MATH342 Feedback and Solutions 10

1. Using Gauss' reciprocity and since $991 \equiv 1 \mod 3$,

$$\left(\frac{3}{991}\right) = (-1)^{445\times 1}\left(\frac{991}{3}\right) = -\left(\frac{991}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

$$\left(\frac{12}{991}\right) = \left(\frac{3}{991}\right)\cdot\left(\frac{4}{991}\right) = (-1)\left(\frac{4}{991}\right) = (-1)\cdot 1 = -1$$

since 4 is a square integer.

By Gauss' quadratic reciprocity:

$$\left(\frac{5}{991}\right) = (-1)^{475\times 2}\left(\frac{991}{5}\right) = \left(\frac{991}{5}\right) = \left(\frac{1}{5}\right) = 1\,.$$

$$\left(\frac{-10}{991}\right) = \left(\frac{-1}{991}\right)\times\left(\frac{2}{991}\right)\times\left(\frac{5}{991}\right) = (-1)\times 1\times 1 = -1$$

because $991 \equiv -1 \mod 8 \equiv -1 \mod 4$ and for any odd prime p

$$\left(\frac{-1}{p}\right) = 1 \Leftrightarrow p \equiv 1 \mod 4$$

$$\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \mod 8.$$

$$\left(\frac{891}{991}\right) = \left(\frac{-100}{991}\right) = \left(\frac{-10}{991}\right)\times\left(\frac{2}{991}\right)\times\left(\frac{5}{991}\right) = (-1)\times 1\times 1 = -1$$

It is important to remember (as most did) that the formula

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right)$$

only works if both p and q are prime (and both odd). The other main tool that we need is multiplicativity of the Legendre symbol in the numerator, that is

$$\left(\frac{q_1q_2}{p}\right) = \left(\frac{q_1}{p}\right)\times\left(\frac{q_2}{p}\right).$$

There are many ways of doing this. The solution above used a factorisation of -100 – and possibly not the best one, because one could also use $-100 = -1\times 10^2$ since $\left(\frac{10}{991}\right)^2 = 1$ and $\left(\frac{-1}{991}\right) = -1$ because $991 \cong 3 \mod 4$. Most solutions I saw used a factorisation $891 = 3^4\times 11$ and used $\left(\frac{3}{991}\right)^4 = 1$ and worked out $\left(\frac{11}{991}\right)$ using quadratic reciprocity.

2.

a)

$$\left(\frac{31}{97}\right) = (-1)^{48\times 15}\left(\frac{97}{31}\right) = \left(\frac{97}{31}\right) = \left(\frac{4}{31}\right) = 1$$

as $4 = 2^2$ is a square integer. It can be checked directly that $31 \equiv 15^2 \bmod 97$ (but this was not part of the question).

b)

$$\left(\frac{53}{271}\right) = (-1)^{26\times 135}\left(\frac{271}{53}\right) = \left(\frac{271}{53}\right) = \left(\frac{6}{53}\right) = \left(\frac{2}{53}\right)\left(\frac{3}{53}\right) = (-1)\times(-1)^{1\times 26}\left(\frac{53}{3}\right)$$
$$= -\left(\frac{2}{3}\right) = (-1)^2 = 1$$

We used $\left(\frac{2}{53}\right) = -1$ because $53 = 5 \bmod 8$, that is, $53 \not\equiv \pm 1 \bmod 8$. It can be checked directly that $53 \equiv 18^2 \mod 271$ (but this was not part of the question).

c) We have $351 = 3^2 \times 39 = 3^3 \times 13$. So

$$\left(\frac{351}{787}\right) = \left(\frac{3}{787}\right)^3 \left(\frac{13}{787}\right) = (-1)^{3\times 1\times 393}\left(\frac{787}{3}\right)^3 \times (-1)^{6\times 393}\left(\frac{787}{13}\right)$$

$$= -\left(\frac{1}{3}\right)^3 \times \left(\frac{7}{13}\right) = -(-1)^{3\times 6}\left(\frac{13}{7}\right) = -\left(\frac{6}{7}\right) = -\left(\frac{2}{7}\right) \times \left(\frac{3}{7}\right) = -1 \times 1 \times (-1) = 1$$

since $2 = 3^2 \bmod 7$ and 3 is not a square $\bmod 7$. Of course one can continue to use the quadratic recipocity rules to verify this, using

$$\left(\frac{3}{7}\right) = (-1)^{1\times 3}\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

3. By quadratic reciprocity for any odd prime p which is coprime to 5

$$\left(\frac{5}{p}\right) = (-1)^{(p-1)/2\times 2}\left(\frac{p}{5}\right) = \left(\frac{p}{5}\right) = 1 \Leftrightarrow p \equiv \pm 1 \mod 5$$

This is because $p \equiv \pm 1$ or $\pm 2 \mod 5$ and

$$\left(\frac{1}{5}\right) = \left(\frac{-1}{5}\right) = 1, \quad \left(\frac{2}{5}\right) = \left(\frac{-2}{5}\right) = -1,$$

because the quadratic residues $\mod 5$ are 1 and $4 \equiv -1$, and the other (non-quadratic) residues $\mod 5$ are 2 and $3 \equiv -2 \mod 5$.

4. By quadratic reciprocity,

$$\left(\frac{7}{p}\right) = (-1)^{3\times(p-1)/2}\left(\frac{p}{7}\right)$$

So

$$\left(\frac{7}{p}\right) = \begin{cases} \left(\frac{p}{7}\right) & \text{if } p \equiv 1 \bmod 4, \\ -\left(\frac{p}{7}\right) & \text{if } p \equiv -1 \bmod 4. \end{cases}$$

So for any odd prime p which is coprime to 7,

$$\left(\frac{7}{p}\right) = 1 \Leftrightarrow \left(p \equiv 1 \bmod 4 \wedge \left(\frac{p}{7}\right) = 1\right) \vee \left(p \equiv -1 \bmod 4 \wedge \left(\frac{p}{7}\right) = -1\right)$$

Now the quadratic residues $\mod 7$ are 1, 2 and $4 \equiv -3$, while the non-quadratic residues are $-1 \equiv 6$, $-2 \equiv 5$ and 3. So

$$\left(\frac{7}{p}\right) = 1 \Leftrightarrow (p \equiv 1 \mod 4 \wedge p \equiv 1,\ 2 \text{ or } -3 \bmod 7)$$
$$\vee (p \equiv -1 \mod 4 \wedge p \equiv -1,\ -2 \text{ or } 3 \bmod 7.)$$

By the Chinese Remainder Theorem, there is a unique solution $\mod 28$ to $p \equiv a \bmod 4 \wedge p \equiv b$. First we take $p \equiv 1 \bmod 4$ and $p \equiv 1$, 2 or $-3 \mod 7$. The solutions are $p \equiv 1$, 9 or $-3 \mod 28$ respectively. (It is possible to use the formula in the Chinese Remainder Theorem but the solutions are quite easy to spot by inspection, because 28 is not a big number.) Now we take $p \equiv -1 \bmod 4$ and $p \equiv -1$, -2 or $3 \bmod 7$. the solutions are simply the negatives of the previous ones, that is, $p \equiv -1$, -9 or $3 \mod 28$. So we obtain

$$\left(\frac{7}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1,\ \pm 3 \text{ or } \pm 9 \mod 28.$$

Most solutions that I saw did not use the Chinese Remainder Theorem. I think it is probably the quickest way, but any correct solution will do.

5. Suppose that there are only finitely many primes which are $\pm 1 \bmod 5$, and let these primes be q_i, for $1 \le i \le n$. Then write

$$N = -\prod_{i=1}^{n} q_i.$$

Let p be any prime which divides $N^2 - 5$. Then $5 \equiv N^2 \bmod p$, and hence $p \equiv \pm 1 \mod 5$. So then there is i such that $q_i = p$. But then $q_i \mid N$ and $q_i \mid N^2 - 5$ and hence $q_i \mid 5$ and $q_i = 5$. But this is impossible because $q_i \equiv 1 \pm 5$