NATIONAL INSTITUTE OF TECHNOLOGY CALICUT
Department of Computer Science and Engineering
CS4062D: Introduction to Information Security (IIS)
Assignment-1

DATE of issue: 18-01-2022 **Date of submission: 28-01-2022, 11:59 PM**

----

1. Find the $GCD(g)$ of the numbers 743 and 241, and find integers x and y to satisfy $743x + 241y = g$.
2. Given that $(a, 4) = 2$ and $(b, 4) = 2$, prove that $(a + b, 4) = 4$.
3. Prove that if n is odd, $n^2 - 1$ is divisible by 8.
4. Show that any positive integer n can be written as the product of a square number and a squarefree integer.
   (An integer d is squarefree if it's not divisible by any square number larger than 1)
5. Suppose that a a and b are relatively prime. Prove that ab and $a + b$ are relatively prime.
6. Prove that the square of any integer of the form $5k + 1$ is of the same form.
7. Prove that an integer is divisible by 3 if and only if the sum of its digits is divisible by 3. Prove that and integer is divisible by 9 if and only if the sum of its digits is divisible by 9.
8. Prove that any prime of the form $3k + 1$ is of the same form $6k + 1$.
9. Show that $n|(n - 1)!$ for all composite $n > 4$.
10. Prove that if p is a prime and $a^2 \equiv b^2\ (p)$, then $p|(a + b)$ or $p|(a - b)$.
11. Show that if $p \equiv 3\ (4)$, then $\left(\frac{p-1}{2}\right)! = \pm 1\ (p)$.
12. Determine the last three digits of the integer 37^{399997}.
13. Show that if p is a prime then $\binom{p}{k} \equiv 0\ (p)$ for $1 \leq k \leq p$.
14. If m and k are positive integers, prove that the number of positive integers $\leq mk$ that are prime to m is $k\phi(m)$.
15. Find the order of 2 modulo the Fermat number $F_5 = 2^{2^5} + 1$.