合同式と mod 演算の基本

1 導入

この講義の核心は、$a \equiv b \pmod{n}$ とは「余りが同じ」の略記ではなく、「$\mathbb{Z}/n\mathbb{Z}$ という代数系の中で同じ元である」という主張であることだ。

余りで計算できる理由は「直感的に正しそう」だからではない。代表元の選び方によらず演算が定義できる（整合性が保証される）という証明によって正当化される。

2 用語と定義

2.1 合同式

Modular congruence

$$a \equiv b \pmod{n} \iff n \mid (a-b)$$

を 合同式 という。

Modular congruence

「**合同**」**の命名**：幾何学の「合同」（形が一致）から類比。n を法（modulus）としてみると位置が同じ、という感覚。英語 congruence（一致・合同）はガウスが著書「数論探究」（1801 年）で導入。

2.2 剰余類

Residue class

$[a]_n = \{a + kn \mid k \in \mathbb{Z}\}$（$a$ と同じ余りを持つ整数の集合）を a の剰余類という。$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$ は n 個の剰余類からなる。

Residue class

3 方針

1. 合同式の定義を余りと結びつける
2. 足し算・掛け算が代表元に依存しないことを証明（演算の整合性）
3. 逆元の存在条件を特定する
4. フェルマーの小定理で冪乗の計算を高速化する

4 厳密な説明

4.1 1. 余りと合同式の等価性

$a = q_1 n + r, b = q_2 n + r$（同じ余り r）のとき $a - b = (q_1 - q_2)n$ なので $n \mid (a-b)$。逆に $n \mid (a-b)$ なら a と b の除の余りは一致する。

4.2 2. 演算の整合性（最重要 証明）

$a \equiv a' \pmod{n}, b \equiv b' \pmod{n}$ のとき：

和：$(a+b)-(a'+b') = (a-a')+(b-b')$ はともに n の倍数の和なので n の倍数。

積：$ab - a'b' = a(b-b') + b'(a-a')$ はともに n の倍数を含むので n の倍数。

したがって代表元を変えても演算結果の剰余類は変わらない—これが「mod 演算が定義できる」ことの証明である。

4.3 3. $\mathbb{Z}/n\mathbb{Z}$ の構造

n の性質	$\mathbb{Z}/n\mathbb{Z}$ の構造	割り算の可否
n が素数 p	体（有限体 $\mathbb{F}_p$）	0 以外で常に可能
$n = p^k$（素数冪）	局所環	p の倍数でなければ可能
n が合成数	環（体でない）	$\gcd(a,n)=1$ のときのみ可能

4.4 4. 逆元の条件

$$ax \equiv 1 \pmod{n} \text{ が[解/かい]を[持/も]つ} \iff \gcd(a,n) = 1$$

ユークリッド互除法で $\gcd(a,n)=1$ のとき $ax+ny=1$ の整数解 (x_0, y_0) が得られ、$x \equiv x_0 \pmod{n}$ が逆元である。

例：$3x \equiv 1 \pmod{7}$。$\gcd(3,7)=1$ なので存在。$3 \times 5 = 15 = 2 \times 7 + 1$ より $x \equiv 5 \pmod{7}$。

4.5 5. フェルマーの小定理

p が素数で $\gcd(a,p)=1$ のとき：

$$a^{p-1} \equiv 1 \pmod{p}$$

証明の概略：$\{a, 2a, 3a, \ldots, (p-1)a\} \pmod{p}$ は $\{1, 2, \ldots, p-1\}$ の順列である（$\gcd(a,p)=1$ のため零が現れない・重複しない）。両辺の積を比較すると

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

$(p-1)!$ と p は互いに素なので両辺を割って $a^{p-1} \equiv 1$。

応用：$2^{100} \pmod{7}$ の計算。$p=7$ なので $2^6 \equiv 1 \pmod{7}$。$100 = 6 \times 16 + 4$ より $2^{100} = (2^6)^{16} \cdot 2^4 \equiv 1^{16} \cdot 16 \equiv 2 \pmod{7}$。

4.6 6. 冪乗の高速計算（反復二乗法）

$a^n \bmod m$ の計算：

1. n を 2 進数展開: $n = \sum_k b_k 2^k$
2. $a^1, a^2, a^4, a^8, \ldots$ を順次 $\bmod m$ で計算
3. $b_k = 1$ の成分を掛け合わせる

フェルマーの小定理で指数を $p-1$ で削減してから反復二乗法を使うと、RSA暗号の基礎演算に到達する。

4.7　7. 連立合同式

法が互いに素な連立合同条件は中国剰余定理（CRT）で一意に解ける。

→ 講義 **中国剰余定理** lecture math number-theory
https://study.bem130.com/lecture/math/number-theory/中国剰余定理-講義/

5　見分け方

- 余りだけが重要な整数問題 → 合同式へ移行
- 割り算が出た → $\gcd(a,n)=1$ の確認が先
- 大きな冪乗 $a^n \bmod p$ → フェルマーの小定理で指数を削減
- 複数の余り条件 → CRT

6　どこまで成り立つか

mod 演算の感覚は多項式・行列にも広がるが、何を同じとみなすかを改めて定義する必要がある。フェルマーの小定理は素数限定であり、一般の n に対するオイラーの定理 $a^{\phi(n)} \equiv 1 \pmod{n}$ $(\gcd(a,n)=1)$ へ拡張される。

7　最終形

$$\boxed{a \equiv b \pmod{n} \iff n \mid (a-b)}$$

$$\boxed{ax \equiv 1 \pmod{n} \text{ が[解/かい]を[持/も]つ} \iff \gcd(a,n)=1}$$

$$\boxed{a^{p-1} \equiv 1 \pmod{p} \quad (\text{フェルマーの[小定理/しょうていり]}, p \text{ は[素数/そすう]}, \gcd(a,p)=1)}$$

8　一言でいうと

mod 演算が正しいのは直感だからでなく剰余類の演算が整合的に定義できるからであり、フェルマーの小定理はその体の構造が生む最強の計算ツール—現代暗号の根幹に至る。

9　関連リンク

→ 講義 **同値関係と剰余類の基本** lecture math abstract-algebra
https://study.bem130.com/lecture/math/abstract-algebra/同値関係と剰余類の基本-講義/

→ 講義 **ユークリッドの互除法と一次不定方程式** lecture math algebra
https://study.bem130.com/lecture/math/algebra/ユークリッドの互除法と一次不定方程式-講義/

→ 講義 **群の基本** lecture math abstract-algebra
https://study.bem130.com/lecture/math/abstract-algebra/群の基本-講義/

→ 講義 **環の基本** lecture math abstract-algebra
https://study.bem130.com/lecture/math/abstract-algebra/環の基本-講義/