THE UNIVERSITY
of LIVERPOOL

SOLUTIONS FOR MATH142 (MAY 2007)

(All questions are similar to exercises.)

Section A

1. **Base Step.** We have

$$\sum_{k=1}^{1} \frac{k}{2^{k-1}} = 1/1 = 1 = 4 - \frac{1+2}{1},$$

so the claim is true for $n = 1$.

[1 mark]

Induction Step. Suppose that the claim is true for $n \geq 1$. Then

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

So the claim is true for $n + 1$, as desired.

[4 marks]

Conclusion. By the principle of mathematical induction, the claim is true for all positive integers n.

[1 mark]
[Total: 6 marks]

2. By applying the Euclidean Algorithm (using the "matrix method"), we see that $\gcd(3961, 2091) = 17$,

[4 marks]

and that

$$17 = -19 \cdot 3961 + 36 \cdot 2091.$$

[2 marks]
[Total: 6 marks]

3. By applying the Euclidean Algorithm (using the "matrix method"), we see that

$$1 = -6 \cdot 507 + 17 \cdot 179.$$

[4 marks]

So 17 is the inverse of 179 modulo 507.

[2 marks]
[Total: 6 marks]

4.

(a) We have $gcd(25, 30) = 5$. Since this divides 10, the congruence has solutions. Dividing through by the gcd, the equation becomes $5x \equiv 2 \pmod 6$ (2 marks). By inspection, or by using the Euclidean algorithm, the inverse of 5 modulo 6 is 5 (1 mark). So $x \equiv 2 \cdot 5 \equiv 4 \pmod 6$. The five solutions modulo 30 are therefore $4, 10, 16, 22, 28$. (1 mark.)

[4 marks]

(b) We have $gcd(25, 30) = 5$, which does not divide 11. So the congruence has no solution.

[2 marks]

(c) We have $gcd(11, 30) = 1$, so there is exactly one solution. By inspection, or by using the Euclidean algorithm, the inverse of 11 modulo 30 is 11. So the solution is $x \equiv 25 \cdot 11 \equiv 5 \pmod{30}$.

[4 marks]

[Total: 10 marks]

5. The diagrams are obtained in the standard way: list the elements of the domain to the left, the elements of the range to the right, and draw arrows from x to $f(x)$.

The maps in (a) and (c) are injective. Only the map in (a) is surjective. (Two marks for each diagram, plus three marks for the correct statements on injectivity/surjectivity.)

[Total: 9 marks]

6.

$$\begin{aligned} \pi &= (153)(2674); \\ \varrho &= (154237); \\ \pi^2 &= (135)(27)(64); \\ \varrho\pi &= (1435726). \end{aligned}$$

The orders of the permutations are 12, 6, 6 and 7, while their signs are -1, -1, 1 and 1, respectively. (Four marks for the correct cycle representations, two marks for correct orders, and two marks for correct signs.)

[Total: 8 marks]

7. $G_{18} = \{1, 5, 7, 11, 13, 17\}$. **[2 marks]**

*	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1.

[6 marks]

Elements of order 3 are 7 and 13. **[2 marks]**

[Total: 10 marks]

Section B

8.

(a) Write $x = 5 + 17k$; we need to solve $x \equiv 9 \pmod{13}$. That is,

$$4k \equiv 4 \pmod{13},$$

or $k \equiv 1 \pmod{13}$.

[4 marks]

So $x = 5 + 17(1 + 13\ell) = 22 + 221\ell$, or $x \equiv 22 \pmod{221}$.

[2 marks]

(b) $\varphi(n)$ is defined to be the number of invertible congruence classes modulo n (or: the number of integers $1, \ldots, n-1$ coprime to n).

[1 mark]

We have $\varphi(pq) = (p-1)(q-1)$ when p and q are coprime primes.

[1 mark]

So $\varphi(161) = \varphi(7 \cdot 23) = 6 * 22 = 132$.

[2 marks]

(i) Since 10 is coprime to 161, Euler's theorem gives $10^{132} \equiv 1$, and hence $10^{133} \equiv 10$.

[1 mark]

(ii) Similarly, $10^{265} = 10^{132} \cdot 10^{132} \cdot 10 \equiv 10$.

[1 mark]

(iii) We have $10^{134} \equiv 100$ and $2^{138} \equiv 2^6 = 64$, so $10^{134} + 2^6 \equiv 164 \equiv 3$.

[3 marks]

[Total: 15 marks]

9. The axioms for a group G with operation $*$ are

(G1) $a * b \in G$ for all $a, b, \in G$.
(G2) $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.
(G3) There is $e \in G$ such that, for all $a \in G$, $a * e = e * a = a$.
(G4) For all $a \in G$, there is an element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

[3 marks]

(a) (G1), (G2) and (G3) are satisfied, but (G4) is violated (e.g. 1 has no inverse).

[4 marks]

(b) All four group axioms are satisfied.

[4 marks]

(c) (G1) is not satisfied, since e.g. $2 \cdot 4 = 0$. (G2) and (G3) are satisfied, but (G4) is not satisfied (e.g. 2 has no inverse).

[4 marks]

[Total: 15 marks]

10.

(a) A group G is *cyclic* if there is an element $a \in G$ such that $G = \{a^n : n \in \mathbb{Z}\}$.

[1 mark]

We have $G_{14} = \{1, 3, 5, 9, 11, 13\}$.

[1 mark]

$3^1 = 3$, $3^2 = 9$, $3^3 = 13$, $3^4 = 11$, $3^5 = 5$, $3^6 = 1$. All elements of G_{14} are included, so G **is cyclic**.

[3 marks]

(b) H is a *subgroup* of G if it is a group under the operation of G. (Alternatively: if $e \in H$, $a * b \in H$ for all $a, b \in H$, and $a^{-1} \in H$ for all $a \in H$.)

[2 marks]

*	1	9	11
1	1	9	11
9	9	11	1
11	11	1	9

Since $1 \in H$, all entries in the table are in H, and every column contains an entry 1 (i.e., all inverses are in H), we see that H is a subgroup.

[5 marks]

(c) A subgroup of order two of G_{14} is given by $\{1, 13\}$.

[3 marks]

[Total: 15 marks]

11. The code words are:
0000000, 1001011, 0100110, 0011100,
1101101, 1010111, 0111010, 1110001.

[2 marks]

The minimum weight of a non-zero codeword is 3. So two errors are detected, and one error is corrected. **[2 marks]**

The parity check matrix is

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

[2 marks]

The syndromes and coset leaders are as follows:

Syndromes	Coset leaders
1011	1000000
0110	0100000
1100	0010000
1000	0001000
0100	0000100
0010	0000010
0001	0000001

[3 marks]

We now decipher the given message:

Received message w	Syndrome wH	Coset leader h	Corrected message $w+h$	result	letter
0100110	0000	(n.a.)	0100110	010	G
1001101	0110	0100000	1101101	110	O
1101001	0100	0000100	1101101	110	O
0011100	0000	(n.a.)	0011100	001	D
1001111	0100	0000100	1001011	100	L
1100001	1100	0010000	1110001	111	U
0010000	1100	0010000	0000000	000	C
0111010	0000	(n.a.)	0111010	011	K

[6 marks]

[Total: 15 marks]