ELEMENTS OF NUMBER THEORY: LECTURE NOTES

FELIX LAZEBNIK

The goal of these several lectures is to discuss in more details some properties of integers. In what follows $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \dots, n, -n, \dots\}$ will denote the set of all integers and it will be our universe of discourse. By $\mathbb{N} = \{1, 2, 3, \dots, n, \dots\}$ we denote the set of positive integers. If otherwise is stated, letters $a, b, c, \dots, x, y, z$ will be used to represent integers *only*, and we will often allow ourselves not to mention this in the future. We do not give a formal definition of integers, and assume that the reader is well familiar with their basic properties, such as:

- The sum and the product of two integers are integers.

The addition and multiplication of integers satisfy

- Commutative laws: $a + b = b + a$, $ab = ba$.
- Associative laws: $(a + b) + c = a + (b + c)$; $(ab)c = a(bc)$.
- The distributive law: $a(b + c) = ab + ac$.
- There exist unique neutral elements: 0 for the addition, and 1 for the multiplication.
- For every integer a, there exists unique additive inverse, denoted $-a$.
- For every two integers a, b, $ab = 0$ if and only if $a = 0$ or $b = 0$.

We also assume that the First and the Second Principles of Mathematical Induction are valid methods of proving statements of the form $\forall n \in \mathbb{Z}_{\geq n_0}\ [P(n)]$, where $\mathbb{Z}_{\geq n_0}$ is the set of all integers greater or equal to an integer n_0. We will also use

The Well–Ordering Axiom for $\mathbb{Z}_{\geq n_0}$: *Every non–empty subset of $\mathbb{Z}_{\geq n_0}$ contains unique smallest element.*

It can be shown that the Well–Ordering Axiom is equivalent to each of the two Principles of Mathematical Induction.

By $|n|$ we denote the *absolute value* of n, which is equal to n if $n \geq 0$, and is $-n$ if $n < 0$ (e.g. $|5| = 5$, $|0| = 0$, $|-7| = -(-7) = 7$). For every two integers a, b, $|ab| = |a| \cdot |b|$.

Date: April 11, 2007.

The author is thankful to Renate Scheidler, Andrew Duncan, David Kravitz, Keith Mellinger, Kira Mineroff, Ted Moskalenko, and to many students and TA's from his classes whose comments helped to improve these notes.

1. Division of integers: basic properties

For two integers a and $b \neq 0$, there may exist an integer q such that $a = bq$. If this happens, then we say that b **divides** a, and denote this fact by writing $b|a$. If $b|a$, then a is called a **multiple** of b, b is called a **divisor** of a and q is called the **quotient** of the division of a by b. Using "the" in "the quotient" is justified by the fact that if such q exists, then it is unique (will be shown later). Thus $5|(-15)$ since $-15 = 5 \cdot (-3)$, 2 is a divisor of 20 since $20 = 2 \cdot 10$, 0 is a multiple of 5 since $0 = 5 \cdot 0$. If $b|a$, the we also say that a is **divisible** by b.

Why do we need to restrict b from being zero? The reason is the following. The equality $a = 0 \cdot q$ implies $a = 0$, therefore the only number a which seem to allow division by zero is 0 itself. But $0 = 0 \cdot q$ is correct for every q, which means that the quotient of the division of 0 by 0 can be any number. This proved to be too inconvenient when properties of integers (as well as rational or real numbers) are discussed, and therefore the division by zero is not defined at all. In what follows the notation $b|a$ will imply that $b \neq 0$.

In the following theorem we list several important properties related to the division of integers. Though most of them may look familiar or obvious, we are not sure that many readers have ever seen (or attempted) the proofs of these facts. Usually it is not their fault: integers are studied mostly in the 1–8 grades, and the predominant tradition is to postpone all proofs to the high school years. But for some reasons, they are rarely touched in high schools either... In our opinion it is very important to discuss them and the reader should study them very thoroughly.

Theorem 1. *For all integers $a, b, c, \ldots, x, y, z$,*

(i) *if $b|a$, then $b|ca$;*
(ii) *if $c|b$ and $b|a$, then $c|a$ (transitive property);*
(iii) *if $c|a$ and $c|b$, then $c|(a + b)$ and $c|(a - b)$;*
(iv) *if $c|a$ and $c|b$, then $c|(xa + yb)$;*
(v) *if $a \neq 0$, then $a|a$ (reflexive property) and $a|(-a)$;*
(vi) *if $b|a$ and $a \neq 0$, then $|b| \leq |a|$.*
(vii) *1 and -1 are divisors of every number;*
(viii) *a nonzero number has only finite number of divisors. Zero is divisible by any nonzero number.*

Proof.

(i) We have to show that $b|ca$, i.e., the existence of an integer q such that $ca = bq$. If $b|a$, then $a = bq_1$ for some integer q_1. Then $ca = c(bq_1) = b(cq_1)$. Since cq_1 is an integer, then setting $q = cq_1$ we obtain that $b|ca$. □
(ii) We have to show that $c|a$, i.e., the existence of an integer q such that $a = cq$. If $c|b$ and $b|a$, then $b = cq_1$ and $a = bq_2$ for some integers q_1 and q_2. Then $a = bq_2 = (cq_1)q_2 = c(q_1q_2)$. Setting q being equal the integer q_1q_2, we get $a = qc$ which ends the proof. □
(iii) We prove the statement for $a + b$ only. The proof for $a - b$ is absolutely similar. We have to show that $c|(a + b)$, i.e., the existence of an integer q such that $a + b = cq$. Since $c|a$ and $c|b$, there are integers q_1, q_2 such that $a = cq_1$ and $b = cq_2$. Then $a + b = cq_1 + cq_2 = c(q_1 + q_2)$. Since $q_1 + q_2$ is an integer, setting $q = q_1 + q_2$, we obtain that $a + b = cq$. □

(iv) Before we start our proof, we want to point out that this statement is a generalization of the previous one. Indeed, taking $x = y = 1$, we obtain $c|(1\cdot a+1\cdot b) = a+b$, and taking $x = 1, y = -1$, we get $c|(1\cdot a+(-1)b) = a-b$. We wish to present two proofs of (iv): one based on (iii) and (i) and another is independent.

Proof 1. Since $c|a$ and $c|b$, then, from (i), we get that $c|xa$ and $c|yb$. But now it follows from (iii), that $c|(xa + yb)$. □

Proof 2. We have to show that $c|(xa+yb)$, i.e., the existence of an integer q such that $xa+yb = qc$. Since $c|a$ and $c|b$, there are integers q_1, q_2 such that $a = cq_1$ and $b = cq_2$. Then $xa + yb = x(cq_1) + y(cq_2) = c(xq_1 + yq_2)$. Since $xq_1 + yq_2$ is an integer, setting $q = xq_1 + yq_2$, we obtain that $xa + yb = cq$. □

Remark. Since (iv) implies (iii), and the second proof of (iv) is independent of (iii) one might ask why we bothered to prove (iii) at all. Our answer is two-fold. First, a development of a mathematical theory most often follows an 'inductive' path, i.e., a generalization from particular cases to general ones. On the other hand, having (iii) proven, enabled us to construct a proof of (iv) (the first one).

(v) Since $a = a \cdot 1$ and $-a = a(-1)$, the statement follows. (Both 1 and -1 are integers!). □

(vi) Indeed, $b|a$ implies that $a = bq$ for some integer q, and therefore $|a| = |b||q|$. Since a is nonzero, then so is q. Hence $|q| \geq 1$. Together with $|a| = |b| \cdot |q|$, it implies $|b| \leq |a|$. □

(vii) Since for every integer a, $a = 1 \cdot a = (-1) \cdot (-a)$, the statement follows. □

(viii) If $b|a$ and $a \neq 0$, then (vi) gives $|b| \leq |a|$. Since we are dealing with integers only, the latter implies that $b \in \{-a, -a+1, \ldots, -1, 1, \ldots, a-1, a\}$. Therefore a nonzero integer a has at most $2|a|$ divisors, and this proves the first statement. The second statement is obvious, since $0 = b \cdot 0$ for any b. □

Regardless of how basic the statements of Theorem 1 are, in the right hands they become powerful tools and can be used to establish many interesting and much less obvious facts about integers. The latter is not always easy. To the contrary, usually it requires several trials to find (and to write) a proof, and sometimes the solution resists many attempts. Below we give several examples of rather simple applications.

Example 1. Take a two-digit integer, switch the digits, and subtract the obtained number from the original one. Prove the difference will always be divisible by 9.

Solution. Let N be the number. Then $N = \overline{ab} = 10a + b$ for some integers a and b. The bar over ab signifies that a and b are digits in the representation of N in base ten, and is used to distinguish N from the product ab. After the digits are reversed, we obtain a number $M = \overline{ba} = 10b + a$. Then $N - M = (10a + b) - (10b + a) = 9a - 9b = 9(a - b)$. Since $a - b$ is an integer, $9|(N - M)$, and the proof is complete. □

Example 2. Is it possible to pay total of \$100674 for buying several \$12 items and several \$32 dollar items?

Solution. The answer is "No". To show this we assume the contrary, and let integers x and y represent the number of \$12 items and \$32, respectively. Then

the total price is $12x + 32y = 100{,}674$. Since $4|12$ and $4|32$, then $4|(12x + 32y) = 100674$ (according to Theorem 1 (iv)). But 4 does not divide 100674 (check it!). The obtained contradiction proves our answer.

Example 3. Prove that for all $n \in \mathbb{N}$, $27|(10^n + 18n - 1)$.

Proof. We use the method of mathematical induction. For $n = 1$, $10^1 + 18 \cdot 1 - 1 = 27$. Since $27|27$, the statement is correct in this case.

Let $n = k \geq 1$ and let $27|A = 10^k + 18k - 1$.

We wish to show that $27|B = 10^{k+1} + 18(k + 1) - 1 = 10^{k+1} + 18k + 17$.

Consider

$$\begin{aligned} C &= B - 10A \\ &= (10^{k+1} + 18k + 17) - (10^{k+1} + 180k - 10) \\ &= -162k + 27 \\ &= 27(-6k + 1). \end{aligned}$$

Then $27|C$, and $B = 10A + C$. Since $27|A$ (inductive hypothesis) and $27|C$, then B is the sum of two addends each divisible by 27. By Theorem 1 (iii), $27|B$, and the proof is complete. □

Exercise Set 1

The horizontal lines divide the problems in three groups according to their difficulty: easier, intermediate, harder. The division is very subjective, and I am sure many readers will often disagree with the ordering. Those who do not have much experience with the subject may proceed in order.

1. Show that if $a|b$ and $b|a$, then $a = b$ or $a = -b$. Is the converse statement correct?
2. Construct the converse statement to Theorem 1 (i), (iii), (vi). Prove or disprove them.
3. Prove that the sum of any four consecutive integers is an even number.
4. Prove that:
   (i) if n is a perfect square, then n has an odd number of distinct positive divisors;
   (ii) if n is not a perfect square, then n has an even number of distinct positive divisors.
5. Are there integers x and y, such that
   (i) $16x + 10y = -22$?
   (ii) $24x - 54y = 28{,}010$?
   Prove your answers.

---

6. Prove by induction that for all $n \in \mathbb{N}$,
   (i) $5|(n^5 - n)$
   (ii) $7|(n^7 - n)$
   (iii) $9|(4^n + 15n - 1)$
   (iv) $64|(3^{2n+3} + 40n - 27)$.
7. Show that the sum of $2n + 1$ consecutive integers is divisible by $2n + 1$. (For example, for $n = 3$, $16 + 17 + 18 + 19 + 20 + 21 + 22 = 133$ is divisible by 7.)

8. Prove that a 6–digit number of the form $\overline{abcabc}$, a, b, c are the digits, is always divisible by 7,11, and 13.
9. There were seven sheets of paper. Some of them were cut into seven pieces. Some of the obtained pieces were cut again into seven pieces, and so on. At the end 1961 pieces altogether were counted. Prove that the count was wrong.

---

10. 1000 students came to the school. All lockers are open. The first student comes in and closes all lockers. Then the second student comes in and changes the condition of each second locker, i.e., he opens lockers numbered 2,4,6,. . ., 1000. Then the third student comes in and changes the condition of each third locker, i.e., he opens locker 3, closes locker 6, opens locker 9, and so on. Eventually the 1,000th student comes in and changes the condition of the 1000th locker. Which lockers are now closed?
11. Prove that for all $n \in \mathbb{N}$, $133 \,|\, (11^{n+2} + 12^{2n+1})$.
12. Consider any positive integer N whose (decimal) digits read from left to right are in non-decreasing order, but the last two digits (tens and ones) are in increasing order. For example, $a = 1778$, $b = 2344459$, $c = 12225557779$. Note that when each of these numbers is multiplied by 9, the sum of digits in the result is 9:

$$9a = 16002,\ 9b = 21100131,\ 9c = 110030020011.$$

Prove that it is always true, i.e., the sum of digits of $9N$ is 9.

2. Division with remainder

The following theorem will hardly surprise anyone. At the same time it represents one of the most important properties of integers. All it says is that integers can be divided with remainders.

Theorem 2. *(*Division with Remainder Theorem.*) For any two of integers a and b, $b \neq 0$, there exist a unique pair of integers q and r, $0 \leq r < |b|$, such that $a = qb + r$.*

For example:

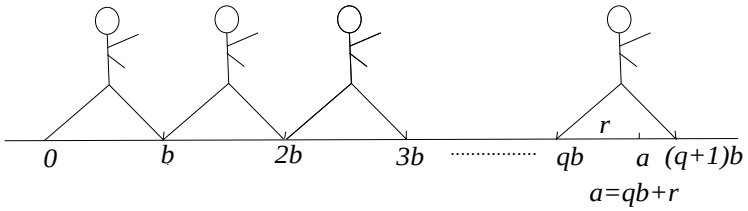
if $(a, b) = (20, 6)$, then $(q, r) = (3, 2)$, since $20 = 3 \cdot 6 + 2$ and $0 \leq 2 < 6$;
if $(a, b) = (-20, 6)$, then $(q, r) = (-4, 4)$, since $-20 = (-4) \cdot 6 + 4$ and $0 \leq 4 < 6$;
if $(a, b) = (20, -6)$, then $(q, r) = (-3, 2)$, since $20 = (-3) \cdot (-6) + 2$ and $0 \leq 2 < |-6| = 6$;
if $(a, b) = (-20, -6)$, then $(q, r) = (4, 4)$, since $-20 = 4 \cdot (-6) + 4$ and $0 \leq 4 < 6$;
if $(a, b) = (120, -8)$, then $(q, r) = (-15, 0)$, since $120 = (-15) \cdot (-8) + 0$ and $0 \leq 0 < |-8| = 8$;
if $(a, b) = (0, 7)$, then $(q, r) = (0, 0)$, since $0 = 0 \cdot 7 + 0$ and $0 \leq 0 < 7$.

If $a = qb + r$ and $0 \leq r < |b|$, then we will continue calling q the **quotient** of the division of a by b and we will refer to r as the **remainder** of the division of a by b.

Proof. We break the proof into two parts: the existence of q and r and their uniqueness.

Existence. In case the reader experiences difficulties with this rather boring proof, we recommend that he (she) illustrates the arguments by a proper numerical example.

Let us first assume that $a \geq 0$ and $b > 0$; all other cases will be easily reduced to this one. Intuitively, the theorem states that "walking" along x-axis with step of length b one can reach a or stop before reaching a at distance r from a, where $r < b$.



We form a set $A = \{a - xb : a \geq xb, x \in \mathbb{Z}\}$ by subtracting from a all multiples of b which do not exceed a. Clearly $A \neq \emptyset$, since $a = a - 0 \cdot b \in A$, and all elements of A are non–negative integers. By the Well-Ordering Axiom, A contains the smallest element. Let us call it r and, since r is in A it is of the form $r = a - qb$, for some q. We are going to show that q and r satisfy the statement of the theorem. Obviously, $a = qb + r$. To show that $0 \leq r < |b| = b$, we assume the contrary, namely $r \geq b$ and arrive to a contradiction. Thus suppose $r \geq b$, and let $r' = r - b$. Then $a = qb + r = (qb + b) + (r - b) = (q + 1)b + r'$, and hence $r' = a - (q + 1)b$. Since $r' \geq 0$ and r' is of the form $a - xb$, then $r' \in A$. Since $0 \leq r' < r$, we found an element in A smaller than r. This contradicts the definition of r as being the smallest member of A. The source of the contradiction is our assumption that $r \geq b$. Therefore $0 \leq r < b$ and the proof of the existence is completed (in this case).

The case when $a \geq 0$, but $b < 0$, can be reduced to the previous one. Indeed, since $-b > 0$, there are integers q' and r such that $a = q'(-b) + r = (-q')b + r$ and $0 \leq r < -b = |b|$ (by the case above!). Setting $q = -q'$, we get $a = qb + r$ with $0 \leq r < |b|$ and the proof is completed.

The case when $a < 0$ and $b > 0$, can again be reduced to the first case. Indeed, since $-a > 0$, there are integers q' and r' such that $-a = q'b + r'$, with $0 \leq r' < b$. If $r' = 0$, then $a = (-q')b + 0$, and the proof is complete. If $0 < r' < b$, then $a = (-q')b - r' = (-q' - 1)b + (b - r')$. Setting $q = -q' - 1$ and $r = b - r'$, we get $a = qb + r$, where $0 < r < b = |b|$, and the proof is completed.

The case when $a < 0$ and $b < 0$, is left to the reader.

Uniqueness. We have to show that if $a = qb + r = q_1 b + r_1$, with $0 \leq r < |b|$ and $0 \leq r_1 < |b|$, then $q = q_1$ and $r = r_1$. Indeed, $qb + r = q_1 b + r_1 \iff r - r_1 = (q_1 - q)b$, and so

$$|r - r_1| = |q_1 - q||b|. \tag{1}$$

If $q_1 = q$, then $|r - r_1| = 0 \iff r = r_1$, and the statement is proven. If $q \neq q_1$, then $|q_1 - q| \geq 1$ and the right hand side of (1) is *at least* $|b|$. But the left hand side of (1) represents the distance between two integer points of the real line segment $[0, |b| - 1]$, and therefore is *at most* $|b| - 1$. The obtained contradiction shows that the case $q \neq q_1$ is not possible. This proves that the representation is unique. □

The following two examples illustrate some immediate applications of Theorem 2.

Example 4. If $a = 5k + 2$, then we know that when a divided by 5, k is the quotient and 2 is the remainder. Indeed, just divide a by 5 with the remainder and apply Theorem 2.

Example 5. Every integer n can be written in one and only one of the following four forms: $n = 4k$, or $n = 4k + 1$, or $n = 4k + 2$, or $n = 4k + 3$, where k is an integer. Indeed, just divide n by 4 with the remainder and apply the Division with Remainder Theorem.

Examples below suggest more interesting applications of Theorem 2.

Example 6. When n is divided by 8, the remainder is 5. What is the remainder of the division of $n^3 + 5n$ by 8?

Solution. By Theorem 2, $n = 8k + 5$, for some integer k. Then

$$\begin{aligned} n^3 + 5n &= (8k + 5)^3 + 5(8k + 5) \\ &= 8^3k^3 + 3(8^2k^2)5 + 3(8k)5^2 + 5^3 + 5(8k) + 5^2 \\ &= 8(8^2k^3 + 3(8k^2)5 + 3k5^2 + 5k) + 150 \\ &= 8(8^2k^3 + 3(8k^2)5 + 3k5^2 + 5k + 18) + 6. \end{aligned}$$

Thus $n^3 + 5n = 8q + 6$, where $q = 8^2k^3 + 3(8k^2)5 + 3k5^2 + 5k + 18$. Therefore (Theorem 2 again!) the remainder of the division of $n^3 + 5n$ by 8 is 6.

Example 7. Prove that $M = m(m + 1)(2m + 1)$ is divisible by 6 for all integers m.

Proof. By the Division with Remainder Theorem, $m = 6k + r$, where k is an integer and r is an element of the set $\{0, 1, 2, 3, 4, 5\}$. Let us evaluate M for each possible value of r.

If $r = 0$, then $M = 6k(6k + 1)(12k + 1)$.
If $r = 1$, then $M = (6k + 1)(6k + 2)(12k + 3) = 6(6k + 1)(3k + 1)(4k + 1)$.
If $r = 2$, then $M = (6k + 2)(6k + 3)(12k + 5) = 6(3k + 1)(2k + 1)(12k + 5)$.
If $r = 3$, then $M = (6k + 3)(6k + 4)(12k + 7) = 6(2k + 1)(3k + 2)(12k + 7)$.
If $r = 4$, then $M = (6k + 4)(6k + 5)(12k + 9) = 6(3k + 2)(6k + 5)(4k + 3)$.
If $r = 5$, then $M = (6k + 5)(6k + 6)(12k + 11) = 6(6k + 5)(k + 1)(12k + 11)$.

As we see, in each of the cases $6|M$, and the problem is solved. □

The last example shows that concentrating on the remainders one can reduce a problem of establishing a property of *infinitely* many integers to a problem of verifying the property for *finite* number of cases. The importance of this idea is hard to overestimate. More on this will be presented in the next section.

Exercise Set 2

1. When n is divided by 9, the remainder is 5. What is the remainder of the division of $n(n^2+7n-2)$ by 9?
2. Prove that $m(m^2+5)$ is divisible by 6 for all integers m.
3. Prove that if both a and b divided by n give remainders 1, then ab divided by n gives remainder 1. Use the method of mathematical induction to prove a similar result for any $k \geq 2$ integers.
4. Prove that for all $n \in \mathbb{N}$, 15^n divided by 7 gives remainder 1.
5. Prove that the product of
   (i) two consecutive integers is always divisible by 2;
   (ii) three consecutive integers is always divisible by 3;
   (iii) five consecutive integers is always divisible by 5;
   (iv) Generalize the statements (i) – (iii). You do not have to prove your generalization.
6. Prove that the difference of squares of two consecutive odd integers is always divisible by 8.

---

7. (i) Show that a square of an integer cannot give the remainder 2 when divided by 3, i.e., $n^2 \neq 3k+2$ for any integers n, k.
   (ii) Prove that if $3|(a^2+b^2)$ for some integers a and b, then $3|a$ and $3|b$. (Hint: use part (i).)
   (iii) Prove that in a right triangle with integer side lengths, the length of at least one leg must be divisible by 3.
8. Explain the following "faster" way of squaring the integers ending with digit 5: Let $N = \overline{a5}$ where a is the number formed by the all the digits of N but 5. Then N^2 can be obtained by multiplying a by $a+1$ and attaching 25 at the end of the product.

   For example: $35^2 = 1{,}225$ can be computed by multiplying 3 ($= a$) by 4 ($= a+1$) and attaching 25 to 12; $235^2 = 55{,}225$ can be computed by multiplying 23 ($= a$) by 24 ($= a+1$) and attaching 25 to 552.
9. Prove that among any $n+1$ integers, $n \in \mathbb{N}$, there are at least two whose difference is divisible by n. (Hint: think about the remainders these integers give when divided by n.)

---

10. Let a, b, c be the measures of three sides of a right triangle and a, b, c be integers. Prove that one of the numbers a, b, c is divisible by 5.
11. Prove that at least one of the last two digits of a square of an integer is even. (Is 234345456567439 a perfect square?)
12. Prove that when the process of long division is used for 2 integers, say m and n, then the resulting decimal fraction is always a repeating one, i.e.

$$\begin{aligned}\frac{m}{n} &= a_n a_{n-1} \dots a_1 a_0 \,.\, b_1 \dots b_k c_1 \dots c_p c_1 \dots c_p c_1 \dots c_p \dots \\ &= a_n a_{n-1} \dots a_1 a_0 \,.\, b_1 \dots b_k (c_1 \dots c_p).\end{aligned}$$

Here a_i's represent digits of the integer part of the fraction, b_j's represent digits which appear after the decimal point and which precede the repeating string of digits, and c_k's are the digits which form the repeating string of digits $c_1 \dots c_p$, called a *period* of the

decimal fraction. Here the finite decimal fractions are viewed as infinite with 0 repeated. For example: $20/7 = 2.857142857142\ldots = 2.(857142)$ (a period is 857142), $74/8 = 9.25000\ldots = 9.25(0) = 9.25$ (a period is 0), $-1127/90 = -12.5222\ldots = -12.5(2)$ (a period is 2).

Prove that the number p of digits in a period is never greater than $|n| - 1$.

3. Congruences

Please look again over Example 7. What becomes clear is that often, when divisibility of integers is discussed, the answer depends not on the actual integers involved but on the remainders they produce when divided by a given number. This phenomenon is captured well through the definition of a congruence, introduced by K.F. Gauss (1777–1855). The language of congruences has proven to be a very convenient in number theory and its applications. The goal of this section is to learn it.

For a positive integer m, two integers a and b are called **congruent modulo** m, written $a \equiv b \pmod{m}$, if a and b give equal remainders when divided by m. For example, $16 \equiv 6 \pmod 5$, $16 \equiv -9 \pmod 5$, $35 \equiv 0 \pmod 7$, every two integers are congruent modulo 1.

The following statement collects most properties of the congruences we will be concerned with.

Theorem 3. *For any modulus $m \in \mathbb{N}$, and all integers a, b, c, d, x, n, $n \geq 2$,*

(i) $a \equiv a \pmod m$ *(reflexive property)*
(ii) $a \equiv b \pmod m \iff b \equiv a \pmod m$ *(symmetric property)*
(iii) *If* $a \equiv b \pmod m$ *and* $b \equiv c \pmod m$, *then* $a \equiv c \pmod m$ *(transitive property)*
(iv) $a \equiv b \pmod m \iff m|(a-b) \iff a = mt + b$ for some t
(v) *If* $a \equiv b \pmod m$ *and* $c \equiv d \pmod m$, *then* $a + c \equiv b + d \pmod m$ *and* $a - c \equiv b - d \pmod m$
(vi) *If* $a \equiv b \pmod m$, *and* $c \equiv d \pmod m$, *then* $ac \equiv bd \pmod m$. *In particular,* $ac \equiv bc \pmod m$.
(vii) *If* $a \equiv b \pmod m$, *then* $a^n \equiv b^n \pmod m$
(viii) *If* $a \equiv r \pmod m$ *and* $0 \leq r < m$, *then* r *is the remainder of the division of* a *by* m.

As we see, some of the properties of congruences remind us the corresponding properties of equalities. In particular, congruences by the same modulus can be added, subtracted, multiplied, and both sides of a congruence can be raised to the same power.

Proof. Properties (i),(ii) and (iii) follow immediately from the definition of congruences.

(iv) $a \equiv b \pmod m$ means that a and b give the same remainder, call it r, when divided by m. Let $a = mq_1 + r$ and $b = mq_2 + r$. Then $a - b = (q_1 - q_2)m$, and, since $q_1 - q_2$ is an integer, $m|(a-b)$. Thus we have shown that $a \equiv b \pmod m \implies m|(a-b)$. To prove the converse, i.e., $m|(a-b) \implies a \equiv b$

(mod m), we divide a and b by m with remainders. Let $a = q_1m + r_1$ and $b = q_2m + r_2$, where $0 \leq r_1, r_2 < m$. Then $a - b = (q_1 - q_2)m + (r_1 - r_2)$. Since $m|(a-b)$, then $m|[(a-b)-(q_1-q_2)m] = r_1-r_2$, (by Theorem 1 (iii)). So $m|(r_1 - r_2)$. But $-(m-1) \leq r_1 - r_2 \leq m-1$, since $0 \leq r_1, r_2 < m$. The only integer in $\{-(m-1), -(m-2), \ldots, 0, \ldots, m-2, m-1\}$ divisible by m is 0. So $r_1 - r_2 = 0$, hence $r_1 = r_2$. But this means that $a \equiv b \pmod{m}$, and the proof of the first equivalence is finished. The second equivalence is obvious. □

The statement (iv) provides an equivalent definition of the congruences, namely that two integers are called congruent by module m if their difference is divisible by m. The equivalence of the two definitions is very useful. We apply it heavily in the following proofs of (v)–(viii).

(v) By (iv) ($\Longrightarrow$ direction), $a - b = q_1m$ and $c - d = q_2m$, for some integers q_1, q_2. Then $(a+c)-(b+d) = (a-b)+(c-d) = q_1m+q_2m = (q_1+q_2)m$, and therefore $m|[(a+c)-(b+d)]$. By (iv) ($\Longleftarrow$ direction), $a + c \equiv b + d \pmod{m}$, and the proof is finished. The case $a - c \equiv b - d \pmod{m}$ can be proven in absolutely similar way and is left to the reader. □

(vi) By (iv), it is sufficient to show that $m|(ac-bd)$. We use a trick of rewriting $ac - bd$ as $(a - b)c + b(c - d)$. By (iv) again, $m|(a - b)$ and $m|(c - d)$. Therefore (by Theorem 1 (iv)) $m|(a - b)c + b(c - d) = ac - bd$, and the proof is finished. The second statement follows, since, due to (i), $x \equiv x \pmod{m}$. □

(vii) Perhaps, the shortest way to proceed is by induction. For $n = 2$ the statement follows from (vi): take $a = c$ and $b = d$. Suppose the statement is proven for $n = k \geq 2$, i.e., $a^k \equiv b^k \pmod{m}$. We want to show that it is correct for $n = k + 1$, i.e., that $a^{k+1} \equiv b^{k+1} \pmod{m}$. This follows immediately from (vi) if we multiply two congruences: $a^k \equiv b^k \pmod{m}$ (which is correct by the inductive hypothesis) and $a \equiv b \pmod{m}$ (given). □

Another proof could be obtained by using the formula $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$. Since $m|(a - b)$, then $m|(a^n - b^n)$, and, by (iv), $a^n \equiv b^n \pmod{m}$. □

(viii) By (iv), $m|(a-r)$, hence $a - r = qm$ for some q. So $a = qm + r$. Since $0 \leq r < m$, the statement follows from the Division with Remainder Theorem. □

Several immediate illustrations of the theorem follows.

- $17 \equiv -533 \pmod{10}$, since $17 - (-533) = 550$, which is divisible by 10 (here we used property (iv).)
- To find the remainder of the division of the product $32517 \cdot 5328$ by 14, we can first divide each factor by 14 with remainder, then multiply the obtained remainders, and then divide their product by 14. Using congruences, this can be written as: $32517 \equiv 9 \pmod{14}$, $5328 \equiv 8 \pmod{14}$, and

$$32517 \cdot 5328 \equiv 9 \cdot 8 = 72 \equiv 2 \pmod{14}$$

(here we used (vi) and (viii)).
- Since $2^4 = 16 \equiv 1 \pmod{15}$, then $2^{1000} = (2^4)^{250} \equiv 1^{250} = 1 \pmod{15}$. Since $0 \leq 1 < 15$, 1 is the remainder of the division of 2^{1000} by 15. (Here

we used mainly properties (vii) and (viii). But (i) and (iii) were used too! Do you see where?)

- Since $128 \equiv 30 \pmod{14}$, then $98 = 128 - 30 \equiv 0 \pmod{14}$. Indeed, here we used that $30 \equiv 30 \pmod{14}$ (by (i)), then subtracted this congruence from the original one (used (v)).

Example 8. What is the remainder of the division of $N = 375 \cdot 2^{100} - 35^{87}$ by 6 ?

Solution. Here we stop writing the references to the parts of Theorem 3, but we do use them constantly. All congruences below are modulo 6. We have: $375 \equiv 3 \pmod{6}$, $2^{100} = (2^5)^{20} = 32^{20} \equiv 2^{20} = (2^5)^4 = 32^4 \equiv 2^4 = 16 \equiv 4 \pmod{6}$. Also, since $35 \equiv -1 \pmod{6}$, then $35^{87} \equiv (-1)^{87} = -1 \pmod{6}$. Therefore $N = 375 \cdot 2^{100} - 35^{87} \equiv 3 \cdot 4 - (-1) = 13 \equiv 1 \pmod{6}$. Since $0 \leq 1 < 6$, the remainder of the division of N by 6 is 1.

Example 9. In this example we rewrite the solutions of the problems from Examples 6 and 7. The advantages of the new language become apparent.

- *When n is divided by 8, the remainder is 5. What is the remainder of the division of $n^3 + 5n$ by 8?*

Solution. Since $n \equiv 5 \pmod{8}$, then $n^3 \equiv 5^3 = 25 \cdot 5 \equiv 1 \cdot 5 = 5 \pmod{8}$, $5n \equiv 5 \cdot 5 = 25 \equiv 1 \pmod{8}$. Adding we get $n^3 + 5n \equiv 5 + 1 = 6 \pmod{8}$. Therefore the remainder is 6. A shorter presentation could be just one line

$$n^3 + 5n \equiv 5^3 + 5 \cdot 5 = 5^2(5 + 1) = 25 \cdot 6 \equiv 1 \cdot 6 = 6 \pmod{8}.$$

- *Prove that $M = m(m + 1)(2m + 1)$ is divisible by 6 for all integers m.*

Solution. The integer m is congruent by mod 6 to one and only one of the numbers $\{0, 1, 2, 3, 4, 5\}$. All congruences below are by mod 6.

If $m \equiv 0$, then $M \equiv 0 \cdot 1 \cdot 1 = 0$; if $m \equiv 1$, then $M \equiv 1 \cdot 2 \cdot 3 = 6 \equiv 0$; if $m \equiv 2$, then $M \equiv 2 \cdot 3 \cdot 5 = 6 \cdot 5 \equiv 0$; if $m \equiv 3$, then $M \equiv 3 \cdot 4 \cdot 7 = 12 \cdot 7 \equiv 0$;
if $m \equiv 4$, then $M \equiv 4 \cdot 5 \cdot 9 = 36 \cdot 5 \equiv 0$; if $m \equiv 5$, then $M \equiv 5 \cdot 6 \cdot 5 \equiv 0$.

As we see, in each case $M \equiv 0 \pmod{6}$ and so $6|M$.

Another illustration of the use of congruences is provided by the well–known rules for the divisibility of a number by 3,4,8,9,11. The statements of the following theorem are actually stronger, and the divisibility rules follow from them immediately.

Theorem 4. *Let $N = \overline{a_{n-1} \dots a_1 a_0}$ be an n–digit positive integer, where a_0 is the number of units, a_1 be the number of tens, and so on. Then*

(i) $N \equiv a_0 + a_1 + \cdots + a_{n-1} \pmod{3}$
(ii) $N \equiv a_0 + a_1 + \cdots + a_{n-1} \pmod{9}$
(iii) $N \equiv a_0 - a_1 + \cdots + (-1)^{n-1} a_{n-1} \pmod{11}$
(iv) $N \equiv \overline{a_1 a_0} \pmod{4}$, *where $\overline{a_1 a_0}$ is the number formed by two last digits of N*
(v) $N \equiv \overline{a_2 a_1 a_0} \pmod{8}$, *where $\overline{a_2 a_1 a_0}$ is the number formed by three last digits of N*

Thus

$254361 \equiv 2+5+4+3+6+1 \equiv 2+2+1+0+0+1 = 6 \equiv 0 \pmod 3$, and so $3|254361$;

$254361 \equiv 2+5+4+3+6+1 \equiv 3 \pmod 9$, so 254361 divided by 9 gives remainder 3;

$254361 \equiv -2+5-4+3-6+1 \equiv -3 \equiv 8 \pmod{11}$, so 254361 divided by 11 gives remainder 8;

$123356 \equiv 56 \equiv 0 \pmod 4$, so $4|123356$;

$123356 \equiv 356 \equiv 4 \pmod 8$, so 12356 divided by 8 gives remainder 4.

Proof.

(i) If $a_0, a_1, \ldots, a_{n-1}$ are digits of N, then $N = a_{n-1}10^{n-1} + a_{n-2}10^{n-2} + \cdots + 10a_1 + a_0$. But $1 \equiv 10 \equiv 10^2 \equiv \ldots \equiv 10^{n-1} \pmod 3$. Hence $N \equiv a_0 + a_1 + \cdots + a_{n-1} \pmod 3$. □

(ii) The proof is exactly the same as in (i). □

(iii) $10 \equiv -1 \pmod{11}$. So $-1 \equiv 10 \equiv 10^3 \equiv 10^5 \equiv \ldots \pmod{11}$ and $1 \equiv 10^2 \equiv 10^4 \equiv 10^6 \equiv \ldots \pmod{11}$. Therefore $N = a_{n-1}10^{n-1} + a_{n-2}10^{n-2} + \cdots + 10a_1 + a_0 \equiv a_0 - a_1 + \cdots + (-1)^{n-1}a_{n-1} \pmod{11}$. □

(iv) $N = a_{n-1}10^{n-1} + a_{n-2}10^{n-2} + \cdots + 10a_1 + a_0 = 100(a_{n-1}10^{n-3} + a_{n-2}10^{n-4} + \cdots + a_2) + (10a_1 + a_0) \equiv 10a_1 + a_0 = \overline{a_1a_0} \pmod 4$. □

(v) Left to the reader. □

Exercise Set 3

1. Write the solutions of Problems 1–7 of Exercise Set 2 by using congruences.
2. Use congruences to to prove that for all positive integers n, $5|(n^5 - n)$ (the problem already appeared as 6(a) in Exercise Set 1).
3. (a) What is the last digit of the number 3^{100}?
   (b) By finding the last digit of the number $9^{1972} - 7^{1972}$, prove that it is divisible by 10.
   (*Hint*: the last digit of the number is the remainder of the division of the number by 10.)
4. Form the converse statements for (v)–(vii) of Theorem 3. By giving counterexamples, prove that all of them are false.
5. Prove part (v) of Theorem 4.

---

6. Find the remainder of the division of 37^{1992} by 17.
7. Find the last two digits of the number 37^{1992}.
   (*Hint*: the 2–digit number formed by the last two digits of a number is the remainder of the division of the number by 100.)
8. Prove that the sum of squares of three integers cannot give remainder 7 when divided by 8. Are there three integers x, y, z such that $x^2+y^2+z^2 = 23654009839$?

---

9. Are there integers x, y, z such that $x^3 + y^3 + z^3 = 1234567894$?
   (*Hint*: Think about the corresponding congruence modulo 9.)

10. Let A be an arbitrary 1972–digit number divisible by 9. Let a be the sum of digits of A, b be the sum of digits of a and c be the sum of digits of b. Prove that the value of c is the same for every A and find it.

4. GCD and the Euclidean Algorithm

Given two integers a and b, any integer d which divides both of them is called a **common divisor** of a and b. If $a = b = 0$, then any nonzero number d is their common divisor, and the set of all common divisors is infinite. If at least one of a or b is not zero, say $b \neq 0$, then the set of common divisors is finite, since by Theorem 1 (vi), for every divisor d of b, $|d| \leq |b|$. In what follows we will always assume $b \neq 0$. For example, the set of common divisors of 12 and 30 is $\{\pm 1, \pm 2, \pm 3, \pm 6\}$, and the set of common divisors of 0 and -8 is $\{\pm 1, \pm 2, \pm 4, \pm 8\}$. It turns out, and it will be proven below, that among common divisors of a and b there will always be two which are divisible by each of their common divisors. In the examples above they are ± 6 and ± 8, respectively. Concentrating on positive ones we make the following definition: given $a, b \in \mathbb{Z}$, $b \neq 0$, the **greatest common divisor** of a and b, denoted $\gcd(\mathbf{a}, \mathbf{b})$, is a positive common divisor of a and b which is divisible by each of their common divisors. We will see that the concept of the gcd is very useful, and it will allow us to discover many deep properties of integers.

Just a few comments before we proceed. First it has to be proven that the $\gcd(a, b)$ exists, and we do it in Theorem 5. Next, one can wonder why we did not define the $\gcd(a, b)$ simply as the greatest (in terms of magnitude) common divisor of a and b, since the existence of such is obvious. Indeed, it can be shown, that this definition would be equivalent to ours, but a proof of the equivalence will be comparable in difficulty with the one of Theorem 5. The real reason for choosing the definition we suggested lies outside the scope of this course: it is easier to generalize it to many algebraic systems other then $\mathbb{Z}$, e.g. to polynomials, where the concept of the gcd plays as important role as it does in $\mathbb{Z}$.

The following procedure allows both to prove the existence of the gcd, and gives an effective method to compute it. It goes back to Euclid's ($365 \sim 300$ B.C.) *Elements* (Book VII, Prop. 2), and is often called the **Euclidean Algorithm**. With no exaggeration, it is considered as one of the most fruitful ideas in mathematics. Here it is.

- Divide a by b with remainder: $a = q_1 b + r_1$. If $r_1 = 0$, i.e., $b|a$, then set $d = |b|$, and stop. Else
- divide b by r_1 with remainder: $b = q_2 r_1 + r_2$. If $r_2 = 0$, i.e., $r_1|b$, then set $d = r_1$, and stop. Else
- divide r_1 by r_2 with remainder: $r_1 = q_3 r_2 + r_3$. If $r_3 = 0$, i.e., $r_2|r_1$, then set $d = r_2$, and stop. Else, and so on.

Since we have $|b| > r_1 > r_2 > \ldots \geq 0$, the algorithm has to terminate, otherwise it would produce an *infinite decreasing sequence of non–negative integers*(!) The latter is impossible, since the set of members of such a sequence would violate the Well–Ordering Axiom. Let the algorithm take n divisions to terminate, i.e., $r_n = 0$, $n \geq 1$. Thus we have:

$$
\begin{aligned}
a &= q_1 b + r_1, \\
b &= q_2 r_1 + r_2, \\
&\cdots\cdots\cdots \\
r_{n-4} &= q_{n-2} r_{n-3} + r_{n-2}, \\
r_{n-3} &= q_{n-1} r_{n-2} + \mathbf{r_{n-1}}, \\
r_{n-2} &= q_n \mathbf{r_{n-1}}.
\end{aligned} \tag{4.1, 4.2}
$$

Then $d = |b|$ if $n = 1$, and $d = r_{n-1}$ if $n > 1$. We claim that $d = \gcd(a, b)$. In order to prove this we have to show that

(i) (i) $d > 0$ and is a common divisor of a and b, and
(ii) (ii) d is divisible by any common divisor of a and b.

If $n = 1$, then $b|a$. Since $b|b$, then d $(= |b|)$ is a common divisor of a and b, and (i) is checked. If c is a common divisor of a and b, then it is a divisor of d $(= |b|)$. Thus (ii) is checked, and $d = \gcd(a, b)$ in this case.
If $n > 1$, then $r_n = 0$, $d = r_{n-1}$, and $r_{n-1}|r_{n-2}$ (for $n = 2$, define $r_0 = a$). Since $r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}$, then $r_{n-1}|r_{n-3}$. Since $r_{n-4} = q_{n-2} r_{n-3} + r_{n-2}$, and r_{n-1} divides both r_{n-2} and r_{n-3}, then $r_{n-1}|r_{n-4}$. "Moving up" in the table, we eventually obtain that d $(= r_{n-1})$ divides b, and then that d divides a, and therefore (i) is checked.
Let c be a common divisor of a and b. Then from the first equation, $c|r_1 = a - q_1 b$. Dividing b and r_1, $c|r_2 = b - q_2 r_1$. Dividing r_1 and r_2, $c|r_3 = r_1 - q_3 r_2$. "Moving down" in the table, we eventually obtain $c|r_{n-2}$, and then that $c|r_{n-1} = d$. Hence (ii) is checked, and $d = \gcd(a, b)$ in this case.

Therefore we proved the following

Theorem 5. *Let $a, b \in \mathbb{Z}$ and $b \neq 0$. Then the greatest common divisor of a and b exists and can be found by the Euclidean Algorithm.*

Example 10. Using the Euclidean Algorithm, find the $\gcd(78, 32)$.

Solution.

Applying the Euclidean Algorithm, we get:

$$
\begin{aligned}
78 &= 2 \cdot 32 + 14, \\
32 &= 2 \cdot 14 + 4, \\
14 &= 3 \cdot 4 + \mathbf{2}, \\
4 &= 2 \cdot \mathbf{2}.
\end{aligned} \tag{4.3}
$$

Therefore the $\gcd(78, 32) = 2$.

For $a, b \in \mathbb{Z}$ any number of the form $xa + yb$, $x, y \in \mathbb{Z}$ is called a **linear combination** of a and b. For example, $4 \cdot 7 + 10 \cdot (-3) = -2$ is a linear combination of 7 and -3 (or of 4 and 10, since $7 \cdot 4 + (-3) \cdot 10 = 4 \cdot 7 + 10 \cdot (-3)$); 7 is a linear combination of 23 and -8, since $7 = 1 \cdot 23 + 2 \cdot (-8)$; 5 is a linear combination of 5 and 18, since $5 = 1 \cdot 5 + 0 \cdot 18$; $0 = 0 \cdot a + 0 \cdot b$ is a linear combination of any two

numbers a and b. Let us denote the set of all linear combinations of a and b by $L_{a,b}$, i.e., $L_{a,b} = \{xa + yb : x, y \in \mathbb{Z}.\}$. Thus $-2 \in L_{4,10}$, $7 \in L_{23,-8}$, $5 \in L_{5,18}$.

Let $n\mathbb{Z} = \{nt \ : t \in \mathbb{Z}\}$ denote the set of all multiples of n. The following theorem uncovers important relations between the greatest common divisor of a and b and the set $L_{a,b}$.

Theorem 6. *Let $a, b \in \mathbb{Z}$ and $b \neq 0$, and $d = \gcd(a, b)$. Then*

(i) *d is the smallest positive linear combination of a and b*
(ii) *$L_{a,b} = d\mathbb{Z}$*

Before proceeding with a proof we illustrate (i) by an example. Suppose we want to show that $2 = \gcd(78, 32)$ is a linear combination of 78 and 32.

From the third equality of (4.3), $2 = 14 + 4 \cdot (-3)$. So 2 is a linear combination of 14 and 4. Solving the second equality of (4.3) for 4 and substituting the result in $2 = 14 + 4 \cdot (-3)$, we get $2 = 14 + (32 + 14 \cdot (-2)) \cdot (-3) = 32 \cdot (-3) + 14 \cdot 7$. So 2 is a linear combination of 32 and 14. Solving the first equality of (4.2) for 14 and substituting the result in $2 = 32 \cdot (-3) + 14 \cdot 7$, we get $2 = 32 \cdot (-3) + (78 + 32 \cdot (-2)) \cdot 7 = 78 \cdot 7 + 32 \cdot (-17)$. So $2 = \gcd(78, 32)$ is a linear combination of 78 and 32. It is the smallest positive element of $L_{78,32}$, since each element of $L_{78,32}$ is divisible by 2.

Proof.

(i) First we show that $d \in L_{a,b}$. By theorem 5, $d = r_{n-1}$. From the $(n-1)$st division with remainder in the Euclidean algorithm (4.1), we obtain

$$d = r_{n-1} = r_{n-3} - q_{n-1}r_{n-2} = r_{n-3} \cdot 1 + r_{n-2}(-q_{n-1}),$$

so d is a linear combination of r_{n-3} and r_{n-2}. Expressing r_{n-2} from the $(n-2)$nd division of (4.1), and substituting it above we get

$$\begin{aligned} d = r_{n-1} &= r_{n-3} \cdot 1 + (r_{n-4} - q_{n-2}r_{n-3})(-q_{n-1}) \\ &= r_{n-3}(1 + q_{n-1}q_{n-2}) + r_{n-4}(-q_{n-1}), \end{aligned}$$

so d is a linear combination of r_{n-4} and r_{n-3}. Expressing r_{n-3} from the $(n-3)$rd division of (4.1), and substituting it above we get that d is a linear combination of r_{n-5} and r_{n-4}, and so on. "Moving up " this way we eventually obtain that d is a linear combination of a and b. It must be the smallest positive one, since d divides each element of $L_{a,b}$ (Theorem 1 (iv)). □

(ii) Since d divides both a and b, it divides every element of $L_{a,b}$, then $L_{a,b} \subseteq d\mathbb{Z}$. Since $d \in L_{a,b}$ (by (i)), then $d = ua + vb$ for some u and v. Therefore any multiple of d is again a linear combination of a and b: $dt = (ut)a + (vt)b \in L_{a,b}$. Hence $d\mathbb{Z} \subseteq L_{a,b}$. Having both inclusions we conclude that $L_{a,b} = d\mathbb{Z}$. □

As we can see from the example and the proof above, integers u and v in a representation $\gcd(a, b) = ua + vb$ can be computed via subsequent 'backward' substitutions of the remainders appearing in the Euclidean algorithm. For a convenient computing scheme of doing this, see Baker and Ebert [1].

We call integers a and b **relatively prime**, if $\gcd(a, b) = 1$. The latter is equivalent to 1 being a linear combination of a and b. For example, 6 and 25 are

relatively prime, or 12 and 19. As an immediate corollary from Theorem 6, we have the following very useful statement.

Corollary 1. *The following three statements are equivalent:*

(i) *a and b are relatively prime*
(ii) *1 is a linear combination of a and b*
(iii) *$L_{a,b} = \mathbb{Z}$, i.e., every integer is a linear combination of a and b.*

The following statements further illustrate the importance of the notion of relative primeness.

Theorem 7.

(i) *if $c|ab$ and $\gcd(a, c) = 1$, then $c|b$*
(ii) *if $\gcd(a, c) = \gcd(b, c) = 1$, then $\gcd(ab, c) = 1$*
(iii) *if $a|c$, $b|c$ and $\gcd(a, b) = 1$, then $ab|c$*
(iv) $\gcd(a, b) = d \iff \gcd(a/d, b/d) = 1$
(v) *if $\gcd(c, n) = 1$, then $a \equiv b \pmod{n} \iff ac \equiv bc \pmod{n}$, i.e., both sides of a congruence can be multiplied or divided by an integer relatively prime to n.*

Proof.

(i) Since $\gcd(a, c) = 1$, $1 = ax+cy$ for some integers x, y. Then $b = (ab)x+cby$. But $ab = qc$ for some integer q. Hence $b = (qc)x + cby = c(qx + by)$, which implies that $c|b$. □
(ii) Since $\gcd(a, c) = \gcd(b, c) = 1$, then $1 = ax+cy = bu+cv$ for some integers x, y, u, v. Then $1 = 1\cdot 1 = (ax+cy)(bu+cv) = (ab)(xu)+c(ybu+axv+cyv)$. Therefore $1 \in L_{ab,c}$, or $\gcd(ab, c) = 1$.
(iii) Since $a|c$, then $c = qa$ for some $q \in \mathbb{Z}$. Then $b|qa$. Since $\gcd(a, b) = 1$, then, by (i), $b|q$. Therefore $q = q_1 b$ and $c = (q_1 b)a = q_1(ab)$, which implies that $ab|c$. □
(iv) Left to the reader. □
(v) The fact that both sides of a congruence can be multiplied by an arbitrary integer was proven in Theorem 3 (vi). Therefore we just have to show that for c relatively prime to n, $ac \equiv bc \pmod{n} \iff ac - bc = (a - b)c \equiv 0 \pmod{n} \iff n|(a-b)c$. Using part (i), of this theorem, we conclude that $n|(a - b)$. This proves that $a \equiv b \pmod{n}$. □

Here are a few typical applications of Theorem 7:

- if $8|(25n)$, then $8|n$ (by (i));
- a number is divisible by both 10 and 9, if and only if it is divisible by 90 (by (iii) and Theorem 1 (ii));
- to prove that for all $n \in \mathbb{N}$, $30|(n^5 - n)$, it is sufficient to show that $n^5 - n$ is divisible by 5 and 6, or by 2, 3, and 5 (by (iii));
- $10x \equiv 35 \pmod{27}$ implies $2x \equiv 7 \pmod{27}$ (by (v)).

We know that many problems in mathematics can be solved by using linear equations with one unknown, i.e., equations which are equivalent to $ax = b$, where a and b are known real numbers, and x has to be determined. The theory of such

equations is very simple: if $a = 0$, but $b \neq 0$, there are no solutions; if $a = b = 0$, every real number is a solution; and if $a \neq 0$, then there exists a unique solution which can be found in these steps:

$$\begin{aligned} ax = b &\iff a^{-1}(ax) = a^{-1}b \\ &\iff (a^{-1}a)b = a^{-1}b \\ &\iff 1x = a^{-1}b \\ &\iff x = a^{-1}b. \end{aligned}$$

This argument uses the fact that multiplying both sides of an equation by a nonzero number we obtain an equivalent equation. Then it uses the existence of the multiplicative inverse for every nonzero real number.

A somewhat similar theory can be constructed for linear congruences, which we write as $ax \equiv b \pmod{n}$, where a, b, and n are known integers, and x denotes the unknown. For example, one can be interested in finding all integers x such that $7x \equiv 6 \pmod{12}$. Experimenting with different simple linear congruences, we can easily find examples of ones which have a solution and of ones which do not. E.g., $4x \equiv 1 \pmod{3}$ is satisfied by each $x \equiv 1 \pmod{3}$. On the other hand, $4x \equiv 1 \pmod{6}$ has no solutions: if it did, then $4x-1 = 6t$ for some integer t, or $1 = 4x-6t$, and so $2|1$, a contradiction. Thinking about solving $ax \equiv b \pmod{n}$ in general, we can try to mimic ideas used for solving linear equations. Namely, we can try to multiply both sides of it by an integer c such that the obtained congruence is equivalent to the original one, and $ca \equiv 1 \pmod{n}$. The following theorem states the important case when this is possible.

Theorem 8. *Let $ax \equiv b \pmod{n}$ be a linear congruence with respect to x and $\gcd(a, n) = 1$. Then there exists an integer c such that $ca \equiv 1 \pmod{n}$, and all solutions of the congruence can be written in the form $x \equiv cb \pmod{n}$.*

Proof. According to Corollary 1 (ii), there exist integers u and v such that $ua + vn = 1$. Let $c = u$. Then $ca = 1-vn \equiv 1 \pmod{n}$. The fact that the multiplication of both sides of $ax \equiv b \pmod{n}$ by c leads to an equivalent congruence follows from Theorem 7 (v). Therefore $ax \equiv b \pmod{n} \iff c(ax) \equiv cb \pmod{n} \iff (ca)x \equiv cb \pmod{n} \iff 1 \cdot x \equiv cb \pmod{n} \iff x \equiv cb \pmod{n}$. □

We would like to remark that number c in the above theorem is not determined uniquely, moreover there are infinitely many such c. This is because there are infinitely many u satisfying $ua + vn = 1$: for every (u, v) satisfying this equality, the pair $(u - bt, v + at)$ also satisfies the equality for every t. Nevertheless, each value of c leads to the same set of solutions of $ax \equiv b \pmod{n}$.

What can be said about the solutions of $ax \equiv b \pmod{n}$ when $\gcd(a, n) \neq 1$? The answer follows quickly from Theorem 8, see Exercise 6 at the end of this section.

Example 11.

(i) Solve $7x \equiv 5 \pmod{12}$
(ii) Find all integers x which give remainder 2 when divided by 6, and which give remainder 10 when divided by 11.

Solution.

(i) We notice that $7 \cdot 7 \equiv 1 \pmod{12}$. Multiplying both sides of the congruence by 7 we get $x \equiv 35 \equiv 11 \pmod{12}$. The answer also can be written as $\{x : \ x = 11 + 12t, t \in \mathbb{Z}\}$, or just as $\{11 + 12t, t \in \mathbb{Z}\}$.

Instead of 'noticing', we could proceed with the Euclidean Algorithm: $12 = 1 \cdot 7 + 5$, $7 = 1 \cdot 5 + 2$, $5 = 2 \cdot 2 + 1$. Therefore $1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (7 - 1 \cdot 5) = (-2) \cdot 7 + 3 \cdot 5 = (-2) \cdot 7 + 3 \cdot (12 - 1 \cdot 7) = 3 \cdot 12 + (-5) \cdot 7$. Then, like in the proof of Theorem 8, we multiply both sides of our congruence (i) by -5, and we get $-35x \equiv -25 \pmod{12}$. Since $-35 \equiv 1 \pmod{12}$, and $-25 \equiv 11 \pmod{12}$, we obtain $x \equiv 11 \pmod{12}$, i.e., the same answer.

If the modulus n is large, proceeding with the Euclidean Algorithm can be much faster than attempting to notice the number c.

(ii) We are asked to solve simultaneously two congruences: $x \equiv 2 \pmod{6}$ and $x \equiv 10 \pmod{11}$. One way to proceed is as follows. The general solution for the first congruence can be written in the form $x = 2 + 6t$, where $t \in \mathbb{Z}$. This formula describes *all* solutions of the first congruence. Therefore we can try to find those values of t for which these solutions will satisfy the second congruence as well. To do this we substitute the expression in the second congruence. We obtain: $2 + 6t \equiv 10 \pmod{11} \iff 6t \equiv 8 \pmod{11}$. The last congruence, which has t as the unknown, can be solved easily, since the $\gcd(6, 11) = 1$. Multiplying both sides by 2 we get: $6t \equiv 8 \iff 12t \equiv 16 \iff t \equiv 5 \pmod{11}$. Therefore $t = 5 + 11k$, where $k \in \mathbb{Z}$, and these are all values of t for which solutions $x = 2 + 6t$ of the first congruence are also solutions of the second one. Hence $x = 2 + 6t = 2 + 6 \cdot (5 + 11k) = 32 + 66k$, and the set $\{32 + 66k, k \in \mathbb{Z}\}$ is the solution set of the system of congruences.

Exercise Set 4

1. (i) By using Euclidean Algorithm find the $\gcd(112, 356)$.
   (ii) Describe the set of all integers c, such that the equation $112x + 356y = c$ has an integer solution (x, y).
2. Prove that:
   (i) $\gcd(n, n + 1) = 1$
   (ii) $\gcd(n, n + 2) = 1$ or 2
   (iii) $\gcd(a, b) = \gcd(a, a + b)$
   (iv) $\gcd(3n + 1, 10n + 3) = 1$.
3. The difference of two odd integers x and y is 4. Prove that x and y are relatively prime.
4. Form the converse statements for (ii) and (iii) of Theorem 7. Prove or disprove them.
5. Prove part (iv) of Theorem 7.
6. If $d = \gcd(a, n) \neq 1$, then the existence of a solution of a linear congruence $ax \equiv b \pmod{n}$ will depend on b. If $d \not| b$, then no solutions exist (it is obvious, do you see why?). If $d | b$, let $a = da_1, b = db_1$ and $n = dn_1$. Prove that $ax \equiv b \pmod{n} \iff a_1 x \equiv b_1 \pmod{n_1}$. Since $\gcd(a_1, n_1) = 1$ (Theorem 7 (iv)), we reduced the problem to the case described in Theorem 8. Therefore if $d | b$, solutions exist and can be found effectively.

7. Find the least integer $N \geq 2$ which gives remainder 1 when divided by each of the numbers 3, 4, 5, 7.
8. Find the least positive integer N such that when N divided by 3 the remainder is 2, when N divided by 4 the remainder is 3, when N divided by 5 the remainder is 4, and when N divided by 7 the remainder is 6.
9. (i) Describe the set of all integers x satisfying the following two congruences simultaneously:

$$x \equiv 3 \pmod 7, \qquad x \equiv 6 \pmod 8.$$

(ii) Describe the set of all integers x satisfying the following three congruences simultaneously:

$$x \equiv 3 \pmod 7, \qquad x \equiv 6 \pmod 8, \qquad x \equiv 2 \pmod{25}.$$

(iii) Let $a, b \in \mathbb{N}$ and $a_1, b_1 \in \mathbb{Z}$. Prove that if a, b are relatively prime, then the system of congruences

$$x \equiv a_1 \pmod a, \qquad x \equiv b_1 \pmod b$$

has a solution. This statement (as well as 9(i) of Exercise Set 5) represents a particular case of so–called Chinese Remainder Theorem.

10. Prove that for all $n \in \mathbb{N}$, $30|(n^5 - n)]$.
11. Let a, b, c be any three integers, no two of which are zero.
    (i) Suppose $d = \gcd(\gcd(a, b), c)$. Prove that $d > 0$ and divides each of the numbers a, b, c.
    (ii) Prove that d (from (i)) is divisible by any common divisor of the numbers a, b, c.
    (iii) Prove that for any three integers a, b, c, not all zeros, $\gcd(\gcd(a, b), c) = \gcd(\gcd(b, c), a) = \gcd(\gcd(a, c), b)$.

    Properties (i) and (ii) suggest to call d the greatest common divisor of numbers a, b, c, and we denote it by $\gcd(a, b, c)$. Then (iii) says that this definition does not depend on the order of the numbers.

---

12. Prove that for any positive integer n there are two integers a and b such that the Euclidean algorithm applied to a and b consists of exactly n divisions.
13. Can you give an example of an infinite sequence of integers with the property that every two its members are relatively prime? Of course, a sequence of all prime numbers will do, but we have not proven yet that there are infinitely many primes.

    Show that the sequence $a_n = 2^{2^n} + 1$, $n \geq 0$, provides such an example, i.e., prove that

$$\gcd(2^{2^m} + 1, 2^{2^n} + 1) = 1$$

for each pair of distinct non–negative integers m, n.

5. DIOPHANTINE EQUATIONS

An equation of the form $ax + by = c$, where a, b, c are given integers and x, y unknown integers, is called a **linear diophantine equation** with two unknowns. The term "diophantine" commemorates an ancient Greek mathematician Diophantus (about 250 years A.D.), who investigated integer solutions of different equations. When we refer to an equation as "diophantine" it usually means that the constants in such an equation are integers and that we are interested in integer solutions only. For example: $3x - 4y = 10$ or $x^2 + 2y^2 = z^2$, or $3^x - 2^y = 1$. For many classes of diophantine equations it is extremely hard to find all their solutions. One of the few successes in this regard is the class of linear diophantine equation.

Theorem 9. *Let $a, b, c \in \mathbb{Z}$, $b \neq 0$, and $d = \gcd(a, b)$. The equation*

$$ax + by = c \tag{5.1}$$

has a solution if and only if $d|c$. If $d|c$, then a particular solution (x_0, y_0) of (5.1) can be found by means of the Euclidean algorithm. The set of all solutions of (5.1) can be represented in the form

$$\{(x, y) \ : \ x = x_0 - \frac{b}{d}t, \ y = y_0 + \frac{a}{d}t, \ t \in \mathbb{Z}\}. \tag{5.2}$$

Proof. Equation (5.1) has a solution if and only if c is a linear combination of a and b. By Theorem 6 (ii) , it happens if and only if $d = \gcd(a, b)|c$. Let $d|c$ and $c = c'd$. Then reducing both sides of (5.1) by d, we obtain an equivalent equation

$$a'x + b'y = c', \tag{5.3}$$

where $a' = \frac{a}{d}$, $b' = \frac{b}{d}$, and, by Theorem 7(iv), $\gcd(a', b') = 1$. By using 'backward' substitutions in the Euclidean algorithm applied to a' and b', one can represent 1 as their linear combination. Say $a'u + b'v = 1$. This gives us a particular solution $(x_0, y_0) = (c'u, c'v)$ of (5.3) (or (5.1)), since $a'x_0 + b'y_0 = a'(c'u) + b'(c'v) = c'$.
Now we will describe the set of all solutions of (5.3) (or (5.1)). Let (x, y) represent one of them. Then $a'x+b'y = c'$. Since $a'x_0+b'y_0 = c'$, subtracting these equalities, we get

$$a'(x - x_0) = b'(y_0 - y).$$

Then $a'|b'(y_0 - y)$. Since $\gcd(a', b') = 1$, then, by Theorem 7 (i), $a'|(y_0 - y)$. Let $y_0 - y = a't$. Then $x - x_0 = b't$, and we obtain that every solution of (5.1) is contained in the set (5.2).

The only thing left is to check that (5.2) does not contain any "extraneous" pairs, i.e., that every element of (5.2) is a solution of (5.1). Indeed, let $x = x_0 - \frac{b}{d}s = x_0 - b's$, and $y = y_0 + \frac{a}{d}s = y_0 + a's$ for some integer s. Then $a'x + b'y = a'(x_0 - b's) + b'(y_0 + a's) = (a'x_0 + b'y_0) + (-a'b' + b'a')s = c' + 0 = c'$. Thus every element of (5.2) is a solution of (5.3), and therefore (5.2) is the solution set of (5.1). □

Example 12. Solve the diophantine equation $858x + 253y = 33$.

Solution. First we find $\gcd(858, 253)$ by using the Euclidean algorithm.

$$\begin{aligned} 858 &= 3 \cdot 253 + 99, \\ 253 &= 2 \cdot 99 + 55, \\ 99 &= 1 \cdot 55 + 44, \\ 55 &= 1 \cdot 44 + \mathbf{11}, \\ 44 &= 4 \cdot \mathbf{11}. \end{aligned} \tag{5.4}$$

Therefore the $\gcd(858, 253) = 11$. Since $33 = 3 \cdot 11$, our equation has solutions. By using 'backward' substitutions in (5.4), we get:

$$\begin{aligned} 11 &= 55 + (-1) \cdot 44 \\ &= 55 + (-1) \cdot (99 + (-1) \cdot 55) = 2 \cdot 55 + (-1) \cdot 99 \\ &= 2 \cdot (253 + (-2) \cdot 99) + (-1) \cdot 99 = 2 \cdot 253 + (-5) \cdot 99 \\ &= 2 \cdot 253 + (-5) \cdot (858 + (-3) \cdot 253) = (-5) \cdot 858 + 17 \cdot 253. \end{aligned}$$

Thus $858 \cdot (-5) + 253 \cdot 17 = 11$, and $(x_0, y_0) = (3 \cdot (-5), 3 \cdot 17) = (-15, 51)$ is a particular solution of $858x + 253y = 33$, and the general solution of the equation is

$$\{(x, y) \ : \ x = -15 - \frac{253}{11}t = -15 - 23t, \ y = 51 + \frac{858}{11}t = 51 + 78t, \ t \in \mathbb{Z}\}. \tag{5.5}$$

We would like to make two remarks.

1. When t takes values $0, 1, -1$, we get particular solutions $(-15, 51)$, $(-38, 129)$, $(8, -27)$, respectively. Note that another choice of a particular solution would change only the *form* in which the general solution is written. E.g., replacing $(-15, 51)$ by $(8, -27)$, we get

$$\{(x, y) \ : \ x = 8 - 23s, \ y = -27 + 78s, \ s \in \mathbb{Z}\}. \tag{5.6}$$

It is important to understand that the sets in (5.5) and (5.6) are equal: a pair $(-15 - 23t, \ 51 + 78t)$ from the first set appears in the second set when s takes value $t + 1$, and a pair $(8 - 23s, \ -27 + 78s)$ appears in the first set when $t = s - 1$.

2. The logic of our solution of $858x + 253y = 33$ did not follow the precise path of our solution of the general equation $ax + by = c$ in the proof of Theorem 9. Here a particular solution of the equation was found from the Euclidean algorithm applied to the original numbers a and b rather than to the reduced numbers a' and b'. We did it because we started our solution with finding the $\gcd(858, 253)$, and it would be an extra work to perform a new Euclidean algorithm for the reduced numbers 78 and 23 (even though the latter could be obtained by simple reduction of all equations of (5.4) by 11). On the other hand, if we see immediately that the original equation can be reduced, it is better to be done. Having smaller numbers we can find a particular solution sometimes simply by inspection without invoking the Euclidian algorithm at all. For example, consider a diophantine equation $100x - 40y = 360$. Reducing by 20 we get $5x - 2y = 12$. Now it is easy to notice that $(2, -1)$ is a particular solution. Since $\gcd(5, -2) = 1$, the general solution is $\{(x, y) \ ; \ x = 2 - (-2)t = 2 + 2t, \ y = -1 + 5t, \ t \in \mathbb{Z}\}$.

Example 13. Find all integer solutions of the equation $x^2 - y^2 = 115$.

Solution. We have $x^2 - yv2 = (x-y)(x+y) = 115$. Since both $x-y$ and $x+y$ are integers, the problem is reduced to solving the following 8 systems of two equations with two unknowns, where each case corresponds to factoring 115 into two factors:

$$(x-y, x+y) \in \{(1,115), (-1,-115), (5,23), (-5,-23),$$
$$(115,1), (-115,-1), (23,5), (-23,-5)\}.$$

Solving each system we find the solution set of the equation:

$$\{(58,57), (-58,-57), (14,9), (-14,-9), (58,-57),$$
$$(-58,57), (14,-9), (-14,9)\}.$$

The following observation could speed the solution: if (a,b) satisfies the equation, then so does $(-a,b), (a,-b)$, and $(-a,-b)$. Then it would be sufficient to consider only the systems $(x-y, x+y) = (1,115)$ or $(5,23)$, corresponding $x \geq y \geq 0$.

Example 14. *Prove that the equation $x^2 - 2y^2 + 8z = 3$ has no integer solutions.*

Solution. If y is even, i.e., $y = 2k$, then $x^2 = 3 - 8z + 2y^2 = 3 - 8z + 8k^2 \equiv 3 \pmod 8$. If y is odd, i.e., $y = 2k+1$, then $x^2 = 3 - 8z + 2y^2 = 3 - 8z + 8k^2 + 8k + 2 \equiv 5 \pmod 8$. Thus $x^2 \equiv 3$ or $5 \pmod 8$. But this is impossible, since squares of integers when divided by 8 give remainders 0, 4 or 1 only. Indeed, if $x \equiv 0, 1, 2, 3, 4, 5, 6, 7 \pmod 8$, then $x^2 \equiv 0, 1, 4, 1, 0, 1, 4, 1 \pmod 8$, respectively.

The reader may wonder why in the solution above we decided to pay attention to modulus 8. Let us explain it. It is clear that if a diophantine equation has a solution, then so does the corresponding congruence for an arbitrary modulus m (equal numbers are congruent for every modulus!). The contrapositive to this statement is: if there exists a positive integer m, such that a congruence modulo m has no solution, then the corresponding diophantine equation has no solution. Therefore a general approach of showing that a diophantine equation has no solutions is to find a positive integer m such that the corresponding congruence modulo m has no solutions. One may start with small moduli, like $2, 3, 4, 5, \ldots$. In Example 14 modulus 8 was the first one which worked. Sometimes the needed modulus can be found fast, sometimes it may take long. Unfortunately, the approach may not work at all. There are diophantine equations which have no integer solutions, but the corresponding congruences will have a solution for every modulus $n \geq 2$. One such example is given by the equation $(2x+1)(3x+1) = 0$. Obviously it has no integer solutions. It can be shown that the corresponding congruence $(2x+1)(3x+1) \equiv 0 \pmod n$ has a solution for every $n \geq 2$ (see exercise 9 (ii) from Exercise Set 5).

Exercise Set 5

1. Find the general solution of the following diophantine equations:
   (a) $17x + 10y = 3$
   (b) $540x - 300y = 3540$
   (c) $315x + 66y = 94$.
2. Prove that none of the following diophantine equations has a solution:
   (a) $x^2 - 5y = 3$
   (b) $2x^2 - 5y^2 = 7$.

3. Find at least three integer solutions for each of the following equations:
   (a) $x^2 + y^2 = z^2$
   (b) $x^2 - 5y^2 = 1$
   (c) $x^2 + 1 = 5y$

---

4. Prove that for every integer $c \geq 20$, the diophantine equation $7x + 4y = c$ has a solution (x, y) with both x and y being non–negative integers.
5. Find all integer solutions of the equation $2xy = x^2 + 2y$.
6. Find all integer solutions of the equation $x^3 + 91 = y^3$.
7. Let $a, b \in \mathbb{N}$ be relatively prime. Prove that the equation $ax + by = ab$ has no solution with $x, y \in \mathbb{N}$. (Can it be solved with $x, y \in \mathbb{Z}$?)

---

8. Let a and b be two positive relatively prime integers. Prove that $ab - a - b$ is the greatest integer which cannot be written as $ax + by$ with x and y being non–negative integers.
9. (i) Let $a, b, c \in \mathbb{N}$ and $a_1, b_1, c_1 \in \mathbb{Z}$. Prove that if every two of the integers a, b, c are relatively prime, then the system of congruences

   $$x \equiv a_1 \pmod{a}, \qquad x \equiv b_1 \pmod{b}, \qquad x \equiv c_1 \pmod{c}$$

   has a solution. This statement (as well as 9(iii) of Exercise Set 4) represents a particular case of so–called Chinese Remainder Theorem.
   (ii) Prove that the congruence $(2x + 1)(3x + 1) \equiv 0 \pmod{n}$ has a solution for every integer $n \geq 2$. (Obviously the corresponding equation has no integer solutions.)

6. Primes

An integer $p \neq \pm 1$ is called a **prime** number, or prime, if it divisible only by ± 1 and $\pm p$. The first nine positive primes are 2,3,5,7,11,13,17,19,23. Numbers ± 2 are the only even primes. A number different from ± 1 which is not prime is called a **composite** number, or composite. From now on to the end of the section we restrict our attention to positive integers only. The importance of primes in number theory is mainly due to the following theorem which simply claims that the primes are the ultimate material out of which the world of integers is built up.

Theorem 10. Prime Factorization Theorem. *Every integer $n \geq 2$ is prime or a product of positive primes. If n is represented as product of positive primes in two ways, then these representations differ only in order of the factors.*

Equivalently:
every integer $n \geq 2$ is prime or a product of powers of distinct positive primes with positive integer exponents:

$$n = {p_1}^{e_1} {p_2}^{e_2} \cdots {p_k}^{e_k}. \tag{6.1}$$

Assuming $p_1 < p_2 < \ldots < p_k$, such a representation is unique.

For example, $48 = 2^4 \cdot 3^1 = 3^1 \cdot 2^4$, $90 = 2 \cdot 3 \cdot 5 \cdot 3 = 3 \cdot 5 \cdot 2 \cdot 3 = 2^1 \cdot 3^2 \cdot 5^1$.

Proof. Clearly the two statements of the theorem are equivalent. We prove the first one dividing its proof into two parts: existence of prime factorization and its uniqueness.

Existence. We proceed by induction on n. For $n = 2$ is prime, thus the statement is trivial. Suppose the theorem is proven for all integers m such that $2 \leq m < n$. We want to show that it is true for $m = n$. If n is prime, then the statement is obvious. If n is not prime, then $n = ab$, where $1 < a < n$ and $1 < b < n$. By inductive hypothesis, we know that both a and b are either prime or can be written as product of distinct prime powers, and on substituting for them we get n expressed as a product of prime powers. Adding exponents of the same prime powers (if needed) we get m expressed as a product of powers of distinct primes.

For example, $60 = 6 \cdot 10 = (2 \cdot 3)(2 \cdot 5) = 2 \cdot 3 \cdot 2 \cdot 5 = 2^2 \cdot 3 \cdot 5$.

Uniqueness. In our proof of the uniqueness of prime factorization, we will use the following

Lemma 1. *If p is prime and $p|a_1 a_2 \cdots a_s$, then $p|a_i$ for some i, $1 \leq i \leq s$.*

Proof. Since p is prime, the $\gcd(p, a_i) = 1$ or p for each i. If it is p for at least one i, then p divides the corresponding a_i, and the proof is finished. If for all i, $\gcd(p, a_i) = 1$, then $\gcd(p, a_1 a_2 \cdots a_s) = 1$ (just generalize Theorem 7(ii) by induction on s). This contradicts that $p|a_1 a_2 \cdots a_s$. Therefore p divides some a_i. □

Our proof of uniqueness proceeds by induction on n again. For $n = 2$ is prime, thus the statement is trivial. Suppose the theorem is proven for all integers m such that $2 \leq m < n$. We want to show that it is true for $m = n$. If n is prime, there is nothing to prove. If n is not prime, let

$$n = p_1 \cdots p_k = q_1 \cdots q_t$$

be two representations of n as product of primes (not necessarily distinct). We want to show that $k = t$ and, after a proper rearrangement if necessary, $p_i = q_i$ for all $i = 1, \ldots, k$. Since p_1 is prime dividing $q_1 \cdots q_t$, then, by Lemma 1, $p_1|q_i$ for some i, $1 \leq i \leq k$. Since q_i is also a positive prime, then $p_1 = q_i$. Relabelling q's if necessary, we may assume that $p_1 = q_1$. Thus we have

$$n = p_1 p_2 \cdots p_k = p_1 q_2 \cdots q_t$$

Dividing by p_1, we get $n/p_1 = p_2 \cdots p_k = q_2 \cdots q_t < n$. By inductive hypothesis, n/p_1 is prime or product of primes, such representation is unique up to the order of primes. So $k = t$, and, after a rearrangement if necessary, $p_i = q_i$ for all $i = 2, \ldots, k$. Multiplying both sides of $p_2 \cdots p_k = q_2 \cdots q_k$ by p_1, we prove the uniqueness statement for n. □

Corollary 2. *Let $n = {p_1}^{e_1} {p_2}^{e_2} \cdots {p_k}^{e_k}$, $e_i \geq 1$, $i = 1, 2, \ldots, k$. Then $m|n \iff m = {p_1}^{l_1} {p_2}^{l_2} \cdots {p_k}^{l_k}$, where $0 \leq l_i \leq e_i$, $i = 1, 2, \ldots, k$.*

Proof. If $m|n$, then $n = {p_1}^{e_1}{p_2}^{e_2}\cdots{p_k}^{e_k} = qm$ for some integer q. If either one of prime factorizations of q or m contains a power of a positive prime distinct from each p_i, or if it contains a power of p_i with the exponent greater than e_i, then it will violate the uniqueness of prime factorization of n. This proves the $\Longrightarrow$ part. The converse statement is obvious: $n = ({p_1}^{e_1-l_1}{p_2}^{e_2-l_2}\cdots{p_k}^{e_k-l_k})\cdot({p_1}^{l_1}{p_2}^{l_2}\cdots{p_k}^{l_k}) = ({p_1}^{e_1-l_1}{p_2}^{e_2-l_2}\cdots{p_k}^{e_k-l_k})\cdot m$. Since, for every i, $1 \le i \le k$, $e_i - l_i \ge 0$, then $m|n$. □

Thus $3^2\cdot 17|2\cdot 3^3\cdot 5\cdot 17^2$, and when we say that neither 11 nor 34 divides $2\cdot 33\cdot 5\cdot 172$, we actually use the contrapositive to part $\Longrightarrow$ of Corollary 6.3.

Example 15. *Prove that the only integers satisfying the diophantine equation* $n^2 = 2m^2$*, are* $m = n = 0$*.*

Proof. Clearly $(m, n) = (0, 0)$ is a solution. Suppose $m \neq 0$. Then $n \neq 0$. Every prime power in prime factorizations of both n^2 and m^2 has an even exponent. Consider the exponents of 2 in prime factorizations of n^2 and $2m^2$. Whatever they are, the first is even and the second is odd. This contradicts the uniqueness of prime factorization. Thus $m \neq 0$ is not possible, which ends the proof. □

Remark. The definitions of factors and primes involve solely the operation of multiplication, and have no references to that of addition. The same is true about our proof of the existence of prime factorization. At the first glance it may look that the proof of the uniqueness is also independent on the addition operation. This is not the case, since we used Lemma 1 whose proof depended on the Euclidean algorithm. The latter is clearly inseparable from the addition of integers. There are proofs of Theorem 10 which do not use the Euclidean algorithm, but all of them use the additive properties of $\mathbb{Z}$. Therefore one can ask a question: is it possible to prove Prime Factorization Theorem by using the multiplicative properties of integers *only*? It turns out that no such proof can ever be found, i.e., it is not a matter of our cleverness, but the intrinsic property of integers!

How can one prove a statement like this? The following ingenious argument belongs to D. Hilbert (1862 - 1943).

Consider the set S of all positive integers congruent to 1 modulo 4:

$$S = \{1, 5, 9, 13, 17, 21, 25, 29, \dots\}$$

Multiplying any two numbers from S, we get another number from S (Theorem 3(vi)). Call a number from S a pseudo–prime if it is different from 1 and is not a product of two smaller numbers from S. For example, numbers $5, 9, 13, 17, 21, 29, 33, 49$ are all pseudo–primes, but not 25 ($= 5\cdot 5$), or 45 ($= 5\cdot 9$), or 117 ($= 9\cdot 13$). It is true that every number from S is either a pseudo–prime of can be factored into pseudo–primes, and this can be proved in just the same way as in Theorem 10. But it is not true that the factorization is unique! For example, number $441 = 21\cdot 21 = 9\cdot 49$, and both factorizations use pseudo–primes only and are distinct.

On the other hand the axioms of the multiplication operations on S and $\mathbb{Z}$ are the same, namely: each set is closed under multiplication (i.e., the products of any two elements of a set is an element of the set), both multiplications are commutative, associative and each set contains a multiplicative identity (number 1). At the same time the prime factorization is unique in $\mathbb{N}$ (or $\mathbb{Z}$), but not in S. This argument

shows that a proof of uniqueness can not be based solely on multiplicative axioms of integers.

Let us now consider some other interesting properties of primes. Trying to continue the sequence of positive primes we will experience that the frequency of their appearance decreases with grows. For example, there are 25 primes among $\{1, 2, 3, \ldots, 100\}$, but only 16 primes among $\{1001, 1002, \ldots, 1100\}$, and only 6 primes among $\{100001, 100002, \ldots, 100100\}$. One may start wondering whether we will eventually exhaust all of them. This will never happen! The following proof goes back to Euclid's *Elements* (Book IX, Prop. 20). It is often used as an example of the incredible power of mathematical thinking, in particular, of the method of a proof by contradiction.

Theorem 11. *There are infinitely many prime numbers.*

Proof. By the method of contradiction. Suppose the statement is false, i.e., there are only finitely many primes, say n. Then we can write all of them in the following finite sequence

$$2 = p_1 < 3 = p_2 < \ldots < p_n.$$

Consider a number $N = p_1 p_2 \cdots p_n + 1$. Since $N > p_n$, N is not in the sequence, and therefore it is composite. But any composite number is divisible by a prime due to Theorem 10. Since all primes are listed in the sequence, there exists i, $1 \leq i \leq n$, such that $p_i | N$. On the other hand, $N = qp_i + 1$, where q is the product of all primes but p_i, i.e., N divided by p_i gives remainder 1. The source of the obtained contradiction is our assumption that there are finitely many primes. Therefore the set of primes is infinite. □

Is there any pattern in the distribution of primes?

The following theorems provide some answers.

Theorem 12. *For any $n \in \mathbb{N}$, there exist n consecutive composite integers.*

Proof. The meaning of the theorem is that the "gaps" between two consecutive primes can be as large as we wish. For example, there is a set of a billion consecutive integers with no prime among them. The proof of the theorem is very easy. Consider the following n consecutive integers:

$$(n+1)! + 2, (n+1)! + 3, (n+1)! + 4, \ldots, (n+1)! + (n+1).$$

Since $(n+1)! = 1 \cdot 2 \cdot 3 \cdots n \cdot (n+1)$, the first number is divisible by 2, the second by 3, and so on, the last by $n+1$. Since all number are greater than $n+1$, all of them are composite. □

Note that we did not claim that the set exhibited in the proof above was the first segment of integers with the property. It is easy to see that the sequence

$$P + 2, P + 3, P + 4, \ldots, P + (n+1),$$

where P is just a product of primes not exceeding $n+1$, also consists of n composite numbers, and they are much smaller than the ones above. For example , taking

$P = 2 \cdot 3 \cdot 5 \cdot 7 = 210$, we get 10 consecutive composite integers 212, 213, ..., 222, which are much smaller than the ones starting with $11! + 2$.

In a way, the following statement counterweights Theorem 6.6. It was formulated by J.L.F. Bertrand (1822–1900) in 1845, and proved by P.L. Chebyshev (1821–1894) in 1850. All known proofs use facts that are outside of the scope of our course and we omit them.

Theorem 13. *For any $n \geq 4$, there exists at least one prime number p, such that $n \leq p \leq 2n - 2$.*

All odd primes can be written in the form $4n+1$ or $4n+3$, i.e., are members of the arithmetic series $1, 5, 9, 13, 17, \ldots$ or $3, 7, 11, 15, 19, \ldots$. Are there infinitely many primes of each of the form (i.e., in each of the sequences)? In 1837 an affirmative answer to a much more general question was given by P.G. L. Dirichlet (1805–1859). Here it is. Again, all known proofs are too difficult at this stage, and are omitted.

Theorem 14. *Let a and d be two relatively prime integers. Then the arithmetic sequence*

$$a, a + d, a + 2d, \ldots, a + nd, \ldots$$

contains infinitely many primes.

Thus, there are infinitely many primes in the sequence
$1, 4, 7, 10, 13, \ldots \quad (a = 1, d = 3)$;
or in $5, 13, 21, 29, 37, \ldots \quad (a = 5, d = 8)$;
or in $3, 7, 11, 15, \ldots \quad (a = 3, d = 4)$;
there are infinitely many primes of the form $6n + 1$ $(a = 1, d = 6)$.

Is there any formula for prime numbers?

For example, can one find a function f of one variable such that $f(n)$ is prime for all $n \in \mathbb{N}$?

The quadratic function $y = x^2 + x + 41$ takes prime values for all $x = 1, 2, \ldots, 39$ (as well as $x = -40, -39, \ldots - 2, -1, -0$), but not for $x = 40$. This was observed by L. Euler (1707-1783). One can do even better: $y = x^2 - 79x + 1601$ takes prime values for the first eighty values of x. On the other hand, it is not hard to show that no non-constant polynomial $p(x)$ with integer coefficients can take prime values for all $x \in \mathbb{N}$. But what if f is not a polynomial of one variable?

It was noticed by P. Fermat (1601–1665) that $2^{2^n} + 1$ provides prime values for $n = 0, 1, 2, 3, 4$, and he conjectured that the pattern continues. It was disproved by L. Euler, who showed that $2^{2^5} + 1 = 2^{32} + 1 = 4294967297 = 641 \cdot 6700417$, i.e., is not prime.

Not much progress in finding a formula for primes had been made through the centuries. A breakthrough came in 1947, when Mills proved the existence of a real number α, such that $\lfloor \alpha^{3^n} \rfloor$ is prime for all $n \in \mathbb{N}$. Unfortunately the number α is still unknown. Here $\lfloor \quad \rfloor$ denotes the integer part of a number, i.e., $\lfloor x \rfloor$ is the greatest integer which is $\leq x$. E.g., $\lfloor 5.6 \rfloor = 5$, $\lfloor -5.6 \rfloor = -6$, $\lfloor 7 \rfloor = 7$.

Another deep result in this direction was obtained by Y. Matijasevich in 1972. He proved the existence of a polynomial in 58 variables $x_1, \dots, x_{58}$ of degree 4 with the property that if it is evaluated for all $(x_1, \dots, x_{58}) \in \mathbb{Z}^{58}$, then the set of its positive values is precisely the set of positive primes! Later other examples of such polynomials were found. The one below was found by Jones, Sato, Wada, and Wiens in 1976. Its degree is 25 and it has 26 variables (so we may use all letters of English alphabet).

$$f(a,b,\dots,y,z) = (k+2)\{1-[wz+h+j-q]^2-[(gk+2g+k+1)(h+j)+h-z]^2$$
$$-[2n+p+q+z-e]^2-[16(k+1)^3(k+2)(n+1)^2+1-f^2]^2-[e^3(e+2)(a+1)^2+1-o^2]^2$$
$$-[(a^2-1)y^2+1-x^2]^2-[16r^2y^4(a^2-1)+1-u^2]^2-[((a+u^2(u^2-a))^2-1)(n+4dy)^2$$
$$+1-(x+cu)^2]^2-[n+l+v-y]^2-[(a^2-1)l^2+1-m^2]^2-[ai+k+1-l-i]^2$$
$$-[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2-[q+y(a-p-1)$$
$$+s(2ap+2a-p^2-2p-2)-x]^2-[z+pl(a-p)+t(2ap-p^2-1)-pm]^2\}.$$

Suppose you are given a large integer n and you have to determine whether it is a prime.

How can one check whether a number is prime?

An obvious approach, i.e., trying to divide n by all positive integers less than $n/2$, will work, but it is too slow. A refinement of this idea which speeds the verification is given below.

Theorem 15. *Let $n \geq 2$. If no prime number $p \leq \sqrt{n}$ divides n, then n is prime.*

Proof. We prove the contrapositive statement: a composite number n is divisible by a prime p, $2 \leq p \leq \sqrt{n}$. Indeed, $n = ab$, for some $1 < a \leq b < n$. Then $a|n$ and $a \leq \sqrt{n}$ (else, $n = ab > \sqrt{n} \cdot \sqrt{n} = n$). Then any prime divisor p of a divides n. Since $2 \leq p \leq a \leq \sqrt{n}$, the proof is finished. □

For example, to check whether 143 is prime, it is sufficient to try to divide it by 2,3,5,7,11, since 11 is the largest prime not exceeding $\sqrt{143}$. Since none of these primes divide 143, 143 is prime.

For large numbers this method is still slow; much better methods for testing primality have been developed, but their theory is much more involved. Such tests are important in modern cryptography.

Exercise Set 6

1. Prove that the sum of four consecutive positive integers is never a prime number.
2. Find all $n \in \mathbb{N}$ such that all three numbers n, $n+10$, and $n+14$ are prime.

3. Are the following integers prime? Prove your answers.

(i) 127	(ii) 667	(iii) 1987
(iv) $2^{50} - 3^{20}$	(v) $2^{50} + 10^{50}$	(vi) $2^{50} + 15^{50}$
(vii) $111\ldots111$ (126 ones)	(viii) $2^{1988} - 1$	(ix) $2^{1988} + 1$

(*Hint*: the following identities can be useful: for $n, k \in \mathbb{N}$,

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \ldots + ab^{n-2} + b^{n-1});$$
$$a^{2k+1} + b^{2k+1} = (a+b)(a^{2k} - a^{2k-1}b + a^{2k-2}b^2 - \ldots - ab^{2k-1} + b^{2k}))$$

4. Prove that numbers below cannot be prime simultaneously:
   (i) $n+5$ and $n+10$, $(n \geq 2)$
   (ii) p, $p+2$ and $p+5$, $(p \geq 2)$
   (iii) $2^n - 1$ and $2^n + 1$, $n \geq 3$.
5. (i) Prove that if $2^n - 1$ is prime, then n is prime. Does the converse hold?
   (ii) Prove that if $2^n + 1$ is prime, then n is a power of two. Does the converse hold?
6. Prove that if a cube of a number is divisible by 17, then the number is divisible by 17.

---

7. Prove that the only solution of the diophantine equation
   (i) $n^2 = 5m^2$ is $(0,0)$
   (ii) $n^3 = 40m^3$ is $(0,0)$
8. Show that $n^4 + 4$ is a composite number for all integers $n \geq 2$. (Hint: factor the polynomial.)
9. Let p be a prime integer ≥ 5. Prove that $p^2 - 1$ is divisible by 24.
10. Let p_n denote the n–th positive prime. Thus $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \ldots$. Prove that for $n \geq 5$, $p_n > 2n$.
11. (i) What is the greatest integer n such that 3^n divides 30!?
    (ii) What is the greatest integer n such that 2^n divides $\binom{1000}{500} = 1000!/(500!)^2$? (It can be shown that this number is an integer, but you do not have to do it.)

---

12. Let p be a prime and let e be the greatest integer such that p^e divides $n!$. Prove that
$$e = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \ldots$$
13. Without using Theorem 6.5, prove that there are in infinitely many prime numbers of the form $4n+3$, $n \geq 1$.
14. Prove by induction with respect to a that for any positive prime p, and any integer a, $a^p - a$ is divisible by p (The statement is known as the "Little Fermat Theorem".)
15. Prove that there are infinitely many primes using #13 of Exercise Set 4. A proof based on this idea was suggested by G. Pólya (1887–1984).

Supplementary Problems.

(1) How many zeros are at the end of 1995! ?
(2) (i) Prove that for all $n \in \mathbb{N}$, the fraction $\frac{12n+1}{30n+2}$ is irreducible.
(ii) Find all integers n such that $\frac{19n+17}{7n+11}$ is an integer.
(3) (i) Prove that for all integers n and k, $0 \leq k \leq n$, $k!$ divides $n(n-1)(n-2)\cdots(n-k+1)$.
(ii) Prove that the binomial coefficient $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ is always divisible by 2.
(iii) Prove that the binomial coefficient $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ is always divisible by $n+1$.
(iv) Prove that the multinomial coefficient $\binom{kn}{n,n\ldots,n} = \frac{(kn)!}{n!n!\ldots n!}$ (product of k $n!$'s in the denominator) is always divisible by $k!$.
(4) What is the remainder of the division of 347^{1992} by 17?
(5) Prove that for all integers a, b, c, $6|(a+b+c)$ implies that $6|(a^3+b^3+c^3)$
(6) Prove that for all integers n, n^2+3n+5 is not divisible by 121.
(7) Both integer a and integer b is a sum of squares of two integers. Then ab is the sum of squares of two integers. Prove it.
(8) Solve the diophantine equation $x^3 - 2y^3 - 4z^3 = 0$.
(9) (i) Is number $111\ldots11$ (300 ones) a perfect square?
(10) Can the sum of digits of a perfect square be 1994?
(11) Prove that for every $n \in \mathbb{N}$, there exists an $x \in \mathbb{N}$, such that the number $nx+1$ is composite.

---

(12) Consider the sequence of Fibonacci numbers: $F_1 = F_2 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$. Prove that every positive integer can be represented as the sum of distinct members of the Fibonacci sequence.
(13) Prove that if positive integers m and n are relatively prime, then the same is true for $2^m - 1$ and $2^n - 1$.
(14) Prove that there is no non-constant polynomial $f(x)$ in one variable x with integer coefficients which takes prime values for all $x \in \mathbb{N}$.
(15) Prove that for any integer $n \geq 2$, the sum $1 + 1/2 + 1/3 + \ldots + 1/(n-1) + 1/n$ is never an integer.
(16) Prove that the equation $x^4 - 2y^2 = 1$ has no integer solutions.
(17) Let a and b be integers. If $a^2 + b^2$ is divisible by 21, then it is divisible by 441. Prove it.
(18) Let $a, b, x_0 \in \mathbb{N}$. Prove that some terms of the sequence $x_0,\ x_1 = ax_0 + b,\ x_2 = ax_1 + b, \ldots, x_{n+1} = ax_n + b, \ldots$ are composite numbers.
(19) Consider the sequence of Fibonacci numbers: $F_1 = F_2 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$. Prove that $5|F_{5k}$ for each $k \in \mathbb{N}$.
(20) For each irreducible fraction $\frac{a}{b} \in (0,1)$, consider an open interval $(\frac{a}{b} - \frac{1}{4b^2}, \frac{a}{b} + \frac{1}{4b^2})$. Does the union of all these intervals cover the interval $(0,1)$, i.e., is

$$(0,1) \subseteq \bigcup_{\frac{a}{b} \in (0,1)} (\frac{a}{b} - \frac{1}{4b^2}, \frac{a}{b} + \frac{1}{4b^2}) \ ?$$

---

(21) Prove that there are infinitely many prime integers of the form $4n+1, n \geq 1$.
(22) Consider a sequence of n integers $a_1, a_2, \ldots, a_n$. Prove that there are integers i and j such $1 \leq i \leq j \leq n$ and $n|(a_i + a_{i+1} + \ldots + a_j)$.

(23) Let a, b, k be positive integers, $\gcd(b, 10) = 1$ and $N = \overline{aaa\ldots aaa}$ is obtained by writing a next to each other k times. (For example, if $a = 2446$ and $k = 4$, then $N = 2446244624462446$.) Prove that given a and b, k can be chosen in such a way that $b|N$.

(24) (i) Let A be an infinite set of points in the Euclidean plane such that the distance between any two points is an integer. Prove that all points lie on one line.

(ii) Does the conclusion of part (i) above hold if we require all distances to be rational numbers?

(iii) Is it possible to find an infinite subset of points of the unit circle centered at the origin having all their coordinates rational numbers and all pairwise distances between them to be rational numbers?

(25) Prove that the equation $x^4 + y^4 = z^4$ has no integer solutions (x, y, z) with $xyz \neq 0$.

(26) For $n \in \mathbb{N}$, let $\phi(n)$ represent the number of positive integers less than n and relatively prime to n. Assume $\phi(1) = 1$. The function $\phi(n)$ is called the *Euler's quotient* function.

(i) Prove that if $\gcd(a, b) = 1$, then $\phi(ab) = \phi(a)\phi(b)$.

(ii) What is $\phi(p)$, $\phi(p^2)$, $\phi(p^3)$, or $\phi(p^m)$, if p is prime and $m \in \mathbb{N}$?

(iii) Prove that if $n = {p_1}^{e_1}{p_2}^{e_2}\cdots{p_k}^{e_k}$ is the prime decomposition of n, then

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})\cdots(1 - \frac{1}{p_k}).$$

Some Answers and Hints to Exercises.

Exercise Set 1

(1) Use part (vi) of Theorem 1. The converse is false, since both numbers can be equal to zero.
(2) All converse statements are false. Show this by given a counterexample to each of them.
(3) Denote the smallest of the four consecutive integers by n. Express other numbers in terms on n.
(4) Explore for $n = 4, 6, 8, 9, 15, 16, 20, 25$. Pair the divisors a and n/a.
(5) (i) Yes. (ii) No
(6) Imitate (in a broad sense) the solution to Example 3.

(i) We use the method of mathematical induction. For $n = 1$, the statement is correct, since $1^5 - 1 = 0$ and $5|0$. Suppose the statement is correct for $n = k \geq 1$, i.e., $5|(k^5 - k)$. We want to show that the statement is correct for $n = k + 1$, i.e., that $5|[(k + 1)^5 - (k + 1)]$. Let $A = k^5 - k$ and $B = (k + 1)^5 - (k + 1)$. Raising $k + 1$ to the fifth power, we obtain

$$\begin{aligned} B &= (k^5 + 5k^4 + 10k^3 + 10k^2 + 5k + 1) - (k + 1) \\ &= (k^5 - k) + 5(k^4 + 2k^3 + 2k^2 + k). \end{aligned}$$

Therefore $B = A + 5C$, where $C = k^4 + 2k^3 + 2k^2 + k$. But $5|A$ due to the inductive hypothesis. So B is the sum of two addends each divisible by 5. By Theorem 1 (iii), $5|B$, and the proof is complete. □

(7) Denote the average of the numbers by x. Explain that x must be one of the numbers. Express other numbers in terms on x. Or denote the smallest integer by y and express other numbers in terms on y.
(8) Use the approach of the solution to Example 1.
(9) Experiment. Notice a property of the total number of pieces you obtain.
(10) Explore for the number of lockers from 1 to 30. Use another problem from this Exercise Set.
(11) Imitate (in a broad sense) the solution to Example 3.
(12) Write $N = \overline{a_{n-1}a_{n-2}\ldots a_2a_1a_0}$, where $a_{n-1} \leq a_{n-2} \leq \ldots \leq a_2 \leq a_1 < a_0$ are the (decimal) digits. Then

$$9N = (10 - 1)(10^{n-1}a_{n-1} + 10^{n-2}a_{n-2} + \ldots 10^2a_2 + 10a_1 + a_0).$$

Distribute the product.

Exercise Set 2.

(1) Use the approach of the solution to Example 6.
(2) Use the approach of the solution to Example 7.
(3) Use Theorem Theorem 2.
(4) Use induction or the binomial theorem.
(5) (ii) Write the smallest of your integers as $3k + r$, where $0 \leq r < 3$. Go over all possible values of r. Parts (i) and (iii) can be done similarly.
(6) Denote the smaller of your odd integers by $2n + 1$. ($2n - 1$ is even better!)
(7) Imitate (in a broad sense) the solution to Example 7
(8) Write $N = 10a + 5$.

(9) Divide each number by n. Look at the remainders.
(10) Divide each number by 5 with remainder. Go over different cases.
(11) Write $N = 10a + r,\ 0 \le r < 10$. Or write $N = 100a + r,\ 0 \le r < 100$. (No.)
(12) Start experimenting with several fractions. It has to become clear after a while.

Exercise Set 3

(1) Use the approach of the solution to Example 9.
(2) Use the approach of the solution to Example 9.
(3) (i) 1. Explore the last digit of smaller powers of 3 and see the pattern. Or use the fact that the last digit of a number is the remainder of the division of the number by 10.
(ii) The hint has already been given.
(4) A hint has already been given.
(5) Similar to our proof of part (iv).
(6) The answer is 16. Use the approach of the solution to Example 8.
(7) A hint has already been given. Also use the approach of the solution to Example 8.
(8) First investigate what can be a remainder of the division of a square of an integer by 7.
(9) A hint has already been given. First investigate what can be a remainder of the division of a cube of an integer by 9.
(10) Show that c is quite small. What else is clear about c?

Exercise Set 4.

(1) (i) 4;
(ii) $c = 4k$ where k is an arbitrary integer.
(2) (i) the gcd of two numbers must divide their difference;
(ii) the same idea as in (i);
(iii) Let $d_1 = \gcd(a, b)$ and $d_2 = \gcd(a, a + b)$. Show that $d_1|d_2$ and $d_2|d_1$;
(iv) the gcd of two numbers must divide every linear combination of the numbers.
(3) The gcd of two numbers divides their difference.
(4) Converse to (ii) is correct. Prove it. Converse to (iii) is false. Find a counterexample.
(5) Use Theorem 6 (i).
(6) We have: $ax \equiv b \pmod{n} \iff n|(ax - b) \iff dn_1|(da_1x - db_1) \iff dn_1|d(a_1x - b_1) \iff n_1|(a_1x - b_1) \iff a_1x \equiv b_1 \pmod{n_1}$.
(7) 421. Similar to Example 11(ii). A faster solution follows from the observation that $N - 1$ has to be divisible by 3,4,5,7.
(8) 419. Similar to Example 11(ii). A faster solution follows from the observation that $N + 1$ has to be divisible by 3,4,5,7.
(9) (i) $\{38 + 56s :\ s \in \mathbb{Z}\}$. Similar to Example 11(ii).
(ii) $\{1102 + 1400t :\ t \in \mathbb{Z}\}$. Substitute the general solution of part (i) into the third congruence.

(iii) Write the general solution of the first congruence by using one parameter, say t, and substitute it into the second congruence. Explain that for some values of t the second congruence will be satisfied too.

(10) It is sufficient to prove that each of the numbers 2,3,5 divides $n^5 - n$ for all $n \in \mathbb{N}$. (Why is that?)

(11) Use the definition of the gcd of two numbers

(12) Explore. Find pairs of integers on which the Euclidian algorithm consists of exactly 1, 2, 3, 4, 5, 6 divisions, respectively. Try to generalize.

(13) Assume $m < n$. Prove that the gcd of these numbers must divide $2^{2^n} - 1$. The formula $a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \ldots + ab^{k-2} + b^{k-1})$ may be useful.

Exercise Set 5.

(1) (a) $\{(x, y) : \ x = -1 - 10t, y = 2 + 17t, t \in \mathbb{Z}\}$;
(b) $\{(x, y) : \ x = 6 - 5t, y = -1 - 9t, t \in \mathbb{Z}\}$;
(c) no solutions. Your answers may look different, but they have to produce the same solution sets as in (a),(b),(c).

(2) (a), (b): Use the idea of the solution to Example 14 and the remarks at the end of the section.

(3) (a) $(0, 0, 0), (1, 0, 1), (3, 4, 5)$;
(b) $(1, 0), (-1, 0), (9, 4)$;
(c) $(2, 1), (-2, 1), (8, 13)$

(4) Use induction on c. Both versions of mathematical induction will work.

(5) If $x = 0$, then $y = 0$. So $(0, 0)$ is a solution. If $x \neq 0$, then $x|2y$ (why?). Set $y = kx$, where k is an integer. Continue. Show that the only solution distinct from $(0, 0)$ is $(2, 2)$.

(6) Factor $x^3 - y^3$. Use the idea of the solution to Example 13. The answer is $\{(5, 6), (-6, -5), (-3, 4), (-4, 3)\}$.

(7) Show that $a|y$ and $b|x$.

(8) Use (5.2)

(9) (i) Generalize the solution of problem 9 (iii) of Exercise Set 4.
(ii) Write n in the form $n = 2^a 3^b m$, where $\gcd(2, m) = \gcd(3, m) = 1$. Then use part (i).

Exercise Set 6.

(1) Let n be the smallest of the integers. Continue.

(2) $n = 3$. Show that one of the numbers is divisible by 3.

(3) The following formuli may be useful in some of the problems:

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \ldots + ab^{n-2} + b^{n-1}) \, , n \geq 1 \text{ and}$$

$$a^{2k+1} + b^{2k+1} = (a+b)(a^{2k} - a^{2k-1}b + a^{2k-2}b^2 - \ldots - ab^{2k-1} + b^{2k}) \, , \quad k \geq 1 \, .$$

They can be proved by just multiplying the expressions in the right hand sides and reducing similar terms.

Answers: (i), (iii): Yes; (ii),(iv)–(ix): No.

(4) Think about divisibility of the numbers by 2 or 3.

(5) (i) Use our hint to problem 3 above. No (find a counterexample).
(ii) Use our hint to problem 3 above. No (give a counterexample).
(6) Use Theorem 10.
(7) (i) Similar to Example 15.
(ii) Similar to Example 15. Concentrate on a prime divisor of 40.
(8) A hint is already given.
(9) Explain that among three consecutive integers $p-1, p, p+1$ where p is a prime ≥ 5, one is divisible by 4, another is divisible by 2 and one is divisible by 3. Or: divide p by 12 with the remainder and consider cases corresponding to possible remainders.
(10) Use induction on n.
(11) (i) 14.
(ii) 6. First understand how to find the greatest powers of 2 which divides 1000! and 500!, respectively.
(12) Generalize several numerical examples, including those in problem 11 from this exercise set.
(13) Imitate the Euclid's proof that there are infinitely many primes. Suppose there are only finitely many, say k, positive primes of the form $4n+3$. List all of them in increasing order: $3 = p_1 < 7 = p_2 < 11 = p_3 < \ldots < p_k$. Show that the number $N = 4p_1p_2 \ldots p_k - 1$ is
(a) of the form $4m+3$,
(b) not in the list and therefore is composite,
(c) must be divisible by one of the primes from the list, but is not divisible by any p_i's.
(14) Show that the binomial coefficient $\binom{p}{k}$ is divisible by p for all k, $1 < k < p$.
(15) Think about the prime factorizations of the numbers $2^{2^n} + 1,\ n \geq 0$.

REFERENCES.

(1) R.D. Baker, G.L. Ebert, *Discrete Mathematics*, Kendall/Hunt Publishing Company, Dubuque, Iowa, 1998.
(2) Z.I. Borevich and I.R. Shafarevitch, *Number Theory*, Academic Press, 1966.
(3) H. Davenport, *The Higher Arithmetic*, 5th Edition, Cambridge University Press, 1982.
(4) G.H. Hardy, E.M. Wright, *An Introduction to the Theory of Numbers*, Oxford Science Publ., 5th Edition, 1979.
(5) G.A. Kudrevatov, *A Problem Book on Number Theory*, Prosveschenie, Moscow, 1970. (in Russian).
(6) J.P. Jones,D. Sato, H. Wada, D. Wiens, Diophantine representation of the set of prime numbers, *American Mathematical Monthly*, v. 83, no. 6, 1976, pp. 449–464.
(7) W. Sierpinski, *250 problems from Elementary Number Theory*, Matematicheskoye Prosveschenie, Moscow, 1968. (in Russian).
(8) S. Wolfram, *Mathematica: A System for Doing Mathematics by Computer*, Addison Wesley, 1988.

Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA

E-mail address: lazebnik@math.udel.edu