31.1-6 PI(12) - PI k! (P-K)! PIP! We can use unique factorization for both P! and R! (P-K)! We already levan P! is a multiple of P. It we show [L] (P-K)! is not a multiple of P, we can be sure that in unique unttiplication form, p will not be canceled out and P! is [L! (P-K)! and integer. Because K & P and P-12 <P. and P is prime. the Minigee factorization from of K! (p-K)! will have p° and where thre P! is a K! (P-K)!

31-1-7 alb => b= Ra let x rod 5 = r X= 95 +r 1) for some quotient q 9=[X/b] Pat d= ka into () X= 9ka +r 9ka is a multiple of a so X mod a = r = x mod b So Kmoda = Xmodb r 2a =) (x mod b) mod a = x mod a X = Ymod b => X-4 = 9b 9 = LY/b) b = Kc X-Y= 9ka => a/ X-Y =) X = Y mod a X = Y mod a if Y = Y mod b

Unitée factorization will be a good approuch. First we write B form 3 = P. P. .... Then we do the above ofoation conssively on each Pn until there is only I Proposition all the randoming p Connot de further feuberized. In this recursion, there will be h! Cases and running time would be O(h!)

31.2-3 Branse gcd (ain) divides a mod n, 9 cd Carr) divides kn gcd (an) dividues a+ kn By Gorollary 31.3 = ged (a,n) divides ged (a+14n,n) Also because gcot(an) | a + kn gcd (a,n) = gcd (a+kn,h)

31·2-4 En

Enclid (a,b):

if b > a: a, b = b, a

While b 70:

q= a/b += a %b (% is mod)

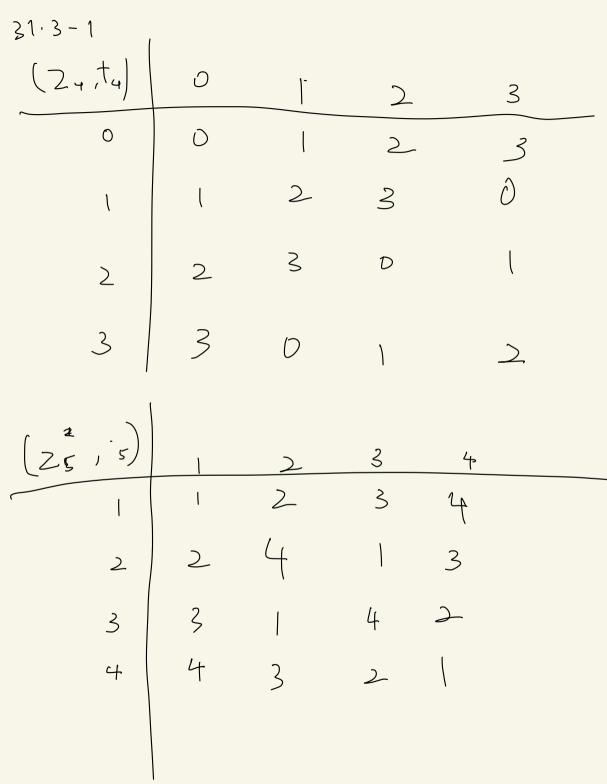
return b if r==0

a, b = b, r

31.2-6 According to Theorem 31,11 gcd (FranFr) = gcd (Fr, Fry) And extended Euclid retard d, X, y where d= 9cd(Fk, Fky) = ax+by d is there fore 1. 10 Fr - by Fr - 1

So  $\alpha = (-1) F_{k-3}$   $b = (-1)^{k-2} F_{k-3}$   $b = (-1)^{k-1} F_{k-2}$ result of extended  $F_{v}$  clid is;

 $\left(\begin{array}{c} \left(\begin{array}{c} \left(-1\right)^{K-2} \\ F_{K-3} \end{array}\right) \left(\begin{array}{c} \left(-1\right)^{K-1} \\ F_{K-2} \end{array}\right)$ 



To Prove they we isomorphic, we need that  $a+b \equiv c \mod it$  and only if  $a(a) \cdot a(b) \equiv d(c) \mod 5$  let a(c) = xy

31,3-2 the number of subgroup is the number of divisor. 9 has 3 divisor, 1, 3,9 Subgroup by I and 9 are just the trivial Sub group {0} 3 and {0,1.....9}=29 Subgroup generaled by sis & 0,3,63 For 213, Beencue Bi Prine, we am use 12 for it. divider of 12 one { 1,2,3,4,6,123 So 6 subgrups for 2" 20) = { a = a mod 13: K713 <1) = {13,93 

and inversity.

Closure; Because a Ob Es' for all a, b Es' are in the subset, It is closed.

Identity; suppose there is a Es', Because

it is closed there must be a = a9

P (-9)

a a = 1. So It has 2 destity.

Associativity: Be ase S is associative, For the same binary opertution, S' is associative for . Inversity, As said above, there is a =1

there is an inverse of a

theorem 31.14 proved

51,3-24 of Pe = per(CP1)