E. Dummit's Math 1365 ~ Intro to Proof, Fall 2019 ~ Homework 4, due Oct 9th.

Justify all responses with clear explanations and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly, and clearly identify all problem numbers. Either staple the pages of your assignment together and write your name on the first page, or paperclip the pages and write your name on all pages.

---

1. Show the following using only the axioms and basic properties of $\mathbb{Z}$:
   (a) If a, b, c are integers, then $(a + c) + b = b + (a + c)$.
   (b) If a, b, c are integers and $ab + ac = 0$, then $a = 0$ or $b = -c$.
   (c) If a, b are integers with $a > 1$ and $b > 1$, then $ab > 1$. [Hint: Compute $a \cdot (b - 1)$.]
   (d) If a, b, c, x, y are integers where $a|b$ and $a|c$, then $a|(xb + yc)$.

---

2. Recall that an integer n is even if $n = 2a$ for some integer a, while an integer n is odd if $n = 2b + 1$ for some integer b. It is a consequence of the division algorithm that every integer is even or odd, and no integer is both even and odd.
   (a) Show that the sum of two even or two odd integers is even, and that the sum of an even integer and an odd integer is odd.
   (b) Show that the product of an even integer with any integer is even, and the product of two odd integers is odd.
   (c) Deduce that n^2 is even if and only if n is even.
   (d) Show that for all positive integers n, the integer $n^2 + n$ is always even.

---

3. The Fibonacci numbers are defined as follows: $F_1 = F_2 = 1$ and for $n \geq 2$, $F_n = F_{n-1} + F_{n-2}$. The first few terms are 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, and so forth.
   (a) Prove that $F_1 + F_2 + F_3 + \cdots + F_n = F_{n+2} - 1$ for every positive integer n.
   (b) Prove that $F_1^2 + F_2^2 + F_3^2 + \cdots + F_n^2 = F_n F_{n+1}$ for every positive integer n.
   (c) Let $\varphi = \dfrac{1+\sqrt{5}}{2}$ and $\overline{\varphi} = \dfrac{1-\sqrt{5}}{2}$. Prove that $F_n = \dfrac{1}{\sqrt{5}}(\varphi^n - \overline{\varphi}^n)$ for every positive integer n. [Hint: First show $\varphi^2 = \varphi + 1$ and likewise for $\overline{\varphi}$.]

---

4. Suppose a and b are relatively prime integers.
   (a) Show that $\gcd(a + b, a - b)$ must either equal 1 or 2.
   (b) Give examples showing that both possibilities can occur in part (a).

---

5. For each pair of integers (a, b), use the Euclidean algorithm to calculate their greatest common divisor $d = \gcd(a, b)$ and also to find integers x and y such that $d = ax + by$.
   (a) $a = 12$, $b = 44$.
   (b) $a = 5567$, $b = 12445$.
   (c) $a = 2019$, $b = 20223$.

---

6. This problem has been moved to homework 5.

---

7. The goal of this problem is to analyze the maximum possible number of divisions that the Euclidean algorithm requires (in the parlance of computer science, this represents the worst-case time complexity). One might expect the slowest possible computation to occur when all of the quotients in the division algorithm are 1, and the resulting gcd is also 1; our goal is to prove this fact.

   (a) As motivation, find a and b such that the Euclidean algorithm takes 6 divisions to compute their gcd of 1, and all of the corresponding quotients are 1. In other words, find a and b such that

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ r_2 &= q_4 r_3 + r_4 \\ r_3 &= q_5 r_4 + r_5 \\ r_4 &= q_6 r_5 \end{aligned}$$

   where $q_1 = q_2 = q_3 = q_4 = q_5 = q_6 = 1$ and $r_5 = 1$.

   (b) Prove that the Euclidean algorithm requires exactly n divisions to compute $\gcd(F_{n+2}, F_{n+1})$, where F_n is the nth Fibonacci number, as defined in problem 3.

   (c) Suppose that $b \le a$ and that a and b are integers for which the Euclidean algorithm requires at least $n \ge 2$ divisions to compute $\gcd(a, b)$. Prove that $b \ge F_{n+1}$ and $a \ge F_{n+2}$.

   (d) Deduce that if $b \le a$ and a, b are the smallest integers for which the Euclidean algorithm requires exactly n divisions, then $a = F_{n+2}$ and $b = F_{n+1}$.

   (e) For any positive integers a and b with $b \le a$, conclude that the Euclidean algorithm will compute $\gcd(a, b)$ using at most $\log_\varphi(b) + 3$ divisions, where $\varphi = \dfrac{1+\sqrt{5}}{2}$. [Hint: Use the formula for the Fibonacci numbers from problem 3(d).]

   - Remark: Because $\log_\varphi(b) + 3 < 5\lceil \log_{10}(b) \rceil$, part (d) implies that the Euclidean algorithm will compute $\gcd(a, b)$ with a number of divisions that is at most 5 times the number of digits of b. Thus for example, using the Euclidean algorithm to compute the gcd of two 1000-digit numbers will only take at most 5000 steps (which is very efficient!).
