MATH 4400/6400 – Homework #1
posted January 18, 2023; due Wednesday, January 25

Directions. Give complete solutions, providing full justifications. (Ask me if you have a question about what constitutes a "full" justification.)

Knowledge check (do not turn in)

- Show that for each pair of $a, b \in \mathbf{Z}$, the set $\{ax + by : x, y \in \mathbf{Z}\}$ is an ideal of $\mathbf{Z}$.
- Let $a, b, q, r \in \mathbf{Z}$ satisfy $a = bq + r$. Show that if d is a greatest common divisor of a and b, then d is a greatest common divisor of b and r.

MATH 4400 problems

1. This exercise asks you to fill in details of the proofs for some statements made in class.
   (a) Let $a, b \in \mathbf{Z}$. Show that if $a \mid b$ and $b \mid a$, then $a = \pm b$.
   Hint: You may assume, as stated in class, that if $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$. But make sure your proof also works in the case when one of a, b is 0.
   (b) Suppose d, e are both greatest common divisors of the same pair of integers a, b. Prove that $d = \pm e$.
2. Let $a, b \in \mathbf{Z}$. We know that $\gcd(a, b)$ can be written in the form $ax + by$ for some integers x, y.
   (a) Prove or give a counterexample: If there are integers x and y with $ax + by = 2$, then $\gcd(a, b) = 2$.
   (b) Prove or give a counterexample: If there are integers x and y with $ax + by = 1$, then $\gcd(a, b) = 1$.
3. Suppose $a, b \in \mathbf{Z}$ and $\gcd(a, b) = 1$. Find all possible values of $\gcd(a - b, a + b)$. Justify your answer.
4. Suppose $a, b \in \mathbf{Z}$ and $\gcd(a, b) = 1$. Find all possible values of $\gcd(a + b, a^2 - ab + b^2)$. Justify your answer.
5. Let a, b, c be positive integers with $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$. Find all possible values of $\gcd(a, bc)$. Justify your answer.

In what follows, $\mathrm{ord}_p(n)$ denotes the exponent of p in the prime factorization of n.
For example, $\mathrm{ord}_3(54) = 3$, while $\mathrm{ord}_3(17) = 0$.

The function $\mathrm{ord}_p(\cdot)$ is well-defined (by unique factorization). Note that $\mathrm{ord}_p(n)$ can be defined, equivalently, as the largest nonnegative integer for which $p^{\mathrm{ord}_p(n)} \mid n$.

6. Show that if a, b are positive integers, and p is a prime, then
$$\mathrm{ord}_p(a + b) \geq \min\{\mathrm{ord}_p(a), \mathrm{ord}_p(b)\}.$$
   Prove moreover that equality holds whenever $\mathrm{ord}_p(a) \neq \mathrm{ord}_p(b)$.
   Here the min of two numbers means the smaller of the two, or the common value if the two are equal.

7. Suppose u, v are positive integers and that uv is a perfect square (meaning, m^2 for some integer m). Suppose also that $\gcd(u, v) = 1$. Show that u, v are both perfect squares.

   Hint: First show that a positive integer n is a perfect square if and only if $\mathrm{ord}_p(n)$ is even for all primes p.

8. Let a, b be positive integers. Prove that there is a positive integer L satisfying the following two conditions: (a) $a \mid L$ and $b \mid L$, (b) if M is any positive integer for which $a \mid M$ and $b \mid M$, then $L \mid M$.

   The number L is called a least common multiple of a, b. Here are two possible approaches to this problem: (i) Show directly that the smallest positive common multiple of a, b satisfies these two conditions on L. (ii) Specify an integer satisfying these two conditions by giving its prime factorization.

MATH 6400 problems (extra credit for 4400 students)

G1. Prove that the product of two consecutive positive integers (meaning $n, n+1$) is never a square. Do the same with "two" replaced by "three" and then by "four".

G2. Define a sequence $\{F_n\}$, for integers $n \geq 0$, by setting

$$F_n = 2^{2^n} + 1.$$

Show that for any pair of distinct integers $n, m \geq 0$, we have $\gcd(F_n, F_m) = 1$.

Hint: Compute the first several products of the form $F_0, F_0F_1, F_0F_1F_2, \ldots$; you should notice a pattern, which you can prove by induction. Use this pattern to establish the gcd claim.