Number Theory Theorems-Part 1

1. Bazeout Theorem Proof and Example: Inverse of 101 mod 4620.

goln:

Bézout's Identity states that if a and b are integers with a greatest common divisor d = gcd(ab), then there exist integers α and y such that: $a\alpha + by = d$

Back substitution:

find a stick that 100 = 1 mod 3

Proof:

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

S={ma+nb|m,n EZ, ma+nb>0}

Since at least one of a or b is mon-zero,

the set g is not empty. For example, if a to,

then a = (+1) at Objuilt be in g.

By the Well-Ordering Principle, since g is a

By the Well-Ordering Principle, integers, it must have a

mon-empty set of positive integers, it must have a

smallest positive integer element. Let's call this

smollest element d. Because dis in 8, there exist integers a and y such that:

Now, our goal is to show that this do is indeed the greatest dominon divisor of a and b. we need to show two things:

1. dais a common divisor of a and b: Suppose do does not divide a. Then by the Division Algorithm, we can write a = qd+r, where q is the quotient and r is the reminder, with 0< r<d. Substituting d = ax+ by into this equation, we get:

This shows that r'is also a linear combination of a and b. Since OKPKd, I is a positive integer that is smaller than the smallest positive integer ins, which is d. This is a contradiction. Therefore our initial assumption that Id does not divide a

must be false. Thus, d'adivides ans les lons Similarly, we can show that I divides b. Suppose book d'adoesnot- divide b. Then b= 9'd+r', where 0< r/d. Substituting d= ax + by, we get: r'= b-q'd = b-q'(ax+by) = a(-q'x)+b(1-q'y) Again, r'is positive linear combination of a and smaller than do, which is a contradiction, Therefore, d'imust divide bos 300 motionella Since dédivides both a and bit is a common Substituting d = act by debnation to attacking net: (12) Any common divisor of a and b also divides & notatione beniany common divisor of a and b. This means that there exist integers K and I such that was Ket and b=10. Substituting these into nothe equation d=ax+by, we get:

d=(ke)x+(10)y= o(kx+ty) lolling and

since Kathy is an integer, this equation shows that a divides d.

Since d is a common divisor of a and b, and any other common divisor a also dévides d, d must be the greatest common divisor of a and

Therefore, d=gcd (a,b) (0231,101) 100,08

This completes the proof of Bézout's Identity.

Find the inverse of 101 mod 4620

we want to find or such that:

1010 = 1 (mod 4626)

This means we need to solve: (a) 9012 more

6.5-1-6-8=(6-1-65) 1 101x+46204=1

: (1) elate (10)

Using Bezout Theorem

Step1: Apply the Euclidean Algorithm

we divide until the remainder is 0:

4620 = 48x 101+78 ->1

```
Since Kathy is (2) (2) $ 400 x 10 10 20 1000 some
     76 = 1×26+23 -> (3) b sobivib o torto
Some 26 = 1x23+3 roctvib > (4) moro o ai b sonie
So, ged (101, 4620) = 1; so inverse exists 300
 Step 2: Back-substitute to express 1 as a combination
   of 101 and 9620 som 101 to sensini ent brit
              we want to find or such that:
    From step(G): 1=3-1.2
    From Step (5)=: 2=23-7.3000 200 2000 2001
       1= 100001 + 1= 3-1(23-7.3) = 8.3-1.23
    From step (4): 3 = 28 - 1.23 and two sed Briel
             mid large 4 8 (26-1.23) - 1.23 = 8:26-9.23
          eve divide contil the remander is o:
              4620 = 48x 101+78 --> 1
```

```
From Step (3): 23 = 75-2.26 ( asbring) sesaids.
  1=8.26-9(76-2.26) = 8.26-9.76+18.26 = (8+18)-26-97
emporal saniago seiss # (8+18).26-9:75, 10 13!
        : moters of = 26.26, 9.76 ... no box
  From step(2): 26= 101-1.75
  1=2c(101-1.76)-9.76=26.101-26.76-9.76
       (x0 bom) x10 = x = 26-101-(26+9).75
  = 26.101 - 35.75
  From step (1): 76=4620-45.101
  1=20.101-36 (4620-46.101) = 26.101-35.4620+1575.101
                         =(26+1675).101-35.4620
  toot down : 1 bail born = 1,601.101 - 35.4620
                1=1601.101-36.4620
   final result:
  Softher inverse of 101 mod 46200 ist.
              101-1= 1601 (mod 4620)
(in barr) 0 = bar (in born) in = imivip most about Answer: 1601
                                 i te i noi
```

```
2-Chinese Remainder Theorem (CRT) - Proof
     Glatement:
     Let n1, n2,...nx be pairwise coprime integers
     and as, az. . ax & Z. Then the system:
                      ar (mod nr)
     11-8-01-22-101-36=01.6-(mod m2)
      31. (0125)-101-25 = x= ak (mod nk)
     hasa unique, solution modulo. N= m1m2...mk
from step (4): 75=4620-45. "GP-023P=37 : (4) 93ts most
101. Joseph Sketch: 20 = (101. 8 For eacher, define:
    05211-08 Ne - No and find Mi such that
     1 = 1601.101 (inspound) T = ! WIN
                                    Final result;
     Then, define the solution:
            (000) Dome) 2= 2 a; NiMi (mod 4000)
     Each term ainimi z ai (mod ni) and = 0 (mod nj)
     for j = i
```

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

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 \(\int Z\), a\(\pi \) (mod P). The set \(\cap 1\), 2, ..., P-1\(\cap 1\) forms

a multiplicative group modulo P.

Then multiplication by a permutes this set:

\[
\text{a.1, a.2, ... a.(P-1)}
\]

All values are distinct modulo P. So the product of the original and the permuted set are congruent modulo P:

 $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p} \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

(After concelling (P-1)!, which is nonzero mod P)

Example: Computer 7222 mod 11 1 bom of strue Theorem: imprime) use fermat's little Theorem: $222 \pm 10.22 \pm 2$ $\Rightarrow 7^{222} = (70)^{22} = 2$ $\Rightarrow 10 + 22 = 2$ $\Rightarrow 7^{222} = 12272 = 49 \text{ mod } 11$ $\Rightarrow 7 = 1 \cdot 7 = 49 - 4.11$ Answer: $7 = 6 \pmod{11}$:9 : 9 Al. (1 form paszuou si yoyin, i(r-d) bugiseza mobil)