Elliptic Curves and Cryptography (1)

- Many modern cryptosystems are based on prime numbers.
- The basic observation is that the exponentiation

$$A^K \equiv B \pmod{N}$$

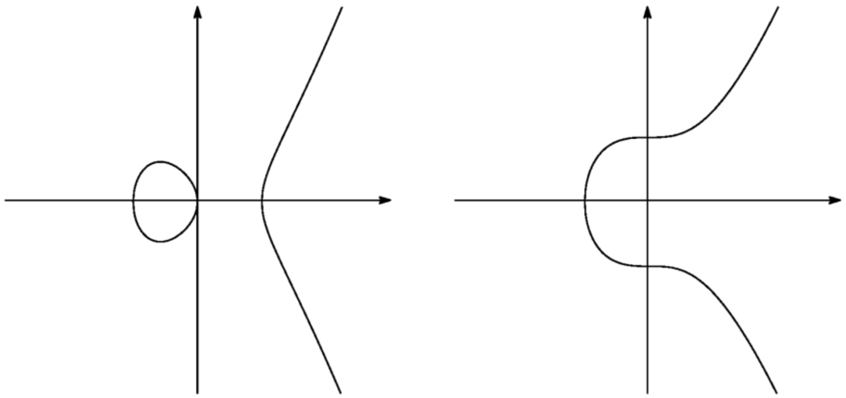
has **no obvious pattern** except for Fermat's Little Thm.

Elliptic Curves and Cryptography (2)

- Recently, cryptosystems based on geometric objects are extensively studied.
- **Elliptic Curve Cryptography** **(ECC)**, invented by Miller and Koblitz in 1985, is one such example
- Currently, people believe, if the size of the keys is the same, **ECC is more efficient and secure than RSA**.

Elliptic Curves and Cryptography (3)

- $P \geq 5$ prime number
- Curves $Y^2 = X^3 + AX + B$ are called **elliptic curves**. Here A, B are integers satisfying **$4A^3 + 27B^2 \not\equiv 0 \pmod{P}$**.



$Y^2 = X^3 - X$ $\quad$ $Y^2 = X^3 + 1$

Elliptic Curves and Cryptography (4)

- Points on elliptic curves are mysterious objects in mathematics.
- In Cryptography, we are interested in mod P points:
  - (S,T) $(0 \le S, T \le P-1)$ is called a **mod P point** if
    $$T^2 \equiv S^3 + AS + B \pmod{P}.$$
  - The **point at infinity** ∞ is also considered.

Elliptic Curves and Cryptography (5)

Example (P=5)

The elliptic curve $Y^2 = X^3 - X$ has 8 points (mod 5).

∞, (0,0), (1,0), (2,1), (2,4), (3,2), (3,3), (4,0)

S	0	1	2	3	4
$S^3 - S \pmod 5$	0	0	1	4	0

T	0	1	2	3	4
$T^2 \pmod 5$	0	1	4	4	1