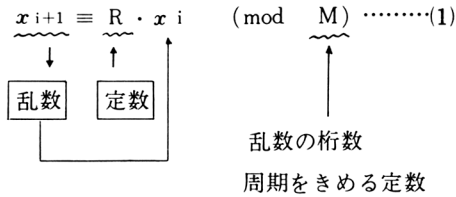


$$\begin{aligned} \text{解} \quad x &\equiv 7+6 \pmod{12} & x &= 1 \\ x &\equiv 3+12 \pmod{12} & x &= 3 \\ 2 &\equiv x+5 \pmod{12} & x &= 9 \\ 6 &\equiv x+8 \pmod{12} & x &= 10 \end{aligned}$$

Ⅲ) 乗算式合同法

初期値： x_0



〔式の意味〕Rに x_i をかけ、その結果をMで割りその余りを x_{i+1} とする。

計算機では、 x_i に初期値が入ってできた乱数 x_{i+1} を x_i に入れる。以上をくり返す。

〔例〕(1) 式に初期値 $x_0 = 32868, R = 3125$
 $M = 10^4$ を入れると下表の通りになる。

i	$R \cdot x_i$	x_{i+1}
0		32768
1	102334464	4464
2	13941072	1072
3	3347855	7855
4	54231165	1165
5	3638295	8295
:	:	:
:	:	:
9	26882784	2784
10	8694432	4432

この場合の周期は、 $P = 5 \cdot 10^{4-2} = 500$ となるので、上表の $i = 500$ になると、1回目にもどる。すなわち同じ乱数がくり返される。

Ⅳ) 乗算合同法の条件

I B M社「データ処理技術」(1959)によれば乗算式合同法は、次のような手順と条件のもとで使うのがよいとされている。よいというのは、プログラムの簡便さ、計算機の負担の軽さ、処理速度が速いなどのことである。

(1) 1語がbビットの2進演算計算機の場合

- ①初期値 x_0 として正の奇数
- ②定数Rとして2になるべく近く
 $R = 8t \pm 3$ (tは正の整数)
 を満たすものを選ぶ。

③次の計算をくり返す

$$x_{i+1} \equiv R \cdot x_i \pmod{2^b}$$

$R \cdot x_i$ は処理後2ビットとなり、その下のbビットを x_{i+1} に当てる。

(その際、計算機によっては、負の符号がついたり、オーバーフローとして扱われたり、エラーになったりする場合があるから注意すること)

④これによって x_i の系列は

1から $2^b - 1$ の間に一様に分布する正の整数の一様分布乱数が求まる。

(通常これを0から 2^b の一様分布乱数といっていることが多い)

⑤一様分布乱数列の周期Pは

$$P = 2^{b-2} \text{ となる。}$$

(2) 1語がdディジット(桁)の10進演算機の場合

①初期値 x_0 として、2および5で割りきれない正の整数を選ぶ。

②定数Rとして $10^{d/2}$ になるべく近く

$$R = 200t \pm r \quad (t \text{ は正の整数})$$

を満たすものを選ぶ。ただし

$$r = 3, 11, 13, 19, 21, 27, 29, 37, 53$$

$$59, 61, 67, 69, 77, 83, 91$$

のうちから1つ選ぶものとする。

③次の計算をくり返す。

$$x_{i+1} \equiv R \cdot x_i \pmod{10^d}$$

$R \cdot x_i$ は2dディジット(桁)になる。

そのd桁を x_{i+1} とする。

(計算機によっては若干の注意が必要である。)

④これによって x_i の系列は

1から $10^d - 1$ の間に一様に分布する整数の一様分布乱数が求まる。

⑤一様分布乱数の周期Pは

$$P = 5 \cdot 10^{d-2} \text{ となる。}$$

4 乗算合同式による乱数作成実習

乱数発生プログラミングに際し留意すべきこ