Daniel Oliveros A02093272
September 15, 2017

Homework 2

Problem #1
Suppose a, b, and c are integers. Please prove that the equation $ax + by = c$ has solutions in integers if and only if the greatest common divisor of a and b is a divisor of c.

To prove this, we will determine how assuming either statement leads us to the other. So, for the equation $ax + by = c$:

Statement P: "$ax + by = c$ has integer solutions"
Statement Q: "The greatest common divisor of a and b is a divisor of c"

There will be two steps to this proof. One where we show how, by assuming P to be true, we can arrive to the conclusion that Q also is, and one where we do the same process from the other end.

So, for $P \Rightarrow Q$:
We can start by assuming that $ax + by = c$ has integer solutions, that is, we can assume $x, y \in \mathbb{Z}$. In order to prove c must be a multiple of a and b's greatest common divisor, we will rewrite the formula to account for the fact that, for $gcd(a, b) = d$, $d|a$ and $d|b$. So:

$$\begin{aligned} ax + by = &\quad c \\ dk_1x + dk_2y = &\quad c \\ d(k_1x + k_2y) = &\quad c \end{aligned}$$

Since x and y are assumed to be integers, then we can rewrite the value $k_1x + k_2y$ as a simple constant k, such that:

$$\begin{aligned} d(k_1x + k_2y) = &\quad c \\ d(k) = &\quad c \end{aligned}$$

And from here, since we have determined c to be equal to d times some integer, we have concluded d to be a divisor of c.

And now, for $Q \Rightarrow P$:
To prove this relation, we will start by assuming $gcd(a, b)|c$. As complementary information, we will also use **Bézout's lemma**, which states that, for two nonzero integers a and b, $gcd(a, b)$ is the smallest nonnegative integer expressible as $ax_0 + by_0 = d$, defining d to be equal to $gcd(a, b)$. From this lemma, we can determine that there exists a tuple of integers (x_0, y_0), such that $ax_0 + by_0 = d$. So, with all these concepts in mind, we can determine that, since $d|c$, then $ax_0 + by_0|c$, which means$c = k(ax_0 + by_0)$. This means that there exists integer solutions x_0, y_0 that are valid solutions for x and y to the equation $ax + by = c$.

Problem # 2
Define the set E to be the set of even integers; that is, $E = \{x \in \mathbb{Z} : x = 2k, \text{where } k \in \mathbb{Z}\}$. Define the set F to be the set of integers that can be expressed as the sum of two odd numbers; that is,
$F = \{y \in \mathbb{Z} : y = a + b,\ \text{where } a = 2k_1 + 1 \text{ and } b = 2k_2 + 1\}$. Please prove $E = F$.

Once more, to prove this we will determine how assuming either set leads us to the other. So, for the sets $E$and F :

Statement P**:** "$E = \{x \in \mathbb{Z} : x = 2k, \text{where } k \in \mathbb{Z}\}$"
Statement Q**:** "$F = \{y \in \mathbb{Z} : y = a + b, \text{ where } a = 2k_1 + 1 \text{ and } b = 2k_2 + 1\}$"

There will be two steps to this proof. One where we show how, by starting from set P, we can arrive to the conclusion that Q is a similar set, and one where we do the same process from the other end.

So, for $P \Rightarrow Q$**:**

We can write any element x within the set E as $x = 2k$, which can be rewritten as $x = k + k$. From here, by adding and subtracting a number a, the resulting element x would be: $x = (k - a) + (k + a)$. In the case where k is an even number, by making a an odd number this would be the result:

$$x = (k - a) + (k + a)$$
$$x = (2k_1 - a) + (2k_1 + a)$$

Assuming a to be an odd number, it can be rewritten as $a = 2k_2 + 1$

$$x = (2k_1 - (2k_2 + 1)) + (2k_1 + (2k_2 + 1))$$
$$x = (2k_1 - 2k_2 - 1) + (2k_1 + 2k_2 + 1)$$
$$x = (2(k_1 - (k_2 - 1)) + 1) + (2(k_1 + k_2) + 1)$$

We can add up these constants to a single constant for each number

$$x = (2k_3 + 1) + (2k_4 + 1)$$

And, in the case where k is an odd number, by making a an even one, this would be the result:

$$x = (k - a) + (k + a)$$
$$x = (2k_1 + 1 - a) + (2k_1 + 1 + a)$$

Assuming a to be an even number, it can be rewritten as $a = 2k_2$

$$x = (2k_1 + 1 - 2k_2) + (2k_1 + 1 + 2k_2)$$
$$x = (2(k_1 - k_2) + 1) + (2(k_1 + k_2) + 1)$$

We can add up these constants to a single constant for each number

$$x = (2k_3 + 1) + (2k_4 + 1)$$

So, since we can rewrite any element in E to be equal to a similar element in F, we have proven this side of the relation.

And now, for $Q \Rightarrow P$:

We can write any element x within the set F as $x = a + b$, which can be rewritten as $x = (2k_1 + 1) + (2k_2 + 1)$. From here, by adding up all the constants and grouping them up, we can show that any element in F can be similar to an element in E, so:

$$x = (2k_1 + 1) + (2k_2 + 1)$$
$$x = 2k_1 + 2k_2 + 2$$
$$x = 2(k_1 + k_2 + 1)$$

We can add up these constants to a single constant

$$x = 2k_3$$

So, since we can rewrite any element in F to be equal to a similar element in E, we have proven this side of the relation as well.

We have proven how we can rewrite any element in E as an element in F and likewise for the other side of the process. Therefore, we have proven E to be equal to F.