§5.3 The Greatest Common Divisor and Chinese Remainder Theorem (CRT)

illusion

Especially made for smy

School of Mathematical Science, XMU

Monday 24th February, 2025

http://illusion-hope.github.io/25-Spring-SMY-Discussion-Session/

HW-1

(1) [法一] $ax^4+bx^2+cx+1=(x-1)^2(x+1)(ax+1)$

$a=1,\ b=-2,\ c=0$ $=(x^2-2x+1)(x+1)(ax+1)$

$=ax^4+(-a+1)x^3+\underbrace{-(a+1)}x^2+(a-1)x+1$

(1) (USTC, 2019) 已知 $(x-1)^2(x+1)\mid(ax^4+bx^2+cx+1)$，求 a,b,c；

(2) 求 $(x+1)(x-1)$ 除 $f(x)=x^4+x^3+x+1$ 所得的商和余式;

(2') 求 99999999 除 1000100000000010001 所得的商和余数。

[法二] $f(1)=0,\ f(-1)=0$

$\begin{cases}a+b+c+1=0\\ a+b-c+1=0\\ 4a+2b+c=0\end{cases}$ 三连板 $c=0$

$f'(1)=a$

$\begin{cases}a+b=-1\\ 4a+2b=0\end{cases}$

$(x-1)^2\mid f(x)\Rightarrow x-1\mid f'(x)$

$f(x)=(x-1)^2g(x)$

$f'(x)=2(x-1)g(x)+(x-1)^2g'(x)$

$=(x-1)[2g(x)+(x-1)g'(x)]$

$(f(x),f'(x))=1$

$\Leftrightarrow f(x)$ 无重因式

$\Leftrightarrow$ 在 $\mathbb{C}$ 上无重根.

HW-1

x^2+x+1

x^2-1 $\sqrt{x^4+x^3+0x^2+x+1}$

$x^4+0x^3-x^2$

x^3+x^2+x+1

x^3+0x^2-x

x^2+2x+1

x^2+0x-1

$2x+2$

$f(1)=4 \quad f(-1)=0$

$\frac{4}{2}x+\frac{0-(-1)\cdot 4}{2}$

$=2x+2$

(1) (USTC, 2019) 已知 $(x-1)^2(x+1) \mid (ax^4+bx^2+cx+1)$，求 a, b, c；

(2) 求 $(x+1)(x-1)$ 除 $f(x)=x^4+x^3+x+1$ 所得的商和余式;

(2') 求 99999999 除 1000100000000010001 所得的商和余数。

10^8-1

$10^{16}+10^{12}+10^4+1$

$=(10^4-1)(10^4+1)$

例 1

If $m, n, p \in \mathbb{N}^*$ have the same parity, then $x^2 - x + 1 \mid x^{3n} - x^{3m+1} + x^{3p+2}$.

Check the converse of this proposition is also true.

Hint: $x^2 - x + 1 \mid x^3 + 1 \mid x^{3(2k)+l} + x^{3+l}$, $x^2 - x + 1 \mid x^3 + 1 \mid x^{3(2k-1)+l} + x^l$.

$x^3+1 = (x+1)(x-\omega_1)(x-\omega_2) = 0$ $\omega_i^3 = -1$. $(-1)^n - (-1)^m \cdot \omega_i + (-1)^p \omega_i^2 = 0$

x^2-x+1

n.m.p 不同奇偶性

$\omega_i^2 - \omega_i - 1 = 0$ 是否成立?

$-1 - \omega_i + \omega_i^2 = 0$

$1 + \omega_i + \omega_i^2 = 0 \Rightarrow x^3 = 1$ X

$1 - \omega_i - \omega_i^2 = 0$

$\omega_i^2 = \omega_i - 1 \Rightarrow \omega_i - 1 - \omega_i - 1 = -2 \neq 0$ 矛盾!

[证=] $x^2-x+1 \mid x^{3n}-x^{3m+1}+x^{3p+2}$

· 两偏奇

$x^2-x+1 \mid x^3+1 \mid x^{3(2k)}+x^3$

$x^{3n}-x^{3m+1}+x^{3p+2} = x^{3n}+x^3-(x^{3m+1}+x^4)+(x^{3p+2}+x^5)-x^3(1-x+x^2)$.

不妨 $x^2-x+1 \mid x^{3(2k-1)+l}+x^{3+l}$，其中 $k\in\mathbb{N}^*$，$l=0,1,2$.

$\Rightarrow x^2-x+1 \mid x^{3+l}-x^l$ （$+x^l-x^l$）

$l=2$ 时，$x^2-x+1 \mid x^5-x^2 \Rightarrow x^5-x^2=(x^2-x+1)(x^3+(-1)x^2+0)$

同除 x^2 $\Rightarrow x^3-1=(x^2-x+1)(x-1)=(x-1)(x^2+x+1)$

命题！

$l=1$ 时, $x^2-x+1 \mid x^4-x \Rightarrow x^4-x=(x^2-x+1)(x^2-x)$

$\Rightarrow x^3-1=(x^2-x+1)(x-1)$. 成立!

$l=0$ 时, $x^2-x+1 \mid x^3-1 \Rightarrow (x^2-1)=(x^2-x+1)(x-1)$ ×

· 西奇一伦

$$x^2-x+1 \mid x^3+1 \mid \underline{x^{3(2k-1)}+1}$$

$$\mid x^{3n}+1-(x^{3m+1}+x)+(x^{3p+2}+x^2)-(x^2-x+1)$$

$$x^2-x+1 \mid \underline{x^{3(2k)+l}}+x^l$$

$$+x^{3+l}-x^{3+l}$$

$$\Rightarrow x^2-x+1 \mid -x^{3+l}+x^l,\ l=0,1,2.$$ 同上直接等出来成立!

例 2

Determine all polynomials $f(x) \in F[x]$ such that $f[f(x)] = f^n(x)$, where $n \in \mathbf{N}^*$ is a given positive integer. **Note: You can only use the method of divisibility.**

Hint: $f^l(x) \mid f^n(x) = f[f(x)],\ \forall\ 1 \le l \le n.$

首先考虑 $\deg f(x) > 0$ 的 case.

$\deg f(x) = k. \Rightarrow f^n(x) = (a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0)^n.$

$f[f(x)] = a_k[f(x)]^k + a_{k-1}[f(x)]^{k-1} + \cdots + a_1 f(x) + a_0.$

$kn = \deg[f(x)]^k = k \cdot k. \Rightarrow \boxed{n = k.}$

$f^l(x) \mid f^n(x) = f[f(x)].$ $\quad l \le n.$

$f(x) \mid a_k[f(x)]^k + a_{k-1}[f(x)]^{k-1} + \cdots + a_1 f(x) + a_0 \Rightarrow f(x) \mid a_0 \Rightarrow a_0 = 0.$

$\deg > 0$

$f^2(x) \mid a_k[f(x)]^k + a_{k+1}[f(x)]^{k+1} + \cdots + a_1 f(x) \Rightarrow f^2(x) \mid a_1 f(x) \Rightarrow a_1 f(x) \equiv 0.$

且 $f(x) \neq 0 \Rightarrow a_1 = 0.$

(3) 同. $f^2, \cdots, f^n \Rightarrow a_2 = \cdots = a_{n-1} = 0$

$f^n(x) = a_n[f(x)]^n \Rightarrow a_n = 1.$

$f(x)$ 非零多项式

□

Euclidean Algorithm and Bézout's Theorem

Slogan: $f(x) = q(x)g(x) + r(x) \rightsquigarrow (f(x), g(x)) = (g(x), r(x))$.

d_1 d_2

$d_2 \mid g(x)$ $d_2 \mid r(x) + g(x)q(x) = f(x)$ $d_2 \mid d_1$

$d_1 \mid g(x)$ $d_1 \mid f(x) - g(x)q(x) = r(x)$ $d_1 \mid d_2$.

Thm 3

(Bézout's Theorem) Given two polynomials $f(x), g(x) \in F[x]$, then $(f(x), g(x))$ exists and there exist $u(x), v(x) \in F[x]$ such that

$$(f(x), g(x)) = u(x)f(x) + v(x)g(x).$$

Notes:

- $u(x), v(x)$ **are not unique**. The non-uniqueness comes from the fact that if $u(x), v(x)$ satisfy the equation, then so do $\tilde{u}(x) = u(x) + kg(x), \tilde{v}(x) = v(x) - kf(x)$ for any constant $k \in F$, i.e.,

$$(f(x), g(x)) = [u(x) + kg(x)]f(x) + [v(x) - kf(x)]g(x).$$

$$\begin{bmatrix} 1 & 0 & f(x) \\ 0 & 1 & g(x) \end{bmatrix} \to \begin{bmatrix} 1 & -q_1 & r_1 \\ 0 & 1 & g \end{bmatrix} \rightsquigarrow 1\cdot f(x) - q\cdot g(x) = r(x)$$

$f(x) = qg + r$

$[\deg f(x) > \deg g(x)]$

$\downarrow \quad g = q_2 r_1 + r_2.$

$$\begin{bmatrix} 1 & -q_1 & r_1 \\ -q_2 & 1+q_1q_2 & r_2 \end{bmatrix}$$

$\downarrow \cdots$

$uf + vg = r_{n+1} := d(x)$

$$\begin{bmatrix} u & v & r_{n+1} \\ * & & 0 \end{bmatrix}$$

$r_n = q_{n+2} r_{n+1}$ $\quad \boxed{r_{n+1} \mid r_n}$

$\Rightarrow \boxed{uf + vg = r_{n+1}}$

Try

Suppose $f(x) = x^4 - x^3 - x^2 + 2x - 1, g(x) = x^3 - 2x + 1$. Figure out $u(x)$, $v(x), (f(x), g(x))$.

$$\begin{bmatrix} 1 & & x^4-x^3-x^2+2x-1 \\ & 1 & x^3-2x+1 \end{bmatrix} \to \begin{bmatrix} 1 & 1-x & x^2-x \\ 0 & 1 & x^3-2x+1 \end{bmatrix}$$

$$\begin{array}{r|l} x & \\ \hline x^3-2x+1 & x^4-x^3-x^2+2x-1 \\ & x^4+0x^3-2x^2+x \\ \hline & -x^3+x^2+x-1 \\ & -x^3+0x^2+2x-1 \\ \hline & x^2-x \end{array}$$

$$\begin{array}{r|l} x+1 & \\ \hline x^2-x & x^3+0x^2-2x+1 \\ & x^3-x^2 \\ \hline & x^2-2x+1 \\ & x^2-x \\ \hline & -x+1 \end{array}$$

$$\to \begin{bmatrix} 1 & 1-x & x^2-x \\ -x-1 & x^2 & -x+1 \end{bmatrix}$$

$$(x+1)f(x) - x^2 g(x) = x-1$$

- **Special Case**: $(f(x), g(x)) = 1 \rightsquigarrow u(x), v(x)$ are **unique** if $\deg u(x) < \deg g(x), \deg v(x) < \deg f(x)$! $\rightsquigarrow$ Try to prove it.

  $\rightsquigarrow$ This conclusion will be used in the proof of Lagrange Interpolation Formula.

$\exists u, v$, $u(x)f(x) + v(x)g(x) = 1$. 如何限制次数?

若 $\deg u(x) \geq \deg g(x)$. 则 $u(x) = g(x)q(x) + r(x)$. $\deg r < \deg g$

$r(x)f(x) + \big(g(x)q(x)f(x) + v(x)g(x)\big) = 1$

$v(x)f(x) + \big(g(x)f(x) + v(x)\big)g(x) = 1$ 1 怎么用?

$\deg < \deg g$ 就像余数?

$\rightsquigarrow v(x)f(x) = \underbrace{1}_{\triangleq} - \underbrace{\big(g(x)f(x) + v(x)\big)}_{\triangleq t(x)}g(x)$.

$\Rightarrow \deg v + \deg f = \deg g + \deg t(x)$

$\because \deg v < \deg g \Rightarrow \deg t(x) < \deg f(x)$ 这样的 t.

唯一性.

$\tilde{u}f + \tilde{v}g = uf + vg = 1.$

$\Rightarrow (\tilde{u}-u)f = (v-\tilde{v})g.$ Goal: $u=\tilde{u}$, $v=\tilde{v}$.

$f \mid (v-\tilde{v})g$ $(f,g)=1 \Rightarrow f \mid v-\tilde{v}$ (?) $\Rightarrow v-\tilde{v}=0$

$\deg(v-\tilde{v}) \le \max\{\deg v, \deg \tilde{v}\} < \deg f$!

同理 $g \mid (\tilde{u}-u)f \Rightarrow \tilde{u}=u$.

证毕.

Explore Corresponding Characterizations of GCD

Def 4

We say that $d(x)$ is a greatest common divisor of $f(x)$ and $g(x)$ if $d(x)$ is a common divisor of $f(x)$ and $g(x)$ that all other common divisors divide.

Set $\Omega := \{u(x)f(x) + v(x)g(x) \mid u(x), v(x) \in F[x]\}$, then the definition is equal to:

(1) A common divisor that has the maximal degree;

$\rightsquigarrow$ GCDs have the same degree and are associate.

$\rightsquigarrow\rightsquigarrow$ The one whose leading coefficient is 1 is denoted as $(f(x), g(x))$.

(2) A **nonzero** polynomial $d(x) \in \Omega$ with minimal degree;

(3) A nonzero polynomial $d(x) \in \Omega$ divides all other elements in Ω.

(3') (3) $\Leftrightarrow d(x) \mid f(x)$, $d(x) \mid g(x)$.

Explore Corresponding Characterizations of GCD

Def 4

We say that $d(x)$ is a greatest common divisor of $f(x)$ and $g(x)$ if $d(x)$ is a common divisor of $f(x)$ and $g(x)$ that all other common divisors divide.

Set $\Omega := \{u(x)f(x) + v(x)g(x) \mid u(x), v(x) \in F[x]\}$, then the definition is equal to:

(1) A common divisor that has the maximal degree;

$\rightsquigarrow$ GCDs have the same degree and are associate.

$\rightsquigarrow\rightsquigarrow$ The one whose leading coefficient is 1 is denoted as $(f(x), g(x))$.

(2) A **nonzero** polynomial $d(x) \in \Omega$ with minimal degree;

(3) A nonzero polynomial $d(x) \in \Omega$ divides all other elements in Ω.

(3') (3) $\Leftrightarrow d(x) \mid f(x), d(x) \mid g(x)$.

(1) $(f(x), g(x)) = d(x) \Leftrightarrow (f(x^n), g(x^n)) = d(x^n)$;

(2) $(f(x), g(x)) = d(x) \Rightarrow (f^n(x), g^n(x)) = d^n(x)$.

⇒

1° $d(x) \mid f(x)$, $d(x) \mid g(x)$ $\Rightarrow d(x^n) \mid f(x^n)$, $d(x^n) \mid g(x^n)$

2° $\forall\ h(x) \mid f(x^n)$, $h(x) \mid g(x^n) \Rightarrow h(x) \mid d(x^n)$

$f(x)\,u(x) + v(x)\,g(x) = d(x) \Rightarrow f(x^n)u(x^n) + v(x^n)\,g(x^n) = d(x^n)$

⇐

1° $d(x^n) \mid f(x^n) \Rightarrow d(x) \mid f(x)$

$d(x^n) \mid g(x^n) \Rightarrow d(x) \mid g(x)$

} Lecture 1

2° 设 $f(x) = f_1(x)\,d(x)$, $g(x) = g_1(x)\,d(x)$

$\Rightarrow f(x^n) = f_1(x^n)\,d(x^n)$ $g(x^n) = g_1(x^n)\,d(x^n)$

$(f(x^n), g(x^n)) = d(x^n) \Rightarrow (f_1(x^n), g_1(x^n)) = 1$

$\Rightarrow (f_1(x), g_1(x)) = 1$?

反证, $(f_1, g_1) = d \neq 1$

$\Rightarrow d(x^n)$也一定那么这些多项式!

$\Rightarrow uf_1 + vg_1 = 1$

$\Rightarrow uf + vg = d^n$ 得证.

- Specially, $(f(x), g(x)) = 1 \Leftrightarrow (f(x^n), g(x^n)) = 1$, $\exists n$.

(2) $(f(x), g(x)) = d(x) \Rightarrow (f^n(x), g^n(x)) = d^n(x)$.

1° common divisor √.

2° $f = f_1 d$ $g = g_1 d$ $\Rightarrow f^n = f_1^n d^n$. $g^n = g_1^n d^n$

$(f_1, g_1) = 1 \Rightarrow (f_1^n, g_1) = 1 \Rightarrow (f_1^n, g_1^n) = 1$ √

□□.

例 8

Given two polynomials in $\mathbf{C}[x]$: $f(x) = a_0 + a_1x + a_2x^2 + a_{10}x^{10} + \cdots + a_{13}x^{13}$ $(a_{13} \neq 0)$ and $g(x) = b_0 + \cdots + b_3x^3 + b_{11}x^{11} + \cdots + b_{13}x^{13}$ $(b_3 \neq 0)$, try to prove that $\deg(f(x), g(x)) \leq 6$.

Hint: Recall that $\deg(f, g) = \arg\min_{u,v}\{\deg(uf + vg) \mid u, v \in F[x]\}$.

pf:

$f(x) = f_1(x) + x^{10} f_2(x)$, $\deg f_1 \leq 2$, $f_2 \neq 0$ (3')

$g(x) = g_1(x) + x^{11} g_2(x)$, $\deg g_1 = 3$, $\deg g_2 \leq 2$

$\cdot\, xg_2(x)$ $\cdot\, f_2(x)$

$\deg\left| xg_2(x)f(x) - f_2(x)g(x) \right| = \deg\left| xg_2(x)f_1(x) - f_2(x)g_1(x) \right|$

$\deg xg_2(x)f_1(x) \leq 5$, $\deg f_2(x)g_1(x) = 6$

$= 6$

$\deg(f, g) \leq 6$ ∎

例 10

Suppose $f(x), g(x), h(x) \in F[x], \boldsymbol{A} \in M_n(F)$ and $f(\boldsymbol{A}) = \boldsymbol{O}$.

(1) If $(f(x), g(x)) = d(x)$, then $r[g(\boldsymbol{A})] = r[d(\boldsymbol{A})]$;

(2) If $(f(x), g(x)) = 1$, then $g(\boldsymbol{A})$ is invertible;

(3) If $f(x) = g(x)h(x)$, then $g(\boldsymbol{A}), h(\boldsymbol{A})$ will not be invertible at the same time.

Notes:

- (Chapter 1) $\boldsymbol{A}^2 - \boldsymbol{A} + 2\boldsymbol{E} = \boldsymbol{O} \rightsquigarrow \boldsymbol{A} - 3\boldsymbol{E}$ 必定可逆；
- (Chapter 1) $\boldsymbol{A}^2 = \boldsymbol{E}, \boldsymbol{A} - \boldsymbol{E} \neq \boldsymbol{O} \rightsquigarrow \boldsymbol{A} + \boldsymbol{E}$ 必不可逆；
- (Chapter 4) $\varphi \in \mathcal{L}(V), \varphi^n + a_{n-1}\varphi^{n-1} + \cdots + a_1\varphi + a_0 = \mathscr{O}\ (a_0 \neq 0) \rightsquigarrow \varphi$ 必定可逆(为同构映射)。

$u(x)f(x) + v(x)g(x) = d(x)$

$\Downarrow$

$v(A)g(A) = d(A)$

$\Rightarrow r[g(A)] \geq r[d(A)]$

$d(x) \mid g(x) \Rightarrow g(A) = g(A)d(A)$

$\Rightarrow r[g(A)] \leq r[d(A)]$

Revisit An Example in Lecture 1

例 11

Prove that when $f(x) \in F[x]$ is divided by $(x-a)(x-b)$ $(a \neq b)$, the reminder $r(x)$ is

$$\frac{f(a)-f(b)}{a-b}x + \frac{af(b)-bf(a)}{a-b}.$$

We only need to find $g(x)$ such that $f(x) \equiv g(x) \pmod{(x-a)(x-b)}$ with its degree lower than 2. $\tilde{g}(x) \equiv g(x) \pmod{2次}$ $(x-a)(x-b) \mid g(x)-\tilde{g}(x) \Rightarrow g = \tilde{g}$.

$\rightsquigarrow$ Notice that $f(a) = f(a) \Leftrightarrow x-a \mid f(x)-f(a) \Leftrightarrow f(x) \equiv f(a) \pmod{x-a}$.

$$\rightsquigarrow \begin{cases} f(x) \equiv f(a) \pmod{x-a} \\ f(x) \equiv f(b) \pmod{x-b} \end{cases}$$

① 易之极

$\rightsquigarrow$ CRT

$f(x) = f(a) + u_1(x)(x-b) + f(b) + u_2(x)(x-a)$

$a-b \mid 1$, $1 \pmod{x-a}$

$b-a \mid 1$, $0 \pmod{x-b}$

$(x-b, x-a)=1 \Rightarrow \frac{1}{a-b}(x-b) - \frac{1}{a-b}(x-a) = 1$

$\frac{1}{a-b}(x-b) \equiv 1 \pmod{x-a}$

$\frac{1}{b-a}(x-a) \equiv 1 \pmod{x-b}$

$$\begin{cases} g(x) \equiv g_1(x) \pmod{p_1(x)} \\ g(x) \equiv g_2(x) \pmod{p_2(x)} \\ \vdots \\ g(x) \equiv g_n(x) \pmod{p_n(x)} \end{cases}$$

$p_1(x), \cdots, p_n(x)$ 两两互素

$G(x)$

$g(x) = u_1(x) \prod_{i\neq 1} p_i(x) + u_2(x) \prod_{i\neq 2} p_i(x) + \cdots + u_n(x) \prod_{i\neq n} p_i(x)$

g_1 g_2 g_n $\equiv 1$

$(p_2 \cdot p_1) = \cdots = (p_n, p_1) = 1$

$\Rightarrow (p_2 \cdots p_n, p_1) = 1$

$\Rightarrow u(x) p_2 \cdots p_n + v(x) p_1 = 1$

$\Rightarrow u(x) p_2 \cdots p_n \equiv 1 \pmod{p_1}$

- $u_i(x)$?

$\Rightarrow (p_i(x), p_j(x)) = d$? ☆

§ 5.4

$$g(x) \equiv G(x) \pmod{p_i(x)}$$

$$\equiv g_i(x)$$

$$p_i(x) \mid g(x) - G(x) \Rightarrow p_1(x) \cdots p_n(x) \mid g(x) - G(x)$$

$$\Rightarrow g(x) \equiv G(x) \pmod{p_1(x) \cdots p_n(x)}$$

$\Sigma \deg p_i(x)$

차수 $< \Sigma \deg p_i(x)$

$$G(x) = g(x) p_1 \cdots p_n + \tilde{G}(x)$$

$$\equiv \tilde{G}(x)$$

✓ 차수가 충분히 작다.

Chinese Reminder Theorem (CRT)

Thm 12

Given polynomials $f_1(x), \cdots, f_n(x)$, any two of which are relatively prime, then for $g_1(x), \cdots, g_n(x)$ such that $\deg g_i(x) < \deg f_i(x)$, there exists a unique polynomial $g(x)$ such that

$$g(x) \equiv g_i(x) \pmod{f_i(x)},$$

where $\deg g(x) < \sum_{i=1}^{n} \deg f_i(x)$.

(1) Create one $g(x)$ satisfying all the conditions $\rightsquigarrow \sum_{i=1}^{n} \left\{ u_i(x) \prod_{j \neq i} f_j(x) \right\} \cdot g_i(x)$

(2) Unique $\rightsquigarrow$ Relatively Prime

Examples

例 14

求一个次数最低的 $f(x) \in F[x]$ 满足 $(x-3)^2$ 除 $f(x)$ 余 $3x-7$, x^2 除 $f(x)$ 余 x^2+2x+3.

例 15

已知 $r_1(x) = x^2+2x+3, r_2(x) = 3x-7, A = \mathrm{diag}\{A_1, A_2\}, B = \mathrm{diag}\{B_1, B_2\}$,

$$A_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, A_2 = \begin{bmatrix} 3 & 1 \\ 0 & 3 \end{bmatrix}, B_1 = \begin{bmatrix} 3 & 2 & 1 \\ 0 & 3 & 2 \\ 0 & 0 & 3 \end{bmatrix}, B_2 = \begin{bmatrix} 2 & 3 \\ 0 & 2 \end{bmatrix}.$$

先验证 $r_i(A_i) = B_i$，再求一个次数最低的多项式 $f(x)$ 满足 $f(A) = B$.

例 14

求一个次数最低的 $f(x) \in F[x]$ 满足 $(x-3)^2$ 除 $f(x)$ 余 $3x-7$, x^2 除 $f(x)$ 余 x^2+2x+3.

$$\begin{cases} f(x) \equiv 3x-7 \pmod{(x-3)^2} \\ f(x) \equiv x^2+x+3 \pmod{x^2} \\ \quad\equiv 2x+3 \end{cases}$$

$$\begin{bmatrix} 1 & & x^2-6x+9 \\ & 1 & x^2 \end{bmatrix}$$

$$\to \begin{bmatrix} 1 & -1 & -6x+9 \\ 0 & 1 & x^2 \end{bmatrix} \to \begin{bmatrix} & * & \\ \frac{1}{6}x-\frac{1}{4} & -\frac{1}{6}x+\frac{5}{4} & -\frac{3}{2} \end{bmatrix}$$

$$x^2 = -\frac{1}{6}x(-6x+9)+\frac{3}{2}x$$

$$= \left(-\frac{1}{6}x+\frac{1}{4}\right)(-6x+9)-\frac{3}{2}$$

$$\equiv \left[\left(\frac{1}{6}x-\frac{1}{4}\right)(x-3)^2+\left(-\frac{1}{6}x+\frac{5}{4}\right)x^2\right] = 1 \cdot \left(-\frac{2}{3}\right) \quad \checkmark$$