初等数论
第二章 同余

卢 伟
Email: luwei3@mail.sysu.edu.cn

中山大学 数据科学与计算机学院

第一章主要内容

- 整除的性质: $c|b, b|a \Rightarrow c|a; a|b, b|a \Rightarrow a = \pm b; c|a, c|b \Rightarrow c|(sa \pm tb)$
- 素数的性质: 任何合数n都有素数的因子: 所有n的正数的因子中最小的那一个, $p \leq \sqrt{n}$; 素数一定有无穷多个; 如果对所有的小于等于$\sqrt{n}$的素数q来说, q都不能整除n, 那么n一定是素数; 判断n是否为素数; 查找小于n的素数的方法, 爱拉托色尼筛法; 切比雪夫不等式不超过x的素数的个数.
- 欧几里德除法: $a \in \mathbb{Z}, b \in \mathbb{Z}^+, \exists (q, r) s.t. a = bq + r, 0 \leq r < b$; 正整数的$b$进制表示$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$

第一章主要内容

- 最大公约数，互素定义，$a_1,\ldots,a_n$ 两两互素与$a_1,\ldots,a_n$互素的区别:
  - 最大公因数的简单性质：如果$p\nmid a$，则$(a,p)=1; a=bq+c\Rightarrow(a,b)=(b,c)$; 辗转相除法求最大公因数
  - 辗转相除法导出的性质
    (a) $\exists s,t\in\mathbb{Z}, s.t. (a,b)=s\cdot a+t\cdot b$; s和t的求法
    (b) 最大公约数的等价定义，互素的等价定义; $(a_1,a_2,a_3)=((a_1,a_2),a_3)$ (c) $\forall m\in\mathbb{Z}^+, (am,bm)=(a,b)m; (\frac{x}{(x,y)},\frac{y}{(x,y)})=1$ (d) $(a,c)=1\Rightarrow(ab,c)=(b,c); (a_1,c)=(a_2,c)=\ldots=(a_n,c)=1\Rightarrow(a_1a_2\ldots a_n,c)=1; (a,c)=1, c|ab\Rightarrow c|b; p|ab\Rightarrow p|ap|b; n>1$可唯一表示成: $n=p_1^{\alpha_1}\cdot p_2^{\alpha^2}\cdot\ldots\cdot p_t^{\alpha^t}, \alpha_1,\alpha_2,\ldots,\alpha_t\in\mathbb{Z}^+$
- 最小公倍数:
  $a|b, b|m\Rightarrow[a,b]|m; (a,b)=1\Rightarrow[a,b]=ab; a|m, b|m, (a,b)=1\Rightarrow ab|m; [p,q]=pq; a_1|m, a_2|m,\ldots,a_n|m\Rightarrow[a_1,a_2,\ldots,a_n]|m; [a,b]=\frac{ab}{(a,b)}; [a_1,a_2,a_3]=[[a_1,a_2],a_3]; \forall a,b\in\mathbb{Z}^+, \exists a'|a, b'|b, (a',b')=1, s.t. a'\cdot b'=[a,b]$

例题: 对于任给的正整数k, 必有k个连续正整数都是合数.

证明: $k=1$的话, 很显然, 比如4:
$k=2$的话, 可以构造这样的数为$(2+1)!+2,(2+1)!+3$; $k=3$的话, 可以构造这样的数为$(3+1)!+2,(3+1)!+3,(3+1)!+4$; $k=4$的话, 可以构造这样的数为$(4+1)!+2,(4+1)!+3,(4+1)!+4,(4+1)!+5$; ....

一般地, 对于任给的正整数k, 可以构造这样的正整数为
(k+1)!+2,(k+1)!+3,(k+1)!+4,(k+1)!+5,(k+1)!+6,. . . ,(k+1)!+(k+1)

1. 同余

同余: 给定一个正整数m, 设a, b是任意两个整数, 如果m整除$a-b$:

$$m|(a-b)$$

(即存在$k \in \mathbb{Z}, s.t., a-b=km(i.e., a=km+b)$)
则称a与b模m同余, 记作$a \equiv b(\bmod m)$

否则, 称a与b模m不同余, 记作$a \not\equiv b(\bmod m)$

比如, 7|(27 − 6), 1是29被7除的余数,
所以: $27 \equiv 6(\bmod 7), 29 \equiv 1(\bmod 7)$

同余的基本性质

1. 任意整数与它自身模m同余: $a \equiv a \bmod m$; 此即自反性.
2. 如果a与b模m同余, 则b与a模m同余: 即

$$a \equiv b \bmod m \Rightarrow b \equiv a \bmod m$$

   这是因为

$$a \equiv b \bmod m \Rightarrow \exists k \in \mathbb{Z}, s.t. a = km + b$$

$$\Rightarrow \exists(-k) \in \mathbb{Z}, s.t. b = (-k)m + a \Rightarrow b \equiv a \bmod m$$

   此即对称性.
3. 如果a与b模m同余, b与c模m同余, 则称a与c模m同余:

$$a \equiv b \bmod m, b \equiv c \bmod m \Rightarrow a \equiv c \bmod m$$

   事实上,

$$a \equiv b \bmod m \Rightarrow \exists k_1 \in \mathbb{Z}, s.t. a = k_1 m + b$$

$$b \equiv c \bmod m \Rightarrow \exists k_2 \in \mathbb{Z}, s.t. b = k_2 m + c$$

   从而 $a = k_1 m + (k_2 m + c) = (k_1 + k_2)m + c$
   即a与c模m同余, 此即传递性.

示例: $m \in \mathbb{Z}^+, a \in \mathbb{Z}, C_a \triangleq \{c|a \equiv c \bmod m, c \in \mathbb{Z}\}$, 则

- C_a必非空;
  显然, 因为$a \in C_a$.
- 任意整数必包含在$C_0, C_1, \ldots, C_{m-1}$中的一个;
  $\forall c \in \mathbb{Z}, \exists q \in \mathbb{Z}, 0 \le r < m, s.t. c = qm + r$, 从而$c \equiv r \bmod m$.
  根据上述集合的定义, $c \in C_r$.
- $C_a = C_b \iff a \equiv b \bmod m$;
  "$\Rightarrow$"比较简单: $b \in C_b = C_a \Rightarrow b \equiv a \bmod m$
  "$\Leftarrow$": 给定$a \equiv b \bmod m$, 要证明$C_a = C_b$, 需要说明$\forall c \in C_a \Rightarrow c \in C_b$和$\forall c \in C_b \Rightarrow c \in C_a$.

  $$\forall c \in C_a \Rightarrow c \equiv a \bmod m \Rightarrow c \equiv b \bmod m \Rightarrow c \in C_b$$

  对$\forall c \in C_b \Rightarrow c \in C_a$ 类似可证.
- $C_a \cap C_b = \phi \iff a \not\equiv b \bmod m$
  "$\Rightarrow$": 如果$a \equiv b \bmod m$的话, 则有$C_a \cap C_b = C_a$而不是空集;
  "$\Leftarrow$": 如果$C_a \cap C_b \neq \phi$的话, 比如$c \in C_a \cap C_b$, 则有$c \equiv a \bmod m, c \equiv b \bmod m$, 从而应该有$a \equiv b \bmod m$, 这与已知条件矛盾.

- 设m整除a的余数为r, m除b的余数为r'(r, r'为欧几里德除法的余数), 则

$$a \equiv b \bmod m \iff r = r'$$

已知: $a = km + r, b = k'm + r'(0 \leq r, r' < m)$
"$\Longleftarrow$":

$$r = r' \Rightarrow a - b = (k - k')m \Rightarrow a \equiv b \bmod m$$

"$\Longrightarrow$":

$$a - b = (k - k')m + (r - r')$$

而a与b模m同余, 即m整除$(a - b)$, 故$r - r' = 0$.

- 给定正整数m, 且$a_1 \equiv b_1 \bmod m, a_2 \equiv b_2 \bmod m$, 则$(a_1 \pm a_2) \equiv (b_1 \pm b_2) \bmod m$
事实上,

$$a_1 \equiv b_1 \bmod m \Rightarrow a_1 = k_1 m + b_1$$

$$a_2 \equiv b_2 \bmod m \Rightarrow a_2 = k_2 m + b_2$$

$$\therefore (a_1 + a_2) = (k_1 + k_2)m + (b_1 + b_2)$$

$$\therefore (a_1 + a_2) \equiv (b_1 + b_2) \bmod m$$

同样地, $(a_1 - a_2) \equiv (b_1 - b_2) \bmod m$

- 给定正整数m，且$a_1 \equiv b_1 \bmod m, a_2 \equiv b_2 \bmod m$，则$(a_1 \cdot a_2) \equiv (b_1 \cdot b_2) \bmod m$

事实上,

$$a_1 \equiv b_1 \bmod m \Longrightarrow a_1 = k_1 m + b_1$$

$$a_2 \equiv b_2 \bmod m \Longrightarrow a_2 = k_2 m + b_2$$

$$\begin{aligned}\therefore (a_1 \cdot a_2) &= (k_1 m + b_1)(k_2 m + b_2) = k_1 k_2 m^2 + k_1 b_2 m + k_2 b_1 m + b_1 b_2 \\ &= (k_1 k_2 m + k_1 b_2 + k_2 b_1) m + b_1 b_2\end{aligned}$$

$$\therefore (a_1 \cdot a_2) \equiv (b_1 \cdot b_2) \bmod m$$

  - 特殊地,我们有$\forall 0 \leq i \in \mathbb{Z}, a \equiv b \bmod m \Longrightarrow a^i \equiv b^i \bmod m$
  - $x \equiv y \bmod m, a_0 \equiv b_0 \bmod m, a_1 \equiv b_1 \bmod m, \ldots, a_k \equiv b_k \bmod m$

    $$\Longrightarrow (a_0 + a_1 x + a_2 x^2 + \ldots + a_k x^k) \equiv (b_0 + b_1 y + b_2 y^2 + \ldots + b_k y^k) \bmod m$$

示例:

给定十进制数$n=(a_k a_{k-1}\dots a_2 a_1 a_0)_{10}(0\le a_i\le 9)$, 则

$$3|n \iff 3|(a_k+a_{k-1}+\ldots+a_2+a_1+a_0)$$

$$9|n \iff 9|(a_k+a_{k-1}+\ldots+a_2+a_1+a_0)$$

事实上,

$$\left.\begin{array}{c} n=a_k\cdot 10^k+a_{k-1}\cdot 10^{k-1}+\ldots a_2\cdot 10^2+a_1\cdot 10+a_0 \\ 10\equiv 1 \bmod 3 \end{array}\right\} \Longrightarrow$$

$$a_k\cdot 10^k+a_{k-1}\cdot 10^{k-1}+\ldots a_2\cdot 10^2+a_1\cdot 10+a_0\equiv a_k\cdot 1^k+a_{k-1}\cdot 1^{k-1}+\ldots a_2\cdot 1^2+a_1\cdot 1+a_0$$

$$\therefore n\equiv(a_k+a_{k-1}+\ldots+a_2+a_1+a_0) \bmod 3$$

根据性质: 设m整除a的余数为r, m除b的余数为r'(r,r'为欧几里德除法的余数), 则$a\equiv b \bmod m \iff r=r'$. 即3除$n$的欧几里德除法余数与3除$(a_k+a_{k-1}+\ldots+a_2+a_1+a_0)$ 的欧几里德除法余数相同), 所以3除n的欧几里德除法余数为0当且仅当3除$(a_k+a_{k-1}+\ldots+a_2+a_1+a_0)$的欧几里德除法余数为0, 即

$$3|n \iff 3|(a_k+a_{k-1}+\ldots+a_2+a_1+a_0)$$

对9的情况证明完全类似.

示例:
给定1000进制数$n = (a_k a_{k-1} \dots a_2 a_1 a_0)_{1000} (0 \le a_i \le 999)$，则

$$7|n \iff 7|[(a_0+a_2+a_4+\dots)-(a_1+a_3+a_5+\dots)]$$

$$11|n \iff 11|[(a_0+a_2+a_4+\dots)-(a_1+a_3+a_5+\dots)]$$

$$13|n \iff 13|[(a_0+a_2+a_4+\dots)-(a_1+a_3+a_5+\dots)]$$

事实上，$1000 = 7 \times 11 \times 13 - 1 \Longrightarrow 1000 \equiv -1 \bmod 7$

$$\therefore 1000^{2k} \equiv 1 \bmod 7, 1000^{2k+1} \equiv -1 \bmod 7$$

$$a_0 + a_1 \cdot 1000 + a_2 \cdot 1000^2 + a_3 \cdot 1000^3 + \dots a_k \cdot 1000^k$$

$\equiv a_0 + a_1 \cdot (-1) + a_2 \cdot (-1)^2 + a_3 \cdot (-1)^3 + a_4 \cdot (-1)^4 \dots a_k \cdot (-1)^k \bmod 7$
即

$$n \equiv (a_0+a_2+a_4+\dots)-(a_1+a_3+a_5+\dots) \bmod 7$$

$$\therefore 7|n \iff 7|[(a_0+a_2+a_4+\dots)-(a_1+a_3+a_5+\dots)]$$

对11,13的情况证明完全类似.

示例: $m,n,a\in\mathbb{Z}^+$, 如果$n^a\not\equiv 0 \bmod m, n^a\not\equiv 1 \bmod m$, 则存在$n$的一个素因子$p$使得$p^a\not\equiv 0 \bmod m, p^a\not\equiv 1 \bmod m$.

对于0的情况比较显然, 因为如果不存在素因子p_i使得$p_i^a\not\equiv 0 \bmod m$的式子成立, 亦即对所有的素因子$p_i$都有$p_i^a\equiv 0 \bmod m$的式子成立. 比如说对$n$的一个素因子$p_1$有$p_1^a\equiv 0 \bmod m$,

$$\therefore m|p_1^a$$

$$\therefore m|n^a(\because p_1^a|n^a)$$

这与条件$n^a\not\equiv 0 \bmod m$矛盾.

对于1的情况, 如果不存在素因子p_i使得$p_i^a\not\equiv 1 \bmod m$的式子成立, 亦即对所有的素因子$p_i$都有$p_i^a\equiv 1 \bmod m$的式子成立, 比如说$n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots p_s^{\alpha_s}$, 则有

$$p_1^a\equiv 1 \bmod m \Longrightarrow [p_1^a]^{\alpha_1}\equiv 1 \bmod m$$
$$p_2^a\equiv 1 \bmod m \Longrightarrow [p_2^a]^{\alpha_2}\equiv 1 \bmod m$$
$$\ldots\ldots$$
$$p_s^a\equiv 1 \bmod m \Longrightarrow [p_s^a]^{\alpha_s}\equiv 1 \bmod m$$
$$\therefore [p_1^a]^{\alpha_1}\cdot[p_2^a]^{\alpha_2}\cdot[p_3^a]^{\alpha_3}\ldots[p_s^a]^{\alpha_s}\equiv 1 \bmod m$$
$$\therefore [p_1^{\alpha_1}]^a\cdot[p_2^{\alpha_2}]^a\cdot[p_3^{\alpha_3}]^a\ldots[p_s^{\alpha_s}]^a\equiv 1 \bmod m$$
$$\therefore n^a\equiv 1 \bmod 1$$

与已知条件矛盾.

$$ad \equiv bd(\bmod m) \stackrel{?}{\Longrightarrow} a \equiv b \bmod m$$

反例: $5 \times 2 \equiv 3 \times 2 \bmod 4$, 但$5 \not\equiv 3 \bmod 4$.

- $\left.\begin{array}{c} ad \equiv bd \bmod m \\ (d,m)=1 \end{array}\right\} \Longrightarrow a \equiv b \bmod m$

  事实上,

  $$ad \equiv bd \bmod m \Longrightarrow m|(ad-bd) \Longrightarrow m|[d(a-b)]$$

  又因为$(d,m)=1$ (根据第一章$(a,c)=1, c|ab \Rightarrow c|b$)
  故有$m|(a-b)$

- $\left.\begin{array}{c} a \equiv b \bmod m \\ k>0 \end{array}\right\} \Longrightarrow (ak) \equiv (bk) \bmod (mk), \overset{(k,m)=1}{(ak) \equiv (bk) \bmod m}$

  事实上,

  $$a \equiv b \bmod m \Rightarrow m|(a-b) \Rightarrow (mk)|[k(a-b)]$$

  $$\Rightarrow (mk)|(ka-kb) \Rightarrow (ak) \equiv (bk) \bmod (mk)$$

- $\left.\begin{array}{c} a \equiv b \bmod m \\ d|a,b,m \end{array}\right\} \Longrightarrow \frac{a}{d} \equiv \frac{b}{d} \bmod \frac{m}{d}$

事实上, $a \equiv b \bmod m \Longrightarrow (a-b) = km \Longrightarrow \frac{a-b}{d} = \frac{km}{d}$

$\Longrightarrow \frac{a}{d} - \frac{b}{d} = k \cdot \frac{m}{d} \Longrightarrow \frac{a}{d} \equiv \frac{b}{d} \bmod \frac{m}{d}$

- $\left.\begin{array}{c} a \equiv b \bmod m \\ d|m \end{array}\right\} \Longrightarrow a \equiv b \bmod d$

事实上, $a \equiv b \bmod m \Longrightarrow m|(a-b) \Longrightarrow d|(a-b) \Longrightarrow a \equiv b \bmod d$

- $\left.\begin{array}{c} a \equiv b \bmod m_1 \\ a \equiv b \bmod m_2 \\ \cdots \\ a \equiv b \bmod m_k \end{array}\right\} \Longrightarrow a \equiv b \bmod [m_1, m_2, \ldots, m_k]$

事实上,

$$a \equiv b \bmod m_i \Longrightarrow m_i|(a-b)(i=1,2,\ldots,k)$$

$$\therefore [m_1, m_2, \ldots, m_k]|[a-b]$$

$$\therefore a \equiv b \bmod [m_1, m_2, \ldots, m_k]$$

特别的,$a \equiv b \bmod p, a \equiv b \bmod q, (p \neq q) \Longrightarrow a \equiv b \bmod pq$

- $a \equiv b \bmod m \Longrightarrow (a,m) = (b,m)$

事实上, $a \equiv b \bmod m \Longrightarrow a = mk + b \Longrightarrow (a,m) = (b,m)$.

同余的定义和性质

1. $a \equiv a; a \equiv b \bmod m \Rightarrow b \equiv a \bmod m; a \equiv b \bmod m, b \equiv c \bmod m \Rightarrow a \equiv c \bmod m$
2. $a = km + r, b = k'm + r', 0 \leq r, r' < m$，则$a \equiv b \bmod m \iff r = r'$
3. 给定正整数m，且$a_1 \equiv b_1 \bmod m, a_2 \equiv b_2 \bmod m$，则$(a_1 \pm a_2) \equiv (b_1 \pm b_2) \bmod m$
4. 给定正整数m，且$a_1 \equiv b_1 \bmod m, a_2 \equiv b_2 \bmod m$，则$(a_1 \cdot a_2) \equiv (b_1 \cdot b_2) \bmod m$
   - 特殊地,我们有$\forall 0 \leq i \in \mathbb{Z}, a \equiv b \bmod m \Longrightarrow a^i \equiv b^i \bmod m$
   - $x \equiv y \bmod m, a_0 \equiv b_0 \bmod m, a_1 \equiv b_1 \bmod m, \ldots, a_k \equiv b_k \bmod m$
     $\Longrightarrow (a_0 + a_1 x + a_2 x^2 + \ldots + a_k x^k) \equiv (b_0 + b_1 y + b_2 y^2 + \ldots + b_k y^k) \bmod m$
5. $\left.\begin{array}{c} ad \equiv bd \bmod m \\ (d, m) = 1 \end{array}\right\} \Longrightarrow a \equiv b \bmod m$
6. $\left.\begin{array}{c} a \equiv b \bmod m \\ k > 0 \end{array}\right\} \Longrightarrow (ak) \equiv (bk) \bmod (mk), (ak) \equiv (bk) \bmod m$

同余的定义和性质

7. $$\left.\begin{array}{c} a \equiv b \bmod m \\ d|a,b,m \end{array}\right\} \Longrightarrow \frac{a}{d} \equiv \frac{b}{d} \bmod \frac{m}{d}$$
8. $$\left.\begin{array}{c} a \equiv b \bmod m \\ d|m \end{array}\right\} \Longrightarrow a \equiv b \bmod d$$
9. $$\left.\begin{array}{c} a \equiv b \bmod m_1 \\ a \equiv b \bmod m_2 \\ \cdots \\ a \equiv b \bmod m_k \end{array}\right\} \Longrightarrow a \equiv b \bmod [m_1, m_2, \ldots, m_k]$$
   $$a \equiv b \bmod p, a \equiv b \bmod q, (p \neq q) \Longrightarrow a \equiv b \bmod pq$$
10. $a \equiv b \bmod m \Longrightarrow (a, m) = (b, m)$

2. 剩余类

- 剩余类：称

$$C_a \triangleq \{c | c \equiv a \bmod m, c \in \mathbb{Z}\}$$

为模m的a的剩余类. 这个集合中有无数多个元素. C_a中的任意元素称为这个类的剩余或代表元.
模m的剩余类有m个:

$$C_0, C_1, \ldots, C_{m-1}$$

- 完全剩余系：如果

$$r_0, r_1, \ldots, r_{m-1} \in \mathbb{Z}$$

且它们中的任意两个都不在同一个剩余类中(比如, $r_0 \in C_0, r_1 \in C_1, \ldots, r_{m-1} \in C_{m-1}$), 则称

$$\{r_0, r_1, \ldots, r_{m-1}\}$$

为模m的一个完全剩余系.
易见:$\{0, 1, 2, 3, \ldots, m-1\}$是一个完全剩余系, 称之为模$m$的最小非负完全剩余系;
$\{1, 2, 3, \ldots, m\}$是一个完全剩余系, 称之为最小正完全剩余系.

示例:
$\{r_0, r_1, \ldots, r_{m-1}\}$是模$m$的一个完全剩余系 $\Longleftrightarrow$ $r_i \not\equiv r_j \bmod m, i \neq j,$
$i, j = 0, 1, \ldots, m-1.$

"$\Longrightarrow$:" 如果存在$i \neq j, s.t., r_i \equiv r_j \bmod m$, 则它们就会在同一个剩余类中, 这与条件$\{r_0, r_1, \ldots, r_{m-1}\}$是模$m$的一个完全剩余系矛盾.

"$\Longleftarrow$:" 这个m个数两两不同余, 从而它们处于不同的剩余类中, 从而他们一起构成了一个完全剩余系. $\diamond$

小结论

(i) 整数a与正整数m互素, b是任意一个整数, 则: 当x取遍模m的一个完全剩余系中的数时, 相应的数$ax+b$也构成模m的一个完全剩余系.

证明: 假设x取遍一个完全剩余系$r_0, r_1, \ldots, r_{m-1}$, 只需要说明得到的$m$个整数$ar_0+b, ar_1+b, ar_2+b, \ldots, ar_{m-1}+b$两两不同余即可.

如果说这些数中存在两个同余, 比如$ar_0+b \equiv ar_1+b \bmod m$, 此即

$$m|(ar_0+b-ar_1-b) \Longrightarrow m|[a(r_0-r_1)]$$

而a与m互素, 所以

$$m|(r_0-r_1)$$

即

$$r_0 \equiv r_1 \bmod m$$

不可能. $\diamond$

小结论

(ii) 设m_1与m_2互素，如果x_1取遍模m_1的完全剩余系中的数，x_2取遍模m_2的完全剩余系中的数时，则$m_2x_1+m_1x_2$取遍模m_1m_2完全剩余系中的数.

证明: x_1有m_1种取法，x_2有m_2种取法，所以$m_2x_1+m_1x_2$有m_1m_2中取法，我们只需要说明这m_1m_2个值两两不同余即可.

如果存在两个数: m_2a+m_1b和$m_2a'+m_1b'$模m_1m_2同余(即x_1取$a, a', a \neq a'$, x_2取$b, b', b \neq b'$)，即

$$m_2a+m_1b \equiv m_2a'+m_1b' \bmod m_1m_2$$

从而

$$m_2a+m_1b \equiv m_2a'+m_1b' \bmod m_1$$

又

$$-m_1b \equiv -m_1b' \bmod m_1$$

所以

$$m_2a \equiv m_2a' \bmod m_1$$

而m_1与m_2互素，从而

$$a \equiv a' \bmod m_1$$

矛盾

简化剩余类

如果一个模m的完全剩余类中有元素与m互素，则这个剩余类被称为简化剩余类.

事实上，这时候，这个类中所有元素均与m互素:
比如简化剩余类中与m互素的那个元素为a, $(a,m)=1$, 对这个剩余类中的任一个元素c, $c \equiv a \bmod m$, 即

$$c = mk + a \Longrightarrow (c,m) = (m,a)$$

$$\therefore (c,m) = 1 \iff (m,a) = 1$$

将小于m与m互素的正整数的个数记作$\varphi(m)$, 称之为欧拉函数. 不是单调函数
模m的简化剩余类的个数是$\varphi(m)$.

比如$\varphi(10) = 4$, $(1,3,7,9$与10互素$)$.

这样模10的简化剩余类就是C_1, C_3, C_7, C_9.

简化剩余系

在模m的所有简化剩余类中各取一个元素构成的集合叫做模m的简化剩余.

比如, $1, 2, 3, \ldots, m-1, m$中与m互素的整数全体构成模m的一个简化剩余系, 称之为模m的最小简化剩余系.

比如, $\{1, 3, 7, 9\}$是模10的一个简化剩余系和最小简化剩余系, $\{1, 7, 11, 13, 17, 19, 23, 29\}$是模30的一个简化剩余系($\varphi(30) = 8$).

$\{1, 2, 3, \ldots, p-1\}$(p为素数)是模p的一个简化剩余系, 且有

$$\varphi(p) = p - 1$$

事实上,容易看到任意$\varphi(m)$个两两模m不同余, 并与m互素的整数一起都构成了一个模m的简化剩余系.

示例: $(a,m)=1$, 如果x取遍模m的一个简化剩余系中的元素, 则ax也取遍模m的一个简化剩余系中的元素.

证明: 对于x取的模m的一个简化剩余系中的任意元素, 总有

$$(x,m)=1$$

所以

$$(ax,m)=1$$

即相应的元素ax也与m互素.
还需要说明x取了这个剩余系中的不同的值m_1, m_2时, 相应的am_1, am_2不同余.
否则,

$$\left.\begin{array}{c} am_1 \equiv am_2 \bmod m \\ (a,m)=1 \end{array}\right\} \Longrightarrow m_1 \equiv m_2 \bmod m$$

矛盾. $\diamond$

示例: $(a,m)=1, \exists a' \in \mathbb{Z}, 1 \le a' < m, s.t., aa' \equiv 1 \bmod m$

证明:

$$(a,m)=1 \Longrightarrow \exists s,t,s.t., sa+tm=1$$

$$\Longrightarrow sa+tm \equiv 1 \bmod m$$

$$\Longrightarrow sa \equiv 1 \bmod m$$

取

$$a' = (s \bmod m)$$

即得所求(从证明过程可以看到,在$1 \sim m$之间,这个a'是唯一的). $\diamond$
比如

$$2 \cdot 4 \equiv 1 \bmod 7$$

$$3 \cdot 5 \equiv 1 \bmod 7$$

$$6 \cdot 6 \equiv 1 \bmod 7$$

这个结论在密码学中经常用到, 逆元的概念.

这个示例的一个应用: p是素数, 则$(p-1)! \equiv -1 \bmod p$

定理（wilson定理）

p是素数，则$(p-1)! \equiv -1 \bmod p$ (P - 2)! = 1 mod P

证明：将p看作上面的m，a任意取$1,2,3,\ldots,p-1$，都与p互素，所以会相应的存在$1\sim p-1$中的唯一的数a'使得$aa' \equiv 1 \bmod p$成立.

下面我们来看看这个对应的a'何时会就是a本身：如果$a=a'$，则有$a^2 \equiv 1 \bmod p$，即$(a-1)(a+1) \equiv 0 \bmod p$，也就是$p|[(a-1)(a+1)]$，而$a$的可能的取值是$1,2,3,\ldots,p-1$，所以$a=1$，或$a=p-1$.

从而，只有当a取值为1或$p-1$时，使得$aa' \equiv 1 \bmod p$ 成立的那个$1\sim p$中的唯一的数a'就是1或$p-1$；除此之外的可能取值$2,3,4,\ldots,p-2$的a，相应的使得$aa' \equiv 1 \bmod p$成立的那个$2\sim p-2$中的唯一的数a'是不等于a的，
打个比方来说，
$a=2$时，使得$aa' \equiv 1 \bmod p$成立的a'是4;
$a=3$时，使得$aa' \equiv 1 \bmod p$成立的a'是5;
$a=6$时，使得$aa' \equiv 1 \bmod p$成立的a'是8;
$a=7$时，使得$aa' \equiv 1 \bmod p$成立的a'是9;
$\ldots\ldots$
这样$p-3$个数可以两两配对使得$aa' \equiv 1 \bmod p$;

从而

$$2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot \ldots \cdot (p-2) \equiv 1 \bmod p$$

又因为

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

所以,

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot \ldots \cdot (p-2) \cdot (p-1) = 1 \cdot [2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot \ldots \cdot (p-2)] \cdot (p-1)$$

$$\equiv 1 \cdot (p-1) \equiv -1 \bmod p \qquad \diamond$$

这个结论也被称为Wilson定理.

示例: m_1与m_2互素, 如果x_1取遍模m_1的简化剩余系, x_2取遍模m_2的简化剩余系时, 则$m_2x_1+m_1x_2$遍历模m_1m_2的一个简化剩余系.

证明: 由

$$a=bq+c\Longrightarrow(a,b)=(b,c)$$

知

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

又因为

$$(x_1,m_1)=1$$

我们有

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

即$m_2x_1+m_1x_2$与m_1互素, 类似可得$m_2x_1+m_1x_2$与m_2互素, 从而$m_2x_1+m_1x_2$与m_1m_2互素.

为说明$m_2x_1+m_1x_2$遍历模m_1m_2的一个简化剩余系, 还需要说明任意一个模m_1m_2的简化剩余都具有形式:

$$m_2x_1+m_1x_2,\ \text{where } (x_1,m_1)=1,(x_2,m_2)=1$$

事实上我们知道任意一个模m_1m_2的剩余都具有形式:

$$m_2x_1+m_1x_2$$

一个剩余$m_2x_1+m_1x_2$要称为简化剩余必须满足$(m_2x_1+m_1x_2,m_1m_2)=1$, 而

$$(m_2x_1+m_1x_2,m_1m_2)=1 \Longrightarrow (m_2x_1+m_1x_2,m_1)=1$$

$$\Longrightarrow (m_2x_1,m_1)=1 \Longrightarrow (x_1,m_1)=1$$

类似地可以推出

$$(m_2x_1+m_1x_2,m_1m_2)=1 \Longrightarrow (x_2,m_2)=1$$

这就说明了任意一个模m_1m_2的简化剩余都具有:

$$m_2x_1+m_1x_2,\ \text{where } (x_1,m_1)=1,(x_2,m_2)=1$$

这样的形式.

3. 欧拉函数的性质

(1) $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$

事实上，在大于等于0，小于p^α的数中：

$$\begin{array}{cccc}
0 & 1 & \dots & p-1 \\
p & p+1 & \dots & 2p-1 \\
2p & 2p+1 & \dots & 3p-1 \\
3p & 3p+1 & \dots & 4p-1 \\
\dots & \dots & \dots & \dots \\
(p^{\alpha-1}-1)p & (p^{\alpha-1}-1)p+1 & \dots & p^{\alpha-1}\cdot p-1
\end{array}$$

与p^α有公因子(大于1)的只是第一列，其他列的数均与p^α互素.
比如数$3p+1$与p^α互素，因为否则有公因子p的话，

$$p|3p, p|(3p+1) \Longrightarrow p|1$$

不可能，再如$(p^{\alpha-1}-1)p+1$与p^α互素，因为否则有公因子$p^i(i<\alpha)$的话，则有公因子p，

$$p|(p^{\alpha-1}-1)p, p|((p^{\alpha-1}-1)p+1) \Longrightarrow p|1$$

不可能.
其他类似.

这样与p^α互素的数的个数就是

$$p^\alpha - p^{\alpha-1}$$

即

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1 - \frac{1}{p})$$

◇

(2) $(m,n)=1 \Longrightarrow \varphi(mn)=\varphi(m)\varphi(n)$

这是因为, 我们已经知道: x遍历模m的简化剩余系, y遍历模n的简化剩余系时, 会有$xn+ym$遍历模mn的一个简化剩余系,

一方面, 模mn的一个简化剩余系所含元素个数是

$$\varphi(mn)$$

另一方面, x遍历模m的简化剩余系, y遍历模n的简化剩余系时, 得到$xn+ym$的个数是

$$\varphi(m)\varphi(n)$$

从而

$$\varphi(mn)=\varphi(m)\varphi(n)$$

◇

示例: 计算

$$\varphi(77)=\varphi(7)\varphi(11)=6\cdot 10=60$$
$$\varphi(30)=\varphi(2)\varphi(3)\varphi(5)=1\cdot 2\cdot 4=8$$

拆成多个数时必须两两互素

特殊地, p,q是素数时,

$$\varphi(pq)=\varphi(p)\varphi(q)=(p-1)(q-1)=pq-p-q+1$$

(3) 对任意正整数n, 其标准分解式为

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$$

有

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdot \ldots \cdot \varphi(p_s^{\alpha_s})$$

$$p_1^{\alpha_1}(1 - \frac{1}{p_1}) \cdot p_2^{\alpha_2}(1 - \frac{1}{p_2}) \cdot \ldots \cdot p_s^{\alpha_s}(1 - \frac{1}{p_s})$$

$$= n \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2}) \cdot \ldots \cdot (1 - \frac{1}{p_s})$$

但是如果不知道n的分解式的话, 求其欧拉函数值是困难的.

(4) $n \in \mathbb{Z}^+, \sum_{d|n} \varphi(d) = n$

证明: 设d是n的因数(比如$n = 8$时, d可取$1, 2, 4$或是8), 对于$\{1, 2, 3, 4, \ldots, n\}$的$n$个数进行分类,

$$\Phi_d = \{m | 1 \leq m \leq n, (m, n) = d\}$$

比如, $n = 8$的话, 有$\Phi_1 = \{1, 3, 5, 7\}$, $\Phi_2 = \{2, 6\}$, $\Phi_4 = \{4\}$, $\Phi_8 = \{8\}$

可以看到, 按照这个分类, $\{1, 2, 3, 4, \ldots, n\}$中的每个数属于且仅属于一个$\Phi$的集合中. 这样$n$就对于这些集合所含的元素个数之和.
我们知道

$$(m, n) = d \iff (\frac{m}{d}, \frac{n}{d}) = 1$$

所以集合Φ_d等价于下面的说法

$$\Phi_d = \{m | 1 \leq m \leq n, (\frac{m}{d}, \frac{n}{d}) = 1\}$$

即

$$\Phi_d = \{m = dk | 1 \leq k \leq \frac{n}{d}, (k, \frac{n}{d}) = 1\}$$

这样Φ_d的元素个数就是满足条件

$$1 \leq k \leq \frac{n}{d}, (k, \frac{n}{d}) = 1$$

的k的个数, 即$\varphi(\frac{n}{d})$. 从而$n = \sum_d \varphi(\frac{n}{d})$

事实上，

$$\sum_{d}\varphi(\frac{n}{d})=\sum_{d}\varphi(d)$$

比如$n=8$时，

$$\sum_{d}\varphi(\frac{n}{d})=\varphi(\frac{8}{1})+\varphi(\frac{8}{2})+\varphi(\frac{8}{4})+\varphi(\frac{8}{8})$$

$$=\varphi(8)+\varphi(4)+\varphi(2)+\varphi(1)=\varphi(1)+\varphi(2)+\varphi(4)+\varphi(8)$$

$$=\sum_{d}\varphi(d)$$

(5) $1 < m \in \mathbb{Z}, (a,m) = 1 \Longrightarrow a^{\varphi(m)} \equiv 1 \bmod m$

证明: 设$r_1, r_2, r_3, \ldots, r_{\varphi(m)}$是$1, 2, 3, \ldots, m-1, m$中与$m$互素的整数全体, 它们构成模$m$的一个简化剩余系(最小简化剩余系),

因为$(a,m) = 1$
所以$ar_1, ar_2, ar_3, \ldots, ar_{\varphi(m)}$也构成模$m$的一个简化剩余系,
这样,

$$\{ar_1 (\bmod m), ar_2 (\bmod m), \ldots, ar_{\varphi(m)} (\bmod m)\} = \{r_1, r_2, r_3, \ldots, r_{\varphi(m)}\}$$

换句话说, 即

$$ar_1 \cdot ar_2 \cdot \ldots \cdot ar_{\varphi(m)} \equiv r_1 r_2 r_3 \ldots r_{\varphi(m)} \bmod m$$

整理:

$$(r_1 r_2 r_3 \ldots r_{\varphi(m)})(a^{\varphi(m)} - 1) \equiv 0 \bmod m$$

但

$$(r_1, m) = 1, (r_2, m) = 1, \ldots, (r_{\varphi(m)}, m) = 1 \Longrightarrow ((r_1 r_2 r_3 \ldots r_{\varphi(m)}), m) = 1$$

从而

$$a^{\varphi(m)} - 1 \equiv 0 \bmod m \qquad \diamond$$

这个结论被称为著名的Eular定理

示例:

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

这是因为:

$$(2, 11) = 1, \varphi(11) = 10$$

$$23 \nmid a \Longrightarrow a^{22} \equiv 1 \bmod 23$$

这是因为

$$23 \nmid a \Longrightarrow (a, 23) = 1$$

$$\varphi(23) = 22$$

(6) p是素数, $a \in \mathbb{Z}$, 则$a^p \equiv a \bmod p$

证明:

- 如果$p|a$的话, 有
$$p|a, p|a^p$$
从而
$$p|a^p - a$$
即
$$a^p \equiv a \bmod p$$
- 如果$p \nmid a$的话, 则
$$(a, p) = 1$$
从而
$$a^{\varphi(p)} \equiv 1 \bmod p$$
即
$$a^{p-1} \equiv 1 \bmod p$$
从而
$$a^p \equiv a \bmod p \qquad \diamond$$

这就是著名的Fermat定理

4. 模指数计算

计算

$$b^n \bmod m$$

可以递归地计算

$$[b^{n-1} \bmod m] \cdot b \bmod m$$

这需要做$n-1$次模乘运算，费时.

将n写成2进制形式

$$n = n_0 + n_1 2 + n_2 2^2 + \ldots + n_{k-1} 2^{k-1}$$

这里n_i的取值为0或1.
这样，

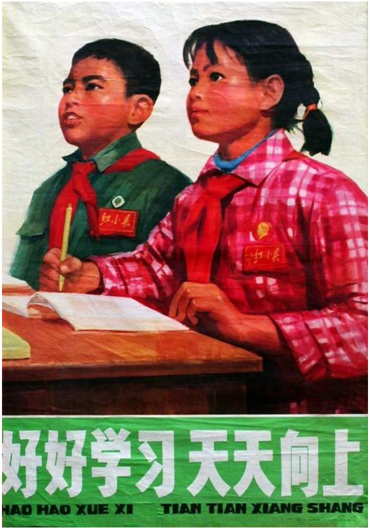
$$b^n = b^{n_0} \cdot b^{n_1 2} \cdot b^{n_2 2^2} \cdot \ldots \cdot b^{n_{k-1} 2^{k-1}}$$

$$b^n = b^{n_0} \cdot b^{n_1 2} \cdot b^{n_2 2^2} \cdot \ldots \cdot b^{n_{k-1} 2^{k-1}}$$

具体来说，置$a = 1$;

- 如果$n_0 = 1$，计算$a_0 \equiv a \cdot b \bmod m$
  否则，置$a_0 = a$;
  计算$b_1 = b^2 \bmod m$
- 如果$n_1 = 1$，计算$a_1 \equiv a_0 \cdot b_1 \bmod m$
  否则，置$a_1 = a_0$;
  计算$b_2 = b_1^2 \bmod m$, (i.e., $(b^2)^2 \bmod m$)
- 如果$n_2 = 1$，计算$a_2 \equiv a_1 \cdot b_2 \bmod m$
  否则，置$a_2 = a_1$;
  计算$b_3 = b_2^2 \bmod m$, (i.e., $(b^{2^3}) \bmod m$)
- ......
- 如果$n_{k-1} = 1$，计算$a_{k-1} \equiv a_{k-1} \cdot b_{k-1} \bmod m$
  否则，置$a_{k-1} = a_{k-2}$;
  输出a_{k-1}即为所求.

按每步2次模乘运算计，总共需要$2k$次模乘运算，这里k就是n的二进制表示长度.
这种计算模指数的方法称为模重复平方计算法.


好好学习 天天向上
HAO HAO XUE XI TIAN TIAN XIANG SHANG