Fermat Little Theorem

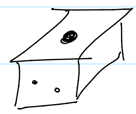
Wednesday, February 16, 2022 12:39 PM

Recall : Pseudorandum Numbers

$$x_n = (a \cdot x_{n-1} + c) \bmod m$$

e.g. $m = 9$, $a = 7$, $c = 4$, $x_0 = 3$

$$\begin{aligned}
x_1 &= 7\cdot(3) + 4 \equiv 7 \pmod 9 \\
x_2 &= 7\cdot(7) + 4 \equiv 8 \pmod 9 \\
x_3 &= 7(8) + 4 \equiv 6 \pmod 9 \\
x_4 &= 7(6) + 4 \equiv 1 \pmod 9 \\
x_5 &= 7(1) + 4 \equiv 2 \pmod 9 \\
x_6 &= 7(2) + 4 \equiv 0 \pmod 9 \\
x_7 &= 7(0) + 4 \equiv 4 \pmod 9 \\
x_8 &= 7(4) + 4 \equiv 5 \pmod 9 \\
x_9 &= 7(5) + 4 \equiv 3 \longrightarrow \text{seed } x_0
\end{aligned}$$



1 — 6

7

8

6

⋮

1] Fermat Little Theorem: (FLT)

if p is prime, then $\forall a$

$$a^p \equiv a \pmod p$$

if a is co-prime to p

$$a^{p-1} \equiv 1 \pmod p$$

e.g.

$\underbrace{\overset{-}{2}\overset{+}{6}\overset{-}{2}}_{+2}\ \underbrace{\overset{+}{7}\overset{-}{8}\overset{+}{2}}_{+1} = 3$

$\underbrace{262}_{+2}\ \underbrace{782}_{+1} = 5$

$0\underbrace{\cancel{5665}}\underbrace{24}_{2}$

e.g.

$$\underline{0566524}^{987} \pmod{11}$$

$$\equiv 2^{987} \qquad 987 \xrightarrow{\text{mod } 10 \text{ by FLT}} 7$$

mod 11

$$\equiv 2^{980} \cdot 2^{7}$$

$$\equiv (2^{10})^{98} \cdot 2^{7}$$

$$\equiv (1)^{98} \cdot 2^{7}$$

$$\equiv 128 \equiv 7 \pmod{11}$$

$a^{n} \pmod{p}$

$a \xrightarrow{\text{mod } p} \bar{a}$, $n \xrightarrow{\text{mod } (p-1)} \bar{n}$

$\bar{a}^{\bar{n}}$

2] Primality Test :

Test if n is prime

① choose a base b, with $\gcd(b, n) = 1$

② if $b^{n-1} \not\equiv 1 \pmod{n}$

$\Longrightarrow$ not prime

else goto ①

e.g.

① is 1003 prime

test $2^{1002} \equiv 990 \pmod{1003}$

$\not\equiv 1$

$\Longrightarrow$ not prime

3] Pseudoprimer

e.g. is 341 prime

test $2^{340} \equiv 1 \pmod{341}$

test $2^{340} \equiv 1 \pmod{341}$

$\Longrightarrow$ pseudoprime to base - 2

$3^{340} \equiv 56 \pmod{341} \Rightarrow$ Not prime

4) Carmichael Numbers

if n is composite and pseudo prime to all basis then it is called a Carmichael number

e.g. $561 = 3.11.17$ is a Carmichael number

$4^{560} \equiv 1 \pmod{561}$

5) Note: for numbers $< 10^{10}$

455×10^6 are primes

only 149×10^3 are pseudoprime to base 2