Exercise Sheet 5

This sheet is due in the lecture on Tuesday 4th November, and will be discussed in the exercise class on Friday 7th November.

Exercise 5.1. *Evaluating Legendre symbols by Gauss' lemma.*

(1) Use Gauss' lemma to determine $(\frac{5}{7})$, $(\frac{3}{11})$, $(\frac{6}{13})$.

(2) For any odd prime p, use Gauss' lemma to determine $(\frac{-1}{p})$ and $(\frac{2}{p})$.

(3) For any odd prime p, use Lemma 5.2 to determine $(\frac{-1}{p})$.

Exercise 5.2. *Special cases of Dirichlet's theorem.*

(1) Show that there are infinitely many primes which are congruent to -1 modulo 6. (Hint: follow the proof of Proposition 5.4 (1) to design the formula for N.)

(2) Show that there are infinitely many primes which are congruent to -1 modulo 8. (Hint: follow the proof of Proposition 5.4 (2) to design the formula for N. You need Proposition 4.5 (2) to analyse prime factors of N.)

Exercise 5.3. *Quadratic residues for powers of odd primes.*

Let p be an odd prime, $e > 0$ and $p \nmid a$.

(1) Assume a is a quadratic residue modulo p^{e+1}. Show that a is a quadratic residue modulo p^e.

(2) Assume a is a quadratic residue modulo p^e. Show that a is a quadratic residue modulo p^{e+1}. (Hint: if $x^2 \equiv a \pmod{p^e}$, then we can write $x^2 = a + bp^e$. Set $y = x + cp^e$ and show that we can find c such that $y^2 \equiv a \pmod{p^{e+1}}$.)

(3) Conclude by induction that a is a quadratic residue modulo p^e iff $(\frac{a}{p}) = 1$.

Exercise 5.4. *Fermat's two square problem.*

Let p be an odd prime. Recall the ring of Gaussian integers $\mathbb{Z}[i]$ from Exercise 1.4.

(1) Suppose $p \equiv 1 \pmod 4$. Show that there exist integers s and t such that $pt = s^2 + 1$. Conclude that p is not a prime in $\mathbb{Z}[i]$. (Hint: -1 is a quadratic residue modulo p; remember that $\mathbb{Z}[i]$ has unique factorisation as in Exercise 1.4 (3).)

(2) Suppose $p \equiv 1 \pmod 4$. Use part (1) to show that p is the sum of two squares; i.e. $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$. (Hint: part (1) implies $p = \alpha\beta$ for some non-units α and β in $\mathbb{Z}[i]$. Then use Exercise 1.4 (1) and (4).)

(3) Suppose $p \equiv 3 \pmod 4$. Show that p cannot be written as the sum of two squares.