Constructing elliptic curves for cryptography

Reinier Bröker
Fields Institute & University of Calgary

ECC
September 2006
Point counting. Given an elliptic curve $E/F_q$, find $N = \#E(F_q)$.

Curve construction. Given an integer $N \geq 1$, find a finite field $F_q$ and an elliptic curve $E/F_q$ with
\[
\#E(F_q) = N.
\]

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

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

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

- find a prime $p \in \mathcal{H}_N$
- try random curves over $\mathbb{F}_p$ 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.

<table>
<thead>
<tr>
<th>A</th>
<th>01</th>
<th>G</th>
<th>07</th>
<th>M</th>
<th>13</th>
<th>S</th>
<th>19</th>
<th>Y</th>
<th>25</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>02</td>
<td>H</td>
<td>08</td>
<td>N</td>
<td>14</td>
<td>T</td>
<td>20</td>
<td>Z</td>
<td>26</td>
</tr>
<tr>
<td>C</td>
<td>03</td>
<td>I</td>
<td>09</td>
<td>O</td>
<td>15</td>
<td>U</td>
<td>21</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>04</td>
<td>J</td>
<td>10</td>
<td>P</td>
<td>16</td>
<td>V</td>
<td>22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td>05</td>
<td>K</td>
<td>11</td>
<td>Q</td>
<td>17</td>
<td>W</td>
<td>23</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F</td>
<td>06</td>
<td>L</td>
<td>12</td>
<td>R</td>
<td>18</td>
<td>X</td>
<td>24</td>
<td>‘</td>
<td>00</td>
</tr>
</tbody>
</table>

The text

THE TENTH WORKSHOP ON ELLIPTIC CURVE CRYPTOGRAPHY

becomes

2008050020051420080023151811190815160015140005121
2091620090300032118220500031825162015071801160825.
CM-approach

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

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

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

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

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

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

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 $\mathbb{C}$

• the elliptic curve $\mathbb{C}/\mathcal{O}_\Delta$ has endomorphism ring $\mathcal{O}_\Delta$

• let $j : \mathbb{H} \to \mathbb{C}$ be the modular function with $q$-expansion $j(z) = 1/q + 744 + 196884q + \ldots$ in $q = \exp(2\pi i z)$

• a curve $\tilde{E}/\mathbb{C}$ with $j$-invariant $j(\mathcal{O}_\Delta)$ has

$$\text{End}(\tilde{E}) \cong \mathcal{O}_\Delta.$$
CM-theory

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

$$P^j_\Delta = \prod_{a \in \text{Pic}(\mathcal{O}_\Delta)} (X - j(a)) \in \mathbb{Z}[X]$$

- $\deg(P^j_\Delta) = \#\text{Pic}(\mathcal{O}_\Delta)$
- $P^j_\Delta$ splits completely modulo $p$
- the roots of $P^j_\Delta \in \mathbb{F}_p[X]$ are $j$-invariants of curves having $p + 1 \pm t$ points over $\mathbb{F}_p$
$\Delta$ is too large

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

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

Write $D = \text{disc}(\mathbb{Q}(\sqrt{\Delta}))$. 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 $\Delta$. 
Selecting $\Delta = \Delta(p)$

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

$$\Delta = \Delta(p) = (p + 1 - N)^2 - 4p$$

$$= (N + 1 - p)^2 - 4N < 0.$$  

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 $\sqrt{D} \mod N$. 
The 98-digit number \( N = 2008050020051420080023151811190815160015140005121 \)
\( 2091620090300032118220500031825162015071801160825 \)
factors as
\[ 5^2 \cdot 37 \cdot 43891 \cdot 4069873068732879945307 \cdot 5774937222668311111 \]
\[ 850635085409 \cdot 2104404326791903799448806821567569117773. \]

For this number, \( p = N + 1 - x \) is prime and
\[ x^2 + 69883f^2 = 4N \]
for
\[ x = 6500790348838149718101229536168465632114530731985 \]
\[ f = 23337722256431421393424354567844988122834747045. \]
Computing the Hilbert class polynomial

Two approaches:

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

• $p$-adic (Couveignes-Henocq, Bröker)
  • find a curve $E$ over a finite field $\mathbb{F}_p$ with CM by $\mathcal{O}_D$
  • lift $E$ to its canonical lift $\tilde{E}$ over $\mathbb{Q}_p$
  • compute conjugates of $j(\tilde{E}) \in \mathbb{Q}_p$ under $\text{Pic}(\mathcal{O}_D)$
  • expand $\prod_{a \in \text{Pic}(\mathcal{O}_D)} (X - j(\tilde{E})^a) \in \mathbb{Z}[X]$.
We have $\text{Pic}(\mathcal{O}_{-69883}) \cong \mathbb{Z}/30\mathbb{Z}$ and $P_{-69883}^j$ has degree 30.

Putting $p = 2008050020051420080023151811190815160015140005120$
$5590829741461882400119270495656696382957270428841$
and $a = 4160067948947022493017061849805493054348735874377$
$051460570206996500827805133274044168689303740462 \in \mathbb{F}_p$,

the curve defined by $Y^2 = X^3 + aX - a$

has exactly $N = 2008050020051420080023151811190815160015140005121$
$2091620090300032118220500031825162015071801160825$

points over $\mathbb{F}_p$. 
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 $\mathbb{Z}[^D]$. 

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 $\mathbb{Z}[\sqrt{D}]$ 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

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

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:

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

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

\[ P^j_{-71} = X^7 + 313645809715X^6 - 3091990138604570X^5 \]
\[ + 98394038810047812049302X^4 \]
\[ - 823534263439730779968091389X^3 \]
\[ + 5138800366453976780323726329446X^2 \]
\[ - 425319473946139603274605151187659X \]
\[ + 737707086760731113357714241006081263 \in \mathbb{Z}[X] \]

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

\[ P^f_{-71} = X^7 - X^6 - X^5 + X^4 - X^3 - X^2 + 2X + 1 \in \mathbb{Z}[X] \]
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
  \[(\text{Stab}_{\text{SL}_2(\mathbb{Z})}(f) \cap \Gamma_0(l)) \backslash \mathbb{H}.\]

- in practice roughly as fast as complex analytic 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 \(\mathbb{C}(j)\).

Examples.

• \(f = \frac{\eta(z/5)\eta(z/7)}{\eta(z) \eta(z/35)} \Rightarrow r(f) = 1/24\)

Question. What is the best we can do?
Reduction factor and modular curves

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

We have

$$\Gamma(N) \subseteq \Gamma(f) \subseteq \text{PSl}_2(\mathbb{Z}),$$

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

The quotient $\Gamma(f) \backslash \overline{H}$ 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 $e_N(P, Q) = \zeta_N = \exp(2\pi i / N)$.
Recall: the reduction factor $r(f)$ equals

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

We have $r(f) = \frac{\deg(f : X(f) \to P^1_C)}{[C(j, f) : C(j)]}$, and we want a lower bound.
Gonality

- \( k/\mathbb{Q}(\zeta_N) \) a field, \( X/k \) modular curve of level \( N \)

- Gonality \( \gamma_k(X) = \min\{\deg(\pi) \mid \pi : X \to \mathbb{P}^1_k\} \)

- 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 \((\deg f : X(f) \to \mathbb{P}^1_C) \geq \gamma_C(X(f))\).

**Theorem.** *(Abramovich, 1996)*

\[
\gamma_C(X(f)) \geq \frac{7}{800} [\text{PSl}_2(\mathbb{Z}) : \text{Stab}(f)].
\]

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

Selbergs eigenvalue conjecture (1965) \(\implies\)

\[
\gamma_C(X(f)) \geq \frac{1}{96} [\text{PSl}_2(\mathbb{Z}) : \text{Stab}(f)].
\]
Lower bounds for reduction factor

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

Conclude:

$$r(f) = \frac{\deg(f : X(f) \to \mathbb{P}^1_C)}{\deg(j : X(f) \to \mathbb{P}^1_C)} \geq \frac{\gamma_C(X(f))}{[\text{PSl}_2(\mathbb{Z}) : \text{Stab}(f)]} \geq \frac{7}{800}.$$ 

Selberg $\implies r(f) \geq \frac{1}{96}$.

(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 $f = f = \zeta_{48}^{-1} \frac{\eta(z+1)}{\eta(z)}$ 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 $N = 123456789012345678901234567890123456789012345678901234568197$.

The smallest discriminant is $D = -2419$.

Put $p =$ 1234567890123456789012345678906548333745250859666737125236501 and $a =$ 78876029697996107120563826094864556580999965110862558799913.

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 $O_{-2643}$ has degree 10.

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

8458056486565936512237652841333264553215217112754643811915821850974645489404750231147592143592559339578866382553735051053044671640374122234098596409974252884562499270564901121156297774779178779582840887816679654402922517128777298665945336904757693591176046585470459013993991378208897869072558443280832231943562217674139516706917651715833885756514082522496689090975644895221448877817321348993895877536973618765771003069120306851480849793026370359289958346073691051219444222624641876110189738884015438837.
The elliptic curve defined by

\[ Y^2 = X^3 + aX - a \]

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

\( a = \)

\[ \begin{align*}
9420276755252566933833099351124178879877353183222495194374495573364668257357464198256 \\
153297838596710844146775609963043909069022366557998223663915368890013769018164491219 \\
3546065002707808343543649806284472915990423081084754533082533834055862656561526761617 \\
8608216303258939553425021460110980964458699283822816293522936106746236153721341651172 \\
0819576299098156590938724644500034622413542838563230733095660554575247247828252501415 \\
5021786923269821685873130994314509756214224559718811685141038855700698654258329134984 \\
1307996991930834357864048973650614861406595212886194845028945666156681634719079010599 \\
3362955522952533044139552844026797765297304929105950831769789963534701625957277784639 \\
314577023841730469200623034625799689208906608506588056485854053663099058750881517418 \\
310308874555173345620773218208258663254902874212740241465804748840559143595318030116 \\
6080264070444543971880726805158813870076789748866907115735777032850686494487115766062 \\
0893328934288125370416591734465007305172885000137791108145491358.
\end{align*} \]