## Exercise Sheet 4

*This sheet is due in the lecture on Tuesday 28th October, and will be discussed in the exercise class on Friday 31st October.*

**Exercise 4.1.** *Computation of the Legendre symbol.*

(1) Evaluate the Legendre symbol $(\frac{474}{733})$ without using the Jacobi symbol.

(2) Evaluate the Legendre symbol $(\frac{-113}{997})$.

(3) Evaluate the Legendre symbol $(\frac{514}{1093})$.

**Exercise 4.2.** *Primes for which a given number is a quadratic residue.*

(1) Find all odd primes for which 5 is a quadratic residue.

(2) Find all odd primes for which $-3$ is a quadratic residue.

**Exercise 4.3.** *Properties of Jacobi symbols.*

(1) Let $b$ be a positive odd integer and $\mathrm{hcf}(a, b) = 1$. If $a$ is a quadratic residue modulo $b$, show that the Jacobi symbol $(\frac{a}{b}) = 1$.

(2) Use Definition 4.9 and Proposition 4.4 (1) to give a proof of Proposition 4.12 (1); i.e. for any positive odd integer $b$, show that

$$\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right).$$

**Exercise 4.4.** *Quadratic residues and the Legendre symbol.*

(1) Find all quadratic residues and non-residues modulo 13.

(2) Let $p$ be an odd prime and $a$ any integer. Show that the number of solutions to the congruence $x^2 \equiv a \pmod{p}$ is given by $1 + (\frac{a}{p})$.

(3) Use part (2) to show that $\displaystyle\sum_{a=0}^{p-1}\left(\frac{a}{p}\right) = 0$. (Hint: each congruence class modulo $p$ is a solution to $x^2 \equiv a \pmod{p}$ for a unique $a \in \{0, 1, \cdots, p-1\}$.)

(4) Use part (3) to show that, in the set $\{1, 2, \cdots, p-1\}$, there are as many quadratic residues as non-residues modulo $p$. Is your answer to part (1) consistent with this result?