

Theorem: Given $(m',n') = d$ where both m' and n' are not zero there exist integers x and y such that $m'x + n'y = d$

Let $m = m'/d$ and let $n = n'/d$

So we have to prove that given $(m,n) = 1$ that x and y can be found such that $mx + ny = 1$

We only prove for m and n both positive, because we only have to change the signs of x or y or both if m or n or both are negative

Now if $m=n=1$ then let $x=1$ and $y=0$ and we are finished. If not we go on.

By symmetry we assume $m > n$, then clearly $m = na_1 + b_1$ where b_1 the remainder.
So $b_1 < n$

Now let $im = na_i + b_i$ with $0 < i < n$ and $b_i < n$

Note that b_i cannot be zero

If $b_i = 0$ then we have for some $0 < i < n$ that $im = na_i$, but $(m,n) = 1$ so i must contain all the factors of n , but $i < n$ and therefore cannot contain all the factors of n .
So b_i cannot be zero.

Therefore for $0 < i < n$ we have that $0 < b_i < n$

Suppose that for some i and j where i is not equal to j and both i and j are bigger than 0 but smaller than n that $b_i = b_j$.

By symmetry we assume $i > j$

Then we have that $im = na_i + b_i$ and $jm = na_j + b_j$

So $im - jm = km = na_i - na_j = na_k$

Therefore $km = na_k$

Note $k < i < n$

n must divide k because $(n,m) = 1$, but this is impossible because $k < n$

So our assumption that $b_i = b_j$ can only be right if $i=j$

Therefore for $i = 1, 2, 3, 4, 5, 6, \dots, n-1$ we will have $n-1$ different b_i 's as well.

And because $0 < b_i < n$ one of those b_i must equal one.

Therefore we will have that $im = na_i + 1$ for some $n > i > 0$

Let $i = x$ and $a_i = -y$ then $xm = -ny + 1$ and thus $mx + ny = 1$

and thus by multiplying the equation with d we have $m'x + n'y = d$

END

This same type of procedure can be used to get the GCD of two numbers not both zero.

Let us suppose we want to get the GCD of m' and n'

Suppose by symmetry that $m' > n'$ and that a GCD $d > 1$ is present.

We again form $im' = n'a_i + b'_i$ for $0 < i < n'$ with b'_i the remainder $< n'$

Let $n'/d = n$ and $m = m'/d$ and $b'_i = db_i$

Now let us examine the equation $im' = n'a_i + b'_i$ when $i = n < n'$

When $i = n$ we have $nm' = n'a_i + b'_i$

So then $m' = da_i + b'_i / n$

Now $(n, d) = 1$ and $b'_i = db_i$, so $b'_i / n = db_i / n$

Therefore n divides d , but that is impossible and thus when $i = n$ we have $b'_i \neq 0$

Thus if $(m', n') = d > 1$ we will get for some $i < n'$ that $im' = n'a_i$

And clearly the GCD if present of m' and n' is $(m', n) = m'/a_i = n'/i$ when $b_i = 0$

What we therefore do when we are looking for a GCD is to increase i from $i=1$ up to $i = n'-1$ and observe the remainder b'_i .

If the remainder becomes zero in this interval for an $0 < i < n'$ we can stop because then m' and n' has a GCD and it will be n'/i

END

Examples

$$(12,5) = 1$$

$$12 = 5 \cdot 2 + 2$$

remainder of 2

$$12 \cdot 2 = 5 \cdot 4 + 4 \text{ remainder of 4}$$

$$12 \cdot 3 = 5 \cdot 7 + 1 \text{ remainder of 1}$$

$$\text{So } 12 \cdot 3 - 5 \cdot 7 = 1$$

Example

$$(35, 6) = 1$$

$$35 = 6 \cdot 5 + 5$$

$$35 \cdot 2 = 6 \cdot 11 + 4$$

$$35 \cdot 3 = 6 \cdot 17 + 3$$

$$35 \cdot 4 = 6 \cdot 23 + 2$$

$$35 \cdot 5 = 6 \cdot 29 + 1$$

$$(30,22)=?$$

$$30 = 22 + 8$$

$$30 \cdot 2 = 22 \cdot 2 + 16$$

$$30 \cdot 3 = 22 \cdot 4 + 2$$

$$30 \cdot 4 = 22 \cdot 5 + 10$$

$$30 \cdot 5 = 22 \cdot 15$$

.

.

.

$$30 \cdot 11 = 22 \cdot 15$$

$$\text{So GCD} = 30/15 = 22/11 = 2$$

END