第四章 同余式、幂与费马小定理

张志强

智能信息处理研究中心
http://rciip.hrbeu.edu.cn

同余式

- 如果m整除a-b，我们说a与b模m同余，并记为 $a \equiv b \pmod{m}$
  - 例如，5|(7-2)，6|(47-35)
  - 我们有 $7 \equiv 2 \pmod{5}$, $47 \equiv 35 \pmod{6}$
- 如果a除以m得余数r，则a与r模m同余，注意$0 \leqslant r < m$，因此任意一个整数均与0~m-1之间的一个数模m同余。数m叫做同余式的模。

同余式的性质

- 具有相同模的同余式与通常的等式类似
  $a_1 \equiv b_1 (\mathrm{mod}\ m)$, $a_2 \equiv b_2 (\mathrm{mod}\ m)$，则有
  $a_1 \pm a_2 \equiv b_1 \pm b_2 (\mathrm{mod}\ m)$, $a_1 a_2 \equiv b_1 b_2 (\mathrm{mod}\ m)$
- 注意：用数除同余式并非总是可能的，即$ac \equiv bc (\mathrm{mod}\ m)$，则$a \equiv b (\mathrm{mod}\ m)$未必成立。
  - 例如，$15*2 \equiv 20*2 (\mathrm{mod}\ 10)$，但 $15 \not\equiv 20 (\mathrm{mod}\ 10)$

同余式的性质

- 特别是
  - $uv \equiv 0 (\mathrm{mod}\ m)$,
  - 但$u \not\equiv 0 (\mathrm{mod}\ m)$，且$v \not\equiv 0 (\mathrm{mod}\ m)$
  - 例如$6*4 \equiv 0 (\mathrm{mod}\ 12)$，但$6 \not\equiv 0 (\mathrm{mod}\ 12)$，且$4 \not\equiv 0 (\mathrm{mod}\ 12)$
- 然而还有，$7*3 \equiv 2*3 (\mathrm{mod}\ 5)$, $7 \equiv 2 (\mathrm{mod}\ 5)$
- 当$\gcd(c,m)=1$时，则可以从同余式$ac \equiv bc (\mathrm{mod}\ m)$两边消去c。有兴趣的同学可以尝试着去证明一下这个结论。

练习

- 请证明3|n(n+1)(2n+1),n≥0

证明1：

- 基本思路：利用同余式的性质
- 提示：3一定整除n(n+1)(n+2)

证明2：

- 基本思路：数学归纳法

带未知数的同余式

- 如，x+12≡5(mod 8)，要求解出满足上述条件的x
  - 我们可以按照一般的解方程方法处理，如两边同时减去12，得x≡5-12 ≡-7(mod 8)，或者可用等价解x≡1(mod 8)来表示
  - 注意：-7与1对模8是相同的，因为他们的差被8整除
  - 练习：解　4x ≡3(mod 19)

带未知数的同余式

- 如果其他方法失效，存在一个通用方法“穷举法”。要解模m的同余式，可让每个变量试取0,1,2,3,…,m-1。例如

$$x^2+2x-1 \equiv 0 \pmod 7$$

- 可以去试x=0,x=1,…,x=6，这导出两个解

$$x \equiv 2 \pmod 7 \text{ 与 } x \equiv 3 \pmod 7$$

- 注意：我们将$x \equiv 2 \pmod 7$与$x \equiv 9 \pmod 7$看做相同的解，因为他们模7相同，以后提到“求同余式所有解”时，是指求所有不同余的所有解。

带未知数的同余式

- 是否存在无解的同余式？
  - Yes，如 $x^2 \equiv 3 \pmod{10}$
  - 这与存在方程没有实数解的情形类似
- 对于形如$ax \equiv c \pmod m$的同余式如何求解？
  - 例1，$6x \equiv 15 \pmod{514}$
  - 例2，$18x \equiv 8 \pmod{22}$

带未知数的同余式

- 求解形如$ax \equiv c \pmod m$的同余式，就是想需要求整数x使得m整除ax-c，如果能够求得y使得ax-c=my，则数m就能整除ax-c，因此$ax \equiv c \pmod m$当且仅当线性方程ax- my =c有解。
- 令g=gcd(a,m)
  - 观察1：形如ax-my的每个数均为g的倍数，因此如果g不整除c，则ax- my =c没有解，从而$ax \equiv c \pmod m$也没有解

带未知数的同余式

- 假设g整除c，由前面线性方程定理可知au+mv=g总有解，设其解为$u=u_0$，$v=v_0$，由于g整除c，所以可用整数c/g乘以方程得

$$a\frac{cu_0}{g}+m\frac{cv_0}{g}=c$$

- 这说明 $x_0 \equiv \frac{cu_0}{g} \pmod m$ 是同余式

$ax \equiv c \pmod m$的解

这只是一个解，其余的解？

带未知数的同余式

- 假设x_1是$ax \equiv c(\text{mod } m)$的其他解，则$ax_1 \equiv ax_0(\text{mod } m)$，所以m整除$ax_1 - ax_2$，这说明下式成立

$$\frac{m}{g} \quad \text{整除} \quad \frac{a(x_1 - x_0)}{g}$$

- 我们已知m/g与a/g没有公因数，从而m/g必整除x_1-x_0，换句话说存在整数k使得

$$x_1 = x_0 + k \cdot \frac{m}{g}$$

- 由m的倍数得到的任何两个不同解被认为是相同的，所以恰好有g个不同的解，这些解通过k=0,1,…,g-1而得到

线性同余式定理

- 定理：设a，c与m是整数，m≥1，且g=gcd(a,m)。
  - (a)如果g†c，则同余式$ax \equiv c(\text{mod } m)$没有解
  - (b)如果g|c，则同余式$ax \equiv c(\text{mod } m)$恰好有g个不同解，要求这些解，首先求方程au+mv=g的一个解(u_0,v_0)，则$x_0=c*u_0/g$是$ax \equiv c(\text{mod } m)$的解，不同解的完全集由下式给出

$$x_1 = x_0 + k \cdot \frac{m}{g}, \qquad k = 0,1,\ldots,g-1$$

练习

- 试求下列同余式的解
  - $943x \equiv 381 \pmod{2576}$
    - 已知gcd(943,2576)=23
  - $893x \equiv 266 \pmod{2432}$
    - 已知gcd(893,2432)=19

费马小定理

- 幂模
  - 所谓幂模就是形如 $a^k \pmod{m}$ 的模，其中a和k均为整数
- 问题
  - 考察这些幂中存在什么模式？
- 先考察m=p的情形，其中p是素数
  - 因为这时容易识别出模式

费马小定理

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2	4	1	2	4	1	2	4
3	2	6	4	5	1	3	2
4	2	1	4	2	1	4	2
5	4	6	2	3	1	5	4
6	1	6	1	6	1	6	1

$a^k \pmod 7$

a	a^2	a^3	a^4	a^5	a^6
0	0	0	0	0	0
1	1	1	1	1	1
2	4	3	1	2	4
3	4	2	1	3	4
4	1	4	1	4	1

$a^k \pmod 5$

a	a^2	a^3	a^4
0	0	0	0
1	1	1	1
2	1	2	1

$a^k \pmod 3$

费马小定理

- 观察$a^2 \pmod 3$， $a^4 \pmod 5$和$a^6 \pmod 7$三列
  - 除去顶端的1个0，这些列中的每一项都是1，这是普遍规律，还是一个巧合？
    - $1^{10} \equiv 1 \pmod{11}$, $2^{10} \equiv 1 \pmod{11}$,
    - $3^{10} \equiv 1 \pmod{11}, \ldots, 9^{10} \equiv 1 \pmod{11}$,
    - $10^{10} \equiv 1 \pmod{11}$
  - 猜想：$a^{p-1} \equiv 1 \pmod p$, $1 \leqslant a < p$
    - 当然对a的取值不一定非得如此限制，如果a_1和a_2是p的不同倍数，则其幂对模p相同，所以对a的真正限制实际上是它不是p的倍数
    - 此结果由费马1640年给Bessy的信中首次提出，但没给证明的细节

费马小定理

- 定理4.1 设p是素数，a是任意整数且$a \not\equiv 0 \pmod p$，则 $a^{p-1} \equiv 1 \pmod p$
  - 定理的用途，例如，下列同余式是否正确
    - $6^{22} \equiv 1 \pmod{23}$　　$73^{100} \equiv 1 \pmod{101}$
    - 这个同余式的含义是指$6^{22}-1$是23的倍数，按照正常的思路需要计算出$6^{22}-1$的值，然后再除以23来验证是否被23整除
    - $6^{22}-1=23*5\ 722\ 682\ 775\ 750\ 745$

费马小定理

- 费马小定理的应用(一)
  - 例如，计算$2^{35} \pmod 7 = ?$
  - 我们可以利用$2^6 \equiv 1 \pmod 7$的结论，已知35=6*5+5，可以将上式简化为

    $2^{35}=2^{6*5+5}=(2^6)^5*2^5 \equiv 1^5*2^5 \equiv 32 \equiv 4 \pmod 7$
- 练习
  - 试解同余式$x^{103} \equiv 4 \pmod{11}$

费马小定理

- 解：由费马小定理得$x^{10} \equiv 1 \pmod{11}$，两边自乘10次方的$x^{100} \equiv 1 \pmod{11}$，然后乘以$x^3$得$x^{103} \equiv x^3 \pmod{11}$。要解原同余式，正好需要解$x^3 \equiv 4 \pmod{11}$，通过尝试x=0,x=1,…，x=10，可解这个同余式。

$x \pmod{11}$	0	1	2	3	4	5	6	7	8	9	10
$x^3 \pmod{11}$	0	1	8	5	9	4	7	2	6	3	10

最终解为$x \equiv 5 \pmod{11}$

费马小定理

- 在开始正式证明费马小定理之前，我们先看一个特例 $3^6 \equiv 1 \pmod{7}$
  - 要证明上式很简单，因为$3^6-1=728=7*104$，但这不是我们的目的，我们的目的在于能够找到一个证明思路
  - 看另外一种证明思路，我们由数1,2,3,4,5,6分别乘以3开始模7化简，得

$x \pmod{7}$	1	2	3	4	5	6
$3x \pmod{7}$	3	6	2	5	1	4

费马小定理

- 观察的结论
  - 在第二行中1,2,3,4,5,6几个数字各出现一次，虽然次序与第一行不一致
  - 两行数字乘积模7具有相同的结果

    $(3*1)(3*2)(3*3)(3*4)(3*5)(3*6) \equiv 1*2*3*4*5*6 (\mathrm{mod}\ 7)$
  - 将上式左端提出6个因数3得

    $3^6*6! \equiv 6! (\mathrm{mod}\ 7)$
  - 注意6!与7互素（为什么？），所以可以消去6!，得$3^6 \equiv 1 (\mathrm{mod}\ 7)$

费马小定理

- 猜想：设p是素数，a是任意整数且$a \not\equiv 0 (\mathrm{mod}\ p)$，则数

  $a,2a,3a,\ldots,(p-1)a \pmod p$ 与数

  $1,2,3,\ldots,(p-1) \pmod p$ 相同，尽管它们的次序不同
- 证明：$a,2a,3a,\ldots,(p-1)a$这p-1个数显然没有一个被p整除(如果这些数模p的值都不一样，就说明这p-1数恰为1,2,3,…, p-1这p-1个数)，假设从这个数列中取两个数ja和ka，并假设它们模p同余，即$ja \equiv ka (\mathrm{mod}\ p)$，则有p|(j-k)a，因为假设p不整除a，所以p|(j-k)，这是用素数整除性定理。已知$1 \leqslant j,k \leqslant p-1$，则$|j-k|<p-1$，那么只有在j-k=0的情况下才能让p|(j-k)成立，从而j=k，这表明a,2a,3a,…,(p-1)a中的不同乘积对模p不同。

费马小定理

- 费马小定理证明：

由上面的断言可知数列a,2a,3a,…,(p-1)a (mod p)与数列1,2,3,…,(p-1)(mod p)相同，所以第一个数列的乘积等于第二个数列中数的乘积：

$a*2a*3a*,\ldots,*(p-1)a \equiv 1*2*3*,\ldots,*(p-1) \pmod p$

左边可以提出p-1个a得

$$a^{p-1}*(p-1)! \equiv (p-1)! \pmod p$$

由于(p-1)!与p互素，因此两边可消去(p-1)!，得

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

费马小定理

- 费马小定理的应用(二)
  - 判断一个数是否是素数，例如已知

$$2^{1234566} \equiv 899\ 557 \pmod{1234567}$$

  - 则这意味着1234567这个数一定不是素数，实事上1234567=127*9721