Cannonballs, Triangles, and Secrets

An introduction to elliptic curve cryptography

Larry Washington, University of Maryland

The Mathematical Association of America
Maryland-District of Columbia-Virginia Section
A Pile of Cannonballs

A Square of Cannonballs
The number of cannonballs in $x$ layers is

$$1 + 4 + 9 + \ldots + x^2$$

$$= x (x + 1) (2x + 1)/6$$

$x=3$:

$$1 + 4 + 9 = 3(4)(7)/6 = 14$$
If $x$ layers of the pyramid yield a $y$ by $y$ square, we need

$$y^2 = 1 + 4 + 9 + \ldots + x^2$$

$$y^2 = x(x + 1)(2x + 1)/6$$
$y^2 = x (x + 1) (2x + 1)/6$
\[ y^2 = x (x + 1) (2x + 1)/6 \quad \text{and} \quad y = x \]
1 + 4 + 9 + \ldots + 24^2 = 70^2
Is there a right triangle with rational sides whose area is 5?

\[ a^2 + b^2 = c^2 \]
\[ \frac{ab}{2} = 5 \]

If we have a, b, c, let \[ x = \frac{1}{4} c^2 \]

Then \[ x - 5 = \frac{1}{4} (c^2 - 2ab) = \frac{1}{4} (a^2 + b^2 - 2ab) = \frac{1}{4} (a-b)^2 \]

Similarly, \[ x + 5 = \frac{1}{4} (a+b)^2 \]

Therefore, \[ x^3 - 25x = x(x-5)(x+5) \] is a square.
We need points on the curve \( y^2 = x^3 - 25x \) with rational coordinates.

\((x, y) = (-4, 6)\) is a point on the curve. Draw the tangent line at this point.

The intersection point has \( x = 1681/144 = (41/12)^2 \).
Area = 5
We can use the tangent line at this new point and find another triangle:

\[ x = \left(\frac{3344161}{1494696}\right)^2, \quad y = \text{a big fraction} \]
We could produce many more . . .
But soon the whole page would not be large enough to contain the numbers.
An elliptic curve is the graph of an equation

\[ y^2 = \text{cubic polynomial in } x \]

For example,

\[ y^2 = x^3 - 5x + 12 \]
Start with $P_1$. We get $P_2$. 
Using $P_1$ and $P_2$, we get $P_3$. 
Using $P_1$ and $P_3$, we get $P_4$. 
We get points $P_1, P_2, P_3, \ldots, P_n, \ldots$

**Useful facts:**

If we take the line through $P_m$ and $P_n$ and reflect the third point of intersection across the y-axis, we get $P_{n+m}$

If we start with $P_1$, after $m$ steps we get $P_m$
If we start with $P_m$, after $n$ steps we get $P_{mn}$
All of these calculations are done mod a big prime. Otherwise, the computer overflows.

Given \( n \), it is easy to compute \( P_n \) (even when \( n \) is a 1000-digit number)

Given \( P_n \), it is very difficult to figure out the value of \( n \).
Is this good for anything?
There is no branch of mathematics, however abstract, which may not someday be applied to the phenomena of the real world.

—Nikolai Lobachevsky (1792-1856)
“Do you know the secret?”
The Eavesdropper
The secret is a 200-digit integer $s$. Prove to me that you know the secret.

I send you a random point $P_1$.

You compute $P_s$ and send it back to me.

If your answer is correct, I decide that you know the secret.
Diffie – Hellman Key Establishment

Alice and Bob want to agree on a key for use in a cryptosystem.

1. They choose an elliptic curve and a point \( P_1 \) on the curve.

2. Alice chooses a secret integer \( a \) and Bob chooses a secret integer \( b \).

3. Alice computes \( P_a \) and Bob computes \( P_b \). They exchange \( P_a \) and \( P_b \).

4. Alice does \( a \) steps starting with \( P_b \) and computes \( P_{ba} \), and Bob computes \( P_{ab} \).

5. They use the coordinates of \( P_{ab} \) to construct the desired key.
Lived from ?? to ??

Probably about 1800 years ago.
Diophantus passed one sixth of his life in childhood, one twelfth in youth, and one seventh as a bachelor. Five years after his marriage was born a son who died four years before his father, at half his father’s age.

How many years did Diophantus live?
Diophantus passed one sixth of his life in childhood, one twelfth in youth, and one seventh as a bachelor. Five years after his marriage was born a son who died four years before his father, at half his father’s age.

How many years did Diophantus live?

84
Problem 1

To divide a given number into two having given difference.

Given number 100,

Given difference 40.

Lesser number is $x$. Larger is $x + 40$.

Therefore

$$2x + 40 = 100$$

$$x = 30$$

The required numbers are 70, 30.
K^β φ Δ^γ ισMδ

2x^3 - 3x^2 = 4

σαισMβ

x = 2
\[\Delta y_{1e} \Phi M\lambda \varsigma \ \epsilon \nu \ \mu \omicron \rho \iota \omega \ \Delta y_{1a} M\lambda \varsigma \ \phi \ \Delta y_{1}\beta\]

\[
(15 \ x^2 - 36)/(x^4 + 36 - 12 \ x^2)
\]
+, -  1489
=  1557
x  1620
.  1600
>  1600
a_2, a_3, a_4, ...  1634
a^2, a^3, a^4, ...  1637 (Descartes)
Diophantus’s goal:
Given a solution of an equation, find another solution.

Given a point on a curve, find another point.
Using $P_1$ and $P_3$, we get $P_4$. 
**Problem:** Find rational $x$ and $y$ such that $x^2 + y^2 = 1$.

We know the easy solution $x=1, y=0$.

Draw the line through this point with slope, say, $-2$.

The second point of intersection gives a new point, in this case $x = 3/5, y = 4/5$. 
What happens if we try higher degree curves?

\[ y^2 = x^5 - 7x^3 + 6x + 17 \]
Faltings’s Theorem (1983):

A higher degree curve (technically: genus > 1) has only a finite number of points with rational coordinates.
THANK YOU