Tutorial 1

Last date of submission: 9th September 2021 (midnight)

1. For positive integers a and b, prove that if $a^3 \mid b^2$ then $a \mid b$.
2. For primes p and q prove that if $q \mid 2^p - 1$, then $p < q$.
3. Show that if $n > 1$ is an odd integer, then $\phi(2n) = \phi(n)$.
4. Find all integers a such that $a^2 + 2$ is divisible by $2a - 1$.
5. For integer $n > 0$ and $a > 1$, prove that

$$\gcd\left(\frac{a^n - 1}{a - 1}, a - 1\right) = \gcd(a - 1, n)$$

6. Prove that if p be a prime, then $\sqrt{p}$ is irrational.
7. Solve the congruence $42x \equiv 12 \pmod{90}$.
8. Find the number of solutions in ordered pairs of positive integers (x, y) of the equation $\frac{1}{x} + \frac{1}{y} = \frac{1}{n}$, where n is a positive integer.
9. Find the number of solutions in ordered pairs of positive integers (x, y) of the equation $\frac{1}{x} + \frac{1}{y} = \frac{1}{84}$.
10. Solve the following system of linear congruence equations,

    $x \equiv 3 \bmod 7$

    $x \equiv 11 \bmod 18$

    $x \equiv 5 \bmod 24$

11. Carmichael number is a composite number n which satisfies the congruence relation:

    $$a^{n-1} \equiv 1 \pmod{n} \text{ for all integers } a \text{ which are relatively prime to } n.$$

    Prove that n is Carmichael number iff $\lambda(n) \mid (n - 1)$.

12. Prove that for $n = \prod_{i=1}^{m} p_i$ where p_i, $i = 1 \ldots m$ are primes

    $$\lambda(n) = \min\{k_1 (p_1 - 1) : k_i (p_i - 1) = k_1 (p_1 - 1), i = 1, 2, \cdots, m\}$$

13. Prove that for any prime $p = 4k + 1$, $(2k)!$ is square root of -1 modulo p.

14. Decrypt the following ciphertext (assuming that it is encrypted using affine cipher):

    ZRCIPZAHOPWZWVMUCSPCZQCUUIMCUORWSRWUWVZCLLWMWNLCZAZRAUCORAI
    PCWVFAUUCUUWAVAHZRCGCYIVXEVWVZCLLWMWNLCZAILLAZRCPUZRCEUCHEL
    VCUUAHUESRQCUUIMCUCUFCSWILLYWVZWQCAHOIPWUANJWAEURAVZRCAZRCPR
    IVXZRCWPUALEZWAVQIYNCIQIZZCPAHMPCIZWQFAPZIVSCZAZRAUCHPAQORAQZR
    CGCYWUSAVSCILCX

15. Decrypt the following ciphertext (assuming that it is encrypted using simple substitution cipher):

BMJJADAJGCAGQZPAKZPIZEJAZLRAQQALSGZJSGKAGLZNAPQMLJGCAZLRAU
APXMLAQFMTJRALHMXGSBMJJADAJGCASAZBFAQTQKZLXSFGLDQZLRETGJR
QMTPBMLCGRALBASMCZBASFALAVBFZJJALDAQZLRQSPTDDJAQGLMTPCTST
PAGLQSAZRMCHTQSCMBTQQGLDMLSFAQSTRXZNAPQMLKTQSNZPSGBGNZS
AGLMSFAPZBSGUGSGAQZLRQMBGZJGQAZQKTBFZQNMQQGEJAZQZJJSFAQAS
FGLDQFAJNGLSFAMUAPZJJRAUAJMNKALSMCZNAPQML