MERSENNE TWISTER

Generator bez większych problemów przechodzi (prawie) wszystkie testy.

Dwa razy generator nie przeszedł testu 3, lecz P-value jest tam większa od 1, co jest ciężkie do zinterpretowania i (myślę że) skłaniałoby raczej do spodziewania się błędu po stronie strony internetowej (implementacji testu NIST), aniżeli samej metodologii czy wartości wyrzuconych przez generator.

Raz nie przeszedł testu 4, lecz był bardzo blisko (zabrakło 0,002 w P-value).

Raz nie przeszedł testu 8, lecz był bardzo blisko (zabrakło 0,002 w P-value). Test sprawdza jak bardzo da się skompresować dany ciąg bitów, a Mersenne Twister znany jest z „odporności" na kompresowanie. Nie uznałbym tego negatywnego wyniku za „bardzo" istotny.

W jednej próbie wystąpił błąd w teście 13 i 14 (ciężko mi powiedzieć dlaczego, ale spodziewam się winy po stronie strony).

Raz „oblał" test 14 (zabrakło 0,005). Oznacza to, że w tym teście była lekka tendencja do przebywania w danym „stanie" ciut częściej lub rzadziej niż zakładano od PRNG.

Wnioski z tych testów płyną następujące: Mersenne Twister jest bardzo dobrym generator liczb pseudo losowych, czasami zdarzy mu się wypaść poza „strefę przyzwoitości" i nie przejść danego testu. Jednak wypadki takie nie są ani częste, ani bardzo drastyczne (P-value są bardzo niewiele poniżej zakładanego zakresu).