DISCRETE ASSIGNMENT 3
21K-3153

(Q1)

(a) $q = 2$, $r = 5$

(b) $q = -10$, $r = 1$

(c) $789 \div 23$
$q = 34$, $r = 7$

(d) $10001 \div 13$
$q = 77$, $r = 0$

(e) $10 \div 19$
$q = 0$, $r = 10$

(f) $3 \div 5$
$q = 0$, $r = 3$

(g) $-1 \div 3$
$q = 0$, $r = -1$

(h) $4 \div 1$
$q = 4$, $r = 0$

Date:
M T W T F S S

Q2(a) $q = a \text{ div } d$ $r = a \bmod d$

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

(i) $a = -111$, $m = 99$

$q = -111 \text{ div } 99$ $r = -111 \bmod 99$

$q = -2$ $r = 87$

(ii) $a = -9999$, $m = 101$

$q = -99$ $r = 0$

$$\begin{array}{r} -99 \\ 101 \overline{)\,-9999} \\ +9999 \\ \hline 0 \end{array}$$

(iii) $a = 10299$, $m = 999$

~~q = 9300~~ ~~q = 309~~

$q = 10$, $r = 309$

$$\begin{array}{r} 10 \\ 999 \overline{)\,10299} \\ 9990 \\ \hline 309 \end{array}$$

(iv) $a = 123456$, $m = 1001$

$q = 123$, $r = 333$

(b) congruent to 5 modulo 17

(i) 80

$80 \equiv 5 \pmod{17}$

$80 \bmod 17 = 12$

$5 \bmod 17 = 5$

$$\begin{array}{r} 4 \\ 17 \overline{)\,80} \\ -68 \\ \hline 12 \end{array}$$

$80 \not\equiv 5 \pmod{17}$ as $\frac{80-5}{17} = 4.41$

17 does not divide $a-b$

(ii) 103

$103 \equiv 5 \bmod 17$

$\frac{103-5}{17} = 5.76$ thus

$103 \not\equiv 5 \bmod 17$

(iii) -29

$-29 \equiv 5 \bmod 17$

$\frac{-29-5}{17} = -2$ thus correct

$\boxed{-29 \equiv 5 \bmod 17}$

(iv) -122

$\frac{-122-5}{17} = -7.4$, ~~thus~~ 17 does not divide a-b

thus $-122 \not\equiv 5 \bmod 17$

(Q3) (a) Pairwise relatively prime

(i) 11, 15, 19

$\gcd(11,15) = 1$ $\gcd(11,19) = 1$

$\gcd(15,19) = 1$

thus relatively prime

(ii) 14, 15, 21

gcd(14, 15)

15 = q(14) + r

15 = (1)(14) + 1

14 = q(1) + r

14 = (14)(1) + 0

$\boxed{gcd = 1}$

gcd(15, 21) = $\boxed{3}$

thus not relatively prime

21 = (1)(15) + 7

15 = (2)(7) + 1

7 = (7)(1) + 0

(iii) 12, 17, 31, ~~30~~ 37

gcd(12, 17) = 1 — 17 prime

gcd(17, 31) = 1 — 17 & 31 prime

gcd(17, 37) = 1 — 17 & 37 prime

gcd(12, 31) = 1 — 31 prime

gcd(31, 37) = 1 — 31 & 37 prime

gcd(12, 37) = 1 — 37 prime

(iv) 7, 8, 9, 11

gcd(7, 8) = 1
gcd(7, 9) = 1
gcd(7, 11) = 1
gcd(8, 9) = 1
gcd(8, 11) = 1
gcd(9, 11) = 1

(b) prime factorization

(i) 88 = 2 × 2 × 2 × 11

(ii) 126 = 2 × 3 × 3 × 7

(iii) 729 = 3 × 3 × 3 × 3 × 3 × 3

(iv) 1001 = 11 × 7 × 13

(v) 1111 = 11 × 101

(vi) 909 = 3 × 3 × 101

2	126
3	63
3	21
7	7
	1

2	88
2	44
2	22
11	11
	1

3	909
3	303
101	101
	1

11	1111
	101

11	1001
7	91
13	13
	1

3	729
3	243
3	81
3	27
3	9
3	3
	1

Q(4)

gcd(144, 89)

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

GCD = $\boxed{1}$

~~gcd (1001, 100001)~~

~~100001 = (99) (1001) + (902)~~

$1 = 1\cdot 3 - 1\cdot 2$	$3 = 1\cdot 8 - 1\cdot 5$
$2 = 1\cdot 5 - 1\cdot 3$	$5 = 1\cdot 13 - 1\cdot 8$
	$8 = 1\cdot 21 - 1\cdot 13$
$1 = 1\cdot 3 - 1(1\cdot 5 - 1\cdot 3)$	$13 = 1\cdot 34 - 1\cdot 21$
$1 = 1\cdot 3 - 1\cdot 5 + 1\cdot 3$	$21 = 1\cdot 55 - 1\cdot 34$

$34 = 1\cdot 89 - 1\cdot 55$

~~$55 = 1\cdot 144 - 1\cdot 89$~~

$1 = 1\cdot(1\cdot 8 - 1\cdot 5) - 1\cdot(1\cdot 13 - 1\cdot 8) + 1\cdot(1\cdot 8 - 1\cdot 5)$

$1 = 1\cdot 8 - 1\cdot 5 - 1\cdot 13 + 1\cdot 8 + 1\cdot 8 - 1\cdot 5$

$1 = 1\cdot 8 - 1\cdot(1\cdot 13 - 1\cdot 8) - 1\cdot 13 + 1\cdot 8 + 1\cdot 8 - 1\cdot(1\cdot 13 - 1\cdot 8)$

$1 = 1\cdot 8 - 1\cdot 13 + 1\cdot 8 - 1\cdot 13 + 1\cdot 8 + 1\cdot 8 - 1\cdot 13 + 1\cdot 8$

~~$1 = 1\cdot(1\cdot 21 - 1\cdot 13) - 1\cdot 13 + 1\cdot 8(1\cdot 21 - 1\cdot 13) - 1\cdot$~~

$1 = 5\cdot 8 - 3\cdot 13$

$1 = 5\cdot(1\cdot 21 - 1\cdot 13) - 3(1\cdot 34 - 1\cdot 21)$

$1 = 5\cdot 21 - 5\cdot 13 - 3\cdot 34 + 3\cdot 21$

$1 = 8\cdot 21 - 5\cdot 13 - 3\cdot 34$

~~$1 = 8\cdot(1\cdot 55 - 1\cdot 34) - 5\cdot(1\cdot 34 - 1\cdot 21) - 3\cdot 8$~~

$1 = 8(1\cdot 55 - 1\cdot 34) - 5\cdot(1\cdot 34 - 1\cdot 21) - 3(1\cdot 89 - 1\cdot 55)$

$1 = 8\cdot 55 - 8\cdot 34 - 5\cdot 34 + 5\cdot 21 - 3\cdot 89 + 3\cdot 55$

$1 = 11\cdot 55 - 11\cdot 34 + 5\cdot 21 - 3\cdot 89$

~~$1 = 1$~~

$1 = 11\cdot(1\cdot 144 - 1\cdot 89) - 11(1\cdot 89 - 1\cdot 55) + 5\cdot(1\cdot 55 - 1\cdot 34) - 3\cdot 89$

$1 = (34)\cdot 144 - (55)\cdot 89$

Date:

$\gcd(1001, 100001)$

$100001 = 99(1001) + 902$

$1001 = (1)902 + 99$

$902 = (9)99 + 11$

$99 = (9)11 + 0$

99

$1001 \overline{)100001}$

$11 = 1.902 - 9.99$

$99 = 1.1001 - 1.902$

$902 = 1.100001 - 99.1001$

$11 = 1.902 - 9.99$

$11 = 1(1.100001 - 99.1001) - 9.(1.1001 - 1.902)$

$1.100001 - 99.1001 \quad - 9.1001 + 9.902$

$11 = 1.100001 - 108.1001 + 9.(1.100001 - 99.1001)$

$11 = 1$

$1.100001 - 108.1001 + 9.100001 - 891.1001$

$11 = (10).(100001) - (999).(1.001)$

(Q5) Congruence using modular inverse

(a) $55x \equiv 34 \pmod{89}$

$\gcd(55, 34)$

$89 = 1.55 + 34$

$55 = (1)34 + 21$

$34 = (1)(21) + 13$

$21 = (1)13 + 8$

$13 = (1)(8) + 5$

$8 = (1)5 + 3$

$5 = (1)3 + 2$

$3 = (1)2 + 1$

$2 = (2)1 + 0$

URBANE

Date: M T W T F S S

$1 = 1\cdot 3 - 1\cdot 2$

$2 = 1\cdot 5 - 1\cdot 3$

$3 = 1\cdot 8 - 1\cdot 5$

$5 = 1\cdot 13 - 1\cdot 8$

$8 = 1\cdot 21 - 1\cdot 13$

$13 = 1\cdot 34 - 1\cdot 21$

$21 = 1\cdot 34 - 1\cdot 55$ $\quad 1\cdot 55 - 1\cdot 34$

$34 = 1\cdot 89 - 1\cdot 55$

$1 = 1\cdot 3 - 1\cdot 2$

$1 = 1\cdot 3 - (1\cdot 5 - 1\cdot 3)$

$1 = 1\cdot 3 - 1\cdot 5 + 1\cdot 3$

$1 = 2\cdot 3 - 1\cdot 5$

$1 = 2\cdot (1\cdot 8 - 1\cdot 5) - 1\cdot 5$

$1 = 2\cdot 8 - 2\cdot 5 - 1\cdot 5$

$1 = 2\cdot 8 - 3\cdot 5$

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

$1 = 2\cdot 8 - 3\cdot 13 + 3\cdot 8$

$1 = 5\cdot 8 - 3\cdot 13$

$1 = 5\cdot (1\cdot 21 - 1\cdot 13) - 3\cdot 13$

$1 = 5\cdot 21 - 5\cdot 13 - 3\cdot 13$

$1 = 5\cdot 21 - 8\cdot 13$

$1 = 5\cdot 21 - 8\cdot (1\cdot 34 - 1\cdot 21)$

$1 = 5\cdot 21 - 8\cdot 34 + 8\cdot 21$

$1 = 13\cdot 21 - 8\cdot 34$

~~$1 = 13(1\cdot 34 - 1\cdot 21) - 8\cdot 34$~~

~~$1 = 13\cdot 34 - 13\cdot 21 - 8\cdot 34$~~

~~$1 = 5\cdot 34 - 13\cdot 21$~~

$13\cdot (1\cdot 55 - 1\cdot 34) - 8\cdot 34$

$13\cdot 55 - 13\cdot 34 - 8\cdot 34$

$1 = (13)(55) - (21)(34)$

$55 \cdot$ ~~13~~

$1 = 13\cdot 55 - 21\cdot (1\cdot 89 - 1\cdot 55)$

$1 = 34\cdot 55 - 21\cdot 89$

$\cancel{55}\, x \equiv 34 \times 34 \pmod{89}$

$x = 1156 \pmod{89}$

$1156 = (12)89 + 88$

$\boxed{x = 88}$

~~$13(1\cdot 34 - 1\cdot 55) - 8\cdot 34$~~

~~$13\cdot 34 - 13\cdot 55 - 8\cdot 34$~~

~~$5\cdot 34 - 13\cdot 55$~~

URBANE

(b) $89x \equiv 2 \pmod{232}$

$\gcd(232, 89)$

$232 = (2)(89) + 54$

$89 = (1)54 + 35$

$54 = (1)35 + 19$

$35 = (1)(19) + 16$

$19 = (1)(16) + 3$

$16 = (5)(3) + 1$

$3 = (3)1 + 0$

$1 = 1\cdot16 - 5\cdot3$

$3 = 1\cdot19 - 1\cdot16$

$16 = 1\cdot35 - 1\cdot19$

$19 = 1\cdot54 - 1\cdot35$

$35 = 1\cdot89 - 1\cdot54$

$54 = 1\cdot232 - 2\cdot89$

$1 = 1\cdot16 - 5(1\cdot19 - 1\cdot16)$

$1 = 1\cdot16 - 5\cdot19 + 5\cdot16$

$1 = 6\cdot16 - 5\cdot19$

$1 = 6\cdot(1\cdot35 - 1\cdot19) - 5\cdot19$

$1 = 6\cdot35 - 6\cdot19 - 5\cdot19$

$1 = 6\cdot35 - 11\cdot19$

$1 = 6\cdot35 - 11(1\cdot54 - 1\cdot35)$

$1 = 6\cdot35 - 11\cdot54 + 11\cdot35$

$1 = 17\cdot35 - 11\cdot54$

$1 = 17(1\cdot89 - 1\cdot54) - 11\cdot54$

$1 = 17\cdot89 - 17\cdot54 - 11\cdot54$

$1 = 17\cdot89 - 28\cdot54$

$1 = 17\cdot289 - 28(1\cdot232 - 2\cdot89)$

$1 = 17\cdot89 - 28\cdot232 + 56\cdot89$

$1 = 73\cdot89 - 28\cdot232$

$\cancel{89 \times 73}x = 2 \times 73 \pmod{232}$

$x = 146 \bmod 232$

$146 = (0)232 + 146$

$\boxed{x = 146}$

Date:

(Q6) Chinese remainder

~~$x \equiv 2 \pmod 3$ $x \equiv$~~

$x \equiv 1 \pmod 5$ $\quad x \equiv 2 \pmod 6$ $\quad x \equiv 3 \pmod 7$

$a_1 = 1$ $\quad a_2 = 2$ $\quad a_3 = 3$

$m_1 = 5$ $\quad m_2 = 6$ $\quad m_3 = 7$

$M = 210$

$M_1 = \frac{210}{5} = \boxed{42}$ $\quad M_2 = \boxed{35}$ $\quad M_3 = \boxed{30}$

$y_1 = M_1^{-1} \bmod m_1$

$y_1 = 42^{-1} \bmod 5$

$42 = (8)5 + 2$

$5 = (2)(2) + 1$

$2 = (2)(1) + 0$

$2 = 1 \cdot 42 - 8 \cdot 5$

$1 = 1 \cdot 5 - 2 \cdot 2$

$1 = 1 \cdot 5 - 2(1 \cdot 42 - 8 \cdot 5)$

$1 = 1 \cdot 5 - 2 \cdot 42 + 16 \cdot 5$

$1 = 17 \cdot 5 - 2 \cdot 42$

$-2 + 5 = \boxed{3}$

$y_2 = 35^{-1} \bmod 6$

$35 = (5)6 + 5$

$6 = (1)5 + 1$

$5 = (5)1 + 0$

$5 = 1 \cdot 35 - 5 \cdot 6$

$1 = 6 - 1 \cdot 5$

$1 = 1 \cdot 6 - 1 \cdot (35 - 5 \cdot 6)$

$1 = 1 \cdot 6 - 1 \cdot 35 + 5 \cdot 6$

$1 = 6 \cdot 6 - 1 \cdot 35$

$y_2 = -1 + 6 = \boxed{5}$

$y_3 = 30^{-1} \bmod 7$

$30 = 4 \cdot 7 + 2$

$7 = 3 \cdot 2 + 1$

$2 = (2)1 + 0$

$2 = 1 \cdot 30 - 4 \cdot 7$

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

$1 = 1 \cdot 7 - 3 \cdot (1 \cdot 30 - 4 \cdot 7)$

$1 \cdot 7 - 3 \cdot 30 + 12 \cdot 7$

$13 \cdot 7 - 3 \cdot 30$

$-3 + 7 = \boxed{4} \to y_3$

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

$(128 + 350 + 360) \bmod 210$

$\cancel{838 \bmod 210}$

$\cancel{838 = 3\ 210 + 208}$

$836 \bmod 210$

$836 = 3\ 210 + \boxed{206}$

$\boxed{206}$

(6a) a

(ii) $x \equiv 1 \pmod 2$ $x \equiv 2 \pmod 3$ $x \equiv 3 \pmod 5$

$x \equiv 4 \pmod{11}$

$M = 330$

$m_1 = 2$ $m_2 = 3$ $m_3 = 5$ $m_4 = 11$

$M_1 = 165$ $M_2 = 110$ $M_3 = 66$ $M_4 = 30$

$y_1 = 165^{-1} \bmod 2$

$165 = (82)2 + 1$

$2 = (2)(1) + 0$

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

$y_1 = 1$

$y_2 = 110^{-1} \bmod 3$

$110 = 36(3) + 2$

$3 = (1)(2) + 1$

$2 = (2)(1) + 0$

$1 = 1 \cdot 3 - 1 \cdot 2$

$2 = 1 \cdot 110 - 36 \cdot 3$

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

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

$37 \cdot 3 - 1 \cdot 110$

$y_2 = -1 + 3 = \boxed{2}$

Date: M T W T F S S

$y_3 = 66^{-1} \bmod 5$

$66 = 13(5) + 1$

$5 = (5)(1) + 0$

$1 = \boxed{1} \cdot 66 - 13 \cdot 5$

y_3

$y_4 = 30^{-1} \bmod 11$

$30 = (2)11 + 8$

$11 = (1)8 + 3$

$8 = (2)3 + 2$

$3 = (1)(2) + 1$

$2 = (2)(1) + 0$

$1 = 1 \cdot 3 - 1 \cdot 2$

$2 = 1 \cdot 8 - 2 \cdot 3$

$3 = 1 \cdot 11 - 1 \cdot 8$

$8 = 1 \cdot 30 - 2 \cdot 11$

$1 = 1 \cdot 3 - 1(1 \cdot 8 - 2 \cdot 3)$

$1 = 1 \cdot 3 - 1 \cdot 8 + 2 \cdot 3$

$1 = 3 \cdot 3 - 1 \cdot 8$

$1 = 3 \cdot (1 \cdot 11 - 1 \cdot 8)$

$1 = 3 \cdot 11 - 3 \cdot 8 - 1 \cdot 8$

$1 = 3 \cdot 11 - 4 \cdot 8$

$1 = 3 \cdot 11 - 4(1 \cdot 30 - 2 \cdot 11)$

$1 = 3 \cdot 11 - 4 \cdot 30 + 8 \cdot 11$

$1 = 11 \cdot 11 - 4 \cdot 30$

$y_4 = -4 + 11 = \boxed{7}$

Date:

$x = (1\times165\times1 + 2\times110\times2 + 3\times66\times1 + 4\times30\times7)$ mod 330

1643 mod 330 = 323

(b) $x_1 = 3 \bmod 5$

3 mod 6

1 mod 7

0 mod 11

$M = 2310$

$M_1 = 462$ $M_2 = 385$ $M_3 = 330$ $M_4 = 210$

$y_1 = 462^{-1} \bmod 5$

$462 = 92(5) + 2$

$5 = (2)(2) + 1$

$2 = (2)(1) + 0$

$1 = 1\cdot5 - 2\cdot2$

$2 = 1\cdot462 - 92\cdot5$

$1 = 1\cdot5 - 2(1\cdot462 - 92\cdot5)$

$1\cdot5 - 2\cdot462 + 184\cdot5$

$185\cdot5 - 2\cdot462$

$y_1 = -2 + 5 = \boxed{3}$

$y_2 = 385^{-1} \bmod 6$

~~385 = (77)5 + 0~~

$385 = (64)(6) + 1$

$6 = (6)(1) + 0$

$1 = \boxed{1} \cdot 385 - 64 \cdot 6$

$\boxed{1} \to y_2$

$y_3 = 330^{-1} \bmod 7$

$330 = (47)(7) + 1$

$7 = (7)(1) + 0$

$1 = \boxed{1} 330 - 47 \cdot 7$

$\boxed{1} \to y_3$

$y_4 = 210^{-1} \bmod 11$

$210 = (19) 11 + 1$

$11 = (11)(1) + 0$

$1 = 1 \cdot 210 - 19 \cdot 11$

$1 \to y_4$

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

$5643 \bmod 2310$

$5643 = (2)(2310) + 1023$

$\boxed{1023 \text{ orange}}$

(Q7) find inverse

(a) $a=2, m=17$

2 modulo 17

$\gcd(2,17)$

$17=(8)(2)+1$	$1=17-8\cdot 2$
$2=(2)(1)+0$	
$\downarrow$ gcd $=1$	

$-8+17=\boxed{9}$

(b) $a=34, m=89$

34 modulo 89

$89=(2)34+21$	$1=1\cdot 3-1\cdot 2$
$34=(1)(21)+13$	$2=1\cdot 5-1\cdot 3$
$21=(1)(13)+8$	$3=1\cdot 8-1\cdot 5$
$13=(1)(8)+5$	$5=1\cdot 13-1\cdot 8$
$8=(1)5+3$	$8=1\cdot 21-1\cdot 13$
$5=(1)(3)+2$	$13=1\cdot 34-1\cdot 21$
$3=(1)(2)+1$	$21=1\cdot 89-2\cdot 34$
$2=(2)(1)+0$	

$1 = 1\cdot 3 - 1\cdot 2$

$1 = 1\cdot 3 - 1(1\cdot 5 - 1\cdot 3)$

$1 = 1\cdot 3 - 1\cdot 5 + 1\cdot 3$

$1 = 2\cdot 3 - 1\cdot 5$

$1 = 2\cdot(1\cdot 8 - 1\cdot 5) - 1\cdot 5$

$1 = 2\cdot 8 - 2\cdot 5 - 1\cdot 5$

$1 = 2\cdot 8 - 3\cdot 5$

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

$1 = 2\cdot 8 - 3\cdot 13 + 3\cdot 8$

$1 = 5\cdot 8 - 3\cdot 13$

$1 = 5\cdot(1\cdot 21 - 1\cdot 13) - 3\cdot 13$

$1 = 5\cdot 21 - 5\cdot 13 - 3\cdot 13$

$1 = 5\cdot 21 - 8\cdot 13$

$1 = 5\cdot 21 - 8\cdot(1\cdot 34 - 1\cdot 21)$

$1 = 5\cdot 21 - 8\cdot 34 + 8\cdot 21$

$1 = 13\cdot 21 - 8\cdot 34$

$1 = 13\cdot(1\cdot 89 - 2\cdot 34) - 8\cdot 34$

$1 = 13\cdot 89 - 26\cdot 34 - 8\cdot 34$

$1 = 13\cdot 89 - 34\cdot 34$

$-34 + 89 = \boxed{55}$

(c) $a = 144, m = 233$

$144 \bmod 233$

$233 = (1)144 + 89$	$1 = 1\cdot3 - 1\cdot2$
$144 = (1)89 + 55$	$2 = 1\cdot5 - 1\cdot3$
$89 = (1)55 + 34$	$3 = 1\cdot8 - 1\cdot5$
$55 = (1)34 + 21$	$5 = 1\cdot13 - 1\cdot8$
$34 = (1)(21) + 13$	$8 = 1\cdot21 - 1\cdot13$
$21 = (1)(13) + 8$	$13 = 1\cdot34 - 1\cdot21$
$13 = (1)(8) + 5$	$21 = 1\cdot55 - 1\cdot34$
$8 = (1)5 + 3$	$34 = 1\cdot89 - 1\cdot55$
$5 = (1)3 + 2$	$55 = 1\cdot144 - 1\cdot89$
$3 = (1)(2) + 1$	
$2 = (2)(1) + 0$	

$1 = 2\cdot3 - 1\cdot5$

$1 = 2\cdot8 - 3\cdot5$

$1 = 5\cdot8 - 3\cdot13$

$1 = 5\cdot21 - 8\cdot13$

$1 = 1\cdot21 - 8\cdot34$

$1 = 13\cdot55 - 21\cdot(89 - 55)$

$1 = 89\cdot144 - (-55)\cdot233$

a inverse $= 89$

Date: M T W T F S S

(d) $a = 200$, $n = 1001$

$1001 = (200)(5) + 1$

$(1)(1001) - (200)(5) = 1$

$5 - 1001 = \boxed{-996}$

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

(g)

STOP POLLUTION

19|20|15|16 16|15|12|12|21|20|9|15|14

(i) $(p+4) \bmod 26$

~~23~~ 24

23 24 19 20 20 19 16 16 26 24 13 19 18

W X S T T S P P Y X M S R

(ii) $(p+21) \bmod 26$ or just -5

14 15 10 11 11 10 7 7 16 15 4 10 9

N O J K K J G G P O D J I

(h) Decrypt $(p+10) \bmod 26$ -10

Date: M T W T F S S

CEBB OXNOB XYG

19 21 18 18 5 14 4 5 18 14 15 23

S U R R E N D E R N O W

(ii) LO WI PBSOXN

~~13 14 22 8 15 1 18~~

12 15 23 9 16 2 19 15 24 14

~~1 5 13 8 25 6 18~~

1 5 13 25 6 18 9 5 14 4

B E M Y F R I E N D

(9) Fermat

$5^{2003} \bmod 7$

$5^{7-1} \equiv 1 \bmod 7$

$5^{6} \equiv 1 \bmod 7$

$2003 = (333)(6) + 5$

$5^{333 \times 6 + 5}$

$5^{333 \times 6} \times 5^{5} \bmod 7$

$(5^{6})^{333}$

$1 \times 5^{5} \bmod 7 = 3125 \bmod 7$

$3125 = (446)(7) + \boxed{3}$

$$\boxed{5^{2003} \bmod 7 = 3}$$

(ii) $5^{2003} \bmod 11$

$5^{11-1} = 1 \bmod 11$

$5^{10} = 1 \bmod 11$

$2003 = (200)(10) + 3$

$5^{200 \times 10 + 3} \rightarrow 5^{200 \times 10} \times 5^3 \rightarrow (5^{10})^{200} \times 5^3 \bmod 11$

5^3

$125 \bmod 11$

$125 = (11)(11) + \boxed{4}$

$125 \bmod 11 = 4$

(iii) $5^{2003} \bmod 13$

$5^{12} = 1 \bmod 13$

$\cancel{2003 = (154)(13) + 1}$

$2003 = (166)(12) + 11$

$\cancel{5^{154 \times 13 + 1} \rightarrow 5^{154 \times 13} \times 5 \bmod 13}$

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

48828125 mod 13

$48828125 = (3756009)(13) + \boxed{8} \rightarrow 5^{11} \bmod 13$

(8)

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Date: M T W T F S S

(10)

I LOVE DISCRETE MATHEMATICS

9 12 15 22 5 4 9 19 3 18 5 20 5 13 1 20 8 5 13 1 20 9 3 19

2 ORYH GLVFUHWH PDWKHPDWLFV

(b) (i) Decrypt

MID TWO ASSIGNMENT

(ii) FAST NUCES UNIVERSITY

11(a) $h(k) = k \bmod 97$

(i) 034567981

$34567981 = (356370)97 + \boxed{91}$

(ii) 183211232 $= (1888775)97 + \boxed{57}$

(iii) 220195744 $= (2270059)97 + \boxed{21}$

(iv) 98755335 $= (1016601)97 + \boxed{5}$

Date:
M T W T F S S

(b) $h(k) = k \bmod 101$

(i) $104578890 = (1035434)101 + \boxed{58}$

(ii) $432222187 = (4279427)101 + \boxed{60}$

(iii) $37220191 9 = (368516 7)101 + 32$

(iv) $501338753 = (4963750)\ 101 + \boxed{3}$

(12) $x_{n+1} = (4x_n + 1) \bmod 7 \qquad x_0 = 3$

$x_1 = (12+1) \bmod 7 = 6$

$x_2 = (24+1) \bmod 7 = 4$

$x_3 = (16+1) \bmod 7 = 3$

$x_4 = (12+1) \bmod 7 = 6$

$x_5 = (24+1) \bmod 7 = 4$

$\vdots$

$x_{18} = 3 \qquad x_{19} = 6$

$\vdots$

$x_{20} = (24+1) \bmod 7 = 4$

$x_6 = 3$	$x_{12} = 3$
$x_7 = 6$	$x_{13} = 6$
$x_8 = 4$	$x_{14} = 4$
$x_9 = 3$	$x_{15} = 3$
$x_{10} = 6$	$x_{16} = 6$
$x_{11} = 4$	$x_{17} = 4$

$\boxed{6, 4, 3, 6, 4, 3, 6, 4, 3, 6, 4, 3, 6, 4, 3, 6, 4, 3, 6, 4}$

Date:
M	T	W	T	F	S	S

(13) (a)

(i) 732321 84434

$21+3+6+3+6+1+24+4+12+3+12+X = 0 \pmod{10}$

$95+X = 0 \pmod{10}$

$\boxed{X=5}$

(ii) 6362399 1346

$18+3+18+2+9+9+27+1+9+4+18+X = 0 \pmod{10}$

$118+X = 0 \bmod 10$

$\boxed{X=2}$

(b) (i) 036000291452

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

$60 \equiv 0 \pmod{10}$ ✓

valid

(ii) 012345678903

$0+1+6+3+12+5+18+7+24+9+0+3$

$88 \not\equiv 0 \bmod (10)$

invalid

Date: M T W T F S S

(13) (a)

(i) 732321 84434

$21+3+6+3+6+1+24+4+12+3+12+X = 0 \pmod{10}$

$95+X = 0 \pmod{10}$

$\boxed{X=5}$

(ii) 6362399 1346

$18+3+18+2+9+9+27+1+9+4+18+X = 0 \pmod{10}$

$118+X = 0 \bmod 10$

$\boxed{X=2}$

(b) (i) 036000291452

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

$60 \equiv 0 \pmod{10}$ ✓

Valid

(ii) 012345678903

$0+1+6+3+12+5+18+7+24+9+0+3$

$88 \not\equiv 0 \bmod (10)$

invalid

Date: M T W T F S S

14(a) 1 2 3 4 5 6 7 8 9

0-07-119881

~~0+0+14+3+4+45+48+56+~~

$0+0+21+4+5+54+56+64+9+x \equiv 0 \bmod 11$

$213+x \equiv 0 \pmod{11}$

~~2200 mod 11~~ 8

$213 = (19)\,11 + \boxed{4}$

$\boxed{x=4}$

1 2 3 4 5 6 7 8 9 10

(b) 0-321-500Q1-8

$0+6+6+4+25+0+0+8Q+9+80$

$130+8Q \equiv 0 \bmod 11$

~~130 = (11) (11) + 9~~

inspecting

180

$130+8(3) \equiv 0 \bmod 11$

$\boxed{Q=3}$

Date:

(b)

(15) $n = 43 \times 59 = 2537$

$$\overbrace{0\,19}\ \overbrace{19\,0}\ \overbrace{2\,10}$$

ATTACK

00 1919002 10

$k = (42)(58) = 2436$

$e = 13$

$C = M^{e} \bmod n$

$C = 0^{13} \bmod \cancel{2436}\ 2537$

$C = 0019^{13} (\bmod 2537)$

$C = 1900^{13} (\bmod 2537)$

$C = 0210^{13} (\bmod 2537)$

Q16(a) $27 \times 37 = 999$ offices

(b) $12 \times 2 \times 3 = 72$ shirts

17(a) diff letter initial

$26 \times 26 \times 26 = \boxed{17576 \text{ initials}}$

(b) $26 \times 25 \times 24 = \boxed{15600}$ initials

18(a) ~~$16^{10} + 16^{26} + 16^{3}$~~

18(a) $16^{10} + 16^{26} + 16^{58}$ keys

(b) $26^4 - 26^3 = 66,351$ strings

26 26 26 26 25 25 25 25 without x

19(a) each value can be mapped to one of 2 values

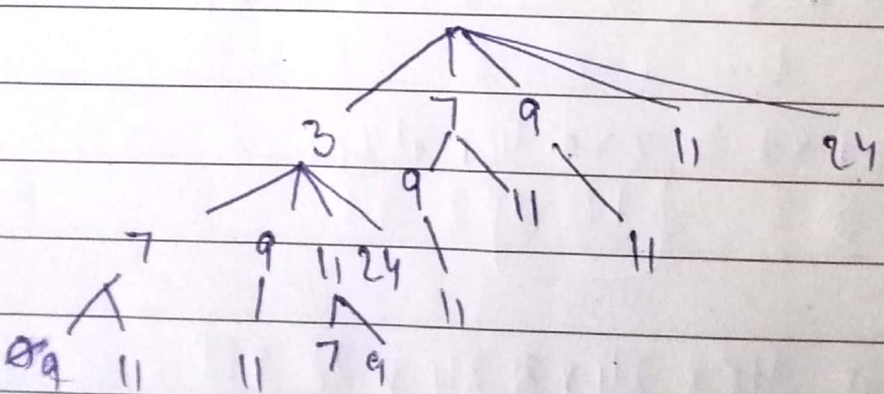
$\boxed{2^m}$

(b) $5 \times 4 \times 3 \times 2 \times 1 = \boxed{120}$

Q20(a)

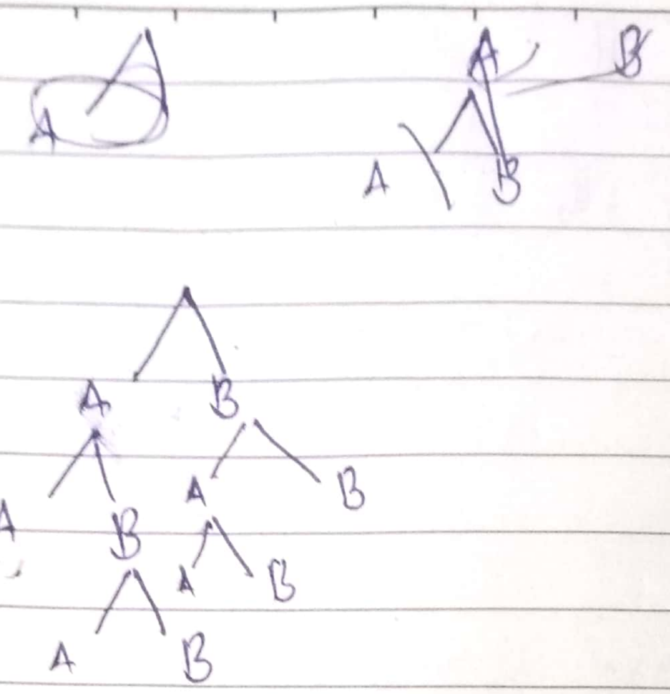
I^5

2^{10}



3

(b)



21 (a) $^8C_3 = 56$ ways

(b) $^{12}C_6 = 924$ ways

(c) $15 \times 14 = 210$

23 (a) $^5C_1 \times {}^3C_2 \times {}^4C_1 \times {}^6C_3 = \boxed{1200}$

(b) $15 \times 48 \times 24 \times 34 \times 28 \times 28 =$ 460,615,680 faces

Date: M T W T F S S

24(a)

2 2 2 2 2 2 2
10 10 10 10 10 10 10

10^7 10^7 2^7 $= 128$

begins

2 2 2 2 2 2 2 2 0 0

$2^8 = 256$ ends

$\cap = 2^5 = 32$

~~A∪B = A+B − A∩B~~ = $\boxed{352}$ strings

$2^8 + 2^7 - 2^5 =$

(b)

2^4 2^3

$2^4 + 2^3 - 2^2$ = $16+8-4 = \boxed{20 \text{ strings}}$

25(a) 30 students, 30 last names

26 possibilities that are unique

$\frac{30}{26} = 2$

(b) $\frac{8\,008\,278}{1000000} = 9$

Date: M T W T F S S

(c) $\frac{677}{38} = 18$

(Q26) x^5 in $(1+x)^{11}$

~~$11C6 \, x^{11-6}$~~

462

$11C5 \, 1^{11-5} \, x^5 = \boxed{462}$

(b) $a^7 b^{17}$ in $(2a-b)^{24}$

$24C17 \, (2a)^7 (-b)^{17}$

$24C17 \, 2^7 (-1)^{17} (a)^7 (b)^{17}$

$-443013 12$

(27) (a) $36! = 3.72 \times 10^{41}$

(b) $36P7$

(c) $20! \times 16!$

Q 28(a)

$n > 5$

$2^{n+5} - 1$ $\qquad$ $2^n - 1$

$2^n \times 32 - 1$

$64^n - 1$ $\qquad$ if $n = 7$

$128 - 1 = \boxed{127}$

prime

(b) $\qquad a \quad p$

~~if $\frac{a}{p}$ then $\frac{a+1}{p}$~~ $\qquad$ Contradiction

$\frac{a}{p} = r \qquad \frac{a+1}{p} = s$

$a = r \cdot p \qquad a = sp - 1$

$sp - 1 = r \cdot p$

$sp - r \cdot p = 1$

$p(s-r) = 1 \quad \rightarrow \frac{1}{p} = s - r$

$p\left(\frac{a+1-a}{p}\right) = 1$

$1 = 1$

if p is -1 or 1 only then can $(s-r)$ be integers, however since P is prime, it has to be > 1, thus our supposition is false, thus original statement is true

$\frac{n}{2}$ ⊙ $d|n$

Date:

M T W T F S S

29(a) $\sqrt{(a+b)} = \sqrt{a} + \sqrt{b}$

$$\sqrt{(a+b)}^2 = (\sqrt{a} + \sqrt{b})^2$$

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

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

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

$$(\sqrt{a}\sqrt{b})^2 = (0)^2$$

$$ab = 0$$ either $a=0$ or $b=0$

(b) if $|x|>1$, then $x>1$ or $x<-1$ for all $x \in R$

contrapositive

$x \leq 1$ and $x \geq -1$ then $|x| \leq 1$

$$-1 \leq x \leq 1$$

modulus would be equal to $|x| \leq 1$

Contraposition true, hence statement true

Date:

(30)(a) Counter example, prime number, $n+2$ is prime

$13+2 = \boxed{15} \rightarrow$ not prime

(b) ~~suppose if~~ prime numbers were finite, the largest possible prime number P ~~would be the largest possible integer N.~~
~~since N+1 > N~~ would divide the largest possible integer N.

if $n+1 > N$ then no greatest integer, ~~and~~ no greatest prime number.

Q31(a) ~~n+m odd~~ n and m odd, n+m even
Contradiction is $n+m =$ odd
n+m odd
$n = 2k+1$ $m = 2k+1$
$n+m =$ ~~2 2~~ $4k+2$
~~$2(2k)+1$~~ $2(2k+1)$ $2k+1 = R$
$\boxed{2R}$ ~~$\rightarrow$ n+m is even~~

~~our supposition~~

Date: M T W T F S S

Q3 (a) ~~D.~~ contradiction:

n and m even, n+m odd

$n = 2k$ $m = 2k$

$n+m = \boxed{4k} \rightarrow n+m$ even

our supposition was false hence statement true

(b) m+n is even $\longrightarrow$ (n and m even) or (n and m odd)

Contraposition:

n and m odd $\rightarrow$ m+n odd

$2k+1 + 2k+1$

$4k+2$

$\underbrace{2(2k+1)}_{\text{even}}$ even our supposit is false
hence statement true

n and m even $\rightarrow$ m+n odd

$2k + 2k$

$4k \rightarrow$ even

our ~~statement~~ supposition
is ~~again~~ false again, thus
original true

Date:

3(a) contradiction : $6-7\sqrt{2}$ is irration

suppose $6-7\sqrt{2}$ is rational

$\neg p \to q$

$$6-7\sqrt{2} = \frac{a}{b} \qquad b \neq 0$$

$$a,b \in \mathbb{Z}$$

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

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

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

according to rational rules, $\sqrt{2}$ is a ration, but $\sqrt{2}$ is irrational

(b) $\sqrt{2}+\sqrt{3}$ is irrational

suppose they are rational and sum is rational

$$\sqrt{2} = \frac{a}{b} \qquad \sqrt{3} = \frac{c}{d} \qquad b,d \neq 0$$

$$a,b,c,d \in \mathbb{Z}$$

$$\sqrt{2}+\sqrt{3} = \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

$$(\sqrt{2}+\sqrt{3})^2 = \frac{(ad+bc)^2}{(bd)^2}$$

$$4 + 2\sqrt{2}\sqrt{3} + 9 = \frac{(ad+bc)^2}{(bd)^2}$$

$$\sqrt{6} = \frac{ad + 2ad + bc}{b^2d^2} - 13$$

show $\sqrt{6}$ is rational, but $\sqrt{6}$ cannot be rational

(Q33) $1^2 + 2^2 + 3^2 + \dots n^2 =$

$(n(n+1)(2n+1))/6$

P(1)

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

$1 = \frac{(1)(2)(3)}{6} = \frac{\cancel{6}}{\cancel{6}} = 1$

true

P(k)

$1 + 4 + 9 \dots k^2 = (k)(k+1)(2k+1)/6$

P(k+1)

$\underbrace{1 + 4 + 9 + \dots k^2}_{} + (k+1)^2 = (k+1)(k+2)(2k+3)/6$

$2(k+1)+1$

$2k+2+1$

$2k+3$

$(k^2+3k+2)(2k+3)$

$2k^3 + 4k^2 + 6k^2 + 9k + 6$

$2k^3 + 9k^2 + 13k + 6$

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

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

$(k+1)(2k^2+k)(6k^2+12k+6) \rightarrow \boxed{\frac{(k+1)(k+2)(2k+3)}{6}}$

(b) $1+2+2^2 \cdots 2^n = 2^{n+1} - 1$

$P(0)$

$2^0 = 2^{0+1} - 1$

$1 = 2 - 1$

$1 = 1$

$P(k)$

$1 + 2 + 2^2 \cdots 2^k = 2^{k+1} - 1$

$P(k+1)$

$\underbrace{1+2+2^2 \cdots + 2^k} + 2^{k+1} = 2^{k+2} - 1$

$2^{k+1} - 1 + 2^{k+1}$

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

$\boxed{2^{k+2} - 1 = 2^{k+2} - 1} \rightarrow LHS = RHS$

Date:

(c) $1^3 + 2^3 + 3^3 + n^3 = \frac{1}{4} n^2 (n+1)^2$

$P(1)$

$1^3 = \frac{1}{4}(1)(1+1)^2$

$1 = \frac{1}{4} \times 4 = \boxed{1 = 1}$

$P(k)$

$1^3 + 2^3 + 3^3 - \ldots + k^3 = \frac{1}{4}(k)^2(k+1)^2$

$\frac{(k^2)(k^2+2k+1)}{4}$

$P(k+1)$

$\underbrace{1^3 + 2^3 + 3^3 - \ldots + k^3}, + \overline{k+1}^3 = \frac{1}{4}(k+1)^2(k+2)^2$

$\frac{(k^2)(k^2+2k+1) + 4(k+1)^3}{4}$

$\frac{(k^2+2k+1)(k^2+4k+4)}{4}$

$\frac{(k)^2 (k+1)^2 + 4(k+1)^3}{4} \quad k(k+1)$

$\frac{(k)^2 (k+1)^2 + (k^2+4k+4)(k+1)^2}{4}$

LHS = RHS

Date: M T W T F S S

Q34

(a) Combinations:

(1) Organizing Teams:

Organizing a huge number of people in separate teams is done ~~o~~ by using combination for e.g 2000 ~~people~~ have to be organized in teams ~~for~~ to build a shopping mall architects. 2000 architect in 7 teams for e.g

(2) University subjects:

Choosing courses and subjects ~~o~~ ~~are~~ can ~~do~~ also be done by combinations. A students can have the choice of 100s of subjects but only have time for 8 in a day. Combination can help choose ~~subjects~~ the ways ~~o~~ to choose subjects

(b) Permutations

(1) ~~Password~~ Protien Formation

~~Highly encrypted and random pa~~

Proteins in our body are ~~a~~ ~~connection~~ connected amino acids, these amino acids have to be in a specific order or the protein will not function.

(2) Password cracking:

~~A~~ Figuring out how many ways a given password can be by its length and other information can help crack ~~o~~ the password more easily by running every possibility.

(c) Binomial Theorem

(i) Economy

The binomial theorem can be used to predict how a country's economy will function in the future and can help avoid economic instability.

(ii) IP addresses

Due to the range of the theorem and the higher amount of electrical devices nowadays, the theorem can be used to generate IP addresses in a very large range.

(d) Proofs

(i) Truths that cannot be calculated:

Proofs help us establish facts that cannot be articulated yet, but can still be used in fields. For e.g. we can prove that prime numbers are infinite but no computer can generate infinite prime numbers yet. However, this proof helps in many fields of maths.

(ii) Discovering new theorems:

A proof can be a base for new theorems and more understanding of the universe. New proofs lead to more theories and more proofs.

Date:
M T W T F S S

(9) Induction.

(1) Puzzle solving skills:

The concept of mathematical induction can help solve puzzle by figuring out patterns. If taught to kids, can make them smarter and more knowledgeable

(2) Computer science

Inductions are used to prove ~~the~~ an algorithm works and how it ~~runs~~ runs ~~it~~ in a particular time ~~()~~.

A common case is recursion, where a base case and extra cases are given in a function.