

**READING TO ACCOMPANY CSU-P MATH 319
NUMBER THEORY
SPRING TERM, 2014**

JONATHAN A. PORITZ *AFTER* WISSAM RAJI

1. WELL-ORDERING AND DIVISION

1.1. The Well-Ordering Principle and Mathematical Induction. In this section, we present three basic tools that will often be used in proving properties of the integers. We start with a very important property of integers called the well-ordering principle. We then state what is known as the pigeonhole principle, and then we proceed to present an important method called mathematical induction.

1.1.1. *The Well-Ordering Principle.*

Definition 1.1. Given a set S of numbers (of any kind), we say that $\ell \in S$ is a **least element of S** if $\forall x \in S$, either $x = \ell$ or $\ell < x$.

The Well-Ordering Principle. Every non-empty set of natural numbers has a least element.

This principle is often taken as an axiom.

1.1.2. *The Pigeonhole Principle.*

The Pigeonhole Principle. Let $s, k \in \mathbb{N}$ satisfy $s > k$. If s objects are placed in k boxes, then at least one box contains more than one object.

Date: 17 February 2014 00:51 These notes are adapted by Jonathan Poritz from **An Introductory Course in Elementary Number Theory** by Wissam Raji, see www.saylor.org/books/. Both these notes and Raji's text are released under a Creative Commons **CC BY 3.0** license, see

<https://creativecommons.org/licenses/by/3.0/>



Proof. Suppose that none of the boxes contains more than one object. Then there are at most k objects. This leads to a contradiction with the fact that there are s objects for $s > k$. $\square$

1.1.3. **The Principle of Mathematical Induction.** We now present a valuable tool for proving results about integers. This tool is the principle of mathematical induction.

Theorem 1.2. The First Principle of Mathematical Induction: Let $S \subset \mathbb{N}$ be a set satisfying the following two properties:

- (1) $1 \in S$; and
- (2) $\forall k \in \mathbb{N}, k \in S \Rightarrow k + 1 \in S$.

Then $S = \mathbb{N}$.

More generally, if $\mathcal{P}(n)$ is a property of natural numbers which may or may not be true for any particular $n \in \mathbb{N}$, satisfying

- (1) $\mathcal{P}(1)$ is true; and
- (2) $\forall k \in \mathbb{N}, \mathcal{P}(k) \Rightarrow \mathcal{P}(k + 1)$

then $\forall n \in \mathbb{N}, \mathcal{P}(n)$ is true.

We use the well-ordering principle to prove the first principle of mathematical induction

Proof. Let S be the set from the first part of the theorem and let T be the set of natural numbers not in S . We will use a proof by contradiction, so assume T is non-empty.

Then, by the well-ordering principle, T contains a least element ℓ .

Note that $1 \in S$, so $1 \notin T$ and thus $\ell > 1$. Therefore $\ell - 1$ is a natural number. Since ℓ is the least element of T , $\ell - 1$ is not in T , it is therefore in S .

But by the defining properties of S , since $\ell - 1 \in S$, $\ell = \ell - 1 + 1 \in S$, which contradicts the fact that ℓ is a least element of T , so in T , so not in S .

This contradiction implies that the assumption that T is non-empty is false, hence $S = \mathbb{N}$.

For the second part of the theorem, let $S = \{n \in \mathbb{N} \mid \mathcal{P}(n) \text{ is true}\}$ and apply the first part. $\square$

We now present some examples in which we use the principle of induction.

Example 1.3. Use mathematical induction to show that $\forall n \in \mathbb{N}$

$$(1.1) \quad \sum_{j=1}^n j = \frac{n(n+1)}{2}.$$

First note that

$$\sum_{j=1}^1 j = 1 = \frac{1 \cdot 2}{2}$$

and thus the the statement is true for $n = 1$. For the remaining inductive step, suppose that the formula holds for some particular $n \in \mathbb{N}$, that is $\sum_{j=1}^n j = \frac{n(n+1)}{2}$. We show that

$$\sum_{j=1}^{n+1} j = \frac{(n+1)(n+2)}{2}.$$

to complete the proof by induction. Indeed

$$\sum_{j=1}^{n+1} j = \sum_{j=1}^n j + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2},$$

and the result follows.

Example 1.4. Use mathematical induction to prove that $n! \leq n^n \forall n \in \mathbb{N}$.

Note that $1! = 1 \leq 1^1 = 1$. We now present the inductive step. Suppose that

$$n! \leq n^n$$

for some $n \in \mathbb{N}$, we prove that $(n+1)! \leq (n+1)^{n+1}$. Note that

$$(n+1)! = (n+1)n! \leq (n+1) \cdot n^n < (n+1)(n+1)^n = (n+1)^{n+1}.$$

This completes the proof.

Theorem 1.5. The Second Principle of Mathematical Induction: Let $S \subset \mathbb{N}$ be a set satisfying the following two properties:

- (1) $1 \in S$; and
- (2) $\forall k \in \mathbb{N}, 1, \dots, k \in S \Rightarrow k + 1 \in S$.

Then $S = \mathbb{N}$.

More generally, if $\mathcal{P}(n)$ is a property of natural numbers which may or may not be true for any particular $n \in \mathbb{N}$, satisfying

- (1) $\mathcal{P}(1)$ is true; and
- (2) $\forall k \in \mathbb{N}$, if $\mathcal{P}(1), \dots, \mathcal{P}(k)$ are all true, then $\mathcal{P}(k + 1)$ is also true

then $\forall n \in \mathbb{N}, \mathcal{P}(n)$ is true.

To prove the second principle of induction, we use the first principle of induction.

Proof. Let S be a set of integers as in the first part of the theorem. For $n \in \mathbb{N}$, let $\mathcal{P}(n)$ be the mathematical property “ $1, \dots, n \in S$ ”. Then we can apply the First Principle of Mathematical Induction to prove that $\forall n \in \mathbb{N} \mathcal{P}(n)$ is true, which means $S = \mathbb{N}$. [Details left to the reader.]

The second part of the theorem follows from the first in exactly the same way that the second part of the First Principle of Mathematical Induction followed from the first. $\square$

Exercises

- (1) Prove using mathematical induction that $n < 3^n$ for all positive integers n .
- (2) Show that $\sum_{j=1}^n j^2 = \frac{n(n+1)(2n+1)}{6}$.
- (3) Use mathematical induction to prove that $\sum_{j=1}^n (-1)^{j-1} j^2 = (-1)^{n-1} n(n+1)/2$.
- (4) Use mathematical induction to prove that $\sum_{j=1}^n j^3 = [n(n+1)/2]^2$ for every positive integer n .
- (5) Use mathematical induction to prove that $\sum_{j=1}^n (2j-1) = n^2$.
- (6) Use mathematical induction to prove that $2^n < n!$ for $n \geq 4$.
- (7) Use mathematical induction to prove that $n^2 < n!$ for $n \geq 4$.

1.2. Algebraic Operations With Integers. On $\mathbb{Z}$, the set of integers, there are two basic binary operations, namely **addition** (denoted by $+$) and **multiplication** (denoted by $\cdot$), which satisfy the following well known properties:

(1) **Commutativity of addition and multiplication**

$$\begin{aligned}\forall a, b \in \mathbb{Z} : \quad a + b &= b + a \\ a \cdot b &= b \cdot a\end{aligned}$$

(2) **Associativity of addition and multiplication**

$$\begin{aligned}\forall a, b, c \in \mathbb{Z} : \quad (a + b) + c &= a + (b + c) \\ (a \cdot b) \cdot c &= a \cdot (b \cdot c)\end{aligned}$$

(3) **Distributivity of multiplication over addition**

$$\forall a, b, c \in \mathbb{Z} : \quad a \cdot (b + c) = a \cdot b + a \cdot c.$$

In the set $\mathbb{Z}$ there are “identity elements” for the two operations $+$ and $\cdot$, and these are the elements 0 and 1 respectively, that satisfy the basic properties

$$\begin{aligned}\forall a \in \mathbb{Z} : \quad a + 0 &= 0 + a = a \\ a \cdot 1 &= 1 \cdot a = a.\end{aligned}$$

The set $\mathbb{Z}$ allows **additive inverses** for its elements, in the sense that for every $a \in \mathbb{Z}$ there exists another integer in $\mathbb{Z}$, denoted by $-a$, such that

$$(1.2) \quad a + (-a) = 0.$$

While for multiplication, only the integer 1 has a **multiplicative inverse** in the sense that 1 is the only integer a such that there exists another integer, denoted by a^{-1} or by $1/a$, (namely 1 itself in this case) such that

$$(1.3) \quad a \cdot a^{-1} = 1.$$

From the operations of addition and multiplication one can define two other operations on $\mathbb{Z}$, namely **subtraction** (denoted by $-$) and **division** (denoted by $/$). Subtraction is a binary operation on $\mathbb{Z}$, *i.e.*, defined for any two integers in $\mathbb{Z}$, while division is not a binary operation and thus is defined

only for some specific pairs of integers in $\mathbb{Z}$. Subtraction and division are defined as follows:

- (1) $\forall a, b \in \mathbb{Z}$, $a - b$ is defined to be $a + (-b)$
- (2) Given $a, b \in \mathbb{Z}$, where $b \neq 0$, if $\exists c \in \mathbb{Z}$ such that $a = b \cdot c$ then a/b is defined to be c .

1.3. Divisibility and the Division Algorithm. We now discuss the concept of divisibility and its properties.

1.3.1. Integer Divisibility.

Definition 1.6. If a and b are integers such that $a \neq 0$, then we say a **divides** b and write $a \mid b$ if there exists an integer k such that $b = ka$. That is, given $a, b \in \mathbb{Z}$ such that $a \neq 0$, we write $a \mid b$ if $\exists k \in \mathbb{Z}$ s.t. $b = ka$.

If a divides b , we also say a is a **factor** [or **divisor**] of b , and b is a **multiple** of a . If a does not divide b , we write $a \nmid b$.

For example, $2 \mid 4$ and $7 \mid 63$, while $5 \nmid 26$.

Definition 1.7. Given $a \in \mathbb{Z}$, we say a is **even** if $2 \mid a$, i.e., if $\exists k \in \mathbb{Z}$ s.t. $a = 2k$. In contrast, given $a \in \mathbb{Z}$, we say a is **odd** if $2 \nmid a$.

It is a consequence of the Division Algorithm, below, that if a is odd then $\exists k \in \mathbb{Z}$ s.t. $a = 2k + 1$.

Proposition 1.8. $\forall a \in \mathbb{Z}$ we have $a \mid 0$.

Proposition 1.9. If $b \in \mathbb{Z}$ is such that $|b| < a$, and $b \neq 0$, then $a \nmid b$.

Proposition 1.10. Given $a, b \in \mathbb{Z}$, $a \mid b \Leftrightarrow a \mid |b|$.

Theorem 1.11. If a, b and c are integers such that $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. Since $a \mid b$ and $b \mid c$, we know $\exists k_1, k_2 \in \mathbb{Z}$ such that $b = k_1 a$ and $c = k_2 b$. Hence $c = k_1 k_2 a$ and so $a \mid c$. $\square$

Example 1.12. Since $6 \mid 18$ and $18 \mid 36$, then $6 \mid 36$.

The following theorem states that if an integer divides two other integers then it divides any linear combination of these integers.

Theorem 1.13. $\forall a, b, c, m, n \in \mathbb{Z}$, if $c \mid a$ and $c \mid b$ then $c \mid (ma + nb)$.

Proof. Since $c \mid a$ and $c \mid b$, $\exists k_1, k_2 \in \mathbb{Z}$ such that $a = k_1c$ and $b = k_2c$. Thus

$$ma + nb = mk_1c + nk_2c = c(mk_1 + nk_2),$$

and hence $c \mid (ma + nb)$. $\square$

Theorem 1.13 can be generalized to any finite linear combination as follows. If

$$n \in \mathbb{N}, a, b_1, \dots, b_n \in \mathbb{Z} \text{ and } a \mid b_1, a \mid b_2, \dots, a \mid b_n$$

then

$$(1.4) \quad a \mid \sum_{j=1}^n k_j b_j$$

$\forall k_1, \dots, k_n \in \mathbb{Z}$. It would be a nice exercise to prove this generalization by induction.

1.3.2. The Division Algorithm.

Theorem 1.14. The Division Algorithm Given $a, b \in \mathbb{Z}$ such that $b > 0$, there exist unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < b$. This q is called the **quotient** and r the **remainder when a is divided by b** .

Proof. Consider the set $A = \{a - bk \geq 0 \mid k \in \mathbb{Z}\}$. Note that A is nonempty since for $k < a/b$, $a - bk > 0$. By the well-ordering principle, A has a least element $r = a - qb$ for some $q \in \mathbb{Z}$. Notice that $r \geq 0$ by construction. Now if $r \geq b$ then (since $b > 0$)

$$r > r - b = a - qb - b = a - (q + 1)b \geq 0.$$

This leads to a contradiction since r is assumed to be the least positive integer of the form $r = a - qb$. As a result we have $0 \leq r < b$.

We will show that q and r are unique. Suppose that $a = q_1b + r_1$ and $a = q_2b + r_2$ with $0 \leq r_1 < b$ and $0 \leq r_2 < b$. Then we have

$$a - a = q_1b + r_1 - (q_2b + r_2) = (q_1 - q_2)b + (r_1 - r_2) = 0.$$

As a result we have

$$(q_1 - q_2)b = r_2 - r_1.$$

Thus we get that

$$b \mid (r_2 - r_1).$$

And since $-\max(r_1, r_2) \leq |r_2 - r_1| \leq \max(r_1, r_2)$, and $b > \max(r_1, r_2)$, then $r_2 - r_1$ must be 0, i.e. $r_2 = r_1$. And since $bq_1 + r_1 = bq_2 + r_2$, we also get that $q_1 = q_2$. This proves uniqueness. $\square$

Example 1.15. If $a = 71$ and $b = 6$, then $71 = 6 \cdot 11 + 5$. Here $q = 11$ and $r = 5$.

Exercises

- (1) Show that $5 \mid 25$, $19 \mid 38$ and $2 \mid 98$.
- (2) Use the division algorithm to find the quotient and the remainder when 76 is divided by 13.
- (3) Use the division algorithm to find the quotient and the remainder when -100 is divided by 13.
- (4) Show that if a, b, c and d are integers with a and c nonzero, such that $a \mid b$ and $c \mid d$, then $ac \mid bd$.
- (5) Show that if a and b are positive integers and $a \mid b$, then $a \leq b$.
- (6) Prove that the sum of two even integers is even, the sum of two odd integers is even and the sum of an even integer and an odd integer is odd.
- (7) Show that the product of two even integers is even, the product of two odd integers is odd and the product of an even integer and an odd integer is even.
- (8) Show that if m is an integer then 3 divides $m^3 - m$.
- (9) Show that the square of every odd integer is of the form $8m + 1$.
- (10) Show that the square of any integer is of the form $3m$ or $3m + 1$ but not of the form $3m + 2$.
- (11) Show that if $ac \mid bc$, then $a \mid b$.
- (12) Show that if $a \mid b$ and $b \mid a$ then $a = \pm b$.

1.4. Representations of Integers in Different Bases. In this section, we show how any positive integer can be written in terms of any positive base integer expansion in a unique way. Normally we use decimal notation to represent integers, we will show how to convert an integer from decimal notation into any other positive base integer notation and vice versa. Using the decimal notation in daily life is more traditional probably only because we have ten fingers. (What about our toes? you cry. I don't know. And apparently the Babylonians had 30 fingers on each hand, or 15 on each hand and each foot, since they used base 60.)

Notation An integer a written in base b expansion is denoted by $(a)_b$.

Theorem 1.16. *Let $b \in \mathbb{Z}$ satisfy $b > 1$. Then $\forall m \in \mathbb{N}, \exists l \in \mathbb{N}$ and $\exists a_1, \dots, a_l \in \mathbb{Z}$ such that*

$$m = a_l b^l + a_{l-1} b^{l-1} + \dots + a_1 b + a_0,$$

$$0 \leq a_j < b \text{ for } j = 0, 1, \dots, l, \text{ and}$$

$$a_l \neq 0.$$

Proof. Fix an $m \in \mathbb{N}$. We start by dividing m by b and we get

$$m = q_0 b + a_0, \quad 0 \leq a_0 < b.$$

If $q_0 \neq 0$ then we continue to divide q_0 by b and we get

$$q_0 = q_1 b + a_1, \quad 0 \leq a_1 < b.$$

We continue this process and hence we get

$$q_1 = q_2 b + a_2, \quad 0 \leq a_2 < b,$$

.

.

.

$$q_{l-2} = q_{l-1} b + a_{l-1}, \quad 0 \leq a_{l-1} < b,$$

$$q_{l-1} = 0 \cdot b + a_l, \quad 0 \leq a_l < b.$$

Note that the sequence $q_0, q_1, \dots$ is a decreasing sequence of non-negative integers with a last term q_l that must be 0.

Now substituting the equation $q_0 = q_1b + a_1$ in $m = q_0b + a_0$, we get

$$m = (q_1b + a_1)b + a_0 = q_1b^2 + a_1b + a_0,$$

Successively substituting the equations in m , we get

$$\begin{aligned} m &= q_2b^3 + a_2b^2 + a_1b + a_0, \\ &\cdot \\ &\cdot \\ &\cdot \\ &= q_{l-1}b^l + a_{l-1}b^{l-1} + \dots + a_1b + a_0, \\ &= a_lb^l + a_{l-1}b^{l-1} + \dots + a_1b + a_0. \end{aligned}$$

What remains to prove is that the representation is unique. Suppose now that

$$m = a_lb^l + a_{l-1}b^{l-1} + \dots + a_1b + a_0 = c_lb^l + c_{l-1}b^{l-1} + \dots + c_1b + c_0$$

where if the number of terms is different in one expansion, we add zero coefficients to make the number of terms agree. Subtracting the two expansions, we get

$$(a_l - c_l)b^l + (a_{l-1} - c_{l-1})b^{l-1} + \dots + (a_1 - c_1)b + (a_0 - c_0) = 0.$$

If the two expansions are different, then there exists $0 \leq j \leq l$ such that $c_j \neq a_j$. As a result, we get

$$b^j((a_l - c_l)b^{l-j} + \dots + (a_{j+1} - c_{j+1})b + (a_j - c_j)) = 0$$

and since $b \neq 0$, we get

$$(a_l - c_l)b^{l-j} + \dots + (a_{j+1} - c_{j+1})b + (a_j - c_j) = 0.$$

We now get

$$a_j - c_j = (a_l - c_l)b^{l-j} + \dots + (a_{j+1} - c_{j+1})b,$$

and as a result, $b \mid (a_j - c_j)$. Since $0 \leq a_j < b$ and $0 \leq c_j < b$, we get that $a_j = c_j$. This is a contradiction and hence the expansion is unique. $\square$

Base 2 representation of integers is called binary representation. Binary representation is useful for computers: the coefficients $a_0, \dots, a_l$ of a binary representation all satisfy $0 \leq a_j < 2$, hence they are 0 or 1. Thus to represent an integer on l wires, one can have each wire either have voltage (1) or not (0). (In fact, the word *bit* is a contraction of *binary digit*.)

Computer programmers also frequently use base 8 and base 16, called *octal* and *hexadecimal* or *hex*, respectively. The Babylonians used base 60.

Example 1.17. To find the expansion of 214 base 3:

we do the following

$$214 = 3 \cdot 71 + 1$$

$$71 = 3 \cdot 23 + 2$$

$$23 = 3 \cdot 7 + 2$$

$$7 = 3 \cdot 2 + 1$$

$$2 = 3 \cdot 0 + 2$$

As a result, to obtain a base 3 expansion of 214, we take the remainders of divisions and we get that $(214)_{10} = (21221)_3$.

Example 1.18. To find the base 10 expansion, i.e. the decimal expansion, of $(364)_7$:

We do the following: $4 \cdot 7^0 + 6 \cdot 7^1 + 3 \cdot 7^2 = 4 + 42 + 147 = 193$.

When using a base $b > 10$, we can add some characters to represent numbers greater than 9. It is common to use the letters A (or a), B , C , etc. For example $(46BC29)_{13}$ where $A = 10$, $B = 11$, $C = 12$.

Exercises

- (1) Convert $(7482)_{10}$ to base 6 notation.
- (2) Convert $(98156)_{10}$ to base 8 notation.

- (3) Convert $(101011101)_2$ to decimal notation.
- (4) Convert $(AB6C7D)_{16}$ to decimal notation.
- (5) Convert $(9A0B)_{16}$ to binary notation.

1.5. The Greatest Common Divisor. In this section we define the greatest common divisor (gcd) of two integers and discuss its properties. We also prove that the greatest common divisor of two integers is a linear combination of these integers.

Two integers a and b , not both 0, can have only finitely many divisors (see Problem 5 of §1.3), and thus can have only finitely many divisors in common. In this section, we are interested in the greatest of these common divisors.

Definition 1.19. Given $a, b \in \mathbb{Z}$, not both zero, the **greatest common divisor** is the largest integer that divides both a and b , and is written $\gcd(a, b)$ (or sometimes just (a, b)).

When it makes some formulæ simpler, we will write $\gcd(0, 0) = 0$.

Example 1.20. The greatest common divisor of 24 and 18 is 6. In other words $\gcd(24, 18) = 6$.

Here is a useful concept:

Definition 1.21. $a, b \in \mathbb{Z}$ are said to be **relatively prime** if $\gcd(a, b) = 1$.

Example 1.22. The greatest common divisor of 9 and 16 is 1, thus they are relatively prime.

Note that every integer has positive and negative divisors. If a is a positive divisor of m , then $-a$ is also a divisor of m . Therefore by our definition of the greatest common divisor, we can see that $\gcd(a, b) = \gcd(|a|, |b|)$.

We can use the gcd of two integers to make relatively prime integers:

Theorem 1.23. If $a, b \in \mathbb{Z}$ have $\gcd(a, b) = d$ then $\gcd(a/d, b/d) = 1$.

Proof. Fix $a, b \in \mathbb{Z}$. We will show that a/d and b/d have no common positive divisors other than 1. Let $k \in \mathbb{N}$ be a divisor of both a/d and b/d , so $\exists m, n \in \mathbb{N}$ such that

$$a/d = km \quad \text{and} \quad b/d = kn$$

Thus we get that

$$a = kmd \quad \text{and} \quad b = knd.$$

Hence kd is a common divisor of both a and b . Also, $kd \geq d$. However, d is the greatest common divisor of a and b . As a result, we get that $k = 1$. $\square$

The next theorem shows that the greatest common divisor of two integers does not change when we add a multiple of one of the two integers to the other.

Theorem 1.24. *Let $a, b, c \in \mathbb{Z}$. Then $\gcd(a, b) = \gcd(a + cb, b)$.*

Proof. We will show that every divisor of a and b is also a divisor of $a + cb$ and b and vice versa. Hence they have exactly the same divisors. So we get that the greatest common divisor of a and b will also be the greatest common divisor of $a + cb$ and b . Let k be a common divisor of a and b . By Theorem 1.13, $k \mid (a + cb)$ and hence k is a divisor of $a + cb$. Now assume that l is a common divisor of $a + cb$ and b . Also by Theorem 1.13 we have ,

$$l \mid ((a + cb) - cb) = a.$$

As a result, l is a common divisor of a and b and the result follows. $\square$

Example 1.25. Notice that $(4, 14) = (4, 14 - 3 \cdot 4) = (4, 2) = 2$.

We now present a theorem which proves that the greatest common divisor of two integers can be written as a linear combination of the two integers.

Theorem 1.26. *Let $a, b \in \mathbb{Z}$ not both be zero. Then $\gcd(a, b)$ is the smallest natural number which is of the form $d = ma + nb$ for some $m, n \in \mathbb{Z}$.*

Proof. Assume without loss of generality that $a, b \in \mathbb{N}$ are positive integers. Consider the set

$$S = \{d \in \mathbb{N} \mid d = ma + nb \text{ for some } m, n \in \mathbb{Z}\}.$$

S is non-empty since $a = 1 \cdot a + 0 \cdot b$ and $b = 0 \cdot a + 1 \cdot b$ are both in S . Let $d \in \mathbb{N}$ be the least element of S , whose existence is guaranteed by the well-ordering principle. Notice $d = ma + nb$ for some $m, n \in \mathbb{Z}$, since $d \in S$. We still must prove that d divides both a and b and that it is the greatest such common divisor.

By the division algorithm, $\exists q, r \in \mathbb{Z}$ such that

$$a = qd + r, \quad 0 \leq r < d.$$

Thus we have

$$r = a - qd = a - q(ma + nb) = (1 - qm)a - qnb.$$

We then have that r is a linear combination of a and b . Since $0 \leq r < d$ and d is the least positive integer which is a linear combination of a and b , we must have $r = 0$ and so $a = qd$. Hence $d \mid a$.

The same sort of argument will show that $d \mid b$.

Now notice that if there is a divisor c that divides both a and b . Then c divides any linear combination of a and b by Theorem 1.13. Hence $c \mid d$. This proves that any common divisor of a and b divides d . Hence $c \leq d$, and d is the greatest common divisor. $\square$

There is a simple application of this which will be very useful in the future:

Corollary 1.27. *If $a, b \in \mathbb{Z}$ are relatively prime, then $\exists m, n \in \mathbb{Z}$ such that $ma + nb = 1$.*

Definition 1.28. For some $n \in \mathbb{N}$, let $a_1, a_2, \dots, a_n \in \mathbb{Z}$ not be all 0. The **greatest common divisor** of these integers is the largest integer that divides all of them, and is denoted $\gcd(a_1, \dots, a_n)$.

Definition 1.29. For some $n \in \mathbb{N}$, $a_1, a_2, \dots, a_n \in \mathbb{Z}$ are said to be **mutually relatively prime** if $\gcd(a_1, a_2, \dots, a_n) = 1$.

Example 1.30. The integers 3, 6, 7 are mutually relatively prime since $(3, 6, 7) = 1$ although $(3, 6) = 3$.

Definition 1.31. For some $n \in \mathbb{N}$, $a_1, a_2, \dots, a_n \in \mathbb{Z}$ are called **pairwise relatively prime** if $\forall i, j \in \mathbb{N}$ such that $i \leq n, j \leq n$, and $i \neq j$, we have $\gcd(a_i, a_j) = 1$.

Example 1.32. The integers 3, 14, 25 are pairwise relatively prime. Notice also that these integers are mutually relatively prime.

Proposition 1.33. For $n \in \mathbb{N}$ and $a_1, \dots, a_n \in \mathbb{Z}$, if $a_1, a_2, \dots, a_n$ are pairwise relatively prime then they are mutually relatively prime.

Exercises

- (1) Find the greatest common divisor of 15 and 35.
- (2) Find the greatest common divisor of 100 and 104.
- (3) Find the greatest common divisor of -30 and 95.
- (4) Let $m \in \mathbb{N}$. Find the greatest common divisor of m and $m + 1$.
- (5) Let $m \in \mathbb{N}$, find the greatest common divisor of m and $m + 2$.
- (6) Show that if $m, n \in \mathbb{Z}$ have $\gcd(m, n) = 1$, then $\gcd(m + n, m - n) = 1$ or 2.
- (7) Show that if $m \in \mathbb{N}$, then $3m + 2$ and $5m + 3$ are relatively prime.
- (8) Show that if $a, b \in \mathbb{Z}$ are relatively prime, then $\gcd(a + 2b, 2a + b) = 1$ or 3.
- (9) Show that if $a_1, a_2, \dots, a_n \in \mathbb{Z}$ are not all 0 and $c \in \mathbb{N}$, then $\gcd(ca_1, ca_2, \dots, ca_n) = c \cdot \gcd(a_1, a_2, \dots, a_n)$.

1.6. The Euclidean Algorithm. In this section we describe a systematic method that determines the greatest common divisor of two integers, due to Euclid and thus called the Euclidean algorithm.

Lemma 1.34. If $a, b, q, r \in \mathbb{Z}$ and $a = qb + r$, then $\gcd(a, b) = \gcd(r, b)$.

Proof. Note that by theorem 8, we have $\gcd(bq + r, b) = \gcd(r, b)$. □

Now to the Euclidean algorithm in its general form, which basically states that the greatest common divisor of two integers is the last non zero remainder of successive divisions.

Theorem 1.35. *Let $a, b \in \mathbb{N}$ and assume $a \geq b$. Define $r_0 = a$, $r_1 = b$, $s_0 = 1$, $s_1 = 0$, $t_0 = 0$, and $t_1 = 1$. Then apply the division algorithm successively to obtain quotients and remainders $q_j, r_j \in \mathbb{N}$ satisfying $r_j = r_{j+1}q_{j+1} + r_{j+2}$ and $0 \leq r_{j+2} < r_{j+1}$ for all $j = 0, 1, \dots, n-2$ where n is defined so that $r_{n+1} = 0$. Along the way, also define $s_{j+1} = s_{j-1} - q_{j+1}s_j$ and $t_{j+1} = t_{j-1} - q_{j+1}t_j$. Then $\gcd(a, b) = r_n = s_{n+1}a + t_{n+1}b$.*

Proof. By applying the division algorithm, we see that

$$\begin{aligned} r_0 &= q_1 r_1 + r_2 & 0 \leq r_2 < r_1, \\ r_1 &= q_2 r_2 + r_3 & 0 \leq r_3 < r_2, \\ &\cdot \\ &\cdot \\ &\cdot \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n & 0 \leq r_n < r_{n-1}, \\ r_{n-1} &= q_n r_n. \end{aligned}$$

Notice that, we will have a remainder of 0 eventually since all the remainders are integers and every remainder in the next step is less than the remainder in the previous one. By Lemma 1.34, we see that

$$\gcd(a, b) = \gcd(b, r_2) = \gcd(r_2, r_3) = \dots = \gcd(r_n, 0) = r_n.$$

□

Note: We did not actually prove that the s_j 's and t_j 's can be used, as claimed, as coefficients to write the gcd as a linear combination of a and b ; we ignored them, and instead proved the more limited theorem, which is called the **Euclidean Algorithm**. The full version is called the **extended Euclidean Algorithm**, and its proof is left as an exercise.

Example 1.36. We will find the greatest common divisor of 4147 and 10672:

Note that

$$10672 = 4147 \cdot 2 + 2378,$$

$$4147 = 2378 \cdot 1 + 1769,$$

$$2378 = 1769 \cdot 1 + 609,$$

$$1769 = 609 \cdot 2 + 551,$$

$$609 = 551 \cdot 1 + 58,$$

$$551 = 58 \cdot 9 + 29,$$

$$58 = 29 \cdot 2,$$

Hence $\gcd(4147, 10672) = 29$.

Exercises

- (1) Use the Euclidean algorithm to find the greatest common divisor of 412 and 32 and express it in terms of the two integers.
- (2) Use the Euclidean algorithm to find the greatest common divisor of 780 and 150 and express it in terms of the two integers.
- (3) Find the greatest common divisor of 70, 98, 108.
- (4) Let $a, b \in \mathbb{N}$ be even. Prove that $\gcd(a, b) = 2 \gcd(a/2, b/2)$.
- (5) Show that if $a \in \mathbb{N}$ is even and $b \in \mathbb{N}$ is odd, then $\gcd(a, b) = \gcd(a/2, b)$.
- (6) Prove the *extended* part of the Extended Euclidean Algorithm.