Amin Zolfagharian - 610300118

Problem 1.

(i)

$$6^3 \overset{55}{\equiv} 216 \overset{55}{\equiv} 51$$

51 is the encrypted message.

(ii) First we need to find d. We know that $de \overset{(p-1)(q-1)}{\equiv} 1$ where $pq = 55$. Thus we have $p = 5$ and $q = 11$ and $de = 3d \overset{40}{\equiv} 1$. Which implies that $d = 27$. Now we can decrypt the message.

$$6^{27} \overset{55}{\equiv} (-4)^9 \overset{55}{\equiv} (-64)^3 \overset{55}{\equiv} (-9)^3 \overset{55}{\equiv} -14 \overset{55}{\equiv} 41$$

The decrypted message is 41.

Problem 2.

Let us have $a^2 = b^2 + c^2$. Then we know that there exists some $m, n \in \mathbb{Z}$ such that:

$$\begin{gathered} b = 2mn \\ c = m^2 - n^2 \end{gathered}$$

Now if the area is of the form x^2 then we have:

$$x^2 = S = bc/2 = mn(m^2 - n^2)$$

Let $d = (m, n)$, and $m = dm'$, $n = dn'$:

$$x^2 = d^2 m'n'd^2(m'^2 - n'^2) \implies x^2/d^4 = m'n'(m'^2 - n'^2)$$

Where we have $(m', n') = 1$. And since $(m', n') = (m' - n', n')$, then we have:

$$x^2 = m'n'(m' - n')(m' + n')$$

And since all factors are relatively prime to the other then we have all m', n', $m'^2 - n'^2$ are all squared:

$$\begin{gathered} m' = z^2 \\ n' = y^2 \\ m'^2 - n'^2 = w^2 \\ \implies z^4 - y^4 = w^2 \end{gathered}$$

Which I proved doesn't have an answer on problem 1 part 2 of the HW7.

Problem 3.

For any $a \in \mathbb{N}$, Let $m = a + 1$ and $n = a$. Then $2mn, m^2 - n^2, m^2 + n^2$ form a triangle. Now note that:

$$m^2 - 2mn + n^2 = (m - n)^2 = (a + 1 - a)^2 = 1$$
$$\implies m^2 + n^2 = 2mn + 1$$

Which shows that for any a we have a triple, with two consecutives numbers.

Problem 4.