中国剰余定理

1 導入

この講義の核心は、**「互いに素な法で与えられた複数の余り条件は、合わせた法のもとで一意の解を持つ」**ことである。

「3 で割ると 2 余り、5 で割ると 3 余る整数は？」という問題を体系的に解く道具が中国剰余定理（CRT）である。中国の古典「孫子算経」（3 〜 5 世紀）に現れたことから命名。

2 用語と定義

2.1 中国剰余定理

Chinese Remainder Theorem

定理：$m_1, m_2, \ldots, m_k$ が互いに素（$\gcd(m_i, m_j) = 1$、$i \neq j$）なとき、連立合同式

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad \ldots, \quad x \equiv a_k \pmod{m_k}$$

は $M = m_1 m_2 \cdots m_k$ を法として一意の解を持つ。

「中国剰余定理」の命名：Chinese Remainder Theorem の訳。余り（remainder）＝剰余。東洋で独立に発見された事実を西洋の数学者が命名した。

定義が実現する性質：M の倍数域（$0 \le x < M$）内にちょうど 1 つの解が存在する。

2.1.1 一意性の直観

法	情報量
$x \bmod m_1$	m_1 通りの可能性を 1 通りに限定
$x \bmod m_2$	さらに m_2 分の 1 に限定
⋮	⋮
全条件	$M = m_1 \cdots m_k$ 通りのうち 1 通りに限定

3 方針

構成的証明（解の構成）：各 i について $M_i = M / m_i$（m_i 以外の積）を作り、M_i の $\bmod m_i$ における逆元 M_i^{-1} を求めて

$$x \equiv \sum_{i=1}^{k} a_i M_i M_i^{-1} \pmod{M}$$

と構成する。逆元の計算にユークリッド互除法を使用する。

4 直感的な説明

「振り子を 3 秒周期と 5 秒周期で同時に鳴らすと 15 秒周期で一致する」。3 と 5 が互いに素なので、$[0, 15)$ のどの余り組み合わせもちょうど 1 回現れる。CRT はこの「余り組み合わせ → 元の数」の逆引を与える。

5 厳密な説明

5.1 1. 存在の構成

各 i に対して $M_i = M/m_i$ と置く。$\gcd(M_i, m_i) = 1$（仮定より）なので、ユークリッド互除法で $M_i^{-1} \bmod m_i$ が存在する。

$$x_0 = \sum_{i=1}^{k} a_i M_i M_i^{-1}$$

確認：$x_0 \bmod m_i$ を計算すると、$j \neq i$ の項はすべて m_i の倍数（$m_i \mid M_j$）なので 0、i 番目の項は $a_i M_i M_i^{-1} \equiv a_i \cdot 1 = a_i \pmod{m_i}$。

5.2 2. 一意性の証明

x_0 と x_1 がともに全条件を満たすとき、$x_0 - x_1 \equiv 0 \pmod{m_i}$ $(\forall i)$。各 m_i が互いに素なので $x_0 - x_1 \equiv 0 \pmod{M}$。

5.3 3. 2 変数の具体的な計算手順

$x \equiv a_1 \pmod{m_1}$、$x \equiv a_2 \pmod{m_2}$（$\gcd(m_1, m_2) = 1$）を解く：

方法 1（代入法）：$x = a_1 + m_1 t$ と置き、$a_1 + m_1 t \equiv a_2 \pmod{m_2}$ から $t \equiv (a_2 - a_1) m_1^{-1} \pmod{m_2}$ を求める。

方法 2（構成公式）：$M = m_1 m_2$、$M_1 = m_2$、$M_2 = m_1$ として上記の公式を適用する。

例：$x \equiv 2 \pmod 3$、$x \equiv 3 \pmod 5$

$M = 15$、$M_1 = 5$、$M_2 = 3$。

$5 \cdot M_1^{-1} \equiv 1 \pmod 3 \Longrightarrow 2M_1^{-1} \equiv 1 \pmod 3 \Longrightarrow M_1^{-1} = 2$

$3 \cdot M_2^{-1} \equiv 1 \pmod 5 \Longrightarrow 3M_2^{-1} \equiv 1 \pmod 5 \Longrightarrow M_2^{-1} = 2$

$x_0 = 2 \cdot 5 \cdot 2 + 3 \cdot 3 \cdot 2 = 20 + 18 = 38 \equiv 8 \pmod{15}$

確認：$8 = 2 \cdot 3 + 2$（mod 3 で 2）、$8 = 1 \cdot 5 + 3$（mod 5 で 3）。

5.4 4. 3 変数の例

$x \equiv 1 \pmod 3$、$x \equiv 2 \pmod 4$、$x \equiv 3 \pmod 5$（$\gcd(3,4) = \gcd(3,5) = \gcd(4,5) = 1$）。

$M = 60$、$M_1 = 20$、$M_2 = 15$、$M_3 = 12$。

$M_1^{-1} \equiv 20^{-1} \equiv 2^{-1} \equiv 2 \pmod 3$

$M_2^{-1} \equiv 15^{-1} \equiv 3^{-1} \equiv 3 \pmod 4$（$3 \cdot 3 = 9 \equiv 1$）

$M_3^{-1} \equiv 12^{-1} \equiv 2^{-1} \equiv 3 \pmod 5$（$2 \cdot 3 = 6 \equiv 1$）

$x_0 = 1 \cdot 20 \cdot 2 + 2 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 = 40 + 90 + 108 = 238 \equiv 58 \pmod{60}$

5.5 5. CRT の代数的意味

$\gcd(m_i, m_j) = 1$（$i \neq j$）のとき環の同型

$$\mathbb{Z}/M\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$$

が成立する。これが CRT の代数的な本質であり、M の剰余類の情報が各法の余りの組み合わせに一対一で対応することを意味する。

6 応用：調日算

「月曜日から何日後かを求める」などの曜日計算は $\bmod 7$ の計算である。複数の周期が絡む場合に CRT が使用できる。詳細は調日算の講義で扱う。

→ 講義 **調日算** lecture math number-theory
https://study.bem130.com/lecture/math/number-theory/調日算-講義/

7 見分け方

- 余り条件が複数あり、法が互いに素 → CRT で一意に解ける
- 法が互いに素でない場合 → まず互いに素な部分に分解するか、一般化 CRT を使用する
- M の剰余環の計算 → CRT で小さな法に分解して並列計算する

8 どこまで成り立つか

法が互いに素でない場合は解の存在条件が変わる（$a_1 \equiv a_2 \pmod{\gcd(m_1, m_2)}$ が必要）。存在する場合の一意性は $\operatorname{lcm}(m_1, m_2)$ を法とした意味に弱まる。

9 最終形

$$\boxed{x \equiv \sum_{i=1}^{k} a_i M_i M_i^{-1} \pmod M, \quad M_i = \frac{M}{m_i}, \quad M_i M_i^{-1} \equiv 1 \pmod{m_i}}$$

10 一言でいうと

互いに素な法の余り条件は独立な情報を与え、積の法のもとで一意の解が構成できる—中国の古典から現代の暗号理論まで貫く定理。

11 関連リンク

→ 講義 **合同式と mod 演算の基本** lecture math abstract-algebra
https://study.bem130.com/lecture/math/abstract-algebra/合同式と mod 演算の基本-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 **調日算** lecture math number-theory
https://study.bem130.com/lecture/math/number-theory/調日算-講義/