MA 222: Elementary Number Theory and Algebra
Mid semester examination
Model solutions and marking scheme

---

1. Determine the last two digits in the decimal representation of $3^{40000004}$. [1]

   Solution. Since $\gcd(3, 100) = 1$, we have $3^{\phi(100)} = 3^{40} \equiv 1 \pmod{100}$.
   Now, $3^{40000004} = 3^{40000000} \times 3^4 \equiv 81 \pmod{100}$. Hence, the last two digits are 81. $\square$

2. Find the remainder of 65^{123456} when it is divided by 10000. [3]

   Solution. We have $10000 = 10^4 = 2^4 \times 5^4$. Now,

$$65^{123456} \equiv 1 \pmod{2^4} \quad \text{and} \quad 65^{123456} \equiv 0 \pmod{5^4}.$$

[1]

   Hence, $x_0 = 65^{123456}$ is a simultaneous solution of the congruences $x \equiv 1 \pmod{2^4}$ and $x \equiv 0 \pmod{5^4}$.
   Now, applying CRT, we find another simultaneous solution x_1 of the congruences $x \equiv 1 \pmod{2^4}$ and $x \equiv 0 \pmod{5^4}$. Let $m_1 = 2^4$, $m_2 = 5^4$, $a_1 = 1, a_2 = 0$. Then, we have $b_1 \equiv (5^4)^{-1} \equiv 1 \pmod{2^4}$ and $b_2 \equiv (2^4)^{-1} \equiv 586 \pmod{5^4}$ (since $a_2 = 0$, so we need not evaluate b_2). Hence,

$$x_1 = (5^4 \times 1 \times 1) + (2^4 \times 586 \times 0) = 5^4 = 625.$$

[1]

   Thus, $65^{123456} = x_0 \equiv x_1 \equiv 625 \pmod{10000}$.
   Hence, the required remainder is 625. [1] $\square$

3. Let $\{a_1, a_2, \ldots, a_{101}\}$ and $\{b_1, b_2, \ldots, b_{101}\}$ be complete residue systems modulo 101 such that $a_{101} \equiv b_{101} \equiv 0 \pmod{101}$. Can $\{a_1b_1, a_2b_2, \ldots, a_{101}b_{101}\}$ be a complete residue system modulo 101? [2]

   Solution. Suppose that $\{a_1b_1, a_2b_2, \ldots, a_{101}b_{101}\}$ is a complete residue system modulo 101. By Wilson's theorem, we have $a_1a_2 \cdots a_{100} \equiv b_1b_2 \cdots b_{100} \equiv 100! \equiv -1 \pmod{101}$. Hence, $a_1b_1a_2b_2 \cdots a_{100}b_{100} \equiv 1 \pmod{101}$. [1]

   But, $a_{101}b_{101} \equiv 0 \pmod{101}$, so again by Wilson's theorem $a_1b_1a_2b_2 \cdots a_{100}b_{100} \equiv 100! \equiv -1 \pmod{101}$, a contradiction. Hence, $\{a_1b_1, a_2b_2, \ldots, a_{101}b_{101}\}$ can't be a complete residue system modulo 101. [1] $\square$

4. Let $a_1 = 3$ and $a_{n+1} = 3^{a_n}$ for $n \geq 1$. Prove that $a_4 \equiv a_3 \pmod{100}$. [2]

   Solution. We have $a_1 = 3, a_2 = 3^3, a_3 = 3^{3^3}$ and $a_4 = 3^{3^{3^3}}$.
   We have $\phi(100) = \phi(4)\phi(25) = 2 \times 20 = 40$. By Euler's theorem, we have $3^{40} \equiv 1 \pmod{100}$, and hence

$$3^{3^4} = 3^{81} = 3^{2 \times 40 + 1} \equiv 3 \pmod{100}. \qquad [1]$$

Now, $a_4 = 3^{3^{3^3}} = \left(3^{3^4}\right)^{3^{3^3-4}} \equiv 3^{3^{3^3-4}} = 3^{3^{23}} \pmod{100}$. Applying this repeatedly, we have

$$a_4 = 3^{3^{3^3}} = 3^{3^{27}} \equiv 3^{3^{23}} \equiv 3^{3^{19}} \equiv \cdots \equiv 3^{3^7} \equiv 3^{3^3} = a_3 \pmod{100}. \qquad [1]$$

$\square$

5. Solve the congruence $x^2 + x + 47 \equiv 0 \pmod{343}$. [3]

Solution. We have $343 = 7^3$. We first consider the equation $f(x) = x^2 + x + 47 \equiv 0 \pmod 7$, equivalently, $x^2 + x - 2 \equiv 0 \pmod 7$. We find that $x \equiv 1 \pmod 7$ and $x \equiv 5 \pmod 7$ are the only solutions of $x^2 + x - 2 \equiv 0 \pmod 7$.
Now, $f'(x) = 2x + 1$ and $f'(1) = 3 \not\equiv 0 \pmod 7$ and $f'(5) = 11 \not\equiv 0 \pmod 7$. Thus, $a_1 = 1$ and $b_1 = 5$ are both non-singular roots of $x^2 + x + 47 \equiv 0 \pmod 7$. [1]
By Hensel's lemma, $a_1 = 1$ lifts to $a_2 = a_1 - f(a_1) \times \overline{f'(a_1)} = 1 - 49 \times 5 \equiv 1 \pmod{7^2}$.
Hence, $a_3 = a_2 - f(a_2) \times \overline{f'(a_1)} = 1 - 49 \times 5 \equiv 99 \pmod{7^3}$ is a required solution. [1]

Now, $b_1 = 5$ lifts to $b_2 = b_1 - f(b_1) \times \overline{f'(b_1)} = 5 - 77 \times 2 \equiv 47 \pmod{7^2}$.
Hence, $b_3 = b_2 - f(b_2) \times \overline{f'(b_1)} = 47 - 2303 \times 2 \equiv 243 \pmod{7^3}$ is the other required solution. [1] $\square$

6. Find all the *finite* subsets of $\mathbb{Z}$ which are *monoids* under multiplication. [1]

Solution. $\{0\}$, $\{1\}$, $\{1, -1\}$, $\{-1, 0, 1\}$, and $\{0, 1\}$. $\square$

7. Prove that every finitely generated subgroup of $(\mathbb{Q}, +)$ is cyclic. [2]

Solution. Let $H = \langle a_1, a_2, \ldots, a_m \rangle$ be a finitely generated subgroup of $(\mathbb{Q}, +)$. Then, $H = a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_m\mathbb{Z}$. [1]
Let $a_i = \frac{p_i}{q_i}$. Let $\ell = \operatorname{lcm}(q_1, q_2, \ldots, q_m)$.
Then, $H \leq \frac{1}{\ell}\mathbb{Z}$. Since $\frac{1}{\ell}\mathbb{Z} = \langle \frac{1}{\ell} \rangle$ is cyclic, so H is also cyclic. [1] $\square$

8. What is the value of α for which $\{\alpha, 1, 3, 9, 19, 27\}$ becomes a cyclic group under multiplication modulo 56? [1]

Solution. We have

$$3^2 = 9, \quad 3^3 = 27, \quad 3^4 = 81 \equiv 25 \pmod{56}, \quad 3^5 \equiv 19 \pmod{56}, \quad 3^6 \equiv 1 \pmod{56}.$$

Hence, $\alpha = 25$. $\square$

9. Let G be a group and $x \in G$. If $o(x) = 5$, can the centralizer of x and the centralizer of x^3 be equal? [1]

Solution. Let $a \in G$. If $ax = xa$, then $ax^3 = xax^2 = x^2ax = x^3a$.
If $ax^3 = x^3a$, then $ax = ax^6 = x^3ax^3 = x^6a = xa$.
Hence, $C_G(x) = C_G(x^3)$. $\square$

10. Let G be a group and $a \in G$ be an element of order 30. Find all the distinct left cosets of $\langle a^9 \rangle$ in $\langle a \rangle$. [2]

Solution. We have $o(a^9) = 10$. Hence, there are 3 distinct left cosets of $\langle a^9 \rangle$ in $\langle a \rangle$. We have $\langle a^9 \rangle = \{a^{3k} : k = 0, 1, 2, \ldots, 9\}$. [1]

Hence, the distince left cosets are $\langle a^9 \rangle$, $a\langle a^9 \rangle$ and $a^2\langle a^9 \rangle$. [1] □

11. Let $f \in S_7$. If $f^5 = (2\ 3\ 4\ 1\ 6\ 5\ 7)$, then find f. [2]

Solution. We have $7 = o(f^5) = \frac{o(f)}{\gcd(5, o(f))}$. Hence, $o(f)$ is a multiple of 7. In S_7, possible orders of elements are 1, 2, 3, 4, 5, 6, 7, 10, 12. Hence, $o(f) = 7$, and $f = f^{15}$. [1]

Now, $f^{10} = (2\ 3\ 4\ 1\ 6\ 5\ 7)(2\ 3\ 4\ 1\ 6\ 5\ 7) = (1\ 5\ 2\ 4\ 6\ 7\ 3)$ and
$f^{15} = (2\ 3\ 4\ 1\ 6\ 5\ 7)(1\ 5\ 2\ 4\ 6\ 7\ 3) = (1\ 7\ 4\ 5\ 3\ 6\ 2)$. Hence, $f = (1\ 7\ 4\ 5\ 3\ 6\ 2)$. [1] □

12. Let G be a group. If $a \in G$ is the only element of order 2, then prove that a lies in the center of G. [2]

Solution. Let $x \in G$. Then $o(a) = o(xax^{-1})$. [1]

Since a is the only element of order 2, so $xax^{-1} = a$ for every $x \in G$. That is, $xa = ax$ for every $x \in G$. Hence, a is in the center of G [1] □

13. (a) Write down all the elements of S_4 of order 4. [1]
 (b) Write down all the subgroups of S_4 of order 4. [2]

Solution. (a) An element of S_4 has order 4 if and only if it is a 4-cycle. There are six 4-cycles which are $(1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 4\ 2), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)$. [1]

(b) The six elements of order 4 give 3 cyclic subgroups of order 4, which are
$\{(1), (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\}$,
$\{(1), (1\ 2\ 4\ 3), (1\ 4)(2\ 3), (1\ 3\ 4\ 2)\}$,
$\{(1), (1\ 3\ 2\ 4), (1\ 2)(3\ 4), (1\ 4\ 2\ 3)\}$. [1]
There are four non-cyclic subgroups of order 4 in S_4, which are
$\{(1), (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$,
$\{(1), (1\ 3), (2\ 4), (1\ 3)(2\ 4)\}$,
$\{(1), (1\ 4), (2\ 3), (1\ 4)(2\ 3)\}$,
$\{(1), (1\ 4)(2\ 3), (1\ 3)(2\ 4), (1\ 2)(3\ 4)\}$. [1]

□

14. Determine all the group homomorphisms $f : \mathbb{Z}_4 \to S_3$. [2]

Solution. Method 1: Since $\mathbb{Z}_4$ is cyclic, so if $f : \mathbb{Z}_4 \to S_3$ is a homomorphism, then $f(k) = kf(1)$ for any $k \in \mathbb{Z}_4$. Since $o(f(1))|4$ and S_3 has no element of order 4, so $o(f(1)) = 1$ or $o(f(1)) = 2$. [1]

Thus, we have 4 homomorphisms from $\mathbb{Z}_4$ to S_3, namely
$f_1 : 1 \mapsto (1)$
$f_2 : 1 \mapsto (1\ 2)$

$f_3 : 1 \mapsto (1\ 3)$
$f_4 : 1 \mapsto (2\ 3)$. [1]
Method 2: We know that $|\mathrm{Im}(f)|$ divides $|\mathbb{Z}_4| = 4$ and $|\mathrm{Im}(f)|$ divides $|S_3| = 6$. Hence, $|\mathrm{Im}(f)| = 1$ or $|\mathrm{Im}(f)| = 2$. The rest follows similarly as shown in Method-1. $\square$

15. Give an example of a *non-abelian* group all of whose subgroups are normal. [2]

Solution. Let $Q_8 = \{I, -I, A, -A, B, -B, C, -C\}$,
where $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, C = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$.
Let H be a subgroup of Q_8. Then $|H| = 1, 2, 4, 8$. If $|H| = 1, 8$, then H is a normal subgroup of Q_8. If $|H| = 4$, then it has index 2, and hence normal. [1]

If $|H| = 2$, then $H = \{I, -I\}$. If $x \in Q_8$, then $xH = \{x, -x\} = Hx$.
Hence, H is normal. [1] $\square$

16. Does there exist an onto homomorphism from $(\mathbb{Q}, +)$ to $(\mathbb{Z}, +)$? [2]

Solution. Let $f : (\mathbb{Q}, +) \to (\mathbb{Z}, +)$ be an onto homomorphism. Since f is onto, let $q \in \mathbb{Q}$ be such that $f(q) = 1$. [1]

Since f is a homomorphism, so $1 = f(q) = f(q/2 + q/2) = 2f(q/2)$. But, $f(q/2)$ is an integer, and hence $2f(q/2) = 1$ is a contradiction. This proves that there can't be any onto homomorphism from $(\mathbb{Q}, +)$ to $(\mathbb{Z}, +)$. [1] $\square$

• • •