Math 302
Introduction to Proofs
via Number Theory

Robert Jewett
(with small modifications by B. Ćurgus)

June 25, 2007

Contents

Chapter 1

The Integers

The only numbers in these notes are the integers (or the whole numbers). The set of all integers is denoted by $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$. We shall employ the standard facts about addition, multiplication and order of integers.

1.1 Axioms of $\mathbb{Z}$

The following are the basic properties (axioms) of $\mathbb{Z}$ that relate to addition and multiplication and the order relation ($<$) in $\mathbb{Z}$:

Axiom 1 (A1)**.** If $a, b \in \mathbb{Z}$, then the sum $a + b$ is uniquely defined element in $\mathbb{Z}$.

Axiom 2 (A2)**.** $a + (b + c) = (a + b) + c$ for all $a, b, c \in \mathbb{Z}$.

Axiom 3 (A3)**.** $a + b = b + a$ for all $a, b \in \mathbb{Z}$.

Axiom 4 (A4)**.** There is an element 0 of $\mathbb{Z}$ such that $0 + a = a + 0 = a$ for all $a \in \mathbb{Z}$.

Axiom 5 (A5)**.** If a is an element of $\mathbb{Z}$, then the equation $a + x = 0$ has a solution $-a \in \mathbb{Z}$.

Axiom 6 (M1)**.** If $a, b \in \mathbb{Z}$, then the product $a \cdot b$ (usually denoted by ab) is uniquely defined element in $\mathbb{Z}$.

Axiom 7 (M2)**.** $a(bc) = (ab)c$ for all $a, b, c \in \mathbb{Z}$.

Axiom 8 (M3)**.** $ab = ba$ for all $a, b \in \mathbb{Z}$.

Axiom 9 (M4)**.** There is an element $1 \neq 0$ of $\mathbb{Z}$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in \mathbb{Z}$.

Axiom 10 (M5)**.** If a, b, c are integers, $c \neq 0$, and $ac = bc$, then $a = b$.

Axiom 11 (DL)**.** $a(b + c) = ab + ac$ for all $a, b, c \in \mathbb{Z}$.

Axiom 12 (O1)**.** If $a, b \in \mathbb{Z}$, then exactly one of the following three statements is true: $a < b$ or $a = b$, or $b < a$.

Axiom 13 (O2)**.** Given any $a, b, c \in \mathbb{Z}$, if $a < b$ and $b < c$, then $a < c$.

Axiom 14 (O3)**.** Given any $a, b, c \in \mathbb{Z}$, if $a < b$ then $a + c < b + c$.

Axiom 15 (O4)**.** Given any $a, b, c \in \mathbb{Z}$, if $a < b$ and $0 < c$, then $ac < bc$.

There is one more axiom of $\mathbb{Z}$ that we will introduce in Section 1.3. Based on the given axioms one can prove all familiar properties of addition and multiplication in $\mathbb{Z}$. Few examples are given in the following exercise.

Exercise 1.1.1.* Prove the following statements using the given axioms $\mathbb{Z}$.

(a) If a is an integer, then $0 \cdot a = 0$.

(b) If a is an integer, then $-(-a) = a$.

(c) If a and b are integers, then $(-a)b = -(ab)$.

(d) If a and b are integers, then $(-a)(-b) = ab$.

(e) If a and b are integers and $a < b$, then $-b < -a$.

(f) If a and b are integers and, $0 < a$ and $0 < b$, then $0 < ab$.

(g) If a is an integer and $a \neq 0$, then $0 < a^2$.

(h) $0 < 1$.

(i) Assume that a and b are integers. Then $ab = 0$ if and only if $a = 0$ or $b = 0$.

Remark 1.1.2. Note that we can not freely divide in $\mathbb{Z}$. We can divide only when we can divide "evenly". That is, the expression b/a is used only when a and b are integers, $a \neq 0$, and there exists an integer k such that $b = ak$. In that case we would write $b/a = k$.

Definition 1.1.3. Integers a such that $a > 0$ are called *positive integers* (or natural numbers). The set of all positive integers is denoted by $\mathbb{N}$.

In your proofs you can use the standard facts about addition, multiplication and inequalities between integers without proofs. It is a good strategy to write down a specific property that you are using and make sure that it is valid.

The symbol * means that a formal proof can be found at the end of the chapter.

1.2 Multiples and Divisors

Definition 1.2.1. Let a and b be integers. We say that b is a *multiple* of a if there exists an integer k such that $b = ak$. We say that a *divides* b, and we write $a|b$, if $a \neq 0$ and there exists an integer k such that $b = ak$.

Example 1.2.2. From Definition 1.2.1: $10, 5, -5$ and 0 are multiples of -5. Also, 0 is a multiple of 0, but 0 does not divide 0.

Proposition 1.2.3.* Let a, b and c be integers. If $a|b$ and $a|c$, then $a|(b + c)$.

Proposition 1.2.4. Let a, b and c be integers. If $a|b$ and $b|c$, then $a|c$.

Proposition 1.2.5. If a, b and c are integers and $ab|c$, then $a|c$ and $b|c$.

Proposition 1.2.6. If a, b and c are integers and $ac|bc$, then $a|b$.

Proposition 1.2.7. If a, b and c are integers, $c \neq 0$, and $a|b$, then $ac|bc$.

Proposition 1.2.8. Let a, b and c be integers. If $a|b$ and $a|(b+c)$, then $a|c$.

Proposition 1.2.9. If a, b and c are integers and $a|b$, then $a|bc$.

1.3 Minimum and Maximum

Definition 1.3.1. If $\mathcal{P}$ is a mathematical property, then the set S of all integers with that property is denoted by

$$S = \{x \ : \ x \in \mathbb{Z}, \ x \ \text{ has the property } \ \mathcal{P}\}.$$

Definition 1.3.2. Let S be a subset of $\mathbb{Z}$. An integer a is called a *lower bound* for S if $a \leq s$ for all $s \in S$. A set of integers is *bounded below* if it has a lower bound. An integer b is called an *upper bound* for S if $s \leq b$ for all $s \in S$. A set of integers is *bounded above* if it has an upper bound.

Definition 1.3.3. Let S be a subset of $\mathbb{Z}$. An integer m is called a *minimum* of S if

- m is a lower bound for S and
- m is an element of S.

The minimum of S is denoted by $\min S$.

Definition 1.3.4. Let S be a subset of $\mathbb{Z}$. An integer M is called a *maximum* of S if

- M is an upper bound for S and
- M is an element of S.

The maximum of S is denoted by $\max S$.

Axiom 16 (The Well-Ordering Axiom)**.** Let S be a nonempty subset of $\mathbb{Z}$. If S is bounded below, then S has a minimum.

Proposition 1.3.5.* Let S be a nonempty subset of $\mathbb{Z}$. If S is bounded above, then S has a maximum.

Proposition 1.3.6.* Let a be an integer and let n be a positive integer. Then the set of all multiples of n which do not exceed a has a maximum.

Proposition 1.3.7. Let a be an integer that is greater than 1. Then the set of all integers which divide a and are greater than 1 has a minimum.

Proposition 1.3.8. Let a and b be integers. Suppose that a and b are not both 0. Then there exists a greatest integer d that divides both a and b. Moreover, d is positive.

Proposition 1.3.9. Let a and b be positive integers. Then there exists a least integer that is positive and is a multiple of both a and b.

Remark 1.3.10. These five propositions will be used later. The proof of Proposition 1.4.1 depends on Proposition 1.3.6, and Proposition 1.3.7 is implicit in the statement of Proposition 1.6.4. The definitions in 2.1.1 and 2.1.6 in the next chapter are justified by Propositions 1.3.8 and 1.3.9.

Example 1.3.11. Here are sets of integers that illustrate the four propositions.

(a) The multiples of 5 that do not exceed -7: $T = \{-10, -15, -20, \ldots\}$.

(b) The divisors of 12 that are greater than 1: $U = \{2, 3, 4, 6, 12\}$.

(c) The integers that divide both 12 and -30: $V = \{-6, -3, -2, -1, 1, 2, 3, 6\}$.

(d) The positive common multiples of 6 and 10: $W = \{30, 60, 90, \ldots\}$.

1.4 Remainders

Proposition 1.4.1.* Let a be an integer and let n be a positive integer. Then there exist unique integers q and r such that

$$a = nq + r \quad \text{and} \quad 0 \leq r \leq n - 1.$$

Definition 1.4.2. The integer r in Proposition 1.4.1 is called the *remainder* left by a when divided by n.

Example 1.4.3. When divided by 5, the integer 17 leaves a remainders of 2: $17 = 5 \cdot 3 + 2$. When divided by 5, the integer -17 leaves a remainder of 3: $-17 = 5(-4) + 3$.

Definition 1.4.4. Let a be an integer. Let r be the remainder left by a when divided by 2. We say that a is *even* if $r = 0$ and that a is *odd* if $r = 1$.

Proposition 1.4.5. If a and b are even integers, then $a + b$ and ab are even integers.

Proposition 1.4.6. If a and b are odd integers, then $a + b$ is even and ab is odd.

Proposition 1.4.7. If a is an even integer and b is an odd integer, then $a + b$ is odd and ab is even.

Proposition 1.4.8. If a is an integer, then $a(a + 1)$ is even.

Proposition 1.4.9. Let n be a positive integer. Then among any n consecutive integers there exists an integer divisible by n.

1.5 Square and Triangular Numbers

Definition 1.5.1. An integer a is a *perfect square* (or a *square number*, or a *square*) if there exists an integer k such that $a = k^2$. An integer a is *triangular* (or a *triangular number*) if there exists an integer k such that $a = k(k+1)/2$. By Proposition 1.4.9, $k(k+1)$ is even.

Example 1.5.2. Here are some square and triangular numbers:

k	-3	-2	-1	0	1	2	3	4	5	6	7	8	9
k^2	9	4	1	0	1	4	9	16	25	36	49	64	81
$\frac{k(k+1)}{2}$	3	1	0	0	1	3	6	10	15	21	28	36	45

Proposition 1.5.3. If a is an even square, then there exists an integer k such that $a = 4k$.

Proposition 1.5.4. If a is an odd square, then there exists an integer k such that $a = 8k + 1$.

Proposition 1.5.5. If a is a triangular number, then $8a + 1$ is a perfect square.

Proposition 1.5.6.* If a is an integer and $8a + 1$ is square, then a is triangular.

Proposition 1.5.7. The sum of any two consecutive triangular numbers is a perfect square.

Proposition 1.5.8. If a is a triangular number, then $9a + 1$ is triangular also.

Proposition 1.5.9. When divided by 3, a square number leaves a remainder or 0 or 1.

Proposition 1.5.10. When divided by 3, a triangular number leaves a remainder of 0 or 1.

Remark 1.5.11. Let k be a positive integer. Then k^2 dots can be arranged in a square.

Since the sum of the first k positive integers is equal to $\frac{k(k+1)}{2}$, that many dots can be arranged in a triangle. Below is an illustration for the case where $k = 4$.

1.6 The Prime Numbers

Definition 1.6.1. An integer a is *composite* if there exist integers b and c such that $a = bc,\ b > 1,\ c > 1$. Notice that a composite integer must be greater than 1. A *prime* (or *prime number*) is an integer that is greater than 1 but not composite.

Example 1.6.2. Here are the first forty primes:
2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67
71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149
151 157 163 167 173 .

Proposition 1.6.3. If p is a prime greater than 3, then p leaves a remainder of 1 or 5 when divided by 6.

Proposition 1.6.4.* Let a be an integer greater than 1 and let d be the smallest integer that divides a and is greater than 1. Then d is a prime.

Proposition 1.6.5. Let a be an integer, not equal to 1 or -1. Then there exists a prime that divides a.

Proposition 1.6.6. Let a be an integer greater than 1. Suppose that a is not divisible by any prime p such that $p^2 \leq a$. Then a is a prime.

Exercise 1.6.7. Factor 123456 into primes.

1.7 Problems

Problem 1.7.1. Prove that when divided by a positive even integer, an odd integer leaves an odd remainder.

Problem 1.7.2. With the use of a calculator, show that 10001 is composite.

Problem 1.7.3. Without the use of a calculator, show that 1000000000001 is composite.

Problem 1.7.4. Prove that the sum of the first k positive integers is equal to $\frac{k(k+1)}{2}$ by showing how to combine a pair of equal triangular arrays into a rectangular array.

Problem 1.7.5. Prove Proposition 1.5.7 by showing how to break a square array up into two triangular arrays.

Problem 1.7.6. Prove Proposition 1.5.5 by combining eight copies of a triangular array into a square array with one dot missing.

Problem 1.7.7. Can you prove Proposition 1.5.8 with arrays?

1.8 Projects

Project 1.8.1. Each of the three integers $0, 1$ and 36 is both square and triangular. Find some other triangular squares and investigate their properties.

Project 1.8.2. A *double triangular number* is an even integer a such that both a and $a/2$ are triangular. Two examples are 0 and 6, but there are others. Investigate the properties of the double triangular numbers, and determine their relation to the triangular squares.

Project 1.8.3. Show that if a is a triangular number, then $25a + 3$ and $49a + 6$ are also triangular. Generalize this result.

1.9 Proofs and Suggestions

Proof of Proposition 1.1.1. (a) By Axiom 6 $0 \cdot a$ is an integer. By Axiom 5 there exists an integer $-(0 \cdot a)$ such that $0 \cdot a + (-(0 \cdot a)) = 0$. By Axiom 4 we have $0 + 0 = 0$. Therefore $a \cdot (0 + 0) = a \cdot 0$. By Axiom 11 it follows that $a \cdot 0 + a \cdot 0 = a \cdot 0$. Adding $-(0 \cdot a)$ to both sides of the last equality and we get $(a \cdot 0 + a \cdot 0) + (-(0 \cdot a)) = a \cdot 0 + (-(0 \cdot a))$. By Axiom 2 the last equality can be rewritten as $a \cdot 0 + (a \cdot 0 + (-(0 \cdot a)) = a \cdot 0 + (-(0 \cdot a))$. By Axiom 5, we conclude that $a \cdot 0 + 0 = 0$, that is, $a \cdot 0 = 0$.

The proofs of (b) and (c) are similar. The proof of (d) uses (b) and (c).

(e) Assume $a < b$. By Axiom 14 we have $a + (-b) < b + (-b)$. Thus $(-b) + a < 0$. Using Axiom 14 again we conclude that $((-b) + a) + (-a) < 0 + (-a)$, and consequently $-b < -a$.

The part (f) is a special case of Axiom 15.

(g) Consider two different cases: $0 < a$ and $a < 0$. If $0 < a$, then (f) implies that $0 < aa = a^2$. If $a < 0$, then, by (e), $-0 < -a$, and since $-0 = 0$ we have $0 < -a$. By the first part of this proof, we conclude that $0 < (-a)^2$. By the part (d) we have $(-a)^2 = a^2$. Therefore $0 < a^2$.

(h) Since $0 \neq 1$ by Axiom 9, we can apply (g) and conclude $0 < 1^2$. Axiom 9 also implies that $1^2 = 1 \cdot 1 = 1$. Therefore $0 < 1$.

We prove "only if" part of (i), that is we prove the implication:

$$ab = 0 \quad \text{implies} \quad a = 0 \quad \text{or} \quad b = 0. \tag{1.9.1}$$

Assume that $ab = 0$. Consider two cases: Case 1: $a = 0$ and Case 2: $a \neq 0$.

Case 1. In this case the implication (1.9.1) is true and there is nothing to prove.

Case 2. Since in this case we assume that $a \neq 0$, by (a) we can write $ab = a0$. Now, since $a \neq 0$, by Axiom 10 we conclude that $b = 0$. □

Proof of Proposition 1.2.3.

(1) Let a, b and c be integers, and suppose that $a|b$ and $a|c$.

(2) By Definition 1.2.1, $a \neq 0$ and there exist integers k and m such that $b = ak$ and $c = am$.

(3) $b + c = ak + am = a(k + m)$.

(4) $a|(b + c)$.

□

Proof of Proposition 1.3.5.

(1) Consider the set $T = \{x : \text{ there exists } r \in S \text{ such that } x = -r\}$.

(2) Let b be an upper bound for S. Then $s \leq b$ for all $s \in S$.

(3) Let x be an arbitrary integer in T. Then there exists an integer $r \in S$ such that $x = -r$.

(4) Since $r \in S$, by the line (2), $r \leq b$. By Exercise 1.1.1 (e), $-b \leq -r$. Therefore, by the line (3), $-b \leq x$.

(5) Since $x \in T$ was arbitrary, (4) implies that $-b$ is a lower bound for T.

(6) Since S is nonempty, the set T is nonempty.

(7) By the lines (5) and (6), Axiom 16 implies that T has a minimum m. By Definition 1.3.3, $m \leq x$ for all $x \in T$ and $m \in T$.

(8) Since $m \in T$, the line (1) implies that there exists $M \in S$ such that $m = -M$.

(9) By the definition of T in (1), for an arbitrary $s \in S$, the integer $-s$ belongs to T. Therefore $m \leq -s$ for all $s \in S$. Therefore $s \leq -m$ for all $s \in S$, that is $s \leq M$ for all $s \in S$.

(10) By the lines (8) and (9) the integer M is a maximum of S.

□

Proof of Proposition 1.3.6.

(1) Let a be an integer and let n be a positive integer.

(2) Let $S = \{x : x \in Z,\ x \text{ is a multiple of } n,\ x \leq a\}$.

(3) If $a \geq 0$, then $0 \in S$.

(4) If $a < 0$, then $na \in S$.

(5) S is non-empty.

(6) S is bounded above by a.

(7) By Proposition 1.3.5, S has a maximum.

□

Suggestion for Proposition 1.3.7. Let $S = \{x : x \in Z,\ x \text{ divides } a,\ x > 1\}$.

Proof of Proposition 1.4.1.

(1) Let a be an integer and let n be a positive integer.

(2) By Proposition 1.3.6, there exists a greatest multiple of n that does not exceed a. Call it c.

(3) There exists an integer q such that $c = nq$.

(4) Let $r = a - nq$. Then $r \geq 0$.

(5) $nq + n$ is a multiple of n and is greater than c.

(6) Since c is maximal, $nq + n > a$.

(7) $n > a - nq = r$.

(8) $a = nq + r$ and $0 \leq r \leq n - 1$.

(9) Suppose that q' and r' are integers, $a = nq' + r'$, and $0 \leq r' \leq n - 1$.

(10) $nq + r = nq' + r'$.

(11) $nq - nq' = r' - r$.

(12) $0 - (n - 1) \leq r' - r \leq (n - 1) - 0$.

(13) $-n < n(q - q') < n$.

(14) $-1 < q - q' < 1$.

(15) $q' = q$.

(16) $r' = r$.

□

Suggestion for Proposition 1.4.9. Let n consecutive integers be given, and suppose that a is the first and that b is the last. Let r be the remainder left by b when divided by n. Show that $b - r$ is divisible by n and lies between a and b.

Proof of Proposition 1.5.6.

(1) Let a be an integer and suppose that $8a + 1$ is square.

(2) There exists k such that $8a + 1 = k^2$.

(3) k^2 is odd.

(4) By 1.4.6, k is not even. Hence, k is odd.

(5) There exists m such that $k = 2m + 1$.

(6) $8a + 1 = (2m + 1)^2 = 4m^2 + 4m + 1 = 4m(m + 1) + 1$.

(7) $a = \frac{m(m+1)}{2}$.

(8) a is triangular.

□

Suggestion for Proposition 1.5.9. Let $a = k^2$ and consider three cases: $k = 3q$, $k = 3q + 1$, and $k = 3q + 2$.

Suggestion for Proposition 1.5.10. One possibility is to let $a = \frac{k(k+1)}{2}$ and consider six cases. Another is to use Proposition 1.5.5.

Proof of Proposition 1.6.4*, Proof by contradiction.*

(1) Let a be an integer greater than 1 and let d be the smallest integer that divides a and is greater than 1. Assume that d is composite.

(2) There exist integers b and c such that $d = bc,\ \ b > 1,\ \ c > 1$.

(3) By Proposition 1.2.4, $b|a$ and $1 < b < d$.

(4) This contradicts (1).

□

Proof of Proposition 1.6.4*, Proof of the contrapositive.*

(1) Let a be an integer greater than 1 and let d be a divisor of a that is composite.

(2) There exist integers b and c such that $d = bc,\ \ b > 1,\ \ c > 1$.

(3) By Proposition 1.2.4, $b|a$ and $1 < b < d$.

(4) d is not the smallest integer that divides a and is greater than 1.

□

Suggestion for Proposition 1.6.5. Consider three cases: a is positive, negative or zero.

Comments on Sections 2 through 5

1. The fundamental notion in number theory is that of one integer dividing another integer evenly.

2. Proposition 1.4.1 is traditionally called the *Division Algorithm.*

3. Triangular numbers were studied in ancient times. It was known to Pythagoras that $\frac{k(k+1)}{2}$ dots can be put into a triangular array.

4. Eratosthenes devised an algorithm for determining primes. Suppose that the primes less than a given positive integer c are known. List the integers from c to $c^2 - 1$. In the list, cross out all multiples of the known primes. The numbers that remain are the primes between c and $c^2 - 1$. This algorithm is known as the *Sieve of Eratosthenes.*