Blum-Blum-Shub PRG

BBS fixed parameter M

from seed y_0 generate

$$y_{n+1} \equiv y_n^2 \pmod M$$

$M = pq$
p, q large primes
$\equiv 3 \pmod 4$

$PRG(y_0) = x_1 x_2 x_3 \cdots$
where x_i is the least bit of y_i
$x_i \equiv y_i \pmod 2$

EG $M = \underset{7 \cdot 11}{77}$ $\quad y_0 = 3$

$y_1 = y_0^2 \equiv 9 \pmod{77}$ $\quad x_1 = 9 \equiv 1 \pmod 2$
$y_2 = y_1^2 \equiv 4$ $\quad x_2 \equiv 0$
$y_3 = y_2^2 \equiv 16$ $\quad x_3 \equiv 0$

output: $1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1 \cdots$
period 4

comments

- each y_i is an invertible (if y_0 is) quadr. residue
  $\frac{\phi(M)}{4} = \frac{\phi(p)\phi(q)}{4}$ many — here: $\frac{6 \cdot 10}{4} = 15$
- period of BBS PRG divides $\operatorname{lcm}(\phi(p-1), \phi(q-1))$
  here: $\operatorname{lcm}(\phi(6), \phi(10)) = \operatorname{lcm}(2,4) = 4$
- -1 is a quadr. residue mod p $\iff$ $p \equiv 1 \pmod 4$
  in that case: $x \mapsto x^2 \pmod p$ restricted to invertible quadratic residues is not 1-1
- BBS is unpredictable $\iff$ the following is hard

  quadratic residuosity problem
  given $x \pmod M$, decide if x is a quadr. residue

  current best solution: factor M
- in practice: BBS too slow