第八章 模p平方剩余

张志强

智能信息处理研究中心

http://rciip.hrbeu.edu.cn

模p与原根

- 费马小定理告诉我们，如果a与p互素，则有$a^{p-1}\equiv 1(\mathrm{mod}\ p)$
  - 事实上不只有a的p-1幂与1模p同余，还存在其他的幂次与1模p同余，例如$2^3\equiv 1(\mathrm{mod}\ 7)$
  - 那么对于给定的a，最小的与1模p同余的幂次是多少呢？
- 我们称这种最小的指数为a模p的次数(或阶)，$e_p(a)=$(使得$a^e\equiv 1(\mathrm{mod}\ p)$的最小指数$e\geqslant 1$)
- 例，找出2模7的次数(阶)
  - 计算2的各次幂对模7的最小正剩余，$2^1\equiv 2(\mathrm{mod}\ 7)$，$2^2\equiv 4(\mathrm{mod}\ 7)$，$2^3\equiv 1(\mathrm{mod}\ 7)$，则有$e_7(2)=3$
- 由费马小定理可知$e_p(a)\leqslant p-1$

模p与原根

p=5
$1^1 \equiv 1 \pmod 5$
$2^4 \equiv 1 \pmod 5$
$3^4 \equiv 1 \pmod 5$
$4^2 \equiv 1 \pmod 5$

p=7
$1^1 \equiv 1 \pmod 7$
$2^3 \equiv 1 \pmod 7$
$3^6 \equiv 1 \pmod 7$
$4^3 \equiv 1 \pmod 7$
$5^6 \equiv 1 \pmod 7$
$6^2 \equiv 1 \pmod 7$

p=11
$1^1 \equiv 1 \pmod{11}$
$2^{10} \equiv 1 \pmod{11}$
$3^5 \equiv 1 \pmod{11}$
$4^5 \equiv 1 \pmod{11}$
$5^5 \equiv 1 \pmod{11}$
$6^{10} \equiv 1 \pmod{11}$
$7^{10} \equiv 1 \pmod{11}$
$8^{10} \equiv 1 \pmod{11}$
$9^5 \equiv 1 \pmod{11}$
$10^2 \equiv 1 \pmod{11}$

- 两个观察
  - 使得$a^e \equiv 1 \pmod p$的最小指数e整除p-1
  - 总有一些a需要指数p-1

次数整除性质

- 定理(次数整除性质)：设a是不被素数p整除的整数，假设$a^n \equiv 1 \pmod p$，则次数$e_p(a)$整除n。特别地，次数$e_p(a)$总整除p-1

证明1：设$G=\gcd(e_p(a),n)$，并设(u,v)是方程$e_p(a)u-nv=G$的正整数解，则有

$$a^{ep(a)u}=(a^{ep(a)})^u \equiv 1^u \equiv 1 \pmod p$$

$$a^{ep(a)u}=a^{nv+G}=(a^{nv})*a^G \equiv 1^v*a^G \equiv a^G \pmod p$$

这表明$a^G \equiv 1 \pmod p$，但是$e_p(a)$是与1模p同余的最小幂次，所以有$G \geqslant e_p(a)$。另一方面，$G=\gcd(e_p(a),n)$，所以G整除$e_p(a)$与n，即$G \leqslant e_p(a)$，因此有$G= e_p(a)$，这就证明了$e_p(a)$整除n。

最后由费马小定理可知$a^{p-1} \equiv 1 \pmod p$，取n=p-1即可得定理结论

次数整除性质

- 例如，请确定x=10和x=15是否是方程$2^x \equiv 1 (\mathrm{mod}\ 7)$的解？
- 解：由于已知$e_7(2)=3$，因为3不整除10，但3整除15，由定理可知x=10不是解，x=15是解

模p原根

- 对那些$e_p(a)=p-1$的数a来说$a,a^2,a^3,\ldots,a^{p-1}(\mathrm{mod}\ p)$必须都是模p不同的，为什么？
  - 反证：否则存在$1\leqslant i<j\leqslant p-1$，使得$a^i\equiv a^j(\mathrm{mod}\ p)$，而这意味着$a^{j-i}\equiv 1(\mathrm{mod}\ p)$，其中指数j-i小于p-1，这与已知$e_p(a)=p-1$矛盾。
- 模p原根的定义
  - 具有最高次数$e_p(g)=p-1$的数g称为模p的原根
  - 例如，2与3是模5的原根，3与5是模7的原根

原根定理

- 定理：每个素数p都有原根。更精确地，有恰好 $\phi(p-1)$ 个模p的原根
  - 例如，素数11具有 $\phi(10)=4$ 个原根，其原根分别为2,6,7,8
  - 定理没有给出如何求这些原根的方法，一个通用的方法就是逐个检查a=2,a=3,…,直到 $e_p(a)=p-1$ 的a的值。

求原根的样例

- 例，请求出11的所有原根(作业)
- 解：首先由定理知，11有 $\phi(11-1)=4$ 个原根。下面需要依次求出a=2,3,…,10模p的阶。如何求阶？根据次数整除定理，$e_p(a)|p-1$，即$e_p(a)$只可能是(p-1)的因数，因此只需查看如下的正数剩余是否为1，其中1,2,5,10是10的因数
  - $a^1 \pmod{11}$, $a^2 \pmod{11}$, $a^5 \pmod{11}$, $a^{10} \pmod{11}$
  - 当只有$a^{10} \pmod{11}=1$时，a才是原根
  - 经过计算后得到a=2,6,7,8是11的原根

原根与指标

- 模素数p的原根g有个很漂亮的体现，就是每个模p的非零数都是以g的幂次出现的，因此对于任意的数$1 \leqslant a < p$，我们可以选择幂$g, g^2, g^3, \ldots, g^{p-1}$中恰好一个与a模p同余，相应的指数被称为以g为底的a模p的指标，假设a与p已给定，则记为l(a)
- 例1，如果使用模13的原根2为底，则因为$2^4 = 16 \equiv 3 \pmod{13}$，所以l(3)=4
- 例2，$2^9 = 512 \equiv 5 \pmod{13}$，因此l(5)=9

原根与指标

- 为求任何特定数的指标，例如a=7，只需计算幂$2,2^2,2^3,\ldots(\mathrm{mod}\ 13)$直至得到与7同余的数。
- 还有一种方法就是制作2模13的所有幂的表格

I	1	2	3	4	5	6	7	8	9	10	11	12
$2^I \pmod{13}$	2	4	8	3	6	12	11	9	5	10	7	1

a	1	2	3	4	5	6	7	8	9	10	11	12
I(a)	12	1	4	2	9	5	11	3	8	10	7	6

指标法则

- 定理：指标满足下述法则：

  (1).$I(ab) \equiv I(a)+I(b) \pmod{p-1}$ [乘积法则]

  (2).$I(a^k) \equiv kI(a) \pmod{p-1}$ [幂法则]

- 证明(1)：设g是原根，由指标的定义有 $g^{I(ab)} \equiv ab \equiv g^{I(a)} g^{I(b)} \equiv g^{I(a)+I(b)} \pmod{p}$，这意味着$g^{I(ab)-I(a)-I(b)} \equiv 1 \pmod{p}$，由于g是原根，因此有I(ab)-I(a)-I(b)一定是p-1的倍数，(1)证毕。

- 证明(2)：练习

简要回顾

- 第4章介绍过线性同余式$ax \equiv c \pmod{m}$
  - 令g=gcd(a,m)，如果g不整除c，无解
  - 如果g整除c，则有g个解

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

  - 其中x_0是au+mv=g的解， k=0,1,…,g-1

二次同余式方程

- 在实际中，我们还需要解答如下的一些问题：
  - 3是否与某个数的平方模7同余？
  - 同余式$x^2 \equiv -1 \pmod{13}$是否有解？
  - 对哪些素数p，同余式$x^2 \equiv 2 \pmod{p}$有解？

- 前2个问题可以很容易作答
  - 分别计算0~6的平方，再模7，检验是否余3

二次同余式方程

$0^2 \equiv 0 \pmod 7$

$1^2 \equiv 1 \pmod 7$

$2^2 \equiv 4 \pmod 7$

$3^2 \equiv 2 \pmod 7$

$4^2 \equiv 2 \pmod 7$

$5^2 \equiv 4 \pmod 7$

$6^2 \equiv 1 \pmod 7$

$0^2 \equiv 0 \pmod{13}$

$1^2 \equiv 1 \pmod{13}$

$2^2 \equiv 4 \pmod{13}$

$3^2 \equiv 9 \pmod{13}$

$4^2 \equiv 3 \pmod{13}$

$5^2 \equiv 12 \pmod{13}$

$6^2 \equiv 10 \pmod{13}$

$7^2 \equiv 10 \pmod{13}$

$8^2 \equiv 12 \pmod{13}$

$9^2 \equiv 3 \pmod{13}$

$10^2 \equiv 9 \pmod{13}$

$11^2 \equiv 4 \pmod{13}$

$12^2 \equiv 1 \pmod{13}$

二次同余式方程

b	b^2
0	0
1	1
2	4
3	4
4	1

模5

b	b^2
0	0
1	1
2	4
5	4
6	1

模7

b	b^2
0	0
1	1
2	4
3	9
4	5
5	3
6	3
7	5
8	9
9	4
10	1

模11

b	b^2
0	0
1	1
2	4
3	9
4	3
5	12
6	10
7	10
8	12
9	3
10	9
11	4
12	1

模13

二次同余式方程

- 可能观察到的一些结论
  - 除了0，这个表是对称的
  - 每个平方剩余都出现两次
- 如何用公式来表示这个模式呢？
  - 数b的平方剩余与数p-b的平方剩余是模p相同的，即$b^2 \equiv (p-b)^2 \pmod p$
  - Proof: $(p-b)^2=p^2-2pb+b^2 \equiv b^2 \pmod p$
  - 如果列出模p的所有（非零）平方剩余，只需计算出其中的一半即可
  - $1^2 \pmod p$, $2^2 \pmod p$, $3^2 \pmod p$,…,$[(p-1)/2]^2 \pmod p$

几个基本概念

- 与一个平方数模p同余的非零数称为模p的二次剩余，简记为QR
- 不与任何一个平方数模p同余的数，称为模p的(二次)非剩余，简记为NR
- 与0模p同余的数既不是二次剩余，也不是二次非剩余

几个基本概念

b	b^2
0	0
1	1
2	4
3	9
4	3
5	12
6	10
7	10
8	12
9	3
10	9
11	4
12	1

模13

- 判断下列说法是否正确
  - 3和12是模13的QR 
  - 2和5是模13的NR 
  - 7和8是模13的QR 
- 模13的QR集合是{1,3,4,9,10,12}，NR集合是{2,5,6,7,8,11}
- 模7的QR是{1,2,4}，NR是{3,5,6}
- 有什么发现？

模p平方剩余

- 定理：设p是一个奇素数，则恰有(p-1)/2个模p的二次剩余，且恰有(p-1)/2个模p的二次非剩余。

证明：二次剩余是非零数，它们是模p平方剩余，因此他们是这些数$1^2,2^2,\ldots,(p-1)^2(\mathrm{mod}\ p)$，前面我们讲过，只需计算到一半，$1^2,2^2,\ldots,[(p-1)/2]^2(\mathrm{mod}\ p)$，因为剩下的平方剩余$[(p+1)/2]^2,\ldots,(p-1)^2\ (\mathrm{mod}\ p)$，则会出现与前面颠倒的数。因此，要证明恰好有(p-1)/2个二次剩余，只需验证$1^2,2^2,\ldots,[(p-1)/2]^2$模p是两两不同的。

假设b_1和b_2都是1到(p-1)/2之间的数，且满足$b_1^2\equiv b_2^2(\mathrm{mod}\ p)$，则有$p|(b_1^2-b_2^2)=(b_1-b_2)(b_1+b_2)$。由于$(b_1+b_2)$是2到(p-1)之间的数，因此不可能被p整除，故p一定整除(b_1-b_2)，但是$|b_1-b_2|<(p-1)/2$，所以只有$b_1-b_2=0$，即$b_1=b_2$。

模p平方剩余

- 问题1：假设取两个二次剩余并对它们作乘积，那么结果是一个QR还是一个NR，或是有时是QR有时是NR？
  - 3和10是模13的QR，它们的乘积$30 \equiv 4 \pmod{13}$，也是模13的QR，因为$2^2 \equiv 4 \pmod{13}$
  - 事实上，两个平方数的乘积还是一个平方数，如果a_1和a_2都是模p的QR，则意味着存在b_1和b_2，使得$a_1 \equiv b_1^2 \pmod{p}$，$a_2 \equiv b_2^2 \pmod{p}$，两者相乘得到$a_1 a_2 \equiv b_1^2 b_2^2 \pmod{p}$，说明$a_1 a_2$是一个QR

模p平方剩余

- 问题2：如果一个QR和一个NR做乘积，或是对两个NR作乘积，结果如何？
  - 观察几个实例

QR×NR≡??(mod p)	
2×5≡3(mod 7)	NR
5×6≡8(mod 11)	NR
4×5≡7(mod 13)	NR
10×7≡5(mod 13)	NR

NR×NR≡??(mod p)	
3×5≡1(mod 7)	QR
6×7≡9(mod 11)	QR
5×11≡3(mod 13)	QR
7×11≡12(mod 13)	QR

模p平方剩余

- 猜想：一个二次剩余与一个二次非剩余相乘得到一个二次非剩余；两个二次非剩余的乘积是一个二次剩余
  - 用符号表示如下
    - QR×QR=QR
    - QR×NR=NR
    - NR×NR=QR

模p平方剩余

- 设g是模p的一个原根(原根定理保证了其存在性)那么g的幂:$g,g^2,g^3,g^4,\ldots,g^{p-2},g^{p-1}$给出了模p的所有非零剩余，其中一半是二次剩余，一半是二次非剩余，那么如何确定哪些是二次剩余，哪些是二次非剩余?
- g^2是一个QR，为什么？
  - $g^4,g^6,\ldots$等g的每个偶次幂都是一个QR，恰好有一半是偶次幂，一半是奇次幂。偶次幂是二次剩余，奇次幂是二次非剩余。

二次剩余乘法法则

- 我们用另一种方式来叙述，a模p的指标(对原根g)是满足性质$a \equiv g^{I(a)} \pmod p$的幂I(a)，因此若a与g的偶次幂同余，则a的指标是偶数，若a与g的奇数幂同余，则a的指标是奇数
- 定理(二次剩余乘法法则-版本1)：设p为奇素数，则
  - (i)两个模p的二次剩余的乘积是二次剩余；
  - (ii)二次剩余与二次非剩余的积是二次非剩余；
  - (iii)两个二次非剩余的积是二次剩余；

二次剩余乘法法则

- 证明：对与p互素的任意两个数a,b，由指标的乘法法则知$I(ab)\equiv I(a)+I(b) \pmod{p-1}$，由于p是奇素数，因此p-1是偶数，从而有$I(ab)\equiv I(a)+I(b) \pmod 2$ (为什么？)下面我们分别讨论a和b的不同取值情况：
  - (i)若a与b都是二次剩余，则I(a)和I(b)都是偶数，因此$I(ab) \equiv I(a)+I(b) \equiv 0+0\equiv 0 \pmod 2$

    故I(ab)是偶数，从而ab是二次剩余
  - (ii) 略(练习)
  - (iii) 略(练习)

二次剩余乘法法则

- 请观察如下法则，是否有似曾相识的感觉？
  - QR×QR=QR，QR×NR=NR，NR×NR=QR
- 如果另QR表示+1，NR表示-1，则QR与NR的性质与+1和-1的性质类似
- 勒让德符号
  - a模p的勒让德符号是

$$\left(\frac{a}{p}\right)=\begin{cases}1, & \text{若a是模p的二次剩余}\\ -1, & \text{若a是模p的二次非剩余}\end{cases}$$

$$\left(\frac{3}{13}\right)=1 \qquad \left(\frac{11}{13}\right)=-1 \qquad \left(\frac{2}{7}\right)=1 \qquad \left(\frac{3}{7}\right)=-1$$

二次剩余乘法法则

- 定理(二次乘法法则-版本2)：设p是奇素数，则

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right)$$

- 例如，假定想知道75是不是模97的平方剩余，可以计算

$$\left(\frac{75}{97}\right)=\left(\frac{3*5*5}{97}\right)=\left(\frac{3}{97}\right)\left(\frac{5}{97}\right)\left(\frac{5}{97}\right)=\left(\frac{3}{97}\right)$$

- 由于$10^2\equiv 3 \pmod{97}$，所以3是一个QR，因此

$$\left(\frac{75}{97}\right)=\left(\frac{3}{97}\right)=1$$

作业

- 请判断24是不是模43的平方剩余?