初等数论

整除, 同余和不定方程

LeyuDame

2024 年 10 月 30 日

定义

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.

性质

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

如果 $a|b, b|c$, 那么 $a \mid c$. 这表明整除具有传递性.

性质

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

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

证明.

由条件，可设 $n = au, n = bv, u, v$ 为整数. 于是

$$
\begin{aligned}
n &= n(ax + by) && (1)\\
&= nax + nby && (2)\\
&= abvx + abuy && (3)\\
&= ab(vx + uy) && (4)
\end{aligned}
$$

因此

$$ab \mid n$$

$\square$