Contents

0.1 Bezout's identity

For any two non-zero natural numbers a and b we can select natural numbers x and y such that

$ax + by = c$

The value of c is always a multiple of the greatest common denominator of a and b.

In addition, there exist x and y such that c is the greatest common denominator itself. This is the smallest positve value of c..

Let's take two numbers of the form $ax + by$:

$d = as + bt$

$n = ax + by$

Where $n > d$. And d is the smallest non-zero natural number form.

We know from Euclidian division above that for any numbers i and j there is the form $i = jq + r$.

So there are values for q and r for $n = dq + r$.

If r is always zero that means that all values of $ax + by$ are multiples of the smallest value.

$n = dq + r$ so $r = n - dq$.

$r = ax + by - (as + bt)q$

$r = a(x - sq) + b(y - tq)$

This is also of the form $ax + by$. Recall that r is the remainder for the division of d and n, and that $d = ax + by$ is the smallest positive value.

r cannot be above or equal to d due to the rules of euclidian division and so it must be 0.

As a result we know that all solutions to $ax + by$ are multiples of the smallest value.

As every possible $ax + by$ is a multiple of d, d must be a common divisor to both numbers. This is because $a.0 + b.1$ and $a.1 + b.0$ are also solutions, and d is their divisor.

So we know that the smallest positive solution is a common mutliple of both numbers.

We now need to show that that d is the largest common denominator. Consider a common denominator c.

$a = pc$

$b = qc$

And as before:

$d = ax + by$

So:

$d = pcx + qcy$

$d = c(px + qy)$

So $d \geq c$