§3. 同余理论及其环论解释

$15 \div 7 = 2 \cdots\cdots ①$

§3.1 同余式

为了便于余数的计算，我们引入同余号 "$\equiv$"

定义：$m \in \mathbb{N}_+$，若 $m \mid a-b$，则称 a 与 b 模 m 同余 (congruent modulo m)

记作 $a \equiv b \bmod m$. 否则记作 $a \not\equiv b \bmod m$.

例：$a \equiv \begin{cases} 0 \bmod 2 & 2 \mid a \ (\text{偶数}) \\ 1 \bmod 2 & 2 \nmid a \ (\text{奇数}) \end{cases}$

同余的基本性质

性质：1). 同余为 $\mathbb{Z}$ 上的等价关系，即

- 自反性：$a \equiv a \bmod m \quad (\forall a)$
- 对称性：$a \equiv b \bmod m \Rightarrow b \equiv a \bmod m$
- 传递性：$a \equiv b \bmod m \ \& \ b \equiv c \bmod m \Rightarrow a \equiv c \bmod m$

2). $\left.\begin{array}{l} a \equiv b \bmod m \\ c \equiv d \bmod m \end{array}\right\} \Rightarrow \begin{cases} a \pm c \equiv b \pm d \bmod m \\ a \cdot c \equiv b \cdot d \bmod m \end{cases}$

3). 若 $a_i \equiv b_i \bmod m \ (\forall i = 1, \cdots, n)$，则对任意整系数多项式 $f(x_1, \cdots, x_n)$，我们有

$$f(a_1, \cdots, a_n) \equiv f(b_1, \cdots, b_n) \bmod m.$$

4). $a \equiv b \bmod m \ \& \ d \mid m \Rightarrow a \equiv b \bmod d$

5). $a \equiv b \bmod m \overset{d \neq 0}{\Longleftrightarrow} da \equiv db \bmod dm$

6). $a \equiv b \bmod m_i \ (i = 1, \cdots, n) \Longleftrightarrow a \equiv b \bmod \operatorname{lcm}(m_1, \cdots, m_n)$

7). $ac \equiv bc \bmod m \Rightarrow a \equiv b \bmod \dfrac{m}{\gcd(m, c)}$

特别地，若 m 与 c 互素，则 $ac \equiv bc \bmod m \Rightarrow a \equiv b \bmod m$.

Pf: (1) 自反性: $m \mid 0 = a-a \Rightarrow a \equiv a \bmod m$

对称性: $a \equiv b \bmod m \Rightarrow m \mid a-b \Rightarrow m \mid b-a \Rightarrow b \equiv a \bmod m$.

传递性: $\left.\begin{array}{l} a \equiv b \bmod m \Rightarrow m \mid (a-b) \\ b \equiv c \bmod m \Rightarrow m \mid (b-c) \end{array}\right\} \Rightarrow m \mid (a-b)+(b-c) = a-c$

$\Rightarrow a \equiv c \bmod m$.

(2). $\left.\begin{array}{l} a \equiv b \bmod m \Rightarrow m \mid a-b \\ c \equiv d \bmod m \Rightarrow m \mid c-d \end{array}\right\}$

$\Rightarrow \begin{cases} m \mid (a-b) \pm (c-d) = (a \pm c) - (b \pm d) \Rightarrow a \pm c \equiv b \pm d \bmod m. \\ m \mid (a-b)c + (c-d)b = ac - bd \Rightarrow ac \equiv bd \bmod m. \end{cases}$

(3). 由(2)的第2条知于为单项式 $a x_1^{i_1} \cdots x_n^{i_n}$ 时 结论成立.

由(1)的第一条知 对一般的多项式均成立.

(4). $\left.\begin{array}{l} a \equiv b \bmod m \Rightarrow m \mid a-b \\ d \mid m \end{array}\right\} \Rightarrow d \mid a-b \Rightarrow a \equiv b \bmod d.$

(5). $a \equiv b \bmod m \overset{\text{def}}{\Leftrightarrow} m \mid a-b \overset{d \neq 0}{\Leftrightarrow} dm \mid d(a-b) = da-db \overset{\text{def}}{\Leftrightarrow} da \equiv db \bmod dm.$

(6). $\Leftarrow$): $a \equiv b \bmod lcm(m_1, \cdots, m_n) \xrightarrow[(4)]{m_i \mid lcm(m_1 \cdots m_n)} a \equiv b \bmod m_i \quad (\forall i)$

$\Rightarrow$): $a \equiv b \bmod m_i \ (\forall i) \Rightarrow m_i \mid a-b \ (\forall i)$

$\Rightarrow lcm(m_1, \cdots, m_n) \mid a-b$

$\Rightarrow a \equiv b \bmod lcm(m_1, \cdots, m_n)$

(7). $ac \equiv bc \bmod m \Rightarrow m \mid c(a-b) \Rightarrow \frac{m}{gcd(m,c)} \mid \frac{c}{gcd(m,c)} \cdot (a-b)$

$\xrightarrow{gcd\left(\frac{m}{gcd(m,c)}, \frac{c}{gcd(m,c)}\right) = 1} \frac{m}{gcd(m,c)} \mid a-b \Rightarrow a \equiv b \bmod \frac{m}{gcd(m,c)}$

例: 一个正整数模9同余于其所有数位上的数之和.

eg. $57863 \equiv 5+7+8+6+3 = 29 \equiv 2+9 = 11 \equiv 1+1 = 2 \bmod 9$

§3.2. 同余方程(组).

定义 (同余类): $\forall r\in\mathbb{Z}$, 称 $\mathbb{Z}$ 的子集

$$[r] := r+m\mathbb{Z} := \{\cdots, r-2m, r-m, r, r+m, r+2m, \cdots\} = \{r+km \mid k\in\mathbb{Z}\}$$

为 r 所在的 模 m 的同余类, 也记作 $\bar{r}$. 称 r 为 $[r]$ 的一个代表.

注: 1). $a\equiv b \bmod m \Leftrightarrow [a]=[b]$

2). $a\not\equiv b \bmod m \Leftrightarrow [a]\cap[b]=\phi$.

3). $\mathbb{Z} = [0]\sqcup[1]\sqcup\cdots\sqcup[m-1]$ …… 无交并.

同余方程:

定理: $ax\equiv b \bmod m$ 有解 $\Leftrightarrow \gcd(a,m)\mid b$. 且此时, 解集为 模 $\frac{m}{\gcd(a,m)}$ 的一个同余类, 也为 $\gcd(m,c)$ 个模 m 的同余类的并

特别地 $ax\equiv 1 \bmod m$ 有解 $\Leftrightarrow \gcd(a,m)=1$.

Pf: (1) 记 $d=\gcd(a,b)$

$\Rightarrow$: $ax\equiv b \bmod m$ 有解 $\Rightarrow \exists c$ s.t. $b\equiv ac \bmod m$

$\Rightarrow b\equiv ac \bmod d \Rightarrow b\equiv 0 \bmod d \Rightarrow d\mid b$

($\Rightarrow \exists c,e$ s.t. $ac-b=me \Rightarrow b=ac-me \Rightarrow d\mid b$)

$\Leftarrow$: 设 $d=ax'+my'$ $(x',y'\in\mathbb{Z})$.

$\Rightarrow b=a\cdot(\frac{b}{d}x')+m(\frac{b}{d}y')$ $(\frac{b}{d}x', \frac{b}{d}y'\in\mathbb{Z})$

$\Rightarrow x=\frac{b}{d}x'$ 为同余方程的解.

(2). 设 x_0 为 $ax\equiv b \bmod m$ 的一个解. 即 $ax_0\equiv b \bmod m$.

$ax\equiv b \bmod m \Leftrightarrow ax\equiv ax_0 \bmod m$

$\overset{(7)}{\Leftrightarrow} x\equiv x_0 \bmod \frac{m}{\gcd(a,m)} \Leftrightarrow x\in[x_0]=x_0+\frac{m}{\gcd(a,m)}\cdot\mathbb{Z}$

例：$24x \equiv 7 \bmod 59$

	59	1	0
2	24	0	1
2	11	1	-2
5	2	-2	5
	1	11	-27

解：由欧氏算法可得 $\gcd(24,59)=1$ 且

$1 = 11\times 59 - 27\times 24.$

$\Rightarrow -27\times 24 \equiv 1 \bmod 59 \Rightarrow 24\times(-27\times 7) \equiv 7 \bmod 59$

$\Rightarrow x \equiv -27\times 7 = 47 \bmod 59$

例：$15x \equiv 9 \bmod 21 \Rightarrow 5x \equiv 3 \bmod 7 \Rightarrow x \equiv 5^{-1}\times 3 = 9 \bmod 7 = 2 \bmod 7$

解：$\gcd(15,21) = 3 = -2\times 21 + 3\times 15$ (由欧氏算法得)

	21	1	0
1	15	0	1
2	6	1	-1
	3	-2	3

$\Rightarrow 9 = 3\times 3 = 3\times(-2\times 21 + 3\times 15) \equiv 15\times 9 \bmod 21$

$\Rightarrow x \equiv 9 \bmod \frac{21}{3} = 2 \bmod 7$

同余方程组.

定理(中国剩余定理)：设 $m = m_1 m_2 \cdots m_n$，其中 $m_1, \cdots, m_n \in \mathbb{N}$ 两两互素，$a_1, \cdots, a_n \in \mathbb{Z}$.

则方程组 $\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \\ \vdots \\ x \equiv a_n \bmod m_n \end{cases}$ 有解，且解集为模 m 的一个同余类.

Pf：(1) 记 $\hat{m}_i = m_1 \cdots m_{i-1} m_{i+1} \cdots m_n$. 则 $\gcd(m_i, \hat{m}_i) = 1$.

$\Rightarrow \exists\, b_i \in \mathbb{Z}$ s.t. $\hat{m}_i b_i \equiv 1 \bmod m_i$

$\Rightarrow \hat{m}_i b_i a_i \equiv \begin{cases} a_i \bmod m_i \\ 0 \bmod m_j \quad (j \neq i) \end{cases}$

令 $x_0 = \sum_{i=1}^{n} \hat{m}_i b_i a_i$ 则 $\forall\, j = 1, \cdots, n$.

$x_0 \equiv \sum_{i=1}^{n} \hat{m}_i b_i a_i \equiv \hat{m}_j b_j a_j \equiv a_j \bmod m_j \quad \forall (j)$

因此方程有解.

b). $x \equiv a_i \pmod{m_i}\ \forall i \Leftrightarrow x \equiv x_0 \pmod{m_i}\ \forall i$

$\Leftrightarrow m_i \mid x - x_0 \quad \forall i$

$\Leftrightarrow m = \operatorname{lcm}(m_1, \cdots, m_n) \mid x - x_0$

$\Leftrightarrow x \equiv x_0 \bmod m.$

因此，解集为模 m 的一个同余类.

例 (孙子算经):

三三数之余二
五五数之余三
七七数之余二
问物几何？

三人同行七十稀
五树梅花廿一枝
七子团圆正半月
除百零五便得知.

$$\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 5 \\ x \equiv 2 \bmod 7 \end{cases}$$

$x = ?$

$M_1 = 2 \cdot 5 \cdot 7 = 70$

$M_2 = 3 \times 7 = 21$

$M_3 = 3 \times 5 = 15$

$70 \times 2 + 21 \times 3 + 15 \times 2 \equiv 23 \bmod 105$

§3.3. 欧拉定理与费马小定理.

设 m 为正整数. 记 $\varphi(m)$ 为 $\{0,1,\cdots,m-1\}$ 中与 m 互素的数的个数. 函数 $\varphi: m \mapsto \varphi(m)$ 称为 **欧拉函数**.

e.g. $\varphi(1)=1,\ \varphi(2)=1,\ \varphi(3)=2,\ \varphi(4)=2,\ \varphi(5)=4,\ \varphi(6)=2,\cdots$

定理 (欧拉): 若 $(a,m)=1$, 则 $a^{\varphi(m)} \equiv 1 \bmod m$.

Pf: 考虑集合 $\Sigma = \{ i \mid 0 \le i < m \text{ 且 } \gcd(i,m)=1 \}$. 则

- $\forall i \in \Sigma$, $\exists!\ q_i, r_i$ s.t. $ai \equiv mq_i + r_i$ $0 \le i < m$.
- $\gcd(ai,m)=1 \Rightarrow \gcd(r_i,m)=1 \Rightarrow r_i \in \Sigma$

$\Rightarrow$ 自映射 $\lambda: \Sigma \to \Sigma$, $i \mapsto r_i$

断言: λ 为双射. (仅需证明单性)

单: $r_i = r_j \Rightarrow ai \equiv aj \bmod m \Rightarrow i \equiv j \bmod m \Rightarrow i = j$.

于是: $\prod_{i\in\Sigma} (ai) \equiv \prod_{i\in\Sigma} r_i \equiv \prod_{i\in\Sigma} i \bmod m$

另一方面: $\prod_{i\in\Sigma} (ai) \equiv a^{\varphi(m)} \cdot \prod_{i\in\Sigma} i \bmod m$

于是 $a^{\varphi(m)} \equiv 1 \bmod m$. ($\prod_{i\in\Sigma} i$ 与 m 互素).

推论 (费马): 若 p 为素数, 则对任意 $a \in \mathbb{Z}$ 有 $a^p \equiv a \bmod p$.

Pf: · $p \nmid a$: 欧拉定理 $\Rightarrow a^{p-1} \equiv 1 \bmod p \Rightarrow a^p \equiv a \bmod p$

$p \mid a$: $a^p \equiv 0 \equiv a \bmod p$.

§3.4 环 $\mathbb{Z}/m\mathbb{Z}$

$$[r] = m\mathbb{Z}+r = \{mk+r \mid k\in\mathbb{Z}\}$$

$$\Rightarrow \quad \mathbb{Z} = [0] \sqcup [1] \sqcup \cdots \sqcup [m-1]$$

$$\mathbb{Z}/m\mathbb{Z} := \{[0], [1], \cdots, [m-1]\}$$ 由 m 个同余类组成的集合.

e.g. $\mathbb{Z}/2\mathbb{Z} = \{$偶数集, 奇数集$\}$

在 $\mathbb{Z}/m\mathbb{Z}$ 上可定义如下两个二元运算:

$$[a]+[b] := [a+b]$$

$$[a]\cdot[b] := [ab]$$

上述运算是良定义的.

$$\begin{array}{ccc} [a]+[b] := [a+b] & & [a]\cdot[b] := [a\cdot b] \\ \| \quad \| \quad\quad \| ? & & \| \quad \| \quad\quad \| \\ [a']+[b'] := [a'+b'] & & [a']\cdot[b'] := [a'\cdot b'] \end{array}$$

$$\left.\begin{array}{l} [a]=[a'] \Leftrightarrow a\equiv a' \bmod m \\ [b]=[b] \Leftrightarrow b\equiv b' \bmod m \end{array}\right\} \Rightarrow \begin{cases} a+b\equiv a'+b' \bmod m \Leftrightarrow [a+b]=[a'+b'] \\ a\cdot b\equiv a'b' \bmod m \Leftrightarrow [a\cdot b]=[a'\cdot b'] \end{cases}$$

定理: $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ 构成 m 元交换环.

证明: 直接验证

1). $+, \cdot$ 满足交换律, 结合律和分配律

2). $[0]$ 为 $+$ 单位元, $[-a]$ 为 $[a]$ 的负元

3). $[1]$ 为 $\cdot$ 单位元.

$\mathbb{Z}/m\mathbb{Z}$ 的单位群有如下刻画：

定理：$(\mathbb{Z}/m\mathbb{Z})^\times = \{ [a] \mid \gcd(a,m)=1,\ 0 \le a < m \}$

特别地 $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times|$.

Pf: $[a] \in (\mathbb{Z}/m\mathbb{Z})^\times \Leftrightarrow \exists b \in \mathbb{Z}$ s.t. $[a][b]=[1]$

$\Leftrightarrow \exists b \in \mathbb{Z}$ s.t. $ab \equiv 1 \bmod m$

$\Leftrightarrow ax \equiv 1 \bmod m$ 有解

$\Leftrightarrow \gcd(a,m)=1$.

定理：p 素 $\Rightarrow$ $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ 为 p 元有限域

↖ p 元素数域

Pf: $\mathbb{F}_p$ 为(非零)交换环，且任意非零元可逆. □

引理：设 $R_1, R_2, \cdots, R_n$ 为 n 个环，在笛卡儿集

$$R = R_1 \times R_2 \times \cdots \times R_n = \{(r_1, r_2, \cdots, r_n) \mid r_i \in R_i\}$$

上我们定义运算：

$$(r_1, r_2, \cdots, r_n) + (r_1', r_2', \cdots, r_n') := (r_1+r_1', r_2+r_2', \cdots, r_n+r_n')$$

$$(r_1, r_2, \cdots, r_n) \cdot (r_1', r_2', \cdots, r_n') := (r_1 r_1', r_2 r_2', \cdots, r_n r_n')$$

$(R, +, \cdot)$ 构成环，其中

$$0_R = (0_{R_1}, 0_{R_2}, \cdots, 0_{R_n})$$

$$1_R = (1_{R_1}, 1_{R_2}, \cdots, 1_{R_n})$$

$$-(r_1, r_2, \cdots, r_n) = (-r_1, -r_2, \cdots, -r_n)$$

§3.5 群元素的阶.

$(G,\cdot)$ = 群. $\forall g\in G$. $g^m := \begin{cases} \underbrace{gg\cdots g}_{m} & m>0 \\ 1 & m=0 \\ \underbrace{g^{-1}\cdots g^{-1}}_{-m} & m<0 \end{cases}$

定义: 设 $g\in G$. 若存在 $n\in\mathbb{N}_+$ 使得 $g^n=1$, 则称 满足 $g^n=1$ 的最小的正整数 n 为 g 的阶 (order), 记作 $ord(g)$ 或 $o(g)$.
若上述 n 不存在, 则称 g 为阶为无限. 记作 $ord(g)=\infty$. (或 $o(g)=\infty$)

注: $o(g)=1 \Leftrightarrow g=1_G$

引理: 若 $ord(g)=k<\infty$. 则 1) $g^n=1 \Leftrightarrow n\equiv 0 \bmod k$ $(k\mid n)$

2) $g^i=g^j \Leftrightarrow i\equiv j \bmod k$ $(k\mid i-j)$

3) $\{1,g,\cdots,g^{k-1}\}$ 为包含 g 的最小子群.

若 $ord(g)=\infty$, 则 $\forall i\neq j$, 均有 $g^i\neq g^j$.

证(1): $\forall n=kq+r$ $0\le r<k$

$g^n=1 \Leftrightarrow g^r=1$ $(0\le r<k)$ $\overset{ord(g)=k}{\Longleftrightarrow}$ $r=0 \Leftrightarrow k\mid n$

(2): $g^i=g^j \Leftrightarrow g^{i-j}=1 \overset{(1)}{\Leftrightarrow} k\mid i-j$

(3): 若 $H\ni g$ 为子群包含 g, 则 $\forall i\ge 1$, $g^i\in H$ & $e=g^0\in H \Rightarrow \{1,g,\cdots,g^{k-1}\}\subseteq H$

仅需证明 $\{1,g,\cdots,g^{k-1}\}$ 为子群. 由 2) 易知, 其关于乘法和取逆封闭.

(4) 反证: 若 $i\neq j$ 且 $g^i=g^j$. 不妨设 $j>i$. 则

$g^{j-i}=1 \Rightarrow ord(g)\neq\infty$ ↯.

定理：设G为有限群，则 $\forall g\in G,\ \mathrm{ord}(g)<\infty$ 且 $\mathrm{ord}(g)\mid |G|$.

证：$\forall x\in G$ 考察子集 $H_x:=\{g^i\cdot x \mid i\in\mathbb{Z}\}\subseteq G$.

(1) $|G|<\infty\Rightarrow |H_x|<\infty\Rightarrow \exists i<j$ s.t. $g^i=g^j\Rightarrow g^{j-i}=1\Rightarrow \mathrm{ord}(g)<\infty$.

(2) 记 $d=\mathrm{ord}(g)$. 则 $g^i=g^j\Leftrightarrow i\equiv j\pmod d$. 因此

$$H:=H_{1_G}=\{1,g,\cdots,g^{d-1}\}$$

- $\varphi_x: H\xrightarrow{1:1} H_x$ 为双射 $\quad g^i\mapsto g^i\cdot x$ （$g^ix=g^jx\Rightarrow g^i=g^j$，$\Rightarrow \varphi_x=$单）
- $H_x\cap H_y\neq\phi\Leftrightarrow H_x=H_y$ （$\Leftarrow$：√. $\Rightarrow$：设 $g^ix=g^jy$. 则 $g^kx=g^{k-i}\cdot g^ix=g^{k-i+j}y\in H_y$. $\Rightarrow H_x\subseteq H_y$；类似地，$H_y\subseteq H_x$）

$\Rightarrow |G|$ 为 $|H|=\mathrm{ord}(g)$ 的倍数 □

§3.5 环论及群论解释.

同余方程：环 $\mathbb{Z}/m\mathbb{Z}$ 上的一元一次方程 $ax=b$ 其中 $a,b\in\mathbb{Z}/m\mathbb{Z}$.

群同态 $\varphi_a:\mathbb{Z}/m\mathbb{Z}\xrightarrow{a}\mathbb{Z}/m\mathbb{Z}$, $x\mapsto ax$

$\operatorname{im}(\varphi_a)=\gcd(a,m)\cdot\mathbb{Z}/m\mathbb{Z}$

$\ker(\varphi_a)=\frac{m}{\gcd(a,m)}\mathbb{Z}/m\mathbb{Z}$

$$\#\varphi_a^{-1}(b)=\begin{cases}\#\ker(\varphi_a) & b\in\operatorname{im}(\varphi_a)\\ 0 & b\notin\operatorname{im}(\varphi_a)\end{cases}$$

中国剩余定理：$\varphi:\mathbb{Z}/m\mathbb{Z}\xrightarrow{\sim}\mathbb{Z}/m_1\mathbb{Z}\times\mathbb{Z}/m_2\mathbb{Z}\times\cdots\times\mathbb{Z}/m_n\mathbb{Z}$ 为环同构.

$$\bar{r}\mapsto(\bar{r},\ \bar{r},\ \ldots,\ \bar{r})$$

pf: $\forall\bar{r}\in\ker\varphi\Rightarrow r\in m_1\mathbb{Z}\cap m_2\mathbb{Z}\cap\cdots\cap m_n\mathbb{Z}=m\mathbb{Z}\Rightarrow\bar{r}=0\in\mathbb{Z}/m\mathbb{Z}$

$\Rightarrow\varphi=$单

$\#\mathbb{Z}/m\mathbb{Z}=\#(\mathbb{Z}/m_1\mathbb{Z}\times\cdots\times\mathbb{Z}/m_n\mathbb{Z})$ $\Rightarrow\varphi$ 为双射 $\Rightarrow\varphi$ 为同构.

推论：设 $m_1,\ldots,m_n$ 两两互素. 则

(1) $(\mathbb{Z}/m_1\cdots m_n\mathbb{Z})^\times\simeq(\mathbb{Z}/m_1\mathbb{Z})^\times\times\cdots\times(\mathbb{Z}/m_n\mathbb{Z})^\times$ ····(groups)

(2) $\varphi(m_1\cdots m_n)=\varphi(m_1)\cdot\varphi(m_2)\cdot\cdots\cdot\varphi(m_n)$

(3) $\varphi(p_1^{\alpha_1}\cdots p_s^{\alpha_s})=p_1^{\alpha_1-1}(p_1-1)\cdots p_s^{\alpha_s-1}(p_s-1)$

欧拉定理：$a\bmod m\in(\mathbb{Z}/m\mathbb{Z})^\times$ 的阶整除 $(\mathbb{Z}/m\mathbb{Z})^\times$ 的阶

费马定理：$x^p=x$ 在 $\mathbb{F}_p$ 中的解集为全集. 特别地.

$$x^p-x=x(x-1)\cdots(x-(p-1)).$$ (看成 $\mathbb{F}_p$ 上的多项式)