PNM简要介绍（Singulet31258）

注：以下多项式均默认以 x 为自变量。
多项式牛顿法，Polynomial Newton's Method，简称 PNM。
给定函数 A，已知有多项式 B 满足 $x^n|A(B)$，求模 x^n 意义下的 B。（注：$A(B)$ 是关于多项式 B 的函数，这意味着其他多项式在这里相当于常数）
解：设模 $x^{\lfloor \frac{n}{2} \rfloor}$ 意义下的解为 C。那么 $B-C$ 的最低次项为 $x^{\lfloor \frac{n}{2} \rfloor+1}$ 项。于是有：

$$\forall i \geq 2, x^n|(B-C)^i$$

将 $A(B)$ 在 C 处泰勒展开，可得：（注意，$A^{(i)}$ 表示 A 的 i 阶导数，$A' = A^{(1)}$）

$$\begin{aligned} A(B) &= \sum_{i=0}^{\infty} \frac{A^{(i)}(C)(B-C)^i}{i!} &(1) \\ &\equiv A(C) + A'(C)(B-C) \equiv 0(\bmod x^n) &(2) \end{aligned}$$

因此，$B \equiv C - \frac{A(C)}{A'(C)}(\bmod x^n)$
这个公式被称为“多项式牛顿迭代公式（Polynomial Newton Iterative Formula，简称 $PNIF$）”。这个算法是一个倍增算法，它就是本篇 PDF 所介绍的 PNM。
设规模为 n 的 PNM 所需时间为 $T(n)$，则有：

$$T(n) = T(\frac{n}{2}) + f(n)$$

其中 $f(n)$ 表示计算规模为 n 的 $PNIF$ 的时间复杂度。
记多项式 A 的 x^k 项系数为 a_k（这里 A 可以换成其他任何大写字母，而 a 对应这个字母的小写形式），这里假设所有的系数都是非负整数，且对 P 取模，P 的值由具体的题目要求而定。
例题：
1.多项式求逆（inv）。给定多项式 A，求模 x^n 意义下的多项式 A^{-1}。
解：设 $F(B) = B^{-1} - A$，则本题转化为求 $x^n|F(B)$ 的解 B。

$$B \equiv C - \frac{F(C)}{F'(C)} \equiv C - \frac{C^{-1} - A}{-C^{-2}} \tag{3}$$
$$\equiv C + C^2(C^{-1} - A) \equiv 2C - AC^2 \tag{4}$$
$$\equiv C(2 - AC)(\mathrm{mod} x^n) \tag{5}$$

边界条件：模 x 意义下的解 $B \equiv a_0^{-1}(\mathrm{mod} x)$。此处 $f(n) = O(n \log n)$，由主定理可得，$T(n) = O(n \log n)$。
2.多项式指数函数（exp）。给定多项式 A，求模 x^n 意义下的多项式 e^A。
解：设 $F(B) = \ln B - A$，则本题转化为求 $x^n | F(B)$ 的解 B。

$$B \equiv C - \frac{F(C)}{F'(C)} \equiv C - \frac{\ln C - A}{C^{-1}} \tag{6}$$
$$\equiv C(1 - \ln C + A)(\mathrm{mod} x^n) \tag{7}$$

边界条件：模 x 意义下的解 $B \equiv 1(\mathrm{mod} x)$（不能是 e 的非零整数次方，因为 e 的非零整数次方在模意义下不收敛，这也意味着 $a_0 = 0$ 必须成立）。此处 $f(n) = O(n \log n)$，由主定理可得，$T(n) = O(n \log n)$。
3.多项式开方。给定多项式 A，求模 x^n 意义下的多项式 $A^{\frac{1}{k}}$，其中 k 是一个整数。
解：设 $F(B) = B^k - A$，则本题转化为求 $x^n | F(B)$ 的解 B。

$$B \equiv C - \frac{F(C)}{F'(C)} \equiv C - \frac{C^k - A}{kC^{k-1}} \tag{8}$$
$$\equiv \frac{(k-1)C^k + A}{kC^{k-1}}(\mathrm{mod} x^n) \tag{9}$$

边界条件：模 x 意义下的解 $B \equiv a_0^{\frac{1}{k}}(\mathrm{mod} x)$（这里要求 a_0 必须是模 P 意义下的 k 次剩余）。此处 $f(n) = O(n \log n)$，由主定理可得，$T(n) = O(n \log n)$，当 $k = 2$ 时为平方根（$sqrt$），当 $k = 3$ 时为立方根（$cbrt$）。
4.多项式三角函数、反三角函数、双曲函数、反双曲函数。这些函数实际上都是对数函数与指数函数的组合，故时间复杂度均为 $O(n \log n)$。
5.多项式幂函数（pow）。给定多项式 A，求模 x^n 意义下的多项式 A^k，其中 k 是一个常数。
解：$A^k = e^{k \ln A}$，时间复杂度为 $O(n \log n)$。
扩展内容：（高阶多项式全家桶）
多项式对数函数（ln）：给定多项式 A，求模 x^n 意义下的多项式 $\ln A$。
解：设多项式 $B = \ln A$，则 $B = \int \mathrm{d}B = \int A^{-1}A'\mathrm{d}x$。对 A 求逆，求导，然后再乘起来，最后再求不定积分，即可得到 B，时间复杂度为 $O(n \log n)$。与指数函数类似，这里 a_0 必须为 1，不定积

分的 C 只能取 0 这一个值。
多项式除法与取模（div, mod）：给定 $n-1$ 次多项式 A 和 $m-1$ 次多项式 B（$m<n$），求 $n-m$ 次多项式 Q 与低于 $m-1$ 次的多项式 R，满足 $A=QB+R$（这里 Q 被称作 $\frac{A}{B}$ 的商式（Quotient），R 被称作 $\frac{A}{B}$ 的余式（Remainder），可记作：$R=A\text{mod}B$）。
解：设 $\text{rev}F$ 表示多项式 F 的各项系数翻转后得到的多项式。那么有 $\text{rev}F(x)=x^{\deg F}F(\frac{1}{x})$，其中 $\deg F$ 表示 F 的次数（degree），假设 R 为 $m-2$ 次多项式（若实际次数小于 $m-2$，在高次项系数补 0 即可）：

$$A(x)=Q(x)B(x)+R(x)\Rightarrow$$
$$x^{n-1}A(\frac{1}{x})=x^{n-1}(Q(\frac{1}{x})B(\frac{1}{x})+R(\frac{1}{x}))=$$
$$x^{n-m}Q(\frac{1}{x})x^{m-1}B(\frac{1}{x})+x^{n-m+1}x^{m-2}R(\frac{1}{x})\Rightarrow$$
$$\text{rev}A(x)=\text{rev}Q(x)\text{rev}B(x)+x^{n-m+1}\text{rev}R(x)$$

于是有：

$$\text{rev}A(x)\equiv\text{rev}Q(x)\text{rev}B(x)(\text{mod}x^{n-m+1})$$

由于 Q 与 $\text{rev}Q$ 的最高次项均为 x^{n-m}（此处省略了系数），因此在模 x^{n-m+1} 意义下，Q 与 $\text{rev}Q$ 均不受任何影响。于是有：

$$\text{rev}Q=\frac{\text{rev}A}{\text{rev}B}\text{mod}x^{n-m+1}$$

于是我们便求出来 $\text{rev}Q$，各项系数再翻转回来即得到 Q。然后计算 $R=A-QB$ 即可得到 R。时间复杂度为 $O(n\log n)$。
常系数齐次线性递推
多项式平移|连续点值平移
多项式多点求值|快速插值
以上内容在洛谷上均有对应的模板题。