

Proof of the Euclidean Algorithm

Contents

| | | |
|----------|--|----------|
| 1 | Number Theory | 2 |
| 1.1 | Euclidean Algorithm | 2 |
| 1.2 | Divisibility Sets | 2 |
| 1.3 | Corollary: Divisibility of r | 2 |

1 Number Theory

1.1 Euclidean Algorithm

Theorem 1.1 (Euclidean Algorithm). *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then there exist $q, r \in \mathbb{Z}$ such that*

$$a = bq + r, \quad 0 \leq r < |b|.$$

Furthermore, the greatest common divisor of a and b , denoted $\gcd(a, b)$, satisfies

$$\gcd(a, b) = \gcd(b, r).$$

1.2 Divisibility Sets

Definition 1.2. *For integers a and b , not both zero, define*

$$D(a, b) = \{d \in \mathbb{Z} : d \mid a \text{ and } d \mid b\}.$$

The $\gcd(a, b)$ of a and b is

$$\max(D(a, b)).$$

1.3 Corollary: Divisibility of r

Corollary 1.3. *Given a, b , and r as in Theorem 1.1, if $d \mid a$ and $d \mid b$, then $d \mid r$.*

Proof. Since $d \mid a$ and $d \mid b$, we can write $a = nd$ and $b = md$ for some integers n, m . Then, by the division relation $a = bq + r$, we have

$$r = a - bq = nd - (md)q = d(n - mq),$$

so $d \mid r$. □

Proof. From Corollary 1.3, this means

$$\forall d \in D(a, b), \text{ since } d \mid a \text{ and } d \mid b, d \mid r.$$

Hence, with $d \mid b$ and $d \mid r$, by using Definition 1.2, we know that $d \in D(b, r)$.

It follows that, for the integers a and b under consideration,

$$\forall d \in D(a, b), d \in D(b, r),$$

meaning

$$D(a, b) \subseteq D(b, r).$$

Using an identical argument applied to integers b and r , we have

$$\forall d \in D(b, r), d \mid b, \text{ and } d \mid r, \text{ so } d \mid a,$$

and so,

$$\forall d \in D(b, r), d \in D(a, b),$$

meaning

$$D(b, r) \subseteq D(a, b).$$

As both $D(b, r) \subseteq D(a, b)$ and $D(a, b) \subseteq D(b, r)$, we conclude that

$$D(a, b) = D(b, r).$$

Since $D(a, b) = D(b, r)$, it follows that

$$\max D(a, b) = \max D(b, r).$$

Moreover, by Definition 1.2,

$$\gcd(a, b) = \max D(a, b) \quad \text{and} \quad \gcd(b, r) = \max D(b, r).$$

Therefore,

$$\boxed{\gcd(a, b) = \gcd(b, r)}.$$

□