Math 230 **Spring 2019**
Homework 4 **Drew Armstrong**

Problem 1. Linear Diophantine Equations. Use the Extended Euclidean Algorithm to find all integers $x, y \in \mathbb{Z}$ satisfying the following equation:

$$345x + 234y = 123.$$

Problem 2. Euclid's Lemma. For all integers $a, b, c \in \mathbb{Z}$ prove that

$$(a|bc \wedge \gcd(a,b) = 1) \Rightarrow (a|c).$$

[Hint: If $\gcd(a,b) = 1$ then one can use the Extended Euclidean Algorithm to find integers $x, y \in \mathbb{Z}$ satisfying $ax + by = 1$. Multiply both sides of this equation by c.]

Problem 3. Prime Numbers. Given integers $d, n \geq 1$ we say that d is a *proper divisor* of n if $d|n$ and $1 < d < n$. An integer $p \geq 2$ is called *prime* if if has no proper divisors.

(a) Prove that every integer $n \geq 2$ has a prime divisor. [Hint: Assume for contradiction that there exists a positive integer with no prime divisor and let m be the smallest such integer. Since m is not prime it must have a proper divisor. Now what?]

(b) **Euclid's Proof of Infinite Primes.** In this problem you will prove that there exist infinitely many prime numbers. So assume for contradiction that there are only finitely many primes, and call them $2 = p_1 < p_2 < \cdots < p_k$. Now consider the number

$$n = (p_1 p_2 \cdots p_k) + 1.$$

From part (a) you know that there exists a prime factor $p|n$. But show that this p cannot be equal to any of $p_1, p_2, \ldots, p_k$.

Problem 4. Base-b Arithmetic. Let us fix an integer $b \geq 2$ called the "base."

(a) For all integers $k \geq 1$ observe that $(b-1)(1 + b + b^2 + \cdots + b^{k-1}) = b^k - 1$.

(b) **Existence.** For all integers $n \geq 0$ consider the following statement:

$$P(n) := \text{“}\exists\, r_0, r_1, r_2, \ldots \in \{0, 1, \ldots, b-1\}, n = r_0 + r_1 b + r_2 b^2 + \cdots .\text{”}$$

Fix $n \geq 0$ and assume for induction that $P(n)$ is true. In this case, prove that $P(n+1)$ is also true. [Hint: You have assumed $n = r_0 + r_1 b + r_2 b^2 + \cdots$ for some integers $r_0, r_1, r_2, \ldots \in \{0, 1, \ldots, b-1\}$. Let $k \geq 0$ be the smallest index such that $r_k \neq b - 1$ and show that $n + 1 = (r_k + 1)b^k + r_{k+1} b^{k+1} + r_{k+2} b^{k+2} + \cdots$. You will need part (a).]

(c) **Uniqueness.** For all integers $k \geq 0$ consider the statement $Q(k) :=$ "For all integers $r_0, \ldots, r_k$ and $s_0, \ldots, s_k$ in the set $\{0, 1, \ldots, b-1\}$ we have

$$(r_0 + r_1 b + \cdots + r_k b^k = s_0 + s_1 b + \cdots s_k b^k) \Rightarrow (r_0 = s_0 \wedge r_1 = s_1 \wedge \cdots \wedge r_k = s_k).\text{”}$$

Fix $k \geq 0$ and assume for induction that $Q(k)$ is true. In this case, prove that $Q(k+1)$ is also true. [Hint: Assume that $n = r_0 + \cdots + r_{k+1} b^{k+1} = s_0 + \cdots + s_{k+1} b^{k+1}$. Now use the fact that the quotient and remainder of n mod b are **unique**.]