



Generator liczb pseudolosowych (PRNG - Pseudorandom Number Generator) to prosty algorytm matematyczny, który generuje liczby wyglądające na losowe, ale są one w rzeczywistości deterministyczne - ich sekwencja zależy od wartości początkowej (tzw. ziarna, ang. **seed**). PRNG są powszechnie wykorzystywane w kryptografii, symulacjach komputerowych oraz grach komputerowych.

Najprostszy i jeden z najczęściej używanych generatorów to **liniowy generator kongruencyjny** :

$$x_n = (ax_0 + c) \bmod m$$

gdzie: x_n - bieżąca liczba losowa, a - mnożnik, c - stała przesunięcia, mod - **operacja modulo**, x_0 wartość początkowa (ziarno)



Modulo - operacja wyznaczania reszty z dzielenia jednej liczby przez drugą


$$x_n = (ax_0 + c) \bmod m$$

Stosując **liniowy generator kongruencyjny** obliczmy kolejne liczby losowe dla: a) $a = 2, c = 1, m = 3, x_0 = 0$

Ten generator ma okres równy 2 (bo liczby powtarzają się co 2 kroki).

Stosując **liniowy generator kongruencyjny** obliczmy kolejne liczby losowe dla: a) $a = 2, c = 1, m = 3, x_0 = 2$

Otrzymujemy sekwencję: 2, 2, 2... (ciąg się nie zmienia - generator jest uwięziony na wartości 2)

Stosując **liniowy generator kongruencyjny** obliczmy kolejne liczby losowe dla: a) $a = 3, c = 2, m = 5, x_0 = 0$



Jak jest największa zaleta języka Pascal? User-friendly

Generowanie liczb pseudolosowych w Pascalu

W Pascalu do generowania liczb pseudolosowych używa się dwóch podstawowych poleceń: **Randomize** (ang. losowo) – inicjuje **generator liczb pseudolosowych** oraz **Random(N)** – zwraca liczbę losową.

Uwaga! Jeśli N jest podane otrzymujemy liczbę całkowitą z zakresu 0 ... N-1. Gdy N nie jest podane, otrzymujemy liczbę rzeczywistą z zakresu [0,1).

```
program LosowaLiczba;  
  
begin  
  
    randomize; { Inicjalizacja generatora losowego }  
  
    writeln('Losowa liczba z zakresu 0 - 100');  
  
    writeln(Random(101));  
  
end.
```

Random(101) zwróci liczbę całkowitą z przedziału 0 - 100



```
program LosowaLiczbaRzeczywista;  
begin  
  randomize; {inicjalizacja generatora losowego}  
  writeln('Losowa liczba rzeczywista z zakresu 0 - 1');  
  writeln(random);  
end.
```

```
program liczba_losowa;  
begin  
  randomize; {inicjalizacja generatora losowego}  
  writeln('Losowa liczba rzeczywista z zakresu 0 - 1');  
  writeln(random());  
end.
```

Otrzymana liczba jest zazwyczaj podawana w **notacji wykładniczej** z użyciem litery E (eksponenta) zamiast $\times 10^x$

Duże liczby:

$$\begin{aligned}5 \times 10^6 &= 5E6 \\ 1.23 \times 10^9 &= 1.23E9 \\ 9.87 \times 10^5 &= 9.87E5\end{aligned}$$

Małe liczby:

$$\begin{aligned}4 \times 10^{-4} &= 4E-4 \\ 8.9 \times 10^{-7} &= 8.9E-7 \\ 1.23 \times 10^{-3} &= 1.23E-3\end{aligned}$$


Formatowanie liczb całkowitych

Liczby całkowite można wyświetlić, określając **minimalną szerokość pola**. Składnia:

```
writeln(liczba:szerokość);
```

Jeśli liczba ma mniej cyfr niż szerokość, zostanie dopełniona odpowiednią liczbą spacji z lewej strony.

```
program FormatIntegers;  
begin  
  writeln(123);  
  writeln(123:0);  
  writeln(123:6);  
  writeln(12345:3);  
end.
```

Wynik:123

Wynik:123

Wynik: 123 (trzy spacje przed liczbą)

Wynik:12345 (bo szerokość < liczba)

Uwaga! Zmienna całkowita typu **Longint**

Formatowanie liczb zmiennoprzecinkowych

Liczby zmiennoprzecinkowe można wyświetlić w dwóch formatach:

a) Standardowy (:n) – określa minimalną szerokość pola.

b) Z określoną liczbą miejsc po przecinku (:m:n) – gdzie m – szerokość pola a n liczba miejsc po przecinku

```
program Format;  
begin  
  writeln(12.345);  
  writeln(12.345:8);  
end.
```

Wynik:12.345

Wynik: 12.345 (dwie spacje przed)

```
program FormatPrecision;  
begin  
  writeln(12.34567:10:2);  
  writeln(12.34567:8:4); { Wynik:12.3457 }  
  writeln(3.14:5:2);      { Wynik: 3.14 }  
end.
```

Wynik: 12.35 (zaokrąglenie + pięć spacji przed)

Wynik: 12.3457 (zaokrąglenie + spacja przed)

Wynik: 3.14 spacja przed

Jeśli chcesz wylosować liczbę całkowitą z przedziału [A, B], użyj wzoru: **$A + \text{Random}(B - A + 1)$**

Przykład dla przedziału [50, 150]:

```
program LosowaZPrzedzialu;  
var  
    A, B, losowa: integer;  
begin  
    randomize;  
    A := 50;  
    B := 150;  
    losowa := A + Random(B - A + 1);  
    writeln('Losowa liczba z przedzialu [50-150]: ', losowa:4);  
end.
```

Jeśli chcesz wylosować liczbę z przedziału [A, B], użyj wzoru: **$A + \text{Random}() * (B - A)$**

Przykład dla przedziału [1.5, 5.5]:

```
program LosowaRzeczywistaZakres;  
var  
    A, B, losowa: real;  
begin  
    randomize;  
    A := 1.5;  
    B := 5.5;  
    losowa := A + Random *(B - A);  
    writeln('Losowa liczba rzeczywista z przedzialu [1.5-5.5]: ', losowa:5:2);  
end.
```