TOPIC NAME : DAY : TIME : DATE : / /

Shafinaj Jerin Asha

IT-21031

Assignment-03

Number theory theorem

Question: Bazeout Theorem Proof and Example [inverse of 101 and mod 4620]

Answer: Bezouts 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.

Proof :

Assume gcd $(a,b)=1$ and a/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, $a|tbc$ and a divides $sac+tbc$

Since $a|sac$ and $a|tbc$.

Example : Find an inverse of 101 modulo 4620

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

$4620 = 45\times101+75$

$101 = 1\cdot75+26$

$75 = 2\cdot26+23$

$26 = 1\cdot23+3$

$23 = 7\cdot3+2$

$3 = 1\cdot2+1$

$2 = 2\cdot1$

$1 = 3-1\cdot2$

$1 = 3-1\cdot(23-7\cdot3) = -1\cdot23+8\cdot3$

$1 = -1\cdot23+8\cdot(26-1\cdot23) = 8\cdot26-9\cdot23$

$1 = 8\cdot26-9\cdot(75-2\cdot26) = 26\cdot26-9\cdot75$

$1 = 26\cdot(101-1\cdot75)-9\cdot75$

$= 26\cdot101-35\cdot75$

$1 = 26\cdot101-35\cdot(4620-45\cdot101)$

TOPIC NAME : DAY : TIME : DATE : / /

$= -35 \cdot 4260 + 1601 \cdot 101$

Bezout co-efficients: -35 and 1601

1601 is an inverse of 101 modulo 4260

② Chinese Remainder Theorem - Proofs

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

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

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

that there is a solution x with $0 \leq x < m$

and all other solutions

TOPIC NAME : DAY TIME : DATE : / /

Proof: We'll show that a solution exists by describing a way to construct the solution showing that the solution is unique modullo m is Exercise 30

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

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

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 $k = 1, 2, \dots, n$

Hence, x is a simultaneous solution to the n congrurnces.

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

3. Formad's Little theorem Proof - Example

7^{1222} mod 11.

Formad'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 we have.

$a^p \equiv a \pmod{p}$ $\square$

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

Example: Find 7^{222} mod 11.

Fermat's little theorem, we know that

TOPIC NAME :

DAY :

TIME : DATE : / /

$7^{10} \equiv 1 \pmod{11}$ 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, $7^{222} \bmod 11 = 5$