

## 1.4.1 求解线性同余方程

□例: 求解线性同余方程  $101x \equiv 2 \pmod{4620}$ .

□解:

- 在前面的例子中已经求解到101模4620的逆为1601.
- 因此在同余方程两边同时乘以1601得:  $1601 * 101 * x \equiv 2 * 1601 \pmod{4620}$ .
- 其中  $1601 * 101 \equiv 1 \pmod{4620}$ , 化解可得  $x \equiv 2 * 1601 \pmod{4620} \equiv 3202 \pmod{4620}$ .
- 所以, 该同余方程的解是使得  $x \equiv 3202 \pmod{4620}$  的所有整数  $x$ , 比如3202, 7822, ...以及-1418, -6038,...

【备注:前面的例子中已经求解101模4620的逆为1601】

## 1.4.1 求解线性同余方程

- 如果线性同余方程中  $ax \equiv b \pmod{m}$ ,  $a, m$  不互素的情况下该如何求解呢?
- 【定理】: 同余方程  $ax \equiv b \pmod{m}$  有解的充要条件是  $\gcd(a, m) \mid b$ .
- 证明略

## 1.4.1 求解线性同余方程

□例: 求解线性同余方程  $35x \equiv 10 \pmod{15}$

□解:

- 求解  $\gcd(35, 15) = 5$ , 因此不能直接使用模逆来求解. 但  $\gcd(35, 15) = 5 \mid 10$ , 因此方程有解.
- 注意到 35, 10, 15 存在公约数 5. 因此可以化解为  $7x \equiv 2 \pmod{3}$
- 求解可得  $x \equiv 2 \pmod{3}$  的所有整数  $x$ . 因此  $x = 3t + 2$ ,  $t$  为整数.
- 这其中小于 15 的正整数分别有 2 ( $t = 0$  时), 5 ( $t = 1$  时), 8 ( $t = 2$  时), 11 ( $t = 3$  时), 14 ( $t = 4$  时)
- 因此, 该同余方程的解是满足  $x \equiv 2, 5, 8, 11, 14 \pmod{15}$  的所有整数  $x$ , 比如 2, 5, 8, 11, 14, ... 及 -1, -4, -7, ...

【基础知识: 设  $d \geq 1$ , 则  $a \equiv b \pmod{m} \Leftrightarrow da \equiv db \pmod{dm}$ 】

## 1.4.1 求解线性同余方程

□例: 求解线性同余方程 $6x \equiv 3 \pmod{9}$ .

□解:

- $\gcd(6, 9) = 3 \mid 3$ , 方程有解.
- 注意到6, 3, 9存在公约数3. 因此可以化解为 $2x \equiv 1 \pmod{3}$
- 求解可得 $x \equiv 2 \pmod{3}$ 的所有整数 $x$ . 因此 $x = 3t + 2$ ,  $t$ 为整数.
- 这其中小于9的正整数分别有2( $t = 0$ 时), 5( $t = 1$ 时), 8( $t = 2$ 时)
- 因此, 该同余方程的解是满足 $x \equiv 2, 5, 8 \pmod{9}$ 的所有整数 $x$ , 比如2, 5, 8, ...及-1, -4, -7, ...

## 1.4.2 中国剩余定理

□在古代中国, 数学家孙子问道:

➤有物不知其数, 三分之余二, 五分之余三, 七分之余二, 此物几何?

□翻译过来就是下列**同余方程组**的解是什么:

➤  $x \equiv 2 \pmod{3},$

➤  $x \equiv 3 \pmod{5},$

➤  $x \equiv 2 \pmod{7}?$

□中国剩余定理、反向替换等方法都可以来求解该问题.

## 1.4.2 中国剩余定理

- 例:求解孙子的提问,  $x \equiv 2 \pmod{3}$ ,  $x \equiv 3 \pmod{5}$ ,  $x \equiv 2 \pmod{7}$
- 【解法编成歌诀: “三人同行七十稀, 五树梅花廿一支, 七子团圆正半月, 除百零五便得知”】
  - 三人同行七十稀: 把除以3所得的余数用70乘
  - 五树梅花日一枝: 把除以5所得的余数用21乘
  - 七子团圆正半月: 把除以7所得的余数用15乘
  - 除百零五便得知: 把上述三个积加起来, 减去105的倍数(其中 $105=3*5*7$ ), 所得的差即为所求
  - 因此列式为 $2 \times 70 + 3 \times 21 + 2 \times 15 = 233$ ,  $233 - 105 \times 2 = 23$

## 1.4.2 中国剩余定理

□ **中国剩余定理** (Chinese remainder theorem, CRT), 又称为孙子定理 (实际上是秦九韶发现的).

□ **【中国剩余定理】**: 令  $m_1, m_2, \dots, m_n$  为大于1的**两两互素**的正整数, 而  $a_1, a_2, \dots, a_n$  是任意整数, 则同余方程

➤  $x \equiv a_1 \pmod{m_1}$

➤  $x \equiv a_2 \pmod{m_2}$

➤ ...

➤  $x \equiv a_n \pmod{m_n}$

存在着唯一的解  $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_n M_n y_n$ , 这其中  $m = m_1 m_2 \dots m_n$ ,  $M_i = \frac{m}{m_i}$ , 由于  $\gcd(M_i, m_i) = 1$ , 必存在整数  $y_i$  使得  $M_i y_i \equiv 1 \pmod{m_i}$ ,  $i = 1, 2, \dots, n$ .

## 1.4.2 中国剩余定理

□例:求解孙子的提问,  $x \equiv 2 \pmod{3}$ ,  $x \equiv 3 \pmod{5}$ ,  $x \equiv 2 \pmod{7}$

□解:

- 令  $m=3 \cdot 5 \cdot 7=105$ ,  $M_1=m/3=35$ ,  $M_2=m/5=21$ ,  $M_3=m/7=15$ .
- 可以算出,  $y_1=2$  是  $M_1=35$  模 3 的逆, 因为  $35 \cdot 2 \equiv 2 \cdot 2 \equiv 1 \pmod{3}$ ;  $y_2=1$  是  $M_2=21$  模 5 的逆, 因为  $21 \equiv 1 \pmod{5}$ ;  $y_3=1$  是  $M_3=15$  模 7 的逆, 因为  $15 \equiv 1 \pmod{7}$
- 因此,  $x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \pmod{105}$
- 从而, 我们得出 23 是方程组的一个最小的正整数解.

## 1.4.2 反向替换方法

- 在中国剩余定理中要求  $m_1, m_2, \dots, m_n$  是两两互素的正整数. 但实际中可能并不一定满足. 因此, 我们还可以用一种称为**反向替换**的方法来求解同余方程组.
- 例: 利用反向替换的方法求解孙子的提问,  $x \equiv 2 \pmod{3}, x \equiv 3 \pmod{5}, x \equiv 2 \pmod{7}$
- 解:
  - 第一个同余方程可以重写为  $x = 3t + 2$ , 其中  $t$  是整数 (回顾定理4:  $a \equiv b \pmod{m}$ , 当且仅当存在整数  $k$  使得  $a = b + km$ )
  - 将它放入第二个同余方程可得  $3t + 2 \equiv 3 \pmod{5}$ .
  - 解它可得  $t \equiv 2 \pmod{5}$ .
  - 第二个同余方程可以重写为  $t = 5u + 2$ , 其中  $u$  是整数.

## 1.4.2 反向替换方法

□解(续):

- 将它放入刚才的等式  $x = 3t + 2$ , 可得  $x = 3(5u + 2) + 2 = 15u + 8$ .
- 再将它放入第三个同余方程可得  $15u + 8 \equiv 2 \pmod{7}$ .
- 解它可得  $u \equiv 1 \pmod{7}$ .
- 第三个同余方程可以重写为  $u = 7v + 1$ , 其中  $v$  是整数.
- 将它放入刚才的等式  $x = 15u + 8$ , 可得  $x = 15(7v + 1) + 8 = 105v + 23$ .
- 将这个转换为一个同余式, 就能找到同余方程组的解,  $x \equiv 23 \pmod{105}$ .

## 1.4.2 反向替换方法

□例: 韩信点兵问题. 一队士兵已知少于105人, 排成每行3人余2人, 每行5人余1人, 每行7人余6人. 问这队士兵至少有多少人?

□解: 易知等价求满足如下三个同余方程组的最小正整数:

$$x \equiv 2 \pmod{3}$$

$$x \equiv 1 \pmod{5}$$

$$x \equiv 6 \pmod{7}$$

- 由第一个同余式, 存在整数 $k$ 使得 $x = 3k + 2$ , 代入第二个同余式得 $3k + 2 \equiv 1 \pmod{5}$ , 即 $3k \equiv 4 \pmod{5}$ . 它有唯一解 $k \equiv 3 \pmod{5}$ . 故存在整数 $r$ 使得 $k = 5r + 3$ ,
- 从而 $x = 3(5r + 3) + 2 = 15r + 11$ , 代入第三个同余式得 $15r + 11 \equiv 6 \pmod{7}$ , 即 $15r \equiv 2 \pmod{7}$ . 它有唯一解 $r \equiv 2 \pmod{7}$ . 故存在整数 $s$ 使得 $r = 7s + 2$ ,
- 从而 $x = 15(7s + 2) + 11 = 105s + 41$ , 即要求的解为41. 将这个转换为一个同余式, 就能找到同余方程组的解,  $x \equiv 41 \pmod{105}$ . 因此士兵为41人.

## 1.4.3 大整数的计算机算术

- 假定 $m_1, m_2, \dots, m_n$ 是两两互素的模数, 并令 $m$ 为其乘积. 根据中国剩余定理可以证明满足 $0 \leq a < m$ 的整数 $a$ 可以唯一地表示为一个 $n$ 元组, 其元素由 $a$ 除以 $m_i$ 的余数组成,  $i = 1, 2, \dots, n$ . 即 $a$ 可以唯一地表示为

$$(a \bmod m_1, a \bmod m_2, \dots, a \bmod m_n)$$

- 证明略.

## 1.4.3 大整数的计算机算术

□例: 当整数用二元组表示, 其中第一个元素是该整数除以3的余数, 第二个元素是该整数除以4的余数. 那么分别写出小于12的非负整数的二元组表示.

□解: 根据题目要求分别求解  $(a \bmod 3, a \bmod 4)$ ,  $0 \leq a < 12$ . 因此:

$0=(0,0)$	$1=(1,1)$	$2=(2,2)$	$3=(0,3)$
$4=(1,0)$	$5=(2,1)$	$6=(0,2)$	$7=(1,3)$
$8=(2,0)$	$9=(0,1)$	$10=(1,2)$	$11=(2,3)$

## 1.4.3 大整数的计算机算术

- 假定在某台计算机上做小于100的整数算术运算比做大整数算术快. 如果我们将整数表示为除以100以内的两两互素的模的余数, 那么可以将计算限制在100以内的整数中.
- 例: 在计算机中将整数表示为除以99, 98, 97, 95(它们是两两互素)的4元组. 那么计算123684和413456之和.
- 解:
  - 整数 $123684 = (33, 8, 9, 89)$ ,  $413456 = (32, 92, 42, 16)$
  - 为了计算和的结果, 我们不是直接将这两个整数做求和运算. 我们是将四元组的对应分量相加, 再按相应的结果进行各自的除以对应模的余数降低四元组分量的结果. 即
  - $123684 + 413456 = (33, 8, 9, 89) + (32, 92, 42, 16) = (65 \bmod 99, 100 \bmod 98, 51 \bmod 97, 105 \bmod 95) = (65, 2, 51, 10)$

## 1.4.3 大整数的计算机算术

□如果需要找出(65,2,51,10)所表示的整数, 那么需要求解同余方程组

$$x \equiv 65 \pmod{99}$$

$$x \equiv 2 \pmod{98}$$

$$x \equiv 51 \pmod{97}$$

$$x \equiv 10 \pmod{95}$$

□使用前述方法可以求解得到该方程组唯一小于 $99 * 98 * 97 * 95 = 89403930$ 的解是537140. 计算可知 $123684 + 413456 = 537140$ 确实是这两个整数的和.

□总结: 只有当我们需要恢复(65,2,51,10)所表示的整数, 那么我们不得不做一次大于100的整数算术运算.

## 1.4.4 费马小定理



Pierre de Fermat  
(1601-1665)



华中科技大学  
计算机科学与技术学院  
School of Computer Science & Technology, HUST

- **费马小定理** (菲尔马小定理): 如果 $p$ 为素数,  $a$ 和 $p$ 互素, 则 $a^{p-1} \equiv 1 \pmod{p}$ . 定理的另外一种形式: 如果 $p$ 为素数, 对每个整数 $a$ ,  $a^p \equiv a \pmod{p}$ .
- 该定理的证明自行验证.
  - 该定理在计算整数高次幂的模 $p$ 余数时非常有用.
  - 可以用来验证是否为素数(必要不充分条件). 只能说明不满足上式, 那么一定不是素数.

## 1.4.4 费马小定理

□例: 计算  $7^{222} \bmod 11$ .

□解: 根据费马小定理, 11 是素数, 并且  $\gcd(7, 11) = 1$ ,  $7^{10} \equiv 1 \pmod{11}$ . 所以对每个正整数  $k$  有  $(7^{10})^k \equiv 1 \pmod{11}$ . 因此,  $7^{222} = 7^{22 \times 10 + 2} = (7^{10})^{22} \times 7^2 \equiv (1)^{22} \times 49 \equiv 5 \pmod{11}$ . 因此  $7^{222} \bmod 11 = 5$ .

□备注: 还可以用之前学的模指数运算来求解.

## 1.4.4 费马小定理

□例: 计算  $29^{25} \bmod 11$ .

□解:

- $29 \equiv 7 \pmod{11}$
- 那么,  $29^{25} \equiv 7^{25} \pmod{11}$
- 根据费马小定理,  $7^{10} \equiv 1 \pmod{11}$ , 所以对每个正整数  $k$  有  $(7^{10})^k \equiv 1 \pmod{11}$ .
- 因此,  $7^{25} = 7^{2 \times 10 + 5} = (7^{10})^2 \times 7^5 \equiv (1)^2 \times 7 \times (-4)^4 \equiv 7 \times 256 \equiv 7 \times 3 \equiv 10 \pmod{11}$ . 因此  $29^{25} \bmod 11 = 10$ .

## 1.4.5 伪素数

- 【定义】:令 $b$ 是一个正整数, 如果 $n$ 是一个正合数, 且 $b^{n-1} \equiv 1 \pmod{n}$ , 则 $n$ 称为以 $b$ 为基数的**伪素数**.
- 给定一个正整数 $n$ , 使得 $2^{n-1} \equiv 1 \pmod{n}$ . 如果存在这样的 $n$ , 则 $n$ 要么是素数(参见费马小定理), 要么是一个以2为基数的伪素数.
- 例: $2^{5-1} = 16 \equiv 1 \pmod{5}$ , 5为素数.
- 例: $2^{341-1} \equiv 1 \pmod{341}$ , 且 $341 = 11 * 31$ , 341是以2为基数的伪素数.

【费马小定理: 如果 $p$ 为素数,  $a$ 和 $p$ 互素, 则 $a^{p-1} \equiv 1 \pmod{p}$ .  
或者表达为: 如果 $p$ 为素数, 对每个整数 $a$ ,  $a^p \equiv a \pmod{p}$ 】

## 1.4.5 卡米切尔数



Robert Carmichael  
(1879-1967)



清华大学  
计算机科学与技术学院  
School of Computer Science & Technology, Tsinghua University

- 【定义】：一个正合数 $n$ ，如果对于所有满足 $\gcd(b, n) = 1$ 的正整数 $b$ 都有同余式 $b^{n-1} \equiv 1 \pmod{n}$ 成立，则称为**卡米切尔数**(carmichael number, 或称卡迈克尔数, 卡米歇尔数).
- 判断一个数是否为卡米切尔数常会用到的性质:
- 假设 $m_1, m_2, \dots, m_n$ 是大于等于2的整数且两两互素.  $m = m_1 m_2 \dots m_n$   
如果 $a \equiv b \pmod{m_i}$ , 其中 $i=1, 2, \dots, n$ , 则 $a \equiv b \pmod{m}$
- 备注:证明略

## 1.4.5 卡米切尔数

□例: 561是否是卡米切尔数?

□解:

- 首先注意561是合数, 因为进行素因子分解可得 $561 = 3 \cdot 11 \cdot 17$ .
- 其次, 如果 $\gcd(b, 561) = 1$ , 则 $\gcd(b, 3) = \gcd(b, 11) = \gcd(b, 17) = 1$ .
- 利用费马小定理可得 $b^2 \equiv 1 \pmod{3}$ ,  $b^{10} \equiv 1 \pmod{11}$ ,  $b^{16} \equiv 1 \pmod{17}$ .
- 从而,  $b^{560} = (b^2)^{280} \equiv 1 \pmod{3}$ ,  $b^{560} = (b^{10})^{56} \equiv 1 \pmod{11}$ ,  $b^{560} = (b^{16})^{35} \equiv 1 \pmod{17}$ .
- 对于满足 $\gcd(b, 561) = 1$ 的正整数 $b$ , 都有 $b^{560} \equiv 1 \pmod{561}$ . 所以, 561是卡米切尔数.

## 1.4.6 原根

□ 【定义】：模素数 $p$ 的一个**原根**是 $\mathbb{Z}_p$ 中的整数 $r$ , 使得 $\mathbb{Z}_p$ 中的每个非零元素都是 $r$ 的一个幂次.

- $r$ 的幂次的结果形成了一个完整的循环, 覆盖了 $1, 2, \dots, p-1$ 的所有可能的元素. 原根的关键性质包括:
- 1) 并非所有数都有原根;
- 2) 不唯一: 一个素数 $p$ 如果有原根, 通常不止一个;
- 3) 保证了一一对应: 幂次 $r^x$  (其中 $x$ 从1到 $p-1$ ) 与结果 $y$  (从1到 $p-1$ )之间是一一对应的.

## 1.4.6 原根

□例: 判断2是否是模7的原根, 3是否是模7的原根?

□解:

- 在 $Z_7$ 中计算2的幂次时, 可得 $2^1 \bmod 7 = 2$ ,  $2^2 \bmod 7 = 4$ ,  $2^3 \bmod 7 = 1$ ,  $2^4 \bmod 7 = 2$ ,  $2^5 \bmod 7 = 4$ ,  $2^6 \bmod 7 = 1$ . 可以看到 $Z_7$ 中的非零元素(1,2,...,6)不全在2的幂次结果中, 所以2不是模7的原根.
- 在 $Z_7$ 中计算3的幂次时, 可得 $3^1 \bmod 7 = 3$ ,  $3^2 \bmod 7 = 2$ ,  $3^3 \bmod 7 = 6$ ,  $3^4 \bmod 7 = 4$ ,  $3^5 \bmod 7 = 5$ ,  $3^6 \bmod 7 = 1$ . 因为 $Z_7$ 中的非零元素都是3的幂次, 所以3是原根.

## 1.4.6 离散对数

- 【定义】：假设 $p$ 是一个素数,  $r$ 是一个模 $p$ 的原根, 而 $a$ 是1和 $p-1$ 之间的一个整数. 如果 $r^e \bmod p = a$ , 且 $1 \leq e \leq p - 1$ , 我们说 $e$ 是以 $r$ 为底 $a$ 模 $p$ 的**离散对数**, 并记作 $\log_r a = e$  (这里隐含理解为有素数 $p$ ).
- 离散对数也称指标. 一般来说寻找离散对数是一个非常困难的问题, 这个问题的困难性也就成为了许多密码系统安全性的基础.
- 例: 分别找出以3为底3模7的离散对数, 以3为底5模7的离散对数
- 解: 上面计算模7的3幂次时得到 $3^1 \bmod 7 = 3$ ,  $3^5 \bmod 7 = 5$ 都在 $\mathbb{Z}_7$ 中, 故以3为底3和5模7的离散对数分别是1和5. 我们写成 $\log_3 3 = 1$ ,  $\log_3 5 = 5$ .

## 第1.4节 求解同余方程小结

- 线性同余方程  $ax \equiv b \pmod{m}$ , 通过  $a$  模  $m$  的逆  $\bar{a}$  来求解
- 同余方程组求解, 中国剩余定理  $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n$ , 或者反向替换
- $a^{p-1} \equiv 1 \pmod{p}$ , 费马小定理
- 以  $b$  为基数的伪素数,  $b^{n-1} \equiv 1 \pmod{n}$  成立的合数  $n$
- 卡米切尔数, 合数  $n$  使得对所有满足  $\gcd(b, n) = 1$  的正整数  $b$ ,  $n$  是以  $b$  为基数的伪素数
- 素数  $p$  的原根,  $Z_p$  中的整数  $r$  使得每个不能被  $p$  整除的整数模  $p$  同余  $r$  的一个幂次
- 以  $r$  为底  $a$  模  $p$  的离散对数, 满足  $0 \leq e \leq p-1, r^e \equiv a \pmod{p}$  的整数  $e$