求解同余方程

小节概要4

Linear Congruences(线性同余方程)

The Chinese Remainder Theorem(中国剩余定理)

Fermat's Little Theorem(费马小定理)

Pseudoprimes(伪素数)

Primitive Roots and Discrete Logarithms

(原根和离散对数)

Linear Congruences (线性同余式)

定义:形如 $ax \equiv b \pmod{m}$ 的同余式，其中 m 为正整数，a 和 b 是整数，x 是变量，称为线性同余式.

线性同余式 $ax \equiv b \pmod{m}$ 的解是所有满足该同余式的整数 x.

定义: 如果整数 $\bar{a}$ 满足$\bar{a}a \equiv 1 \pmod{m}$称 $\bar{a}$为 a 的模 m 的逆元.

例子: 5 是 3 模 7 的逆元，因为 $5 \cdot 3 = 15 \equiv 1 \pmod{7}$

求解线性同余式的一种方法是使用 a 的逆元 $\bar{a}$ （如果它存在）。虽然不能直接将同余式的两边除以 a，但可以通过乘以 $\bar{a}$ 来解 x.

a modulo m的逆元

以下定理保证了，当 a 和 m 互素时，a 在模 m 下的逆元存在。两个整数 a 和 b 当 gcd (a,b)=1时互素.

定理 1:如果 a 和 m 是互素的整数且 m>1，那么 a 在模 m 下有逆元。此外，这个逆元在模 m 下是唯一的。（这意味着存在一个唯一的正整数 $\bar{a}$ 小于 m，它是 a 在模 m 下的逆元，且 a 的任何其他模 m 下的逆元都与 $\bar{a}$ 在模 m 下同余

证明:由于 gcd (a,m)=1，根据贝祖定理，存在整数 s 和 t 使得:

- 因此, $sa + tm \equiv 1 \pmod{m}$.
- 由于 $tm \equiv 0 \pmod{m}$, 所以$sa \equiv 1 \pmod{m}$
- 因此，s 是 a 在模 m 下的逆元.
- 逆元的唯一性也可以被证明.

求解逆元1

欧几里得算法和贝祖系数为我们提供了一种系统的方法来寻找逆元.

例子:求 3 在模 7 下的逆元.

解:由于 gcd(3,7)=1，根据上页定理1，3 在模 7 下的逆元存在.

- 使用欧几里得算法: 7 = 2·3 + 1.
- 从这个等式，我们得到：−2·3+1·7=1,可以看出，−2 和 1 是 3 和 7 的贝祖系数.
- 因此，−2 是 3 在模 7 下的逆元.
- 同时，任何与 −2 在模 7 下同余的整数也是 3 的模 7 逆元，例如 5、−9、12 等.

求解逆元2

例子:求 101 在模 4620 下的逆元.

解:先使用欧几里得算法证明 gcd(101,4620)=1.

4620 = 45·101 + 75

101 = 1·75 + 26

75 = 2·26 + 23

26 = 1·23 + 3

23 = 7·3 + 2

3 = 1·2 + 1

2 = 2·1

因为最后一个非零余数是 1,
gcd(101,4260) = 1

贝祖系数 : – 35 and 1601

Working Backwards:

1 = 3 – 1·2

1 = 3 – 1·(23 – 7·3) = – 1 ·23 + 8·3

1 = –1·23 + 8·(26 – 1·23) = 8·26 – 9 ·23

1 = 8·26 – 9 ·(75 – 2·26)= 26·26 – 9 ·75

1 = 26·(101 – 1·75) – 9 ·75

= 26·101 – 35 ·75

1 = 26·101 – 35 ·(4620 – 45·101)

= – 35 ·4620 + 1601·101

101 在模 4620 下的逆元为 1601

用逆元求解线性同余式

我们可以通过两边同时乘以 $\bar{a}$ 来解方程 $ax \equiv b \pmod{m}$.

例子:解方程 $3x \equiv 4 \pmod{7}$

解:之前已经找到 −2 是 3 在模 7 下的逆元。我们将方程两边同时乘以 −2

$$-2 \cdot 3x \equiv -2 \cdot 4 \pmod{7}.$$

因为 $-6 \equiv 1 \pmod{7}$ 并且 $-8 \equiv 6 \pmod{7}$, 因此如果x 是解, 则有 $x \equiv -8 \equiv 6 \pmod{7}$

我们需要确定每一个满足 $x \equiv 6 \pmod{7}$ 的 x 是否都是方程的解。假设 $x \equiv 6 \pmod{7}$ ，可验证 $3x \equiv 3 \cdot 6 = 18 \equiv 4 \pmod{7}$，这表明所有这样的 x 都满足这个同余式.

因此，解集是所有满足 $x \equiv 6 \pmod{7}$ 的整数，即 $x = 6, 13, 20$或者 $x = -1, -8, -15$

The Chinese Remainder Theorem (中国剩余定理) 1

在公元一世纪，中国数学家孙子提出了以下问题：“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？”

这个谜题可以被转化为解以下同余方程组的问题:

$x \equiv 2 \pmod 3$,

$x \equiv 3 \pmod 5$,

$x \equiv 2 \pmod 7$

我们将看到一个被称为中国剩余定理的定理是如何用于解决孙子的这个问题的.

中国剩余定理2

定理 2: (*The Chinese Remainder Theorem*) 设 $m_1,m_2,\ldots,m_n$是两两互素的大于 1 的正整数并且$a_1,a_2,\ldots,a_n$ 是任意整数.对于以下同余方程组

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

.

.

.

$x \equiv a_n \pmod{m_n}$

此方程组有唯一的模 $m = m_1m_2 \cdots m_n$的解

(即，存在一个解 x，使得 $0 \le x < m$，且所有其他解均与该解模 m 同余.)

证明:我们将通过描述一种构造解的方法来证明解的存在性.

中国剩余定理3

为了构造解，首先令$M_k=m/m_k$ 对于 $k = 1,2,\ldots,n$ 以及 $m = m_1 m_2 \cdots m_n$.
因为 $\gcd(m_k, M_k) = 1$, 根据前述定理1, 存在整数y_k, 它是 M_k 在 模 m_k下的逆元， *使得*

$$M_k\, y_k \equiv 1 \pmod{m_k}.$$

然后构造和

$$x = a_1\, M_1\, y_1 + a_2\, M_2\, y_2 + \cdots + a_n\, M_n\, y_n .$$

注意到因为$M_j \equiv 0 \pmod{m_k}$ 当 $j \neq k$,所以在这个和中，除了第 k 项外，所有项模 m_k 都同余于 0 .
由于 $M_k\, y_k \equiv 1 \pmod{m_k}$, 我们有 $x \equiv a_k\, M_k\, y_k \equiv a_k \pmod{m_k}$, 对于 $k = 1,2,\ldots,n$.
因此，x 是以下 n 个同余方程的同时解.

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

中国剩余定理解的唯一性证明

设有两两互质的正整数$n_1, n_2, ..., n_k$，以及任意整数$a_1, a_2, ..., a_k$，那么同余方程组

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

有唯一解模 $N = n_1 n_2 ... n_k$。

唯一性：要证明解的唯一性，假设存在两个解 x 和 y，它们都满足上述的同余方程组。那么我们有

$$x \equiv a_i \pmod{n_i} \quad 和 \quad y \equiv a_i \pmod{n_i} \quad 对于所有\ i = 1, 2, ..., k.$$

因此，对于所有的 i，我们有

$$x \equiv y \pmod{n_i}.$$

这意味着 n_i 整除 $x - y$ 对于所有的 i。

由于n_1,n_2…和n_k两两互质,且n_1|(x-y),n_2|(x-y)…,n_k|(x-y)，可证明N=(n_1*n_2*..*n_k) | (x-y)；

既然 N|(x−y)，这意味着 x≡y (mod N)。因此，任何两个解 x 和 y 在模 N 下都是相同的，这证明了解的唯一性。

中国剩余定理4

例:我们将应用中国剩余定理来解决孙子的问题:

$x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$.

- 令 $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, $M_3 = m/7 = 15$.
- 我们注意到
  - 2 是M_1 = 35 模 3的逆元 因为 $35 \cdot 2 \equiv 2 \cdot 2 \equiv 1 \pmod 3$
  - 1 是M_2 = 21 模 5的逆元 因为 $21 \equiv 1 \pmod 5$
  - 1 是M_3 = 15 模 7的逆元 因为 $15 \equiv 1 \pmod 7$
- 因此,

  $x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3$

  $= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \pmod{105}$
- 所以，23 是满足所有方程的最小正整数解

反向替换方法

我们还可以通过将线性同余方程组中的每个同余方程转化为等式，代入变量的值到另一个同余方程中，并持续进行这个过程，直到解决所有同余方程，从而解决具有互素模数的线性同余方程组。这种方法称为回代法.

例:使用回代法找到所有满足以下条件的整数 x使得 $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 6$, and $x \equiv 3 \pmod 7$.

解:第一个同余方程可以重写为 $x=5t+1$，其中 t 是一个整数.

- 代入第二个同余方程得到$5t + 1 \equiv 2 \pmod 6$.
- 解这个方程得$t \equiv 5 \pmod 6$.
- 使用定理4得到 $t=6u+5$，其中 u 是一个整数.
- *代回*$x = 5t + 1$, 解得 $x = 5(6u + 5) + 1 = 30u + 26$.
- 再代入第三个方程得到$30u + 26 \equiv 3 \pmod 7$.
- 解得$u \equiv 6 \pmod 7$.
- 使用定理4得到 $u=7v+6$，其中 v 是一个整数.
- 将 $u=7v+6$ 代入 $x=30u+26$ 中得到,$x = 30(7v + 6) + 26 = 210u + 206$.

将这个结果转化为同余方程，我们得到解$x \equiv 206 \pmod{210}$.

Wilson Theorem (威尔逊定理)

Wilson定理：P是素数当且仅当 (p-1)! ≡ -1(mod *p*).

引理：如p为素数且 $x^2 \equiv 1 \pmod p$，则$x \equiv 1 \pmod p$或 $x \equiv -1 \pmod p$.

引理证明：$p \mid (x^2-1)$,即 $p \mid (x+1)(x-1)$,因p为素数,则 $p \mid (x+1)$或 $p \mid (x-1)$，得证。

Wilson定理证明：

① 先证当(p-1)! ≡ -1(mod *p*)时, p为素数：

设n|p且n≠p，则$n \in \{1, 2, \cdots, p-1\}$，能推导出 n|(p−1)!；根据条件，

p| ((p-1)!+1)，因为n | p,则 推出 **n | ((p-1)!+1)**；又已推出 n|(p−1)!, 得n|1， 则n=1，推出p的因子只有p和1，则p为素数.

② 再证当p为素数时，(p-1)! ≡ -1(mod p)成立：

(p-1)!=1*(p-1)*(2*3*…*(p-2))=(p-1)*((p-3)/2对互逆的数相乘)(mod p)=(p-1) (mod p)=-1 (mod p), 得证.

引例：6! (mod 7)=1*(2*4)*(3*5)*6 (mod 7)= 6 (mod 7)= -1 (mod 7);

欧拉函数与欧拉定理

欧拉函数ϕ(n)： 比n小且与n互素的正整数的个数.

例：ϕ(6)=2 [1,5]；　　ϕ(7)=6 [1,2,3,4,5,6]

欧拉函数ϕ(n)的计算： 如果p是素数，则ϕ(p)=p-1. 如果n=pq，且p和q是两个不同的素数，则ϕ(n)=(p-1)(q-1).

欧拉定理：如果 gcd(a,n)=1，则$a^{\phi(n)} \equiv 1 \pmod n$.

证明：设X={x | x为小于n的正整数且gcd(x,n)=1}， 则 |X|=ϕ(n);

对元素a且gcd(a,n)=1,有集合aX={ax mod n| x∈X}；

因为gcd(a, n)=gcd(x, n)=1, 可知gcd(ax, n)=1； 再看aX集合中任意两个元素

$ax_i \equiv ax_j \pmod n$是否成立；如成立，则推出$n|(x_i-x_j)$, 即$x_i=x_j$，矛盾⇒不成立

因此aX=X, 即两个集合相等;

将集合X和集合aX中所有元素相乘，得： $\prod_{x\in X} x = \prod_{y\in aX} y = \prod_{x\in X} ax \mod n$

再将以上等式两边都乘x mod n的逆，等式最左边为1，等式最右边为$a^{\phi(n)}$,

因此$a^{\phi(n)} \equiv 1 \pmod n$, 得证.

欧拉定理推论

欧拉定理推论：如果 gcd(a,n)=1，则$a^x \equiv a^{x \pmod{\phi(n)}} \pmod{n}$.

证明：x=q*ϕ(n)+r, r= x mod ϕ(n),

则 $a^x = a^{q\phi(n)+r} = (a^{\phi(n)})^q a^r \equiv a^r \equiv a^{x \pmod{\phi(n)}} \pmod{n}$.

欧拉定理推论应用：计算2^{999} mod 21=?

因n=21=3*7，则ϕ(21)=2*6=12, 又因为gcd(2,21)=1,

则2^{999} mod 21=$2^{999 \bmod 12}$=2^3=8 (mod 21)

在RSA公钥密码算法正确性证明中也会用到上述推论.

Fermat's Little Theorem (费马小定理)

定理 3:如果 p 是一个素数且 a 是一个不被 p 整除的整数，则有

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

此外，对于每个整数 a，都有

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

Pierre de Fermat

(1601-1665)

费马小定理在计算整数的大次幂的模 p 的余数时非常有用.

例: 计算 7^{222} **mod** 11.

根据费马小定理，我们知道$7^{10} \equiv 1 \pmod{11}$, 所以 $(7^{10})^k \equiv 1 \pmod{11}$, 对于每个正整数 k. 因此,

$$7^{222} = 7^{22 \cdot 10 + 2} = (7^{10})^{22} 7^2 \equiv (1)^{22} \cdot 49 \equiv 5 \pmod{11}.$$

因此, 7^{222} **mod** 11 = 5.

Pseudoprimes(伪素数)1

根据费马小定理，对于素数 $n>2$，有

$$2^{n-1} \equiv 1 \pmod{n}.$$

但如果这个同余方程成立，n 不一定是素数.合成整数n 满足 $2^{n-1} \equiv 1 \pmod{n}$被称为该基数2下的伪素数.

例: 整数 341 是基数 2 的伪素数.

$341 = 11 \cdot 31$

$2^{340} \equiv 1 \pmod{341}$

我们可以将 2 替换为任意整数$b \geq 2$.

定义:设 b 是一个正整数。如果 n 是一个合数，并且 $b^{n-1} \equiv 1 \pmod{n}$，那么 n 被称为基数 b 的伪素数

伪素数2

给定一个正整数 n，如果$2^{n-1} \equiv 1 \pmod{n}$:

- 如果 n 不满足该同余方程，它是合数.
- 如果 n 满足该同余方程，它可能是素数，也可能是基数 2 的伪素数.

使用额外的基数 b 进行类似的测试，可以提供更多关于 n 是否为素数的证据.

与素数相比，在不超过正实数 x 的正整数中，基数 b 的伪素数相对较少.

- 例如，在小于 10^{10}的正整数中，有 $455,052,512$ 个素数，但只有 $14,884$ 个基数 2 的伪素数.

Primitive Roots(原根)

定义:模素数 p 的原根是 $\mathbf{Z}_p$ 中的一个整数 r，使得 $\mathbf{Z}_p$ 中的每一个非零元素都是 r 的某个幂

例:对于素数 11，2 是一个原根，因为 $\mathbf{Z}_{11}$ 中的每个元素都可以表示为 2 的某个幂。计算如下

$2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 5,\ 2^5 = 10,$

$2^6 = 9,\ 2^7 = 7,\ 2^8 = 3,\ 2^9 = 6,\ 2^{10} = 1.$

例:对于质数 11，3 不是一个原根，因为并非所有 $\mathbf{Z}_{11}$ 中的元素都是 3 的某个幂。计算如下.

$3^1 = 3, 3^2 = 9, 3^3 = 5, 3^4 = 4, 3^5 = 1$,因此，3 的幂循环重复，并不能生成所有 $\mathbf{Z}_{11}$中的元素.

重要事实:对于每个素数 p，总存在一个原根.

Discrete Logarithms(离散对数)

假设 p 是一个素数，r 是模 p 的一个原根。如果 a 是一个位于 1 和 p–1 之间的整数，即 a 是 $\mathbf{Z}_p$ 的一个元素，那么存在一个唯一的指数 e使得$r^e = a$ 在 $\mathbf{Z}_p$ 中成立， 也就是 $r^e \bmod p = a$.

定义：设 p 是一个素数，r 是模 p 的一个原根，且 a 是位于 1 到 p–1 之间的整数。如果 $r^e \bmod p = a$ ，且 $1 \le e \le p-1$，我们称 e 是以 r 为底数 a为模 p的离散对数， 写作$\log_r a = e$ (其中素数 p 是默认的).

例 1:我们写作$\log_2 3 = 8$因为以2为底3模11的离散对数是 8，即$2^8 \bmod 11 = 3$.

例 2:我们写作$\log_2 5 = 4$因为以2为底5模11的离散对数是 4，即$2^4 \bmod 11 = 5$.