Number Theory

(1) Bazeout, theorem proof and Example:

Inverse of 101 mod 46020.

Solⁿ:

Bezout's identity states that if a and b are integers with a greatest common divisor $d = \gcd(a, b)$, then there exist integers x and y ~~sh~~ such that, $ax + by = d$.

Proof :

Consider the set S of all linear combinati of a and b that result in a positive integer:

$$S = \{ma + nb \mid m, n \in \mathbb{Z},\ ma+nb > 0\}$$

Since at least one of d or b is non-zero, the set S is not empty. For, example, if $a \neq 0$, then $|a| = (\pm 1) a + 0b$ will be in S

Let's call this smallest element d.
Because d is in the S, there exist integers x and y such that, ~~ax+by+c~~
$ax + by = d$.

Now our goal is to show that d is indeed the ~~griearst~~ test common divisor of a and b; we need to show two things:

1. d is a common divisor of a and b :

Suppose d doesn't divided a. Then by the Divisor Algorithm, we can write $a = qd + r$, where q is the quotient and r is the eminder with $0 < r < d$.

Substituting $d = ax + by$, into this equation we get,

$$r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy).$$ r' is positive

~~ke~~ linear combination of a and smaller than d, which is a contradiction.

2. Any common divisor of a and b also divides d:

Let, c be any common divisor of a and b. This means that there exist integers k and such that $a = kc$ and $b = 1c$. Substituting these into the equation $d = ax + by$, we get,

$$d = (kc)x + (1c)y = c(kx + y)$$

Since, $kx+ky$ is an integer, this equation shows that c divides d,

Therefore, $d = \gcd(a, b)$

This completes the proof of Bezout's identity

Find the inverse of 101 mod 4620.

We want to find x such that,

$$101\,\cancel{m}x \equiv 1 \pmod{4620}$$

This means we need to solve: $101x + 4620y = 1$

Using Bezout's theorem,

Step1: Apply the euclidean Algorithm, we divide ~~utt~~ until the remainder is 0:

$$4620 = 45 \times 101 + 75 \quad \text{—— (1)}$$

$$101 = 1 \times 75 + 26 \quad \text{—— (2)}$$

$$75 = 1 \times 26 + 23 \quad \text{—— (3)}$$

$$26 = 1 \times 23 + 3 \quad \text{—— (4)}$$

$$23 = 7 \times 3 + 2 \quad \text{—— (5)}$$

$$3 = 1 \times 2 + 1 \quad \text{—— (6)}$$

$$2 = 2 \times 1 + 0 \quad \text{—— Done}$$

So, $\gcd(101, 4620) = 1$, So, inverse exists.

Setp2: Back - substitute to express 1 as a combination of 101 and 4620

from step (6): $1 = 3 - 1 \cdot 2$

from step (5): $2\cancel{0} = 23 - 7 \cdot 3$

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

from step (4): $3 = 26 - 1 \cdot 23$

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

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

from step (3):

$23 = 75 - 2 \cdot 26$

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

$= 8 \cdot 26 - 9 \cdot 75 + 18 \cdot 26$

$= (8 + 18) \cdot 26 - 9 \cdot 75$

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

from step (2):

$26 = 101 - 1 \cdot 75$

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

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

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

From step (1): $75 = 4620 - 45 \cdot 101$

$$1 = 26 \cdot 101 - 35(4620 - 45 \cdot 101)$$
$$= 26 \cdot 101 \cdot 35 \cdot 4620 + 15 \cdot 75 \cdot 101$$
$$= (26 + 15 \cdot 75) \cdot 101 - 35 \cdot 4620$$
$$= 1601 \cdot 101 - 35 \cdot 4620$$

final result: $1 = 1601 \cdot 101 - 35 \cdot 4620$

So, the inverse of 101 mod 4620 is

$$101^{-1} \equiv 1601 \pmod{4620}$$

Chinese Remainder Theorem (CRT):-

Statement:

Let, $n_1, n_2, \ldots n_k$ be pairwise coprime. integer and $a_1, a_2 \ldots a_k \in \mathbb{Z}$. Then the system,

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\vdots$$
$$x \equiv a_k \pmod{n_k}$$

Proof Sketch:

Let, $N = n_1 n_2 \cdots n_k$, for each i, define:

$$N_i = \frac{N}{n_i}$$, and find M_i such that

$$N_i M_i \equiv 1 \pmod{n_i}$$

Then, define the solution:

$$x = \sum_{i=1}^{k} a_i M_i N_i \pmod N$$

Each term $a_i N_i M_i \equiv a_i \pmod{n_i}$ and $\equiv 0 \pmod{n_j}$ for, $j \neq i$.

Farmat's Little Theorem:

If p is a prime number and $a \not\equiv 0 \pmod p$

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

Proof:

Let, $a \in \mathbb{Z}$, $a \not\equiv 0 \pmod{P}$, The set $\{1, 2, \ldots P-1\}$ forms a multiplicative group modulo P

Then, multiplication by a permutes this set: $a_1, a_2, \ldots\ldots a(P-1)$

$$a^{P-1} \cdot (P-1)! \equiv (P-1)! \pmod{P}$$

$$\Rightarrow a^{P-1} \equiv 1 \pmod{P}$$

Example: Compute, $7^{222} \bmod 11$

use fermat's little theorem,

$7^{10} \equiv 1 \bmod 11$ (since 11 is prime)

Now,

$$222 = 10 \cdot 22 + 2$$

$$\Rightarrow 7^{222} = (7^{10})^{2} \cdot 7^{2}$$

$$\Rightarrow 7^{222} = 1^{22} \cdot 7^{2} = 49 \bmod 11$$

$$= 49 - 4 \cdot 11$$

$$= 49 - 44 = 5.$$