Assignment - 1

Instructions

i) *Section I* contains 15 theoretical problems. Attempt at least 8 of them.

ii) *Section II* contains Programming tasks. Attempt at least one of them.

iii) The submission for *Section I* has to be done in this *drive link*. You can submit either latex or handwritten solutions.

iv) The submission for *Section II* has to be done in the *'Assignment-1'* folder of the github repository *'Number-Theory-Cryptography'*. The README.md file will be updated with further instructions.

Section I

1. x, y are natural numbers such that
$$\text{lcm}(x, y) + \gcd(x, y) = x + y$$
Prove that $x|y$ or $y|x$.

2. For integers $m \geq n \geq 1$, the following expression is always an integer.
$$\frac{\gcd(m, n)}{n}\binom{n}{m}$$

3. For natural numbers n, m
   (a) Prove that if $n > m$, then $\gcd(m, n) = \gcd(m, n - m)$.
   (b) express $\gcd(2022^m - 1, 2022^n - 1)$ in terms of $\gcd(m, n)$.
   (c) express $\gcd(2021^m + 2023^m, 2021^n + 2023^m)$ in terms of m, n.

4. Let sequences $\{a_n\}$ and $\{b_n\}$ be defined by the relation
$$a_n + b_n\sqrt{2021} = (2022 + \sqrt{2021})^n \text{ for all } n \in \mathbb{N}$$
Find $\gcd(a_n, b_n)$ for all natural numbers n.

5. l, m, n are natural numbers such that
$$\frac{1}{n} - \frac{1}{m} = \frac{1}{l}$$
Prove that $\gcd(l, m, n) \cdot lmn$ and $\gcd(l, m, n) \cdot (m - n)$ are perfect squares.

6. Let p be an odd prime and a, b be relatively prime positive integers. Prove that
$$\gcd(a + b, \frac{a^p + b^p}{a + b}) = 1 \text{ or } p$$

7. A set S containing natural numbers is *good* if it satisfies

$$m, n \in S \implies \frac{m+n}{\gcd(m,n)} \in S$$

Find all non-empty *good* sets.

8. For natural numbers n, m. Prove that

$$\operatorname{lcm}(n,m) + \operatorname{lcm}(n+1, m+1) > \frac{2mn}{\sqrt{|n-m|}}$$

9. Find all pairs of natural numbers (a, b) such that

$$\frac{a^2+b}{b^2-a} \quad \text{and} \quad \frac{b^2+a}{a^2-b}$$

are both integers.

10. Find all triples (p, m, n) of natural numbers, where p is a prime and $p^m = n^5 + n^4 + 1$.

11. Find all triples of natural numbers (l, m, n) which satisfy

$$\left(1+\frac{1}{l}\right)\left(1+\frac{1}{m}\right)\left(1+\frac{1}{n}\right) = 3$$

12. Find the number of 6-digit numbers in base 6 divisible by $(111)_6$ which have all distinct digits.

13. For a natural number n, find $x, y \in \mathbb{Q} \setminus \mathbb{Z}$, such that $x^i - y^j \in \mathbb{Z}$ for all $i \in \{1, 2, \ldots, n\}$.

14. Find the smallest integer n such the following equation has a solution in $\mathbb{R}^n$

$$a_1^3 + a_2^3 + \cdots + a_n^3 = 4000^{4000}$$

15. Let $p_1 < p_2 < \cdots < p_n$ be the first n primes. Prove that the following expression will never be a non-zero integer for any choice of integers $a_1, a_2, \ldots, a_n$.

$$a_1\sqrt{p_1} + a_2\sqrt{p_2} + \cdots + a_n\sqrt{p_n}$$

Section II

1. For given integers m, n, recall that *Bezout's Identity* gives the existence of integers x, y such that

$$\gcd(m,n) = mx + ny$$

   (a) What can you say about the uniqueness of such pairs of integers (x, y)?

   (b) Write a *C++/Python* program which outputs a pair (x, y) satisfying the above identity for an input (m, n).

2. You are part of the cybersecurity team tasked with decoding the transmissions amongst a terrorist organization called *Sphinx*. Your team has successfully intercepted a few messages, which are of form (n, a, b), where n is a positive integer which may have upto 10^6 digits, and a, b are positive integers less than 10^6. Your team commander performed a power analysis on a terrorists computer and was able to figure out their cryptographic algorithm. But for him to able to decode the message, he needs you to find a way to cut the number n (base 10) into two parts n_1 and n_2 such that $a|n_1$ and $b|n_2$ (For example for $(97502821, 25, 91)$ we can choose $n_1 = 9750$ and $n_2 = 2821$). Write a *C++/Python* program that performs this operation quickly so that you can halt *Sphinx's* plans as fast as possible.