2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199

More Fun with Prime Numbers

# Week 5
# Mystery of Prime Numbers:
## Past, Present, and Future


Tetsushi Ito

Department of Mathematics
Kyoto University


# Points on Elliptic Curves (1)

## Elliptic curves

- $Y^2 = X^3 + AX + B$

  A, B are integers s.t. $\mathbf{4A^3 + 27B^2 \neq 0}$.
- **Mod P points** play an important role in Elliptic Curve Cryptography (ECC).
- We are also interested in **rational points** (i.e., points whose coordinates are **rational numbers**).

# Points on Elliptic Curves (2)

## Rational Points

- $Y^2 = X^3 - X$ has only **4 rational points**:

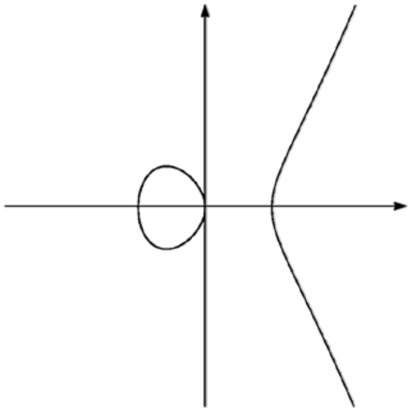
  $\infty, (0,0), (1,0), (-1,0)$

- $Y^2 = X^3 + 1$ has only **6 rational points**:

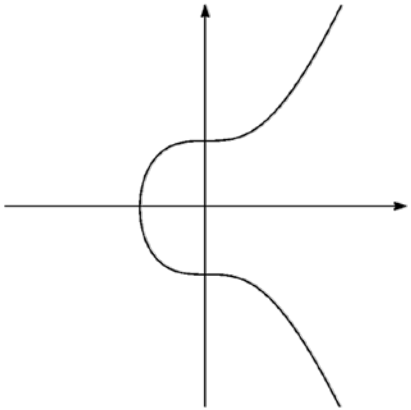
  $\infty, (-1,0)$

  $(0,1), (0,-1)$

  $(2,3), (2,-3)$



$Y^2 = X^3 - X$



$Y^2 = X^3 + 1$

# Points on Elliptic Curves (3)

## Rational Points

- $Y^2 = X^3 - 2$ has only **3 integral points**:

  $\infty$, (3,5), (3,–5)

- It has infinitely many **rational points**:

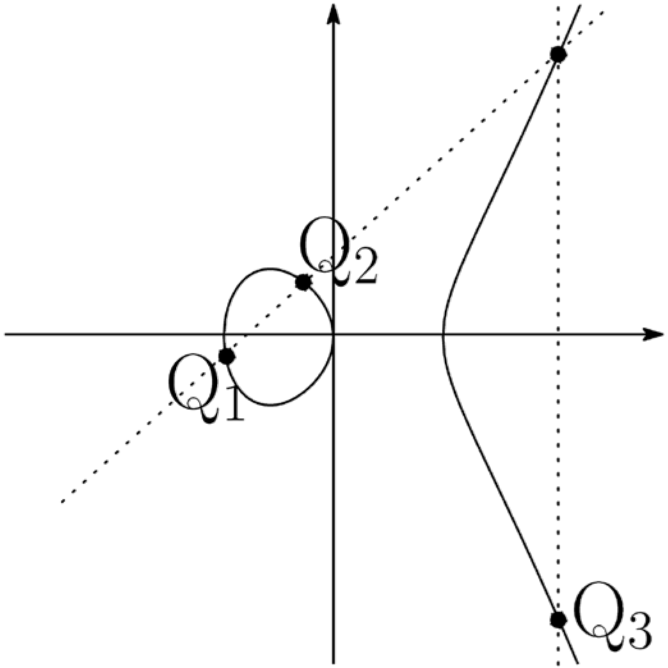
$$\left(\frac{129}{1000}, \pm\frac{383}{1000}\right), \left(\frac{164323}{29241}, \pm\frac{66234835}{5000211}\right), \left(\frac{2340922881}{58675600}, \pm\frac{113259286337279}{449455096000}\right), \ldots$$

- Which elliptic curves have finitely/infinitely many rational points?
- How can we find all integral/rational points?

# Points on Elliptic Curves (4)

(Recall) **Group Law**

- From given points $Q_1$ and $Q_2$, we can create a new point $Q_3$.
- **$Q_3 = Q_1 \oplus Q_2$.**



# Points on Elliptic Curves (5)

**$Q = (S, T)$**

- **$[-1]Q$** $= (S, -T)$.
- **$[N]Q$** $= Q \oplus \cdots \oplus Q \quad (N-1 \text{ times})$
- **$[-N]Q$** $= [-1]([N]Q)$
- For integers $N_1, \cdots, N_M$,

$$[N_1]Q_1 \oplus \cdots \oplus [N_M]Q_M$$

is **generated by $Q_1, \cdots, Q_M$**.