【初等整数論】

とりあえず、「整数＝縛りのきつい数」と考えて，整数ゆえの条件の絞り方を身につけよう．

☆整数の基本的性質

・約数と倍数

約数（devisor） もしくは 因数（factor）

倍数（multiple）

$a, b, k \in \mathbb{Z}$ のとき

$a = kb$と書けるなら

bはaの　　である．

aはbの　　である．

※約数や倍数における負の数や 0 の扱い

ある整数の約数……　　－　　0　　＋

ある整数の倍数……　　－　　0　　＋

0　の約数……

0　の倍数……

・素数 p の定義

i）　p

ii）　p

iii）　約数は

※ 1 は素数か否か？
例）素因数分解の一意性について検討すればわかる．

☆約数の個数と総和

ある自然数 n が，素数$p, q, r, \cdots$と自然数$a, b, c, \cdots$を用いて

$n = p^a q^b r^c \cdots$と素因数分解されるとする．$(p < q < r < \cdots)$

このとき

n の約数の個数は

総和は

☆公約数と公倍数

ある複数の整数の共通の約数：公約数(common devisor, common factor)

ある複数の整数の共通の倍数：公倍数(common multiple)

※最大公約数(greatest common devisor(measure, factor))：G.C.D.　G.C.M.
　最小公倍数(least common multiple)：L.C.M.

・２数の G.C.D.と L.C.M.

ある整数a, bについて，

$gcd(a, b) \cdot lcm(a, b) = ab$

☆互いに素とは

「互いに素数」という意味ではない.

ある複数の整数の G.C.D.が１であるとき，これらの数は互いに素であるという.

例）８　と　１５　は互いに素？
　　６　と　　９　は互いに素？
　　５と１０と１８は互いに素？

☆ユークリッドの互除法

２つの自然数（または整式）の G.C.D.を求める手法……史上最古のアルゴリズム

「イメージ」

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

例題１）gcd (3007,1649)を求めよ.

例題２）

$111 = 4 \times 26 + 7$

$26 = 3 \times 7 + 5$

$7 = 1 \times 5 + 2$

$5 = 2 \times 2 + 1$

上の計算表を参考にして，以下の問いに答えよ．

(1)$26x + 111y = 1$ となる整数x, yの組を 1 組求めよ．

(2)$26x$を 111 で割ったときに余りが 3 となるような自然数xを 1 つ求めよ．

☆剰余による分類

aをbで割ったとき、商がqで余りがr

$(a, b, q, r \in Z, \quad b \geq 2, \quad 0 \leq r \leq b-1)$

$$a = qb + r$$

例）11 を 4 でわると

-14 を 5 でわると

※合同式

剰余による分類を簡潔に記述する.

$a \equiv b(mod\ n)$

$a \equiv b\ mod\ n$

$a \equiv_n b$

「２つの整数a, bはnを法(modulus)として合同である」

というのは 「$a-b$ は n で割り切れる」という意味で,

要するに 「a と b は 等しい」ということ.

合同式の性質

$a \equiv b, \quad c \equiv d(mod\ n)$のとき

i) $a \pm c \equiv b \pm d$

ii) $ac \equiv bd$

iii) $a^m \equiv b^m \quad (m \in \mathbb{N})$

例）$m \equiv 4\ (mod\ 5)$のとき，m^2について考える.

※本来$(mod\ n)$は全ての ≡ について毎回書かねばならないが，実際は面倒なので省略することが多い．入試における答案では,

$a \equiv b\ \left(\text{以下全て} mod\ n\right)$

などと書いておけば、以後の$(mod\ n)$の表記は略せる.

☆n 進法

n 進法で$abcd =$

10 進法で$abcd =$

2 進法で$1011 =$

例）10 進法における 2014 を 2 進法に直せ.

☆「全ての～で成り立つ」

…「必要性で押して十分性を確認」

☆ディオファントス方程式

係数が整数の不定方程式をディオファントス方程式という.

※不定方程式とは，未知数よりも変数の方が多い（解が定まらない）方程式のことをいう.

・2 変数の一次ディオファントス方程式

i)直線タイプ　→　格子点のイメージで解く（互除法利用）

$ax + by + c = 0$

・2 変数の二次ディオファントス方程式

ii)楕円タイプ　→　どちらかの文字について解く…$x = \alpha \pm \sqrt{\beta}$（$\beta \geq 0$ で範囲が絞れる）

$ax^2 + bxy + cy^2 + dx + ey + f = 0$

iii)それ以外（判別式で絞れない）　→　因数分解モドキでシラミツブシ

$axy + bx + cy + d = 0$

$ax^2 + bxy + cy^2 + dx + ey + f = 0$

iv)他にも「平方完成で絞る」など解法はいろいろあるので，興味があれば研究してみよう.

☆不等式で挟む（範囲で絞る）

例）$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1\ (x \leq y \leq z)$をみたす自然数$x, y, z$の組をすべて求めよ.

おまけ

・オイラーの関数（トーシェント関数，ϕ関数）

ある自然数nについて，n以下でnと互いに素な数の個数を$\phi(n)$とすると

$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots$（ただし、$p_1, p_2 \cdots$は$n$の素因数とする）

・ルジャンドルの定理（のうちのひとつ）

ある素数pと自然数m, nについて$p^m \leq n < p^{m+1}$が成り立つとき

$n!$に含まれるpの個数を$f(n,p)$とすると　$f(n,p) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^m}\right]$

例　1）100! は 2 で何回割れるか.

　　2）$(p^n)!$はpで何回割れるか．ただし，pは素数，nは自然数とする.

・中国剰余定理

二元 Ver.

与えられた 2 整数 m，n が互いに素ならば，任意に与えられる整数 a，b に対し，連立合同方程式

$\begin{cases} x \equiv a \,(mod\, m) \\ x \equiv b \,(mod\, n) \end{cases}$ を満たす整数 x が，mn を法として一意的に存在する．

一般化拡張 Ver.

与えられた k 個の整数 m_1，m_2，…，m_k がどの二つも互いに素ならば，

任意に与えられる整数 a_i $\left(i = 1,\ 2,\ \cdots,\ k \right)$ に対し，k本の連立合同方程式

$x \equiv a_i \,(mod\, m_i)$ を満たす整数 x が $m_1 m_2 \cdots m_k$ を法として一意的に存在する．

例題　x を 3 で割って 1 余り、5 で割って 2 余り、7 で割って 3 余る数とする。
　　このとき，xを $105 = 3 \cdot 5 \cdot 7$ で割った余りを求めよ．