NOTE: $a \mid b$ means a measures b

Definition: Let $d \mid a$ mean d measures a. When we say “d measures a” we mean that d fits a evenly, meaning a is a multiple of d
For example, 3 measures 15 because 3 fits into 15 evenly because 3×5=15.

Common Notion: if $d \mid a$ and $d \mid b - a$ then $d \mid b$.
Example:

d
——|

b *a*
——|——|——|——|——|——|——|——|

b
——|——|——|——|——|

Proposition 1. *Two unequal numbers being set out, and the less being continually subtracted in turn from the greater, if the number which is left never measures the one before it until an unit as left, the original numbers will be prime to one another*
Proposition 2. *Given two numbers not prime to one another, to find their greatest common measure.*

Algorithm:

Let a_1 and a_2 be the given numbers ($a_1 > a_2$). Find a common measure d.

$a_1 - m_1 a_2 = a_3$
$a_2 - m_2 a_3 = a_4$
$a_3 - m_3 a_4 = a_5$
…
$a_{n-2} - m_{n-2} a_{n-1} = a_n$ *where* $a_n \mid a_{n-1}$

Note that you subtract <u>continuously</u> meaning you subtract the term from the preceding one as many times as you can.
So if $a_4 = 30$ and $a_5 = 7$, you first subtract 7 from 30. That gives you 17. That is still greater than 7 so you subtract again and get 10. Subtract again to get 3. Now because 7 is bigger than 3, stop at 3. Therefore, you can subtract 7 from 30 three times, meaning you take $m_4 = 3$ for $a_3 - m_3 a_4 = a_5$.

<u>Example:</u>
80, 75

Proofs:

How we know we will eventually reach such an a_n such that $a_n \mid a_{n-1}$
Suppose we know for certain that if we continue the algorithm, we will eventually get 0. Let this number be $a_{n+1} = 0$. Then, we know from the algorithm that we got this number using $a_{n-1} - m_{n-1}a_n = a_{n+1}$. Setting $a_{n+1} = 0$, we have $a_{n-1} - m_{n-1}a_n = 0$. Therefore, $a_{n-1} = m_{n-1}a_n$, so $a_n \mid a_{n-1}$. This means that *if* we can proof that applying the algorithm will eventually get us to 0, then we know for certain that we can find an a_n such that $a_n \mid a_{n-1}$.

Now, let's proof we will reach 0:
Starting with a_1 and a_2 (with $a_1 > a_2$), we obtain $a_3, a_4, \dots, a_n$ by subtracting. Because we get each new term by subtracting a_{n-1} from a_{n-2} until the remainder (which is a_n) is less than a_{n-1} (i.e. until $a_n < a_{n-1}$), we know that each new term is less than the preceding one. Therefore, we have $a_1 > a_2 > a_3 > a_4 > \dots > a_n$. If we keep applying this algorithm, we know we have to arrive at 0 at some point because, if we don't, each term in the sequence will always get smaller and smaller but will always be greater than 0. This is absurd, because if you start out with any number (100 for example), you can't keep subtracting whole numbers from it forever.

Proof that the algorithm finds the greatest common measure
Here is the algorithm:

Let a_1 and a_2 be the given numbers ($a_1 > a_2$). Find a common measure d.

$a_1 - m_1a_2 = a_3$

$a_2 - m_2a_3 = a_4$

$a_3 - m_3a_4 = a_5$

...

$a_{n-2} - m_{n-2}a_{n-1} = a_n$ *where* $a_n \mid a_{n-1}$

Note the common notion (if $d \mid x$ and $d \mid y - x$ then $d \mid y$). Because $a_n \mid a_{n-1}$, we know $a_n \mid m_{n-2}a_{n-1}$. And because $a_n \mid a_n$, we know $a_n \mid a_{n-2} - m_{n-2}a_{n-1}$.

If we set $x = m_{n-2}a_{n-1}$ and $y = a_{n-2}$, we can replace…

$a_n \mid a_{n-2} - m_{n-2}a_{n-1}$ with $a_n \mid y - x$

and $a_n \mid x$

From the common notion (just replacing d with a_n) we discover $a_n \mid y$, which is the same as $a_n \mid a_{n-2}$. Now, we can keep applying this same reasoning to conclude that each of $a_{n-3}, a_{n-4}, \dots, a_2, a_1$ are all also measured by a_n. Because measures our original numbers a_1 and a_2, a_n is a common measure.

Now, we must proof that it is the *greatest* common measure. It must be the greatest, for if not, then let g be the greatest, so $g \mid a_1$ and $g \mid a_2$. Because g measures a_2, it also measures its multiple m_1a_2. From this we find that g measures a_3, because g measures both a_1 and m_1a_2 so their remainder a_3 is also measured by g (if this step doesn't make sense, look at the picture from the common notion and see if you can see why). We can apply this same reasoning (using $g \mid a_2$ and $g \mid a_3$) to show $g \mid a_4$, and so on until we get to $g \mid a_n$. Now, we hypothesized that g was greater than a_n, but now we found that g measures a_n. But g can't fit into something smaller than itself, so this is a contradiction. Therefore, a_n *must* be the greatest common measure.