Applied Cryptography
CPEG 472/672
Lecture 11B

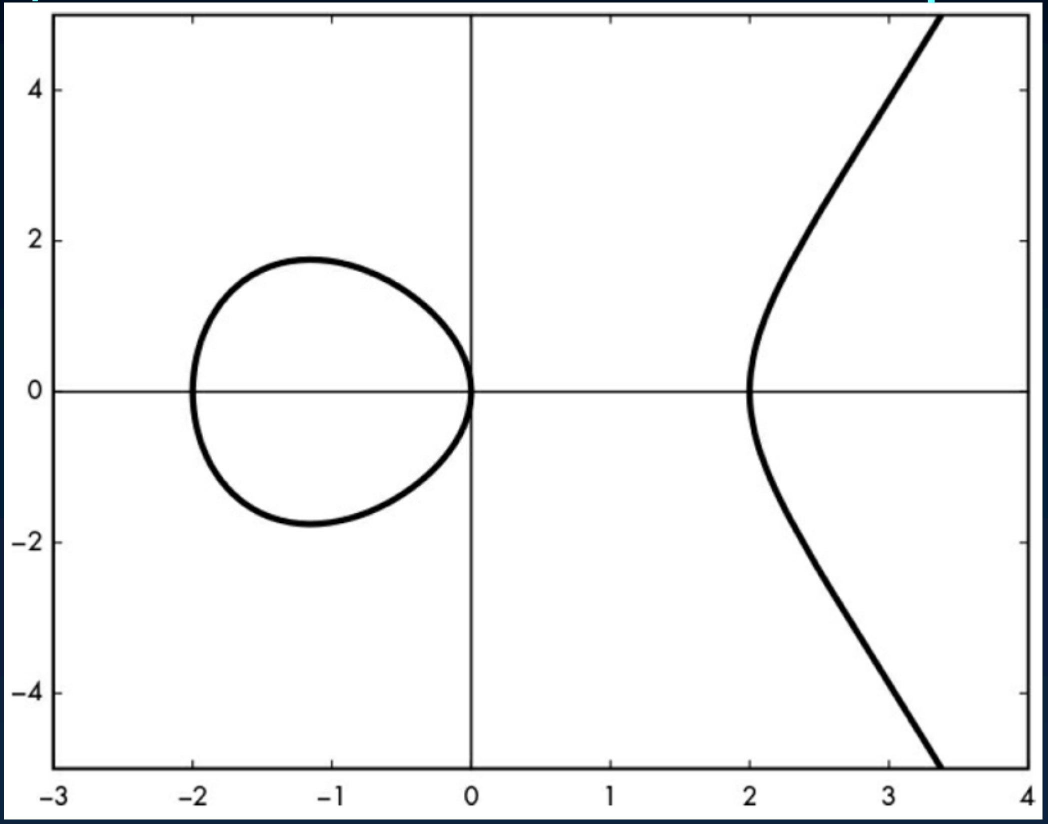
Instructor: Nektarios Tsoutsos

Elliptic Curves (EC)

- More powerful & efficient than RSA, D-H
  - Smaller integers for same security
  - 256-bit EC is equivalent to 4096-bit RSA
- More complicated math that RSA, D-H
  - OpenSSL (2005), OpenSSH (2011)
  - Used in Bitcoin, smart phones etc.
- Most application rely on ECDLP
  - Elliptic curve counterpart of DLP
  - Main idea: addition of 2D points on a curve

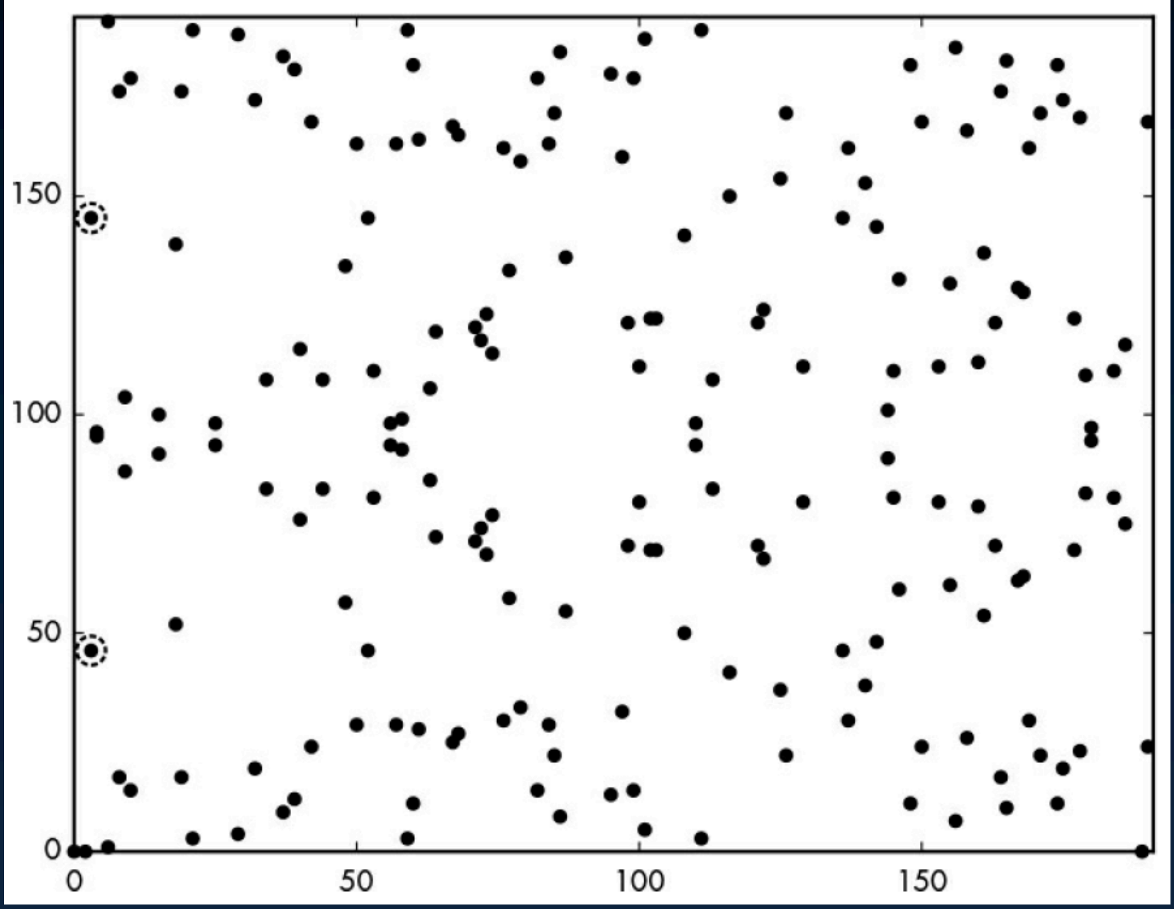
What is an EC?

- A group of points on a plane
  - Curve equation $y^2 = x^3 + ax + b$
  - The values of a, b define the curve shape
- Example
  - a=-4
  - b=0
- Select x value
  - Solve y
  - Not all x have real solution



EC over integers

- In this case we use integers on $\mathbb{Z}_p$
  - No real numbers, everything is mod p
- Example
  - $\mathbb{Z}_{191}$
  - $\mathrm{a} = -4, \mathrm{b} = 0$
- Horizontal symmetry
- About p points



Square roots modulo a prime

- In General: Find y so that $y^2 = x \bmod p$
- In case of EC:
  - $y^2 = x^3 + ax + b \bmod p$
  - Find y for a given x in $\mathbb{Z}_p$

Finite Field Arithmetic on $\mathbb{Z}_p$

- Example using $\mathbb{Z}_{191}, a = -4, b = 0$:
  - $x = 3$
  - $y^2 = 3^3 - 4 \cdot 3 + 0 = 27 - 12 = 15 \bmod 191$
  - How to find y? $y = 46$ or $y = 145$
  - We use the Tonelli algorithm (demo today)

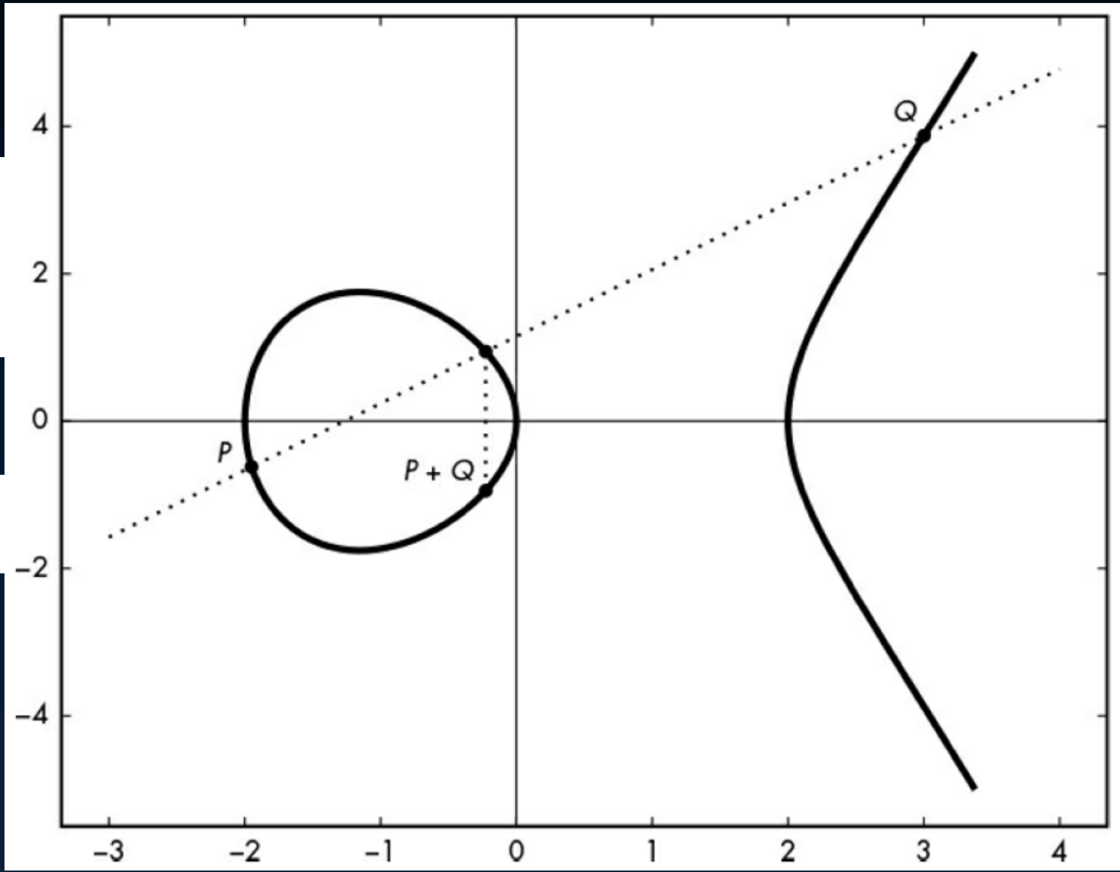
Addition of points

- Special rules apply: Addition law on EC
- $R = P + Q$

$$
\begin{aligned}
x_R &= (m^2 - x_P - x_Q) \bmod p \\
y_R &= [y_P + m(x_R - x_P)] \bmod p \\
&= [y_Q + m(x_R - x_Q)] \bmod p
\end{aligned}
$$

- If $P \neq Q$:

$$m = (y_P - y_Q)(x_P - x_Q)^{-1} \bmod p$$



Addition of points (2)

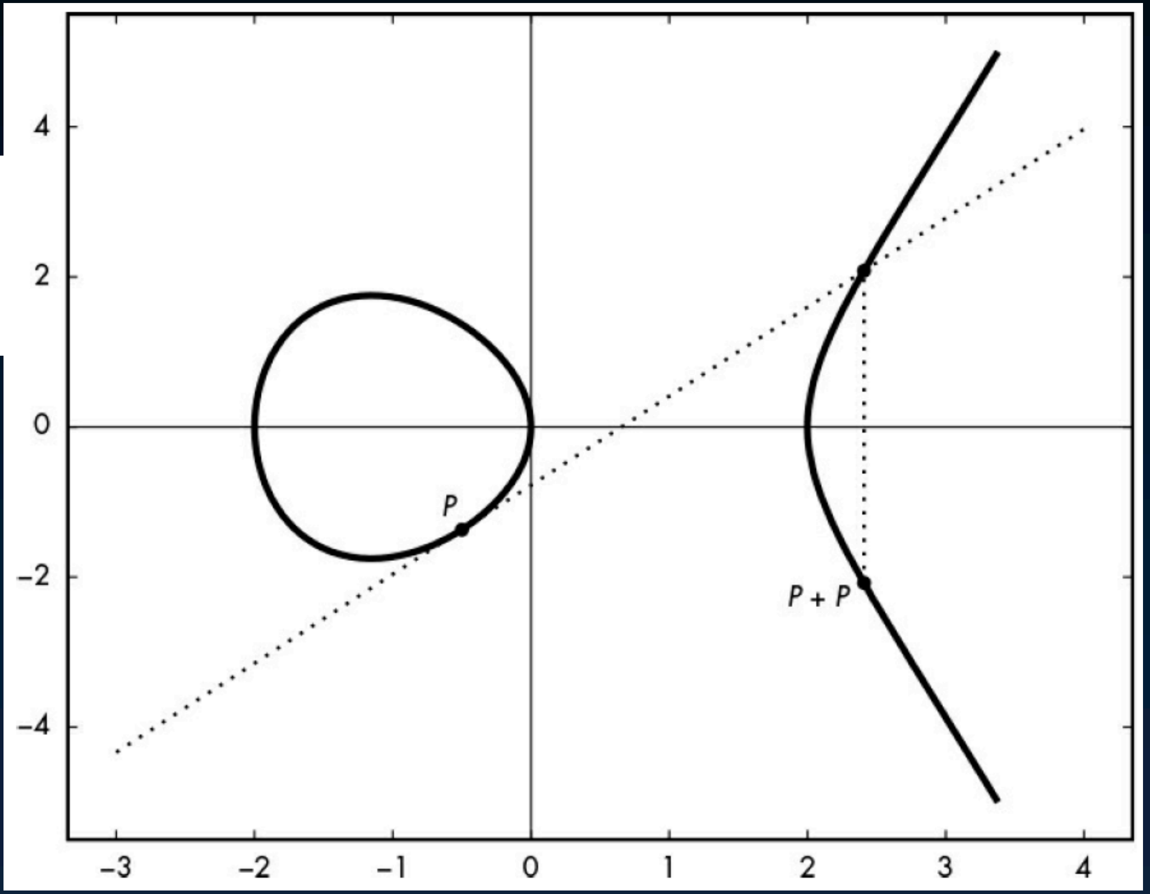
- Special rules apply: Addition law on EC
- $R = P + Q$

$$\begin{aligned} x_R &= (m^2 - x_P - x_Q) \bmod p \\ y_R &= [y_P + m(x_R - x_P)] \bmod p \\ &= [y_Q + m(x_R - x_Q)] \bmod p \end{aligned}$$

- If $P = Q$:

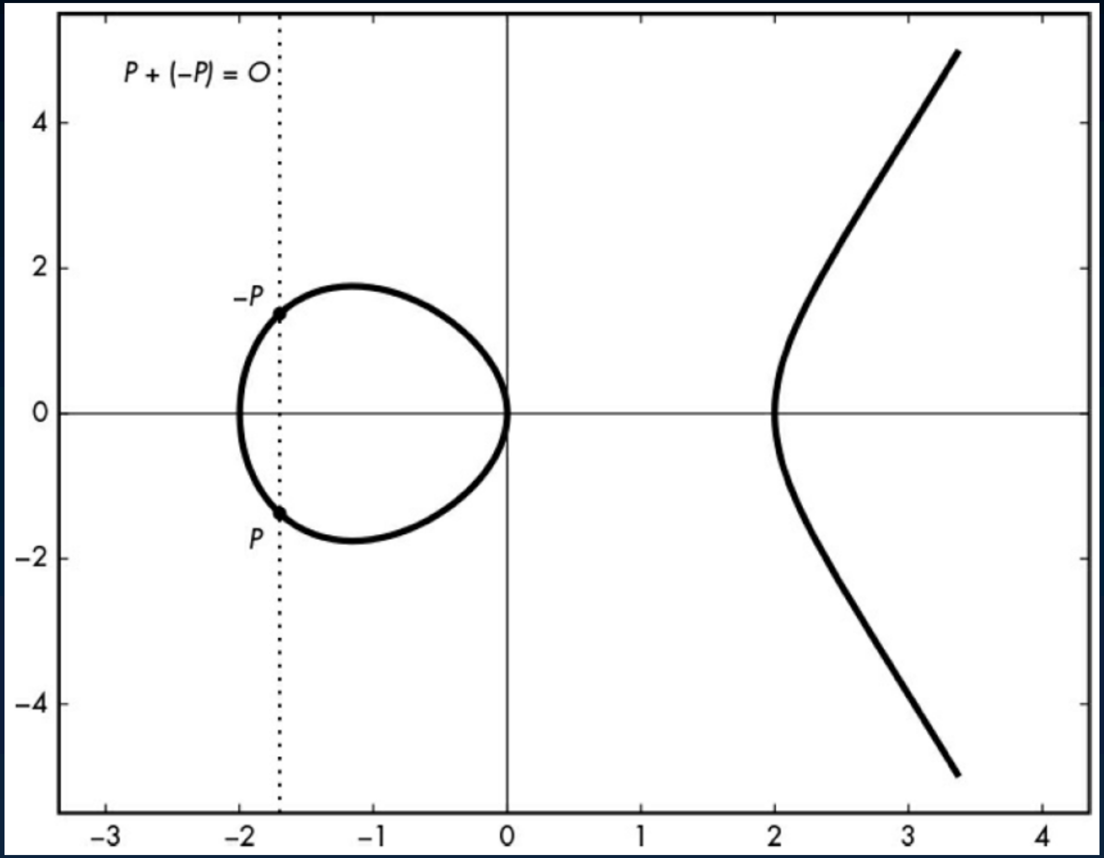
$$m = (3x_P^2 + a)(2y_P)^{-1} \bmod p$$

  - Doubling of P



Addition of points (3)

- Special rules apply: Addition law on EC
- What is $P + (-P)$?
- $P = (x_P, y_P)$
- $-P = (x_P, -y_P)$
- $P + (-P) = \mathcal{O}$
- Point of infinity
  - Equivalent to a zero element



Multiplication of point by value

- Multiplication of P by value k
  - Returns point kP
  - E.g., if $k = 3$ then $3P = P + P + P$
- Naïve technique: do $k - 1$ additions
  - Similar to naïve exponentiation in RSA
- Fast technique: use intermediate values
  - Example for $k = 8$:
  - $P_2 = P + P$, $P_4 = P_2 + P_2$, $P_8 = P_4 + P_4$
  - 3 additions instead of 7 using naïve

The ECDLP problem

- Given a point Q so that $Q = kP$, find k
  - Similar to DLP where we want the exponent
- The ECDLP is believed to be hard
  - Needs smaller numbers vs DLP to he hard
- When p is n bits, we get $n/2$ bits security
  - E.g., 256-bit p gives 128 bits of security
- How to find k?
  - Find collision $c_1 P + d_1 Q = c_2 P + d_2 Q$
  - Then $k = (c_1 - c_2)/(d_2 - d_1)$

Hands-on exercises

- Square roots modulo prime (Tonelli)
- Point addition on $\mathbb{Z}_p$
- CoCalc example of point addition
- Visual example of point addition

Reading for next lecture

- Aumasson: Chapter 12 until the end
  - We will have a short quiz on the material