ユークリッドの互除法と一次不定方程式

1 導入

この講義の核心は、**最大公約数は余りへ落としても変わらず、その事実を逆向きにたどると $ax+by=d$ の形の方程式が解ける**ことである。
互除法を「gcd を求める手順」としてだけ覚えると浅い。本質は、整数の割り算の構造と一次不定方程式の可解条件を結ぶ中心的な道具である。

2 用語と定義

2.1 最大公約数
Greatest common divisor

$\gcd(a,b)$ とは、a と b の共通約数のうち最大のものである。$\gcd(a,b)=d$ は「a と b を公平に割り切れる最大の単位」を意味する。

2.2 一次不定方程式
Linear Diophantine equation

$$ax+by=c$$

のように、係数が整数で整数解を求める方程式を一次不定方程式という。
Linear Diophantine equation
「不定」の命名：解が一意でなく（不定＝定まらない）、無数に存在し得ることから命名。Diophantine（ディオファントス）はこの種類の方程式を研究した 3 世紀のギリシャ数学者の名に由来。

2.3 ユークリッドの互除法

「互」の命名：互いに除り合う操作の繰り返しから命名。英語 Euclidean algorithm（ユークリッドの算法）は古代ギリシャの数学者ユークリッドが著書「原論」（紀元前 3 世紀）に記したことから命名。

3 方針

$\gcd(a,b)=\gcd(b,r)$（$a=bq+r$）を繰り返し、余りが 0 になった直前の値が gcd である。そのあと逆向きに代入（**拡張互除法**）して $\gcd(a,b)=ax+by$ の形に表現する。

4 厳密な説明

4.1 1. なぜ余りへ落としてよいか

$a = bq + r$ のとき、a と b の共通約数 d は $r = a - bq$ も割るので d は b と r の共通約数でもある。逆も同様に成立するので

$$\gcd(a, b) = \gcd(b, r)$$

余りへ落としても共通約数の集合が変わらない—これが互除法の核心である。

4.2 2. ユークリッドの互除法（例：$\gcd(84, 30)$）

ステップ	割り算	余り
1	$84 = 30 \times 2 + 24$	$r = 24$
2	$30 = 24 \times 1 + 6$	$r = 6$
3	$24 = 6 \times 4 + 0$	$r = 0 \rightarrow$ 終了

$\gcd(84, 30) = 6$。

4.3 3. 拡張互除法：gcd を $ax + by$ の形へ

ステップ 2 から逆向きに代入する：

$$6 = 30 - 24 \times 1$$

ステップ 1 より $24 = 84 - 30 \times 2$ を代入：

$$6 = 30 - (84 - 30 \times 2) = 3 \times 30 - 84 = (-1) \times 84 + 3 \times 30$$

したがって $x = -1, y = 3$ が一つの解である。

4.4 4. 一次不定方程式の可解条件

$ax + by = c$ が整数解を持つための必要十分条件：

$$\gcd(a, b) \mid c$$

証明（必要条件）：$d = \gcd(a, b)$ とすると $a = da', b = db'$ なので $ax + by = d(a'x + b'y)$ は必ず d の倍数。
証明（十分条件）：$c = dk$ かつ $d = ax_0 + by_0$ なら $c = a(kx_0) + b(ky_0)$。
一般解：一つの解 (x_0, y_0) があれば全解は

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t \qquad (t \in \mathbb{Z})$$

4.5 5. mod 逆元との関係

$ax \equiv 1 \pmod{n}$ が解けることと $\gcd(a, n) = 1$ は同値である。これは $ax + ny = 1$（一次不定方程式）が解けることと同値だからである。互除法は mod 逆元の計算（中国剰余定理の中核）を支える。

5 複数の解法

方法 1（素因数分解）：a, b が小さければ素因数分解で gcd を直接計算できる。ただし大きな数では非効率。
方法 2（互除法）：一般的手法。$O(\log \min(a,b))$ ステップで 終了 する。
方法 3（行列 表現）：拡張互除法の係数を 2×2 行列の積として管理する方法。実装で頻用される。

6 見分け方

- gcd を求めたい → 余りへ落とせるかを確認
- $ax + by = c$ の形が出た → まず $\gcd(a,b) \mid c$ を確認
- mod 演算で割り算したい（逆元）→ 互除法で逆元の存在と値を計算

7 どこまで成り立つか

2 変数の一次不定方程式の範囲である。より多変数・高次では異なる手法が必要になる。また多項式の gcd（多項式環上の互除法）へ拡張できる。

8 最終形

$$\boxed{\gcd(a,b) = \gcd(b,r) \quad (a = bq + r)}$$

$$\boxed{ax + by = c \text{ が[整数解/せいすうかい]を[持/も]つ} \iff \gcd(a,b) \mid c}$$

$$\boxed{x = x_0 + \tfrac{b}{d}t, \quad y = y_0 - \tfrac{a}{d}t \quad (t \in \mathbb{Z})}$$

9 一言でいうと

互除法は gcd を求めるだけでなく、mod 逆元・一次不定方程式・中国剰余定理を支える中心的な道具である。

10 関連リンク

→ 講義 **整数の性質の基本** lecture math algebra
https://study.bem130.com/lecture/math/algebra/整数の性質の基本-講義/

→ 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 **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/

→ 講義 **連分数展開** lecture math number-theory
https://study.bem130.com/lecture/math/number-theory/連分数展開-講義/