

素数 (prime number) 若 $a \in \mathbb{N}^+$, a 为素数 若 $\forall b \in \mathbb{N}^+, b|a \Rightarrow b=1$ 或 $b=a$

性质:

1. 素数有无穷多个

反证: 若有限, 取所有素数 $p_1, p_2, \dots, p_n$

$(p_1, n)=1$, $p_1 p_2 \dots p_n + 1$ 也为素数

令 $N = p_1 p_2 \dots p_n + 1$, $\forall p_i, p_i \nmid N$ (均余1)

fact: $\forall a$ 为合数, 存在至少一个素因子

a 为合数, 则 $\exists kb < a$ st $b|a$ (华数定理)

而 N 没有素因子 $\Rightarrow N$ 为素数

对应逆数, 弱约名 $\Leftrightarrow$ 素元

2. 素数的另一定义: p 为素数当且仅当: $\forall a, b$ 若 $p|ab$ 则 $p|a$ 或 $p|b$

证: 若 p 为素数, $\forall a, b$ 满足 $p|ab$ 则:

若 $(p, a)=1 \Rightarrow p|b$ (欧几里德)

若 $(p, a) \neq 1 \Rightarrow (p, a)=p$ (p 只有 1, p 两个因子) $\Rightarrow p|a$

反过来, 对子数 q 满足 $\forall a, b \in \mathbb{Z}$ 若 $q|ab$ 则 $q|a$ 或 $q|b$, 则 q 为素数.

反证: 设 $\exists q$ 不是素数, 满足: $\forall a, b \in \mathbb{Z}$, 若 $q|ab$ 则 $q|a$ 或 $q|b$

则取 $q = st$, $s, t \neq 1$, 则 $s \nmid q, t \nmid q$

此时: $q|st$ 但 $q \nmid s$ 且 $q \nmid t$ (因 $0 < 1 < s, t < q$) 矛盾故 q 必为素.

算术基本定理(素因子分解/唯一分解)

$\forall n \in \mathbb{N}^+$, 可唯一分解为:

$$n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}, \quad p \text{ 为素数, 且 } r_1, \dots, r_k \in \mathbb{N}^+$$

存在性: 任何整数都可表示为有限个素数的乘积

反证: 设 $\exists n$ 不能表示为有限个素数乘积, 取其中最小的记作 n_0

$n_0 = p_1 p_2 \dots p_k$, 则 $\forall p_i \in \{p_1, \dots, p_k\}$ 有 $\frac{n_0}{p_i} < n_0$, 但依然可以分解为有限个素数乘积
与 n_0 最小矛盾 $\Rightarrow$ 存在性得证

应设 n 不可以表示为有限个素数乘积, 取其中最小的记为 n_0

n_0 为合数则可分解为 $n_0 = s \cdot t$ $1 < s, t < n_0$, 而 s, t 由归纳假设, 均可表示为有限个素数乘积

$\Rightarrow n_0$ 也可...

唯一性:

[引理] 设 $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ 不妨设 $\{p_i\} \uparrow$

$$= q_1^{s_1} q_2^{s_2} \dots q_l^{s_l} \quad \{q_i\} \uparrow$$

由 $q_1 | n \Rightarrow q_1 | p_1^{r_1} \dots p_k^{r_k}$ 则 $q_1 | p_1$ 或 $q_1 | \frac{n}{p_1}$

若 $q_1 \neq p_1$ 则 $q_1 | \frac{n}{p_1}$ 依此将左项分解. 定 $\exists p_i$ s.t. $q_1 = p_i$

作归纳:

$n=1, 2$ 时有唯一的素因子分解.

设 $1 \leq n \leq k$ 有唯一素因子分解.

考虑 $n=k+1$, 设 n 存在两种分解: $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k} = q_1^{s_1} q_2^{s_2} \dots q_l^{s_l}$

则 $q_1 | p_1^{r_1} \dots p_k^{r_k}$ 由上述引理, $\exists p_i = q_1$ 则

$$\begin{cases} \frac{n}{p_i} = p_1^{r_1} \dots p_i^{r_i-1} \dots p_k^{r_k} \\ \frac{n}{q_1} = q_1^{s_1-1} q_2^{s_2} \dots q_l^{s_l} \end{cases} \quad \text{由归纳假设 } \frac{n}{p_i} = \frac{n}{q_1} < n \text{ 有唯一的素因子分解}$$

$$\Rightarrow n = \frac{n}{p_i} \cdot p_i \text{ 和 } n = \frac{n}{q_1} \cdot q_1 \text{ 的分解是一致的}$$