

## 4400/6400 PROBLEM SET 5

PETE L. CLARK

A sufficient number of problems: 4 for 4400 students, 5 for 6400 students.

5.1) Evaluate these Legendre symbols (the denominators are all prime numbers):

$$\left(\frac{85}{101}\right), \left(\frac{29}{241}\right), \left(\frac{101}{1987}\right), \left(\frac{31706}{43789}\right).$$

5.2) Make up another six Legendre symbol problems, with numbers ranging from 3 to 5 digits (for this you will need to do something to find some primes in this range, but for instance you can find lists of primes on the internet), and solve them. Try to find the approximate range in which it becomes difficult to do the computations directly in terms of Legendre symbols – i.e., by factoring at every stage – and hence it becomes preferable to use the Jacobi symbol.

5.3) For each of the following integers  $N$ , find all primes  $p$  such that  $N$  is a square modulo  $p$ :

- a) 31.
- b) 2007.
- c) The year of your birth.

5.4) Prove that the quadratic reciprocity law is equivalent to: for distinct odd primes  $p, q$ ,

$$\left(\frac{p}{q}\right) = \left(\frac{(-1)^{\frac{q-1}{2}} q}{p}\right).$$

5.5) Prove Lemma 6 of [Quadratic Reciprocity II: The Proofs].

5.6)\* Prove that the Quadratic Reciprocity Law is equivalent to Corollary 12 in [Quadratic Reciprocity I]. (This was Euler’s formulation of the QR Law.)

5.7)\* Show that the Jacobi symbol obeys the laws of quadratic reciprocity. (Suggestion: look this one up. Do give references to any sources you consult.)

5.8)\*\* In [Quadratic Reciprocity II], we computed the square of the Gauss sum:  $\tau^2 = p^* = (-1)^{p-1} 2p$ . Of course this means that  $\tau = \pm\sqrt{p^*}$ . Show that in fact  $\tau = \sqrt{p^*}$ .

Remark: This conjecture was made by Gauss in 1801. From then on “seldom a week had passed” in which he did not try to prove his conjecture. He succeeded in 1805, writing “Wie der Blitz einschlägt, hat sich das Räthsel gelöst.” All of this is to convince you that 5.7) is **very difficult**. However, for one bonus point, translate this quotation into English.

- 5.9G) [This problem requires a knowledge of basic Galois theory] Let  $p > 2$  be a prime number and define  $\Phi_p(t) = \frac{t^p-1}{t-1} = 1 + \dots + t^{p-1}$ . This is the minimal polynomial of any primitive  $p$ th root of unity  $\zeta_p$ .
- Show that  $\Phi_p(t)$  is irreducible over  $\mathbb{Q}$ . (Hint: do something sneaky and then apply the Eisenstein criterion.)
  - Let  $K_p = \mathbb{Q}(\zeta_p)$ . Show that  $K_p/\mathbb{Q}$  is a Galois extension of degree  $p-1$  whose Galois group is  $(\mathbb{Z}/p\mathbb{Z})^\times$ . Although we haven't proved it yet, this group is cyclic, and you may use this fact.
  - Show that  $K_p$  has a unique quadratic subfield  $\mathbb{Q}(\sqrt{d})$ . What is  $d$ ?