2.4.

(1) 求整系数多项式

$f(x) = 28x^4 + 98x^3 + 36x^2 + 89x + 108$ 的次数

次数：$\gcd(28, 98, 36, 89, 108)$

$= 2$

(2) 将 $g = xy^2 + x^2y + x^2 + 2xy^2 - xy + y^2 - 2y - 1$

看做 $Z[x]$ 上 y 的多项式

求其次数.

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

$\gcd(x^2+2x-1,\ x^2-x-2,\ x^2-1)$

$= x+1$

次数为 $x+1$

2.7 $m_1 = x^2+1$

$m_2 = x^2+2x+1 = (x+1)^2$

$m_3 = x^2-x+1$

$\hat{m}_1 = (x+1)^2(x^2-x+1) = x^4+x^3+x+1$

$\hat{m}_2 = (x^2+1)(x^2-x+1) = x^4-x^3+2x^2-x+1$

$\hat{m}_3 = (x^2+1)(x+1)^2 = x^4+2x^3+2x^2+2x+1$

1° 求 m_1 与 $\hat{m}_1$ 的 $s_1\hat{m}_1 + t_1 m_1 = 1$

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

$r_0 = x^4+x^3+x+1$ $\quad s_0 = 1$ $\quad t_0 = 0$

$r_1 = x^2+1$ $\quad s_1 = 0$ $\quad t_1 = 1$

$r_2 = 2$

$s_2 = 1$ $\quad t_2 = 0 - (x^2+x-1)\cdot 1 = -(x^2+x-1)$

$\hat{m}_1 - (x^2+x-1)m_1 = 2$

$\frac{1}{2}\hat{m}_1 - \frac{1}{2}(x^2+x-1)m_1 = 1$

即 $s_1 = \frac{1}{2}$

$$
\begin{array}{r|l}
 & x^2-3x+7 \\
\hline
x^2+2x+1 & x^4-x^3+2x^2-x+1 \\
 & x^4+2x^3+x^2 \\
\hline
 & -3x^3+x^2-x+1 \\
 & -3x^3-6x^2-3x \\
\hline
 & 7x^2+2x+1 \\
 & 7x^2+14x+7 \\
\hline
 & -12x-6
\end{array}
$$

$$
\begin{array}{r|l}
 & x+1 \\
\hline
x+1 & x^2-3x+7 \\
 & x^2+x \\
\hline
 & -4x+7 \\
 & -4x-4 \\
\hline
 & 11
\end{array}
$$

$\hat{m}_1 - (x+1)(x^2-3x+7)m_1 = -6(x+1)$

$(x+1)\hat{m}_1 - (x+1)^2(x^2-3x+7)m_1 = -6m_1$

$\hat{m}_2 = (x^2-3x+7)m_2 + (-12x-6)$

$m_2 = (-\frac{1}{12}x - \frac{1}{8})(-12x-6) + \frac{1}{4}$

有 $4m_2 + (\frac{1}{3}x + \frac{1}{2})(-12x-6) = 1$

又 $(-12x-6) = \hat{m}_2 - (x^2-3x+7)m_2$

即 $4m_2 + (\frac{1}{3}x + \frac{1}{2})(\hat{m}_2 - (x^2-3x+7)m_2) = 1$

$s_2 = \frac{x}{3} + \frac{1}{2}$

3.1 $\hat{m}_3 = x^4+2x^3+2x^2+2x+1$

$m_3 = x^2-x+1$

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

$\hat{m}_3 = (x^2+3x+4)\cdot m_3 + 3x - 3$

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

$m_3 = \frac{1}{3}x(3x-3) + 1$

$m_3 - \frac{1}{3}x(3x-3) = 1$

$m_3 - \frac{1}{3}x(\hat{m}_3 - (x^2+3x+4)m_3) = 1$

$s_3 = -\frac{x}{3}$

$c_1 = \mathrm{rem}(\frac{x+1}{2}, x^2+1)$

$= \frac{x+1}{2}$

$c_2 = \mathrm{rem}(\frac{x}{3}+\frac{1}{3}, x^2+x+1)$

$= \frac{x}{3}+\frac{1}{2}$

$c_3 = \mathrm{rem}(-\frac{x}{3}(x+1), x^2-x+1)$

$= \frac{1}{3}$

$f_1(x) = 3(x+1)(x^9+x^3+x+1) + (2x+3)(x^9-x^3+2x^2-x+1)$
$+ 2(x^9+2x^3+2x^2+2x+1)$

$= 5x^5+9x^4+8x^3+11x^2+9x+8$

2.10 $p(x) \in K[x]$ 为一个不可约多项式，证明剩余类环 $K[x]/\langle p(x)\rangle$ 为一个域

解. 由于 $p(x)$ 为不可约多项式.

$p(x)$ 生成的理想为素理想

又 $\langle p(x)\rangle$ 不是极大理想

由 $K[x]$ 为 PID

存在非平凡多项式整除 $p(x)$

与 $p(x)$ 不可约矛盾.

则 $\langle p(x)\rangle$ 为极大理想

$K[x]/\langle p(x)\rangle$ 为一个域

3.6.
(1) $\deg f = m$

则 $f = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0$

$\mathrm{res}(f(x), x-y)$

$= \begin{vmatrix} a_m & a_{m-1} & \cdots & a_0 & & \\ & -y & & & & \\ & & -y & & & \\ & & & \ddots & \ddots & \\ & & & & \ddots & -y \end{vmatrix}_{m}$

$= a_m(-y)^m - a_{m-1}(-y)^{m-1} + a_{m-2}(-y)^{m-2} \cdots + (-1)^m a_0$

$= (-1)^m(a_m y^m + a_{m-1}y^{m-1} \cdots + a_0)$

12

$f(x) = a_m(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m)$

$g(x) = b_n(x-\beta_1)(x-\beta_2)\cdots(x-\beta_n)$

$h(x) = c_k(x-\gamma_1)(x-\gamma_2)\cdots(x-\gamma_k)$

$fg(x) = a_m b_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m)(x-\beta_1)(x-\beta_2)\cdots(x-\beta_n)$

由 3.5 Bezout(3)

有 $\mathrm{res}(fg, h)$

$= (a_m b_n)^k \cdot c_k^{m+n} \prod_{i=1}^{m}\prod_{j=1}^{k}(\alpha_i-\gamma_j) \times \prod_{i=1}^{n}\prod_{j=1}^{k}(\beta_i-\gamma_j)$

$\mathrm{res}(f, h)$

$= a_m^k \cdot c_k^m \prod_{i=1}^{m}\prod_{j=1}^{k}(\alpha_i-\gamma_j)$

$\mathrm{res}(g, h)$

$= b_n^k c_k^m \prod_{i=1}^{n}\prod_{j=1}^{k}(\beta_i-\gamma_j)$

则有 $\mathrm{res}(fg, h) = \mathrm{res}(f, h)\mathrm{res}(g, h)$

(3) $(fg)' = f'g + fg'$

1° f, g 有重因式

有 $\mathrm{Disc}(fg) = 0$ 又 $\mathrm{res}(f, g) = 0$

证毕.

2° f, g 没有重因式

设 $f(x) = a_m(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m)$

$g(x) = b_n(x-\beta_1)(x-\beta_2)\cdots(x-\beta_n)$

设 $f'g+fg' = a_m b_n(m+n)(x-r_{m+n-1})\cdots(x-r_1)$

$fg = a_m b_n(x-\alpha_1)\cdots(x-\alpha_m)(x-\beta_1)\cdots(x-\beta_n)$

$\mathrm{res}(fg, f'g+fg') = a_m b_n(-1)^{\frac{(m+n)(m+n-1)}{2}}\mathrm{Disc}(fg)$

$= (a_m b_n)^{m+n-1}\prod_{i=1}^{m}(f'g+fg')(\alpha_i)\prod_{i=1}^{n}(f'g+g'f)(\beta_i)$

$= (a_m b_n)^{m+n}\prod_{i=1}^{m} f'(\alpha_i)\, g(\alpha_i)\prod_{i=1}^{n}(g'(\beta_i)f(\beta_i))$

$= [a_m^{n-1}\prod_{i=1}^{m} f'(\alpha_i)][b_n^{m-1}\prod_{i=1}^{n} g'(\beta_i)][a_m^n\prod_{i=1}^{m} g(\alpha_i)]$
$[b_n^m\prod_{i=1}^{n} f(\beta_i)]$

$= \mathrm{res}(f, f')\,\mathrm{res}(g, g')\,\mathrm{res}(f, g)\cdot\mathrm{res}(f, g)$ 证毕

$h_2 = b^2 - x^2 + 2cx - c^2 - y^2 = -x^2 + 2cx + b^2 - c^2 - y^2$

3.8.

$$f = res_x(h_1, h_2) = \begin{vmatrix} -1 & 0 & a^2-y^2 & & \\ & -1 & 0 & a^2-y^2 & \\ & 2c & b^2-c^2-y^2 & 0 & \\ & -1 & 2c & b^2-c^2-y^2 & \\ & & -1 & 0 & a^2-y^2 \\ & & 2c & b^2-c^2-y^2 & 0 \\ & & -1 & 0 & a^2-y^2 \\ & & 2c & b^2-c^2-y^2 & \end{vmatrix}$$

$$= -1 \cdot \begin{vmatrix} -1 & 0 & a^2-y^2 & 0 \\ 2c & b^2-c^2-y^2 & 0 & a^2-y^2 \\ -1 & 2c & b^2-c^2-y^2 & 0 \\ 0 & -1 & 0 & a^2-y^2 \end{vmatrix} - 1 \cdot \begin{vmatrix} 0 & a^2-y^2 & 0 & \\ -1 & 0 & a^2-y^2 & \\ 2c & b^2-c^2-y^2 & 0 & \\ -1 & 2c & b^2-c^2-y^2 & \end{vmatrix}$$

$$= \begin{vmatrix} b^2-c^2-y^2 & 0 \\ 2c & b^2-c^2-y^2 \end{vmatrix} - \begin{vmatrix} 2c & a^2-c^2-y^2 \\ -1 & 2c \end{vmatrix} + (a^2-y^2) \begin{vmatrix} -1 & a^2-y^2 \\ -1 & b^2-c^2-y^2 \end{vmatrix}$$

$$= (b^2-c^2-y^2)^2 - 4c^2 - (b^2-c^2-y^2)(a^2-y^2)$$

3.8. 仿由 3.5 (3)

$res_x(h_1, h_2)$

$= [b^2-y^2-(c-\sqrt{a^2-y^2})^2] \cdot [b^2-y^2-(c+\sqrt{a^2-y^2})^2]$

$= [b^2-y^2-(c^2+a^2-y^2-2c\sqrt{a^2-y^2})] \cdot [b^2-y^2-(c^2+a^2-y^2+2c\sqrt{a^2-y^2})]$

$= (b^2-c^2-a^2+2c\sqrt{a^2-y^2})(b^2-c^2-a^2-2c\sqrt{a^2-y^2})$

$= (b^2-c^2-a^2)^2 - 4c^2(a^2-y^2)$

$= 4c^2y^2 - 16\Delta^2$

$res_y(f, h_3) = 4c^2(2\Delta+2\Delta)(2\Delta-2\Delta)$

$= 0$

3.10

$n=2 \quad d_1=3 \quad d_2=2 \Rightarrow d=4 \quad m = C_5^1 = 5$

$\nu = C_3^1 + C_0^1 = 5$

$T_4 = \{x^4, x^3y, x^2y^2, xy^3, y^4\}$

$T_{111} = \{x, y\} \quad T_{101} = \{x^2, xy, y^2\}$

Macaulay 矩阵 M

$$\begin{array}{c} xA \\ yA \\ x^2B \\ xyB \\ y^2B \end{array} \begin{pmatrix} a_{30} & a_{21} & a_{12} & a_{03} & 0 \\ 0 & a_{30} & a_{21} & a_{12} & a_{03} \\ b_{20} & b_{11} & b_{02} & 0 & 0 \\ 0 & b_{20} & b_{11} & b_{02} & 0 \\ 0 & 0 & b_{20} & b_{11} & b_{02} \end{pmatrix}$$

$S_{111} = \phi \quad S_{101} = \beta \quad S = 1$

Macaulay 结式为 det(M)

$$Syl(f,g) = \begin{pmatrix} a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & a_3 & a_2 & a_1 & a_0 \\ b_{20} & b_{11} & b_{02} & 0 & 0 \\ 0 & b_{20} & b_{11} & b_{02} & 0 \\ 0 & 0 & b_{20} & b_{11} & b_{02} \end{pmatrix}$$

4.1 解：证明：由于 $\phi_p(f)$ 与 $\phi_p(g)$ 互素

有 $gcd(f,g)_p = \bar{c} \cdot gcd(f_p, g_p)$

$= \bar{c}$

又 $\because$ 即 $gcd(f,g)_p$ 为常数

即 $gcd(f,g)$ 为一个正整数

$\phi_5(f) = x^8 + x^6 + 2x^4 + 2x^3 + x^2 + 2x$

$\phi_5(g) = 3x^6 + x^2 + x + 1$

又 $\phi_5(f)$ 与 $\phi_5(g)$ 互素

则有 $f(x)$ 与 $g(x)$ 互素

42. 写出多项式 $85x^5+155x^4+37x^3+35x^2-97x-50$ 用 5-adic 表示

$85 = 3\cdot5^3+2\cdot5+0\cdot1 = 5^3-2\cdot5^2+2\cdot5+0\cdot1$

$55 = 2\cdot5^2+1\cdot5$

$37 = 1\cdot5^2+2\cdot5+2\cdot1$

$35 = 1\cdot5^2+2\cdot5$

$-97 = -5^3+5^2+5-2\cdot1$

$-50 = -2\cdot5^2$

$f(x) = (\underline{5}^3-2\cdot5^2+2\cdot5)\cdot\underline{x}^5+(2\cdot5^2+1\cdot5)x^4$

$+(1\cdot5^2+2\cdot5+2\cdot1)x^3$

$+(1\cdot5^2+2\cdot5)x^2$

$+(-5^3+5^2+5-2)x-2\cdot5^2$

$=(x^5-x)\cdot5^3+(-2x^5+2x^4+x^3+x^2+x-2)\cdot5^2$

$+(2x^5+x^4+2x^3+2x^2+x)\cdot5$

$+2x^3-2x$

43 令 $\exists = \langle x+1, y+1\rangle$，写出多项式 $\underline{y^3}-y^2-2xy+\underline{3y^2}-12y^2+5x$ 用 $\exists$-adic 表示

解 $(y+1)^3 = y^3+3y^2+3y+1$

代入

原式 $=(y+1)^3-3y-1-y^2-2xy-12y^2+5x$

$=\underline{(y+1)^3}-3\underline{(y+1)}+2-\underline{(y+1)y^2}+y^2$

$-2\underline{(x-1)y}-2y-4y^2+\underline{5(x+1)}$

$+5$

$=(y+1)^3-(3+y^2)(y+1)+(5-2y)(x+1)$

$-2y-11y^2+7$

44. 用根号法求下面多项式的最大公因式

$f(x) = x^4+25x^3+145x^2-171x-360$

$g(x) = x^5+14x^4+15x^3-x^2-14x-15$

解 $b = g.c.d.(lc(f), lc(g)) = 1$

① 取 $p=5$

$f_5(x) = x^4-x = x(x^3-1)$

$g_5(x) = -x^4-x^2+x = -x(x^3-x+1)$

则 $g.c.d(f_5, g_5) = x$

② 取 $p=7$

$f_7(x) = x^4-3x^3-2x^2-3x-3 = x^2(x^2-3x-2)-3$

$g_7(x) = x^5+x^3-x^2+1 = (x^3-1)(x^2+1)$

$\because \lambda(f_7(x), g_7(x)) = 1$

则 $f(x)$ 与 $g(x)$ 的最大公因式为 1

45. 选取 $p=5$，用 Newton 迭代法求多项式

$x^6+93x^5+3258x^4+53041x^3+40725x^2$

$+1453125x+1953125$.

解：令 $F(y) = f-y^3$

首先 $f-y^3 \equiv 0 \bmod 5$

有 $\overline{u_0} = x(x+1)$ 令 $u_0 = \phi_5^{-1} = x^2+x$

$u^{(0)} = u_0$

$F'(u_0) = -3u_0^2 = -3x^2(x+1)^2$

$= -3x^2(x^2+2x+1)$

$= -3x^4-6x^3-3x^2$

$\phi_5(F'(u_0)) = 2x^4-x^3+2x^2$

$F(u^{(0)}) = x^6+93x^5+3258x^4+53041x^3$

$+40725x^2+1453125x+1953$

$-x^3(x+1)^3$

$= 90x^5+3255x^4+53040x^3$

$F(u^{(0)})/5 = 18x^5 + 651x^4 + 10608x^3 + 81450x^2$

$+ 290625x + 390625$

$\phi_5(F(u^{(0)})/5) = -2x^5 + x^4 - 2x^3$

$\bar{u}_1 = -\dfrac{\phi_5(F(u^{(0)})/5)}{\phi_5(F'(u^{(0)}))}$

$= x \qquad u_1 = x$

$u^{(1)} = u_0 + 5u_1$

$= x^2 + x + 5x$

$= x^2 + 6x$

$F(u^{(1)}) = 75x^5 + 3150x^4 + 52825x^3$

$+ 407250x^2 + 1453125x$

$+ 1953125$

$F(u^{(1)})/25 = 3x^5 + 126x^4 + 2113x^3$

$+ 16290x^2 + 58125x + 78125$

$\phi_5(F(u^{(1)})/25) = -2x^5 + x^4 - 2x^3$

$\bar{u}_2 = \dfrac{-\phi_5(F(u^{(1)})/25)}{\phi_5(F'(u^{(0)}))}$

$= x$

$u^{(2)} = u_1 + 25u_2$

$= x^2 + 31x$

$F(u^{(2)}) = 375x^4 + 23250x^3 + 407250x^2$

$+ 1453125x + 1953125$

$F(u^{(2)})/125 = 3x^4 + 186x^3 + 3258x^2$

$+ 11625x + 15625$

$\phi_5(F(u^{(2)})/125) = -2x^4 + x^3 - 2x^2$

$\bar{u}_3 = 1$

$u^{(3)} = u_0 + 125u_3$

$= x^2 + 31x + 125$

$F(u^{(3)}) = 0$

解得 $y = x^2 + 31x + 125$.

49. 用 Berlekamp 算法求多项式

$x^6 - 3x^5 + x^4 - 3x^3 - x^2 - 3x + 1$

在 $Z_{11}[x]$ 中的不可约分解

令 $p = x^6 - 3x^5 + x^4 - 3x^3 - x^2 - 3x + 1$

$\deg p = 6$

于是构造 C 为 6 阶矩阵

列等于 x^{11} x^{22} x^{33} x^{44} x^{55}

按 p 手算

$x^{11} = x^5(x^6 - 3x^5 + x^4 - 3x^3 - x^2 - 3x + 1)$

$+ 3x^{10} - x^9 + 3x^8 + x^7 + 3x^6 - x^5$

$= x^5 \cdot p + x^4(x^6 - 3x^5$

$x^5 + 3x^4 + 8x^3$

$x^6 - 3x^5 + x^4 - x^3 - x^2$) x^{11}

$x^{11} - 3x^{10} + x^9 - 3x^8 - x^7 - 3x^6 + x^5$

$3x^{10} - x^9 + 3x^8 + x^7 + 3x^6 - x^5$

$3x^{10} - 9x^9 + 3x^8 - 9x^7 - 3x^6 - 9x^5$

$+ 3x^4$

$8x^9 + 10x^7 + 6x^6 + 8x^5$

$- 3x^4$

$x^{11} \equiv 5x^5 - 5x^4 - 3x^3 - 3x^2 + 5x + 3 \bmod p$

$x^{22} \equiv -x^4 + x^3 - 5x^2 - 5x + 3 \bmod p$

$x^{33} \equiv -5x^4 + 3x^3 - x^2 + 4x - 2 \bmod p$

$x^{44} \equiv -3x^5 - x^2 - 3x - 4.$

$x^{55} \equiv -3x^5 - x^4 - 3x^3 - 4x^2 - x - 3$

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 5 & -5 & -3 & -3 & 5 & 3 \\ 0 & -1 & 1 & -5 & -5 & 3 \\ 0 & -5 & 3 & -1 & -1 & -2 \\ -3 & 0 & -2 & -1 & -3 & -4 \\ -3 & -1 & -3 & -4 & -1 & -3 \end{bmatrix}$$

$$C=\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 3 & 5 & -3 & -3 & -5 & 5 \\ 3 & -5 & -5 & 1 & -1 & 0 \\ -2 & 4 & -1 & 3 & -4 & -2 \\ -4 & -3 & -1 & 0 & 0 & -3 \\ -3 & -1 & -4 & -3 & -1 & -3 \end{bmatrix}$$

求出对应因特征因子为

并计算对应的不变因子

得到 分解结果为

$(x+1)\cdot(x^2+5x+3)(x^3+2x^2+3x+4)$

4.11 设

$A=x^4-394x^3-4193x^2+126x+596$

$\equiv (x^2+x+1)(x^2+x-1) \bmod 3$

用 Hensel 提升求多项式 A 在 Z[x] 中的因式分解

例 $B_0=x^2+x+1$

$C_0=x^2+x-1$

则 $\bar{U}=-1 \quad \bar{V}=1$

$E_0=A-B_0C_0$

$=-396x^3-4194x^2+126x+597$

$\frac{E_0}{3}=-132x^3-1398x^2+42x+199$

$\frac{E_0}{3}\cdot\bar{V}=66x^3+699x^2-21x-\frac{199}{2}$

$\Delta B_0=66x^2-97x-\frac{199}{2}$

$\frac{E_0}{3}\bar{U}=-66x^3-699x^2+21x+\frac{199}{2}$

$lc_p(\frac{E_0}{3}\bar{U})=1$

$\Delta B=1$

$\Delta C_0=1$

$B_1=x^2+x+4$

$C_1=x^2+x+2$

$E_1=-396x^3-4200x^2+120x+1598$

$\frac{E_1}{3}=x^2+x+1$

等注无法继续

仍对这一程序

分别为

原式 $=(x^2-404x+149)(x^2+10x-4)$

$\frac{E_0}{3}=-132x^3-1398x^2+42x+199$

$lc_p(\frac{E_0}{3}\bar{U})=1$

$lc_p(B_0)=x^2+x+1$

则 $\Delta B_1=1$

同理 $\Delta C_1=-1$

$B_1=x^2+x+4$

$C_1=x^2+x-4$

$\frac{E_1}{9}=-44x^3-466x^2+14x+68$

$lc_p(\frac{E_1}{9})=x^3-x^2-x-1$

$lc_p(B_1)=x^2+x+1$

$rem(lc_p(\frac{E_1}{9}),lc_p(B_1))=1$

依此类推

等到 原式 $=(x^2-404x+149)\cdot(x^2+10$