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

Juliana V. Belding

University of Maryland
Department of Mathematics
College Park, MD

February 5, 2008
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.
- The **$j$-invariant**

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

classifies elliptic curves up to isomorphism.
Example

\[ E : y^2 = x^3 + 1 \text{ over } \mathbb{R} \]

There is a way to define \textbf{addition of points} on the curve, so including the point at infinity \( P_\infty \),

\[ E(F) \text{ is a group!} \]
The group of points of an elliptic curve $E$ over $\mathbb{F}_p$

Let $F = \mathbb{F}_p$, the finite field of $p$ elements.

- $E(\mathbb{F}_p)$ is the set of all pairs

  \[(x_0, y_0)\]

  with $x_0, y_0 \in \{0, 1, 2, ..., p - 1\}$ such that

  \[y_0^2 = x_0^3 + Ax_0 + B.\]

- $E(\mathbb{F}_p)$ is finite.

Q: How large is $E(\mathbb{F}_p)$?
Finding points of $E$ over $\mathbb{F}_p$

$$y^2 = x^3 + 1 \text{ over } \mathbb{F}_7$$

- Take any $x_0$ in $\mathbb{F}_7$. Does

$$x_0^3 + Ax_0 + B$$

have a square root $y_0$ in $\mathbb{F}_7$?
- Eg: For $x_0 = 1$, we get $1^3 + 1 \equiv 2$
- Is 2 a square modulo 7?
- Yes:

$$3^2 \equiv 2 \text{ and } 4^2 \equiv 2 \text{ in } \mathbb{F}_7$$

- So $(2, 3)$ and $(2, 4)$ are points of $E$. 
How large is $E(\mathbb{F}_p)$?

- If $x_0^3 + Ax_0 + B$ is a square, we get two points (usually).
- Half the elements of $\mathbb{F}_p$ are squares.
- So, we expect $p + 1$ points in $E(\mathbb{F}_p)$ including $P_\infty$.

The group of points of $E$ has $N = 12$ elements:

$$E(\mathbb{F}_7) = \{(0, 1), (0, 6), (1, 3), (1, 4), (2, 3), (2, 4), (3, 0), (4, 3), (4, 4), (5, 0), (6, 0), P_\infty\}$$

The error is $t = p + 1 - N = -4$. 
How large is $E(\mathbb{F}_p)$?

**Hasse’s Theorem**: The “error" $t = p + 1 - N$ satisfies

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

**Our Goal**

Given $p, N$ satisfying Hasse’s Theorem,

find a curve $E$ over $\mathbb{F}_p$ with exactly $N$ points.

Q: Why?
The Discrete Logarithm Problem

Let \( m \cdot P = P + P + \ldots + P \).

The **Discrete Logarithm Problem** in \( E(\mathbb{F}_p) \):

Given \( P \) and \( Q = m \cdot P \), find the “multiplier” \( m \).

Q: When is this “hard” to solve?
Solving the DLP: Brute Force

Compute multiples of $P$ until one matches $Q$:

\[
\begin{align*}
1P &= Q \ ? \\
2P &= Q \ ? \\
3P &= Q \ ? \\
\vdots \\
m \cdot P &= Q \ !!
\end{align*}
\]

If brute force is essentially the only way to solve it, then the DLP is "hard" and...

We can use $m$ to disguise information!
An Example: The Discrete Logarithm Problem in $E$

Given $P = (1, 3), Q = (0, 6)$ find $m$ such that

$$m \cdot P = P + P + \ldots + P = Q$$

**Brute force**

- $2 \cdot P = (0, 1)$
- $3 \cdot P = (3, 0)$
- $4 \cdot P = (0, 6)$
- So $m = 4$. 
A Cryptographic Curve: NIST P-192

\[ y^2 = x^3 + Ax + B \]

where \( A = -3 \) and \( B = \)

\[
2455155546008943817740293915197451784769108058161191238065
\]

over \( \mathbb{F}_p \) where \( p = \)

\[
6277101735386680763835789423207666416083908700390324961279
\]

This group has

\[
6277101735386680763835789423176059013767194773182842284081
\]

points!
Cryptographic Curve

A cryptographic curve is an elliptic curve $E$ over $\mathbb{F}_p$ with

- $N = \#E(\mathbb{F}_p)$ a large (almost) prime number ($\approx 10^{80}$)
- Not vulnerable to special attacks ($N \neq p$ or $p + 1$)

Q: How can we use $E$ for cryptography?
Two parties A and B exchange information privately using a secret shared key $K$:

- A “locks” the message with $K$ and sends it to B

$$A^{K(message)} \rightarrow B$$

- B can “unlock” the message using $K$
- Nobody else can read the locked message if $K$ is private.

Q: How can A and B agree on a secret key $K$ over a non-secure channel?
Diffie-Hellman Key Exchange

- A, B choose a curve $E$ and a prime $p$
- A, B choose a point $P$ of $E(\mathbb{F}_p)$
- A chooses a secret integer $a$ and sends $a \cdot P = Q$ to B
- B chooses a secret integer $b$ and sends $b \cdot P = R$ to A

\[
\begin{align*}
A & \xrightarrow{Q} B \\
A \xleftarrow{R} B
\end{align*}
\]
Diffie-Hellman Key Exchange, cont.

- A computes \( a \cdot R = a(b \cdot P) = (ab)P \)
- B computes \( b \cdot Q = b(a \cdot P) = (ab)P \)
- The **shared private key** is

\[
K = (ab)P
\]

Everybody knows \( Q, R \) and \( P \)...

but nobody can know \( K \) without knowing either \( a \) or \( b \)!
Constructing a curve with $N$ points

Goal (V1)

Given $p, N$ satisfying Hasse’s Theorem, with $N$ (almost) prime, find a curve $E$ over $\mathbb{F}_p$ with exactly $N$ points.

At this point, we don’t know know if such a curve even exists...

... but if it does, what can we say?
The Endomorphism Ring of $E$

- The **endomorphism ring** of $E$ is all rational maps
  
  $$\phi : E \rightarrow E$$

  that preserve addition.

- The operations are addition and composition of maps.

- Every $E$ has **multiplication-by-$m$** maps:

  $$[m]P := \underbrace{P + P + \ldots + P}_m.$$ 

  so $\mathbb{Z} \subset \text{End}(E)$. 
Key Tool: The Frobenius Endomorphism

- For $E$ over $\mathbb{F}_p$, the **Frobenius map**
  \[
  \pi : (x, y) \mapsto (x^p, y^p)
  \]
  is also an endomorphism of $E$.

- Recall
  \[x \in \mathbb{F}_p \text{ if and only if } x^p = x.\]

- So
  \[P = (x, y) \in E(\mathbb{F}_p) \text{ if and only if } \pi(P) = P\]

- $\pi$ gives us information about $\#E(\mathbb{F}_p)$. 
The Frobenius Endomorphism, cont.

**Fact:** If the Frobenius satisfies

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

then $E$ over $\mathbb{F}_p$ has $N = p + 1 - t$ points.

**Goal (V2)**

Find a curve $E$ with $\text{End}(E) = \mathbb{Z}[\pi]$ where

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

This curve will have $N$ points over $\mathbb{F}_p$. 
When is a prime $p$ the sum of two squares?

$$p = x^2 + y^2?$$

Eg: $5 = 1^2 + 2^2$

**Fermat’s Theorem**

For $p$ odd, $p = x^2 + y^2$ for $x, y \in \mathbb{Z}$ if and only if $p \equiv 1 \mod 4$.

More generally, for $D > 0$,

When is $p = x^2 + y^2 D$?
Q: How does this relate to the Frobenius $\pi$?

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

- By Hasse’s Thm, 
  $$t^2 - 4p \leq 0$$

- For $f, D \in \mathbb{Z}^+$ with $D$ squarefree write 
  $$t^2 - 4p = -f^2D$$
  
  $$\Rightarrow 4p = t^2 + f^2D$$

- For $N = 2 \cdot \text{prime}$, $t$ is even, so divide by 4: 
  $$p = x^2 + y^2D$$

for integers $x, y$. 
Given $p, N$ satisfying Hasse’s theorem, we can solve

$$p = x^2 + y^2D$$

for integers $x, y$ and some $D > 0$ directly related to $p$ and $N$ (via the “error" $t$).

And, if $E$ exists, the Frobenius element in $\text{End}(E)$ will be

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

for this $x$ and $y$. 
The Complex Connection

**Goal (V2)**

Find a curve $E$ over $\mathbb{F}_p$ with $\text{End}(E) = \mathbb{Z}[\pi]$.

**Key Theorem:** (Deuring)

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

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

if the $j$-invariant of $\tilde{E}$ “makes sense” in $\mathbb{F}_p$. 
Eg: When is $i$ in $\mathbb{F}_p$?

The complex number $i$ satisfies a polynomial with *integer* coefficients:

$$X^2 + 1 = 0.$$ 

So we can look for solutions to $X^2 + 1 = 0$ 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 $\mathbb{F}_7$. 

The Hilbert Class Polynomial

**Key Theorem:** (Complex Multiplication)

- If \( \text{End}(\tilde{E}) = \mathbb{Z}[\pi] \), then \( j(\tilde{E}) \) is a root of a polynomial \( H_D(X) \) with *integer* coefficients.

- This is called the **Hilbert class polynomial** of \( K = \mathbb{Q}(\sqrt{-D}) \).

**Goal (V3)**

Find roots (if any) of \( H_D(X) \) in \( \mathbb{F}_p \).

These will be \( j \)-invariants of curves \( E \) over \( \mathbb{F}_p \) with \( N \) points.
Q: Does $H_D(X)$ have roots in $\mathbb{F}_p$?

**Key Theorem:** (Class Field Theory)

$H_D(x)$ has roots in $\mathbb{F}_p$

if and only if

$$p = x^2 + y^2D$$

for some integers $x, y$
... so $E$ exists!

Since $p, N$ satisfy Hasse’s theorem,

$$p = x^2 + y^2 D$$

for $x, y \in \mathbb{Z}$.

This implies that $H_D(x)$ has roots in $\mathbb{F}_p$.

**Mission Accomplished:**

These are $j$-invariants of curves $E$ over $\mathbb{F}_p$ with $N$ points!
Eg: \( p = 661 \) and \( N = 2 \cdot 347 = 694 \)

- Check that \( t = p + 1 - N = -32 \) satisfies Hasse’s Theorem:
  \[
  32 \leq 2\sqrt{661} \approx 51
  \]

- So there is a curve \( E \) with
  \[
  \#E(\mathbb{F}_{661}) = 694.
  \]

- To find it, write
  \[
  t^2 - 4p = -1620 = -18^2 \cdot 5
  \]

- So
  \[
  D = 5, f = 18, t = 32
  \]
Eg: \( p = 661 \) and \( N = 2 \cdot 347 = 694 \)

For \( f = 18, \ t = 32, \) we have

\[
4 \cdot 661 = t^2 + f^2 \cdot 5
\]

So, for \( x = 16, \ y = 9 \)

\[
661 = x^2 + y^2 \cdot 5
\]
Eg: \( p = 661 \) and \( N = 2 \cdot 347 = 694 \)

- In \( \mathbb{Z}[X] \),
  \[
  H_5(X) = X^2 - 1264000X - 681472000.
  \]

- In \( \mathbb{F}_{661}[X] \),
  \[
  H_5(X) = x^2 + 493X + 492.
  \]

- It has two roots:
  \( j = 169, 660 \).

The root \( j = 169 \) gives
\[
E : y^2 = x^3 + 24x + 500.
\]

*By construction*, this curve has 694 points over \( \mathbb{F}_{661} \)!!
Conclusion

- Elliptic curves are useful for cryptographic protocols, e.g.: key exchange
- We can find $E$ with $N$ points using roots of $H_D(X)$ in $\mathbb{F}_p$.
- $H_D(X)$ has roots in $\mathbb{F}_p$ exactly when $p$ is of the form $x^2 + y^2D$
- So it’s enough to know $H_D(X)$...
Computing $H_D(X)$

$$H_D(X) = X^d + ... + C$$

- For cryptography, $D$ should be large (world record: $\approx 10^{10}$)
- Degree $d$ is large: $\approx \sqrt{D}$.
- Coefficients $C$ are huge: $\approx \sqrt{D}$ digits.
- Storing $H_D$ takes space $\approx D$ (world record: 5 GB, 3 days)

My Current Research: A $p$-adic method to compute $H_D(X)$
Thanks to...

- Harvard Math Table
- Dr. Larry Washington and Dr. Reinier Broker