THE GREATEST COMMON DIVISOR gcd(N,M)

An important quantity associated with the solution of Diophantine equations and number theory in general is the greatest common divisor gcd(N,M) of two integers N and M. It is also referred to in the literature as the greatest common factor or the greatest common denominator and represents essentially the largest integer which divides exactly into both N and M. For example gcd(256,96)=32. There are several different ways available for calculating the gcd(N,M). These include a simple number factoring procedure involving prime number products, the Euclidan algorithm , and finally calling up built-in computer routines present in many PCs. Let us look at each of these approaches in more detail.

We begin with the most intuitively obvious approach of factoring the two numbers N and M into their integer prime number product forms and then taking the product of those primes the two numbers have in common. This will be the gcd. Take the case of gcd(251986,230748). Here we factor things into the product -

$$251986=2\cdot 7\cdot 41\cdot 439 \quad \text{and} \quad 230748=2^2\cdot 3\cdot 7\cdot 41\cdot 67$$

and note that $2\cdot 7\cdot 41=574$ is a common factor. Hence gcd(251986,230748)=574.

Next we look at the Euclidian Algorithm. It works as follows. Take , as an example, the integers N=764 and M=352 and divide N by M to find 2 plus a remainder of 60. Next divide the remainder 60 into 352 yielding 5 plus a remainder of 52. Then divide 52 into 60 to get 1 plus a remainder of 8. Next divide 8 into 52 to get 6 plus a remainder of 4. Finally dividing 4 into 8 we have 2 without remainder. Thus the gcd(764,352)=4. Symbolically we have-

764/352→ 352/60→60/52→52/8→8/4 since 8/4=2 with no remainder , hence-

gcd(764,352)=4

Note that we can represent the ratio of N/M as a finite continued fraction. For the last case one can write-

$$764/352 = 2 + \cfrac{1}{5+\cfrac{1}{1+\cfrac{1}{6+\frac{1}{2}}}}$$

which is really just another way to write out the Euclidian Algorithm.

As a third approach for finding gcds one can use electronic computers with an appropriate built-in mathematics program. For example, I use MAPLE to find almost instantaneously the gcds of two large integers N and M. The computer operation for one particular case reads-

gcd(13471928834584,10982314867728);

and produces a gcd(N,M)=6 in a split second. Carrying out this operation by hand would take considerably longer.

One of the more important uses of the gcd arises in connection with solving the linear Diophantine equation-

$$ax+by=c$$

where a ,b, and c are integers and one looks for solutions where x and y are also integers. Consider first the special case of a=7 , b=4 and c=1. Here we have gcd(4,7)=1=7x+4y. We see at once by inspection that x=3 produces y=-5. Likewise for x=7 yields y=-12 and x=-1 produces y=2. One notices that the integer spacing between the xs is 4 and between the ys 7. That is this Diophantine equation is satisfied by the solution pairs-

$$[x,y]=[3\mathrm{mod}4,-(5\mathrm{mod}7)]$$

Notice that the mod numbers just correspond to the a and b in gcd(a,b). The integer solution pairs all lie along the same straight line in the x-y plane. Another of these pairs would be [43,-75].

When c differs from 1 in the above linear Diophantine equation, one first converts to the new variables X=x/c and Y=y/c to get the equation-

$$aX+bY=1=\gcd(a,b) \text{ for all a and b whose gcd equals unity.}$$

Consider a=12 , b=-5 and c=4. This implies gcd(12,5)=1=12X-5Y. One obvious solution is X=3 and Y=7 and the other integer pairs follow from {X,Y]=[3mod5,7mod12]. So that solution pairs include {X,Y]=[-2,-5],[8,19],[13,31], etc. . It follows that-

$$12x-5y=4 \text{ has the integer solution pairs } [x,y]=[4(3\mathrm{mod}5),4(7\mathrm{mod}12)]$$

which includes the pairs [52,124] and [-48,-116].

We can also use the gcd operation to factor certain semi-primes . A semi-prime is a number N=pq composed of the product of two prime numbers such as p=11 and q=23 where N=253. One way to factor such a number is to first introduce the new numbers n=(q+p)/2 and

m=(q-p)/2. This allows one to write n^2-N=m^2 . If one chooses the right number for n >sqrt(N) it is sometimes possible to have m^2 be a perfect square. Under that condition the factors p and q can be determined by performing the operation-

gcd(n-m,N)=p or q

In the above example sqrt(253)=15.90.. so we choose for n some integer above this value. Trying n=17 we find m=sqrt(289-253)=6. Thus gcd((17-6),253)=gcd(11,253)=11=p. The other factor follows from N/p = 253/11=23=q.

May 2012