Thm ⑥ : Let a & b be integers, not both zero. For a positive integer d, $d = \gcd(a,b)$ if and only if.

(a) d/a and d/b.

(b) whenever, c/a and c/b, then c/d.

Proof. Try to prove!

The Euclidean Algorithm

The Euclidean Algorithm is described as follows: Let a and b be two integers whose greatest common divisor is desired.

Since $\gcd(|a|,|b|) = \gcd(a,b)$, so there is no harm in assuming that $a \geq b > 0$.

The first step is to apply the Division Algorithm to a and b to get

$$a = q_1 b + r_1, \quad 0 \leq r_1 < b.$$

If $r_1 = 0$, then b/a and $\gcd(a,b) = b$.

When $r_1 \neq 0$, divide b by r_1 to produce integers q_2 and r_2 satisfying

$$b = q_2 r_1 + r_2, \quad 0 \leq r_2 < r_1.$$

If $r_2 = 0$, then stop, otherwise, proceed as before to obtain

$$r_1 = q_3 r_2 + r_3, \quad 0 \leq r_3 < r_2.$$

This division process continues until some zero remainder appears, say, at the $(n+1)^{th}$ stage where r_{n-1} is divided by r_n. [a zero remainder occurs since the decreasing sequence $b > r_1 > r_2 > \cdots \geq 0$ cannot contain more than b integers].

Scanned with CamScanner

So, we get the following system of equations:

$$\left.\begin{aligned} a &= q_1 b + r_1, & 0 < r_1 < b \\ b &= q_2 r_1 + r_2, & 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3, & 0 < r_3 < r_2 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n, & 0 < r_n < r_{n-1} \end{aligned}\right\} \longrightarrow (*)$$

$$r_{n-1} = q_{n+1} r_n + 0.$$

In this manner, r_n, the last non-zero remainder that appears is equal to $\gcd(a,b)$.

<u>Lemma</u>: If $a = qb + r$, then $\gcd(a,b) = \gcd(b,r)$.

<u>Proof</u>:- If $d = \gcd(a,b)$, then the relations d/a and d/b together imply that $d/a - qb$, or, d/r.

Thus, d is a common divisor of both b and r.

On the other hand, if c is an arbitrary common divisor of b and r, then $c / qb + r$, hence c/a.

This gives c a common divisor of a and b, so $c \leq d$.

It follows from the definition of $\gcd(b,r)$ that $d = \gcd(b,r)$.

<u>Note</u>: Using the above lemma, we simply work down the displayed system of equations, obtaining

$$\gcd(a,b) = \gcd(b, r_1) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n$$

as claimed.

Scanned with CamScanner

So, we get the following system of equations: (10)

$$\left.\begin{aligned}
a &= q_1 b + r_1, & 0 < r_1 < b \\
b &= q_2 r_1 + r_2, & 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3, & 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n, & 0 < r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n + 0.
\end{aligned}\right\} \longrightarrow (*)$$

In this manner, r_n, the last non-zero remainder that appears is equal to $\gcd(a, b)$.

<u>Lemma</u>: If $a = qb + r$, then $\gcd(a,b) = \gcd(b, r)$.

<u>Proof</u>:- If $d = \gcd(a, b)$, then the relations d/a and d/b together imply that $d/a - qb$, or, d/r.
Thus, d is a common divisor of both b and r.
On the other hand, if c is an arbitrary common divisor of b and r, then $c / qb + r$, hence c/a.
This gives c a common divisor of a and b, so
$c \leq d$.
It follows from the definition of $\gcd(b, r)$ that $d = \gcd(b, r)$.

<u>Note</u>: Using the above lemma, we simply work down the displayed system of equations, obtaining
$\gcd(a,b) = \gcd(b, r_1) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n$
as claimed.

Scanned with CamScanner

Ex: Check how the Euclidean Algorithm works in a concrete case by calculating, say $\gcd(12378, 3054)$. The appropriate applications of the Division Algorithm produce the equations

$$12378 = 4 \cdot 3054 + 162$$
$$3054 = 18 \cdot 162 + 138$$
$$162 = 1 \cdot 138 + 24$$
$$138 = 5 \cdot 24 + 18.$$
$$24 = 1 \cdot 18 + \boxed{6}$$
$$18 = 3 \cdot 6 + 0.$$

So, the last non-zero remainder appearing in these equations, namely, the integer 6, is the greatest common divisor of 12378 and 3054:

$$6 = \gcd(12378, 3054).$$

To represent 6 as a linear combination of integers 12378 and 3054.

We start with the ~~2nd last~~ following:

$$\begin{aligned}
6 &= 24 - 18 \\
&= 24 - (138 - 5 \cdot 24) \\
&= 6 \cdot 24 - 138 \\
&= 6(162 - 138) - 138 \\
&= 6 \cdot 162 - 7 \cdot 138 \\
&= 6 \cdot 162 - 7(3054 - 18 \cdot 162) \\
&= 132 \cdot 162 - 7 \cdot 3054 \\
&= 132(12378 - 4 \cdot 3054) - 7 \cdot 3054 \\
&= 132 \cdot 12378 + (-535)\, 3054.
\end{aligned}$$

Scanned with CamScanner

Thus, —

$$6 = \gcd(12378, 3054) = 12378x + 3054y,$$

where $x = 132$ and $y = -535$.

Note:- This is not the only way to express the integer 6 as a linear combination of 12378 & 3054; among other possibilities, we could add and subtract $3054 \cdot 12378$ to get

$$6 = (132 + 3054)\,12378 + (-535 - 12378)\,3054$$

$$= 3186 \cdot 12378 + (-12913)(3054).$$

Note: (a) In the above example, the smaller integer is (3054). 3054 has 4 digits. So the total number of divisions cannot be greater than 20; in actuality only six divisions were needed. This is by The French Mathematician Gabriel Lame.

(b) One observation is that for each $n > 0$, it is possible to find integers a_n & b_n such that exactly n divisions are required to compute $\gcd(a_n, b_n)$ by the Euclidean Algorithm. (Prove Later!)

Thm 7: If $k > 0$, then $\gcd(ka, kb) = k\gcd(a, b)$.

Proof:- If each of the equations appearing in the Euclidean Algorithm for a & b (see pag (10) (*)) is multiplied by k, we get —

$$ak = q_1 bk + r_1 k, \quad 0 < r_1 k < bk$$

$$bk = q_2 (r_1 k) + r_2 k, \quad 0 < r_2 k < r_1 k$$

$$\vdots$$

Scanned with CamScanner

$$r_{n-2}k = q_n (r_{n-1} k) + r_n k, \quad 0 < r_n k < r_{n-1} k$$

$$r_{n-1} k = q_{n+1} (r_n k) + 0.$$

It is clearly the Euclidean Algorithm applied to the integers ak and bk, so that their gcd is the last non-zero remainder $r_n k$; i.e

$$\gcd(ka, kb) = r_n k = k \gcd(a,b).$$

Corollary: For any integer $k \neq 0$, $\gcd(ka, kb) = |k| \gcd(a,b)$.

Proof: Prove it!

Note; $\gcd(ak, bk)$ is the smallest positive integer of the form $(ak)x + (bk)y$, which is equal to k times the smallest (+)ve integer of the form $ax+by$; the latter value is equal to $k \gcd(a,b)$.

We see that —

$$\gcd(12,30) = 3 \gcd(4,10) = 3 \cdot 2 \gcd(2,5) = 6 \cdot 1 = 6.$$

→ An integer c is said to be a common multiple of two non-zero integers a and b whenever $a|c$ & $b|c$. Zero is a common multiple of a and b.

For nontrivial existence of common multiples, note that the products ab and $-(ab)$ are both common multiple of a and b, one of these is (+)ve.

By Well-Ordering Principle, the set of positive common multiples of a and b must contain a smallest integer call it the least common multiple of a and b.

Scanned with CamScanner

Def^n:- The least common multiple of two non-zero integers a and b, denoted by $\mathrm{lcm}(a,b)$, is the (+)ve integer m satisfying the following:

(a) $a|m$ and $b|m$

(b) If $a|c$ and $b|c$, with $c>0$, then $m \le c$.

eg:- The positive common multiples of integers -12 and 30 are $60, 120, 180, \cdots$, hence, $\mathrm{lcm}(-12,30)=60$.

Remark:- Given non-zero integers a and b, $\mathrm{lcm}(a,b)$ always exist and $\mathrm{lcm}(a,b) \le |ab|$.

Thm 8:- For positive integers a and b

$$\gcd(a,b)\,\mathrm{lcm}(a,b) = ab.$$

Proof:- Put $d=\gcd(a,b)$ and write $a=dr$, $b=ds$ for integers r and s.

If $m=\frac{ab}{d}$, then $m=as=rb$, the effect of which is to make m a common multiple (positive) of a & b.

Now, let c be any positive integer that is a common multiple of a and b; say, $c=au=bv$.

We know, $\exists$ integers x and y satisfying

$$d=ax+by.$$

As a result, $\frac{c}{m}=\frac{cd}{ab}=\frac{c(ax+by)}{ab}=\frac{c}{b}(x)+\frac{c}{a}(y)$

$= vx+uy.$

$\Rightarrow m|c$. So $m \le c$. Thus by Def^n of lcm, $m=\mathrm{lcm}(a,b)$.

$\Rightarrow \boxed{\mathrm{lcm}(a,b)=\frac{ab}{d}=\frac{ab}{\gcd(a,b)}}$

Scanned with CamScanner