Shor Algorithm

Sunday, December 11, 2022 8:31 PM

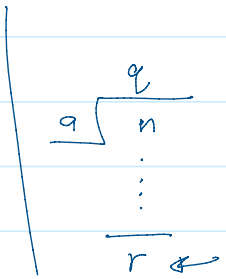
1] Modular Arithmetic

Calculations are done in modulo n

2] The mod function

for any integer a and $n > 0$, $a \bmod n$ is the remainder r of $a \div n$

i.e. $a = q \cdot n + r \quad ; \quad 0 \le r < n$



e.g.

$143 \bmod 7 = 3$

$11 \bmod 3 = 2$

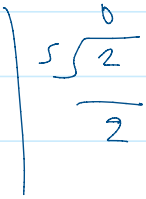
$10 \bmod 3 = 1$

$9 \bmod 3 = 0$

$8 \bmod 5 = 2$

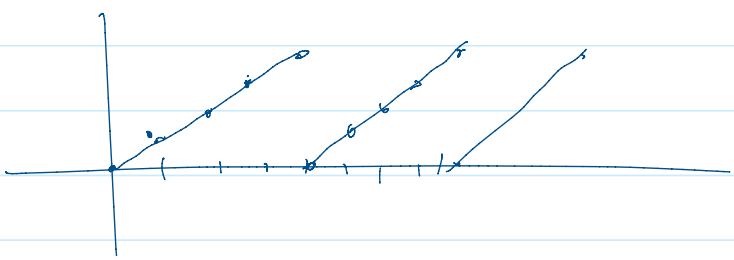
$7 \bmod 3 = 1$

$17 \bmod 3 = 2$



3] e.g. The mod 5 function

a	0	1	2	3	4	5	6	7
$a \bmod 5$	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0



4] The $F_{a,N}(x)$ mod function

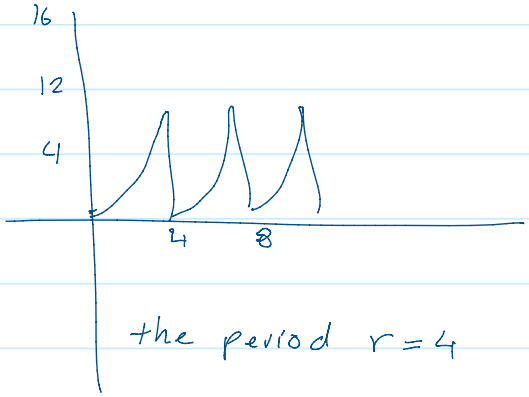
$$F_{a,N}: \mathbb{Z} \longrightarrow \{0, 1, 2, \cdots, N-1\}$$

$$F_{a,N}(x) = a^x \bmod N$$

$$15 \overline{)\,45}\quad 3,\ 45,\ 0$$

e.g. $a = 2$, $N = 15$

	x	2^x	$F = 2^x \bmod 15$
	1	2	2
	2	4	4
	3	8	8
$r \longrightarrow$	4	16	1
	5	32	2
	6	64	4
	7	128	8
	8	256	1
	9	512	2
	10	1024	4



the period $r = 4$

5] Greatest Common Divisor $\gcd(a, b)$

e.g. $\gcd(24, 36)$

common factors: 2, 3, 4, 6, 12

$\therefore \gcd(24, 36) = 12$

6] Euclidean Algorithm: $\gcd(a, b) = \gcd(b \bmod a, a)$

e.g. $36 = 1 \cdot 24 + 12$
$24 = 2 \cdot 12 + 0$ ← gcd

gcd (24, 36)
= gcd (12, 24)
= gcd (0, 12) = 12

e.g. Find gcd (252, 414)

$414 = 1 \cdot 252 + 162$
$252 = 1 \cdot 162 + 90$
$162 = 1 \cdot 90 + 72$
$90 = 1 \cdot 72 + 18$
$72 = 4 \cdot 18 + 0$ ← gcd

252

7] Shor Algorithm

See the ppt slides on Shor's algrithm