

合同式

m : 1 以上の整数を一つ取って固定

m で割った余りのみに注目して計算する

a と b とが m を法として合同
(congruent modulo m)
$$a \equiv b \pmod{m}$$

\Leftrightarrow a と b とを m で割った余りが等しい

$\Leftrightarrow m \mid (a - b)$ ($a - b$ が m で割切れる)

$\Leftrightarrow \exists k \in \mathbb{Z} : a - b = mk$

合同式の基本性質 (同値律)

以下暫く、
法 m を固定して考えて $(\text{mod } m)$ を省略

- $a \equiv a$ (反射律)
- $a \equiv b \implies b \equiv a$ (対称律)
- $a \equiv b, b \equiv c \implies a \equiv c$ (推移律)

合同関係 \equiv は同値関係である (同値律を満たす)

合同式の基本性質 (演算との関係)

- $x \equiv y \implies x \pm c \equiv y \pm c, cx \equiv cy$
- $a \equiv a', b \equiv b'$
 $\implies a \pm b \equiv a' \pm b', ab \equiv a'b'$

加減乗は余りだけを見て計算が出来る

では除法は？

拡張版 Euclid の互除法

2 整数 $a, b \in \mathbb{Z}$ の最大公約数を

$d := \gcd(a, b)$ とするとき、

$$\exists x, y \in \mathbb{Z} : ax + by = d$$

特に、 a, b が互いに素なとき、

$$\exists x, y \in \mathbb{Z} : ax + by = 1$$

$I := \{ax + by \mid x, y \in \mathbb{Z}\}$ とするとき、

$$I = d\mathbb{Z} (= \{dz \mid z \in \mathbb{Z}\})$$

拡張版 Euclid の互除法

証明 1 : 互除法の algorithm

- $a_0 := a, a_1 := b$
- $a_i \neq 0$ であるうちは、

$$a_{i-1} = q_i a_i + a_{i+1}, \quad 0 \leq a_{i+1} < |a_i|$$

で a_{i+1} を定める

- $a_{n+1} = 0$ となったとき、 $d = a_n$

このとき、

$$\{a_{i-1}x + a_i y \mid x, y \in \mathbb{Z}\} = \{a_i x + a_{i+1} y \mid x, y \in \mathbb{Z}\}$$

拡張版 Euclid の互除法

証明 2 : $I = \{ax + by \mid x, y \in \mathbb{Z}\}$ の性質の観察

- $d \mid a, d \mid b$ より $I \subset d\mathbb{Z}$
- $m := \min\{x \in I \mid x > 0\}$ とすると、 $I = m\mathbb{Z}$
- m は a, b の公約数 (前回ここまで)
- d は a, b の最大公約数なので $m \leq d$
- $I = m\mathbb{Z} \subset d\mathbb{Z}$ より $d \mid m$

$$\therefore m = d !!$$

合同式の基本性質 (逆数・除法)

- $c, m \in \mathbb{Z}$ に対し、
 $\exists x \in \mathbb{Z} : cx \equiv 1 \pmod{m} \iff \gcd(c, m) = 1$
- $\gcd(c, m) = 1$ ならば、
 $ca \equiv cb \pmod{m} \implies a \equiv b \pmod{m}$

法 m と互いに素な整数でなら、両辺を割れる

例 : affine 暗号

文字種を m 種類とし、
各文字は $0, 1, \dots, m-1$ に符号化されているとする

鍵 : $a, b \in \mathbb{Z} (0, 1, \dots, m-1 \text{ のどれかとしてよい})$
但し、 a は m と互いに素とする

暗号化 : $E(x) \equiv ax + b \pmod{m}$ (**affine 変換**)

復号 : $D(y) \equiv a^{-1}(y - b) \pmod{m}$

秘密鍵 (共通鍵) 暗号の特徴

暗号化鍵・復号鍵が同じ

- 一般に原理は簡単で高速
- 事前の鍵共有の必要
- 通信相手毎に別の鍵が必要

現代における暗号への要請

現在の情報化社会では

様々な場面で暗号が使われている

例：インターネット取引（ネットショッピングなど）

- 不特定多数の人と暗号通信をしたい
- 事前に鍵を共有できない

→ 共通鍵暗号では実現が困難

→ 公開鍵暗号・鍵共有方式のアイデア

(1976 ~ 77)

公開鍵暗号

暗号化鍵 (公開鍵) ・ 復号鍵 (秘密鍵) が別

- 事前の鍵共有の必要無し
→ 見ず知らずの人からも送ってもらえる
- 認証 ・ 署名機能がある
 - 改竄 ・ なり済ましの対策
 - 否認防止の機能も持つ

公開鍵暗号

但し、一般には、
暗号化・復号が共通鍵暗号に比べて低速

そこで、

- 始めに公開鍵暗号方式で鍵を送付・共有
- その鍵を用いて秘密鍵暗号方式で通信

というように、組合わせて用いることが多い

公開鍵暗号の特徴

- 暗号化は誰でも出来る
- 復号は秘密鍵を知らないと出来ない
(もの凄く時間が掛かる)

そんな都合の良い仕組みが本当にあるのか？

→ ある!! (多分大丈夫)

計算困難な問題 を利用 (素因数分解・離散対数問題)

代表的な公開鍵暗号方式

- **RSA 暗号 (Rivest-Shamir-Adleman)**
- **Diffie-Hellman 鍵共有**
- **ElGamal 暗号**