

## MATH237 — Discrete Mathematics

# Division & Factorization

### M-Strand, Lecture 2

## Division of Integers

In this section we work with the set of integers

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$$

With addition and subtraction, for any  $a, b \in \mathbb{Z}$  it is true that the numbers  $-a$ ,  $-b$ ,  $a + b$  and  $a - b$  all remain in  $\mathbb{Z}$ .

For multiplication,  $ab \in \mathbb{Z}$ , but  $\frac{1}{a}$  and  $\frac{1}{b}$  are not elements of  $\mathbb{Z}$ .

Nevertheless, some quotients  $\frac{a}{b}$  do give numbers in  $\mathbb{Z}$ .

We want to study this more closely.

**Definition.** Suppose that  $a, b \in \mathbb{Z}$  and  $a \neq 0$ . Then we say that  $a$  **divides**  $b$ , denoted  $a \mid b$ , if there exists  $c \in \mathbb{Z}$  such that  $b = ac$ .

We also say that  $a$  is a **divisor** of  $b$ , or that  $b$  is a **multiple** of  $a$ .

2

## Division of Integers

Here are some simple examples and properties of ‘divides’ as defined in this way.

**Examples:** We have  $2 \mid 6$ , and  $13 \mid 78$ , and  $25 \mid 125$ , and  $7 \mid 28$ , etc.

**Reflexivity:** For every  $a \in \mathbb{Z} \setminus \{0\}$ , we have  $a \mid a$  and  $a \mid -a$ .

**Units:** For every  $a \in \mathbb{Z} \setminus \{0\}$ , we have  $1 \mid a$  and  $-1 \mid a$ .

**Zero Divisors:** If  $ab = 0$  then either  $a = 0$  or  $b = 0$ .

**Transitivity:** If  $a, b, c \in \mathbb{Z} \setminus \{0\}$  satisfy  $a \mid b$  and  $b \mid c$ , then  $a \mid c$ .

To see this, note that  $a \mid b$  and  $b \mid c$  means that there must be integers  $m, n \in \mathbb{Z}$  such that  $b = am$  and  $c = bn$ ; so that  $c = (am)n = a(mn)$ . Clearly  $mn \in \mathbb{Z}$ .

3

## Division of Integers

A slightly more complicated property is:

**Integer Linear Combination:** If  $a, b, c \in \mathbb{Z}$  satisfy  $a \mid b$  and  $a \mid c$ , then for every  $x, y \in \mathbb{Z}$  we have  $a \mid (bx + cy)$ .

To see this, note that  $a \mid b$  and  $a \mid c$  means that there are integers  $m, n \in \mathbb{Z}$  such that  $b = am$  and  $c = an$ .

Now  $bx + cy = (am)x + (an)y = a(mx + ny)$  and  $mx + ny \in \mathbb{Z}$ .

A useful consequence of this is the **Rule of “2 out of 3”**:

Suppose  $x, y, z \in \mathbb{Z}$  are such that  $x + y = z$ , and there is  $a \in \mathbb{N}$  which divides two of  $x, y, z$ ; then  $a$  divides all three of  $x, y, z$ .

*Proof.* Since  $z = x + y = 1 \times x + 1 \times y$ ,

then  $x = z - y = 1 \times z + (-1) \times y$

and  $y = z - x = 1 \times z + (-1) \times x$ .

So whichever are the two known multiples of  $a$ , then the third can be written as an integer linear combination of these.

Hence the third is also a multiple of  $a$ . □

4

## Division and Remainders

**Theorem.** Suppose that  $a \in \mathbb{N}$  and  $b \in \mathbb{Z}$ . then there exist unique  $q, r \in \mathbb{Z}$  such that  $b = aq + r$  and  $0 \leq r < a$ .

The method of proof is to show that there are pairs of numbers  $(q, r)$  such that  $b = aq + r$ , but among such pairs there is exactly one for which  $0 \leq r < a$ .

*Proof.* Consider the set of numbers  $S = \{b - as \geq 0 : s \in \mathbb{Z}\}$ .

Then  $S$  is clearly a non-empty subset of  $\mathbb{N} \cup \{0\}$ . It follows from the Well-Ordering Principle that  $S$  has a smallest element. Let  $r$  be this smallest element, and let  $q \in \mathbb{Z}$  be such that  $b - aq = r$ .

Clearly  $r \geq 0$ , so it remains to show that  $r < a$ . But if  $r \geq a$  then  $b - (q + 1)a = (b - aq) - a = r - a \geq 0$ , so that  $b - (q + 1)a \in S$ .

But  $b - (q + 1)a < r$  would contradict  $r$  being smallest in  $S$ .

Next we show that such numbers  $r, q$  are unique. Suppose that

$b = aq_1 + r_1$  and  $b = aq_2 + r_2$  with  $0 \leq r_1 < a$  and  $0 \leq r_2 < a$ .

Then  $a|q_1 - q_2| = |r_1 - r_2| < a$ .

Since  $|q_1 - q_2| \in \mathbb{N} \cup \{0\}$ , we have  $q_1 = q_2$  and so  $r_1 = r_2$  also.  $\square$

5

## Greatest Common Divisor

Given integers  $a, b \in \mathbb{Z}$ , then any natural number  $d$  that divides both is said to be a **common divisor** of  $a$  and  $b$ .

**Theorem.** Suppose  $a, b \in \mathbb{N}$ ; there is a unique  $d \in \mathbb{N}$  such that

1.  $d|a$  and  $d|b$ ; and
2. if  $x \in \mathbb{N}$  and  $x|a$  and  $x|b$ , then  $x|d$ .

**Definition.** The number  $d$  is called the **greatest common divisor** of  $a$  and  $b$ , denoted by  $d = \gcd(a, b)$ .

We say that numbers  $a, b \in \mathbb{N}$  are **coprime** (or **relatively prime**) if  $\gcd(a, b) = 1$ .

To compute the greatest common divisor by finding all the common divisors of  $a$  and  $b$  is very tedious, and may be quite impractical; especially for numbers  $a$  and  $b$  having only large prime factors.

An alternative characterisation of  $\gcd(a, b)$  is as the smallest positive linear combination of  $a$  and  $b$ ; ...

6

## GCD as Linear Combination

**Theorem.** Suppose  $a, b \in \mathbb{N}$ . Then there exist  $x, y \in \mathbb{Z}$  such that  $\gcd(a, b) = ax + by$ .

*Proof.* Consider the set  $S = \{ax + by > 0 : x, y \in \mathbb{Z}\}$ . It is easy to see that  $S$  is a non-empty subset of  $\mathbb{N}$ , so by the Well-Ordering Principle,  $S$  has a least element,  $d_0$  say, with  $d_0 = ax_0 + by_0$ .

We show that  $d_0|ax + by$  for every  $x, y \in \mathbb{Z}$  (not both zero).

Suppose there exist  $x_1, y_1 \in \mathbb{Z}$  such that  $d_0 \nmid (ax_1 + by_1)$ ; then there exist  $q, r \in \mathbb{Z}$  such that  $ax_1 + by_1 = d_0q + r$  and  $1 \leq r < d_0$ . Then  $r = ax_1 + by_1 - (ax_0 + by_0)q = a(x_1 - x_0q) + b(y_1 - y_0q) \in S$ , contradicting  $d_0$  being the smallest element of  $S$ .

Now  $d_0$  divides  $a = 1 \times a + 0 \times b$  and similarly  $d_0$  divides  $b = 0 \times a + 1 \times b$ . Finally, by the rule of '2 out of 3', any common divisor of  $a$  and  $b$  divides any linear combination  $ax + by$ , in particular  $d_0$ . Thus  $\gcd(a, b) = d_0$ .  $\square$

**Theorem.** Suppose that  $a, b \in \mathbb{N}$  are coprime. Then there exist  $x, y \in \mathbb{Z}$  such that  $ax + by = 1$ .

7

## Euclidean Algorithm

**Theorem (Euclidean Algorithm).** Suppose  $a, b \in \mathbb{N}$  with  $a > b$ .

Suppose further that  $q_1, q_2, \dots, q_n, q_{n+1} \in \mathbb{Z}$  and  $r_1, r_2, \dots, r_n \in \mathbb{N}$  satisfy  $0 < r_n < r_{n-1} < \dots < r_2 < r_1 < b$  and

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n \\ r_{n-1} &= r_nq_{n+1} \end{aligned}$$

Then  $\gcd(a, b) = r_n$ .

*Proof.* First we show  $\gcd(a, b) = \gcd(b, r_1)$ . Note that  $\gcd(a, b)|b$  and  $\gcd(a, b)|a - bq_1 = r_1$ , so  $\gcd(a, b)|\gcd(b, r_1)$ .

Now  $\gcd(b, r_1)|bq_1 + r_1 = a$ , so that  $\gcd(b, r_1)|\gcd(a, b)$ .

Similarly  $\gcd(b, r_1) = \gcd(r_1, r_2) = \gcd(r_2, r_3) = \dots = \gcd(r_{n-1}, r_n)$ .

Now  $\gcd(r_{n-1}, r_n) = \gcd(r_nq_{n+1} + r_n, r_n) = r_n$ , so  $\gcd(a, b) = r_n$ .  $\square$

8

## Euclidean Algorithm

Find the greatest common divisor of  $a = 5111$  and  $b = 589$ .

$$5111 = 8 \times 589 + 399$$

$$589 = 1 \times 399 + 190$$

$$399 = 2 \times 190 + 19$$

$$190 = 10 \times 19$$

Thus  $\gcd(5111, 589) = 19$ .

Note furthermore that  $\gcd(a, b)$  is an integer linear combination of  $a$  and  $b$ ; for example:

$$\begin{aligned} 19 &= 399 - 2 \times 190 \\ &= 399 - 2 \times (589 - 1 \times 399) \\ &= 3 \times 399 - 2 \times 589 \\ &= 3 \times (5111 - 8 \times 589) - 2 \times 589 \\ &= 3 \times 5111 - 26 \times 589 \end{aligned}$$

9

## Factorization and Primes

**Definition.** Suppose that  $a \in \mathbb{N}$  and  $a > 1$ . Then we say that  $a$  is **prime** if it has exactly two positive divisors, namely 1 and  $a$ . When  $a$  is not prime, we say that it is **composite**.

**Theorem.** Suppose  $a, b \in \mathbb{N}$ , and that  $p \in \mathbb{N}$  is a prime. If  $p \mid ab$  then either  $p \mid a$  or  $p \mid b$ .

*Proof.* Suppose that  $p \nmid a$ . Let  $S = \{x \in \mathbb{N} : p \mid ax \text{ and } p \nmid x\}$ . We need to show that  $S$  is empty. Suppose, on the contrary, that  $S \neq \emptyset$ . Now since  $S \subseteq \mathbb{N}$  it follows from the Well-Ordering Principle that  $S$  has a smallest element,  $c$  say. Then  $p \mid ac$  and  $p \nmid c$ ; and since  $p \nmid a$  then  $c > 1$ . This will lead to a contradiction, as follows. If  $c > p$  then we would have  $p \mid a(c - p)$  but  $p \nmid (c - p)$ , so that  $c - p \in S$  contradicting  $c$  being the least element. Hence  $1 < c < p$ ; so there exist  $q, r \in \mathbb{Z}$  such that  $p = cq + r$  and  $0 \leq r < c$ . Since  $p$  is prime then  $r \neq 0$ , so  $1 \leq r < c$ . However,  $ar = ap - acq$  so that  $p \mid ar$ ; giving  $p \mid ar$  and  $p \nmid r$ . But  $r < c$ , which contradicts  $c$  being the smallest element of  $S$ .  $\square$

10

## Factorization and Primes

The previous result can be extended easily into the following:

**Theorem.** Suppose that  $a_1, \dots, a_k \in \mathbb{Z}$ , and that  $p \in \mathbb{N}$  is a prime. If  $p \mid a_1 \dots a_k$ , then  $p \mid a_j$  for some  $j \in \{1, 2, \dots, k\}$ .

**Theorem (Fundamental Theorem of Arithmetic).**

Suppose that  $n \in \mathbb{N}$  with  $n > 1$ . Then  $n$  is representable as a product of primes, uniquely up to the order of factors.

Taking into account the natural ordering by size of the primes ...

**Theorem.** Suppose that  $n \in \mathbb{N}$  with  $n > 1$ . Then  $n$  is uniquely representable as

$$n = p_1^{m_1} \dots p_r^{m_r}$$

for some  $r \in \mathbb{N}$ , where  $p_1 < \dots < p_r$  are primes and where  $m_j \in \mathbb{N}$  for every  $j = 1, \dots, r$ .

This representation is called the **canonical decomposition** of  $n$ .

11

## GCD using primes

The canonical decomposition gives yet another characterisation of the greatest common divisor,  $\gcd(a, b)$  of  $a$  and  $b$ .

Suppose the primes  $p_1 < p_2 < \dots < p_r$  are all the distinct prime factors of  $a$  and  $b$ , and

$$a = p_1^{u_1} \dots p_r^{u_r} \quad \text{and} \quad b = p_1^{v_1} \dots p_r^{v_r}$$

with  $u_1, \dots, u_r, v_1, \dots, v_r \in \mathbb{N} \cup \{0\}$ . These products of primes are essentially the canonical decompositions, but extended so that  $p_j^0$  occurs in the product for  $a$  when  $p_j$  is a factor of  $b$  but not  $a$ , and similarly a trivial factor occurs for prime factors of  $a$  but not  $b$ . The greatest common divisor is given by the product of primes:

$$\gcd(a, b) = \prod_{j=1}^r p_j^{\min\{u_j, v_j\}}$$

12