NATIONAL UNIVERSITY OF SINGAPORE
MATHEMATICS SOCIETY

PAST YEAR PAPER SOLUTIONS
with credits to Teo Wei Hao

MA2202 Algebra I
AY 2006/2007 Sem 2

Question 1

If $a \in \mathbb{Z}$ such that $7 \nmid a$, then by Fermat's Little Theorem, $a^6 \equiv 1 \mod 7$.
This give us $a^{6601} = a \cdot a^{6 \cdot 1100} = a \cdot \left(a^6\right)^{1100} \equiv a \cdot 1^{1100} = a \mod 7$.
Else if $7 \mid a$, then $a^{6601} \equiv 0 \equiv a \mod 7$. Thus for all $a \in \mathbb{Z}$, we have $7 \mid a^{6601} - a$.

If $a \in \mathbb{Z}$ such that $23 \nmid a$, then by Fermat's Little Theorem, $a^{22} \equiv 1 \mod 23$.
This give us $a^{6601} = a \cdot a^{22 \cdot 300} = a \cdot \left(a^{22}\right)^{300} \equiv a \cdot 1^{300} = a \mod 23$.
Else if $23 \mid a$, then $a^{6601} \equiv 0 \equiv a \mod 23$. Thus for all $a \in \mathbb{Z}$, we have $23 \mid a^{6601} - a$.

If $a \in \mathbb{Z}$ such that $41 \nmid a$, then by Fermat's Little Theorem, $a^{40} \equiv 1 \mod 41$.
This give us $a^{6601} = a \cdot a^{40 \cdot 165} = a \cdot \left(a^{40}\right)^{165} \equiv a \cdot 1^{165} = a \mod 41$.
Else if $41 \mid a$, then $a^{6601} \equiv 0 \equiv a \mod 41$. Thus for all $a \in \mathbb{Z}$, we have $41 \mid a^{6601} - a$.

Since $7, 23$ and 41 are pairwise coprime, we conclude that $6601 = 7 \cdot 23 \cdot 41 \mid a^{6601} - a$.
Thus $a^{6601} \equiv a \mod 6601$.

Question 2

(a) Since $a \mid bc$, there exists $n \in \mathbb{Z}$ such that $an = bc$.
Let $d_1 = \gcd(a, b)$ and $d_2 = \gcd(a, c)$. Thus there exists $s_1, s_2, t_1, t_2 \in \mathbb{Z}$ such that

$$\begin{aligned} as_1 + bt_1 &= d_1 \\ as_2 + ct_2 &= d_2. \end{aligned}$$

This give us,

$$\begin{aligned} d_1 d_2 = (as_1 + bt_1)(as_2 + ct_2) &= a^2 s_1 s_2 + abt_1 s_2 + acs_1 t_2 + bct_1 t_2 \\ &= a^2 s_1 s_2 + abt_1 s_2 + acs_1 t_2 + ant_1 t_2 \\ &= a(as_1 s_2 + bt_1 s_2 + cs_1 t_2 + nt_1 t_2). \end{aligned}$$

Thus $a \mid d_1 d_2$.

(b) Let $d_1 = \gcd(2^m - 1, 2^n - 1)$ and $d_2 = \gcd(m, n)$. Thus there exists $s, t \in \mathbb{Z}$ such that $ms + nt = d_2$.

Since $d_1 \mid 2^m - 1$, we have $2^m \equiv 1 \mod d_1$. Similarly, $2^n \equiv 1 \mod d_1$.
Thus, we get $2^{d_2} = 2^{ms+nt} = (2^m)^s \cdot (2^n)^t \equiv 1^s \cdot 1^t = 1 \mod d_1$, i.e. $d_1 \mid 2^{d_2} - 1$.

Since $2^{d_2} - 1 \mid 2^{d_2} - 1$, we have $2^{d_2} \equiv 1 \mod 2^{d_2} - 1$.
Since $d_2 \mid m$, there exists $a \in \mathbb{Z}$ such that $ad_2 = m$. Thus $2^m = \left(2^{d_2}\right)^a \equiv 1^a = 1 \mod 2^{d_2} - 1$.
This give us $2^{d_2} - 1 \mid 2^m - 1$. Similarly, $2^{d_2} - 1 \mid 2^n - 1$, and so $2^{d_2} - 1 \mid d_1$.

Therefore, we conclude that $d_1 = 2^{d_2} - 1$.

Question 3

For all $a, b \in G$, we have $a^3b^3 = (ab)^3 = ababab$, and so $a^2b^2 = baba$.
Similarly from $a^5b^5 = (ab)^5$, we get $a^4b^4 = (ba)^4 = (baba)^2 = \left(a^2b^2\right)^2 = a^2b^2a^2b^2$.
This give us $a^2b^2 = b^2a^2$, i.e. $baba = b^2a^2$.
Therefore $ab = ba$, i.e. G is abelian.

Question 4

(a) We have $\alpha = \begin{pmatrix} 1 & 8 & 6 & 7 & 2 & 5 & 3 \end{pmatrix}\begin{pmatrix} 4 & 9 \end{pmatrix}$. Thus $\alpha^{-1} = \begin{pmatrix} 1 & 3 & 5 & 2 & 7 & 6 & 8 \end{pmatrix}\begin{pmatrix} 4 & 9 \end{pmatrix}$.
Also, $\mathrm{sgn}(\alpha) = -1$.

(b) We have $\alpha = \begin{pmatrix} 1 & 3 & 2 & 4 \end{pmatrix}\begin{pmatrix} 1 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 4 & 3 \end{pmatrix}$, and so $\alpha^{-1} = \begin{pmatrix} 2 & 3 & 4 \end{pmatrix}$.
Also $\beta = \begin{pmatrix} 2 & 6 \end{pmatrix}\begin{pmatrix} 3 & 2 & 6 & 8 \end{pmatrix} = \begin{pmatrix} 3 & 6 & 8 \end{pmatrix}$.

$$\begin{aligned} \alpha\beta\alpha^{-1} &= \begin{pmatrix} 2 & 4 & 3 \end{pmatrix}\begin{pmatrix} 3 & 6 & 8 \end{pmatrix}\begin{pmatrix} 2 & 3 & 4 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 6 & 8 \end{pmatrix}. \end{aligned}$$

(c) Every element in S_5 can be written as a complete factorization into disjoint cycles. The order of each cycle is the number of elements in the cycle. Thus the largest order is equivalent to the largest LCM possible of a partition of 5. By listing out all the partitions, we get $2 + 3 = 5$ to give the largest LCM of $2 \times 3 = 6$. It is easy to check that $\begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 4 & 5 \end{pmatrix}$ has order 6, and thus it is an element with the largest order in S_5.

Question 5

(a) $([3]_8)^2 = ([5]_8)^2 = ([7]_8)^2 = [1]_8$, thus $(\mathbb{Z}/8\mathbb{Z})^* \simeq V$, the Klein 4-group, and so is not cyclic.

(b) All the generators of $(\mathbb{Z}/11\mathbb{Z})^*$ are $[2]_{11}, [6]_{11}, [7]_{11}$ and $[8]_{11}$.

Question 6

Let us arbitrarily name one of the sector as 1, and allocate the remaining sectors number 2 to 9 in a clockwise direction. Let $C = \{c_1, c_2, c_3, c_4\}$ be the set of 4 colours.
Let $A = \{(a_1, a_2, \ldots, a_9) \mid a_i \in C, i = 1, 2, \ldots 9\}$ correspond to the colouring given to sector 1 to 9.

Let $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}$, and group $G = \langle g \rangle$. We define an action $\alpha : G \times A \to A$ such that $\alpha_\sigma(a_1, a_2, \ldots a_9) = \left(a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(9)}\right)$. We notice that $B_1, B_2 \in A$ give the same resulted disk iff there exists $\sigma \in G$ such that $\alpha_\sigma(B_1) = B_2$. Thus the number of orbits N correspond to the number of distinct disk.

Let $\sigma \in G$, we have $B \in A$ to be fixed by σ iff sectors of B which numbers in the same disjointed cycle have the same colour. This give us $\mathrm{Fix}(1_G) = 4^9$, $\mathrm{Fix}(g^3) = \mathrm{Fix}(g^6) = 4^3$, and
$\mathrm{Fix}(g) = \mathrm{Fix}(g^2) = \mathrm{Fix}(g^4) = \mathrm{Fix}(g^5) = \mathrm{Fix}(g^7) = \mathrm{Fix}(g^8) = 4$. Thus,

$$\begin{aligned} N &= \frac{1}{|G|}\sum_{\sigma \in G} \mathrm{Fix}(\sigma) \\ &= \frac{1}{9}\left(4^9 + 2 \cdot 4^3 + 6 \cdot 4\right) = 29144. \end{aligned}$$

Therefore there are 29144 distinct flags in total.

Question 7

(a) Let denote $\sqrt{-1} = i$. We have,

$$\begin{aligned} BAB &= \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ &= A. \end{aligned}$$

(b) By performing matrix operations, we obtain $B^2 = A^2$ and $A^4 = I$.

Thus we have,

$$\begin{aligned} (A)^2 &\neq I, \\ \left(A^2\right)^2 = A^4 &= I, \\ \left(A^3\right)^2 = A^4 \cdot A^2 = A^2 &\neq I, \\ (B)^2 = A^2 &\neq I, \\ (BA)^2 = (BAB)A = A^2 &\neq I, \\ \left(BA^2\right)^2 = BA^2BA^2 = BB^2BB^2 = \left(B^2\right)^3 = \left(A^2\right)^3 = A^6 = A^2 &\neq I, \\ \left(BA^3\right)^2 = BAA^2BAA^2 = BAB^2BAB^2 = A(BAB) = A^2 &\neq I. \end{aligned}$$

Therefore the only element of order 2 in G is A^2.

(c) No.
D_8 has 2 elements of order 2, but G has only 1.

Question 8

Let $H \leq G$ such that $|H| = |K|$. Since $K \lhd G$, by Second Isomorphism Theorem, we get $HK \leq G$, $H \cap K \lhd H$, and $H/(H \cap K) \simeq HK/K$, i.e. $[H : H \cap K] = [HK : K]$.

Now $HK/K \leq G/K$, thus $[HK : K] \mid [G : K]$ by Lagrange Theorem.
However $[H : H \cap K] = |H|/|H \cap K| \mid |H| = |K|$ by consequence of Lagrange Theorem.
Thus, $|HK/K| \mid \gcd(|K|, [G : K]) = 1$, and so $|HK/K| = 1$.
This force $HK/K = \{K\}$, and so for all $h \in H$, $k \in K$, we have $hK = hkK = K$, i.e. $h \in K$.
Since $|H| = |K|$, we have $H = K$, i.e. K is the unique subgroup of G having order $|K|$.