Slides of Discrete Mathematics based on Susanna Epp's Textbook

Moses A. Boudourides[1]

Visiting Associate Professor of Computer Science
Haverford College

[1] Moses.Boudourides@cs.haverford.edu

Chapter 4b

Elementary Number Theory and Methods of Proof, IIII, V, VI

September 20, 22, & 24, 2021

4.4 The Quotient–Remainder Theorem

Theorem (The Quotient–Remainder Theorem)

Given any integer n and positive integer d, there exist unique integers q and r such that

$$n = dq + r \qquad \text{and} \qquad 0 \leq r < d.$$

Definition

Given an integer n and a positive integer d,

$$\begin{aligned} n \text{ div } d &= \text{the integer quotient obtained} \\ &\quad \text{when } n \text{ is divided by } d, \text{ and} \\ n \bmod d &= \text{the nonnegative integer remainder obtained} \\ &\quad \text{when } n \text{ is divided by } d. \end{aligned}$$

Symbolically, if n and d are integers and $d > 0$, then

$$n \text{ div } d = q \text{ and } n \bmod d = r \iff n = dq + r,$$

where q and r are integers and $0 \leq r < d$.

4.4 Modular Arithmetic Example

Example

If, for some integer m, $m \bmod 11 = 6$, what is $4m \bmod 11$?

$m \bmod 11 = 6$ means that $m = 11q + 6$, for some integer $q > 6$. Hence, $4m = 44q + 24$. To factor 11 from 24, we write $24 = 11 \cdot 2 + 2$, which implies that $4m = 11 \cdot 4 \cdot q + 11 \cdot 2 + 2 = 11(4q + 2) + 2$, where $4q + 2$ is a positive integer and the nonnegative remainder $2 < 4q+2$, since $q > 0$. In other words, $4m \bmod 11 = 2$.

If, for some integer m, $m \bmod 7 = 4$, what is $5m \bmod 7$?

Now, $m = 7q+4$, for some integer $q > 4$. Hence, $5m = 35q+20$. To factor 7 from 20, we write $20 = 7 \cdot 2+6$, which implies that $5m = 7 \cdot 5 \cdot q+7 \cdot 2+6 = 7(5q+2)+6$, where $5q+2$ is a positive integer and the nonnegative remainder $6 < 5q + 2$, since $q \geq 1 > \frac{4}{5}$. In other words, $5m \bmod 11 = 6$.

4.4 Parity and Consecutiveness of Integers

Definitions

- The **parity** of an integer refers to whether the integer is even or odd.
- Two integers are **consecutive** if their difference is ± 1.

Proposition

Every integer is either even or odd.

Proposition

Any two consecutive integers have opposite parity.

4.4 An Example and Division into Cases

Example

Show that the square of any odd integer is of the form $8m+1$, for some integer m.

Proof: Let n odd, i.e., $n = 2k+1$, for some integer k. Then $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$. Let us consider the number $k(k+1)$. Since the two integers $k, k+1$ are cosecutive, the previous proposition implies that one of them should be even and the other odd, meaning that their product should be even and, thus, $k(k+1) = 2m$, for some integer m. Therefore, $n^2 = 4 \cdot 2m + 1 = 8m + 1$.

Method of Proof by Division into Cases

To prove a statement of the form "If A_1 or A_2 or ... or A_n then C," prove all of the following:

If A_1 then C,
If A_2 then C,
$\vdots$
If A_n then C.

Solution of the Example by Cases

Example

Show that the square of any odd integer is of the form $8m + 1$, for some integer m.

Proof: Let n odd, i.e., $n = 2k + 1$, for some integer k. However, there are two cases for the integer k: either k is even, i.e., $k = 2p$, for some integer p, or k is odd, i.e., $k = 2q + 1$, for some integer q. Thus, either the odd n is $n = 2(2p)+1 = 4p+1$ (case 1) or it is $n = 2(2q+1)+1 = 4q+3$ (case 2).

Case 1: $n = 4p+1$ and, hence, $n^2 = (4p+1)^2 = 16p^2+8p+1 = 8(2p^2+p)+1$, which is of the form $n^2 = 8m + 1$, for the integer $m = 2p^2 + p$.

Case 2: $n = 4q + 3$ and, hence, $n^2 = (4q + 3)^2 = 16q^2 + 24q + 9 = (16q^2 + 24q + 8) + 1 = 8(2q^2 + 3q + 1) + 1$, which is again of the form $n^2 = 8m + 1$, for the integer $m = 2q^2 + 3q + 1$.

Another Example Solved by Cases

Example

Show that, for any integer n, $n^2 - 2$ is not divisible by 5.

Proof: By the quotient-remainder theorem, any number divisible by 5 must take one of the forms:

$$5k, 5k+1, 5k+2, 5k+3, \text{ or } 5k+4,$$

for some integer k (each time different). Therefore, assuming that $n^2 - 2$ was divisible by 5, we would need to negate five cases.

Case 1: $n = 5k$ implying that $n^2 - 2 = 25k^2 - 2 = 25k^2 + (-5+5) - 2 = (25k^2 - 5) + 3 = 5(5k^2 - 1) + 3$, i.e., $(n^2 - 2) \bmod 5 = 3$, which is false, because $n^2 - 2$ being divisible by 5 means that $(n^2 - 2) \bmod 5 = 0$.

Case 2: $n = 5k + 1$ implying that $n^2 - 2 = 25k^2 + 10k + 1 - 2 = 25k^2 + 10k + (-5+5) - 1 = (25k^2 + 10k - 5) + 4 = 5(5k^2 + 2k - 1) + 4$, i.e., $(n^2 - 2) \bmod 5$ is found to be 4, instead of 0, which results something false again.

Case 3: $n = 5k+2$ implying that $n^2 - 2 = 25^2 + 20k + 4 - 2 = 25^2 + 20k + 2 = 5(5k^2 + 4k) + 2$, i.e., $(n^2 - 2) \bmod 5$ is found to be 2, instead of 0, false again.

Case 4: $n = 5k+3$ implying that $n^2 - 2 = 25^2 + 30k + 9 - 2 = 25^2 + 30k + 5 + 2 = 5(5k^2 + 6k + 1) + 2$, i.e., $(n^2 - 2) \bmod 5$ is found to be 2, instead of 0, false again.

Case 5: $n = 5k + 4$ implying that $n^2 - 2 = 25^2 + 40k + 16 - 2 = 25^2 + 40k + 10 + 4 = 5(5k^2 + 8k + 2) + 4$, i.e., $(n^2 - 2) \bmod 5$ is found to be 4, instead of 0, false again.

4.5 Proof by Contradiction

Method of Proof by Contradiction

1. Suppose that the statement to be proved is false.
2. Then show that this supposition leads to a contradiction.
3. Therefore, the statement to be proved is true.

Examples of Statements Proved by Contradiction

- There is no greater integer.
- There is no integer that is both even and odd.
- The sum of any rational number and any irrational number is irrational.

4.5 An Example of a Proof by Contradiction

Hints how a Particular Proof by Contradiction Works

Prove by contradiction that every integer greater than 11 is a sum of two composite numbers.

Solution Hints:

1. Let us assume there exists an integer n such that $n > 11$ and n is not the sum of two composite numbers. This means that if, for two integers n_1, n_2, we have $n = n_1 + n_2$, both n_1 and n_2 cannot be composite, i.e., one of them has to be prime and the other composite.
2. We need to reach a contradiction each time we are representing n as the sum of two integers. The question is how are we going to select those integers summing up to n? An obvious answer is when we consider $n = (n - m) + m$, where $n - m$ and m are not both composite. For instance, we can take m to be even, but greater than 2, which would necessarily make m to be composite. On the other side, $n - m$ needs to be greater than 2 (in order to be possibly classified as prime) and since m has been already chosen to be an even greater than 2, necessarily, m should be one of 4, 6, and 8 (why?).

4.5 An Example of a Proof by Contradiction (continuation)

4. Therefore, for each one of the three cases $n = (n-4)+4, n = (n-6)+6, n = (n-8)+8$, it is implied that, respectively, the numbers $n-4, n-6, n-8$ are prime.
5. Using the Quotient-Remainder Theorem, since $n > 11$, n should be of the form $n = 3q + r$, for unique integers q, r such that and $0 \leq r < 3$, which means that $r = 0, 1, 2$ are the only possible remainders for the division of such n with 3.
6. The next step is to show that for each of three numbers $n-4, n-6, n-8$ (which are greater than 3, since $n > 11$) one of the possible remainders of their division with 3 contradicts the fact that these three numbers are all prime. Let us consider them separately:
   - 6.1 For the number $n-4$, we have $n-4 = 3q + r - 4$ and then the remainder $r = 1$ makes this number be $n-4 = 3q+1-4 = 3q-3 = 3(q-1)$, which is compostite and this is a cotradiction to the primeness of $n-4$.
   - 6.2 For the number $n-6$, we have $n-6 = 3q + r - 6$ and then the remainder $r = 0$ makes this number be $n-4 = 3q+0-6 = 3q-6 = 3(q-2)$, which is compostite and this is a cotradiction to the primeness of $n-6$.
   - 6.3 For the number $n-8$, we have $n-4 = 3q + r - 8$ and then the remainder $r = 2$ makes this number be $n-4 = 3q+2-8 = 3q-6 = 3(q-2)$, which is compostite and this is a cotradiction to the primeness of $n-8$.

4.5 Proof by Contraposition

Method of Proof by Contraposition

1. Formulate the statement to be proved in the form $\forall x \in D,$ if $P(x),$ then $Q(x)$.
2. Then use a direct proof to show the contraposition that, if $\exists x \in D,$ such that $Q(x)$ was false, then this would imply that $P(x)$ was false too.
3. Therefore, the statement to be proved is true.

Examples of Statements Proved by Contradiction

- For all integers n, if n^2 is even, then n is even.
- For all integers n, if $n^2 - 6n + 5$ is odd, then n is odd.
- For all integers a, b, n, if $n \nmid ab$, then $n \nmid a$ and $n \nmid b$.
- For all $x \in \mathbb{R}$, if $x^3 \leq 0$, then $x \leq 0$.

4.5 An Example of a Proof by Contraposition

An Example of a Proof by Contraposition

Prove by contraposition that, for all integer a, if $a \bmod 6 = 3$ then $a \bmod 3 \neq 2$.

Proof: To use contraposition means that we need to prove the following statement:

$$\exists a \in \mathbb{Z} \text{ such that, if } a \mod 3 = 2, \text{ then } a \mod 6 \neq 3.$$

So, let the number a be any multiple of 3 plus 2 (i.e., $a \in \{5, 8, 11, 14, 17, \ldots\}$). In other words, $a \bmod 3 = 2$, which means that $a = 3q + 2$, for some integer q such that $2 < q$. There are two cases for q: q even (bigger than 4) or q odd (bigger than 3). In the former case, $q = 2k$, for some integer $k > 1$, and, hence, $a = 3(2k)+2 = 6k+2$, which means that $a \bmod 6 = 2 \neq 3$. In the latter case, $q = 2k + 1$, for some integer $k > 1$, and, hence, $a = 3(2k + 1) + 2 = 6k + 5$, which means that $a \bmod 6 = 5 \neq 3$.

4.6 Examples of Indirect Arguments

Examples of Indirect Arguments

- $\sqrt{2}$ is irrational.
- $1 + 3\sqrt{2}$ is irrational.
- For any integer a and any prime number p, if $p|a$, then $p \nmid (a + 1)$.
- The set of prime numbers is infinite.

4.6 Uniqueness of Quotient and Remainder

Theorem (Uniqueness of Quotient and Remainder in the Quotient-Remainder Theorem)

If $a, d \in \mathbb{Z}, d > 0$, *and if there exist* $q_1, r_1, q_2, r_2 \in \mathbb{Z}$ *such that*

$$a = dq_1 + r_1, \text{ where } 0 \leq r_1 < d,$$
$$a = dq_2 + r_2, \text{ where } 0 \leq r_2 < d,$$

then

$$q_1 = q_2 \text{ and } r_1 = r_2.$$

Sketch of Proof: First, show that $dq_1 + r_1 = dq_2 + r_2$ (A) implies that $d|(r_2 - r_1)$. Next, show that $|r_2 - r_1| < d$. Why then (A) would imply that $r_2 - r_1 = 0$? Consequently, show that $q_1 = q_2$. Why?

4.6 Uniqueness of Quotient and Remainder

Lemma

For any $a \in \mathbb{Z}$, if $5|a^2$, then $5|a$.

Sketch of Proof: Suppose the opposite, i.e., that there exists $a \in \mathbb{Z}$ such that $5|a^2$ and $5 \nmid a$. The former condition would imply that $a^2 = 5q$, for some $q \in \mathbb{Z}$ (A). The latter condition and the Quotient–Remainder Theorem imply that $a = 5k + r$, for some $k \in \mathbb{Z}$, where $r = 1, 2, 3, 4$. (Why has $r = 0$ been excluded?) Therefore, we have four cases: $a = 5k + 1$, $a = 5k + 2$, $a = 5k + 3$, $a = 5k + 4$. In the first case, $a = 5k + 1$, we get $a^2 = (5k + 1)^2 = 5(5k^2 + 2k) + 1$, which is of the form $a^2 = 5q_1 + 1$, for some $q_1 \in \mathbb{Z}$ (B). However, by the quotient and remainder uniqueness, conditions (A) and (B) are contradictory. Examine the three remaining

Proposition

$\sqrt{5} \notin \mathbb{Q}$.

Sketch of Proof: If $\sqrt{5} \in \mathbb{Q}$, then $\sqrt{5} = \frac{m}{n}$, for some $m, n \in \mathbb{Z}\,(n \neq 0)$ having no common factors. Thus, $5 = \frac{m^2}{n^2}$ or $m^2 = 5n^2$ (A). In other words, $5|m^2$ and, hence, according to the above Lemma, $5|m$ or $m = 5k$, for some $k \in \mathbb{Z}$, which means that $m^2 = (5k)^2 = 5(5k^2)$ (B). Why then (A) and (B) would imply that $n^2 = 5k^2$? Actually, the latter means that $5|n^2$ and, again by the above Lemma, $5|n$. But, then, the assumption that m and n have no common factors would be contradicted.

4.6 More Propositions (Problems)

Proposition

For any $a \in \mathbb{Z}$, $9 \nmid (a^2 - 3)$.

Sketch of Proof: Assume the opposite, i.e., $a^2 - 3 = 9b$, for some $b \in \mathbb{Z}$, which would imply that $a^2 = 9b + 3 = 3(3b + 1)$ (A) or that $3|a^2$ and, thus, thanks to the Lemma, $3|a$. Then $a = 3c$, for some $c \in \mathbb{Z}$, and, hence, $a^2 = 9c^2 = 3(3c^2)$ (B). Why then would conditions (A) and (B) imply that $3b + 1 = 3c^2$? This would mean that $3|3b + 1$, but together with the obvious fact that $3|3b$, we have reached a contradiction (3 as prime number cannot divide two consecutive integers).

Proposition

$\sqrt{2} + \sqrt{3} \notin \mathbb{Q}$.

Sketch of Proof: Assume the opposite, i.e., $\sqrt{2} + \sqrt{3} = \frac{a}{b}$, for some $a, b \in \mathbb{Z}\,(b \neq 0)$. Thus, $a = (\sqrt{2} + \sqrt{3})b$, from which we get $\sqrt{3} = \frac{a}{b} - \sqrt{2}$. Squaring the latter and multiplying by b^2 yields (fill up details) $b^2 = a^2 - 2ab\sqrt{2}$, something which would represent $\sqrt{2} = \frac{a^2 - b^2}{2ab} \in \mathbb{Q}$ (why?) and this would be a contradiction.

4.6 An Alternative Proof of the Infinitude of Primes

Theorem

The set of prime numbers is infinite.

Sketch of Proof: Suppose not. Then there would exist a finite set of primes $P = \{2, 3, \ldots, p\}$, in which p is the largest prime and there would exist no other prime outside P. Let $M = p! + 1$. Notice that any prime in the finite set P would divide $p!$, but none would divide M (why?). However, we know that any number $M > 1$ should be divisible by a prime (Theorem 4.3.4 of divisibility by a prime), which means that there would exist a prime q such that $q|M$. Now, $q \notin P$, i.e., it would be impossible that prime $q \leq p$, because we have shown that none prime in P would divide M. Therefore, we found a prime q outside P, which is a contradiction.

4.6 Another Proposition (Problem)

Proposition

For any $n \in \mathbb{Z}$, if $n > 2$, then there exists a prime number p such that $n < p < n!$.

Sketch of Proof: By the divisibility by a prime Theorem 4.3.4, $n! - 1$ is divisible by a prime p (why?). Now, the fact that $p|(n! - 1)$ (A) makes $p \leq (n! - 1)$ and, thus, $p \leq n!$. On the other side, either $p > n$ or $p \leq n$. The latter inequality would imply that $p|n!$, but this would lead to a contradiction if it was satisfied together with (A). Hence, the former inequality ($n < p$) is true.