【多项式】多项式逆元/开方/取模/多点求值/插值/牛顿迭代/对数/exp/幂

多项式求逆元

已知多项式$F(x)$，求$F(x)$在保留前n项（当然n要是2的次幂）的情况下的逆元$G(x)$，也就是：

$$F(x)G(x) \equiv 1 \pmod{x^n}$$

首先，如果$n=1$，那么直接就是常数项的逆元，

如果$n>1$，那么怎么办?
设：$G'(x)$使得$F(x)G'(x) \equiv 1 \pmod{x^{n/2}}$，且我们已知$G'(x)$
第一个式子可以变成：

$$F(x)G(x) \equiv 1 \pmod{x^{n/2}}$$

（把模数开了个方，依旧成立）
把两个式子相减：

$$F(x)(G(x)-G'(x)) \equiv 0 \pmod{x^{n/2}}$$

$$G(x)-G'(x) \equiv 0 \pmod{x^{n/2}}$$

同时平方：（当然模数也平方依旧成立）

$$(G(x)-G'(x))^2 \equiv 0 \pmod{x^n}$$

$$G^2(x)+G'^2(x)-2G(x)G'(x) \equiv 0 \pmod{x^n}$$

两边同时乘上$F(x)$，消掉部分$G(x)$：

$$G(x)+G'^2(x)F(x)-2G'(x) \equiv 0 \pmod{x^n}$$

$$G(x) \equiv 2G'(x)-G'^2(x)F(x) \pmod{x^n}$$

那么，$G(x)$就可以快速求出了，
（同时发现，只要常数项有逆元，这个多项式就有逆元）
复杂度：$T(n)=T(n/2)+O(n\log(n))=O(n\log(n))$

多项式开方

多项式的开方同样可以以这种方法做出来，

已知多项式$F(x)$，求$F(x)$在保留前n项（当然n要是2的次幂）的情况下的平方根$G(x)$，也就是：

$$G^2(x) \equiv F(x) \pmod{x^n}$$

首先，如果$n=1$，那么直接就是常数项的开方，可以暴力枚举，也可以用二次项剩余（CZY的二次剩余Cipolla算法学习小记），

对于$n>1$的情况，
设：$G'(x)$使得$G'(x)^2 \equiv F(x) \pmod{x^{n/2}}$，且我们已知$G'(x)$，
（把平方写在后面好看QuQ）

第一个式子可以变成：

$$G^2(x) \equiv F(x) \pmod{x^{n/2}}$$

（把模数开了个方，依旧成立）
把两个式子相减：

$$G^2(x) - G'(x)^2 \equiv 0 \pmod{x^{n/2}}$$

因式分解：

$$(G(x) + G'(x))(G(x) - G'(x)) \equiv 0 \pmod{x^{n/2}}$$

可得$G(x)$有两个解（平方嘛），讨论$G(x) - G'(x) \equiv 0 \pmod{x^{n/2}}$的情况，

$$G(x) - G'(x) \equiv 0 \pmod{x^{n/2}}$$

（历史总是惊人的相识）
同时平方：（当然模数也平方依旧成立）

$$(G(x) - G'(x))^2 \equiv 0 \pmod{x^n}$$

$$G^2(x) + G'(x)^2 - 2G(x)G'(x) \equiv 0 \pmod{x^n}$$

因为：$G^2(x) \equiv F(x) \pmod{x^n}$

$$F(x) + G'(x)^2 - 2G(x)G'(x) \equiv 0 \pmod{x^n}$$

$$G(x) \equiv \frac{F(x)+G'(x)^2}{2G'(x)} \pmod{x^n}$$

那么，$G(x)$就可以快速求出了，
（同时发现，只要常数项是二次项剩余且有逆元，这个多项式就可以开方）
复杂度：$T(n) = T(n/2) + 2 * O(n\log(n)) = O(n\log(n))$

多项式取模

已知$A(x), B(x)$，求$D(x) = A(x) \mod B(x)$，
令$A(x) = B(x)C(x) + D(x)$
设$n = A(x)的次数$，$m = B(x)的次数$，显然有$m \le n$，
上面的等式两边同时乘上x^n得：

$$x^n A(\frac{1}{x}) = x^m B(\frac{1}{x})x^{n-m}C(\frac{1}{x}) + x^n D(\frac{1}{x})$$

（$\frac{1}{x}$的作用相当于是把多项式头尾翻转一下）

设$A'(x) = x^n A(\frac{1}{x})$，$B'(x) = x^m B(\frac{1}{x})$，$C'(x) = x^{n-m}C(\frac{1}{x})$，$D'(x) = x^n D(\frac{1}{x})$

可以发现，经过翻转后，
$D'(x)$中只有次数$\in [n-m+1, n]$的项是有效的，其他项均为0，，
$A'(x)$中次数$\in [0, n]$的项是有效的，
$B'(x)$中次数$\in [0, m]$的项是有效的，
$C'(x)$中次数$\in [0, n-m]$的项是有效的，

现在再对原来的等式 $\mod x^{n-m+1}$，也就是

$$A'(x) = B'(x)C'(x) + D'(x) \mod x^{n-m+1}$$

这样$D'(x)$这一项就能模掉了，也就是：

$$A'(x) = B'(x)C'(x) \mod x^{n-m+1}$$

$$\frac{A'(x)}{B'(x)} = C'(x) \mod x^{n-m+1}$$

因为$C'(x)$的次数范围刚好在模以内，所以就可以直接求出$C'(x)$，变换得$C(x)$，
求出了$C(x)$,剩下直接减就好了

$$D(x) = A(x) - B(x)C(x)$$

复杂度：$O(n\log(n))$

多项式多点求值

已知多项式$F(x)$，给出$a_1,a_2,...,a_n$，要求$F(a_1),F(a_2),...,F(a_n)$

先抛出一个显然的结论：$F(a_1)=F(x) \mod (x+a_1)$，
（意思是：多项式$F(x)$模多项式$(x+a_1)$的余数就是当$x=a_1$时$F(x)$的值）

有这个结论就好办了，
设多项式$C_{l,r}(x)=\prod_{i=l}^{r}(x+a_i)$，$G_{l,r}(x)=F(x) \mod C_{l,r}(x)$，
考虑分治求解，
显然的：$G_{l,mid}(x)=G_{l,r}(x) \mod C_{l,r}(x)$，右边同理，
这样当l=r时$G_{l,l}(x)$就是$F(a_l)$的值了，
做两遍分治FFT，

复杂度：$O(n\log^2(n))$

多项式插值

给出$a_1,b_1,a_2,b_2,...,a_k,b_k$，要求多项式$F(x)$满足$F(a_i)=b_i$，

考虑使用拉格朗日插值法，

$$F(x)=\sum_{i=1}^{k}b_i(\prod_{1\le j\le k,i\not=j}\frac{x-a_j}{a_i-a_j})$$

将式子拆成两部分：

$$F(x)=\sum_{i=1}^{k}b_i(\prod_{1\le j\le k,i\not=j}\frac{1}{a_i-a_j})(\prod_{1\le j\le k,i\not=j}(x-a_j))$$

先做前面那一部分：（先取个倒数方便书写）
设$G_i=\prod_{1\le j\le k,i\not=j}(a_i-a_j)$，$M(x)=\prod_{j=1}^{k}(a_i-a_j)$
显然有$M(a_i)=0$，

有：

$$G_i=\lim_{x\to a_i}\frac{M(x)-M(a_i)}{x-a_j}$$

我们发现这个东西相当于$M(x)$在$x=a_i$处的导数，于是有：

$$G_i=\lim_{x\to a_i}\frac{M(x)-M(a_i)}{x-a_j}=M'(a_i)$$

所以对$M'(x)$做一次多点求值即可，

这个东西还可以用洛必达法则证明，
设$f(x)=x-a_i$
已知有$\lim_{x\to a_i}M(x)=0,\lim_{x\to a_i}f(x)=0$
所以：

$$\lim_{x\to a_i}\frac{M(x)}{f(x)}=\lim_{x\to a_i}\frac{M'(x)}{f'(x)}=M'(a_i)$$

现在的原始变成了：

$$F(x)=\sum_{i=1}^{k}b_iG_i(\prod_{1\le j\le k,i\ne j}(x-a_j))$$

这个东西可以直接使用分治FFT实现，分治的时候记录两个多项式分别表示是否已经空缺了一位，

复杂度：$O(n\log^2(n))$

多点求值+几遍分治FFT常数爆炸

多项式牛顿迭代

已知多项式$G(x)$，要求多项式F使得$G(F)=0\mod x^n$

前置技能：

泰勒展开

对于多项式$f(x)$它在x_0处的泰勒展开为：

$$f(x)=f(x_0)+\frac{f'(x)}{1!}(x-x_0)+\frac{f''(x)}{2!}(x-x_0)^2+.....$$

考虑倍增求F

现在要求的F是$\mod x^{2n}$的，假设我们已经求出了F_0表示$\mod x^n$时的答案，

把$G(F)$在F_0处展开：

$$G(F)=G(F_0)+G'(F_0)(F-F_0)+\frac{1}{2}G''(F_0)(F-F_0)^2\mod x^{2n}$$

我们注意到是在$\mod x^{2n}$意义下的，而从第3项开始最低次项的指数均大于2n，所以可以直接省去，于

是：

$$G(F)=G(F_0)+G'(F_0)(F-F_0) \mod x^{2n}$$

又因为$G(F)=0 \mod x^{2n}$，

$$0=G(F_0)+G'(F_0)F-G'(F_0)F_0 \mod x^{2n}$$

$$F=F_0-\frac{G(F_0)}{G'(F_0)}$$

多项式求对数

给出多项式$G(x)$，要求$F(x)$使得$F(x)=\ln(G(x)) \mod x^n$

对两边同时求导，最后再积分回来，
有：

$$(\ln(G(x)))'=\frac{G'(x)}{G(x)}$$

所以

$$F(x)=\int\frac{G'(x)}{G(x)}dx$$

复杂度：$O(n\log(n))$

多项式求EXP

给出多项式$G(x)$，求$F(x)$满足$F(x)=e^{G(x)}$，

考虑使用牛顿迭代，
设多项式$g(x)=ln(x)-G(x)$，即$g(F)=0$

$$F=F_0-\frac{g(F_0)}{g'(F_0)}$$

又因为

$$g'(F_0)=(\ln(F_0))'-(A)'=\frac{1}{F_0}$$

所以：

$$F=F_0-F_0(\ln(F_0)-A)$$

复杂度：$O(n\log(n))$

多项式求幂

给出多项式$F(x)$，求$F(x)^k$，

$$F(x)^k=e^{k\ln(F(x))}$$

这样如果k不为整数也能求了

复杂度：$O(n\log(n))$
