NATIONAL UNIVERSITY OF SINGAPORE
MATHEMATICS SOCIETY

PAST YEAR PAPER SOLUTIONS
with credits to Lin Mingyan Simon

MA2202 Algebra I
AY 2010/2011 Sem 1

Question 1

(a) Firstly, we have $n^2-3n^5 = n^2(1-3n^3)$. As $n^3 \equiv 0,1,6 \bmod 7$, it follows that $1-3n^3 \equiv 1,4,5 \bmod 7$, and hence $7 \nmid 1-3n^3$. Hence, we have $7|\, n^2(1-3n^3) \Leftrightarrow 7|\, n^2 \Leftrightarrow n = 7$, and thus $f(7) = 7$.
As a consequence, we see that for $n = 1,2,3,4,5,6$, one has $f(n) = r_n = (n^2-3n^5-7q_n) \bmod 7 = n^2(1-3n^3) \bmod 7$. Then by direct computation, it is easy to see that $f(1) = 5$, $f(2) = 6$, $f(3) = 1$, $f(4) = 3$, $f(5) = 2$, $f(6) = 4$.
Therefore, we see that the element $\alpha = (1\,5\,2\,6\,4\,3) \in S_7$ may be used to represent the bijection f.

(b) We have $\alpha = (1\,5\,2\,6\,4\,3) = (1\,5\,2\,6\,4\,3)(7)$. Thus one has $\mathrm{sgn}(\alpha) = (-1)^{7-2} = -1$.

Question 2

Let the number of stolen coins be x. Then by the question, x satisfies the following set of relations:

$$x \equiv 2 \pmod{13}, \quad (1)$$
$$x \equiv 2 \pmod{9}, \quad (2)$$
$$x \equiv 0 \pmod{5}. \quad (3)$$

From (3) we deduce that $x = 5k$ for some $k \in \mathbb{Z}$. Substituting this into (2), we get $5k \equiv 2 \pmod 9$, which would imply that $k \equiv 10k \equiv 2 \cdot 5k \equiv 2 \cdot 2 \equiv 4 \pmod 9$. Hence, we have $k = 9m+4$ for some $m \in \mathbb{Z}$, and consequently $x = 5k = 45m+20$.
Finally, by substituting the last equation into (1), one has $45m+20 \equiv 2 \pmod{13}$, or equivalently, $6m \equiv 8 \pmod{13}$. This would imply that $m \equiv 66m \equiv 11 \cdot 6m \equiv 11 \cdot 8 \equiv 10 \pmod{13}$. Hence, we have $m = 13n+10$ for some $n \in \mathbb{Z}$, and consequently $x = 45m+20 = 585n+470$.
As $x \geq 0$, we see that the least possible value of x is 470. We check that $x = 470$ indeed satisfies the 3 relations above, so the least number of coins that could have been stolen is 470.

Question 3

Let us arbitrarily label one of the beads as 1, and label the remaining beads 2-4 in a clockwise direction. Let $C = \{c_1, c_2, c_3\}$ be the set of 3 colours. Let $A = \{(a_1,a_2,a_3,a_4) | a_i \in C, i = 1,2,3,4\}$ denote the set of colourings (a_1,a_2,a_3,a_4) given to beads 1 to 4 in the ascending order.

Note that the colourings (a_1,a_2,a_3,a_4), (a_2,a_3,a_4,a_1), (a_3,a_4,a_1,a_2), (a_4,a_1,a_2,a_3), (a_1,a_4,a_3,a_2), (a_4,a_3,a_2,a_1), (a_3,a_2,a_1,a_4) and (a_2,a_1,a_4,a_3) would all give rise to the same bracelet. Henceforth, we let $r = (1\,2\,3\,4) \in S_4$ and $s = (2\,4) \in S_4$, and denote the group $G = \langle r, s\rangle$.

As we have the order of r and s to be 4 and 2 respectively, and $rs = (1\,2\,3\,4)(2\,4) = (1\,2)(3\,4) = (2\,4)(1\,4\,3\,2) = (2\,4)(1\,2\,3\,4)^{-1} = sr^{-1}$, we must have $G = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$.

We define a group action $\alpha : G \times A \to A$, such that $\alpha(\sigma, (a_1, a_2, a_3, a_4)) = (a_{\sigma(1)}, a_{\sigma(2)}, a_{\sigma(3)}, a_{\sigma(4)})$, where $\sigma \in G$. We note that $A_1, A_2 \in A$ would give rise to the same bracelet if and only if there exists some $\sigma \in G$ such that $\alpha(\sigma, A_1) = A_2$. Hence, the number of orbits N would correspond to the total number of distinct bracelets.

Now, let $\text{Fix}(g)$ denote the number of elements in A that is fixed by the element g under the group action α, i.e. $\alpha(g, X) = X$. Note that an element $X \in A$ is fixed by $g \in G$ if and only if beads of X whose corresponding numbers in the same disjointed cycle have the same colour. Based on this, we see that $\text{Fix}(e) = 3^4 = 81$, $\text{Fix}(r) = 3$, $\text{Fix}(r^2) = 3^2 = 9$, $\text{Fix}(r^3) = 3$, $\text{Fix}(s) = 3^3 = 27$, $\text{Fix}(sr) = 3^2 = 9$, $\text{Fix}(sr^2) = 3^3 = 27$, $\text{Fix}(sr^3) = 9$. Hence, by the Burnside's Lemma, we have

$$\begin{aligned} N &= \frac{1}{|G|} \sum_{\sigma \in G} \text{Fix}(\sigma) \\ &= \frac{1}{8} \big(\text{Fix}(e) + \text{Fix}(r) + \text{Fix}(r^2) + \text{Fix}(r^3) + \text{Fix}(s) + \text{Fix}(sr) + \text{Fix}(sr^2) + \text{Fix}(sr^3)\big) \\ &= \frac{1}{8}(81 + 3 + 9 + 3 + 27 + 9 + 27 + 9) = 21. \end{aligned}$$

We conclude that there are 21 distinct bracelets of 4 beads each, each of which can be coloured red, blue or white.

Question 4

(a) The elements of $(\mathbb{Z}/21\mathbb{Z})^*$ are $[1]_{21}, [2]_{21}, [4]_{21}, [5]_{21}, [8]_{21}, [10]_{21}, [11]_{21}, [13]_{21}, [16]_{21}, [17]_{21}, [19]_{21}, [20]_{21}$. The elements of $(\mathbb{Z}/13\mathbb{Z})^*$ are $[1]_{13}, [2]_{13}, [3]_{13}, [4]_{13}, [5]_{13}, [6]_{13}, [7]_{13}, [8]_{13}, [9]_{13}, [10]_{13}, [11]_{13}, [12]_{13}$.

(b) Firstly, we shall show that $(\mathbb{Z}/21\mathbb{Z})^*$ is not cyclic. Take any $a \in \mathbb{Z}$ such that $0 < a < 21$ and $(a, 21) = 1$. Then one has $(a, 3) = (a, 7) = 1$. This implies that $a^2 \bmod 3 = 1$ and $a^3 \bmod 7 = 1$. Hence, we must have $a^6 \bmod 21 = 1$, which implies that the order of each element in $(\mathbb{Z}/21\mathbb{Z})^*$ is at most 6. As the order of the group $(\mathbb{Z}/21\mathbb{Z})^*$ is 12, we conclude that $(\mathbb{Z}/21\mathbb{Z})^*$ is not cyclic.

On the other hand, we note that the order of any element in $(\mathbb{Z}/13\mathbb{Z})^*$ must divide 12. Bearing this in mind, and observing that $2^2 \bmod 13 = 4 \neq 1$, $2^3 \bmod 13 = 8 \neq 1$, $2^4 \bmod 13 = 3 \neq 1$, $2^6 \bmod 13 = 12 \neq 1$, we see that the order of the element $[2]_{13}$ in $(\mathbb{Z}/13\mathbb{Z})^*$ must be equal to 12. Hence, we have $(\mathbb{Z}/13\mathbb{Z})^* = \langle [2]_{13} \rangle$, so $(\mathbb{Z}/13\mathbb{Z})^*$ is necessarily cyclic.

Hence, the two groups $(\mathbb{Z}/21\mathbb{Z})^*$ and $(\mathbb{Z}/13\mathbb{Z})^*$ are not isomorphic to each other.

Question 5

(a) We have $\alpha^{m+1}\beta^{m+1} = (\alpha\beta)^{m+1} = (\alpha\beta)^m\alpha\beta = \alpha^m\beta^m\alpha\beta$ for all $\alpha, \beta \in G$, so after simplification one has $\alpha\beta^m = \beta^m\alpha$. Similarly, by using the fact that $\alpha^{m+1}\beta^{m+1} = (\alpha\beta)^{m+2}$, we get $\alpha\beta^{m+1} = \beta^{m+1}\alpha$. Hence, we have $\beta^{m+1}\alpha = \alpha\beta^{m+1} = (\alpha\beta^m)\beta = \beta^m\alpha\beta$, which after simplification, gives us $\beta\alpha = \alpha\beta$. This shows that G is abelian so we are done.

(b) Take $G = S_3$ and $m = 6$. Clearly, G is non-abelian. Also, as $|G| = 6$, we must have $\sigma^6 = (1)$ for all $\sigma \in G$, so one has $(\alpha\beta)^6 = (1) = (1)(1) = \alpha^6\beta^6$, and $(\alpha\beta)^7 = \alpha\beta = \alpha^7\beta^7$ for all $\alpha, \beta \in G$.

Question 6

Define the map $\phi : G \to G/M \times G/N$ as follows: $\phi(g) = (gM, gN)$ for all $g \in G$. We shall show that ϕ is a surjective group homomorphism with kernel $M \cap N$. Let $g_1, g_2 \in G$. One has $\phi(g_1g_2) = (g_1g_2M, g_1g_2N) = (g_1M, g_1N) \cdot (g_2M, g_2N) = \phi(g_1) \cdot \phi(g_2)$. So ϕ is a group homomormphism.

Next, take any $g, h \in G$. Since $G = MN$, we must have $g = m_1n_1$ and $h = m_2n_2$ for some $m_1, m_2 \in M$ and $n_1, n_2 \in N$. Then we have

$$\begin{aligned}
\phi(n_1m_2) &= \phi(n_1) \cdot \phi(m_2) \\
&= (n_1M, n_1N) \cdot (m_2M, m_2N) \\
&= (m_1^{-1}gM, N) \cdot (M, hn_2^{-1}N) \quad \text{(because } m_1 \in M \text{ and } n_1 \in N.) \\
&= (m_1^{-1}Mg, N) \cdot (M, hn_2^{-1}N) \quad \text{(because } M \text{ is normal in } G; \text{ hence } gM = Mg.) \\
&= (Mg, N) \cdot (M, hN) \quad \text{(because } m_1^{-1} \in M \text{ and } n_2^{-1} \in N.) \\
&= (gM, N) \cdot (M, hN) \quad \text{(because } M \text{ is normal in } G; \text{ hence } gM = Mg.) \\
&= (gM, hN).
\end{aligned}$$

Hence, this shows that ϕ is surjective.

Finally, we have

$$\begin{aligned}
\ker(\phi) &= \{g \in G | \phi(g) = (M, N)\} \\
&= \{g \in G | (gM, gN) = (M, N)\} \\
&= \{g \in G | gM = M, gN = N\} \\
&= \{g \in G | g \in M \text{ and } g \in N\} = M \cap N.
\end{aligned}$$

Therefore, by the First Isomorphism Theorem, one has $G/(M \cap N) \simeq G/M \times G/N$ as desired.

Question 7

(a) Take any $h_1, h_2 \in H$. We have $\vartheta(h_1h_2) = g(h_1h_2)g^{-1} = (gh_1g^{-1})(gh_2g^{-1}) = \vartheta(h_1)\vartheta(h_2)$, so this shows that ϑ is a group homomorphism from H to G.

(b) Since ψ is a group homomorphism, it follows that for all $h_1, h_2 \in H$, one has $h_1h_2 = (h_2^{-1}h_1^{-1})^{-1} = \psi(h_2^{-1}h_1^{-1}) = \psi(h_2^{-1})\psi(h_1^{-1}) = h_2h_1$. Therefore, H is abelian.

(c) Pick any $g \notin H$. Then one has g to have an order of 2 (so that $g = g^{-1}$), and $G = H \cup gH$. Also, we note that for all $h \in H$, one has $gh \in gH$. Therefore, it follows that gh has an order of 2, which would imply that $(gh)^2 = ghgh = e$. Thus, one has $h^{-1} = ghg = ghg^{-1}$.

Hence, we see that $\vartheta(h) = ghg^{-1} = h^{-1} \in H$ for all $h \in H$, where ϑ is the group homomorphism as defined in part (a), so in fact ϑ is a group homomorphism from H to H. Hence, we must have $\vartheta = \psi$, where ψ is the group homomorphism as defined in part (b). As ϑ is a group homomorphism, we see that by part (b) H is necessarily abelian. We are done.