LAIBA FATIMA

22k - 5195

3rd Assignment

Date: M T W T F S S

Q1 a, $\frac{7|19}{14}$ / 5

$q = 2 \quad r = 5$

b, $-111 = 11(-11) + 10$

$q = -11 \quad r = 10$

c, $789 = 23(34) + 7$

$q = 34 \quad r = 7$

d, $1001 = 13(77) + 0$

$q = 77 \quad r = 0$

e, $10 = 19(0) + 10$

$q = 0 \quad r = 10$

f, $3 = 5(0) + 3$

$q = 0 \quad r = 3$

g, $-1 = 3(-1) + 2$

$q = -1 \quad r = 2$

h, $4 = 1(4) + 0$

$q = 4 \quad r = 0$

Q2 a, $q = a \text{ div } m \quad r = a \bmod m$

i, $a = -111 \quad m = 99$

$-111 \text{ div } 99 = -2$

$-111 \bmod 99 = 87$

$q = -2 \quad r = 87$

ii $a = -9999 \quad m = 101$

$-9999 \text{ div } 101 = -99$

$-9999 \bmod 101 = 0$

$q = -99 \quad r = 0$

iii, $a = 10299 \quad m = 999$

$10299 \text{ div } 999 = 10$

$10299 \bmod 999 = 309$

$q = 10 \quad r = 309$

iv $a = 123456 \quad m = 1001$

$123456 \text{ div } 1001 = 113$

$123456 \bmod 1001 = 333$

$q = 113 \quad r = 333$

bi, $a = 80 \quad b = 5 \quad m = 17$

$\frac{a-b}{m} = \frac{80-5}{17} = \frac{75}{17}$

so $80 \not\equiv 5 \pmod{17}$

ii $a = 103 \quad b = 5 \quad m = 17$

$\frac{a-b}{m} = \frac{103-5}{17} = \frac{98}{17}$

so $103 \not\equiv 5 \pmod{17}$

iii, $a = -29$ $b = 5$ $m = 17$

$\frac{-29-5}{17} = \frac{-34}{17} = -2$

So $-29 \equiv 5 \bmod 17$

iv, $a = -122$ $b = 5$ $m = 17$

$\frac{-122-5}{17} = \frac{-127}{17}$

So $-122 = 5 \bmod 17$

Q3 a i, gcd(11,15) = 1 gcd(15,19) = 1 gcd(11,19) = 1 Yes

ii gcd(14,15) = 1 gcd(14,21) = 7 gcd(15,21) = 3 No

gcd(14,21) = 7

$14 = 7 \times 2$

$21 = 7 \times 3$

gcd(15,21) = 3

$15 = 5 \times 3$

$21 = 7 \times 3$

iii, gcd(12,17) = 1 gcd(12,31) = 1 gcd(12,37) = 1 Yes
gcd(17,31) = 1 gcd(17,37) = 1 gcd(31,37) = 1

iv, gcd(7,8) = 1 gcd(7,9) = 1 gcd(7,11) = 1
~~gcd(17,31) = 1~~ ~~gcd(17,37) = 1~~ ~~gcd(31,37) = 1~~ Yes
gcd(8,9) = 1 gcd(8,11) = 1 gcd(9,11) = 1

b i, $2 \times 2 \times 2 \times 11 = 2^3 \times 11$

ii $2 \times 3 \times 3 \times 7 = 2 \times 3^2 \times 7$

iii $3 \times 3 \times 3 \times 3 \times 3 \times 3 = 3^6$

iv $7 \times 13 \times 11$

v, 11×101

vi, $3 \times 3 \times 101 = 3^2 \times 101$

Date: M T W T F S S

Q4 $144 = 89(1) + 55$
$89 = 55(1) + 34$
$55 = 34(1) + 21$
$34 = 21(1) + 13$
$21 = 13(1) + 8$
$13 = 8(1) + 5$
$8 = 5(1) + 3$
$5 = 3(1) + 2$
$3 = 2(1) + 1$
$2 = (1)(1) + 0$
gcd = 1

GCD (1001, 100001)
$100001 = 1001(99) + 902$
$1001 = 902(1) + 99$
$902 = 99(9) + 11$
$99 = (11)(9) + 0$
gcd = 11

Q5 a) $a = 55$ $b = 34$ $m = 89$ GCD $(a, m) = 1$ GCD (55, 89)

$89 = 55(1) + 34$
$55 = 34(1) + 21$
$34 = 21(1) + 13$
$21 = 13(1) + 8$
$13 = 8(1) + 5$
$8 = 5(1) + 3$
$5 = 3(1) + 2$
$3 = 2(1) + 1$
$2 = 1(1) + 0$

$1 = 3 \times 1 - 2 \times 1$
$3 \times 1 - 1(5 - 3 \times 1)$
$3 \times 1 - 5 + 3 \times 1$
$2 \times (8 - 5 \times 1) - 5$
$2 \times 8 - 2 \times 5 - 1 \times 5$
$2 \times 8 - 3(13 - 8 \times 1)$
$2 \times 8 - 39 - 3 \times 8$
$-3 \times 13 - 1(21 - 13 \times 1)$
$-3 \times 13 - 1 \times 21 + 1 \times 13$
$-2(34 - 21 \times 1) - 1 \times 21$
$-2 \times 34 + 2 \times 21 - 1 \times 21$

$= -2 \times 34 + 1 \times (55 - 34 \times 1)$
$= -2 \times 34 + 1 \times 55 - 1 \times 34$
$= -3 \times (89 - 55 \times 1) + 1 \times 55$
$= -3 \times 89 + 3 \times 55 + 1 \times 55$
$= \underbrace{-3 \times 89}_{ra} + \underbrace{4 \times 55}_{q}$

$55 \times 4 \times u = 34 \times 4 \pmod{89}$
$u = 136 \pmod{89}$
$= 47$

Date: M T W T

b, $a = 89 \quad b = 2 \quad m = 232$

$232 = 89(2) + 54$
$89 = 54(1) + 35$
$54 = 35(1) + 19$
$35 = 19(1) + 16$
$19 = 16(1) + 3$
$16 = 3(5) + 1$
$3 = 1(3) + 0$

$1 = 16x1 + 3x5$
$16x1 - 5(19 - 16x1)$
$16x1 - 5x19 + 5x16$
$6x(35x1 - 19x1) - 5x19$
$6x35 - 6x19 - 5x19$
$6x35 - 11(54x1 - 35x1)$
$6x35 - 11x54 + 11x35$
$17x(89x1 - 54x1) - 11x54$
$17x89 - 17x54 - 11x54$
$17x89 - 28(232x1 - 89x2)$
$17x89 - 28x232 + 56x89$
$73x89 - 28x232$
$73(89) + (-28)(232)$
$\hookrightarrow a = 73$

$89x73x_4 = 2x27 \pmod{232}$
$u = 146 \pmod{232}$
$= 146$

Q6 a) $a_1 = 1$, $a_2 = 2$, $a_3 = 3$

$m_1 = 210/5 = 42$
$m_2 = 210/6 = 35$
$m_3 = 210/7 = 30$

$y_u = m_h^{-1} \bmod m_u$
y_1

$y_1 = 42 \bmod 5$
$42 = 5(8) + 2$
$5 = 2(2) + 1$
$2 = 2(1) + 0$

$1 = 5x1 - 2x2$
$5x1 - 2(42x1 - 5x8)$
$5x1 - 2x42 + 16x5$
$21(5) + (-2)(42)$

$a_1 = -2 + 5 = 3$

Date: M T W T F S S

$y_2 = 35 \bmod 6$

$35 = 6(5) + 5$

$6 = 5(1) + 1$

$5 = 5(1) + 0$

$1 = 6 \times 1 - 5 \times 1$

$6 \times 1 - 1(35 \times 1 - 6 \times 5)$

$6(6) + (-1)(35)$

$a_2 = -1 + 6 = 5$

$y_3 = 30 \bmod 7$

$30 = 7(4) + 2$

$7 = 2(3) + 1$

$2 = 1(2) + 0$

$1 = 7 \times 1 - 2 \times 3$

$7 \times 1 - 3(30 - 7 \times 4)$

$7 \times 1 - 3 \times 30 + 14 \times 7$

$15 \times 7 - 3 \times 30$

$15(7) + (-3)(30)$

$a_3 = -3 + 7 = 4$

$(a_1 m_1 y_1 + a_2 m_2 y_2 + a_3 m_3 y_3) \bmod m$

$(1 \times 42 \times 3) + (2 \times 35 \times 5) + (3 \times 30 \times 4) \bmod 210$

$836 \bmod (210) = 206$

If, $u_1 = 1 \pmod 2$

$u_2 = 2 \pmod 3$

$u = 3 \pmod 5$

$u = 4 \pmod{11}$

$a_1 = 1, a_2 = 2, a_3 = 3, a_4 = 4$

$m = 2 \times 3 \times 5 \times 11 = 330$

$m_1 = 330/2 = 165$ $\quad m_3 = 66$

$m_2 = 330/3 = 110$ $\quad m_4 = 30$

$y_1 = 165 \bmod 2$

$165 = 2(82) + 1$

$2 = 1(2) + 0$

$1 = 1 \times 165 - 2 \times 82$

$(165)(1) + (-2)(82)$

$a_1 = 1$

$y_2 = 110 \bmod 3$

$110 = 3(36) + 2$

$3 = 2(1) + 1$

$1 = 3 \times 1 - 2 \times 1$

$3 \times 1 - 1(110 \times 1 - 3 \times 36)$

$3 \times 1 - 110 \times 1 + 3 \times 36$

$3 \times 37 + (-1)(110)$

$3(37) + (-1)(110)$

$a_2 = -1 + 3 = 2$

Date: M T W T

$y_3 = 66 \bmod 5$

$66 = 5(13) + 1$

$5 = 1(5) + 0$

$1 = 66(1) + (-13)(5)$

$a_3 = 1$

$y_4 = 30 \bmod 11$

$30 = 11(2) + 8$

$11 = 8(1) + 3$

$8 = 3(2) + 2$

$3 = 2(1) + 1$

$1 = 3 \times 1 - 1 \times 2$

$3 \times 1 - 1(8 \times 1 - 3 \times 2)$

$3 \times 1 - 8 \times 1 + 3 \times 2$

$3 \times 3 - 8 \times 1$

$3(11 \times 1 - 8 \times 1) - 8 \times 1$

$3 \times 11 - 3 \times 8 - 8 \times 1$

$3 \times 11 - 4 \times (30 + 11 \times 2)$

$3 \times 11 - 4 \times 30 + 8 \times 11$

$11 \times 11 - 4 \times 30$

$11(11) + (-4)(30)$

$a_4 = -4 + 11 = 7$

$x = (a_1 m_1 y_1 + a_2 m_2 y_2 + a_3 m_3 y_3 + a_4 m_4 y_4) \bmod m$

$[(1 \times 165 \times 1) + (2 \times 110 \times 2) + (3 \times 66 \times 1) + (4 \times 30 \times 7)] \bmod 330$

$= 1643 \bmod 330 = 332$

b) $m = m_1 \times m_2 \times m_3 \times m_4$

$5 \times 6 \times 7 \times 11 = 2310$

$a_1 = 3 \quad a_2 = 3 \quad a_3 = 1 \quad a_4 = 0$

$m_1 = 462 \quad m_2 = 385 \quad m_3 = 330 \quad m_4 = 210$

$y_1 = 462 \bmod 5$

$462 = 5(92) + 2$

$5 = 2(2) + 1$

$1 = 5 \times 1 - 2 \times 2$

$5 \times 1 - 2(462 \times 1 - 5 \times 92)$

$5 \times 1 - 2 \times (462 + 184 \times 5)$

$5(185) + (-2)(462)$

$y_1 = -2 \bmod 5 = 3$

Date: M T W T F S S

$y_2 = 330 \bmod 6$ $\quad 1 = 1 \times 385 + (-64)(6)$ $\quad y_2 = 1$

$385 = 6(64) + 1$

$y_3 = 330 \bmod 7$ $\quad 1 = (4)(330) + (-47)(7)$ $\quad y_3 = 1$

$330 = 7(47) + 1$

$y_4 = 210 \bmod 11$ $\quad 1 = (1)(210) + (-19)(11)$ $\quad y_4 = 1$

$210 = 11(19) + 1$

$u = (a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 + a_4 M_4 y_4) \bmod m$

$(3 \times 462 \times 3) + (3 \times 385 \times 1) + (1 \times 330 \times 1) + (0 \times 210 \times 1) \bmod 2310$

$u = 5643 \bmod 2310 = 1023$

@7a, $y = 2 \bmod 17$ $\quad \gcd(17, 2)$

$17 = 2(8) + 1$

$1 = 17 \times 1 - 2 \times 8$

$17(1) + (-2)(8)$

$a = -8 + 17 = 9$

b) $\gcd(34, 89)$

$89 = 34(2) + 21$

$34 = 21(1) + 13$

$21 = 13(1) + 8$

$13 = 8(1) + 5$

$8 = 5(1) + 3$

$5 = 3(1) + 2$

$3 = 2(1) + 1$

$1 = 3 \times 2 - 1(5 \times 1 - 3 \times 1)$

$2 \times 3 - 5 \times 1$

$2(8 \times 1 - 5 \times 1) - 5 \times 1$

$8 \times 2 - 3 \times 5$

$8 \times 2 - 3 \cdot (13 \times 1 - 8 \times 1)$

$8 \times 2 - 3 \times 13 + 8 \times 3$

$5 \times (21 \times 1 - 13 \times 1) - 3 \times 13$

$5 \times 21 - 8 \times (34 \times 1 - 21 \times 1)$

$5 \times 21 - 8 \times 34 + 8 \times 21$

$13 \times (89 - 34 \times 2) - 8 \times 34$

$13 \times 89 - 26 \times 34 - 8 \times 34$

$13(89) + (-34)(34)$

$a = -34 + 89 = 55$

Date: M T W T F

c, gcd(144, 233)

$233 = 144(1) + 89$
$144 = 89(1) + 55$
$89 = 55(1) + 34$
$55 = 34(1) + 21$
$34 = 21(1) + 13$
$21 = 13(1) + 8$
$13 = 8(1) + 5$
$8 = 5(1) + 3$
$5 = 3(1) + 2$
$3 = 2(1) + 1$

$1 = 3x1 - 2x1$
$3x1 - 1(5x1 - 3x1)$
$3x1 - 5x1 + 3x1$
$2x(8x1 - 5x1) 5x1$
$2x8 - 5x2 - 5x1$
$2x8 - 3(13x1 - 8x1)$
$2x8 - 3x13 + 3x8$
$-3x13 + 5(21 - 13x1)$
$-3x13 + 5x21 - 5x13$

$-8x(34x1 - 21x1) + 5x21$
$-8x34 + 8x21 + 5x21$
$-8x34 + 13(55x1 - 34(1)$
$-8x34 + 13x55 - 13x34$
$-21(89x1 - 55x1) + 13x55$
$-21x89 + 21x55 + 13x55$
$-21x89 + 34(144x1 - 89x1)$
$-21x89 + 34x144 - 89x34$
$-55(233x1 - 144x1) + 34x144$
$-55x233 + 55x144 + 34x144$
$(233)(-55)(89)(144$
$c^{-1} = 89$

d, gcd(200, 1001)
$1001 = 200(5) + 1$
$1 = 1001(1) + (-5)(200)$

$a = -5 + 1001 = 996$

Q8 a,
STOP POLLUTION
18 19 14 15 15, 14, 11, 11, 20, 19, 18, 14, 15

encrypted message is
WXST TSPPYXMSR

$f(18) = (18+4) \bmod 26 = 22$ (W)
$f(19) = (19+4) \bmod 26 = 23$ (X)
$f(14) = (14+4) \bmod 26 = 18$ (S)
$f(15) = (15+4) \bmod 26 = 19$ (T)
$f(11) = (11+4) \bmod 26 = 15$ (P)
$f(20) = (20+4) \bmod 26 = 24$ (Y)
$f(8) = (8+4) \bmod 26 = 12$ (M)
$f(13) = (13+4) \bmod 26 = 17$ (R)

Date: M T W T F S S

ii STOP POLLUTION

18, 19, 14, 15, 15, 14, 11, 11, 20, 19, 8, 14, 3

encrypted message is

NOJK KJGGPODJI

$f(S) = (18 + 21) \bmod 26 = 13$ (N)

$f(T) = (19 + 21) \bmod 26 = 14$ (O)

$f(O) = (24 + 21) \bmod 26 = 9$ (J)

$f(P) = (15 + 21) \bmod 26 = 10$ (K)

$f(L) = (11 + 21) \bmod 26 = 6$ (G)

$f(T) = (8 + 21) \bmod 26 = 3$ (D)

$f(N) = (13 + 21) \bmod 26 = 13$ (J)

bi CEBBOXNOB XXGA

2, 4, 1, 1, 14, 13, 13, 14, 1, 23, 24, 6

$f^{-1}(C) = (2 - 10) \bmod 26 = -8 + 26 = 18$ (S)

$f^{-1}(E) = (4 - 10) \bmod 26 = -6 + 26 = 20$ (U)

$f^{-1}(O) = (14 - 10) \bmod 26 = 4$ (E)

$f^{-1}(X) = (23 - 10) \bmod 26 = 13$ (N)

$f^{-1}(N) = (13 - 10) \bmod 26 = 3$ (D)

$f^{-1}(G) = (6 - 10) \bmod 26 = -4 + 26 = 22$ (W)

$f^{-1}(B) = (1 - 10) \bmod 26 = -9 + 26 = 17$ (R)

$f^{-1}(Y) = (24 - 10) \bmod 26 = 14$ (O)

SURRENDER NOW

ii LO WI PBSOXYN

11, 14 22, 8 15, 1, 18, 14, 23, 13

$p^{-1}(L) = (11 - 10) \bmod 26 = 1$ (B)

$p^{-1}(O) = (14 - 10) \bmod 26 = 4$ (E)

$p^{-1}(W) = (22 - 10) \bmod 26 = 12$ (M)

$p^{-1}(I) = (8 - 10) \bmod 26 = -2 + 26 = 22$ (Y)

$p^{-1}(P) = (15 - 10) \bmod 26 = 5$ (F)

$p^{-1}(B) = (1 - 10) \bmod 26 = -9 + 26 = 17$ (R)

$p^{-1}(S) = (18 - 10) \bmod 26 = 8$ (T)

$p^{-1}(X) = (23 - 10) \bmod 26 = 13$ (N)

$p^{-1}(N) = (13 - 10) \bmod 26 = 3$ (D)

BE MY FRIEND

Date: M T W T

Q9 i, $5^{-2003} \bmod 7$ — $a^{p-1} = 1 \bmod p$

$5^5 \times (5^6)^{333} \bmod 7$ — $5^{7-1} = 1 \bmod 7$

$5^5 \times 1 \bmod 7$ — $5^6 = 1 \bmod 7$

$3125 \bmod 7$

3 — $2003 = 6(333) + 5$

ii, $5^{-2003} \bmod 11$ — $5^{11-1} = 1 \bmod 11$

$(5^{10})^{200} \times 5 \bmod 11$ — $5^{10} = 1 \bmod 11$

$1 \times 125 \bmod 11$ — $2003 = R(200) + 3$

4

iii, $5^{2003} \bmod 13$ — $5^{13-1} = 1 \bmod 13$

$(5^{12})^{166} \times 5^{11} \bmod 13$ — $5^{12} = 1 \bmod 13$

$1 \times 5^{11} \bmod 13$ — $2003 = 12(166) + 11$

$48828125 \bmod 13$

8

Q10 a, I LOVE DISCRETE MATHEMATICS — $f(p) = (p+3) \bmod 26 =$

$f(I) = (8+3) \bmod 26 = 11$ (L)

$f(L) = (11+3) \bmod 26 = 14$ (O)

$f(O) = (14+3) \bmod 26 = 17$ (R)

$f(V) = (21+3) \bmod 26 = 24$ (Y)

$f(E) = (4+3) \bmod 26 = 7$ (H)

$f(D) = (3+3) \bmod 26 = 6$ (G)

$f(S) = (18+3) \bmod 26 = 21$ (V)

$f(C) = (2+3) \bmod 26 = 5$ (F)

$f(R) = (17+3) \bmod 26 = 20$ (U)

$f(T) = (19+3) \bmod 26 = 22$ (W)

$f(M) = (12+3) \bmod 26 = 15$ (P)

$f(A) = (0+3) \bmod 26 = 3$ (D)

$f(H) = (7+3) \bmod 26 = 10$ (K)

encrypted text

L ORYH GLVFUHWH

PDWKHPDWLFV

Date: M T W T F S S

i) PLGWZR DVVLJQPHQW $f(p) = (p-3) \bmod 26$

$f^{-1}(P) = (15-3) \bmod 26 = 12$ (M)
$f^{-1}(L) = (11-3) \bmod 26 = 8$ (I)
$f^{-1}(G) = (6-3) \bmod 26 = 3$ (D)
$f^{-1}(W) = (22-3) \bmod 26 = 19$ (T)
$f^{-1}(Z) = (25-3) \bmod 26 = 22$ (W)
$f^{-1}(R) = (17-3) \bmod 26 = 14$ (O)
$f^{-1}(D) = (3-3) \bmod 26 = 0$ (A)
$f^{-1}(V) = (21-3) \bmod 26 = 18$ (S)
$f^{-1}(J) = (9-3) \bmod 26 = 6$ (G)
$f^{-1}(Q) = (16-3) \bmod 26 = 13$ (N)
$f^{-1}(H) = (7-3) \bmod 26 = 4$ (E)

Decrypted message is
MID TWO ASSIGNMENT

ii) IDVW QXFHV XQLYHUVLWB $f(p) = (p-3) \bmod 26$

$f^{-1}(I) = (8-3) \bmod 26 = 5$ (F)
$f^{-1}(D) = (13-3) \bmod 26 = 0$ (A)
$f^{-1}(V) = (20-3) \bmod 26 = 17$ (S)
$f^{-1}(W) = (22-3) \bmod 26 = 19$ (T)
$f^{-1}(Q) = (16-3) \bmod 26 = 13$ (N)
$f^{-1}(X) = (23-3) \bmod 26 = 20$ (U)
$f^{-1}(F) = (5-3) \bmod 26 = 2$ (C)
$f^{-1}(H) = (7-3) \bmod 26 = 4$ (E)
$f^{-1}(L) = (11-3) \bmod 26 = 8$ (I)
$f^{-1}(Y) = (24-3) \bmod 26 = 21$ (V)
$f^{-1}(U) = (20-3) \bmod 26 = 17$ (R)
$f^{-1}(B) = (1-3) \bmod 26 = -2 \bmod 26 = 24$ (Y)

Decrypted message
FAST NUCES UNIVERSITY

Date: M T W T

Q11 a) i, $03456798 \bmod 97 = 91$

ii $18321232 \bmod 97 = 57$

iii $22019574 \bmod 97 = 21$

iv $98725535 \bmod 97 = 5$

b i, $10457869 \bmod 101 = 58$

ii, $43222187 \bmod 101 = 60$

iii $37229191 \bmod 101 = 32$

iv $50133875 3 \bmod 101 = 3$

Q12 $u_1 = (4 \times 3 + 1) \bmod 7$

$(13) \bmod 7 = 6$

$u_2 = (4 \times 6 + 1) \bmod 7$

$(25) \bmod 7 = 4$

$u_3 = (4 \times 4 + 1) \bmod 7$

$(17) \bmod 7 = 3$

$u_4 = (4 \times 3 + 1) \bmod 7$

$(13) \bmod 7 = 6$

$u_5 = (4 \times 6 + 1) \bmod 7$

$(25) \bmod 7 = 4$

$u_6 = (4 \times 4 + 1) \bmod 7$

$(17) \bmod 7 = 3$

Q13 ai, 7323218 4434

$7 \times 3 + 3 + 2 \times 3 + 3 + 2 \times 3 + 1 + 8 \times 3 + 4 + 4 \times 3 + 3 + 3 \times 4 \times u_{12} = 0 \bmod 10$

$21 + 3 + 6 + 3 + 6 + 1 + 24 + 4 + 12 + 3 + 12 + u_{12} = 0 \bmod 10$

$95 + u_{12} = 0 \bmod 10$

Check digit is $u_{12} = 5$

ii 6362 3991 346

$6 \times 3 + 3 + 6 \times 3 + 2 + 3 \times 3 + 9 + 9 \times 9 + 1 + 3 \times 3 + 4 + 6 \times 3 + u_{12} = 0 \bmod 10$

$172 + u_{12} = 0 \bmod 10$

Check digit (12) = 8

Date:
M T W T F S S

b) i. 036000291452

$0\times3+3+6\times3+0+0+0+2\times3+9+1\times3+4+5\times3+2 = 0 \bmod 10$

$0+3+18+6+9+3+4+15+2$

$60 = 0 \bmod 10$

Valid UPC code

ii 012345678903

$0\times3+1+2\times3+3+4\times3+5+6\times3+7+8\times3+9+0\times3+3 = 0 \bmod 10$

$1+6+3+12+5+18+7+24+9+3 = 0 \bmod 10$

$88 \neq 0 \bmod 10$

Q14 a ISBN = 10 0-07-119881 (first nine digits) Check digits?

$1\times0+2\times0+7\times3+1\times4+1\times5+9\times6+8\times7+8\times8+9\times1+x_{10} = 0 \bmod 11$

$21+4+5+54+56+64+9+x_{10} = 0 \bmod 11$

$213+x_{10} = 0 \bmod 11$

Check digit $x_{10} = 4$

b, 0-321-50061-8 Find value of Q

$x_{10} = 1\times0+2\times3+3\times2+1\times4+5\times5+8\times Q+9\times1 \bmod 11$

$6+6+4+25+8Q+9 \bmod 11$

$8Q+50 \bmod 11$ Check digit = 8

$8 = 8Q+50 \bmod 11$

$8 = 8Q+6 \bmod 11$

$8-6 = 8Q+6-6 \bmod 11$

$8Q \bmod 11 = 2$

$7\times8Q \bmod 11 = 2\times7 \bmod 11$

$Q \bmod 11 = 14 \bmod 11$

$Q \bmod 11 = 3$

$\therefore 50 \bmod 11 = 6$

Q has to be 3 so that it is smaller than 11 and blue (Q-9)

$Q = 3$

$3 \bmod 11 = 3$ proved

Date:
M T W T

Q15 ATTACK

00 19 19 00 02 10

$C = 0019 \bmod 2537$

$C = 1900 \bmod 2537$

$C = 0210 \bmod 2537$

$n = pq$

$h = (p-1)(q-1)$

Check

GCD (e, h) = 1

$C = m^e \bmod n$

$h = 43 \times 59 = 2537$

$h = (43-1)(59-1) = 2436$

$e = 13$

Q16 a, There are $37 \times 37 = 99$ offices in the building

b, $12 \times 2 \times 3$ shifts are required (72)

Q17 a, People can have $26 \times 26 \times 26 = 26^3$ different three letter initials.

b, people can have $26 \times 25 \times 24 = 15,600$ different three-letter initials with none of the letters repeated.

Q18 a, There are 16 place values for hexadecimal number 0 to 9, A, B, C, D, E, and F

So, $16^{10} + 16^{28} + 16^{58}$ different WEP keys are possible

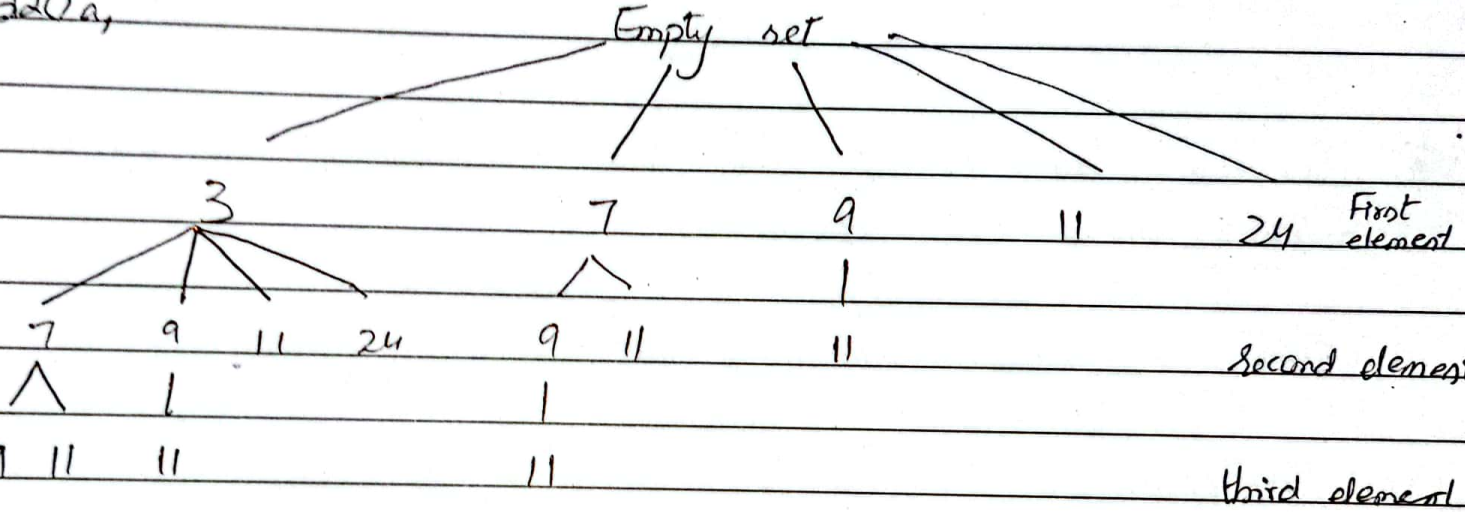
b, There ~~are~~ 16 would be $26^4 - 25^4 = 66,351$ strings

Q19 a, Since each value of the domain can be mapped to one of two values Number of functions are $2 \times 2 \times 2 \times 2 \times \dots \times m = 2^n$

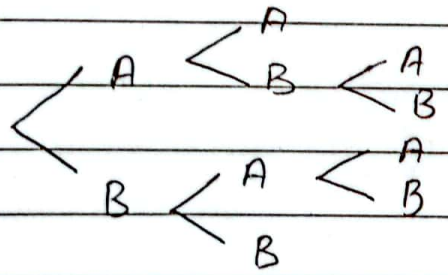
Date: M T W T F S S

b, Each successive element from the domain will have one option that its predecessors as it is one-to-one function.
So, numbers of function are $5 \times 4 \times 3 \times 2 \times 1 = 120$

Q20 a,



b



Q21 a, There are ${}^{8}C_3 = 56$ ways to choose the students

b, There are ${}^{12}C_6 = 924$ ways to select the elective courses

c, ${}^{9}C_5 = 126$ different teams can be selected

Q22 a, ${}^{20}P_5 = 1860,480$ ways to choose a chairperson, assistant chairperson, treasurer, community adviser and record keeper.

Date: M T W

Q22 b, There are $^{14}P_4 = 43,680$ ways each ordered students to complete in the race

c, There are $^{15}P_2 = 210$ ways student can be chosen for these 2 position

Q23 a, $^5C_1 \times {}^3C_2 \times {}^4C_1 \times {}^6C_3 = 1200$ sandwiches can be made from 1 meat 2 bread, 1 cheese and 3 condiments

b, There are $15 \times 48 \times 24 \times 34 \times 28 \times 28 = 462,615,680$ different faces

Q24 a, A = strings begin with three 0s $= 2^7 = 128$ $A \cap B = 2^5 = 32$

B = strings end with 2 0s $= 2^8 = 256$ $A \cup B = A + B - A \cap B = 128 + 256 - 32 = 352$

b, A = Strings begin with 0s $= 2^4 = 16$ $A \cap B = 2^2 = 4$

B = strings end with two 1s $= 2^3 = 8$ $A \cup B = A + B - A \cap B = 16 + 8 - 4 = 20$

Q25 a, first letter of each last name are the pigeonholes

letters of the alphabet are pigeons

Generalized pigeonhole principle, $\left[\frac{30}{26}\right] = 2$. Atleast 2 students have last names that begin with the same letter

b, Generalized pigeonhole principle $\left[\frac{8008278}{1000000}\right] = 9$

c, Pigeonholes = 38 time pigeons = 677 classes

$\left[\frac{677}{28}\right] = 18$ classes are meeting

Since each class is meeting in a different room, we need 18 rooms

Date: M T W T F S S

Q26 a, $^{n}C_{8} = {}^{n}C_{5} = 462$

b. $^{n}C_{8} = {}^{24}C_{17}(2)^{7} \cdot (-1)^{17} = -44,301,312$

Q27 a, There are 36 students. They can be put in a row in 36! ways

b, Ordered arrangement of 7 out of 36 students - P(36,7)

c, Ordered arrangement of all 16 men and all 20 women. product rule, this can be done in 20! x 16! ways

Q28 a, $2^{n}-1 = 2^{7}-1 = 128-1$

$128-1=127$ ∴ 7 is the integer that is $n \geq 5$ and $2^{n}-1$ is a prime no.

Proved!

b, a = integer
p = prime number
p|a p|(a+1)

$a = p \cdot r$ $a+1 = p \cdot s$

$1 = (a+1) - a$

$p \cdot s - p \cdot r$

$p \cdot (s-r)$ where $s-r \in Z$

∴ This implies that p|1. since p is prime $p \geq 1$

But the only divisor of 1 are 1 and -1. So, the supposition is false. The statement is true.

Q29 a, $\sqrt{a+b} = \sqrt{a} + \sqrt{b}$

$a+b = a+b+2\sqrt{a}\sqrt{b}$

$0 = 2\sqrt{a}\sqrt{b} = 2\sqrt{ab}$

$0 = ab$

either a or b is 0

lets take $a=3$ $b=4$

$\sqrt{a+b} = \sqrt{3+0} = \sqrt{3}$

$\sqrt{0} + \sqrt{3} = \sqrt{3}$

given condition is satisfied if we take $a=3$ and $b=0$

Date: M T W T

b, if $u \leq 1$ and $u \geq -1$ then $|u| \leq 1$

$u \leq 1$ and $u \geq -1$

$-1 \leq u \leq 1 \quad : |u| \leq 1$ Equivalently $|u| \geq 1$

Q30 a, $n = 7$

$n+2 = 7+2 = 9$ not a prime number

b, $p_1 = 2 \quad p_2 = 3 \quad p_3 = 5 \ldots p_n$

$N = p_1 \times p_2 \times p_3 \ldots p_n + 1$

N is divisible by p $p|N$

p is prime so p must equal a prime no.

$p \nmid (p_1 p_2 p_3 \cdots p_n + 1)$

So, $p \nmid N$

Then $p|N$ and $p \nmid N$ Contradiction!

Supposition is false, Theorem is true.

Q31 a, $n = 2p+1$

$m = 2q+1$

$n+m = (2p+1)+(2q+1)$

$= 2p+2q+2 = 2 \times (p+q+1)$ even!

Contradicting the assumption $n+m$ is odd.

b, $m+n$ = odd

m = even n = odd

$m = 2p \quad n = 2q+1$

$m+n = (2p)+(2q+1)$

$= 2 \times (p+q) + 1$

$= 2 \times x + 1$

Hence $m+n$ is odd

Contrapositive statement is true

Since implication is logically equivalent to Contrapositive, so implication is true.

Q32 a Suppose $6-7\sqrt{2}$ is rational

$6-7\sqrt{2} = a/b \quad b \neq 0$

$7\sqrt{2} = 6 - a/b \quad 7\sqrt{2} = \frac{6b-a}{b}$

$\sqrt{2} = \frac{6b-a}{7b}$

$6b-a$ and $7b$ are integers and $\sqrt{2}$ is quotient

$\sqrt{2}$ is rational

This contradicts because $\sqrt{2}$ is irrational

Supposition is false. $6 \times \sqrt{2}$ is rational

Date: M T W T F S S

b Suppose $\sqrt{2}+\sqrt{3}$ is rational

$\sqrt{2}+\sqrt{3} = a/b$

$2+3+2\sqrt{2}\sqrt{3} = \frac{a^2}{b^2}$

$2\sqrt{2}\times 3 = a^2/b^2 - 5$

$\sqrt{6} = \frac{a^2-5b^2}{2b^2}$

$\sqrt{6}$ is the quotient of a^2-2b^2 and $2b^2$ which are integers.

$\sqrt{6}$ is irrational. Contradiction $\sqrt{6}$ is not rational

Supposition is false and $\sqrt{2}+\sqrt{3}$ is irrational

Q33 a. P(n) denotes the equation

P(1) is true

n = 1

L.H.S of P(1) = $1^2 = 1$

R.H.S of P(1) = $\frac{1+(1+1)(2(1)+1)}{6}$

$= \frac{1\times 2\times 3}{6} = 6/6 = 1$

LHS = RHS . P(1) is true

$1^2+2^2+3^2+\ldots+k^2 = \frac{k(k+1)(2k+1)}{6}$ — ①

$1^2+2^2+3^2+\ldots+(k+1)^2 = \frac{(k+1)(k+1+1)(2(k+1)+1)}{6}$ — ②

$1^2+2^2+3^2+\ldots+(k+1)^2 = 1^2+2^2+3^2+\ldots+k^2+(k+1)^2$

$= \frac{k(k+1)(2k+1)}{6} + (k+1)^2$

$(k+1)\left[\frac{k(2k+1)}{6} + k+1\right)$

$k+1\ \left[\frac{2k^2+k+6k+6}{6}\right]$

$\frac{(k+1)(k+2)(2k+3)}{6}$

$= \frac{(k+1)(k+1+1)(2(k+1)+1)}{6}$

b, P(n): $1+2+2^2+\ldots+2^n = 2^{n+1}-1$

P(0) is true

L.H.S of P(0) = 1 R.H.S of P(0) = $2^{0+1}-1 = 2-1 = 1$

$1+2+2^2+\ldots+2^k = 2^{k+1}-1$ — ①

$1+2+2^2+\ldots+2^{k+1} = 2^{k+1+1}-1$ — ②

$1+2+2^2+\ldots+2^{k+1} = (1+2+2^2+\ldots+2^k)+2^{k+1}$

$= (2^{k+1}-1)+2^{k+1}$

$2\times 2^{k+1}-1 = 2^{k+1+1}-1$ = R.H.S of 2

Date: M T W T F S S

c, Show its True for $n=1$

1. $1^3 = 1/4 \times 1^2 \times 2^2$ is True

2. Assume its true for $n=k$

$1^3+2^3+3^3+\dots+k^3 = 1/4\,k^2(k+1)^2$ is True (Assuming)

$1^3+2^3+3^3+\dots+(k+1)^3 = 1/4\,(k+1)^2(k+2)^2$ True for "k+1"

$1^3+2^3+3^3+\dots+k^3 = 1/4\,k^2(k+1)^2$

$1/4\,k^2(k+1)^2 + (k+1)^3 = 1/4\,(k+1)^2(k+2)^2$

$k^2(k+1)^2 + 4(k+1)^3 = 1/4\,(k+1)^2(k+2)^2$

$k^2 + 4(k+1) = (k+2)^2$

$k^2 + 4k + 4 = k^2 + 4k + 4$

It is true $1^3+2^3+3^3+\dots+(k+1)^3 = 1/4\,(k+1)^2(k+2)^2$ is true.

Q34 a, Combination

1. Password generation
2. Sports tournament formats

b, Permutations

1. DNA sequencing
2. Routing and Scheduling

c, Binomial Theorem

1. Probability Distribution
2. Risk analysis in finance

d, Proof methods

1. Cryptography
2. Software Verification

e, Mathematical induction

1. Network protocols
2. Algorithm design and analysis