升幂引理

内容

升幂（Lift the Exponent，LTE）引理是初等数论中比较常用的一个定理。

定义 $\nu_p(n)$ 为整数 n 的标准分解中素因子 p 的幂次，即 $\nu_p(n)$ 满足 $p^{\nu_p(n)} \mid n$ 且 $p^{\nu_p(n)+1} \nmid n$.

由于升幂引理内容较长，我们将其分为三部分介绍：

以下内容设 p 为素数，x, y 为满足 $p \nmid x$ 且 $p \nmid y$ 的整数，n 为正整数。

第一部分

对所有的素数 p 和满足 $(n, p) = 1$ 的整数 n，

1. 若 $p \mid x - y$，则：

$$\nu_p\left(x^n - y^n\right) = \nu_p(x - y)$$

2. 若 $p \mid x + y$，则对奇数 n 有：

$$\nu_p\left(x^n + y^n\right) = \nu_p(x + y)$$

证明

若 $p \mid x - y$，则不难发现 $p \mid x - y \iff x \equiv y \pmod{p}$，则显然有：

$$\sum_{i=0}^{n-1} x^i y^{n-1-i} \equiv n x^{n-1} \not\equiv 0 \pmod{p}$$

进而由 $x^n - y^n = (x - y) \sum_{i=0}^{n-1} x^i y^{n-1-i}$ 可知命题得证。

对 $p \mid x + y$ 的情况证明方法类似。

第二部分

若 p 是奇素数，

1. 若 $p \mid x - y$，则：

$$\nu_p\left(x^n - y^n\right) = \nu_p(x - y) + \nu_p(n)$$

2. 若 $p \mid x+y$，则对奇数 n 有：

$$\nu_p\left(x^n+y^n\right)=\nu_p(x+y)+\nu_p(n)$$

证明

若 $p \mid x-y$，令 $y=x+kp$，我们只需证明 $p \mid n$ 的情况。

- 若 $n=p$，则由二项式定理：

$$\begin{aligned}\sum_{i=0}^{p-1} x^{p-1-i} y^i &= \sum_{i=0}^{p-1} x^{p-1-i} \sum_{j=0}^{i}\binom{i}{j} x^j(kp)^{i-j} \\ &\equiv p x^{p-1} \pmod{p^2}\end{aligned}$$

  从而

$$\nu_p\left(x^n-y^n\right)=\nu_p(x-y)+1$$

- 若 $n=p^a$，则由数学归纳法可得

$$\nu_p\left(x^n-y^n\right)=\nu_p(x-y)+a$$

因此命题得证。

对 $p \mid x+y$ 的情况证明方法类似。

第三部分

若 $p=2$ 且 $p \mid x-y$，

1. 对奇数 n 有（与第一部分的 1 相同）：

$$\nu_p\left(x^n-y^n\right)=\nu_p(x-y)$$

2. 对偶数 n 有：

$$\nu_p\left(x^n-y^n\right)=\nu_p(x-y)+\nu_p(x+y)+\nu_p(n)-1$$

另外对上述的 x,y,n，我们有：

若 $4 \mid x-y$，则：

- $\nu_2(x+y)=1$
- $\nu_2\left(x^n-y^n\right)=\nu_2(x-y)+\nu_2(n)$

证明

我们只需证明 n 为偶数的情况。由于此时 $p \nmid \binom{p}{2}$，故我们不能用第二部分的方法证明。

令 $n = 2^a b$，其中 $a = \nu_p(n)$，$2 \nmid b$，从而

$$\begin{aligned}\nu_p\left(x^n - y^n\right) &= \nu_p\left(x^{2^a} - y^{2^a}\right) \\ &= \nu_p\left((x-y)(x+y)\prod_{i=1}^{a-1}\left(x^{2^i} + y^{2^i}\right)\right)\end{aligned}$$

注意到 $2 \mid x - y \implies 4 \mid x^2 - y^2$，从而 $(\forall i \geq 1)$，$x^{2^i} + y^{2^i} \equiv 2 \pmod 4$，进而上式可变为：

$$\nu_p\left(x^n - y^n\right) = \nu_p(x-y) + \nu_p(x+y) + \nu_p(n) - 1$$

因此命题得证。

参考资料

1. Lifting-the-exponent lemma - Wikipedia