Subject / Theme :

Date : / /

☐ Sat ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri

Abida Sultana

IT-21032

Assignment-03

Number theory theorem

(1) Question:- Bazeout theorem Proof and Example [inverse of 101 and mod 4620]

Answer:

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

Definition: If a and b are positive integers, then integers s and t such that $gcd(a,b) = sa+tb$ are called Bezout coefficients of a and b. The equation $gcd(a,b) = sa+tb$ is called Bezout's identity.

By Bezout's theorem, the gcd of integers a and b can be expressed in the form $sa+tb$ where s and t are integers. This is a linear combination with integer coefficients of a and b.

Subject / Theme :

Date : / /

☐ Sat ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri

Proof : Assume $\gcd(a,b) = 1$ and $a \mid bc$

. Since $\gcd(a,b)=1$, by Bezout's theorem there are integers s and t such that, $sa+tb=1$

Multiplying both sides of the equation by c, yields $sac+tbc=c$

we know that, $a \mid tbc$ and a divides $sac+tbc$

since $a \mid sac$ and $a \mid tbc$

we conclude $a \mid c$, since, $sac+tbc=c$.

Example : Find an inverse of 101 modulo 4620

Solution :- First use the Eucldian algorithm to show that $\gcd(101, 4620)=1$.

$4260 = 45 \times 101 + 75$

$101 = 1 \cdot 75 + 26$

$75 = 2 \cdot 26 + 23$

$26 = 1 \cdot 23 + 3$

$23 = 7 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1$

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

Working Backwards :

$1 = 3 - 1 \cdot 2$

$1 = 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3$

$1 = -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23$

$1 = 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = 26 \cdot 26 - 9 \cdot 75$

$1 = 26(101 - 1 \cdot 75) - 9 \cdot 75$

$= 26 \cdot 101 - 35 \cdot 75$

$1 = 26 \cdot 101 - 35 \cdot (4262 - 45 \cdot 101)$

$= -35 \cdot 42620 + 1601 \cdot 101$

Bezout co-efficients : -35 and 1601

1601 is an inverse of 101 modulo 4260.

Subject / Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐Wed ☐Thu ☐Fri

② Chinese Remainder Theorem - Proof:

Solve: The chinese remainder Theorem.

Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \ldots, a_n$ arbitrary integers.

Then the system

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

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

(That is, there is a solution x with $0 \leq x < m$ and all other solutions are congruent modulo m to this solution.)

proof: We'll show that a solution exists by describing a way to construct the solution, showing that the solution is unique modulo m is Exercise 30.

Scanned with CamScanner

Subject / Theme : Date : / /

☐ Sat ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri

To construct a solution first let $M_k = m/m_k$ for $k = 1, 2, \ldots, n$ and $m = m_1 m_2 \cdots m_n$.

Since $\gcd(m_k, M_k) = 1$, by Theorem 1, there is an integer y_k, an inverse of M_k modulo m_k, such that

$$M_k y_k \equiv 1 \pmod{m_k}.$$

From the sum,

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n.$$

Note that because $M_j \equiv 0 \pmod{m_k}$ whenever $j \neq k$, all terms except the kth term in this sum are congruent to 0 modulo m_k.

Because, $M_k y_k \equiv 1 \pmod{m_k}$, we see that $x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$, for $k = 1, 2, \ldots, n$.

Hence, x is a simultaneous solution to the n congruences,

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

Subject / Theme:

Date: / /
☐ Sat ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri

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

$7^{\wedge}222$ mod 11

Fermat's Little Theorem:

If p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$

Furthermore, for every integer a we have $a^p \equiv a \pmod{p}$

Fermat's Little theorem is useful in computing the remainders modulo p of large powers of integers.

Example:- Find 7^{222} mod 11

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. Therefor,

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

Hence, 7^{222} mod $11 = 5$