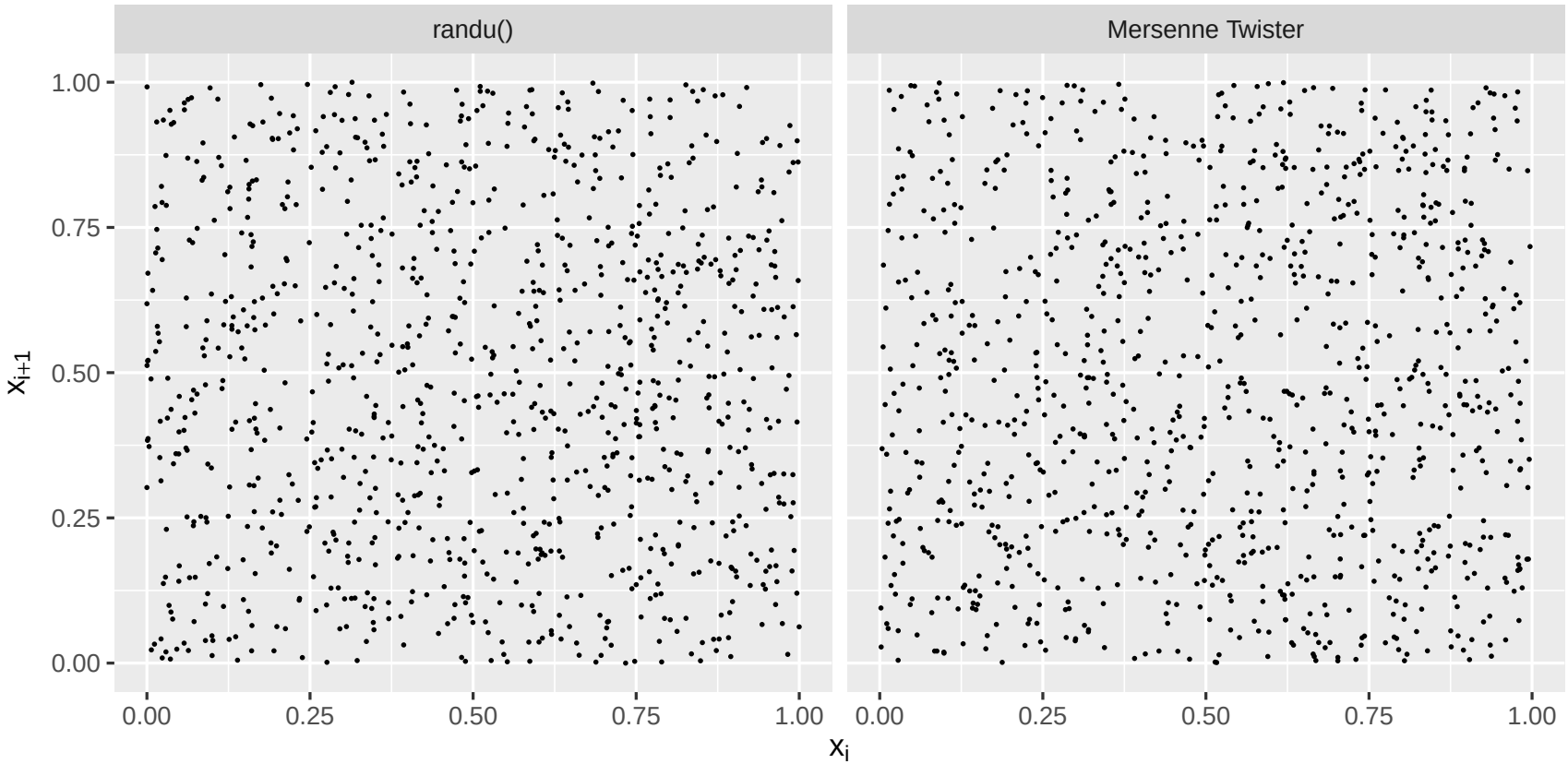
RNG: Randu vs Mersenne Twister

The `randu()` function is a linear congruential method

$$X_n = (aX_{n-1} + c) \quad \text{modulo} \quad m$$

with $a = 65,399$, $c = 0$ and $m = 2^{31}$. For example, take $X_0 = 1$ and 2,000 consecutive values scaled by $1/m$ to lie in the range $(0, 1)$.



Note that $a = 65,539 = 2^{16} + 3$ and so

$$X_{i+1} = aX_i = (2^{16} + 3)X_i$$

and using arithmetic mod 2^{31}

$$\begin{aligned} X_{i+2} = aX_{i+1} = (2^{16} + 3)X_{i+1} = (2^{16} + 3)^2 X_i = (2^{32} + 6 \times 2^{16} + 9)X_i \\ = (2 \times 2^{31} + 6 \times 2^{16} + 9)X_i = (6(2^{16} + 3) - 9)X_i = 6X_{i+1} - 9X_i \end{aligned}$$

Hence, $9X_i - 6X_{i+1} + X_{i+2} = 0 \bmod 2^{31}$ and so $(9X_i - 6X_{i+1} + X_{i+2})/2^{31}$ is an integer.