Euclid's Algorithm

Given three integers a,b,ca,b,c, can you write cc in the form

c=ax+byc=ax+by

for integers xx and yy? Can there be more than one solution? Can you find them all? Before answering this, let us answer a seemingly unrelated question:

How do you find the greatest common divisor (gcd) of two integers a,ba,b?

We denote the greatest common divisor of aa and bb by gcd(a,b)gcd(a,b), or sometimes even just (a,b)(a,b). If (a,b)=1(a,b)=1 we say aa and bb are *coprime*.

The obvious answer is to list all the divisors aa and bb, and look for the greatest one they have in common. However, this requires aa and bb to be factorized, and no one knows how to do this efficiently.

Amazingly, a few simple observations lead to a far superior method: Euclid’s algorithm, or the Euclidean algorithm. First, if dd divides aa and dd divides bb, then dd divides their sum. Similarly, dd must also divide their difference, aa - bb, where aa is the larger of the two. But this means we’ve shrunk the original problem: now we just need to find gcd(a,a−b)gcd(a,a−b). We can repeat until we reach a trivial case.

Hence we can find gcd(a,b)gcd(a,b) by doing something that most people learn in primary school: division and remainder. We give an example and leave the proof of the general case to the reader.

Suppose we wish to compute gcd(27,33)gcd(27,33). First, we divide the bigger one by the smaller one:

33=1×27+633=1×27+6

Thus gcd(33,27)=gcd(27,6)gcd(33,27)=gcd(27,6). Repeating this trick:

27=4×6+327=4×6+3

and we see gcd(27,6)=gcd(6,3)gcd(27,6)=gcd(6,3). Lastly,

6=2×3+06=2×3+0

So since 6 is a perfect multiple of 3, gcd(6,3)=3gcd(6,3)=3, and we have found that gcd(33,27)=3gcd(33,27)=3.

This algorithm does not require factorizing numbers, and is fast. We obtain a crude bound for the number of steps required by observing that if we divide aa by bb to get a=bq+ra=bq+r, and r>b/2r>b/2, then in the next step we get a remainder r′≤b/2r′≤b/2. Thus every two steps, the numbers shrink by at least one bit.

Extended Euclidean Algorithm

The above equations actually reveal more than the gcd of two numbers. We can use them to find integers m,nm,n such that

3=33m+27n3=33m+27n

First rearrange all the equations so that the remainders are the subjects:

6=33−1×276=33−1×27

3=27−4×63=27−4×6

Then we start from the last equation, and substitute the next equation into it:

3=27−4×(33−1×27)=(−4)×33+5×27)3=27−4×(33−1×27)=(−4)×33+5×27)

And we are done: m=−4,n=5m=−4,n=5.

If there were more equations, we would repeat until we have used them all to find mm and nn.

Thus in general, given integers aa and bb, let d=gcd(a,b)d=gcd(a,b). Then we can find integer mm and nn such that

d=ma+nbd=ma+nb

using the extended Euclidean algorithm.

The General Solution

We can now answer the question posed at the start of this page, that is, given integers a,b,ca,b,c find all integers x,yx,y such that

c=xa+yb.c=xa+yb.

Let d=gcd(a,b)d=gcd(a,b). Since xa+ybxa+yb is a multiple of dd for any integers x,yx,y, solutions exist only when dd divides cc.

So say c=kdc=kd. Using the extended Euclidean algorithm we can find m,nm,nsuch that d=ma+nbd=ma+nb, thus we have a solution x=km,y=knx=km,y=kn.

Suppose x′,y′x′,y′ is another solution. Then

c=xa+yb=x′a+y′bc=xa+yb=x′a+y′b

Rearranging,

(x′−x)a=(y−y′)b(x′−x)a=(y−y′)b

Since dd is the greatest common divisor, b/db/d does not divide aa. But it must divide the right-hand side (since bb appears there) so (x′−x)(x′−x) is some multiple of b/db/d, that is

x′−x=tb/dx′−x=tb/d

for some integer tt. Then solving for (y−y′)(y−y′) gives

y′−y=ta/dy′−y=ta/d

Thus x′=x+tb/dx′=x+tb/d and y′=y−ta/dy′=y−ta/d for some integer tt.

But if we replace tt with any integer, x′x′ and y′y′ still satisfy c=x′a+y′bc=x′a+y′b. Thus there are infinitely many solutions, and they are given by

x=km+tb/d,y=kn+ta/d.x=km+tb/d,y=kn+ta/d.

for all integers tt.

Later, we shall often wish to solve 1=xp+yq1=xp+yq for coprime integers pp and qq. In this case, the above becomes

x=m+tq,y=n+tp.x=m+tq,y=n+tp.