信息安全中的数学基础

张宗洋
zongyangzhang@buaa.edu.cn
电子信息工程学院

本课件基于西安电子科技大学许春香教授课件制作

第六章 同余式

第六章 同余式

6.1 剩余系（掌握）

6.2 同余式概念与一次同余式（熟练）

6.3 中国剩余定理（熟练）

6.4 素数模同余式（掌握）

6.1 剩余系

设m是正整数，模m同余的全体整数是一个模m剩余类，即可表示为

$a = qm+r$， $0 \leq r < m$，$q = 0$，± 1，± 2，…，

的整数是一个模m剩余类

剩余类中的每个数都称为该类的代表

r称为该类的最小非负剩余

模m剩余类共有m个

剩余系

例6-1　全部模8的剩余类为

{0，±8，±2×8，±3×8，…},

{1，1±8，1±2×8，1±3×8，…},

{2，2±8，2±2×8，2±3×8，…},

…

{7，7±8，7±2×8，7±3×8，…}.

在数轴上，一个剩余类做任意整数间隔的平移仍然是一个剩余类，或是另一个剩余类，或是它自己.

剩余类性质

设m是一个正整数,对任意整数a,令

$$C_a = \{c \mid a \equiv c \pmod{m}, c \in Z\}$$

因$a \in C_a$,所以$C_a \neq \phi$.

定理 设m是一个正整数,则

(i) 任一整数必包含在一个C_r中,$0 \le r \le m-1$;

(ii) $C_a = C_b \Leftrightarrow a \equiv b \pmod{m}$;

(iii) $C_a \cap C_b = \phi \Leftrightarrow a \not\equiv b \pmod{m}$;

证 (i) 设a为任一整数, 由欧几里得除法,有

$$a = mq + r, \qquad 0 \le r < m$$

因此 $r \equiv a \pmod{m}$,于是$a \in C_r$.

(ii) 设$C_a = C_b$,则$a \in C_a = C_b$, 于是$a \equiv b \pmod{m}$.

反之(从右到左), 设$a \equiv b \pmod{m}$. 对任意$c \in C_a$,则

$$a \equiv c \pmod{m}$$

于是$b \equiv c \pmod{m}$, 所以$c \in C_b$, 故$C_a \subset C_b$.

同理可证$C_b \subset C_a$. 从而$C_a = C_b$.

(iii) 由(ii)即得必要性. 下证充分性.

（反证法）设$a \not\equiv b \pmod{m}$. 若$C_a \cap C_b \neq \phi$,

则有$c \in C_a, c \in C_b$, 于是有

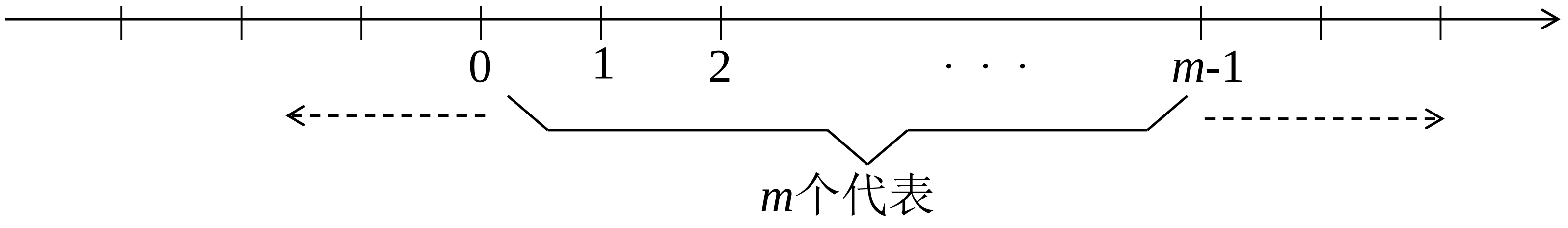
$$a \equiv c \pmod{m} \text{ 及 } b \equiv c \pmod{m}$$

从而$a \equiv b \pmod{m}$, 与假设矛盾.故$C_a \cap C_b = \phi$.

剩余系

定义6-1 从模m剩余类中各取一个代表，则称这些代表的集合为模m的一个完全剩余系.

显然一个完全剩余系在数轴上的任意整数间隔的平移都是一个完全剩余系：



剩余系

定义6-2 {0，1，2，…，m–1}称为模m的最小非负完全剩余系．当m是偶数时，

$\{-\frac{m}{2}, -\frac{m}{2}+1, \ldots, -1, 0, 1, \ldots, \frac{m}{2}-1\}$

或

$\{-\frac{m}{2}+1, \ldots, -1, 0, 1, \ldots, -1, \frac{m}{2}-1, \frac{m}{2}\}$

称为模m的绝对值最小完全剩余系．

当m是奇数时，

$\{-\frac{m-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-1}{2}\}$

称为模m的绝对值最小完全剩余系．

剩余系

例6-4　1）模32的最小非负完全剩余系：

{0，1，2，…，31}.

2）模32的绝对值最小完全剩余系：

{–16，–15，…，–1，0，1，…，14，15}

或

{–15，–14，…，–1，0，1，…，15，16}.

3）模31的绝对值最小完全剩余系：

{–15，–14，…，–1，0，1，…，14，15}.

剩余系

定理6-1 设a是一个整数且$(a, m)=1$，b是任意整数. 如果x遍历模m的一个完全剩余系，则$ax+b$也遍历模m的完全剩余系.

即如果

$$\{x_0, x_1, \ldots, x_{m-1}\}$$

是模m的一个完全剩余系，则

$$\{ax_0+b, ax_1+b, \ldots, ax_{m-1}+b\}$$

也是模m的完全剩余系.

剩余系

证明　只需证明$\{ax_0+b，ax_1+b，…，ax_{m-1}+b\}$两两不同余就行了．用反证法．

假设　　　$ax_i+b \equiv ax_j+b \pmod{m}$，其中$i\neq j$，

则　　　　　$ax_i \equiv ax_j \pmod{m}$，

因为$(a，m)=1$，于是

$$x_i \equiv x_j \pmod{m},$$

这与$\{x_0，x_1，…，x_{m-1}\}$

是模m的一个完全剩余系相矛盾，故定理证得．

剩余系

定理6-2　如果x_1，x_2分别遍历模m_1和模m_2的完全剩余系，且$(m_1, m_2) = 1$，则$m_2x_1+ m_1x_2$遍历模m_1m_2的完全剩余系.

证明　当x_1，x_2分别遍历模m_1和模m_2的完全剩余系时，$m_2x_1+ m_1x_2$遍历m_1m_2个整数．现在证明这m_1m_2个整数两两不同余就行了．用反证法.

假设x_1，y_1 模m_1不同余，或x_2，y_2 模m_2不同余，但

$$m_2x_1+ m_1x_2 \equiv m_2y_1+ m_1y_2 \pmod{m_1m_2}$$

$$m_2x_1+ m_1x_2 \equiv m_2y_1+ m_1y_2 \pmod{m_1}$$

则　$m_2x_1 \equiv m_2y_1 \pmod{m_1}$

由　$(m_1, m_2) = 1$，得$x_1 \equiv y_1 \pmod{m_1}$

同理得$x_2 \equiv y_2 \pmod{m_2}$.结果矛盾，故定理得证.

剩余系

定义6-3 如果一个模m的剩余类里面的数与m互素，则称它为与模m互素的剩余类．从与模m互素的每个剩余类中各取一个数构成的集合称为模m的一个简化剩余系.

例6-5 模16的2个简化剩余系为：(模m的一个简化剩余系含有$\varphi(m)$个元素)

{1，3，5，7，9，11，13，15}

{17，19，21，23，25，27，29，31}

定理：设r_1,r_2是同一模m剩余类的两个剩余

则$(r_1,m)=1$ 当且仅当 $(r_2,m)=1$.

欧拉函数

定义：设m是正整数，则比m小且于m互素的正整数个数，记作φ(m)，叫做欧拉函数。

例：m=10， φ(m)=4. (1，3，5，7)

定理：设$m=p^{\alpha}$,则$\varphi(m)=p^{\alpha-1}(p-1)$.

$$
\begin{array}{cccc}
1, & \cdots & p-1 & p \\
p+1, & \cdots & p+p-1 & 2p \\
2p+1, & \cdots & 2p+p-1 & 3p \\
\vdots & \vdots & \vdots & \vdots \\
(p^{\alpha-1}-1)p+1 & & (p^{\alpha-1}-1)p+p-1 & p^{\alpha}
\end{array}
$$

简化剩余系

定理6-3　设a是一个整数且$(a, m)=1$．如果x遍历模m的一个简化剩余系，则ax也遍历模m的简化剩余系．即如果

$$\{x_0, x_1, \ldots, x_{\varphi(m)-1}\}$$

是模m的一个简化剩余系，则

$$\{ax_0, ax_1, \ldots, ax_{\varphi(m)-1}\}$$

也是模m的简化剩余系．

简化剩余系

证明　显然ax遍历$\varphi(m)$个整数．由于$(a，m)=1$和$(x，m)=1$，则$(ax，m)=1$．

现在证明$\{ax_0，ax_1，\ldots，ax_{\varphi(m)-1}\}$两两不同余．

用反证法．假设

$$ax_i \equiv ax_j \pmod{m}，其中 i\neq j，$$

因为$(a，m)=1$，于是

$$x_i \equiv x_j \pmod{m}，$$

这与$\{x_0，x_1，\ldots，x_{\varphi(m)-1}\}$是模$m$的一个简化剩余系相矛盾，故定理证得．

简化剩余系

定理6-4　如果x_1，x_2分别遍历模m_1和模m_2的简化剩余系，且$(m_1, m_2) = 1$，则$m_2x_1 + m_1x_2$遍历模m_1m_2的简化剩余系.

证明　当x_1，x_2分别遍历模m_1和模m_2的完全剩余系时，$m_2x_1 + m_1x_2$遍历模m_1m_2的完全剩余系.

现在证明

$$(m_2x_1 + m_1x_2,\ m_1m_2) = 1,$$

当且仅当

$$(x_1,\ m_1) = 1,\ (x_2,\ m_2) = 1.$$

简化剩余系

如果

$$(x_1, m_1) = 1, (x_2, m_2) = 1$$

又因为$(m_1, m_2) = 1$，则

$$(m_1x_2, m_2) = 1, (m_2x_1, m_1) = 1$$

于是

$$(m_1x_2 + m_2x_1, m_2) = 1, (m_2x_1 + m_1x_2, m_1) = 1$$

故

$$(m_2x_1 + m_1x_2, m_1m_2) = 1$$

反过来，如果

$$(m_2x_1 + m_1x_2, m_1m_2) = 1$$

简化剩余系

则 $(m_2x_1+m_1x_2，m_1)=1$

$(m_2x_1+m_1x_2，m_2)=1.$

于是 $(m_2x_1，m_1)=1，(m_1x_2，m_2)=1.$

又因为$(m_1，m_2)=1$，所以

$(x_2，m_2)=1，(x_1，m_1)=1.$

故 $(x_2，m_2)=1，(x_1，m_1)=1$

$\Leftrightarrow (m_2x_1+m_1x_2，m_1m_2)=1.$

可见当x_1，x_2分别遍历模m_1和模m_2的简化剩余系时，$m_2x_1+m_1x_2$遍历模m_1m_2的简化剩余系.

定理证得.

简化剩余系

推论6-1 如果m_1，m_2是两个正整数，且$(m_1, m_2) = 1$，则$\varphi(m_1m_2) = \varphi(m_1)\varphi(m_2)$.

证明　当x_1，x_2分别遍历模m_1和模m_2的简化剩余系时，$m_2x_1 + m_1x_2$遍历模m_1m_2的简化剩余系，即遍历$\varphi(m_1m_2)$个整数.

而x_1跑遍$\varphi(m_1)$个整数，x_2跑遍$\varphi(m_2)$个整数，故$m_2x_1 + m_1x_2$跑遍$\varphi(m_1)\varphi(m_2)$个整数.

简化剩余系

定理：设m是一个正整数，a是满足(a,m)=1的整数，则存在唯一的整数a’，1≤a’<m，使得

$$aa' \equiv 1 \pmod{m}$$

证一：当k遍历模m的最小简化剩余系，ka也遍历m的最小简化剩余系.

证二：构造性证明.

简化剩余系

定理6-5 设正整数m的标准分解式为

$$m = p_1^{k_1} p_2^{k_2} \ldots p_l^{k_l}$$

则

$$\varphi(m) = m(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_l})$$

$p_1^{k_1}$

简化剩余系

证明　由上面的推论有

$$\varphi(m)=\varphi(p_1^{k_1})\varphi(p_2^{k_2})\cdots\varphi(p_l^{k_l})$$

由于p是素数，则 $\{0，1，2，\ldots，p^i-1\}$

中全部与p^i不互素的正整数为

$$\{0，p，2p，\ldots，(p^{i-1}-1)p\},$$

共有p^{i-1}个，于是

$$\varphi(p^i) = p^i - p^{i-1} = p^i(1-1/p).$$

将上式代入$\varphi(m)$中定理便证得.

简化剩余系

定理6-6　模*m*剩余类环中与*m*互素的剩余类构成乘法群.

证明　设模*m*剩余类环中与*m*互素的剩余类集合为*S*，*S*含有$\varphi(m)$元素：

$$S=\{\overline{r_1},\overline{r_2},\ldots,\overline{r_{\varphi(m)}}\}$$

其中$(r_i, m) = 1$，$1 \le i \le \varphi(m)$.

如果$(r_i, m) = 1$，$(r_j, m) = 1$，则

$(r_ir_j, m) = 1$，

于是如果 $\overline{r_i} \in S, \overline{r_j} \in S$，则

乘法封闭.

$$\overline{r_i}\,\overline{r_i}=\overline{r_ir_j}$$

简化剩余系

由于S是剩余类环的子集，则结合律显然满足.

如果

$$rr_i \equiv rr_j \pmod{m},\ (r,\ m) = 1,$$

则

$$r_i \equiv r_j \pmod{m},$$

于是如果 $\overline{r_i} \in S, \overline{r_j} \in S, \overline{r} \in S,$ 且 $\overline{r}\,\overline{r_i} = \overline{r}\,\overline{r_j}$

则 $\overline{r_i} = \overline{r_j}$

所以S中消去律满足.

故S是乘法群.

简化剩余系

推论6-2设m是正整数，如果$(r，m)=1$，则存在s使$sr\equiv 1 \pmod{m}$. 反之也成立。

推论1换句话说，就是如果r，m互素，则r在模m下必存在逆元s

证明：因为$(r，m)=1$，则存在s，t使

$$sr+tm=1,$$

故

$$sr\equiv 1 \pmod{m}.$$

逆元s的求法要利用欧几里得除法.

剩余系

推论6-3 （欧拉定理）设m是正整数，如果$(a, m)=1$，则

$$r^{\varphi(m)} \equiv 1 \pmod{m}$$

证明：取模m的一个简化剩余系 $b_1,\dots,b_{\varphi(m)}$ ，由定理6-3知 $rb_1,\dots,rb_{\varphi(m)}$ 也是模m的一个简化剩余系，从而有

$$\prod_{i=1}^{\varphi(m)} b_i \equiv \prod_{i=1}^{\varphi(m)} (rb_i) \equiv r^{\varphi(m)} \prod_{i=1}^{\varphi(m)} b_i \pmod{m}$$

因为

$$\forall 1 \le i \le \varphi(m), (b_i, m) = 1$$

所以

欧拉定理在密码技术中具有重要应用，如RSA

故有

$$r^{\varphi(m)} \equiv 1 \pmod{m}$$

例1 设$m=7, a=2$,有$(2,7)=1, \varphi(7)=6.$

取模7的最小非负简化剩余系1, 2, 3, 4, 5, 6, 则有

$$2\cdot 1\equiv 2,\quad 2\cdot 2\equiv 4,\quad 2\cdot 3\equiv 6,$$

$$2\cdot 4\equiv 1,\quad 2\cdot 5\equiv 3,\quad 2\cdot 6\equiv 5 \pmod 7$$

于是

$$(2\cdot 1)(2\cdot 2)(2\cdot 3)(2\cdot 4)(2\cdot 5)(2\cdot 6)$$

$$\equiv 2\cdot 4\cdot 6\cdot 1\cdot 3\cdot 5 \pmod 7$$

即 $2^6(1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6)\equiv 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6 \pmod 7$

所以 $2^6\equiv 1 \pmod 7$ $\quad (2^6=64\equiv 1 \pmod 7)$

例2 设$m=30, a=7$,因$(7,30)=1, \varphi(30)=8$,所以

$$7^8 \equiv 1 \pmod{30}$$

例3 设$m=11, a=2$,因$(2,11)=1, \varphi(11)=10$,所以

$$2^{10} \equiv 1 \pmod{11}$$

$$2^{11} \equiv 2 \pmod{11}$$

例4 设$m=23$,若$23 \nmid a$,则$(a,23)=1, \varphi(23)=22$,所以

$$a^{22} \equiv 1 \pmod{23}$$

$$a^{23} \equiv a \pmod{23}$$

m为素数时,有*Fermat*定理

剩余系

推论6-4（费马定理）如果p是素数，则$r^p \equiv r \pmod{p}$

证明　p是素数，$\varphi(p) = p-1$.

如果$(r，p) = 1$，由欧拉定理有

$$r^{p-1} \equiv 1 \pmod{p},$$

故

$$r^p \equiv r \pmod{p}.$$

如果$(r，p) \neq 1$，由于p是素数，则$p \mid r$，于是

$$r^p \equiv r \equiv 0 \pmod{p}.$$

综合之，总有

$$r^p \equiv r \pmod{p}.$$

例5 (RSA)设p,q是两个不同的奇素数,

$$n = pq,\ (a, pq) = 1,$$

如果整数e满足$1 < e < \varphi(n), (e, \varphi(n)) = 1$,那么存在整数$d, 1 \le d < \varphi(n)$,使得

$$ed \equiv 1 \pmod{\varphi(n)}$$

而且对于整数$a^e \equiv c \pmod{n}, 1 \le c < n$,有

$$c^d \equiv a \pmod{n}.$$

证 因$(e, \varphi(n)) = 1$,则存在整数$d, 1 \le d < \varphi(n)$,使得

$$ed \equiv 1 \pmod{\varphi(n)}$$

由定理2.3.4

于是存在正整数k,使得 $ed=1+k\varphi(n)$.

因$(a,pq)=1$,所以$(a,p)=1$,由Euler定理

$$a^{\varphi(p)}\equiv 1 \pmod p$$

$\Rightarrow a^{k\varphi(p)\varphi(q)}\equiv 1 \pmod p$ $\Rightarrow a^{k\varphi(n)}\equiv 1 \pmod p$

（2.1节定理4）

于是 $a^{1+k\varphi(n)}\equiv a \pmod p$

即 $a^{ed}\equiv a \pmod p$

同理 $a^{ed}\equiv a \pmod q$

$a^{ed}\equiv a \pmod{[p,q]}$ (2.1节定理12)

于是 $a^{ed}\equiv a \pmod n$

因$[p,q]=pq=n$

因此,由 $c \equiv a^e \pmod{n}$,可得

$$c^d \equiv (a^e)^d \equiv a^{ed} \equiv a \pmod{n}$$

定理3(*Wilson*定理) 设p是一个素数,则

$$(p-1)! \equiv -1 \pmod{p}$$

证 （归纳法）$p=2$时, $(2-1)! \equiv -1 \pmod{2}$,结论成立.

设 $p \geq 3$,则对于每个$a, 1 \leq a < p$,存在唯一的整数$a', 1 \leq a' < p$,使得

$$aa' \equiv 1 \pmod{p}$$

由定理2.3.4

于是 $a' = a \Leftrightarrow a^2 \equiv 1 \pmod{p}$

这时,$a = 1$或$a = p-1$.

因此当a与a'取$2, \cdots, p-2$中的数时,$a \neq a'$.

把$2, 3, \cdots, p-2$中的a与a'配对, 有

$$\underbrace{(aa')(aa')\cdots(aa')}_{\frac{p-3}{2}\text{对}} = 2\cdot 3\cdots p-2$$

（aa'的所有可能情况对）

因 $aa' \equiv 1 \pmod{p}$

所以 $2\cdot 3\cdots p-2 \equiv 1 \pmod{p}$

故 $(p-1)! \equiv 1\cdot(p-1) \equiv -1 \pmod{p}$

例6 设$p=17$,有

$$2\cdot 9=18\equiv 1,\quad 3\cdot 6=18\equiv 1,\quad 4\cdot 13=52\equiv 1,$$

$$5\cdot 7=35\equiv 1,\quad 8\cdot 15=120\equiv 1,\quad 10\cdot 12=120\equiv 1,$$

$$11\cdot 14=154\equiv 1 \pmod{17}$$

而 $1\cdot 16=16\equiv -1 \pmod{17}$

因此

$$1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9\cdot 10\cdot 11\cdot 12\cdot 13\cdot 14\cdot 15\cdot 16$$

$$=(1\cdot 16)(2\cdot 9)(3\cdot 6)(4\cdot 13)(5\cdot 7)(8\cdot 15)(10\cdot 12)(11\cdot 14)$$

$$\equiv(-1)\cdot 1\cdot 1\cdot 1\cdot 1\cdot 1\cdot 1\cdot 1$$

$$\equiv -1 \pmod{17}$$

即 $16!\equiv -1 \pmod{17}$

6.2 同余式概念与一次同余式

定义6-4　设$f(x)$为多项式：

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

其中n是正整数，a_i $(0 \le i \le n)$是整数，则

$$f(x) \equiv 0 \pmod{m}$$

称为模m的同余式．如果$a_n \not\equiv 0 \pmod{m}$，则 n称为同余式的次数．如果x_0满足

$$f(x_0) \equiv 0 \pmod{m}$$

则$x \equiv x_0 \pmod{m}$称为同余式的解．

不同的解指互不同余的解．

同余式概念

例6-8　求下列同余式的解.

1）$x^5 + 2x^4 + x^3 + 2x^2 - 2x + 3 \equiv 0 \pmod 7$

解　$x \equiv 1，5，6 \pmod 7$

2）$x^4 - 1 \equiv 0 \pmod{16}$

解　$x \equiv 1，3，5，7，9，11，13，15 \pmod{16}$

3）$x^2 + 3 \equiv 0 \pmod 5$

解　无解.

一次同余式

$$(a,m)=1,\ ax\equiv 1 \pmod{m}$$

$$\Downarrow$$

$$(a,m)=1,\ ax\equiv b \pmod{m}$$

$$\Downarrow$$

$$ax\equiv b \pmod{m}$$

一次同余式

定理6-7　一次同余式$ax \equiv b \pmod{m}$，$a \not\equiv 0 \pmod{m}$，有解的充分必要条件为

$$(a,m) \mid b.$$

证明　先证充分条件：

设 $a' = \dfrac{a}{(a,m)}$，$m' = \dfrac{m}{(a,m)}$ 于是$(a', m')=1$.

$$a'x \equiv \frac{b}{(a,m)} \pmod{m'}$$

$$x \equiv a'^{-1} \frac{b}{(a,m)} \pmod{m'}$$

一次同余式

$$a'x \equiv \frac{b}{(a,m)} \pmod{m'}$$

$$x \equiv a'^{-1} \frac{b}{(a,m)} \pmod{m'}$$

同余式 $a'x \equiv \frac{b}{(a,m)} \pmod{m'}$ 与 $ax \equiv b \pmod{m}$ 是等价的，故 $ax \equiv b \pmod{m}$ 的解：

$$x \equiv a'^{-1} \frac{b}{(a,m)} \pmod{m'}$$

一次同余式

充分条件证得，下面证必要条件.

同余式$ax \equiv b \pmod{m}$有解，则存在$x \equiv x_0 \pmod{m}$和整数k使

$$ax_0 = b+km$$

即

$$ax_0 - km = b$$

于是由$(a, m) \mid a$，$(a, m) \mid m$，得$(a, m) \mid b$

定理证毕.

一次同余式

我们再来讨论 $ax \equiv b \pmod{m}$，a≠0(modm)的解 .

$$x \equiv a'^{-1}\frac{b}{(a,m)} \pmod{m'}$$

设 $x_0 \equiv a'^{-1}\frac{b}{(a,m)}$ ，则上式可表示为

$$x \equiv a'^{-1}\frac{b}{(a,m)} \pmod{m'} = x_0 + km', k = 0, \pm 1, \pm 2 \ldots$$

对于模**m**可以写成： $x \equiv x_0 + km' \pmod{m} \; 0 \le k < (a,m)$

这(**a**，**m**)个数对于模**m**两两不同余，

故同余式 $ax \equiv b \pmod{m}$ 有(**a**，**m**)个解.

一次同余式

例6-9　求$980x \equiv 1500 \pmod{1600}$的解.

解　此题中，$a = 980$，$m = 1600$，$b = 1500$，$(a，m) = 20$，$a' = 49$，$m' = 80$.

1）首先采用欧几里得算法求$a'^{-1}(\mathrm{mod}\,m')$.

由于$(a'，m') = 1$，所以存在r，s，使$a'r + m's = 1$

$80 = 49 + 31$，

$49 = 31 + 18$，

$31 = 18 + 13$，

$18 = 13 + 5$，

$13 = 2\times5 + 3$，

$5 = 3 + 2$，

$3 = 2 + 1$.

$2=1\times2$

一次同余式

$80 = 49 + 31$,

$49 = 31 + 18$,

$31 = 18 + 13$,

$18 = 13 + 5$,

$13 = 2\times5 + 3$,

$5 = 3 + 2$,

$3 = 2 + 1$.

$2=1\times2$

于是我们有

$31 = 80 - 49 = m' - a'$

$18 = a' - 31 = 2a' - m'$,

$13 = 31 - 18 = 2m' - 3a'$,

$5 = 18 - 13 = 5a' - 3m'$,

$3 = 13 - 2\times5 = 8m' - 13a'$,

$2 = 5 - 3 = 18a' - 11m'$,

$1 = 3 - 2 = 19m' - 31a'$.

所以$19m' - 31a' = 1$,

则$- 31a' \equiv 49a' \equiv 1 \pmod{80}$

故$a'^{-1} \equiv 49$.

一次同余式

2）求x_0.

$$x_0 \equiv a'^{-1}\frac{b}{(a,m)}(\bmod m') \equiv 49\times\frac{1500}{20} \equiv 75(\bmod 80)$$

3）同余式的解共有20个，它们为

$x \equiv 75+80k \ (\bmod\ 1600)$，$k=0$，1，…，19.

6.3 中国剩余定理

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \quad\cdots \\ x \equiv b_k \pmod{m_k}. \end{cases}$$

定理6-8（中国剩余定理）设m_1，m_2，…，m_k两两互素，则上面的同余式组有解，且有唯一解：

$$x = M_1^{-1}M_1b_1 + M_2^{-1}M_2b_2 + \ldots M_k^{-1}M_kb_k \pmod{m} \quad (✦)$$

其中$m = m_1m_2\ldots m_k$， $M_i = \dfrac{m}{m_i}$， $M_i^{-1}M_i \equiv 1 \pmod{m_i}$

i =1，2，…，k.

证明 （1）存在性。 （2）唯一性

中国剩余定理

例6-13　解同余式组：

$$x \equiv 1 \pmod 5,$$
$$x \equiv 5 \pmod 6,$$
$$x \equiv 4 \pmod 7,$$
$$x \equiv 10 \pmod{11}.$$

按中国剩余定理求解如下：

$$m = 5\times6\times7\times11 = 2310,$$

$$M_1 = 6\times7\times11 = 462,\quad M_1^{-1} = 3 \pmod 5,$$

$$M_2 = 5\times7\times11 = 385,\quad M_2^{-1} = 1 \pmod 6,$$

$$M_3 = 5\times6\times11 = 330,\quad M_3^{-1} = 1 \pmod 7,$$

$$M_4 = 5\times6\times7 = 210,\quad M_4^{-1} = 1 \pmod{11},$$

$$x \equiv 3\times462 + 385\times5 + 330\times4 + 210\times10 \equiv 6731$$

$$\equiv 2111 \pmod{2310}.$$

中国剩余定理

定理6-9 当m_1，m_2，…，m_k两两互素时，同余式

$$a \equiv b \pmod{m_1 m_2 \ldots m_k},$$

等价于同余式组

$$\begin{cases} a \equiv b \bmod m_1 \\ a \equiv b \bmod m_2 \\ \vdots \\ a \equiv b \bmod m_k \end{cases}$$

中国剩余定理

证明　由$a \equiv b \pmod{m_1 m_2 \ldots m_k}$，有

$$m_1 m_2 \ldots m_k \mid (a-b),$$

于是有

$$m_1 \mid (a-b),$$
$$m_2 \mid (a-b),$$
$$\ldots$$
$$m_k \mid (a-b).$$

所以有

$$a \equiv b \pmod{m_1},$$
$$a \equiv b \pmod{m_2},$$
$$\ldots$$
$$a \equiv b \pmod{m_k}.$$

中国剩余定理

反过来，如果 $a \equiv b \pmod{m_1}$,

$$a \equiv b \pmod{m_2},$$

$$\cdots$$

$$a \equiv b \pmod{m_k}.$$

即

$$m_1 \mid (a-b),$$

$$m_2 \mid (a-b),$$

$$\cdots$$

$$m_k \mid (a-b).$$

因为m_1，m_2，…，m_k两两互素，则

$$m_1 m_2 \ldots m_k \mid (a-b),$$

故有 $a \equiv b \pmod{m_1 m_2 \ldots m_k}$.

中国剩余定理

例6-15　解下列同余式组：

$$x \equiv 3 \pmod 8$$
$$x \equiv 11 \pmod{20}$$
$$x \equiv 1 \pmod{15}$$

解　化为下列同余式组：

$$x \equiv 3 \pmod 8$$
$$x \equiv 11 \pmod 4 \equiv 3 \pmod 4$$
$$x \equiv 11 \pmod 5 \equiv 1 \pmod 5$$
$$x \equiv 1 \pmod 3$$
$$x \equiv 1 \pmod 5$$

中国剩余定理

满足第一个同余式必然满足第二个同余式，去掉第二个同余式．现在我们得到与原同余式组等价并且能利用中国剩余定理求解的同余式组：

$$x \equiv 3 \pmod 8,$$

$$x \equiv 1 \pmod 3,$$

$$x \equiv 1 \pmod 5.$$

最后解出同余式组的解：

$$x \equiv 91 \pmod{120}.$$

中国剩余定理

定理6-10 在定理6-8的条件下，如果b_1，b_2，…，b_k分别遍历模m_1，m_2，…，m_k的完全剩余系，则

$$x = M_1^{-1}M_1b_1 + M_2^{-1}M_2b_2 + \ldots M_k^{-1}M_kb_k \pmod{m}$$

遍历模m的完全剩余系.

证明 令 $x_0 = M_1^{-1}M_1b_1 + M_2^{-1}M_2b_2 + \ldots M_k^{-1}M_kb_k$

显然当b_1，b2，…，b_k分别跑遍模m_1，m_2，…，m_k的完全剩余系时，x_0跑遍$m = m_1m_2\ldots m_k$个数，现在证明x_0两两不同余.

中国剩余定理

假设

$$M_1^{-1}M_1b_1+M_2^{-1}M_2b_2+\ldots M_k^{-1}M_kb_k$$
$$\equiv M_1^{-1}M_1b_1'+M_2^{-1}M_2b_2'+\ldots M_k^{-1}M_kb_k'\pmod m$$

则

$$M_i^{-1}M_ib_i\equiv M_i^{-1}M_ib_i'\pmod{m_i},i=1,2,\ldots k$$

于是

$$b_i\equiv b'_i\pmod{m_i}，i=1，2，\ldots，k.$$

由于b_i，b'_i属于模m_i的同一剩余，所以

$$b_i=b'_i，i=1，2，\ldots，k，$$

故x_0两两不同余．定理证毕．

6.4 素数模同余式

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 \pmod p$其中$p$是素数，$a_n \not\equiv 0 \pmod p$，

定理6-11 素数模p的同余式与一个次数不超过$p-1$的素数模同余式等价.

证明 由多项式带余除法我们有：

$$f(x) = (x^p - x)q(x) + r(x),\ \deg(r(x)) \le p-1.$$

由费马定理有：

$$x^p - x \equiv 0 \pmod p.$$

素数模同余式

故

$$f(x) \equiv r(x) \pmod{p}.$$

即同余式

$$f(x) \equiv 0 \pmod{p}$$

与同余式

$$r(x) \equiv 0 \pmod{p}$$

等价.

素数模同余式

例6.4.1　求解同余式：

$5x^{15} + x^{14} + x^{10} + 8x^5 + 7x^2 + x + 11 \equiv 0 \pmod 3$.

解　做带余除法：

$5x^{15} + x^{14} + x^{10} + 8x^5 + 7x^2 + x + 11$

$= (x^3 - x)(5x^{12} + x^{11} + 5x^{10} + x^9 + 5x^8 + 2x^7 + 5x^6$

$+ 2x^5 + 5x^4 + 2x^3 + 13x^2 + 2x + 13) + 9x^2 + 14x + 11$.

$\Leftrightarrow$　$9x^2 + 14x + 11 \equiv 0 \pmod 3$

$\Leftrightarrow$　$2x + 2 \equiv 0 \pmod 3$

解为：　$x \equiv 2 \pmod 3$

素数模同余式

$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 \pmod{p}$其中$p$是素数，$a_n \not\equiv 0 \pmod{p}$ （1）

定理6.4.2 设

$$x \equiv \beta_i \pmod{p}\ (i = 1，2，\ldots，k，k \le n)$$

是素数模同余式(1)的k个不同解，则

$f(x) \equiv (x-\beta_1)(x-\beta_2)\ldots(x-\beta_k) f_k(x) \pmod{p}$，

其中$f_k(x)$的次数$\deg(f_k(x)) = n-k$，首项系数为a_n.

证明 由带余除法得

$$f(x) = (x-\beta_1) f_1(x) + r，$$

因为

$$f(\beta_1) \equiv 0 \pmod{p}，$$

素数模同余式

则

$$r \equiv 0 \pmod{p},$$

所以

$$f(x) \equiv (x - \beta_1)\, f_1(x) \pmod{p},$$

其中$f_1(x)$的次数$\deg(f_1(x)) = n-1$，首项系数为a_n.

现在证明$x \equiv \beta_i \pmod{p}$ ($i = 2$，…，k)是

$$f_1(x) \equiv 0 \pmod{p}$$

的解.

素数模同余式

当$x \equiv \beta_i \pmod p$　($i = 2$，…，k)时，

$$f(\beta_i) \equiv (\beta_i - \beta_1) f_1(\beta_i) \equiv 0 \pmod p,$$

由于β_1，β_2，…，β_k是不同的解，

则$\beta_i - \beta_1 \not\equiv 0 \pmod p$，

又因为p是素数，

故

$f_1(\beta_i) \equiv 0 \pmod p$　($i = 2$，…，k).

类似继续可证明定理.

素数模同余式

例6.4.2 同余式$x^5 + 4x^2 + 2 \equiv 0 \pmod 7$，直接验证有解

$$x_1 \equiv 1 \pmod 7,$$
$$x_2 \equiv 5 \pmod 7,$$

则

$$x^5 + 4x^2 + 2 \equiv (x-1)(x-5)(x^3 + 6x^2 + 3x + 6) \pmod 7$$

素数模同余式

由费马定理，对于任意整数*r*都有

$$r^p \equiv r (\mathrm{mod}\ p),$$

这表明$x \equiv 1，2，…，p-1\ (\mathrm{mod}\ p)$

是同余式$x^{p-1} \equiv 1 (\mathrm{mod}\ p)$的解

素数模同余式

推论 p是素数，则

$(x^{p-1}-1) \equiv (x-1)(x-2)\ldots(x-(p-1)) \pmod p$

将 $x \equiv 0 \pmod p$

代入上式得到：

$(p-1)! + 1 \equiv 0 \pmod p$.

该式在数论中称为Wilson定理，它表明了素数的一个特性，可以用来检验素数.

素数模同余式

$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 \pmod{p}$其中$p$是素数，$a_n \neq 0 \pmod{p}$　　　（1）

定理6.4.3　素数模同余式(1)解的个数不超过它的次数.

证明　用反证法. 不妨设同余式(1)有n+1个不同解:

$x \equiv \beta_i \pmod{p}$ (i = 1，2，…，n，n+1).

利用前n个解分解$f(x)$得

$$f(x) \equiv (x-\beta_1)(x-\beta_2)\ldots(x-\beta_n)f_n(x) \pmod{p},$$

而

$$f_n(x) = a_n,$$

所以

$$f(x) \equiv a_n(x-\beta_1)(x-\beta_2)\ldots(x-\beta_n) \pmod{p}.$$

素数模同余式

由于

$$f(\beta_{n+1}) \equiv 0 \pmod{p},$$

于是

$a_n(\beta_{n+1}-\beta_1)(\beta_{n+1}-\beta_2)\ldots(\beta_{n+1}-\beta_n) \pmod{p} \equiv 0 \pmod{p}$,

因为β_1，β_2，…，β_n，β_{n+1}是不同的解，所以上式是不可能的，与假设矛盾.

定理证得.

素数模同余式

定理6.4.4 如果$n \le p$，则下列首一素数模同余式

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \equiv 0 \pmod{p} \quad (3)$$

有n个解的充分必要条件是在模p下$f(x)$整除$x^p - x$.

证明 $x^p - x$可分解为

$$(x^p - x) \equiv x(x-1)(x-2)\dots(x-(p-1)) \pmod{p}.$$

必要条件证明：

假设同余式(3)有n个解且这n个解为

$$x \equiv \beta_i \pmod{p} \ (i = 1，2，\dots，n),$$

则$f(x) \equiv (x-\beta_1)(x-\beta_2)\dots(x-\beta_n) \pmod{p}$

显然有

$$f(x) \mid (x^p - x).$$

素数模同余式

充分条件证明：

如果

$$f(x) \mid (x^p - x),$$

而$f(x)$是n次同余式，则它可分解为$(x^p - x)$中的n个因子，假设

$$f(x) \equiv (x-\beta_1)(x-\beta_2)\ldots(x-\beta_n) \pmod{p},$$

且β_1，β_2，…，β_n模p两两不同余，则同余式(3)显然有n个解.

素数模同余式

例3　判断同余式

$2x^3 + 5x^2 + 6x + 1 \equiv 0 \pmod 7$

是否有3个解.

解　先将同余式化为首一同余式：

求出首项系数的逆：$2^{-1} = 4 \pmod 7$，

于是同余式等价于

$x^3 - x^2 + 3x + 4 \equiv 0 \pmod 7$.

素数模同余式

做带余除法：

$x^7 - x \equiv (x^3 - x^2 + 3x + 4)(x^4 + x^3 - 2x^2 - 2x) + (7x^2 + 7x)$

$\equiv (x^3 - x^2 + 3x + 4)(x^4 + x^3 - 2x^2 - 2x) \pmod 7$，

所以 $(x^3 - x^2 + 3x + 4) \mid x^7 - x$

原同余式有3个解。

素数模同余式

例4　解同余式

$3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \equiv 0$ (mod 5).

解　做带余除法：

$3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x$

$\equiv (x^5 - x)(3x^9+4x^8+2x^6+3x^5+5x^4+2x^2+4x+5) + (3x^3+x^2+x)$ (mod 5)，

则原同余式与

$3x^3+x^2+x \equiv 0$ (mod 5)

等价.

素数模同余式

我们还可以利用费马定理来解上述同余式．由费马定理，我们总有

$x^5 - x \equiv 0 \pmod{5}$，

即$x^5 \equiv x \pmod{5}$，

于是

$3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x$

$\equiv 3x^4x^{5\times2} + 4x^3x^{5\times2} + 2xx^{5\times2} + x^4x^5 + xx^5 + x^3 + 12x^2 + x$

$\equiv 3x^4x^2 + 4x^3x^2 + 2xx^2 + x^4x + xx + x^3 + 12x^2 + x$

$\equiv 3x^2 + 4x + 2x^3 + x + x^2 + x^3 + 12x^2 + x$

$\equiv 3x^3 + 16x^2 + 6x$

$\equiv 3x^3 + x^2 + x$

$\equiv 0 \pmod{5}$，

素数模同余式

这样也得到了与前一种方法得到的同样的等价同余式.

利用费马定理有时候是更有效的方法，可以根据具体情况选择哪种解法.

本章作业：

1, 2, 3, 4, 5， 6(1)(4)(8), 7(1)(8)(9), 8(2), 9, 11, 12, 13, 14, 16, 19, 20(1)

谢谢