前置知识

费马小定理

若$p \in prime$，$gcd(a,p)=1,$则$a^{p-1} \equiv 1 \mod p$

欧拉定理

若$gcd(a,m)=1,$则$a^{\phi(m)} \equiv 1 \mod m$

拉格朗日定理

若$p \in prime,$多项式$A(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_0$
$(p$不是a_n的约数$)$的同余方程$A(x) \equiv 0 \mod p$至多由n个不同解

阶

满足$a^n \equiv 1 \mod m$的最小整数解n存在，则称n为a模m的阶。

性质

①$a, a^2, \ldots, a^{\delta_m(a)} \mod m$不同

②若$a^n \equiv 1 \mod m$，则$\delta_m(a)|n$

③若$gcd(a,m)=gcd(b,m)=1$，则$\delta_m(ab)=\delta_m(a)\delta_m(b)$的充要条件为$gcd(\delta_m(a),\delta_m(b))=1$

原根

设$m \in N_+, a \in Z, gcd(a,m)=1, \delta_m(a)=\varphi(m)$，则称a为模m的原根。

性质

①设$m \geq 3, gcd(a,m)=1$，则a为模m的原根的充要条件为对于$\varphi(m)$的素因数p,

$$都有a^{\frac{\varphi(m)}{p}}! \equiv 1 \mod m$$

②若m有原根，则m的原根有且只有$\varphi(\varphi(m))$个

③一个数有原根，当且仅当$m \in 2,4,p^a,2p^a | p \in prime, a \in N_+$

④若m有原根，其最小原根不大于$\sqrt[4]{m}$

NTT 快速数论变换

令x为$p \in prime$的一个原根，n为2的正整数次幂，设$g_n^k=x^{k\frac{p-1}{n}}$，则有以下性质：

①$g_n^t(t \in [0,n) \cap Z)$在$\mod p$意义下互不相同

②$g_{2n}^{2k}=g_n^k$

③$g_n^n \equiv 1 \mod p, g_n^{\frac{n}{2}} \equiv -1 \mod p \Longrightarrow g_n^{k+\frac{n}{2}} \equiv -g_n^k \mod p$

常用模数

998244353，469762049，1004535809的原根都是3

任意模数的多项式乘法

参考资料

https://www.bilibili.com/video/BV1hf4y1J73N