信息安全数学基础3－同余式
（《数论讲义》第二章）

杨礼珍

同济大学计算机科学与技术系, 2018

Outline

本章作业

- 阅读《数论讲义》第二章第1-7、9节
- 《数论讲义》第二章习题2、3、4、6、8、12、14、22(1)、24(2)
- 重要定理、结论在课件中用红字标出。

1 同余的定义和基本性质

定义：$\forall m \in \mathbb{Z}^+$，如果$m$除整数$a, b$的余数相同，则说$a, b$对模数$m$ 同余，记作

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

如果余数不同，则说a, b对模数m不同余，记作

$$a \not\equiv b \pmod{m}$$

由同余定义，立即可得以下性质：

1. $a \equiv a \pmod{m}$(自反性)
2. 若$a \equiv b \pmod{m}$，则$b \equiv a \pmod{m}$. (对称性)
3. 若$a \equiv b \pmod{m}$，$b \equiv c \pmod{m}$，则$a \equiv c \pmod{m}$. (传递性)

定理1：整数a, b对模数m同余的充分必要条件是$m|a-b$.

证明： **必要性证明.**设$a \equiv b \pmod{m}$，则存在整数$q_1, q_2, r (0 \leq r < m)$有

$$\left.\begin{array}{rcl} a & = & mq_1 + r \\ b & = & mq_2 + r \end{array}\right\} \Rightarrow a - b = m(q_1 - q_2) \Rightarrow m|a-b$$

充分性证明.设

$$\begin{array}{rcll} a & = & mq_1 + r_1 & (0 \leq r_1 < m) \\ b & = & mq_2 + r_2 & (0 \leq r_2 < m) \end{array}$$

那么有

$$\left.\begin{array}{r} m|a-b = m(q_1 - q_2) + r_1 - r_2 \\ 0 \leq |r_1 - r_2| < m \end{array}\right\} \Rightarrow |r_1 - r_2| = 0 \Rightarrow r_1 = r_2$$

- **由定理1得到：** $a \equiv b \pmod{m}$当且仅当$\exists k \in \mathbb{Z}$有$a = b + km$。我们在证明中，经常用到此结论。
  - 例. 已知$0 \leq a < 5$且有$a \equiv 13 \pmod{5}$，则有$a = 3$。
  - 例. 已知$0 \leq a < 10$且有$a \equiv 13 \pmod{5}$，则有$a = 3, 8$。
- **注意事项：** 若$a = b$显然有$a \equiv b \pmod{m}$，但反之未必成立。
  如果已知$a, b \in \mathbb{Z}_m$，由带余除法的唯一性知道，$a \equiv b \pmod{m}$意味着$a = b$。

定理2： 如果$a \equiv b \pmod{m}$, $\alpha \equiv \beta \pmod{m}$，则有

1. $ax + \alpha y \equiv bx + \beta y \pmod{m}$，其中$x, y \in \mathbb{Z}$;
2. $a\alpha \equiv b\beta \pmod{m}$;
3. $a^n \equiv b^n \pmod{m}$，其中$n > 0$;
4. $f(a) \equiv f(b) \pmod{m}$，其中$f(x)$为任意给定的整系数多项数.

证明： 均由同余定义证明。

1. 因为$m|a-b, m|\alpha-\beta$，故有
$$m|x(a-b)+y(\alpha-\beta) = (ax+\alpha y)-(bx+\beta y).$$
2. 由$m|\alpha(a-b)+b(\alpha-\beta) = a\alpha - b\beta$便知。
3. 由(2)可证。
4. 由(1)和(3)可证。

1 同余的定义和基本性质
定理1、2的应用

例1： 若整数$n > 0$的十进制表示为

$$n = a_0 + 10a_1 + 10^2a_2 + \ldots + 10^ka_k$$

那么$9|n$的当且仅当$9|(a_0 + a_1 + \ldots + \ldots a_k)$

证明：

$$9|n = (a_0 + 10a_1 + 10^2a_2 + \ldots + 10^ka_k) - 0$$

$$\overset{\text{由定理1}}{\Longleftrightarrow} \quad 0 \equiv a_0 + 10a_1 + 10^2a_2 + \ldots + 10^ka_k \pmod 9$$

$$\overset{\text{由定理2的(4)}}{\Longleftrightarrow} \quad 0 \equiv a_0 + a_1 + a_2 + \ldots + a_k \pmod 9 (\text{由} 10^i \equiv 1 \pmod 9)$$

类似练习：

P60练习2. 给出整数能被11整除的判别法。

1 同余的定义和基本性质
定理1、2的应用

例2：$641|F_5 = 2^{2^5} + 1 = 2^{32} + 1.$
证明：

$$2^8 = 256, 2^{16} = 256^2 = 65536 \equiv 154 \pmod{641}$$

$$2^{32} \equiv (154)^2 = 23716 \equiv 640 \equiv -1 \pmod{641}$$

例3：当n是奇数时，$3|2^n + 1$；当n是偶数时，$3 \nmid 2^n + 1$
证明：

$$\begin{aligned} 2 \equiv -1 \pmod 3 \quad &\Rightarrow \quad 2^n \equiv (-1)^n \pmod 3 \\ &\Rightarrow \quad \begin{cases} \text{当}n\text{为奇，}2^n \equiv -1 \pmod 3 \Rightarrow 3|2^n + 1 \\ \text{当}n\text{为偶，}2^n \equiv 1 \pmod 3 \Rightarrow 3 \nmid 2^n + 1 \end{cases} \end{aligned}$$

定理3：若$c \neq 0, (m,c) = d$，则$ac \equiv bc \pmod{m}$当且仅当

$$a \equiv b \pmod{\frac{m}{d}} \tag{1}$$

证明：

$$\left.\begin{array}{r} ac \equiv bc \pmod{m} \Leftrightarrow m|c(a-b) \Leftrightarrow \frac{m}{d}|\frac{c}{d}(a-b) \\ (m,c) = d \Rightarrow \left(\frac{m}{d}, \frac{c}{d}\right) = 1 \end{array}\right\}$$

$\Longleftrightarrow \frac{m}{d}|(a-b) \Longleftrightarrow$ (1)成立. 证毕.

- 课本中只指出定理3的必要性成立，其实充分性也成立。
- 实际中，我们应用的更多的是定理3的以下2个推论。联合以下2个推论又可反推定理3。

推论*：若$x \neq 0$，则$ax \equiv bx \pmod{mx} \Longleftrightarrow a \equiv b \pmod{m}$.

推论**：若$(x,m) = 1$，则有

$$ax \equiv bx \pmod{m} \Longleftrightarrow a \equiv b \pmod{m}.$$

- **注意事项：** 由$a \equiv b \pmod{m}$可推出$ax \equiv bx \pmod{m}$。但如果$(x, m) \neq 1$，反之未必成立。
  - **例.** $2 \cdot 3 \equiv 2 \cdot 8 \pmod{10}$，但$3 \not\equiv 8 \pmod{10}$。
- **应用：**
  - **例.** 求$3x \equiv 9 \pmod{10}$。
    解：因为$(3, 10) = 1$，由推论**得到$x \equiv 3 \pmod{10}$.
  - **例：** 求$3x \equiv 9 \pmod{12}$。
    解：由推论*得到$x \equiv 3 \pmod{4}$。

定理4：$a \equiv b \pmod{m_i}$,$i = 1, 2, \ldots, n$，当且仅当

$$a \equiv b \pmod{[m_1, \ldots, m_n]} \qquad (2)$$

证明：必要性：因为$m_i | a - b, i = 1, \ldots, n$，
把$a - b$和$m_i (i = 1, \ldots, n)$都写成因子相同的标准分解式，即可知

$$[m_1, \ldots, m_n] | a - b \Longrightarrow (2)\text{成立}.$$

充分性：

(2)成立 $\Longrightarrow [m_1, \ldots, m_n] | a-b \Longrightarrow m_i | a-b \Longrightarrow a \equiv b \pmod{m_i}$

- 课本只给出了定理4的必要性。
- 定理4的以下特殊情形在证明中应用较多：
  - 若$a \equiv b \pmod{mn}$则$a \equiv b \pmod{m}$.
- 如果把定理4的$[m_1, \ldots, m_n]$改成$m_1 m_2 \cdots m_n$必要性未必成立。
  - 例：
$$6 \equiv 12 \pmod{6}, 6 \equiv 12 \pmod{3},$$
但
$$6 \not\equiv 12 \pmod{18}.$$

2 剩余类和完全剩余系

定义： 设$m \in \mathbb{Z}^+$

$$C_r = \{qm + r | q \in \mathbb{Z}\} = r + m\mathbb{Z}, r = 0, 1, \ldots, m-1$$

则$C_0, \ldots, C_{m-1}$叫做模数m的剩余类。

定理1： 设$m > 0$，$C_0, \ldots, C_{m-1}$是模数m的剩余类，则有

1. $C_0 \cup C_1 \cup \ldots \cup C_{m-1} = \mathbb{Z}$.
2. $x, y \in C_r \Longleftrightarrow x \equiv y \pmod{m}$. (注：即$i \neq j$时$C_i \cap C_j = \varnothing$)

证明：

1. 对$\forall a \in \mathbb{Z}$，$\exists q, 0 \leq r < m$有

$$a = qm + r \Longrightarrow a \in C_r$$

2.

$$x, y \in C_r \Leftrightarrow \left\{ \begin{array}{c} x = q_1 m + r \\ y = q_2 m + r \end{array} \right\} \Leftrightarrow x \equiv y \pmod{m}$$

定义： 从模数m的剩余类$C_0, C_1, \ldots, C_{m-1}$中各取一数$a_j \in C_j, j = 0, 1, \ldots, m-1$，则称$a_0, a_1, \ldots, a_{m-1}$为模数$m$的一组**完全剩余系**。

- $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$称为模数$m$的**非负最小完全剩余系**。

定理2： m个整数作为模数m的一组完全剩余系的充分必要条件是两两对模数m不同余。

证明： 由完全剩余系的定义立得。

定理3： 设$(k,m)=1$，$a_1,\ldots,a_m$是模数m的一组完全剩余系，则$ka_1,\ldots,ka_m$是模数m的一组完全剩余系.

证明1： 反证法。若存在$i\neq j$有$ka_i\equiv ka_j \pmod{m}$，因为$(k,m)=1$，则$a_i\equiv a_j \pmod{m}$，这与假设矛盾。因此命题成立。

证明2(课本的证明)：反证法。若存在$i\neq j$有

$$\left.\begin{array}{r} ka_i\equiv ka_j \pmod{m} \Rightarrow m|k(a_i-a_j) \\ (k,m)=1 \end{array}\right\} \Rightarrow \quad m|a_i-a_j$$

$$\Rightarrow \quad a_i\equiv a_j \pmod{m}$$

$$\Rightarrow \quad i=j\text{矛盾！}$$

因此命题成立。

定理4：设$m_1>0, m_2>0$，$(m_1,m_2)=1$，而x_1,x_2分别通过(遍历)模数m_1,m_2的完全剩余系，则$m_2x_1+m_1x_2$通过模数m_1m_2的完全剩余系。

证明：由假设知道x_1,x_2分别通过m_1,m_2个整数，因此$m_2x_1+m_1x_2$通过m_1m_2个整数。由定理2只需要证明这m_1m_2个整数对模数m_1m_2两两不同余就够了。假定

$$m_2x_1'+m_1x_2'\equiv m_2x_1''+m_1x_2'' \pmod{m_1m_2} \qquad (3)$$

则由(3)可得

$$\begin{aligned} & m_2x_1'+m_1x_2'\equiv m_2x_1''+m_1x_2'' \pmod{m_1} \\ \Rightarrow\quad & m_2x_1'\equiv m_2x_1'' \pmod{m_1} \\ \Rightarrow\quad & x_1'\equiv x_1'' \pmod{m_1}(\text{因为}(m_1,m_2)=1) \end{aligned}$$

同理，由(3)可得$x_2'\equiv x_2'' \pmod{m_2}$。这说明，当$x_1,x_2$分别通过$m_1,m_2$的完全剩余系时，$m_2x_1+m_1x_2$通过$m_1m_2$的完全剩余系。

注：也可由§6介绍的中国剩余定理证明定理4.

完全剩余系的相关练习：

练习6. 证明：若$m_i > 0(i = 1, \ldots, k)$，$x_i$通过模数$m_i$的任一完全剩余系，则

$$x_1 + m_1 x_2 + m_1 m_2 x_3 + \ldots + m_1 m_2 \ldots m_{k-1} x_k$$

通过模数$m_1 \ldots m_k$的一组完全剩余系.

提示：对k进行数学归纳法。当$k = 1$时，证明若x_1, x_1'和x_2, x_2'分别取自模数m_1, m_2的一组完全剩余系，若$x_1 + m_1 x_2 \equiv x_1' + m_1 x_2' \pmod{m_1 m_2}$则$x_1 = x_1'$，$x_2 = x_2'$。

练习7. 证明：若$x_n, x_{n-1}, \ldots, x_1, x_0$互相独立地通过$-1, 0, 1$时，

$$3^n x_n + 3^{n-1} x_{n-1} + \ldots + 3x_1 + x_0$$

表示所有下面的数

$$-H, \ldots, -1, 0, 1, \ldots, H, H = \frac{3^{n+1} - 1}{3 - 1}.$$

并且每一个数都有惟一的表示法。由此说明应用$n + 1$个特制的砝码，在天平上可以量出1到H（单位：g）的任何一个数。

练习21. 证明：

当$u = 0, 1, \ldots, p^{s-t} - 1$，$v = 0, 1 \ldots, p^t - 1$，$t \leq s$时，$x = u + p^{s-t} v$通过$p^s$的一个完全剩余系。

练习7、21的提示：应用练习6的结论。

引理1：设正整数m，整数a,b满足

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

则$\exists a' \in \mathbb{Z}$有$aa' \equiv 1 \pmod{m}$ 当且仅当$\exists b' \in \mathbb{Z}$有$bb' \equiv 1 \pmod{m}$。且

$$a' \equiv b' \pmod{m}.$$

证明： 若有$aa' \equiv 1 \pmod{m}$，则

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

反之，若有$bb' \equiv 1 \pmod{m}$，则$ab' \equiv bb' \equiv 1 \pmod{m}$。
若有$aa' \equiv 1 \pmod{m}$及$bb' \equiv 1 \pmod{m}$，则

$$a' \equiv b'b \cdot a' \equiv b' \cdot ba' \equiv b' \cdot aa' \equiv b' \pmod{m}.$$

推论：若$a \in \mathbb{Z}_m$存在逆元，则逆元惟一。

- **引理1应用例子**：由

$$3 \equiv 29 \pmod{26}, 3 \times 9 \equiv 1 \pmod{26}$$

可得

$$29 \times 9 \equiv 1 \pmod{26}$$

引理2：对$m \in \mathbb{Z}^+, a \in \mathbb{Z}_m$，$a^{-1} \bmod m$存在$\Longleftrightarrow (a, m) = 1$.

证明思路：" $\Rightarrow$ ".

$$1 = aa^{-1} \bmod m \Rightarrow aa^{-1} = tm + 1 \Rightarrow (a, m) = 1$$

" $\Leftarrow$ ".

$$(a, m) = 1 \Rightarrow \exists s, t \in \mathbb{Z}, \text{S.T.} sa + tm = 1$$
$$\Rightarrow sa = -tm + 1 \Rightarrow 1 = sa \bmod m \text{，即} s = a^{-1} \bmod m \text{，得证！}$$

引理3：设p为素数，对$x \in \mathbb{Z}_p^*$，$x = x^{-1} \bmod p$当且仅当$x \in \{1, p-1\}$.

证明思路：

$$\begin{aligned} x = x^{-1} \bmod p \quad & \Leftrightarrow \quad x^2 \equiv 1 \pmod{p} \\ & \Leftrightarrow \quad (x-1)(x+1) \equiv 0 \pmod{p} \\ & \Leftrightarrow \quad p \mid (x-1)(x+1), \\ & \quad\quad \text{又} 0 \le x-1 \le p-2, 2 \le x+1 \le p \\ & \Leftrightarrow \quad x \in \{1, p-1\} \end{aligned}$$

引理2、3的应用

定理6(Wilson定理)： 设p为素数，则

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

证明思路： 引理2说明，$S=\{2,\ldots,p-2\}$中元素都有模p乘法逆元，引理3说明其逆元不等于其本身。因此可以把S中元素分成$\frac{p-3}{2}$对，每一对数a,b满足$ab \equiv 1 \pmod p$。那么有

$$2 \cdot 3 \cdot \cdots \cdot p-2 \equiv 1 \pmod p$$

则

$$(p-1)! \equiv 1 \cdot p-1 \equiv -1 \pmod p \Longrightarrow \text{命题}$$

Wilson定理的证明中对互逆的元素进行配对抵消。对这一技巧的应用的练习有3、8、12、38。

练习3. 证明：若$n \equiv 0 \pmod 2$，$a_1, \ldots, a_n$和$b_1, \ldots, b_n$是模数n的任意两组完全剩余系，则$a_1 + b_1, \ldots, a_n + b_n$不是模数$n$的完全剩余系。

提示：注意$i + n - i \equiv 0 \pmod n$，并考虑和式。

练习8. 证明：若$m > 2$，$a_1, \ldots, a_{\varphi(m)}$为模数$m$的任一缩系，则

$$\sum_{i=1}^{\varphi(m)} a_i \equiv 0 \pmod m.$$

提示：若$(a, m) = 1$，则$(m - a, m) = 1$。

练习12. 证明：若p是奇素数，则

1. $1^2 \cdot 3^2 \ldots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p$；
2. $2^2 \cdot 4^2 \ldots (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p$。

提示：$p - i \equiv -i \pmod p$。

练习28. 证明：若p是一个奇素数，$q = \frac{p-1}{2}$，则

$$(q!)^2 + (-1)^q \equiv 0 \pmod p.$$

提示：$p - i \equiv -i \pmod p$。

2 剩余类和完全剩余系
定义在$\mathbb{Z}_m$上的代数结构

定义： $\mathbb{Z}_m^* = \{x \in \mathbb{Z}_m | \gcd(x, m) = 1\}$.
定理： $(\mathbb{Z}_m^*, \cdot)$是Abel群，其中·表示模m乘法运算。
证明： 若$a, b \in \mathbb{Z}_m^*$，则$(ab, m) = 1$，因此$ab \in \mathbb{Z}_m^*$。满足封闭性。
容易验证1是单位元、满足交换律和结合律。
由引理2知道，任意$a \in \mathbb{Z}_m^*$存在逆元。

- $(\mathbb{Z}_m, \cdot)$不是群，其中·表示模m乘法运算。因为0没有逆元。
- $(\mathbb{Z}, \cdot)$不是群，其中·表示mod m乘法运算。因为没有单位元。注意，当$x > m$时，$x \cdot 1 \neq x$.

2 剩余类和完全剩余系
定义在$\mathbb{Z}_m$上的代数结构

- $(\mathbb{Z}_m, +, \cdot)$构成交换环：因为由《数论讲义》第1章第1节的定理2得到
  - $(\mathbb{Z}_m, +)$是交换群，加法单位元为0，元素a的加法逆元为$-a$.
  - $\forall a, b \in \mathbb{Z}_m$有$ab \in \mathbb{Z}_m$，且$ab = ba$.
  - $\forall a, b, c \in \mathbb{Z}_m$有$(ab)c = a(bc)$
  - $\forall a \in \mathbb{Z}_m$有$1 \cdot a = a \cdot 1 = a$，因此1是乘法单位元.
  - 关于加法和乘法满足分配律。
- 当且仅当p为素数时，$(\mathbb{Z}_p, +, \cdot)$是域。因为：
  - 由引理1知道，当且仅当p为素数时，$\mathbb{Z}_P^* = \mathbb{Z}_p \setminus \{0\}$的所有元素存在乘法逆元，因而对乘法运算是Abel群。

2 剩余类和完全剩余系
定义在$\mathbb{Z}_m$上的代数结构

令C_a表示整数a所在的模m剩余类。定义

$$\mathbb{Z}/(m)=\{C_a|a\in\mathbb{Z}\}$$

（有的书把$\mathbb{Z}/(m)$写成$\mathbb{Z}/m\mathbb{Z}$。）则有：

定理： $\mathbb{Z}/(m)=\{C_0,C_1,\ldots,C_{m-1}\}$是交换环，称为模数$m$的剩余类环。其中对于任意$i,j\in\mathbb{Z}_m$，定义

- 加法：$C_i+C_j=C_{i+j}$
- 乘法：$C_iC_j=C_{ij}$

证明： 首先$\mathbb{Z}/(m)$上定义的加法和乘法是合理定义的（或单值），即若$C_a=C_{a'},C_b=C_{b'}$，则

$$C_a+C_b=C_{a'}+C_{b'},C_aC_b=C_{a'}C_{b'}.$$

容易验证$\mathbb{Z}/(m)$对加法是Abel群，其中C_0是单位元，$-C_a=C_{-a}$。$\mathbb{Z}/(m)$对乘法满足封闭性、结合律，C_1是单位元。

2 剩余类和完全剩余系
定义在$\mathbb{Z}_m$上的代数结构

- $(\mathbb{Z}_m, +, \cdot)$与$\mathbb{Z}/(m)$同构：存在这两个环上的同构映射。定义映射
$$f : \mathbb{Z}_m \to \mathbb{Z}/(m), f(i) = C_i,$$
则f是环$\mathbb{Z}_m$和$\mathbb{Z}/(m)$上的同构映射，即f满足：
  - $f(1) = C_1$
  - $f(i + j) = C_{i+j} = C_i + C_j = f(i) + f(j)$
  - $f(ij) = C_{ij} = C_i C_j = f(i)f(j)$
  - f是双射

  $(\mathbb{Z}_m, +, \cdot)$与$\mathbb{Z}/(m)$同构，说明他们实质上是一样的，除了元素表示和运算符号表示不同。

3 缩系

定义： 如果一个模数m的剩余类里面的数与m互素，就把它叫做一个与模数m互素的剩余类。在与模数m互素的全部剩余类中，各取一个数所组成的集叫做模数m的一组缩系。

- $\mathbb{Z}_m^* = \{x \in \mathbb{Z}_m | \gcd(x, m) = 1\}$是模数$m$的一组缩系。
- 定义欧拉函数$\phi(m) = |\mathbb{Z}_m^*|$
- $(\mathbb{Z}_m^*, \cdot)$是Abel群，其中$\cdot$表示模m乘法运算。

3 缩系

定理3： 若$(a,m)=1$，x通过模数m的缩系，则ax也通过模数m的缩系。

证明： 不失一般性，我们只需要证明对任意$a\in\mathbb{Z}_m^*$，

$$\{ax \bmod m | a\in\mathbb{Z}_m^*\}=\mathbb{Z}_m^*$$

$\mathbb{Z}_m^*$对模m乘法运算是群，满足封闭性，因此只需要证明：
$\forall b,c\in\mathbb{Z}_m^*$，且$b\neq c$必有$ab\not\equiv ac \pmod{m}$。
如若不然：

$$a^{-1}\cdot ab\equiv a^{-1}\cdot ac \pmod{m}\Rightarrow b\equiv c \pmod{m}\text{，矛盾！}$$

定理4（欧拉定理）： 设$m>1$，$(a,m)=1$，则

$$a^{\phi(m)} \equiv 1 \pmod m$$

证明： 由定理3知对任意$a\in\mathbb{Z}_m^*$，

$$\{ax \bmod m | a\in\mathbb{Z}_m^*\}=\mathbb{Z}_m^*$$

设$\mathbb{Z}_m^*=\{r_1,r_2,\ldots,r_{\phi(m)}\}$，那么有

$$\begin{aligned}
(a\cdot r_1)\times(a\cdot r_2)\times\ldots\times(a\cdot r_{\phi(m)}) &\equiv a^{\phi(m)}r_1r_2\ldots r_{\phi(m)} \pmod m\\
&\equiv r_1r_2\ldots r_{\phi(m)} \pmod m\\
&\Downarrow\\
a^{\phi(m)} &\equiv 1 \pmod m
\end{aligned}$$

注： 定理4说明了，$(a,m)=1$时，$a^{-1}\equiv a^{\phi(m)-1} \pmod m$

定理5(费马小定理)：若p是素数，则

$$a^p \equiv a \pmod p$$

证明：

- 情况1：$\gcd(a,p)=1$。p为素数，所以$\phi(p)=p-1$，从定理4得到$a^{p-1}\equiv 1 \pmod p$，因此$a^p\equiv a \pmod p$.
- 情况2：$\gcd(a,p)\neq 1$。因为p为素数，那么$a\equiv 0 \pmod p$，因此$a^p\equiv a \pmod p$.

定理6： 设$m_1 > 0, m_2 > 0, (m_1, m_2) = 1$，$x_1, x_2$分别通过模数$m_1, m_2$的缩系，则$m_2x_1 + m_1x_2$通过模数$m_1m_2$的缩系。

证明： 我们由第二节定理4知道，若$(m_1, m_2) = 1$，当x_1, x_2分别通过模数m_1, m_2的完全剩余系时，$m_2x_1 + m_1x_2$通过模数m_1m_2的完全剩余系。因此我们只需要证明：
$(x_1, m_1) = 1, (x_2, m_2) = 1$当且仅当$(m_2x_1 + m_1x_2, m_1m_2) = 1$。
因为$(m_1, m_2) = 1$，由第2节定理4（该定理可改成充要条件）得到：

$$(m_2x_1 + m_1x_2, m_1m_2) = 1 \Longleftrightarrow$$
$$\begin{cases} (m_2x_1 + m_1x_2, m_1) = 1 & \Leftrightarrow & (m_2x_1, m_1) = 1 & \Leftrightarrow & (x_1, m_1) = 1 \\ (m_2x_1 + m_1x_2, m_2) = 1 & \Leftrightarrow & (m_1x_2, m_2) = 1 & \Leftrightarrow & (x_2, m_2) = 1 \end{cases}$$

后面的充分必要条件分别可由欧几里德算法原理、定理3得到。

- **备注：** 定理6也可由后面的中国剩余定理推出。

推论： 若$(m_1, m_2) = 1$，则$\phi(m_1 m_2) = \phi(m_1)\phi(m_2)$。
定理7: 设n的标准分解$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$，则

$$\phi(n) = n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_k}).$$

证明: 由上面定理得到$\phi(n) = \phi(p_1^{a_1}) \dots \phi(p_k^{a_k})$. 且有

$$\begin{aligned}
\phi(p^a) &= |\{x \in \mathbb{Z}_{p^a} : (x, p^a) = 1\}| \\
&= |\{x \in \mathbb{Z}_{p^a} : (x, p) = 1\}| \\
&= p^a - |\{x \in \mathbb{Z}_{p^a} : (x, p) \neq 1\}| \\
&= p^a - |\{x \in \mathbb{Z}_{p^a} : p|x\}| \\
&= p^a - |\{tp : t \in \mathbb{Z}_{p^{a-1}}\}| \\
&= p^a - p^{a-1} \\
&= p^a(1 - \frac{1}{p})
\end{aligned}$$

由此得证。

相关练习：练习4给出了费马小定理的另一证明，练习5的证明利用了费马小定理。
以下二个练习均利用了以下结论，后面也有定理的证明要用到该结论。证明留给同学们思考。

- 设p为素数，$0 < k < p$，则$p|\binom{p}{k}$.

练习4. 证明：若p是素数，则对任意的整数$h_1, \ldots, h_a$均有

$$(h_1 + \ldots + h_a)^p \equiv h_1^p + \ldots + h_a^p \pmod p,$$

由此推出费马小定理，进而推出欧拉定理。
提示：对a应用数学归纳法，并注意到当$0 < k < p$时$p|\binom{p}{k}$。
练习5. 证明：若$m^p + n^p \equiv 0 \pmod p$，则$m^p + n^p \equiv 0 \pmod{p^2}$，这里$p$是奇素数。
提示：由费马小定理和命题假设得到存在整数k有$m = pk - n$。

4 一次同余式

定义： 设$f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$，其中$n>0, a_i(i=0,\ldots,n)$是整数，又设$m>0$，则

$$f(x)\equiv 0 \pmod{m} \tag{4}$$

叫做模数m的**同余式**。若$a_n\not\equiv 0 \pmod{m}$，则n叫做(4)的**次数**，如果x_0满足$f(x_0)\equiv 0 \pmod{m}$，则$x\equiv x_0 \pmod{m}$叫做同余式(4)的**解**。不同的解是指互不同余的解。

例1： 用验算的方法知同余式

$$x^5+2x^4+x^3+2x^2-2x+3\equiv 0 \pmod{7}$$

仅有解$x\equiv 1,5,6 \pmod{7}$.

例2：同余式

$$x^4 - 1 \equiv 0 \pmod{16}$$

有8个解：$x \equiv 1, 3, 5, 7, 9, 11, 13, 15 \pmod{16}$.

例3：同余式

$$x^2 + 3 \equiv 0 \pmod{5}$$

没有解。

例4：设N_p表示以下同余式的解的个数

$$y^2 - x^3 + 1 \equiv 0 \pmod{p}, p\text{为素数}$$

则有$N_2 = 2, N_3 = 3, N_5 = 5, N_7 = 3$等等。

以下几个定理完全解决了一元一次同余式的解的问题。

定理1： 设$(a,m)=1, m>0$，则同余式

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

恰有一个解。

证明1： 不失一般性，设$a \in \mathbb{Z}_m^*$。因为$(a,m)=1$，因此$a^{-1} \bmod m$存在，

1. **存在解：** $aa^{-1}b \equiv b \pmod{m}$，因此$x = a^{-1}b \bmod m$为解。
2. **解唯一：** 若存在x, y有$ax \equiv ay \pmod{m}$，那么

$$x \equiv a^{-1}ax \equiv a^{-1}ay \equiv y \pmod{m}.$$

证明2（课本证明）： 因为$1, 2, \ldots, m$组成模数m的完全剩余系，$(a,m)=1$，故$a, 2a, \ldots, ma$也组成模数m的一组完全剩余系，故其中恰有一个数设为aj，适合$aj \equiv b \pmod{m}$，$x \equiv j \pmod{m}$就是所求的惟一解。

定理3：设$(a, m) = d$，$m > 0$，同余式

$$ax \equiv b \pmod{m} \tag{5}$$

有解的充分必要条件是$d|b$.
证明1：必要性：如果(5)有解，则由$d|a, d|m$推出$d|b$。
充分性：由第1节定理3的推论*知，同余式(5)等价于

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}} \tag{6}$$

因$\left(\frac{a}{d}, \frac{m}{d}\right) = 1$，故同余式(6) 有一组解，即(5)有一组解。
证明2：$ax \equiv b \pmod{m}$等价于存在整数y有$ax - b = ym$，即

$$ax + ym = b$$

由第一章第8节的定理1知该一次不定方程有解当且仅当

$$(a, m)|b$$

定理4： 设$(a, m) = d, m > 0, d|b$，则同余式

$$ax \equiv b \pmod{m} \tag{7}$$

恰有d个解。设t是其中一个解，则模数m的d个互不同余的解为

$$x = t + k \cdot \frac{m}{d}, k = 0, 1, 2, \ldots, d-1$$

证明思路： x是(7)的解当且仅当x是以下同余式(8)的解。

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}} \tag{8}$$

设t是(8)的解，则

$$x \equiv t \pmod{\frac{m}{d}}$$

那么

$$x = t + k \cdot \frac{m}{d}, k = 0, \pm 1, \pm 2, \ldots$$

对模数m来说，恰好可选出d个互不同余的整数解：

$$x = t + k \cdot \frac{m}{d}, k = 0, 1, 2, \ldots, d-1$$

4 一次同余式

对定理4的应用是本节重点。相关练习：课本练习22.

定理5: 设$k \geq 1$，同余式

$$a_1 x + \ldots + a_{k-1} x_{k-1} + a_k x_k + b \equiv 0 \pmod{m} \tag{9}$$

有解的充分必要条件是

$$(a_1, \ldots, a_k, m) | b. \tag{10}$$

若(10)满足，则(9)的解数为$m^{k-1}(a_1, \ldots, a_k, m)$
证明: 用数学归纳法证明。(1)$k = 1$时，由定理3、4知道为真。
(2)设$(a_1, \ldots, a_k, m) = d, (a_1, \ldots, a_{k-1}, m) = d_1$，则$(d_1, a_k) = d$.

$$(9) \Rightarrow a_k x_k + b \equiv 0 \pmod{d_1} \ (\text{因为} d_1 | (a_1, \ldots, a_{k-1})) \tag{11}$$

由定理4知(11) 有$(a_k, d_1) = d$个
解$x_k = t + \frac{d_1}{d} k \bmod d_1, k = 0, \ldots, d-1$. 故对模数$m$来说有$d \cdot \frac{m}{d_1}$个解

$$(t + \frac{d_1}{d} k + d_1 t) \bmod m, k = 0, \ldots, d-1, t = 0, \ldots, \frac{m}{d_1}$$

而对(11)的一个解x_k，设$\frac{a_k x_k + b}{d_1} = b_1$,由归纳法假定

$$a_1 x + \ldots + a_{k-1} x_{k-1} + b_1 d_1 \equiv 0 \pmod{m}$$

的解数为$m^{k-2}(a_1, \ldots, a_{k-1}, m) = m^{k-2} d_1$，故(9)的解数为

$$m^{k-2} d_1 \cdot d \cdot \frac{m}{d_1} = m^{k-1} d$$

5 模数是素数的同余式

定理1:设p是一个素数,

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

是一个整系数多项式，则同余式

$$f(x) \equiv 0 \pmod p \tag{12}$$

最多有n个（模p不同的）解。
注: 若x_0满足(12)，以下简称为$f(x)$的解。

证明: 对$f(x)$的次数n进行归纳。
(1)当$n=1$时，

$$f(x)=a_1x+a_0\equiv 0 \pmod p \tag{13}$$

由$a_1\not\equiv 0 \pmod p \Rightarrow (a_1,p)=1\Rightarrow$ (13)恰有一个解。
(2)设对$n-1(n\geq 2)$时定理成立，现在证明(12)最多有n个解。
当$n\geq p$时，解个数$\leq|\mathbb{Z}_p|=p$，结论成立。
当$n\leq p-1$。设x_0是$f(x)$ 的一个解，那么

$$f(x)-f(x_0)=\sum_{k=1}^{n}a_k(x^k-x_0^k)=(x-x_0)g(x)$$

其中$g(x)$是首项系数为a_n的$n-1$次整系数多项式。则对$f(x)$的解$x\not\equiv x_0 \pmod p$有

$$\begin{array}{rccll} & f(x) & \equiv & 0 & \pmod p \\ \Leftrightarrow & f(x)-f(x_0) & \equiv & 0 & \pmod p \\ \Leftrightarrow & (x-x_0)g(x) & \equiv & 0 & \pmod p \\ \Leftrightarrow & g(x) & \equiv & 0 & \pmod p \quad (\text{因为}(x-x_0,p)=1) \end{array}$$

由归纳假设，$g(x)$最多有$n-1$个解，所以$f(x)$最多有n个解。

5 模数是素数的同余式

注.

- 定理1用代数的语言描述是：有限域$\mathbb{Z}_p$上的n次方程

  $$f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0, a_i\in\mathbb{Z}_p(i=0,\ldots,n)$$

  且$a_n\neq 0$。则$f(x)$最多有n个解。
- 定理1可推广到一般域上：设F是域，其加法单位元为0。$f(x)$是F上的n次多项式

  $$f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0, a_i\in F(i=0,\ldots,n)$$

  且$a_n\neq 0$，则$f(x)=0$在域F上最多有n个解。

5 模数是素数的同余式

以下几个定理是对定理1的应用.
定理2: 设同余式

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

的解的个数$> n$，这里p是素数，a_i是整数$(i = 0, 1, \ldots, n)$，则$a_i \equiv 0 \pmod p (i = 0, 1, \ldots, n)$.
证明思路:如果$f(x)$有某些系数不被p整除，设这些系数的下标最大值为k，则$k \leq n$，k次同余式

$$a_k x^k + a_{k-1} x^{k-1} + \ldots + a_1 x + a_0 \equiv 0 \pmod p, p \nmid a_k$$

的解的个数$\geq k$，与定理1矛盾。因此$f(x)$的所有系数被p整除。

定理3:对于任给素数p，多项式

$$f(x) = (x-1)(x-2)\dots(x-p+1) - x^{p-1} + 1$$

的所有系数被p整除.

证明思路:$f(x)$的次数$\leq p-2$。如果$f(x) \equiv 0 \pmod p$的解的个数$> p-2$，那么由定理2知道$f(x)$的所有系数被p整除。现证明之。

对任意$x \in \mathbb{Z}_p^*$有

$$\begin{cases} x^{p-1} - 1 \equiv 0 \pmod p \quad \text{(费马小定理)} \\ (x-1)(x-2)\dots(x-p+1) \equiv 0 \pmod p \end{cases}$$

$$\Rightarrow f(x) \equiv 0 \pmod p \text{的解的个数} \geq p-1 > p-2$$

定理4(Wolstenholme定理):设素数$p>3$，则有

$$s_{p-2}=\sum_{k=1}^{p-1}\frac{(p-1)!}{k}\equiv 0 \pmod{p^2}.$$

证明:设

$$\begin{aligned} g(x) &= (x-1)(x-2)\ldots(x-p+1) \\ &= x^{p-1}-s_1x^{p-2}+s_2x^{p-3}+\ldots-s_{p-2}x+(p-1)! \end{aligned}$$

$$\left.\begin{array}{l} (1)\,g(x)=f(x)+x^{p-1}-1\text{，}f(x)\text{由定理3所定义} \\ \qquad\quad \Rightarrow g(x),f(x)\text{的}x^j(1\le j\le p-2)\text{的系数都为}\pm s_j \\ (2)\text{根据定理3，}f(x)\text{的所有系数被}p\text{整数} \end{array}\right\}$$

$$\Longrightarrow p|s_j(1\le j\le p-2)$$

$$\begin{aligned} & g(p)=(p-1)!=p^{p-1}-s_1p^{p-2}+\ldots-ps_{p-2}+(p-1)! \\ \Rightarrow\ & p^{p-1}-s_1p^{p-2}+\ldots+p^2s_{p-3}-ps_{p-2}=0 \\ \Rightarrow\ & ps_{p-2}\equiv 0 \pmod{p^3}\ (\text{由}p>3\text{、上式两边取模数}p^3\text{，及}p|s_j\text{得到}) \\ \Rightarrow\ & s_{p-2}\equiv 0 \pmod{p^2} \end{aligned}$$

5 模数是素数的同余式

本节重点是对定理1的应用。相关练习：课本练习14。

- 练习14.证明：对任意整数x，$\frac{1}{5}x^5+\frac{1}{3}x^3+\frac{7}{15}x$是一个整数。
  提示：即证明$\frac{1}{15}(3x^5+5x^3+7x)$是整数，等价于证明$3x^5+5x^3+7x\equiv 0 \pmod{15}$。应用定理1（或直接应用定理2）和下一节的中国剩余定理完全证明。

6 孙子剩余定理及其应用举例

定理1(中国剩余定理或孙子定理) 假定$m_1, \ldots, m_k$为两两互素的正整数，又假定$b_1, \ldots, b_k$为整数，那么同余方程组

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x &\equiv b_k \pmod{m_k} \end{aligned}$$

有模$M = m_1 \times m_2 \times \ldots \times m_k$的唯一解，且由下式给出

$$x = \sum_{i=1}^{k} b_i M_i M_i' \bmod M$$

其中

$$M_i = \frac{M}{m_i}, M_i' = M_i^{-1} \bmod m_i, 1 \le i \le k.$$

证明:解的正确性可直接验证。我们看到：

$$M_i \equiv \frac{M}{m_i} \equiv \frac{m_1 m_2 \dots m_k}{m_i} \pmod{m_j} \begin{cases} = 0, j \neq i \\ \neq 0, j = i \end{cases}$$

因而

$$M_i M_i' \bmod m_j = \begin{cases} 0, j \neq i \\ 1, j = i \end{cases}$$

因此

$$x = \sum_{i=1}^{k} b_i M_i M_i' \bmod M \equiv b_j \pmod{m_j}$$

解唯一性证明（反证法）：如果解不唯一，即存在$x \not\equiv y \bmod M$同时满足同余方程组，那么有

$$x - y \not\equiv 0 \bmod M$$

那么存在s, t且$0 < t < M$满足

$$x - y = sM + t = sm_1 m_2 \dots m_k + t$$

因为$m_1, m_2, \dots, m_k$互素，必然存在m_j使得$t \nmid m_j$，也就是

$$x - y = sm_1 \dots m_j \dots m_k + t \equiv t \not\equiv 0 \bmod m_j$$

另一方面$x - y \equiv a_j - a_j \equiv 0 \bmod m_j$, 矛盾！因此解是唯一的。

Example

例 假定$k = 3, m_1 = 7, m_2 = 11, m_3 = 13$，同余方程组

$$x \equiv 5 \pmod 7, x \equiv 3 \pmod{11}, x \equiv 10 \pmod{13}$$

存在模$M = 7 \times 11 \times 13 = 1001$的唯一解。解如下计算：

$$M_1 = 143, M_2 = 91, M_3 = 77$$

$$M_1' = M_1^{-1} \bmod m_1 = 5, M_2' = 4, M_3' = 12$$

因此

$$x = (5 \times 143 \times 5 + 3 \times 91 \times 3 + 10 \times 77 \times 12) \pmod{1001} = 894$$

定义映射

$$\varphi : \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_k} \to \mathbb{Z}_M, M = m_1 m_2 \ldots m_k$$
$$\forall (b_1, b_2, \ldots, b_k) \in \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_k}$$
$$\varphi(b_1, b_2, \ldots, b_k) = x$$

其中$x \in \mathbb{Z}_M$是以下同余方程组的解

$$\begin{array}{rcll} x & \equiv & b_1 & \pmod{m_1} \\ \vdots & & \vdots & \\ x & \equiv & b_k & \pmod{m_k} \end{array} \tag{14}$$

当正整数$m_1, m_2, \ldots, m_k$两两互素时，φ是双射，因为：

- φ为单射：由中国剩余定理，其解唯一，因此是单射。
- φ为满射：显然，对于任意$x \in \mathbb{Z}_M$，$b_i = x \bmod m_i (1 \leq i \leq k)$满足同余方程组(14)。

φ也是$\mathbb{Z}^*_{m_1} \times \mathbb{Z}^*_{m_2} \times \ldots \times \mathbb{Z}^*_{m_k} \to \mathbb{Z}^*_M$上的双射，因为：

- $(b_1, \ldots, b_k) \in \mathbb{Z}^*_{m_1} \times \mathbb{Z}^*_{m_2} \times \ldots \times \mathbb{Z}^*_{m_k}$，那么$(b_i, m_i) = 1 \Rightarrow (x, m_i) = 1$，因此$(x, M = m_1 \ldots m_k) = 1$，即$x \in \mathbb{Z}^*_M$。
- 若$x \in \mathbb{Z}^*_M$，即$(x, M) = 1$，那么$1 = (x, m_i) = (b_i, m_i)$，即$b_i \in \mathbb{Z}^*_{m_i}$。

因为φ为$\mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^* \times \ldots \times \mathbb{Z}_{m_k}^* \to \mathbb{Z}_M^*$上的双射，因此

$$\phi(M) = |\mathbb{Z}_M^*| = |\mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^* \times \ldots \times \mathbb{Z}_{m_k}^*| = \phi(m_1) \ldots \phi(m_k)$$

$k = 2$时为第3节推论：若$(m_1, m_2) = 1$，则$\phi(m_1 m_2) = \phi(m_1)\phi(m_2)$。

第2节定理4及第3节定理6：设$m_1>0, m_2>0, (m_1,m_2)=1$，那么：
（1）x_1,x_2分别通过模数m_1,m_2的完全剩余系，则$m_2x_1+m_1x_2$通过模数m_1m_2的完全剩余系；
（2）x_1,x_2分别通过模数m_1,m_2的缩系，则$m_2x_1+m_1x_2$通过模数m_1m_2的缩系。
证明思路:前面所定义的函数$\varphi:\mathbb{Z}_{m_1}\times\mathbb{Z}_{m_2}\to\mathbb{Z}_{m_1m_2}$是双射。那么任意整数$x_1,x_2$，有唯一$b_1\in\mathbb{Z}_{m_1}, b_2\in\mathbb{Z}_{m_2}$，有

$$\varphi(b_1,b_2)\equiv m_2x_1+m_1x_2 \pmod{m_1m_2} \Rightarrow \begin{cases} b_1 &= m_2x_1 \bmod m_1 \\ b_2 &= m_1x_2 \bmod m_2 \end{cases}$$

因为$(m_1,m_2)=1$，当x_1,x_2分别通过模数m_1,m_2的完全剩余系时，b_1,b_2也分别通过模数m_1,m_2的完全剩余系，即b_1,b_2将分别遍历$\mathbb{Z}_{m_1},\mathbb{Z}_{m_2}$，那么$\varphi(b_1,b_2)$遍历$\mathbb{Z}_{m_1m_2}$，即$m_2x_1+m_1x_2$通过模数$m_1m_2$的完全剩余系。现在证明了（1）。
由

$$(m_2x_1+m_1x_2, m_1m_2)=1 \Longleftrightarrow (x_1,m_1)=1, (x_2,m_2)=1$$

得到(2)。

孙子定理在RSA公钥密码体制中的应用。 RSA公钥密码体制的解密过程如下：

输入 n, y, a，其中$n = pq$，p, q为大素数。

计算 $y^a \bmod n$

使用平方—乘算法计算$y^a \bmod n$的计算时间为$c\log(n)^2 \log a$，一般a的长度和n接近，那么其计算时间为$c(\log n)^3$.
如果知道素数p, q（它们可作为公钥的一部分），就可以利用中国剩余定理节约计算时间：

预计算： $a_p \leftarrow a \bmod p-1, a_q \leftarrow a \bmod q-1,$
$M_p = q^{-1} \bmod p, M_q = p^{-1} \bmod q.$

1. 计算$x_p \leftarrow y^{a_p} \bmod p, x_q \leftarrow y^{a_q} \bmod q$
2. 计算$x \leftarrow M_p q x_p + M_q p x_q \bmod n$。由中国剩余定理知道，$x$是以下同余方程组的解

$$\left.\begin{array}{lll} x & \equiv y^{a_p} \equiv & y^a \bmod p \\ x & \equiv y^{a_q} \equiv & y^a \bmod q \end{array}\right\} \Leftrightarrow x \equiv y^a \bmod pq$$

第1步骤的计算时间为$c(\log(p)^3 + \log(q)^3)$，一般p, q长度约为n的一半，那么计算时间为$\frac{1}{4}c(\log n)^3$。第2步骤的计算时间为$O((\log n)^2)$。大约节约了75%的时间。

定理2： 一次同余式组

$$x \equiv b_1 \pmod{m_1}, x \equiv b_2 \pmod{m_2} \tag{15}$$

可解的充分必要条件是$(m_1, m_2) | b_1 - b_2$，且当(15)可解时对模数$[m_1, m_2]$有惟一解。

证明: 必要性： 设(15)有公解x_0，$(m_1, m_2) = d$，则有

$$x_0 \equiv b_1 \pmod{d}, x_0 \equiv b_2 \pmod{d},$$

两式相减即得$d | b_1 - b_2$。

充分性：

$$x \equiv b_1 \pmod{m_1} \quad \Leftrightarrow \quad x = b_1 + m_1 y，代入x \equiv b_2 \pmod{m_2}得$$

$$m_1 y \equiv b_2 - b_1 \pmod{m_2} \quad (*)$$

因为$(m_1, m_2) | b_2 - b_1$，故(*)有解，那么(15)有解。

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \end{cases} \Rightarrow \begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{\frac{m_2}{(m_1, m_2)}} \end{cases}$$

$$\Rightarrow \quad 由中国剩余定理，对模数 m_1 \cdot \frac{m_2}{(m_1, m_2)} = [m_1, m_2]解惟一.$$

对一次同余方程组

$$
\begin{aligned}
x &\equiv b_1 \pmod{m_1} \\
x &\equiv b_2 \pmod{m_2} \\
&\cdots \\
x &\equiv b_k \pmod{m_k}
\end{aligned}
$$

$k \geq 3$的情形，可先解前面两个得

$$
\begin{aligned}
x &\equiv b_1 \pmod{m_1} \\
x &\equiv b_2 \pmod{m_2}
\end{aligned}
\Rightarrow
\begin{cases}
\text{无解} \\
\text{或} x \equiv b_2' \pmod{[m_1, m_2]}
\end{cases}
$$

和下一个同余式联合得到

$$
\begin{aligned}
x &\equiv b_2' \pmod{[m_1, m_2]} \\
x &\equiv b_3 \pmod{m_3}
\end{aligned}
\Rightarrow
\begin{cases}
\text{无解} \\
\text{或} x \equiv b_3' \pmod{[m_1, m_2, m_3]}
\end{cases}
$$

$$\cdots$$

$$
\begin{aligned}
x &\equiv b_{k-1}' \pmod{[m_1, \ldots, m_{k-1}]} \\
x &\equiv b_k \pmod{m_k}
\end{aligned}
\Rightarrow
\begin{cases}
\text{无解} \\
\text{或} x \equiv b_k' \pmod{[m_1, \ldots, m_k]}
\end{cases}
$$

定理3： 若$m_1, m_2, \ldots, m_k$是k个两两互素的正整数，$m = m_1 \ldots m_k$，则同余式

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

有解的充分必要条件是同余式

$$f(x) \equiv 0 \pmod{m_i} (i = 1, \ldots, k)$$

的每一个有解。并且，若用T_i表示$f(x) \equiv 0 \pmod{m_i}$的解数，T表示(*)的解数，则$T = T_1 T_2 \ldots T_k$.

证明思路： 因为$m_1, m_2, \ldots, m_k$两两互素，应用中国剩余定理得到

$$f(x) \equiv 0 \pmod{m} \Leftrightarrow \left.\begin{array}{l} f(x) \equiv 0 \pmod{m_1} \Leftrightarrow x \equiv u_1 \pmod{m_1} \\ f(x) \equiv 0 \pmod{m_2} \Leftrightarrow x \equiv u_2 \pmod{m_2} \\ \qquad\qquad \ldots \\ f(x) \equiv 0 \pmod{m_k} \Leftrightarrow x \equiv u_k \pmod{m_k} \end{array}\right\}$$
$$\Leftrightarrow x \equiv u \pmod{m = m_1 m_2 \ldots m_k}$$

以上u_i表示$f(x) \equiv 0 \pmod{m_i}$的某个解，u表示$f(x) \equiv 0 \pmod{m}$的某个解。

从以上的一一对映关系可以看出，$T = T_1 T_2 \ldots T_k$。

本节重点是对中国剩余定理及其推广（定理2，定理3）的应用。相关练习：课本练习10、15、20、24。

例： 解同余式$6x^3+27x^2+17x+20\equiv 0 \pmod{30}$.

解： 设$f(x)=6x^3+27x^2+17x+20$，由定理3知解同余式$f(x)\equiv 0 \pmod{30}$等价于解同余方程组

$$\begin{array}{lll} f(x)\equiv 0 \pmod 5 & \Rightarrow & x\equiv 0,1,2 \pmod 5 \\ f(x)\equiv 0 \pmod 6 & \Rightarrow & x\equiv 2,5 \pmod 6 \end{array}$$

由中国剩余定理

$$\begin{array}{l} x\equiv b_1 \pmod 5 \\ x\equiv b_2 \pmod 6 \end{array} \Leftrightarrow x\equiv 6b_1+25b_2 \pmod{30}$$

b_1分别取$0,1,2$，b_2分别取$2,5$时，得到$f(x)\equiv 0 \pmod{30}$的6个解

$$x\equiv 2,5,11,17,20,26 \pmod{30}.$$

练习10. 证明：若n是任意整数，则$n^9 - n^3 \equiv 0 \pmod{504}$.
提示：$504 = 2^2 \cdot 3^3 \cdot 7$。应用中国剩余定理。
练习15. 求出最小的正整数，它的$\frac{1}{2}$是一个整数的平方，它的$\frac{1}{3}$是一个整数的三次方，它的$\frac{1}{5}$是一个整数的五次方。
提示：先求x满足$x \equiv 0 \pmod 2, x \equiv 0 \pmod 3, x \equiv 0 \pmod 5$。
练习20. 证明：对于任给的$n > 1$，存在$m > 0$，使同余式

$$x^2 \equiv 1 \pmod m$$

解的个数大于n.
提示：可取$m = p_1 p_2 \dots p_n$，$p_1, \dots, p_n$是n个不同的素数。
练习24. 解下列同余式组：

1. $x \equiv 1 \pmod 7, x \equiv 3 \pmod 5, x \equiv 5 \pmod 9$;
2. $3x \equiv 5 \pmod 4, 5x \equiv 2 \pmod 7$;
3. $4x \equiv 3 \pmod{25}, 3x \equiv 8 \pmod{20}$;
4. $x \equiv 8 \pmod{15}, x \equiv 15 \pmod 8, x \equiv 13 \pmod{25}$.

提示：应用第4节（一次同余式）的解法和本节的中国剩余定理及其推广。

7 模数是素数幂的同余式

本节讨论模数是素数幂的同余式

$$f(x) = a_n x^n + \ldots + a_1 x_+ a_0 \equiv 0 \pmod{p^\alpha}, \quad (*)$$

$$n > 0, p^\alpha \not| a_n,$$

其中p是素数，$\alpha \geq 1$。
显然，适合(*)的每一个整数都适合同余式

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

但反之未必成立。
例： 2是$x^{10} - 1 \equiv 0 \pmod{11}$的解，但不是$x^{10} - 1 \equiv 0 \pmod{11^2}$的解。

定理1：设$x \equiv x_1 \pmod{p}$，即

$$x = x_1 + pt_1(t_1 = 0, \pm 1, \pm 2, \ldots) \qquad (**)$$

是(#)的一个解，且$p \nmid f'(x_1)$，这里$f'(x) = \sum_{i=1}^{n} ia_i x^{i-1}$表示$f(x)$的导函数，则(**)恰好给出(*)的一个解$x \equiv x_\alpha \pmod{p^\alpha}$，即

$$x = x_\alpha + p^\alpha t_\alpha(t_\alpha = 0, \pm 1, \pm 2, \ldots),$$

其中$x_\alpha \equiv x_1 \pmod{p}$.

证明：对α进行数学归纳法。当$\alpha = 1$时，定理显然成立。

现假定定理对$\alpha - 1 \geq 1$时成立，即(**)恰好给出了$f(x) \equiv 0 \pmod{p^{\alpha-1}}$的一个解

$$x = x_{\alpha-1} + p^{\alpha-1}t_{\alpha-1}(t_{\alpha-1} = 0, \pm 1, \pm 2, \ldots), \text{且} x_{\alpha-1} \equiv x_1 \pmod{p}.$$

把$x = x_{\alpha-1} + p^{\alpha-1}t_{\alpha-1}$代入(*)得

$$f(x) = a_n(x_{\alpha-1}+p^{\alpha-1}t_{\alpha-1})^n+\ldots+a_1(x_{\alpha-1}+p^{\alpha-1}t_{\alpha-1})+a_0 \equiv 0 \pmod{p^\alpha}$$

又由于

$$\begin{aligned}
& a_k(x_{\alpha-1} + p^{\alpha-1}t_{\alpha-1})^k \\
= & a_k x_{\alpha-1}^k + a_k \cdot k x_{\alpha-1}^{k-1} p^{\alpha-1} t_{\alpha-1} + a_k \cdot \binom{k}{2} x_{\alpha-1}^{k-2} p^{2\alpha-2} t_{\alpha-1}^2 + \ldots \\
\equiv & a_k x_{\alpha-1}^k + a_k \cdot k x_{\alpha-1}^{k-1} p^{\alpha-1} t_{\alpha-1} \pmod{p^\alpha}
\end{aligned}$$

证明续：因此可得

$$\begin{aligned}
&f(x_{\alpha-1}) + p^{\alpha-1} t_{\alpha-1} f'(x_{\alpha-1}) \equiv 0 \pmod{p^\alpha} \Rightarrow \\
&\left.\begin{aligned} p^{\alpha-1} t_{\alpha-1} f'(x_{\alpha-1}) \equiv -f(x_{\alpha-1}) \pmod{p^\alpha} \\ \text{由归纳假设知} f(x_{\alpha-1}) \equiv 0 \pmod{p^{\alpha-1}} \end{aligned}\right\} \Rightarrow \\
&\left.\begin{aligned} t_{\alpha-1} f'(x_{\alpha-1}) \equiv -\frac{f(x_{\alpha-1})}{p^{\alpha-1}} \pmod{p} \\ \text{由归纳假设知} x_{\alpha-1} \equiv x_1 \pmod{p} \end{aligned}\right\} \Rightarrow \\
&\left.\begin{aligned} t_{\alpha-1} f'(x_1) \equiv -\frac{f(x_{\alpha-1})}{p^{\alpha-1}} \pmod{p} \\ \text{由归纳假设知} (f'(x_1), p) = 1 \end{aligned}\right\} \Rightarrow \\
&\text{上式恰好有一解} t_{\alpha-1} = t'_{\alpha-1} + pt_\alpha (t_{\alpha=0,\pm1,\ldots}),
\end{aligned}$$

这就得到了(*)的解

$$\begin{aligned}
x &= x_{\alpha-1} + p^{\alpha-1}(t'_{\alpha-1} + pt_\alpha) \\
&= x_{\alpha-1} + p^{\alpha-1} t'_{\alpha-1} + p^\alpha t_\alpha (t_\alpha = 0, \pm 1, \ldots)
\end{aligned}$$

令$x_{\alpha-1} + p^{\alpha-1} t'_{\alpha-1} = x_\alpha$，即$x \equiv x_\alpha \pmod{p^\alpha}$是(*)的一个解，且$x_\alpha \equiv x_1 \pmod{p}$。

7 模数是素数幂的同余式

推论： 设$f(x)\equiv 0 \pmod p$和$f'(x)\equiv 0 \pmod p$无公解，则同余式$f(x)\equiv 0 \pmod{p^\alpha}$和$f(x)\equiv 0 \pmod p$的解数相同。

- 定理1的证明是构造性的，它提供了一个由$f(x)\equiv 0 \pmod{p^{\alpha-1}}$的解给出$f(x)\equiv 0 \pmod{p^\alpha}$的解的方法。
- 课本练习25、26、27可由本节定理1及其证明中提供的构造方法给出，练习27还需要联合中国剩余定理。