2/11/22

Bezout's Theorem

Lemma:- If a, b and c are positive integers such that $\gcd(a,b)=1$ and $a|bc$ then $a|c$

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

$$\boxed{sa+tb=1}$$

- 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 $a|tbc$.
- we conclude $a|c$, since $sac+tbc=c$

$3 - 23 + 7 \cdot 3$
$8 \cdot 3$

Find an inverse of 101 modulo 4620.

Solution:-

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

$4620 = 45 \times 101 + 75$

$101 = 1 \times 75 + 26$

$75 = 2 \cdot 26 + 23$

$26 = 1 \cdot 23 + 3$

$23 = 7 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1$

$\gcd(101, 4260) = 1$

Bezout co-efficients:

-35 and 1601

Working Backwards

$1 = 3 - 1 \cdot 2$

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

$= -1 \cdot 23 + 8 \cdot 3$

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

$= 8 \cdot 26 - 9 \cdot 23$

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

$= -9 \cdot 75 + 26 \cdot 26$

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

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

$\therefore 1 = 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101)$

$= -35 \cdot 4620 + 1601 \cdot 101$

1601 is an inverse of 101 modulo 4620.

The chinese Remainder Theorem

Theorem:- Let $m_1, m_2, m_3 \cdots m_n$ be pairwise relatively prime positive integer greater than one and $a_1, a_2, \cdots a_n$ 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 $m = m_1 m_2 \cdots m_n$

Proof:-

To construct a solution first Let $M_k = m/m_k$ for $k = 1, 2, \cdots n$ and $m = m_1 m_2 \cdots m_n$.
Since $\gcd(m_k, M_k) = 1$; ~~by~~ there is an integer y_k an inverse of M_k modulo m_k such that.

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

Form the sum

$$x = a_1 M_1 M_1^{-1} + a_2 M_2 M^{-1} + \cdots + a_n M_n M_n^{-1}$$

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 $M_k M_k^{-1} \equiv 1 \pmod{m_k}$, we see that

$$x \equiv a_k M_k M_k^{-1} \equiv a_k \pmod{m_k}, \text{ for } k = 1, 2, \ldots n$$

Hence, x is a simultaneous solution to the n congruences

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$\vdots$$

$$x \equiv a_n \pmod{m_n}$$

CamScanner

Fermat's Little Theorem:-

proof :-

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 $7^{222} \bmod 11$

By Fermat's little theorem, we know that $7^{11-1} \equiv 1 \pmod{11}$

and $7^{10} \equiv 1 \pmod{11}$ and so,

CamScanner

$(7^{10})^k \equiv 1 \pmod{11}$, for every positive integer k. therefore,

$$7^{222} = 7^{22 \cdot 10 + 2}$$

$$\cancel{= (7^{10})^{22} \cdot 7^2 \equiv 1^{22} \pmod{11}}$$

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

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

CamScanner