$Euclidian\ Algorithm\ In\ \mathbb{Z}$

$Definition:$ ————————————————————————————————

$$for\ c \in \mathbb{Z}_+^*\ to\ be\ the\ Greatest\ Common\ Divisor(gcd)\ of\ a\ and\ b$$

$$i)\ c\ must\ divid\ a\ and\ b$$

$$ii)\ any\ divisor\ of\ a\ and\ b\ must\ divid\ c$$

$$c = \max\left[k \in \mathbb{Z}^*,\ k|a\ and\ k|b\right]$$

$$iii) we\ define\ gcd(0,0) = 0$$

$$and\ because\ gcd\ must\ be\ positive$$

$$\forall a, b \in \mathbb{Z}\quad gcd(a,b) = gcd(-a,b) = gcd(a,-b) = gcd(-a,-b) = gcd(|a|,|b|)\ =\ c$$

————————————————————————————————

$* \longrightarrow\ Algorithm\ for\ finding\ gcd(a,b)$

$for\ a,b \in \mathbb{Z}$ because $gcd(a,b)$ is positive and for sake of the argument we suppose $a \geqslant b > 0,$
negative value is just change of sign the value will be the same.

$algstart:$
$\exists d \in \mathbb{Z}^+\ d = gcd(a,b)$
$\exists q_1, r_1 \in \mathbb{Z}^+\ \ a = q_1 {*} b + r_1$ with $q_1 = \left\lfloor \frac{a}{b} \right\rfloor$ and $0 \leqslant r_1 < b$
$if\ r_1 = 0$ then $gcd(a,b) = b$
else
so we know that $d|a$ and $d|b$ by the $fifth$ property of the normal division $d|a - q_1 b,$ hence $d|r_1$
the next step is to $find$ the gcd of r_1 and b because $a|q_1{*}b + r_1,$ wich will be equal to d lets prove it.
suppose that $c|r_1$ and $c|b$ that means $c|q_1{*}b + r_1$ implying $c|a$ so c is a dividor of both a and b by
$definition$ $d \geqslant c$ both divid r_1 and $b,$ hence $gcd(b, r_1).$ (this step is true for every iteration)
now lets $find$ d in the next step
$\exists q_2, r_2 \in \mathbb{Z}^+\ \ a = q_2{*}b + r_2$ with $q_2 = \left\lfloor \frac{b}{r1} \right\rfloor$ and $0 \leqslant r_2 < r_1$
$if\ r_2 = 0$ then $gcd(b, r_1) = r_1$
else
if we continue like this we can notice that we started by $0 \leqslant r_1 < b$ and now we have $0 \leqslant r_2 < r_1$
because of the nature of the set $\mathbb{Z}$ this cant continue for ever so
$\forall b \in \mathbb{Z}^+\ \ \exists n \in \mathbb{N}\quad 0 \leqslant r_n < r_{n-1} < \ldots\ < r_1 < b\ \Longrightarrow\ r_n = 0$
this is true because if we take the oposite sence

$\exists b \in \mathbb{Z}^+ \ \ \forall n \in \mathbb{N} \quad 0 \leqslant r_n < r_{n-1} < \ldots \ < r_1 < b \ and \ r_n \neq 0$
$the \ most \ major \ value \ can \ r_i \ take \ is \ r_i \ = \ b - i \ so \ we \ take \ n = b + 1, \ wich \ contradict \ that \ 0 \leqslant r_n,$
$hence \ the \ order \ property, \ so \ we \ are \ sure \ that \ is \ algorithm \ will \ eventually \ for \ some \ larger \ finite$
$n, \ r_n = 0 \ so \ after \ n \ iteration$

$$\exists q_n, r_n \in \mathbb{Z}^+ \ r_{n-2} = q_n * r_{n-1} + r_n \ with \ q_n = \left\lfloor \frac{r_{n-2}}{r_{n-1}} \right\rfloor \ and \ 0 \leqslant r_n < r_{n-1} \ with \ r_n = 0$$

$meaning \ gcd(r_{n-1}, r_n) = gcd(r_{n-1}, 0) = r_{n-1} \ because \ everything \ divid \ 0, \ hence \ d = r_{n-1}$
$: endalg$