第二章 同余

任课教师：胡丽琴
网络空间安全学院

问题引入

问题

- 大家2018年12月6日有课吗？
- 今天星期二，那么从今天算起，第2^{53}天是星期几？

问题引入

- 3145×92653=291_93685的横线处漏写了一个数字，你能以最快的速度补出吗？

- 13511，13903，14589被自然数m除所得的余数相同，问：m最大值是多少？

- 你知道7^{7^7}的个位数是多少吗？

问题

问题

同余相关内容

- 同余的基本性质
- Euler定理Fermat小定理
- 模重复平方计算法
- 大素数的生成

同余相关内容

- 同余的基本性质
- Euler定理Fermat小定理
- 模重复平方计算法
- 大素数的生成

● 问题引入

- 设有26个英文字符，将它们作移位变换，有

字符	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*
⇕																										
字符	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*	*a*	*b*	*c*

- 将这26个字符数字化

字符	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*
⇕																										
数字	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

问题引入

- 问：能否用一个数学函数来表示上述变换?

- 类似地，可以构造如下的数字变换，问能否用一个数学函数表述?

数字	0	1	2	3	4	5	6	7	8	9	10	11	12
数字	7	28	6	24	43	13	52	49	37	42	9	36	38

问题

● 同余的概念

- **定义 2.1.1** 给定一正整数m，两个整数a，b叫做模m同余，如$a-b$被m整除或$m|a-b$, 记作$a\equiv b(\mathrm{mod}\ m)$；否则叫做模$m$不同余，记作$a\not\equiv b(\mathrm{mod}\ m)$。

例

$19\equiv 7(\mathrm{mod}\ 12)$　$29\equiv 1(\mathrm{mod}\ 7)$

$27\equiv 6(\mathrm{mod}\ 7)$　$23\equiv -5(\mathrm{mod}\ 7)$

● 同余的等价定义

- **定理 2.1.1**设m是一个正整数，a，b是两个整数，则

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

的充要条件是存在一个整数k使得$a=b+km$。

例

- 判断下列数对是否模11同余。
  - 59和1478
  - 721和1573

同余的等价定义

- **例** 已知 $190 \equiv 50 \pmod{70}$，那么 $190 \equiv 50 \pmod{7}$？$190 \equiv 50 \pmod{35}$？

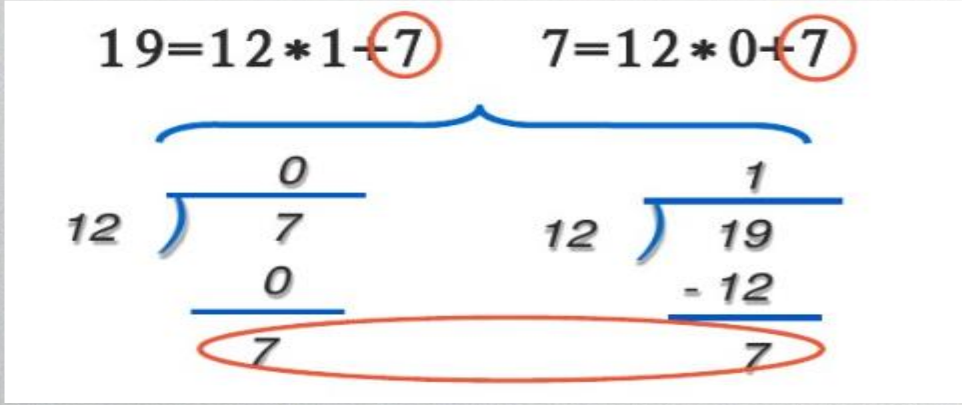
性质

- **定理 2.1.8** 设 m 是一个正整数，$a \equiv b \pmod{m}$。如果 $d|m$，则 $a \equiv b \pmod{d}$。

- **定理 2.1.10** 设 $a \equiv b \pmod{m}$，则 $(a,m) = (b,m)$。

● 同余的概念

- 数学中的同余
- Euclid除法：$a=qb+r$，$0\leq r<b$，同余就是余数相等。
- 如：



同余的性质

- **定理 2.1.3** 设m是一个正整数，则整数a,b模m同余的充要条件是a,b被m除的余数相同。

例

- $39=5\times7+4$，$25=3\times7+4$，所以$39\equiv25 \pmod 7$
- $59=5\times11+4$，$70=6\times11+4$，所以$59\equiv70 \pmod{11}$

● 同余的性质

- **例** 已知$39\equiv 4 \pmod 7$，$22\equiv 1 \pmod 7$，那么
  - $39+22\equiv ? \pmod 7$
  - $39-22\equiv ? \pmod 7$
  - $39\times 22\equiv ? \pmod 7$
  - $39^2\equiv ? \pmod 7$

● 同余的性质

■ **定理 2.1.4** 设m是一个正整数，a , b , c , d是四个整数。如果$a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, 则

- $a+c \equiv b+d \pmod{m}$
- $ac \equiv bd \pmod{m}$.

● 同余的性质

- 例：今天星期二，那么从今天算起，第2^{53}天是星期几？

- 解：$2^1 \equiv 2 \pmod 7$，$2^2 \equiv 4 \pmod 7$，$2^3 \equiv 1 \pmod 7$

  而$53 \equiv 2 \pmod 3$，所以$2^{53} \equiv 2^2 \equiv 4 \pmod 7$.

  故第2^{53}天是星期六。

● 同余的性质

- 应用：如何快速判断一个十进制数能否被3整除？比如： 248901
  - 方法：将该整数的各位数作和后判断
- 问：为什么可以这么判断？

同余的性质

- 关键：10=3×3+1,100=33×3+1，…，即：$10\equiv 1 \pmod 3$，$100\equiv 1 \pmod 3$，$10^i\equiv 1 \pmod 3$，$i\geq 1$.所以，若 $n=a_m 10^m+a_{m-1}10^{m-1}+\ldots+a_1\times 10+a_0$，则

$$3|n \Leftrightarrow 3|a_m+a_{m-1}+\ldots+a_1+a_0$$

- 7^{7^7}的个位数是多少?

● 同余的性质

- 例 已知$19 \equiv 5 \pmod 7$，那么$19 \times 4 \equiv 5 \times 4 \pmod 7$？

$19 \times 4 \equiv 5 \times 4 \pmod{7 \times 4}$？

性质

- **定理 2.1.6** 设m是一个正整数，$a \equiv b \pmod m$，$k > 0$，则$ak \equiv bk \pmod{mk}$。

● 同余的性质

- 例 95≡25(mod 7)，其中95=19×5，25=5×5
- 那么，19≡5(mod 7)？

例

- 例 273≡143(mod 5)，其中273=13×21，143=11×13
- 那么21≡11(mod 5)？

● 同余的性质

- 问：是不是所有的$ad \equiv bd \pmod{m}$都能得到$a \equiv b \pmod{m}$？如果是，请尝试证明，如果不是，请给出反例。

性质

- **定理 2.1.5** 设m是一个正整数，$ad \equiv bd \pmod{m}$。如果$(d,m)=1$，则$a \equiv b \pmod{m}$。

● 同余的性质

- 例 $190\equiv 50 \pmod{70}$，$(190,50)=10$

> 可以得到：$19\equiv 5 \pmod 7$？因为$10|70$.

- $190\equiv 50 \pmod{28}$，那么$19\equiv 5 \pmod{28}$成立吗？

> $19\not\equiv 5 \pmod{28}$

- 总结一下，我们能得到怎样的同余式呢？

同余的性质

- **定理 2.1.7** 设m是一个正整数，$a \equiv b \pmod{m}$。如果整数$d|(a,b,m)$，则

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

- 例 190≡50(mod 7)，190≡50(mod 10)，有190≡50(mod 70)；470≡50(mod 14)，470≡50(mod 20)，能否得到470≡50(mod 280)？

同余的性质

- **定理 2.1.9** 设$m_1,m_2,\ldots,m_k$是k个正整数，$a\equiv b\ (\mathrm{mod}\ m_i)$，$i=1,2,\ldots,k$，则$a\equiv b(\mathrm{mod}\ [m_1,m_2,\ldots,m_k])$。

例

- 设p，q是不同素数。如果整数a,b满足

$$a\equiv b\ (\mathrm{mod}\ p),\quad a\equiv b\ (\mathrm{mod}\ q),$$

则有$a\equiv b(\mathrm{mod}\ pq)$。

同余的性质

- 例 39≡39(mod 7)

  39≡32(mod 7) 32≡25(mod 7)

  39与25是否模7同余?

- **定理 2.1.2** 设m是一个正整数，则模m同余是等价关系，即
  - 自反性：$a \equiv a \pmod{m}$.
  - 对称性: 若$a \equiv b \pmod{m}$, 则$b \equiv a \pmod{m}$.
  - 传递性: 若$a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$, 则$a \equiv c \pmod{m}$

同余的性质

总结

- 同余具有加法和乘法运算性质
- 同余具有自反性、对称性和传递性等性质

● 剩余类

- 设m是一个正整数。对任意正整数a，令

$$C_a=\{c|c\in \mathbf{Z},\ a\equiv c(\text{mod } m)\}.$$

C_a是非空集合，因为$a\in C_a$.

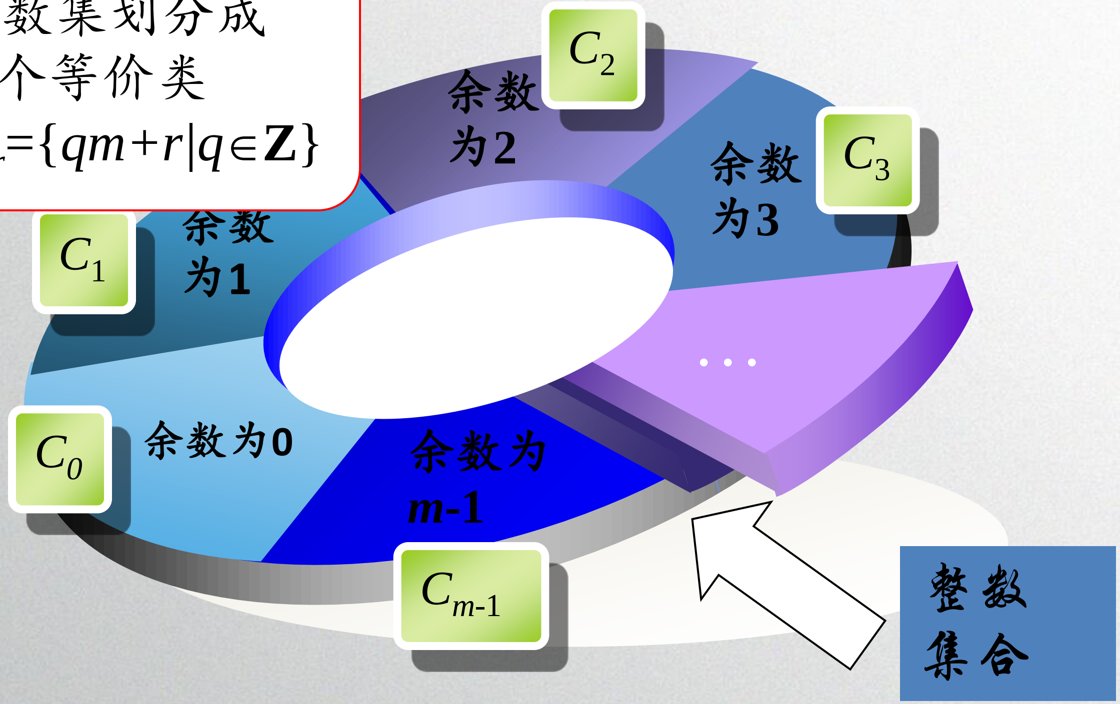
定理 2.1.11 设m是一个正整数，则

- 任一整数必包含在一个C_r中，$0\le r\le m-1$；
- $C_a=C_b$的充要条件是$a\equiv b(\text{mod } m)$；
- C_a与C_b的交集为空集的充要条件是$a\not\equiv b(\text{mod } m)$。

剩余类

1、整数集划分成 m个等价类

2、$C_r=\{qm+r|q\in\mathbf{Z}\}$



● 完全剩余类

- **定义2.1.2** C_a叫做模m的**剩余类**。一个剩余类中的任一数叫做该类的**剩余**或**代表元**。若$r_0, r_1, \ldots, r_{m\text{-}1}$是$m$个整数，并且其中任何两个数都不在同一个剩余类里，则$r_0, r_1, \ldots, r_{m\text{-}1}$叫做模$m$的一个**完全剩余系**。

● 完全剩余类

- **定义2.1.2** C_a叫做模m的**剩余类**。一个剩余类中的任一数叫做该类的**剩余**或**代表元**。若$r_0, r_1, \ldots, r_{m-1}$是$m$个整数，并且其中任何两个数都不在同一个剩余类里，则$r_0, r_1, \ldots, r_{m-1}$叫做模$m$的一个**完全剩余系**。

● 剩余类

- 模m的剩余类有m个，即$C_0, C_1,\ldots, C_{m-1}$，它们作为新的元素组成一个新集合，通常写成

$$\mathbf{Z}/m\mathbf{Z}=\{C_0, C_1,\ldots, C_{m-1}\}=\{C_a|0\le a\le m-1\}.$$

特别地，当$m=p$为素数时，我们也写成

$$\mathbf{F}_p=\mathbf{Z}/p\mathbf{Z}=\{C_0, C_1,\ldots, C_{p-1}\}=\{C_a|0\le a\le p-1\}.$$

剩余类

- **Z**/m**Z**中元素间的加法运算为$C_a \oplus C_b = C_{a+b}$.
- **Z**/m**Z**中元素间的乘法运算为$C_a \otimes C_b = C_{a \times b}$

运算

- **Z**/m**Z**中元素间的运算往往通过剩余类中的剩余或代表元来给出，这时需要注意该运算不依赖于剩余或代表元的选取。

● 剩余类

- 例 设m=3， 则$\mathbf{Z}/3\mathbf{Z}=\{C_0, C_1, C_2\}$.
  - $C_0=\{\ldots\ldots,-9,-6,-3,0,3,6,9,\ldots\ldots\}=C_3=C_6=\ldots$
  - $C_1=\{\ldots\ldots,-8,-5,-2,1,4,7,10,\ldots\ldots\}=C_4=C_7=\ldots$
  - $C_2=\{\ldots\ldots,-7,-4,-1,2,5,8,11,\ldots\ldots\}=C_5=C_8=\ldots$
  - 因此， $C_0\oplus C_1=C_3\oplus C_4=C_6\oplus C_7=\ldots$

    $C_0\otimes C_1=C_3\otimes C_4=C_6\otimes C_7=\ldots$

完全剩余系

- 例：设正整数m=10。对任意正整数a，集合

$$C_a=\{a+10k|k\in\mathbf{Z}\}$$

是模m的一个剩余类。

- 0,1,2,3,4,5,6,7,8,9是模10的一个完全剩余系。
- 0,3,6,9,12,15,18,21,24,27是不是模10的一个完全剩余系？
- 9,10,11,22,33,44,55,66,77,88是不是模10的一个完全剩余系?

完全剩余系

定理

- 设m是一个正整数，则m个整数$r_0, r_1, \ldots, r_{m-1}$是一个完全剩余系的充要条件是它们模$m$两两不同余。

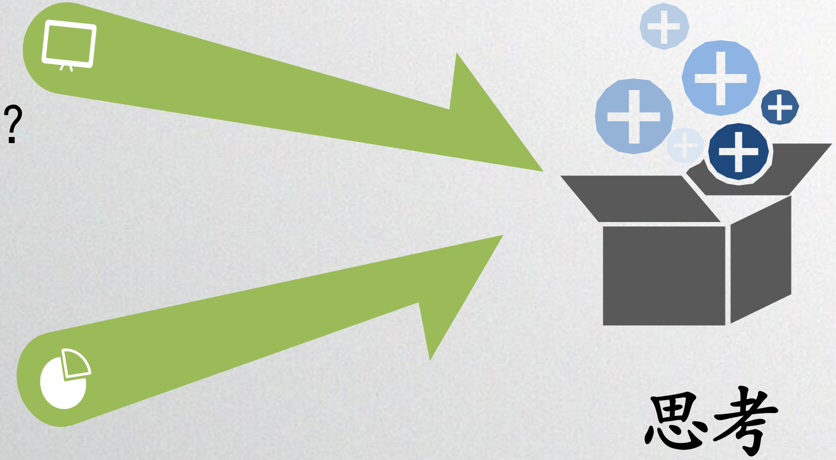
完全剩余系

- 例：设m是一个正整数则
  - $0, 1, \ldots, m-1$是模m的一个完全剩余系，叫做模m的**最小非负完全剩余系**。
  - $1, 2, \ldots, m$是模m的一个完全剩余系，叫做模m的**最小正完全剩余系**。
  - 类似地，还有**最大非正完全剩余系**、**最大负完全剩余系**、**绝对值最小完全剩余系**

● 完全剩余系

- 既然完全剩余系是不唯一的，不同的剩余系之间有什么关系呢？

- 一个完全剩余系的所有元素通过线性变换后，还是完全剩余系吗？



● 完全剩余系

检验

- 设$x_0, x_1, \ldots, x_{m-1}$是模$m$的一个完全剩余系

- $b+x_0, b+x_1, \ldots, b+x_{m-1}$是模$m$的一个完全剩余系吗？

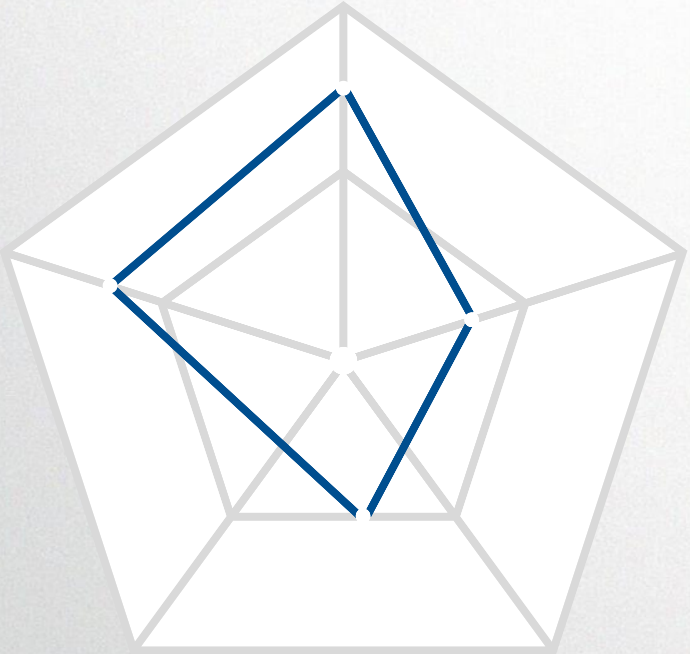
- $ax_1, \ldots, ax_{m-1}$是模m的一个完全剩余系吗？

✓ $m=5, b=2, a=2$
✓ $m=6, b=2, a=2$

● 完全剩余系

定理 2.1.13

- 设m是一个正整数，a是满足$(a,m)=1$的整数，b是任意整数。若x遍历m的一个完全剩余系，则$ax+b$也遍历模m的一个完全剩余系。



完全剩余系

- 例：设m=10,a=7,b=7，则形为ax+b的10个数为5,12,19,26,33,40,47,54,61,68构成模10的一个完全剩余系
- 例：利用模5,6的完全剩余系构造模30的一个完全剩余系。
- 判断：0,5,2,7,4,9,6,11,8,13是不是模10的一个完全剩余系？

● 完全剩余系

- **定理 2.1.14** 设m_1，m_2是两个互素的正整数。若x_1，x_2分别遍历m_1，m_2的完全剩余系，则$m_2x_1+m_1x_2$遍历模m_1m_2的完全剩余系。

定理

- 设p, q是两个不同的素数，$n=pq$，则对任意的整数c，存在唯一的整数x, y满足

$$qx+py\equiv c(\text{mod } n),\ 0\le x<p,\ 0\le y<q.$$

同余相关内容

- 同余的基本性质
- **Euler定理Fermat小定理**
- 模重复平方计算法
- 大素数的生成

● Euler函数

- 在10以内，与10互素的正整数有多少个？
- **定义2.2.1** 设m是一个正整数，则m个整数$0,1,\ldots,m-1$与m互素的整数个数，记作$\varphi(m)$，通常叫做**Euler函数**。

> $\varphi(1)=1$，$\varphi(2)=1$，$\varphi(3)=2$，$\varphi(4)=2$，$\varphi(5)=4$，$\varphi(6)=2$，$\varphi(7)=6$，$\varphi(8)=4$，$\varphi(9)=6$，…

> 所以，大家发现什么特点了吗？

● Euler函数

- 在10以内，与10互素的整数有多少个？
- **定义2.2.1** 设m是一个正整数，则m个整数$0,1,\ldots,m-1$与m互素的整数个数，记作$\varphi(m)$，通常叫做Euler函数。
  - $\varphi(1)=1$，$\varphi(2)=1$，$\varphi(3)=2$，$\varphi(4)=2$，$\varphi(5)=4$，$\varphi(6)=2$，$\varphi(7)=6$，$\varphi(8)=4$，$\varphi(9)=6$，…
  - 所以，大家发现什么特点了吗？

Euler定理

当p为素数时，$\varphi(p)=p-1$.

$2^6 \pmod 5=?$

$2^{2014} \pmod{11}=?$

● 简化剩余系

■ **定义2.2.2** 一个模m的剩余类叫做简化剩余类，如果该类中存在一个与m互素的剩余。

定义

➤ 请给出模10的一个简化剩余类

➤ 请给出模10的所有简化剩余类

简化剩余系

- **定理2.2.1** 设r_1与r_2是同一模m剩余类的两个剩余，则r_1与m互素的充要条件是r_2与m互素。

- 模m的简化剩余类全体组成的集合通常写成$(\mathbf{Z}/m\mathbf{Z})^*=\{C_a|0\le a\le m-1, (a,m)=1\}$.

- 特别地，当$m=p$为素数时，我们也写成$\mathbf{F}_p^*=(\mathbf{Z}/p\mathbf{Z})^*=\{C_1,\dots, C_{p-1}\}=\mathbf{F}_p\backslash\{C_0\}$.

● 完全剩余系

定义

- **定义2.2.3** 设m是一个正整数，在模m的所有不同简化剩余类中，从每个类任取一个数组成的整数的集合，叫做模m的**简化剩余系**。

- 模m的简化剩余系的元素个数是多少？

- 模m的简化剩余系的元素个数为$\varphi(m)$，即$|(\mathbf{Z}/m\mathbf{Z})^*|=\varphi(m)$.

简化剩余系

- **例** 设m=10，则10个整数0,1,2,3,4,5,6,7,8,9中与10互素的整数为1,3,7,9，所以$\varphi(10)$=4，1,3,7,9是模10的最小非负简化剩余系。

- **例** 设m=30，则模m的简化剩余系是？

- **例** 当m=p为素数，则模m的简化剩余系是？
- 如何判断一组数是否构成模m的简化剩余系？

简化剩余系

- **定理2.2.2** 设m是一个正整数。若$r_1,r_2,\ldots,r_{\varphi(m)}$是$\varphi(m)$个与$m$互素的整数，并且两两模$m$不同余，则$r_1,r_2,\ldots,r_{\varphi(m)}$是模$m$的一个简化剩余系。

- 思考：简化剩余系是否唯一？

- 一个简化剩余系的所有元素通过线性变换后，还是简化剩余系吗？

● 简化剩余系

- 检验：设$x_1, \ldots, x_{\varphi(m)}$是模$m$的一个简化剩余系，$b+x_0$，$b+x_1, \ldots, b+x_{\varphi(m)}$和$ax_1, \ldots, ax_{\varphi(m)}$是模$m$的一个简化剩余系吗？

定理

- **定理2.2.3** 设m是一个正整数，a是满足$(a,m)=1$的整数。如果x遍历模m的一个简化剩余系，则ax也遍历模m的一个简化剩余系。

简化剩余系

例 设$m=7$，a表示第一列，与m互素的给定数；x表示第一行对应的数，遍历模m的简化剩余系；a所在行与x所在列的交叉位置表示ax模m的最小非负剩余，则有右表：

a \ x	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

简化剩余系

- 在整数集合中，加法有单位元0(任意整数加0还是这个整数)，对于任意的整数a，存在整数$-a$，使得$a+(-a)=0$。
- 非零整数集合乘法的单位元1(任意整数乘1还是这个整数)，对于任意非零整数a，是否存在整数b，使得$ab=1$？

简化剩余系

思考

- 如果把集合扩大到非零有理数集合呢？
- 模m同余情况下呢？对于任意非零整数a，是否存在整数b，使得$ab\equiv 1 \pmod{m}$?
- 设m=30，a_1=3，a_2=7，是否存在整数b_1，b_2，使得$a_1b_1\equiv 1 \pmod{m}$，$a_2b_2\equiv 1 \pmod{m}$？

简化剩余系

◆ **定理2.2.4** 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'，$1\le a'<m$，使得

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

● 简化剩余系

性质

- 给定正整数m和与m互素的整数a，由于$1\le a'<m$的a'是唯一存在的，一般记作a^{-1}.

- 给定正整数m和与m互素的整数a，如何计算整数a^{-1}，使得$aa^{-1}\equiv 1 \pmod{m}$？

- 提示：利用广义Euclid除法。

因为$(a,m)=1$，故存在整数s,t，使得$sa+tm=(a,m)=1$。

因此$a^{-1}\equiv s \pmod{m}$，$1\le a^{-1}<m$，满足$aa^{-1}\equiv 1 \pmod{m}$。

简化剩余系

例：利用模5,6的完全剩余系构造模30的一个完全剩余系。

- 换成简化剩余系呢？
- 例：利用模5,6的简化剩余系可以构造模30的一个简化剩余系吗？

简化剩余系

- **定理 2.2.5** 设m_1, m_2是互素的两个正整数。如果x_1, x_2分别遍历m_1, m_2的简化剩余系，则$m_2x_1+m_1x_2$遍历模m_1m_2的简化剩余系。

- 给定一个正整数n，那么怎么求$\varphi(n)$呢？

● Euler函数

思考

- 例 设$m=20$，求$\varphi(m)$。
- 例 设$m=30$，求$\varphi(m)$。

- **定理 2.2.6** 设m, n是互素的两个正整数。则

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

- 例 设$m=77$，求$\varphi(m)$。
- 例 设$m=16$，求$\varphi(m)$；$m=27$呢？

Euler函数

- **定理** 当$n=p^a$为素数幂时，$\varphi(n)=p^a-p^{a-1}$.

- 证明：模n的完全剩余系为

$0, 1, \ldots, p-1,$

$p, p+1, \ldots, 2p-1,\ \ \ldots\ldots,$

$p(p^{a-1}-1), p(p^{a-1}-1)+1, \ldots, p^a-1,$

共p^a个整数，其中与n不互素的整数为：

$p\cdot 0, p\cdot 1, \ldots, p(p^{a-1}-1)$，因此，$\varphi(n)=p^a-p^{a-1}$。

Euler函数

- **定理 2.2.7** 设正整数n的标准分解式为

$$n=p_1^{\alpha 1}p_2^{\alpha 2}\ldots p_k^{\alpha k}$$

则

$$\varphi(n)=n\Pi_{p|n}(1-1/p)=n(1-1/p_1)\ldots(1-1/p_k)$$

- **推论** 设p, q是不同的素数，则

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

Euler函数

- 这样是不是就可以求出所有整数的欧拉函数？
- 注：当n为合数，且不知道n的因数分解时，很难求出n的Euler函数$\varphi(n)$。
- **例** 设正整数n是两个不同素数的乘积。证明：如果已知n和n的Euler函数$\varphi(n)$，则可以求出n的因数分解。

● Euler定理

性质

- **例** 设$m=7$，$a=2$，我们有$(2,7)=1$，$\varphi(7)=6$。考虑模7的最小非负简化剩余系。当x遍历模7的最小非负简化剩余系时，ax模7会怎样？

$2\cdot1\equiv2 \pmod 7$，$2\cdot2\equiv4 \pmod 7$，$2\cdot3\equiv6 \pmod 7$，

$2\cdot4\equiv1 \pmod 7$，$2\cdot5\equiv3 \pmod 7$，$2\cdot6\equiv5 \pmod 7$，

上述同余式左右对应相乘，有

$$(2\cdot1)\cdot(2\cdot2)\cdot(2\cdot3)\cdot(2\cdot4)\cdot(2\cdot5)\cdot(2\cdot6)\equiv1\cdot2\cdot3\cdot4\cdot5\cdot6 \pmod 7,$$

Euler定理

- 整理得：

$$2^6\cdot(1\cdot2\cdot3\cdot4\cdot5\cdot6)\equiv1\cdot2\cdot3\cdot4\cdot5\cdot6(\mathrm{mod}\ 7)$$

那么我们可以得到什么结论？

- 因为$1\cdot2\cdot3\cdot4\cdot5\cdot6\equiv1\cdot(2\cdot4)\cdot(3\cdot5)\cdot6\equiv-1(\mathrm{mod}\ 7)$，所以

$$2^6\equiv1(\mathrm{mod}\ 7)。$$

● Euler定理

性质

- **例** 设$m=30$，$a=7$，我们有$(30,7)=1$，$\varphi(30)=$？考虑模30的最小非负简化剩余系。当x遍历模30的最小非负简化剩余系时，ax模30会怎样？

$$7\cdot1\equiv7，7\cdot7=49\equiv19，7\cdot11=77\equiv17，$$

$$7\cdot13=91\equiv1，7\cdot17=119\equiv29，7\cdot19=133\equiv13，$$

$$7\cdot23\equiv7\cdot(-7)\equiv11，7\cdot29\equiv7\cdot(-1)\equiv23 \pmod{30}，$$

Euler定理

$7^8\cdot(1\cdot7\cdot11\cdot13\cdot17\cdot19\cdot23\cdot29)\equiv1\cdot7\cdot11\cdot13\cdot17\cdot19\cdot23\cdot29 \pmod{30}$

另一方面，$(1\cdot7\cdot11\cdot13\cdot17\cdot19\cdot23\cdot29, 30)=1$，因此

$$7^8\equiv1 \pmod{30}。$$

- **定理2.2.9(Euler定理)** 设m是大于1的整数，a是满足$(a,m)=1$的整数，则

$$a^{\varphi(m)}\equiv1 \pmod{m}.$$

Fermat函数

- **定理2.2.10(Fermat)** 设p是一个素数，则对任意整数a，我们有

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

- 设p是一个素数，a是满足$(a,p)=1$的整数，则

$$a^{p-1} \equiv 1 \pmod{p}.$$

Wilson定理

- **例** 设$p=7$，我们有

$$1\cdot2\cdot3\cdot4\cdot5\cdot6\equiv(1\cdot6)\cdot(2\cdot4)\cdot(3\cdot5)\equiv-1 \pmod 7.$$

- **例** 设$p=17$，则最小非负简化剩余系元素乘积是什么？如何快速算出来？

- **定理2.2.11(Wilson)** 设p是一个素数，则

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

同余相关内容

- 同余的基本性质
- Euler定理Fermat小定理
- **模重复平方计算法**
- 大素数的生成

引入

- **例** 计算$312^{13}\ (\mathrm{mod}\ 667)$.

- 解法：先计算$312^{2}\ (\mathrm{mod}\ 667)$，再计算

$$312^{3}\ (\mathrm{mod}\ 667)$$

$$\equiv(312^{2}\ (\mathrm{mod}\ 667))\ 312\ (\mathrm{mod}\ 667)$$

依次下去，递归地得到$312^{13}\ (\mathrm{mod}\ 667)$。

- 有没有更快速一点的算法呢？

● 模重复平方计算法

问题

- 设m和n是一个大整数，如何计算

$$b^n \pmod{m}?$$

- 一般可以递归地计算

$$b^n \equiv (b^{n-1} \pmod{m}) \cdot b \pmod{m}$$

- 如此需要计算$n-1$次模余运算。
- 那么如果计算$12996^{227} \pmod{37909}$呢?

模重复平方计算法

- 模重复平方计算法计算$b^n \pmod{m}$

- 首先，将n写成二进制：

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

其中$n_i\in\{0,1\}$，$i=0,1,\ldots,k-1$，则

$b^n \pmod{m}$的计算可归结为：

$$b^n\equiv b^{n_0}(b^2)^{n_1}\ldots(b^{2^{k-2}})^{n_{k-2}}(b^{2^{k-1}})^{n_{k-1}} \pmod{m}$$

● 模重复平方计算法

- 模重复平方计算法具体描述如下：

➢ 将n写成二进制：

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

其中$n_i\in\{0,1\}$，$i=0,1,\ldots,k-1$。

0)令$a=1$，并计算

$$a_0\equiv a\cdot b^{n_0}(\mathrm{mod}\ m),\ b_1\equiv b^2(\mathrm{mod}\ m).$$

● 模重复平法计算法

算法

1）计算

$$a_1 \equiv a_0 \cdot b_1^{n_1} \pmod{m},\ b_2 \equiv b_1^2 \pmod{m},$$

…………

$k-2$）计算

$$a_{k-2} \equiv a_{k-3} \cdot b_{k-2}^{n_{k-2}} \pmod{m},\ b_{k-1} \equiv b_{k-2}^2 \pmod{m},$$

$k-1$）计算

$a_{k-1} \equiv a_{k-2} \cdot b_{k-1}^{n_{k-1}} \pmod{m}$, a_{k-1}就是$b^n \pmod{m}$.

模重复平方计算法

$$\underbrace{\underbrace{\underbrace{\underbrace{\underbrace{b^{n_0}}_{a_0}(\underbrace{b^{2}}_{b_1})^{n_1}}_{a_1}\cdots}_{\vdots}(\underbrace{b^{2^{k-2}}}_{b_{k-2}})^{n_{k-2}}}_{a_{k-2}}(\underbrace{b^{2^{k-1}}}_{b_{k-1}})^{n_{k-1}}}_{a_{k-1}}\ (\bmod\ m)$$

$$\begin{cases} b_0 = b = b^{2^0},\ a_0 \equiv a b_0^{n_0} \pmod m, \\ b_1 \equiv b^2 = b_0^2,\ a_1 \equiv a_0 b_1^{n_1} \pmod m, \\ \cdots\cdots\cdots \\ b_i \equiv b^{2^i} = b_{i-1}^2,\ a_i \equiv a_{i-1} b_i^{n_i} \pmod m, & i > 1. \\ \cdots\cdots\cdots \\ b_{k-1} \equiv b^{2^{k-1}} = b_{k-2}^2,\ a_{k-1} \equiv a_{k-2} b_{k-1}^{n_{k-1}} \pmod m. \end{cases}$$

模重复平方计算法

- 例 计算2^{35}(mod 47).
- 解：$35=1+2+0\cdot2^2+0\cdot2^3+0\cdot2^4+1\cdot2^5$，设$a=1$，

0) $n_0=1$, 因此$a_0\equiv a\cdot b\equiv 2$(mod 47)，$b_1\equiv b^2\equiv 2^2\equiv 4$(mod 47);

1) $n_1=1$,因此$a_1\equiv a_0\cdot b_1\equiv 2\cdot 4\equiv 8$(mod 47),

$b_2\equiv {b_1}^2\equiv 4^2\equiv 16$(mod 47);

2) $n_2=0$,因此$a_2=a_1\equiv 8$(mod 47)，$b_3\equiv {b_2}^2\equiv 16^2\equiv 21$(mod 47);

3) $n_3=0$,因此$a_3=a_2\equiv 8$(mod 47)，$b_4\equiv {b_3}^2\equiv 21^2\equiv 18$(mod 47);

4) $n_4=0$,因此$a_4=a_3\equiv 8$(mod 47)，$b_5\equiv {b_4}^2\equiv 18^2\equiv 42$(mod 47);

5) $n_5=1$,因此$a_5=a_4\cdot b_5\equiv 8\cdot 42\equiv 7$(mod 47).

同余相关内容

- 同余的基本性质
- Euler定理Fermat小定理
- 模重复平方计算法
- 大素数的生成

● 大素数生成

问题

- **Fermat小定理** 设n是素数，a是满足$(a,n)=1$的整数，则

$$a^{n-1}\equiv 1(\bmod n).$$

- 设m是大于1的整数，**存在**整数a满足$(a,m)=1$，$a^{m-1}\equiv 1\ (\bmod m)$，那么$m$是素数吗？

问题引入

- $8^{62}=(2^6)^{31}\cdot 2^2\equiv 1(\mathrm{mod}\ 63)$.

- 如果有存在一个整数b，$(b,n)=1$，使得

$$b^{n-1}\not\equiv 1(\mathrm{mod}\ n),$$

则n是一个合数。

大素数生成

- **定义2.4.1** 设n是一个奇合数。如果整数b，$(b,n)=1$使得同余式

$$b^{n-1}\equiv 1 \pmod{n}$$

成立，则n叫做对于基b的伪素数。

- **例** 整数63是对于基$b=8$的伪素数。
- **例** 整数$341=11\cdot 33$，$561=3\cdot 11\cdot 17$，$645=3\cdot 5\cdot 43$都是对于基$b=2$的伪素数。

大素数生成

- **定理2.4.2** 设n是一个奇合数，则
  - n是对于基b的伪素数当且仅当使得$b^e \equiv 1 \pmod{n}$的最小正整数e整除$n-1$；
  - 如果n是对于基b_1和基b_2的伪素数，则n是对于基b_1b_2的伪素数；
  - 如果n是对于基b的伪素数，则n是对于基b^{-1}的伪素数；
  - 如果有一个整数b, $(b, n)=1$，使得同余式$b^{n-1} \equiv 1 \pmod{n}$不成立，则模$n$的简化剩余系中至少有一半的数使得该同余式不成立。

大素数生成

- 设n是一个大奇数，定理2.4.2的第四条说明，对于随机选取的整数b，$(b,n)=1$，如果$b^{n-1}\equiv 1 \pmod n$，则n是合数的可能性小于50%。

➢ 由此，可以给出判断一个大奇数n是否为素数的方法。

● Fermat素性检测

Fermat素性检验

算法

- 给定奇数$n \geq 3$和安全参数t。

1. 随机选取整数b，$2 \leq b \leq n-2$；
2. 计算$r \equiv b^{n-1} \pmod{n}$；
3. 如果$r \neq 1$，则n是合数；
4. 上述过程重复t次

大素数生成

- 在运用Fermat素性检验算法时，会遇到如下形式的整数，须尽可能的避开它。

- **定义2.4.2** 合数n称为Carmichael数，如果对所有的正整数b，$(b, n)=1$，都有

$$b^{n-1}\equiv 1 \pmod{n}$$

成立。

- **例** 整数561=3·11·17是一个Carmichael数。

同余关系及其应用

- 国际图书标准(ISBN编码)

> ISBN 是国际通用的图书或独立的出版物(除定期出版的期刊)代码，出版社可以通过ISBN清晰地辨认所有非期刊书籍，一个ISBN只有一个或一份相应的出版物与之对应。

> ISBN编号对出版商、书商的工作有很大的益处，体现在：ISBN是机读的编码，从图书的生产到发行、销售都始终如一，使得图书的发行、定购、库存控制等程序都简化了。

同余关系及其应用

- 2007年1月1日前，ISBN由10位数字组成，分四个部分：组号(国家、地区、语言的代号)，出版社号，书序号和检验码。2007年1月1日起，实行新版ISBN，由13位数字组成，分为5段，在原来的10位数字前加上3位EAN(欧洲商品编号)，图书产品代码“978”。

同余关系及其应用

- **13位ISBN编码**
  - 第一组：978或979(3位EAN，即欧洲商品编号)
  - 第二组：国家，语言或区位代码
  - 第三组：出版社代码；由各国家或地区的国际标准书号分配中心，分给各个出版社。
  - 第四组：书序码；该出版物代码，由出版社具体给出。
  - 第五组：校验码。只有一位，从0到9。

● 同余关系及其应用

ISBN 978-7-04-031181-5

9 787040 311815 >

- ISBN：987-7-04-0331181-5
  - 第一组：978或979
  - 国家，语言或区位代码：7
  - 出版社代码：04
  - 书序码：033118
  - 校验码：5

- 将13位编码从左到右排序，前12位奇数位乘以1，偶数位乘以2，作和后模10，与校验码对比是否相同。