

*Theorem: Given  $(m,n) = d$  where both  $m$  and  $n$  not zero there exists unique  $x,y$  integer such that  $mx + ny = d$*

This proof is usually done by using Euler's unique factorization algorithm for finding the greatest common divider of two integers. I have found an alternative method which I think is unique.

Proof : Let  $m = hd$  and  $n = jd$  .

Therefore  $(h,j)=1$

So we have to prove that an  $x$  and  $y$  exists so that  $hdx + jdy = d$  or

$$hx + jy = 1$$

Let  $h > j$  , then clearly  $h = ja_1 + b_1$  where  $b$  the remainder. So  $b < j$

Let  $b_1' + b_1 = j$  , also let  $h' = h - j$

Now we devise the following algorithm

$$h = ja_1 + b_1 \qquad \text{remainder } b_1$$

$$h + b_1' = ja_1 + b_1 + b_1' = j(a_1 + 1) = ja_2$$

$$h + b_1' + h - b_1' = 2h = ja_2 + h - b_1' = ja_2 + ja_3 + b_2 = ja_4 + b_2 \qquad \text{remainder } b_2$$

$$2h + b_2' = ja_4 + b_2' + b_2 = ja_5$$

$$2h + b_2' + h - b_2' = 3h = ja_5 + h - b_2' = ja_5 + ja_6 + b_3 = ja_7 + b_3 \qquad \text{remainder } b_3$$

The algorithm should become clear by now.

When we have a remainder on the right side we add  $(j - \text{that remainder})$  on both sides.

When we have a remainder on the left side we add  $(h - \text{that remainder})$  on both sides.

So in general our equation for our remainder on the right side is as follows.

$$vh = ja_i + b_v$$

Notice that for all  $v < j$  we have that the remainders  $b_v$  are all unique and none are equal to any other  $b$  remainder.

If we had some equal remainders for  $v < j$  we would have had the following.

$$vh = ja_i + b_v \quad \text{and} \quad sh = ja_s + b_v \quad \text{and thus} \quad vh - sh = zh = ja_i + b_v - (ja_s + b_v) = ja_z$$

$$\text{So } hz = jt$$

But this cannot be as  $(h,j) = 1$  and we can only have that  $hj = jh$  and we know that  $z < j$  and  $t < h$ .

Therefore if we continue the algorithm we would get the integers from 0 to  $j-1$  for  $v \leq j$

Therefore the remainder one would at some stage surface as a remainder and we would then have that

$$vh = ja_i + 1 \quad \text{and thus that} \quad hx + jy = 1 \quad \text{if } v = x \quad \text{and} \quad a_i = -y$$

and thus by multiplying the equation with  $d$  we have  $mx + ny = d$

Example to demonstrate the proof.

$$(12,5) = 1$$

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

$$12 + 3 = 5 \cdot 3$$

$$12 \cdot 2 = 5 \cdot 3 + 9 = 5 \cdot 3 + 5 \cdot 1 + 4 = 5 \cdot 4 + 4 \quad \text{remainder of 4}$$

$$12 \cdot 2 + 1 = 5 \cdot 5$$

$$12 \cdot 3 = 5 \cdot 5 + 11 = 5 \cdot 5 + 5 \cdot 2 + 1 = 5 \cdot 7 + 1 \quad \text{remainder of 1}$$

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

Example

$$(35, 6) = 1$$

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

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

$$35 \cdot 2 = 6 \cdot 6 + 34 = 6 \cdot 6 + 6 \cdot 5 + 4 = 6 \cdot 11 + 4$$

$$35 \cdot 2 + 2 = 6 \cdot 12$$

$$35 \cdot 3 = 6 \cdot 12 + 33 = 6 \cdot 12 + 6 \cdot 5 + 3 = 6 \cdot 17 + 3$$

$$35.3 + 3 = 6.18$$

$$35.4 = 6.18 + 32 = 6.18 + 6.5 + 2 = 6.23 + 2$$

$$35.4 + 4 = 6.24$$

$$35.5 = 6.24 + 31 = 6.24 + 6.5 + 1 = 6.29 + 1$$

---