初等数论笔记

rogeryoungh

2021 年 5 月 11 日

目录

第一章　初等数论

注意我们的理论基础是整数，尽量通过分类讨论的方式得到结论。而且也要把握脉络，抓住重点，不要迷失于无谓的细节中。

自然数 $\mathbb{N}$ 、正整数 $\mathbb{N}^+$ 和整数 $\mathbb{N}$ 我们是熟知的。

1.1　整数公理

整数的公理

我们熟知一些整数的代数算律

结合律：$(a+b)+c=(a+b)+c$。

交换律：$a+b=b+a$。

消去律：

定义 1.1.1　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 1.1.2　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 1.1.3　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 1.1.4　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 1.1.5　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。设存在两对 q_1, r_1 和 q_2, r_2 使得

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

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 $b \mid (r_1 - r_2)$。而 $|r_1 - r_2| < |b|$，又引理知有 $|r_1 - r_2| = 0$。故

$$r_1 = r_2, q_1 = r_2$$

即两对相同。 $\square$

定义 1.1.6 【素数】 若一个大于 1 的正整数，只能被 1 和它本身整除，不能被其他正整数整除，这样的数叫做素数。

若能被其他正整数整除，则称为合数。因此一个正整数必然是素数、合数或 1。