整数の性質の基本

1 導入

この講義の核心は、**整数の問題では値そのものより「割ったときにどうなるか」を見ること**である。
連続量でなく飛び飛びの値しか取らない整数には、近似でなく「割り切れるか・余りがいくつか」という離散的な情報が本質として効く。

2 用語と定義

2.1 約数 Divisor

$b \mid a$（b は a を割り切る）とは、$a = bq$（q は整数）が成立することである。このとき b を a の約数という。
「約」の命名：約は「切り詰める・縮める」意味。a を縮める因子であることから命名。英語 divisor は「割るもの」の意。

2.2 倍数 Multiple

a が b の倍数とは、$b \mid a$ が成立することである。
「倍」の命名：倍は「2 倍・3 倍」の倍。整数倍になっている数の全体の集合を指す。英語 multiple は「複数の」の意。

2.3 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。

2.4 互いに素 Coprime

$\gcd(a, b) = 1$ のとき、a と b は互いに素であるという。
「素」の命名：共通因子が「素（1）」しかない、という意。英語 coprime（co = 共に、prime = 素）。

2.5 素数 Prime number

2 以上の整数で、1 と自分自身しか正の約数を持たない数を **素数** という。
「素」の命名：因数分解の最小単位であることから命名。英語 prime（原初の）。

3 約数と倍数の対比

	約数 Divisor	倍数 Multiple
定義	$b \mid a$ を満たす b	$b \mid a$ を満たす a

視点	a を小さく見る	b を大きく見る
個数	有限（a 以下）	無限
例（$a=12$）	1, 2, 3, 4, 6, 12	12, 24, 36, …

4 方針

整数問題では、まず「何で割ると整理しやすいか」を決め、余り・最大公約数・素因数分解のどれで攻めるかを判断する。

5 厳密な説明

5.1 1. 余りで見る（偶奇）

整数 n を 2 で割ると余りは 0 か 1 である：

$$n = 2k \quad \text{または} \quad n = 2k+1$$

これが偶数と奇数の基本形である。n^2 が偶数なら n も偶数、n^2 が奇数なら n も奇数—これは対偶として頻出。

5.2 2. 倍数判定の整理

整数	条件	理由
2 の倍数	末尾の桁が偶数	$10^k \equiv 0 \pmod 2$
3 の倍数	各桁の和が 3 の倍数	$10 \equiv 1 \pmod 3$
9 の倍数	各桁の和が 9 の倍数	$10 \equiv 1 \pmod 9$
5 の倍数	末尾が 0 か 5	$10^k \equiv 0 \pmod 5$
11 の倍数	桁の交互和が 11 の倍数	$10 \equiv -1 \pmod{11}$

5.3 3. 最大公約数と最小公倍数

$$\gcd(a,b)\cdot\operatorname{lcm}(a,b) = ab \qquad (a,b>0)$$

これは素因数分解の指数を min（gcd）と max（lcm）で処理することから直接 導かれる。

5.4 4. 素因数分解の一意性（算術の基本定理）

2 以上の任意の整数は、素数の積として本質的に一意に分解できる：

$$n = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k} \qquad (p_1<p_2<\cdots<p_k \text{ が[素数/そすう]})$$

一意性の保証がなければ「因数分解する」という操作は意味を失う。

5.5 5. 互いに素の性質

$\gcd(a,b)=1$ のとき：

- $a \mid bc \Longrightarrow a \mid c$（互いに素な性質のみを使う）
- $ax + by = 1$（一次不定方程式の解が存在）
- $ab \mid c$ かつ $a \mid c$ かつ $b \mid c$ のとき相互に利用できる

5.6 6. 合同式へ

$a - b$ が n の倍数なら、a と b は n で割った余りが同じである。この「余りが同じ」という同値関係から

$$a \equiv b \pmod{n}$$

という記法が生まれ、整数を余りごとの 塊 （剰余類）として代数的に扱える。

6 見分け方

- 偶奇が絡む → $2k,\ 2k+1$ を試みる
- 割り切れるかが主題 → 余りか約数で整理
- 互いに素・公約数が出る → gcd を考え余りへ落とす
- 余りだけが重要 → 合同式へ移行

7 どこまで成り立つか

素因数分解の一意性は自然数（および整数）の世界での事実であり、ガウス整数（$a+bi$）のような拡張では一意性が保たれるか別途確認が必要になる。

8 最終形

$$\boxed{n = 2k \quad \text{または} \quad n = 2k+1}$$

$$\boxed{\gcd(a,b) \cdot \operatorname{lcm}(a,b) = ab}$$

$$\boxed{n = p_1^{e_1} \cdots p_k^{e_k} \text{（[一意/いちい][分解/ぶんかい]）}}$$

9 一言でいうと

整数では「何で割ると整理しやすいか」を最初に決めることが鍵—余り・最大公約数・素因数分解の三つの視点が全ての基盤となる。

10 関連リンク

→ 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 **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 **整数論ポータル** lecture math number-theory
https://study.bem130.com/lecture/math/number-theory/整数論ポータル-講義/