【知识总结】多项式全家桶（一）（NTT、加减乘除和求逆）

我这种数学一窍不通的菜鸡终于开始学多项式全家桶了……

必须要会的前置技能：FFT（不会？戳我：【知识总结】快速傅里叶变换（FFT））

以下无特殊说明的情况下，多项式的长度指多项式最高次项的次数加1

一、NTT

跟 FFT 功能差不多，只是把复数域变成了模域（计算复数系数多项式相乘变成计算在模意义下整数系数多项式相乘）。你看 FFT 里的单位圆是循环的，模一个质数也是循环的嘛 qwq。n次单位根w_n 怎么搞？看这里：【BZOJ3328】PYXFIB（数学）（内含相关证明。只看与原根和单位根相关的内容即可。）

注意裸的 NTT 要求模数p存在原根并且$p-1$ 是2的若干次幂的倍数（这个次数要大于多项式次数n）。于是通常就会用著名的 NTT 模数：$998244353=2^{23}\times 7\times 17+1$ 。

节约篇幅，代码先不放了。后面所有代码里都有 NTT 模板……

二、多项式求逆

对于n次多项式A，如果有多项式B满足$AB\equiv 1 \mod x^{n+1}$，则称B是A在模x^{n+1}意义下的逆元（和整数逆元差不多）。通常采用倍增的方法求逆元。通常都会规定多项式系数在模p的意义下。

首先，A在模x的意义下就只有一个常数项，所以此时的逆元B也只有一个常数项，就是A的常数项模p的逆元。

如果我们知道B_0是A在模$x^{\lceil\frac{n}{2}\rceil}$意义下的逆元，现在要求$B$是$A$在模$x^n$意义下的逆元。根据题设，显然有：

$$AB=1 \mod x^n$$

很明显，AB的1到$n-1$次项系数全是0，所以模一个x的低于n次幂也一定是1。所以

$$AB_0=AB=1 \mod x^{\lceil\frac{n}{2}\rceil}$$

那么

$$B-B_0=0 \mod x^{\lceil\frac{n}{2}\rceil}$$

两边和模数同时平方：

$$B^2+B_0^2-2BB_0=0 \mod x^n$$

两边同时乘A，得到（别忘了$AB=1 \mod x^n$）：

$$B+AB_0^2-2B_0=0 \mod x^n$$

然后移项，得到：

$$B=2B_0-AB_0^2 \mod x^n$$

照着这个式子递归算就行了。

由于后面带余除法的代码包含求逆，所以代码同样略去……

三、加减乘除

加减法：直接每项对应相加减。

乘法：这就是 NTT 的目的啊喂！

除法：如果不是带余除法直接乘逆元。下面着重介绍带余除法。

已知$n-1$ 次多项式F和$m-1$ 次多项式G，求$n-m$ 次多项式Q和多项式R（R的次数小于$m-1$ ），满足：

$$F(x)=Q(x)G(x)+R(x)\mod x^n$$

很明显，主要的难点在于式子里有个叫做R的嘴子（兔崽子Tzz）。如果能把它搞掉该多好……

注意到R的次数小于$m-1$ ，那么我们把它翻转，末尾补0，是不是就可以把它模成0了？定义$\mathrm{Tzz}_{A,n}$ 表示把A视作一个长为n的多项式（高次项补0）后翻转的结果。即

$\mathrm{Tzz}_{A,n}(x)=x^{n-1}A(\frac{1}{x})=\sum\limits_{i=0}^{n-1}a_ix^{n-i-1}$

给$F=QG+R$ 的每个多项式都代入同一个数，这个多项式也一定是成立的。所以：

$$F(\frac{1}{x})=Q(\frac{1}{x})G(\frac{1}{x})+R(\frac{1}{x})$$

两边同乘x^{n-1} ，得到：

$$x^{n-1}F(\frac{1}{x})=x^{n-m}Q(\frac{1}{x})\cdot x^{m-1}G(\frac{1}{x})+x^{n-1}R(\frac{1}{x})$$

即

$$\mathrm{Tzz}_{F,n}=\mathrm{Tzz}_{Q,n-m+1}\mathrm{Tzz}_{G,m}+\mathrm{Tzz}_{R,n}$$

现在$\mathrm{Tzz}_{R,n}$ 的最高次项是$n-1$ ，但是从常数项到$n-m$ 次项全是0（因为R的长度最多就是$m-1$ ）。所以现在如果模$n-m+1$ ，那么$\mathrm{Tzz}_{R,n}$ 就是0了，而$\mathrm{Tzz}_{Q,n-m+1}$ 因为最高次是$n-m$ 所以不会受到影响。

于是用$\mathrm{Tzz}_{F,n}$ 乘上$\mathrm{Tzz}_{G,m}$ 的逆元就是$\mathrm{Tzz}_{Q,n-m+1}$ ，翻回去就能得到Q。

最后把Q代进原式，乘一乘减一减就能算出R。

所以这样为什么是对的？（以下“低次项”指翻转后的前$n-m$ 项，“高次项”指翻转后的后m项）首先在模x^{n-m+1} 意义下肯定能保证低次项是对的（即$\mathrm{Tzz}F,n$ 与$\mathrm{Tzz}_{G,m}\mathrm{Tzz}_{Q,n-m+1}$ 的前$n-m$ 项相等）。至于高次项，反正有$\mathrm{Tzz}_{R,n}$ 来补锅，所以即使不对也没关系。

完结撒花。

全文完