28/08/2022/xyz

Name: **Roll No.**

MA 222: Elementary Number Theory and Algebra

Max. Marks: 10 Quiz- I Max. Time: 50 minutes

$\mathbb{Z}$:= the set of integers, $\mathbb{Q}$:= the set of rational numbers, and $\mathbb{R}$:= the set of real numbers.

1. What are the positive integers n such that 11 divides $2^n + 2$? [1]
   Answer: $n \equiv 6 \pmod{10}$.
   Solution: By Fermat's little theorem, we have $2^{10} \equiv 1 \pmod{11}$. We need to find an n such that $2^n \equiv -2 \pmod{11}$, and note that $2^1 \equiv 2,\ 2^2 \equiv 2,\ 2^3 \equiv 8,\ 2^4 \equiv 5,\ 2^5 \equiv -1,\ 2^6 \equiv -2 \pmod{11}$.
   For any $k \in \mathbb{N} \cup \{0\}$, $2^{10k+6} = 2^{10k} \cdot 2^6 \equiv 1 \cdot (-2) \pmod{11}$. This implies 11 divides $2^n + 4$ when $n \equiv 6 \pmod{10}$.

2. For $n \geq 0$, let [2]

$$A_n = 2^{3n} + 3^{6n+2} + 5^{6n+2}.$$

   What is the greatest common divisor of the numbers $A_0, A_1, A_2, \ldots, A_{88888}$?
   Answer: 7.
   Solution: $A_0 = 35$ and gcd of the above numbers will divide A_n for all $n \geq 0$. Therefore, the only possibilities for gcd can be 1, 5, 7, or 35. Also, 5 does not divide A_1 since $A_1 \equiv 4 \pmod{5}$. Thus gcd cannot be equal to 5 or 35.
   By Fermat's little theorem, we have $3^6 \equiv 1 \pmod{7}$ and $5^6 \equiv 1 \pmod{7}$. Therefore,

$$\begin{aligned} A_n &\equiv 2^{3n} + 3^2 + 5^2 \\ &\equiv 1 + 6 \equiv 0 \pmod{7}. \end{aligned}$$

   This implies that 7 divides A_n for all $n \geq 0$ and hence gcd is 7.

3. What is the remainder of $5 \times 50! + 5!$ when it is divided by 53? [1]
   Answer: 38.
   Solution: By Wilson's theorem, $52! \equiv -1 \pmod{53}$. Then

$$\begin{aligned} 52 \times 51 \times 50! &\equiv -1 \pmod{53} \\ (-2) \times (-1) \times 50! &\equiv -1 \pmod{53} \\ 50! &\equiv -27 \pmod{53} \qquad (2 \times 27 = 54 \equiv 1 \pmod{53}) \end{aligned}$$

   Now, $5! + (5 \times 50!) = 120 + (5 \times 50!) \equiv 14 - (5 \times 27) \equiv 38 \pmod{53}$.

4. What is the smallest positive integer x_0 satisfying [1]

$$x_0 \equiv 3 \pmod{5} \quad \text{and} \quad x_0 \equiv 7 \pmod{13}?$$

Answer: 33.
Solution: Here $m_1 = 5,\ m_2 = 13,\ a_1 = 3$, and $a_2 = 7$. Then $m = 65$. By Chinese remainder theorem, solution is given by

$$x_0 = \frac{m}{m_1} b_1 a_1 + \frac{m}{m_2} b_2 a_2,$$

where $13b_1 \equiv 1 \pmod 5$ and $5b_2 \equiv 1 \pmod{13}$. We get $b_1 = 2$ and $b_2 = 8$. So, $x_0 = 13 \times 2 \times 3 + 5 \times 8 \times 7 = 358$. The smallest solution is given by $358 \pmod{65} = 33$.

5. What is the remainder of $7^{493828002}$ when it is divided by 10000? [1]
Answer: 49.
Solution: By Euler's theorem, $7^{\phi(10^4)} \equiv 1 \pmod{10^4}$, i.e., $7^{4000} \equiv 1 \pmod{10^4}$. Now,

$$7^{493828002} = \left(7^{4000}\right)^{123457} \cdot 7^2 \equiv 1 \cdot 7^2 \equiv 49 \pmod{10^4}.$$

6. For $a, b \in \mathbb{R}$, define $f_{a,b} : \mathbb{R} \to \mathbb{R}$ by $f_{a,b}(x) = ax + b$. Then $G = \{f_{a,b} : a, b \in \mathbb{R}, a \neq 0\}$ is a group under composition of functions.

   (a) What is the inverse of $f_{1,5}$ in G? [1]
   Answer: $f_{1,-5}$ or $f_{1,-5}(x) = x - 5$.
   Solution: If $f_{a,b}$ is the inverse of $f_{1,5}$ then $f_{1,5} \circ f_{a,b}(x) = x = f_{a,b} \circ f_{1,5}(x)$, for all $x \in \mathbb{R}$, i.e., $f_{1,5}(ax + b) = ax + b + 5 = x$, which gives $a = 1$ and $b = -5$. Hence, $f_{1,-5}$ is the inverse of $f_{1,5}$.

   (b) What are the elements of order 2 in G? [1]
   Answer: $f_{-1,b}$, $b \in \mathbb{R}$.
   Solution: Let $f^2_{a,b}(x) = x$, for all $x \in \mathbb{R}$. Thus, $f^2_{a,b}(x) = f_{a,b}(ax + b) = a(ax + b) + b = a^2x + ab + b = x$, which implies $a^2 = 1$ and $ab = -b$. Now, if $a = 1$ then $b = 0$, which gives $f_{1,0}$. But it is of order 1. And if $a = -1$ then b can be any real number. Therefore, for any $b \in \mathbb{R}$, $f_{-1,b}$ is an order 2 element in G.

7. Which of the following group(s) is(are) **not** cyclic? [1]
(A) $(2022\mathbb{Z}, +)$ (B) $(\mathbb{Q}, +)$ (C) $(U(8), \cdot)$ (D) $(U(10), \cdot)$
Answer: (B), (C).
Solution: (A) is cyclic: The group $(2022\mathbb{Z}, +)$ is cyclic with 2022 as a generator since any element of the group is of the form $2022n$, for some $n \in \mathbb{Z}$.
(B) is not cyclic: Suppose $\frac{a}{b}$ is a generator of $(\mathbb{Q}, +)$, where $a, b \in \mathbb{Z}$ and $b \neq 0$. Then we can write $\frac{1}{2b} = n\frac{a}{b}$, for some $n \in \mathbb{Z}$, i.e., $\frac{1}{2} = na$. This is a contradiction since right hand side is an integer whereas left hand side is not.
(C) is not cyclic: No element in $U(8) = \{1, 3, 5, 7\}$ has order 4.
(D) is cyclic: In $U(10) = \{1, 3, 7, 9\}$, the order of 3 is 4.

8. What are the subsets of $\mathbb{Z}$ which are groups under multiplication? [1]
Answer: $\{0\}$, $\{1\}$, $\{1, -1\}$.

• • •