Mark Petersen

Exercise 0.1. Find the largest possible integer that can't be written as an integral linear combination of $5, 9, 11$ and prove that your answer is correct.

Disproof: We wish to show that every integer can be written as an integral linear combination of $5, 9, 11$. We begin by showing that every integer greater than or equal to zero can be written as an integral linear combination $5, 9, 11$, and then we will show that every negative integer can be written as a linear combination of $5, 9, 11$. We work the first part by induction.

We want to show that the open sentence

$$P(n): \text{ every non negative integer can be written as an integral linear combinatio of } 5, 9, 11$$

is true for all $n \in \mathbb{Z} \geq 0$. We show this by strong induction.

Base Cases: We verify $P(0)$ through $P(4)$

$$\begin{aligned}
P(0) :&0 \cdot 5 + 0 \cdot 9 + 0 \cdot 11 \\
P(1) :&2 \cdot 5 + (-1) \cdot 9 + 0 \cdot 11 \\
P(2) :&0 \cdot 5 + (-1) \cdot 9 + 1 \cdot 11 \\
P(3) :&(-6) \cdot 5 + 0 \cdot 9 + 3 \cdot 11 \\
P(4) :&(-8) \cdot 5 + 0 \cdot 9 + 4 \cdot 11
\end{aligned}$$

Induction Step: Let $k \in \mathbb{Z} \geq 5$. We assume by strong induction that $P(k-4) \wedge P(k-3) \wedge \ldots \wedge P(k)$ and we want to show that $P(k+1)$ is true which is the statement: $k+1$ can be written as an integral linear combination of $5, 9, 11$. Since

$$k + 1 = k - 4 + 5$$

and since we assume that $P(k-4)$ is true, we know that $k - 4 = x \cdot 5 + y \cdot 9 + z \cdot 11$for some $x, y, z \in \mathbb{Z}$. Substituting this into the above equation yields

$$\begin{aligned}
k + 1 &= x \cdot 5 + y \cdot 9 + z \cdot 11 + 5 \\
&= (x+1) \cdot 5 + y \cdot 9 + z \cdot 11,
\end{aligned}$$

which shows that $k+1$ can be written as an integral linear combination of $5, 9, 11$. Thus $P(k+1)$ is true. Therefore the open sentence $P(n)$ is true for all non negative integers.

Now that we know that $P(n)$ is true, we can easily show that all of the negative integers can be written as a linear combination of $5, 9, 11$. To show this we assume directly that $a \in \mathbb{Z} < 0$, and that $P(n)$ is true. Well we know that $-a = x \cdot 5 + y \cdot 9 + z \cdot 11$ for some $x, y, z \in \mathbb{Z}$. Multiplying both sides by negative one yields

$$a = (-x) \cdot 5 + (-y) \cdot 9 + (-z) \cdot 11$$

which shows that any negative integer can be written as a linear combination of $5, 9, 11$. Thus showing that every integer can be written as a linear combination of $5, 9, 11$. Therefore, there is not largest integer that can't be written as an integral linear combination of $5, 9, 11$. ■

Exercise 0.2. Prove that $3 \mid \left(5^{2n} - 1\right)$ for all natural numbers n.

Proof: We wish to show that the open sentence

$$P(n): \; 3 \mid \left(5^{2n} - 1\right)$$

is true for all $n \in \mathbb{N}$. We work this by induction.

Base Case: We first verify $P(1)$ which is the statement

$$\begin{aligned} 3 \mid \left(5^2 - 1\right) &= 3 \mid (25 - 1) \\ &= 3 \mid 24, \end{aligned}$$

which is true since $24 = 3 \cdot 8$.

Induction Step: Let $k \in \mathbb{N}$. We suppose that $P(k)$ is true and want to show that $P(k+1)$ is true which is the statement $3 \mid \left(5^{2(k+1)} - 1\right)$ is true. We do this by looking closely at the statement $P(k+1)$, and letting $m \in \mathbb{Z}$.

$$\begin{aligned} 3 \mid \left(5^{2(k+1)} - 1\right) &= 3 \mid \left(5^{2k+2} - 1\right) \\ &= 3 \mid \left(5^{2k} 5^2 - 1\right) \\ &= 3 \mid \left(5^{2k}(1 + 24) - 1\right) \\ &= 3 \mid \left(5^{2k} - 1 + 24 \cdot 5^{2k}\right) \\ &= 3 \mid \left(3m + 24 \cdot 5^{2k}\right) \quad \text{(Since we assume } P(k) \text{ to be true)} \\ &= 3 \mid \left(3\left(m + 8 \cdot 5^{2k}\right)\right), \end{aligned}$$

which is true since $3 \mid 3x$ for any $x \in \mathbb{Z}$. Since the induction step and base case are true, the open sentence $P(n)$ is true for all n. ■

Exercise 0.3. Define a relation R on $\mathbb{R}$ by aRb if $|a - b| < 1$. Prove or disprove the following.

a) R is reflexive
Proof: We assume directly that $a \in \mathbb{R}$, then $a - a = 0$ for all a. Since $0 < 1$, aRa is true for all $a \in \mathbb{R}$. Therefore R is reflexive. ■

b) R is symmetric
Proof: Let $a, b \in \mathbb{R}$. We assume directly that $|a - b| < 1$. This is equivalent to $-1 < a - b < 1$. Multiplying the inequality by -1 yields $-1 < b - a < 1$ which is equivalent to $|b - a| = 1$. Thus R is symmetric. ■

c) R is transitive
Disproof: We disprove it by showing that there exists an $a, b, c \in \mathbb{R}$ such that if $|a - b| < 1$, $|b - c| < 1$ and $|a - c| \geq 1$.
Let $a = 1.1$, $b = 0.2$, and $c = 0$. Then $|a - b| < 1$,$|b - c| < 1$ and$|a - c| \geq 1$. Thus R is not transitive. ■

d) R is antisymmetric
Disproof: We disprove it by showing that there exists an $a, b \in \mathbb{R}$ such that if $|a - b| < 1$, $|b - a| < 1$ and $a \neq b$. Let $a = 0.1$ and $b = 0$, Then $|0.1 - 0| < 1$ and $|0 - 0.1| < 1$ and $0.1 \neq 0$. Therefore, R is not antisymmetric. ■

Exercise 0.4. Use the extended Euclidean algorithm to find the GCD of 8642 and 3219, and then express that GCD as a linear combination of 8642 and 3219.

Using the extended Euclidean algorithm we get the series of steps

$$\begin{aligned} 8642 &= 3219 \cdot 2 + 2204 \\ 3219 &= 2204 + 1015 \\ 2204 &= 1015 \cdot 2 + 174 \\ 1015 &= 174 \cdot 5 + 145 \\ 174 &= 145 + 29 \\ 145 &= 29 \cdot 5 + 0 \end{aligned}$$

Hence the GCD $(8642, 3219) = 29$. To express the GCD as a linear combination we use the series of steps previously calculated.

$$\begin{aligned}
29 &= 174 - 145 \\
&= 174 - (1015 - 174 \cdot 5) \\
&= 174 \cdot 6 - 1015 \\
&= (2204 - 1015 \cdot 2) \cdot 6 - 1015 \\
&= 2204 \cdot 6 - 1015 \cdot 13 \\
&= 2204 \cdot 6 - (3219 - 2204) \cdot 13 \\
&= 2204 \cdot 19 - 3219 \cdot 13 \\
&= (8642 - 3219 \cdot 2) \cdot 19 - 3219 \cdot 13 \\
&= 19 \cdot 8642 - 32 \cdot 3219
\end{aligned}$$

Thus $29 = 19 \cdot 8642 - 32 \cdot 3219$

Exercise 0.5. Prove that $S \cap (T \cup R) = (S \cap T) \cup R \iff R \subseteq T$

Disproof: This is a biconditional statement so we only need to disprove one way to disprove the statement. We will disprove

$$R \subseteq T \implies S \cap (T \cup R) = (S \cap T) \cup R.$$

We suppose directly that S, T, R are sets and that $R \subseteq T$. We need to show that $S \cap (T \cup R) \subseteq (S \cap T) \cup R$ and that $S \cap (T \cup R) \supseteq (S \cap T) \cup R$.

$(\supseteq)$: Let $x \in (S \cap T) \cup R$, then $x \in S$ and $x \in T$ or $x \in R$. This gives us three cases.

Case 1. Let $x \in R$ such that $x \notin S \cap T$. This can happen when $x \in R$ but $x \notin S$. Well if $x \notin S$, then $x \notin S \cap (T \cup R)$ since $x \notin S$ and for $x \in S \cap (T \cup R)$, $x \in S$ and $x \in T \cup R$. This is a contradiction.

We can also show it with an example. Let $R = \{1\}$, $T = \{1, 2\}$, $S = \{3\}$. Then $S \cap (T \cup R) = \emptyset$and $(S \cap T) \cup R = R$. We note that $R \subseteq T$, but $S \cap (T \cup R) \neq (S \cap T) \cup R$. Which shows that the statement is false. ■