计算物理——针对 LCG 的一点思考

白博臣

(四川大学　物理学拔尖计划)

摘　要

为了以后能摆大烂而创造了一个模板，为了展现转行效果而开始啊对对对对对对对对对对对对对对对对对

关键词：摆大烂、啊对对对

Abstract

Attention！If you input "different", the computer will output "different", but if you input "dif{}ferent", the computer will output "different"

1 LCG 简介

LCG(Linear congruential generator) 即线性同余发生器，是利用求余运算的随机数发生器。其递推公式为：

$$
\begin{aligned}
x_n &= (ax_{n-1} + c) \pmod{M}, \quad n = 1, 2, \ldots \\
&m\text{为模数；} 0 < m \\
&a\text{为乘数；} 0 \le a < m \\
&c\text{为增量；} 0 \le c < m \\
&x_0\text{为初始种子；} 0 \le x_0 < m
\end{aligned} \tag{1}
$$

得到的序列 x_n 为非负整数，$0 \le x_n \le M$。最后令 $R_n = x_n/M$，则 $R_n \in [0, 1)$，把 R_n 作为均匀随机数序列。该算法的基本思想是因为很大的整数前面的位数是重要的有效位数而后面若干位有一定随机性。因为线性同余法的递推算法仅依赖于前一项，序列元素取值只有 M 个可能取值，所以产生的序列 $x_0, x_1, x_2, \ldots$ 一定会重复。若存在正整数 n 和 m 使得 $x_n = x_m (m < n)$，则必有 $x_{n+k} = x_{m+k}, k = 0, 1, 2, \ldots$ 即 $x_n, x_{n+1}, x_{n+2}, \ldots$ 重复了 $x_m, x_{m+1}, x_{m+2}, \ldots$，称这样的 $n - m$ 的最小值 T 为此随机数发生器在初值 x_0 下的周期，易得，$T \le M$.

2 问题发现

本课程 EX12 要求复现 PPT 中的某个图像 (如下):

在复现过程中，发现两个奇怪的现象：

1. 针对图像中参数为 $m = 2^{31} - 1, a = 4, c = 1$ 的折线，我们发现初始值 (种子值) 对折线最后的收敛值有影响。

2. 针对图像中参数为 $m = 27, a = 26, c = 5$ 的折线，我们发现其收敛值根据种子值的不同最后稳定在两个值。

现对两个问题进行进一步阐述。

2.1 问题一阐述

当选取种子值 $x_0 = 1$ 时，我们可以得到 Figure2，而当我们更改种子值为 $x_0 = 12345678$ 时，得到的图像为 Figure3.

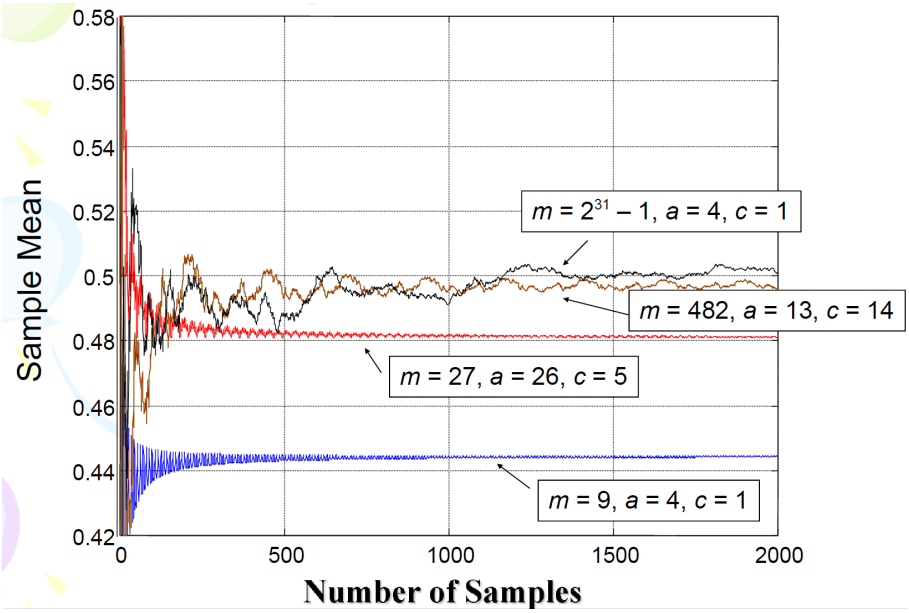

Figure 1: EX12 要求复现四组参数值下 LCG 的期望收敛性

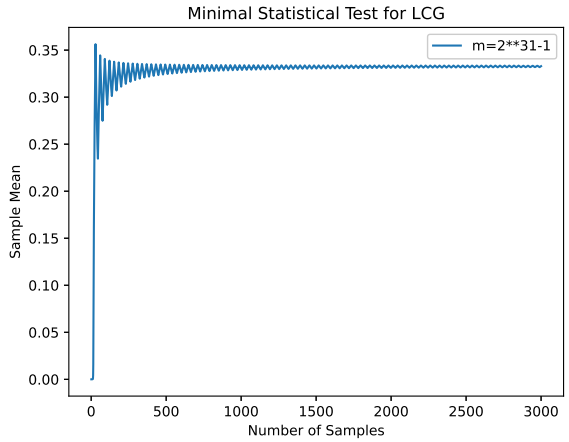

Figure 2: 种子值取 1 时，最后并没有收敛到 0.5，而是在 0.30.35 之间

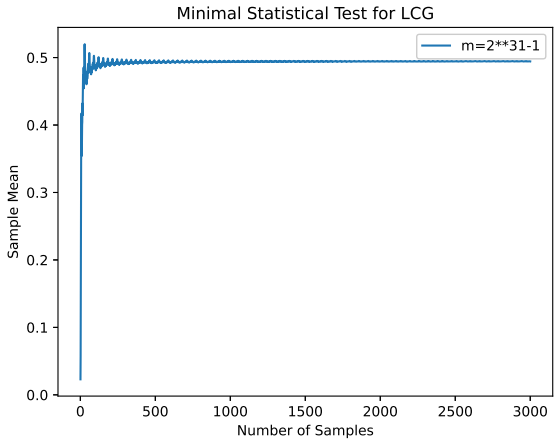

Figure 3: 种子值取 12345678 时，最后收敛到 0.5 左右，“成功”复现图像

通过调整种子值的大小我们可以控制最终随机数的期望，但是按照随机数的要求，我们不应该令随机数的期望与种子值有关 (至少应维持在 0.5 左右)。所以我对该组参数的选取持质疑态度，在后面问题解答中我将提出我的看法。

2.2 问题二阐述

当参数为 $m = 27, a = 26, c = 5$ 时，我们先选取种子值为 $x_0 = 4$ 得到 Figure4，再选取种子值为 $x_0 = 6$ 得到 Figure5.

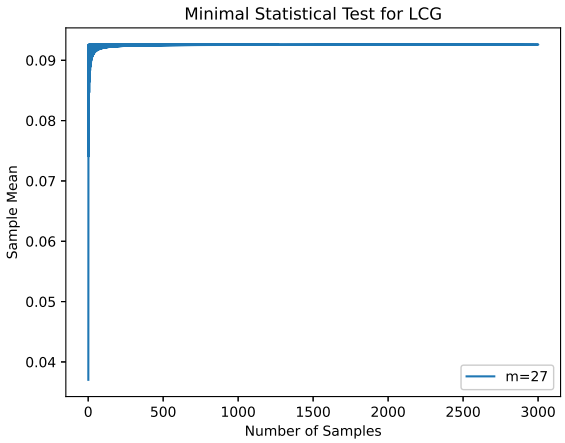

Figure 4: 种子值取 4 时，期望收敛到 0.1 左右

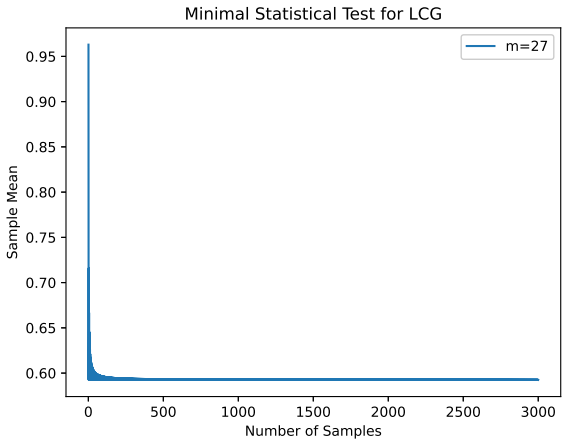

Figure 5: 种子值取 6 时，期望收敛到 0.6 左右

后续我们选取不同种子值，发现在 $x_0 \leq 5$ 时，最终期望均收敛到 0.1 左右，而对于 $x_0 > 5$ 时，最终期望值均收敛到 0.6 左右，不管如何改变种子值的选取，我们都发现该组参数下的期望值始终不会趋于 0.5 左右，无法复现题目中要求的图像。

3 问题解答

针对上述两个问题，我不得不从数学角度思考线性同余本身的一些特性，希望能够从中得出问题的解答。

3.1 数学求解

首先，我们可以先不考虑递推关系后的取余运算，而是直接先根据递推关系求得通项公式再取余运算，证明如下：

设 $x_n = x' + d * m$，其中 x' 是 x_n 模 m 后的余数，d 是整数，根据递推关系，

$$x_n = (ax_{n-1} + c)(modM)$$

代入后得：

$$x_n = (a(x'_{n-1} + d * m))(modM)$$

在取余运算中 $a * d * m$ 项被约去，所以先代入通项公式再取模与先取模再代入递推关系得到的结果是一样的。

所以线性同余递推关系可改写为：

$$x_{n+1} = a^n(x_0 + \frac{c}{a-1}) - \frac{c}{a-1} \tag{2}$$