

Division Algorithm

Theorem (Division Algorithm): If $a, b \in \mathbb{Z}$ with $a > 0$ then there exist unique integers q, r such that

$$b = qa + r \quad \text{and} \quad 0 \leq r < a .$$

Proof of the Existence: Consider

$$S \stackrel{\text{def}}{=} \{b - ka : k \in \mathbb{Z}\} .$$

This set contains a positive (≥ 0) integer; namely if $b \geq 0$, then $b - 0a \in S$, and if $b < 0$ then $b - ba = b(1 - a) \in S$. The set $S_+ \stackrel{\text{def}}{=} \{s \in S : s \geq 0\}$ is thus not empty. It has a least element r . In other word, r is the smallest positive integer in S .

Being a member of S , r is of the form

$r = b - qa$ for some q . Hence

$$b = qa + r \quad \text{and} \quad r \geq 0 .$$

It is left to be shown that $r < a$.

BWoC assume $r \geq a$. Then

$$0 \leq r' \stackrel{\text{def}}{=} r - a = b - (q+1)a$$

would be a member of S_+ smaller than r , impossible.

Proof of the Uniqueness: Suppose there are two pairs (q, r) and (\bar{q}, \bar{r}) with

$$b = qa + r \quad \text{and} \quad 0 \leq r < a$$

$$b = \bar{q}a + \bar{r} \quad \text{and} \quad 0 \leq \bar{r} < a. \quad \text{Then}$$

$$0 = (q - \bar{q})a + (r - \bar{r}) \quad \text{and} \quad |r - \bar{r}| < a$$

$$\implies |q - \bar{q}|a = |r - \bar{r}| \quad \text{and} \quad a ||r - \bar{r}| ,$$

which implies $|r - \bar{r}| = 0$ and $|q - \bar{q}| = 0$, i.e.,
 $q = \bar{q}$ and $r = \bar{r}$. **QED**

Ideals

Definition: A non-void subset \mathcal{I} of \mathbb{Z} is an **Ideal** if for all $a, b, z \in \mathbb{Z}$

a) $a, b \in \mathcal{I} \implies a+b \in \mathcal{I}$ and

b) $z \in \mathbb{Z} \wedge a \in \mathcal{I} \implies za \in \mathcal{I}$.

Examples:

1) The even numbers form an ideal.

2) The odd numbers don't.

3) The set $\{0\}$ is an ideal, and so is \mathbb{Z} .

These two are the **Trivial Ideals**.

4) If $g \in \mathbb{Z}$ then the set

$$((g)) \stackrel{\text{def}}{=} \{zg : z \in \mathbb{Z}\}$$

of all multiples of g is an ideal, called the **Principal Ideal** with **Generator** g .

Clearly $((g)) = ((-g))$, so most principal ideals have at least two generators.

[Which one does not? Can a principal ideal have three distinct generators?]

Clearly $((g)) = ((-g))$, so most principal ideals have at least two generators.

[Which one does not? Can a principal ideal have three distinct generators?]

5) Let $a, b \in \mathbb{Z}$. The set

$$((a, b)) \stackrel{\text{def}}{=} \{xa + yb : x, y \in \mathbb{Z}\}$$

of all **linear combinations of a, b** forms an ideal, **the Ideal Generated by a, b** . Clearly $((a, b))$ contains $a = 1a + 0b$ and $b = 0a + 1b$. If an ideal \mathcal{I} contains the elements a and b then it contains the set $((a, b))$. Therefore $((a, b))$ is the smallest ideal containing the integers a and b as elements.

6) Let $a_1, \dots, a_n \in \mathbb{Z}$. The set

$$((a_1, \dots, a_n)) \stackrel{\text{def}}{=} \{x_1a_1 + \dots + x_na_n : x_i \in \mathbb{Z}\}$$

of all linear combinations of a_1, a_2, \dots, a_n

forms an ideal, **the Ideal Generated by** a_1, \dots, a_n . This is the smallest ideal containing the integers a_1, \dots, a_n and is a subset of every ideal that contains them.

7) The intersection of two ideals is an ideal.

8) $\{0\} = ((0))$ and $\mathbb{Z} = ((1))$.

9) If g is an element of the ideal \mathcal{I} then $((g)) \subseteq \mathcal{I}$.

Theorem: Every ideal is a principal ideal.

Proof: Let \mathcal{I} be an ideal. We have to show that there exists an integer g so that

$$\mathcal{I} = ((g)) .$$

Case 1): $\mathcal{I} = \{0\}$. Then $\mathcal{I} = ((0))$.

Case 2): \mathcal{I} contains a non-zero element a . Then it also contains $-a = -1 \times a$, so it

contains a strictly positive element. Let g be the smallest strictly positive element of \mathcal{I} . This is my candidate for the generator. Let $a \in \mathcal{I}$. Then there are $q, r \in \mathbb{Z}$ with

$$a = qg + r \quad \text{and} \quad 0 \leq r < g .$$

Clearly $0 \leq r = a - qg \in \mathcal{I}$, whence $r = 0$.
(Why?)

contains a strictly positive element. Let g be the smallest strictly positive element of \mathcal{I} . This is my candidate for the generator. Let $a \in \mathcal{I}$. Then there are $q, r \in \mathbb{Z}$ with

$$a = qg + r \quad \text{and} \quad 0 \leq r < g .$$

Clearly $0 \leq r = a - qg \in \mathcal{I}$, whence $r = 0$. (Why?)

Thus $a = qg$. This shows that an arbitrary element a of \mathcal{I} is a multiple of g , thus $\mathcal{I} \subset ((g))$. Since $((g)) \subseteq \mathcal{I}$, $((g)) = \mathcal{I}$. **QED**

The Greatest Common Divisor

Let $a, b \in \mathbb{Z}$. There exists a $g \in \mathbb{Z}$ such that

$$((a, b)) = ((g)) .$$

Since $a \in ((a, b)) = ((g))$, a is a multiple of g :

$$g|a , \text{ and } g|b$$

is seen in the same way. This makes g a **Common Divisor** of a and b .

Let d be another common divisor of a and b . Since there exist (why?) $x, y \in \mathbb{Z}$ with

$$g = xa + yb , \text{ we have } d|g$$

(why?). Hence g is a common divisor of a, b that is a multiple of any other common divisor: a common divisor of a, b that is divided by any other common divisor deserves the name **Greatest Common Divisor**.

["Greatest" does not refer to the order \leq on \mathbb{Z} !] If g is a greatest common divisor $\gcd(a, b)$ of a, b then clearly so is $-g$; and these are the only ones (iff $a = b = 0$ then they agree.) For if \bar{g} is another greatest common divisor of a, b then $g|\bar{g}$ and $\bar{g}|g$, whence $\bar{g} = \pm g$.

Summary: The greatest common divisors of two integers a, b are precisely the generators of the ideal $((a, b))$.

Henceforth **The Greatest Common Divisor** of a, b and the notation $\gcd(a, b)$ for it shall mean the positive greatest common divisor (which is of course the one and only positive generator of the ideal $((a, b))$).

Lemma: Let $a, b, n \in \mathbb{Z}$, $n \geq 0$. Then

$$n \times \gcd(a, b) = \gcd(n \times a, n \times b)$$

Proof: a) Let g, γ be the positive generators of $G \stackrel{\text{def}}{=} ((a, b))$ and $\Gamma \stackrel{\text{def}}{=} ((na, nb))$, respectively. We want to prove that $\gamma = ng$.

Since there exist x, y with $g = xa + yb$ and thus $ng = nxa + nyb \in \Gamma$, we have $\gamma | ng$.

b) Conversely, there are ξ, η so that

$$\gamma = \xi na + \eta nb = n(\xi a + \eta b) = nqg$$

for some $q \in \mathbb{Z}$. Hence $ng | \gamma$. a) and b) imply $\gamma = ng$. QED

Now that we know that any two integers a, b have a positive (≥ 0) greatest common divisor $\gcd(a, b)$, the positive generator of the ideal $((a, b))$, the problem arises to com-

pute it. This will be achieved by the Euclidean Algorithm below. First a

Lemma: Let $a, b, q, r \in \mathbb{Z}$.

If $b = qa + r$ **then** $((b, a)) = ((a, r))$.

Proof:

$a, r \in ((a, r)) \implies b \in ((a, r)) \implies ((a, b)) \subseteq ((a, r))$.

$a, b \in ((a, b)) \implies r \in ((a, b)) \implies ((a, r)) \subseteq ((a, b))$.

Hence $((a, b)) = ((a, r))$. **QED**

If $a = 0$ **then** $\gcd(a, b) = |b|$. **If** $b = 0$ **then** $\gcd(a, b) = |a|$. **In the case that** $a \neq 0 \neq b$ **the Euclidean Algorithm kicks in. We'll illustrate it by an example. First observe that**

$$((a, b)) = ((|a|, |b|)) \quad \text{why?}$$

To compute $\gcd(a, b)$ we may thus assume that $a, b > 0$.

Let us compute $\gcd(250, 111)$.

$$\begin{aligned} 250 &= 2 \times 111 + 28 &\implies ((250, 111)) &= ((111, 28)) \\ 111 &= 3 \times 28 + 27 &\implies ((111, 28)) &= ((28, 27)) \\ 28 &= 1 \times 27 + 1 &\implies ((28, 27)) &= ((27, 1)) = ((1)) \end{aligned}$$

We have $((250, 111)) = ((1))$, therefore

$$\gcd(250, 111) = 1 ,$$

which makes 250 and 111 **Relatively Prime**.

We know that there exist x, y so that

$$1 = x \times 250 + y \times 111$$

(how?). Let us find such x, y :

$$\begin{aligned} 1 &= 28 - 27 = 28 - (111 - 3 \times 28) = 4 \times 28 - 111 \\ &= 4 \times (250 - 2 \times 111) - 111 = 4 \times 250 - 9 \times 111. \end{aligned}$$

Example: For $n = 2, 3, \dots$,

$8n+3$ and $5n+2$ are relatively prime.

$$\begin{aligned}8n+3 &= 1 \times (5n+2) + (3n+1) \\ ((8n+3, 5n+2)) &= ((5n+2, 3n+1)) \\ 5n+2 &= 1 \times (3n+1) + (2n+1) \\ ((5n+2, 3n+1)) &= ((3n+1, 2n+1)) \\ 3n+1 &= 1 \times (2n+1) + n \\ ((3n+1, 2n+1)) &= ((2n+1, n)) \\ 2n+1 &= 2 \times n + 1 \\ ((2n+1, n)) &= ((n, 1)) = ((1)) .\end{aligned}$$

Example: Griffin finds himself on a lonely island with a bathtub full of beer, a rusty can holding 17 ounces, and another one holding 55 ounces. His cake recipe asks for precisely one ounce of beer. How can he manage that?

$$55 = 3 \times 17 + 4 \quad \implies ((55, 17)) = ((17, 4))$$

$$17 = 4 \times 4 + 1 \quad \implies ((17, 4)) = ((4, 1)) = ((1))$$

Hence

$$\begin{aligned} \gcd(55, 17) = 1 &= 17 - 4 \times 4 = 17 - 4 \times (55 - 3 \times 17) \\ &= 13 \times 17 - 4 \times 55 : \end{aligned}$$

Thirteen times he fills the small container with beer, decants it into the larger container, dumping out the beer in that whenever it is full (four times). He'll be left with one ounce in the large container.

Example: The XYZ Company has a dinner for all its employees. A place setting costs \$45, except for the women, who get an extra little vase with a flower for an additional \$2. The company lays out a total

of \$1613 for this dinner. How many male and female employees does XYZ company have?

First, $\gcd(45, 47) = 1 = 23 \cdot 45 - 22 \cdot 47$.

Therefore

$$1613 = (1613 \cdot 23 - k \cdot 47) \times 45 + (k \cdot 45 - 1613 \cdot 22) \times 47$$

for all $k \in \mathbb{Z}$. We want $k \in \mathbb{Z}$ so that both parentheses are positive:

$$789.34 \approx \frac{1613 \cdot 23}{47} \geq k \geq \frac{1613 \cdot 22}{45} \approx 788.58$$

implies $k = 789$ and

$$1613 = 16 \times 45 + 19 \times 47 :$$

XYZ company has 16 male and 19 female employees.