Exam 2 (Part 2)

Your Name:

Names of Any Collaborators:

Instructions

Submit your solutions to the following questions by 5PM on **Friday, March 28**. This part of Exam 2 is worth a total of 16 points and is worth 50% of your overall score on Exam 2. Your overall score on Exam 2 is worth 15% of your overall grade.

I expect your solutions to be *well-written, neat, and organized*. Do not turn in rough drafts. What you turn in should be the "polished" version of potentially several drafts. Feel free to type up your final version. The LaTeX source file of this exam is also available if you are interested in typing up your solutions using LaTeX. I'll gladly help you do this if you'd like.

Reviewing material from previous courses and looking up definitions and theorems you may have forgotten is fair game. However, when it comes to completing the following problems, you should *not* look to resources outside the context of this course for help. That is, you should not be consulting the web, other texts, other faculty, or students outside of our course in an attempt to find solutions to the problems you are assigned. This includes ChatGPT, Chegg, and Course Hero. On the other hand, you may use each other, the textbook, me, and your own intuition. Further information:

1. You may freely use any theorems that we have discussed in class, but you should make it clear where you are using a previous result and which result you are using. For example, if a sentence in your proof follows from Theorem X.Y, then you should say so.
2. Unless you prove them, you cannot use any results from the course notes that we have not yet covered.
3. You are **NOT** allowed to consult external sources when working on the exam. This includes people outside of the class, other textbooks, and online resources.
4. You are **NOT** allowed to copy someone else's work.
5. You are **NOT** allowed to let someone else copy your work.
6. You are allowed to discuss the problems with each other and critique each other's work.

I will vigorously pursue anyone suspected of breaking these rules.

You should **turn in this cover page** and all of the work that you have decided to submit. **Please write your solutions and proofs on your own paper.** To convince me that you have read and understand the instructions, sign in the box below.

Signature:

Good luck and have fun!

You may need to digest some new content in the book to complete the following problems. We will spend some time discussing these concepts in class during the time you have available to work on the exam. However, you should not wait until I have discussed the relevant topics. Just dig in and get started.

When completing each of the tasks below, you may utilize any result in the book that comes before the particular problem/theorem, regardless of whether you proved the previous result or not.

Warning: This exam is not easy! You will need to budget time to work on it. You will likely need assistance from your peers and from me. Also, it'll be very easy for me to determine whether you've cheated by using something like ChatGPT since the approach I'm asking you to take is likely not the one the Internet usually takes. Don't be tempted.

1. (4 points) Prove Theorem 4.38 (Well-Ordering Principle), which states that every nonempty subset of the natural numbers has a least element.

   Hint: It might be surprising that this seemingly obvious result needs proof. Here is the approach I want you to take. We will utilize a proof by contradiction, together with induction. For sake of contradiction, suppose there exists a set S that is a nonempty subset of $\mathbb{N}$ that does not have a least element. Use complete induction to prove that for every $n \in \mathbb{N}$, $n \notin S$.

2. (4 points each) Digest Definition 6.1, Theorem 6.7 (Division Algorithm), and Definition 6.10, and then complete **two** of the following.

   (a) Prove Theorem 6.6, which says that if n is a natural number greater than 1, then n can be expressed as a product of primes. That is, we can write

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

   where each of $p_1, p_2, \ldots, p_k$ is a prime number (not necessarily distinct).

   Hint: Let S be the set of natural numbers for which the theorem fails. For sake of a contradiction, assume $S \neq \emptyset$. By the Well-Ordering Principle (Theorem 4.38), S contains a least element, say n. Then n cannot be prime since this would satisfy the theorem. So, it must be the case that n has a divisor other than 1 and itself. This implies that there exists natural numbers a and b greater than 1 such that $n = ab$. Since n was our smallest counterexample, what can you conclude about both a and b? Use this information to derive a contradiction for n.

   (b) Prove Theorem 6.13 (Special Case of Bézout's Lemma), which says if $p, a \in \mathbb{Z}$ such that p is prime and p and a are relatively prime, then there exists $s, t \in \mathbb{Z}$ such that $ps + at = 1$.

   Hint: consider the set $S \coloneqq \{ps + at > 0 \mid s, t \in \mathbb{Z}\}$. First, observe that $p \in S$ (choose $s = 1$ and $t = 0$). It follows that S is nonempty. By the Well-Ordering Principle (Theorem 4.38), S contains a least element, say d. This implies that there exists $s_1, t_1 \in \mathbb{Z}$ such that $d = ps_1 + at_1$. Our goal is to show that $d = 1$. Now, choose $m \in S$. Then there exists $s_2, t_2 \in \mathbb{Z}$ such that $m = ps_2 + at_2$. By the definition of d, we know $d \leq m$. By the Division Algorithm, there exists unique $q, r \in \mathbb{N} \cup \{0\}$ such that $m = qd + r$ with $0 \leq r < d$. Now, solve for r and then replace m and d with $ps_1 + at_1$ and $ps_2 + at_2$, respectively. You should end up with an expression for r involving p, a, s_1, s_2, t_1, and t_2. Next, rearrange this expression to obtain r as a linear combination of p and a (i.e., a sum of a multiple of p and a multiple of a). What does the minimality of d imply about r? You should be able to conclude that m is a multiple of d. That is, every element of S is a multiple of d. However, recall that $p \in S$, p is prime, and p and a are relatively prime. What can you conclude about d?

(c) Prove Theorem 6.15 (Euclid's Lemma), which says if a prime p divides ab, where $a, b \in \mathbb{N}$, then either p divides a or p divides b.

Hint: Note that if p divides a, the conclusion is certainly true. So, assume otherwise. That is, assume that p does not divide a, so that p and a are relatively prime. Apply Theorem 6.13 to p and a and then multiply the resulting equation by b. Try to conclude that p divides b.

3. (4 points) Prove Theorem 6.17 (Fundamental Theorem of Arithmetic), which says that every natural number greater than 1 can be expressed uniquely (up to the order in which they appear) as the product of one or more primes.

Hint: Let n be a natural number greater than 1. By Theorem 6.6, we know that n can be expressed as a product of primes. All that remains is to prove that this product is unique (up to the order in which they appear). For sake of a contradiction, suppose $p_1 p_2 \cdots p_k$ and $q_1 q_2 \cdots q_l$ are both prime factorizations of n. Your goal is to prove that $k = l$ and that each p_i is equal to some q_j. Make repeated use of Euclid's Lemma.

