ON THE EUCLIDEAN ALGORITHM AND ITS INVERSE

If one takes two numbers such as $24=2^3 \cdot 3$ and $36=2^2 \cdot 3^2$ one notes the overlap of $2^2 \cdot 3=12$. This overlap is called the greatest common divisor or gcd for short. For this case we can write-

\[ \text{gcd}(36,24)=12 \]

There are several additional ways we can find this gcd. One of the simplest, but sometimes long, procedures involves factoring out the smaller common terms. Thus for the above case we have-

\[ (36,24) \rightarrow (9,6) \rightarrow (3,2) \text{ so } 36/3=12 \text{ the gcd} \]

A third method for finding the gcd of two positive integers is via the Euclid Algorithm. It works as follows-

\[
\begin{align*}
36 &= 24(1)+12 \\
24 &= 12(2)+0
\end{align*}
\]

with the gcd given by the last term of the equation preceding the equation ending in a zero. This algorithm will work for any positive integer pair. Let us demonstrate things for $\text{gcd}(176,62)$. Written out by hand, we have-

\[
\begin{align*}
176 &= 62(2)+52 \\
62 &= 52(1)+10 \\
52 &= 10(5)+2 \\
10 &= 2(5)+0
\end{align*}
\]

So 2 is the gcd and we can write $\text{gcd}(176,62)=2$. Most advanced computer math programs have the gcd for any integer pair programmed. Thus, for example,

\[
\text{gcd}(278356,578912)=4 \quad \text{and} \quad \text{gcd}(47924106633,36792187469)=1
\]

There also exists an Extended (Inverse) Euclidean Algorithm. This works as follows using the special case of gcd$(589,104)=1$ -
An inverse form is possible for any combination of positive integers $N$ and $M$. The extended Euclidean Algorithm allows one to write:

$$1 = M(a) + N(b)$$

with the numbers $a$ and $b$ determined via this extended approach. The gcd$(M,N)$ need not necessarily be one for this inverse to exist.

An important side calculation using the inverse (or extended) Euclidean approach involves finding the appropriate positive integer corresponding to the fraction $1/N$ when we apply mod$(M)$. This inversion works only as long as gcd$(N,M)=1$. Let us demonstrate for gcd$(31,13)=1$. Here we are looking for the equivalent of $13^{-1}$. Working out the details we get the following:

So here $13^{-1}=12 \mod(31)$. Such fractional numbers become important in the factoring process for large semi-primes involving elliptic equations.

Consider one last example of gcd$(17,6)=1$. Here we have from the extended algorithm that $17=6(2)+5$ and $6=5(1)+1$. Eliminating 5 we get –

$$1 = 6(3) - 17(1) \quad \text{so that} \quad 1 = -17 \mod(6)$$
That this must be correct is seen by simply adding 18=3\times6 to -17 to get 1.

U.H.Kurzweg  
October 20, 2019  
Gainesville, Florida