Homework 4: Number and Set Theory

Due date: Wednesday July 23rd at 11:59 PM
If you work with others (and you should!), remember to follow the collaboration policy outlined in the syllabus.
In general, you are graded on both the clarity and accuracy of your work. Your solution should be clear enough that someone in the class who had not seen the problem before would understand it.
We sometimes describe approximately how long our explanations are. These are intended to help you understand approximately how much detail we are expecting. You are allowed to have longer explanations, but explanations significantly longer than necessary may receive deductions.

Be sure to read the grading guidelines on the assignments page for more information on what we're looking for.

In order to assist with the transition from formal proofs to English proofs, we've published a style guide on the website containing some tips. This guide contains references to proof materials that we haven't taught yet, so don't worry if some of these terms are unfamiliar.

1. Quartic Modulo

Prove that for all integers, a, b, and n, where $n > 0$: if $a \equiv b \pmod{n}$, then $a^4 \equiv b^4 \pmod{n}$. For this problem, you may not use facts proven in lecture (e.g., you may not use that $a \equiv b \pmod{n} \rightarrow ac \equiv bc \pmod{n}$). You can use the definitions of modular equivalence and divides, and do any algebra you like on regular equations.
Hint: Our first algebra step involves multiplying by $b+a$. We suggest basing future algebra steps off that one.

2. GCD Proof

Bezout's Theorem tells us that if x and y are positive integers, then there exist some integers a and b such that $\gcd(x, y) = ax + by$. However, the converse isn't always true: there could exist some integers a and b such that $d = ax + by$, but d isn't necessarily $\gcd(x, y)$. In this problem, we will see a special case where the converse does hold.

(a) For all **positive** integers x and y, prove the following claim: if there exist some integers a and b such that $ax + by = 1$, then $\gcd(x, y) = 1$.

You may use without proof that if any integer k satisfies $k|1$, then k must be either 1 or -1. **Hint:** The facts about GCD that you will need for this problem are that if $d = \gcd(x, y)$ then $d|x$ and $d|y$, and it is the largest integer that does this.

(b) Use part (a) to show that $\gcd(m, m + 1) = 1$ for all positive integers m.

3. A Proof By Contradiction

Use a proof by contradiction to show the following claim: for all integers n, if $n \equiv 3 \pmod{8}$, then $n \not\equiv 0 \pmod{6}$.
Hint: You may use without proof that a number cannot be both even and odd.

4. Set Computation

Let $A = \{2, 4, 6\}$, $B = \{4, 6, 8\}$, and the universe be $\mathbb{Z}$, the set of integers. Compute each of the following sets. You only need to provide your final solution; showing work is not required, but it may help with earning partial credit if your solution is incorrect. Recall that the order in which you list the elements of a set does not matter.

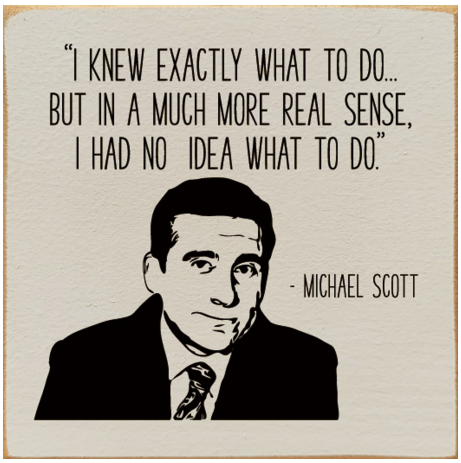
(a) $A \times (\varnothing \cup \{5\})$

(b) $\mathcal{P}(\mathcal{P}(\varnothing))$

(c) $(A \times B) \cap (B \times A)$

(d) $\mathcal{P}(B \setminus \overline{A})$

5. Let's Settle Our Differences



The characters in this problem are based on The Office.

Congratulations! You have been promoted to Assistant to the Regional Manager at Dunder Mifflin (don't tell Dwight!). As your first task as Assistant to the Regional Manager you have three sets of paper: A, B, and C. Jim has told you that the relation between the sets of paper is $(A \cup B) \setminus C$. Michael believes the relation between the sets of paper is $(A \setminus C) \cup (B \setminus C)$. Pam suggests you show Michael that Jim's statement is a subset to Michael's, but warns you that Michael does not have the patience to read a full formal proof. Your job: Suppose A, B, and C are sets. Prove in English $(A \cup B) \setminus C \subseteq (A \setminus C) \cup (B \setminus C)$.

6. We've Got The Power

Prove or disprove the following claims. For each claim, please specify clearly if you are proving or disproving it.

(a) For all sets S and T: $\mathcal{P}(S \cap T) \subseteq \mathcal{P}(S) \cap \mathcal{P}(T)$.

(b) For all sets S and T: $\mathcal{P}(S \cup T) \subseteq \mathcal{P}(S) \cup \mathcal{P}(T)$.

7. Keeping up with the Cartesians

(a) Prove that for all sets A, B, C, if A is non-empty and $A \times B = A \times C$, then $B = C$.
Hint: Write a subset proof in each direction.

(b) Does the claim in part (a) still hold if A is empty? Why or why not?

8. Exponentially increasing fun [Extra Credit]

You will submit this question to the separate gradescope box for "Homework 4 Extra Credit."

Since $a \equiv a \ \% \ n \pmod{n}$, we know that we can reduce the base of an exponent in $\pmod{n}$ arithmetic. That is:

$$a^k \equiv (a \ \% \ n)^k \pmod{n}.$$

But the same is **not** true of the exponent! That is, we cannot say that $a^k \equiv a^{(k \ \% \ n)} \pmod{n}$. Consider, for instance, that $2^{10} \equiv 1 \pmod{3}$ but $2^{(10 \ \% \ 3)} \equiv 2 \pmod{3}$. The correct way to simplify exponents is quite a bit more subtle. In this problem you'll prove it in steps.

For these proofs you may use any theorem on the number theory reference sheet, even the ones we haven't proven yet in class.

(a) Let $R = \{t \in \mathbb{Z} : 1 \leq t \leq n-1 \wedge \gcd(t, n) = 1\}$. Define the set $aR = \{(ax) \ \% \ n : x \in R\}$. Prove that $aR = R$ for every integer $a > 0$ with $\gcd(a, n) = 1$.

(b) Consider the product of all elements in R (taken $\pmod{n}$) and consider the product of all the elements in aR (again, taken $\pmod{n}$). By comparing these two expressions, conclude that for all $a \in R$ we have $a^{\varphi(n)} \equiv 1 \pmod{n}$ where $\varphi(n) = |R|$.

(c) Use the previous part to show that for any $b \geq 0$ and $a \in R$ we have $a^b \equiv a^{(b \ \% \ \varphi(n))} \pmod{n}$.

(d) Now suppose that $y = x^e \ \% \ n$ for some x with $\gcd(x, n) = 1$ and e some integer ≥ 0 such that $\gcd(e, \varphi(n)) = 1$. Let $d = e^{-1} \ \% \ \varphi(n)$. Prove that $y^d \equiv x \pmod{n}$.

(e) Prove the following two facts about φ: First, if p is prime then $\varphi(p) = p - 1$. Second, for any positive integers a and b with $\gcd(a, b) = 1$, we have $\varphi(ab) = \varphi(a)\varphi(b)$.

These facts together are the basis for the most-widely used "public key encryption system." One chooses $n = pq$ for large primes p and q, and a value of e. The numbers n and e are made public to anyone who wants to send a message securely. To send a message x, the sender computes $y = x^e \ \% \ n$ and sends y (the "encrypted text"). To decrypt, one computes $y^d \ \% \ n$ (note that the recipient must be the one who chose p, q so they can calculate d). The security of the system relies on it being hard to compute d from just e and m.

9. Feedback [Extra Credit]

Answer these questions on the separate gradescope box for this question.

Please keep track of how much time you spend on this homework and answer the following questions. This can help us calibrate future assignments and future iterations of the course, and can help you identify which areas are most challenging for you.

- How many hours did you spend working on this assignment (excluding any extra credit questions, if applicable)? Report your estimate to the nearest hour.
- Which problem did you spend the most time on?
- Any other feedback for us?