MATH 4573: HOMEWORK 1

INSTRUCTOR: TYLER GENAO

Due: January 23, 2026.

This homework has two sections: the first section has the assigned problems that you will turn in to Gradescope for credit. The second section contains recommended and bonus problems, either from myself, the textbook or other sources. These latter problems are not graded for credit, but you may find them to be useful practice and/or interesting!

For any assigned problem in this homework, **you must show all of your work in order to receive full credit. Your solutions can only cite §1.1 − 1.2 of our notes, as well as the definition of prime/composite and the result that for prime p, one has $p \mid ab \Rightarrow p \mid a$ or $p \mid b$. Everything else must be proven.**

1. Problems to Submit

Exercise 1. We will prove the following result using **induction:**

> **Proposition.** *For any integer $n > 0$, one has $5 \mid (9^n - 4^n)$.*

a) First, convince yourself that this result might be true: for each integer $1 \leq n \leq 4$, compute $9^n - 4^n$ and write it as a multiple of 5.

We will break this proof into steps:

b) *Check the base case:* write down your answer for $n = 1$, and confirm that it is a multiple of 5.
c) *Induction hypothesis:* assume that the proposition is true for all integers k with $1 \leq k < n$. Use this to prove the proposition for $k = n$. (*Hint:* observe that $9^n - 4^n = (5 + 4) \cdot 9^{n-1} - 4 \cdot 4^{n-1}$.)

Exercise 2. Prove the following result via **contradiction:**

> **Proposition.** *For any integer $n \geq 0$, one has $4 \nmid (n^2 + 2)$.*

Exercise 3. We will prove the following result by proving its equivalent **contrapositive:**

> **Proposition.** *Let $a > 1$ be an integer. Then $2^a + 1$ is not divisible by $2^a - 1$.*

a) First, state the contrapositive of the proposition: i.e., $\neg q \Rightarrow \neg p$.
b) Prove the contrapositive statement.

Since the proposition and its contrapositive are equivalent, we have thus proven the proposition.

Date: Assigned January 16, 2026.

c) Based on your work above, make a conjecture about the GCD of $2^a - 1$ and $2^a + 1$. Try and prove it if you can!

Exercise 4. This exercise will get you acquainted with GCD calculations by hand.

a) Use the Euclidean Algorithm to compute the GCD of $a = 2026$ and $b = 365$.
b) Next, compute the GCD of $a = 2026$ and $b = 365$ using Blankinship's Algorithm. Using this work, also write your GCD as a $\mathbb{Z}$-linear combination of a and b.
c) Use either the Euclidean Algorithm or Blankinship's Algorithm to compute the GCD of $a = 1995$ and $b = 163$, and to write this GCD as a $\mathbb{Z}$-linear combination of a and b.

Exercise 5. Show that if positive integers a and b satisfy $\gcd(a, b) = \operatorname{lcm}(a, b)$, then $a = b$.

Exercise 6. Show that for integers a, b and c, one has $a \mid bc$ if and only if $\frac{a}{\gcd(a,b)} \mid c$.

Exercise 7. Determine whether the following statements are true or false. If a statement is true, then prove it; if it is false, then provide a counterexample.

a) For a prime p, if $p \mid a^2$ then $p \mid a$.
b) If $\gcd(a, b) = \gcd(a, c)$ then $\operatorname{lcm}(a, b) = \operatorname{lcm}(a, c)$.
c) If $n \mid a^2$ then $n \mid a$.
d) If $n \mid a^2 - 1$ then $n \mid a^4 - 1$.

Exercise 8. Who did you consult for this assignment? What resources did you use?

2. Other Recommended Problems

From [NZM91, §1.2], pages 17–18: $\#6, 9, 10, 12, 13, 14, 15, 17, 20, 21, 23$.
From [NZM91, §1.3], pages 28–29: $\#1, 6, 7$.

Bonus Exercise 9. Suppose that a and b are integers with $\gcd(a, b) = 1$. Show that if $a \mid n$ and $b \mid n$, then $ab \mid n$.

Bonus Exercise 10. If you have some experience programming, create a script which computes the GCD of any two integers and expresses it as a $\mathbb{Z}$-linear combination of the two.

References

[NZM91] I. Niven, H.S. Zuckerman and H.L. Montgomery, *An introduction to the theory of numbers*, 5th Ed., John Wiley & Sons, Inc., New York (1991).