Steven Rosendahl
Homework 3

1. Suppose that $a, b \in \mathbb{Z}$ and define the set $J = ax + by | x, y \in \mathbb{Z}$. Prove that $J = Z$ if and only if $gcd(a, b) = 1$.

   Assume $J = \mathbb{Z}$. We know that $1 \in \mathbb{Z}$, so $1 \in J$, and $1 \in \{ax + by | x, y \in \mathbb{Z}\}$. Therefore $1 = ax + by$, so $gcd(a, b) = 1$ by Bezout's Identity.

   Assume $gcd(a, b) = 1$. Then there exists $u, v \in \mathbb{Z}$ such that $1 = au + bv$ by Bezuot's Identity. We know that any $n \in \mathbb{Z}$, we can represent it as $1 \cdot n = a \cdot un + b \cdot vn$. Let $x = un$ and $y = vn$. Then we have $n = ax + by$ where $ax + by \in \mathbb{Z}$. Since n is any arbitrary integer, we can say that $ax + by$ is any arbitrary integer for any $x, y \in \mathbb{Z}$, or $\{ax + by | x, y \in \mathbb{Z}\} = \mathbb{Z}$

   $\triangle$

2. We define the *Fibonacci Sequence* to be the sequence of integers $x_0, x_1, x_2, \ldots$ satisfying the properties

   $$x_0 = 0, \quad x_1 = 1, \quad \text{and} \quad x_n = x_{n-1} + x_{n-2} \text{ for all } n \geq 2.$$

   Prove that $gcd(x_n, x_{n-1}) = 1$ for all $n \geq 1$. (Hint: Try using induction on n.)

   For the base case, $n = 2$, we have that

   $$\begin{aligned} x_2 &= x_1 + x_0 \\ &= 1 + 0 \\ &= 1 \\ x_1 &= 1 \\ gcd(x_1, x_2) &= 1. \end{aligned}$$

   We can assume that $gcd(x_n, x_{n-1}) = 1$ for $n \geq 2$. We now need to show that $gcd(x_{n+1}, x_n) = 1$ for $n \geq 1$. We also have that $x_{n+1} = x_n + x_{n-1}$, so $gcd(x_{n+1}, x_n) = gcd(x_n + x_{n-1}, x_n)$. By Bezout's Identity, we know that $gcd(x_n + x_{n-1}, x_n) = (x_n + x_{n-1})u + x_n v$ for some $u, v \in \mathbb{Z}$. Then

   $$\begin{aligned} gcd(x_n + x_{n-1}, x_n) &= x_n u + x_{n-1} u + x_n v \\ &= x_{n-1} u + x_n(u + v) \\ &= x_{n-1} u + x_n w \\ &= gcd(x_{n-1}, x_n) \\ &= 1 \text{ by the induction hypothesis.} \end{aligned}$$

   Therefore, $gcd(x_{n+1}, x_n) = 1$.

   $\triangle$

3. Let a, b, x be positive integers with $x \geq 2$ and set $d = gcd(a, b)$.

   (a) Prove that $x^d - 1$ divides $gcd(x^a - 1, x^b - 1)$.

   We know that $d = gcd(a, b)$, so $d | a$ and $d | b$. We have $a = dn$ and $b = dm$. Then $x^a - 1 = x^{dn} - 1$ and $x^b - 1 = x^{dm} - 1$. We know that $x^{dn} = (x^d)^n$, so we can rewrite $x^{dn} - 1$ as $(x^d)^n - 1$. Now we have that $(x^d)^n - 1 = (x^d - 1)(x^{dn-1} + x^{dn-2} + \cdots + 1)$. Recall that $(x^d)^n - 1 = x^a - 1$, so we have $x^a - 1 = (x^d - 1)j$, where $j = (x^{dn-1} + x^{dn-2} + \cdots + 1) \in \mathbb{Z}$. Therefore, $(x^a - 1) | (x^d - 1)$. We can apply the same argument for $x^b - 1$, and we will find that $(x^b - 1) | (x^d - 1)$. Since $(x^d - 1)$ divides both $(x^b - 1)$ and $(x^a - 1)$, it divides $gcd(x^a - 1, x^b - 1)$.

   (b) Prove that $x^d - 1$ is a multiple of $gcd(x^a - 1, x^b - 1)$ and conclude that $x^d - 1 = gcd(x^a - 1, x^b - 1)$. (Hint: We know that there exist integers u and v such that $d = au + bv$. Now show that there exist integers α and β such that $x^d - 1 = \alpha(x^a - 1) + \beta(x^b - 1)$.)

Since we know $d = au + bv$ for $u, v \in \mathbb{Z}$, we can say

$$\begin{aligned} x^d - 1 &= x^{au+bv} - 1 \\ &= x^{au}x^{bv} - 1 \\ &= x^{au}x^{bv} - 1 + x^{au} - x^{au} \\ &= x^{au} \cdot (x^{bv} - 1) + 1 \cdot (x^{au} - 1). \end{aligned}$$

If we let $a =^{au}$ and $b = 1$, then we have $x^d - 1 = a \cdot (x^{bv} - 1) + b \cdot (x^{au} - 1)$. Therefore, by Bezout's Identity, $x^d - 1 = gcd(x^a - 1, x^b - 1)$.

△

4. Show that the equation $1495x + 50060y = 4$ has no solutions for $x, y \in \mathbb{Z}$.

$$\begin{aligned} 50060 &= 1495(33) + 725 \\ 1495 &= 725(2) + 45 \\ 725 &= 45(16) + 5 \\ 45 &= 5(9) + 0 \\ gcd(50060, 1495) &= 5 \end{aligned}$$

However, $5 \nmid 4$, so there is no solution.

5. Find all solutions to the equation $7x + 4y = 1$ for $x, y \in \mathbb{Z}$.

$$\begin{aligned} 7 &= 4 \cdot 1 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

$$\begin{aligned} 1 &= 4 \cdot 1 - 3 \cdot 1 \\ &= 4 \cdot 1 - (7 - 4) \cdot 1 \\ &= 4 \cdot 1 - 7 \cdot 1 + 4 \cdot 1 \\ &= 4 \cdot 2 - 7 \cdot 1 \end{aligned}$$

$x = 1 + 7n$ and $y = 2 + 4n$ are solutions to the Diophantine equation.

6. Find all solutions to the equation $1485x + 1745y = 15$ for $x, y \in \mathbb{Z}$.

$$\begin{aligned} 1745 &= 1485(1) + 260 \\ 1485 &= 260(5) + 185 \\ 260 &= 185(1) + 75 \\ 185 &= 72(2) + 35 \\ 75 &= 35(2) + 5 \\ 35 &= 7(5) + 0 \\ gcd(1745, 1485) &= 5 \end{aligned}$$

$$\begin{aligned} 5 &= 75 - 35(2) \\ 5 &= 75 - (185 - 75(2))(2) \\ &= 75(5) - 185(2) \\ 5 &= (260 - 185(1))(5) - 185(2) \\ &= 260(5) - 187(7) \\ 5 &= 260(5) - (1485 - 260(5))(7) \\ &= 260(40) + 1485(-7) \\ 5 &= (1745 - 1485(1))(40) + 1485(-7) \\ &= 1745(40) + 1485(-47) \\ 15 &= 1745(120) + 1485(-141) \end{aligned}$$

$x = -141 + \frac{349n}{3}$ and $y = 120 + 99n$ are solutions to the equation.

7. Suppose you have two small champagne glasses, one holding 8 ounces and another holding 5 ounces. Is it possible to fill one of the glasses with exactly 1 ounce of champagne? If so, how can this be done? If not, prove that it cannot be done.

We need to find a solution to the Diophantine Equation

$$8x + 5y = 1.$$

We know that $gcd(8, 5) = 1$, and $1|1$, so there is a solution. Working backwards through the Euclidian Algorithm gives us

$$\begin{aligned} 1 &= 3 - 2(1) \\ &= 3(2) - 5 \\ &= 8(2) + 5(-3). \end{aligned}$$

Therefore, if we fill the first glass up twice and empty the second glass three times, we will end up with 1 ounce leftover.