

Proposition: (division with remainder)

If $n, d \in \mathbb{Z}$ and $d \neq 0$, then

\exists unique integers q and r with

$$n = qd + r \quad \text{and} \quad 0 \leq r < |d|$$

($q = \text{quotient}$, $r = \text{remainder}$)

proof: Assume $n \geq 0$. If $n < d$,

take $q = 0$ and $r = n$.

Use induction! Assume that

$n \geq d$ and that $\forall m \in \mathbb{Z}$

with $1 \leq m < n$, \exists

q_m and r_m with

$$m = q_m d + r_m \quad \text{Since}$$

$n \geq d$, we have either

$n = d$, in which case

we can choose $q = 1$ and $r = 0$,

or $n > d$, in which case

$0 < n - d < n$. Then

\exists integers s, t with

$$(n - d) = s d + t \quad \text{and}$$

$$0 \leq t < d.$$

Then

$$n = (sd + d) + t$$

$$n = d(s+1) + t,$$

So with $q = s+1$ and

$t = r$, we have the result.

Now assume $n < 0$. If

$d \mid n$, then we can take

$$r = 0 \text{ and } q = \frac{n}{d}.$$

If d does not divide n ,
apply the result to $-n > 0$:

$\exists s, t \in \mathbb{Z}$ with

$$-n = sd + t, \quad 0 < t < d.$$

Then

$$n = -(sd + t)$$

$$n = -sd - t$$

$$n = -sd - \underbrace{d + d}_{=0} - t$$

$$n = d(-s-1) + (d-t)$$

Since $t > 0$, $d-t < d$

and $t < d \Rightarrow 0 < d-t$,

Setting $r = d-t$ and $q = -s-1$,

we get the result for $n < 0$.

We have established the existence of q and r for all $n \in \mathbb{Z}$.

Uniqueness: Suppose \exists

q_1 and r_1 with

$$q_1 d + r_1 = n = qd + r,$$

$$0 \leq r_1 < d.$$

Then

$$q_1 d - qd = r - r_1,$$

$$\text{So } (q_1 - q)d = r - r_1.$$

Therefore, $d \mid (r - r_1)$.

But $0 \leq r, r_1 < d$,

So

$$|r - r_1| \leq \max\{r, r_1\} < d.$$

If d divides $r - r_1$

and $|r - r_1| < d$, then

$$r - r_1 = 0, \text{ so } r = r_1.$$

We immediately get from

$$q_1 d + r_1 = q d + r \quad \text{that}$$

$$q_1 = q, \text{ and uniqueness}$$

is established.



Notation: $\max\{n, m\}$

= maximum of n and m

Definition: (gcd) Let $m, n \in \mathbb{Z}$,
 $m \neq 0 \neq n$. Then $d \in \mathbb{N}$
is called the **greatest
common divisor** (gcd) of
 m and n if

1) $d \mid m$ and $d \mid n$

2) If $k \in \mathbb{N}$ and

$k \mid m$, $k \mid n$, then

$d \geq k$.

Proposition: If $m, n \in \mathbb{Z}$, let

$$I(m, n) = \{am + bn \mid a, b \in \mathbb{Z}\}.$$

Then

(1) $\forall s, t \in I(m, n), s+t \in I(m, n)$
and $-s \in I(m, n)$

(2) $\forall s \in \mathbb{Z}$, if

$$sI(m, n) = \{st \mid t \in I(m, n)\},$$

then $sI(m, n) \subseteq I(m, n)$

3) If $k \mid m$ and $k \mid n$, $k \in \mathbb{Z}$,

then if $t \in I(m, n)$,

$k \mid t$.

proof: Let $s, t \in I(m, n)$.

Then $\exists a_1, a_2, b_1, b_2 \in \mathbb{Z}$

with

$$s = a_1 n + b_1 m$$

$$t = a_2 n + b_2 m$$

Then

$$S+t = (a_1n + b_1m) + (a_2n + b_2m)$$

$$S+t = a_1n + a_2n + b_1m + b_2m$$

$$S+t = (a_1 + a_2)n + (b_1 + b_2)m.$$

With $a = a_1 + a_2 \in \mathbb{Z}$ and $b = b_1 + b_2 \in \mathbb{Z}$,

we have $S+t = an + bm \in I(m, n)$.

Also ,

$$-s = -(a_1n + b_1m)$$

$$-s = -a_1n - b_1m$$

$$-s = (-a_1)n + (-b_1)m$$

Since $a_1, b_1 \in \mathbb{Z}$, $-a_1, -b_1 \in \mathbb{Z}$,

So with $a = -a_1$, $b = -b_1$,

$$-s = an + bm \in I(m, n) -$$

2) Let $s \in \mathbb{Z}$, $t \in I(m, n)$.

Then $\exists a, b \in \mathbb{Z}$ with

$$t = an + bm.$$

$$st = s(an + bm)$$

$$st = san + sbm$$

$$st = (sa) \cdot n + (sb) \cdot m$$

Since $s, a, b \in \mathbb{Z}$, $sa, sb \in \mathbb{Z}$,

so $st \in I(m, n)$.

3) Suppose $k \mid n$ and $k \mid m$.

Then $\exists d, r \in \mathbb{Z}$,

$$n = kd$$

$$m = kr$$

Let $t \in I(m, n)$. Then \exists

$a, b \in \mathbb{Z}$,

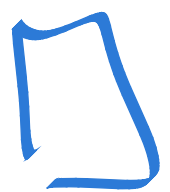
$$t = an + bm$$

Substituting,

$$t = a(kl) + b(kr)$$

$$t = (al + br)k$$

Since $a, l, b, r \in \mathbb{Z}$, we
have that $al + br \in \mathbb{Z}$, and
so $k \mid t$.



A side: in some texts or papers,
you may see (a, m)
written for $\gcd(a, m)$.

Lemma: Let $m, n \in \mathbb{Z}$, $m \neq 0 \neq n$.

If $d \in \mathbb{N}$, $d \mid m$ and $d \mid n$,

then if also $d \in I(m, n)$,

we have that $d = \gcd(m, n)$.

proof: Suppose that $k \in \mathbb{N}$ and

$k \mid m$, $k \mid n$. Then

by the previous proposition,

since $d \in I(m, n)$,

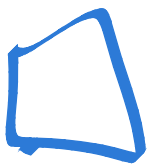
$k \mid d$. As $k, d \in \mathbb{N}$,

we must have that

$k \leq d$. From this,

we conclude that

$$d = \gcd(m, n).$$



The Euclidean Algorithm for the GCD

The Euclidean Algorithm is a procedure for obtaining the gcd of two nonzero integers -

The algorithm: Take $m, n \in \mathbb{Z}$

and suppose neither is 0.

We may assume that

$|m| \geq |n|$ without loss of

generality.

Then $\exists q_1, r_1 \in \mathbb{Z}$

$0 \leq r_1 < |n|$, with

$$n = q_1 a + r_1$$

Repeat!

$\exists q_2, r_2 \in \mathbb{Z}$,

$0 \leq r_2 < r_1$, with

$$r_1 = q_2 a + r_2$$

Keep going until
you can't obtain any
more remainders - at
most $|n|$ steps.