前回：

- **同値関係による類別・商集合**
- **剰余環 $\mathbb{Z}/m\mathbb{Z}$**

今回はその補足から

合同式 $a \equiv b \pmod{m}$ は、
剰余環 $\mathbb{Z}/m\mathbb{Z}$ 内での等式 $\overline{a} = \overline{b}$ と思える

今までの合同式に関する定理を、
剰余環 $\mathbb{Z}/m\mathbb{Z}$ の性質として書き直しておこう

合同式の基本性質

以下暫く、法 m を固定して $\pmod m$ を省略

- **合同関係 $\equiv$ が同値関係**
  - $\star$ $a \equiv a$ **(反射律)**
  - $\star$ $a \equiv b \Longrightarrow b \equiv a$ **(対称律)**
  - $\star$ $a \equiv b, b \equiv c \Longrightarrow a \equiv c$ **(推移律)**
  - $\longrightarrow$ **類別・商集合 $\mathbb{Z}/m\mathbb{Z}$ が作れる**
- **演算との関係**
  - $\star$ $x \equiv y \Longrightarrow x \pm c \equiv y \pm c, cx \equiv cy$
  - $\star$ $a \equiv a', b \equiv b' \Longrightarrow a \pm b \equiv a' \pm b', ab \equiv a'b'$
  - $\longrightarrow$ **商集合 $\mathbb{Z}/m\mathbb{Z}$ に加法・乗法が引起こり、可換環を成す**

剰余環 $\mathbb{Z}/m\mathbb{Z}$ の性質： 乗法群 $(\mathbb{Z}/m\mathbb{Z})^\times$

拡張版 Euclid の互除法より

$$\gcd(a, m) = 1 \Longrightarrow \exists x, y \in \mathbb{Z} : ax + bm = 1$$

$\longrightarrow$ $a \in \mathbb{Z}/m\mathbb{Z}$ **に対し、**

$$\gcd(a, m) = 1 \Longrightarrow \exists x \in \mathbb{Z}/m\mathbb{Z} : ax = 1$$

即ち、

$$(\mathbb{Z}/m\mathbb{Z})^\times = \{a \in \mathbb{Z}/m\mathbb{Z} \,|\, \gcd(a, m) = 1\}$$

有限体 $\mathbb{Z}/p\mathbb{Z}$

特に、法が素数 p のとき、
$a \in \mathbb{Z}/p\mathbb{Z}$ に対し、

$$a \neq 0 \Longrightarrow \exists x \in \mathbb{Z}/p\mathbb{Z} : ax = 1$$

即ち、

$$(\mathbb{Z}/p\mathbb{Z})^{\times} = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$$

このように、
0 以外の元が全て可逆である可換環 $\cdots$ 体 (field)

$\mathbb{Z}/p\mathbb{Z}$: 有限体・p 元体 ($\mathbb{F}_p$ とも書く)

affine 暗号

- **文字種：** m **種類 (**$0, 1, \ldots, m-1$ **に符号化)**
- **鍵：** $a, b \in \mathbb{Z}$ **(**$0, 1, \ldots, m-1$ **のどれか)**
  但し、 $\gcd(a, m) = 1$ **とする**
- **暗号化：** $E(x) \equiv ax + b \pmod{m}$
- **復号：** $D(y) \equiv c(y - b) \pmod{m}$
  (ここに c **は** $ac \equiv 1 \pmod{m}$ **を満たす整数)**

$\longrightarrow$

- **文字集合 (alphabet)：** $\mathbb{Z}/m\mathbb{Z}$
- **鍵：** $(a, b) \in (\mathbb{Z}/m\mathbb{Z})^{\times} \times \mathbb{Z}/m\mathbb{Z}$
- **暗号化：** $E : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}\ ; x \longmapsto ax + b$
- **復号：** $D : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}\ ; y \longmapsto a^{-1}(y - b)$

Fermat の小定理

p : **素数のとき、**

- $\forall a \in \mathbb{Z} : (a, p) = 1 \Longrightarrow a^{p-1} \equiv 1 \pmod{p}$
- $\forall a \in \mathbb{Z} : a^p \equiv a \pmod{p}$

$\longrightarrow$

- $\forall a \in \mathbb{Z}/p\mathbb{Z} : a \neq 0 \Longrightarrow a^{p-1} = 1$
- $\forall a \in \mathbb{Z}/p\mathbb{Z} : a^p = a$

実は、群論の基本的な性質

- G : **有限群、** $\#G = n$ **のとき**

$$\forall a \in G : a^n = 1$$

からも直ちに分かる

原始根の存在

p : **素数に対し、**

- $\forall a \in \mathbb{Z} : (a, p) = 1 \Longrightarrow a^{p-1} \equiv 1 \pmod{p}$
- **逆に** $\mathrm{ord}(g \bmod p) = p - 1$ **のとき、**
  x **が** p **を法とする原始根であるという**
- **このとき、** $g^1 (= g), g^2, \ldots, g^{p-2}, g^{p-1} (\equiv 1)$ **に、**
  0 **を除く全ての剰余類が現れる**
- **原始根が存在する**

$\longrightarrow$

- $\forall a \in (\mathbb{Z}/p\mathbb{Z})^\times : a^{p-1} = 1$
- $\exists g \in (\mathbb{Z}/p\mathbb{Z})^\times : (\mathbb{Z}/p\mathbb{Z})^\times = \langle g \rangle$
- **特に、** $(\mathbb{Z}/p\mathbb{Z})^\times$ **は巡回群**
  実は一般に、体の乗法群の有限部分群は巡回群

中国式剰余定理 (孫子の定理)

$(m, n) = 1$ **のとき、**

- $a \equiv b \pmod{mn}$
$$\iff a \equiv b \pmod{m}, a \equiv b \pmod{n}$$

$\longrightarrow$

$$\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$ **(環同型)**

離散対数問題 (Discrete Logarithm Problem)

p：素数

$g \in \mathbb{Z}$ を 1 つ取って固定
問題：x を与えたとき、

$$g^a \equiv x \pmod{p}$$ を満たす a を見出せ。

$\longrightarrow$
$G = (\mathbb{Z}/p\mathbb{Z})^\times$
$g \in G$ を 1 つ取って固定
問題：$x \in G$ を与えたとき、

$$g^a = x$$ を満たす a を見出せ。

群 $G = (\mathbb{Z}/p\mathbb{Z})^\times$ に於ける離散対数問題

離散対数問題の一般化

以前扱った離散対数問題は、

有限アーベル群 $G = (\mathbb{Z}/p\mathbb{Z})^{\times}$ に於ける

離散対数問題であると言える

実は、有限アーベル群があれば、

離散対数問題が定式化できる

問題：

G：有限アーベル群

$g \in G$ を 1 つ取って固定

このとき、$x \in G$ に対し、

$$g^{a} = x$$

を満たす a を見出せ。

離散対数問題の一般化

任意の有限アーベル群 G に対して、
離散対数問題が考えられるが、

暗号に用いるには、

- 解くのは困難
- 作るのは (冪の計算は) 高速

である必要がある

例： $G = \mathbb{Z}/m\mathbb{Z}$ (加法群) に於ける離散対数問題

$g \in G$ を 1 つ取って固定したとき、
$x \in G$ に対し、$ag = x$ を満たす a を求めること

$\longrightarrow$ 互除法で容易に (高速に) 求まる

離散対数問題の一般化

離散対数問題が

- 解くのは困難
- 作るのは (冪の計算は) 高速

である (暗号に使える) 有限アーベル群の例

- 有限体上の楕円曲線の有理点の群
  (楕円曲線暗号)
- 有限体上の超楕円曲線の Jacobian の有理点の群
  (超楕円曲線暗号)
- 代数体の ideal 類群