Discrete Mathematics
CMSC 27100
Winter Quarter 2022
Practice Midterm Answer Key

1 Mathematical Sets

Exercise 1.1

a) $A = \{p \in \mathbb{P} : p > 10\}$

Explanation: Denote our set by A. Firstly, let us ensure that we are only considering prime numbers. Then for our set, we wish to only consider a $p \in \mathbb{P}$ if it satisfies the condition of being greater than 10. Thus, we say $A = \{p \in \mathbb{P} \colon p > 10\}$. □

b) $B = \{z \in \mathbb{Z} : z < 0 \vee (z \in \mathbb{P})\}$

Explanation: Denote our set by B. Similar to part a), we ensure we only consider integers if we first start with a $z \in \mathbb{Z}$. Afterwards, we want such an integer z to either be negative or prime. We can write that z is negative by writing $z < 0$ and we can write that z is prime by writing $z \in \mathbb{P}$. Thus, we can write $B = \{z \in \mathbb{Z} \colon (z \in \mathbb{Z} \setminus (\mathbb{N} \cup \{0\})) \vee (z \in \mathbb{P})\}$. □

c) $C = \{n \in \mathbb{N} \colon \sqrt{n} \in \mathbb{N}\}$

Explanation: Denote our set by C. Again, like before we first take $n \in \mathbb{N}$. Now we want such an n to only be included in C is its root is also a natural number. This means that $\sqrt{n}$ must also be in $\mathbb{N}$. Thus, $C = \{n \in \mathbb{N} \colon \sqrt{n} \in \mathbb{N}\}$. □

Note: This set of numbers is equal to the set of positive squares, so we can also write $C = \{x^2 : x \in \mathbb{N}\}$

d) $D = \{n \in \mathbb{N} \colon \sqrt[3]{n} \in \mathbb{P} \wedge \frac{n^2}{2} \in \mathbb{N}\}$

Explanation: Denote our set by D. Take $n \in \mathbb{N}$. We see that we have an "and" condition, which means both given conditions must be met for our n to be included in D. The first condition is that the third root is prime, meaning $\sqrt[3]{n} \in \mathbb{P}$. However, this n must also have a square which is even. So, $\frac{n^2}{2} \in \mathbb{N}$. Thus, our set $D = \{n \in \mathbb{N} \colon \sqrt[3]{n} \in \mathbb{P} \wedge \frac{n^2}{2} \in \mathbb{N}\}$. □

Note: If n^2 is even then n is also even. If n is even and $\sqrt[3]{n}$ is an integer then $\sqrt[3]{n}$ is even as well. The only even prime is 2 so in order for n to be in D, we must have that $\sqrt[3]{n} = 2$. This implies that $n = 8$. Thus, the only natural number n which can be in D is 8. Since $8 \in D$, we have that $D = \{8\}$.
Extra: If you find yourself struggling to write sets, it can help to physically write some examples down of items that are and are not in the set. For example, in part d) maybe you randomly pick the number 7. Well 7 does not have a third root in the primes, so $7 \notin D$. Now consider 8. We know that $\sqrt[3]{8} = 2$, so the first condition is met. Also, $8^2 = 64$, which is even. Thus, we know that 8 is in D.

Exercise 1.2

a) *Solution:* $A \cap B = \{17\}$, $A \cup B = \{1, 2, 17, 31, 12, 13, 16, 8, 22\}$, and $A \setminus B = \{1, 2, 31, 12\}$.

Note: First think about what this notation means. $A \cap B$ means we want elements that we can find in both A and in B. Looking at the given elements of A and B, we see that $A \cap B = \{17\}$. Since $A \cap B = \{17\}$, when we go to write the set of $A \cup B$, we need only include 17 once. So, $A \cup B = \{1, 2, 17, 31, 12, 13, 16, 8, 22\}$, all elements of A or of B. Finally, the only shared element between A and B is 17, which means that $A \setminus B = A \setminus \{17\}$, which is all elements in A without 17. Thus, $A \setminus B = \{1, 2, 31, 12\}$. □

b) *Solution:* $|A \times B| = |A| * |B| = 5 * 5 = 25$. While writing out every combination of $A \times B$ is the easiest way to find the number of elements it has, this can get cumbersome if say A has 106 elements and B has 240 elements. Instead, let's write out the first few pairings and see if we can find a pattern. The first element of A is 1, and we want to match 1 to every element of B. Then we will have $(1, 13), (1, 17), (1, 16)$, and so on. We do the same thing for the next element of A, which is 2. And for the third, fourth, and fifth elements of A. So when we arrive at an element in A, it must map each element in B before we move to the next element of A. Then the number of elements in $A \times B$ is the number of elements in A times the number of elements in B (which is $|A \times B| = |A| \cdot |B|$).

Extra: If $|A| = 106$ and $|B| = 240$, there will be $106 \cdot 240$ pairings possible. But is it necessarily true that each pairing is distinct from the others? Consider whether or not the distinctness of the elements in A and B ensures the distinctness of the elements in $A \times B$. □

Exercise 1.3

a) *Proof.* **Preface:** Before starting this proof, let us first address how to handle such proofs as shown on the practice midterm. We want to show that A and $(A \setminus B) \cup (A \cap B)$ are the same set, which is to say they contain all the same elements. Then we start with an arbitrary element in A and prove this element must be in $(A \setminus B) \cup (A \cap B)$. Then all elements of A are in $(A \setminus B) \cup (A \cap B)$. Afterwards, we take an arbitrary $y \in (A \setminus B) \cup (A \cap B)$ and show that it is in A too. Then all elements of $(A \setminus B) \cup (A \cap B)$ are in A. If all elements in A are in $(A \setminus B) \cup (A \cap B)$ and all elements of $(A \setminus B) \cup (A \cap B)$ are in A, then by definition the two sets are equal. This means if you get stuck on such set equality problems, try focusing on the elements inside of the sets instead of the sets themselves.

Proof: Take $x \in A$. Then either x is an element of B or it is not an element of B. If $x \notin B$, then $x \in A \setminus B$. If $x \in B$, we can say $x \in A \cap B$ since $x \in A$. Then we have proven any element in A must be an element in $(A \setminus B) \cup (A \cap B)$. This means that $A \subseteq (A \setminus B) \cup (A \cap B)$.

Now take $y \in (A \setminus B) \cup (A \cap B)$. If $y \in A \setminus B$, it is clearly also an element of A. If $y \in A \cap B$, then $y \in A$ and $y \in B$. Then for any $y \in (A \setminus B) \cup (A \cap B)$, we know that $y \in A$. This means that $(A \setminus B) \cup (A \cap B) \subseteq A$.

We have shown that $A \subseteq (A \setminus B) \cup (A \cap B)$ and $(A \setminus B) \cup (A \cap B) \subseteq A$ which proves that $A = (A \setminus B) \cup (A \cap B)$. □

b) *Proof.* Take $x \in (A \setminus B) \cap C$. This means that $x \in A$ and $x \in C$, from which we can deduce $x \in A \cap C$. But why does the backwards direction (i.e. $A \cap C \subseteq (A \setminus B) \cap C$) not hold? Well, consider the sets $A = \{1, 2, 3\}$, $B = \{1, 4, 5\}$, and $C = \{1, 6, 3\}$. Then $A \cap C = \{1, 3\}$. However, $A \setminus B = \{2, 3\}$. Then $(A \setminus B) \cap C = \{3\}$. Clearly, $\{1, 3\} \not\subset \{3\}$, so the backwards direction does not always hold. Note that this direction does not hold when A, B, and C all have an element in common. □

2 Mathematical Sets w/ Quantifiers

Exercise 2.1

a) *Solution:*
Original Statement: $\exists p \in \mathbb{P}(p+1 \in \mathbb{P})$

Negation: $\forall p \in \mathbb{P}(p+1 \notin \mathbb{P})$

This statement is true as if we take $p = 2$ then $p + 1 = 3 \in \mathbb{P}$. □

b) *Solution:*
Original Statement: $\forall n \in \mathbb{N}\left((\frac{n}{2} \in \mathbb{N} \wedge \sqrt{n} \in \mathbb{Q}) \rightarrow \sqrt{n} \in \mathbb{N}\right)$.

Negation: $\exists n \in \mathbb{N}\left((\frac{n}{2} \in \mathbb{N} \wedge \sqrt{n} \in \mathbb{Q}) \wedge \sqrt{n} \notin \mathbb{N}\right)$.

This statement is true. In fact, if $n \in \mathbb{N}$ and $\sqrt{n} \in \mathbb{Q}$, then $\sqrt{n} \in \mathbb{N}$. □

c) *Solution:*
Original Statement: $\forall z \in \mathbb{Z}(\exists z' \in \mathbb{Z}(z' > z^2))$.

Negation: $\exists z \in \mathbb{Z}(\forall z' \in \mathbb{Z}(z' \leq z^2))$.

This statement is true. Given any $z \in \mathbb{Z}$, we can take $z' = z^2 + 1$ and we will have that $z' \in \mathbb{Z}$ and $z' > z^2$. □

3 Divisibility

Exercise 3.1

a) *Solution:* This statement is true. Since $z_1 z_2 | pz_3$, there is an integer q such that $pz_3 = qz_1 z_2$. Now observe that $pz_3 = (qz_2)z_1$ and $qz_2 \in \mathbb{Z}$ so $z_1 | pz_3$. Similarly, $pz_3 = (qz_1)z_2$ and $qz_1 \in \mathbb{Z}$ so $z_2 | pz_3$. □

b) *Solution:* This statement is false. Consider $a = 8$. Then $\sqrt{8} \notin \mathbb{N}$. However, if we consider $z = 144$, then we find that $8|144$ and that $\sqrt{z} = 12$.

Note: As was done in sections 1 and 2, it is good to break down the question so you do not become confused. What are we being asked for here? We first want a natural number whose root is not a natural number. Then we want any number besides 1,4,9,16,..., and so on. One helpful tip to choosing such a number is to make it even. Because even numbers all share 2 as a divisor, you can often find counterexamples more easily when starting with an even example. If you do choose an odd number, it is normally a good idea to avoid primes, as a prime number has no divisors besides itself and 1. These tips are not all-encompassing, but can help if you get stuck. So let's say we chose our a. After we have this number, we want a z where $a|z$ and $\sqrt{z} \in \mathbb{N}$ too. However, there is also the constraint this z is not of the form a^k (i.e. if we chose $a = 6$, then we cannot chose $z = 36$ since $36 = 6^2$). Since we're only concerned with values of z where $\sqrt{z} \in \mathbb{N}$, then only consider the numbers in $\mathbb{N}$ which have natural roots. From here, you should guess and check a few reasonable selections of z (6 is even so choosing $z = 81$ is not a good pick). At this point, if you have not found such a counterexample where $a|z$ and $\sqrt{z} \in \mathbb{N}$, consider whether the statement is actually false. If you still think it is false, choose a different a and repeat the process. Hopefully, these tips can help you with such proofs in the future. □

Exercise 3.2

a) *Solution:* **Number of Divisors:** Since $120 = 2^3 \cdot 3^1 \cdot 5^1$, then there are $(3+1)(1+1)(1+1) = 4 \cdot 2 \cdot 2 = 16$ positive divisors of 120.

Sum of Divisors: To find the sum of these positive divisors, first consider a prime factor of our number. Next, call the exponent of this prime factor n and take the sum $\sum_{i=0}^{n} p_j^i$. For example, because we have 2^3, then our sum for this prime factor would be $\sum_{i=0}^{n} 2^i = 2^0 + 2^1 + 2^2 + 2^3 = 1+2+4+8 = 15$. Now do this summation for every prime factor of our number. Then we will have $1+3 = 4$ and $1+5 = 6$ as well. Finally, to get the sum of the positive divisors, take the product of all these sums. Then for 120, the sum of its positive divisors would be $15 \cdot 4 \cdot 6 = 15 \cdot 24 = 360$. □

b) *Solution:* **Number of Divisors:** Since $210 = 2 \cdot 3 \cdot 5 \cdot 7$, then there are $(1+1)(1+1)(1+1)(1+1) = 2 \cdot 2 \cdot 2\dot{2} = 16$ positive divisors of 210.

Sum of Divisors: Using the same algorithm as part a), then the sum of the positive divisors of 210 is $(1+2)(1+3)(1+5)(1+7) = 3 \cdot 4 \cdot 6 \cdot 8 = 12 \cdot 48 = 576$. □

c) *Solution:* **Number of Divisors:** This one seems daunting at first, but we do not even need to do long division. Since $5 \cdot 200 = 1000$ and $1000 - 15 = 985$, then we know that $5 \cdot (200 - 3) = 5 \cdot 197 = 985$. Then 5 is clearly prime, and it turns out that 197 is also prime as it is not divisible by 2, 3, 5, 7, 11, or 13 (to check if n is prime, it is sufficient to check whether n is divisible by a prime p such that $p \leq \sqrt{n}$). Then there are $(1+1)(1+1) = 4$ positive divisors of 985.

Sum of Divisors: Using the same algorithm as part a), then the sum of the positive divisors of 985 is $(1+5)(1+197) = 6 \cdot 198 = 1188$. □

Exercise 3.3

a) *Solution:* The divisors of 10 are 1,2,5, and 10. Most obviously, we have $\{p^9 : p \in \mathbb{P}\}$, which has an exponent of 9. Then (9+1)=10, so numbers of this form have only 10 positive divisors. How do

we arrive at the other sets which we need? Well, we know that 2 and 5 are divisors whose product is 10. Then we want to have exponents that when we add 1 to each of them, we get 2 and 5 respectively. So subtract 1 from both 2 and 5. Then the exponents we need for our next set are 1 and 4. So the set $\{p^4q\colon p, q \in \mathbb{P}, q \neq p\}$ will give us numbers with only 10 positive divisors. Since there is no other way to break up the divisors of 10, these are the only two sets which contain numbers with exactly 10 positive divisors. Thus, we have $\{p^9\colon p \in \mathbb{P}\} \cup \{p^4q\colon p, q \in \mathbb{P}, q \neq p\}$ as the two sets which contain exactly two positive divisors. □

b) *Solution:* The only number with 1 positive divisor is 1, so include $\{1\}$ at the end. We need the sets that contain numbers with 6,5,4,3, and 2 divisors. Start at 2 since it is easiest. This would then be the set of all prime numbers, as we would have $\{p\colon p \in \mathbb{P}\}$. Next, we have 3. Since 3 is prime, then the only numbers which have exactly 3 divisors are of the form $\{p^2\colon p \in \mathbb{P}\}$. Next we have 4. Then the divisors of 4 are 1,2, and 4. Then firstly we have $\{p^3\colon p \in \mathbb{P}\}$ as one of our sets with numbers that have 4 positive divisors. Second, we know that since $2 \cdot 2 = (1+1)(1+1)$, then $\{pq\colon p, q \in \mathbb{P}, p \neq q\}$ is another set with two positive divisors. Moving onto 5, we know that 5 is prime so only $\{p^4\colon p \in \mathbb{P}\}$ will contain numbers with 5 positive divisors. Finally, we have 6, which has divisors 1,2,3, and 6. Then again $\{p^5\colon p \in \mathbb{P}\}$ only contains numbers with 6 positive divisors. Also, since 2 and 3 are prime, then the only other set which contains numbers with 6 positive divisors is $\{p^2q\colon p, q \in \mathbb{P}, q \neq p\}$. Thus, the collection of sets which contain at least 6 positive divisors is $\{1\} \cup \{p\colon p \in \mathbb{P}\} \cup \{p^2\colon p \in \mathbb{P}\} \cup \{p^3\colon p \in \mathbb{P}\} \cup \{pq\colon p, q \in \mathbb{P}, p \neq q\} \cup \{p^4\colon p \in \mathbb{P}\} \cup \{p^5\colon p \in \mathbb{P}\} \cup \{p^2q\colon p, q \in \mathbb{P}, q \neq p\}$. □

4 GCD and LCM w/ Euclid's Algorithm

Exercise 4.1

a) *Solution:* We can find $gcd(x, y)$ and integers a, b such that $gcd(x, y) = ax + by$ as follows.

1. $46 = 34 + 12$. Rearranging, we have that $12 = 46 - 34$.
2. $34 = 2*12+10$. Rearranging, we have that $10 = 34-2*12 = 34-2*(46-34) = 3*34-2*46$.
3. $12 = 10+2$. Rearranging, we have that $2 = 12-10 = (46-34)-(3*34-2*46) = 3*46-4*34$.

12 is divisible by 2, so $gcd(x, y) = 2$ and we have that $gcd(x, y) = 2 = 3 * 46 - 4 * 34$. □

b) *Solution:* We can find $gcd(x, y)$ and integers a, b such that $gcd(x, y) = ax + by$ as follows.

1. $126 = 87 + 39$. Rearranging, we have that $39 = 126 - 87$.
2. $87 = 2*39+9$. Rearranging, we have that $9 = 87-2*39 = 87-2*(126-87) = 3*87-2*126$.
3. $39 = 4*9+3$. Rearranging, we have that $3 = 39-4*9 = (126-87)-4*(3*87-2*126) = 9*126-13*87$.

9 is divisible by 3, so $gcd(x, y) = 3$ and we have that $gcd(x, y) = 3 = 9 * 126 - 13 * 87$. □

Exercise 4.2

a) *Solution:* Applying Euclid's algorithm, we have that $36 = 24 + 12$. 24 is divisible by 12, so $gcd(24, 36) = 12$ and $lcm(24, 36) = \frac{24*36}{12} = 72$. □

b) *Solution:* Applying Euclid's algorithm, we have that $72 = 51+21$. $51 = 2*21+9$. $21 = 2*9+3$. 9 is divisble by 3 so $gcd(51, 72) = 3$ and $lcm(51, 72) = \frac{51*72}{3} = 1224$. □

c) *Solution:* This question never explicitly asks for the GCD, so we can completely circumvent finding it. Why? Well, if we look at x and y, then we see that $x|y$. Then this automatically makes $gcd(x, y) = x$ and $lcm(x, y) = y$. Thus, $lcm(x, y) = y = 162$.

Extra: While it will likely not be an explicitly required part of any exam you take, it is good to consider why $x|y$ means $gcd(x, y) = x$ and $lcm(x, y) = y$. Does the backwards direction also hold (i.e. if $gcd(x, y) = x$ or $lcm(x, y) = y$, is it always true that $x|y$). Considering these concepts can help you understand the material on a richer scale and give you insight on how to answer certain proofs in the future. □

5 Proofs Via Contradiction and Induction

Exercise 5.1

a) *Proof.* Let $p \in \mathbb{P}$. Assume for contradiction that $\sqrt{p} \in \mathbb{N}$. Then there exists a $k \in \mathbb{N}$ such that $\sqrt{p} = k$. If we square both sides of this equation, this would mean that $p = k^2$. Since $p \neq 1$, then we know $k \neq 1$ either. Because $k \neq 1$, then clearly $k \neq p$ either (as the only time $x = x^2$ is when $x = 1$). Then we know that k is a divisor of p that is not p and is not 1. This is a clear contradiction to the fact that p is a prime number, which means our underlying assumption was wrong. Thus, if $p \in \mathbb{P}$, then we know that $\sqrt{p} \notin \mathbb{N}$.

In fact, $\sqrt{p} \notin \mathbb{Q}$. To prove this, assume that $\sqrt{p} = \frac{x}{y}$ where $x, y \in \mathbb{N}$ and $gcd(x, y) = 1$ (for any positive rational number, we can always find such an x and y by canceling common factors from the numerator and denominator). Squaring both sides, we have that $p = \frac{x^2}{y^2}$ so $x^2 = py^2$.

Since p is prime and $p|x * x$, by the prime property, we have that $p|x$ or $p|x$. Either way, $p|x$, so there is an integer q such that $x = pq$. We now have that $y^2 = pq^2$. Following similar logic, $p|y$ which contradicts the assumption that $gcd(x, y) = 1$ □

b) *Proof.* If $\sum_{i=1}^{n} x_i = x_n$ then subtracting x_n from both sides, we have that $\sum_{i=1}^{n-1} x_i = 0$.

Assume that $x_j > 0$ for some $j \in [n-1]$. If so, then since $x_i \geq 0$ for all $i \in [n-1]$, $\sum_{i=1}^{n-1} x_i \geq x_j > 0$, which is a contradiction. Thus, we must have that $x_j = 0$ for all $j \in [n-1]$. □

Exercise 5.2

a) *Proof.* **Base Case:** Let us start with the base case, which is at $n = 1$. Then we are given $a_1 = 1$. Plugging $n = 1$ into 2^{n-1}, then we get

$$2^{1-1} = 2^0 = 1 = a_1.$$

Then our base case holds, so let us move on to the inductive step.

Inductive Step: Start with the inductive hypothesis, which is that $a_n = 2^{n-1}$. Let us now prove this means that $a_{n+1} = 2^{(n+1)-1} = 2^n$. Consider $a_{n+1} = 2a_n$. By the inductive hypothesis

$$a_{n+1} = 2a_n = 2 \cdot 2^{n-1} = 2^{n-1+1} = 2^n.$$

This completes the inductive step. Thus, we have shown that for the given recursive function, then $a_n = 2^{n-1}$. □

b) *Proof.* **Base Case:** Again, let us start with the base case of $n = 1$. Then we must consider $\sum_{i=1}^{1} i$.

Obviously, this is just equal to 1. If we consider $\frac{n(n+1)}{2}$, then when plugging in we get

$$\frac{n(n+1)}{2} = \frac{1(1+1)}{2} = \frac{2}{2} = 1.$$

Then our base case holds.

Inductive Step: Assume that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. We now consider $\sum_{i=1}^{n+1} i$ and must show it equals $\frac{(n+1)((n+1)+1)}{2}$. Observe that $\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + n + 1$. Plugging in the inductive hypothesis,

$$\sum_{i=1}^{n} i + n + 1 = \frac{n(n+1)}{2} + n + 1 = \frac{n^2+n}{2} + n + 1 = \frac{n^2}{2} + \frac{n}{2} + n + 1 = \frac{n^2}{2} + \frac{3n}{2} + 1 =$$
$$\frac{n^2+3n+2}{2} = \frac{(n+1)(n+2)}{2} = \frac{(n+1)((n+1)+1)}{2}.$$

This completes the inductive step. Thus, we have shown via induction that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. $\square$

6 More Proofs

Exercise 6.1.

Proof. Since k is any natural number, there are one of two cases: either k is even or k is odd. If k is even, we can write $k = 2q$ for some integer q so $\frac{(k-1)k}{2} = q(k-1) \in \mathbb{Z}$. If k is odd then we can write $k = 2q+1$ for some integer q so $\frac{(k-1)k}{2} = \frac{(2q)k}{2} = qk \in \mathbb{Z}$.

Note: A combinatorial argument for this is that $\frac{(k-1)k}{2}$ is the number of ways to choose 2 objects from k objects and this is always an integer. □

Exercise 6.2.

Proof. Consider $a^{\log(b)}$. Note that since a, b are positive, then we know $log(a)$ and $\log(b)$ are defined values. So, we can rewrite $a = e^{\log(a)}$. Then

$$a^{\log(b)} = (e^{\log(a)})^{\log(b)} = e^{\log(a)\log(b)} = e^{\log(b)\log(a)} = (e^{\log(b)})^{\log(a)} = b^{\log(a)}.$$

□

Exercise 6.3.

Proof. We know that

$$\binom{n}{2} = \frac{n!}{2!(n-2)!} = \frac{n(n-1)}{2} = \frac{n^2-n}{2} \text{ and}$$
$$\binom{n}{3} = \frac{n!}{3!(n-3)!} = \frac{n(n-1)(n-2)}{6} = \frac{(n^2-n)(n-2)}{6} = \frac{n^3-3n^2+2n}{6}.$$

This would mean that

$$\binom{n}{2} + \binom{n}{3} = \frac{n^2-n}{2} + \frac{n^3-3n^2+2n}{6} = \frac{3n^2-3n}{6} + \frac{n^3-3n^2+2n}{6} = \frac{n^3-n}{6} =$$
$$\frac{n(n^2-1)}{6} = \frac{n(n+1)(n-1)}{6} = \binom{n+1}{3}.$$

□

Exercise 6.4.

(a) *Proof.* Consider the number 4, which has factors 1, 2, and 4. Then 4 is an even 3-prime number. Now assume for contradiction that we have a 3-prime number x which is even and not equal to 4. Then we know that x has at least divisors 1, 2, and x. We know there must also be some factor y where $2 * y = x$, but since $x \neq 4$, then $y \neq 2$. Since $x = 2$ is not 3-prime, then this must mean y is distinct to 1, 2, and x, i.e. there is a fourth divisor of x. Thus, a 3-prime number must be odd if it is not equal to 4. □

(b) *Proof.* Let x be 3-prime. Then we know that x has factors 1, x, and a for some natural number a. Suppose for contradiction that a is not prime. Then a must be the product of two natural numbers b and c where neither b nor c are equal to 1 or x. However, this would mean that b and c must be factor of x, which is a contradiction. Then a 3-prime number only has factors 1, x, and p for some prime number p. □

(c) *Proof.* First, assume that x is 3-prime. Then we know that x has factors 1, x, and p only, where p is a prime number. However, since p is not equal to 1 and not equal to x (because a 3-prime number must have 3 distinct factors), we know $p^2|x$. By the definition of factors, we must also have that $x|p^2$, which means that $x = p^2$. Now assume that we have any prime number p and $x = p^2$. Since p only has factors 1 and p, then p^2 must only have factors 1, p, and p^2. Then x only has factors 1, p, and p^2, i.e. x must be 3-prime. □

Exercise 6.5.

Proof. Firstly, note that $\sqrt{x} = x^{\frac{1}{2}}$. Then

$$\sqrt{x\sqrt{x}} = (x \cdot x^{\frac{1}{2}})^{\frac{1}{2}} = x^{\frac{1}{2}} \cdot x^{\frac{1}{4}} = x^{\frac{3}{4}}.$$

Using our given infinite sum, we can rewrite

$$\sqrt{x\sqrt{x\sqrt{x...}}} = \prod_{n=1}^{\infty} x^{\frac{1}{2^n}} = x^{\sum_{n=1}^{\infty} \frac{1}{2^n}} = x.$$

□

7 GCD and LCM w/ Prime Factorization

Exercise 7.1

a) *Solution:* Given $x = 12$ and $y = 16$, then we have $x = 2^2 \cdot 3$ and $y = 2^4$. Now $gcd(x, y) = 2^{\min\{2,4\}} * 3^{\min\{1,0\}} = 2^2 = 4$ and $lcm(x, y) = 2^{\max\{2,4\}} * 3^{\max\{1,0\}} = 2^4 * 3^1 = 48$ □

b) *Solution:* Given $x = 49$ and $y = 14$, then $x = 7^2$ and $y = 2 \cdot 7$. Now $gcd(x, y) = 2^{\min\{0,1\}} * 7^{\min\{2,1\}} = 7^1 = 7$ and $lcm(x, y) = 2^{\max\{0,1\}} * 7^{\max\{2,1\}} = 2^1 * 7^2 = 98$ □

c) *Solution:* Given $x = 72$ and $y = 20$, then $x = 2^3 \cdot 3^2$ and $y = 2^2 \cdot 5$. Now $gcd(x, y) = 2^{\min\{3,2\}} * 3^{\min\{2,0\}} * 5^{\min\{0,1\}} = 2^2 = 4$ and $lcm(x, y) = 2^{\max\{3,2\}} * 3^{\max\{2,0\}} * 5^{\max\{0,1\}} = 2^3 * 3^2 * 5^1 = 360$ □

Exercise 7.2

a) *Solution:* This statement is false. Let $p \in \mathbb{P}$. If we take $n = p^2$ then $gcd(p, n) = gcd(p, p^2) = p$ but $lcm(p, n) = lcm(p, p^2) = p^2$. That said, if we added the condition that $p \nmid n$ then this statement would be true.

In Depth Explanation: Note the only way that $lcm(p, n) = pn$ is if p and n are relatively prime. This statement would have been true with the extra parameter that $n \neq p^k$ for any $k \in \mathbb{N}$, but as it currently stands it's not entirely true. Just to give a hard example, consider $p = 3$. Then $p^2 = 9$, which means $p^2 \neq p$. Then let $n = 9$. Then $gcd(3, 9) = 3$, so $lcm(3, 9) = \frac{3 \cdot 9}{3} = 9$. When you come across statements like this that seem obviously true, be sure to consider even the most basic of cases (such as simply squaring our number p). Sometimes you can disprove a claim fairly quickly with such an approach. Also, when considering the question, what is it actually asking us? Sure, we want to know if the LCM of a prime number with another distinct number will be their product, but more deeply there is another question. Essentially, the question is asking if it is necessarily true that a prime number be relatively prime with every other natural number. When you reword the question like this, it becomes clear why it is a false statement, as simply squaring this prime disproves the claim. □

b) *Solution:* This statement is false. Consider $x = 6$, $y = 18$, and $z = 9$. Then $6|18$ and $9|18$, but $6 * 9 = 54$ and $54 \nmid 18$.

As a tip for questions using divisors, if a question does not mention prime numbers, try to avoid using them in your examples. Because of the property that prime numbers are only divisible by 1, they usually make for a pretty weak counterexample. □

c) *Solution:* Note: This problem should have specified that x is a natural number.

This statement is true. To prove this, recall that $\prod_{j=1}^{\infty} p_j^{a_j} \mid \prod_{j=1}^{\infty} p_j^{b_j}$ if and only if $a_j \leq b_j$ for all $j \in \mathbb{N}$. Thus, the only positive divisors of $p_1p_2p_3$ are 1, p_1, p_2, p_3, p_1p_2, p_1p_3, p_2p_3, and $p_1p_2p_3$. All of these numbers except $p_1p_2p_3$ are positive divisors of p_1p_2, p_1p_3, or p_2p_3 and we cannot have that $x = p_1p_2p_3$ as $x < p_1p_2p_3$. Thus, x is a positive divisor of p_1p_2, p_1p_3, or p_2p_3, as needed. □

d) *Solution:* This statement is false. If we take any $x \in \mathbb{N}$ and take $y = -x$ then $gcd(x, y) = x$ so $x|gcd(x, y)$ and $y \mid gcd(x, y)$ but $y \neq x$.

If we added the condition that $x > 0$ and $y > 0$ then this statement would be true. To see this, observe that $gcd(x, y)|x$ and $gcd(x, y)|y$. Since $x|gcd(x, y)$, and $gcd(x, y)|y$, we have that $x|y$. Similarly, since $y|gcd(x, y)$, and $gcd(x, y)|x$, we have that $y|x$. If $x, y \in \mathbb{N}$, $x|y$, and $y|x$ then $x = y$. □

8 Modular Arithmetic

Exercise 8.1

a) *Solution:* Considering $20 + 33 \mod 41$, we have $20 + 33 \mod 41 = 53 \mod 41 = 12$. □

b) *Solution:* Considering $6 \cdot 21 \mod 18$, we have $6 \cdot 21 \mod 18 = 126 \mod 18 = 0$, as $126 = 7 \cdot 18$. □

c) *Solution:* Because 23 is prime and $22 = 23 - 1$, then we can deduce that $22! \equiv -1 \mod 23$ so $22! \mod 23 = -1 \mod 23 = 22$. Thus, $22! \mod 23 = 22$. □

d) *Solution:* Notice that for 7^8, we have $8 = 2^3$. For any number $k \in \mathbb{N}$ where $k = 2^i$ for some $i \in \mathbb{N}$, then we can use a special technique to arrive at our answer for p^k, where $p \in \mathbb{N}$. First, consider $p \mod n$ (in our case, $p = 7$ and $n = 20$). Then clearly $7 \mod 20 = 7$. This is where the technique comes in. We can say that $7^2 \mod 20 = (7 \mod 20)^2 \mod 20 = 49 \mod 20 = 9$. While this does not seem to have helped us yet, we can repeat this again until we reach 7^8. Then $7^4 \mod 20 = (7^2 \mod 20)^2 \mod 20 = 9^2 \mod 20 = 81 \mod 20 = 1$. Finally, we would have $7^8 = (7^4 \mod 20)^2 \mod 20 = 1^2 \mod 20 = 1 \mod 20 = 1$. Thus, we can deduce through this technique that $7^8 \mod 20 = 1$. □

Exercise 8.2

a) *Solution:* Note that $gcd(12, 21) = 3$, which is not equal to 1. Then we know that we cannot find the inverse of 12 in $\mathbb{Z}_{21}$. □

b) *Solution:* $gcd(18, 25)$ so the inverse of 18 exists in $\mathbb{Z}_{25}$. The standard way to find 18^{-1} is by using Euclid's algorithm. Here we can observe that $18 \equiv -7 \mod 25$ and $-7 * 7 \equiv 1 \mod 25$ as $-7 * 7 = -49 = -1 * 50 + 1$. Thus, the inverse of 18 in $\mathbb{Z}_{25}$ is 7. □

9 Chinese Remainder Theorem and Totient Function

Exercise 9.1

a) *Solution:* First, we set our values for each a_i and each n_i. Then $a_1 = 6$, $a_2 = 13$, $n_1 = 14$, and $n_2 = 19$. Take n_1 first. Then we wish to find $(\frac{N}{n_1})^{-1}$ in $\mathbb{Z}_{n_1}$ (where N is the product of all n_i). Then we want to find 19^{-1} in $\mathbb{Z}_{14}$. Since 19 and 14 are relatively prime, this is possible. Note that $19 \equiv 5 \mod 14$, so we really want to find 5^{-1} in $\mathbb{Z}_{14}$. There is a section on how to find inverses, so we will not explicitly write down these steps. However, we will find that $5^{-1} = 3$ in $\mathbb{Z}_{14}$, as $5 \cdot 3 = 15 \equiv 1 \mod 14$. Then our value of $c_1 = 3$. Our value of $e_1 = c_1 \cdot \frac{N}{n_1} = 3 \cdot 19 = 57$. Now let us move on to n_2. Again, we want to find $(\frac{N}{n_2})^{-1}$ in $\mathbb{Z}_{n_2}$, which is to say we want 14^{-1} in $\mathbb{Z}_{19}$. Then we will find that $14^{-1} = 15$ in Z_{19}, as $14 \cdot 15 = 210 \equiv 1 \mod 19$. Then our value for $e_2 = c_2 \cdot \frac{N}{n_2} = 15 \cdot 14 = 210$. Then we will find $x = (a_1 \cdot e_1 + a_2 \cdot c_2)$. Then $x = (6 \cdot 57) + (13 \cdot 210) \mod n_1 n_2 = 342 + 2730 \mod n_1 n_2 = 3072 \mod n_1 n_2$. Then $3072 \mod n_1 n_2 = 3072 \mod 266 = 146$. Checking $x = 146$, we know that $146 \equiv 6 \mod 14$ and $146 \equiv 13 \mod 19$. Thus, our value of x is 146. □

b) *Solution:* Set $a_1 = 4$, $a_2 = 7$, and $a_3 = 2$. Set $n_1 = 9$, $n_2 = 8$, and $n_3 = 7$. Let us first find c_1. Then $c_1 = (\frac{N}{n_1})^{-1} = (8 \cdot 7)^{-1} = 56^{-1}$ in $\mathbb{Z}_9$. Then $56 \equiv 2 \mod 9$, which means we want to find 2^{-1} in $\mathbb{Z}_9$. Then $c_1 = 2^{-1} = 5$ in $\mathbb{Z}_9$. Then $e_1 = 5 \cdot 56 = 280$. Secondly, let us find c_2. Then $c_2 = (9 \cdot 7)^{-1} = 63^{-1}$ in $\mathbb{Z}_8$. Then $63 \equiv 7 \mod 8$ in $\mathbb{Z}_8$. Then we find that $c_2 = 7$, so $e_2 = 7 \cdot 63 = 441$. Lastly, $c_3 = 72^{-1}$ in $\mathbb{Z}_7$. Then $72 \equiv 2 \mod 7$, so we want 2^{-1} in $\mathbb{Z}_7$, which is 4. Then $c_3 = 4$, and hence $e_3 = 4 \cdot 72 = 288$. Then $x = (4 \cdot 280) + (7 \cdot 441) + (2 \cdot 288) \mod n_1 n_2 n_3 = 1120 + 3087 + 576 \mod n_1 n_2 n_3 = x = 4783 \mod n_1 n_2 n_3$. Then $x = 4783 \mod n_1 n_2 n_3 = 4783 \mod 504 = 247$. Checking $x = 247$, we have $247 \equiv 4 \mod 9$, $247 \equiv 7 \mod 8$, and $247 \equiv 2 \mod 7$. Thus, we know that $x = 247$. □

Exercise 9.2

a) *Solution:* Since 19 is prime, then we know $\Phi(19) = 19 - 1 = 18$. □

b) *Solution:* The prime factorization of 34 is $34 = 17 \cdot 2$. Then we have $\Phi(34) = (17-1)(2-1) = 16$. □

c) *Solution:* The prime factorization of 105 is $105 = 3 \cdot 5 \cdot 7$. Then we have $\Phi(105) = (3-1)(5-1)(7-1) = 2 \cdot 4 \cdot 6 = 48$. □

d) *Solution:* The prime factorization of 87 is $87 = 3 \cdot 29$. Then we have $\Phi(87) = (3-1) \cdot (29-1) = 2 \cdot 28 = 56$. □

e) *Solution:* The prime factorization of 136 is $2^3 \cdot 17$. Because the exponent of 2^3 is not 1, then we will have to multiply our value by $2^{3-1} = 2^2$ now. Then $\Phi(136) = (2-1)2^2 \cdot (17-1) = 4 \cdot 16 = 64$. □

f) *Solution:* The prime factorization of 468 is $2^2 \cdot 3^2 \cdot 13$. Then we have $\Phi(468) = (2-1)2^{2-1} \cdot (3-1)3^{2-1} \cdot (13-1) = 2 \cdot 2(3) \cdot 12 = 12 \cdot 12 = 144$. □

Extra: If you look at every answer above, you will notice they are all even numbers. Will Euler's Totient function always return an even number? If so, why will this happen? Think about any possible counterexamples that could disprove this claim.

10 Fermat's Little Theorem

Exercise 10.1

a) *Solution:* The first part of solving a problem like this is to find Euler's Totient function for the mod we are in. In this case, we have $17^{94} \mod 31$, so we are in mod 31. Then $\Phi(31) = 30$, as 31 is prime. Then to find 17^{94}, we can use the generalization of Fermat's Little Theorem to take the exponent of 17 mod $\Phi(31)$. Then we have $17^{94} \mod 31 \equiv 17^{94 \mod 30} \mod 31 = 17^4 \mod 31$. Using the technique from Exercise 7.1d), then

$$\begin{aligned}
&17 \mod 31 = 17 \\
&17^2 \mod 31 = (17 \mod 31)^2 \mod 31 = 17^2 \mod 31 = 289 \mod 31 = 10 \\
&17^4 \mod 31 = (17^2 \mod 31)^2 \mod 31 = 10^2 \mod 31 = 100 \mod 31 = 7.
\end{aligned}$$

Thus, we know that $17^{94} \mod 31 = 7$. □

b) *Solution:* Since $gcd(12, 18) \neq 1$, we should find the answer modulo 2 and the answer modulo 9 and combine them using the Chinese Remainder Theorem.

$12^{62} \mod 2 = 0$ and $12^{62} \mod 9 = 0$ so $12^{62} \mod 18 = 0$. In this case, we could have also seen this by observing that $18|12^2$ as $12^2 = 144 = 8 * 18$. □

c) *Solution:* Observe that $9^2 = 81$ so $9^2 \equiv 1 \mod 80$. Thus, $9^{139} \mod 81 = 9^{139 \mod 2} \mod 80 = 9^1 \mod 80 = 9$.

Detailed explanation: Since $\Phi(80) = 32$, then $9^{139} \equiv 9^{139 \mod 32} \mod 80 = 9^{11} \mod 80$. Notice that 11 is not of the form 2^k, so we will need a new method to find $9^{11} \mod 80$. Let us use a modified version of our previous technique, where we increment our steps by 1 rather than 2^k. This sounds confusing at first, but let's break it down. Set $e' = 1$. Find $9 \mod 80$. Then $9 \mod 80 = 9$. Denote this value as c. Now increment e' by 1, so that $e' = 2$. Now consider $9 \cdot c \mod 80$, which is $9 \cdot 9 \mod 80 = 1$. Reassign c to this value and increment e' by 1 again. We will repeat this process until $e' = 12$, at which point our value of c is the correct answer. The reason we stop at 12 is because our exponent for 9^{11} 12=11+1. This would indicate we are at 9^{11}. We will now go through the rest of the steps, starting at $e' = 2$. Then

$$\begin{aligned}
&9 \cdot c \mod 80 = 9 \cdot 1 \mod 80 = 9 \mod 80 = 9, && e' = 4, c = 9 \\
&9 \cdot c \mod 80 = 9 \cdot 9 \mod 80 = 81 \mod 80 = 1, && e' = 5, c = 1 \\
&9 \cdot c \mod 80 = 9 \cdot 1 \mod 80 = 9 \mod 80 = 9, && e' = 6, c = 9 \\
&9 \cdot c \mod 80 = 9 \cdot 9 \mod 80 = 81 \mod 80 = 1.
\end{aligned}$$

We could continue this technique over and over, but we see that for odd numbers of e' we return $c = 9$ and for even values of e' we return $c = 1$. Since 11 is odd, then we know $c = 9$ at 9^{11}. Thus, we know that $9^{139} \equiv 9^{11} \mod 80 = 9$. □