第 23卷第 6期　　商丘师范学院学报　　Vol 23 No. 6
2007 年 6 月　　JOURNAL OF SHANGQIU TEACHERS COLLEGE　　June, 2007

混合线性同余发生器的周期分析

张广强[1], 张小彩[2]
(1. 华北水利水电学院 数学与信息科学学院,河南 郑州 450011; 2. 河南工业大学 理学院,河南 郑州 450052)

摘　要:结合文献[1]给出了混合线性同余发生器达到满周期的条件,并给出了系统的数学证明.
关键词:混合同余线性发生器;序列;周期
中图分类号: O242　　**文献标识码**: A　　**文章编号**: 1672 - 3600(2007)06 - 0040 - 03

The analysis on the period of mixed linear congruential generators

ZHANG Guang-qiang[1], ZHANG Xiao-cai[2]
(1. College of Mathematics and Information Sciences, North China Institute of Water Conservancy and Hydroeletric Power, Zhengzhou 450011, China; 2. College of Science, Henan University of Technology, Zhengzhou 450052, China)

Abstract: In this paper, based on the document[1] it gives the situation, where mixed linear congruential generators reach the maximal period, and presents the systematic mathematical proof.
Key words: mixed linear congruential generator; sequence; period

1　混合线性同余发生器

目前应用最广泛的随机数发生器之一就是线性同余发生器(Linear Congruential Generator, LCG for short). 它是由 Lehmer 在 1951年提出的. 它包括混合同余发生器(Mixed LCG, MLCG for short)和乘同余发生器(Pure Multiplicative LCG, PMLCG for short). 它是目前使用最普通、发展最迅速的数学方法.

LCG的一般递推公式为:

$$\begin{aligned} x_n &= ax_{n-1} + c \pmod m \\ r_n &= x_n / m \end{aligned} \qquad (n = 1, 2, \cdots) \qquad (1)$$

其中, a为乘子(Multiplier), c为增量(Increment), m为模数(Modulus), x_0为初始值,即种子(Seed); 且 $0 < a, c, x_0 < m$.

当(1)式中增量 $c > 0$时, LCG称为 MLCG; 当 $c = 0$时, LCG称为 PMLCG.

定义 1　(序列)对初始值 x_0,由(1)式产生的随机数列 $\{x_i\}$ $(n = 1, 2, \cdots)$称之为 LCG序列.

定义 2　(周期)在 LCG序列 $\{x_i\}$中,满足 $x_k = x_0$的最小正整数 k称为该序列的周期,记作 $d = k$ 若 $d = m$,则称该序列达到满周期.

本文主要研究分析 MLCG序列 $\{x_i\}$的周期,即选取什么样的乘子 a和增量 c才能使得 MLCG序列 $\{x_i\}$达到满周期.

2　周期分析(选取准则)

下面首先介绍几个重要引理.

引理 1　如果 $a \mid bc$,且 $(a, b) = 1$,则 $a \mid c$

证明: $a \mid bc \Rightarrow bc = ak \quad k \in Z$

$(a, b) = 1 \Rightarrow$存在 $m, n \in Z$使得 $ma + nb = 1$

从而 $amc + bnc = c$,即 $amc + nak = c$,即 $a(mc + nk) = c$

收稿日期: 2006 - 09 - 27; **修回日期**: 2006 - 12 - 08
作者简介:张广强(1980 -),男,河南漯河人,华北水利水电学院教师,硕士,主要从事计算机随机模拟方面的研究.

因此 $a \mid c$

引理 2[4]　任何自然数 m 均可分解成: $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, p_i 为素数, $\alpha_i \in Z^+$ $(i = 1, \cdots, n)$, 且分解是唯一的.

引理 3　设 $\{x_i\}$ 是产生的随机数序列, 且 $a \geq 2$, 则

$$x_{i+k} = a^k x_i + (a^k - 1)\, c/(a - 1) \pmod m \qquad k \geq 0$$

特别地, $x_k = a^k x_0 + (a^k - 1)\, c/(a - 1) \pmod m \qquad k \geq 0$

证明: (数学归纳法)

当 $k = 0$ 时, 显然成立.

假设 $x_{i+k} = a^k x_i + (a^k - 1)\, c/(a - 1) \pmod m$ 成立!

则 $x_{i+(k+1)} = a x_{i+k} + c \pmod m = a[a^k x_i + (a^k - 1)\, c/(a - 1)] + c \pmod m = a^{k+1} x_i + (a^{k+1} - a)\, c/(a - 1) + c \pmod m$

$= a^{k+1} x_i + [(a^{k+1} - a)/(a - 1) + 1]\, c \pmod m = a^{k+1} x_i + (a^{k+1} - 1)\, c/(a - 1) \pmod m$

综之, $x_{i+k} = a^k x_i + (a^k - 1)\, c/(a - 1) \pmod m \qquad k \geq 0$.

特别地, 取 $i = 0$, 则 $x_k = a^k x_0 + (a^k - 1)\, c/(a - 1) \pmod m \qquad k \geq 0$.

引理 4　设 $\{x_i\}$ 是 MLCG 产生的随机数序列, 其周期为 d, $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots\cdots p_n^{\alpha_n}$, p_i $(i = 1, 2, \cdots, n)$ 为素数, $\alpha_i \in Z^+$ $(i = 1, 2, \cdots, n)$; $\{x_{j\,i}\}$ 是 MLCG$(x_{j\,0}, a_j, c_j, m_j)$ 产生的随机数序列, 其周期为 d_j, 其中 $x_{j\,0} = x_0 \pmod{m_j}$, $a_j = a \pmod{m_j}$, $c_j = c \pmod{m_j}$, $m_j = p_j^{\alpha_j}$, $(j = 1, \cdots, n)$, 则 $d = \mathrm{lcm}(d_1, \cdots, d_n)$, 即 $d_1, \cdots, d_n$ 的最小公倍数.

证明: 不是一般性, 不妨设 $m = p_1^{\alpha_1} p_2^{\alpha_2} = m_1 m_2$, 从而 $(m_1, m_2) = 1$.

$$x_n = (a x_{n-1} + c) \bmod (m_1 m_2) \tag{1}$$

由 (1)式知:

$$x_{1,n} = (a_1 x_{1,n-1} + c_1) \bmod (m_1) \tag{2}$$

$$x_{2,n} = (a_2 x_{2,n-1} + c_2) \bmod (m_2) \tag{3}$$

从而由上述 (1)式知: $x_n \pmod{m_1} = (a_1 x_{1,n-1} + c_1) \bmod (m_1)$, 于是 $x_{1,n} = x_n \bmod (m_1)$.

同理可得: $x_{2,n} = x_n \bmod (m_2)$.

不妨设 $d^* = \mathrm{lcm}(d_1, d_2)$, 下证 $d^* = d$.

一方面: $x_{k+d} = x_k$ $(k \geq 0)$, 则 $x_{k+d} \pmod{m_1} = x_k \pmod{m_1}$, 即 $x_{1,k+d} = x_{1,k}$.

从而 $d_1 \mid d$

同理 $d_2 \mid d$

故

$$d^* = \mathrm{lcm}(d_1, d_2) \mid d \tag{4}$$

另一方面: $x_{1,k+d_1} = x_{1,k}$ $(k \geq 0)$, 即 $a_1 x_{1,k-1+d_1} + c_1 \pmod{m_1} = a_1 x_{1,k-1} + c_1 \pmod{m_1}$.

从而 $x_{k+d_1} = a x_{k-1+d_1} + c \pmod{m_1 m_2} = a x_{k-1} + c \pmod{m_1 m_2} = x_k$, 即 $x_{k+d_1} = x_k$. 则 $d \mid d_1$.

同理: $d \mid d_2$.

故

$$d \mid \mathrm{lcm}(d_1, d_2) = d^* \tag{5}$$

由 (4)和 (5)式知: $d = d^* = \mathrm{lcm}(d_1, d_2)$.

归纳之, $d = \mathrm{lcm}(d_1, \cdots, d_n)$, 即 $d_1, \cdots, d_n$ 的最小公倍数.

引理 5　设 p 为素数, $\alpha \in Z^+$, 且 $p^\alpha > 2$, 如果 $x = 1 \pmod{p^\alpha}$, $x \neq 1 \pmod{p^{\alpha+1}}$;

则 $x^p = 1 \pmod{p^{\alpha+1}}$, $x^p \neq 1 \pmod{p^{\alpha+2}}$.

证明: 因为 $x = 1 \pmod{p^\alpha}$, $x \neq 1 \pmod{p^{\alpha+1}}$,

则有 $x = 1 + q p^\alpha$, 其中 $q \in Z$ 且 $q \nmid P$.

从而 $x^p = (1 + q p^\alpha)^p = 1 + C_p^1 q p^\alpha + C_p^2 q^2 p^{2\alpha} + \cdots + C_p^{p-1} q^{p-1} p^{(p-1)\alpha} + q^p p^{p\alpha}$

$= 1 + q p^{\alpha+1} (1 + C_p^2 q p^{\alpha-1} \cdots + C_p^{p-1} q^{p-2} p^{(p-1)\alpha-1} + q^{p-1} p^{(p-1)\alpha-1})$

$= 1 + q p^{\alpha+1} Q$

其中, $Q = 1 + C_p^2 q p^{\alpha-1} \cdots + C_p^{p-1} q^{p-2} p^{(p-1)\alpha-1} + C_p^p q^{p-1} p^{(p-1)\alpha-1} \in Z$.

显然, $x^p = 1 \pmod{p^{\alpha+1}}$.

因为 $p \mid C_p^2 q p^{\alpha-1}, \cdots, p \mid C_p^{p-1} q^{p-2} p^{(p-1)\alpha-1}, p \mid C_p^p q^{p-1} p^{(p-1)\alpha-1}$

则 $p \nmid Q = 1 + C_p^2 q p^{\alpha-1} \cdots + C_p^{p-1} q^{p-2} p^{(p-1)\alpha-1} + C_p^p q^{p-1} p^{(p-1)\alpha-1}$.

故 $x^p \neq 1 \pmod{p^{\alpha+2}}$.

综上知, $x^p = 1 \pmod{p^{\alpha+1}}$, $x^p \neq 1 \pmod{p^{\alpha+2}}$.

引理 6　如果 $a = 1 \pmod 4$, 则 $(a^{2^\alpha} - 1)/(a - 1) = 0 \pmod{2^\alpha}$　$\alpha > 1$.

证明: $a = 3 \pmod 4 \Rightarrow a = 3 + 4t$　$t \in Z \Rightarrow a = 1 + 2(1 + 2t) \Rightarrow a = 1 \pmod 2$

所以, $a^2=(3+4t)^2=9+24t+16t^2=1+8(1+3t+2t^2)\Rightarrow \begin{cases} a^2=1(\mathrm{mod}2^3) \\ a^2\neq 1(\mathrm{mod}2^4) \end{cases}$

由引理 5知: $\begin{cases} a^4=1(\mathrm{mod}2^4) \\ a^4\neq 1(\mathrm{mod}2^5) \end{cases}$, ……, $\begin{cases} a^{2^{\alpha-1}}=1(\mathrm{mod}2^{\alpha+1}) \\ a^{2^{\alpha-1}}\neq 1(\mathrm{mod}2^{\alpha+2}) \end{cases}$

即 $a^{2^{\alpha-1}}-1=0(\mathrm{mod}2^{\alpha+1})\Rightarrow a^{2^{\alpha-1}}-1=k_1 2^{\alpha+1}\quad k_1\in Z^+\Rightarrow (a^{2^{\alpha-1}}-1)/2=k_1 2^{\alpha}\Rightarrow (a^{2^{\alpha-1}}-1)/2=0(\mathrm{mod}2^{\alpha})$

又 $a=1(\mathrm{mod}2)\Rightarrow a-1=0(\mathrm{mod}2)$

则 $(a^{2^{\alpha-1}}-1)/2=0(\mathrm{mod}2^{\alpha})\Rightarrow (a^{2^{\alpha-1}}-1)/(a-1)=0(\mathrm{mod}2^{\alpha})$.

定理 1 如果下列 3个条件都满足,则 MLCG达到满周期 (即周期 $d=m$)

(1) $(c,m)=1$,即 c,m 互素;

(2)对 m 的任一素因子 p有 $a=1(\mathrm{mod}p)$;

(3)如果 $4|m$,则 $a=1(\mathrm{mod}4)$.

证明: (1) $a=1$的情况,

显然 $a=1$满足条件 (2)和 (3),且 $x_i=x_{i-1}+c(\mathrm{mod}m)\quad (i=1,2,\cdots)$

从而 $x_i=x_0+ic(\mathrm{mod}m)$,于是 $x_d=x_0\Rightarrow dc=0(\mathrm{mod}m)$,即 $m|dc$;

因为 $(c,m)=1$,所以由引理 1知: $m|d$,从而 $d=m$.

(2) $a\geq 2$的情况,

由引理 2知,模数 m 可分解为: $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$, p_i为素数, $\alpha_i\in Z^+$ $(i=1,\cdots,n)$由引理 4知,仅仅分析 $m=p^{\alpha}$, p为素数, $\alpha\in Z^+$的情形即可.

①当 $p\neq 2$时,

由条件 (2)中 $a=1(\mathrm{mod}p)$知: $a=1+k_1p^{\gamma}$, $p^{\gamma}>2$且 $k_1\neq qp$, γ, $q\in Z^+$

从而 $a=1(\mathrm{mod}p^{\gamma})$, $a\neq 1(\mathrm{mod}p^{\gamma+1})\quad \gamma\geq 1$

由引理 5知: $a^p=1(\mathrm{mod}p^{\gamma+1})$, $a^p\neq 1(\mathrm{mod}p^{\gamma+2})$

递推之,得一般式: $a^{p^{\omega}}=1(\mathrm{mod}p^{\gamma+\omega})$, $a^{p^{\omega}}\neq 1(\mathrm{mod}p^{\gamma+\omega+1})\quad \omega\geq 0$

从而 $(a^{p^{\omega}}-1)/(a-1)=0(\mathrm{mod}p^{\omega})$, $(a^{p^{\omega}}-1)/(a-1)\neq 0(\mathrm{mod}p^{\omega+1})\quad \omega\geq 0$

则 $$(a^{p^{\alpha}}-1)/(a-1)=0(\mathrm{mod}p^{\alpha}) \tag{6}$$

由引理 3知: $x_k=a^kx_0+(a^k-1)c/(a-1)(\mathrm{mod}m)\qquad k\geq 0$

于是取 $x_0=0$时,有 $x_k=(a^k-1)c/(a-1)(\mathrm{mod}p^{\alpha})\qquad k\geq 0$

则 $x_d=x_0=0\Rightarrow (a^d-1)c/(a-1)=0(\mathrm{mod}p^{\alpha})$

又 $(c,m)=(c,p^{\alpha})=1$,则由引理 1知:

$$(a^d-1)/(a-1)=0(\mathrm{mod}p^{\alpha}) \tag{7}$$

由 (6)和 (7)式知: $d=p^{\alpha}$,即 $d=m$.

②当 $p=2,\alpha\geq 2$,即 $4|p^{\alpha}$时,

由引理 6知:

$$(a^{2^{\alpha}}-1)/(a-1)\equiv(\mathrm{mod}2^{\alpha})\quad \alpha>1 \tag{8}$$

由 (7)和 (8)式知: $d=2^{\alpha}$,即 $d=m$.

3 小结与展望

长周期是判断随机数发生器好坏的一个不可缺少的条件,因此随机数发生器周期性的研究具有一定的意义. 本文主要就是研究一类比较流行的发生器 ——线性同余类发生器的周期,利用数论和有限域的一些结论严格地给出了此发生器达到满周期的条件证明.

下一步的工作将继续研究其它类型发生器的周期,以及各种组合类发生器的周期规律.

参考文献:

[1] Kao C and Tang H C. Systematic searches for good multiple recursive random number generators[J]. Computers and Operations Research, 1997, 24(10): 899 - 905.

[2] L'Ecuyer, P. Tables of linear congruential generators of different sizes and good laticce structure[J]. Mathematics of Computation, 1999, 68(225): 249 - 260.

[3] 高惠旋. 统计计算 [M]. 北京:北京大学出版社, 1995. 81 - 121.

[4] Knuth D E. The art of computer programming vol2: seminumerical algorithms, 3rd edition[M]. Addison-Wesley, 2002. 10 - 118.

【责任编辑:徐明忠】