Modular curves over number fields and ECM

F. Morain

ANTS XV

Bristol (home of the *hill climbing* algorithms)

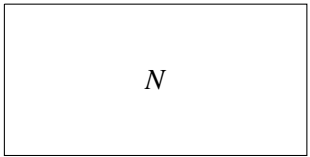
August 8, 2022

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

I. Motivation

The factoring problem: write $N = \prod_{i=1}^{k} p_i^{e_i}$.

Pre-quantum factorization era: how to factor a given (large [1]) integer N?



[1] $N > 55$

Factoring integers

Few ideas:

- trial division;
- Pollard's RHO;
- Pollard's $p-1$ and variants: $p+1$, ECM, etc.;
- Shanks's SQUFOF;
- Kraitchik: find non trivial solutions to $x^2 \equiv 1 \bmod N$ (quadratic sieve in $L_N[1/2,c]$; number field sieve in $L_N[1/3,c]$).

Two contexts:

- smoothness testing of small numbers (e.g., for NFS): a lot of small numbers to be treated as fast as possible;
- record numbers: spend a lot of time with these methods before resorting to heavy methods such as NFS.

$L_N[\alpha,c] = \exp((c+o(1))(\log N)^{\alpha}(\log\log N)^{1-\alpha})$.

Using number fields to factor N

In NFS, we use a polynomial $f(X) \in \mathbb{Z}[X]$ and a known root of $f(m) \equiv 0 \bmod N$, so that we can use $K = \mathbb{Q}[X]/(f(X))$ as an ancillary field.

The first examples include: $f(X) = \Phi_d(X)$, $X^n - a$, etc. First targets were Cunningham numbers $b^s \pm 1$.

The same reasonning enables use to use elliptic curves over number fields to factor such numbers with ECM.

II. ECM

Group law for prime $p > 3$: classical chord-and-tangent $\oplus$ on $(X : Y : Z)$ belonging to $E : Y^2Z = X^3 + AXZ^2 + BZ^3$, $4A^3 + 27B^2 \neq 0$; $O_p = (0 : 1 : 0)$.

For composite N: $\gcd(4A^3 + 27B^2, N) = 1$ and

$$E_N = \{\ (x, y, z),\ y^2z \equiv X^3 + AXZ^2 + BZ^3 \bmod N\ \} \cup \{\ O_N\ \},$$

It is possible to define properly a group law on E_N (Bosma & Lenstra, etc., Edwards, etc.).

Reduction for $p \mid N$ $\quad \rho_p :$

$$\begin{array}{rcl} E_N & \to & E_p \\ O_N & \mapsto & O_p \\ (x : y : z) & \mapsto & (x \bmod p : y \bmod p : z \bmod p). \end{array}$$

"Law": $P_1 \oplus_N P_2 = P_3 = (X_3 : Y_3 : Z_3)$ s.t.

$$\begin{cases} \gcd(Z_3, N) \neq 1 \\ \text{or } \rho_p(P_3) = \rho_p(P_1) \oplus \rho_p(P_2) \text{ for all } p \mid N \end{cases}$$

The ECM algorithm

Algorithm 1: Factoring with elliptic curves

Function ECM$(N, J, (E, P_0))$

Input : N; J max iterations; E a curve modulo N and P_0 on E

Output: A factor of N or FAILURE

$P \leftarrow P_0$

for $j \leftarrow 2$ **to** J **do**

$P \leftarrow [j]P$

// $P = [j!]P_0 = (X_j : Y_j : Z_j)$

if $d = \gcd(Z_j, N) > 1$ **then**

return d

return FAILURE

Works when for some $p \mid N$, $\#\rho_p(E) \mid J!$

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

Analysis of ECM_PLAIN

ECM_PLAIN: we iterate a certain number of times with different (E, P_0) obtained with random A, random $P_0 = (x_0 : y_0 : 1)$ and $B = y_0^2 - (x_0^3 + Ax_0) \bmod N$.

Conj. (H. W. Lenstra, Jr.) ECM_PLAIN finds $p \mid N$ in average time $K(p)(\log N)^2$ where $K(x)$ is s.t.

$$K(x) = \exp\left(\sqrt{(2+o(1))\log x \log\log x}\right) = L_x[1/2, \sqrt{2}]$$

when $x \to +\infty$, using $L_p[1/2, 1/\sqrt{2}]$ curves.

In practice

First factorizations at the end of 1985.

Equations and addition laws: all are possible, with different merits:

- Chudnovsky & Chudnovsky;
- Montgomery: $by^2 = x^3 + ax^2 + x$;
- Edwards: $au^2 + v^2 = 1 + du^2v^2$;
- Kohel, etc.

Algorithmic improvements: phase 1 (PRAC, addition-subtraction chains), phase 2 (fast polynomial arithmetic); 30dd factors easy to find.

Reference implementation: GMP-ECM (P. Zimmermann *et al.*). Record 79dd (2012), see `http://wwwmaths.anu.edu.au/~brent/ftp/champs.txt`.

Finding *good* curves: early attempts

Thm: $E(\mathbb{F}_p) = E_1 \times E_2$, $m_1 \mid m_2$, $m_1 \mid p-1$.

$\Rightarrow$ what really matters is the smoothness of $\mathrm{ord}(P) \mid m_2$.

Ideas: increase smoothness of m_2, either forcing m_1 to be large (bounded by $\sqrt{p}+1$), or m_2 to have a given divisor d (and check that m_2/d still behaves as a random number w.r.t. smoothness).

What can be done:

- Find some E s.t. $E_{\mathrm{tor}}(K)$ contains some (large) $\mathscr{T} = \mathbb{Z}/M_1\mathbb{Z} \times \mathbb{Z}/M_2\mathbb{Z}$, in which case $E \bmod p$ will have $M_1 \mid m_1$, $M_2 \mid m_2$ (if (p) splits in K).
- Find an infinite family *ditto*.
- Find infinite family (E, P) with P of infinite order. **Relaxed in this talk**

What is a good curve, actually?

Montgomery: an interesting quantity is

$$c(\ell) = \lim_{x \to +\infty} \frac{1}{\pi(x)} \sum_{p \leq x} \mathrm{val}_\ell(\#E(\mathbb{F}_p)).$$

It should be close to

$$\overline{\mathrm{val}}_\ell(E)) = \sum_{k \geq 1} k \cdot \mathrm{Prob}(\{p \text{ prime s.t. } \mathrm{val}_\ell(\#E(\mathbb{F}_p)) = k\}).$$

Idea: (Barbulescu *et al.*) for p of size n,

$$\mathrm{Prob}(\#E(\mathbb{F}_p) \text{ is } B-\text{smooth}) \approx \mathrm{Prob}(m \text{ of size } ne^{\alpha(E)} \text{ is } B-\text{smooth})$$

where (by analogy with NFS)

$$\alpha(E) = \textstyle\sum_\ell \alpha_\ell(E), \text{ with } \alpha_\ell(E) = \log \ell(1/(\ell-1) - \overline{\mathrm{val}}_\ell(E)).$$

Barbulescu *et al.*

Thm. For $E/\mathbb{Q}$ and exact value for $\overline{\text{val}}_\ell(E))$ using Serre's results on torsion points:
(i) $|\alpha(E)| < \infty$.
(ii) $\alpha(E) \geq \alpha_0 \approx -0.812$.

The more $\alpha(E)$ is negative, the better.

$\Rightarrow$ new families (Suyama11, $\alpha(E) = -3.3825$) + Gélin/Kleinjung/Lenstra.

Justifies one way to increase $\overline{\text{val}}_\ell(E)$: have rational ℓ^k-torsion points for some small ℓ and $k > 0$.

III. Using modular curves

Modular curves $X_1(M_1, M_2)_K$ parametrizing elliptic curves E/K having torsion group containing $\mathbb{Z}/M_1\mathbb{Z} \times \mathbb{Z}/M_2\mathbb{Z}$, $M_1 \mid M_2$.

Genus 0 and 1:

M_1	M_2	K	L
1	$\in \{2, \ldots, 10\}, 12$	$\mathbb{Q}$	$\mathbb{Q}$
2	$\in \{2, 4, 6, 8\}$	$\mathbb{Q}$	$\mathbb{Q}$
3	$\in \{3, 6\}$	$\mathbb{Q}$	$\mathbb{Q}(\zeta_3)$
4	4	$\mathbb{Q}$	$\mathbb{Q}(\zeta_4)$
5	5	$\mathbb{Q}$	$\mathbb{Q}(\zeta_5)$

M_1	M_2	$X_1(M_1, M_2)$
1	11	$s^2 - s = t^3 - t^2$
1	14	$s^2 + st + s = t^3 - t$
1	15	$s^2 + st + s = t^3 + t^2$
2	10	$s^2 = t^3 + t^2 - t$
2	12	$s^2 = t^3 - t^2 + t$
3	9	$s^2 = t^3 + 16$
4	8	$s^2 = t^3 - t$
6	6	$s^2 = t^3 + 1$

See Sutherland's tables available on the web, for larger values of genera.

Mazur's theorem and beyond

Thm. (Mazur, 1977) The possible torsion groups of $E/\mathbb{Q}$ are

$$E_{\mathrm{tor}}(\mathbb{Q}) = \begin{cases} \mathbb{Z}/m\mathbb{Z}; & m = 1, 2, \ldots, 10 \text{ or } 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}; & m = 1, 2, 3, 4; \end{cases}$$

and for each of them, we have infinite families (Kubert).

$\Rightarrow$ what happens for a number field?

Thm (Merel, 1996) if E/K of degree d has a point of order p, then $p < 3^{3d^2}$. And there exists a constant $|E_{\mathrm{tor}}| < B(d)$.

Improved to $p < (1 + 3^{d/2})^2$ by Oesterlé.

Thm (Parent, 1999) $p^n \leq 65(3^d - 1)(2d)^6$ for $p \geq 5$; + results for $p \in \{2, 3\}$.

Quadratic fields

Thm. (Kenku/Momose; Kamienny) Let K be a quadratic field and E/K.
The possible torsion groups of $E(K)$ are

$$E_{\mathrm{tor}}(K) = \begin{cases} \mathbb{Z}/m\mathbb{Z}; & 1 \leq m \leq 18, m \neq 17, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}; & 1 \leq m \leq 6, \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}. \end{cases}$$

. . . but does not answer the question for given K. . .

To complicate things: there are curves E/K whose torsion properties appear in L/K.

Higher degree number fields: see references in the paper.

New families

Prop. (for $X_1(4,8)$) Let (t,s) be a point on $X_1(4,8)$, i.e., $s^2 = t^3 - t$. Consider the curve E_t in Edwards form

$$u^2 + v^2 = 1 + d_t u^2 v^2$$

with $d_t = ((t^2-2t-1)/(t^2+2t-1))^4$. Then $E_t/\mathbb{Q}(s,t)$ has torsion group containing $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.

Prop. (for $X_1(2,12)$) Let (t,s) be a point on $X_1(2,12)$, i.e., $s^2 = t^3 - t^2 + t$. Consider the curve $E_{t,s}$ in Edwards form

$$u^2 + v^2 = 1 + d_{t,s} u^2 v^2$$

with

$$d_{t,s} = \left(\frac{8st(t+1)(t-1)^3 - t^8 + 4t^7 - 4t^6 - 20t^5 + 26t^4 - 20t^3 - 4t^2 + 4t - 1}{(t^2+1)^3 (t^2 - 4t + 1)} \right)^2.$$

Then $E_{t,s}$ has torsion group containing $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ over $\mathbb{Q}(s,t)$.

Gathering everything together

For a given K such that $X_1(M_1, M_2)_K$ has generator G

for $k = 1 \ldots$

1. compute the elliptic curve $E_k(K)$ associated with $[k]G$;
2. Use D. Simon's program (say, pari-gp, SageMath) to find if $E_k(K)$ has rank > 0 with generator P_∞.
3. If yes, reduce $(E_k(K), P_\infty)$ modulo N and use it in ECM.

In practice, the height of E_k increases very fast $\Rightarrow$ replace this with a modulo N direct version (see paper).

What is a good curve (cont'd)

In theory:

- when you want $E(K)_{tors} = \mathbb{Z}/M_1\mathbb{Z} \times \mathbb{Z}/M_2\mathbb{Z}$, take a point on $X_1(M_1, M_2)_K$.
- If the genus is 0 or 1, hope for infinite families; otherwise, sporadic examples.
- Adding conditions on the rank of E is sometimes possible (completely done over $\mathbb{Q}$: Atkin+M., Montgomery, etc.).

Approximate $\alpha(E/K)$ for Galois K of degree d by replacing $\alpha_\ell(E)$ with

$$c(\ell) = \lim_{x \to +\infty} \frac{1}{\#\Pi_K(x)} \sum_{p \leq x, p \in \Pi_K} \frac{1}{d} \sum_{i=1}^{d} \mathrm{val}_\ell(\#E_{\theta_i}(\mathbb{F}_p))$$

where $\Pi_K = \{p \text{ prime}, (p) \text{ splits in } K\}$, $M_K(X) = \prod_{i=1}^{d}(X - \theta_i) \bmod p$.

Numerical example

$X_1(11) : s^2 - s = t^3 - t^2$ yield curves (Kubert form)

$$Y^2 + aXY + bY = X^3 + bX^2$$

with

$$a = ((t-1)s - t^3 + t^2 + t)/t, \quad b = t(t-1)(s-t).$$

Over $K\langle T\rangle = \mathbb{Q}(\sqrt{6})$ with point of infinite order $G_K = (18 - 7T : 103 - 42T : 1)$.

k	$[k]G_K = (t,s)$	rank
1	$(18-7T, 103-42T, 1)$	1

$$\alpha = -3.178$$

Application: factoring numbers $b^{6n} \pm 1$.

Statistics for α

M_1, M_2	poly	k	α
$4,8$	$\Phi_{10}(X)$	1	-4.225
$4,8$	$X^4+X^3+2X^2-4X+3$	59	-4.178
$4,8$	X^2+5	85	-4.150
$2,12$	$X^4+X^3+2X^2-4X+3$	21	-3.871
$2,12$	$X^4+X^3+2X^2-4X+3$	10	-3.857
$2,12$	$X^4+X^3+2X^2-4X+3$	75	-3.857
$2,12$	$X^4+X^3+2X^2-4X+3$	66	-3.853
$2,12$	X^2+5	49	-3.847
11	$\Phi_8(X)$	91	-3.248
11	$\Phi_8(X)$	10	-3.243
11	$\Phi_8(X)$	56	-3.234
11	$\Phi_8(X)$	43	-3.232
11	$X^4+X^3+2X^2-4X+3$	43	-3.231

Fine points

- CM curves have to be avoided (or handled with care);
- If $\sigma \in \mathrm{Aut}_K$, $\sigma(E)$ can be used unless $\simeq E$;
- $\mathbb{Q}$-curves are not interesting: E isogenous to $\sigma(E)$; if K is Galois, isogenous cases can be detected by inspection mod small primes; use Cremona+Najman when K is not Galois.
- What if we do not find a point of infinite order? Use twists.
  - start from $E_1 : Y^2 = X^3 + AX + B$; put $\lambda = x_0^3 + Ax_0 + B$; then $(x_0, 1)$ is a point on $E_\lambda : \lambda Y^2 = X^3 + AX + B$.
  - If $(\lambda/p) = +1$ for $p \mid N$, then $E_\lambda(\mathbb{F}_p)$ will have the desired torsion. $\Rightarrow$ try several values of x_0 (compare Lucas sequences for the $p+1$ method).

IV. Some factorizations

Using $X_1(2,12)_K$ where $K = \mathbb{Q}[X]/(X^3+X^2-22X+5) \subset \mathbb{Q}(\zeta_{67})$; generator $P_\infty = (28/3 - T/4 - T^2/3, -649/24 + 7T/8 + 7/6T^2)$.

N factor of (dd)	$p \mid N$	dd	torsion
$908,67-(190dd)$	$31492\ldots13889$	48	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$
$\langle 2\rangle \times \langle 2\cdot 3\cdot 7^2\cdot 17\cdot 47\cdot 127\cdot 157\cdot 503\cdot 54277\cdot 683759\cdot 11269243\cdot 16866691\cdot 9474758309\rangle$			
$737,67+(184dd)$	$87091\ldots40299$	48	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$
$\langle 2\rangle \times \langle 2^3\cdot 3\cdot 5\cdot 19\cdot 907\cdot 5413\cdot 8807\cdot 22973\cdot 553103\cdot 4764239\cdot 6769901\cdot 10778026289\rangle$			
$682,67+(185dd)$	$39604\ldots28371$	46	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$
$\langle 2\rangle \times \langle 2^3\cdot 3^2\cdot 13\cdot 67\cdot 5441\cdot 11353\cdot 19319\cdot 59581\cdot 319399\cdot 13319101\cdot 104393045839\rangle$			
$564,67-(182dd)$	$12006\ldots40793$	46	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$
$\langle 2\rangle \times \langle 2^2\cdot 3^2\cdot 5\cdot 293\cdot 225089\cdot 459509\cdot 1811561\cdot 4338643\cdot 8046043\cdot 1740216437\rangle$			
$517,67-(180dd)$	$43673\ldots26931$	50	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$
$\langle 2\rangle \times \langle 2^4\cdot 3^5\cdot 11\cdot 17\cdot 31^2\cdot 47\cdot 40151\cdot 500389\cdot 717341\cdot 761489\cdot 1183837\cdot 51181421299\rangle$			

More examples

N factor of (dd)	$p \mid N$	dd	torsion, poly
$90,136+(243)$	$95029\ldots16961$	50	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}, Z^2+2$
$\langle 2\rangle \times \langle 2\cdot 3^3\cdot 5\cdot 7\cdot 17\cdot 23^2\cdot 557\cdot 93169\cdot 191507\cdot 211093\cdot 3555857\cdot 19430611\cdot 19286145689\rangle$			
$59,148+(246)$	$61536\ldots56977$	52	$\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}, Z^2-37$
$\langle 2^2\rangle \times \langle 2^4\cdot 3^4\cdot 31\cdot 383\cdot 659\cdot 12413\cdot 44087\cdot 176261\cdot 269231\cdot 4538333\cdot 5268647\cdot 244317397\rangle$			
$74,145+(210)$	$32422\ldots86401$	52	$\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}, Z^2-5$
$\langle 2^2\rangle \times \langle 2^3\cdot 11\cdot 13\cdot 53\cdot 839\cdot 1427\cdot 32647\cdot 658663\cdot 792277\cdot 1532647\cdot 8783009\cdot 48689154383\rangle$			
$517,67-(180)$	$43673\ldots26931$	50	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}, Z^2-67$
$\langle 2\rangle \times \langle 2^4\cdot 3^5\cdot 11\cdot 17\cdot 31^2\cdot 47\cdot 40151\cdot 500389\cdot 717341\cdot 761489\cdot 1183837\cdot 51181421299\rangle$			
$69,145-(196)$	$43973\ldots68891$	50	$\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}, Z^2-29$
$\langle 2\rangle \times \langle 2^3\cdot 5\cdot 13\cdot 1381\cdot 834469\cdot 1456837\cdot 3504673\cdot 29722321\cdot 37912759\cdot 6377193661\rangle$			
$69,145+(136)$	$23129\ldots88531$	52	$\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}, Z^2-29$
$\langle 2\rangle \times \langle 2^2\cdot 11\cdot 13\cdot 43\cdot 66499\cdot 236681\cdot 351023\cdot 1047667\cdot 3274151\cdot 18302677\cdot 135555908207\rangle$			

Conclusions

- The quest for large torsion over $\overline{\mathbb{Q}}$ is bound to finish. Result so far: some extra families.
- Barbulescu + Shinde: special modular curves for curves with exceptional $\rho_{E,m}$.
- Properly define $\alpha(E)$ for E/K. For the time being, generalization to $E/\mathbb{Q}$ as seen in E/K.