

Constructing elliptic curves with a given number of points

Reinier Bröker

Joint work with Peter Stevenhagen



Diamant/Eidma-symposium
November 2005

Elliptic curves

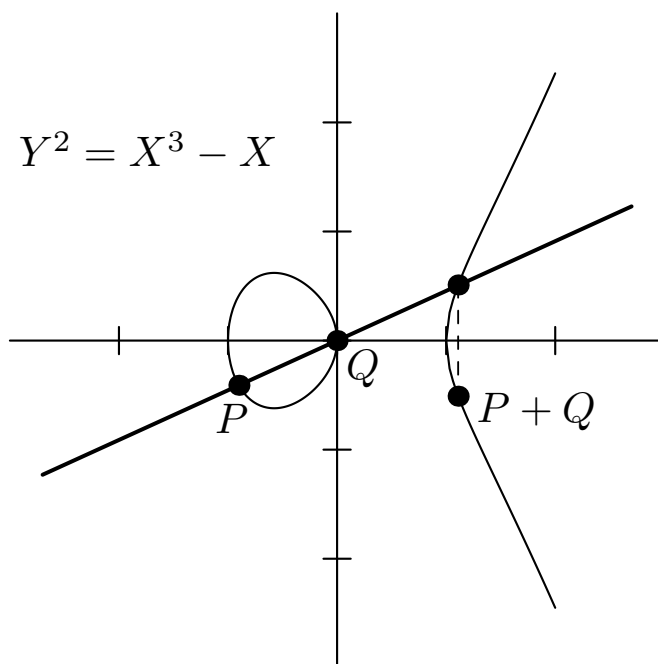
Over any field K , an elliptic curve E can be given by a *Weierstraß equation*.

For $\text{char}(K) \neq 2, 3$, this equation looks like

$$Y^2 = X^3 + aX + b$$

with $a, b \in K$.

The set $E(K)$ of K -rational points has a natural group operation.



Discrete log

Discrete log in $E(\mathbf{F}_p)$:

given $P, Q \in E(\mathbf{F}_p)$, find an integer $k \in \mathbf{Z}$ with $kP = Q$ (if it exists).

For large ($\approx 10^{60}$) prime values of $\#E(\mathbf{F}_p)$, this problem is **hard**.

Cryptography in cellphones is based on the discrete log problem for a ‘hard’ curve E/\mathbf{F}_p .



Finding hard curves

Hasse (1933):

$$\#E(\mathbf{F}_p) \in \mathcal{H}_p = [p+1-2\sqrt{p}, p+1+2\sqrt{p}].$$

Schoof (1985):

polynomial time algorithm to compute $\#E(\mathbf{F}_p)$.

Naïve algorithm.

- pick a prime $p \approx 10^{60}$;
- try random curves over \mathbf{F}_p until we find one of prime order.

Algorithm is heuristic polynomial time.

Topic of today's talk

Problem. Given an integer $N \in \mathbf{Z}_{\geq 1}$, find a finite field \mathbf{F}_p and an elliptic curve E/\mathbf{F}_p with

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

For cryptography: N is prime, $\approx 10^{60}$.

Problem has a solution if and only if

$$N \in \mathcal{H}_p = [p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$$

for some prime p .

Equivalently: if there is a prime

$$p \in \mathcal{H}_N.$$

Heuristics.

One of every $\log N$ integers around N is prime. (*Prime number theorem*).

Hence: problem has *many* solutions.

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 running time: $O(N^{1/2+\varepsilon})$.

Not feasible for $N \gg 10^{18}$.

The DIAMANT curve

Standard encoding of messages.

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

The text

DISCRETE INTERACTIVE ALGORITHMIC
MATHEMATICS ALGEBRA NUMBER THEORY

becomes

040919031805200500091420051801032
009220500011207151809200813090300
130120080513012009031900011207050
218010014211302051800200805151825.

Endomorphisms

The ring $\text{End}(E)$ consists of all *morphisms* $E \rightarrow E$.

Examples.

$$[n] : P \mapsto nP \quad (n \in \mathbf{Z})$$

The Frobenius morphism

$$F_p : (x, y) \mapsto (x^p, y^p)$$

plays a key role in Hasse's theorem:

$$E(\mathbf{F}_p) = \ker([1] - F_p).$$

Endomorphisms versus number of points

Any curve E/\mathbf{F}_p has Frobenius

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

If E has $N = p + 1 - t$ points, then F_p satisfies

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

and we have $\Delta = t^2 - 4p < 0$.

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

Assume $t \neq 0$ and $\Delta < -4$.

Conclusion.

$$\text{End}(E) \supset \mathcal{O}_\Delta \iff \#E(\mathbf{F}_p) = p + 1 \pm t$$

Complex elliptic curves

An elliptic curve $E : Y^2 = X^3 + aX + b$ is determined up to \bar{K} -isomorphism by its j -invariant

$$j(E) = 1728 \frac{4a^3}{4a^3 - 27b^2}.$$

Isomorphic curves have isomorphic endomorphism rings.

Idea.

- view \mathcal{O}_Δ as a lattice in \mathbf{C} ;
- the complex elliptic curve $\mathbf{C}/\mathcal{O}_\Delta$ has endomorphism ring \mathcal{O}_Δ ;
- compute the j -invariant of $\mathbf{C}/\mathcal{O}_\Delta$ and somehow reduce $j(\mathbf{C}/\mathcal{O}_\Delta) \bmod p$.

Finding $j(E)$ by complex analytic means

- over \mathbf{C} , the j -invariant of an elliptic curve E with $\text{End}(E) \cong \mathcal{O}_\Delta$ is a root of

$$H_\Delta = \prod_{[a,b,c]} \left(X - j\left(\frac{-b + \sqrt{\Delta}}{2a}\right) \right) \in \mathbf{Z}[X];$$

- here $j : \mathbf{H} \rightarrow \mathbf{C}$ is the complex analytic modular function with Fourier expansion $j(\tau) = 1/q + 744 + \dots$ in $q = \exp(2\pi i\tau)$;
- $[a, b, c]$ range over the reduced quadratic forms $ax^2 + bxy + cy^2$ of discriminant $b^2 - 4ac = \Delta$;
- H_Δ splits completely modulo p ;
- the roots of $H_\Delta \in \mathbf{F}_p[X]$ are j -invariants of curves having $p + 1 - t = N$ points.

Δ is too large

Running time of computing H_Δ is $O(|\Delta|^{1+\varepsilon})$.
Current ‘world record’ is $\Delta \approx -10^{10}$.

For $N \approx 10^{130}$, we usually have $\Delta(p) \approx -10^{130}$. This is not feasible.

Recall. We want an elliptic curve E with

$$\text{End}(E) \supset \mathcal{O}_\Delta.$$

If $\Delta = f^2 D$ with $D = \text{disc}(\mathbf{Q}(\sqrt{\Delta}))$, we can replace Δ by D in the algorithm!

Every $p \in \mathcal{H}_N$ yields a value of $\Delta = \Delta(p)$ and consequently a value of $D = D(p)$.

Selecting $\Delta = \Delta(p)$

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

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

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 the corresponding value of $\sqrt{D} \bmod N$.

THE DIAMANT CURVE

The 131-digit number $N =$

04091903180520050009142005180103200
92205000112071518092008130903001301
20080513012009031900011207050218010
014211302051800200805151825.

factors as

$5^2 \cdot 2789 \cdot 27631 \cdot 88756834388326096017134$
 $677101020761 \cdot 23929764201107791531310$
 $051280122889132144407049639576738543$
 $462231560414747662456677827.$

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

$$x^2 + 93259y^2 = 4N$$

for

$$x = 403579981434633684320964763414216$$
$$845863656770521823527227071442797$$
$$y = 925798643265707473815872621599344$$
$$80145707300635969452465614407.$$

THE DIAMANT CURVE

The class polynomial H_{-93259} has degree 70 and coefficients up to 1173 digits.

It splits completely mod $p =$

4091903180520050009142005180103200
9220500011207151809200813090299726
5400990783783247109352477928333721
46357440780228272973733709029

Any of its zeroes yields a curve with $N =$

04091903180520050009142005180103200
92205000112071518092008130903001301
20080513012009031900011207050218010
014211302051800200805151825.

points.

THE DIAMANT CURVE

Put $a =$

$$\begin{aligned} &376492989622301050534438298878 \\ &274854764865682012808348161456 \\ &5000197813828094392 \in \mathbf{F}_p. \end{aligned}$$

The curve defined by

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

has exactly N points.

A cryptographic curve

Take the 60-digit prime $N =$
123456789012345678901234567890
123456789012345678901234568197.

The smallest discriminant is $D = -2419$.

Put $p =$
123456789012345678901234567890
654833374525085966737125236501
and $a =$
788760296979961071205638260948
64556580999965110862558799913 $\in \mathbf{F}_p$.

The curve defined by

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

has exactly N points.

How small can we expect D to be?

- for simplicity, consider *primes* N ;
- for $4N = x^2 - Dy^2$, the ‘probability’ that $N + 1 - x$ or $N + 1 + x$ is prime is $\frac{2}{\log N}$; (*Prime number theorem*)
- the fraction of primes p that can be written as $p = \frac{x^2 - Dy^2}{4}$ grows like $|D|^{-1/2}$ (*Chebotarev and Brauer-Siegel*);
- the number of solutions to $x^2 - Dy^2 = 4N$ for $|D| < B$ grows like

$$\sum_{|D| < B} \frac{1}{\sqrt{|D|}} \approx \sqrt{B};$$

- we need $\log N$ solutions, so take

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

- minimal D is of size $(\log N)^2$.

Counting solutions to $x^2 - Dy^2 = 4N$

$N = \text{nextprime}(10^{20})$, D ranges

bound on D	# solutions
100	18
400	50
1600	108
6400	201

$N = \text{nextprime}(10^{30})$, D ranges

bound on D	# solutions
100	38
400	73
1600	156
6400	317

A large example

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

$$D = -2643.$$

The class polynomial H_{-2643} has degree
10.

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

84580564865659365122376528413332645532152171
12754643811915821850974645489404750231147592
14359255933957886638255373505105304467164037
41222340985964099742528845624992705649011211
56297774779178779582840887816679654402922517
12877729866594533690475769359117604658547045
90139939913782088978690725584432808323194356
22176741395167069176517158338857565140825224
96689090975644895221448877817321348993895877
53697361876577100306912030685148084979302637
03592899583460736910512194442226246418761101
8973884015438837.

The elliptic curve defined by

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

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

$a =$

942027675525256693383309935112417887987735318322429519437449
5573364668257357464198256153297838596710844146775609963043909
0699022366557998223663915368890013769018164491219354606500270
7808343543649806284472915990423081084754533082533834055862656
5615267616178608216303258939553425021460110980964458699283822
8162935229361067462361537213416511720819576299098156590938724
6445000346224135428385632307330956605545752472478282525014155
0217869232698216858731309943145097562142245597188116851410388
5570069865425832913498413079969919308343578640489736506148614
0659521288619484502894566615668163471907901059933629555229525
3304413955284402679776529730492910595083176978996353470162595
7277784639314577023841730469200623034625799689208906608506588
0564885854053663099058750881517418310308874555173345620773218
2082586632549028742127402414658047488405591433595318030116608
0264070444543971880726805158813870076789748866907115735777032
8506864944871157660620893328934288125370416591734465007305172
8850001137791108145491358.