MAT215 ELEMENTARY NUMBER THEORY & CRYPTOGRAPHY PROBLEM SHEET 1

MANJIL SAIKIA

Any letter denoting a number (such as a, b, c, n, etc.) is always considered to be an integer, unless otherwise mentioned.

(1) Prove that $\sqrt{7}$ is irrational.
(2) Prove that any prime of the form $3n + 1$ is also of the form $6m + 1$.
(3) Which primes are of the form $n^3 - 1$?
(4) Show that $n^4 + 4$ is never a prime, when $n > 1$.
(5) If $p \neq 1$ is an odd prime, then prove that either $p^2 - 1$ or $p^2 + 1$ is divisible by 10.
(6) If p_n is the n-th prime number, then show that $p_n \leq 2^{2^{n-1}}$.
(7) If $n > 2$, prove that there exists a prime p such that $n < p < n!$.
(8) If p_i is the i-th prime number, then show that $p_1 p_2 \cdots p_n + 1$ is never a perfect square.
(9) Show that there exists k consecutive composite numbers, for every integer k.
(10) Show that there are infinitely many primes of the form $4k + 3$.
(11) If p and $p^2 + 8$ are both primes, then show that $p^3 + 4$ is also a prime.
(12) How many zeroes does 100! end in?

Here are some advanced problems for you to try.[1]

(a) Prove that for a positive integer s, we have
$$\sum_{n=1}^{\infty} n^{-s} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}.$$
(b) How many steps are required for the Euclidean Algorithm to terminate if the input is $\gcd(a, b)$?

Date: 28 August 2025.

[1] Note that these problems are slightly harder, and if you are unable to solve them, it is perfectly fine. We will not ask problems of such difficulty in the mid-semester examination.