**MTH 505: Number Theory** **Spring 2020**
**Homework 1** **Drew Armstrong**

---

**Problem 1.** Find the complete integer solution $x, y \in \mathbb{Z}$ to the following Diophantine equation:

$$1035x + 644y = 299.$$

**Problem 2.** Let $a, b, c, x \in \mathbb{Z}$ be any integers satisfying $a = bx + c$. In this case prove that

$$\gcd(a, b) = \gcd(b, c).$$

[Hint: Show that the sets of common divisors are the same: $\text{Div}(a, b) = \text{Div}(b, c)$. It follows that the greatest element of each set is the same.]

**Problem 3.** Consider any non-zero integers $a, b, c \in \mathbb{Z}$. In class I defined the greatest common divisor $\gcd(a, b, c)$ as the greatest element of the following set of common divisors:

$$\text{Div}(a, b, c) = \{d \in \mathbb{Z} : d|a \text{ and } d|b \text{ and } d|c\}.$$

Prove that the same concept can also be defined recursively, as follows:

$$\gcd(a, b, c) = \gcd(\gcd(a, b), c).$$

**Problem 4.** In this problem you will give a **non-constructive** proof of Bézout's identity. Consider two nonzero integers $a, b \in \mathbb{Z}$ and define the set

$$S = \{ax + by : x, y \in \mathbb{Z} \text{ and } ax + by > 0\}.$$

This set is non-empty because it contains $|a|$, hence it has a least element by well-ordering. Let $d \in S$ denote this least element.

(a) Prove that $d$ is a common divisor of $a$ and $b$. [Hint: Let $r$ be the remainder of $a$ mod $d$. If $r \neq 0$ show that $r$ is an element of $S$ that is smaller than $d$.]

(b) Continuing from (a), show that $d$ is the **greatest** common divisor of $a$ and $b$. [Hint: Let $e$ be any common divisor of $a$ and $b$. Use (a) to show that $e \leqslant d$.]

**Problem 5. Euclid's Lemma.** For any integers $a, b, c \in \mathbb{Z}$ with $a|bc$ and $\gcd(a, b) = 1$, prove that $a|c$. [Hint: From Bézout's identity we know that $ax + by = 1$ for some $x, y \in \mathbb{Z}$. Multiply both sides by $c$.]

**Problem 6. Lamé's Theorem.** Consider some integers $a, b \in \mathbb{Z}$ with $a > b \geqslant 0$ and suppose that the Euclidean algorithm uses $n$ divisions with remainder to compute $\gcd(a, b)$. In this case, Lamé's Theorem says that we must have $a \geqslant F_{n+1}$ and $b \geqslant F_n$, where the Fibonacci numbers are defined by $F_0 = 0$, $F_1 = 1$ and $F_m = F_{m-1} + F_{m-2}$.

(a) Prove Lamé's Theorem by induction on $n$, starting with $n = 0$ and $n = 1$.

(b) Prove by induction that for all $n \geqslant 2$ we have

$$F_n > \phi^{n-2} = \left(\frac{1 + \sqrt{5}}{2}\right)^{n-2}.$$

(c) Assuming that $n \geqslant 2$, combine parts (a) and (b) to prove that we have $n < 5d + 2$, where $d$ is the number of decimal digits in $b$.