

Tutorial 9

1. Given a theorem: Let a and b be two integers in which atleast one is non-zero then there exists x and y such that $GCD(a, b) = ax + by$.

Prove that if $d = GCD(a, b)$ then $\frac{a}{d}$ and $\frac{b}{d}$ are relatively prime.

2. Prove the following:

(a) If $a \equiv b \pmod{m}$ then $ac \equiv bc \pmod{m}$

(b) If $a \equiv b \pmod{m}$ then $a^k \equiv b^k \pmod{m}$ for all $k \geq 1$

3. Find the GCD of the following using Euclidean Algorithm:

(a) (1475, 1200)

(b) (766, 1235)

4. Find the remainder when 3^{28} is divided by 5.

(Note: Use the properties of congruence relation)

5. Perform the following operations in Z_n :

(a) Add 7 to 14 in Z_{15} .

(b) Subtract 11 from 7 in Z_{13} .

(c) Multiply 123 by -10 in Z_{19} .

(Note: Operations in Z_n can be done in this way – $(a + b) \pmod{n} = c$. Subtraction and Multiplication can also be done in the similar way).