MPRI – Cours 2.12.2

F. Morain

Lecture II: Integer factorization

2013/06/26

The slides are available on http://www.lix.polytechnique.fr/Labo/Francois.Morain/MPRI/2012

I. Introduction

Input: an integer N;

Output: $N = \prod_{i=1}^{k} p_i^{\alpha_i}$ with p_i (proven) prime.

Major impact: estimate the security of RSA cryptosystems.

Also: primitive for a lot of number theory problems.

How do we test and compare algorithms?

- Cunningham project,
- RSA Security (partitions, RSA keys) – though abandoned?
- Decimals of π.

What is the factorization of a random number?

$N = N_1 N_2 \cdots N_r$ with N_i prime, $N_i \geq N_{i+1}$.

Prop. $r \leq \log_2 N$; $\overline{r} = \log\log N$.

Size of the factors: $D_k = \lim_{N\rightarrow+\infty} \log N_k / \log N$ exists and

k	D_k
1	0.62433
2	0.20958
3	0.08832

"On average"

$$N_1 \approx N^{0.62}, \quad N_2 \approx N^{0.21}, \quad N_3 \approx N^{0.09}.$$

$\Rightarrow$ an integer has one "large" factor, a medium size one and a bunch of small ones.

II. Smoothness testing

Def. a B-smooth number has all its prime factors $\leq B$.

B-smooth numbers are the heart of all efficient factorization or discrete logarithm algorithms.

De Bruijn's function: $\psi(x, y) = \#\{z \leq x, z \text{ is } y-\text{smooth}\}$.

Thm. (Candfield, Erdős, Pomerance) $\forall\, \varepsilon > 0$, uniformly in $y \geq (\log x)^{1+\varepsilon}$, as $x \rightarrow \infty$

$$\psi(x, y) = \frac{x}{u^{u(1+o(1))}}$$

with $u = \log x / \log y$.

Rem. Algorithms for computing $\psi(x, y)$ by Bernstein, Sorenson, etc.

B-smooth numbers (cont'd)

Prop. Let $L(x) = \exp\left(\sqrt{\log x \log\log x}\right)$. For all real $\alpha > 0$, $\beta > 0$, as $x \to \infty$

$$\psi(x^\alpha, L(x)^\beta) = \frac{x^\alpha}{L(x)^{\frac{\alpha}{2\beta}+o(1)}}.$$

Ordinary interpretation:

> a number $\leq x^\alpha$ is $L(x)^\beta$-smooth with probability
>
> $$\frac{\psi(x^\alpha, L(x)^\beta)}{x^\alpha} = L(x)^{-\frac{\alpha}{2\beta}+o(1)}.$$

Trial division

Algorithm: divide $x \leq X$ by all $p \leq B$, say $\{p_1, p_2, \ldots, p_m\}$.

Cost: all $p \leq B$ costs you $\pi(B)$ divisions steps. More precisely

$$\sum_{p \leq B} T(x, p) = O(m \lg X \lg B).$$

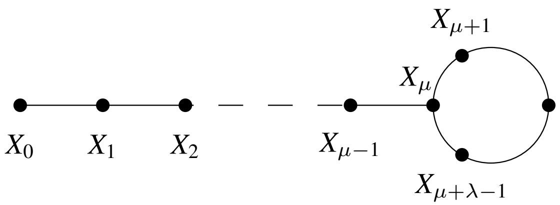
Implementation: use any method to compute and store all primes $\leq 2^{32}$ (one char per $(p_{i+1} - p_i)/2$; see Brent).

Useful generalization: given $x_1, x_2, \ldots, x_n \leq X$, can we find the B-smooth part of the x_i's more rapidly than repeating the above in $O(nm \lg B \lg X)$?

Yes: use product trees and fast arithmetic.

III. Pollard's RHO method

Prop. Let $f : E \to E$, $\#E = m$; $X_{n+1} = f(X_n)$ with $X_0 \in E$.



Thm. (Flajolet, Odlyzko, 1990) When $m \to \infty$

$$\overline{\lambda} \sim \overline{\mu} \sim \sqrt{\frac{\pi m}{8}} \approx 0.627\sqrt{m}.$$

Epact

Prop. There exists a unique $e > 0$ (epact) s.t. $\mu \leq e < \lambda + \mu$ and $X_{2e} = X_e$. It is the smallest non-zero multiple of λ that is $\geq \mu$: if $\mu = 0$, $e = \lambda$ and if $\mu > 0$, $e = \lceil \frac{\mu}{\lambda} \rceil \lambda$.

Floyd's algorithm:

```
X <- X0; Y <- X0; e <- 0;
repeat
    X <- f(X); Y <- f(f(Y)); e <- e+1;
until X = Y;
```

Thm. $\overline{e} \sim \sqrt{\frac{\pi^5 m}{288}} \approx 1.03\sqrt{m}$.

Application to the factorization of N

Idea: suppose $p \mid N$ and we have a random $f \bmod N$ s.t. $f \bmod p$ is "random".

```
function f(x, N) return (x^2 + 1) mod N; end.
function rho(N)
1. [initialization] x:=1; y:=1;
2. [loop]
     repeat
       x:=f(x, N); y:=f(f(y, N), N);
       g:=gcd(x-y, N);
     until g > 1;
3. return g;
```


Theoretical results

Conjecture. RHO finds $p \mid N$ using $O(\sqrt{p})$ iterations.

Thm. (Bach, 1991) Proba RHO with $f(x) = x^2 + 1$ finding $p \mid N$ after k iterations is at least

$$\frac{\binom{k}{2}}{p} + O(p^{-3/2})$$

when p goes to infinity.

Practice

- **Choosing f:**
  - some choices are bad, as $x \mapsto x^2$ et $x \mapsto x^2 - 2$.
  - Tables exist for given f's.
- **Trick:** compute $\gcd(\prod_i (x_{2i} - x_i), N)$, using backtrack whenever needed.
- **Improvements:** reducing the number of evaluations of f, the number of comparisons (see Brent, Montgomery).

IV. Pollard's $p-1$ method

History:

- Invented by Pollard in 1974.
- Williams: $p+1$.
- Bach and Shallit: Φ_k factoring methods.
- Shanks, Schnorr, Lenstra, etc.: quadratic forms.
- Lenstra (1985): ECM.

Overall scheme:

- First phase is generic.
- Second phases:
  - generic: standard, Brent;
  - adapted to finite fields: BSGS + fast convolutions.

First phase

Idea: assume $p \mid N$ and a is prime to p. Then

$$(p \mid a^{p-1} - 1 \text{ and } p \mid N) \Rightarrow p \mid \gcd(a^{p-1} - 1, N).$$

Generalization: if R is known s.t. $p - 1 \mid R$,

$$\gcd((a^R \bmod N) - 1, N)$$

will yield a factor.

How do we find R? Only reasonable hope is that $p - 1 \mid B_1!$ for some (small) B_1. In other words, $p - 1$ is B_1-smooth.

Algorithm: $R = \prod_{p^\alpha \leq B_1} p^\alpha = \text{lcm}(2, \ldots, B_1)$.

Rem. (usual trick) we compute $\gcd(\prod_k ((a^{r_k} - 1) \bmod N), N)$.

Second phase: the classical one

Let $b = a^R \bmod N$ and $\gcd(b - 1, N) = 1$.
Hyp. $p - 1 = Qs$ with $Q \mid R$ and s prime, $B_1 < s \leq B_2$.

Test: is $\gcd(b^s - 1, N) > 1$ for some s.

$s_j = j$-th prime. In practice all $s_{j+1} - s_j$ are small (Cramer's conjecture implies $s_{j+1} - s_j \leq (\log B_2)^2$).

- Precompute $c_\delta \equiv b^\delta \bmod N$ for all possible δ (small);
- Compute next value with one multiplication $b^{s_{j+1}} = b^{s_j} c_{s_{j+1} - s_j} \bmod N$.

Cost: $O((\log B_2)^2) + O(\log s_1) + (\pi(B_2) - \pi(B_1))$ multiplications $+(\pi(B_2) - \pi(B_1))$ gcd's. When $B_2 \gg B_1$, $\pi(B_2)$ dominates.

Rem. We need a table of all primes $< B_2$; memory is $O(B_2)$.

Record. Nohara (66dd of $960^{119} - 1$, 2006; see http://www.loria.fr/~zimmerma/records/Pminus1.html).

Second phase: using the birthday paradox

Consider $\mathcal{B} = \langle b \bmod p \rangle$; $s := \#\mathcal{B}$.

If we draw $\approx \sqrt{s}$ elements at random in $\mathcal{B}$, then we have a collision (birthday paradox).

Algorithm: build (b_i) with $b_0 = b$, and

$$b_{i+1} = \begin{cases} b_i^2 \bmod N & \text{with proba } 1/2, \\ b_i^2\, b \bmod N & \text{with proba } 1/2. \end{cases}$$

We gather $r \approx \sqrt{s}$ values and compute

$$\prod_{i=1}^{r} \prod_{j \neq i} (b_i - b_j) = \text{Disc}(P(X)) = \prod_i P'(b_i) \text{ where } P(X) = \prod_{i=1}^{r} (X - b_i).$$

Using fast polynomial algorithmes takes $O(\mathsf{M}(r) \log r)$ operations modulo N.

V. ECM

- Due to Lenstra in 1985.
- Improvements: Chudnovsky & Chudnovsky; Brent; Montgomery; Suyama; Atkin-FM; etc.
- Powerful method since complexity depends on $p \mid N$: 30dd factors easy; record 79dd (2012), see `http://wwwmaths.anu.edu.au/~brent/ftp/champs.txt`.
- Reference implementation: GMP-ECM (P. Zimmermann); see Zimmermann & Dodson.

A) Pseudo-addition

Let $\gcd(4a^3 + 27b^2, N) = 1$ and

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

Reduction for $p \mid N$

$$\begin{array}{rrcl} \pi_p : & E_N & \rightarrow & E_p \\ & O_N & \mapsto & O_p \\ & (x,y,z) & \mapsto & (x \bmod p, y \bmod p, z \bmod p). \end{array}$$

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

Or: add M_1 and M_2 as if N were prime and wait for something to happen.

B) Factoring with elliptic curves: theory

Ex. Let $N = 143$. Consider $P = (0,1,1)$ on

$$E_N : y^2 \equiv x^3 + x + 1 \bmod N.$$

Computing $[3!]P$:

	P	$Q = [2]P$	$[2]Q$	$[2]Q \oplus Q = [6]P$
N	$(0,1,1)$	$(36,124,1)$	$(127,71,1)$	
11	$(0,1,1)$	$(3,3,1)$	$(6,5,1)$	$(0,10,1)$
13	$(0,1,1)$	$(10,7,1)$	$(10,6,1)$	$(0,1,0)$

From the last line, we add two opposite points mod 13 and

$$\lambda = (124 - 71) \times (36 - 127)^{-1} \bmod 143.$$

but the inverse leads to

$$\gcd(36 - 127, 143) = \gcd(52, 143) = 13.$$

Verification: $\#E_{11} = 14$ (resp. $\#E_{13} = 18 = 2 \times 3^2$); $ord(P_{11}) = 7$ (resp. $ord(P_{13}) = 6$).

The algorithm

```
procedure ECM_PLAIN(N, J)
1. d:=1;
2. choose random x0,y0,a in [0..N-1];
3. b:=(y0^2-x0^3-a*x0) mod N;
4. Delta:=gcd(4*a^3+27*b^2, N);
5. if Delta=N then goto 2; // bad luck!
6. if 1 < Delta < N then
      return Delta; // incredible luck!
7. P:=(x0,y0);
// we operate on E_N : y^2 = x^3 + ax + b mod N containing P
8. for j:=2..J do
      P:=[j]P;
      if some factor d is found then return d;
9. if d=1 then goto 2; // same player try again
```

Rem. the easiest way to have (E,P) is the one given, since we cannot compute $\sqrt{z}$ modulo N.

Question: what is selecting an Edwards pair (E,P) at random?

Analysis of ECM_PLAIN

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

$$K(x) = \exp\left(\sqrt{(2 + o(1)) \log x \log\log x}\right) = L(x)^{\sqrt{2}+o(1)}$$

when $x \rightarrow +\infty$, using $L(p)^{1/\sqrt{2}+o(1)}$ curves.

Proof sketch

ECM_PLAIN succeeds whenever $\#E_p \mid J!$ for some J.

Heuristically: $\#E_p \approx p \Rightarrow \#E_p$ behaves like a random number $\approx p$
$\Rightarrow$ proba $\#E_p \mid J! \approx \frac{1}{p}\psi(p, J)$.

Choosing $J = L(p)^\beta$ yields

$$\frac{1}{p}\psi(p, J) = L(p)^{-1/(2\beta)+o(1)}$$

$\Rightarrow$ we need $L(p)^{1/(2\beta)}$ elliptic curves.

Running time: computing $[J!]P$ is $O(J \log J) = O(L(p)^{\beta+o(1)})$ so total time is

$$O(L(p)^{\beta+1/(2\beta)+o(1)})$$

minimized for $\beta = 1/\sqrt{2}$. $\square$

In practice

First factorizations at the end of 1985.

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

- Chudnovsky & Chudnovsky;
- Montgomery: $by^2 = x^3 + ax^2 + x$, special multiplication algorithm (PRAC);
- Edwards, Kohel, etc.

Algorithmic improvements: phase 1 (addition-subtraction chains), phase 2 (fast polynomial arithmetic).

C) Advanced ECM

Thm. (Lenstra 1987, Howe 1993) Fix p. Then

$$\mathrm{Proba}_{E/\mathbb{F}_p}(\ell^a \mid \#E(\mathbb{F}_p)) \approx \begin{cases} \frac{1}{\ell^{a-1}(\ell-1)} & \text{if } p \not\equiv 1 \bmod \ell^c, \\ \frac{\ell^{b+1}+\ell^b-1}{\ell^{a+b-1}(\ell^2-1)} & \text{if } p \equiv 1 \bmod \ell^c \end{cases}$$

where $b = \lfloor a/2 \rfloor$, $c = \lceil a/2 \rceil$.

(Proof depends on properties of the modular curve $X_0(\ell)$).

Ex. For $\ell = 2$, (x, y) is of order 2 iff $y = 0$, hence look at roots of $x^3 + ax + b$, that can be 0, 1 or 3, hence in 2 cases out of 3.

Another probability model

(Barbulescu, Bos, Bouvier, Kleinjung, Montgomery, ANTS X)

In real life: start from $E/\mathbb{Q}$ and study its reduction modulo p as p varies.

Thm. $\mathrm{Proba}(E(\mathbb{F}_p)[\ell] \sim \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}) = 1/\#\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q})$.

Ex. $E_1 : y^2 = x^3 + 5x + 7$, for which $[\mathbb{Q}(E_1[3]) : \mathbb{Q}] = 48$. One computes $proba = 1/48$ (compared to $20/48$ for $\mathbb{Z}/3\mathbb{Z}$).

Moreover, (complicated) formulas for $\mathrm{Proba}(\ell^k \mid \#E(\mathbb{F}_p))$, showing that it is $> 1/\ell^k$.

D) Curves with large torsion groups for ECM

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

In general: $m_1 \ll m_2$, so $P \in E_2$. What really matters is the smoothness of $\mathrm{ord}(P) \mid m_2$.

Goal: increase smoothness of m_2, either forcing m_1 to be large, or m_2 to have a given divisor.

What can be done:

- (D_0) Find some E s.t. $E_{tors}(K)$ contains some (large) $\mathcal{T} = \mathbb{Z}/M_1\mathbb{Z} \times \mathbb{Z}/M_2\mathbb{Z}$, in which case $E \bmod p$ will have $M_1 \mid m_1$, $M_2 \mid m_2$ (if (p) splits in K).
- (E_∞) Find an infinite family *ditto*.
- (P_∞) *ditto* plus a point P of infinite order.
- Impose some model (Weierstrass, Edwards); sometimes models impose themselves.

The big picture

General problem: given $K \subset \overline{\mathbb{Q}}$, what are the possible torsion groups for $E(K)$?

Thm. (Mazur, 1977) finite list for $\mathbb{Q}$.

Thm. (Merel, 1996) Let E/K where K has degree $d > 1$. If $E(K)$ has a point of order p, then $p < d^{3d^2}$.

$\Rightarrow$ study the modular curves $X_1(M_1, M_2)$.

Def. $X_1(M_1, M_2)$ with $M_1 \mid M_2$; $X_1(M) = X_1(1, M)$, $X_1(M, M) = X(M)$.

Rem. $X_1(M_1, M_2)$ enjoys a so-called modular interpretation, but we do not need it in this talk.

$X_1(M)$ by hand

$M = 2$: $\ominus P = P \iff Y = X^3 + AX + B = 0$.
$M = 3$: $[2]P = \ominus P$ is equivalent to

$$[2]_x = X \iff \left(-12\,XY^2 + 9\,X^4 + 6\,X^2A + A^2\right),$$

$$[2]_y = -Y \iff \left(3\,X^2 + A\right)\left(-12\,XY^2 + 9\,X^4 + 6\,X^2A + A^2\right).$$

$$\Rightarrow 3\,X^4 + 6\,X^2A - A^2 + 12\,XB = 0.$$

Making $A = 3k, B = 2k$ gives $3\,X^4 + 18\,X^2k - 9\,k^2 + 24\,Xk = 0$

```
> algcurves[genus](%, X, k);
        0
> algcurves[parametrization](curv,X,k,t);
# van Hoeij
```

$$(X, k) = \left(-2\,\frac{(2+t)\,t}{t^2-3}, -4/3\,\frac{t^3\,(2+t)}{(t^2-3)^2}\right).$$

Finish with $k = j/(1728 - j)$.

$X_1(M)$ as a curve

(Kim and Koo, Bull. Austral. Math. Soc. 54, 1996) $g(X_1(M)) = 0$ for $1 \le M \le 4$ and

$$g(X_1(M)) = 1 + \frac{M^2}{24}\prod_{p\mid M}\left(1 - \frac{1}{p^2}\right) - \frac{1}{4}\sum_{d\mid M, d>0}\varphi(d)\varphi(M/d).$$

Rem. $g(X_1(\ell)) = (\ell-5)(\ell-7)/24$.

Ex. this is an integer for all prime $\ell \ge 5$.

Coro. $g(X_1(M)) = 0$ for $1 \le M \le 10$, 12.
$g(X_1(M)) = 1$ for $M \in \{11, 14, 15\}$.

More computations:

- By hand: Reichert (Math. Comp. 1986), Sutherland (Math. Comp. 2012).
- Using modular forms: Baaziz (Math. Comp. 2010).
- More properties: Rabarison 2010.

The situation over $\mathbb{Q}$

Thm. (Mazur, 1977): the only possible torsion groups for $E(\mathbb{Q})$ are

$$\begin{cases} \mathbb{Z}/M\mathbb{Z}; & M = 1, 2, \ldots, 10 \text{ or } 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/M_2\mathbb{Z}; & M_2 = 2, 4, 6, 8. \end{cases}$$

All these $X_1(M_1, M_2)$ have genus 0 and Kubert gave Weierstrass parametrizations for them ($\rightarrow E_\infty$).

Montgomery: $X_1(12)$ (for P_∞).

Atkin, M.: (P_∞) for $X_1(M_2)$ with $M_2 \in \{5, 7, 9, 10\}$ and $X_1(2, 8)$.

BeBiLaPe09: things redone for Edwards form.

See also Rabarison 2010 for $X_1(2, 4)$ and $X_1(2, 6)$ (for E_∞).

The situation for quadratic fields (1/2)

Thm. (Kenku/Momose; Kamienny) Let K be a quadratic field. The only possible torsion groups for $E_{tors}(K)$ are among

$$\mathbb{Z}/M\mathbb{Z}, 1 \leq M \leq 18, M \neq 17,$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/M_2\mathbb{Z}, M_2 \in \{2, 4, 6, 8, 10, 12\},$$

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

Given K, not all possible $\mathcal{T}$'s can actually been found!

Thm. (Najman, 2010–2011)
1) For $K = \mathbb{Q}(\zeta_4)$, Mazur + $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.
2) For $K = \mathbb{Q}(\zeta_3)$, Mazur + $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

For a given K, see the methods in Kamienny/Najman, 2012.

The situation for quadratic fields (2/2)

M_1	M_2	g	E_∞	P_∞
3	3	0		$\mathbb{Q}(\zeta_3)$, Brier/Clavier
4	4	0		$\mathbb{Q}(\zeta_4)$, Brier/Clavier
3	6	0		$\mathbb{Q}(\zeta_3)$, Brier/Clavier
1	11	1	many $\mathbb{Q}(\sqrt{d})$, Rabarison	some
1	14	1	many $\mathbb{Q}(\sqrt{d})$, Rabarison	some
1	15	1	many $\mathbb{Q}(\sqrt{d})$, Rabarison	some
1	13	2	some $\mathbb{Q}(\sqrt{d})$, Rabarison	
1	16	2	some $\mathbb{Q}(\sqrt{d})$, Rabarison	
1	18	2	some $\mathbb{Q}(\sqrt{d})$, Rabarison	

The case $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Hessian form:

$$U^3 + V^3 + W^3 = 3DUVW,$$

with $D^3 \neq 1$.

Three points at ∞: $\Omega_r = (1 : -\omega^r : 0)$, $0 \leq r < 3$, where $\omega^2 + \omega + 1 = 0$. Take $O_E = \Omega_0$.

Nice addition law: same code for $\oplus$ and $[2]$ and $\ominus$, since

$$\ominus[u : v : w] = [v : u : w]$$

Also:

$$[2]P = O_E \iff P = [u : u : 1].$$

$$[3]P = O_E \iff u = 0 \text{ or } v = 0.$$

Action: $[u : v : w]^{\zeta_3} = [\zeta_3 u : \zeta_3^2 v : w]$.

The case $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ (Brier/Clavier)

Start from: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$: $Y^2 = (X-u)(X-v)(X+u+v)$.

$P = (x, y) = [2]Q \iff x - u, x - v$ and $x + u + v$ are squares.

$$a = -27\lambda^4(\tau^8 + 14\tau^4 + 1), b = 54\lambda^6(\tau^{12} - 33\tau^8 - 33\tau^4 + 1).$$

Point of infinite order:

$$\tau = \frac{\nu^2 + 3}{2\nu}, \quad \lambda = 8\nu^3.$$

See BrCl10 (Nancy) for more.

Rem. Can be put in Montgomery form.

Use: $p \equiv 1 \bmod 4$ for $p \mid N \mid b^{2r} + 1$ (more later).

Higher degree number fields

Particular cases:

- Cubic: Jeon, Kim, Schweizer (AA 2004),
  $\mathbb{Z}/M\mathbb{Z}$ for $1 \le M \le 20$, $M \ne 17, 19$,
  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/M_2\mathbb{Z}$ for $1 \le M_2/2 \le 7$ (conjecturally).
  See also Jeon/Kim/Lee 2011.
- Quartic: Jeon, Kim, Park (JLMS 2006),
  $\mathbb{Z}/M\mathbb{Z}$ for $1 \le M \le 24$, $M \ne 19, 23$,
  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/M_2\mathbb{Z}$ for $1 \le M_2/2 \le 9$,
  $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/M_2\mathbb{Z}$ for $1 \le M_2/3 \le 3$,
  $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/M_2\mathbb{Z}$ for $1 \le M_2/4 \le 2$,
  $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ (conjecturally).
  See also Jeon/Kim/Lee 2012, 2013.

Implications for ECM: scarce, since these are families with varying field K_t.

JeKiLe12

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$: over some $\mathbb{Q}(\sqrt{A_t + B_t\sqrt{d_t}})$.

$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$: $\mathbb{Q}(\sqrt{3t(4-t^3)}, \sqrt{-3})$.

$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$: $\mathbb{Q}(\sqrt{-1}, \sqrt{4it^2+1})$.

$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$: $\mathbb{Q}(\sqrt{-3}, \sqrt{8t^3+1})$.

The case $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

(See, e.g., Kohel11)

Model for $X_1(5)$**:**

$$a(u) = -(u^4 - 228u^3 + 494u^2 + 228u + 1)/48;$$

$$b = (u^6 + 522u^5 - 10005u^4 - 10005u^2 - 522u + 1)/864;$$

Prop. Let $u = t^5$. Then $E_t : Y^2 = X^3 + a(t^5)X + b(t^5)$ has full 5-torsion over $K_5 = \mathbb{Q}(\zeta_5)$ (model for $X(5)$).

Interesting for $p = 1 \bmod 5$; e.g., $p \mid N \mid b^{5n} - 1$.

Faster step 2 with optimal degree.

Pb: no point of infinite order known on $\mathbb{Q}(t)$.

$X(5)$: cont'd

$$
\begin{aligned}
tU_0^2 + U_2U_3 - U_1U_4 &= 0,\\
tU_0U_1 + U_2U_4 - U_3^2 &= 0,\\
U_1^2 + U_0U_2 - U_3U_4 &= 0,\\
U_1U_2 + U_0U_3 - U_4^2 &= 0,\\
U_2^2 - U_1U_3 + tU_0U_4 &= 0.
\end{aligned}
$$

Base point: $O_E = (0:1:1:1:1)$.

Projection to $(U_0 : U_1 : U_4)$:

$$U_1^5 + U_4^5 - (t-3)U_1^2U_4^2U_0 + (2t-1)U_1U_4U_0^3 - tU_0^5 = 0.$$

Back to quadratic fields: Rabarison's thesis

Gives parametrizations for all $X_1(M)$ of small genera.

Largest example of $g = 1$: $X_1(15) : s^2 + ts + s = t^3 + t^2$.

$$a = 1 - c = \frac{(t^2 - t)s + (t^5 + 5t^4 + 9t^3 + 7t^2 + 4t + 1)}{(t+1)^3(t^2+t+1)},$$

$$b = \frac{t(t^4 - 2t^2 - t - 1)s + t^3(t+1)(t^3 + 3t^2 + t + 1)}{(t+1)^6(t^2+t+1)}.$$

General form of an elliptic curve with a 15-torsion point (namely $P_0 = (0,0)$):

$$E : y^2 + axy + by = x^3 + bx^2$$

$X_1(15)$ as a curve

Prop. $X_1(15)(\mathbb{Q})$ has rank 0 and $X_1(15)(\mathbb{Q})_{tors} = \mathbb{Z}/4\mathbb{Z}$.

Prop. If K is quadratic, then

$$X_1(15)(K)_{tors} = \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \text{if } K = \mathbb{Q}(\sqrt{-15}),\\ \mathbb{Z}/8\mathbb{Z} & \text{if } K = \mathbb{Q}(\sqrt{-3}) \text{ or } \mathbb{Q}(\sqrt{5}),\\ \mathbb{Z}/4\mathbb{Z} & \text{otherwise.} \end{cases}$$

$X_1(15)$ in ECM

Letting d vary, we can hit $K = \mathbb{Q}(\sqrt{d})$ for which $X_1(15)(K)$ has rank 1 and explicit point P_X of infinite order. $\Rightarrow$ we obtain an infinite family of curves defined over $\mathbb{Q}(\sqrt{d})$ having torsion group $\mathbb{Z}/15\mathbb{Z}$.

Algorithm build(d, P_X)
1. compute $(t,s) = [k]P_X$.
2. deduce a and b.

For instance, $d = 3$ yields $t = -1/2$, $s = -(1+\sqrt{3})/4$.
Usable when $\sqrt{3} \bmod N$ is known.
With non-zero proba, we get $\mathbb{Z}/30\mathbb{Z}$ modulo p or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$ modulo p.

Implementation in GMP-ECM: all cases $X_1(M)$ of genus 1 + table of precomputed d, P_X for $|d| \le 100$. Would be easy to enlarge (with Denis Simon's pari program, Magma).

A new project

Big numbers? Cunningham numbers too difficult to harvest, ditto for many other tables.

Test numbers: $X_{2k} = 2^{2k} - 3$ for the special case $d = 3$ and all $2k \leq 1200$.

With only 10 curves per number, $B_1 = 10^8$: $1288377494293776070458041778724723574112719 \mid X_{1110}$.

```
ord(P)=[ <2, 1>, <3, 2>, <5, 1>, <101, 1>,
<2383, 1>, <6373, 1>, <216127, 1>, <2387303, 1>,
<34875647, 1>, <518647684813, 1> ]
```

Hope for more!

Atkin's trick

Pb. What if we do know a point of infinite order over $E \bmod N$?

Lemma. (AtMo93) Let $\lambda \equiv x_0^3 + ax_0 + b \bmod N$. Then $(\lambda x_0, \lambda^2)$ is a point on $E_\lambda : Y^2 = X^3 + a\lambda^2 X + b\lambda^3$.

If $(\lambda/p) = +1$ for $p \mid N$, then E_λ will have the desired torsion.

$\Rightarrow$ try several values of x_0.

Conclusions

- The quest for large torsion over $\overline{\mathbb{Q}}$ is bound to finish. Result so far: some extra families.
- Same work to be done for HECM???

More stuff in the dev version GMP-ECM, not discussed earlier:

- More ec forms.
- Addition-subtraction chains.