U20CS005.

PAGE NO.
DATE / /

Tutorial-4

Q1 a) Given a = 84 and b = 320, find gcd(a,b) and value of s and t.

→

Q	A	B	R	s_1	s_2	s	t_1	t_2	t
0	84	320	84	1	0	1	0	1	0
3	320	84	68	0	1	-3	1	0	1
1	84	68	16	1	-3	4	0	1	-1
4	68	16	4	-3	4	-19	1	-1	5
4	16	4	0	4	-19	80	-1	5	-21
-	4	0	-	-19	80	-	5	-21	-
	↓ gcd			↓ s			↓ t		

gcd(84, 320) = 4 , s = -19 , t = 5.

b) Given a = 161 and b = 28, find gcd(a,b) and value of s and t

Q	a	b	R	s_1	s_2	s	t_1	t_2	t
5	161	28	21	1	0	1	0	1	-5
1	28	21	7	0	1	-1	1	-5	6
3	21	7	0	1	-1	4	-5	6	-23
-	7	0	-	-1	4	-	6	-23	-
	↓ gcd			↓ s			↓ t		

gcd(161, 28) = 7 , s = -1 , t = 6.

c) Given a = 17 and b = 0, find gcd(a,b) and value of s and t

Q	a	b	R	s_1	s_2	s	t_1	t_2	t
-	17	0	-	1	0	-	0	1	-
	↓ gcd			↓ s			↓ t		

gcd(17, 0) = 17, s = 1, t = 0.

d) Given a = 0 & b = 45, find gcd(a,b) & values of s & t.

Q	a	b	R	s_1	s_2	s	t_1	t_2	t	gcd(0,45) = 45
0	0	45	0	1	0	1	0	1	0	
-	45	0	-	0	1	-	1	0	-	s = 0, t = 1
	↓ gcd			↓ s			↓ t			

PAGE NO.
DATE / /

2. Find the result of $6^{10} \bmod 11$

→ $6^{10} \bmod 11 = (6^2)^5 \bmod 11$

$= (36)^5 \bmod 11$

$= 3^5 \bmod 11$

$= (27)(9) \bmod 11$

$= (27 \bmod 11 \times 9 \bmod 11) \bmod 11$

$= (5 \times 9) \bmod 11$

$= 45 \bmod 11$

$6^{10} \bmod 11 = 1$

3. Find the result of $3^{12} \bmod 11$

→ $3^{12} \bmod 11 = (3^3)^4 \bmod 11$

$= (27)^4 \bmod 11$

$= (5^4) \bmod 11$

$= (25)(25) \bmod 11$

$= (25 \bmod 11 \times 25 \bmod 11) \bmod 11$

$= 9 \bmod 11$

$3^{12} \bmod 11 = 9$

4. We know that 61 is a prime, let us see if it passes the Miller-Rabin test.

→ Miller-Rabin test

S-1) Find m and k such that $n-1 = m \times 2^k$

S-2) If $k \leq 1$, calculate T such that $T = a^m \bmod n$

If $T = \pm 1$, no. is prime

Else composite

If $k > 1$, calculate T' such that $T' = T^2 \bmod n$,

$T = a^m \bmod n$

If $T' = -1$, no. is composite prime

Else composite

choose a such that $1 < a < n-1$.

$n-1 = m \times 2^k$

$60 = 15 \times 2^2$

let $a=2$, $T = a^m \bmod n$.

$n=61$, $m=15$

$\Rightarrow T = 2^{15} \bmod 61$

$T = (2^6 \times 2^6 \times 2^3) \bmod 61$

$= (64)(64)(8) \bmod 61$

$= ((64^2 \bmod 61)(8 \bmod 61)) \bmod 61$

$= (9 \times 8) \bmod 61$

$= 72 \bmod 61$

$\Rightarrow T = 11.$

$T' = T^2 \bmod 61$

$= 11^2 \bmod 61$

$= (122-1) \bmod 61$

$T' = -1. \Rightarrow n=61$ is a prime number

5. a) Show that inverse of $5 \bmod 101$ is 5^{99}.

→ $5^{-1} \bmod 101$

$a^{p-1} \equiv 1 \bmod p.$

$a^{-1} \bmod p. \equiv a^{p-2} \bmod p$

$= 5^{101-2} \bmod 101$

$5^{-1} \bmod 101 = 5^{99} \bmod 101$

b) Use repeated squaring to simplify $5^{99} \bmod 101$

→ $5^1 \bmod 101 = 5$

$5^2 \bmod 101 = 25$

$5^4 \bmod 101 = 625 \bmod 101 = 19$

$5^8 \bmod 101 = (5^4)^2 \bmod 101 = 19^2 \bmod 101 = 58.$

$5^{16} \bmod 101 = (5^8)^2 \bmod 101 = 58^2 \bmod 101 = (116)(29) \bmod 101 = 31$

$5^{32} \bmod 101 = (31)^2 \bmod 101 = 52$

$5^{64} \bmod 101 = 52^2 \bmod 101 = 49^2 \bmod 101 = (343)(7) \bmod 101 = 78.$

99 in binary = 1100011

$\Rightarrow 5^{99} = 5^{(64+32+2+1)}$

$5^{99} \bmod 101 = 5^{64} \cdot 5^{32} \cdot 5^{2} \cdot 5^{1} \bmod 101$

$= (78)(52)(25)(5) \bmod 101$

$= (390)(260)(5) \bmod 101$

$= (390 \bmod 101 \times 260 \bmod 101 \times 5 \bmod 101) \bmod 101$

$= ((-14) \times (-43) \times 5) \bmod 101$

$= (14)(215) \bmod 101$

$= (14 \bmod 101 \times 215 \bmod 101) \bmod 101$

$= (14 \times 13) \bmod 101$

$5^{99} \bmod 101 \equiv 81$

c) Hence solve the equation $5x \equiv 31 \bmod 101$

→ $5x \equiv 31 \bmod 101$

$5^{-1} \times 5x \equiv 5^{-1} \times 31 \bmod 101$

$x = (5^{-1} \bmod 101 \times 31 \bmod 101) \bmod 101$

$= (5^{99} \bmod 101 \times 31 \bmod 101) \bmod (101)$

(From Fermat's little theorem)

$= (81 \times 31) \bmod 101$

$= (-20)(31) \bmod 101$

$x = ((-1) \bmod 101 \times 620 \bmod 101) \bmod 101$

$= (100 \times 14) \bmod 101$

$= 1400 \bmod 101$

$x = 87.$