Def. 23 Let a and b be positive integers. Then a divided by b has quotient q and remainder r means that

$$a = b \cdot q + r, \quad 0 \leq r < b.$$

The values of q and r are uniquely determined by a and b!

Now we want to find $\gcd(a,b)$. We divide a by b and get

$$a = b \cdot q + r, \quad 0 \leq r < b$$

If d is any common divisor of a and b, then d is also a divisor of r. Similarly, if e is a common divisor of b and r, then e is also a divisor of a. In other words, the common divisors of a and b are the same as the common divisors of b and r, i.e., $\gcd(a,b) = \gcd(b,r)$.

We repeat the process, dividing b by r gives

$$b = r \cdot q' + r', \quad 0 \leq r' < r.$$

Analoglously, we have $\gcd(b,r) = \gcd(r,r')$.

Repeating this process, the remainder becomes smaller until it becomes 0. Then we have $\gcd(s,0) = s$, which is equal to $\gcd(a,b)$.

This method is called Euclidean Algorithm.