

4400/6400 PROBLEM SET 10

Recommendation: Do as many as you can!

10.1) Evaluate the following Legendre symbols:

$$\left(\frac{85}{101}\right), \left(\frac{29}{541}\right), \left(\frac{101}{1987}\right), \left(\frac{31706}{43789}\right).$$

10.2) Let p and q be distinct odd primes. What is the conditional probability that p is a square modulo q , given that q is a square modulo p ?

10.3) 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.

Remark: In all cases your answer should be a set of congruence classes.

10.4) Prove Corollary 5 from Handout 15 (Quadratic Reciprocity I).

10.5) Prove that $\mathbb{Z}[\sqrt{d}]$ is a PID for the following values of d : 2, -2, 3.

(Suggestion: As in the case of $d = -1$, it is sufficient to show that for any element $\alpha \in \mathbb{Q}(\sqrt{d})$, there exists an element $z \in \mathbb{Z}[\sqrt{d}]$ such that $|N(\alpha - z)| < 1$. Explain why, and then show this.)

10.6) Find all primes of the form $x^2 - dy^2$ for $d = 2, -2$.

10.7)** Show that the Jacobi symbol obeys the laws of quadratic reciprocity (i.e., prove Theorem 8 in Handout 15).

10.8) Show that Quadratic Reciprocity is equivalent to the identity

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right).$$

10.9) Prove Lemma 6 in Handout 16 (Quadratic Reciprocity II).

10.10) [Notation as in §4 of Handout 16] By evaluating $\sum_{t=0}^{p-1} \left(1 + \left(\frac{t}{p}\right)\right) \zeta^t$ in two different ways, prove that

$$\tau = \sum_{t=0}^{p-1} \zeta^{t^2}.$$

10.11)*** We computed exactly the square of the Gauss sum: $\tau^2 = p^*$. This means that when $p \equiv 1 \pmod{4}$, τ itself is either equal to \sqrt{p} or $-\sqrt{p}$, and when $p \equiv -1 \pmod{4}$, τ is either equal to \sqrt{pi} or $-\sqrt{pi}$. Show that, in all cases, the plus

sign holds.

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 on August 30, 1805, writing “Wie der Blitz einschlägt, hat sich das Räthsel gelöst.” One bonus point for translating this quotation.

10.12G) Let R be an integral domain with quotient field F . R is said to be **integrally closed** if every α in F which is *integral* over R - i.e., satisfies a monic polynomial with R -coefficients - is in fact an element of R .

a) Show that a PID is integrally closed. (Hint: the proof is essentially that of Theorem 5 in Handout 2, which is in fact a special case.)

b) Show that if $d \equiv 1 \pmod{4}$ is a nonsquare integer, then the element $\theta_d = \frac{1+\sqrt{d}}{2}$ of $\mathbb{Q}(\sqrt{d})$ is integral over \mathbb{Z} . Deduce that $\mathbb{Z}[\sqrt{d}]$ is not a PID.

c) For any integral domain R , let R_c be the set of all elements of the quotient field F which are integral over R . By Handout 3, R_c is a ring which contains R . Show that R_c is integrally closed. (You may wish to consult Algebra Handout 3.)

d)* Show that when $d \equiv 1 \pmod{4}$, the integral closure of $\mathbb{Z}[\sqrt{d}]$ is $\mathbb{Z}[\theta_d]$. In all other cases, the ring $\mathbb{Z}[\sqrt{d}]$ is integrally closed.

Remark: By part a), when $d \equiv 1 \pmod{4}$, it is the ring $\mathbb{Z}[\theta_d]$ which has “a fighting chance” at being a PID; sometimes it is and sometimes it isn’t. In every case it satisfies a weaker condition - it is a **Dedekind domain** - which allow us to uniquely factor *ideals* into prime *ideals*, a fact which goes a long way towards repairing the defects of unique factorization. At this point we have arrived on the doorstep of algebraic number theory, so we stop: you can knock if you wish, or run away!