求素数原根的判准法和降幂法

李作新　　卢庆堂

中国科学院沈阳计算技术研究所　　沈阳鼓风机厂

摘　要

本文给出求解素数模 P 和模 P^{α} ($\alpha>1$)之原根的两种算法，从而解决了用计算机求大素数原根的困难。

一、引言*

随机数的优劣，直接影响诸如 Monte carlo 方法等相关结果的质量。而对确定字长的计算机而言，用乘同余法生成伪随机数的最大循环长度和偏度，又与大素数模及模的原根密切相关[1]。于是，能否给出求大素数原根的算法，成为寻找优良的随机数必须解决的问题。

迄今为止，已知求原根的方法是根据下述定理[2]：

定理1.1. 设 g 是 P 的平方非剩余，$P-1=q_0^{\alpha_0}q_1^{\alpha_1}q_2^{\alpha_2}\cdots q_k^{\alpha_k}$ 是 $P-1$ 的标准分解式，若恒有

$$g^{\frac{P-1}{q_i}}\not\equiv 1 \pmod P,\quad i=0,1,2,\cdots,k \qquad (1.1)$$

则 g 就是 P 的原根。其中 $\alpha_i>1$，$q_0=2$；$q_1,q_2\cdots q_k$ 是互异的素因数.

---

* 本文中所用的文字，均表示整数。P 表示奇素数。文中提到的最小剩余，均指非负的最小剩余。模 P 的剩余或原根，简述为 P 的剩余或原根。

该定理等价于g是P的二次和q_i次非剩余[2][3]

即：$$x^{q_i} \not\equiv g \pmod{P},\ i=0,1,2,\cdots K \qquad (1.2)$$

但是对较大的素数P，用计算机求解(1.1)或(1.2)式，都要占用很大机时，甚至难以实现[4]。下面给出求P^{α}原根的两种算法，从数论可知，这是有普遍性的。

二、列推法

1. $\alpha=1$的情况

从(1.2)式出发，但是为了避免直接求非剩余的困难，先去寻求(1.2)式有解的最小剩余，记为$a_{q_i}(x)$，该最小剩余依x值而定。即从同余式

$$x^{q_i} \equiv a_{q_i}(x) \pmod{P},\ i=0,1,2,\cdots,K \qquad (2.1)$$

出发，对确定的x求出$a_{q_i}(x)$。再从P的最小完全剩余组中去掉$a_{q_i}(x)$，$i=0,1,\cdots,K$，余者就是全D非剩余即P的全D原根。然而，按此方法，要试过所有奎数的x值之后，才能得到全D对应的$a_{q_i}(x)$。显然，这在实际上是行不通的。不过，当$x>P$时，即$x=nP+x_1$，$x_1<P$，则x^{L}和x_1^{L}对P同余。故大于P的x值可不考虑。再注意

定理2.1 如果$a_L(K)$是$x=K$时P的L次最小剩余，则$x=P-K$时的最小剩余$a_L(P-K)$由下式确定。

$$a_L(P-K)=\begin{cases} a_L(K), & L\text{是偶数} \\ P-a_L(K), & L\text{是奇数} \end{cases} \qquad (2.2)$$

又由

$$(-x)^L = (-1)^L x^L \equiv \begin{cases} a_L(K) \pmod p, & L: \text{偶数} \\ p - a_L(K) \pmod p, & \text{奇数} \end{cases}$$

可知，为求$a_{q_i}(x)$，只需考虑$0 < x \leq \frac{p-1}{2}$的x值。(2.2)式可用于确定$\frac{p-1}{2} < x < p$时对应的$a_{q_i}(x)$。

因平方剩余和非剩余各有$\frac{p-1}{2}$个及(2.2)式便可推知$a_2(1), a_2(2), \cdots, a_2(\frac{p-1}{2})$必互不相等，并可用下述递推公式确定它们。

定理2.2 若$a_2(K)$和$a_2(K-1)$分别是$x=K$，$x=K-1$时，p的最小平方剩余，则有

$$a_2(K) \equiv a_2(K-1) + 2K - 1 \pmod p \qquad (2.3)$$

再确定p的q_i次剩余。

因为$q_1, q_2, \cdots, q_K$均为奇素数，故$a_{q_i}(K)$可写为$a_{L+2}(K)$，L为奇数。那么$a_{L+2}(K)$的递推公式可由下述定理给出。

定理2.3：若$a_{L+2}(K)$是$x=K$时，p的$L+2$次最小剩余，则有：

$$a_{L+2}(K) \equiv a_2(K) a_L(K) \pmod p \qquad (2.4)$$

此即由$a_2(K)$和$a_L(K)$，求$a_{L+2}(K)$的递推公式。

$2^\alpha > 1$的情况

解决这种情况，可以下列(2)出发。

引2.2，如果g是P的原根，必存在一个t，使得$(g+Pt)^{P-1}=1+uP$，其中$P\nmid u$。而对任意$\alpha>1$，则$g+Pt$就是P^{α}的原根。

注意，因为g是P的原根，故有

$$g^{P-1}=1+PT_0 \qquad (2.5)$$

又因为$(g+Pt)^{P-1}=1+P(T_0-g^{P-2}t+PT)=1+Pu$其中$T=g^{P-2}t+C_{P-1}^{2}g^{P-3}t^2+\cdots+P^{P-3}t^{P-1}$。从而得到

$$u=T_0-g^{P-2}t+PT$$

可见$P\nmid u$等价于$u_1=T_0-g^{P-2}t$不能被P除尽。若由此出发，找一个t使得$P\nmid u_1$，必须先用(2.5)式求出T_0。这对一个较大的素数P，也并不容易。然而，直接求T_0被P除的余数，可使问题简化。为此，先求g^{P-1}被P^2除的余数，记为γ。则g^{P-1}可表为

$$g^{P-1}=P^2T_1+\gamma \qquad (2.6)$$

再由(2.5)式可得到$1+PT_0=P^2T_1+\gamma$，所以$T_0=PT_1+\frac{\gamma-1}{P}$，可见，$\frac{\gamma-1}{P}$就是$T_0$被$P$除的余数。$\gamma$由(2.6)式决定。对于大素数$P$来说，求$\gamma$要比求$T_0$容易得多。这样，$P\nmid u_1$又等价于$\frac{\gamma-1}{P}-g^{P-2}t$不能被$P$除尽。于是得到：

定理2.4. 如果g是P的原根，对任意$\alpha>1$，若t满足

$$t\neq\frac{\gamma-1}{P}g^{P-2} \qquad (2.7)$$

而且 $P \nmid t$，那么 $g+Pt$ 就是 P^2 的原根，其中 t 由 $g^{P-1}=P^2T_1+Y$ 确定。

三 降幂法

从(1.1)式出发，对 a 是否 P 的平方非剩余的判断，先给出一个计林公式；对同余式 $a^{\frac{P-1}{q_i}} \equiv 1 \pmod P$ 的检验，再给出降幂法。

定理3.1，令 $a_1=a$，$a_2=P$，而且 $a<P$，并作下面分解：

$$\begin{aligned} a_1 &= \lambda_1 a_2 + 2^{L_2} a_3, \\ a_2 &= \lambda_2 a_3 + 2^{L_3} a_4, \\ &\cdots\cdots \\ a_{n-1} &= \lambda_{n-1} a_n + 2^{L_n} a_{n+1} \end{aligned} \qquad (3.1)$$

直到 $a_{n+1}=1$ 为止，其中 a_2，a_3，…，a_n 均为奇数，则 a 是 P 的平方非剩余的必要条件是

$$\sum_{i=2}^{n} \frac{a_i^2-1}{8} L_i + \frac{1}{4}\sum_{i=2}^{n-1}(a_i-1)(a_{i+1}-1) \equiv 1 \pmod 2 \qquad (3.2)$$

定理3.2，如果 a 是 P 的平方非剩余，则

$a^{\frac{P-1}{q_i}} \equiv 1 \pmod P$ 等价于

$$a^{\frac{P-1}{2q_i}} \equiv P-1 \pmod P,\ i=1,2,\cdots,K \qquad (3.3)$$

其中 q_i 是 $P-1$ 的标准分解式中的素因子。

这条定理，把对同余式 $a^{\frac{P-1}{q_i}} \equiv 1 \pmod P$ 的计林归结为对 $a^{\frac{P-1}{2q_i}} \equiv P-1 \pmod P$ 的计林。从而幂指数下降为原来的 $\frac{1}{2}$。但是，当 P 很大时，$\frac{P-1}{2q_i}$ 还可能很大，因而必须继续降幂。为此，先把 q_i 从大到小排列起来。即：

$q_1 > q_2 > \cdots > q_K$，所以 $\frac{P-1}{2q_1} < \frac{P-1}{2q_2} < \cdots < \frac{P-1}{2q_K}$。

令 $\alpha_1 = \frac{P-1}{2q_1}$，$\alpha_i = \frac{P-1}{2q_i} - \frac{P-1}{2q_{i-1}}$，$i = 2, 3, \cdots, K$。

于是又有：

定理3.3．$a^{\frac{P-1}{2q_i}} \equiv P-1 \pmod{P}$ 等价于同余式

$$R_i a^{\alpha_i} \equiv P-1 \pmod{P}, \quad i = 1, 2, \cdots, K. \qquad (3.4)$$

其中 $R_1 = 1$，R_i（$i = 2, 3, \cdots, K$）是 $R_{i-1} a^{\alpha_{i-1}}$ 对 P 的最小剩余。

该定理把对（3.3）式的讨论又归结为对（3.4）式的讨论，幂指数又进一步得到下降。

最后再讨论 $R_i a^{\alpha_i}$ 对 P 的最小剩余。为编写程序方便，把 $R_i a^{\alpha_i}$ 写为 $c_1 b_1^{n_1}$。下面就来求 $c_1 b_1^{n_1}$ 对 P 的最小剩余。具步骤如下：

(1) 求满足 $b_1^{K_1-1} < P < b_1^{K_1}$ 的 K 值；

(2) 把 $b_1^{K_1}$ 和 n_1 表为

$$b_1^{K_1} = \lambda_1 P + b_2$$

$$n_1 = n_2 K + r_1 \quad ;$$

(3) 再把 $c_1 b_1^{r_1}$ 表为 $c_1 b^{r_1} = \alpha_1 P + c_2$

容易证明 $c_1 b_1^{n_1} \equiv c_2 b_2^{n_2} \pmod{P}$。重复这三步，设进行到第 i 步，求满足下式的 K_i：

$b_i^{K_i - 1} < P < b_i^{K_i}$。仿此 $b_i^{K_i} = \lambda_i P + b_{i+1}$，

$n_i = n_{i+1} K_i + r_i$，$c_i b_i^{r_i} = \alpha_i P + c_{i+1}$；可得

$$c_i b_i^{n_i} \equiv c_{i+1} b_{i+1}^{n_{i+1}} \pmod{P} \qquad (3.5)$$

如此进行，直到 $n_{i+1} = 0$；或 $b_{i+1} = 1$ 为止，这时

$$c_i b^{n_i} \equiv c_{i+1} \pmod{P} \qquad (3.6)$$

再由 $c_1 b_1^{n_1} \equiv c_2 b_2^{n_2} \pmod{P}$

$c_2 b_2^{n_2} \equiv c_3 b_3^{n_3} \pmod{P}$

.....

$c_{i-1} b_{i-1}^{n_{i-1}} \equiv c_i b_i^{n_i} \pmod{P}$

以及(3.1)式可推得

$$c_1 b^{n_1} \equiv c_{i+1} \pmod{P} \qquad (3.7)$$

因为 $c_{i+1} < P$，所以 c_{i+1} 就是 $c_1 b_1^{n_1}$ 对 P 的最小剩余

再回到(3.4)式。计算步骤如下，先计算 $R_1 \equiv a^{\alpha_1} \pmod{P}$ 的最小剩余 R_2，再计算 $R_2 \alpha^{\alpha_2}$ 对 P 的最小剩余 R_3，等等，依此可计算(3.4)式的全 D 剩余。如果这些剩余不等于 P-1 而且 a 又是 P 的平方非剩余，则这个 a 就是 P 的原根

本文所介绍的方法既能求出全 D 元根又可求出某一范围内的元根。若把 α_1 的初值选为最小正元根的下界[5]，或根据需要设定 α_1 的初值，计算可更为简洁。

参 考 文 献

(1) 李炯新、卢庆堂，近似随机数的偏度，计算物理中一届学术论文集。

(2) И.М.维诺格拉陀夫，数论基础，高教出版社，(1956)

(3) 张德馨，整数论，科学出版社，(1958)

(4) 华罗庚，数论引论，科学出版社，(1979)

(5) 王 元，论素数的最小正原根，数学学报9，1959，432－441。