Computational Number Theory - Theory Assignment 1

Vishal Vijay Devadiga (CS21BTECH11061)

Question 1

Find an integer solution of $6x + 10y = 2$

Solution

Let $d = gcd(6, 10) = 2$.

$d \mid 6$ and $d \mid 10$. So, $d \mid 6x + 10y$. Also, $d \mid 2$.

By Bezout's Lemma, there exists $x_0, y_0 \in \mathbb{Z}$ such that $6x_0 + 10y_0 = 2$.

Using the Extended Euclidean Algorithm, we get:

$$6(x + y) + 4y = 2$$

$$6a + 4y = 2$$

where $a = x + y$.

$$2a + 4(a + y) = 2$$

$$2a + 4b = 2$$

where $b = a + y$.

A simple solution to this equation is $a = 1$ and $b = 0$. Backtracking, we get:

$$a = 1, b = 0$$

$$y = b - a = \boxed{-1}$$

$$x = a - y = \boxed{2}$$

Therefore, an integer solution to the given equation is $(x, y) = (2, -1)$.

Question 2

Find an integer solution of $6x + 10y + 15z = 1$

Solution

Let $d_1 = gcd(6, 10) = 2$

$d_1 \mid 6$ and $d_1 \mid 10$. So, $d_1 \mid 6x + 10y$.

By Bezout's Lemma, there exists $x_0, y_0 \in \mathbb{Z}$ such that $6x_0 + 10y_0 = 2w$.

Substituting $6x + 10y = 2w$ in the given equation, we get:

$$2w + 15z = 1$$

Let $d_2 = gcd(2, 15) = 1$

$d_2 \mid 2$ and $d_2 \mid 15$. So, $d_2 \mid 2w + 15z$.

By Bezout's Lemma, there exists $w_0, z_0 \in \mathbb{Z}$ such that $2w_0 + 15z_0 = 1$.

Using the Extended Euclidean Algorithm, we get:

$$2(w + 7z) + z = 1$$

$$2a + z = 1$$

where $a = w + 7z$.

A simple solution to this equation is $a = 0$ and $z = 1$.

Backtracking, we get:

$$a = 0, z = 1$$

$$w = a - 7z = \boxed{-7}$$

Substituting $w = -7$ in $6x + 10y = 2w$, we get:

$$6x + 10y = -14$$

Multiplying the solution obtained in Question 1 by -7, we get:

$$x = \boxed{-14}$$

$$y = \boxed{7}$$

Therefore, an integer solution to the given equation is $(x, y, z) = (-14, 7, 1)$.

Question 3

Show that if a, m, n are natural numbers with $a > 1$ then,

$$gcd(a^m - 1, a^n - 1) = a^{gcd(m,n)} - 1$$

Solution

Let $d = gcd(m, n)$. Then, $d \mid m$ and $d \mid n$.

To show that $a * d - 1$ is the greatest common divisor of $a^m - 1$ and $a^n - 1$, we need to show:-

1) $a^d - 1 \mid a^m - 1$
2) $a^d - 1 \mid a^n - 1$
3) For $\forall e \in \mathbb{Z}$, if $e \mid a^m - 1$ and $e \mid a^n - 1$, then $e \mid a^d - 1$

$$a^m - 1 = a^{dq} - 1$$

where $q = \dfrac{m}{d}$.

$$a^m - 1 = (a^d)^q - 1$$

$$a^m - 1 = (a^d - 1)(a^{d(q-1)} + a^{d(q-2)} + \cdots + a^d + 1)$$

Thus $a^d - 1 \mid a^m - 1$.

Similarly, $a^d - 1 \mid a^n - 1$.

Now, let $e \in \mathbb{Z}$ such that $e \mid a^m - 1$ and $e \mid a^n - 1$.

Let o be the order of a modulo e. Then, $o \mid m$ and $o \mid n$.

Since $d = gcd(m, n)$, $o \mid d$.

Thus, $a^d \equiv 1 \pmod{e}$.

$$a^d - 1 \equiv 0 \pmod{e}$$

Thus, $e \mid a^d - 1$.

Therefore, $a^d - 1$ is the greatest common divisor of $a^m - 1$ and $a^n - 1$.

Question 4

Describe all integer solutions of $2x + 3y + 5z = 0$

Solution

Let the value of x be fixed to be k. Then, we get:

$$3y + 5z = -2k$$

Let $d = gcd(3, 5) = 1$.

$d \mid 3$ and $d \mid 5$. So, $d \mid 3y + 5z$.

By Bezout's Lemma, there exists $y_0, z_0 \in \mathbb{Z}$ such that $3y_0 + 5z_0 = d$.

Using the Extended Euclidean Algorithm, we get:

$$3(y + z) + 2z = -2k$$

$$3a + 2z = -2k$$

where $a = y + z$.

$$2(z + a) + a = -2k$$

$$2b + a = -2k$$

where $b = z + a$.

A simple solution to this equation is $a = 0$ and $b = -k$.

Backtracking, we get:

$$a = 0, b = -k$$

$$z = b - a = -k$$

$$y = a - z = \boxed{k}$$

$$x = \boxed{k}$$

To find all integer solutions, we need to find all possible values of $3y + 5z = -2k$.

Let $y = k + 5t$ and $z = -k - 3t$ where $t \in \mathbb{Z}$.

Substituting these values in $3y + 5z = -2k$, we get:

$$3(k + 5t) + 5(-k - 3t) = -2k$$

Thus, all integer solutions of $2x + 3y + 5z = 0$ are $(x, y, z) = (k, k + 5t, -k - 3t)$ where $k, t \in \mathbb{Z}$.