The University Of Sheffield.

SCHOOL OF MATHEMATICS AND STATISTICS **Spring Semester 2012–2013**

Numbers and Groups **2 hours**

Answer ***all questions****.*
You should justify your answers carefully unless the question states otherwise.

1 (i) Explain how we can use the Chinese Remainder Theorem to solve any pair of simultaneous congruences

$$\begin{aligned} x &\equiv a \pmod{y} \\ x &\equiv b \pmod{z} \end{aligned}$$

where y and z are coprime. ***(1 mark)***

(ii) Solve the following pair of simultaneous congruences:

$$\begin{aligned} x &\equiv a \pmod{11} \\ x &\equiv b \pmod{10} \end{aligned}$$

(2 marks)

(iii) Assuming your statement in part (i), prove by induction on n that for any $n \geq 2$ we can solve the set of n simultaneous congruences

$$\begin{aligned} x &\equiv a_1 \pmod{k_1} \\ x &\equiv a_2 \pmod{k_2} \\ &\vdots \\ x &\equiv a_n \pmod{k_n} \end{aligned}$$

where for any $i \neq j$ the pair k_i, k_j are coprime.

(4 marks)

2 (i) Let $f : A \longrightarrow B$ and $g : B \longrightarrow C$ be functions. Prove that if the composite gf is surjective then g must be surjective. Must f be surjective?

(4 marks)

(ii) Consider the function $f : \mathbb{Z} \longrightarrow \{0, 1, 2, 3, 4\}$ defined by

$$f(a) \equiv a \pmod 5.$$

Is f injective? Is f surjective? Justify your answers carefully. ***(3 marks)***

3 (i) Let (a_n) be a sequence of real numbers. State the formal definition of what it means for (a_n) to converge to $a \in \mathbb{R}$. ***(1 mark)***

(ii) Prove from first principles that the following sequence of real numbers does not converge in $\mathbb{R}$:

$$a_n = \begin{cases} 0 & n \equiv 0 \pmod{10} \\ 1 & n \not\equiv 0 \pmod{10} \end{cases}$$

(5 marks)

(iii) Is the sequence in part (ii) bounded? Justify your answer. ***(1 mark)***

4 (i) For each of the permutations $\alpha \in S_6$ shown below, find the cycle decomposition of $\alpha(1\ 2\ 3\ 4)\alpha^{-1}$.

(a) $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 3 & 4 & 5 & 2 \end{pmatrix}$;

(b) $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 4 & 3 & 6 \end{pmatrix}$;

(c) $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 4 & 3 & 6 & 1 \end{pmatrix}$.

What pattern do you notice? Assuming this pattern continues, find a permutation $\beta \in S_6$ for which $\beta(1\ 2\ 3\ 4)\beta^{-1} = (3\ 4\ 5\ 6)$, and state the order of $\alpha(1\ 2\ 3\ 4)\alpha^{-1}$ for any $\alpha \in S_6$. ***(6 marks)***

(ii) In $GL_2(\mathbb{Z}_7)$, let $A = \begin{pmatrix} \overline{2} & \overline{3} \\ \overline{1} & \overline{0} \end{pmatrix}$ and $B = \begin{pmatrix} \overline{0} & \overline{6} \\ \overline{6} & \overline{0} \end{pmatrix}$.

(a) Find A^{-1} and calculate ABA^{-1}.

(b) Find the orders of B and ABA^{-1}.

(4 marks)

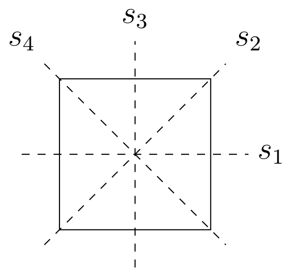
(iii) Let G be any group and let $g, h \in G$. Show that the order of ghg^{-1} is the same as the order of h. ***(3 marks)***

5 (i) For a permutation $\alpha \in S_n$, define what it means for α to be even, what it means for α to be odd, and what is meant by the sign of α. For $n \geq 2$, consider the relation $\sim$ on S_n given by

$$\alpha \sim \beta \iff \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta) = 1.$$

Is $\sim$ an equivalence relation? ***(4 marks)***

(ii) Let $D_4 = \{r_0, r_1, r_2, r_3, s_1, s_2, s_3, s_4\}$ denote the group of symmetries of the square, as usual, where $r_i = \text{rot}_{\frac{i\pi}{2}}$ for each i and the s_j are reflections in the lines indicated below.



Write down the elements of the cyclic subgroup $H = \langle r_3 \rangle$ of D_4. How many distinct left-cosets of H are there in G? Show that the left-coset s_1H is not subgroup of G. ***(3 marks)***

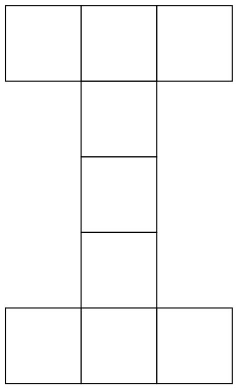
(iii) State Lagrange's Theorem. Consider the subset of $S = \{\overline{0}, \overline{4}, \overline{8}\}$ of $\mathbb{Z}_{10}$. Explain why the size of S shows that S is not a subgroup of $\mathbb{Z}_{10}$ under addition, then find a counter-example to one of SG1, SG2 or SG3. ***(3 marks)***

(iv) Let G be a group, and consider the function $f : G \to G \times G$ given by $f(g) = (g, g)$. Show that the image of f is a subgroup of $G \times G$. ***(3 marks)***

6 (i) Define what is meant by a non-empty set G being a group under an operation $\odot$. ***(4 marks)***

(ii) Let S be a non-empty set and let $\odot$ be an operation for which $a \odot b = b$ for all $a, b \in S$. Show that S is a group under $\odot$ if and only if S contains just one element. ***(4 marks)***

(iii) A stained-glass tile is to be formed from small coloured glass squares stuck together in the shape below.



Find the number of essentially different colourings of the tile using 4 green and 5 blue squares, making your method clear. ***(5 marks)***

End of Question Paper