信息安全数学基础

韩　琦

计算机科学与技术学院

Detailed overview

模数的阶

定义

设$m > 0, (a, m) = 1$,称使$a^l \equiv 1 (mod\ m)$成立的最小正整数l为a 对**模数m的阶**，记为$ord_m(a)$,有时在模数m不变时，也简记为$ord(a)$。

阶的性质

1. 如果$a \equiv a' (mod\ m)$，则$ord_m(a) = ord_m(a')$。
2. $a^n \equiv 1 (mod\ m)$的充分必要条件是$ord_m(a) | n$，从而$ord_m(a) | \phi(m)$。
3. 记$ord_m(a) = l$，则$1, a, a^2, \cdots, a^{l-1}$对模数$m$两两不同余。
4. 记$ord_m(a) = l, \lambda > 0, ord_m(a^\lambda) = l_\lambda$，则$l_\lambda = \frac{l}{(\lambda, l)}$，从而$ord_m(a^\lambda) = l$对$\phi(l)$的个数$a^\lambda, (\lambda, l) = 1, 0 < \lambda \leq l$都成立。

模数的阶

定义

设$m > 0, (a, m) = 1$,称使$a^l \equiv 1 (mod\ m)$成立的最小正整数l为a 对**模数m的阶**，记为$ord_m(a)$,有时在模数m不变时，也简记为$ord(a)$。

阶的性质

1. 如果$a \equiv a' (mod\ m)$，则$ord_m(a) = ord_m(a')$。
2. $a^n \equiv 1 (mod\ m)$的充分必要条件是$ord_m(a) | n$，从而$ord_m(a) | \phi(m)$。
3. 记$ord_m(a) = l$，则$1, a, a^2, \cdots, a^{l-1}$对模数$m$两两不同余。
4. 记$ord_m(a) = l, \lambda > 0, ord_m(a^\lambda) = l_\lambda$，则$l_\lambda = \frac{l}{(\lambda, l)}$，从而$ord_m(a^\lambda) = l$对$\phi(l)$的个数$a^\lambda, (\lambda, l) = 1, 0 < \lambda \leq l$都成立。

模数的阶

定义

设$m > 0, (a, m) = 1$,称使$a^l \equiv 1 (mod\ m)$成立的最小正整数l为a 对**模数m的阶**，记为$ord_m(a)$,有时在模数m不变时，也简记为$ord(a)$。

阶的性质

1. 如果$a \equiv a' (mod\ m)$，则$ord_m(a) = ord_m(a')$。
2. $a^n \equiv 1 (mod\ m)$的充分必要条件是$ord_m(a) | n$，从而$ord_m(a) | \phi(m)$。
3. 记$ord_m(a) = l$，则$1, a, a^2, \cdots, a^{l-1}$对模数$m$两两不同余。
4. 记$ord_m(a) = l, \lambda > 0, ord_m(a^\lambda) = l_\lambda$，则$l_\lambda = \frac{l}{(\lambda, l)}$，从而$ord_m(a^\lambda) = l$对$\phi(l)$的个数$a^\lambda, (\lambda, l) = 1, 0 < \lambda \leq l$都成立。

模数的阶

定义

设$m > 0, (a, m) = 1$,称使$a^l \equiv 1 (mod\ m)$成立的最小正整数l为a 对**模数m的阶**，记为$ord_m(a)$,有时在模数m不变时，也简记为$ord(a)$。

阶的性质

1. 如果$a \equiv a' (mod\ m)$，则$ord_m(a) = ord_m(a')$。
2. $a^n \equiv 1 (mod\ m)$的充分必要条件是$ord_m(a) | n$，从而$ord_m(a) | \phi(m)$。
3. 记$ord_m(a) = l$，则$1, a, a^2, \cdots, a^{l-1}$对模数$m$两两不同余。
4. 记$ord_m(a) = l, \lambda > 0, ord_m(a^\lambda) = l_\lambda$，则$l_\lambda = \frac{l}{(\lambda, l)}$，从而$ord_m(a^\lambda) = l$对$\phi(l)$的个数$a^\lambda, (\lambda, l) = 1, 0 < \lambda \leq l$都成立。

模数的阶

定义

设$m > 0, (a, m) = 1$,称使$a^l \equiv 1 (mod\ m)$成立的最小正整数l为a 对**模数m的阶**，记为$ord_m(a)$,有时在模数m不变时，也简记为$ord(a)$。

阶的性质

1. 如果$a \equiv a' (mod\ m)$，则$ord_m(a) = ord_m(a')$。
2. $a^n \equiv 1 (mod\ m)$的充分必要条件是$ord_m(a) | n$，从而$ord_m(a) | \phi(m)$。
3. 记$ord_m(a) = l$，则$1, a, a^2, \cdots, a^{l-1}$对模数$m$两两不同余。
4. 记$ord_m(a) = l, \lambda > 0, ord_m(a^\lambda) = l_\lambda$，则$l_\lambda = \frac{l}{(\lambda, l)}$，从而$ord_m(a^\lambda) = l$对$\phi(l)$的个数$a^\lambda, (\lambda, l) = 1, 0 < \lambda \leq l$都成立。

模数的阶

定义

设$m > 0, (a, m) = 1$,称使$a^l \equiv 1 (mod\ m)$成立的最小正整数l为a 对**模数m的阶**，记为$ord_m(a)$,有时在模数m不变时，也简记为$ord(a)$。

阶的性质

1. 如果$a \equiv a' (mod\ m)$，则$ord_m(a) = ord_m(a')$。
2. $a^n \equiv 1 (mod\ m)$的充分必要条件是$ord_m(a)|n$，从而$ord_m(a)|\phi(m)$。
3. 记$ord_m(a) = l$，则$1, a, a^2, \cdots, a^{l-1}$对模数$m$两两不同余。
4. 记$ord_m(a) = l, \lambda > 0, ord_m(a^\lambda) = l_\lambda$，则$l_\lambda = \frac{l}{(\lambda, l)}$，从而$ord_m(a^\lambda) = l$对$\phi(l)$的个数$a^\lambda, (\lambda, l) = 1, 0 < \lambda \leq l$都成立。

原根及其存在性

定义（原根）

设整数$m > 0,(g,m) = 1$,如果$ord_m(g) = \phi(m)$,则称g为模数m的一个原根。

定理

设$m > 0,(g,m) = 1$,则g为(模数)m的一个原根的充分必要条件是$g, g^2, \cdots, g^{\phi(m)}$为模数$m$的一组既约剩余系。

定理

设p是一个奇素数,则模p有一个原根。

定理

整数m有原根的充分必要条件是$m = 2, 4, p^a, 2p^a (a \geq 1, p$为奇素数)。

原根及其存在性

定义（原根）

设整数$m > 0, (g, m) = 1$,如果$ord_m(g) = \phi(m)$,则称g为模数m的**一个原根**。

定理

设$m > 0, (g, m) = 1$,则g为(模数)m的一个原根的充分必要条件是$g, g^2, \cdots, g^{\phi(m)}$为模数$m$的一组既约剩余系。

定理

设p是一个奇素数,则模p有一个原根。

定理

整数m有原根的充分必要条件是$m = 2, 4, p^a, 2p^a (a \geq 1, p$为奇素数$)$。

原根及其存在性

定义（原根）

设整数$m > 0, (g, m) = 1$,如果$ord_m(g) = \phi(m)$,则称g为模数m的**一个原根**。

定理

设$m > 0, (g, m) = 1$,则g为(模数)m的一个原根的充分必要条件是$g, g^2, \cdots, g^{\phi(m)}$为模数$m$的一组既约剩余系。

定理

设p是一个奇素数,则模p有一个原根。

定理

整数m有原根的充分必要条件是$m = 2, 4, p^a, 2p^a (a \geq 1, p$为奇素数)。

原根及其存在性

定义（原根）

设整数$m > 0, (g, m) = 1$,如果$ord_m(g) = \phi(m)$,则称g为模数m的**一个原根**。

定理

设$m > 0, (g, m) = 1$,则g为(模数)m的一个原根的充分必要条件是$g, g^2, \cdots, g^{\phi(m)}$为模数$m$的一组既约剩余系。

定理

设p是一个奇素数,则模p有一个原根。

定理

整数m有原根的充分必要条件是$m = 2, 4, p^a, 2p^a (a \geq 1, p$为奇素数)。

阶的计算方法

设整数a满足$(a,m)=1, m>0$，因为$ord_m(a)|\phi(m)$，故$ord_m(a)$可通过依次计算$a_{d_1}, a_{d_2}, \cdots, a_{d_s}$模$m$的余数是否等于1求出，这里$1=d_1<d_2<\cdots<d_s=\phi(m)$是$\phi(m)$的所有正因数。

定理

设$m=\prod_{i=1}^{s} p_i^{l_i}$为标准分解式，记$ord_{p_i^{l_i}}(a)=f_i(i=1,2,\cdots,s)$，$ord_m(a)=f$，则$f$等于$f_1, f_2, \cdots, f_s$的最小公倍数：$f=[f_1, f_2, \cdots, f_s]$.

阶的计算方法

设整数a满足$(a,m)=1, m>0$，因为$ord_m(a)|\phi(m)$，故$ord_m(a)$可通过依次计算$a_{d_1}, a_{d_2}, \cdots, a_{d_s}$模$m$的余数是否等于1求出，这里$1=d_1<d_2<\cdots<d_s=\phi(m)$是$\phi(m)$的所有正因数。

定理

设$m=\prod_{i=1}^{s} p_i^{l_i}$为标准分解式，记$ord_{p_i^{l_i}}(a)=f_i(i=1,2,\cdots,s)$，$ord_m(a)=f$，则$f$等于$f_1, f_2, \cdots, f_s$的最小公倍数：$f=[f_1, f_2, \cdots, f_s]$.

定理

设p是一个素数,$a \neq \pm 1, (a,p) = 1, ord_{p^j}(a) = f_j$，则$f_{j+1} = f_j$或者$f_{j+1} = pf_j$。进一步，

1. 当$p \neq 2$时，又设$p^i || a^{f_2} - 1$（即$p^i | a^{f_2} - 1$但$p^{i+1} \nmid a_{f_2} - 1$），则

$$有 f_j = \begin{cases} f_2, & 2 \leq j \leq i \\ p^{j-i} f_2, & j > i \end{cases}$$

2. 当$p = 2$时，又设$a = 2^r a_1 + 1, 2 \nmid a_1, r \geq 2$，则

$$有 f_j = \begin{cases} 1, & 1 \leq j \leq r \\ 2, & j = r+1 \\ 2^{j-r}, & j > r+1 \end{cases}$$

。设$a = 2^r a_1 - 1, 2 \nmid a_1, r \geq 2$，则

$$有 f_j = \begin{cases} 1, & j = 1 \\ 2, & 2 \leq j \leq r+1 \\ 2^{j-r}, & j > r+1 \end{cases}$$

例

设$m = 648, a = 343$，计算$ord_m(a)$。

解 $m = 648 = 2^3 \times 3^4, a = 343 = 7^3$，由$7 = 2^3 - 1$根据定理5-5的(2)得$ord_{2^3}(7) = 2$；

由$7 \not\equiv 1(mod\ 3^2), 7^2 \equiv 4 \not\equiv 1(mod\ 3^2), 7^3 \equiv 1(mod\ 3^2)$，根据阶的定义得$ord_{3^2}(7) = 3$，再由$7^3 - 1 = 342 = 3^2 \times 2 \times 19$，根据定理5-5的(1)及$i = 2$得$ord_{3^4}(7) = 3^{4-2} \times 3 = 3^3$；根据定理5-4得$ord_{2^3 \times 3^4}(7) = [2, 3^3]$；最后根据阶的性质(4)得$ord_m(a) = \frac{2 \times 3^3}{(3, 2 \times 3^3)} = 2 \times 3^2 = 18$

原根的计算方法

定理

设奇素数p满足如下标准素因子分解$p-1=\prod_{i=0}^{s} p_i^{a_i}, 2=p_0<p_1<\cdots<p_s$。又设整数$a$满足如下条件$(a,p)=1, a^{\frac{p-1}{p_i}} \not\equiv 1(mod\ p), i=0,1,\cdots,s$，则$a$为$p$的原根。

例 (求素数$p=47$的一个原根)

解 对$p=47$，有标准素因子分解$47-1=46=2\times 23$。

1. 取整数$a=2,(2,47)=1, 2^{23}\equiv 1(mod\ 47)$，失败。
2. 取整数$a=3,(3,47)=1, 3^{23}\equiv 1(mod\ 47)$，失败。
3. 取整数$a=5,(5,47)=1, 5^{23}\equiv -1\not\equiv 1(mod\ 47)$，
   $5^2=25\not\equiv 1(mod\ 47)$，根据定理5-7知$a=5$是$p=47$的一个原根。

原根的计算方法

定理

设奇素数p满足如下标准素因子分解$p-1=\prod_{i=0}^{s} p_i^{a_i}, 2=p_0<p_1<\cdots<p_s$。又设整数$a$满足如下条件$(a,p)=1, a^{\frac{p-1}{p_i}} \not\equiv 1(mod\ p), i=0,1,\cdots,s$，则$a$为$p$的原根。

例 (求素数$p=47$的一个原根)

解 对$p=47$，有标准素因子分解$47-1=46=2\times 23$。

1. 取整数$a=2,(2,47)=1, 2^{23}\equiv 1(mod\ 47)$，失败。
2. 取整数$a=3,(3,47)=1, 3^{23}\equiv 1(mod\ 47)$，失败。
3. 取整数$a=5,(5,47)=1, 5^{23}\equiv -1\not\equiv 1(mod\ 47)$，
   $5^2=25\not\equiv 1(mod\ 47)$，根据定理5-7知$a=5$是$p=47$的一个原根。

原根的计算方法

定理

设奇素数p满足如下标准素因子分解$p-1=\prod_{i=0}^{s} p_i^{a_i}, 2=p_0<p_1<\cdots<p_s$。又设整数$a$满足如下条件$(a,p)=1, a^{\frac{p-1}{p_i}} \not\equiv 1(mod\ p), i=0,1,\cdots,s$，则$a$为$p$的原根。

例 (求素数$p=47$的一个原根)

解 对$p=47$，有标准素因子分解$47-1=46=2\times 23$。

1. 取整数$a=2,(2,47)=1, 2^{23}\equiv 1(mod\ 47)$，失败。
2. 取整数$a=3,(3,47)=1, 3^{23}\equiv 1(mod\ 47)$，失败。
3. 取整数$a=5,(5,47)=1, 5^{23}\equiv -1\not\equiv 1(mod\ 47)$，
   $5^2=25\not\equiv 1(mod\ 47)$，根据定理5-7知$a=5$是$p=47$的一个原根。

素数的简单判别法–整除判别法

定理

设正整数$p > 1$，如果对于所有的正整数$q, 1 < q \leq \sqrt{p}$，都有$q \nmid p$，则p为素数。

例 (用整除判别法证明$p = 97$是一个素数)

证明：由$\sqrt{p} = \sqrt{97} < \sqrt{100} = 10$及小于10的素数2,3,5,7都不能整除$p = 97 : p = 97 = 2 \times 48 + 1 = 3 \times 32 + 1 = 5 \times 19 + 2 = 7 \times 13 + 6$，由整除判别法就得到$p = 97$是一个素数。

素数的简单判别法–整除判别法

定理

设正整数$p > 1$，如果对于所有的正整数$q, 1 < q \leq \sqrt{p}$，都有$q \nmid p$，则p为素数。

例 (用整除判别法证明$p = 97$是一个素数)

证明：由$\sqrt{p} = \sqrt{97} < \sqrt{100} = 10$及小于10的素数2,3,5,7都不能整除$p = 97 : p = 97 = 2 \times 48 + 1 = 3 \times 32 + 1 = 5 \times 19 + 2 = 7 \times 13 + 6$，由整除判别法就得到$p = 97$是一个素数。

素数的简单判别法–整除判别法

定理

设正整数$p > 1$，如果对于所有的正整数$q, 1 < q \leq \sqrt{p}$，都有$q \nmid p$，则p为素数。

例 (用整除判别法证明$p = 97$是一个素数)

证明： 由$\sqrt{p} = \sqrt{97} < \sqrt{100} = 10$及小于10的素数2,3,5,7都不能整除$p = 97 : p = 97 = 2 \times 48 + 1 = 3 \times 32 + 1 = 5 \times 19 + 2 = 7 \times 13 + 6$，由整除判别法就得到$p = 97$是一个素数。

素数的简单判别法–威尔逊判别法

定理

设p是大于1的正整数，则p是一个素数的充分必要条件是$(p-1)! \equiv -1(mod\ p)$。

例 (用威尔逊判别法证明$p = 23$是一个素数)

证明：$(p-1)! = (23-1)! = 22! \equiv -1(mod\ 23)$，故23是一个素数。

素数的简单判别法–威尔逊判别法

定理

设p是大于1的正整数，则p是一个素数的充分必要条件是$(p-1)! \equiv -1(mod\ p)$。

例 (用威尔逊判别法证明$p = 23$是一个素数)

证明：$(p-1)! = (23-1)! = 22! \equiv -1(mod\ 23)$，故23是一个素数。

素数的简单判别法–威尔逊判别法

定理

设p是大于1的正整数，则p是一个素数的充分必要条件是$(p-1)! \equiv -1(mod\ p)$。

例 (用威尔逊判别法证明$p = 23$是一个素数)

证明：$(p-1)! = (23-1)! = 22! \equiv -1(mod\ 23)$，故23是一个素数。

素数的确定判别法1

定理（莱梅，D.H.Lehmer)

设正奇数$p>1, p-1=\prod_{i=1}^{s} p_i^{a_i}, 2=p_1<p_2<\cdots<p_s$，$p_i(i=1,\cdots,s)$为素数。如果对每个$p_i$，都有$a_i$，满足$a_i^{\frac{p-1}{p_i}} \not\equiv 1(mod\ p)$和$a_i^{p-1} \equiv 1(mod\ p), i=1,\cdots,s$，则$p$为素数。

例 (用莱梅判别法证明$p=37$是一个素数)

证明：$p-1=37-1=36=2^2\times 3^2$,

取$a_1=2, a_1^{37-1}\equiv 1(mod\ 37), a_1^{\frac{37-1}{2}} \equiv -1 \not\equiv 1(mod\ 37)$,

取$a_2=3, a_2^{37-1}\equiv 1(mod\ 37), a_2^{\frac{37-1}{3}} \equiv -1 \not\equiv 1(mod\ 37)$，由莱梅判别法就得到$p=37$是一个素数。

素数的确定判别法1

定理（莱梅，D.H.Lehmer)

设正奇数$p>1, p-1=\prod_{i=1}^{s} p_i^{a_i}, 2=p_1<p_2<\cdots<p_s$，
$p_i(i=1,\cdots,s)$为素数。如果对每个p_i，都有a_i，满
足$a_i^{\frac{p-1}{p_i}} \not\equiv 1(mod\ p)$和$a_i^{p-1} \equiv 1(mod\ p), i=1,\cdots,s$，则$p$为素数。

例 (用莱梅判别法证明$p=37$是一个素数)

证明：$p-1=37-1=36=2^2\times 3^2$,
取$a_1=2, a_1^{37-1}\equiv 1(mod\ 37), a_1^{\frac{37-1}{2}} \equiv -1 \not\equiv 1(mod\ 37)$,
取$a_2=3, a_2^{37-1}\equiv 1(mod\ 37), a_2^{\frac{37-1}{3}} \equiv -1 \not\equiv 1(mod\ 37)$，由莱梅判别法
就得到$p=37$是一个素数。

素数的确定判别法1

定理（莱梅，D.H.Lehmer)

设正奇数$p>1, p-1=\prod_{i=1}^{s} p_i^{a_i}, 2=p_1<p_2<\cdots<p_s$，$p_i(i=1,\cdots,s)$为素数。如果对每个$p_i$，都有$a_i$，满足$a_i^{\frac{p-1}{p_i}} \not\equiv 1(mod\ p)$和$a_i^{p-1} \equiv 1(mod\ p), i=1,\cdots,s$，则$p$为素数。

例 (用莱梅判别法证明$p=37$是一个素数)

证明： $p-1=37-1=36=2^2\times 3^2$，

取$a_1=2, a_1^{37-1} \equiv 1(mod\ 37), a_1^{\frac{37-1}{2}} \equiv -1 \not\equiv 1(mod\ 37)$，

取$a_2=3, a_2^{37-1} \equiv 1(mod\ 37), a_2^{\frac{37-1}{3}} \equiv -1 \not\equiv 1(mod\ 37)$，由莱梅判别法就得到$p=37$是一个素数。

素数的确定判别法2

定理（普罗兹，Proth）

设正奇数$p > 1, p - 1 = mq$，其中q是一个奇素数且满足$2q + 1 > \sqrt{p}$(即$m < 4(q + 1)$)。如果有a满足条件$a^{p-1} \equiv 1(mod\ p)$和$a^m \not\equiv 1(mod\ p)$，则p为素数。

例 (用普罗兹判别法证明$p = 31$是一个素数)

证明：$p = 31 = 6 \times 5 + 1, q = 5$是一个奇素数，且$2q + 1 = 2 \times 5 + 1 = 11 > \sqrt{31}$，又有$a = 3$满足$a^{31-1} = a^6 \equiv 16 \not\equiv 1(mod\ 31)$，由普罗兹判别法就得到$p = 31$是一个素数。

素数的确定判别法2

定理（普罗兹，Proth）

设正奇数$p > 1, p - 1 = mq$，其中q是一个奇素数且满足$2q + 1 > \sqrt{p}$(即$m < 4(q + 1)$)。如果有a满足条件$a^{p-1} \equiv 1 (mod\ p)$和$a^m \not\equiv 1 (mod\ p)$，则$p$为素数。

例 (用普罗兹判别法证明$p = 31$是一个素数)

证明：$p = 31 = 6 \times 5 + 1, q = 5$是一个奇素数，且$2q + 1 = 2 \times 5 + 1 = 11 > \sqrt{31}$，又有$a = 3$满足$a^{31-1} = a^6 \equiv 16 \not\equiv 1 (mod\ 31)$，由普罗兹判别法就得到$p = 31$是一个素数。

素数的确定判别法2

定理（普罗兹，Proth）

设正奇数$p > 1, p - 1 = mq$，其中q是一个奇素数且满足$2q + 1 > \sqrt{p}$(即$m < 4(q + 1)$)。如果有a满足条件$a^{p-1} \equiv 1(mod\ p)$和$a^m \not\equiv 1(mod\ p)$，则p为素数。

例 (用普罗兹判别法证明$p = 31$是一个素数)

证明： $p = 31 = 6 \times 5 + 1, q = 5$是一个奇素数，且$2q + 1 = 2 \times 5 + 1 = 11 > \sqrt{31}$，又有$a = 3$满足$a^{31-1} = a^6 \equiv 16 \not\equiv 1(mod\ 31)$，由普罗兹判别法就得到$p = 31$是一个素数。

作业

1. 计算下列整数的阶$ord_m(a)$：
   1. $m = 123,\ a = 13$
   2. $m = 2^7 \times 3^4 \times 7^2,\ a = 13$
   3. $m = 2^5 \times 7^4,\ a = 3^4$
2. 计算下列素数的一个原根： 41， 61， 97
3. 判断下列整数是否为素数：
   1. 67
   2. $73 = 2^3 \times 3^2 + 1$
   3. $2543 = 62 \times 41 + 1$

编程作业

实现一种素性判断的方法，并比赛从1开始寻找素数(限时一分钟，同样平台上运行)。

谢谢！

hanqi_xf@hit.edu.cn