Constructing elliptic curves for cryptography

Reinier Bröker
Fields Institute & University of Calgary

ECC
September 2006

Point counting. Given an elliptic curve $E/\mathbf{F}_q$, find $N = \#E(\mathbf{F}_q)$.

Curve construction. Given an integer $N \geq 1$, find a finite field $\mathbf{F}_q$ and an elliptic curve $E/\mathbf{F}_q$ with

$$\#E(\mathbf{F}_q) = N.$$

For both problems, input and output are of size

$$\log(q) \approx \log(N).$$

Curve construction

Necessary condition: there is a prime power q in the Hasse interval

$$\mathcal{H}_N = [N - 2\sqrt{N} + 1, N + 2\sqrt{N} + 1].$$

We can (and will) restrict to *primes* $q = p$. The condition above is then also sufficient.

It is *not* known whether

$$\bigcup_p \mathcal{H}_p \supseteq \mathbf{Z}_{>0}.$$

In practice: *many* primes $p \in \mathcal{H}_N$.

Naïve algorithm

- find a prime $p \in \mathcal{H}_N$
- try random curves over $\mathbf{F}_p$ until you find a curve with N points
- expected run time: $O(N^{1/2+\varepsilon})$.

Not feasible for $N \gg 10^{15}$.

For crypto we want $N \approx 10^{60}$ prime.

The curve for this workshop

Standard encoding of messages.

A	01	G	07	M	13	S	19	Y	25
B	02	H	08	N	14	T	20	Z	26
C	03	I	09	O	15	U	21		
D	04	J	10	P	16	V	22		
E	05	K	11	Q	17	W	23		
F	06	L	12	R	18	X	24	‘ ’	00

The text

THE TENTH WORKSHOP ON ELLIPTIC CURVE CRYPTOGRAPHY

becomes

2008050020051420080023151811190815160015140005121
20916200903000321182205000318251620150718011608 25.

CM-approach

For any $p \in \mathcal{H}_N$, the desired curve $E/\mathbf{F}_p$ has Frobenius

$$F_p : E \to E \qquad (x, y) \mapsto (x^p, y^p).$$

Write $N = p + 1 - t$, then F_p satisfies

$$F_p^2 - tF_p + p = 0 \in \mathrm{End}(E)$$

of discriminant $\Delta = t^2 - 4p < 0$.

For $t \neq 0$, we have $\mathrm{End}(E) \subset \mathbf{Q}(\sqrt{\Delta})$.

We want an elliptic curve with endomorphism ring containing the imaginary quadratic order $\mathcal{O}_\Delta$.

Complex elliptic curves

- view $\mathcal{O}_\Delta$ as a lattice in $\mathbf{C}$
- the elliptic curve $\mathbf{C}/\mathcal{O}_\Delta$ has endomorphism ring $\mathcal{O}_\Delta$
- let $j : \mathbf{H} \to \mathbf{C}$ be the modular function with q-expansion $j(z) = 1/q + 744 + 196884q + \ldots$ in $q = \exp(2\pi i z)$
- a curve $\widetilde{E}/\mathbf{C}$ with j-invariant $j(\mathcal{O}_\Delta)$ has

$$\mathrm{End}(\widetilde{E}) \cong \mathcal{O}_\Delta.$$

CM-theory

- $j(\widetilde{E})$ lies in the ring class field for $\mathcal{O}_\Delta$
- $j(\widetilde{E})$ is a root of the *Hilbert class polynomial*

$$P_\Delta^j = \prod_{\mathfrak{a} \in \mathrm{Pic}(\mathcal{O}_\Delta)} (X - j(\mathfrak{a})) \in \mathbf{Z}[X]$$

- $\deg(P_\Delta^j) = \#\mathrm{Pic}(\mathcal{O}_\Delta)$
- P_Δ^j splits completely modulo p
- the roots of $P_\Delta^j \in \mathbf{F}_p[X]$ are j-invariants of curves having $p + 1 \pm t$ points over $\mathbf{F}_p$

Δ is too large

For $N \approx 10^{97}$ we have $\Delta \approx -10^{97}$. We cannot compute P_Δ^j for discriminants of this size.

Recall: we require that $\mathcal{O}_\Delta$ contains an element π of norm p with $N = p + 1 - \mathrm{Tr}(\pi)$.

Write $D = \mathrm{disc}(\mathbf{Q}(\sqrt{\Delta}))$. Then p splits in $\mathcal{O}_D$ in the same way as it does in $\mathcal{O}_\Delta$.

We may therefore work with D instead of Δ.

Selecting $\Delta = \Delta(p)$

We want to minimize the field discriminant D of $\mathbf{Q}(\sqrt{\Delta})$ with

$$\begin{aligned}\Delta = \Delta(p) &= (p+1-N)^2 - 4p \\ &= \underbrace{(N+1-p)}_{x}{}^2 - 4N < 0.\end{aligned}$$

We try to find a solution to

$$x^2 - Df^2 = 4N$$

for a *small* fundamental discriminant $D < 0$ for which $N + 1 - x$ is prime.

If there is a solution, Cornacchia's algorithm will find it efficiently given a value of $\sqrt{D} \bmod N$.

The 98-digit number $N =$
$$200805002005142008002315181119081516001514000512120916200903000321182205000318251620150718011608 25$$
factors as
$5^2 \cdot 37 \cdot 43891 \cdot 406987306873287994530 7 \cdot 5774937222668311 1\backslash\backslash$
$8506350854 09 \cdot 21044043267919037994488068215675691177 73.$

For this number, $p = N + 1 - x$ is prime and

$$x^2 + 69883 f^2 = 4N$$

for

$x = 650079034883814971810122953616846563211453073 1985$
$f = 233377222564314213934243545678449881228347470 45.$

Computing the Hilbert class polynomial

Two approaches:

- complex analytic (classical)
  - evaluate $j : \mathbf{H} \to \mathbf{C}$ in points $\tau \in \mathbf{H}$ corresponding to the ideal classes of $\mathcal{O}_D$
  - expand $\prod_\tau (X - j(\tau)) \in \mathbf{Z}[X]$.

- p-adic (Couveignes-Henocq, Bröker)
  - find a curve E over a finite field $\mathbf{F}_p$ with CM by $\mathcal{O}_D$
  - lift E to its canonical lift $\widetilde{E}$ over $\mathbf{Q}_p$
  - compute conjugates of $j(\widetilde{E}) \in \mathbf{Q}_p$ under $\mathrm{Pic}(\mathcal{O}_D)$
  - expand $\displaystyle\prod_{\mathfrak{a} \in \mathrm{Pic}(\mathcal{O}_D)} (X - j(\widetilde{E})^{\mathfrak{a}}) \in \mathbf{Z}[X]$.

We have $\mathrm{Pic}(\mathcal{O}_{-69883}) \cong \mathbf{Z}/30\mathbf{Z}$ and P^j_{-69883} has degree 30.

Putting $p =$
$$2008050020051420080023151811190815160015140005120$$
$$55908297414618824001192704956566963829572704288 41$$
and $a =$
$$41600679489470224930170618498054930543487358743 77$$
$$05146057020699650082780513327404416868930374046 2 \in \mathbf{F}_p,$$

the curve defined by
$$Y^2 = X^3 + aX - a$$
has exactly $N =$
$$2008050020051420080023151811190815160015140005121$$
$$20916200903000321182205000318251620150718011608 25$$
points over $\mathbf{F}_p$.

How small can we expect D to be?

Lemma. Let $N > 2$ be prime and $D < 0$ with $N \nmid D$. Then $4N$ can be written as

$$4N = x^2 - Df^2$$

if and only if N splits completely in the ring class field of $\mathbf{Z}[\sqrt{D}]$.

Given D, we can use Cornacchia's algorithm to find a possible solution to $x^2 - Df^2 = 4N$.

We also want that $N + 1 - x$ is prime.

Heuristics for size of D

- Fraction of primes splitting completely in the ring class field of $\mathbf{Z}[\sqrt{D}]$ is $\frac{1}{2|\mathrm{Pic}(\mathcal{O}_D)|} \approx \frac{1}{2\sqrt{|D|}}$. (*Chebotarev*, *Siegel*)

- If N splits, the 'probability' that $N+1-x$ or $N+1+x$ is prime is $\frac{2}{\log(N)}$. (*Prime number theorem*)

- Solving $\displaystyle\sum_{|D|<B} \frac{1}{2\sqrt{|D|}} = O(\log(N))$ for B yields

$$B = O((\log N)^2).$$

Heuristic runtime: $O((\log N)^{4+\varepsilon})$.

For general N we get $O(2^{\omega(N)}(\log N)^{4+\varepsilon})$, with $\omega(N)$ the number of distinct prime divisors of N.

Practical problem

The coefficients of P_D^j are *huge*. Example:

$$P_{-23}^j = X^3 + 3491750X^2 - 5151296875X + 12771880859375 \in \mathbf{Z}[X].$$

We can use smaller modular functions f of level $N \geq 1$ to gain a constant factor in size of the coefficients of P_D^j.

The value $f(\frac{-1+\sqrt{D}}{2})$ lies in the ray class field of conductor N. Sometimes also in the Hilbert class field.

For every D there is a smaller function f we can use. The factor we gain depends on f.

Smaller polynomials

$$
\begin{aligned}
P^{j}_{-71} = {} & X^7 + 313645809715X^6 - 3091990138604570X^5 \\
& + 983940388100478120493 02X^4 \\
& - 8235342634397307799680913 89X^3 \\
& + 5138800366453976780323726329446X^2 \\
& - 4253194739461396032746051511876 59X \\
& + 7377070867607311133577142410060812 63 \in \mathbf{Z}[X]
\end{aligned}
$$

$$
\begin{aligned}
P^{\gamma_2}_{-71} = {} & X^7 + 6745X^6 - 327467X^5 + 51857115X^4 + 2319299751X^3 \\
& + 41264582513X^2 - 307873876442X + 903568991567 \in \mathbf{Z}[X]
\end{aligned}
$$

$$
P^{\mathfrak{f}}_{-71} = X^7 - X^6 - X^5 + X^4 - X^3 - X^2 + 2X + 1 \in \mathbf{Z}[X]
$$

Computing P_D^f

- complex analytic approach: well understood
  (*Shimura reciprocity*, Stevenhagen, Gee, Schertz)
  - Fast implementations by e.g. Morain, Enge.
- p-adics: can work with f as well (Bröker)
  - algorithm combines Shimura reciprocity with modular curves
  - main tool: *modular polynomials*, i.e., a model for the curve

$$(\mathrm{Stab}_{\mathrm{SL}_2(\mathbf{Z})}(f) \cap \Gamma_0(l))\backslash\mathbf{H}.$$

  - in practice roughly as fast as complex analytic algorithm.

The reduction factor

For $|D| \to \infty$, the logarithmic height of P_D^f is a factor

$$r(f) = \frac{\deg_j(\Psi(j, X))}{\deg_X(\Psi(j, X))}$$

of the logarithmic height of P_D^j. Here: $\Psi(j, X)$ is minimal polynomial of f over $\mathbf{C}(j)$.

Examples.

- $f = \mathfrak{f} \Longrightarrow \Psi(j, X) = (X^{24} - 16)^3 - jX^{24}$ and $r(f) = 1/72$
- $f(z) = \frac{\eta(z/5)\eta(z/7)}{\eta(z)\eta(z/35)} \Longrightarrow r(f) = 1/24$

Question. What is the best we can do?

Reduction factor and modular curves

Let $\Gamma(f) = \mathrm{Stab}(f) \subset \mathrm{PSl}_2(\mathbf{Z})$ be the stabilizer of f in $\mathrm{PSl}_2(\mathbf{Z})$.

We have

$$\Gamma(N) \subseteq \Gamma(f) \subseteq \mathrm{PSl}_2(\mathbf{Z}),$$

with $N \in \mathbf{Z}_{\geq 1}$ the level of f.

The quotient $\Gamma(f)\backslash\overline{\mathbf{H}}$ is a compact Riemann surface.

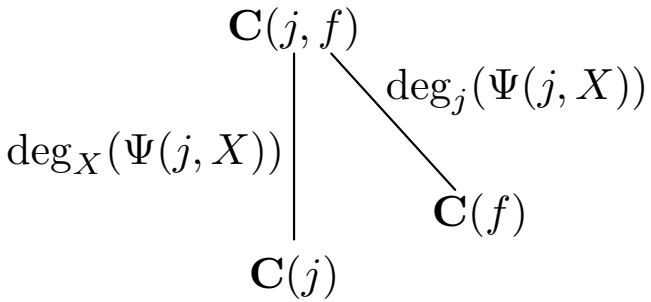
The corresponding modular curve $X(f)$ is a quotient of $X(N)$.

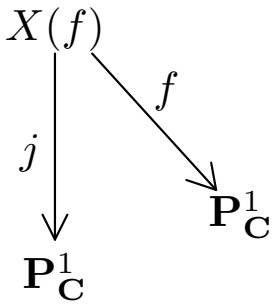
The curve $X(N)$ parametrizes triples (E, P, Q) with $P, Q \in E[N]$ a basis for $E[N]$ with $e_N(P, Q) = \zeta_N = \exp(2\pi i/N)$.

Reduction factor and modular curves

Recall: the reduction factor $r(f)$ equals

$$r(f) = \frac{\deg_j(\Psi(j,X))}{\deg_X(\Psi(j,X))} = \frac{[\mathbf{C}(j,f):\mathbf{C}(f)]}{[\mathbf{C}(j,f):\mathbf{C}(j)]}.$$





We have $r(f) = \dfrac{\deg(f : X(f) \twoheadrightarrow \mathbf{P}^1_{\mathbf{C}})}{[\mathbf{C}(j,f):\mathbf{C}(j)]}$, and we want a *lower bound*.

Gonality

- $k/\mathbf{Q}(\zeta_N)$ a field, X/k modular curve of level N
- *Gonality* $\gamma_k(X) = \min\{\deg(\pi) \mid \pi : X \twoheadrightarrow \mathbf{P}^1_k\}$
- for field L/k, put $\gamma_L(X) = \gamma_L(X \times_k L)$
- $\gamma_L(X) \leq \gamma_k(X)$, equality for $k = \overline{k}$.

Lower bounds for gonality

We have $(\deg f : X(f) \twoheadrightarrow \mathbf{P}^1_{\mathbf{C}}) \geq \gamma_{\mathbf{C}}(X(f))$.

Theorem. (*Abramovich, 1996*)

$$\gamma_{\mathbf{C}}(X(f)) \geq \frac{7}{800}[\mathrm{PSl}_2(\mathbf{Z}) : \mathrm{Stab}(f)].$$

Theorem has been improved for curves like $X_0(N)$ and $X_1(N)$.

Selbergs eigenvalue conjecture (1965) $\Longrightarrow$

$$\gamma_{\mathbf{C}}(X(f)) \geq \frac{1}{96}[\mathrm{PSl}_2(\mathbf{Z}) : \mathrm{Stab}(f)].$$

Lower bounds for reduction factor

Galois theory: $[\mathbf{C}(j,f):\mathbf{C}(j)] = [\mathrm{PSl}_2(\mathbf{Z}):\mathrm{Stab}(f)]$.

Conclude:

$$r(f) = \frac{\deg(f : X(f) \twoheadrightarrow \mathbf{P}^1_{\mathbf{C}})}{\deg(j : X(f) \twoheadrightarrow \mathbf{P}^1_{\mathbf{C}})} \geq \frac{\gamma_{\mathbf{C}}(X(f))}{[\mathrm{PSl}_2(\mathbf{Z}):\mathrm{Stab}(f)]} \geq \frac{7}{800}.$$

Selberg $\Longrightarrow r(f) \geq \dfrac{1}{96}$.

(We have $7/800 \approx 0.00875$ and $1/96 \approx 0.01042$.)

Computing class polynomials

Computing P_D^j can be improved by using smaller functions f.

Best function depends on discriminant D.

For $f = \mathfrak{f} = \zeta_{48}^{-1} \dfrac{\eta(\frac{z+1}{2})}{\eta(z)}$ we gain a factor 72.

We cannot expect to gain more than factor 96 for *any* function.

A cryptographic curve

Take the 60-digit prime $N =$
$1234567890123456789012345678901234567890123456789012345678901234568197.$

The smallest discriminant is $D = -2419$.

Put $p =$
$1234567890123456789012345678906548333745250859667371252365 01$
and $a =$
$7887602969799610712056382609486455658099996511086255879991 3.$

The curve defined by

$$Y^2 = X^3 + 4aX - 8a$$

has exactly N points.

A large example

For $N = 10^{1000} + 453 = \text{nextprime}(10^{1000})$ we find

$$D = -2643.$$

A class polynomial for $\mathcal{O}_{-2643}$ has degree 10.

It factors completely mod $p = N + 1 - x$ with $x =$

$$\begin{aligned}
&845805648656593651223765284133326455321521711275464381191582185097\\
&464548940475023114759214359255933957886638255373505105304467164037\\
&412223409859640997425288456249927056490112115629777477917877958284\\
&088781667965440292251712877729866594533690475769359117604658547045\\
&901399399137820889786907255844328083231943562217674139516706917651\\
&715833885756514082522496689090975644895221448877817321348993895877\\
&536973618765771003069120306851480849793026370359289958346073691051\\
&219444222624641876110189738840154388 37.
\end{aligned}$$

The elliptic curve defined by

$$Y^2 = X^3 + aX - a$$

has exactly $N = \text{nextprime}(10^{1000})$ points.

$a =$

94202767552525669338330993511241788798773531832242951943744955733646682573574641982561532978385967108441467756099630439090699022366557998223663915368890013769018164491219354606500270780834354364980628447291599042308108475453308253383405586265656152676161786082163032589395534250214601109809644586992838228162935229361067462361537213416511720819576299098156590938724644500034622413542838563230733095660554575247247828252501415502178692326982168587313099431450975621422455971881168514103885570069865425832913498413079969919308343578640489736506148614065952128861948450289456661566816347190790105993362955522952533044139552844026797765297304929105950831769789963534701625957277846393145770238417304692006230346257996892089066085065880564885854053663099058750881517418310308874555173345620773218208258663254902874212740241465804748840559143359531803011660802640704445439718807268051588138700767897488669071157357770328506864944871157660620893328934288125370416591734465007305172885000113779110814549135 8.