$
- $H = C_{\mathrm{ns}}^{+}(3) = \langle \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} \rangle$
- $\sigma_1 = I$, $\sigma_2 = \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}$, $\sigma_3 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$

For each $\tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, compute the matrix of $f(z) \mapsto f(\frac{az+b}{cz+d})$ in basis $\{f_v\}_v$.

Computing g : example

Example

- basis : $f_{0,1}$, $f_{1,0}$, $f_{1,1}$, $\cancel{f_{1,2}}$
- $H \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = \langle -I, \tau \rangle$ where $\tau = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$.
- $f_{0,1} \mapsto f_{2,0} = f_{1,0}$, $f_{0,1} \mapsto f_{1,0}$ and $f_{1,1} \mapsto f_{2,1} = f_{1,2} = (-1)f_{0,1} + (-1)f_{1,1} + (-1)f_{1,2}$.
- Matrix of τ is such that : $M_\tau - I = \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & -1 \\ 0 & 0 & -2 \end{pmatrix}$

Computing g : example

Example

- basis : $f_{0,1}$, $f_{1,0}$, $f_{1,1}$, $\cancel{f_{1,2}}$
- $H \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = \langle -I, \tau \rangle$ where $\tau = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$.
- $f_{0,1} \mapsto f_{2,0} = f_{1,0}$, $f_{0,1} \mapsto f_{1,0}$ and $f_{1,1} \mapsto f_{2,1} = f_{1,2} = (-1)f_{0,1} + (-1)f_{1,1} + (-1)f_{1,2}$.
- Matrix of τ is such that : $M_\tau - I = \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & -1 \\ 0 & 0 & -2 \end{pmatrix}$
- Step 1.a. $w = f_{1,0} + f_{0,1}$ is a generator over $\mathbb{Q}(\zeta_3)$ of the linear combinations fixed by τ. i.e. kernal of $M_\tau - I$.
- Step 1.b. If we had more than one vector $w_1, \ldots, w_k$ we would compute the $\mathbb{Q}$-linear combinations of $\{\zeta_3^i w_j \mid i, j\}$ which are fixed by H not only by $H \cap \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$.
- Step 1.c. Make a symmetric polynomial of conjugates of w by a system of representatives of H/H_1. Here $g = w \cdot w^\sigma$ with $\sigma = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ is such that $H = H_1 \cup H_1\sigma$. Hence $g = (f_{0,1} + f_{1,0})(f_{1,1} + f_{1,2})$.

Computing the charpoly of g (step 2)

Algorithm

1. Step 2.a. Compute the q-expansion of each f_v and deduce the one of g.
2. Step 2.b. Compute $x^n + \sum_{i=0}^{n-1} a_i x^i = \prod_{\sigma \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/H}(x - g^\sigma)$ where $n = [\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : H]$.
3. Step 2.c. For each $c \in \mathbb{Q}(j)$, solve the linear system $\sum_{i=0}^{n} \alpha_i c j^i - \sum_{k=0}^{n} \beta_k j^k = 0$ to obtain $c = \frac{\sum \beta_k j^k}{\sum \alpha_i j^i}$. Output

$$X_H(j, x) = x^n + \sum_{i=0}^{n-1} c_i(j) x^i.$$

Example. poly=

$$(x - (-4 + 48q^{\frac{1}{3}} - 968q - 384q^{\frac{4}{3}} + O(q^2))$$

1. $(x - (-4 + 48\zeta_3 q^{\frac{1}{3}} - 968q - 384\zeta_3 q^{\frac{4}{3}} + O(q^2))$
   $(x - (-4 + 48\zeta_3^2 q^{\frac{1}{3}} - 968q - 384\zeta_3^2 q^{\frac{4}{3}} + O(q^2)))$
2. $C(j, x) = 64j^3 + 48j^2x + 12jx^2 + x^3 - 110592j^2$ isomorphic to $C(j, x) = j - x^3$.

Alternative method : Siegel functions

Definition

For any $v \in \mathbb{Q}^2$ we call Siegel function

$$g_v = -e^{v_2(v_1-1)} q^{\frac{1}{2}B_2(v_1)}(1-q^{v_1}e^{2\pi i v_2}) \prod_{i=1}^{\infty}(1-q^{n+v_1}e^{2\pi i v_2})(1-q^{n-v_1}e^{-2\pi i v_2})$$

Properties

1. g_v^{2N} is a modular function of level N. A Klein form is g_v/η^2 has weight -1.
2. $\mathbb{Q}(\zeta_N, \{g_v\}_v) = \mathcal{F}_N$.
3. For any $\alpha \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, $g_{\alpha v}(z) = g(z \circ \alpha)$.
4. The only zeros and poles are at the cusps we and a closed formula for their order.

Literature

One generates several Γ-modular forms as $\prod g_v^{e_v}$ which have a single pole. Then one computes a polynomial to cancel these functions and obtains a model of $\mathcal{H}^*/\Gamma$.

1. Ligozat 1977, Halberstadt 1998, Chen and Cummins 2004, Daniels 2013 made numerical examples.
2. Zywina 2015 and later Zywina and Sutherland 2017 compute models systematically for all prime-powers ℓ^k with $\ell \leq 37$ when $g = 0$.

Objectives

1. Given a number field k, classify automatically the ECM-friendly curves with coeffs over K (results can be easily checked).

2. For all primes p up to a large bound compute the equations in a certified manner (ball arithmetic) and fast (using arp software ?). Use quadratic Chabauty to prove the set of K-rational points.