

```

1  /**
2  * Construct this Random object with
3  * initial state obtained from system clock.
4  */
5  public Random( )
6  {
7      this( (int) ( System.currentTimeMillis( )
8              % Integer.MAX_VALUE ) );
9  }
10
11 /**
12 * Construct this Random object with
13 * specified initial state.
14 * @param initialState the initial state.
15 */
16 public Random( int initialState )
17 {
18     if( initialState < 0 )
19         initialState += M;
20
21     state = initialState;
22     if( state == 0 )
23         state = 1;
24 }

```

Figure 9.2 Constructors for class Random

Generating a number a second time results in a repeating sequence. In our case the sequence repeats after $M - 1 = 10$ numbers. The length of the sequence until a repeated number occurs is called the *period* of the sequence. The period obtained with this choice of A is clearly as good as possible, since all nonzero numbers smaller than M are generated. (We must have a repeated number generated on the 11th iteration.)

If M is prime, several choices of A give a full period of $M - 1$. This type of generator is called a *full-period linear congruential generator*. Some choices of A do not give a full period. For instance, if $A = 5$ and $X_0 = 1$, the sequence has a short period of 5:

5, 3, 4, 9, 1, 5, 3, 4, ...

If M is chosen to be a large, 31-bit prime, the period should be significantly large for most applications. The 31-bit prime $M = 2^{31} - 1 = 2,147,483,647$ is a common choice. For this prime, $A = 48,271$ is one of the many values that gives a full-period linear congruential generator. Its use has been well-studied and is recommended by experts in the field. As will be shown later in the chapter, tinkering with random number generators usually means breaking, so we are well advised to stick with this formula until told otherwise.

A random-number generator with period P generates the same sequence of numbers after P iterations.

A full-period linear congruential generator has period $M - 1$.