7

Random-Number Generation

Random numbers are a necessary basic ingredient in the simulation of almost all discrete systems. Most computer languages have a subroutine, object, or function that will generate a random number. Similarly, simulation languages generate random numbers that are used to generate event times and other random variables. This chapter describes the generation of random numbers and their subsequent testing for randomness. Chapter 8 shows how random numbers are used to generate a random variable for many probability distributions.

7.1 Properties of Random Numbers

A sequence of random numbers, $R_1, R_2, \ldots,$ must have two important statistical properties, uniformity and independence. Each random number R_i is an independent sample drawn from a continuous uniform distribution between zero and 1. That is, the pdf is given by

$$f(x) = \begin{cases} 1, & 0 \le x \le 1 \\ 0, & \text{otherwise} \end{cases}$$

This density function is shown in Figure 7.1. The expected value of each R_i is given by

$$E(R) = \int_0^1 x\,dx = \left.\frac{x^2}{2}\right|_0^1 = \frac{1}{2}$$

and the variance is given by

$$V(R) = \int_0^1 x^2 dx - [E(R)]^2 = \left.\frac{x^3}{3}\right|_0^1 - \left(\frac{1}{2}\right)^2 = \frac{1}{3} - \frac{1}{4} = \frac{1}{12}$$

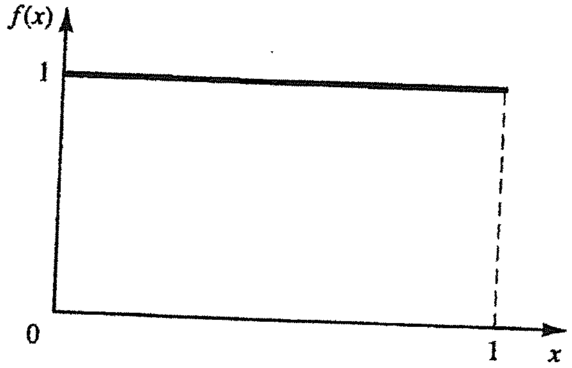

Figure 7.1. The pdf for random numbers.

Some consequences of the uniformity and independence properties are the following:

1. If the interval $(0, 1)$ is divided into n classes, or subintervals of equal length, the expected number of observations in each interval is N/n, where N is the total number of observations.
2. The probability of observing a value in a particular interval is independent of the previous values drawn.

7.2 Generation of Pseudo-Random Numbers

Notice that the title of this section has the word "pseudo" in it. "Pseudo" means false, so false random numbers are being generated! In this instance, "pseudo" is used to imply that the very act of generating random numbers by a known method removes the potential for true randomness. If the method is known, the set of random numbers can be replicated. Then an argument can be made that the numbers are not truly random. The goal of any generation scheme, however, is to produce a sequence of numbers between zero and 1 which simulates, or imitates, the ideal properties of uniform distribution and independence as closely as possible.

When generating pseudo-random numbers, certain problems or errors can occur. These errors, or departures from ideal randomness, are all related to the properties stated previously. Some examples include the following:

1. The generated numbers may not be uniformly distributed.
2. The generated numbers may be discrete-valued instead of continuous-valued.
3. The mean of the generated numbers may be too high or too low.
4. The variance of the generated numbers may be too high or too low.

5. There may be dependence. The following are examples:

   (a) Autocorrelation between numbers.

   (b) Numbers successively higher or lower than adjacent numbers.

   (c) Several numbers above the mean followed by several numbers below the mean.

Departures from uniformity and independence for a particular generation scheme may be detected by tests such as those described in Section 7.4. If such departures are detected, the generation scheme should be dropped in favor of an acceptable generator. Generators that pass all the tests in Section 7.4, and even more stringent tests, have been developed; thus, there is no excuse for using a generator that has been found to be deficient.

Usually, random numbers are generated by a digital computer as part of the simulation. Numerous methods can be used to generate the values. In selecting among these methods, or routines, there are a number of important considerations:

1. The routine should be fast. Individual computations are inexpensive, but simulation may require many hundreds of thousands of random numbers. The total cost can be managed by selecting a computationally efficient method of random-number generation.

2. The routine should be portable to different computers, and ideally to different programming languages. This is desirable so that the simulation program produces the same results wherever it is executed.

3. The routine should have a sufficiently long cycle. The cycle length, or period, represents the length of the random-number sequence before previous numbers begin to repeat themselves in an earlier order. Thus, if 10,000 events are to be generated, the period should be many times that long.

   A special case of cycling is degenerating. A routine degenerates when the same random numbers appear repeatedly. Such an occurrence is certainly unacceptable. This can happen rapidly with some methods.

4. The random numbers should be replicable. Given the starting point (or conditions), it should be possible to generate the same set of random numbers, completely independent of the system that is being simulated. This is helpful for debugging purposes and is a means of facilitating comparisons between systems (see Chapter 12). For the same reasons, it should be possible to easily specify different starting points, widely separated, within the sequence.

5. Most important, and as indicated previously, the generated random numbers should closely approximate the ideal statistical properties of uniformity and independence.

Inventing techniques that seem to generate random numbers is easy; inventing techniques that really do produce sequences that appear to be independent, uniformly distributed random numbers is incredibly difficult. There is now a vast literature and a rich theory on the topic, and many hours of testing have been devoted to establishing the properties of various generators. Even when a technique is known to be theoretically sound, it is seldom easy to implement it in a way that will be fast and portable. Therefore, this chapter aims to make the reader aware of the central issues in random-variate generation in order to enhance understanding and to show some of the techniques that are used by those working in this area.

7.3 Techniques for Generating Random Numbers

The linear congruential method of Section 7.3.1 is the most widely used technique for generating random numbers, so we describe it in detail. We also report an extension of this method that yields sequences with a longer period. Many other methods have been proposed, and they are reviewed in Bratley, Fox, and Schrage [1987], Law and Kelton [2000], and Ripley [1987].

7.3.1 Linear Congruential Method

The linear congruential method, initially proposed by Lehmer [1951], produces a sequence of integers, $X_1, X_2, \ldots$ between zero and $m - 1$ according to the following recursive relationship:

$$X_{i+1} = (aX_i + c) \bmod m, \quad i = 0, 1, 2, \ldots \tag{7.1}$$

The initial value X_0 is called the seed, a is called the constant multiplier, c is the increment, and m is the modulus. If $c \neq 0$ in Equation (7.1), the form is called the *mixed congruential method*. When $c = 0$, the form is known as the *multiplicative congruential method*. The selection of the values for a, c, m, and X_0 drastically affects the statistical properties and the cycle length. Variations of Equation (7.1) are quite common in the computer generation of random numbers. An example will illustrate how this technique operates.

EXAMPLE 7.1

Use the linear congruential method to generate a sequence of random numbers with $X_0 = 27, a = 17, c = 43$, and $m = 100$. Here, the integer values generated will all be between zero and 99 because of the value of the modulus. Also, notice that random integers are being generated rather than random numbers. These random integers should appear to be uniformly distributed on the integers zero to 99. Random numbers between zero and 1 can be generated by

$$R_i = \frac{X_i}{m}, \quad i = 1, 2, \ldots \tag{7.2}$$

The sequence of X_i and subsequent R_i values is computed as follows:

$$X_0 = 27$$

$$X_1 = (17 \cdot 27 + 43) \bmod 100 = 502 \bmod 100 = 2$$

$$R_1 = \frac{2}{100} = 0.02$$

$$X_2 = (17 \cdot 2 + 43) \bmod 100 = 77 \bmod 100 = 77$$

$$R_2 = \frac{77}{100} = 0.77$$

$$*[3pt]X_3 = (17 \cdot 77 + 43) \bmod 100 = 1352 \bmod 100 = 52$$

$$R_3 = \frac{52}{100} = 0.52$$

$$\vdots$$

Recall that $a = b \bmod m$ provided that $(a - b)$ is divisible by m with no remainder. Thus, $X_1 = 502 \bmod 100$, but 502/100 equals 5 with a remainder of 2, so that $X_1 = 2$. In other words, $(502 - 2)$ is evenly divisible by $m = 100$, so $X_1 = 502$ "reduces" to $X_1 = 2 \bmod 100$. (A shortcut for the modulo, or reduction operation for the case $m = 10^b$, a power of 10, is illustrated in Example 7.3.) ◀

The ultimate test of the linear congruential method, as of any generation scheme, is how closely the generated numbers $R_1, R_2, \ldots$ approximate uniformity and independence. There are, however, several secondary properties which must be considered. These include maximum density and maximum period.

First, notice that the numbers generated from Equation (7.2) can only assume values from the set $I = \{0, 1/m, 2/m, \ldots, (m - 1)/m\}$, since each X_i is an integer in the set $\{0, 1, 2, \ldots, m - 1\}$. Thus, each R_i is discrete on I, instead of continuous on the interval [0, 1]. This approximation appears to be of little consequence, provided that the modulus m is a very large integer. (Values such as $m = 2^{31} - 1$ and $m = 2^{48}$ are in common use in generators appearing in many simulation languages.) By maximum density is meant that the values assumed by $R_i, i = 1, 2, \ldots,$ leave no large gaps on [0, 1].

Second, to help achieve maximum density, and to avoid cycling (i.e., recurrence of the same sequence of generated numbers) in practical applications, the generator should have the largest possible period. Maximal period can be achieved by the proper choice of a, c, m, and X_0 [Fishman, 1978; Law and Kelton, 2000].

- For m a power of 2, say $m = 2^b$, and $c \neq 0$, the longest possible period is $P = m = 2^b$, which is achieved provided that c is relatively prime to m (that is, the greatest common factor of c and m is 1), and $a = 1 + 4k$, where k is an integer.

- For m a power of 2, say $m = 2^b$, and $c = 0$, the longest possible period is $P = m/4 = 2^{b-2}$, which is achieved provided that the seed X_0 is odd and the multiplier, a, is given by $a = 3 + 8k$ or $a = 5 + 8k$, for some $k = 0, 1, \ldots$.
- For m a prime number and $c = 0$, the longest possible period is $P = m-1$, which is achieved provided that the multiplier, a, has the property that the smallest integer k such that $a^k - 1$ is divisible by m is $k = m - 1$.

Example 7.2

Using the multiplicative congruential method, find the period of the generator for $a = 13, m = 2^6 = 64$, and $X_0 = 1, 2, 3$, and 4. The solution is given in Table 7.1. When the seed is 1 and 3, the sequence has period 16. However, a period of length eight is achieved when the seed is 2 and a period of length four occurs when the seed is 4. ◀

In Example 7.2, $m = 2^6 = 64$ and $c = 0$. The maximal period is therefore $P = m/4 = 16$. Notice that this period is achieved using odd seeds $X_0 = 1$ and $X_0 = 3$, but even seeds, $X_0 = 2$ and $X_0 = 4$, yield periods of eight and four, both less than the maximum. Notice that $a = 13$ is of the form $5 + 8k$ with $k = 1$, as required to achieve maximal period.

When $X_0 = 1$, the generated sequence assumes values from the set $\{1, 5, 9, 13, \ldots, 53, 57, 61\}$. The "gaps" in the sequence of generated random numbers, R_i, are quite large (i.e., the gap is $5/64 - 1/64$ or 0.0625). Such a gap gives rise to concern about the density of the generated sequence.

Table 7.1. Period Determination Using Various Seeds

i	X_i	X_i	X_i	X_i
0	1	2	3	4
1	13	26	39	52
2	41	18	59	36
3	21	42	63	20
4	17	34	51	4
5	29	58	23	
6	57	50	43	
7	37	10	47	
8	33	2	35	
9	45		7	
10	9		27	
11	53		31	
12	49		19	
13	61		55	
14	25		11	
15	5		15	
16	1		3	

The generator in Example 7.2 is not viable for any application—its period is too short, and its density is insufficiently low. However, the example shows the importance of properly choosing a, c, m, and X_0.

Speed and efficiency in using the generator on a digital computer are also a selection consideration. Speed and efficiency are aided by use of a modulus, m, which is either a power of 2 or close to a power of 2. Since most digital computers use a binary representation of numbers, the modulo, or remaindering, operation of Equation (7.1) can be conducted efficiently when the modulo is a power of 2 (i.e., $m = 2^b$). After ordinary arithmetic yields a value for $aX_i + c$, X_{i+1} is obtained by dropping the leftmost binary digits in $aX_i + c$ and then using only the b rightmost binary digits. The following example illustrates, by analogy, this operation using $m = 10^b$, because most human beings think in decimal representation.

Example 7.3

Let $m = 10^2 = 100$, $a = 19$, $c = 0$, and $X_0 = 63$, and generate a sequence of random integers using Equation (7.1).

$$\begin{aligned}
X_0 &= 63 \\
X_1 &= (19)(63) \bmod 100 = 1197 \bmod 100 = 97 \\
X_2 &= (19)(97) \bmod 100 = 1843 \bmod 100 = 43 \\
X_3 &= (19)(43) \bmod 100 = 817 \bmod 100 = 17 \\
&\vdots
\end{aligned}$$

When m is a power of 10, say $m = 10^b$, the modulo operation is accomplished by saving the b rightmost (decimal) digits. By analogy, the modulo operation is most efficient for binary computers when $m = 2^b$ for some $b > 0$. ◀

Example 7.4

The last example in this section is in actual use. It has been extensively tested [Learmonth and Lewis, 1973; Lewis et al., 1969]. The values for a, c, and m have been selected to ensure that the characteristics desired in a generator are most likely to be achieved. By changing X_0, the user can control the repeatability of the stream.

Let $a = 7^5 = 16{,}807$, $m = 2^{31}-1 = 2{,}147{,}483{,}647$ (a prime number), and $c = 0$. These choices satisfy the conditions that insure a period of $P = m - 1$ (well over 2 billion). Further, specify a seed, $X_0 = 123{,}457$. The first few numbers generated are as follows:

$$X_1 = 7^5(123{,}457) \bmod (2^{31} - 1) = 2{,}074{,}941{,}799 \bmod (2^{31} - 1)$$
$$X_1 = 2{,}074{,}941{,}799$$
$$R_1 = \frac{X_1}{2^{31}} = 0.9662$$
$$X_2 = 7^5(2{,}074{,}941{,}799) \bmod (2^{31} - 1) = 559{,}872{,}160$$
$$R_2 = \frac{X_2}{2^{31}} = 0.2607$$
$$X_3 = 7^5(559{,}872{,}160) \bmod (2^{31} - 1) = 1{,}645{,}535{,}613$$
$$R_3 = \frac{X_3}{2^{31}} = 0.7662$$
$$\vdots$$

Notice that this routine divides by $m+1$ instead of m; however, for such a large value of m, the effect is negligible. ◀

7.3.2 Combined Linear Congruential Generators

As computing power has increased, the complexity of the systems that we are able to simulate has also increased. A random-number generator with period $2^{31}-1 \approx 2 \times 10^9$, such as the popular generator described in Example 7.4, is no longer adequate for all applications. Examples include the simulation of highly reliable systems, in which hundreds of thousands of elementry events must be simulated to observe even a single failure event; and the simulation of complex computer networks, in which thousands of users are executing hundreds of programs. An area of current research is deriving generators with substantially longer periods.

One fruitful approach is to combine two or more multiplicative congruential generators in such a way that the combined generator has good statistical properties and a longer period. The following result from L'Ecuyer [1988] suggests how this can be done:

If $W_{i,1}, W_{i,2}, \ldots, W_{i,k}$ are any independent, discrete-valued random variables (not necessarily identically distributed), but one of them, say $W_{i,1}$, is uniformly distributed on the integers 0 to $m_1 - 2$, then

$$W_i = \left(\sum_{j=1}^{k} W_{i,j}\right) \bmod m_1 - 1$$

is uniformly distributed on the integers 0 to $m_1 - 2$.

To see how this result can be used to form combined generators, let $X_{i,1}, X_{i,2}, \ldots, X_{i,k}$ be the ith output from k different multiplicative congruential generators, where the jth generator has prime modulus m_j, and the multiplier a_j is chosen so that the period is $m_j - 1$. Then the jth generator is producing integers $X_{i,j}$ that are approximately uniformly distributed on 1 to $m_j - 1$, and $W_{i,j} = X_{i,j} - 1$ is approximately uniformly distributed on 0 to $m_j - 2$. L'Ecuyer [1988] therefore suggests combined generators of the form

$$X_i = \left(\sum_{j=1}^{k} (-1)^{j-1} X_{i,j} \right) \bmod m_1 - 1$$

with

$$R_i = \begin{cases} \dfrac{X_i}{m_1}, & X_i > 0 \\ \dfrac{m_1 - 1}{m_1}, & X_i = 0 \end{cases}$$

Notice that the "$(-1)^{j-1}$" coefficient implicitly performs the subtraction $X_{i,1} - 1$; for example, if $k = 2$, then $(-1)^0(X_{i,1} - 1) - (-1)^1(X_{i,2} - 1) = \sum_{j=1}^{2}(-1)^{j-1}X_{i,j}$.

The maximum possible period for such a generator is

$$P = \frac{(m_1 - 1)(m_2 - 1)\cdots(m_k - 1)}{2^{k-1}}$$

which is achieved by the following generator:

Example 7.5

For 32-bit computers, L'Ecuyer [1988] suggests combining $k = 2$ generators with $m_1 = 2147483563$, $a_1 = 40014$, $m_2 = 2147483399$, and $a_2 = 40692$. This leads to the following algorithm:

1. Select seed $X_{1,0}$ in the range $[1, 2147483562]$ for the first generator, and seed $X_{2,0}$ in the range $[1, 2147483398]$.
   Set $j = 0$.
2. Evaluate each individual generator.

$$\begin{aligned} X_{1,j+1} &= 40014 X_{1,j} \bmod 2147483563 \\ X_{2,j+1} &= 40692 X_{2,j} \bmod 2147483399 \end{aligned}$$

3. Set

$$X_{j+1} = (X_{1,j+1} - X_{2,j+1}) \bmod 2147483562$$

4. Return

$$R_{j+1} = \begin{cases} \dfrac{X_{j+1}}{2147483563}, & X_{j+1} > 0 \\ \dfrac{2147483562}{2147483563}, & X_{j+1} = 0 \end{cases}$$

5. Set $j = j + 1$ and go to step 2.

This combined generator has period $(m_1 - 1)(m_2 - 1)/2 \approx 2 \times 10^{18}$. Perhaps surprisingly, even such a long period may not be adequate for all applications. See L'Ecuyer [1996, 1999] for combined generators with periods as long as $2^{191} \approx 3 \times 10^{57}$. ◀

7.4 Tests for Random Numbers

The desirable properties of random numbers — uniformity and independence — were discussed in Section 7.1. To insure that these desirable properties are achieved, a number of tests can be performed (fortunately, the appropriate tests have already been conducted for most commercial simulation software). The tests can be placed in two categories according to the properties of interest. The first entry in the list below concerns testing for uniformity. The second through fifth entries concern testing for independence. The five types of tests discussed in this chapter are as follows:

1. *Frequency test.* Uses the Kolmogorov-Smirnov or the chi-square test to compare the distribution of the set of numbers generated to a uniform distribution.
2. *Runs test.* Tests the runs up and down or the runs above and below the mean by comparing the actual values to expected values. The statistic for comparison is the chi-square.
3. *Autocorrelation test.* Tests the correlation between numbers and compares the sample correlation to the expected correlation of zero.
4. *Gap test.* Counts the number of digits that appear between repetitions of a particular digit and then uses the Kolmogorov-Smirnov test to compare with the expected size of gaps.
5. *Poker test.* Treats numbers grouped together as a poker hand. Then the hands obtained are compared to what is expected using the chi-square test.

In testing for uniformity, the hypotheses are as follows:

$$H_0\colon R_i \sim U[0,1]$$
$$H_1\colon R_i \not\sim U[0,1]$$

The null hypothesis, H_0, reads that the numbers are distributed uniformly on the interval [0, 1]. Failure to reject the null hypothesis means that no evidence of nonuniformity has been detected on the basis of this test. This does not imply that further testing of the generator for uniformity is unnecessary.

In testing for independence, the hypotheses are as follows:

$$H_0\colon R_i \sim \text{independently}$$
$$H_1\colon R_i \not\sim \text{independently}$$

This null hypothesis, H_0, reads that the numbers are independent. Failure to reject the null hypothesis means that no evidence of dependence has been detected on the basis of this test. This does not imply that further testing of the generator for independence is unnecessary.

For each test, a level of significance α must be stated. The level α is the probability of rejecting the null hypothesis given that the null hypothesis is true, or

$$\alpha = P(\text{reject } H_0 | H_0 \text{ true})$$

The decision maker sets the value of α for any test. Frequently, α is set to 0.01 or 0.05.

If several tests are conducted on the same set of numbers, the probability of rejecting the null hypothesis on at least one test, by chance alone [i.e., making a Type I (α) error], increases. Say that $\alpha = 0.05$ and that five different tests are conducted on a sequence of numbers. The probability of rejecting the null hypothesis on at least one test, by chance alone, may be as large as 0.25.

Similarly, if one test is conducted on many sets of numbers from a generator, the probability of rejecting the null hypothesis on at least one test by chance alone [i.e., making a Type I (α) error], increases as more sets of numbers are tested. For instance, if 100 sets of numbers were subjected to the test, with $\alpha = 0.05$, it would be expected that five of those tests would be rejected by chance alone. If the number of rejections in 100 tests is close to 100α, then there is no compelling reason to discard the generator. The concept discussed in this and the preceding paragraph is discussed further at the conclusion of Example 7.12.

If one of the well-known simulation languages or random-number generators is used, it is probably unnecessary to use the tests mentioned above and described in Sections 7.4.1 through 7.4.5. (However, a generator such as RANDU, distributed by IBM in the late 1960s and still available on some computers, has been found unreliable due to autocorrelation among triplets of random numbers.) If a new method has been developed, or if the generator that is at hand is not explicitly known or documented, then the tests in this chapter should be applied to many samples of numbers from the generator. Some additional tests that are commonly used, but are not covered here, are Good's serial test for sampling numbers [1953, 1967], the median-spectrum test [Cox and Lewis, 1966; Durbin, 1967], and a variance heterogeneity test [Cox and Lewis, 1966]. Even if a set of numbers passes all the tests, it is no guarantee of randomness. It is always possible that some underlying pattern will go undetected.

In this book we emphasize empirical tests that are applied to actual sequences of numbers produced by a generator. There are also families of theoretical tests that evaluate the choices for m, a, and c without actually generating any numbers, the most common being the spectral test. Many of these tests assess how k-tuples of random numbers fill up a k-dimensional unit cube. These tests are beyond the scope of this book; see, for instance, Ripley [1987].

In the examples of tests that follow, the hypotheses are not restated. The hypotheses are as indicated in the paragraphs above.

7.4.1 Frequency Tests

A basic test that should always be performed to validate a new generator is the test of uniformity. Two different methods of testing are available. They are the Kolmogorov-Smirnov and the chi-square test. Both of these tests measure the degree of agreement between the distribution of a sample of generated random numbers and the theoretical uniform distribution. Both tests are based on the null hypothesis of no significant difference between the sample distribution and the theoretical distribution.

1. *The Kolmogorov-Smirnov test.* This test compares the continuous cdf, $F(x)$, of the uniform distribution to the empirical cdf, $S_N(x)$, of the sample of N observations. By definition,

$$F(x) = x, \quad 0 \le x \le 1$$

If the sample from the random-number generator is $R_1, R_2, \ldots, R_N$, then the empirical cdf, $S_N(x)$, is defined by

$$S_N(x) = \frac{\text{number of } R_1, R_2, \ldots, R_N \text{ which are } \le x}{N}$$

As N becomes larger, $S_N(x)$ should become a better approximation to $F(x)$, provided that the null hypothesis is true.

In Section 5.6, empirical distributions were described. The cdf of an empirical distribution is a step function with jumps at each observed value. This behavior was illustrated by Example 5.34.

The Kolmogorov-Smirnov test is based on the largest absolute deviation between $F(x)$ and $S_N(x)$ over the range of the random variable. That is, it is based on the statistic

$$D = \max |F(x) - S_N(x)| \tag{7.3}$$

The sampling distribution of D is known and is tabulated as a function of N in Table A.8. For testing against a uniform cdf, the test procedure follows these steps:

Step 1. Rank the data from smallest to largest. Let $R_{(i)}$ denote the ith smallest observation, so that

$$R_{(1)} \le R_{(2)} \le \cdots \le R_{(N)}$$

Step 2. Compute

$$D^+ = \max_{1 \le i \le N} \left\{ \frac{i}{N} - R_{(i)} \right\}$$

$$D^- = \max_{1 \le i \le N} \left\{ R_{(i)} - \frac{i-1}{N} \right\}$$

Step 3. Compute $D = \max(D^+, D^-)$.

Step 4. Determine the critical value, D_α, from Table A.8 for the specified significance level α and the given sample size N.

Step 5. If the sample statistic D is greater than the critical value, D_α, the null hypothesis that the data are a sample from a uniform distribution is rejected. If $D \leq D_\alpha$, conclude that no difference has been detected between the true distribution of $\{R_1, R_2, \ldots, R_N\}$ and the uniform distribution.

EXAMPLE 7.6

Suppose that the five numbers 0.44, 0.81, 0.14, 0.05, 0.93 were generated, and it is desired to perform a test for uniformity using the Kolmogorov-Smirnov test with a level of significance α of 0.05. First, the numbers must be ranked from smallest to largest. The calculations can be facilitated by use of Table 7.2. The top row lists the numbers from smallest ($R_{(1)}$) to largest ($R_{(5)}$). The computations for D^+, namely $i/N - R_{(i)}$, and for D^-, namely $R_{(i)} - (i-1)/N$, are easily accomplished using Table 7.2. The statistics are computed as $D^+ = 0.26$ and $D^- = 0.21$. Therefore, $D = \max\{0.26, 0.21\} = 0.26$. The critical value of D, obtained from Table A.8 for $\alpha = 0.05$ and $N = 5$, is 0.565. Since the computed value, 0.26, is less than the tabulated critical value, 0.565, the hypothesis of no difference between the distribution of the generated numbers and the uniform distribution is not rejected.

Table 7.2. Calculations for Kolmogorov-Smirnov Test

$R_{(i)}$	0.05	0.14	0.44	0.81	0.93
i/N	0.20	0.40	0.60	0.80	1.00
$i/N - R_{(i)}$	0.15	0.26	0.16	—	0.07
$R_{(i)} - (i-1)/N$	0.05	—	0.04	0.21	0.13

The calculations in Table 7.2 are illustrated in Figure 7.2, where the empirical cdf, $S_N(x)$, is compared to the uniform cdf, $F(x)$. It can be seen that D^+ is the largest deviation of $S_N(x)$ above $F(x)$, and that D^- is the largest deviation of $S_N(x)$ below $F(x)$. For example, at $R_{(3)}$ the value of D^+ is given by $3/5 - R_{(3)} = 0.60 - 0.44 = 0.16$ and of D^- is given by $R_{(3)} - 2/5 = 0.44 - 0.40 = 0.04$. Although the test statistic D is defined by Equation (7.3) as the maximum deviation over all x, it can be seen from Figure 7.2 that the maximum deviation will always occur at one of the jump points $R_{(1)}, R_{(2)}, \ldots$, and thus the deviation at other values of x need not be considered. ◄

2. *The chi-square test.* The chi-square test uses the sample statistic

$$\chi_0^2 = \sum_{i=1}^{n} \frac{(O_i - E_i)^2}{E_i}$$

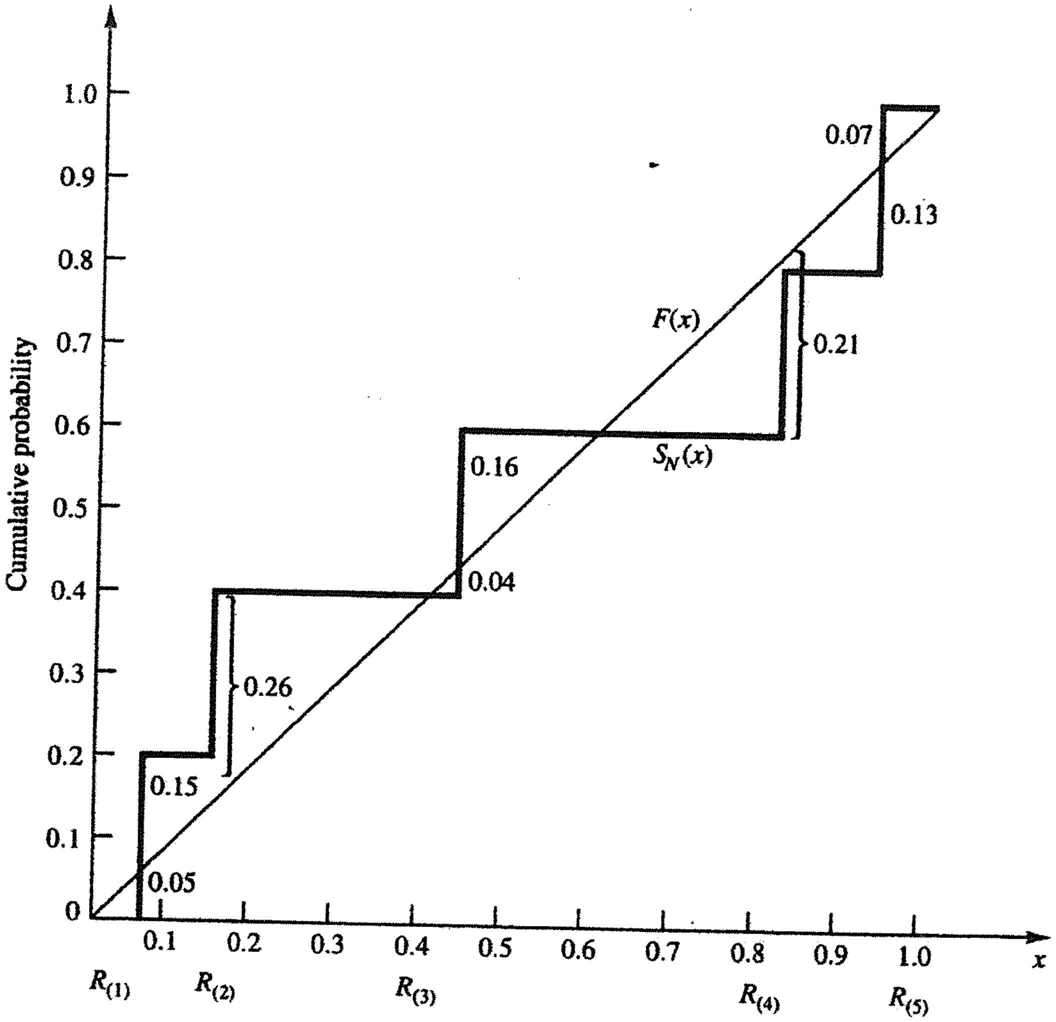

Figure 7.2. Comparison of $F(x)$ and $S_N(x)$.

where O_i is the observed number in the ith class, E_i is the expected number in the ith class, and n is the number of classes. For the uniform distribution, E_i, the expected number in each class is given by

$$E_i = \frac{N}{n}$$

for equally spaced classes, where N is the total number of observations. It can be shown that the sampling distribution of χ_0^2 is approximately the chi-square distribution with $n - 1$ degrees of freedom.

Example 7.7

Use the chi-square test with $\alpha = 0.05$ to test whether the data shown below are uniformly distributed. Table 7.3 contains the essential computations. The test uses $n = 10$ intervals of equal length, namely $[0, 0.1), [0.1, 0.2), \ldots, [0.9, 1.0)$. The value of χ_0^2 is 3.4. This is compared with the critical value $\chi^2_{0.05,9} = 16.9$. Since χ_0^2 is much smaller than the tabulated value of $\chi^2_{0.05,9}$, the null hypothesis of a uniform distribution is not rejected.

0.34	0.90	0.25	0.89	0.87	0.44	0.12	0.21	0.46	0.67
0.83	0.76	0.79	0.64	0.70	0.81	0.94	0.74	0.22	0.74
0.96	0.99	0.77	0.67	0.56	0.41	0.52	0.73	0.99	0.02
0.47	0.30	0.17	0.82	0.56	0.05	0.45	0.31	0.78	0.05
0.79	0.71	0.23	0.19	0.82	0.93	0.65	0.37	0.39	0.42
0.99	0.17	0.99	0.46	0.05	0.66	0.10	0.42	0.18	0.49
0.37	0.51	0.54	0.01	0.81	0.28	0.69	0.34	0.75	0.49
0.72	0.43	0.56	0.97	0.30	0.94	0.96	0.58	0.73	0.05
0.06	0.39	0.84	0.24	0.40	0.64	0.40	0.19	0.79	0.62
0.18	0.26	0.97	0.88	0.64	0.47	0.60	0.11	0.29	0.78

◀

Different authors have offered considerations concerning the application of the χ^2 test. In the application to a data set the size of that in Example 7.7, the considerations do not apply. That is, if 100 values are in the sample and from 5 to 10 intervals of equal length are used, the test will be acceptable. In general, it is recommended that n and N be chosen so that each $E_i \geq 5$.

Both the Kolmogorov-Smirnov and the chi-square test are acceptable for testing the uniformity of a sample of data, provided that the sample size is large. However, the Kolmogorov-Smirnov test is the more powerful of the two and is recommended. Furthermore, the Kolmogorov-Smirnov test can be applied to small sample sizes, whereas the chi-square is valid only for large samples, say $N \geq 50$.

Imagine a set of 100 numbers which are being tested for independence where the first 10 values are in the range 0.01–0.10, the second 10 values are in the range 0.11–0.20, and so on. This set of numbers would pass the frequency tests with ease, but the ordering of the numbers produced by the generator would not be random. The tests in the remainder of this chapter are concerned with the independence of random numbers which are generated. The presentation of the tests is similar to that by Schmidt and Taylor [1970].

Table 7.3. Computations for Chi-Square Test

Interval	O_i	E_i	$O_i - E_i$	$(O_i - E_i)^2$	$\dfrac{(O_i - E_i)^2}{E_i}$
1	8	10	−2	4	0.4
2	8	10	−2	4	0.4
3	10	10	0	0	0.0
4	9	10	−1	1	0.1
5	12	10	2	4	0.4
6	8	10	−2	4	0.4
7	10	10	0	0	0.0
8	14	10	4	16	1.6
9	10	10	0	0	0.0
10	11	10	1	1	0.1
	100	100	0		3.4

7.4.2 Runs Tests

1. *Runs up and runs down.* Consider a generator that provided a set of 40 numbers in the following sequence:

0.08 0.09 0.23 0.29 0.42 0.55 0.58 0.72 0.89 0.91
0.11 0.16 0.18 0.31 0.41 0.53 0.71 0.73 0.74 0.84
0.02 0.09 0.30 0.32 0.45 0.47 0.69 0.74 0.91 0.95
0.12 0.13 0.29 0.36 0.38 0.54 0.68 0.86 0.88 0.91

Both the Kolmogorov-Smirnov test and the chi-square test would indicate that the numbers are uniformly distributed. However, a glance at the ordering shows that the numbers are successively larger in blocks of 10 values. If these numbers are rearranged as follows, there is far less reason to doubt their independence:

0.41 0.68 0.89 0.84 0.74 0.91 0.55 0.71 0.36 0.30
0.09 0.72 0.86 0.08 0.54 0.02 0.11 0.29 0.16 0.18
0.88 0.91 0.95 0.69 0.09 0.38 0.23 0.32 0.91 0.53
0.31 0.42 0.73 0.12 0.74 0.45 0.13 0.47 0.58 0.29

The runs test examines the arrangement of numbers in a sequence to test the hypothesis of independence.

Before defining a run, a look at a sequence of coin tosses will help with some terminology. Consider the following sequence generated by tossing a coin 10 times:

$$H\ T\ T\ H\ H\ T\ T\ T\ H\ T$$

There are three mutually exclusive outcomes, or events, with respect to the sequence. Two of the possibilities are rather obvious. That is, the toss can result in a head or a tail. The third possibility is "no event." The first head is preceded by no event and the last tail is succeeded by no event. Every sequence begins and ends with no event.

A run is defined as a succession of similar events preceded and followed by a different event. The length of the run is the number of events that occur in the run. In the coin-flipping example above there are six runs. The first run is of length one, the second and third of length two, the fourth of length three, and the fifth and sixth of length one.

There are two possible concerns in a runs test for a sequence of numbers. The number of runs is the first concern and the length of runs is a second concern. The types of runs counted in the first case might be runs up and runs down. An up run is a sequence of numbers each of which is succeeded by a larger number. Similarly, a down run is a sequence of numbers each of which is succeeded by a smaller number. To illustrate the concept, consider the following sequence of 15 numbers:

$^{-}0.87$ $^{+}0.15$ $^{+}0.23$ $^{+}0.45$ $^{-}0.69$ $^{-}0.32$ $^{-}0.30$ $^{+}0.19$ $^{-}0.24$
$^{+}0.18$ $^{+}0.65$ $^{+}0.82$ $^{-}0.93$ $^{+}0.22$ 0.81

The numbers are given a "+" or a "−" depending on whether they are followed by a larger number or a smaller number. Since there are 15 numbers, and they are all different, there will be 14 +'s and −'s. The last number is followed by "no event" and hence will get neither a + nor a −. The sequence of 14 +'s and −'s is as follows:

$$- \quad + \quad + \quad + \quad - \quad - \quad - \quad + \quad - \quad + \quad + \quad + \quad - \quad +$$

Each succession of +'s and −'s forms a run. There are eight runs. The first run is of length one, the second and third are of length three, and so on. Further, there are four runs up and four runs down.

There can be too few runs or too many runs. Consider the following sequence of numbers:

$$0.08 \quad 0.18 \quad 0.23 \quad 0.36 \quad 0.42 \quad 0.55 \quad 0.63 \quad 0.72 \quad 0.89 \quad 0.91$$

This sequence has one run, a run up. It is unlikely that a valid random-number generator would produce such a sequence. Next, consider the following sequence:

$$0.08 \quad 0.93 \quad 0.15 \quad 0.96 \quad 0.26 \quad 0.84 \quad 0.28 \quad 0.79 \quad 0.36 \quad 0.57$$

This sequence has nine runs, five up and four down. It is unlikely that a sequence of 10 numbers would have this many runs. What is more likely is that the number of runs will be somewhere between the two extremes. These two extremes can be formalized as follows: if N is the number of numbers in a sequence, the maximum number of runs is $N - 1$ and the minimum number of runs is one.

If a is the total number of runs in a truly random sequence, the mean and variance of a are given by

$$\mu_a = \frac{2N - 1}{3} \tag{7.4}$$

and

$$\sigma_a^2 = \frac{16N - 29}{90} \tag{7.5}$$

For $N > 20$, the distribution of a is reasonably approximated by a normal distribution, $N(\mu_a, \sigma_a^2)$. This approximation can be used to test the independence of numbers from a generator. In that case the standardized normal test statistic is developed by subtracting the mean from the observed number of runs, a, and dividing by the standard deviation. That is, the test statistic is

$$Z_0 = \frac{a - \mu_a}{\sigma_a}$$

Substituting Equation (7.4) for μ_a and the square root of Equation (7.5) for σ_a yields

$$Z_0 = \frac{a - [(2N - 1)/3]}{\sqrt{(16N - 29)/90}}$$

where $Z_0 \sim N(0, 1)$. Failure to reject the hypothesis of independence occurs when $-z_{\alpha/2} \leq Z_0 \leq z_{\alpha 72}$, where α is the level of significance. The critical values and rejection region are shown in Figure 7.3.

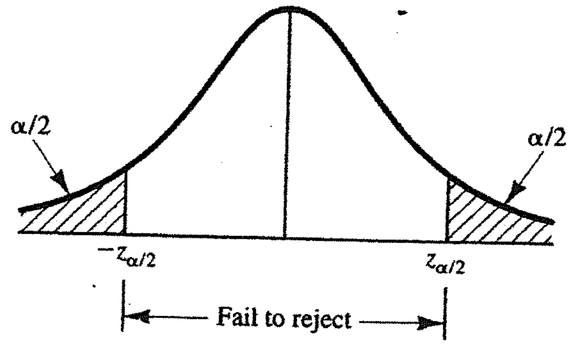

Figure 7.3. Failure to reject hypothesis.

Example 7.8

Based on runs up and runs down, determine whether the following sequence of 40 numbers is such that the hypothesis of independence can be rejected where $\alpha = 0.05$.

0.41	0.68	0.89	0.94	0.74	0.91	0.55	0.62	0.36	0.27
0.19	0.72	0.75	0.08	0.54	0.02	0.01	0.36	0.16	0.28
0.18	0.01	0.95	0.69	0.18	0.47	0.23	0.32	0.82	0.53
0.31	0.42	0.73	0.04	0.83	0.45	0.13	0.57	0.63	0.29

The sequence of runs up and down is as follows:

+ + + − + − + − − − + + − + − − + − +
− − + − − + − + + − − + + − + − − + + −

There are 26 runs in this sequence. With $N = 40$ and $a = 26$, Equations (7.4) and (7.5) yield

$$\mu_a = \frac{2(40) - 1}{3} = 26.33$$

and

$$\sigma_a^2 = \frac{16(40) - 29}{90} = 6.79$$

Then,

$$Z_0 = \frac{26 - 26.33}{\sqrt{6.79}} = -0.13$$

Now, the critical value is $z_{0.025} = 1.96$, so the independence of the numbers cannot be rejected on the basis of this test. ◀

2. *Runs above and below the mean.* The test for runs up and runs down is not completely adequate to assess the independence of a group of numbers. Consider the following 40 numbers:

0.63 0.72 0.79 0.81 0.52 0.94 0.83 0.93 0.87 0.67
0.54 0.83 0.89 0.55 0.88 0.77 0.74 0.95 0.82 0.86
0.43 0.32 0.36 0.18 0.08 0.19 0.18 0.27 0.36 0.34
0.31 0.45 0.49 0.43 0.46 0.35 0.25 0.39 0.47 0.41

The sequence of runs up and runs down is as follows:

+ + + − + − + − − − + + − + − − + − + − − + − −
+ − + + − − + + − + − − + + −

This sequence is exactly the same as that in Example 7.8. Thus, the numbers would pass the runs-up and runs-down test. However, it can be observed that the first 20 numbers are all above the mean $[(0.99 + 0.00)/2 = 0.495]$ and the last 20 numbers are all below the mean. Such an occurrence is highly unlikely. The previous runs analysis can be used to test for this condition, if the definition of a run is changed. Runs will be described as being above the mean or below the mean. A "+" sign will be used to denote an observation above the mean, and a "−" sign will denote an observation below the mean.

For example, consider the following sequence of 20 two-digit random numbers:

0.40 0.84 0.75 0.18 0.13 0.92 0.57 0.77 0.30 0.71
0.42 0.05 0.78 0.74 0.68 0.03 0.18 0.51 0.10 0.37

The pluses and minuses are as follows:

− + + − − + + + − + − − + + + − − + − −

In this case, there is a run of length one below the mean followed by a run of length two above the mean, and so on. In all, there are 11 runs, five of which are above the mean and six of which are below the mean. Let n_1 and n_2 be the number of individual observations above and below the mean and let b be the total number of runs. Notice that the maximum number of runs is $N = n_1 + n_2$, and the minimum number of runs is one. Given n_1 and n_2, the mean—with a continuity correction suggested by Swed and Eisenhart [1943] —and the variance of b for a truly independent sequence are given by

$$\mu_b = \frac{2n_1 n_2}{N} + \frac{1}{2} \tag{7.6}$$

and

$$\sigma_b^2 = \frac{2n_1 n_2 (2n_1 n_2 - N)}{N^2(N-1)} \tag{7.7}$$

For either n_1 or n_2 greater than 20, b is approximately normally distributed. The test statistic can be formed by subtracting the mean from the number of runs and dividing by the standard deviation, or

$$Z_0 = \frac{b - (2n_1n_2/N) - 1/2}{\left[\frac{2n_1n_2(2n_1n_2 - N)}{N^2(N-1)}\right]^{1/2}}$$

Failure to reject the hypothesis of independence occurs when $-z_{\alpha/2} \le Z_0 \le z_{\alpha/2}$, where α is the level of significance. The rejection region is shown in Figure 7.3.

Example 7.9

Determine whether there is an excessive number of runs above or below the mean for the sequence of numbers given in Example 7.8. The assignment of +'s and −'s results in the following:

```
−  +  +  +  +  +  +  +  −  −  −  +  +  −  +  −  −  −  −  −
−  −  +  +  −  −  −  −  +  +  −  −  +  −  +  −  −  +  +  −
```

The values of n_1, n_2, and b are as follows:

$$n_1 = 18 \quad +$$

$$n_2 = 22 \quad -$$

$$N = n_1 + n_2 = 40$$

$$b = 17$$

Equations (7.6) and (7.7) are used to determine μ_b and σ_b^2 as follows:

$$\mu_b = \frac{2(18)(22)}{40} + \frac{1}{2} = 20.3$$

and

$$\sigma_b^2 = \frac{2(18)(22)[(2)(18)(22) - 40]}{(40)^2(40-1)} = 9.54$$

Since n_2 is greater than 20, the normal approximation is acceptable, resulting in a Z_0 value of

$$Z_0 = \frac{17 - 20.3}{\sqrt{9.54}} = -1.07$$

Since $z_{0.025} = 1.96$, the hypothesis of independence cannot be rejected on the basis of this test. ◀

3. *Runs test: length of runs*. Yet another concern is the length of runs. As an example of what might occur, consider the following sequence of numbers:

0.16, 0.27, 0.58, 0.63, 0.45, 0.21, 0.72, 0.87, 0.27, 0.15, 0.92, 0.85, ...

Assume that this sequence continues in a like fashion: two numbers below the mean followed by two numbers above the mean. A test of runs above and below the mean would detect no departure from independence. However, it is to be expected that runs other than of length two should occur.

Let Y_i be the number of runs of length i in a sequence of N numbers. For an independent sequence, the expected value of Y_i for runs up and down is given by

$$E(Y_i) = \frac{2}{(i+3)!}[N(i^2+3i+1) - (i^3+3i^2-i-4)],\ i \le N-2 \quad (7.8)$$

$$E(Y_i) = \frac{2}{N!},\quad i = N-1 \quad (7.9)$$

For runs above and below the mean, the expected value of Y_i is approximately given by

$$E(Y_i) = \frac{Nw_i}{E(I)},\quad N > 20 \quad (7.10)$$

where w_i, the approximate probability that a run has length i, is given by

$$w_i = \left(\frac{n_1}{N}\right)^i \left(\frac{n_2}{N}\right) + \left(\frac{n_1}{N}\right)\left(\frac{n_2}{N}\right)^i,\quad N > 20 \quad (7.11)$$

and where $E(I)$, the approximate expected length of a run, is given by

$$E(I) = \frac{n_1}{n_2} + \frac{n_2}{n_1},\quad N > 20 \quad (7.12)$$

The approximate expected total number of runs (of all lengths) in a sequence of length N, $E(A)$, is given by

$$E(A) = \frac{N}{E(I)},\quad N > 20 \quad (7.13)$$

The appropriate test is the chi-square test with O_i being the observed number of runs of length i. Then the test statistic is

$$\chi_0^2 = \sum_{i=1}^{L} \frac{[O_i - E(Y_i)]^2}{E(Y_i)}$$

where $L = N-1$ for runs up and down and $L = N$ for runs above and below the mean. If the null hypothesis of independence is true, then χ_0^2 is approximately chi-square distributed with $L-1$ degrees of freedom.

Example 7.10

Given the following sequence of numbers, can the hypothesis that the numbers are independent be rejected on the basis of the length of runs up and down at $\alpha = 0.05$?

0.30	0.48	0.36	0.01	0.54	0.34	0.96	0.06	0.61	0.85
0.48	0.86	0.14	0.86	0.89	0.37	0.49	0.60	0.04	0.83
0.42	0.83	0.37	0.21	0.90	0.89	0.91	0.79	0.57	0.99
0.95	0.27	0.41	0.81	0.96	0.31	0.09	0.06	0.23	0.77
0.73	0.47	0.13	0.55	0.11	0.75	0.36	0.25	0.23	0.72
0.60	0.84	0.70	0.30	0.26	0.38	0.05	0.19	0.73	0.44

For this sequence the +'s and −'s are as follows:

+ − − + − + − + + − + − + + − + + − +
− + − − + − + − − + − − + + + − − − + +
− − − + − + − − − + − + − − − + − + + −

The length of runs in the sequence is as follows:

1, 2, 1, 1, 1, 1, 2, 1, 1, 1, 2, 1, 2, 1, 1, 1, 1, 2, 1, 1,
1, 2, 1, 2, 3, 3, 2, 3, 1, 1, 1, 3, 1, 1, 1, 3, 1, 1, 2, 1

The number of observed runs of each length is as follows:

Run Length, i	1	2	3
Observed Runs, O_i	26	9	5

The expected numbers of runs of lengths one, two, and three are computed from Equation (7.8) as

$$E(Y_1) = \frac{2}{4!}[60(1+3+1) - (1+3-1-4)]$$
$$= 25.08$$

$$E(Y_2) = \frac{2}{5!}[60(4+6+1) - (8+12-2-4)]$$
$$= 10.77$$

$$E(Y_3) = \frac{2}{6!}[60(9+9+1) - (27+27-3-4)]$$
$$= 3.04$$

The mean total number of runs (up and down) is given by Equation (7.4) as

$$\mu_a = \frac{2(60)-1}{3} = 39.67$$

Thus far, the $E(Y_i)$ for $i = 1, 2$, and 3 total 38.89. The expected number of runs of length 4 or more is the difference $\mu_a - \sum_{i=1}^{3} E(Y_i)$, or 0.78.

As observed by Hines and Montgomery [1990], there is no general agreement regarding the minimum value of expected frequencies in applying the chi-square test. Values of 3, 4, and 5 are widely used, and a minimum of 5 was suggested earlier in this chapter. Should an expected frequency be too small,

Table 7.4. Length of Runs Up and Down: χ^2 Test

Run Length, i	*Observed Number of Runs, O_i*	*Expected Number of Runs, $E(Y_i)$*	$\dfrac{[O_i - E(Y_i)]^2}{E(Y_i)}$
1	26	25.08	0.03
2	9 }14	10.77 }14.59	}0.02
≥ 3	5	3.82	
	40	39.67	0.05

it can be combined with the expected frequency in an adjacent class interval. The corresponding observed frequencies would then be combined also, and L would be reduced by one. With the foregoing calculations and procedures in mind, we construct Table 7.4. The critical value $\chi^2_{0.05,1}$ is 3.84. (The degrees of freedom equals the number of class intervals minus one.) Since $\chi_0^2 = 0.05$ is less than the critical value, the hypothesis of independence cannot be rejected on the basis of this test. ◀

Example 7.11

Given the same sequence of numbers in Example 7.10, can the hypothesis that the numbers are independent be rejected on the basis of the length of runs above and below the mean at $\alpha = 0.05$? For this sequence, the +'s and −'s are as follows:

```
−  −  −  −  +  −  +  −  +  +  −  +  −  +  +  −  −  +  −  +
−  +  −  −  +  +  +  +  +  +  +  −  −  +  +  −  −  −  −  +
+  −  −  +  −  +  −  −  −  +  +  +  +  −  −  −  −  −  +  −
```

The number of runs of each length is as follows:

Run Length, i	1	2	3	≥ 4
Observed Runs, O_i	17	9	1	5

There are 28 values above the mean ($n_1 = 28$) and 32 values below the mean ($n_2 = 32$). The probabilities of runs of various lengths, w_i, are determined from Equation (7.11) as

$$w_1 = \left(\frac{28}{60}\right)^1 \frac{32}{60} + \frac{28}{60}\left(\frac{32}{60}\right)^1 = 0.498$$

$$w_2 = \left(\frac{28}{60}\right)^2 \frac{32}{60} + \frac{28}{60}\left(\frac{32}{60}\right)^2 = 0.249$$

$$w_3 = \left(\frac{28}{60}\right)^3 \frac{32}{60} + \frac{28}{60}\left(\frac{32}{60}\right)^3 = 0.125$$

$$\vdots$$

The expected length of a run, $E(I)$, is determined from Equation (7.12) as

$$E(I) = \frac{28}{32} + \frac{32}{28} = 2.02$$

Now, Equation (7.10) can be used to determine the expected numbers of runs of various lengths as

$$E(Y_1) = \frac{60(0.498)}{2.02} = 14.79$$

$$E(Y_2) = \frac{60(0.249)}{2.02} = 7.40$$

$$E(Y_3) = \frac{60(0.125)}{2.02} = 3.71$$

The total number of runs expected is given by Equation (7.13) as $E(A) = 60/2.02 = 29.7$. This indicates that approximately 3.8 runs of length four or more can be expected. Proceeding by combining adjacent cells in which $E(Y_i) < 5$ produces Table 7.5.

Table 7.5. Length of Runs Above and Below the Mean: χ^2 Test

Run Length, i	*Observed Number of Runs, O_i*	*Expected Number of Runs, $E(Y_i)$*	$\frac{[O_i - E(Y_i)]^2}{E(Y_i)}$
1	17	14.79	0.33
2	9	7.40	0.35
3 ≥ 4	$\left.\begin{matrix}1\\5\end{matrix}\right\}6$	$\left.\begin{matrix}3.71\\3.80\end{matrix}\right\}7.51$	$\left.\right\}0.30$
	32	29.70	0.98

The critical value $\chi^2_{0.05,2}$ is 5.99. (The degrees of freedom equals the number of class intervals minus one.) Since $\chi_0^2 = 0.98$ is less than the critical value, the hypothesis of independence cannot be rejected on the basis of this test. ◀

7.4.3 *Tests for Autocorrelation*

The tests for autocorrelation are concerned with the dependence between numbers in a sequence. As an example, consider the following sequence of numbers:

0.12	0.01	0.23	0.28	0.89	0.31	0.64	0.28	0.83	0.93
0.99	0.15	0.33	0.35	0.91	0.41	0.60	0.27	0.75	0.88
0.68	0.49	0.05	0.43	0.95	0.58	0.19	0.36	0.69	0.87

From a visual inspection, these numbers appear random, and they would probably pass all the tests presented to this point. However, an examination of the 5th, 10th, 15th (every five numbers beginning with the fifth), and so on, indicates a very large number in that position. Now, 30 numbers is a rather small sample size to reject a random-number generator, but the notion is that numbers in the sequence might be related. In this particular section, a method for determining whether such a relationship exists is described. The relationship would not have to be all high numbers. It is possible to have all low numbers in the locations being examined, or the numbers may alternately shift from very high to very low.

The test to be described below requires the computation of the autocorrelation between every m numbers (m is also known as the lag) starting with the ith number. Thus, the autocorrelation ρ_{im} between the following numbers would be of interest: $R_i, R_{i+m}, R_{i+2m}, \ldots, R_{i+(M+1)m}$. The value M is the largest integer such that $i + (M+1)m \leq N$, where N is the total number of values in the sequence. (Thus, a subsequence of length $M+2$ is being tested.)

Since a nonzero autocorrelation implies a lack of independence, the following two-tailed test is appropriate:

$$H_0\colon \rho_{im} = 0$$
$$H_1\colon \rho_{im} \neq 0$$

For large values of M, the distribution of the estimator of ρ_{im}, denoted $\widehat{\rho}_{im}$, is approximately normal if the values $R_i, R_{i+m}, R_{i+2m}, \ldots, R_{i+(M+1)m}$ are uncorrelated. Then the test statistic can be formed as follows:

$$Z_0 = \frac{\widehat{\rho}_{im}}{\sigma_{\widehat{\rho}_{im}}}$$

which is distributed normally with a mean of zero and a variance of 1, under the assumption of independence, for large M.

The formula for $\widehat{\rho}_{im}$, in a slightly different form, and the standard deviation of the estimator, $\sigma_{\widehat{\rho}_{im}}$, are given by Schmidt and Taylor [1970] as follows:

$$\widehat{\rho}_{im} = \frac{1}{M+1}\left[\sum_{k=0}^{M} R_{i+km}R_{i+(k+1)m}\right] - 0.25$$

and

$$\sigma_{\widehat{\rho}_{im}} = \frac{\sqrt{13M+7}}{12(M+1)}$$

After computing Z_0, do not reject the null hypothesis of independence if $-z_{\alpha/2} \leq Z_0 \leq z_{\alpha/2}$, where α is the level of significance. Figure 7.3, presented earlier, illustrates this test.

If $\rho_{im} > 0$, the subsequence is said to exhibit positive autocorrelation. In this case, successive values at lag m have a higher probability than expected of being close in value (i.e., high random numbers in the subsequence followed by high, and low followed by low). On the other hand, if $\rho_{im} < 0$, the subsequence is exhibiting negative autocorrelation, which means that low random numbers tend to be followed by high ones, and vice versa. The desired property of independence, which implies zero autocorrelation, means that there is no discernible relationship of the nature discussed here between successive random numbers at lag m.

Example 7.12

Test whether the 3rd, 8th, 13th, and so on, numbers in the sequence at the beginning of this section are autocorrelated. (Use $\alpha = 0.05$.) Here, $i = 3$ (beginning with the third number), $m = 5$ (every five numbers), $N = 30$ (30 numbers in the sequence), and $M = 4$ (largest integer such that $3+(M+1)5 \leq 30$). Then,

$$\begin{aligned}\widehat{\rho}_{35} &= \frac{1}{4+1}[(0.23)(0.28) + (0.28)(0.33) + (0.33)(0.27) + (0.27)(0.05)\\ &\quad + (0.05)(0.36)] - 0.25\\ &= -0.1945\end{aligned}$$

and

$$\sigma_{\widehat{\rho}_{35}} = \frac{\sqrt{13(4)+7}}{12(4+1)} = 0.1280$$

Then, the test statistic assumes the value

$$Z_0 = \frac{-0.1945}{0.1280} = -1.516$$

Now, the critical value is

$$z_{0.025} = 1.96$$

Therefore, the hypothesis of independence cannot be rejected on the basis of this test.

It can be observed that this test is not very sensitive for small values of M, particularly when the numbers being tested are on the low side. Imagine what would happen if each of the entries in the foregoing computation of $\widehat{\rho}_{im}$ were equal to zero. Then, $\widehat{\rho}_{im}$ would be equal to -0.25 and the calculated Z would have the value of -1.95, not quite enough to reject the hypothesis of independence. ◀

Many sequences can be formed in a set of data, given a large value of N. For example, beginning with the first number in the sequence, possibilities include (1) the sequence of all numbers, (2) the sequence formed from the first, third, fifth,. . . , numbers, (3) the sequence formed from the first, fourth, . . . , numbers, and so on. If $\alpha = 0.05$, there is a probability of 0.05 of rejecting a true hypothesis. If 10 independent sequences are examined, the probability of finding no significant autocorrelation, by chance alone, is $(0.95)^{10}$ or 0.60. Thus, 40% of the time significant autocorrelation would be detected when it does not exist. If α is 0.10 and 10 tests are conducted, there is a 65% chance of finding autocorrelation by chance alone. In conclusion, when "fishing" for autocorrelation, upon performing numerous tests, autocorrelation may eventually be detected, perhaps by chance alone, even when no autocorrelation is present.

7.4.4 Gap Test

The gap test is used to determine the significance of the interval between the recurrences of the same digit. A gap of length x occurs between the recurrences of some specified digit. The following example illustrates the length of gaps associated with the digit 3:

4, 1, 3, 5, 1, 7, 2, 8, 2, 0, 7, 9, 1, 3, 5, 2, 7, 9, 4, 1, 6, 3
3, 9, 6, 3, 4, 8, 2, 3, 1, 9, 4, 4, 6, 8, 4, 1, 3, 8, 9, 5, 5, 7
3, 9, 5, 9, 8, 5, 3, 2, 2, 3, 7, 4, 7, 0, 3, 6, 3, 5, 9, 9, 5, 5
5, 0, 4, 6, 8, 0, 4, 7, 0, 3, 3, 0, 9, 5, 7, 9, 5, 1, 6, 6, 3, 8
8, 8, 9, 2, 9, 1, 8, 5, 4, 4, 5, 0, 2, 3, 9, 7, 1, 2, 0, 3, 6, 3

To facilitate the analysis, the digit 3 has been underlined. There are eighteen 3's in the list. Thus, only 17 gaps can occur. The first gap is of length 10, the second gap is of length 7, and so on. The frequency of the gaps is of interest. The probability of the first gap is determined as follows:

$$\begin{aligned} P(\text{gap of } 10) &= \overbrace{P(\text{no } 3)\cdots P(\text{no } 3)}^{10 \text{ of these terms}}\, P(3) \\ &= (0.9)^{10}(0.1) \end{aligned}$$

since the probability that any digit is not a 3 is 0.9, and the probability that any digit is a 3 is 0.1. In general,

$$P(t \text{ followed by exactly } x \text{ non-}t \text{ digits}) = (0.9)^x(0.1), \quad x = 0, 1, 2, \ldots$$

In the example above, only the digit 3 was examined. However, to fully analyze a set of numbers for independence using the gap test, every digit, 0, 1, 2, ..., 9, must be analyzed. The observed frequencies of the various gap sizes for all the digits are recorded and compared to the theoretical frequency using the Kolmogorov-Smirnov test for discretized data.

The theoretical frequency distribution for randomly ordered digits is given by

$$P(\text{gap} \le x) = F(x) = 0.1 \sum_{n=0}^{x} (0.9)^n = 1 - 0.9^{x+1} \qquad (7.14)$$

The procedure for the test follows the steps below. When applying the test to random numbers, class intervals such as [0, 0.1), [0.1, 0.2), ... play the role of random digits.

Step 1. Specify the cdf for the theoretical frequency distribution given by Equation (7.14) based on the selected class interval width.

Step 2. Arrange the observed sample of gaps in a cumulative distribution with these same classes.

Step 3. Find D, the maximum deviation between $F(x)$ and $S_N(x)$ as in Equation (7.3).

Step 4. Determine the critical value, D_α, from Table A.8 for the specified value of α and the sample size N.

Step 5. If the calculated value of D is greater than the tabulated value of D_α, the null hypothesis of independence is rejected.

It should be noted that using the Kolmogorov-Smirnov test when the underlying distribution is discrete results in a reduction in the Type I error, α, and an increase in the Type II error, β. The exact value of α can be found using the methodology described by Conover [1980].

Example 7.13

Based on the frequency with which gaps occur, analyze the 110 digits above to test whether they are independent. Use $\alpha = 0.05$. The number of gaps is given by the number of data values minus the number of distinct digits, or $110 - 10 = 100$ in the example. The number of gaps associated with the various digits are as follows:

Digit	0	1	2	3	4	5	6	7	8	9
Number of Gaps	7	8	8	17	10	13	7	8	9	13

The gap test is presented in Table 7.6. The critical value of D is given by

$$D_{0.05} = \frac{1.36}{\sqrt{100}} = 0.136$$

Since $D = \max|F(x) - S_N(x)| = 0.0224$ is less than $D_{0.05}$, do not reject the hypothesis of independence on the basis of this test. ◄

Table 7.6. Gap-Test Example

Gap Length	*Frequency*	*Relative Frequency*	*Cumulative Relative Frequency*	$F(x)$	$\|F(x) - S_N(x)\|$
0–3	35	0.35	0.35	0.3439	0.0061
4–7	22	0.22	0.57	0.5695	0.0005
8–11	17	0.17	0.74	0.7176	0.0224
12–15	9	0.09	0.83	0.8147	0.0153
16–19	5	0.05	0.88	0.8784	0.0016
20–23	6	0.06	0.94	0.9202	0.0198
24–27	3	0.03	0.97	0.9497	0.0223
28–31	0	0.0	0.97	0.9657	0.0043
32–35	0	0.0	0.97	0.9775	0.0075
36–39	2	0.02	0.99	0.9852	0.0043
40–43	0	0.0	0.99	0.9903	0.0003
44–47	1	0.01	1.00	0.9936	0.0064

7.4.5 *Poker Test*

The poker test for independence is based on the frequency with which certain digits are repeated in a series of numbers. The following example shows an unusual amount of repetition:

$$0.255,\quad 0.577,\quad 0.331,\quad 0.414,\quad 0.828,\quad 0.909,\quad 0.303,\ 0.001,\quad \ldots$$

In each case, a pair of like digits appears in the number that was generated. In three-digit numbers there are only three possibilities, as follows:

1. The individual numbers can all be different.
2. The individual numbers can all be the same.
3. There can be one pair of like digits.

The probability associated with each of these possibilities is given by the following:

$$\begin{aligned} P(\text{three different digits}) &= P(\text{second different from the first}) \\ &\qquad \times P(\text{third different from the first and second}) \\ &= (0.9)(0.8) = 0.72 \\ P(\text{three like digits}) &= P(\text{second digit same as the first}) \\ &\qquad \times P(\text{third digit same as the first}) \\ &= (0.1)(0.1) = 0.01 \\ P(\text{exactly one pair}) &= 1 - 0.72 - 0.01 = 0.27 \end{aligned}$$

Alternatively, the last result can be obtained as follows:

$$P(\text{exactly one pair}) = \binom{3}{2}(0.1)(0.9) = 0.27$$

The following example shows how the poker test (in conjunction with the chi-square test) is used to ascertain independence.

Example 7.14

A sequence of 1000 three-digit numbers has been generated and an analysis indicates that 680 have three different digits, 289 contain exactly one pair of like digits, and 31 contain three like digits. Based on the poker test, are these numbers independent? Let $\alpha \doteq 0.05$. The test is summarized in Table 7.7.

The appropriate degrees of freedom are one less than the number of class intervals. Since $47.65 > \chi^2_{0.05,2} = 5.99$, the independence of the numbers is rejected on the basis of this test. ◀

Table 7.7. Poker-Test Results

Combination, i	*Observed Frequency, O_i*	*Expected Frequency, E_i*	$\frac{(O_i - E_i)^2}{E_i}$
Three different digits	680	720	2.22
Three like digits	31	10	44.10
Exactly one pair	289	270	1.33
	1000	1000	47.65

7.5 Summary

This chapter described the generation of random numbers and the subsequent testing of the generated numbers for uniformity and independence. Random numbers are used to generate random variates, the subject of Chapter 8.

Of the many types of random-number generators available, the linear congruential method is the most widely used. Of the many types of statistical tests that are used in testing random-number generators, five different types are described. Some of these tests are for uniformity, the others for testing independence.

The simulation analyst may never work directly with a random-number generator or with the testing of random numbers from a generator. Most computers and simulation languages have routines that generate a random number, or streams of random numbers, for the asking. But even generators that have been used for years, some of which are still in use, have been found to be inadequate. So this chapter calls the simulation analyst's attention to such possibilities, with a warning to investigate and confirm that the generator has been tested thoroughly. Some researchers have attained sophisticated expertise in developing methods for generating and testing random numbers and the subsequent application of these methods. However, this chapter provides only a basic introduction to the subject matter; more depth and breadth are required for the reader to become a specialist in the area. A key reference is Knuth [1981]; see also the reviews in Bratley, Fox and Schrage [1987], Law and Kelton [2000], L'Ecuyer [1998], and Ripley [1987].

One final caution is due. Even if generated numbers pass all the tests (both those covered in this chapter and those mentioned in the chapter), some underlying pattern may go undetected and the generator may not be rejected as faulty. However, the generators available in widely used simulation languages have been extensively tested and validated.

REFERENCES

BRATLEY, P., B. L. FOX, AND L. E. SCHRAGE [1987], *A Guide to Simulation,* 2d ed., Springer-Verlag, New York.

CONOVER, W. J. [1980], *Practical Nonparametric Statistics,* 2d ed., John Wiley, New York.

COX, D. R., AND P. A. W. LEWIS [1966], *The Statistical Analysis of Series of Events,* Barnes and Noble, New York.

DURBIN, J. [1967], "Tests of Serial Independence Based on the Cumulated Periodogram," *Bulletin of the International Institute of Statistics.*

FISHMAN, G. S. [1978], *Principles of Discrete Event Simulation,* John Wiley, New York.

GOOD, I. J. [1953], "The Serial Test for Sampling Numbers and Other Tests of Randomness," *Proceedings of the Cambridge Philosophical Society,* Vol. 49, pp. 276–84.

GOOD, I. J. [1967], "The Generalized Serial Test and the Binary Expansion of 4," *Journal of the Royal Statistical Society,* Ser. A, Vol. 30, No. 1, pp. 102–7.

HINES, W. W., AND D. C. MONTGOMERY [1990], *Probability and Statistics in Engineering and Management Science,* 3d ed., Prentice Hall, Upper Saddle River, NJ.

KNUTH, D. W. [1981], *The Art of Computer Programming,* Vol. 2: *Semi-numerical Algorithms,* 2d ed., Addison-Wesley, Reading, MA.

LAW, A. M., AND W. D. KELTON [2000], *Simulation Modeling & Analysis,* 3d ed., McGraw-Hill, New York.

LEARMONTH, G. P., AND P. A. W. LEWIS [1973], "Statistical Tests of Some Widely Used and Recently Proposed Uniform Random Number Generators," *Proceedings of the Conference on Computer Science and Statistics: Seventh Annual Symposium on the Interface,* Western Publishing, North Hollywood, Calif., pp. 163–71.

L'ECUYER, P. [1988], "Efficient and Portable Combined Random Number Generators," *Communications of the ACM,* Vol. 31, pp. 742–749, 774.

L'ECUYER, P. [1996], "Combined Multiple Recursive Random Number Generators," *Operations Research,* Vol. 44, pp. 816–822.

L'ECUYER, P. [1998], "Random Number Generation," Chapter 4 in *Handbook of Simulation,* John Wiley, New York.

L'ECUYER, P. [1999], "Good Parameters and Implementations for Combined Multiple Recursive Random Number Generators," *Operations Research,* Vol. 47, pp. 159–164.

LEHMER, D. H. [1951], *Proceedings of the Second Symposium on Large-Scale Digital Computing Machinery,* Harvard University Press, Cambridge, MA.

LEWIS, P. A. W., A. S. GOODMAN, AND J. M. MILLER [1969], "A Pseudo-Random Number Generator for the System/360," *IBM Systems Journal,* Vol. 8, pp. 136–45.

RIPLEY, B. D. [1987], *Stochastic Simulation,* John Wiley, New York.

SCHMIDT, J. W., AND R. E. TAYLOR [1970], *Simulation and Analysis of Industrial Systems,* Irwin, Homewood, IL.

SWED, F. S., AND C. EISENHART [1943], "Tables for Testing Randomness of Grouping in a Sequence of Alternatives," *Annals of Mathematical Statistics,* Vol. 14, pp. 66–82.

EXERCISES

1. Describe a procedure to physically generate random numbers on the interval [0, 1] with 2-digit accuracy. [*Hint:* Consider drawing something out of a hat.]

2. List applications, other than systems simulation, for pseudo-random numbers — for example, video gambling games.

3. How could random numbers that are uniform on the interval [0, 1] be transformed into random numbers that are uniform on the interval [−11, 17]? Transformations to more general distributions are described in Chapter 8.

4. Use the linear congruential method to generate a sequence of three two-digit random integers. Let $X_0 = 27, a = 8, c = 47$, and $m = 100$.

5. Do we encounter a problem in the previous exercise if $X_0 = 0$?

6. Use the multiplicative congruential method to generate a sequence of four three-digit random integers. Let $X_0 = 117, a = 43$, and $m = 1000$.

7. The sequence of numbers 0.54, 0.73, 0.98, 0.11, and 0.68 has been generated. Use the Kolmogorov-Smirnov test with $\alpha = 0.05$ to determine if the hypothesis that the numbers are uniformly distributed on the interval [0, 1] can be rejected.

8. Reverse the 100 two-digit random numbers in Example 7.7 to get a new set of random numbers. Thus, the first random number in the new set will be 0.43. Use the chi-square test, with $\alpha = 0.05$, to determine if the hypothesis that the numbers are uniformly distributed on the interval [0, 1] can be rejected.

9. Consider the first 50 two-digit values in Example 7.7. Based on runs up and runs down, determine whether the hypothesis of independence can be rejected, where $\alpha = 0.05$.

10. Consider the last 50 two-digit values in Example 7.7. Determine whether there is an excessive number of runs above or below the mean. Use $\alpha = 0.05$.

11. Consider the first 50 two-digit values in Example 7.7. Can the hypothesis that the numbers are independent be rejected on the basis of the length of runs up and down when $\alpha = 0.05$?

12. Consider the last 50 two-digit values in Example 7.7. Can the hypothesis that the numbers are independent be rejected on the basis of the length of runs above and below the mean, where $\alpha = 0.05$?

13. Consider the 60 values in Example 7.10. Test whether the 2nd, 9th, 16th, ... numbers in the sequence are autocorrelated, where $\alpha = 0.05$.

14. Consider the following sequence of 120 digits:

1	3	7	4	8	6	2	5	1	6	4	4	3	3	4	2	1	5	8	7
0	7	6	2	6	0	5	7	8	0	1	1	2	6	7	6	3	7	5	9
0	8	8	2	6	7	8	1	3	5	3	8	4	0	9	0	3	0	9	2
2	3	6	5	6	0	0	1	3	4	4	6	9	9	8	5	6	0	1	7
5	6	7	9	4	9	3	1	8	3	3	6	6	7	8	2	3	5	9	6
6	7	0	3	1	0	2	4	2	0	6	4	0	3	9	3	6	8	1	5

Test whether these digits can be assumed to be independent based on the frequency with which gaps occur. Use $\alpha = 0.05$.

15. Develop the poker test for:

(a) Four-digit numbers

(b) Five-digit numbers

16. A sequence of 1000 four-digit numbers has been generated and an analysis indicates the following combinations and frequencies.

Combination i	*Observed Frequency, O_i*
Four different digits	565
One pair	392
Two pairs	17
Three like digits	24
Four like digits	2
	1000

Based on the poker test, test whether these numbers are independent. Use $\alpha = 0.05$.

17. Determine whether the linear congruential generators shown below can achieve a maximum period. Also, state restrictions on X_0 to obtain this period.

(a) The mixed congruential method with

$$\begin{aligned} a &= 2{,}814{,}749{,}767{,}109 \\ c &= 59{,}482{,}661{,}568{,}307 \\ m &= 2^{48} \end{aligned}$$

(b) The multiplicative congruential generator with

$$\begin{aligned} a &= 69{,}069 \\ c &= 0 \\ m &= 2^{32} \end{aligned}$$

(c) The mixed congruential generator with

$$\begin{aligned} a &= 4951 \\ c &= 247 \\ m &= 256 \end{aligned}$$

(d) The multiplicative congruential generator with

$$\begin{aligned} a &= 6507 \\ c &= 0 \\ m &= 1024 \end{aligned}$$

18. Use the mixed congruential method to generate a sequence of three two-digit random numbers with $X_0 = 37$, $a = 7$, $c = 29$, and $m = 100$.

19. Use the mixed congruential method to generate a sequence of three two-digit random integers between 0 and 24 with $X_0 = 13$, $a = 9$, and $c = 35$.

20. Write a computer program that will generate four-digit random numbers using the multiplicative congruential method. Allow the user to input values of X_0, a, c and m.

21. If $X_0 = 3579$ in Exercise 17(c), generate the first random number in the sequence. Compute the random number to four-place accuracy.

22. Investigate the random-number generator in a spreadsheet program on a computer to which you have access. In many spreadsheets, random numbers are generated by a function called RAND or @RAND.
    - **(a)** Check the user's manual to see if it describes how the random numbers are generated.
    - **(b)** Write macros to conduct each of the tests described in this chapter. Generate 100 sets of random numbers, each set containing 100 random numbers. Perform each test on each set of random numbers. Draw conclusions.

23. Consider the multiplicative congruential generator under the following circumstances:
    - **(a)** $a = 11, m = 16, X_0 = 7$.
    - **(b)** $a = 11, m = 16, X_0 = 8$.
    - **(c)** $a = 7, m = 16, X_0 = 7$.
    - **(d)** $a = 7, m = 16, X_0 = 8$.

    Generate enough values in each case to complete a cycle. What inferences can be drawn? Is maximum period achieved?

24. For 16-bit computers, L'Ecuyer [1988] recommends combining three multiplicative generators with $m_1 = 32363$, $a_1 = 157$, $m_2 = 31727$, $a_2 = 146$, $m_3 = 31657$, and $a_3 = 142$. The period of this generator is approximately 8×10^{12}. Generate 5 random numbers with the combined generator using initial seeds $X_{i,0} = 100, 300, 500$ for the individual generators $i = 1, 2, 3$.

25. Apply the tests described in this chapter to the generator given in the previous exercise.

26. Use the principles described in this chapter to develop your own linear congruential random-number generator.

27. Use the principles described in this chapter to develop your own combined linear congruential random-number generator.

28. Test the following sequence of numbers for uniformity and independence using procedures you learned in this chapter: 0.594, 0.928, 0.515, 0.055, 0.507, 0.351, 0.262, 0.797, 0.788, 0.442, 0.097, 0.798, 0.227, 0.127, 0.474, 0.825, 0.007, 0.182, 0.929, 0.852.

29. In some applications it is useful to be able to quickly skip ahead in a pseudo-random number sequence without actually generating all of the intermediate values. (a) For a linear congruential generator with $c = 0$, show that $X_{i+n} = (a^n X_i) \bmod m$. (b) Next show that $(a^n X_i) \bmod m = (a^n \bmod m) X_i \bmod m$ (this result is useful because $a^n \bmod m$ can be precomputed, making it easy to skip ahead n random numbers from any point in the sequence). (c) In Example 7.3, use this result to compute X_5 starting with $X_0 = 63$. Check your answer by computing X_5 in the usual way.