Amin Zolfagharian - 610300118

Problem 1.

(i)

$$\left(\frac{1001}{20003}\right) = \left(\frac{7}{20003}\right)\left(\frac{11}{20003}\right)\left(\frac{13}{20003}\right) = -\left(\frac{20003}{7}\right) \times -\left(\frac{20003}{11}\right) \times \left(\frac{20003}{13}\right)$$
$$= \left(\frac{4}{7}\right)\left(\frac{5}{11}\right)\left(\frac{9}{13}\right) = \left(\frac{5}{11}\right)\left(\frac{9}{13}\right) = \left(\frac{11}{5}\right)\left(\frac{13}{9}\right) = \left(\frac{1}{5}\right)\left(\frac{4}{9}\right) = 1$$

(ii) Since Jacobi's sign is only defined for odd $n = 5k + r$ then we have:

$$\left(\frac{5}{n}\right) = \left(\frac{n}{5}\right) = \left(\frac{r}{5}\right)$$

But since we know that only 1 and -1 are quadratic residue modulo 5, then $r = 1, 4$. Thus this only happens for odd ns with the form $5k \pm 1$.

Problem 2.

Suppose m is of the form p^α for some odd prime p. Then if $x \overset{p^\alpha}{\equiv} -x$ we would have $x^2 \overset{p}{\equiv} a$ and therefore $p \mid 2x$ and since p is odd $p \mid x$. Therefore if there exists some $x^2 \overset{p}{\equiv} a$ then $(-x)^2 \overset{p}{\equiv} a$ is another answer for this equation. Therefore if a is quadratic residue modulo p then there are two answers for the equation and with Hensel's lemma we can lift these answers modulo p^α and

$$\prod_{p|p^\alpha}(1 + \left(\frac{a}{p}\right)) = 1 + 1 = 2$$

If a is not quadratic residue modulo p, therefore the equation has 0 answers and we have:

$$\prod_{p|p^\alpha}(1 + \left(\frac{a}{p}\right)) = 1 - 1 = 0$$

Now suppose $x^2 \overset{m}{\equiv} a$ for some odd m and a such that $(a, m) = 1$. Then we have:

$$m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$$
$$\forall i \leq k : x^2 \overset{p_i^{\alpha_i}}{\equiv} a$$

Therefore if a is quadratic residue modulo all p_is then this equation has an anaswer, otherwise there is no answer. Suppose a is not quadratic residue modulo p_i:

$$\prod_{p|m}(1 + \left(\frac{a}{p}\right)) = (1 + \left(\frac{a}{p_i}\right))Y = 0$$

Now if a is quadratic residue modulo all p_is, then each equation $x^2 \overset{p_i^{\alpha_i}}{\equiv} a$ has two answers, with CRT we can deduce that there are 2^k answers for this equation:

$$\prod_{p|m}(1+\left(\frac{a}{p}\right)) = (1+\left(\frac{a}{p_1}\right))(1+\left(\frac{a}{p_2}\right))\dots(1+\left(\frac{a}{p_k}\right)) = (1+1)\dots(1+1) = 2^k$$

Which completes the proof.

Problem 3.

We can rewrite the equation:

$$\begin{gathered} 122 = x^2 + 3xy - 2y^2 \\ \implies 4 \times 122 = 4(x^2 + 3xy - 2y^2) = (2x+3y)^2 - 17y^2 \\ \implies 4 \times 122 \overset{17}{\equiv} (2x+3y)^2 = z^2 \end{gathered}$$

Therefore if this equation has any answers, 4×122 must be quadratic residue modulo 17:

$$\left(\frac{4 \times 122}{17}\right) = \left(\frac{122}{17}\right) = \left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1$$

Therefore 4×122 is not quadratic residue, which means there is no z with above conditions, therefore there is no such x and y.

Problem 4.

(i) Suppose $[a_0; a_1, a_2, \dots a_n]$ and $[b_0; b_1, \dots, b_m]$ represent the same rational number $\frac{x}{y}$. Let i be the first index where $b_i \neq a_i$ (Note that a_i or b_i can be 0). We can write:

$$\begin{gathered} b_i + \frac{1}{b_{i+1} + \frac{1}{\dots}} = a_i + \frac{1}{a_{i+1} + \frac{1}{\dots}} \\ b' = \frac{1}{b_{i+1} + \frac{1}{\dots}} \leq 1 \\ a' = \frac{1}{a_{i+1} + \frac{1}{\dots}} \leq 1 \\ \implies b_i + b' = a_i + a' \\ \implies 0 \neq b_i - a_i = a' - b' \leq 1 \\ \implies a' - b' = 1 \implies a' = 1, b' = 0 \\ \implies a_{i+1} = 1, a_{i+2} = 0, b_{i+1} = 0 \end{gathered}$$

Therefore we have:

$$\begin{gathered} [b_0; b_1, \dots, b_i, b_{i+1}] = [a_0; a_1, \dots, a_{i-1}, a_i + 1] \\ [a_0; a_1, \dots, a_{i+1}, a_{i+2}] = [a_0, a_1, \dots, a_{i-1}, a_i, 1] \end{gathered}$$

This shows that each two finite continued fractions with the same value, they have lengths n and $n+1$ Now if 3 finite continued fractions have the same value, with lengths r, s and t, WLOG:

$$t = s + 1$$
$$t = r + 1 \text{ or } r - 1$$

If $t = r + 1$:

$$r + 1 = s + 1 \implies r = s$$

Which is a contradiction. If $t = r - 1$:

$$r - 1 = s + 1 \implies r = s + 2$$

Which is a also a contradiction, therefore we can't have 3 finite continued fractions with the same values.

Problem 5.

(i) Let $n = p_1 p_2 \dots p_t$, then:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_t}\right)$$

Since for any prime p there exists some number that is not quadratic residue modulo p, suppose a_1 is such number for p_1. By CRT we know there exists some a such that:

$$a \overset{p_1}{\equiv} a_1$$
$$\forall_{1<i\leq t} : a \overset{p_i}{\equiv} 1$$

For this a we have that $\left(\frac{a}{p_1}\right) = -1$ and for $1 < i \leq t$ we have $\left(\frac{a}{p_i}\right) = 1$, therefore:

$$\left(\frac{a}{n}\right) = -1$$

Problem 6.

Let $Ord_{2p+1}(2) = r$. We have $r \mid 2p$.

$$\left(\frac{2}{2p+1}\right) = \left(\frac{2}{8k+3}\right) = (-1)^{((8k+3)^2-1)/8} = -1$$

This shows that 2 is not quadratic residue modulo $2p+1$. Let g be a primitive root modulo $2p+1$, There exists some i such that $g^i \overset{2p+1}{\equiv} 2$, and since 2 is not quadratic residue, therefore i is odd:

$$Ord(2) = Ord(g^i) = \frac{Ord(g)}{(i, Ord(g))} = \frac{2p}{(i, 2p)} = \frac{2p}{(i, p)}$$

Now if $(i,p) = 1$ then 2 is a primitive root and we are done. If $(i,p) = p$ then $Ord(2) = 2$:

$$2^2 \overset{2p+1}{\equiv} 1 \implies 2p+1 \mid 4-1=3 \implies 2p+1 \leq 3 \implies p \leq 1$$

Which is a contradiction sicne p is prime. Thus has order $2p$ and is a primitive root of $2p+1$.

Problem 7.

First we show that 3 is not quadratic residue modulo $p > 3$. Note that since $3 \nmid p$ therefore $2^n + 1 \overset{3}{\equiv} (-1)^n + 1 \neq 0$. this shows that n is even:

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{2^{2k}+1}{3}\right) = \left(\frac{(-1)^{2k}+1}{3}\right) = \left(\frac{2}{3}\right) = -1$$

Now consider a primitive root g modulo p. There exists some i such that $g^i \overset{p}{\equiv} 3$. Since 3 is not quadratic residue, tehrefore i is odd. Now we can calculate the order of 3:

$$Ord(3) = Ord(g^i) = \frac{Ord(g)}{(i, Ord(g))} = \frac{2^n}{(i, 2^n)} = \frac{2^n}{1} = 2^n$$

This proves that 3 is a primitive root modulo p.