11) Find the multiplicative inverse of each of the following using extended Euclidean algorithm

given 2 integers a, b find other 2 integers s, t such that $sx a + t x b = gcd(a, b)$

(a) 38 mod 180 $\quad gcd(38, 180) = 1$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
	180	38		1	0	1	0	1	-4
4	38	28	28	0	1	-1	1	-4	5
1	28	10	10	1	-1	3	-4	5	-14
2	10	8	8	-1	3	-4	5	-14	19
1	8	2	2	3	-4	19	-14	19	-90
4	2	0	0	-4	19	-	19	-90	-
-			-	19					

Now $sx a + t x b = gcd(a, b)$ if $gcd(a, b) = 1$ then inverse of a mod b

$= -4 \times 180 + 19 \times 38$ $\quad$ $r_2 = b \bmod a$

$= 2$

Hence multiplicative inverse doesn't exist

(b) 7 mod 180

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
	180	7		1	0	1	0	1	-25
25	7	5	5	0	1	-1	1	-25	26
1	5	2	2	1	-1	3	-25	26	-77
2	2	1	1	-1	3	-7	26	-77	190
2	1	0	0	3	-7	-	-77	190	-
-			-	-7					

$26 \times 2 \times 77$

$26 + 154$

$sx a + t x b = gcd(a, b)$

$3 \times 180 - 7 \times 77$

$= 1$

Hence multiplicative inverse of

$7 \bmod 180 \Rightarrow -77 \equiv 103 \bmod 180$

So inverse of $7 \bmod 180$ is 103

(c) 132 mod 180

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
	180	132	48	1	0	1	0	1	-1
1	132	48	36	0	1	-2	1	-1	3
2	48	36	12	1	-2	3	-1	3	-4
1	36	12	0	-2	3	-11	3	-4	15
3	12	0	-	3	-11	-	-4	15	-
-									

$sXa + tXb = gcd(a,b)$

$3X180 - 4X132$

$= 12$

Since gcd (a,b) $\neq 1$, so multiplicative inverse doesn't exist

(d) 24 mod 180

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
	180	24	12	1	0	1	0	1	-7
7	24	12	0	0	1	-2	1	-7	15
2	12	0	-	1	-2	-	-7	15	-
-									

$sXa + tXb = gcd(a,b)$

$12X180 - 7X132$

$= 12$

Since gcd (a,b) $\neq 1$, inverse don't exist

12) Find particular and general soln to the following linear diophantine equations

(a) $25x + 10y = 15$

(b)

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
2	25	10	5	1	0	1	0	1	-2
2	10	5	0	0	1	-2	1	-2	5
-	5	0	-	1	-2	-	-2	5	-

$s=1 \quad t=-2 \qquad 5 \times a + t \times b = 25 \times 1 - 2 \times 10$

$= 5$

So, gcd $(25, 10) = 5$

Divide 5 by eqn:

$\frac{25x}{5} + \frac{10y}{5} = \frac{15}{5} \Rightarrow 5x + 2y = 3$

$s=1 \quad t=-2 \qquad a_1 \times s + b_1 \times t = 1$

$5s + 2 \times t = 1$

Particular soln: $x_0 = (c/d)s = 3 \times 1 = 3$

$y_0 = (c/d)t = 3 \times -2 = -6$

General soln:

$x = x_0 + k(b/d) \qquad y = y_0 - k(a/d)$

$= 3 + k(10/5) \qquad = -6 - k(25/5)$

$= 3 + 2k \qquad = -6 - 5k$

when $k=0 \quad x=3 \qquad y = -6 \quad (3, -6)$ is a soln

(b) $19x + 13y = 20$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
-	19	13	6	1	0	1	0	1	-1
1	13	6	1	0	1	-2	1	-1	3
2	6	1	0	1	-2	13	-1	3	-19
6	1	0	-	-2	13	-	3	-19	-

$19 \times -2 + 3 \times 13$

$-38 + 39 = 1 = g(d(a, b))$

$19x + 13y = 20$

General soln:

$19x + 13y = 20$

$x_0 = (c/d)s = 20 \times -2 = -40$

$y_0 = (c/d)t = 20 \times 3 = +60$

Particular soln:

$x = x_0 + (b/d)k \qquad y = y_0 - k(a/b)$

$= -40 + 13k \qquad = 60 - 19k$

$k = 0 \quad x = -40 \qquad y = 60$

$(-40, 60)$ is a soln

(i) $14x + 21y = 77$

$r_1 = 14 \quad r_2 = 21 \quad c = 77$

$-1 - 2 \times 4$

q	r_4	r_2	r	s_1	s_2	s	t_1	t_2	t
0	14	21	14	1	0	1	0	1	0
1	21	14	7	0	1	-1	1	0	1
2	14	7	0	1	-1	3	0	1	-2
-	7	0	-	-1	3	-	1	-2	-

$-1 \times 14 + 1 \times 21 = 7 = \gcd(a, b)$

$-1 \times a + 1 \times b = 7$

General soln

$d = 7$

$\frac{14}{7}x + \frac{21}{7}y = \frac{77}{7} \qquad s = -1 \quad t = 1$

$2x + 3y = 11$

$x_0 = (c/d)s = 11 \times -1 = -11$

$y_0 = (c/d)t = 11 \times 1 = 11$

Particular soln

$x = x_0 + (b/d)k \qquad y = y_0 - k(a/b)$

$= -11 + 3k \qquad = 11 - 2k$

$x = -11 \qquad y = 11$

$(-11, 11)$ is a solution

(d) $40x+16y=88$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
2	40	16	8	1	0	1	0	1	-2
2	16	8	0	0	1	-2	1	-2	5
-	8	0	-	1	-2	-	-2	5	-

$s \times a + t \times b = 1 \times 40 - 2 \times 16$

$40 - 32$

$= 8 = \gcd(a,b)$

general soln:

$\left(\frac{40}{8}\right)x + \left(\frac{16}{8}\right)y = \left(\frac{88}{8}\right)$

$5x + 2y = 11$

$x_0 = (c/d)s = 11 \times 1 = 11$

$y_0 = (c/d)t = 11 \times -2 = -22$

Particular soln:

$X = x_0 + (b/d)k \qquad Y = y_0 - k(a/d)$

$= 11 + 2k \qquad = -22 - k(5)$

$k=0 \quad x = 11 \qquad y = -22$

$(11, -22)$ is a solution

(3) Show that there are no solutions to the following linear equations (a) $15x + 12y = 13$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
1	15	12	3	1	0	1	0	1	-1
4	12	3	0	0	1	-4	1	-1	5
-	3	0	-	1	-4	-	-1	5	-

$s \times a + t \times b = \gcd(a,b)$

$1 \times 15 + -1 \times 12$

$15 - 12 = 3$

Since $d = \gcd(a,b) = 3$ and d doesn't divide c

So there is no solution to the given equation

(b) $18x + 30y = 20$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
0	18	30	18	1	0	1	0	1	0
1	30	18	12	0	1	-1	1	0	1
1	18	12	6	1	-1	0	0	1	-1
2	12	6	0	-1	0	-1	1	-1	3
-	6	0	-	0	-1	-	-1	3	-

$d = \gcd(a,b) = sXa + tXb$

$0X18 + -1X30$

$= -30$

since $d = -30$ doesn't divide 20 so there is no solution

(c) $15x + 25y = 69$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
0	15	25	15	1	0	1	0	1	0
1	25	15	10	0	1	-1	1	0	1
1	15	10	5	1	-1	2	0	1	-1
2	10	5	0	-1	2	-5	1	-1	3
-	5	0	-	2	-5	-	-1	3	-

$d = \gcd(a,b) = sXa + tXb$

$2X15 + -1X25$

$30 - 25$

$= 5$

since $d = 5$ doesn't divide 69. so there is no solution exist

(d) $40x + 30y = 98$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
1	40	30	10	1	0	1	0	1	-1
3	30	10	0	0	1	-3	1	-1	4
-	10	0	-	1	-3	-	-1	4	-

$d = \gcd(a,b) = sXa + tXb$

$= 1X40 + -1X30$

$= 40 - 30$

$= 10$

since $d = 10$ doesn't divide 98, so there is no solution exist

(4) $3x \equiv 4 \pmod 5$

gcd(3,5)

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
0	3	5	3	1	0	1	0	1	0
1	5	3	2	0	1	-1	1	0	1
1	3	2	1	1	-1	2	0	1	-1
2	2	1	0	-1	2	-5	1	-1	2
-	1	0	-	2	-5	-	-1	2	-

gcd(a,b) = sxa + txb

= 2x3 + (-1)x5

= 1 (exactly 1 solution)

$3x \equiv 4 \pmod 5$

$x \equiv 4x(3^{-1}) \bmod 5$

$(3^{-1}) \bmod 5 \quad (3^{-1} = i) \Rightarrow 6i = 1$

$3x2 \bmod 5$

$6 \bmod 5$

$= 1$

So: $x_0 \equiv 4x(2) \bmod 5$

$\equiv 8 \bmod 5$

$= 3$

$x_j = x_{0+1}(5)k$

$k=0 \quad x_1 = 3$

b) $4x \equiv 4 \pmod 6$

gcd(4,6) = 2

q	r_1	r_2	r
1	6	4	2
2	4	2	0
-	2	0	-

gcd = 2 (exactly 2 sol^n)

dividing by 2 we'll get

$2x \equiv 2 \pmod 3$

$x = 2x2^{-1} \bmod 3$

$2^{-1} \bmod 3$ So $2^{-1} \bmod 3 = 2$

$= (2x2) \bmod 3$

$x_0 = 2 \times 2^{-1} \bmod 13$

$2 \times 2 \bmod 13$

$= 1$

$x_1 = x_0 + (n/d)k$

$= 1 + (6/2)k$

$k=0 \quad x_1 = 1$

$k=1 \quad x_1 = 1+3 = 4$

c) $9x \equiv 12 \pmod 7$

$\gcd(9,7) = 1$

q	r_4	r_3	r	s_1	s_2	s	t_1	t_2	t
1	9	7	2	1	0	1	0	1	-1
3	7	2	1	0	1	-3	1	-1	4
2	2	1	0	1	-3	7	-1	4	-9
7	1	0	-	-3	7	-	4	-9	-

$\gcd = 9 \times -3 + 7 \times 4$

$= 1$ (1 solution)

$9x \equiv 12 \pmod 7$

$x \equiv (12 \times 9^{-1}) \bmod 7$

$x_0 = (12 \times 4) \bmod 7$

$= 48 \bmod 7$

$= 6$

$x_1 = x_0 + (n/d)k$

$= 6 + 7k$

$k=0 \quad x_1 = 6$

$9^{-1} \bmod 7$

$= 9 \times 4 \bmod 7$

$= 1$

hence $9^{-1} = 4$

d) $256x \equiv 442 \pmod{60}$

q	r_4	r_2	r	s_1	s_2	s	t_1	t_2	t
4	256	60	16	1	0	1	0	1	-4
3	60	16	12	0	1	-3	1	-4	13
1	16	12	4	1	-3	4	-4	13	-17

3	12	4	0	-3	4	-15	13	-17	+64
-	9	10	-	4	-15	-	-17	64	-

gcd(9,15) = 5×9 + 4×15

4×256 + 17×80

= 4 (since 4 doesn't divide 442

eqn reduced to 64x ≡ So, the following eqn has no solution)

15) Find the solutions to the following linear equations:

(a) $3x + 5 \equiv 4 \pmod 5$

Adding additive inverse of 5 to both side

$3x + 5 - 5 \equiv 4 - 5 \pmod 5$

$3x \equiv -1 \pmod 5$

$3x \equiv 4 \pmod 5$

Since (3, 5 are coprimes gcd(3,5) = 1 (only 1 solution)

So, $3x \equiv 4 \pmod 5$

$x_0 \equiv 4 \times 3^{-1} \bmod 5$

$3^{-1} \bmod 5$

$= (3 \times 2) \bmod 5$

$6 \bmod 5$

$= 1$

So $3^{-1} \bmod 5 = 2$

$x_0 = 4 \times 2 \bmod 5$

$8 \bmod 5$

$= 3$

$x_1 = x_0 + (n)d\ k$

$k = 0$ $x_1 = x_0$

$= 3$

(b) $4x + 6 \equiv 4 \pmod 6$

gcd(4,6) = 2

Adding additive inverse of 6 both side i.e -6

$4x + 6 - 6 \equiv 4 - 6 \pmod 6$

$4x \equiv -2 \bmod 6$

$\equiv 4 \bmod 6$

gcd(4,6) = 2

q	r_1	r_2	r
	6	4	2
1	4	2	0
2	2	0	-

gcd = r_1 = 2

Dividing both side we'll get equation 2 solution)

$2x \equiv 2 \bmod 3$

$x \equiv 2 \times 2^{-1} \bmod 3$ $\quad 2^{-1} \bmod 3 \Rightarrow 2 \times 2 \bmod 3$

$= 4 \bmod 3$

$x_0 = 2 \times 2 \bmod 3$ $\quad = 1$

$= 1$ $\quad$ So $2^{-1} \bmod 3 = 2$

$x_1 = x_0 + (n/d)k$

$= 1 + 1.3k$

$k=0 \quad x_1 = 1$

$k=1 \quad x_1 = 4$

c) $9x + 4 \equiv 12 \pmod 7$

Adding additive inverse of 4 i.e -4 to both sides $9x + 4 - 4 \equiv 12 - 4 \bmod 7$

$9x \equiv 8 \bmod 7$

Since (9,7) are co-prime $\gcd(9,7) = 1$; exactly 1 solution

eqn become $x \equiv 8 \times 9^{-1} \bmod 7$

$9^{-1} \bmod 7$

$(9 \times 4) \bmod 7$

$36 \bmod 7$

$= 1$

So $9^{-1} \bmod 7 = 1$

$x_0 = 8 \times 4 \bmod 7$

$= 32 \bmod 7$

$= 4$

$x_1 = x_0 + (n/d)k$

$= 4 + 7k$

$k=0 \Rightarrow x_1 = 4$ is the solution

d) $232x + 42 \equiv 248 \pmod{50}$

Adding additive inverse of 42 i.e -42 to both sides

$232x + 42 - 42 \equiv 248 - 42 \pmod{50}$

$232x \equiv 206 \pmod{50}$

$\gcd(232, 50)$

gcd = 2

eqn reduced to $116x \equiv 103 \pmod{24}$

$116x \equiv 103 \bmod 24$

$x = 103 \times 116^{-1} \bmod 25 = 103 \times 11 \bmod 24$

$= 1480\ 1133 \bmod 24$

233

$x_1 = x_0 + 25k$

$k=0\ x_1 = x_0 = 33$

$k=0 \quad x_1 = x_0 = 33$

16) prove that Group $Z = \langle Z_4, + \rangle$ is an abelian group

(a) $Z_4 = \{0,1,2,3\}$ with operation addition modulo 4

properties:

closure: $\forall a, b \in Z_4 \rightarrow (a+b) \bmod 4 \in Z_4$

Associativity: $(a+b)+c = a+(b+c) \bmod 4$

identity: $0 \in Z_4$ is identity

i.e $a+0 = a$

inverse: for each a, there exists b such that

$a+b \equiv 0 \bmod 4$

$0+0, \bmod 4 = 0$

$1+3 \bmod 4 = 0$

$2+2 \bmod 4 = 0$

$3+1 \bmod 4 = 0$

hence, Z_4 under addition is an abelian group

(b) show $3+2$ and $3-2 \bmod 4$

$3+2 \bmod 4 = ((3 \bmod 4) + (2 \bmod 4)) \bmod 4$

$= 5 \bmod 4 \quad = 3+2 \bmod 4$

$= 5 \bmod 4$

$= 1$

$3-2 \bmod 4 = (3 \bmod 4 - 2 \bmod 4) \bmod 4$

$(3-2) \bmod 4 = 1 \bmod 4 = 1$

b) For the group $G = \langle Z_6^*, \times \rangle$:

(a) prove that it is an abelian group

Z_6^* is a multiplicative group of integers modulo 6

$Z_6^* = \{1, 5\}$

elements: $\{1, 5\}$

$1 \times 1 = 1$, $1 \times 5 = 5$, $5 \times 5 = 25 \equiv 1 \pmod 6$

Closure: for $\forall a, b \in Z_6^* \rightarrow (a \times b) \bmod 6 \in Z_6^*$

commutative for $\forall a, b \in Z_6^*$ $(a \times b) \bmod 6 = (b \times a) \bmod 6 \in Z_6^*$

identity: $1 \in Z_6^*$ is an identity

ie $1 \times a = a$

inverse: $5 \times 5 \equiv 1 \bmod 6$ exists

so, it is a finite abelian group

(b) show result of 5×1, and $1 \neq 5$

$5 \times 1 \bmod 6 = 5 \bmod 6$

ie $5 \times 1 \bmod 6 = ((5 \bmod 6) \times (1 \bmod 6)) \bmod 6$

$5 \times 1 \bmod 6$

$= 5 \bmod 6$

$1 \neq 5 \bmod 6 = 1 \times 5^{-1} \bmod 6 = (1 \times 5) \bmod 6$

$= ((1 \bmod 6) \times (5 \bmod 6)) \bmod 6$

$= 1 \times 5 \bmod 6$

$= 5 \bmod 6$

$= 5$

$5^{-1} \bmod 6 = (5 \times 5) \bmod 6$

$25 \bmod 6$

$= 1$

So, $5^{-1} \bmod 6 = 5$

c) why we should not worry about division by zero, in this group

in Z_6^*, we only include non-zero elements that are coprime to 6 $\rightarrow$ 0 is excluded, so division by 0 is undefined and avoided

18) sub groups of the

Lagrange's theorem: order of a sub group divides the order of group

(a) $G = \langle Z_{18}, + \rangle$ → order = 18

divisors of 18 → {1, 2, 3, 6, 9, 18}

possible sub group orders $|H|=1$ $|H|=2$ $|H|=3$ $|H|=6$ $|H|=9$ $|H|=18$

(b) $G = \langle Z_{29}, + \rangle$ order = 29 (prime)

divisors = {1, 29}

sub-group orders: $|H|=1$ $|H|=29$

(c) $G = \langle Z_{12}, \times \rangle$ → $Z_{12} = \{1, 5, 7, 11\}$

sub-group orders: {1, 2, 4}

(d) $G = \langle Z_{19}, \times \rangle$:

has $\phi(19) = 18$ elements

sub-group orders = {1, 2, 3, 6, 9, 18}

19) Represent n-bit words as polynomial

(a) 10010 → $0 \times x^0 + 1 \times x^1 + 0 \times x^2 + 0 \times x^3 + 1 \times x^4$

$= x^4 + x$

(b) 10 → $0 \times x^0 + 1 \times x^1$

$= 0 + x$

$= x$

(c) 100001 → $1 \times x^0 + 1 \times x^5$

$= 1 + x^5$

$= x^5 + 1$

(d) 00011 → $1 \times x^0 + 1 \times x^1$

$= 1 + x$

$= x + 1$

20) Find the 4-bit word that is represented by each of the following polynomials

(a) x^2+1 in $GF(2^4)$

Polynomial degree $= 4-1 = 3$

$0.x^4 + 0.x^3 + 1.x^2 + 0.x^1 + 1.x^0$

this is related to 4 bit word 0101

(b) x^2+1 in $GF(2^5)$

degree $= 5$

polynomial degree $= 5-1 = 4$

$0.x^4 + 0.x^3 + 1.x^2 + 0.x^1 + 1.x^0$

collecting word bits $= 00101$

(c) $x+1$ in $GF(2^3)$

polynomial degree $= 2$

$0.x^2 + 1.x^1 + 0.x^0.1$

collecting word bits $= 011$

(d) x^7 in $GF(2^8)$

polynomial degree $= 7$

$1.x^7 + 0.x^6 + 0.x^5 + 0.x^4 + 0.x^3 + 0.x^2 + 0.x^1 + 0.x^0$

collecting word bits $= 10000000$

21) multiply the following 4-bit words using polynomial

(a) 11×10

$11 = x^1 x 1 + x^0 \cdot 1$

$= x+1$

$10 = x^1 + 0 x x^0$

$= x^1$

$(11) \times 10 = (x+1)x$ binary result $= 110$

$= x^2 + x$

(b) 1010 × 1000

1010 = $x^3 + x^2 + 1$ = $x^3 + x$

1000 = x^3

1010 × 1000 = $(x^3 + x)x^3$

= $x^6 + x^4$ = $1.x^6 + 0.x^5 + 1.x^4 + 0.x^3 + 0.x^2 + 0.x + 0$

resulting word bits = 1010000

(c) 11100 × 10000

11100 = $1.x^4 + 1.x^3 + 1.x^2$ 10000 = x^4

= $x^4 + x^3 + x^2$ = x^4

11100 × 10000 = $(x^4 + x^3 + x^2).x^4$

= $x^8 + x^7 + x^6$

resulting word bits = 111000000

22) find multiplicative inverse of the following in GF(2^4):

(a) 1

For a non-zero element $a \in GF(2^4)$, the inverse of the element b such that

$a.b \equiv 1 \bmod p(x)$

$1.b = 1^{-b} \bmod (x^2+x+1)$

$b = 1.1^{-1} \bmod (x^2+x+1)$

$= 1$

(b) x

$x.b = 1 \bmod (x^2+x+1)$

$b = x^{-1} \bmod (x^2+x+1)$

$= x.x \cdot \bmod (x^2+x+1)$

$= x^2 \bmod (x^2+x+1)$

$\neq 1$ (x)

For $b = x+1$

$x.(x^2+1) \bmod (x^2+x+1)$

$= x^2+x \bmod (x^2+x+1)$

$= 1$ So inverse of $(x+1)$

$(x+1)\cdot b \equiv 1 \mod (x^2+x+1)$

$b = (x+1)^{-1} \mod (x^2+x+1)$

let $b = x$ $\quad x(x+1) \mod x^2+x+1$

$x^2+x \mod x^2+x+1$

$= 1$

so inverse of $x+1$ is 1

(Q3) use extended euclidan algorethm to find inverse of (x^4+x^3+1) in GF(25) using modulus (x^5+x^2+1) so inverse = $6x^4 - x^2 + 25/16$

q	r_1	r_2	r	t_1	t_2	t
$x+1$	x^5+x^2+1	x^4+x^3+1	x^3+x^2+x	0	1	$x+1$
x	x^4+x^3+1	x^3+x^2+x	x^2+1	1	$x+1$	x^2+x+1
x	x^3+x^2+x	x^2+1	x^2	$x+1$	x^2+x+1	x^3+x^2+1
1	x^2+1	x^2	1	x^2+x+1	x^3+x^2+1	x^3+x
x^2	x^2	1	0	x^3+x^2+1	x^3+x	x^5+x^2+1
x	1	0	x	x^2+x	x^5+x^2+1	x

(4) using approximation find number of primes between 100,000 and 200,000

$$\pi(200,000) = \frac{200000}{\ln(200000)} = \frac{200000}{12.206} = 16,385$$

$$\pi(100,000) = \frac{100000}{\ln(100000)} = \frac{100000}{11.513} = 8,686$$

$\pi(200000) - \pi(100000)$

$= 16,385 - 8,686$

$= 7,699$

(b) find Number of composite integers between 100,000 and 200,000

total no of integers in range $= 200000 - 100000$

$= 100000$

total no. of integers - total no. of primes

$= 100000 - 7,699$

$= 92,301$

4) Ratio of primes to composite in above range and compare it to the same between 1 and 10

(i) Ratio for 100000 to 200000

primes: 7,699 composites: 92,301

$\text{Ratio} = \frac{7,699}{92,301} \approx 0.083$

(ii) Ratio for 1 to 10

primes: 2, 3, 5, 7 (4)

composites: 4, 6, 8, 9, 10 (5)

Ratio (primes/composites) $= 4/5 = 0.8$

Ratio in (1-10) is higher than ratio in 100000 - 200000

(25) Find the value of

(a) $\phi(29)$

Since 29 is a prime $\phi(29) = 29 - 1 = 28$

(b) $\phi(32)$

$\phi(p^k) = p^k - p^{k-1}$

$\phi(32) = \phi(2^5) = 2^5 - 2^4 = 32 - 16 = 16$

(c) $\phi(80)$

$80 = 2^4 \times 5$

$\phi(80) = \phi(2^4 \times 5) = \phi(2^4) \times \phi(5)$

$= (2^4 - 2^3) \times 4$

$= 8 \times 4 = 32$

(d) $\phi(100)$

$100 = 2^2 \times 5^2$

$\phi(100) = \phi(2^2 \times 5^2) = \phi(2^2) \times \phi(5^2)$

$= (2^2 - 2) \times (5^2 - 5)$

$= 2 \times 20 = 40$

(e) $\phi(101)$

Since 101 is a prime

$\phi(101) = 101 - 1 = 100$

26) Find the result of the following

(a) $5^{15} \bmod 13$

$5^{15} \bmod 13 = (5^{12} \times 5^3) \bmod 13$

$= (5^{12} \bmod 13) \times (5^3 \bmod 13)$

$5^{12} \bmod 13 = 5^{13-1} \bmod 13$ $a^{p-1} \equiv 1 \bmod p$

$= 1 \bmod 13$

$= 1$

$5^3 \bmod 13 = 125 \bmod 13 = 8$

So $5^{15} \bmod 13 = 1 \times 8 = 8$

(b) $15^{18} \bmod 17$

$15^{18} = 15^{17} \times 15$ $a^p \bmod p \equiv a \bmod p$

$15^{18} \bmod 17 = (15^{17} \bmod 17) \times (15 \bmod 17)$

$= 15 \bmod 17 \times 15 \bmod 17$

$= 15 \times 15 = 225 \bmod 17 = 4$

(c) $456^{17} \bmod 17$

$a^p \equiv a \bmod p$

$456^{17} \bmod 17 \equiv 17 \bmod 17$

$\equiv 1$

(d) $145^{102} \bmod 101$

$(145^{102} \bmod 101) = (145^{101} \times 145) \bmod 101$

$= (145^{101} \bmod 101) \times (145 \bmod 101)$

$= (145 \bmod 101) \times (145 \bmod 101)$

$= (44 \times 44) \bmod 101$

$= 817$

27) Find the inverse of the following

(a) $5^{-1} \bmod 13$

$5^{-1} \bmod 13 = 5^{13-2} \bmod 13$

$= 5^{11} \bmod 13 = (5^5 \cdot 5^6) \bmod 13$

$= (5^5 \cdot 5^{6-3}) \bmod 13$

$= (5^5 \cdot (5^2)^3) \bmod 13$ $5^2 \bmod 13 = 25 \bmod 13$

$= (5^5 \cdot (12)) \bmod 13$ $= 12$

$= (5 \cdot 12) \bmod 13 = 60 \bmod 13 = 8$

(b) $15^{-1} \bmod 17$

$= 15^{17-2} \bmod 17$

$= 15^{15} \bmod 17 = (15^3)^5 \bmod 17$ $15^3 \bmod 17$

$= (9)^5 \bmod 17$ $= 9$

$= 8 \bmod 17$

$= 8$

(c) $27^{-1} \bmod 41$

$27^{-1} \bmod 41 = 27^{41-2} \bmod 41 = 27^{39} \bmod 41$

$(27^{39} \bmod 41) = (27^3)^{13} \bmod 41$

$= 3^{13} \bmod 41$

$= (3^1 \cdot 3^6) \bmod 41 = (14 \times 32) \bmod 41$

$= 38$

(d) $70^{-1} \bmod 101$

$70^{-1} \bmod 101 = 70^{101-2} = 70^{99} \bmod 101$

$70^{99} \bmod 11 = (70^9)^{11} \bmod 101 = (60)^{11} \bmod 101$

$= (60 \cdot 60^6) \bmod 11 = (91 \cdot 60) \bmod 101$

$= 6$

28) Find the value of x for the following sets of congurence using chinese remender theorm

(a) $x \equiv 2 \bmod 7 \quad x \equiv 3 \bmod 9$

(i) $m = 7 \times 9 = 63$

(ii) $m_1 = 63/7 = 9 \quad m_2 = 63/9 = 7$

(iii) $m_1^{-1} = 9^{-1} \bmod 7 = 9^{7-2} \bmod 7 = 9^5 \bmod 7 = 4$

$m_2^{-1} = 7^{-1} \bmod 9 = 7^{9-2} \bmod 9 = 7^7 \bmod 9 = 7$

(iv) $x = (a_1 \times m_1 \times m_1^{-1} + a_2 \times m_2 \times m_2^{-1}) \bmod 63$

$(2 \times 9 \times 4 + 3 \times 7 \times 7) \bmod 63$

$= 219 \bmod 63$

$= 30$

(b) $x \equiv 4 \bmod 5$ and $x \equiv 10 \bmod 11$

(i) $m = 5 \times 11 = 55$

(ii) $m_1 = 55/5 = 11 \quad m_2 = 55/11 = 5$

(iii) $m_1^{-1} = 5\ 11^{-1} \bmod 5 = 11^{5-2} \bmod 5 = 11^3 \bmod 5 = 1$

$m_2^{-1} = 5^{-1} \bmod 11 = 5^{11-2} \bmod 11 = 5^9 \bmod 11 = 9$

$x = (a_1 \times m_1 \times m_1^{-1} + a_2 \times m_2 \times m_2^{-1}) \bmod 55$

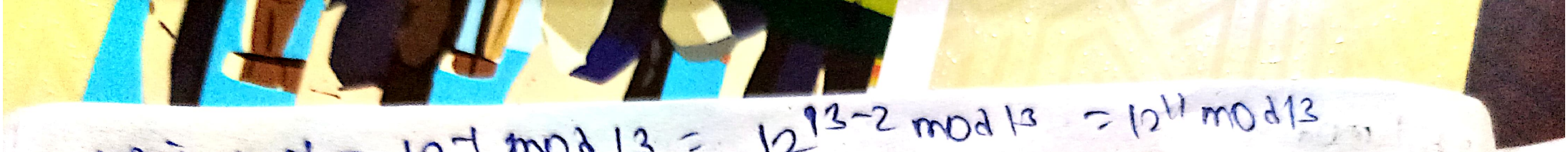
$= (4 \times 5 \times 1 + 10 \times 5 \times 9) \bmod 55$

$= 30$

(c) $x \equiv 7 \bmod 13$, and $x \equiv 11 \bmod 12$

(i) $m = 13 \times 12 = 156$

(ii) $m_1 = 156/13 = 12 \quad m_2 = 156/12 = 13$



(বিকল্প) $m_1^{-1} = 12^{-1} \bmod 13 = 12^{13-2} \bmod 13 = 12^{11} \bmod 13$

$= (12^5 \cdot 12^6) \bmod 13$

$= (12, 1) \bmod 13$

$= 12$

$m_2^{-1} = 13^{-1} \bmod 12 = 13^{7-2} \bmod 12 = 13^{10} \bmod 12$

$= (13^2)^5 \bmod 12$

$= (1)^5 \bmod 12$

$= 1$

$x = (a_1 \times m_1 \times m_1^{-1} + a_2 \times m_2 \times m_2^{-1}) \bmod 156$

$= (7 \times 12 \times 12 + 11 \times 13 \times 1) \bmod 156$

$= 59$

$= (7 \times 12 \times 12 + 11 \times 13 \times 1) \bmod 156$

$= 59$

29) In each of the following ciphers, what is the max^m no. of characters that will be changed in the cipher text, if only one character is changed in plain text

(a) Single transposition : 1 character

It only changes the position of characters, not the characters themselves, so changing one character in plain text just changes that characters in cipher text

Plain text: | h | e | l | l | o | → Cipher text: | L | H | E | O | E |

Index : 1 2 3 4 5 (After permut

Now changing 1 letter: | h | x | l | l | o |

e → x

Cipher text: | L | H | L | O | X |

(b) Double transposition: More than 1 character

- This involves 2 rounds of transposition, so a change in single character could affect more than 1 characters in the cipher text
- It could affect the entire block of text because both rounds of transposition can shift multiple characters

(c) polybain cipher: 2 characters will change in the cipher text

The polyfair cipher work in digraphs of characters). So changing 1 character in the plain text could affect 2 parts in cipher text, since a pair of letter is encoded together

30) For each of the following cipher, say whether it's a stream cipher or block cipher

(a) polyfair cipher: Block cipher → as it works on digraphs. blocks of 2 letters

(b) Auto key cipher: Stream cipher → as key is generated based on plain text and subkeys are automatically created from the plain text cipher characters during encryption process

(c) One-time pad: Stream cipher → as each bit/character is XORed with a key bit/character

(d) Rotor cipher: Stream cipher → as it does character-by-character substitution with changing keys

(e) ~~Stream Cipher:~~
Enigma machine: Stream cipher → as it is based on rotor machine, which processes 1 character at a time

31) Encrypt the message "this is an exercise" using one of the following ciphers and decrypt the message to get the original plain text

(a) Additive cipher with key=20

In additive cipher: $C = (P+K) \bmod 26$

$P = (C-K) \bmod 26$

For this is an exercise

t : (19+20) mod 26 = 13 → N
h : (07+20) mod 26 = 1 → B
i = (08+20) mod 26 = 2 → C
s = (18+20) mod 26 = 12 → M
i = (08+20) mod 26 = 2 → C
s = (18+20) mod 26 = 12 → M

a = (0+20) mod 26 = 20 → U
n = (13+20) mod 26 = 7 → H
e = (4+20) mod 26 = 24 → Y
x = (23+20) mod 26 = 17 → R
e = (4+20) mod 26 = 24 → Y
r = (17+20) mod 26 = 11 → L

C = (2+20) mod 26 = 22 → W

I = (8+20) mod 26 = 2 → C

S = (18+20) mod 26 = 12 → M

E = (4+20) mod 26 = 24 → Y

Cipher text:

NBCMCMUHYRYIWCMY

P = (C-K) mod 26

N = (13-20) mod 26 = 19 → t Y = 24-20 mod 26 = 4 → e

B = (1-20) mod 26 = 7 → h R = 17-20 mod 26 = 23 → x

C = (2-20) mod 26 = 8 → i Y = 24-20 mod 26 = 4 → e

M = (12-20) mod 26 = 18 → S I = 22-20 mod 26 = 17 → r

C = (2-20) mod 26 = 8 → i W = 22-20 mod 26 = 2 → C

M = (12-20) mod 26 = 18 → S C = 2-20 mod 26 = 8 → i

U = (20-20) mod 26 = 0 → Q M = 12-20 mod 26 = 18 → S

H = (7-20) mod 26 = 13 → n Y = 24-20 mod 26 = 4 → e

Plain text: this is an exercise

Multiplicative cipher:

C = (P X k) mod 26

Key = 15 gcd(15, 26) = 1

t = (9 X 15) mod 26 = 25 → Z

h = (7 X 15) mod 26 = 1 → B

i = (8 X 15) mod 26 = 16 → Q

s = (18 X 15) mod 26 = 10 → K

i = (8 X 15) mod 26 = 16 → Q

s = (18 X 15) mod 26 = 10 → K

a = (0 X 15) mod 26 = 0 → A

n = (13 X 15) mod 26 = 13 → N

e = (4 X 15) mod 26 = 8 → I

x = (23 X 15) mod 26 = 7 → H

e = (4 X 15) mod 26 = 8 → I

r = (17 X 15) mod 26 = 21 → V

c = (2 X 15) mod 26 = 4 → E

i = (8 X 15) mod 26 = 16 → Q

s = (18 X 15) mod 26 = 10 → K

e = (4 X 15) mod 26 = 8 → I

cipher text:

ZRQKQK AN CHIVEQKI

$P = (X \times Y^{-1}) \bmod 26$

$15^{-1} \bmod 26$

q	r_1	r_2	r	s_1	s_2	s	t_1	b	t
	26	15	11	1	0	1	0	1	-1
1	15	11	4	0	1	-1	1	-1	2
1	11	4	3	1	-1	3	-1	2	-5
2	4	3	1	-1	3	-4	2	-5	7
1	3	1	0	3	-4	14	-5	7	-26
3	1	0	-	-4	14	-	(7)	-26	-

So $15^{-1} \bmod 26 = 7$

$P = ((X7) \bmod 26$

Z $= (25 \times 7) \bmod 26 = 19 \rightarrow t$

B $= (1 \times 7) \bmod 26 = 7 \rightarrow h$

Q $= (16 \times 7) \bmod 26 = 8 \rightarrow i$

K $= (10 \times 7) \bmod 26 = 18 \rightarrow s$

Q $= (16 \times 7) \bmod 26 = 8 \rightarrow i$

K $= (10 \times 7) \bmod 26 = 18 \rightarrow s$

A $= (0 \times 7) \bmod 26 = 0 \rightarrow a$

N $= (13 \times 7) \bmod 26 = 13 \rightarrow n$

I $= (8 \times 7) \bmod 26 = 4 \rightarrow e$

H $= (7 \times 7) \bmod 26 = 23 \rightarrow x$

I $= (8 \times 7) \bmod 26 = 4 \rightarrow e$

V $= (21 \times 7) \bmod 26 = 17 \rightarrow r$

E $= (4 \times 7) \bmod 26 = 2 \rightarrow c$

Q $= (16 \times 7) \bmod 26 = 8 \rightarrow i$

K $= (10 \times 7) \bmod 26 = 18 \rightarrow s$

I $= (8 \times 7) \bmod 26 = 4 \rightarrow e$

plain text: this is an exercise

Affine cipher:

$e = (a p + b) \bmod 26$ (a = 15, b = 20) given

plain text: this is an exercise

t $= ((15 \times 19) + 20) \bmod 26 = 19 \rightarrow T$

h $= ((15 \times 7) + 20) \bmod 26 = 21 \rightarrow V$

i $= ((15 \times 8) + 20) \bmod 26 = 10 \rightarrow K$

s $= ((15 \times 18) + 20) \bmod 26 = 4 \rightarrow E$

i $= ((15 \times 7) + 20) \bmod 26 = 10 \rightarrow K$

s $= ((15 \times 18) + 20) \bmod 26 = 4 \rightarrow E$

a = (15 × 0 + 20) mod 26 → U
h = (11 × 13 + 20) mod 26 → H
e = (15 × 4 + 20) mod 26 → C
x = (15 × 23 + 20) mod 26 → B
e = (15 × 4 + 20) mod 26 → C
r = (15 × 17 + 20) mod 26 → P
c = (15 × 2 + 20) mod 26 → Y
t = (15 × 8 + 20) mod 26 → K
s = (15 × 18 + 20) mod 26 → E
e = (15 × 4 + 20) mod 26 → C

ciphertext: TVTVKE KE WH CBCPYKEC

$P = a^{-1} \times (c - b) \bmod 26$

$15^{-1} \bmod 26$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
1	26	15	11	1	0	1	0	1	-1
1	15	11	4	0	1	-1	1	-1	2
2	11	4	3	1	-1	3	-1	2	-5
1	4	3	1	-1	3	-4	2	-5	7
3	3	1	0	3	-4	14	-5	7	-26
-	1	0	-	-4	14	-	(7)	-20	-

$15^{-1} \bmod 26 = 7$

$P = 7 \times (15 - 20) \bmod 26$
$= 147 \bmod 26 = 17 \rightarrow R$

~~$T = 7 \times (19 - 20)$~~
~~$V = 7 \times (21$~~

$T = 7 \times (19 - 20) \bmod 26 = 175 \bmod 26 = 19 \rightarrow T$

$V = 7 \times (21 - 20) \bmod 26 = 7 \bmod 26 = 7 \rightarrow H$

$K = 7 \times (10 - 20) \bmod 26 = 112 \bmod 26 = 8 \rightarrow I$

$E = 7 \times (4 - 20) \bmod 26 = 70 \bmod 26 = 18 \rightarrow S$

$K = 7 \times (20 - 20) \bmod 26 = 112 \bmod 26 = 8 \rightarrow I$

$E = 7 \times (4 - 20) \bmod 26 = 70 \bmod 26 = 18 \rightarrow S$

$U = 7 \times (20 - 20) \bmod 26 = 0 \bmod 26 = 0 \rightarrow A$

$H = 7 \times (7 - 20) \bmod 26 = 91 \bmod 26 = 13 \rightarrow N$

$C = 7 \times (2 - 20) \bmod 26 = 56 \bmod 26 = 4 \rightarrow E$

$B = 7 \times (23 - 20) \bmod 26 = 49 \bmod 26 = 23 \rightarrow X$

$Y = 7 \times (24 - 20) \bmod 26 =$
$= 28 \bmod 26 = 2 \rightarrow C$

$K = 7 \times (10 - 20) \bmod 26 =$
$= 112 \bmod 26 = 8 \rightarrow I$

$E = 7 \times (4 - 20) \bmod 26 =$
$= 70 \bmod 26 = 18 \rightarrow S$

$C = 7 \times (2 - 20) \bmod 26 =$

$= 56 \bmod 26 = 4 \rightarrow E$

Plain text: this is an exercise

32) use the vigenere cipher with keyword "Health" to encipher the message "Life is full of surprises"

Plain text	l i f e i s	f u l l o f	s u r p r i s e s
p's value	11 8 5 4 8 18	5 20 11 11 14 5	18 20 17 15 17 8 18 4 18
Key value	h e a l t h 7 4 0 11 19 7	h e a l t h 7 4 0 11 19 7	h e a l t h 7 4 0 11 19 7
c's value	18 12 5 15 1 25	12 24 11 22 7 12	25 24 17 0 10 15 25 8 18
Cipher text	S M F P B Z	M Y L W H M	Z Y R A K P Z I S

Plain text: