初等数论笔记

CHUDENGSHULUNBIJI

rogeryoungh

2021 年 2 月 7 日 · LaTeX

目录

第 1 章 整数的整除性

定义 1.1

对于整数 a,b，其中 $a \neq 0$，若存在整数 c，它使得

$$b = ac$$

则 b 叫做 a 的倍数，a 叫做 b 的因数，记作 $a \mid b$。

有时也称作 a 能整除 b，或 b 能被 a 整除，或 a 能除尽 b，或 b 能被 a 除尽。

若 a 不能整除 b，我们就记作 $a \nmid b$。

引理 1.1

如果对于整数 a,b 满足 $a \mid b$，则有

$$(-a) \mid b, \quad a \mid (-b), \quad (-a) \mid (-b), \quad |a| \mid |b|$$

这个比较显然，由定义知存在 c 使得 $b = ac$，再构造验证即可。

引理 1.2

对于整数 a,b,c 有 $a \mid b, b \mid c$，则有 $a \mid c$。

证明 因为 $a \mid b, b \mid c$，故存在整数 d,e 使得 $b = ad, c = be$。

因此存在整数 $f = de$ 使得 $c = af = ade$，故 $a \mid c$。 □

引理 1.3

对于整数 a,b 有 $|a| \mid |b|$，若 $|a| < |b|$ 则有 $a = 0$。

证明 因为 $|a| \mid |b|$，则存在整数 c 使得 $|a| = |b|c$。那么有

$$0 \leqslant |a| = |b|c < |b|$$

即 $0 \leqslant c < 1$，又 c 为整数，故 $c = a = 0$。 □

定理 1.1

对于整数 a,b，若 $b \neq 0$ 则一定存在唯一一对 q,r 使得

$$a = bq + r, \quad 0 \leqslant r < |b|$$

证明 先证明存在性。

（1）若恰 $b \mid a$，则必存在 c 使得 $a = bc$，此时有 $q = c, r = 0$。

（2）否则一定存在 n 使得 $n|b| < a < (n+1)|b|$，即存在 $0 < r < |b|$ 使得 $a = |b|n + r$。

当 $b > 0$ 时，令 $q = n$；当 $b < 0$ 时，令 $q = -n$ 则有

$$a = bq + r, \quad 0 \leqslant r < |b|$$

再证明唯一性。设

$$a = bq_1 + r_1 = bq_2 + r_2, \quad 0 \leqslant r_1, r_2 < |b|$$

相减有

$$a - a = b(q_1 - q_2) + r_1 - r_2 = 0$$

即 $r_1 - r_2 = -b(q_1 - q_2)$，因此有 $b \mid (r_1 - r_2)$ □