Lucas 定理

引理 1 当 p 是质数，x 是小于 p 的正整数，$\binom{p}{x} \mod p = 0$。

证明

$\because \binom{p}{x} = \frac{p!}{x!(p-x)!}, \therefore p \mid \binom{p}{x}$, 即 $\binom{p}{x} \mod p = 0.$ □

定理 (Lucas 定理) 若 $n = sp + q$,$m = tp + r$。$q, r < p$,

$\binom{n}{m} \equiv \binom{s}{t}\binom{q}{r} \pmod p$

证明

根据二项式定理，$\binom{n}{m}$ 等于 $(1+x)^n$ 展开式中次数为 m 的项的系数。

$$(1+x)^n = (1+x)^{sp+q} = (1+x)^{sp}(1+x)^q$$

由引理 1可得

$$\begin{aligned}(1+x)^n &\equiv (1+x^p)^s(1+x)^q \pmod p \\ &\equiv \sum_{i=0}^{s} \binom{s}{i} x^{ip} \sum_{j=0}^{q} \binom{q}{j} x^j\end{aligned}$$

当且仅当 $i = t$，$j = r$，x 的次数为 m。所以

$$\binom{n}{m} \equiv \binom{s}{t}\binom{q}{r} \pmod p$$

□