# Elliptic curve cryptography

$$y^2 = x^3 + 2x + 2 \mod 17$$ All solutions?

Hint

| $y$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y^2 \bmod 17$ | 0 | 1 | 4 | 9 | 16 | 8 | 2 | 15 | 13 | 13 | 15 |

| $y$ | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|
| $y^2 \bmod 17$ | 2 | 8 | 16 | 9 | 4 | 1 |

| $x$ | possible $y$'s |
|---|---|
| 0 | 6, 11 |
| 1 | — |
| 2 | — |
| 3 | 1, 16 |
| 4 | — |
| 5 | 1, 16 |
| 6 | 3, 14 |
| 7 | 6, 11 |
| 8 | — |
| 9 | 1, 16 |
| 10 | 6, 11 |

| $x$ | possible $y$'s |
|---|---|
| 11 | — |
| 12 | — |
| 13 | 7, 10 |
| 14 | — |
| 15 | — |
| 16 | 4, 13 |

18 total

What do we notice:

1) 18 solutions $(\approx 17)$

~~Each x~~ For $y^2 \equiv x^3 + ax + b \mod p$

$p^2$ possible $(x,y)$

$\approx 1/p$ chance of a given pair working

$\to$ about $p$ solutions.

Hasse Bound

The number of solutions $N$ satisfies

$$p+1-2\sqrt{p} < N < p+1+2\sqrt{p}$$

Thm (Waterhouse): All those possibilities are equally likely.
PSU

2) Possible $y$ pairs always add to 17.

$y^2 = (-y)^2$, and $-y \bmod 17$ is $17-y$

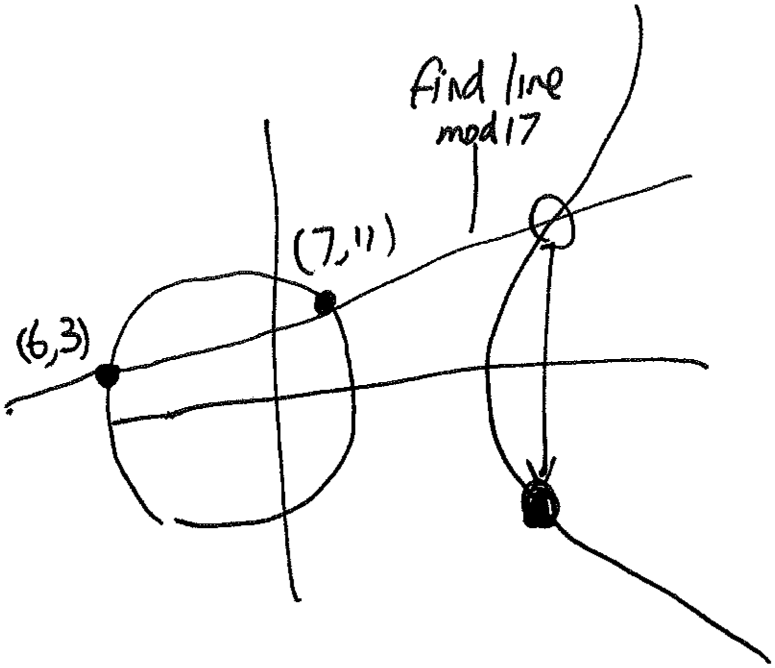
3) For about half x-values there are 2 y's
about half x-values, there are none.

→ Where there is a $y$ that works for given $x$ depends on whether $x^3+ax+b$ is a square modulo $p$. Half of numbers are squares, half aren't.
("Quadratic reciprocity" helps find which are which.)

(There could be some $x$'s where only $y=0$ occurs)

You can still do elliptic curve addition mod $p$!

$(6,3)+(7,11)$




Line:

$y = 8x - 45 = 8x + 6$

Plug in:

$y^2 = x^3 + 2x + 2 \mod 17$

$(8x+6)^2 = x^3 + 2x + 2$

$64x^2 + 96x + 36 = x^3 + 2x + 2$

mod 17

$13x^2 + (??)x + (??) = x^3 + 2x + 2$

$0 \equiv x^3 - 13x^2 + (\text{junk})$

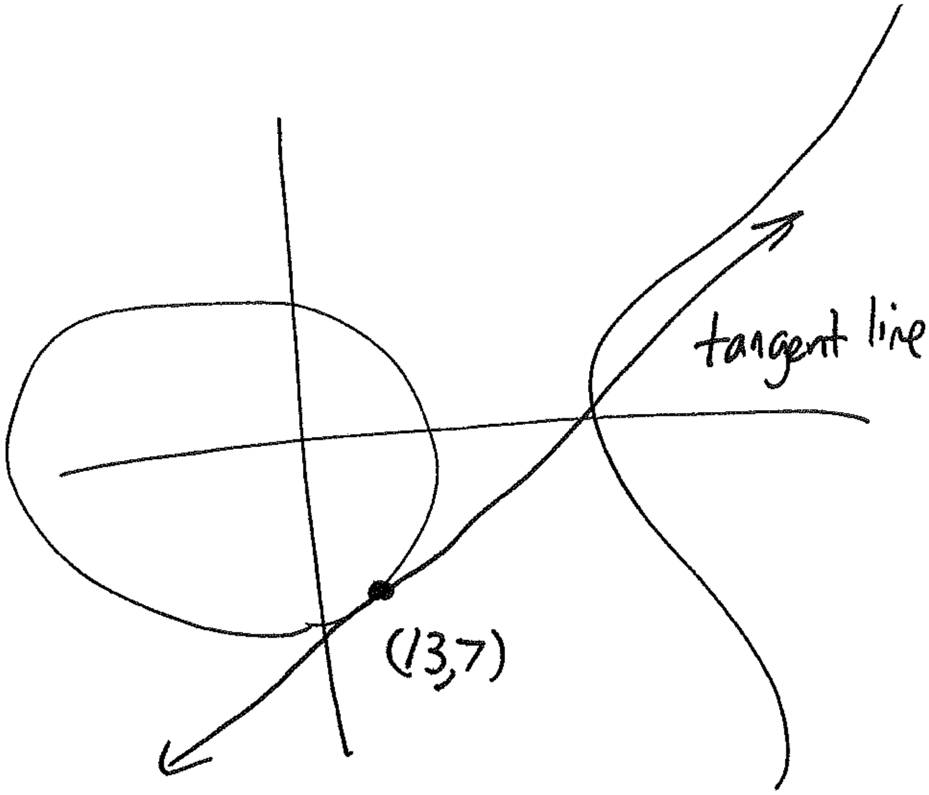
6, 7 are solutions

$\boxed{x = 0}$

$y = 6$ so third point is $(0,6)$

$(6,3) + (7,11) = (0,-6) = (0,11)$.

$(13,7) + (13,7)$




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

$3\cdot 13^2+2$

$=3\cdot(-1)+2=-1=16$

$2y\frac{dy}{dx}=3x^2+2$

at $(x,y)=(13,7)$

$\frac{dy}{dx}=\frac{3x^2+2}{2y}$

$\frac{dy}{dx}=\frac{16}{14}=\frac{-1}{-3}=\frac{1}{3}=6.$

Tangent line:

or $\frac{16}{14}=16\cdot 11=6.$

$\cancel{y=6x+71}$ $y=6x-71$

$=6x+14 \mod 17$

$(6x+14)^2 = x^3+2x+2 \quad \text{mod } 17$

only care about $x^2$ term

$36x^2 + (\text{junk}) = x^3 + (\text{junk})$

$x^3 - 36x^2 + (\text{junk}) = 0$

13 is double root so

$13+13+r=36$

$\boxed{r=10}$

$x=10$

$y=6x+14=74=6.$

so $(13,7)+(13,7)=(10,-6)=(10,11)$

We did $(13,7)+(13,7)$.

How would you find $100\cdot(13,7)$?

$$\left[\ \big((13,7)+\cdots+(13,7)\big) \text{ 100 times}\right]$$

$(13,7)$

$\times 2$

$2\cdot(13,7)=(10,11)$

$\times 2$

$4\cdot(13,7)$

keep doubling

$8\cdot(13,7)$

$16\cdot(13,7)$

$32\cdot(13,7)$

$64\cdot(13,7)$

$128\cdot(13,7)$

$$100\cdot(13,7)=64\cdot(13,7)+32\cdot(13,7)+4\cdot(13,7)$$

NB: This works because + is associative. (E is a group)

$$5P \overset{\text{directly}}{=} (((P+P)+P)+P)+P$$

$$5P=\underbrace{((P+P)+(P+P))}_{4P}+\underset{P}{P}$$

$4P + P$

IV

Calculating 100P

$100\cdot(13,7)$ is easy (repeated doubling)

What if I told you

$n\cdot(13,7)=(0,11)$.

Can you tell me $n$? ← "Elliptic curve discrete log problem"

Only way is brute force!

---

<u>Elliptic curve cryptography</u>

First: Elliptic curve Diffie-Hellman

A & B want to agree on a secret shared key over public channel.

Here's what they do:

First: publicly agree on:

- prime $p$
- an elliptic curve $y^2 = x^3 + ax + b \mod p$
- a point $G = (x, y)$ on elliptic curve

it's safe to always use same curve, $G$.

e.g. use government-issued one NIST P-192

---

Alice picks a number $d_A \in [1, n-1]$ ← $n$ = number of solutions or use $p/2$ if you want.

(keeps secret)

Bob picks a number $d_B \in [1, n-1]$

A computes ~~$d_A$~~, $d_A \cdot G = Q_A$, sends to Bob

B computes $d_B \cdot G = Q_B$, sends to Alice

Now:

Bob does $d_B \cdot Q_A = d_B \cdot (d_A \cdot G)$ $\overset{\text{''}}{K}$

Alice does $d_A \cdot Q_B = d_A \cdot (d_B \cdot G)$

) same thing! (group law is associative)

their shared secret key is the x-coordinate of $K$.

---

What does an eavesdropper know?

$Q_A$ $(p, E, a, b, G)$

$Q_B$

elliptic curve data

But knowing $Q_A$ isn't enough to find $d_A$

knows $Q_A = d_A \cdot G$ (discrete log problem)