Euclidean Algorithm

Firstly, from the previous theorem we know that

$$\gcd(a,b) = \gcd(b,r) \text{ for } a = b \cdot q + r$$

We want to know the result of $\gcd(a,b)$,
let's say $a = r_0$; $b = r_1$; $r = r_2$

$$r_0 = r_1 \cdot q_1 + r_2 \quad \wedge \quad 0 \le r_2 < r_1 \rightarrow \gcd(r_0, r_1)$$

$$r_1 = r_2 \cdot q_2 + r_3 \quad \wedge \quad 0 \le r_3 < r_2 \rightarrow \gcd(r_1, r_2)$$

$$r_2 = r_3 \cdot q_3 + r_4 \quad \wedge \quad 0 \le r_4 < r_3 \rightarrow \gcd(r_2, r_3)$$

$\vdots$

until the remainder is zero

$$r_{n-1} = r_n \cdot q_n + r_{n+1} = 0 \quad \wedge \quad \rightarrow \gcd(\overset{10}{r_{n-1}}, \overset{5}{r_n})$$

$$r_n = 0 \cdot q_n + r_{n+2} \quad \wedge \quad \rightarrow \gcd(r_n, 0)$$

*) Any number's gcd with zero is equal to that number's itself.
Therefore, $\boxed{\gcd(a,b) = \gcd(r_0, r_1) = \gcd(r_n, 0) = r}$

<u>example:</u> $\gcd(252, 198)$

$252 = 198 \cdot 1 + 54$

$198 = 54 \cdot 3 + 36$

$54 = 36 \cdot 1 + 18$

$36 = 18 \cdot 2 + 0$

$18 = 0 \cdot$ $\longrightarrow$ $\gcd(18, 0) = 18$