

# Integers

Discrete Mathematics  
Evgeny Skvortsov

# Integers

*“God made the integers; all else is the work of man”*

Leopold Kroenecker

## Division

- We will mostly learn properties of integers that are related to division
- If  $a$  and  $b$  are integers with  $a \neq 0$ , we say that  $a$  **divides**  $b$  if there is an integer  $c$  such that  $b = ac$ .
- When  $a$  divides  $b$  we say that  $a$  is a **divisor** (**factor**) of  $b$ , and that  $b$  is a **multiple** of  $a$ .
- The notation  $a \mid b$  denotes that  $a$  divides  $b$ . We write  $a \nmid b$  when  $a$  does not divide  $b$ .
- Example. Let  $n$  and  $d$  be positive integers. How many positive integers not exceeding  $n$  are divisible by  $d$ ?

The numbers in question have the form  $dk$ , where  $k$  is a positive integer and  $0 < dk \leq n$ . Therefore,  $0 < k \leq n/d$ . Thus the answer is  $\lfloor n/d \rfloor$

## Properties of Divisibility

### ● Theorem:

● Relation  $|$  on positive integers is a partial order.

### ● Proof

● Reflexivity:  $a|a$ , because  $a = a \cdot 1$

● Antisymmetry: If  $a | b$  and  $b | a$  then by definition  $a = b \cdot c$ ,  $b = a \cdot d$ .  
Thus  $a = a \cdot d \cdot c$ . Note that  $d$  and  $c$  must be positive, and therefore must be equal to 1.

● Transitivity: If  $a | b$  and  $b | c$  then  $b = a \cdot d$ ,  $c = b \cdot e$ . Therefore  $c = a \cdot d \cdot e$  and  $a | c$ .

## Properties of Divisibility and Arithmetic operations

- Let  $a$ ,  $b$ , and  $c$  be integers. Then
  - (i) if  $a \mid b$  and  $a \mid c$ , then  $a \mid (b + c)$ ;
  - (ii) if  $a \mid b$ , then  $a \mid bc$  for all integers  $c$ ;

Proof.

- (i) Suppose  $a \mid b$  and  $a \mid c$ . This means that there are  $k$  and  $m$  such that  $b = ak$  and  $c = am$ .

Then  $b + c = ak + am = a(k + m)$ , and  $a$  divides  $b + c$ .

## Properties of Divisibility (cntd)

● If  $a$ ,  $b$ , and  $c$  are integers such that  $a \mid b$  and  $a \mid c$ , then  $a \mid mb + nc$  whenever  $m$  and  $n$  are integers.

● Proof.

By part (ii) it follows that  $a \mid mb$  and  $a \mid nc$ .

By part (i) it follows that  $a \mid mb + nc$ .

● If  $a \mid b$  and  $b \mid a$ , then  $a = \pm b$ .

● Proof.

Suppose that  $a \mid b$  and  $b \mid a$ . Then  $b = ak$  and  $a = bm$  for some integers  $k$  and  $m$ .

Therefore  $a = bm = akm$ , which is possible only if  $k, m = \pm 1$ .

# The Division Algorithm

- **Theorem** (The division algorithm)

Let  $a$  be an integer and  $d$  a positive integer. Then there are unique integers  $q$  and  $r$ , with  $0 \leq r < d$ , such that  $a = dq + r$

- $d$  is called the **divisor**,  $a$  is called the **dividend**,  $q$  is called the **quotient**, and  $r$  is called the **remainder**

- Examples:

- Let  $a = 101$  and  $d = 11$   
Then  $101 = 11 \cdot 9 + 2$
- Let  $a = -11$  and  $d = 3$   
Then  $-11 = 3 \cdot (-4) + 1$
- Let  $a = 3$  and  $d = 11$   
Then  $3 = 11 \cdot 0 + 3$

## The Division Algorithm (cntd)

- Proof of the Division Algorithm.

- Existence

If  $d \mid a$  then the result follows from the definition of divisibility.

Otherwise let  $S = \{ a - td \mid t \in \mathbb{Z}, a - td > 0 \}$ .

If  $a > 0$  then taking  $t = 0$ , we have  $a - td = a > 0$ . Hence,  $a \in S$  and  $S \neq \emptyset$ .

If  $a \leq 0$ , take  $t = a - 1$ . Then  $a - td = a - (a - 1)d = a(1 - d) + d$ , with  $1 - d \leq 0$ , because  $d \geq 1$ . Therefore  $a - td > 0$  and  $S \neq \emptyset$ .

Thus,  $S$  is a nonempty subset of  $\mathbb{N}$ . By the Well-Ordering Principle, it has a least element  $r$ , where  $0 < r = a - qd$  for some  $q$ .

If  $r > d$ , then  $r = d + c$  for some positive  $c$ , and

$a - qd = r = d + c \Rightarrow c = a - (q + 1)d \in S$ , a contradiction.

If  $r = d$ , then  $a = (q + 1)d$ , a contradiction with  $a \not\mid d$

Therefore  $r < d$ .



## The Division Algorithm (cntd)

### ● Uniqueness.

Suppose that there are two different pairs of quotients and remainders. That is, there exist  $q, r$  and  $u, v$ , with  $0 \leq r < d$  and  $0 \leq v < d$ , such that  $a = qd + r$  and  $a = ud + v$ .

Then

$$qd + r = ud + v$$

$$d \cdot |q - u| = |r - v| < d$$

If  $q \neq u$ , then we have a contradiction.

Therefore  $q = u$ . But then  $r = v$ .

Q.E.D.

## Representation of Integers

- In most case we use decimal representation of integers. For example, 657 means

$$6 \cdot 100 + 5 \cdot 10 + 7 = 6 \times 10^2 + 5 \times 10^1 + 7 \times 10^0$$

- Let  $b$  be a positive integer greater than 1. Then if  $n$  is a positive integer, it can be expressed uniquely in the form

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$

where  $k$  is a nonnegative number,  $a_k, a_{k-1}, \dots, a_1, a_0$  are nonnegative integers less than  $b$ , and  $a_k \neq 0$

- Such a representation of  $n$  is called the **base  $b$  expansion of  $n$** , denoted by  $(a_k a_{k-1} \dots a_1 a_0)_b$

## Binary Expansion

- Important case of a base is 2. The base 2 expansion is called the binary expansion of a number

$$n = a_k \times 2^k + a_{k-1} \times 2^{k-1} + \cdots + a_1 \times 2 + a_0$$

- Find the binary expansion of 165

$$\begin{array}{rcl}
 165 & | & 2 \\
 \hline
 a_0 - \textcircled{1} & & 82 \\
 82 & | & 2 \\
 \hline
 a_1 - \textcircled{0} & & 41 \\
 41 & | & 2 \\
 \hline
 a_2 - \textcircled{1} & & 20 \\
 20 & | & 2 \\
 \hline
 a_3 - \textcircled{0} & & 10 \\
 10 & | & 2 \\
 \hline
 a_4 - \textcircled{0} & & 5 \\
 5 & | & 2 \\
 \hline
 a_5 - \textcircled{1} & & 2 \\
 2 & | & 2 \\
 \hline
 a_6 - \textcircled{0} & & 1 \\
 1 & & 
 \end{array}$$

$165 = (10100101)_2$

$$165 = 2 \cdot 82 + 1$$

$$82 = 2 \cdot 41 + 0$$

$$41 = 2 \cdot 20 + 1$$

$$20 = 2 \cdot 10 + 0$$

$$10 = 2 \cdot 5 + 0$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

$$1 = 2 \cdot 0 + 1$$

## Hexadecimal Expansion

- Using A, B, C, D, E, F for 10, 11, 12, 13, 14, 15, respectively, find the base 16 expansion of 175627

# Primes

- Every integer  $n$  (except for 1 and -1) has at least 2 positive divisors, 1 and  $n$  (or  $-n$ ).
- A positive number that does not have any other positive divisor is called **prime**
- Prime numbers: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, ...
- Mersenne numbers are the numbers of the form  $M_n = 2^n - 1$
- There are many prime numbers among Mersenne numbers. The greatest known prime number is  $M_{32582657} = 2^{32582657} - 1$
- The next candidate is  $M_{M_{61}} = 2^{2305843009213693951} - 1$
- A positive number that is not prime is called **composite**

## Composite Numbers

- Every composite number has a prime divisor.

- Proof.

Let  $S$  be the set of all composite numbers that do not have a prime divisor

Since  $S \subseteq \mathbb{N}$ , by the Well-Ordering Principle, it has a least element  $r$ .

As  $r$  is not prime, it has a divisor, therefore,  $r = uv$  for some positive integers  $u$  and  $v$ .

$u < r$  and  $v < r$ . Therefore  $u \notin S$ , and  $u$  has a prime divisor  $p$ .

Since  $p \mid u$  and  $u \mid r$ , we conclude that  $p \mid r$ , a contradiction.

## How many prime numbers are there?

### ● Theorem (Euclid)

There are infinitely many prime numbers.

### ● Proof.

By contradiction. Suppose that  $\{p_1, p_2, \dots, p_k\}$  is the set of all prime numbers, and let  $a = p_1 p_2 \dots p_k + 1$

Since  $a$  is greater than any member of the list,  $a$  is composite.

By the previous statement,  $a$  has a prime divisor, that is for some  $p_j$  we have

Since  $p_j \mid a$  and  $p_j \mid p_1 p_2 \dots p_k$  we have  $p_j \mid a - p_1 p_2 \dots p_k = 1$   
 A contradiction.

### ● If $n$ is a positive integer, then there are approximately $\frac{n}{\ln n}$ prime numbers not exceeding $n$

## Open Problems about Primes

### ● Goldbach's Conjecture

Every positive even number can be represented as the sum of two prime numbers.

For example:  $4 = 2 + 2$ ,  $8 = 5 + 3$ ,  $42 = 37 + 5$

Goldbach's conjecture is known to be true for even numbers up to  $2 \times 10^{17}$

### ● The Twin Prime Conjecture

Twin primes are primes that differ by 2, such as 3 and 5, 5 and 7, 11 and 13, etc.

The Twin Prime Conjecture asserts that there are infinitely many twin primes.

The record twin primes:  $16,896,987,339,975 \times 2^{171,960} \pm 1$



# Homework

Exercises from the Book

No. 2, 3, 4, 10, 12, 14 (page 603)