# M03-T01
# PRNGs

# Linear Congruential Generator - Example

- Let $\mathbf{x_n = 3x_{n-1} + 5 \bmod 31}$, $n \geq 1$, and $x_0 = 2$
- **Pseudo-random sequences of 10 bits**
  - when $x_0 = 2$

    1101010001
  - **When $x_0 = 3$**

    **0001101001**

$x_n = a x_{n-1} + b \bmod m, \quad n \geq 1$

$x_0 = \text{seed};$ $\boxed{\text{Choice of } a, b, m}$

Not suitable cryptographic application

$a = 3, \; b = 5, \; m = 31.$

$x_0 = 2;$ $x_1, x_2, x_3 \ldots$

Q: Generate a random number of 5-bits

$x_1 = 3 \times 2 + 5 \bmod 31 = 11$

$x_2 = 3 \times 11 + 5 \bmod 31 = 7$

$x_3 = 3 \times 7 + 5 \bmod 31 = 26$

$x_4 = 3 \times 26 + 5 \bmod 31 = 21$

$x_5 = 3 \times 21 + 5 \bmod 31 = 6$

$y_1 = x_1 \bmod 2 = 1$

$y_2 = x_2 \bmod 2 = 1$

$y_3 = x_3 \bmod 2 = 0$

$y_4 = x_4 \bmod 2 = 1$

$y_5 = x_5 \bmod 2 = 0$

# Blum-Blum-Shub Generator - Algorithm

BBS

- **Based on the squaring one-way function**
  - Let p, q be two odd primes and **$p \equiv q \equiv 3 \bmod 4$**
  - Let **n = pq, s is a seed.**
  - Let $\boldsymbol{x_0 = s^2 \bmod n}$ , then define

$$x_i = x_{i-1}^2 \bmod n, \ i \geq 1$$

**Output**

$(x_1, x_2, \ldots, x_k)$

$y_i = x_i \bmod 2$

$Y = (y_1 y_2 \ldots y_k)$ ← pseudo-random sequence of k bits

Example: p=7, q=11, and n=pq = 77. Let seed s=2.

$x_0 = s^2 \bmod 77 = 4$

$x_1 = x_0^2 \bmod 77 = 16$

$x_2 = x_1^2 \bmod 77 = 16^2 \bmod 77 = 25$

$x_3 = x_2^2 \bmod 77 = 25^2 \bmod 77 = 9$

$x_4 = x_3^2 \bmod 77 = 9^2 \bmod 77 = 4$

$x_5 = x_4^2 \bmod 77 = 4^2 \bmod 77 = 16$

$y_1 = x_1 \bmod 2 = 0$

$y_2 = x_2 \bmod 2 = 1$

$y_3 = x_3 \bmod 2 = 1$

$y_4 = x_4 \bmod 2 = 0$

$y_5 = x_5 \bmod 2 = 0$

5-bit random number generated with BBS is 01100

Q: $p = 7,\ q = 11,\ n = 77,$
$s = 5$, generate 5-bit
random number using BBS.

Sol:

$x_0 = s^2 \bmod 77 = 25$

$x_1 = x_0^2 \bmod 77 = 9$

$x_2 = x_1^2 \bmod 77 = 4$

$x_3 = x_2^2 \bmod 77 = 16$

$x_4 = x_3^2 \bmod 77 = 25$

$x_5 = x_4^2 \bmod 77 = 9$

$y_1 = x_1 \bmod 2 = 1$

$y_2 = x_2 \bmod 2 = 0$

$y_3 = x_3 \bmod 2 = 0$

$y_4 = x_4 \bmod 2 = 1$

$y_5 = x_5 \bmod 2 = 1$

$\boxed{10011}$ ??

# Blum-Blum-Shub Generator

- **Euler's criterion**
  - Let p be an odd prime. Then a is a quadratic residue modulo p if and only if $\mathbf{a^{(p-1)/2} \equiv 1 \bmod p}$
- **Legendre symbol**
  - Let p be an odd prime and a be an integer

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p} \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p \end{cases}$$

$$\boxed{\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}}$$

$$\boxed{\left(\frac{2}{3}\right) = 2^{(3-1)/2} = 2 \bmod 3 = -1}$$

1). $\left(\frac{0}{p}\right) = 0$, $\left(\frac{1}{p}\right) = 1$.

2) $\left(a \equiv b \bmod p\right) \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

3). $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

# Blum-Blum-Shub Generator

- **Composite quadratic residues**
  - Let p, q be two odd primes and **n = pq**
  - If (x/n) = (x/p)(x/q) = 1, then
    either (x/p) = (x/q) = 1, x is a quadratic residue modulo n
    or (x/p) = (x/q) = -1, x is a pseudo-square modulo n
  - It is difficult to determine whether x is a quadratic residue modulo n, which as difficult as factoring n=pq.

$$\left(\frac{x}{n}\right) = \begin{cases} 0 & \text{if } \gcd(x,n) > 1 \\ 1 & \text{if } \left(\frac{x}{p}\right) = \left(\frac{x}{q}\right) = 1 \text{ or if } \left(\frac{x}{p}\right) = \left(\frac{x}{q}\right) = -1 \\ -1 & \text{if one of } \left(\frac{x}{p}\right) \text{ and } \left(\frac{x}{q}\right) = 1 \text{ and the other} = -1 \end{cases}$$

  - Example: Let n=15=3*5
    (8/15)=(8/3)(8/5)=(2/3)(3/5)=(-1)(-1)=1;  8 is a pseudo-square
    (4/15)=(4/3)(4/5)=(1)(1)=1;  4 is a quadratic residue

$$\left(\frac{x}{n}\right) = \left(\frac{x}{p}\right)\left(\frac{x}{q}\right) = 1$$

$1 \quad 1 \quad = 1$

$(-1) \quad (-1) \quad = 1$

$n = 15 = 3 * 5$

$8^{\frac{3-1}{2}} = 8 \bmod 3 = -1 \bmod 3$

$\left(\frac{8}{15}\right) = \left(\frac{8}{3}\right)\left(\frac{8}{5}\right) = (-1)(-1) = 1$ PS

$\left(\frac{4}{15}\right) = \left(\frac{4}{3}\right)\left(\frac{4}{5}\right) = 1 \times 1 = 1$ QR

# Blum-Blum-Shub Generator

## •Jacobi symbol

- Let n be an odd positive integer
- **$p_i$ is the prime factor of n** and $e_i$ is the power of the prime factor
- $(a/p_i)$ is the Legendre symbol and (a/n) is the Jacobi symbol

$$\boxed{n = \prod_{i=1}^{k} p_i^{\,e_i}}$$

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \boxed{\left(\frac{a}{p_i}\right)^{e_i}}$$

- Example: Let **n=15=3*5**
(9/15)=(9/3)(9/5)=0
(11/15)=(11/3)(11/5)=(2/3)(1/5)=(-1)(1)=-1
(8/15)=(8/3)(8/5)=(2/3)(3/5)=(-1)(-1)=1

$$\left(\frac{9}{15}\right) = \left(\frac{9}{3}\right)\left(\frac{9}{5}\right)$$
$$= 0$$

$$\left(\frac{11}{15}\right) = \left(\frac{11}{3}\right)\left(\frac{11}{5}\right)$$
$$= (-1)(1)$$
$$= -1$$

$$11^{3-1/2} = 11 \bmod 3$$
$$= 2 \bmod 3$$
$$= -1 \bmod 3$$

$$11^{(5-1)/2} = 11^2 \bmod 5$$

$$\Rightarrow (11 \bmod 5)(11 \bmod 5)$$
$$= 1 \times 1$$
$$= 1 \bmod 5$$