Practice04

Friday, March 24, 2023 1:55 PM

Linear Congruence Generators (LCG)

$0 < m \in \mathbb{Z}$ modulus

$0 < a < m$ multiplier

$0 < c < m$ increment

$0 \leq x_0 < m$ seed

$$x_{n+1} = a \cdot x_n + c \mod m$$

$a = 65539$

$m = 2^{31}$

$c = 0$

$x_0 = 1$

Generate 2000 numbers with this formula!

$$\pi_i = (x_i, x_{i+1}, x_{i+2}, \dots, x_{i+k})$$

$$\pi_1 = (x_1, \dots, x_{1+k})$$

$$\pi_2 = (x_2, \dots, x_{2+k})$$

n-1 dimensional plane in n-dimensional space

$$c_1 x_1 + \dots c_n x_n + c_{n+1} = 0$$

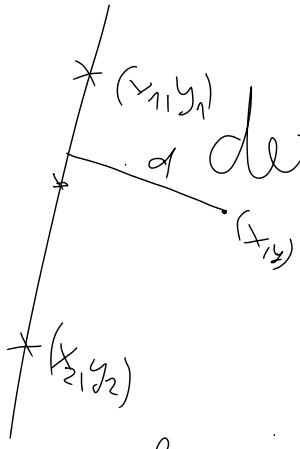
xy 2D $\quad ax + by + c = 0 \quad (y = mx + b)$

$$a x_1 + b y_1 + c = 0$$

$$a x + b y + c = 0$$

$$a x_1 + b y_1 + c = 0$$
$$a x_2 + b y_2 + c = 0$$

$$\begin{pmatrix} x & y & 1 \\ x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \end{pmatrix} \cdot \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$



$$d = \det \begin{pmatrix} x & y & 1 \\ x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \end{pmatrix} = 0$$

gives me signed distance of (x, y) from the line defined by $(x_1, y_1), (x_2, y_2)$

for $i = 0, \dots, j$

$$d_j = \det \begin{pmatrix} x_i & x_{i+1} & 1 \\ x_{i+1} & x_{i+2} & 1 \\ x_{i+2} & x_{i+3} & 1 \end{pmatrix} = k_j \cdot m \quad \text{for some } k \in \mathbb{Z}$$

Calculate $\gcd(d_j)$

$$= bd - c^2 - (ad - cb) + ac - b^2$$

$$\begin{vmatrix} a & b & 1 \\ b & c & 1 \\ c & d & 1 \end{vmatrix} = 1 \cdot \begin{vmatrix} b & c \\ c & d \end{vmatrix} - 1 \cdot \begin{vmatrix} a & b \\ c & d \end{vmatrix} + 1 \cdot \begin{vmatrix} a & b \\ b & c \end{vmatrix}$$

$$\begin{vmatrix} e & f \\ g & h \end{vmatrix} = eh - gf$$

$$\gcd(a, b, c) = \gcd(\gcd(a, b), c)$$

$$\gcd(a,b,c) = \gcd(\gcd(a,b),c)$$
$$\gcd(0,a) = a$$

$$a \cdot x_0 + c \bmod m = x_1$$
$$a \cdot x_1 + c \bmod m = x_2$$

$$a x_0 + c \equiv x_1 \pmod m$$
$$a x_1 + c \equiv x_2 \pmod m$$

$$a(x_0 - x_1) \equiv x_1 - x_2 \pmod m$$
$$a \equiv (x_1 - x_2) \cdot (x_0 - x_1)^{-1} \pmod m$$
$$a = \text{——} \mid \text{——} \bmod m$$

$$c \equiv x_1 - a x_0 \pmod m$$
$$c = x_1 - a x_0 \bmod m$$

Dimension reduction trick

$$ax + by + c = 0$$

If we translate our random points on the plane with a fixed point we only need to calculate det for 2x2 matrix

(x_0, x_1) fixed point plane

$$\det \begin{pmatrix} x_i - x_0 & x_{i+1} - x_0 \\ x_{i+1} - x_1 & x_{i+2} - x_1 \end{pmatrix} = k_i \cdot m \text{ for some } k_i \in \mathbb{Z}$$