Curves, Cryptography, and Primes of the Form $x^2 + y^2D$

Juliana V. Belding
2007 Graduation Conference
University of Maryland
Constructing Cryptographic Curves

For any finite group $G$ order $N$, the **Discrete Log Problem (DLP)** is

Given $a, b \in G$ with $b = a^n$, find $n$. (Mult.)

Given $a, b \in G$ with $b = n \cdot a$, find $n$. (Add.)

Let $\mathbb{F}_p$ be the finite field of $p$ elements and $E$ an elliptic curve. For the group of points of $E$ over $\mathbb{F}_p$, the DLP is computationally infeasible if $N$ is a large prime $\approx 10^{60}$.

**Problem:** Construct an elliptic curve $E$ such that $E(\mathbb{F}_p)$ has large prime order $N$. 
A Brief Introduction To Elliptic Curves

An elliptic curve $E$ over a field $F$ is

$$y^2 = x^3 + Ax + B$$

with $A, B \in F$ and $4A^3 + 27B^2 \neq 0$.

- $E(F) :=$ the set of all pairs $(x, y) \in F \times F$ that satisfy this equation.

- There is a way to define addition of points on the curve, so $E(F)$ is a group.

- The $j$-invariant

$$j(E) = 1728 \frac{4A^3}{4A^3 + 27B^2}$$

classifies elliptic curves up to isomorphism.
**Hasse’s Theorem:** Let $t \in \mathbb{Z}$ be such that $N = p + 1 - t$. Then

$$|t| \leq 2\sqrt{p}.$$  

**Key Theorem:** (Deuring) Given $p, N$ satisfying Hasse’s Theorem, there exists a curve $E$ over $\mathbb{F}_p$ such that $E(\mathbb{F}_p)$ has $N$ points.

Q: But how to find such a curve?

- The **endomorphism ring** of $E$ consists of all rational maps
  $$\phi : E \to E$$
  that preserve addition.

- For every $E$, $\text{End}(E)$ contains $\mathbb{Z}$ as the multiplication-by-$n$ maps:
  $$[n]P := \underbrace{P + P + ... + P}_{n}.$$
For $E$ over $\mathbb{F}_p$, the Frobenius map

$$\pi : (x, y) \rightarrow (x^p, y^p)$$

is also an endomorphism of $E$.

**Fact:** In $\text{End}(E)$,

$$\pi^2 - [t]\pi + [p] = [0].$$

Solving for $\pi$,

$$\pi = \frac{-t \pm \sqrt{t^2 - 4p}}{2}.$$

**Note:** By Hasse’s Thm,

$$t^2 - 4p \leq 0$$

$$\Rightarrow t^2 - 4p = -f^2D$$

$$\Rightarrow 4p = t^2 + f^2D$$

for $t, f, D \in \mathbb{Z}^+$ with $D$ squarefree.

If $N = 2 \cdot \text{prime}$, there are $x, y \in \mathbb{Z}$ such that

$$p = x^2 + y^2D$$
**Problem** Find an elliptic curve $E$ such that $End(E) = \mathbb{Z}[\pi]$ where

$$\pi = -x \pm y\sqrt{-D}.$$ 

Q: How to construct $E$ with $End(E) = \mathbb{Z}[\pi]$?

**Key Theorem:** (Deuring)

$$\tilde{E} \text{ over } \mathbb{C} \rightarrow E \text{ over } \mathbb{F}_p$$

$End(\tilde{E}) = \mathbb{Z}[\pi]$  $End(E) = \mathbb{Z}[\pi]$ 

provided that $j(\tilde{E})$ “makes sense” in $\mathbb{F}_p$. 
Fact: If $\text{End}(\tilde{E}) = \mathbb{Z}[\pi]$, then $j(\tilde{E})$ satisfies a polynomial with integer coefficients.

So we can view this polynomial in $\mathbb{F}_p[x]$, and try to find its roots.

Eg: Solve $x^2 + 1 = 0$ in $\mathbb{F}_p$:

- $i \in \mathbb{F}_5$ since $-1 = 4 = 2^2$ in $\mathbb{F}_5$.

- $i \notin \mathbb{F}_7$ since $-1 = 6$ has no square root in $\mathbb{F}_7$.

Problem: Find an elliptic curve $\tilde{E}$ over $\mathbb{C}$ such that

1. $\text{End}(\tilde{E}) = \mathbb{Z}[\pi]$, and

2. the polynomial of $j(\tilde{E})$ has roots in $\mathbb{F}_p$. 
Fact: It’s straightforward to find an elliptic curve $\tilde{E}$ over $\mathbb{C}$ with

$$\text{End}(\tilde{E}) \simeq \mathbb{Z}[\pi].$$

Key Theorem: The polynomial of $j(\tilde{E})$ is the Hilbert class polynomial $H_D(x)$ of $K = \mathbb{Q}(\sqrt{-D})$, and all its roots are $j$-invariants of elliptic curves with $\text{End}(\tilde{E}) = \mathbb{Z}[\pi]$.

Q: When does $H_D(x)$ have roots in $\mathbb{F}_p$?
Let $\mathcal{O}_D = \mathbb{Z}[\sqrt{-D}]$.

- An **ideal** $I$ of $\mathcal{O}_D$ is a subset of $\mathcal{O}_D$ closed under addition and multiplication by $\mathcal{O}_D$.

- An ideal is **principal** if $I = (\alpha)$ for $\alpha \in \mathcal{O}_D$.

- The ideal $(p)$ **splits** in $\mathcal{O}_D$ if $(p) = \mathcal{P}_1 \mathcal{P}_2$, for two distinct prime ideals.

**Key Theorem:** The polynomial $H_D(x)$ has a root in $\mathbb{F}_p$ if and only if the ideal $(p)$ splits into principal ideals in $\mathcal{O}_D$.

Q: When does $(p)$ split into principal ideals?
Eg: $D = 1$ and the prime 5

The prime 5 can be written as:

$$5 = 1^2 + 2^2 \cdot 1$$

$$\Rightarrow 5 = (1 + 2i)(1 - 2i) \quad \text{in } \mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$$

$$\Rightarrow (5) = (1 + 2i)(1 - 2i) \quad \text{as ideals in } \mathbb{Z}[i]$$

More generally,

$$(p) \text{ splits into principal ideals in } \mathbb{Z}[\sqrt{-D}]$$

if and only if

$$p = x^2 + y^2D \quad \text{for } x, y \in \mathbb{Z}$$
Recall the **Frobenius map** \( \pi \) is

\[
\pi = -x \pm y\sqrt{-D}
\]

\[\implies p = x^2 + y^2D \text{ for integers } x, y\]

\[\implies \text{the ideal } (p) \text{ splits into principal ideals in } \mathcal{O}_D\]

\[\implies H_D(x) \text{ has a root in } \mathbb{F}_p\]

In fact, \( H_D(x) \) will have all its roots in \( \mathbb{F}_p \).

**Solution:** Any root of \( H_D(x) \) in \( \mathbb{F}_p \) will be the \( j \)-invariant of an elliptic curve \( E \) over \( \mathbb{F}_p \) with

\[
\#E(\mathbb{F}_p) = N.
\]
An Example

Let $p = 661$ and $N = 2 \times 347 = 694$.

Find $E$ such that $\#E(\mathbb{F}_{661}) = 694$.

- $t = p + 1 - N = -32$

- $t^2 - 4p = -1620 = 18^2 \cdot 5 \Rightarrow D = 5$.

- $H_{-5}(x) = x^2 - 1264000x - 681472000$

- In $\mathbb{F}_{661}[x], H_{-5}(x) = x^2 + 493x + 492$

Using the root $j = 169$, we create the curve

$$y^2 = x^3 + 24x + 500$$

which has 694 points over $\mathbb{F}_{661}$!

Also note that for $x = 16, y = 9$,

$$661 = x^2 + y^2 \cdot 5$$
Conclusion

• We can construct elliptic curves that are good for cryptography.

• To do this, we must find roots of a certain polynomial $H_D(x)$ in $\mathbb{F}_p$.

• $H_D(x)$ has (all) roots in $\mathbb{F}_p$ exactly when $p$ is of the form $x^2 + y^2D$.

• So it’s enough to know $H_D(x)$...

• **Current Research Directions**
  
  – Improve complex analytic/$p$-adic methods to compute $H_D(x)$. (Atkins, Couveignes)

  – Work with “smaller” polynomials that describe the same $j$. (Bröker)