

Q Question: Bazeat theorem proof and example
[inverse of 101 and mod 420]

Answer:

Bazaut'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 integers coefficients of a and b .

Proof: Answer $\gcd(a, b) = 1$ 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 $sa + tbc = c$

We know that, $a|b$ and $a|c$ divides $a|b+c$
since $a|b$ and $a|c$

We conclude $a|c$, since, $b+c = c$

Example: Find an inverse of 101 modulo 4260

Solution: First use the Euclidean algorithm to show that $\gcd(101, 4260) = 1$

$$4260 = 45 \times 101 + 75$$

$$101 = 1 \cdot 75 + 26$$

$$75 = 2 \cdot 26 + 23$$

$$26 = 1 \cdot 23 + 3$$

$$23 = 7 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

Working Backwards:

$$1 = 3 - 1 \cdot 2$$

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

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

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

$$1 = 26 \cdot 101 - 35 \cdot 75$$

$$1 = 26 \cdot 101 - 35 \cdot (4260 - 45 \cdot 101) = -35 \cdot 4260 + 1601 \cdot 101$$

Bezout coefficients:
-35 and 1601

1601 is an inverse of 101 modulo 4260.

② Chinese Remainder theorem proof

Solve: The Chinese remainder theorem Let m_1, m_2, \dots, m_n the pairwise relatively prime positive integers greater than one and a_1, a_2, \dots, 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 $m = m_1 m_2 \dots m_n$

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.

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

That

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

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 $M_j = 0 \pmod{m_k}$ whenever $j \neq k$, all terms except the k th term in this sum are congruent to 0 modulo m_k .

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

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

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

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

\vdots

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

3. Fermat's Little theorem Proof - example
 $7^{1222} \bmod 11$.

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 integer

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

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

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