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 4a

Elementary Number Theory and Methods of Proof, I, II, II

September 13, 15, & 17, 2021

4.1 Direct Proof and Counterexample I: Assumptions

Assumptions

- Familiarity is assumed with the laws of basic algebra (listed in Appendix A of the textbook).
- The three properties of equality: For all objects A, B, and C, (1) $A = A$, (2) if $A = B$ then $B = A$, and (3) if $A = B$ and $B = C$, then $A = C$.
- In addition, we assume that there is no integer between 0 and 1 and that the set of all integers is closed under addition, subtraction, and multiplication. This means that sums, differences, and products of integers are integers.
- Of course, most quotients of integers are not integers. For example, $3 \div 2$, which equals $\frac{3}{2}$, is not an integer, and $3 \div 0$ is not defined.

4.1 Even, Odd, Prime and Composite Integers

Definition of Even and Odd Integers

An integer n is **even** if, and only if, n equals twice some integer. An integer n is **odd** if and only if n equals twice some integer plus 1. Symbolically, if $n \in \mathbb{Z}$, then

- n is even $\iff \exists\ k \in\ \mathbb{Z}$ such that $n = 2k$.
- n is odd $\iff \exists\ k \in \mathbb{Z}$ such that $n = 2k + 1$.

Definition of Prime and Composite Positive Integers

An integer n is **prime** if and only if $n > 1$ and, for all positive integers r and s, if $n = rs$, then either r or s equals n (and the other, necessarily, to 1). An integer n is **composite** if and only if $n > 1$ and $n = rs$, for some positive integers r and s, with $r < n$ and $s < n$. In symbols: For all $n \in \mathbb{Z}^+$,

- n is prime $\iff \forall\ r, s \in \mathbb{Z}^+$, if $n = rs$ then either $r = 1$ and $s = n$ or $r = n$ and $s = 1$.
- n is composite $\iff \exists\ r, s \in \mathbb{Z}^+$ such that $n = rs$ and $r < n$ and $s < n$.

Python Code

```
def is_evenodd(num):
    if type(num) != int:
        print(num,"is not an integer")
    else:
        if num%2 == 0:
            out="%i is an even integer" %num
#               print(num,"is an even integer")
        else:
            out="%i is an odd integer" %num
#               print(num,"is an odd integer")
    return out

def is_primecomposite(num):
    # prime numbers are greater than 1
    if type(num) != int:
        print(num,"is not an integer")
    else:
        if num <= 1:
            print(num,"is not an integer > 1")
        else:
            if num > 1:
            # check for factors
                for i in range(2,num):
                    if (num % i) == 0:
                        out="%i is a composite number, %i = %ix%i" %(num, num,i,num//i)
                        return out
                        break
                else:
                    out="%i is a prime number" %num
                    return out
```

4.1: Constructive and Nonconstructive Proofs of Existence

Definition

- **Constructive proof of existence** is the demonstration of the existence of certain mathematical object by first identifying or constructing such an object.
- **Nonconstructive proof of existence** is the demonstration of the existence of certain mathematical object without providing a specific example or a means for producing the object. Typically a nonconstructive proof of existence involves showing one of the following:
  - Either that the existence of that object is guaranteed by an axiom or a previously proved theorem without constructing that object (**direct nonconstructive proof**).
  - Or that the assumption that there exists no such object leads to a contradiction (**nonconstructive proof by contradiction**).

4.1: An Example of Constructive Proof of Existence

Example

Show that there exists an even integer n such that n can be written in two ways as a sum of two primes.

```
E100=[n for n in range(2,101) if "even" in is_evenodd(n)]
P100=[n for n in range(2,101) if "prime" in is_primecomposite(n)]
d={}
for n in E100:
    t=[]
    for m1 in P100:
        for m2 in P100:
            if n==m1+m2:
                t.append([m1,m2])
    for s in t:
        if s[::-1] in t and s[0]!=s[1]:
            t.remove(s[::-1])
    if len(t)>1:
        d[n]=t
for k,v in d.items():
    print(k,v)
```

```
10 [[3, 7], [5, 5]]
14 [[3, 11], [7, 7]]
16 [[3, 13], [5, 11]]
18 [[5, 13], [7, 11]]
20 [[3, 17], [7, 13]]
22 [[3, 19], [5, 17], [11, 11]]
24 [[5, 19], [7, 17], [11, 13]]
26 [[3, 23], [7, 19], [13, 13]]
28 [[5, 23], [11, 17]]
30 [[7, 23], [11, 19], [13, 17]]
32 [[3, 29], [13, 19]]
```

4.1: Example of Nonconstructive Proof of Existence by Contradiction

Example (Euclid's Proof that $\sqrt{2}$ is Irrational)

Prove that $\sqrt{2}$ is an irrational number.

Proof: Assume the opposite, i.e., that $\sqrt{2} \in \mathbb{Q}$. This means that $\sqrt{2} = \frac{a}{b}$, for $a, b \in \mathbb{Z}$ ($b \neq 0$), where we may assume that a and b have no common factors (because otherwise we could cancel them). Squaring, we get $2 = \frac{a^2}{b^2}$ or $a^2 = 2b^2$. Hence, a^2 is even and, necessarily, a is even (because the square of an odd number is odd too), i.e., $a = 2k$, for some $k \in \mathbb{Z}$. Substituting in the expression of a, we get $4k^2 = 2b^2$, i.e., that b^2 is even and hence b should be even too. But if both a and b are even, this is a contradiction to the assumption that they have no common factors. Consequently, $\sqrt{2}$ cannot be rational. $\blacksquare$

4.1: Example of Direct Nonconstructive Proof of Existence

Example

Prove that there exist irrational numbers a and b such that the number a^b is rational number.

Proof: We consider $a = b = \sqrt{2}$. If $\sqrt{2}^{\sqrt{2}}$ is rational, we have found the numbers $a = b = \sqrt{2}$. Otherwise (if $\sqrt{2}^{\sqrt{2}}$ is irrational), we consider $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$. Then $a^b = (\sqrt{2})^{(\sqrt{2}\times\sqrt{2})} = (\sqrt{2})^2 = 2$, which is again rational. Thus, we have proven the statement without finding a unique object which satisfies the property of its definition. $\blacksquare$

4.1: Disproving Universal Statements by Counterexample

Disproof by Counterexample

To disprove a universal statement of the form "$\forall x \in D$, if $P(x)$, then $Q(x)$," find a value of x in D for which the hypothesis $P(x)$ is true and the conclusion $Q(x)$ is false. Such an x is called a **counterexample**.

Example

Disprove the statement: $\forall x \in \mathbb{R}$, if $x < 2$, then $x^2 < 4$.

Counterexample: For any $x \leq -2$, $x^2 \geq 4$. ■

The Method of Exhaustion

To prove a universal statement of the form "$\forall x \in D, P(x)$," when D is finite and has a very small size, then we may simply verify $P(x)$, for each individual element $x \in D$.

Example

Show that $\forall x \in \{-1, 0, 1\}, x^3 = x$.

Proof by Exhaustion: $(-1)^3 = -1, 0^3 = 0,$ and $1^3 = 1$. $\blacksquare$

4.1: Proving Universal Statements by Generalization

The Principle of Generalization

To prove a universal statement of the form "$\forall x \in D, P(x)$," then one may consider a **generic** element $x \in D$ and correspondingly prove $P(x)$.

Example 1

Show that $\forall x \in \mathbb{R}, x^2 + 1 > 0$.

Proof: Suppose $x \in \mathbb{R}$. Since the square of any real number is nonnegative, we have $x^2 \geq 0$. Hence, $x^2 + 1 \geq 0 + 1 = 1 > 0$. ■

Example 2

Show that the sum of any two even integers is also even.

Proof: Let $m, n \in \mathbb{Z}$ be even. Since, necessarily, $m = 2p$ and $n = 2q$, for some $p, q \in \mathbb{Z}$, it follows that $m + n = 2p + 2q = 2(p + q)$, for $p + q \in \mathbb{Z}$, i.e., $m + n$ is even. ■

Common Mistakes

- Arguing from examples:

  Because for the particular $m = 14$ and $n = 6$, $m + n = 20$ even, it does not mean that $\forall m, n, m + n$ is even!
- Using the same letter to mean two different things:

  If $m, n \in \mathbb{Z}$ are even, then writing $m = 2k$ and $n = 2k$, for some (and the same) $k \in \mathbb{Z}$ is wrong!
- Jumping to a conclusion:

  If $m, n \in \mathbb{Z}$ are even, then although $m = 2p$ and $n = 2q$, for some $p, q \in \mathbb{Z}$, it is wrong to say that $m + n$ is even, just because $m + n = 2p + 2q$!
- Assuming what is to be proved:

  When two odd integers are multiplied, their product needs to be proved to be odd, not assumed that it is!
- Confusing what is known with what is to be shown!
- Use of *any* rather than *some*!
- Misuse of *if* (as *when*)!

Recall

To disprove an existential statement is equivalent to proving that its negation is true.

Example 2

Show that the following statement is false:

There is a $n \in \mathbb{Z}^+$ such that $n^2 + 3n + 2$ is prime.

Proof: It suffices to show that, for all $n \in \mathbb{Z}^+$, $n^2 + 3n + 2$ is composite. Indeed, $n^2 + 3n + 2$ can be factored as $n^2 + 3n + 2 = (n + 1)(n + 2)$, where both $n + 1$ and $n + 2$ are positive integers greater than 1, and so $n^2 + 3n + 2$ is composite. ■

4.2 Rational Numbers, I

Definition

A real number r is said to be **rational** if $r = \frac{a}{b}$ for some integers a and b with $b \neq 0$. The set of all rational numbers is denoted by $\mathbb{Q}$. Apparently, $\mathbb{Q} \subset \mathbb{R}$.

Theorem

$$\mathbb{Z} \subset \mathbb{Q}.$$

Recognizing Rational Numbers

- Real numbers with finite decimal expansions are rational. Let $x = 78.592$. Then $x = \frac{78592}{1000} \in \mathbb{Q}$.
- Real numbers with repeating decimal expansions are rational.
  - Let $x = 27.\overline{531} = 27.531531\ldots$. So, $1000x = 27531.531531\ldots$ and, hence, $999x = 1000x - x = 27504$. Therefore, $x = \frac{27504}{999} = \frac{3056}{111} \in \mathbb{Q}$.
  - Let $x = 0.35\overline{826} = 0.35826826\ldots$. So, $100000x = 35826.\overline{826}$ and $100x = 35.826$. Hence, $99900x = 100000x - 100x = 35826 - 35 = 35791$. Therefore, $x = \frac{35791}{99900} \in \mathbb{Q}$.

4.2 Rational Numbers, II

Theorem

The sum, product and ratio of two non–zero rational numbers are rational numbers.

Theorem (Expressing rational Numbers in Lowest Terms)

Given $r \in \mathbb{Q}$, there exist unique $a, b \in \mathbb{Z}$ such that $b > 0$, $\gcd(a, b) = 1$ and $r = \frac{a}{b}$.

Theorem (When Decimals Are Rational)

A real number written in decimal form represents a rational number if and only if the decimal part is either finite or repeating. Moreover, a rational number $r = \frac{a}{b}$ written in lowest terms has a finite decimal expansion if and only if 2 and/or 5 are the only prime divisors of b. Otherwise, the decimal part of r repeats.

(A Finite Decimal Expansion)

$$\frac{63}{160} = 0.39375$$

$$\begin{array}{rrl}
 & .39375 & \\
160 \overline{)\ 63.0} & & \\
 -480 & & \\
 \overline{1500} & & \text{remainder } 150 \\
 -1440 & & \\
 \overline{600} & & \text{remainder } 60 \\
 -480 & & \\
 \overline{1200} & & \text{remainder } 120 \\
 -1120 & & \\
 \overline{800} & & \text{remainder } 80 \\
 -800 & & \\
 \overline{0} & & \text{remainder } 0 \leftarrow \text{END}
\end{array}$$

The decimal expansion ends when a remainder of 0 is encountered.

(A Repeating-Decimal Expansion)

$$\frac{389}{3700} = 0.10\overline{513}$$

$$\begin{array}{rrl}
 & .10513 & \\
3700 \overline{)\ 389.0} & & \\
 -3700 & & \\
 \overline{1900} & & \text{remainder } 190 \\
 -0 & & \\
 \overline{19000} & & \text{remainder } 1900 \\
 -18500 & & \\
 \overline{5000} & & \text{remainder } 500 \\
 -3700 & & \\
 \overline{13000} & & \text{remainder } 1300 \\
 -11100 & & \\
 \overline{1900} & & \text{remainder } 1900
\end{array}$$

4.3 Divisibility, I

Definition

Given integers n and d (with $d \neq 0$), we say that d **divides** n, written $d|n$, if $n = dk$ for some integer k. In this case, we also say that n is **divisible** by d, that n is a **multiple** of d, that d is a **divisor** of n, and that d is a **factor** of n. When n is not divisible by d, we write $d \nmid n$.

Theorem (Transitivity of of the Divisibility Relation)

Let $a, b, c \in \mathbb{Z}$. If $a|b$ and $b|c$, then $a|c$.

Theorem

Let $a, b \in \mathbb{Z}$ with $b > 0$. If $a|b$, then $a \leq b$.

Theorem (Fundamental Theorem of Arithmetic)

Any integer $n > 1$ can be written as a product of primes. Moreover, if the primes are written in nondecreasing order, then the factorization is unique. In symbols, if, on the one hand,

$$n = p_1 p_2 \cdots p_i,$$

where $p_1, p_2, \ldots, p_i$ are primes and $p_1 \leq p_2 \leq \cdots \leq p_i$, and, on the other hand,

$$n = p'_1 p'_2 \cdots p'_j,$$

where $p'_1, p'_2, \ldots, p'_j$ are primes and $p'_1 \leq p'_2 \leq \cdots \leq p'_j$, then $i = j$ and

$$p_k = p'_k, \text{ for all } k = 1, 2, \ldots, i.$$

Corollary

Any integer $n > 1$ is divisible by a prime number.

4.3 Divisibility, III

Equivalent Definition of Composite Integers

An integer $n > 1$ is composite if and only if there exists an integer r such that $r|n$ and $1 < r < n$.

Theorem

An integer $n > 1$ is composite if and only if n has a divisor r such that $2 \le r \le \sqrt{n}$.

Proof: If $n > 1$ is composite, there exists integer s such that $s|n$ and $1 < s < n$. There are two cases: either $s \le \sqrt{n}$ or $s > \sqrt{n}$. In the former case, we have reached the conclusion (for $r = s$). In the latter case, since $s|n$, $n = rs$, for a second factor r such that $1 < r < n$. We claim that $r \le \sqrt{n}$. In fact, assuming the opposite, i.e., that $r > \sqrt{n}$, we would get

$$n = rs > \sqrt{n}\sqrt{n} = n,$$

which is a contradiction. Therefore, $r|n$ and $2 \le r \le \sqrt{n}$. Conversly, if n has a divisor r such that $2 \le r \le \sqrt{n}$, then, since for $n > 1$, $\sqrt{n} < n$, we have $1 < r < n$, which implies that n is composite. ■

Python Function to Find all Factors of an Integer

To determine whether integer $n > 1$ is prime, one should check whether none of the integers in the interval from 2 to $\lfloor \sqrt{n} \rfloor$ divides n. Otherwise, one would have found a factor of n so that n would be composite.

```
import math
def primefactors(n):
    fl=[]
    while n % 2 == 0:
        fl.append(2)
        n = int(n / 2)
    for i in range(3,int(math.sqrt(n))+1,2):
        while (n % i == 0):
            fl.append(i)
            n = int(n / i)
    if n > 2:
        fl.append(n)
    p=1
    for i in fl:
        p*=i
    return fl, p
```

Practice Excercises, I

Prove the following statements:

1. The difference of any even integer minus any odd integer is odd.
2. If k is any odd integer and m is any even integer, then $k^2 + m^2$ is odd.
3. If n is any even integer, then $(-1)^n = 1$.
4. The product of any two odd integers is odd.
5. The product of any two rational numbers is a rational number.
6. The difference of any two rational numbers is a rational number.
7. If r and s are rational, then their average is rational.
8. If m is even and n is odd, then $m^2 + 3n$ is odd.

Practice Excercises, II

Prove the following statements:

9. For all integers a, b, c, if $a|b$ and $a|c$ then $a|(b \pm c)$.
10. For all integers a, b, c, if $a|b$ then $a|bc$.
11. A necessary condition for an integer to be divisible by 6 is that it be divisible by 2.