Afsana Akter Mita
ID - IT21053

# Number Theory Theorems - Part 1 (Assignment)

## 1. Bazeout Theorem Proof and Example:

**Bezout's Theorem:** If a and b are positive integers, then there exist integers s and t such that $\gcd(a,b) = sa + tb$

→ If both a and b are zero, $\gcd(a,b) = 0$ and we can choose $s = 0$ and $t = 0$, so the theorem holds. If a or b is zero and then we can assome b is non-zero, which can be $\gcd(a,b) = \gcd(0,b) = |b|$, written as $sa + tb$ where $s = 0$ and $t = 1$

→ Apply the Euclidean algorithm to a anb b. The algorithm generates a sequence of remainders $r_0 = a, r_1 = b$ $r_2, r_3 \ldots$ where each remainder is obtained from the previous two:

$$r_0 = q_1 * r_1 + r_2$$
$$r_1 = q_2 * r_2 + r_3$$
$$\vdots$$
$$r(n-2) = q_n * r(n-1) + r(n)$$
$$r(n-1) = q_{n+1} * r(n) + 0$$

where $q_1, q_2 \cdots$ are integers and $r_n$ is the last non-zero remainder, which is gcd (a,b).

→ Finding s and t : Work backword from the last non-zero remainder, $r(n)$, which is gcd(a,b):

→ From the last equation, $r(n) = r(n-2) - qn * r(n-1)$.

→ Substitute $r(n-2)$ from the previous equation;

$r(n) = [r(n-3) - q(n-1) * r(n-2)] - qn * r(n-1)$

→ continue substituting until you express $r(n)$ as a linear combination of a and b.

→ The process of working backward guarantees that the resulting s and t are the smallest possible integers that satisfy the equation.

Example: Find an inverse of 101 modulo 4620.

⇒ First use the Euclidian algorithm to show that gcd (101, 4620) = 1

$42620 = 45 \cdot 101 + 75$
$101 = 1 \cdot 75 + 26$
$75 = 2 \cdot 26 + 23$
$26 = 1 \cdot 23 + 3$
$23 = 7 \cdot 3 + 2$
$3 = 1 \cdot 2 + 1$
$2 = 2 \cdot 1$

Since the last nonzero remainder is 1, $\gcd(101, 4260) = 1$

Bezout coefficients: $-35$ and $1601$.

Working Backwards:

$1 = 3 - 1 \cdot 2$
$1 = 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3$
$1 = -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23$
$1 = 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = 26 \cdot 26 - 9 \cdot 75$
$1 = 26 \cdot (101 - 1 \cdot 75) - 9 \cdot 75$
$= 26 \cdot 101 - 35 \cdot 75$
$1 = 26 \cdot 101 - 35 \cdot (42620 - 45 \cdot 101)$
$= -35 \cdot 42620 + 1601 \cdot 101$

1601 is an inverse of 101 modulo 42620.

## 2. Chinese Remainder Theorem - Proof.

Let $m_1, m_2, \ldots, m_k$ be pairwise coprime positive integers, and let $a_1, a_2, \ldots, a_k$ be any integers.

Then, the system of congruences:

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x = a_k \pmod{m_k}$$

has a unique solution modulo $m = m_1 \cdot m_2 \cdots m_k$

$\Rightarrow$ Let,

$$M = m_1 \cdot m_2 \cdot \dots \cdot m_k$$

For each $i$, define,

$$M_i = \frac{M}{m_i}$$

So, each $M_i$ is the product of all $m_j$ where $j \neq i$

Since $m_i$ and $M_i$ are coprime, there exists an integer $y_i$ such that,

$$M_i \cdot y_i \equiv 1 \pmod{m_i}$$

Define,

$$x = \sum_{i=1}^{k} a_i \cdot M_i \cdot y_i$$

This is the formula that gives a solution $x$.

We check that $x \equiv a_i \pmod{m_i}$ for each $i$.

For a fixed $i$, all terms in the sum except $a_i M_i y_i$ vanish modulo $m_i$ (because each $M_j \equiv 0 \mod m_i$ for $j \neq i$).

So, $x \equiv a_i \cdot M_i \cdot y_i \pmod{m_i}$

But, $M_i y_i \equiv 1 \mod m_i$

So, $x \equiv a_i \pmod{m_i}$

Thus, the solution satisfies all the given congruences.

If $x$ and $x'$ both satisfy the system, then,

$$x \equiv x' \pmod{m_i} \ \forall i$$

Since all $m_i$ are pairwise coprime, it follows that: $x \equiv x' \pmod{M}$

Therefore, the solution is unique modulo $M$.

(Proved).

## 3. Fermat's Little Theorem - Proof:

Let $p$ be a prime number and let $a$ be an integer not divisible by $p$ ($\gcd(a,p)=1$)

Then → $a^{p-1} \equiv 1 \pmod{p}$

⇒ Considers the set of integers:

$$S = \{1, 2, 3 \cdots\cdots p-1\}$$

Since $p$ is prime, all of these integers are co-prime to $p$.

Now, multiply each element of this set by $a$ (modulo $p$):

$a \cdot 1, a \cdot 2, a \cdot 3 \ldots\ldots a \cdot (p-1)$

call this new set $S'$.

Since gcd $(a, p) = 1$, multiplying by $a$ is a bijection in modular arithmetic.

So, the set $S'$ contains the same elements as $S$, just in a different order.

Thus,

$$a \cdot 1 \cdot a \cdot 2 \ldots\ldots a \cdot (p-1) \equiv 1 \cdot 2 \ldots\ldots (p-1) \pmod p$$

$$a^{p-1} \cdot (1 \cdot 2 \ldots\ldots (p-1)) \equiv (1 \cdot 2 \ldots (p-1)) \pmod p$$

Now, divide both sides by $(p-1)!$, which is allowed because it's not divisible by $p$.

$$a^{p-1} \equiv 1 \pmod p$$

Therefore, for any integer $a$ such that gcd $(a, p) = 1$, we have:

$$a^{p-1} \equiv 1 \pmod p$$

(Proved).

Example: $7^{222} \bmod 11$.

$\Rightarrow$ By Fermat's little theorem; we know that $7^{10} \equiv 1 \pmod{11}$ and so $(7^{10})^k \equiv 1 \pmod{11}$, for every positive integer $k$.

Therefore,

$$7^{222} = 7^{22 \cdot 10 + 2}$$
$$= (7^{10})^{22} 7^2$$
$$\equiv (1)^{22} \cdot 49$$
$$\equiv 5 \pmod{11}.$$

Hence, $7^{222} \bmod 11 = 5$.