LCG

Generator przechodzi większość testów.

Raz nie przeszedł testu 3 (P-value >1 => możliwa wina po stronie strony).

Raz nie przeszedł testu 11, P-value było bardzo niskie. Z definicji LCG jest dość podatny na wpadanie w bardzo krótkie cykle, pętle; stosunkowo łatwo aby występowała duża powtarzalność. Możliwym jest, że coś takiego miało właśnie miejsce i stąd bardzo niska entropia (choć dziwi pomyślne przejście innych testów).

Raz nie przeszedł testu 13 (zabrakło 0,004). Jednak przeszedł test 14. Testy te są w pewien sposób „bliźniacze", 13 bada 8 stanów (stany powyżej najwyższego lub poniżej najniższego są liczone jak najniższy lub najwyższy) a 14 aż 18 stanów. Możliwym jest więc, LCG „lubi wpadać" w stany wyższe i niższe stosunkowo często w porównaniu do tych bliskich zeru.

Wnioski: LCG jest dość dobrym generatorem liczb pseudo losowych, jednak nie tak dobrym jak Mersenne Twister(MT). Rozkład jego „stanów (testy 13 i 14)" nie jest tak dobry jak dla MT (wysoka ilość błędów dla tych testów również nie napawa optymizmem). Natomiast największą jego wadą jest łatwość wpadania w krótkie („mało losowe") cykle.