信息安全数学基础4－群、本原元(原根)和离散对数(指数)
（《数论讲义》第五章）

杨礼珍

同济大学计算机科学与技术系, 2018

Outline

作业：
阅读：

- 《数论讲义》第五章1、2、3、4、6节
- 《密码学原理与实践》5.2.3节
- 《抽象代数基础教程》2.3群P.89-91,P94的定理2.49，P.95-96。

《数论讲义》第五章作业1、2、5、8、21(3题)、22(1题).
本章主要研究群的元素的阶，特别是群$(\mathbb{Z}_m^*, \cdot)$的元素的阶。
本章内容是《密码学原理与实践》第5章及后面所有章节都涉及到的数学基础。

群
群的定义及基本性质

定义：群$(G,\cdot)$，其中G为元素集合，$\cdot$是定义在G上的二元运算，且满足

封闭性： 对$\forall a,b\in G$有$a\cdot b\in G$

结合律： 对$\forall a,b,c\in G$有$(a\cdot b)\cdot c=a\cdot(b\cdot c)$。

存在单位元： $\exists e\in G$，使得对$\forall a\in G$有$e\cdot a=a\cdot e=a$，称e为G的单位元。

所有元素可逆： 对$\forall a\in G$，$\exists b\in G$满足$a\cdot b=b\cdot a=e$，则称b为a的逆元，写为$b=a^{-1}$。

备注：

- $a\cdot b$一般简写为ab。
- 当运算符号表示成$\cdot$时，单位元通常写为1；当运算符号表示成$+$时，单位元通常写为0。
- 如果运算符号可从上下文判断出来，用G表示群。

如果群$(G,\cdot)$满足交换律则称为交换群（或阿贝尔群，当运算符为乘法$\cdot$时，下面称为乘法群）。

交换律： 对$\forall a,b\in G$有$ab=ba$。

如果G为有限集合，则称为有限群。

我们知道的群的例子有：

- $(\mathbb{Z}_m,+)$是有限Abel群。
- $Mat_n(R)$及矩阵加法运算构成Abel群，其中$Mat_n(R)$表示实数域R上的$n\times n$矩阵。
- 一般线性群是$GL(n,R)$及矩阵乘法运算构成的群（不是Abel群），其中$GL(n,R)$表示实数域R上的$n\times n$可逆矩阵。

定理:$(\mathbb{Z}_m^*,\cdot)$是Abel群。

证明:显然$(\mathbb{Z}_m^*,\cdot)$满足封闭性、结合律和交换律，1为单位元。

对$\forall a\in\mathbb{Z}_m^*$，$(a,m)=1$，因此$a$的逆元存在，且由$a^{\phi(m)} \bmod m=1$可知$a^{-1}=a^{\phi(m)-1} \bmod m$。

定理(群的基本性质): 设G是群。

- **(i)** **消去律**成立：如果$xa = xb$或$ax = bx$，则$a = b$。
- **(ii)** **单位元唯一：** e是G中满足对一切$x \in G$有$ex = x = xe$的唯一元素。
- **(iii)** 对每个$x \in G$，其**逆元唯一**：只有一个元素$x' \in G$满足$xx' = e = x'x$。
- **(iV)** 对一切$x \in G$，$(x^{-1})^{-1} = x$。

证明:(i)选取x'满足$x'x = e = xx'$，则

$$a = ea = (x'x)a = x'(xa) = x'(xb) = (x'x)b = eb = b.$$

x在右边时可类似地证明。
(ii)设e_0满足对一切$x \in G, e_0x = x = xe_0$，那么

$$e = e_0e = e_0.$$

(iii)假定$x'' \in G$满足$xx'' = e = x''x$，那么

$$x'' = x''e = x''(xx') = (x''x)x' = ex' = x'.$$

(iV)由定义，$((x)^{-1})^{-1}x^{-1} = e = x^{-1}((x)^{-1})^{-1}$，
而$xx^{-1} = e = x^{-1}x$，根据(iii)，$((x)^{-1})^{-1} = x$。

定义： 称一个表达式$a_1a_2\dots a_n$**不需要加括号**，如果它导出的一切最终乘积都相等，即不论选取怎样的相邻因子相乘，在G中的最终乘积都相等。

例： 如果$abcd$不需要加括号，那么

$$(ab)(cd) = a(bc)d = a(b(cd))$$

定理（广义结合律）: 设G是群，$a_1, a_2, \dots, a_n \in G$，则表达式$a_1a_2\dots a_n$不需要加括号。

证明: 用归纳法。证明过程阅读《抽象代数基础教程》P94的定理2.49。

对矩阵$A, B \in GL(n, R)$，有$(AB)^{-1} = B^{-1}A^{-1}$。一般有：

定理: 设G是群，$a, b \in G$，则

$$(ab)^{-1} = b^{-1}a^{-1}.$$

证明: 根据群的基本性质(iii)，只需证明$(ab)(b^{-1}a^{-1}) = e = (b^{-1}a^{-1})(ab)$。用广义结合律得到

$$(ab)(b^{-1}a^{-1}) = [a(bb^{-1})]a^{-1} = (ae)a^{-1} = aa^{-1} = e.$$

另一等式可类似的证明。

定义： 若G是一个群，$a \in G$，则对$n \geq 1$归纳地定义**幂a^n**：

$$a^1 = a \ \text{和} \ a^{n+1} = aa^n.$$

定义$a^0 = 1$，若n是一个正整数，则定义

$$a^{-n} = (a^{-1})^n.$$

定义：

- **G的阶**定义为G的元素的个数。
- 对$a \in G$，**a的阶(order)**定义为使得$a^m = 1$的最小的正整数m，如果这样的正整数不存在，则称a有**无限阶**。

例: 群$(\mathbb{Z}_m^*, \cdot)$的阶为$\phi(m)$。群$(\mathbb{Z}_4^*, \cdot) = \{1, 3\}$的元素1的阶为1，元素3的阶为2。

备注： 群$(\mathbb{Z}_m^*, \cdot)$中元素a的阶，在《数论讲义》中称为**a对模数m的次数**。

本章主要研究群的元素的阶，特别是群$(\mathbb{Z}_m^*, \cdot)$的元素的阶。

定理（指数律）:设G是一个群，$a, b \in G$，m和n都是整数（不一定是正的）。

(i) $(a^n)^m = a^{nm}$。

(ii) $a^m a^n = a^{m+n}$。

(iii) 若a和b交换(即$ab = ba$)，则$(ab)^n = a^n b^n$。

证明:(i)和(ii)只证明$n, m > 1$时，其他情形留给读者证明。$(a^n)^m$和a^{nm}均来自有nm个因子且每个因子都等于a的表达式。$a^m a^n$和a^{m+n}均来自有$m+n$个因子且每个因子都等于a的表达式。

(iii)当$n \geq 0$时，用归纳法证明。$n = 0, 1$时显然成立。设$n - 1 \geq 1$时成立。由归纳假设、广义结合律和a, b可交换得到

$$\begin{aligned}(ab)^n &= (ab)(ab)^{n-1} = ab(a^{n-1}b^{n-1}) = a(ba^{n-1})b^{n-1} \\ &= a(a^{n-1}b)b^{n-1} = (aa^{n-1})(bb^{n-1}) = a^n b^n\end{aligned}$$

当$n < 0$时，前面已证明$(ab)^{-n} = a^{-n}b^{-n}$。我们有：

$$(a^n b^n)(a^{-n}b^{-n}) = a^n(b^n a^{-n})b^{-n} = a^n(a^{-n}b^n)b^{-n} = (a^n a^{-n})(b^n b^{-n}) = 1$$

因此

$$a^n b^n = (a^{-n}b^{-n})^{-1} = ((ab)^{-n})^{-1} = (ab)^n.$$

我们知道，对群$(\mathbb{Z}_m^*, \cdot)$中任意元素a有$1 \equiv a^{\phi(m)} \pmod{m}$。此结论可推广到一般的有限交换群上。

定理(Lagrange):假定G是一个阶为n的乘法群，且$g \in G$。那么：(1)$g^n = 1$；(2)g的阶整除n。

证明：(1) 假设$G = \{g_1, g_2 \ldots, g_n\}$。如果$g_i \neq g_j$，那么必有$gg_i \neq gg_j$，否则由消去律得到$g_i = g_j$。因此$G = \{gg_1, gg_2, \ldots, gg_n\}$。从而有：

$$g_1 g_2 \ldots g_n = gg_1 \cdot gg_2 \cdot \ldots gg_n = g^n \cdot g_1 g_2 \ldots g_n$$

因此

$$g^n = 1$$

(2) 假设g的阶为m，且$n = mk + r$，其中$0 \leq r < m$。我们有：

$$1 = g^n = g^{km+r} = g^r$$

那么$r = 0$，即$m|n$。证明完毕！

Lagrange定理说明，有限乘法群的元素的阶$\leq$群的阶。因此有下面定义：

定义：设有限乘法群G的阶为n，若元素a的阶为n，则称为**本原元（或原根、生成元）**。

例:

- $\mathbb{Z}_4^* = \{1, 3\}$的本原元为3。
- $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$中元素1的阶为1，元素$3, 5, 7$的阶为2，因此不存在本原元。

引理*:设a是群G的m阶元素。那么，

(i) $a^0 = 1, a^1, \ldots, a^{m-1}$互不相同。

(ii) 对整数n，$a^n = a^{n \bmod m}$。

(iii) 对整数n，$a^n = 1$当且仅当$m|n$。

(iv) 对整数i, j，$a^i = a^j$当且仅当$i \equiv j \pmod{m}$。

证明:(i)若$a^i = a^j, 0 \le i < j \le m-1$，那么有$a^{j-i} = 1$。因为$m > j - i > 0$，与$m$是最小的满足$a^m = 1$的正整数矛盾。因此$a^i \ne a^j$。

(ii-iii)设$n = mk + r$，$0 \le r < m$。那么有

$$a^n = a^{mk+r} = a^{mk} a^r = a^r = a^{n \bmod m}$$

由(i)知道，$a^n = 1 = a^0$当且仅当$n \bmod m = 0$，即$m|n$。

(iv)$a^i = a^j$当且仅当$a^{i-j} = 1$，由(iii)得到又当且仅当$m|i-j$，即$i \equiv j \pmod{m}$。

- 备注：引理*是密码学第6章及之后章节的基础之一，并且可直接给出第6节的定理1。要熟练应用。

定义: 设$(G,\cdot)$是一个群，非空集合$H\subseteq G$。若$1\in H$且$(H,\cdot)$为群，则称H为G的子群。
定义: 设G是一个群，$a\in G$的阶为m，记

$$\langle \mathbf{a}\rangle = \{1=a^0, a, a^2, \ldots, a^{m-1}\} = \{a^i | i\in\mathbb{Z}\}$$

定理: 设G是一个群，$a\in G$的阶为m。那么$\langle a\rangle$是G的子群，称为由a生成的G的循环子群。
证明: (1)对任意$0\le i,j<m$，由引理*的性质(ii)有$a^{i+j}=a^{(i+j)\bmod m}\in\langle a\rangle$，因此满足封闭性。
(2)对任意$a^i,a^j,a^k\in\langle a\rangle$，显然结合律成立$(a^ia^j)a^k=a^i(a^ja^k)=a^{(i+j+k)\bmod m}$。
(3)$1\in\langle a\rangle$为单位元。
(4)对任意$a^i\in\langle a\rangle$，$a^{m-i}a^i=a^m=1$，因此$a^{m-i}\in\langle a\rangle$是$a^i$的逆元。
定义：如果群G存在生成元a，那么$G=\langle a\rangle$，这时称G为a生成的循环群。
例:$\mathbb{Z}_4^*=\langle 3\rangle=\{1,3\}$，$\mathbb{Z}_5^*=\langle 3\rangle=\{1,3,3^2 \bmod 5=4,3^3 \bmod 5=2\}$。特别地，对任意素数$p$，后面将证明$\mathbb{Z}_p^*$是循环群。

离散对数/指数

本节内容可参考《数论讲义》第5章第6节。

离散对数问题

设α为乘法群$(G,\cdot)$上的n阶元素，
且$\beta\in\langle\alpha\rangle=\{1,\alpha,\alpha^2,\ldots,\alpha^{n-1}\}$。求$a(0\le a\le n-1)$满足

$$\alpha^a=\beta$$

a记为$a=\log_\alpha\beta$，称为β的**离散对数**。

备注：《数论讲义》中，当$G=\mathbb{Z}_m^*$时，$\alpha\in\mathbb{Z}_m^*$是本原元，$\beta\in\langle\alpha\rangle$的离散对数又称为对模数$m$的**指数**，记为$ind_\alpha\beta$。

- 本节主要结论：定理1

定理1:设G是乘法群，$g \in G$是k阶元素，对$a, b \in \langle g \rangle$，我们有

(1) $\log_g(ab) \equiv \log_g a + \log_g b \pmod{k}$；

(2) $\log_g a^n \equiv n \log_g a \pmod{k}$，这里$n \geq 1$；

(3) $\log_g 1 = 0, \log_g g = 1$；

(4) 设$\langle g \rangle = \langle g_1 \rangle$，则$\log_g a \equiv \log_{g_1} a \cdot \log_g g_1 \pmod{k}$；

(5) 设$G = \mathbb{Z}_p^*$，p为奇素数，g为本原元，
则$\log_g(-1) = \frac{\phi(p)}{2}$。

证明:(1)由定义和指数律得到

$$ab = g^{\log_g(ab)} = g^{\log_g a} g^{\log_g b} = g^{\log_g a + \log_g b}$$

由引理*(iv)得到，$\log_g(ab) \equiv \log_g a + \log_g b \pmod{k}$。
(2)由定义和指数律得到

$$g^{\log_g(a^n)} = a^n = (g^{\log_g a})^n = g^{n \log_g a}$$

由引理*(iv)得到，$\log_g a^n \equiv n \log_g a \pmod{k}$。
(3)由$g^0 = 1$得到$\log_g 1 = 0$。由$g^1 = g$得到$\log_g g = 1$。

证明（续）: (4)由定义和指数律得到：

$$a = g^{\log_g a} = g_1^{\log_{g_1} a} = (g^{\log_g g_1})^{\log_{g_1} a} = g^{\log_{g_1} a \cdot \log_g g_1}$$

由引理*(iv)得到，$\log_g a \equiv \log_{g_1} a \cdot \log_g g_1 \pmod k$。
(5)当p为素数时，$\mathbb{Z}_p$上的2次方程

$$x^2 - 1 \equiv 0 \pmod p \tag{1}$$

至多在$\mathbb{Z}_p$上有2个不同解。当$p > 2$时，显然$1, p-1$是$\mathbb{Z}_p$上的两个不同解。
由$1 \equiv g^{\phi(p)} \equiv (g^{\frac{\phi(p)}{2}})^2 \pmod p$知道，$g^{\frac{\phi(p)}{2}}$也是方程(1) 的解。
由引理*(i)知道，若g为本原元，$g^{\frac{\phi(p)}{2}} \not\equiv g^0 \equiv 1 \pmod p$。因此

$$g^{\frac{\phi(p)}{2}} \equiv p - 1 \equiv -1 \pmod p$$

即$\log_g(-1) = \frac{\phi(p)}{2}$。
备注:(5)可以推广到更一般的结论：若模数$m > 2$存在本原元g，则$\log_g(-1) = \frac{\phi(m)}{2}$。留到后面证明。

例1:$p = 13$。有：

$$\begin{aligned}&2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 3, 2^5 \equiv 6, 2^6 \equiv 12,\\&2^7 \equiv 9, 2^8 \equiv 9, 2^9 \equiv 5, 2^{10} \equiv 10, 2^{11} \equiv 7, 2^{12} \equiv 1 \pmod{13}\end{aligned}$$

因此2是本原元。得到以下对数表：

N	1	2	3	4	5	6	7	8	9	10	11	12
$\log_2 N$	12	1	4	2	9	5	11	3	8	10	7	6

例2:解同余式

$$3x \equiv 11 \pmod{13} \tag{2}$$

由定理1，解(2)等价于解以下同余式

$$\log_2 3 + \log_2 x \equiv \log_2 11 \pmod{12}$$

由例1的对数表得到

$$\log_2 x \equiv \log_2 11 - \log_2 3 \equiv 7 - 4 \equiv 3 \pmod{12}$$

因此$\log_2 x = 3$，查例1的对数表得到，$x = 3$，或者$x \equiv 2^3 \equiv 8 \pmod{13}$。

定理2:设m有原根g，$(n,m)=1$，同余式

$$x^k \equiv n \pmod{m} \tag{3}$$

有解的充分必要条件是$d=(k,\phi(m))|\log_g n$。如果此同余式有解，则恰有d个解。

证明:(3)等价于

$$\begin{aligned} & g^{k\log_g x} \equiv g^{\log_g n} \pmod{m} \\ \Leftrightarrow\quad & k\log_g x \equiv \log_g n \pmod{\phi(m)} \end{aligned} \tag{4}$$

而(4)对$t=\log_g x$有解，当且仅当$d=(k,\phi(m))|\log_g n$，如果有解则恰有d个t的解，而由每个t的解，恰好得到一个x的解，t的不同解得到不同的x的解。因此如果(3)有解则恰有d个x的解。

定理2的应用 第2章练习26：证明：若p是素数，则$x^{p-1}\equiv 1 \pmod{p^l}$有$p-1$个解，这里$l\geq 1$.

例3:解同余式

$$x^3 \equiv 5 \pmod{13} \tag{5}$$

2是模数13的本原元。由定理2，只需解同余式

$$3\log_2 x \equiv \log_2 5 \equiv 9 \pmod{12}(\text{查例1对数表知}\log_2 5 = 9) \tag{6}$$

因为$3 = (3,12)|9$，因此(6)有3个解，分别是$\log_2 x \equiv 3, 3+\frac{12}{3} = 7, 3+2\cdot\frac{12}{3} = 11 \pmod{12}$，即$\log_2 x = 3, 7, 11$，由例1的对数表知$x = 8, 11, 7$是(5)的3个解。

本节主要结论：

- G是群，若$g \in G$的阶为l，对$\lambda > 0$，g^{λ}的阶为$\frac{l}{(\lambda,l)}$。
- 定理5。特别地，当p为素数，则$(\mathbb{Z}_p^*, \cdot)$为循环群，即存在本原元。

定义： 设$m > 0, (m, a) = 1$，l是使

$$a^l \equiv l \pmod{m}$$

成立的最小正整数，则l叫做a对模数m的**次数（或阶）**

定理1(《数论讲义》): 设a对模数m的次数为l，$a^n \equiv 1 \pmod{m}, n > 0$，则$l|n$.

证明: 设$a \bmod m = a' \in \mathbb{Z}_m^*$，那么$a'$的阶为$l$。因为$1 \equiv a^n \equiv a'^n \bmod m$，由群部分的引理*知道，$l|n$。

推论(《数论讲义》): 设a对模数m的次数为l，则$l|\phi(m)$.

证明: 由$a^{\phi(m)} \equiv 1 \pmod{m}$可得。

定理2(《数论讲义》): 设a对模数m的次数为l，则

$$1, a, a^2, \ldots, a^{l-1}$$

对模数m两两不同余。

证明: 设$a \bmod m = a' \in \mathbb{Z}_m^*$。由群部分的引理*知道，$1, a', a'^2, \ldots, a'^{l-1}$对模数$m$两两不同余。因此$1, a, a^2, \ldots, a^{l-1}$ 也对模数m两两不同余。

定理3(《数论讲义》):设a对模数m的次数为l，$\lambda > 0$,a^λ对模数m的次数为$l_1 = \frac{l}{(\lambda,l)}$

证明:设a^λ对模数m的次数为l_1。

一方面

$$\left.\begin{array}{r} a^{\lambda l_1} \equiv 1 \pmod{m} \Rightarrow l|\lambda l_1 \Rightarrow \frac{l}{(\lambda,l)} \Big| \frac{\lambda}{(\lambda,l)} \cdot l_1 \\ \left(\frac{l}{(\lambda,l)}, \frac{\lambda}{(\lambda,l)}\right) = 1 \end{array}\right\} \Rightarrow \frac{l}{(\lambda, l)} \Big| l_1$$

另一方面

$$(a^\lambda)^{\frac{l}{(\lambda,l)}} = a^{l \cdot \frac{\lambda}{(\lambda,l)}} \equiv 1 \pmod{m} \Rightarrow l_1 \Big| \frac{l}{(\lambda, l)}$$

综上得到$l_1 = \frac{l}{(\lambda,l)}$。

定理3的结论可推广到一般的群上。

定理： 设G是一个群，$g \in G$的阶为l，那么对$\lambda > 0$，g^λ的阶$l_1 = \frac{l}{(\lambda,l)}$。

证明: 证明类似于定理3。一方面

$$\left.\begin{array}{r} a^{\lambda l_1} \Rightarrow l|\lambda l_1 \Rightarrow \frac{l}{(\lambda,l)}\big|\frac{\lambda}{(\lambda,l)} \cdot l_1 \\ \left(\frac{l}{(\lambda,l)}, \frac{\lambda}{(\lambda,l)}\right) = 1 \end{array}\right\} \Rightarrow \frac{l}{(\lambda, l)}\Big|l_1$$

另一方面

$$(a^\lambda)^{\frac{l}{(\lambda,l)}} = a^{l \cdot \frac{\lambda}{(\lambda,l)}} = 1 \Rightarrow l_1\Big|\frac{l}{(\lambda, l)}$$

所以$l_1 = \frac{l}{(\lambda,l)}$。

接下来给出的2个定理用于证明后面的定理5。

定理4(《数论讲义》): 设p是一个素数，如果存在整数a，它对模数p的次数是l，则恰有$\phi(l)$个对模数p两两不同余的整数，它们对模数p的次数都为l。

证明: 由于a对模数p的次数为l，由定理2得到

$$a, a^2, \ldots, a^{l-1}, a^l = 1 \tag{7}$$

对模数p两两不同余，因此它们是同余式

$$x^l \equiv 1 \pmod p$$

的全部解（因为以上方程至多有l个解）。由此可见，次数为l的对模数p两两不同余的整数，包含在(7)中。

对(7)中的任一数$a^\lambda, 1 \le \lambda \le l$，由定理3知其次数为$l$当且仅当$(\lambda, l) = 1$，因此若整数$a$对模数$p$的次数为$l$，则恰有$\phi(l)$ 个整数对模数p两两不同余且次数为l。

有限循环群也有类似定理4的结论。

定理*： 设循环群$G=\langle g\rangle$，且生成元g的阶为n。那么对任意$d|n$，G中阶为d的元素个数为$\phi(d)$，并有

$$n=\sum_{d|n}\phi(d).$$

证明： G中的元素g^i阶为d当且仅当$d=\frac{n}{\gcd(i,n)}$，

$$\begin{aligned}&\Leftrightarrow \gcd(i,n)=\tfrac{n}{d} \quad (*)\\ &\Rightarrow i=\tfrac{n}{d}\cdot k, 1\le k\le d\end{aligned}$$

把$i=\frac{n}{d}\cdot k$代入(*)得到

$$\frac{n}{d}=\gcd(\frac{n}{d}\cdot k,n)=\frac{n}{d}\cdot\gcd(k,d)\Leftrightarrow \gcd(k,d)=1$$

这说明G中阶为d的元素个数为$\phi(d)$个。
因为G中的元素的阶都为n的因子，因此有

$$n=|G|=\sum_{d|n}|\{a\in G|a\text{的阶为}d\}|=\sum_{d|n}\phi(d)$$

《数论讲义》p69第3章第3节定理1:设$n \geq 1$，则有

$$\sum_{d|n} \phi(d) = n.$$

证明:$\mathbb{Z}_n$关于模n的加法运算构成循环群，其中生成元是1，即$\mathbb{Z} =< 1 >$。1的阶为n，由以上定理*即证得。

课本证明:考虑有理数集

$$S=\{\frac{r}{n},r=1,2,3,\ldots,n\},$$

把S中的每一个分数化为既约分数得到S^*，S^*中没有两个分数的值是相同的。对于任一给定的$r\leq n$, $\frac{r}{n}=\frac{h}{k}$是既约分数，则

$$(h,k)=1,h\leq k,k|n \tag{8}$$

反之，对于给定的n，任一满足(8)中三个条件的分数$\frac{h}{k}$在S^*中，这是因为，由$k|n$，可设$n=kg,r=hg$，故$\frac{h}{k}=\frac{hg}{kg}=\frac{r}{n},r\leq n$。满足(8)中的三个条件的分数$\frac{h}{k}$的全体为$\sum_{d|n}\phi(d)$个，而$S^*$中有$n$个分数，故

$$\sum_{d|n}\phi(d)=n.$$

定理5(《数论讲义》):设p为素数，$l|p-1$，则对模数p的次数是l，且互不同余的整数的个数是$\phi(l)$个。

证明: 设$l|p-1$，$\psi(l)$代表$1,2,\ldots,p-1$中对模数p次数为l的个数。因为$1,2,\ldots,p-1$中任一个数的次数都等于且只等于$p-1$的某一个因数，故$\psi(l)\geq 0$，且

$$\sum_{l|p-1}\psi(l)=p-1. \tag{9}$$

另一方面，欧拉函数有

$$\sum_{l|p-1}\phi(l)=p-1. \tag{10}$$

由定理4知$\psi(l)=0$或$\phi(l)$，从而$\psi(l)\leq\phi(l)$，故由(9),(10)得到和式

$$\sum_{l|p-1}(\psi(l)-\phi(l))=0$$

它的左端的每一项都是非负的，所以对$l|p-1$，必须有$\psi(l)=\phi(l)$.

定理5说明，如果p为素数，则$\mathbb{Z}_p^*$中存在$\phi(p-1)$个本原元（即阶为$\phi(p)=p-1$）。

推论: $(\mathbb{Z}_p^*, \cdot)$是循环群。

相关结论 可用类似的方法证明有限域$GF(p^n)$的乘法群也是循环群。这里暂不进一步讨论。

例： 可验证，2是$\mathbb{Z}_{13}^*$的本原元，那么$\mathbb{Z}_{13}^*$的$\phi(12)=(3-1)2(2-1)=4$个本原元分别是：$2, 2^5 \equiv 6, 2^7 \equiv 11, 2^{11} \equiv 7 \pmod{13}$。

2 原根

定义： 设整数$m>0,(g,m)=1$，如果整数g对m的次数为$\phi(m)$，**则g叫做m的原根**。

- 当$g\in\mathbb{Z}_m^*$，g是m的原根当且仅当g是群$(\mathbb{Z}_m^*,\cdot)$的原根，即

$$\langle g\rangle=\mathbb{Z}_m^*$$

本节主要结论：

- m有原根当且仅当$m=2,4,p^l,2p^l$，其中$l\geq 1,p$为奇素数。
    - 充分性：由定理2给出(由第3节的定理1推出)
    - 必要性：由定理3给出

P.132第3节定理1:如果$m = p_1^{l_1} \dots p_k^{l_k}$是$m$的标准分解式，整数$a$对模数$m$的次数等于整数$a$对模数$p_i^{l_i}(i = 1, \dots, k)$的诸次数的最小公倍数。

证明:设f_i表示a对模数$p_i^{l_i}$的次数$(i = 1, \dots, k)$，$d = [f_1, \dots, f_k]$，则由

$$a^d \equiv 1 \pmod{p_i^{l_i}} (i = 1, \dots, k).$$

得(中国剩余定理)

$$a^d \equiv 1 \pmod{m}.$$

如果d不是a对模数m的次数，则设a的次数为$d', 0 < d' < d$，由

$$a^{d'} \equiv 1 \pmod{m},$$

可得

$$a^{d'} \equiv 1 \pmod{p_i^{l_i}} (i = 1, \dots, k).$$

故$f_i | d' (i = 1, \dots, k)$. 与$d$是$f_1, \dots, f_k$的最小公倍数矛盾。证完。

P.132第3节定理1的应用：
练习1. 证明：m是一个素数的充分必要条件是存在某个整数a，a对模数m的次数为$m-1$。

定理2:设$m > 1$，若m有原根，则m必为下列诸数之一：$2, 4, p^l, 2p^l$，这里$l \geq 1$，p是奇素数。
证明:设m的标准分解式为

$$m = p_1^{l_1} p_2^{l_2} \dots p_s^{l_s}.$$

设f_i表示a对模数$p_i^{l_i}$的次数$(i = 1, \dots, s)$，那么$f_i | \phi(p_i^{l_i})$。由第3节定理1得到，a对模数m的次数为$[f_1, \dots, f_s]$。
若m的原根存在，设为a，那么

$$\phi(m) = \phi(p_1^{l_1}) \dots \phi(p_s^{l_s}) = [f_1, \dots, f_s] \leq [\phi(p_1^{l_1}), \dots, \phi(p_s^{l_s})] \qquad (11)$$

要(11)成立，必须有$\phi(p_1^{l_1}), \dots, \phi(p_s^{l_s})$两两互素。而当$p_i, p_j$为奇素数时，$\phi(p_i^{l_i})$和$\phi(p_j^{l_j})$不互素。当$t > 1, p$为奇素数时，$\phi(2^t), \phi(p^k)$不互素。因此$m$只能形如

$$2^t, 2p^l, p^l, l \geq 1, p\text{为奇素数}.$$

若$t > 2$时2^t存在原根，那么2^{t-1}存在原根，证明如下：设2^t的原根为a，a对模数2^{t-1}的次数为r。有

$$a^r \equiv 1 \pmod{2^{t-1}} \Rightarrow \exists k, a^r = k2^{t-1} + 1 \Rightarrow a^{2r} = (k^2 2^{t-2} + k)2^t + 1$$
$$\Rightarrow a^{2r} \equiv 1 \pmod{2^t} \Rightarrow \phi(2^t) = 2^{t-1} | 2r \Rightarrow 2^{t-2} = \phi(2^{t-1}) | r \Rightarrow r = \phi(2^{t-1})$$

可验证2^3不存在原根，因此$t \geqslant 4$时，2^t的原根也不存在。证明完毕。

定理3: $m=2,4,p^l,2p^l(l\geq 1,p$为奇素数)时，m有原根。
证明定理3之前，首先需要证明下面的引理。
引理: 设g是奇素数p的一个原根，满足

$$g^{p-1}\not\equiv 1 \pmod{p^2} \tag{12}$$

则对于每一个$\alpha\geq 2$，有

$$g^{\phi(p^{\alpha-1})}\not\equiv 1 \pmod{p^\alpha} \tag{13}$$

证明: 对α用归纳法。$\alpha=2$时，(13)即(12)，故命题成立。设命题对$\alpha\geq 2$时成立。由欧拉定理知

$$g^{\phi(p^{\alpha-1})}\equiv 1 \pmod{p^{\alpha-1}}.$$

故可设

$$g^{\phi(p^{\alpha-1})}=1+kp^{\alpha-1},p\not|k(\text{由(13)得到})$$

将上式两端自乘p次，可得

$$g^{\phi(p^\alpha)}=(1+kp^{\alpha-1})^p=1+kp^\alpha+k^2\frac{p(p-1)}{2}p^{2(\alpha-1)}+rp^{3(\alpha-1)} \tag{14}$$

其中r是一个整数。因为$2(\alpha-1),3(\alpha-1)\geq\alpha+1$，故由(14)给出

$$g^{\phi(p^\alpha)}\equiv 1+kp^\alpha \pmod{p^{\alpha+1}}.$$

因为$p\not|k$，故上式给出

$$g^{\phi(p^\alpha)}\not\equiv 1 \pmod{p^{\alpha+1}}.$$故(13)对$\alpha+1$也成立。

定理3的证明:$m=2$时，1为原根。$m=4$时，3为原根。
设$m=p^l, p$为奇素数。$l=1$时，已知p有原根存在，设g是p的原根。下面可取得p的原根r有$r^{p-1}\not\equiv 1 \pmod{p^2}$：

- 若$g^{p-1}\not\equiv 1 \pmod{p^2}$，取$r=g$
- 若$g^{p-1}\equiv 1 \pmod{p^2}$，取$r=g+p$，也是$p$的原根，且

$$r^{p-1}-1=(g+p)^{p-1}-1\equiv g^{p-1}+(p-1)pg^{p-2}-1\equiv -pg^{p-2}\not\equiv 0 \pmod{p^2}$$

现在证明r是$p^l(l\geq 2)$的原根。由引理知道，

$$r^{\phi(p^{l-1})}\not\equiv 1 \pmod{p^l}.$$

因此有

$$r^{\phi(p^{l-1})}\equiv r^{\frac{\phi(p^l)}{p}}\not\equiv 1 \pmod{p^l}$$

根据第四节的定理1知道r是模p^l的原根。
设$m=2p^l, p$是奇素数。令g是p^l的一个原根。

- 当g是奇数时，g也是2的原根，因此g对m的次数为$[\phi(2),\phi(p^l)]=\phi(m)$，即$g$为$m$的原根。
- 当g为偶数时，$g+p^l$为奇数，且是2和p^l的原根，同样可证也是m的原根。

我们之前证明了，当p为奇素数时，$\log_2(-1)=\frac{\phi(p)}{2}$。下面证明更一般的结论。

命题: 设m有原根g，那么$\log_g(-1)=\frac{\phi(m)}{2}$，这里$m>2$。

证明: 设$m>2$且有原根g，那么由定理2、3知，$m=4,p^\alpha,2p^\alpha$，其中p为奇素数。这时皆有$\phi(m)\equiv 0 \pmod 2$。

只需要证明$g^{\frac{\phi(m)}{2}}\equiv -1 \pmod m$。

(1)$m=4$时：命题容易验证成立。

(2)$m=p^\alpha$时：由

$$\left.\begin{array}{r} g^{\phi(m)}\equiv 1 \pmod{p^\alpha}\Rightarrow (g^{\frac{\phi(m)}{2}}-1)(g^{\frac{\phi(m)}{2}}+1)\equiv 0 \pmod{p^\alpha} \\ \gcd\left((g^{\frac{\phi(m)}{2}}-1),(g^{\frac{\phi(m)}{2}}+1)\right)=1\text{或}2 \end{array}\right\}$$
$$\Rightarrow p^\alpha|g^{\frac{\phi(m)}{2}}-1\text{或者}p^\alpha|g^{\frac{\phi(m)}{2}}+1$$
$$\Rightarrow g^{\frac{\phi(m)}{2}}\equiv 1 \pmod{p^\alpha}\text{或}g^{\frac{\phi(m)}{2}}\equiv -1 \pmod{p^\alpha}$$

因为g是p^α的原根，所以$g^{\frac{\phi(m)}{2}}\equiv -1 \pmod{p^\alpha}$。

(3)$m=2p^\alpha$时：

$$\left.\begin{array}{l} \text{同理可得}g^{\frac{\phi(m)}{2}}\equiv -1 \pmod{p^\alpha} \\ (2,g)=1\Rightarrow g^{\frac{\phi(m)}{2}}\equiv -1 \pmod 2 \end{array}\right\}$$
$$\Rightarrow g^{\frac{\phi(m)}{2}}\equiv -1 \pmod{2p^\alpha}\text{(由中国剩余定理)}$$

本节给出判断原根的方法，即定理1。

定理1: 设$m > 2$，$\phi(m)$的所有不同素因子是$q_1, q_2, \ldots, q_s$，$(g, m) = 1$，则g是m的一个原根的充分必要条件是

$$g^{\frac{\phi(m)}{q_i}} \not\equiv 1 \pmod{m} (i = 1, 2, \ldots, s) \tag{15}$$

证明. 必要性： 若g是模数m的一个原根，则g对模数m的次数是$\phi(m)$，但$0 < \frac{\phi(m)}{q_i} < \phi(m)(i = 1, \ldots, s)$，故(15)成立。

充分性: 反之，若(15)成立，设g对模数m的次数是f，假定$f < \phi(m)$，因为$f|\phi(m)$，所以整数$\frac{\phi(m)}{f} > 1$，故有某个素因数$q_i|\frac{\phi(m)}{f}$，即$\frac{\phi(m)}{f} = q_i u$，于是$\frac{\phi(m)}{q_i} = fu$，

$$g^{\frac{\phi(m)}{q_i}} = g^{fu} \equiv 1 \pmod{m}$$

这与(15)矛盾。故$f = \phi(m)$，即g是m的一个原根。

4 计算原根的方法

例1:12是41的一个原根。

解:设$m = 41$，$\phi(41) = 2^3 \cdot 5 = 40$，

$$12^{\frac{\phi(m)}{2}} = 12^{20} \not\equiv 1 \pmod{41}$$

$$12^{\frac{\phi(m)}{5}} = 12^{8} \not\equiv 1 \pmod{41}$$

故由定理1知12是41的一个原根。

相关习题：

习题20.用指数表解下列同余式：

1. $8x \equiv 7 \pmod{43}$；
2. $x^8 \equiv 17 \pmod{43}$；
3. $8^x \equiv 3 \pmod{43}$.

提示：用本节定理1求43的原根。随机选择一个整数，然后用定理1判定是否是原根，如果不是则另行选择其他整数，继续判定，直到找到为止。

习题22：在与模数61互素的剩余系中指出：

1. 对模数61次数为10的数；
2. 61的全部原根。

提示：用本节定理1求61的一个原根。随机选择一个整数，然后用定理1判定是否是原根，如果不是则另行选择其他整数，继续判定，直到找到为止。

若g是61的一个原根，根据g^r的次数为$\frac{60}{(r,60)}$计算61的全部原根和所有次数为10的数。

总结

群的基础性质：

- 消去律，单位元唯一，逆元唯一，广义结合律，$(x^{-1})^{-1} = x$，$(ab)^{-1} = b^{-1}a^{-1}$.
- 指数律：$(a^n)^m = a^{nm}$，$a^m a^n = a^{m+n}$，若a和b交换则$(ab)^n = a^n b^n$.
- Lagrange定理：假定G是一个阶为n的乘法群，且$g \in G$。那么：(1)$g^n = 1$；(2)g的阶整除n。
- G是群，$g \in G$的阶为m，则$\langle g \rangle$是G的阶为m的循环子群。

总结

指数的基本性质：设a是群G的m阶元素。那么，

(i) $a^0=1, a^1, \ldots, a^{m-1}$互不相同。

(ii) 对整数n，$a^n=a^{n \bmod m}$。

(iii) 对整数n，$a^n=1$当且仅当$m|n$。

(iv) 对整数i,j，$a^i=a^j$当且仅当$i\equiv j \pmod m$。

离散对数的基本性质：设G是乘法群，$g\in G$是k阶元素，对$a,b\in\langle g\rangle$，我们有

(1) $\log_g(ab)\equiv\log_g a+\log_g b \pmod k$；

(2) $\log_g a^n\equiv n\log_g a \pmod k$，这里$n\geq 1$；

(3) $\log_g 1=0, \log_g g=1$；

(4) 设$\langle g\rangle=\langle g_1\rangle$，
则$\log_g a\equiv\log_{g_1} a\cdot\log_g g_1 \pmod k$；

(5) 设$G=\mathbb{Z}_m^*$有原根且$m>2$，令g为本原元，
则$\log_g(-1)=\frac{\phi(m)}{2}$。

总结

原根的性质：

- G是群，若$g \in G$的阶为l，对$\lambda > 0$，g^{λ}的阶为$\frac{l}{(\lambda,l)}$。
- 设循环群$G = \langle g \rangle$，且生成元g的阶为n。那么对任意$d|n$，G中阶为d的元素个数为$\phi(d)$.
- $(\mathbb{Z}_m^*, \cdot)$为Abel群。$(\mathbb{Z}_m^*, \cdot)$为循环群当且仅当$m = 2, 4, p^l, 2p^l$，其中$l \geq 1$，p为奇素数。
- $\mathbb{Z}_m^*$的原根判定准则：设$m > 2$，$\phi(m)$的所有不同素因子是$q_1, q_2, \ldots, q_s$，$(g, m) = 1$，则g是m的一个原根的充分必要条件是

$$g^{\frac{\phi(m)}{q_i}} \not\equiv 1 \pmod{m} (i = 1, 2, \ldots, s)$$

- $\mathbb{Z}_m^*$的元素次数的计算：如果$m = p_1^{l_1} \ldots p_k^{l_k}$是$m$的标准分解式，整数$a$对模数$m$的次数等于整数$a$对模数$p_i^{l_i} (i = 1, \ldots, k)$的诸次数的最小公倍数。