1.(i) $p = x^2 - xz - xy + yz + 3x^2y^2z^2 - x^3 - 2$

$$= \underbrace{3x^2y^2z^2}_{h_6} - \underbrace{x^3}_{h_3} + \underbrace{x^2 - xz - xy + yz}_{h_2} - \underbrace{2}_{h_0}$$

P的其余 h_i 均为0.

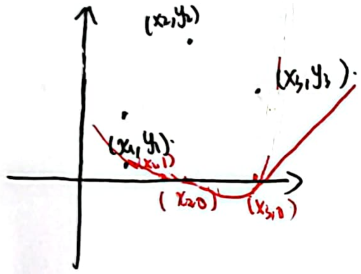
(ii) $\deg_x(p) = 3$, $\deg_y(p) = 2$, $\deg_z(p) = 2$, $\deg(p) = 6$

2. 解: 设 $f(x) = ax^2 + bx + c$, 由 $f(0)=2$, $f(1)=1$, $f(3)=0$, 可得.

法一:

$$\begin{cases} c = 2 \\ a + b + c = 1 \\ 9a + 3b + c = 0 \end{cases} \quad 解之得 \begin{cases} a = \frac{1}{6} \\ b = -\frac{7}{6} \\ c = 2 \end{cases}, \quad 故 f(x) = \frac{1}{6}x^2 - \frac{7}{6}x + 2$$

法二: 拉格朗日插值.



通过 (x_1,y_1), (x_2,y_2), (x_3,y_3) 三点, 平面上可得一个二次曲线

这条二次曲线可看做3条二次曲线相加.

① $f_1(x)$ 满足 $f_1(x_1)=1$, $f_1(x_2)=f_1(x_3)=0$.

② $f_2(x)$ 满足 $f_2(x_1)=0$, $f_2(x_2)=1$, $f_2(x_3)=0$

③ $f_3(x)$ 满足 $f_3(x_1)=0$, $f_3(x_2)=0$, $f_3(x_3)=1$.

$$\Rightarrow f(x) = y_1 f_1(x) + y_2 f_2(x) + y_3 f_3(x)$$

构造 $f_1(x), f_2(x), f_3(x)$.

$$f_1(x) = \frac{(x-x_2)(x-x_3)}{(x_1-x_2)(x_1-x_3)}, \quad 一般地 \quad f_i(x) = \prod_{\substack{1\le j\le 3 \\ j\ne i}} \frac{(x-x_j)}{(x_i-x_j)}.$$

第二题而言, $$f(x) = 2\,\frac{(x-1)(x-3)}{3} + \frac{x(x-3)}{-2} + 0$$

$$= \frac{1}{6}x^2 - \frac{7}{6}x + 2$$

3. 令

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \epsilon_0 & \epsilon_1 & \cdots & \epsilon_{n-1} \\ \vdots & \vdots & & \vdots \\ \epsilon_0^{n-1} & \epsilon_1^{n-1} & \cdots & \epsilon_{n-1}^{n-1} \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \epsilon_0^{-1} & \epsilon_1^{-1} & \cdots & \epsilon_{n-1}^{-1} \\ \vdots & \vdots & \ddots & \vdots \\ \epsilon_0^{-(n-1)} & \epsilon_1^{-(n-1)} & \cdots & \epsilon_{n-1}^{-(n-1)} \end{pmatrix}$$

$C = AB = (c_{ij})_{n\times n}$.

$$c_{ij} = (\epsilon_0^{i-1}\ \epsilon_1^{i-1}\ \cdots\ \epsilon_{n-1}^{i-1}) \begin{pmatrix} 1 \\ \epsilon_{j-1}^{-1} \\ \vdots \\ \epsilon_{j-1}^{-(n-1)} \end{pmatrix}$$

$$= \epsilon_0^{i-1} + \epsilon_1^{i-1}\epsilon_{j-1}^{-1} + \cdots + \epsilon_{n-1}^{i-1}\epsilon_{j-1}^{-(n-1)}.$$

$$= \epsilon_0^{i-1} + \epsilon_1^{i-1}\epsilon_1^{-(j-1)} + \cdots + \epsilon_1^{(i-1)(n-1)}\epsilon_1^{-(n-1)(j-1)} = 1 + \epsilon_1^{i-j} + \cdots + \epsilon_1^{(i-j)(n-1)}$$

① $i=j$, $C_{ii} = 1+1+\cdots+1 = n$.

② $i \neq j$, $C_{ij} = \dfrac{1\cdot(1-(\epsilon_1^{i-j})^n)}{1-\epsilon_1^{i-j}} = \dfrac{1-(\epsilon_1^{n})^{i-j}}{1-\epsilon_1^{i-j}} = \dfrac{1-1}{1-\epsilon_1^{i-j}} = 0$

$\Rightarrow AB = nE$

$\Rightarrow A^{-1} = \frac{1}{n} B$

4. 解: $|z_1+z_2|^2 + |z_1-z_2|^2 = (z_1+z_2)(\bar{z}_1+\bar{z}_2) + (z_1-z_2)(\bar{z}_1-\bar{z}_2)$

$= z_1\bar{z}_1 + \cancel{z_1\bar{z}_2} + \cancel{z_2\bar{z}_1} + z_2\bar{z}_2 + z_1\bar{z}_1 - \cancel{z_1\bar{z}_2} - \cancel{z_2\bar{z}_1} + z_2\bar{z}_2$

$= |z_1|^2 + |z_2|^2 + |z_1|^2 + |z_2|^2$

$= 2(|z_1|^2 + |z_2|^2)$

几何意义: 平行四边形四条边的平方和等于两对角线长度的平方和.

5. 法一: $f(\frac{a}{b}) = a_n(\frac{a}{b})^n + \cdots + a_1\frac{a}{b} + a_0 = 0$

$\Rightarrow a_n a^n + a_{n-1}a^{n-1}b + \cdots + a_1 a b^{n-1} + a_0 b^n = 0$

$\Rightarrow a_n a^n = -a_{n-1}a^{n-1}b - \cdots - a_1 a b^{n-1} - a_0 b^n$

$\Rightarrow b \mid a_n a^n$

$\gcd(a,b) \Rightarrow b \mid a_n$.

同理 $a \mid a_0$

法二: 若 $\alpha = \frac{a}{b} \in \mathbb{Q}$ 为 $f(x)=0$ 的根.

$\gcd(b,a)=1 \Rightarrow bx-a$ 是 $\mathbb{Z}[x]$ 中的本原多项式

claim: 设 $f(x)$, $g(x) \in \mathbb{Z}[x]$, 且 $g(x)$ 是 $\mathbb{Z}[x]$ 中的本原多项式. 若 $f(x)=g(x)h(x)$, $h(x) \in \mathbb{Q}[x]$, 则 $h(x) \in \mathbb{Z}[x]$

证. $f(x) = af_1(x)$, $h(x) = c\,h_1(x)$, 其中 $a \in \mathbb{Z}$, $c \in \mathbb{Q}$, $f_1(x)$, $h_1(x)$ 是 $\mathbb{Z}[x]$ 中本原多项式. 于是

$a f_1(x) = g(x)\, c\, h_1(x) = c\, g(x) h_1(x)$

由 Gauss 引理可知, $g(x)h_1(x)$ 仍为 $\mathbb{Z}[x]$ 中的本原多项式

$\Rightarrow c = \pm a \in \mathbb{Z}$,

$\Rightarrow h(x) \in \mathbb{Z}[x]$.

$\Rightarrow f(x) = (bx-a)g(x)$, 其中 $g(x) = g_{n-1}x^{n-1} + \cdots + g_0 \in \mathbb{Z}[x]$

$\Rightarrow a_n = b\cdot g_{n-1}$, $a_0 = -a g_0$.

$\Rightarrow b \mid a_n \quad a \mid a_0$

6. 证明: $A^2=A \Rightarrow A^2-A=0$

令 $f(x)=x(x-1)$, $p(x)=x$, $q(x)=x-1$, 显然 $\gcd(p,q)=1$

$f(A)=0$.

$\Rightarrow rank(A)+rank(A-E)=n$.

核心分解(线性映射版) 设 $A\in Hom(F^n,F^n)$ 非零, $f\in F[t]$ 且 $f(A)=0$. 再设 $f=pq$, 其中 $p,q\in F[t]$. 且 $\gcd(p,q)=1$. 则

$$\ker(p(A))\oplus\ker(q(A))=F^n.$$

$$\xRightarrow{\text{对应维数}} \dim(\ker(p(A)))+\dim(\ker(q(A)))=n.$$

(方程组版) 设 $A\in M_n(F)$, $f\in F[t]$ 且 $f(A)=0$ 再设 $f=pq$, 其中 $p,q\in F[t]$ 且 $\gcd(p,q)=1$. 则

$$Sol(p(A)x=0)\oplus Sol(q(A)x=0)=F^n.$$

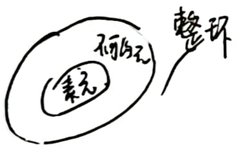
$$\Longrightarrow rank(p(A))+rank(q(A))=n.$$

回顾 唯一因子分解整环

D 是整环

Def. (不可约元). $a\in D^*$ 不可逆, 若 $\exists\, b,c\in D^*$, s.t. $a=bc \Rightarrow b$ 是单位或 c 是单位. 则称 a 是不可约元

(素元) $p\in D^*$ 不可逆, 若对于 $\forall\, a,b\in D^*$, $p\mid ab\Rightarrow p\mid a$ or $p\mid b$. , 则称 p 是素元



唯一因子分解整环 (UFD)

Def (不可约分解). 设 $a\in D^*$ 是不可逆元, 如果存在不可约元 $p_1,\dots,p_n$ 使得 $a=p_1\cdots p_n$.

则称 a 有不可约分解.

Def. (UFD). 如果 D 中每个非零非单位的元素 a 都满足下列两个条件:

(i) a 可以写成 D 中有限多个不可约元素之积 (分解存在性)

(ii) 设 (分解的唯一性)
$a=p_1\cdots p_m=q_1\cdots q_n$,

其中 $p_1,\dots,p_m,q_1,\dots,q_n$ 是 D 中的不可约元, 则 $m=n$ 且适当调整下标后, 我们有

$$p_1\approx q_1,\dots,p_m\approx q_m.$$

UFD 中, 素元 $\Leftrightarrow$ 不可约元

例 域上一元多项式环 $F[x]$.

Prop. 在 UFD 中, 每个非零非可逆元 a 可表示为

$$a=up_1^{m_1}\cdots p_k^{m_k},\quad u\in U_D,\ p_1,\dots,p_k \text{ 是两两互不相伴的不可约元、}$$

$\Downarrow$ 标准不可约分解

无平方部分

设 $f\in F[x]$，则 $\exists!$ 两两不相伴的不可约且首一的多项式 $p_1,p_2,\cdots,p_k\in F[x]$，$m_1,m_2,\cdots,m_k\in \mathbb{Z}^+$，$u\in F^*$，使得

$$f=(\mathrm{lc} f)\, p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}.$$

上述 p_i 称为 f 的 m_i 重因子，$i=1,2,\cdots,k$. 特别地，当 $m_i=1$ 时，p_i 称为单因子. $p_1p_2\cdots p_k$ 称为 f 的无平方部分

注意到 $\gcd(p_i,p_j)=1$，$\forall i\neq j$

计算无平方部分

设 $f=f_nx^n+f_{n-1}x^{n-1}+\cdots+f_1x+f_0\in F[x]$. 定义 f 关于 x 的形式导数：

$$f'=nf_nx^{n-1}+(n-1)f_{n-1}x^{n-2}+\cdots+f_1$$

自行验证：$\forall f,g\in F[x]$.

① $(f+g)'=f'+g'$

② $(fg)'=f'g+fg'$

Thm. 设 F 是特征为 0 的域，$f\in F[x]\setminus F$，则 f 的无平方部分在 F 上与 $f/\gcd(f,f')$ 相伴.

Pf: 不妨设 f 的不可约分解为 $f=p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$.

$$f'=m_1p_1^{m_1-1}p_1'\cdots p_k^{m_k}+\cdots+m_kp_1^{m_1}\cdots p_k^{m_k-1}p_k'$$

$$=\sum_{i=1}^{k}m_i(p_1^{m_1}\cdots p_{i-1}^{m_{i-1}}p_i^{m_i-1}p_i'p_{i+1}^{m_{i+1}}\cdots p_k^{m_k})$$

$$=\underbrace{(p_1^{m_1-1}\cdots p_k^{m_k-1})}_{g}\underbrace{\sum_{i=1}^{k}m_i(p_1\cdots p_{i-1}p_i'p_{i+1}\cdots p_k)}_{h}.$$

$\Rightarrow g\mid f,\quad g\mid f'$

下证 $\gcd(f,h)=1$

假设该结论不成立，则 $\exists i\in\{1,\cdots,k\}$，使得 $p_i\mid h$. 不妨设 $p_1\mid h$.

$\Rightarrow p_1\mid m_1p_1'p_2\cdots p_k$

$\gcd(p_1,p_i)=1$，$i=2,\cdots,k$. 且 m_1 在特征为 0 的域中非零

$\Rightarrow p_1\mid p_1'$

$\Rightarrow \deg(p_1)\le\deg(p_1')\rightarrow\Leftarrow$

$\Rightarrow \gcd(f,h)=1$

$\Rightarrow \gcd(f,f')=g$

$\Rightarrow \dfrac{f}{\gcd(f,f')}\sim p_1\cdots p_k.$

Cor. 设 F 是特征为 0 的域，$f \in F[x] \setminus F$. 则 f 是无平方的 $\Leftrightarrow \gcd(f, f') = 1$

证："$\Rightarrow$" 若 f 无平方，则 $m_1 = \cdots = m_k = 1$,

$$\Rightarrow \gcd(f, f') = p_1^{m_1-1} \cdots p_k^{m_k-1} = 1.$$

"$\Leftarrow$" 若 $\gcd(f, f') = 1$，则 f 与其无平方部分在 F 上相伴，于是 f 是无平方的.

例 计算 $\mathbb{Z}[x]$ 中多项式 $f = x^3 - x^2 - x + 1$ 的无平方部分

$f = x^3 - x^2 - x + 1$, $\quad f' = 3x^2 - 2x - 1$

$$\begin{array}{r|l|l|l}
-\frac{27}{8}x - \frac{9}{8} & 3x^2 - 2x - 1 & x^3 - x^2 - x + 1 & \frac{x}{3} - \frac{1}{9} \\
 & 3x^2 - 3x & x^3 - \frac{2}{3}x^2 - \frac{x}{3} & \\
\hline
 & x - 1 & -\frac{1}{3}x^2 - \frac{2}{3}x + 1 & \\
 & x - 1 & -\frac{1}{3}x^2 + \frac{2}{9}x + \frac{1}{9} & \\
\hline
 & 0 & -\frac{8}{9}x + \frac{8}{9} &
\end{array}$$

$$\Rightarrow \gcd(f, f') = x - 1$$

$$\frac{f}{\gcd(f, f')} = x^2 - 1.$$

例. 设 F 是有限域 $\mathbb{Z}$，令 $p = x^2$，则 $p' = \bar{2}x = \bar{0}$，$\gcd(p, p') = p$，但 p 的无平方部分显然不能是 1.

例 设 $f = x^n + a \in \mathbb{Q}[x]$，其中 $n > 1$，$a \in \mathbb{Q}$. 证明：f 是无平方的当且仅当 $a \neq 0$

证：$f' = nx^{n-1}$. 注意到 $\quad f + \frac{-x}{n} f' = a$.

"$\Rightarrow$" 假设 $a = 0$，由 $n > 1$ 可知 f 有重因子 x 且重数大于 1，故 f 不是无平方的 $\to \Leftarrow$.

$$\Rightarrow a \neq 0$$

"$\Leftarrow$" $a \neq 0$，由 $\underline{\text{Bezout}}$ 关系可知，$\gcd(f, f') = 1$，故 f 是无平方的.

$$\frac{f}{a} + \frac{-x}{na} f' = 1$$

无平方分解

Def. $f \in F[x] \setminus F$，f 是无平方分解表示为

$$f = p_1 p_2^2 \cdots p_k^k.$$

其中 $p_1, \cdots, p_k$ 都是无平方多项式（可能某些 p_i 为 1），且两两互素

记 $f_0 = f$，$f_1 = \gcd(f, f') = p_2 p_3^2 \cdots p_k^{k-1}$.

$$h_1 = \frac{f_0}{f_1} = p_1 p_2 \cdots p_k.$$

$$f_2 = \gcd(f_1, f_1') = p_3 p_4^2 \cdots p_k^{k-2}$$

$$h_2 = \frac{f_1}{f_2} = \frac{p_2 p_3^2 \cdots p_k^{k-1}}{p_3 p_4^2 \cdots p_k^{k-2}} = p_2 p_3 p_4 \cdots p_k.$$

$$\frac{h_1}{h_2}=\frac{p_1p_2\cdots p_k}{p_2p_3\cdots p_k}=p_1$$

......

$$f_{k-2}=p_{k-1}p_k^2$$

$$f_{k-1}=\gcd(f_{k-2},f_{k-2}')=p_k.$$

$$h_{k-1}=\frac{f_{k-2}}{f_{k-1}}=p_{k-1}p_k.$$

$$f_k=\gcd(f_{k-1},f_{k-1}')=1$$

$$h_k=\frac{f_{k-1}}{f_k}=f_{k-1}=p_k.$$

$$\frac{h_{k-1}}{h_k}=p_{k-1}.$$

无平方分解算法.

输入：$f\in F[x]$

输出：$p_1,\cdots,p_k$，无平方多项式且两两互素，使得.

$$f=p_1p_2^2\cdots p_k^k.$$

1.[初始化] 令 $g_1:=\gcd(f,f')$

$h_1:=\frac{f}{g_1}$;

$i:=1$

2.[循环] while $g_i\neq 1$ do

$g_{i+1}:=\gcd(g_i,g_i')$

$h_{i+1}:=\frac{g_i}{g_{i+1}}$;

$p_i:=\frac{h_i}{h_{i+1}}$;

$i:=i+1$;

end do;

3.[处理最后一个因子] $k:=i$; $p_k:=h_k$;

4.[返回] return $p_1,\cdots,p_k$.

例 $f=x^3-x^2-x+1$. 在 $\mathbb{Q}[x]$ 中的无平方分解

解：$f_0=f$, $f'=3x^2-2x-1$

$g_1=\gcd(f,f')=x-1$.

$h_1=\frac{f}{g_1}=x^2-1$

$g_2=\gcd(g_1,g_1')=1$, $h_2=\frac{g_1}{g_2}=x-1$.

$p_1=\frac{h_1}{h_2}=\frac{x^2-1}{x-1}=x+1$.

$p_2=h_2=x-1$.

$\Rightarrow f=(x+1)(x-1)^2$.

中国剩余定理.

(整数版本)

引理 设 $m_1,\cdots,m_k\in\mathbb{Z}^+\setminus\{1\}$ 两两互素，则

(i) $m_1\cdots m_{k-1}$ 与 m_k 互素

(ii) $\operatorname{lcm}(m_1,\cdots,m_k)=m_1\cdots m_k$.

Pf：(i) $\forall i\in\{1,\cdots,k-1\}$, $\gcd(m_i,m_k)=1$,

$\Rightarrow\exists u_i,v_i\in\mathbb{Z}$, s.t $u_im_i+v_im_k=1$. , $i=1,\cdots,k-1$.

k-1 个代子相乘，$1=\prod_{i=1}^{k-1}(u_im_i+v_im_k)=u(m_1\cdots m_{k-1})+vm_k$.

这里 $u=u_1\cdots u_k\in\mathbb{Z}$，$v\in\mathbb{Z}$.

$$\Rightarrow \gcd(m_1,\cdots,m_{k-1},m_k)=1.$$

(ii) 对 k 归纳. 当 $k=2$ 时，$\text{lcm}(m_1,m_2)=\dfrac{m_1m_2}{\gcd(m_1,m_2)}=m_1m_2$.

假设 k-1 时结论成立，令

$$l=\text{lcm}(m_1,m_2,\cdots,m_k)$$

则 l 是 $m_1,\cdots,m_{k-1}$ 的公倍式. 由归纳假设可知 $\text{lcm}(m_1,\cdots,m_{k-1})=m_1\cdots m_{k-1}$.

从而 $m_1\cdots m_{k-1}\mid l$. 又由 $m_k\mid l$.

$$\Rightarrow \text{lcm}(m_1\cdots m_{k-1},m_k)\mid l.$$

由(i)可知 $\gcd(m_1\cdots m_{k-1},m_k)=1$　　k=2 的情形.

$$\Rightarrow \text{lcm}(m_1\cdots m_{k-1},m_k)=m_1\cdots m_{k-1}m_k\mid l.$$

另一方面，$m_1m_2\cdots m_k$ 显然是 $m_1,m_2,\cdots,m_k$ 的公倍式，故 $l\mid m_1\cdots m_{k-1}m_k$.

$$\Rightarrow l=m_1\cdots m_k.$$

Thm. 设 $m_1,\cdots,m_k\in\mathbb{Z}^+\setminus\{1\}$ 两两互素，$r_1,\cdots,r_k\in\mathbb{Z}$. 则存在唯一的 $r\in\mathbb{N}$ 满足

$$\begin{cases} r\equiv r_1 \mod m_1\\ r\equiv r_2 \mod m_2\\ \quad\vdots\\ r\equiv r_k \mod m_k\end{cases}\qquad (*)$$

且 $r<m_1\cdots m_k$.

Pf: (存在性) 对 k 归纳. 当 $k=1$ 时，取 $r=\text{rem}(r_1,m_1)$. 即可.

设 x' 满足 $x'\equiv r_1 \mod m_1,\cdots,x'\equiv r_{k-1}\mod m_{k-1}$

由引理知，$\exists u,v\in\mathbb{Z}$, s.t

$$u(m_1\cdots m_{k-1})+vm_k=1 \quad \text{引理 (ii)} \quad ①$$

令 $x=x'+u(m_1\cdots m_{k-1})(r_k-x')$

则 $x\equiv r_i \mod m_i$，$i=1,2,\cdots,k-1$.

由 ①可得 $x=x'+(1-vm_k)(r_k-x')=r_k-vm_k(r_k-x')$.

$$\Rightarrow x\equiv r_k \mod m_k.$$

7

再令 $r=\text{rem}(x,m_1\cdots m_k)$，则 $0\le r<m_1\cdots m_{k-1}m_k$ 且 r 满足定理中的同余关系.

(唯一性) 设 $\tilde{r}$ 也满足定理中同余关系且 $0\le \tilde{r} < m_1\cdots m_{k-1}m_k$，不妨设 $r\ge\tilde{r}$，则

$r-\tilde{r}\equiv 0 \mod m_i$，$i=1,2,\cdots,k-1,k$.

$\Rightarrow$ $r-\tilde{r}$ 是 $m_1,\cdots,m_{k-1},m_k$ 的公倍式，且 $0\le r-\tilde{r} < m_1\cdots m_{k-1}m_k$.

$\Rightarrow$ $r=\tilde{r}$ (引理(ii))

例 有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二. 问物几何.

解：求解同余方程组
$$\begin{cases} x\equiv 2 \mod 3 \\ x\equiv 3 \mod 5 \\ x\equiv 2 \mod 7 \end{cases}$$

$m_1=3$, $m_2=5$, $m_3=7$. $r_1=2$, $r_2=3$, $r_3=2$.

$x_1=r_1=2$, $2\cdot 3-5=1$ $\Rightarrow$ $u_1=2$.

$x_2=r_1+u_1m_1(r_2-x_1)=2+2\cdot 3\cdot(3-2)=8$.

$1\cdot(3\cdot 5)-2\cdot 7=1$, $u_2=1$

$x_3=x_2+u_2(m_1\cdot m_2)(r_3-x_2)=-82$.

$\Rightarrow$ $r=\mathrm{rem}(-82, 3\cdot 5\cdot 7)=23$.

环同态观点

$$\begin{tikzcd} & \mathbb{Z} \arrow[dl, "\pi_{m_1}"'] \arrow[d, "\pi_{m_2}"] \arrow[dr, bend left, "\pi_{m_k}"] & \\ \mathbb{Z}_{m_1} & \mathbb{Z}_{m_2} \quad \cdots & \mathbb{Z}_{m_k} \end{tikzcd}$$

当 $m_1,m_2,\cdots,m_k$ 互素时，$\forall\ \bar{r}_1\in\mathbb{Z}_{m_1},\cdots,\bar{r}_k\in\mathbb{Z}_{m_k}$，$\exists\, x\in\mathbb{Z}$ 是 $\bar{r}_1\in\mathbb{Z}_{m_1},\cdots,\bar{r}_k\in\mathbb{Z}_{m_k}$ 关于自然投射 $\pi_{m_1},\cdots,\pi_{m_k}$ 的公共原像.