

Constructing elliptic curves for cryptography

Reinier Bröker
Universiteit Leiden



Magma Workshop
July, 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 $N \gg 10^{15} \dots$

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

THIS IS AN ELLIPTIC CURVE FOR THE MAGMA WORKSHOP

becomes

200809190009190001140005121209162009030003211822
050006151800200805001301071301002315181119081516.

CM-approach

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

$$F_p : E \rightarrow E \quad (x, y) \mapsto (x^p, y^p).$$

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

$$F_p^2 - tF_p + p = 0 \in \text{End}_{\mathbf{F}_p}(E)$$

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

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

We want an elliptic curve with endomorphism ring containing \mathcal{O}_Δ .

Complex elliptic curves

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

$$\text{End}_{\mathbf{C}}(\tilde{E}) \cong \mathcal{O}_\Delta.$$

CM-theory

- $j(\tilde{E}) \in \text{RCF}(\mathbf{Q}(\sqrt{\Delta}))$
- $j(\tilde{E})$ is a root of the *Hilbert class polynomial*

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

- $\deg(P_{\Delta}) = |\text{Pic}(\mathcal{O}_{\Delta})|$
- P_{Δ} splits completely modulo p
- the roots of $P_{\Delta} \in \mathbf{F}_p[X]$ are j -invariants of curves having $p + 1 \pm t$ points over \mathbf{F}_p .
- if $\Delta = f^2 D$ with $D = \text{disc}(\mathbf{Q}(\sqrt{\Delta}))$, we can replace Δ by D on this slide!

Selecting $\Delta = \Delta(p)$

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

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

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 $\sqrt{D} \pmod{N}$.

THIS IS AN ELLIPTIC CURVE FOR THE MAGMA WORKSHOP

The 96-digit number $N =$

200809190009190001140005121209162009030003211822
050006151800200805001301071301002315181119081516

factors as

$2^2 \cdot 3^2 \cdot 277 \cdot 224769329 \cdot 14553061967403803 \cdot 615615983179146 \\ 4537443473253176986892125433769826464741790629369269$

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

$$x^2 + 28f^2 = 4N$$

for

$x = 821183028810038874116417736750571646368771466376$

$f = 67848358552397374069358985470720823199328386686.$

[Also solution for $D = -828, -3312, -8011 \dots$]

THIS IS AN ELLIPTIC CURVE FOR THE MAGMA WORKSHOP

We have $\text{Pic}(\mathcal{O}_{-28}) \cong \{1\}$ and $P_{-28} = X - 16581375 \in \mathbf{Z}[X]$.

Putting $p =$

200809190009190001140005121209162009030003211821
228823122990161930884883334550430668812347615141,

an elliptic curve with j -invariant

$$16581375 \in \mathbf{F}_p$$

has exactly $N =$

200809190009190001140005121209162009030003211822
050006151800200805001301071301002315181119081516

points.

Computing the Hilbert class polynomial

Two approaches:

- complex analytic (classical)
 - evaluate $j : \mathbf{H} \rightarrow \mathbf{C}$ 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 \tilde{E} over \mathbf{Q}_p ;
 - compute conjugates of $j(\tilde{E}) \in \mathbf{Q}_p$ under $\text{Pic}(\mathcal{O}_D)$
 - expand $\prod_{\mathfrak{a} \in \text{Pic}(\mathcal{O}_D)} (X - j(\tilde{E})^{\mathfrak{a}}) \in \mathbf{Z}[X]$.

see my PhD-thesis for details

Improvements

The polynomial P_D has huge coefficients for moderately small $|D|$.
Example:

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

Both methods can be improved by using ‘smaller functions’, like the Weber function $\mathfrak{f}(z) = \zeta_{48}^{-1} \cdot \frac{\eta(\frac{z+1}{2})}{\eta(z)}$ or double η -quotients. Example:

$$P_{-23}^{\mathfrak{f}} = X^3 - X^2 + 1 \in \mathbf{Z}[X].$$

Improvements, II

- complex analytic approach: well understood
(*Shimura reciprocity*, Stevenhagen, Schertz)
 - Implemented by e.g. Morain, Enge.
 - In Magma: only a slow version for the Weber- f ...
- p -adics: can adapt the algorithm to work with ‘small’ function f
 - algorithm combines Shimura reciprocity with modular curves.
 - main tool: *modular polynomials*, i.e., a model for the curve

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

- in practice roughly as fast as complex analytic algorithm.

see my PhD-thesis for details

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 $\frac{1}{2|\text{Pic}(\mathcal{O}_D)|} \approx \frac{1}{2\sqrt{|D|}}$. (*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 $\sum_{|D| < B} \frac{1}{2\sqrt{|D|}} = O(\log(N))$ for B yields

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

This leads to an heuristic *polynomial time* algorithm.

A large example

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

$$D = -2643.$$

The class polynomial $P_{-2643} \in \mathbf{Z}[X]$ has degree 10.

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

845805648656593651223765284133326455321521711275464381191582185097
464548940475023114759214359255933957886638255373505105304467164037
412223409859640997425288456249927056490112115629777477917877958284
088781667965440292251712877729866594533690475769359117604658547045
901399399137820889786907255844328083231943562217674139516706917651
715833885756514082522496689090975644895221448877817321348993895877
536973618765771003069120306851480849793026370359289958346073691051
21944422262464187611018973884015438837.

The elliptic curve defined by

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

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

$a =$

```
9420276755252566933833099351124178879877353183224295194374495573364668257357464198256
1532978385967108441467756099630439090699022366557998223663915368890013769018164491219
3546065002707808343543649806284472915990423081084754533082533834055862656561526761617
8608216303258939553425021460110980964458699283822816293522936106746236153721341651172
0819576299098156590938724644500034622413542838563230733095660554575247247828252501415
5021786923269821685873130994314509756214224559718811685141038855700698654258329134984
1307996991930834357864048973650614861406595212886194845028945666156681634719079010599
3362955522952533044139552844026797765297304929105950831769789963534701625957277784639
3145770238417304692006230346257996892089066085065880564885854053663099058750881517418
3103088745551733456207732182082586632549028742127402414658047488405591433595318030116
6080264070444543971880726805158813870076789748866907115735777032850686494487115766062
08933289342881253704165917344650073051728850001137791108145491358.
```