Advanced Discrete Math: Meeting 1

1 Introduction

• Syllabus
• Why study discrete math? (popular b/c of computers)
• Topics we’re likely to cover, quick survey about prior knowledge

2 Proving Properties of the Integers

What’s the difference between advanced calc and calc? Proofs. Similarly, I’m going to start with basic proofs about integers, the prototypical “discrete” objects. Forget everything you knew...

2.1 Assumptions

• We’ll assume basic properties about the integers that we can understand from physical analogs:
  – comparison (less-than relation, etc.)
  – basic operations: addition, subtraction, multiplication (but not division)
  – basic principles: commutative/associative/distributive
  – simple algebra (add number to both sides of equality, still have equality)

• Also assume truth of a key axiom (need because of infinite nature of integers): Well Ordering Principle (WOP): Every nonempty set of nonnegative integers has a least element

• Everything else about integers has to be proved!

2.2 Proving the First Principle of Mathematical Induction

(See Section 3.3.)

• First Principle of Mathematical Induction: Let \( Q() \) be a propositional function over the positive integers such that:

  1. \( Q(1) \) is true
  2. The implication \( Q(n) \rightarrow Q(n + 1) \) has been shown to be true for an arbitrary positive integer \( n \) (and therefore is true for all positive \( n \), by the principle of universal generalization).
Then $Q(n)$ is true for all positive integers $n$, i.e., $\forall n \in \mathbb{Z}^+, Q(n)$.

- Example of universal quantification of propositional function proved true using first principle of mathematical induction: $\forall n > 0, \sum_{i=1}^{n} i = n(n + 1)/2$.

- Proof of First Principle of Mathematical Induction by contradiction:
  - Assume (for purposes of contradiction) that there is a propositional function $Q()$ such that conditions of the first principle of mathematical induction are satisfied but it is not true that $Q(n)$ is true for all positive $n$.
  - Let $S$ be set of all $m$ such that $Q(m)$ is false, that is, $S = \{ m \in \mathbb{Z}^+ : \neg Q(m) \}$.
  - Then by WOP there is a least such $m$. Call it $m_0$.
  - Since $m_0$ is the least integer in $S$, $m_0 - 1$ is an integer that is not in $S$.
  - We know that $m_0 \neq 1$, because $Q()$ is assumed to meet the conditions of the first principle and therefore $Q(1)$ is true.
  - Therefore, $m_0 \geq 2$.
  - Therefore, $m_0 - 1$ is a positive integer not in $S$.
  - By the definitions of $Q()$ and $S$, $Q(m_0 - 1)$ is true.
  - But because $Q()$ meets the conditions of the first principle, if $Q(m_0 - 1)$ is true then $Q(m_0)$ must be as well (by the principle of universal instantiation).
  - We therefore have reached a contradiction, which implies that our initial assumption was false.

2.3 Second Principle

- Second Principle of Math Induction: Let $Q()$ be a propositional function over the positive integers such that:
  1. $Q(1)$ is true
  2. The implication $(Q(1) \land Q(2) \land \cdots \land Q(n)) \rightarrow Q(n + 1)$ has been shown to be true for arbitrary positive integer $n$ (and therefore for all positive integers $n$).

Then $Q()$ is true for all positive integers.

- Second Principle of Math Induc can be similarly proved (homework)

2.4 Division

- Definitions: For integers $a$, $b$, and $c$,
  - $a$ divides $b$ iff $\exists c$ s.t. $ac = b$
- $a$ is a factor of $b$ iff $a$ divides $b$
- $b$ is a multiple of $a$ iff $a$ divides $b$

**Notation** $a | b$, $a \nmid b$

**Theorem 2.3.1:** Basic facts about divisibility that are easily proved from definitions. For all integers $a$, $b$, and $c$,

1. $a | b$ and $a | c$ implies $a | (b + c)$
2. $a | b$ implies $a | bc$
3. $a | b$ and $b | c$ implies $a | c$

**Definitions:** For all integers $i$ greater than 1,

- Iff the only factors of $i$ are 1 and $i$, then $i$ is prime.
- Iff $i$ is not prime, then $i$ is composite.

**A prime factorization** of an integer $n > 1$ is a product of primes, written from smallest to largest, such that the product is equal to $n$. Example: $3 \cdot 5 \cdot 5$ is a prime factorization of 75.

**Fundamental Theorem of Arithmetic:** Every integer greater than 1 has a unique prime factorization. Proof in two parts:

- Every number has a factoring: induction using 2nd principle (Section 3.3 Example 14).
- Every factoring is unique: more involved proof, but not impossible. We’ll return to this later (you’ll do key part for homework: 3.3 # 66. The steps a) through e) are an outline of the proof of the fact that there is a unique gcd of any two positive integers.).

**A prime factorization can be found by the following simple but slow algorithm:** divide out all 2’s, then all 3’s, then all 5’s, ...

**Whether or not a prime factorization can be found efficiently** (computationally) has significant practical importance because the cryptography underlying most e-commerce systems is based on the assumption that it is computationally infeasible to find the prime factorizations of large numbers.

**Note that if checking to see if a number is a prime, only need to check for prime factors up to square root of the number (why?)**

**Division “algorithm”** (actually “theorem”): Every pair of integers (divisor positive) has a unique quotient and remainder (non-negative, < divisor). Symbolically, for every pair of integers $a$ and $d$, $d > 0$, there exist unique $q$ and $r$ such that $a = dq + r$ and $0 \leq r < d$. Proof in two parts again:
Existence (Section 3.3 Example 16): Fix $a$ and $d$ and let $S = \{a - dq : q \text{ is an integer and } a - dq \geq 0\}$. Note that all possible $r$’s are in this set. Note nonempty because can always pick $q$ so that $a - dq$ is positive. So WOP applies, so $S$ has minimum. Then just argue by contradiction that $r$ cannot be as large as $d$.

Uniqueness: Exercise 3.3 # 75.

- Greatest common divisor (gcd)
  - Define: greatest integer that divides both inputs
  - Is this well-defined? Yes. You prove uniquely exist by Exer 3.3 # 66.
  - In fact, proof of # 66 also proves Thm 2.6.1 from which Lemma 2.6.1 follows from which Lemma 2.6.2 follows (proof is 3.3 Ex # 63) and finally uniqueness of factorization follows (proof is after statement of Lemma 2.6.2). We’ll go through this in more detail next time.
  - So if have prime factorizations of $a$ and $b$, then gcd($a, b$) easy to find. The rule used (min exponents) is correct because (Section 2.4 Example 13)
    * gcd found this way is certainly a divisor of $a$ and $b$
    * By the assumption of unique prime factorization, the factorization of any larger number must either contain a prime not in the gcd (but therefore not a factor of at least one of the numbers) or a prime power that is larger than one of the original numbers (and therefore again not a factor of that number).

- Also define relatively prime, pairwise rel. prime. gcd of course easy to find if numbers known to be rel. prime: just 1!

- Definition: lcm (exists by WOP, since set of common multiples is nonempty). Again easy to find if prime factorizations known.

- Thm(2.4.7): $ab = \text{gcd}(a, b) \cdot \text{lcm}(a, b)$

### 2.5 Modular Arithmetic

- Definitions (modular arithmetic):
  - $a \mod m$ (remainder when $a$ divided by $m$)
  - $a \equiv b \pmod m$: (statement that $a - b$ is divisible by $m$), read as “$a$ is congruent to $b$ mod $m$”

- Several properties of congruence:
  - $a \equiv b \pmod m$ iff $a \mod m = b \mod m$
  - $a \equiv b \pmod m$ iff $\exists k. a = b + km$
  - If $a \equiv b \pmod m$ and $c \equiv d \pmod m$ then
\[ (a + c) \equiv (b + d) \pmod{m} \]
\[ (ac) \equiv (bd) \pmod{m} \]

- Applications of modular arithmetic:
  - Hashing (mod is an onto function)
  - Pseudorandom Number Generators (prng’s) often formed using the linear congruential method: \( s_{i+1} = (c_1 s_i + c_2) \mod c_3 \)
  - Ceasar’s cypher (e.g., rot13)
  - Various math questions (what is the day of the week 1000 days from now?)

- Euclid’s gcd algorithm: another way to find gcd that works even if it’s hard to factor the inputs

- Quick example: \( \text{gcd}(54, 24) \):
  
  \[
  54 \mod 24 = 6 \\
  24 \mod 6 = 0 \\
  \text{gcd} = 6 \text{ (last nonzero result)}
  \]

- We’ll prove that this always produces the right result next time.