MATH 4573: HOMEWORK 1

INSTRUCTOR: TYLER GENAO

Due: January 26.

This homework has two sections: the first section has the problems that you'll turn in for credit. The second section contains recommended problems from the textbook, myself or other sources; you are not required to do these, but I recommend that you check them out.

For any problem in the assignment, **you must show all of your work in order to receive full credit.** Please do not use words such as "clear", "obvious" or "trivial" in your solutions.

1. Problems to Submit

Exercise 1. This exercise will get you acquainted with GCD calculations by hand.

a) Use the Euclidean algorithm to compute the GCD of $a = 1876$ and $b = 365$.
b) Next, compute the GCD of $a = 1876$ and $b = 365$ using Blankinship's algorithm with a matrix. Using this work, also write your GCD as a $\mathbb{Z}$-linear combination of a and b.
c) Use Blankinship's algorithm to compute the GCD of $a = 4999$ and $b = 1109$, and write this GCD as a $\mathbb{Z}$-linear combination of a and b.

Exercise 2. Prove the following result, using the proof technique of **induction:**

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

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

We'll break this proof down into steps:

b) *Check the base case:* write down what you got for the first case $n = 1$, and confirm that it's a multiple of 5.
c) *Induction hypothesis:* assume that the proposition is true for all integers $1 \leq k < n$. Using this assumption, prove the proposition for $k = n$.

(*Hint:* for c), observe that $9^n - 4^n = (5 + 4) \cdot 9^{n-1} - 4 \cdot 4^{n-1}$.)

Exercise 3. Prove the following result, using the proof technique of **contradiction:**

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

Exercise 4. We will prove the following result by proving its equivalent **contrapositive:**

Proposition. *Let* a *be a positive integer. If* $a > 1$*, 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.

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

Exercise 5. Show that if $a, b \in \mathbb{Z}^+$ satisfy $\gcd(a, b) = \operatorname{lcm}(a, b)$, then $a = b$.

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

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

a) For prime $p \in \mathbb{Z}^+$, if $p \mid a^3$ then $p \mid a$.
b) If $\gcd(a, b) = \gcd(a, c)$ then $\operatorname{lcm}(a, b) = \operatorname{lcm}(a, c)$.
c) For $n \in \mathbb{Z}^+$, if $n \mid a^3$ 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 the textbook, pages 17–18: $\#6, 7, 9, 10, 12, 13, 14, 15, 17, 20, 21, 23$.
Pages 28–29: $\#1, 6, 7$.

Bonus Exercise 9. Suppose that $a, b \in \mathbb{Z}$ 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.