MIDSEMESTRAL

Elementary Number Theory

Instructor: Ramdin Mawia Marks: **30** **Time:** September 11, 2025; 14:00–17:00.

Attempt FIVE problems. The maximum you can score is 30.

1. Let p be a prime, and n be a positive integer. Prove that the highest power of p dividing $n!$ is given by **7**
$$e = \sum_{j=1}^{\infty} \left[\frac{n}{p^j} \right]$$
where $[x]$ denotes the largest integer $\leqslant x$. Using this or otherwise, prove the following: If $a_1, ..., a_k$ are nonnegative integers such that $a_1 + \cdots + a_k = n$, then $n!/a_1! \cdots a_k!$ is an integer. [*Hint.* $[x] + [y] \leqslant [x + y]$.]

2. If m and n are positive integers having the same prime factors, show that $m/\varphi(m) = n/\varphi(n)$. Using this or otherwise, prove the following: Given any positive integer n, there is a positive integer m such that $\varphi(m) = n!$ [*Hint.* You may choose m and $n!$ to have the same prime factors.] **7**

3. State whether the following statements are true or false, with complete justifications:
   i. If $p \equiv 1 \pmod 4$ is a prime, then $[(\frac{p-1}{2})!]^2 \equiv -1 \pmod p$. **3**
   ii. Let p be an odd prime, k a positive integer and x, y be dinstinct integers such that $x \equiv y \pmod{p^k}$ and $p \nmid xy$. If n is a positive integer such that $n \equiv 0 \pmod{p^\ell}$ for some integer $\ell \geqslant 0$, then **4**
$$x^n \equiv y^n \pmod{p^{k+\ell}}.$$

4. Find the smallest positive integer x (if any) such that $x^5 \equiv 7 \pmod{19}$. **7**

5. Let $p \geqslant 5$ be a prime. Write **7**
$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} = \frac{a}{b}$$
where a and b are integers. Prove that $p|a$. **Bonus (+5 marks)**: Show that in fact $p^2|a$. [*Hint for the bonus problem.* Let $f(X) = (X-1)(X-2)\cdots(X-p+1)$. Prove that there is a polynomial $r(X)$ with integer coefficients such that $X^p - X = Xf(X) + pr(X)$. Compare both sides and evaluate $f(p)$.]

6. Prove that there are infinitely many primes of the form $4k+1$. [*Hint.* Let $n \geqslant 2$ be an integer. Then any prime factor of $N := (n!)^2 + 1$ is of the form $4k + 1$.] **7**

OR

6′. Let $p > 5$ be a prime. Suppose there is an integer a with $1 < a < p - 2$ which has order 3 mod p. Prove that $p \equiv 1 \pmod 6$ and find the order of $a + 1$ mod p.

7. Let p be an odd prime. When do we say that an integer r is a *primitive root* for p? Let $(r, p) = 1$ and $p - 1 = p_1^{e_1} \cdots p_k^{e_k}$ be the prime factorisation of $p - 1$. Prove that r is a primitive root for p if and only if **7**
   i. $r^{p-1} \equiv 1 \pmod p$;
   ii. $r^{(p-1)/p_i} \not\equiv 1 \pmod p$ for any $i = 1, ..., k$.

OR

7′. Find the smallest positive integer x satisfying
$$\begin{aligned} x &\equiv 0 \pmod 3, \\ x &\equiv 1 \pmod 5, \\ x &\equiv 2 \pmod{14}. \end{aligned}$$

–The End–