数论选讲

丁尧尧

February 7, 2017

Contents

本文梳理了一下信息学竞赛中常用的数论知识, 目的在于让大家快速理解入门,
有些地方如果自然思维能很快感觉到其正确性, 就没有深究其细节.

1 基础内容

以下内容, 如果不特别说明, 都是在整数范围内讨论.

1.1 整除

定理 1. 如果对于数 $a, b(b \neq 0)$, 存在数 q, 使得 $a = bq$, 那么我们称 b **整除**a, 记作 $b \mid a$, 称 q 是 b 除 a 的**商**. 如果 $b \mid a$ 我们称 b 是 a 的**一个约数**（或**一个因子**）,a 是 b 的**倍数**, 否则记为 $b \nmid a$.

命题 1. 有 a, b, c 三个数:

- 如果 $a \mid b$,$b \mid c$, 那么 $a \mid c$,
- 如果 $a \mid b$,$a \mid c$, 那么 $a \mid bx + cy$, 其中 x, y

1.2 带余除法

定理 2. 对于数 a 和正数 b, 存在唯一的数 q, r 满足

$$a = bq + r \quad (0 \leq r < b)$$

我们称 r 为 b 除 a 的**余数**.

Proof. 先证存在: 通过改变 bq 中 q 的值, 我们可以得到一系列的数:

$$\cdots, -2b, -b, 0, b, 2b, \cdots$$

从而可以得到一系列的区间: $[ib, (i+1)b)$ (i 是整数). 这些区间是整数的一个分割（并集为整数集合, 任意两个的交集为空）, 所以 a 必定属于其中一个, 假设为 $[kb, (k+1)b)$, 则可以将 q 取成 k,r 取成 $a - kb$, 则得到一组 q, r.

下面证唯一: 如果有两组 q, r: q_1, r_1 和 q_2, r_2（不妨假设 $r_2 > r_1$）, 满足:

$$a = bq_1 + r_1 \quad (0 \leq r_1 < b)$$

$$a = bq_2 + r_2 \quad (0 \leq r_1 < b)$$

做减法

$$r_2 - r_1 = b(q_1 - q_2)$$

因为 $0 \leq r_2 - r_1 < b$, 所以 $r_1 = r_2$, 从而 $q_1 = q_2$. □

1.3 质数

定义 1. 如果一个数 p 满足下面的性质:

- $p > 1$
- p 只有两个正因子（*1* 和它自身）

那么我们称 p 为**质数**或**素数**, 一个大于 1 的数, 如果不是质数, 我们就称其为**合数**,1 既不是质数, 也不是合数.

命题 2. 任何一个合数 a 都存在一个因子 q, 使得 $2 \leq q \leq \sqrt{a}$.

Proof. 因为 a 是合数, 所以必然存在一个因子 q, 从而 a/q 也是 a 的一个因子, 并且满足 $2 \leq q, a/q \leq a-1$, 如果 q 和 a/q 都大于 $\sqrt{a}$, 则 $q \times a/q > a$, 矛盾, 所以 q 与 a/q 中至少有一个数小于等于 $\sqrt{a}$. □

命题 3. 质数有无穷个.

Proof. 反证法.

如果素数只有有限个, 那么假设他们是: $p_1, p_2, \ldots, p_s$, 那么考虑数:$q = p_1 p_2 \ldots p_s + 1$, 因为 $p_i \nmid q$, 所以必然存在一个素数, 不在 $p_1, p_2, \ldots, p_s$ 中. 这与我们假设矛盾. □

1.4 算数基本定理

定理 3. 如果 a 是一个大于 1 的数, 那么 a 可以被分解成一些质数的乘积, 如果将质数从小到大排列, 则这种分解方式是唯一的. 即任何大于 1 的数可以被唯一表示成:

$$a = p_1 p_2 p_3 \ldots p_s \quad (p_1 \leq p_2 \leq p_3 \leq \ldots \leq p_s)$$

如果把相同质数合并, 那么可以被表示成:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_s^{\alpha_s} \quad (p_1 < p_2 < p_3 < \ldots < p_s)$$

Proof. 先证明一个大于 1 的数可以被分解成一些质数的乘积:

归纳法: 首先,2, 3 显然可以写成素数的乘积.

对于数假设 2 到 $q-1$ 都可以写成素数的乘积 ($q \geq 4$), 现证明 q 也可以写成素数的乘积:

如果 q 是质数, 那么显然.

如果 q 是合数, 那么 $q = ab$, 其中 $2 \leq a, b \leq q-1$, 根据假设,a, b 可以被分解成质数的乘积, 那么 q 可以被分写成质数的乘积.

现在证唯一:

如果有两种不同分解方法:

$$a = q_1 q_2 q_3 \ldots q_r$$

$$a = p_1 p_2 p_3 \ldots p_s$$

所以:

$$q_1 q_2 q_3 \ldots q_r = p_1 p_2 p_3 \ldots p_s$$

我们去掉两边公共的质数, 从而得到 (两边不会变成 1, 否则就是相同的分解方案):

$$q'_1 q'_2 \ldots q'_{r'} = p'_1 p'_2 \ldots p'_{s'}$$

而这是不可能的, 因为 q'_1 整除左边不整除右边.(这句话也需要证, 这里我们能理解就行) □

1.5 最大公约数

定义 2. 对于两个数 a, b, 如果存在数 d, 满足 $d \mid a, d \mid b$, 那么我们称 d 是 a, b 的**公因数**, 如果 a, b 不同时为 0, 我们称其公因数中最大的称为**最大公因数**, 记作 $gcd(a, b)$

定义 3. 对于两个非 0 数 a, b, 如果存在数 l, 满足 $a \mid l, b \mid l$, 那么我们称 l 是 a, b 的**公倍数**, 并将其正公倍数中最小的称为**最小公倍数**, 记作 $lcm(a, b)$

假设 a, b 都是正的, 那么我们可以这样来理解最大公因数和最小公倍数:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_s^{\alpha_s} \qquad b = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} \dots p_s^{\beta_s}$$
$$gcd(a, b) = p_1^{min(\alpha_1, \beta_1)} p_2^{min(\alpha_2, \beta_2)} p_3^{min(\alpha_3, \beta_3)} \dots p_s^{min(\alpha_s, \beta_s)}$$
$$lcm(a, b) = p_1^{max(\alpha_1, \beta_1)} p_2^{max(\alpha_2, \beta_2)} p_3^{max(\alpha_3, \beta_3)} \dots p_s^{max(\alpha_s, \beta_s)}$$

它们有一些性质:

命题 4.
1. *$gcd(a, b) = gcd(b, a)$*
2. *$gcd(a, b) = gcd(a, b + ax)$, 从而有 $gcd(a, b) = gcd(b, a \ mod \ b)$*

Proof. 第二个性质, 显然 a, b 与 $a, b + ax$ 有相同的公因数集合, 所以其最大公因数相等. □

1.6 同余

1.7 逆元

1.8 快速幂

1.9 中国剩余定理

1.10 剩余系

1.11 欧拉函数

1.12 欧拉定理

1.13 费马小定理

1.14 Wilson 定理

2 进阶内容

2.1 素数测试

2.2 大数质因数分解

2.3 数论函数

a