多项式基础理论

sjzez czy

2019.2.18

目录

1 多项式求逆

给定 $f(x)$，求 $g(x)$ 满足：

$$f(x) \times g(x) \equiv 1 \pmod{x^{n+1}}$$

设：

$$\begin{cases} A(x)B(x) \equiv 1 \pmod{x^n} \\ A(x)C(x) \equiv 1 \pmod{x^{\frac{n}{2}}} \end{cases}$$

则有：

$$\begin{aligned} & A(x)B(x) \equiv 1 \pmod{x^{\frac{n}{2}}} \\ \Rightarrow & A(x)(B(x)-C(x)) \equiv 0 \pmod{x^{\frac{n}{2}}} \\ \Rightarrow & B(x)-C(x) \equiv 0 \pmod{x^{\frac{n}{2}}} \\ \Rightarrow & (B(x)-C(x))^2 \equiv 0 \pmod{x^n} \\ \Rightarrow & B^2(x)+C(x)^2-2B(x)C(x) \equiv 0 \pmod{x^n} \\ \Rightarrow & A(x)B^2(x)+A(x)C(x)^2-2A(x)B(x)C(x) \equiv 0 \pmod{x^n} \\ \Rightarrow & B(x)+A(x)C(x)^2-2C(x) \equiv 0 \pmod{x^n} \\ \Rightarrow & B(x) \equiv 2C(x)-A(x)C(x)^2 \pmod{x^n} \end{aligned}$$

可见一个多项式是否有逆元只与其常数项是否有逆元有关

2 一阶分治 FFT 转多项式求逆

已知 $\{g_i | i \in [1, n-1] \cap Z\}$，且 $f_0 = 1$，同时有 $f_i = \sum_{j=1}^{i} f_{i-j} g_j$
求 $\{f_i | i \in [0, n-1] \cap Z\}$

设 $F(x) = \sum_{i=0}^{\infty} f_i x^i, G(x) = \sum_{i=0}^{\infty} g_i x^i$，且 $g_0 = 0$
那么有：

$$\begin{aligned} & F(x)G(x) = \sum_{i=0}^{\infty} x^i \sum_{j+k=i} f_j g_k = F(x) - f_0 x^0 \\ \Rightarrow & F(x)G(x) \equiv F(x) - f_0 \pmod{x^n} \\ \Rightarrow & F(x) \equiv \frac{f_0}{1-G(x)} \pmod{x^n} \\ \Rightarrow & F(x) \equiv (1-G(x))^{-1} \pmod{x^n} \end{aligned}$$

3 多项式除法

给定 n 次多项式 $f(x)$ 和 m 次多项式 $g(x)$，求 $n-m$ 次多项式 $h(x)$ 和一个 $m-1$ 次多项式 $r(x)$，满足：

$$f(x) \equiv g(x) \times h(x) + r(x) \pmod{x^{n+1}}$$

设一个 n 次多项式的系数翻转为：

$$\hat{f}(x) = x^n f(\frac{1}{x})$$

同时也可以得到它的逆翻转：

$$f(\frac{1}{x}) = x^{-n} \hat{f}(x)$$

考虑如下变形：

$$\begin{aligned}
&f(x) \equiv g(x) \times h(x) + r(x) \pmod{x^{n+1}} \\
\Rightarrow &f(\frac{1}{x}) \equiv g(\frac{1}{x}) \times h(\frac{1}{x}) + r(\frac{1}{x}) \pmod{x^{n+1}} \\
\Rightarrow &x^{-n}\hat{f}(x) \equiv x^{-m}\hat{g}(x) \times x^{m-n}\hat{h}(x) + x^{1-m}\hat{r}(x) \pmod{x^{n+1}} \\
\Rightarrow &\hat{f}(x) \equiv \hat{g}(x) \times \hat{h}(x) + x^{n-m+1}\hat{r}(x) \pmod{x^{n+1}} \\
\Rightarrow &\hat{f}(x) \equiv \hat{g}(x) \times \hat{h}(x) \pmod{x^{n-m+1}} \\
\Rightarrow &\hat{h}(x) \equiv \frac{\hat{g}(x)}{\hat{f}^{-1}(x)} \pmod{x^{n-m+1}}
\end{aligned}$$

于是可以求出 $h(x)$，之后有：

$$r(x) \equiv f(x) - g(x) \times h(x) \pmod{x^{n+1}}$$

4 多项式牛顿迭代

给定 $f(x)$，求一个 $g(x)$，满足：

$$f(g(x)) \equiv 0 \pmod{x^{n+1}}$$

设 $h(g) = f(g)$，假设已经求得了：

$$h(g_0) \equiv 0 \pmod{x^{\frac{n}{2}}}$$

现在要求 g 使得：

$$h(g) \equiv 0 \pmod{x^n}$$

考虑 $h(g)$ 在 g_0 处的麦克劳林展开：

$$\begin{aligned} h(g) &\equiv \sum_{n=0}^{\infty} \frac{h^{(n)}(g_0)(g-g_0)^n}{n!} \pmod{x^n} \\ \Rightarrow 0 \equiv h(g) &\equiv h(g_0) + h'(g_0)(g-g_0) \pmod{x^n} \\ \Rightarrow g &\equiv g_0 - \frac{h(g_0)}{h'(g_0)} \pmod{x^n} \end{aligned}$$

5 多项式 ln

给定 $f(x)$，求 $g(x) \equiv \ln(f(x)) \pmod{x^{n+1}}$

左右求导后可以得出：

$$\begin{aligned} g'(x) &\equiv \frac{f'(x)}{f(x)} \pmod{x^{n+1}} \\ \Rightarrow g(x) &\equiv \int \frac{f'(x)}{f(x)} dx \pmod{x^{n+1}} \end{aligned}$$

6 多项式 exp

给定 $f(x)$，求 $g(x) \equiv e^{f(x)} \pmod{x^{n+1}}$

先左右取对数：

$$\begin{aligned} \ln(g(x)) &\equiv f(x) \pmod{x^{n+1}} \\ \Rightarrow h(g) &\equiv \ln(g) - f \equiv 0 \pmod{x^{n+1}} \end{aligned}$$

之后对 $h(g)$ 进行牛顿迭代：

$$\begin{aligned} h(g) &\equiv g_0 - \frac{h(g_0)}{h'(g_0)} \pmod{x^n} \\ \Rightarrow h(g) &\equiv g_0 - h(g_0) g_0 \pmod{x^n} \\ \Rightarrow h(g) &\equiv (1 - \ln(g_0) + f) g_0 \pmod{x^n} \end{aligned}$$

7 多项式多点求值

给定 $f(x) = \sum_{i=0}^{n} a_i x^i$，同时有 $n+1$ 个点值 $X = \{x_i | 0 \le i \le n\}$
求 $Y = \{f(x) | x \in X\}$

构造函数 $X_l(x) = \prod_{i=0}^{\lfloor \frac{n}{2} \rfloor} (x - x_i), X_r(x) = \sum_{i=\lfloor \frac{n}{2} \rfloor + 1}^{n} (x - x_i)$

设 $f(x)=A_l(x)X_l(x)+B_l(x)$，则 $\forall x\in X_l, f(x)=B_l(x)$

设 $f(x)=A_r(x)X_r(x)+B_r(x)$，则 $\forall x\in X_r, f(x)=B_r(x)$

换句话说，可以求得 $B_l(x)=f(x) \bmod A_l(x)$，然后递归处理 $[l,\lfloor\frac{n}{2}\rfloor]$，右区间同理

在到达 $l=r$ 的时候，只剩下常数项，可以直接求值

对于 $X(x)$，可以先通过分治预处理出来

8 多项式多点插值

给定点集 $P=\{(x_i,y_i)|0\le i\le n\}$，求多项式 $f(x)$，满足 $\forall 0\le i\le n, f(x_i)=y_i$

考虑拉格朗日插值：

$$f(x)=\sum_{i=0}^{n}\frac{\prod_{j\neq i}(x-x_j)}{\prod_{j\neq i}(x_i-x_j)}y_i=\sum_{i=0}^{n}\frac{p_i}{q_i}y_i$$

那么从分子和分母两部分进行考虑

考虑分母部分，设：

$$M(x)=\prod_{i=0}^{n}(x-x_i)$$

那么有：

$$q_i=\frac{M(x)}{x-x_i}\Big|_{x_i}=\lim_{x\to x_i}\frac{M(x_i)}{x-x_i}=M'(x_i)$$

设 $v_i=\frac{y_i}{\prod_{j\neq i}(x_i-x_j)}$，进一步化简 $f(x)$ 得到：

$$f(x)=\sum_{i=0}^{n}v_ip_i=\sum_{i=0}^{n}v_i\prod_{j\neq i}(x-x_j)$$

构造：

$$\begin{cases}X_l(x)=\prod_{i=0}^{\lfloor\frac{n}{2}\rfloor}(x-x_i)\\ X_r(x)=\prod_{i=\lfloor\frac{n}{2}\rfloor+1}^{n}(x-x_i)\end{cases}$$

则有：

$$\begin{aligned}f(x)=&X_r(x)\left(\sum_{i=0}^{\lfloor\frac{n}{2}\rfloor}v_i\sum_{j\neq i,0\le j\le\lfloor\frac{n}{2}\rfloor}(x-x_j)\right)+X_l(x)\left(\sum_{i=\lfloor\frac{n}{2}\rfloor+1}^{n}v_i\sum_{j\neq i,\lfloor\frac{n}{2}\rfloor+1\le j\le n}(x-x_j)\right)\\ =&X_r(x)f_l(x)+X_l(x)f_r(x)\end{aligned}$$

依然是可以预处理 $X(x)$，对于 $f_l(x),f_r(x)$ 是可以递归求解的，在 $l=r$ 的时候返回 v_l

9 常系数齐次线性递推

设数列 $\{a_n\}$ 满足递推关系：

$$a_n = \sum_{i=1}^{k} b_i a_{n-i}$$

给定 n，求 a_n

9.1 矩阵乘法

一个比较简单的想法就是，构造转移矩阵，然后通过矩阵乘法以及快速幂实现求解

理论基础是矩阵乘法满足结合律，即 $(A \times B) \times C = A \times (B \times C)$，因此可以通过快速幂进行分治的求解

设 M 为转移矩阵，B 为初始矩阵，有：

$$B = \begin{bmatrix} f_{k-1} \\ f_{k-2} \\ \vdots \\ f_1 \\ f_0 \end{bmatrix}$$

且：

$$M = \begin{bmatrix} a_1 & a_2 & a_3 & \cdots & a_{k-2} & a_{k-1} & a_k \\ 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 \end{bmatrix}$$

那么如果要求 f_n，且 $n \geq k$，那么就相当于求 $(M^{n-k+1}B)_{0,0}$

唯一的缺点就是时间复杂度过高，达到了 $O(k^3 \log n)$，可以通过把这一类的转移矩阵转化为多项式来加速运算，达到 $O(k^2 \log n)$ 乃至 $O(k \log k \log n)$

9.2 特征值和特征向量

若有常数 λ，向量 $\vec{v}$，满足 $\lambda\vec{v} = A\vec{v}$ ，则 $\vec{v}$ 为矩阵 A 的一组特征向量，λ 为矩阵 A 的一组特征值

秩为 k 的矩阵有 k 组线性不相关的特征向量

9.3 特征多项式

$\lambda\vec{v}=A\vec{v}\Rightarrow(\lambda I-A)\vec{v}=0$，有解当且仅当 $\det(\lambda I-A)=0$

设 $f(\lambda)=\det(\lambda I-A)$，则 f 是一个 k 次多项式，同时 $\{\lambda|f(\lambda)=0\}$ 构成 k 个特征值

于是可以把 $f(x)$ 写成 $f(x)=\prod_{i=1}^{k}(x-\lambda_i)$ 的形式

根据 **Cayley-Hamilton 定理**，有 $f(A)=O$，其中 O 是零矩阵

设转移矩阵为 M，实际上只需要求出 M^n 就行了，先考虑怎么求 $f(x)$，根据定义，有：

$$f(x)=|xI-M|=\det\left(\begin{bmatrix}x-a_1 & -a_2 & -a_3 & \cdots & -a_{k-2} & -a_{k-1} & -a_k\\ -1 & x & 0 & \cdots & 0 & 0 & 0\\ 0 & -1 & x & \cdots & 0 & 0 & 0\\ 0 & 0 & -1 & \cdots & 0 & 0 & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots\\ 0 & 0 & 0 & \cdots & -1 & x & 0\\ 0 & 0 & 0 & \cdots & 0 & -1 & x\end{bmatrix}\right)$$

直接根据行列式的定义，可以得到：

$$f(\lambda)=\lambda^k-\sum_{i=1}^{k}a_i\lambda^{k-i}$$

因为 $f(M)=O$，于是可以得到 $M^k=\sum_{i=1}^{k}a_iM^{k-i}$

9.4 倍增求解

设 $M^x=\sum_{i=0}^{k-1}a_iM^i, M^y=\sum_{i=0}^{k-1}b_iM^i$，那么有：

$$\begin{aligned}M^{x+y}&=\sum_{i=0}^{k-1}\sum_{j=0}^{k-1}a_iM^ib_jM^j\\&=\sum_{c=0}^{2k-2}M^c\left(\sum_{i+j=c}a_ib_j\right)\end{aligned}$$

设 $M^{x+y}=f(M)g(M)+r(M)$，由于 $f(M)=0$，所以 $M^{x+y}=r(M)$

9.5 计算答案

对于计算答案的时候，假设要计算 M^nB，展开后可以得到：

$$M^nB=\sum_{i=0}^{k-1}a_i\left(M^iB\right)$$

其中 M^xB 对应着原序列的第 $x,x+1,\cdots,x+k-1$ 项，预处理 $f_0\sim f_{2k}$ 即可计算

由于代码实现的原因，实际上在 $k=1$ 的时候要特殊处理，此时就是一个等比数列

10 一阶线性微分方程

10.1 齐次线性方程

10.1.1 形式

$$\frac{dy}{dx}+P(x)y=0$$

10.1.2 求解

$$\begin{aligned}
&\frac{dy}{dx}+P(x)y=0\\
\Rightarrow&\frac{dy}{y}=-P(x)dx\\
\Rightarrow&\int\frac{dy}{y}=c_1-\int P(x)dx\\
\Rightarrow&\ln|y|=c_1-\int P(x)dx\\
\Rightarrow&y=Ce^{-\int P(x)dx}\quad(C=\pm e^{c_1})
\end{aligned}$$

10.2 非齐次线性方程

10.2.1 形式

$$\frac{dy}{dx}+P(x)y=Q(x)$$

10.2.2 求解

可以通过对应的齐次线性方程，使用 **常数变易法**求解

设 $y=u(x)e^{-\int P(x)dx}$，则:

$$\begin{aligned}
&\frac{dy}{dx}=\frac{du}{dx}e^{-\int P(x)dx}-u(x)P(x)e^{-\int P(x)dx}\\
\Rightarrow&\frac{du}{dx}e^{-\int P(x)dx}-u(x)P(x)e^{-\int P(x)dx}+P(x)u(x)e^{-\int P(x)dx}=Q(x)\\
\Rightarrow&\frac{du}{dx}=Q(x)e^{\int P(x)dx}\\
\Rightarrow&\int du=C+\int Q(x)e^{\int P(x)dx}dx\\
\Rightarrow&u(x)=C+\int Q(x)e^{\int P(x)dx}dx\\
\Rightarrow&y=e^{-\int P(x)dx}\left(C+\int Q(x)e^{\int P(x)dx}dx\right)\\
\Rightarrow&y=Ce^{-\int P(x)dx}+e^{-\int P(x)dx}\left(\int Q(x)e^{\int P(x)dx}dx\right)
\end{aligned}$$

可以发现，等式右端第一项是对应的齐次线性方程的通解，第二项是非齐次线性方程的一个特解（在 $C=0$ 时取到）

即 **一阶非齐次线性方程的通解等于对应的齐次方程的通解与非齐次方程的一个特解之和**

11 伯努利方程

11.1 形式

$$\frac{dy}{dx}+P(x)y=Q(x)y^n \quad (n\notin\{0,1\})$$

11.2 求解

在 $n=0$ 的时候，退化成为了 **一阶齐次线性方程**

在 $n=1$ 的时候，退化成为了 **一阶非齐次线性方程**

首先有 $\frac{dy}{dx}+P(x)y=Q(x)y^n \Rightarrow y^{-n}\frac{dy}{dx}+P(x)y^{1-n}=Q(x)$

尝试用 $\frac{d}{dx}y^{1-n}$ 替换 $\frac{dy}{dx}$，得到 $(1-n)y^{-n}\frac{dy}{dx}$

为了消除 $1-n$，引入 $z=y^{1-n}$，则有 $\frac{dz}{dx}=(1-n)y^{-n}\frac{dy}{dx}$，代入原式可得：

$$\begin{aligned}&y^{-n}\frac{dy}{dx}+P(x)y^{1-n}=Q(x)\\ \Rightarrow&\frac{dz}{dx}+(1-n)P(x)z=(1-n)Q(x)\\ \Rightarrow&\frac{dz}{dx}+P_n(x)z=Q_n(x)\end{aligned}$$

那么就又转化为了 **一阶线性方程**，代入公式可以得知：

$$z=e^{-\int(1-n)P(x)dx}\left(C+\int(1-n)Q(x)e^{\int(1-n)P(x)dx}dx\right)$$

由于 $z=y^{1-n}$，所以 $y=z^{\frac{1}{1-n}}$，于是可以得出：

$$y=\left(e^{-\int(1-n)P(x)dx}\left(C+\int(1-n)Q(x)e^{\int(1-n)P(x)dx}dx\right)\right)^{\frac{1}{1-n}}$$

12 黎卡提方程

12.1 形式

$$\frac{dy}{dx}=P(x)y^2+Q(x)y+R(x)$$

一般形式暂时没有通用解法，但对于一些特殊形式还是可以解出来的

12.2 $P(x), Q(x), R(x)$ 中至少两个同时为 0

无非以下三种，均为 **变量分离方程**：

$$\begin{aligned}
&\frac{dy}{dx} = P(x)y^2 \Rightarrow y^2dy = P(x)x \\
&\frac{dy}{dx} = Q(x)y \Rightarrow \frac{dy}{y} = Q(x)dx \\
&\frac{dy}{dx} = R(x)dy = R(x)dx
\end{aligned}$$

12.3 $\frac{dy}{dx} = Q(x)y + R(x)$

退化为 **一阶线性方程**：

$$\frac{dy}{dx} = Q(x)y + R(x)$$

12.4 $\frac{dy}{dx} = P(x)y^2 + Q(x)y$

退化为 **伯努利方程**：

$$\frac{dy}{dx} = P(x)y^2 + Q(x)y$$

12.5 $\frac{dy}{dx} + ay^2 = bx^m$

需要保证：

$$\begin{cases}
a \neq 0 \\
x \neq 0 \\
y \neq 0 \\
m = 0, -2, \frac{-4k}{2k+1}, \frac{-4k}{2k-1}(k = 1, 2, \cdots)
\end{cases}$$

令 $x_1 = ax$，则原式可以规约为 $\frac{dy}{dx} + y^2 = bx^m$

当 $m = 0$ 时，有：

$$\begin{aligned}
&\frac{dy}{dx} + y^2 = b \\
\Rightarrow &\frac{dy}{dx} = b - y^2 \\
\Rightarrow &\frac{dy}{b - y^2} = dx \\
\Rightarrow &\int \frac{dy}{b - y^2} = C + x
\end{aligned}$$

当 $m = -2$ 时，设 $z = xy$，有：

$$\begin{cases} y = \frac{z}{x} \\ \frac{dz}{dx} = \frac{ydx+xdy}{dx} = y + x\frac{dy}{dx} \end{cases}$$

于是有：

$$\begin{aligned} \frac{dz}{dx} =& y + x\left(-y^2 + \frac{b}{x^2}\right) \\ =& \frac{z}{x} - \frac{z^2}{x} + \frac{b}{x} \\ =& \frac{b + z - z^2}{x} \end{aligned}$$

可以得到：

$$\begin{aligned} & \frac{dz}{b + z - z^2} = xdx \\ \Rightarrow & \int \frac{dz}{b + z - z^2} = C + \frac{x^2}{2} \end{aligned}$$

12.6 $\frac{dy}{dx} + ay^2 = \frac{1}{x}y + \frac{b}{x^2}$

设 $z = xy$，则 $y = \frac{z}{x}$，于是有：

$$\begin{aligned} & \frac{dy}{dx} + ay^2 = \frac{1}{x}y + \frac{b}{x^2} \\ \Rightarrow & \frac{1}{x}\left(\frac{dz}{dx} - \frac{z}{x}\right) + a\frac{z^2}{x^2} = \frac{z}{x^2} + \frac{b}{x^2} \\ \Rightarrow & \frac{1}{x}\frac{dz}{dx} = \frac{z}{x^2} - a\frac{z^2}{x^2} + \frac{z}{x^2} + \frac{b}{x^2} \\ \Rightarrow & \frac{1}{x}\frac{dz}{dx} = \frac{2z - z^2 + b}{x^2} \\ \Rightarrow & \int \frac{dz}{2z - x^2 + b} = C + \int \frac{xdx}{x^2} \end{aligned}$$

13 参考文献

黎卡提方程的初等解法