Number Theory - First midterm test
November 11, 2021 : Should be emailed before 5 PM
B. Math. (Hons.) First year
Instructor : B. Sury
Maximum marks 50.

DO NOT consult classmates or others. Be Brief but complete. Results that are assumed without proof have to be stated precisely. For questions with two choices, solve only one of them. All questions carry equal marks.

Q 1. Prove:
(a) If p/q is a rational number that is a root of a polynomial of the form $x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ where c_i's are integers, then p/q must be an integer.
(b) $\sum_{m=k}^{m=n} \binom{m}{k} = \binom{n+1}{k+1}$.
(c) No number in the sequence $11, 111, 1111, \cdots$ can be a perfect square.
(d) For each n, $11^{n+2} + 12^{2n+1}$ is divisible by 133.
(e) For all n, $\phi(n)|n!$.

Q 2.
(i) For any positive integer m and any integer a, prove that $a^{m-\phi(m)} \equiv a^m$ mod m.
(ii) For a positive integer c and co-prime integers a, b, show that there exists an integer d satisfying $\mathrm{GCD}(a + bd, c) = 1$.

OR

(i) For any positive integer m, determine the number of solutions for x mod m of the congruence $x(x-1) \equiv 0$ mod m.
(ii) Obtain the exact number when $m = 100!$ (the last number is factorial of 100).
Hint for (i). Consider the prime power decomposition of m.

Q 3.
(i) Let $F_n = 2^{2^n} + 1$ for any $n \geq 0$. Prove that $2^{F_n - 1} \equiv 1 \bmod F_n$ for all n.
(ii) For the numbers $M_p = 2^p - 1$ where p is a prime, again prove that $2^{M_p - 1} \equiv 1 \bmod M_p$.

OR

Given n distinct primes $\{p_1, p_2, \cdots, p_n\}$, prove that there exist n consecutive integers where the i-th integer is divisible by the i-th prime. Note that we are not assuming $p_1 < p_2$ etc.

Q 4.
(i) If $p > 3$ is a prime, prove that the product of the primitive roots mod p is congruent to 1 mod p.
(ii) Prove that if $p \equiv 1 \bmod 4$ is a prime such that $(p-1)/4$ is also prime, then 2 is a primitive root mod p.
Hint for (i). For a primitive root a mod p, look at the powers which are primitive roots mod p.

OR

Let a, b be positive integers and p be a prime. Consider the sequence of positive integers defined by

$$c_0 = p, c_{n+1} = ac_n + p \quad \forall\ n \geq 0.$$

Prove that some c_n must be composite.

Q 5.
If a is an integer such that $a^2 \equiv -1 \bmod 5^{10}$, show that there exists an integer b such that $b^2 \equiv -1 \bmod 5^{11}$ and $b \equiv a \bmod 5^{10}$.

OR

For a prime p, consider the sum of all $a < p$ which are primitive roots mod p. Show that the sum is $\mu(p-1)$ mod p.