Propeties of integer's

Koneti Jagadish(07CS1003

Theorem 1) If n and m are integers and $n > 0$ we can write m=qn+r for integer's q and r with $0 <= r < n$ moreover there is just one way to do this.

eaxample 1) if n is 3 and m is 16 ,then 16=5*3+1 so q is 5 and r is 1

Theorem 2)Let a,b and c be integers
(a)if a—b and a—c then a—(b+c)
(b)if a—b and a—c where $b > c$ then a—(b-c)
(c)if a—b or a—c then a—bc
(d)if a—b and b—c then a—c

proof

(a)if a—b and a—c then b=k1a and c=k2a for integers k1 and k2. so b+c=(k1+k2)a and a—(b+c)
(b)if a—b and a—c then b=k1a and c=k2a for integers k1 and k2. so b+c=(k1-k2)a and a—(b-c) for not getting negative sign $b > c$
(c)we have b=k1a or c=k2a then either bc=k1ac or bc=k2ab ,so in either case bc is a multiple of a and a—bc
(d)if a—b and b—c we have b=k1a and c=k2b ,so c=k2b=k2(k1a)=(k1k2)a and hence a—c

Theorem 3) Every positive integer $n > 1$ can be written uniquely as

Greatest common Divisior

if a,b and k are in Z+, and k—a and k—b we say that k is a common divisor of a and b.if d is the largest such k,d is called the greatest common divisor or GCD of a and b ,and we write d=GCD(a,b).

Theorem 4) if d is GCD(a,b),then

(a) d=sa+tb for some integers s and t (these are not necessarily positive)
(b) if c is any other common divisor of a and b then c—d

Let x be the smallest positive integer that can be written as sa+tb for some integers s and t and let c be a common divisor of a and b since c—a and c—b it follows from theprem 2 that c—x so $c <= x$ if we can show that x is common divisior of a and b it will then be the greatest comon divisior of a and b and both by theorem 1 ,a=qx+r with $0 <= r < x$ solving for r, we have

$$r = a - qx = a - q(sa + tb) = a - qsa - qtb = (1 - qs)a + (-qt)b$$

if r is not zero , then since $r < x$ and r is the sum of multiple a and amultiple of b we will have a contridiction tothe fact that x is smallest positive number that is sum of multiple of a and b thus r must be 0 and x—a in the same way we can show that x—b .hence proved

Euclidean algorithm

divide b by r1: b=k2r1+r2 0 $<= r2 < r1$
divide r1 by r2:r1=k3r2+r3 0 $<= r3 < r2$

divide r(n-1) by rn: $r(n-1) = kn + 1rn + rn + 1$ 0 $<= r(n+1) < rn$

we show that rn=GCD(a,b).we saw that

GCD(a,b)+GCD (b,r1) repeating this argument with b and r1 we see that GCD (b,r1)=GCD(r1,r2) continuing GCD(a,b)=GCD(b,r1)=.....=GCD(r(n-1),rn).

since r(n-1)=K(n+1)rn,hence rn=GCD(a,b)

Theorem 5)

if a and b are in Z+,$b > a$,then GCD(a,b)=GCD(b,b(+(or)-)a)

proof if c divides a and b ,it divides b(+(or)-)a by theorem 2 since a=b-(b-a)=-b+(b+a).we see also by theorem 2 that a common divisor of b and b(+(or)-)a also divides a and b since a and b have the same common divisor as b abd b(+(or)-)a they must have the same GCD.