初等数论

整除，同余和不定方程

LeyuDame

2024 年 11 月 15 日

整除的概念与基本性质

对任给的两个整数 $a, b(a \neq 0)$, 如果存在整数 q, 使得 $b = aq$, 那么称 b 能被 a 整除 (或称 a 能整除 b), 记作 $a \mid b$. 否则, 称 b 不能被 a 整除, 记作 $a \nmid b$.
如果 $a \mid b$, 那么称 a 为 b 的因数, b 为 a 的倍数.

整除的概念与基本性质

性质 1.1

如果 $a \mid b$, 那么 $a \mid (-b)$ ，反过来也成立; 进一步, 如果 $a \mid b$, 那么 $(-a) \mid b$ ，反过来也成立.

性质 1.2

如果 $a|b, b|c$, 那么 $a \mid c$. (传递性)

性质 1.3

若 $a|b, a|c$, 则对任意整数 x, y, 都有 $a \mid bx + cy$. (即 a 能整除 b, c 的任意一个“线性组合”)

例 1

若 $a|n, b|n$, 且存在整数 x, y, 使得 $ax + by = 1$, 证明: $ab \mid n$.

例 2

证明：无论在数 12008 的两个 0 之间添加多少个 3 ，所得的数都是 19 的倍数.

例 3

已知一个 1000 位正整数的任意连续 10 个数码形成的 10 位数是 2^{10} 的倍数. 证明：该正整数为 2^{1000} 的倍数.

例 4

设 m 是一个大于 2 的正整数，证明：对任意正整数 n ，都有 $2^m - 1 \nmid 2^n + 1$.

素数与合数

性质 1.4

设 n 为大于 1 的正整数, p 是 n 的大于 1 的因数中最小的正整数, 则 p 为素数.

性质 1.5

如果对任意 1 到 $\sqrt{n}$ 之间的素数 p, 都有 $p \nmid n$, 那么 n 为素数. 这里 $n(>1)$ 为正整数.

证明.

事实上, 若 n 为合数, 则可写 $n = pq, 2 \leqslant p \leqslant q$. 因此 $p^2 \leqslant n$, 即 $p \leqslant \sqrt{n}$.
这表明 p 的素因子 $\leqslant \sqrt{n}$, 且它是 n 的因数, 与条件矛盾. 因此 n 为素数. □

素数与合数

性质 1.6

素数有无穷多个.

证明.

若只有有限个素数, 设它们是 $p_1 < p_2 < \cdots < p_n$. 考虑数

$$x = p_1 p_2 \cdots p_n + 1$$

其最小的大于 1 的因数 p, 它是一个素数, 因此, p 应为 $p_1, p_2, \cdots, p_n$ 中的某个数. 设 $p = p_i, 1 \leqslant i \leqslant n$, 并且 $x = p_i y$, 则 $p_1 p_2 \cdots p_n + 1 = p_i y$, 即

$$p_i(y - p_1 p_2 \cdots p_{i-1} p_{i+1} \cdots p_n) = 1.$$

这导致 $p_i \mid 1$. 矛盾.
所以, 素数有无穷多个. $\square$

例 5

设 n 为大于 1 的正整数. 证明: 数 n^5+n^4+1 不是素数.

例 6

考察下面的数列:

$$101, 10101, 1010101, \cdots$$

问: 该数列中有多少个素数?

例 7

求所有的正整数 n, 使得 $\frac{n(n+1)}{2}-1$ 是一个素数.

例 8

对任意正整数 n，证明：存在连续 n 个正整数，它们都是合数.

例 9

设 n 为大于 2 的正整数. 证明: 存在一个素数 p , 满足 $n < p < n!$.

例 10

设 a, b, c, d, e, f 都是正整数, $S = a + b + c + d + e + f$ 是 $abc + def$ 和 $ab + bc + ca - de - ef - ed$ 的因数. 证明: S 为合数.

最大公因数与最小公倍数

带余数除法

设 a, b 是两个整数, $a \neq 0$, 则存在唯一的一对整数 q 和 r, 满足

$$b = aq + r, 0 \leqslant r < |b|$$

其中 q 称为 b 除以 a 所得的商, r 称为 b 除以 a 所得的余数.

性质 1.7 (贝祖 (Bezout) 定理)

设 $d=(a,b)$ ，则存在整数 x,y ，使得

$$ax+by=d$$

性质 1.8

设 d 为 a,b 的公因数, 则 $d\mid(a,b)$.

性质 1.9

设 a,b 是不全为零的整数, 则 a 与 b 互素的充要条件是存在整数 x,y 满足

$$ax+by=1$$

性质 1.10

设 $a|c, b|c$ ，且 $(a,b)=1$ ，则 $ab \mid c$.

性质 1.11

设 $a \mid bc$ ，且 $(a,b)=1$ ，则 $a \mid c$.

性质 1.12

设 p 为素数, $p \mid ab$ ，则 $p \mid a$ 或 $p \mid b$.

公倍数

设 a, b 都是不等于零的整数，如果整数 c 满足 $a \mid c$ 且 $b \mid c$，那么称 c 为 a, b 的公倍数.
在 a, b 的所有正的公倍数中，最小的那个称为 a, b 的最小公倍数，记作 $[a, b]$.

性质 1.13

设 a, b 为非零整数, d, c 分别是 a, b 的一个公因数与公倍数, 则 $d|(a, b), [a, b]|c$.

性质 1.14

设 a, b 都是正整数, 则 $[a, b] = \frac{ab}{(a,b)}$.

性质 1.15

$(a_1, a_2, a_3, \cdots, a_n) = ((a_1, a_2), a_3, \cdots, a_n)$;
而 $[a_1, a_2, a_3, \cdots, a_n] = [[a_1, a_2], a_3, \cdots, a_n]$.

性质 1.16

存在整数 $x_1, x_2, \cdots, x_n$，使得

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = (a_1, a_2, \cdots, a_n)$$

性质 1.17

设 m 为正整数, 则

$$(ma_1, ma_2, \cdots, ma_n) = m(a_1, a_2, \cdots, a_n), \tag{1}$$

$$[ma_1, ma_2, \cdots, ma_n] = m[a_1, a_2, \cdots, a_n]. \tag{2}$$

例 11

设 a, b 为正整数, 且 $\frac{ab}{a+b}$ 也是正整数. 证明: $(a, b) > 1$.

例 12

设正整数 a, b, c 满足 $b^2 = ac$. 证明: $(a, b)^2 = a(a, c)$.

例 13

求所有的正整数 $a, b(a \leqslant b)$，使得

$$ab = 300 + 7[a, b] + 5(a, b). \tag{3}$$

例 14

求所有的正整数 a, b, 使得

$$(a, b) + 9[a, b] + 9(a + b) = 7ab. \tag{4}$$

例 15

Fibonacci 数列定义如下：$F_1 = F_2 = 1, F_{n+2} = F_{n+1} + F_n, n = 1, 2, \cdots$. 证明：对任意正整数 m, n，都有 $(F_m, F_n) = F_{(m,n)}$.

例 16

设 n 为大于 1 的正整数. 证明: 存在从小到大排列后成等差数列 (即从第二项起, 每一项与它前面那项的差为常数的数列) 的 n 个正整数, 它们中任意两项互素.

算术基本定理

定理 1 (算术基本定理)

设 n 是大于 1 的正整数, 则 n 可以分解成若干个素数的乘积的形式, 并且在不考虑这些素数相乘时的前后次序时, 这种分解是唯一的. 即对任意大于 1 的正整数 n, 都存在唯一的一种素因数分解形式:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

这里 $p_1 < p_2 < \cdots < p_k$ 为素数, $\alpha_1, \alpha_2, \cdots, \alpha_k$ 为正整数.

推论 2

设 n 的所有正因数 (包括 1 和 n) 的个数为 $d(n)$, 那么

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_k + 1)$$

推论 3

设 n 的所有正因数之和为 $\sigma(n)$, 那么

$$\sigma(n) = (1 + p_1 + \cdots + p_1^{\alpha_1})(1 + p_2 + \cdots + p_2^{\alpha_2})\cdots\left(1 + p_k + \cdots + p_k^{\alpha_k}\right)$$

推论 4

设 n, m 的素因数分解分别为

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},$$

这里 $p_1 < p_2 < \cdots < p_k$，都为素数, α_i, β_i 都是非负整数, 并且对每个 $1 \leqslant i \leqslant k, \alpha_i$ 与 β_i 不全为零, 那么, 我们有 $(m, n) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$；$[m, n] = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}$，其中 $\gamma_i = \min\{\alpha_i, \beta_i\}, \delta_i = \max\{\alpha_i, \beta_i\}, 1 \leqslant i \leqslant k$.

例 17

在一个走廊上依次排列着编号为 $1,2,\cdots,2012$ 的灯共 2012 盏, 最初每盏灯的状态都是开着的. 一个好动的学生做了下面的 2012 次操作: 对 $1\leqslant k\leqslant 2012$, 该学生第 k 次操作时, 将所有编号是 k 的倍数的灯的开关都拉了一下. 问: 最后还有多少盏灯是开着的?(提示: $44^2=1936, 45^2=2025$)

例 18

求所有的正整数 n, 使得 $n = d(n)^2$.

例 19

设 n 为正整数. 证明: 数 $2^{2^n}+2^{2^{n-1}}+1$ 至少有 n 个不同的素因子.

例 20

设 m, n 是正整数, 且 m 的所有正因数之积等于 n 的所有正因数之积. 问: m 与 n 是否必须相等?

例 21

求所有的正整数 x, y, 使得

$$y^x = x^{50}$$

例 22

给定正整数 $n>1$，设 $d_1, d_2, \cdots, d_n$ 都是正整数，满足：$(d_1, d_2, \cdots, d_n)=1$，且对 $j=1,2,\cdots,n$ 都有 $d_j \mid \sum_{i=1}^n d_i$（这里 $\sum_{i=1}^n d_i = d_1+d_2+\cdots+d_n$）.

(1) 证明：$d_1 d_2 \cdots d_n \mid \left(\sum_{i=1}^n d_i\right)^{n-2}$；

(2) 举例说明：$n>2$ 时，上式右边的幂次不能减小.