```
Judin Kim HW.
0
    (a)
       633=5(153)+21
      153=7(21)+6
       21=3(6)+3
        6-2(3) (3)
        GC0=3 (2) 07 -17 -1
                   (01047 - (5700))
        52=3(15)+7 -> 7=52=3(415)
    b)
        15=2(h)+1
         1= 7(1)
         GC0=1
                 X= (a) int ited
        1= 15-2(1)
        3= 3615)-667) x pp /m001 =0
        3=3(15)-6(52-3(15))
        3=3(15)-6(52)+18(15)
         3=-6 (52)+21(15)
           a=-6 | x bom 81 =
           b=21/12/m 3 =
         5a+23=6mod 499 499=99(5)+4
                         5 = (1)(4)+1
          5a= -17 mod 499
          5a= 482 mad 499 4=(4)(1)
          a=5-1 (482) mod 479 gcel,
           X = 5-11 = 18)
       gcd (499,5)=1 gcd (4,1)=1
       acd (5,4) = 1
```

S S

3

を

3

7

₹ F

7

3

3

3

D

O

Ø

(G)

4

\*

Justin 19m HW, 5x+499y=1 1= 5-(1)(4) 4= 499-99(5) 1=5-(499)-99(5) 1= 5-499+99 (5) 1=(100)(5)-4901 63=3(R)-1 - 1=5001=X)-[= Q(n)+1 X= 100 med 499 a= 100 mod 499 x 452 mod 499 - 48200 mod 499 a= 296 mod 499 9a = -78 mod 8/ 3-=1 b) 90= 3 mod 8 1 5 = d (2100 = a= 9-1 (3 mod 81) gcd(81,9)=97/x

b-Ba = 4 mod 37 - do+ 15 /01 600 -36+39a=12 mod 37 1000 = 16 1- 30a +3b = 0 mod 37 Clark = - 40 69a = = 12 mod 30 69a= 25 mod 37 a= 69-1(25 med 37) (( (1) 16) Ged (69,37)=1 Gred (37,32)=1(E) SI = (E) Gcd (32,5)=1 (1)=6 Gcd (\$,2)=1 Gecel (2/1)=51-18=) 69 = (1) (32) + 32 - 32 = 69 - (1) 37 37=(1) 32+ 5 5= 37-(1)(32) 32= 6(5)+2 = 32-6(5) 5=20)+1/08pm SS =N 2 = 2(1) \ (Elon 5) =0 1=5-2(2) (=75(69)+28(39) 1=5-2(32-6(5)) a=-15(28)hod 771=5-2(32)+12(5) -32 Nd 37 1= \$-2(69-31)+13(37-32) 1= 1- 2(61) +2(31) +13(31)+13(50) 1-11-11-2(69)+157(37)+13(69-37) 1= (1) -2(37)

960 nd 31+76=0nd 371-18-d 36=-960 nd 29 har C1= 2PE+dB-3b= 2 rd 37) 100 0 = 22+006 1 b= 3'(2) mod 57 = 000 69a= 25nod 30 - 9d (37 3) = of Nin 25) 1593 = -0 gd (3,1)= 1 4 100 - 2 11. 1=(06=)-120mod37 J=3(1) -- 1-(25) ND (= 37-12 (3) () los (E(2(2) mil 5)) = -24 mil 3) = 0) (55)(1) - 15 = 3 = 313 Rod(31) = 15 (2)3 - 50 = 6 = 95 + (2)3 = 50 0 = 32 mod(31) + (9)5 = 3 (9)5 = 5 (9)5 = 5 (9)5 = 51= 5-2(2) (= +5(69)+28(70) 1=5-2(32-6(5)) a= -15(28) hod ) 1=5-2(32)+12(5) -32h377 (5-12)=13(37-32) 1= 4-2(11)+3(m)+13(12) (OC-12) E1=(OCTB)+(M)0 - A >1

3a, - gcd(a,b) = gcd(bia) 6kc. of 0) Commutative properly of GCD d-1) - god (b,a) = god (a, blooda) ora 109 cd (a,b) due to substitutions - Thus of M is equen thanks g col (a,b)=1 ( orb/conthey are relatively toppome, solings 9 = gcd(a, b) = gcd(a, b) = 1 5 0d a, b' mustable relatively principality (on) b) - It all there exists some did Z such That 5= ade c= 0 = d@D ... - If ble there exists somed of & Busines ( )? 4ho49m6f=010 If gcd(a, b), tab + by= DEFor some Ky G Z whom i -d(ax+by)=d(1)d(A) istyrngeneture ados bdy = rdbon (1-1) = 101 Not invertible. (=b=C sldifiguri & down ck+b.dy=d sldifiguri & down - down bfx+bdy=d(-) @'d) @(des) b(fx+dy)=d c= adc=lorab(frotdy) das) dess) ... ab/ C = nborn 1 =

40) (a 06) (600) (b 00) (d,0) (d,0) = ((a-b), t(b+a)) modn = 0 modon = 10p = ( A) /2) = € Thus (a0b) € (bea) = 0 6) 19 Assume a⊗b=0-30870 1 à≠0 because regating sps g statement requires negating que (proof by contradiction). - If bto 1 aton then abot 0 - This contradicts our true assumption b) - It all there east , 0= d&o to- (d -.. a8b=0-9 0=0-0-6=0. Lot 5a) conference apple of a Dbs sont old 7I-20 1 - 0 13 hotimentible and 2(H/h-2)= (2+ h-2) mody = not invertible Countereganple: a0b(1) to = (pd +x a) to 101= (1-1) modin = 50 mod n Not muentible. ass is invertible asb = asb) modin (aob) ⊗ (6-10 a-1) 10= phd+x+d Gob (abb x bol x à) modinho =)

