

廣論32位元一階質數乘餘法亂數產生器

翁振益

銘傳大學企業管理學系

摘要

研究中分別利用理論與經驗測試窮舉搜尋32位元一階質數乘餘法亂數產生器最大十個質數，在滿足全週期的85億乘數中，只有36個乘數通過測試。這些乘數其統計性質佳，除此之外，週期長、執行效率高、具有重複性、可攜帶性及齊次性性質，是一理想的亂數產生器。組合法為未來研究亂數產生器之趨勢；同時這些乘數為組合法亂數產生器之基礎，透過這些乘數組合成新的亂數產生器。

關鍵詞：亂數產生器，理論測試，經驗測試，組合法產生器。

EXTENSIVE STUDY ON MULTIPLICATIVE CONGRUENTIAL RANDOM NUMBER GENERATORS OF ORDER ONE WITH PRIME MODULUS FOR 32-BIT MACHINES

Jehn-Yih Wong

Department of Business Administration
Ming Chuan University
Taipei, Taiwan 111, R.O.C.

Key Words: random number generator, theoretical test, empirical test, combined generators.

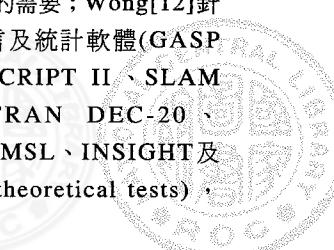
ABSTRACT

This paper presents the results of an exhaustive analysis of the one order multiplicative congruential random number (RN) generators with the ten largest prime moduli in 32-bit machines. Among the 8.5 billion multipliers which are able to produce RNs of a full period, thirty-six multipliers pass all the tests to possess good statistical properties. In addition, those generators devised in this paper possess the properties of long period, efficiency, repeatability, portability and homogeneity, and these properties are necessary for practical simulation use. These generators are also the basis of combined generators, which recently have received a great deal of attention.

一、前 言

Nance及Overstreet[1]指出亂數產生器的研究包含了電腦科學、離散數學、作業研究及統計學等四門學科；Knuth[2]亦指出亂數產生器廣泛應用在模擬、抽樣、數值分析及決策等方面。但多位學者[3-11]指出一些極普遍的

亂數產生器有其缺點，無法滿足實際的需要；Wong[12]針對目前常用的模擬軟體、程式語言及統計軟體(GASP IV、GPSS/H、GPSS/PC、SIMSCRIPT II、SLAM II、SIMPL/I、SIMAN、FORTRAN DEC-20、XCELL+、APL、SAS、SPSS、IMSL、INSIGHT及SIMFACTORY II.5) 做理論測試(theoretical tests)，



結果皆不夠理想。因此設計一理想之亂數產生器，是一件值得研究的事。

一個好的亂數產生器須符合隨機性(randomness)、長週期(long period)、效率高(efficiency)、可攜帶性(portability)、重覆性(repeatability)及齊次性(homogeneity)等性質[11,13,14]。目前一般產生亂數的方法以線性同餘法(linear congruential method)[2,6,15]的使用最為廣泛，而且已有完整的理論基礎，其模式為：

$$R_n = aR_{n-1} + c \bmod m \quad (1)$$

其中模數 m 、乘數 a 為正整數，種子 R_0 和增量 c 為非負整數。Marsaglia[8]指出若 $m=2^e$ ，其所產生出來的亂數不夠隨機，Ripley[14]亦指出此種亂數產生器的統計性質差，因此針對此一缺點可將 m 限制為質數，以改善此一現象，而且其所產生的週期可達 $m-1$ ，稱此方法為質數乘餘法(prime modulus multiplicative congruential generators)。其產生亂數的執行速度快，具有重覆性，可攜帶性及齊次性等性質。Knuth[2]認為此種亂數產生器具有極佳之性質，因此本研究針對模數為 $2^{31}-1$ 的一階質數乘餘法亂數產生器，做一分析研究。

有關乘餘法產生器較重要的研究有Kao[16]、Chang等[17]和Kao及Wong[18,19]對16位元一階質數乘餘法做一系列的研究；Atkinson[3]曾針對 $m=2^{35}$ 及選擇12個乘數的一階乘數乘餘法做理論與經驗測試(empirical tests)，並做一分析比較；Fishman[20]對 $m=2^{32}$ 的一階乘餘法做窮舉搜尋及對 $m=2^{48}$ 的一階乘餘法做部份搜尋，分別找出130及42個質譜值大於等於0.8的乘數。另外Fishman及Moore[5,6]和Wong[12]針對 $m=2^{31}-1$ 的一階質數乘餘法做討論。Marsaglia[21]指出模數為 $m=2^{31}-1$ 的亂數產生器並非是好的亂數產生器；另外L'Ecuyer[22]指出組合法(combination method)為未來亂數產生器之研究趨勢，32位元一階質數乘餘法的週期約為 2^{31} ，是組合法的基礎，若組合 k 個32位元一階質數乘餘法其週期最高可達 $2^{31 \times k}$ [7,23]，因此研究中針對不同的模數 m ，利用窮舉法對一階質數乘餘法做全域搜尋，其中模數 m 採用32位元中最大的十個質數，約有214.47億個乘數需要測試，分別利用理論與經驗測試檢定其隨機性，以找出具有很好的區域性(local)和整體性(global)統計性質的亂數產生器。一個理想之亂數產生器，滿足全週期及具備良好的統計性質是必要條件，因此以下二節加以說明討論。

二、全週期

本文所探討之亂數產生器為一階質數乘餘法，其模式為：

$$R_n = aR_{n-1} \bmod m \quad (2)$$

表一 不同模數所對應的質因數及全週期的乘數個數

模數 m	$m-1$ 的質因數	全週期的乘數個數
$2^{31}-1$	2、3、7、11、31、151、331	534600000
$2^{31}-19$	2、3、59652323	715827870
$2^{31}-61$	2、3、357913931	715827860
$2^{31}-69$	2、1073741789	1073741788
$2^{31}-85$	2、3、7、631、81031	612586800
$2^{31}-99$	2、7、76695841	920350080
$2^{31}-105$	2、3137、342283	1073396352
$2^{31}-151$	2、3、277、323027	713241408
$2^{31}-159$	2、67108859	1073741728
$2^{31}-171$	2、536870869	1073741736

其中模數 m 為質數，乘數 a 為 m 的質根，模數 m 採用32位元中最大的十個質數，分別是 $m=2^{31}-1$ 、 $2^{31}-19$ 、 $2^{31}-61$ 、 $2^{31}-69$ 、 $2^{31}-85$ 、 $2^{31}-99$ 、 $2^{31}-105$ 、 $2^{31}-151$ 、 $2^{31}-159$ 及 $2^{31}-171$ ，Knuth[2]指出，若 m 為一質數，其中 a 是質數 m 的質根，必須滿足[2]：

$$a^{\frac{m-1}{q}} \neq 1 \bmod m \quad (3)$$

q 為所有能整除 $m-1$ 之質數。質根的個數恰為小於 $m-1$ 且與 $m-1$ 互質的正整數個數[24]，滿足全週期 $m-1$ 的乘數個數為[2]：

$$N(m,1) = \varphi(m-1) = (m-1)(1-1/q_1)(1-1/q_2)\dots(1-1/q_n) \quad (4)$$

其中 $\varphi()$ 為尤拉函數(euler function)， q_1, q_2, \dots, q_n 為 $m-1$ 的質因數。

研究中由(3)式可以找到全週期的乘數，當 $m=2^{31}-1$ 時，則2、3、7、11、31及151為 $2^{31}-2$ 的質因數，(4)式可以算出全部的乘數個數，因此其乘數的個數為 $(2^{31}-1-1)(1-1/2)(1-1/3)(1-1/7)(1-1/11)(1-1/31)(1-1/151)(1-1/331)=534600000$ ；當 $m=2^{31}-171$ 時，則2及536870869為 $2^{31}-172$ 的質因數，其乘數的個數為 $(2^{31}-171-1)(1-1/2)(1-1/536870869)=1073741736$ 。由表一得知約有85億個乘數滿足全週期，其週期為 $m-1$ ，利用理論與經驗測試檢定其隨機性，分別敘述於下節。

三、統計測試

1. 理論測試

理論測試並不需要實際產生亂數數列，只要知道產生亂數的模式，即可加以評斷其優劣，因此理論測試可以評估此亂數數列的整體行為。所以必須利用有效率且適用於計算機的理論測試方法加以分析不同乘數的優劣性。最有

表二 32位元中不同模數所對應之乘數通過統計測試之結果

模數	乘數	質譜值	格子值	模數	乘數	質譜值	格子值
2147483587	6442956	.8328	1.4908	2147483587	77658649	.8307	1.5810
2147483587	188783834	.8339	1.6879	2147483587	1081137027	.8347	1.2096
2147483579	97168910	.8317	1.3004	2147483579	1203732352	.8341	1.4223
2147483563	179810926	.8330	1.6029	2147483563	1880963377	.8322	1.8867
2147483549	268379489	.8355	1.6218	2147483543	370263054	.8330	1.3331
2147483543	512158774	.8318	1.3381	2147483543	844142621	.8386	1.1838
2147483477	268399461	.8384	1.3237	2147483477	506863774	.8401	1.3685
2147483477	701820825	.8401	1.6140	2147483477	771565992	.8341	1.7640
2147483477	805270721	.8332	1.4136	2147483477	915607826	.8341	1.2705

名的理論測試方法是質譜檢定(spectral test)[25]，若

$$W_t = \{ W_{i,t} = (X_i, X_{i+1}, \dots, X_{i+t-1}), i=1,2,\dots \}$$

經標準化後，得到

$$U_t = \{ U_{i,t} = (X_i/m, X_{i+1}/m, \dots, X_{i+t-1}/m), i=1,2,\dots \}$$

則其目的是在 t 維空間中，找出一組涵蓋 U_t 中所有點之平行超平面族，並求出兩平行超平面間的最大距離 $d(t,m,a)$ 。Knuth[2]指出質譜檢定是目前所知道的檢定方法中最有效力者，因為不僅一些已知好的亂數產生器能通過此檢定，同時不好的亂數產生器確實無法通過此檢定。Knuth[2]提供一演算法，加以解決此問題。L'Ecuyer等[26]指出 $d(t,m,a)$ 之下限爲 $d^*(t,m)$ ，其值爲 $m^{-1/t}\gamma_t$ ， $\gamma_t=(4/3)^{1/4}、2^{1/6}、2^{1/4}、2^{3/10}$ 及 $(64/3)^{1/12}$ ，其中 $t=2,\dots,6$ 。經標準化後得到 $S(t,m,a)=d^*(t,m)/d(t,m,a)$ ，其值介於0與1之間，定義 $S = \min_t \{ S(t, m, a) \}$ 爲此模式的質譜值，當 S 越大時表示其隨機性越理想。

在質譜檢定中，維度 t 之考量亦依據Fishman及Moore [6]所採用的2至6。由於乘數 a 與 a^{-1} 產生相同的格子結構，所以在做質譜檢定時，只需取全部乘數個數的一半。經窮舉搜尋之後，十個最大質數分別有446、628、682、992、522、840、976、624、952及872質譜值大於等於0.8，由於質譜值沒有一定的衡量標準，本研究乃採用0.83爲臨界值。經窮舉搜尋，不同模數其質譜值大於0.83的個數分別有2、8、16、12、10、4、12、0、12及20個，其所找出的最大質譜值分別是0.8319、0.8355、0.8347、0.8443、0.8446、0.8355、0.8386、0.8263、0.8364及0.8410。

除了質譜檢定，格子檢定亦常用於理論測試中。若 $\alpha_1, \dots, \alpha_t$ 爲構成 t 維格子結構中的基底向量，Beyer等[27]和Marsaglia[8]提供一種測度方法：

$$R(t,m,a) = \max \{ |\alpha_i| \} / \min \{ |\alpha_i| \} \quad (5)$$

爲其格子值，來評估其格子形狀。 $R(t,m,a)$ 的理想值爲1，越接近1表示其隨機性越高。一般而言，當 $R(t,m,a)<2$ 時，表示具有好的格子形狀，當 $R(t,m,a)>=3$ ，表示其格子形狀不理想，Marsaglia[8]提供一演算法計算此問題。

本研究對滿足全週期且質譜值大於等於0.83的乘數進行格子檢定，所採用的維度從2至6。表二列出各乘數其模數值由大而小的排序結果，其中96個乘數的格子值，結果只有七個乘數的格子值大於2。由此可以確信，當一組乘數有較大的質譜值時，同時亦具有良好的格子形狀。去除此七個，以下測試89個乘數。研究中有關全週期的分析和各項統計檢定，皆利用FORTRAN語言在IBM PC 586 機器上完成。

2. 經驗測試

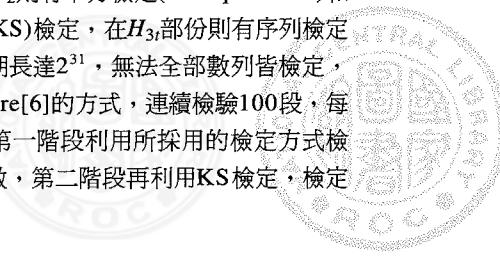
除了利用理論測試評估亂數數列的整體行爲之外，尚需要運用經驗測試以檢定其亂數數列的區域行爲，才能稱得上滿足統計上的隨機性。經驗測試必須實際將亂數數列產生出來，對此數列分段測試，再根據所得結果，評斷其區域行爲的優劣，研究中針對通過理論測試的89個乘數，再利用經驗測試加以檢定其區域行爲。經驗測試可分爲二類，一是檢定此數列之獨立性，二是檢定此數列是否爲均等分配，Fishman[28]將此歸納成3項假說：

H_1 : U_1, \dots, U_n 乃獨立且來自相同的分配。

H_2 : U_1, \dots, U_n 乃來自 $(0,1)$ 的均等分配。

H_3 : $\{ V_i = (U_{i-t+1}, \dots, U_i), i=1, \dots, n/t, n/t \text{ 為整數} \}$ ，乃來自 t 維單位正方體上的均等分配。

研究中在 H_1 部份有連檢定(runs test)和相關檢定(autocorrelation test)， H_2 則有卡方檢定(chi-square test)和Kolmogorov-Smirnov (KS)檢定，在 H_3 部份則有序列檢定(serial test)。由於全週期長達 2^{31} ，無法全部數列皆檢定，因此依據Fishman及Moore[6]的方式，連續檢驗100段，每段二十萬個亂數，首先第一階段利用所採用的檢定方式檢定每一區段二十萬個亂數，第二階段再利用KS檢定，檢定



100個區段所得的統計量是否滿足所需要的分配[29]，其中顯著水準採用 $\alpha=0.1$ 。

在卡方檢定中，區間數的決定對整個檢定的效力有著明顯的差異，Mann及Wald[30]提供了一種方式來決定區間數，其公式為：

$$I = 4\{2[(n-1)^2/z_{1-\alpha}]\}^{1/5} \quad (6)$$

其中 n 與 $Z_{1-\alpha}$ 分別代表樣本數和標準常態分配顯著水準為 $1-\alpha$ 的臨界值，Hamdan[31]指出Mann及Wald[30]所提出的方法，其檢定力保証可以達到 $1/2$ 。Kao及Tang[32]提出在多階質數乘餘法中，對於可以產生全週期的乘數，若將整個區間分成偶數個區間，假設共 $2s$ 個區間，其中前 s 個區間的第 i 段與後 s 個區間的第 i 段其卡方值相等，即前 s 個區間與後 s 個區間相互對稱，因此在作卡方檢定時，只須取一半的亂數個數。

研究中第一階段在卡方檢定部份，區間數的決定利用公式(6)求算，所得區間數，在卡方檢定、2維序列檢定及3維序列檢定分別是500、 20^2 及 7^3 ，因此，其統計量應分別服從自由度為499、399及342的卡方分配。連檢定的統計量近似自由度為6的卡方分配，相關檢定的統計量趨近於一標準的常態分配，研究中在相關檢定部份，考慮前3階，並採用3階統計量最差者。KS檢定的目的在檢定亂數數列的經驗分配與理論上的分配是否一致。其檢定的統計量為：

$$\begin{aligned} Dn^+ &= n^{1/2} \cdot \max_{1 \leq i \leq n} \{i/n - F(U_i)\} \\ Dn^- &= n^{1/2} \cdot \max_{1 \leq i \leq n} \{F(U_i) - (i-1)/n\} \end{aligned} \quad (7)$$

其中

$F(U_i)$ 是 $U(0,1)$ 的機率分配。

Dn^+ 與 Dn^- 的分配近似於 $F(x)=1-e^{-2x^2}$, $x>=0$ [2]。

第二階段再利用KS檢定，檢定其是否滿足所需要的分配。結果如表二所示，表二列出通過所有統計檢定以模數值由大而小排序之結果，共有36個乘數通過所有的檢定，這些乘數具有良好的統計性質。表二只列出 a 與 a^{-1} 之中較小的乘數，所以共有18個。其中 a^{-1} 的求算利用 $a^{-1}=a^{m-2}(\bmod m)$ 的演算法。

四、組合法亂數產生器

組合法乃利用二個或二個以上的亂數產生器組合成新的亂數產生器，Marsaglia[33]指出組合兩個獨立的亂數產生器，不但可以改善亂數數列的均勻性，而且可以改善亂數數列的獨立性，經由實證得知，組合的亂數產生器比較能通過較強的統計檢定。一般組合法有加法與攬合法二種。L'Ecuyer及Tezuka[34]指出，若有 J 個線性同餘產生器，則第 j 個線性同餘產生器之遞迴關係式為：

$$R_{j,i} = a_j R_{j,i-1} \bmod m_j \quad (8)$$

其中模數 m_j , $j=1,2,\dots,J$ 為互質的質數，乘數 a_j 為模數 m_j 的質根，則可以定義兩種的組合方式。第一種組合方式的遞迴關係式為：

$$Z_i = \sum_{j=1}^J \delta_j R_{j,i} \bmod m_i, \quad U_i = Z_i/m_i \quad (9)$$

其中 $\delta_1, \delta_2, \dots, \delta_J$ 為任意非零整數。例如L'Ecuyer[7]提出組合 $X_n=40014X_{n-1} \bmod 2147483563$ 及 $Y_n=40692Y_{n-1} \bmod 2147483399$ ，成為 $Z_n=X_n-Y_n \bmod 2147483563$ ，此時 $\delta_j=(-1)^{j-1}$ ，L'Ecuyer只針對 $a_j \leq \sqrt{m_j}$ 的乘數做討論，所以損失一些統計性質較佳之乘數。另外一種組合方式的遞迴關係式為：

$$W_i = \sum_{j=1}^J \delta_j R_{j,i}/m_j \bmod 1 \quad (10)$$

其中 $\delta_1, \delta_2, \dots, \delta_J$ 為任意非零整數。Deng等[35]提出此種組合方法的理論，且經由實證得知，確實能改善其均勻性和獨立性。例如Wichmann及Hill[23]提出組合 $X_n=171X_{n-1} \bmod 30269$ 、 $Y_n=172Y_{n-1} \bmod 30307$ 及 $Z_n=170Z_{n-1} \bmod 30323$ ，成為 $U_n=X_n/30269+Y_n/30307+Z_n/30323 \bmod 1$ ，此時 $\delta_j=1$ 。

L'Ecuyer[22]指出組合法為未來亂數產生器之研究趨勢，32位元一階質數乘餘法是組合法的基礎，其週期約為 2^{31} ，若組合 k 個32位元一階質數乘餘法其週期最高可達 2^{31k} [7,23]，因此研究中針對不同的模數 m ，利用窮舉法對一階質數乘餘法做全域搜尋，所找出之乘數，皆滿足好的亂數產生器所具備的性質。且可組合成新的亂數產生器。

五、結 論

研究中對32位元一階質數乘餘法模數 m 為最大十個質數做窮舉搜尋，在約有214.47億的乘數中，只有96個乘數其質譜值大0.83。當 $\alpha=0.1$ 時，有36個乘數通過所有的測試，由以上得知此36個乘數具備良好的整體性與區域性的性質。這些亂數產生器的週期約為 2^{31} ，符合隨機性且執行效率高，具有可攜帶性、重覆性及齊次性，滿足實際模擬之需要。L'Ecuyer[22]指出組合法為未來亂數產生器之研究趨勢，組合法亂數產生器，若透過這36個乘數的其中 k 個乘數，所組合而成的亂數產生器，其週期最高可達 2^{31k} 。

六、符號索引

a	乘數
c	增量
$F(U_i)$	$U(0,1)$ 的機率分配
m	模數



n	樣本數
R_0	種子
$R(t, m, a)$	格子值
S	質譜值
$Z_{1-\alpha}$	標準常態分配
$\varphi()$	尤拉函數

七、參考文獻

1. Nance, R. E. and C. Overstreet Jr., "Some Experimental Observation on the Behavior of Composite Random Number Generators," *Operations Research*, Vol. 26, No. 5, pp. 915-935 (1978).
2. Knuth, D. E., *The Art of Computer Programming*, Vol. 2: Semi-numerical Algorithms, 2nd ed., Addison-Wesley, Reading, MA (1981).
3. Atkinson, A. C., "Tests of Pseudo-Random Numbers," *Applied Statistics*, Vol. 29, No. 2, pp. 164-171 (1980).
4. Bratley, P., B. L. Fox, and L. E. Schrage, *A Guide to Simulation*, 2nd ed., Springer-Verlag, New York (1987).
5. Fishman, G. S. and L.R. Moore III, "A Statistical Evaluation of Multiplicative Congruential Random Number Generators with Modulus $2^{31}-1$," *Journal of American Statistical Association*, Vol. 77, No. 377, pp. 129-136 (1982).
6. Fishman, G. S. and L. R. Moore III, "An Exhaustive Analysis of Multiplicative Congruential Random Number Generators with Modulus $2^{31}-1$," *SIAM Journal on Scientific and Statistical Computing*, Vol. 7, No. 1, pp. 24-45 (1986).
7. L'Ecuyer, P., "Efficient and Portable Combined Random Number Generator," *Communications of the Association for Computing Machinery*, Vol. 31, No. 6, pp. 742-749 (1988).
8. Marsaglia, G., *The Structure of Linear Congruential Sequences*, in *Applications of Number Theory to Numerical Analysis* (edited by S.K. Zeremba), Academic Press, New York (1972).
9. Modianos, D. T., R. C. Scott and L. W. Cornwell, "Random Number Generation on Microcomputers," *Interfaces*, Vol. 14, No. 4, pp. 81-87 (1984).
10. Niederreiter, H., "Recent Trends in Random Number and Random Vector Generation," *Annals of Operations Research*, Vol. 31, No. 1-4, pp. 323-346 (1991).
11. Park, S. K. and K.W. Miller, "Random Number Generators: Good Ones Are Hard to Find," *Communications of the Association for Computing Machinery*, Vol. 31, No. 10, pp. 1192-1201 (1988).
12. Wong, J. Y., "Multiplicative Congruential Random Number Generators of Order One with Prime Modulus for 32-Bit Machines," *Journal of Technology*, Vol. 11, No. 4, pp. 563-568 (1996).
13. Marsaglia, G., A. Zaman, and W.W. Tsand, "Toward a Universal Random Number Generator," *Statistics and Probability Letters*, Vol. 9, No. 1, pp. 35-39 (1990).
14. Riply, B. D., "Thoughts on Pseudorandom Number Generators," *Journal of Computational and Applied Mathematics*, Vol. 31, No. 1, pp. 153-163 (1990).
15. Law, A. M. and W. D. Kelton, *Simulation Modeling and Analysis*, 2nd ed., McGraw-Hill, New York (1991).
16. Kao, C., "A Random Number Generator for Microcomputers," *Journal of the Operational Research Society*, Vol. 40, No. 7, pp. 687-691 (1989).
17. Chang, P. L., S. N. Hwang, and C. Kao, "Some Good Multipliers for Random Number Generators for 16-Bit Microcomputers," *Computers and Operations Research*, Vol. 21, No. 2, pp. 199-204 (1994).
18. Kao, C. and J. Y. Wong, "Several Extensively Tested Random Number Generators," *Computers and Operations Research*, Vol. 21, No. 9, pp. 1035-1039 (1994).
19. Kao, C. and J. Y. Wong, "An Exhaustive Analysis of Prime Modulus Multiplicative Congruential Random Number Generators with Modulus Smaller Than 2^{15} ," *Journal of Statistical Computation and Simulation*, Vol. 54, No. 1, pp. 29-35 (1996).
20. Fishman, G. S., "Multiplicative Congruential Random Number Generators with Modulus 2^b : an Exhaustive Analysis for $b=32$ and a Partial Analysis for $b=48$," *Mathematics of Computation*, Vol. 54, No. 189, pp. 331-334 (1990).
21. Marsaglia, G., "Remark on Choosing and Implementing Random Number Generators," *Communications of the Association for Computing Machinery*, Vol. 36, No. 7, pp. 105-108 (1993).
22. L'Ecuyer, P., "Recent Advances in Uniform Random Number Generation," *Proceedings of the 1994 Winter Simulation Conference*, pp. 176-183 (1994).
23. Williams, C. A. and I. D. Hill, "An Efficient and Portable Pseudo-Random Number Generator," *Applied Statistics*, Vol. 31, No. 2, pp. 188-190 (1982).
24. Hardy, G. H. and E. M. Wright, *The Theory of Number*, 4th ed. Clarendon Press, Oxford (1962).

25. Coveyou, R. R. and R. D. MacPherson, "Fourier Analysis of Uniform Random Number Generators," *Journal of Association for Computing Machinery*, Vol. 14, No. 1, pp. 100-119 (1967).
26. L'Ecuyer, P. and F. Blouin, "Linear Congruential Generators of Order $k > 1$," Proceedings of the 1988 Winter Simulation Conference, pp. 432-439 (1988).
27. Beyer, W. A., R. B. Roof and D. Williamson, "The Lattice Structure of Multiplicative Congruential Pseudo-Random Vectors," *Mathematics of Computation*, Vol. 25, No. 114, pp. 345-363 (1971).
28. Fishman, G. S., *Principles of Discrete-Event Simulation*, John Wiley, New York (1978).
29. Collings, B. J., "Compound Random Number Generators," *Journal of American Statistical Association*, Vol. 82, No. 398, pp. 525-527 (1987).
30. Mann, H. B. and A. Wald, "On the Choice of the Number of Intervals in the Application of the Chi-Square Test," *Annals of Mathematical Statistics*, Vol. 13, pp. 306-317 (1942).
31. Hamdan, M. A., "The Number and Width of Classes in the Chi-Square Test," *Journal of American Statistical Association*, Vol. 58, No. 303, pp. 678-689 (1963).
32. Kao, C. and H.C. Tang, "Symmetry Property of Multiplicative Congruential Random Number Generator in Chi-Square Test," *International Journal of Computer Mathematics*, Vol. 55, No. 1-2, pp. 113-118 (1995).
33. Marsaglia, G., "A Current View of Random Number Generation," *Proceedings of sixteenth Symposium on the Interface*, pp. 3-10 (1985).
34. L'Ecuyer, P. and S. Tezuka, "Structural Properties for Two Classes of Combined Random Number Generators," *Mathematics of Computation*, Vol. 57, No. 196, pp. 735-746 (1991).
35. Deng, L.Y., E.O. George, and Y.C. Chu, "On Improving Pseudorandom Number Generators," Proceedings of the 1991 Winter Simulation Conference, pp. 1035-1042 (1991).

86年03月16日 收稿
 86年06月02日 初審
 86年06月12日 複審
 86年06月20日 接受

