MODEL ANSWERS TO THE THIRD HOMEWORK

8.1.1. First note that \( a = 18, \) \( b = 20 \) and \( c = -35 \) have no common factors. \( a \) is divisible by \( 9 = 3^2 \) and \( b \) is divisible by \( 4 = 2^2. \) So we are reduced to considering \( a = 2, \) \( b = 5 \) and \( c = -35. \) \( 5 = (5, -35) \) is a common factor of \( b \) and \( c. \) So we are reduced to considering \( a = 10, \) \( b = 1 \) and \( c = -7. \) We are now ready to apply Legendre’s theorem.

\( a, b \) and \( c \) don’t all have the same sign. We now check whether \(-ab\) is a residue of \(-c\) and \( -bc \) is a residue of \( a. \) \(-10 \) modulo \( 7 \) is the same as \( 4 \) modulo \( 7, \) which is visibly a residue of \( 7. \) However \( 7 \) is not a residue of \( 10, \) since

\[
1^2 = 1 \quad 2^2 = 4 \quad 3^2 = 9 \quad 4^2 \equiv 6 \mod 10 \quad \text{and} \quad 5^2 \equiv 5 \mod 10.
\]

Thus there are no solutions.

8.1.2. Suppose \( x, y \) and \( z \) is a solution of

\[
ax^2 + by^2 + cz^2 = 0,
\]

with \( x, y \) and \( z \) not all zero. Suppose that \( z = 0. \) If \( p|a \) then \( p|by^2. \) But then \( p|y^2, \) so that \( p^2|ax^2. \)

It is enough to find \( x, y \) and \( z \) non-zero such that

\[
\max(x, y, z) < 2 \max(a^2, b^2, c^2),
\]

since we can always flip the sign of any variable.

Possibly switching \( x, y \) and \( z \) and flipping the sign of \( a, b \) and \( c, \) we may assume that \( a > 0, b > 0 \) and \( c > 0. \)

We must have \( z > 0 \) and at least one of \( x \) and \( y > 0. \) Suppose that \( y > 0 \) and yet \( x = 0. \) Then \( by^2 = cz^2. \) The only possibility is that \( b|z \) but then \( b^2|cz^2, \) so that \( b|y^2. \) This is only possible if \( b = 1. \) Similarly \( c = 1. \) In this case we could take the solution \( x = 1, y = 1 \) and

In the proof of (7.1) we find \( x, y \) and \( z \) such that

\[
|x| < \sqrt{|bc|} \quad |y| < \sqrt{|ca|} \quad \text{and} \quad |z| < \sqrt{|ab|}.
\]

and either

\[
a^2 + by^2 + cz^2 = 0 \quad \text{or} \quad a(az + by)^2 + b(yz - ax)^2 + c(z^2 + ab)^2 = 0.
\]

Suppose we have the former case. Using the inequality between arithmetic and geometric means we get

\[
x \leq \frac{b - c}{2} \quad y \leq \frac{a - c}{2} \quad \text{and} \quad z \leq \frac{a + b}{2}.
\]
Since \( a \leq a^2 \) and the average of two of \( a^2, b^2 \) and \( c^2 \) is at most the maximum, it follows easily that
\[
\max(x, y, z) < 2 \max(a^2, b^2, c^2).
\]
In the latter case
\[
|xz + by| < \sqrt{-ac} + b\sqrt{-ac} = 2\sqrt{-ac} \leq b(a - c) \leq 2 \max(a^2, b^2, c^2).
\]
We obtain the same bound for \( yz - ax \) by a symmetric argument. We have
\[
|z^2 + ab| < ab + ab = 2ab \leq 2 \max(a^2, b^2, c^2).
\]

8.1.3. We may as well assume that \( c = 1 \). As \( x^2 + y^2 = z^2 \) it suffices to check that \( x \) and \( y \) have no common factors. As \( a \) and \( b \) have opposite parity, it follows that \( x \) is odd. Suppose \( p|a \) is an odd prime. If \( p|x \) then \( p|b \), which contradicts the fact that \( (a, b) = 1 \). Thus \( x \) and \( y \) are coprime.

8.1.5. We know all of the solutions are given by
\[
x = c(a^2 - b^2) \quad y = 2abc \quad \text{and} \quad z = c(a^2 + b^2),
\]
where \( a \) and \( b \) are integers and \( 2c \in \mathbb{Z} \). If we assume that \( (x, y) = 1 \) and \( x \) is odd then \( y \) is even, \( (a, b) = 1 \) and \( c \neq 1 \). If \( z > 0 \) then \( c = 1 \). We may as well assume that \( a > b \).

This gives us all solutions with \( x \) odd. To get all solutions with \( x \) even just switch \( x \) and \( y \).

8.1.7. We first make the change of variables:
\[
x = x' + y \quad y = y' \quad \text{and} \quad z = z'.
\]
This reduces our quadratic to
\[
x^2 + 2y^2 + 5z^2 + 100yz + 40xz.
\]
Now make the change of variables:
\[
x = x' - 20z \quad y = y' \quad \text{and} \quad z = z'.
\]
This reduces our quadratic to
\[
x^2 + 2y^2 - 395z^2 + 100yz
\]
Now make the change of variables:

\[ x = x', \quad y = y' - 25z \quad \text{and} \quad z = z'. \]

This reduces our quadratic to

\[ x^2 + 2y^2 - 1645z^2. \]

8.1.9. We use the same method as in class. Look at lines through \((-\sqrt{r}, 0)\) of slope \(m\),

\[ y = m(x + \sqrt{r}). \]

Plugging this into the equation for the circle we get

\[ x^2 + m^2(x + \sqrt{r})^2 = r. \]

Thus

\[ (1 + m^2)x^2 + m\sqrt{r}x + m^2r = r. \]

It follows that

\[ x^2 + \frac{m}{1 + m^2}x + \frac{m^2 - 1}{1 + m^2} = 0. \]

The root not corresponding to \(x = -\sqrt{r}\) is then

\[ x = \sqrt{r}\frac{1 - m^2}{1 + m^2} \quad \text{so that} \quad y = \sqrt{r}\frac{2m}{1 + m^2}. \]

Suppose that we could find a parametrisation by rational functions with rational parameters

\[(x, y) = \left(\frac{a(t)}{b(t)}, \frac{c(t)}{d(t)}\right)\]

for the circle \(x^2 + y^2 = 3\). Here \(a(t), b(t), c(t)\) and \(d(t)\) are polynomials in \(t\). \(b(t)\) and \(d(t)\) have only finitely many zeroes. Pick a rational number \(t = t_0\) not one of these zeroes. Then we get a rational point \((x_0, y_0)\) on the circle \(x^2 + y^2 = 3\).

Clearing denominators in the usual way we would get an integral solution of \(x^2 + y^2 - 3z^2 = 0\). By Legendre this would imply \(-1\) is a residue of 3. But \(-1 \equiv 2 \mod 3\) and this is not a residue of 3.