**6.3 Generation of random values.**
(Previous reading: statistical concepts: 3.1, distributions 3.3, and computer arithmetic Appendix 2).
In stochastic models it is necessary to have procedures that generate random values with a given distribution. It will be seen that values with the distributions important in simulation, can be generated from numbers with the **uniform distribution.**

A succession of $n$ random numbers with integer values between 0 and $M$ is a set of values, each is the value of a random variable of the succession $X_1, X_2, ..., X_n$, in which each variable may take integer values with equal probability in the range from 0 to $M$. If $M = 99$ a possible series would be the $n$ numbers: 28, 3, 74, 0, 15, 99, 28,. . .,9,33.
But a succession as 1,35,1,35,1,35,1,35,. . . ,1,35 although it may be possible, it is not considered a "good" succession.
In practice some properties are required:

1. It is expected that in a long succession all the numbers will appear with a frequency that tends to be equal as the length of the succession increases.

2. The self-correlation of the succession (correlation between the given series and the series obtained from it by eliminating in the first one some numbers at the beginning) must tend to zero as the length of the series increases. So in the previous example the correlation coefficient of the series:
$x_i = 28,\ 3,\ 74,\ \ 0,\ 15,\ 99,. \ldots .,9,$
$y_i = 3,\ 74,\ \ 0,\ 15,\ 99,. . . . .,9,\ 33.$ That is to say: $y_i = x_{i+1}$. The value:

$$\rho_1 = \frac{\sum_{i=1}^{m} xy - \frac{1}{m}\sum_{i=1}^{m} x \sum_{i=1}^{m} y}{\sqrt{\sum_{i=1}^{m} x^2 - \frac{1}{m}(\sum_{i=1}^{m} y)^2} \times \sqrt{\sum_{i=1}^{m} y^2 - \frac{1}{m}(\sum_{i=1}^{m} y)^2}}$$

, where $m$ is the length of the series, is called **self-correlation coefficient of first order** (one place was displaced). By displacing 2,3,.. places, self-correlation of second, third,…,order may be obtained. For true random numbers, all must tend to zero as the length of the series increases. This means that each value is not correlated with the previous ones.

3. Dividing the series in successive groups of $k$ numbers and considering each group as a point in the space $R^k$ the points must show an uniform and irregular distribution.

More conditions of this sort and more general criteria of randomness can be found in Knuth 1969. An algorithmic approach to the definition of randomness of a series can be seen in Chaitin 1990.

The above definition is not useful to generate a succession with the computer that is a deterministic machine. So, other approaches to have random numbers available in the computer must be found.

**6.3.1 Pseudo-random numbers with uniform distribution.**

To have a large table of random numbers (obtained, for example from roulette and lottery results) is not a good idea. They have to be stored in mass memory peripherals of low speed access and would maintain a lot of memory used only for simulation applications. To have an special device such a detector of particles from a radioactive material or an electronic device with random noise are not practical solutions. First, because a special equipment would be needed for only one type of application. Second, because the generated series are nor repeatable, and repeatability is, as it will be seen in chapter 9, a desirable property to analyze results of simulation experiments. One proposed method, is to take the time given by the clock of the computer and made some mathematical operation in it to transform the value in a number in the interval (0,1). This method has the problem that the series obtained is not repeatable.

**Congruential methods.**

Since the origin of computers and Montecarlo methods some operations were used to produce successions of numbers that have some random appearance.

A simple algorithm is the following:

1. Fix a value $m$ called the **module**, and a number $a$ called the **multiplier**, both positive integers.

2. Start with a certain positive integer number $r_1$ (called **seed**) from which all the others will be generated. $r_1$ is the first number of the series of the $r_i$ to be generated.

3. Multiply the actual number $r_i$ of the series by $a$ and take the product "module $m$", i.e. **take the rest of the integer division** of $ar_i$ by the integer $m$. This is the following number of the series. The law of generation of the succession is:

$$r_{i+1} = ar_i \bmod(m) \text{ where } i = 1,2,3,....$$

**Example.** If $a = 23,\ r_1 = 31, m = 100$ the series is:

| | |
|---|---|
| | $r_1 = 31$ |
| $31 \times 23 = 713$ | $r_2 = 13$ (713/100=71 remainder 13 |
| $13 \times 23 = 299$ | $r_3 = 99$ |
| $99 \times 23 = 2277$ | $r_4 = 77$ |
| $77 \times 23 = 1171$ | $r_5 = 71$ |
| . . . . . | |
| $39 \times 23 = 897$ | $r_{20} = 97$ |
| $97 \times 23 = 2231$ | $r_{21} = 31 = r_1$ since here the series repeats. |

The remainders are in the interval from 1 to 99.

In the interval (1,99) 20 numbers has been obtained. The complete series is:
(31,13,99,77,71,33,59,57,11,53,19,37,51,73,79,17,91,93,39,97)

that do not appear to have any regularity. However, the series repeat after 20 numbers, they are all odd and all are different, and the extremes 0 and 100 are never obtained. Not a very pleasant behavior for truly random numbers. Nevertheless, by selecting carefully the $r_1, a$ and $m$, (using results from Number Theory) periods of billions of different numbers are obtained. As the interest are in real numbers between 0 and 1 (excluding these two values) the number must be divided by $m$. In the example the numbers $r_i / m$ would be:
0.31,0.13,0.99,. . .,0.97.
when the period is of several billions, the numbers can have 10 figures, which made their reduction to the interval (0,1) very dense (remember that all the integers generated are different) some of them are very near to 0 and others to 1. Some of the decimal numbers are equal because the rounding process, when the calculated $r_i / m$ is transformed in a floating point number that can be represented in the system, will make some numbers with different $r_i$ produce the same floating point decimal number. As all the $r_i$ are different they cover the whole range from 1 to $m-1$ in an uniform way, and the numbers $r_i / m$, when $m$ is large covers uniformly the interval (0,1). That is only an approximation because the floating-point numbers in the computer are not equidistant (see Forsythe et al. 1977 cited in Chapter 4). However in small equal sub-intervals of (0,1) will fall approximately equal quantities of random numbers.
Usually, the number of random numbers used in a simulation run is less than the period length. Starting with different seeds, different series are obtained that correspond to different parts of the period. If the generator algorithm is a good one, this parts are not correlated. This is very important in simulation. When replications of runs of the same model are made, different seeds may be used, and the runs may produce different results that may be attributed to the random factors in the simulated system.
Note that the simulation is seen to be strictly deterministic if the pseudo random generator algorithm and the seed is added to the model (Zeigler 2000), but it is a deterministic process that imitates the random behavior of the system.
The simulation oriented and the general-purpose languages have procedures that return a different pseudo-random number with uniform distribution in the interval (0,1) each time they are called.

### 6.3.2 Random number generation.

It is not possible to expose here all the theorems of Number Theory to prove the following results (see Knuth 1969). The two following theorems are useful:

**T1**. The series $r_{n+1} = (ar_n + c) \bmod(m)$ (linear congruence)
where all the values are positive integers, has period $m$ if and only if:
i) $c$ is prime respect to $m$. ($c$ and m have not common divisors)
ii) $a-1$ is multiple of any prime that divide $m$.
iii) if $m$ is multiple of 4, so it is $a-1$.

To increase the computing speed, $c$ may be taken equal to 0. That is called multiplicative congruence. The period cannot be $m$ because there are not 0 values in the series. In this case, the following theorem may be useful (all the quantities are positive integers)

:

**T2**. The maximum period of $r_{n+1} = ar_n \bmod(m)$ if $m = p^d$ ($p$ prime)
is obtained if:

a) $x_0$ is prime respect to $m$

b) some of the following cases occur:

i) $p^d = 2^d$ and $a \bmod(8) = 3$ or 5. The period length is $2^{d-2}$

ii) $p \neq 2$ and $d = 1$, and $a$ is not a multiple of $p$ and $a^{\frac{p-1}{q}} - 1$ is not divisible by $p$ for any prime $q$ divisor of $p-1$.

iii) $p$ odd and $d > 1$, and $a$ satisfy the condition ii) and $a^{p-1} - 1$ is not divisible by $p^2$.

The maximum period in ii) and iii)is $p^{d-1}(p-1)$ so if $p$ is prime a period of length $p-1$ or more can be obtained.

$a$ may be chosen in such a way that the serial correlation is minimized. Conveyu ### has shown that in the multiplicative case the self-correlation coefficient is: $\frac{1}{a} - \frac{a}{m}$, which is minimum in absolute value if $a^2 = m$ or $a = \sqrt{m}$.

See exercises 13, 14.

After the generator is designed, tests of the randomness must be done. See Knuth 1969 or xxx 19## for some of these tests. The tests consist in designing a function from the numbers in the series which will generate another series whose randomness can be tested. Of course, there must be functions that will produce non-random values. A trivial example for the numbers from the succession $r_{n+1} = ar_n \bmod(m)$ would be the function: $y_n = \frac{ar_n \bmod(m)}{r_{n+1}}$ that is not random at all.

### 6.3.2 Generation of random values from a given distribution.

From the random numbers $r$ with uniform distribution in (0,1), values corresponding with certain probability function can be generated. In the following, the $r$ or $r_i$ are random numbers with uniform distribution in (0,1). Some methods require more than one r value. As is seen this may be a problem when certain variation reduction methods are applied to obtain better results of the simulation.

**1. General uniform distribution**. To obtain values $u$ from an uniform probability function in the interval (a,b) the following transformation can be applied:

$$u = a + (b-a)r$$

The product expands the interval from (0,1) to $(0, b-a)$ the adition displace it $a$ to the right.

**Example.** The numbers $3 + 5r$ are uniformely distributed between 3 and 8.

**2. Arbitrary bounded distribution. Rejection technique.** If $f(u)$ is a probability function defined in $(a,b)$ and $\max(f(x)) \le m$ values from the corresponding distribution are obtained as follows:
i) generate $u_1$ uniformly distributed in $(a,b)$ and $u_2$ uniformly distributed in $(0,m)$
ii) if $u_2 \le f(u_1)$ then accept $u_1$ as the value, otherwise reject both an go to i).
Note that the probability of acceptation is proportional to $f(u_1)$, so that, the accepted numbers will have this distribution. See figure 2.
The efficiency of the method can be improved including the function in a majorizing function $g(x) \ge f(x)$ of known area, instead of a rectangle. The rejection region is that between the two functions.

**3. Distribution function with inverse.** If it is possible to find the inverse $F^{-1}(x)$ of the distribution function $F(x)$ then the values $u = F^{-1}(r)$ have the $F$ as a distribution function. The function distribution of the $u$ so obtained is:

| | |
|---|---|
| $\text{Prob}(u \le x)$ | by definition of distribution function |
| $= \text{Prob}(F^{-1}(r) \le x)$ | by definition of $u$ |
| $= \text{Prob}(r \le F(x))$ | by applying $F$ (which is monotone) to both members of inequality |
| $= F(x)$ | by the uniform distribution of $r$ and from $0 \le F(x) \le 1$ (given a value $s$ between 0 and 1, the probability that $r \le s$ is $s$). |

Comparing the first and last members shows that the distribution of the $u$ is $F$.
The above formula for general uniform distribution is a particular application of this method (see exercise 15).
One advantage of the inversion method is that it uses only one random number and the obtained random variate is a monotone function of the random number. This is important in some variance reduction methods (see 9.5).
Some examples of the application of the method, very useful in simulation follows.

**Example. Exponential distribution.** For the numbers with exponential distribution and mean $m$ it was shown (3.2 and 6.2.2) that $F(x) = 1 - e^{-x/m}$. From this the inverse function results $x = -m\ln(1-F)$. Then the numbers $x = -m\ln(1-r)$ have exponential distribution. Because the numbers $r$ and $1-r$ have the same distribution it results that the values: $u = -m\ln r$ have exponential distribution.

**Example. Function of probability given by a table.**
**a) Discrete variable.**
Probability that the arrived ship were of one of the different types: A, B. C, D, E.

| $t$ | A | B | C | D | E |
|---|---|---|---|---|---|
| $p(t)$ | 0.1 | 0.3 | 0.4 | 0.1 | 0.1 |

Distribution function

| $t$ | A | B | C | D | E |
|---|---|---|---|---|---|

| $F(t)$ | 0.1 | 0.4 | 0.8 | 0.9 | 1.0 |
|---|---|---|---|---|---|

this is a stair function. The inverse is a relation in which to each probability interval corresponds a type:

| Probability interval | 0.0 to <0.1 | 0.1 to <0.4 | 0.4 to <0.8 | 0.8 to <0.9 | 0.9 to $\leq 1.0$ |
|---|---|---|---|---|---|
| Value of $t$ | A | B | C | D | E |

If the random number is $r = 0.61$ (in the third interval) the random value of $t$ =C.
The figure 3 shows clearly the application of the inverse function method to this case.
The method applies to any ordinal scale. The values of the variable that in this case are nominal (see 3.1) are considered ordinal for the purpose of the calculus. The statistic results do not depend of the order in which they are put.

**b) Random values from a frequency table.**
For 100 workers the values of times to accomplish a certain work are represented by the frequency table:

| $x_i$ to $x_{i+1}$ | 80-90 | 90-100 | 95-110 | 110-120 | 120-130 |
|---|---|---|---|---|---|
| $f_i$ | 7 | 19 | 32 | 37 | 5 |

(7 workers finish in a time from 80 to less than 90 minutes, 19 in a time from 90 to less than 100, etc.)
The accumulated frequencies (how many takes a time less than $x$) are:

| | $x_1$ | $x_2$ | $x_3$ | $x_4$ | $x_5$ | $x_6$ |
|---|---|---|---|---|---|---|
| | 80 | 90 | 100 | 110 | 120 | 130 |
| $F_i$ | 0 | 7 | 26 | 58 | 95 | 100 |

between two successive values of $x_i$, $F_i$ changes linearly (see figure 4) . To apply the inverse function method the equations of the line $F_i$ for each interval must be found:

$$F(x) = \frac{F_i(x_{i+1}) - F_i(x_i)}{x_{i+1} - x_i}(x - x_i) + F_i(x_i)$$

According to the inverse function method this must be equated to a random value from a uniform distribution. Then a random value R from a uniform distribution between 0 and the maximum $F_i$ (100 in the example) is found. Then the $i$ interval is found for which:

$$F_i(x_i) < R \leq F_i(x_{i+1})$$

The random value for a variable with such frequency distribution is therefore:

$$x = x_i + \frac{R - F_i(x_i)}{F_i(x_{i+1}) - F_i(x_i)}(x_{i+1} - x_i)$$

In our example for a $r = 0.7$ results $R = 0 + 0.7(100 - 0) = 70$ . It is found $i = 4$
Since, from the table: $F_4(110) = 58 < 70 < 95 = F_4(120)$

$$x = 110 + \frac{70 - 58}{95 - 58}(120 - 110) = 113.2$$

The method can be used in frequency tables with intervals of different sizes.
See exercise 16.