日期: /

1. Vieta 定理，对称多项式基本定理

$f(x)=a_n x^n+a_{n-1}x^{n-1}+\cdots+a_0$ 有根 $x_1, x_2, \cdots, x_n$,

则 $f(x)=a_n(x-x_1)(x-x_2)\cdots(x-x_n)$

展开对比系数得

$$-\frac{a_{n-1}}{a_n}=\sum_{i=1}^{n}x_i$$

$$\frac{a_{n-2}}{a_n}=\sum_{k}\sum_{j<k\le n}x_j x_k$$

...

$$(-1)^n\frac{a_0}{a_n}=\prod_{i=1}^{n}x_i$$

2、多项式计算 行列式

① Vandermonde 矩阵

② $\left((i+j)^{50}+2024\right)_{100\times 100}$

余数定理

$uf+vg=d$

$d=\gcd(f,g)$

多个多项式 Bézout

$(f,g)=1$

$\Rightarrow (f(x^m),g(x^m))=1$

中国剩余定理

3、相伴与互相整除关系

4、A 在一组基下矩阵为 $\begin{pmatrix}B & \\ & C\end{pmatrix}$ 其中 B 可逆，C 幂零.

唯一分解应用

日期: /

② Vandermonde 行列式

$\det A$，其中 $A=\begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ \vdots & \vdots & & \vdots \\ a_1^{n-1} & a_2^{n-1} & \cdots & a_n^{n-1} \end{pmatrix}$

法一：不妨设 $a_1,\cdots,a_n$ 互不相同

设 $f(x)=\det\begin{pmatrix} 1 & 1 & \cdots & 1 \\ x & a_2 & \cdots & a_n \\ \vdots & \vdots & & \vdots \\ x^{n-1} & a_2^{n-1} & \cdots & a_n^{n-1} \end{pmatrix}$

则 $f(x)\in \mathbb{F}[x]$ 且 $\deg f(x)\le n-1$，原式 $=f(a_1)$

而 $f(a_2)=\cdots=f(a_n)=0$

故 $f(x)\sim (x-a_2)\cdots(x-a_n)$

首项系数为 $(-1)^{1+n}\det\begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_2 & a_3 & \cdots & a_n \\ \vdots & \vdots & & \vdots \\ a_2^{n-2} & a_3^{n-2} & \cdots & a_n^{n-2} \end{pmatrix}$

为 $n-1$ 阶 Vandermonde 行列式

递推得 $\det A=\prod_{1\le i<j\le n}(a_j-a_i)$

法二：将 $a_1,\cdots,a_n$ 看作未定元，从而 $\det A\in \mathbb{F}[a_1,\cdots,a_n]$

由 $a_i=a_j$ 时 $\det A=0$ 知 $a_i-a_j\mid \det A$ $(1\le i<j\le n)$

又由 a_i-a_j 两两互素知 $\prod_{1\le i<j\le n}(a_j-a_i)\mid \det A$

日期: /

对比次数得 $\det A \sim \prod_{1\le i<j\le n}(a_j-a_i)$

而 $a_1=0$ 时 $\det A = \prod_{i=2}^{n} a_i \det\begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_2 & a_3 & \cdots & a_n \\ \vdots & \vdots & & \vdots \\ a_2^{n-2} & a_3^{n-2} & \cdots & a_n^{n-2} \end{pmatrix}$

递推得 $\det A = \prod_{1\le i<j\le n}(a_j-a_i)$

3、Bézout 定理的推广

① 设 d 为 f,g 的首一公因式，其中 $f,g\in \mathbb{F}[x]$

则 $d=\gcd(f,g) \Leftrightarrow \exists u,v\in\mathbb{F}[x]$, s.t. $uf+vg=d$

证明: "⇒" 设 $f=d\cdot f_1$, $g=d\cdot g_1$

其中 $\gcd(f_1,g_1)=1$

则由 Bézout 定理, $\exists u_1,v_1\in\mathbb{F}[x]$

s.t. $uf_1+vg_1=1$

从而 $d=d(uf_1+vg_1)=u(df_1)+v(dg_1)=uf+vg$

"⇐": 若 h 为 f 与 g 的公因式

即 $h\mid f$ 且 $h\mid g$

则 $h\mid uf+vg \Rightarrow h\mid d$

又由 d 首1

故 $d=\gcd(f,g)$ □

日期: /

② 设 $f_1, f_2, \cdots, f_n \in \mathbb{F}[x]$

$gcd(f_1, \cdots, f_n) = d$

则 $\exists u_1, \cdots, u_n \in \mathbb{F}[x]$

s.t. $\sum_{i=1}^{n} u_i f_i = d$

证明: 对 n 归纳, $n=2$ 时已知,

若 $n=k$ 时成立, 则 $n=k+1$ 时

设 $d_1 = gcd(f_1, \cdots, f_k)$

则由归纳假设, $\exists v_1, \cdots, v_k \in \mathbb{F}[x]$

s.t. $v_1 f_1 + \cdots + v_k f_k = d_1$

且 $gcd(d_1, f_{k+1}) = d$

由 Bézout 定理, $\exists u, v \in \mathbb{F}[x]$

s.t. $u d_1 + v f_{k+1} = d$

$\Rightarrow u(v_1 f_1 + \cdots + v_k f_k) + v f_{k+1} = d$

取 $u_i = \begin{cases} u v_i & 1 \le i \le k \\ v & i = k+1 \end{cases}$

则 $u_1 f_1 + \cdots + u_{k+1} f_{k+1} = d$ □

日期: /

4. Bézout 定理判断互素

设 $f, g \in \mathbb{F}[x]$ 互素，那么是否 $\forall m \in \mathbb{N}_+$，$f(x^m)$ 与 $g(x^m)$ 互素？

是，证明：$\gcd(f,g)=1 \Rightarrow \exists u, v \in \mathbb{F}[x]$ s.t. $uf+vg=1$

从而 $u(x^m)f(x^m)+v(x^m)g(x^m)=1$

$\Rightarrow \gcd(f(x^m), g(x^m))=1$ ☑

5. 中国剩余定理

设 $f_1, f_2, \cdots, f_n \in \mathbb{F}[x]$ 两两互素，$a_1, \cdots, a_n \in \mathbb{F}[x]$

则 $\exists g \in \mathbb{F}[x]$，$\deg g < \deg(\prod_{i=1}^{n} f_i)$ 且 $g \equiv a_i \pmod{f_i}$ $(i=1,2,\cdots,n)$

证明：由 Bézout 定理，$\exists u_i, v_i \in \mathbb{F}[x]$

s.t. $u_i f_i + v_i \prod_{j\neq i} f_j = 1$ $(i=1,2,\cdots,n)$

取 $g_i = v_i \prod_{j\neq i} f_j$

则 $g_i \equiv 1 \pmod{f_i}$

$g_i \equiv 0 \pmod{f_j}$ $(j\neq i)$

取 $g_0 = \sum_{i=1}^{n} a_i g_i$

则 $g_0 \equiv a_i \pmod{f_i}$

作带余除法 $g_0 = q \prod_{i=1}^{n} f_i + r$

取 $g=r$ 则 $\deg g < \deg(\prod_{i=1}^{n} f_i)$ 且 $g \equiv a_i \pmod{f_i}$ $(i=1,2,\cdots,n)$

日期: /

下证唯一性，若 h 满足 $\deg h<\deg(\prod_{i=1}^{n} f_i)$ 且 $h\equiv a_i \pmod{f_i}$ $(i=1,2,\cdots,n)$

则 $f_i \mid h-g$ 且 $\deg(h-g)<\max\{\deg h,\deg g\}<\deg(\prod_{i=1}^{n} f_i)$

而由 f_i 两两互素知 $\prod_{i=1}^{n} f_i \mid h-g$，从而 $h-g=0$

故唯一. ∎

6. 直接推论：Lagrange 插值

设 $\alpha_1,\cdots,\alpha_n\in\mathbb{F}$ 互不相同，$\beta_1,\cdots,\beta_n\in\mathbb{F}$

则 $\exists!\ g\in\mathbb{F}[x]$ s.t. $\deg g<n$ 且 $g(\alpha_i)=\beta_i$

在中国剩余定理中取 $f_i=(x-\alpha_i)$，$a_i=\beta_i$ 即可

另一证法：线性方程组

设 $f(x)=c_{n-1}x^{n-1}+c_{n-2}x^{n-2}+\cdots+c_0$

则 $f(\alpha_i)=\beta_i$ $(i=1,2,\cdots,n)$

$$\Leftrightarrow \begin{pmatrix} \alpha_1^{n-1} & \alpha_1^{n-2} & \cdots & \alpha_1^1 & 1 \\ \alpha_2^{n-1} & \alpha_2^{n-2} & \cdots & \alpha_2^1 & 1 \\ \vdots & \vdots & & \vdots & \vdots \\ \alpha_n^{n-1} & \alpha_n^{n-2} & \cdots & \alpha_n^1 & 1 \end{pmatrix} \begin{pmatrix} c_{n-1} \\ c_{n-2} \\ \vdots \\ c_0 \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix}$$

经初等列变换系数矩阵为 Vandermonde 矩阵

从而存在唯一解 ∎