MIDSEMESTRAL

Elementary Number Theory

Instructor: Ramdin Mawia Marks: **30** **Time:** September 12, 2024; 10:00–13:00.

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

---

1. Let p be an odd prime and $r \in \mathbb{Z}$ be a primitive root mod p. Prove or disprove: **6**
   i. $r^{(p-1)/2} \equiv -1 \pmod{p}$.
   ii. If $p \equiv 1 \pmod{4}$, then $-r$ is also a primitive root mod p.

2. Find the last 2025 digits of $3^{10^{2024}}$ in the usual decimal notation. Justify all the steps. **6**

3. State whether the following statements are true or false, with complete justifications: **6**
   i. If $p \equiv 1 \pmod{4}$ is a prime, then $[(\frac{p-1}{2})!]^2 \equiv -1 \pmod{p}$.
   ii. If p is an odd prime, then
   $$(1+p)^{p^k} \equiv 1 + p^{k+1} \pmod{p^{k+2}}$$
   for all $k \geqslant 0$.

4. If $\gcd(a, b) = 1$, determine all possible values of $\gcd(a + 2b, 7a + b)$. Give examples where these values are attained. **6**

5. Prove that there are infinitely many primes of the form $3k + 1$. [*Hint.* Assume $p_1, ..., p_n$ are primes of the form $3k + 1$. Use the QRL to prove that any prime factor of $4(p_1 \cdots p_n)^2 + 3$ is also of the form $3k + 1$.] **6**

OR

5′ Prove that there are infinitely many primes of the form $8k - 1$. [*Hint.* Assume $p_1, ..., p_n$ are all the primes of the form $8k - 1$. Look at $(p_1 \cdots p_n)^2 - 2$ and apply QRL.] **6**

6. Describe all primes p for which 7 is a quadratic residue mod p. **6**

7. Given that $p = 102317$ is prime, determine whether the number 102029 is a quadratic residue or nonresidue mod p. [*Hint.* You may use the Reciprocity Law for the Jacobi symbol.] **6**

8. Given that $p = 2^{2^4} + 1 = 65537$ is a prime ("Fermat prime"), prove that $a \in \mathbb{Z}$ is a primitive root mod p if and only if it is a quadratic nonresidue mod p. Use it to find the period[1] of the rational number $1/65537$. **10**

---

[1] The *period* of a rational number is the number of repeating digits in its decimal expansion. Eg. $1/7 = 0.\overline{142857}$ has period 5.