FINDING THE GREATEST COMMON DIVISOR (GCD) USING THE EUCLIDIAN ALGORITHM

All positive integers are either composite or prime with the latter characterized by having no divisors other than one and the number. An elementary method for seeing what the largest common divisor of two real numbers N and M<N is can be found by use of an algorithm dating back to Euclid. We demonstrate the method by using two composite numbers N=4869 and M=2136. The procedure goes as follows-

$$4869 = 2 \cdot 2136 + 597$$
$$2136 = 3 \cdot 597 + 345$$
$$597 = 1 \cdot 345 + 252$$
$$345 = 1 \cdot 252 + 93$$
$$252 = 2 \cdot 93 + 66$$
$$93 = 1 \cdot 66 + 27$$
$$66 = 2 \cdot 27 + 12$$
$$27 = 2 \cdot 12 + 3$$
$$12 = 4 \cdot 3 + 0$$

The remainder term of 3 in the next to last equation is the largest common divisor (gcd). Things can be summarized as -

$$\gcd(4869, 2136) = 3$$

One can also work things backwards. Thus-

$$3 = 27 - 2 \cdot 12 = 27 - 2 \cdot (66 - 2 \cdot 27) = 5 \cdot 27 - 2 \cdot 66 =$$
$$5 \cdot (93 - 1 \cdot 66) - 2 \cdot 66 = 5 \cdot 93 - 7 \cdot 66 = 5 \cdot 93 - 7 \cdot (252 - 2 \cdot 93) =$$
$$19 \cdot 93 - 7 \cdot 252 = 19 \cdot (345 - 1 \cdot 252) - 7 \cdot 252 = 19 \cdot 345 - 26 \cdot 252 =$$
$$19 \cdot 345 - 26 \cdot (597 - 1 \cdot 345) = 45 \cdot 345 - 26 \cdot 597 =$$
$$45 \cdot (2136 - 3 \cdot 597) - 26 \cdot 597 = -161 \cdot 597 + 45 \cdot 2136 =$$
$$-161 \cdot (4869 - 2 \cdot 2136) + 45 \cdot 2136 = -161 \cdot 4869 + 367 \cdot 2136$$

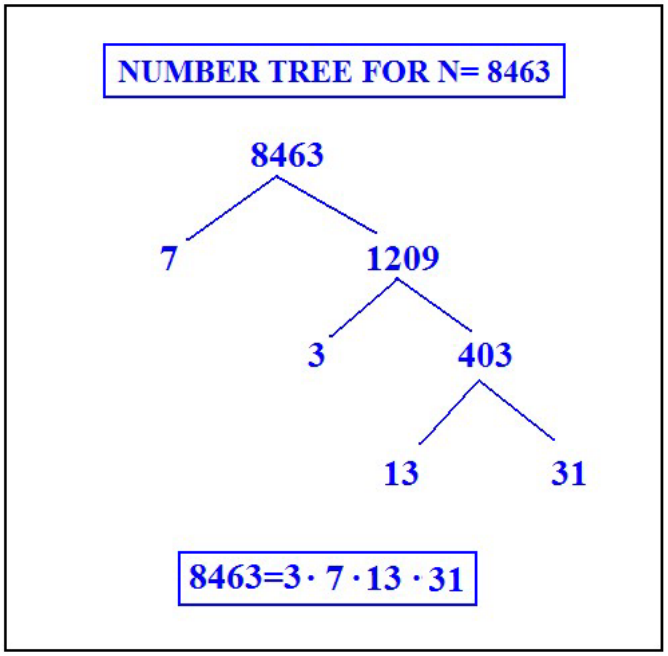
This result may be generalized to read-

$$\gcd(N,M)=\alpha N+\beta M$$

for any real numbers N and M for a specified set of constants α and β. Some other specific examples are-

$$\gcd(13,7)=1=-1\cdot 13+2\cdot 7 \quad \textit{and} \quad \gcd(16,12)=4=1\cdot 16-1\cdot 12$$

An alternative way to find the greatest common denominator of two numbers is to break each number into its product components of prime numbers and then pick out the product of the identical components in each breakdown. This will be the gcd. Take M=2·3·3·7·23=2898 and N=3·7·13·31=8463. Here the common product is 3·7=21 and hence gcd(8463, 2898)=21. This second route for finding the gcd at first glance seems a lot faster. However its drawback is that one has to first factor the numbers N and M into their prime number components. This can be quite time consuming when the numbers are large. Typically one breaks up large composite numbers by use of a number tree. Let me demonstrate for the above number N=8463-



Notice that the final result will always involve the product of prime numbers unless N is already prime by itself.

We point out that the two composite numbers N and M can also have a gcd of 1 as, for example, N=28 and N=9 yielding gcd(28,9)=1. What is certain is that if one has a prime number P then gcd(P, N) will always be one regardless of N.

Next let us use a little modular arithmetic to discuss the special case of the above identity when gcd(N,M)=1. One has-

$$1 = \alpha N + \beta M \,(\mathrm{mod}\, M)$$

which is equivalent to saying the inverse of N is-

$$N^{-1} = \alpha \,(\mathrm{mod}\, M)$$

with α found by inverting the gcd result. Let me demonstrate. Take N=9 and M=11. Here the Euclid Algorithm yields-

$$11 = 1 \cdot 9 + 2$$

$$9 = 4 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

So that gcd(11,9)=1 and –

$$1 = 9 - 4 \cdot 2 = 9 - 4 \cdot (11 - 1 \cdot 9) = 5 \cdot 9 - 4 \cdot 11$$

This produces –

$$9^{-1} = 5(\mathrm{mod}\, 11) = 5, 16, 27, etc$$

and-

$$11^{-1} = -4(\mathrm{mod}\, 9) = 5, 14, 23, etc$$

To demonstrate the use of the modular inverse of a number consider finding a second point $Q(x_2,y_2)$ on the curve $y=x^{1.5}$ which represents the intersection of a tangent line through point P(1,1). The tangent line reads y=0.5(3x-1) and must match $y=x^{1.5}$ at the second intersection point $Q(x_2,y_2)$. That is-

$$4x^3 - 9x^2 + 6x - 1 = 0 = (x-1)^2(4x-1)$$

So the second point becomes Q(1/4,1/8). But this point is actually closer to the origin than is P(1,1). To move further out one makes use of the property of a cubic which states that a second point with $P(x_3,y_3)$ can be found at-

$$x_3 = [y'(x_1)]^2 - 2x_1 \qquad y_3 = y'(x_1)[x_3 - x_1] + y_1$$

For the present example this means x_3=(3/2)2-2 and y_3=(3/2)(x_3-1)+1. Note the 2^{-1} term in both expressions. So let us take a positive odd number N and the number 2 and find the gcd. We have-

$$N = [(N-1)/2] \cdot 2 + 1 \;\; so\ that \; \gcd(N, 2) = 1$$

Inverting, one has-

$$1 = N - \frac{(N-1)}{2} \cdot 2 \,(\mathrm{mod}\, N)$$

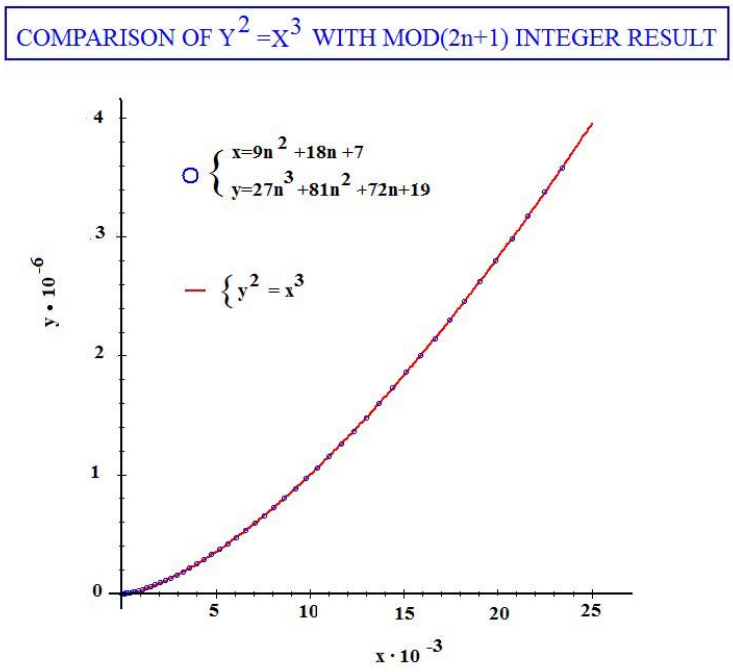
which produces the derivative-

$$y'(x_1) = -\frac{(N-1)}{2} \cdot 3 \,(\mathrm{mod}\, N) = 3 \cdot (\frac{N+1}{2})$$

Substituting, this in turn produces the multiple point results-

$$x_3 = \frac{9}{4}[(N+1)]^2 - 2 \;\; and \;\; y_3 = \frac{3}{2}(N+1)(x_3 - 1) + 1$$

for points along the curve $y^2=x^3$. Thus if N=5 we get x_3=79 and y_3=703. Notice that these points are very close to the curve but will not be directly on it unless $x^3=n^2$ and $y^3=n^3$ where n=1,2,3,… We show the accuracy of this mod inversion process by plotting the coordinates for x and y for N=2n+1 when 0<n<50 versus the curve $y^2=x^3$.



The agreement is quite good. We also notice that y_3 is always an odd number for the odd N case under consideration. Replacing N by 2n+1, one finds that-

$$y_3 = F(n) = 27n^3 + 81n^2 + 72n + 19 \ \ for\ n = 0,1,2,3,...$$

An interesting sidelight is the observation that F(n) is a function rich in prime numbers. Just looking at the first hundred values of n yields a total of 34 primes. These are found for –

$$n = 1,3,4,5,6,8,10,11,16,17,20,22,25,27,29,35,36,42,47,53,54,55,$$
$$61,62,63,65,67,72,79,80,81,82,89,98$$

Even for very large values of n one still finds numerous primes from this formula. One such example occurs for n=649179783461987435895781233986755 and yields the hundred digit prime number –

$$F(n) = 73868405451887922208778130969148550028840679108$$
$$34141437189921100351510917855671874529300764038488029$$

One can also obtain the gdc of more than just two numbers. Take the integers N, M, and K. First evaluate gcd(N,M) and then calculate gcd(K, gcd(M,N)) to get gcd(N,M,K). As a special case take (N,M,K)=(723,263,1271). Here gcd(723,263)=1 and gcd(1271,1)=gcd(723,263,1271)=1.

The gcd is also useful in solving the linear Diophantine equation-

$$ax + by = c$$

Where a, b, and c are integers and we are looking for integer solutions for x and y. Let α=x/c and β=y/c to get the equivalent form-

$$\alpha a + \beta b = 1 = \gcd(a,b)$$

We need only find the values of α and β by inverting the Euclidian Algorithm involving a and b. Let us demonstrate. Consider the specific Diophantine equation-

$$3\alpha + 4\beta = 1 \quad with \quad \gcd(4,3) = 1$$

From the gcd calculation we have-

$$1 = 4 - 1 \cdot 3 \quad so\ that\ \beta = y = 1\ and\ \alpha = x = -1$$

This is of course not the only integer solution. Looking at 1=4-1·3 as a mod(4) operation, we get-

$$x = -1 + 4k\ and\ y = 1 - 3k\ with\ k = 0, \pm 1, \pm 2, \pm 3, \ldots$$

A table of the integer solutions for -2≤k≤2 follows-

k	x	y
-2	-9	7
-1	-4	4
0	-1	1
1	3	-2
2	7	-5

Lets next try a more complicated linear Diophantine equation-

$$312x + 49y = 13$$

This time the Euclidian Algorithm yields-

$$312 = 6 \cdot 49 + 18$$

$$49 = 2 \cdot 18 + 13$$

$$18 = 1 \cdot 13 + 5$$

$$13 = 2 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

So that gcd(312,49)=1. Inverting, one finds after several steps that-

$$1 = -19 \cdot 312 + 121 \cdot 49 \pmod{312}$$

Thus –

$$y = 13(121 + 312k) \; and \; x = 13(-19 + 49k)$$

For k=0 the integer solution becomes (x,y)=(-247,1573).

For linear Diophantine equations the integer solutions always lie exactly on the curve defining x and y in a continuous manner. This will no longer be the case when dealing with non-linear Diophantine equations such as the elliptic equation $x^3+ax+b=y^2$.(see the graph above and the discussion on elliptic equations in the following section)

August 2010