§1 整除性

1.1. 整除记号.

定义 1.1. 我们称 m 整除 n (或 n 可以被 m 整除)，当且仅当 $m > 0$ ，并且 $\frac{n}{m}$ 是一个整数。可记作 $m\backslash n$. 即

$$m\backslash n \Leftrightarrow (m > 0) \wedge (\exists k \in \mathbb{Z}, n = mk).$$

如果 m 不整除 n ，记作 $m \not\backslash n$ 。

定义 1.2 (最大公约数)**.** 两个整数 m, n 的最大公约数是最大的可以整除 m 和 n 的那个数. 即

$$\gcd(m, n) = \max\{k : k\backslash m \text{ 且} k\backslash n\}.$$

比如 $\gcd(12, 18) = 6$ ，那么可以进行分数进行化简, 即 $\frac{12}{18} = \frac{12/6}{18/6} = \frac{2}{3}$.

注: 若 $n > 0$ ，那么 $\gcd(0, n) = n$ ，因为任何一个整数都整除 0 .

定义 1.3 (最小公倍数)**.** 两个整数 m, n 的最小公倍数是最小的可以被 m, n 整除的那个数. 即

$$\operatorname{lcm}(m, n) = \min\{k > 0; m\backslash k \wedge n\backslash k\}$$

1.2. 求最大公约数的算法. 算法描述: $\gcd(m, n)$ 是

- 若 $m = 0$ 成立, 那么 $\gcd(m, n) = n$.
- 否则, $\gcd(m, n) = \gcd(n \bmod m, m)$.

这个递归式是有效的, 因为从公因式的角度来讲, 任何一个 m 和 n 的公因式都一定是 m 和 $n \bmod m$(即 $n - \lfloor \frac{n}{m} \rfloor m$) 的公因式. 下面只要考虑求出来的这个公因数一定是最大的即可.

可以构造一个方程, 来辅助说明这为什么是对的: 考虑找到 m', n', 满足 $m'm + n'n = \gcd(m, n)$, 其中, m', n' 由下面的内容给出:

- 如果 $m = 0$, 那么置 $m' \leftarrow 0, n' \leftarrow 1$.
- 否则, 置 $r \leftarrow n \bmod m$, 并使用 r, m 代替 m, n(这是在倒着做上面的递归算法). 这时候我们需要知道他们前面的系数是什么. 因此需要找到 r, m 前面的系数, 记作 $\overline{r}, \overline{m}$, 满足 $\overline{r}r + \overline{m}m = \gcd(r, m)$.
  - 由于 $r = n - \lfloor \frac{n}{m} \rfloor m$, 并且 $\gcd(r, m) = \gcd(m, n)$, 代入得

$$\bar{r}\left(n - \left\lfloor \frac{n}{m} \right\rfloor m\right) + \bar{m}m = \gcd(m, n).$$

  - 重写上述项, 收集 m, n 项, 就有了

$$\underbrace{\left(\bar{m} - \left\lfloor \frac{n}{m} \right\rfloor \bar{r}\right)}_{m'} m + \underbrace{\bar{r}}_{n'} n = \gcd(m, n).$$

  - 因此我们可以将 $m' \leftarrow \bar{m} - \lfloor \frac{n}{m} \rfloor \bar{r}$, $n' \leftarrow \bar{r}$.

对于上述的过程, 给出一个例子, 如在求 $\gcd(12,18)$ 的时候表示出 6:

$$\begin{aligned} 6 &= 0.0 + 1 \cdot 6 \\ &= (1-0) \cdot 6 + 0.12 \\ &= (-1) \cdot 12 + 1 \cdot 18 \end{aligned}$$

接下来解释为什么是最大的: 假设上述算法得到 $\gcd(m,n) = d$, 以及 $m'm + n'n = d$, 但是存在一个 $d' > d$, 满足 $d \backslash m \wedge d \backslash n$. 由于任何 m,n 的公因子都要整除 $m'm + n'n$, 它也要整除 d, 因此它一定要小于 d. 这就达到了矛盾.

下面介绍几个常用的性质.

性质 1.1. $k \backslash m \wedge k \backslash n \Leftrightarrow k \backslash \gcd(m,n)$.

证明. 若 $k \backslash m, k \backslash n, k \backslash (m'm + n'n) \Rightarrow k \backslash \gcd(m,n)$. □

性质 1.2 (gcd 与公因子的关系)**.** 每一个公因子是他们最大公因数的因子

1.3. 对因子的求和及其常见变形.

性质 1.3 (因子的对偶性)**.**

$$\sum_{m \backslash n} a_m = \sum_{m \backslash n} a_{n/m} \quad , n > 0, n \in \mathbb{Z}.$$

性质 1.4 (求和记号的交换)**.**

$$\sum_{m \backslash n} \sum_{k \backslash m} a_{k,m} = \sum_{k \backslash n} \sum_{l \backslash (m/k)} a_{k,kl}$$

证明. 这是因为可以将求和记号的整除用 Iverson 括号来表达. 即

$$\sum_{m|n} a_m = \sum_k a_m [n = mk]$$

从而, 如果把等式的左手边记作 LHS, 右手边记作 RHS, 有

$$\begin{aligned} \text{LHS} &= \sum_{j,l} \sum_{k,m>0} a_{k,m}[n = jm][m = kl] = \sum_j \sum_{k,l>0} a_{k,kl}[n = jkl] \\ \text{RHS} &= \sum_{j,m} \sum_{k,l>0} a_{k,kl}[n = jk]\left[\frac{n}{k} = ml\right] = \sum_m \sum_{k,l>0} a_{k,kl}[n = mlk] \end{aligned}$$

从而等式的左手边等于等式的右手边. □

这同样可以使用直观的方式: 把要求的和式写成三角形, 然后从两个不同的方面进行描述即可.

§2 质数

下文中, 若无特殊说明, 总是用 p 代表一个质数.

2.1. 基本的定义.

定义 2.1 (质数)**.** 如果一个数 p 有且仅有两个正因数, 也就是 1 和 p, 我们称它为质数. 特别地, 1 不是质数.

定义 2.2 (合数)**.** 有大于 2 个正因子的数叫做合数. 特别地, 1 不是合数.

实际上, 大于 2 的数之间, 一个数要么是质数, 要么是合数. 但不可能同时是两者.

实际上, 质数是构成自然数的骨架. 我们给出如下的定理:

定理 2.1 (唯一分解定理)**.** 任何一个数 n 都可以分解为若干个质数的乘积.

$$n = p_1 \cdots p_m = \prod_{k=1}^{m} p_k, \quad p_1 \leqslant \cdots \leqslant p_m.$$

其中, $p_1, p_2, \cdots, p_m$ 都是质数. 并且这个分解式唯一.

存在性. 使用数学归纳法.

[唯一性] 考虑反证法. 假设同一个数存在两个不同的分解方法

$$\begin{aligned} n &= p_1 \cdots p_m \quad p_1 \le p_2 \le \ldots \le p_m \\ &= q_1 \cdots q_k \qquad q_1 \le q_2 \le \ldots \le q_k \end{aligned}$$

以及 p_i, q_i 都是质数.

$p_1 = q_1$ 假设 $p_1 < q_1$, 根据他们都是质数, 故 $\gcd(p_1, q_1) = 1$. 根据 Euclid 算法, 存在 a, b, 使得

$$ap_1 q_2 \cdots q_k + bq_1 q_i \cdots q_k = q_2 \cdots q_k.$$

$$\text{现在} p_1 \,| ap_1 q_2 \cdots q_k, p_1 | \, bq_1 q_2 \cdots q_k, \Rightarrow p_1 \mid q_2 \cdots q_k$$

而这就意味着 $\frac{q_2 \cdots q_k}{p_1} \in \mathbb{Z}$, 且 $q_2 \cdots q_k$ 有一分解使 q_1 出现. 但是 $q_2 \ldots q_n < n$, 根据归纳法, 其必有唯一分解. 矛盾! 因此, $p_1 = q_1$. 此时可以在等两端同时除以 p_1, q_1. 重复刚才的过程, 可以证明 $p_2 = q_2$ 等.

□

注: 此式子有时候也可以记作

$$n = \prod_{p} p^{n_p}, \quad n_p \geqslant 0.$$

其中 $n_p \geq 0$, n_p 是质数 p 出现的次数.

由此我们便可以得到整数类似于 “坐标” 的表示. 只不过这里的维数是无穷维的.

例如, 下面方框里面的就可以认为是整数的 “坐标”.

$$
\begin{aligned}
12 &= 2^{\boxed{2}} \times 3^{\boxed{1}} \times 5^{\boxed{0}} \times 7^{\boxed{0}} \times \cdots \\
18 &= 2^{\boxed{1}} \times 3^{\boxed{2}} \times 5^{\boxed{0}} \times 7^{\boxed{0}} \times \cdots
\end{aligned}
$$

从而, 12 和 18 的坐标可以记作

$$12 = \langle 2, 1, 0, 0\rangle, 18 = \langle 1, 2, 0, 0, \cdots\rangle$$

在这个坐标系下, 对于一个数的坐标形式, 即 $\langle n_2, n_3, n_5, n_7, \cdots\rangle$, 我们发现

$$
\begin{aligned}
&k = mn && \Leftrightarrow k_p = m_p + n_p, && \forall p. \\
&m \backslash n && \Leftrightarrow m_p \leq n_p \quad , && \forall p \\
&k = \gcd(m, n) && \Leftrightarrow k_p = \min\left(m_p, n_p\right), && \forall p \\
&k = \operatorname{lcm}(m, n) && \Leftrightarrow k_p = \max\left(m_p, n_p\right), && \forall p.
\end{aligned}
$$