1. Write clear definitions of the following terms. (This question counts as two questions in the grading of this exam.)

   (a) Suppose that $a$ and $b$ are integers with $b \neq 0$. What does it mean for $a$ to be divisible by $b$?
   Answer: $a$ is divisible by $b$ if there exists an integer, $t$, such that $a = bt$.

   (b) Suppose that $a$ and $b$ are integers, not both zero. Define what is meant by the greatest common divisor of $a$ and $b$.
   Answer: The greatest common divisor of $a$ and $b$, denoted by $\gcd(a, b)$, is the largest integer that divides both $a$ and $b$.

   (c) What do we mean when we say that two integers, $a$ and $b$, are relatively prime?
   Answer: To say that $a$ and $b$ are relatively prime is to say that $\gcd(a, b) = 1$.

   (d) Suppose that $p$ is an integer with $p > 1$. What do we mean when we say that $p$ is a prime number?
   Answer: $p$ is said to be a prime number if the only positive divisors of $p$ are $1$ and $p$. (Using the notation that we introduced in class, $p$ is said to be prime if $D(p) = \{1, p\}$.)

2. State (but do not prove) the Division Algorithm theorem. I will get you started: “Let $a$ and $b$ be integers with $b > 0$.”

   **Answer:** Let $a$ and $b$ be integers with $b > 0$. Then there are unique integers, $q$ and $r$, such that $a = qb + r$ and $0 \leq r < b$.

3. Suppose that $a$ and $b$ are (given) integers with $b > 0$ and consider the set

$$S = \{a - bt \mid t \in \mathbb{Z} \text{ and } a - bt > 0\}.$$ 

Use the Well–Ordering Principle to explain why $S$ must have a smallest member.

**Explanation:** Since, for any integer $t$, $a - bt$ is an integer and the definition of the set $S$ requires that $a - bt > 0$, we see that $S \subseteq \mathbb{N}$. We will now explain why the set $S$ must not be the empty set by considering two possible cases: If $a > 0$, then the number $a - b(0) = a$ is positive and thus $a \in S$. If $a \leq 0$, then the number

$$x = a - b(a - 1) = b + a(1 - b)$$

is positive because $b > 0$, $a \leq 0$, and $1 - b \leq 0$ and hence $x \in S$. Thus we see that $S \neq \emptyset$. By the Well–Ordering Principle, $S$ must have a smallest member.
4. Let \( a, b, \) and \( c \) be integers with \( a \neq 0 \) and \( b \neq 0 \) and suppose that \( a \) divides \( b \) and also that \( a \) divides \( c \). Prove that if \( m \) and \( n \) are any integers, then \( a \) divides \( mb + nc \).

**Proof:** See notes.

5. Prove *Euclid’s Lemma*: If \( a, b, \) and \( c \) are integers with \( \gcd (a, b) = 1 \) and \( a \) divides \( bc \), then \( a \) divides \( c \).

6. Use Euclid’s Algorithm to show that \( \gcd (491, 286) = 1 \).

**Solution:**

\[
\begin{align*}
491 &= 1(286) + 205 \\
286 &= 1(205) + 81 \\
205 &= 2(81) + 43 \\
81 &= 1(43) + 38 \\
43 &= 1(38) + 5 \\
38 &= 7(5) + 3 \\
5 &= 1(3) + 2 \\
3 &= 1(2) + 1
\end{align*}
\]

from which we conclude that \( \gcd (491, 286) = 1 \).

7. Consider the Diophantine equation

\[491x + 286y = 4.\]

(a) Based on information from problem 5, how do you know that this Diophantine equation has a solution?

(b) Use the work you did in problem 5 to find a solution of this Diophantine equation. (Include gory details.)

(c) Find all solutions of this Diophantine equation.

**Solution:** We know that a Diophantine equation, \( ax + by = c \), has a solution if and only if \( c \) is a multiple of \( \gcd (a, b) \). Since \( \gcd (491, 286) = 1 \) and since 4 is a multiple of 1, we can conclude that the above Diophantine equation has a solution (and hence has infinitely many solutions). We first find a solution of the Diophantine equation
491x + 286y = 1 by working the Euclidean Algorithm in reverse:

\[
1 = 3 - 1 (2) \\
= 3 - 1 (5 - 1 (3)) \\
= -1 (5) + 2 (3) \\
= -1 (5) + 2 (38 - 7 (5)) \\
= 2 (38) - 15 (5) \\
= 2 (38) - 15 (43 - 1 (38)) \\
= -15 (43) + 17 (38) \\
= -15 (43) + 17 (81 - 1 (43)) \\
= 17 (81) - 32 (43) \\
= 17 (81) - 32 (205 - 2 (81)) \\
= -32 (205) + 81 (81) \\
= -32 (205) + 81 (286 - 1 (205)) \\
= 81 (286) - 113 (205) \\
= 81 (286) - 113 (491 - 1 (286)) \\
= -113 (491) + 194 (286).
\]

This shows that \((x, y) = (-113, 194)\) is a solution of the Diophantine equation \(491x + 286y = 1\). In addition, we see that

\[
(4) (-113) (491) + (4) (194) (286) = 4 (1)
\]

and thus \((x, y) = (-452, 776)\) is a solution of the Diophantine equation

\[491x + 286y = 4.\]

All solutions of this equation are given by

\[(x, y) = (-452 + 286t, 776 - 491t)\]

where \(t\) can be any integer.

8. Prove that there is no largest prime number.

**Proof:** See notes.

9. Suppose that \(a_1 = 2\) and suppose that

\[a_{n+1} = \frac{1}{2} (a_n + 6)\]

for all integers \(n \geq 1\). Use the Principle of Induction to prove that \(a_n < 6\) for all integers \(n \geq 1\).

**Proof:** The proposition that we want to prove for all \(n \geq 1\) is

\[P(n): a_n < 6.\]
First observe that $a_1 = 2 < 6$ which means that statement $P(1)$ is true.

Now, if we assume that statement $P(n)$ is true (that is we assume that $a_n < 6$), then we obtain

$$a_{n+1} = \frac{1}{2} (a_n + 6) < \frac{1}{2} (6 + 6) = 6.$$  

Thus the truth of statement $P(n)$ implies the truth of statement $P(n+1)$. By the Induction Principle, we can conclude that statement $P(n)$ is true for all integers $n \geq 1$. 