

## 4400/6400 PROBLEM SET 4

A sufficient number of problems: 5 for 4400 students, 8 for 6400 students.

4.1) Determine exactly which integers  $n$ ,  $1 \leq n \leq 100$ , are sums of two squares.

4.2) a) The first “run” of two consecutive non-negative integers which are not sums of two squares is 6, 7. Determine the first run of at least three consecutive integers which are not sums of two squares; of at least four; of at least five.

b) What is the largest  $k$  such that there exist integers  $n, n+1, \dots, n+k$  which are all sums of two squares.

4.3)\* Prove or disprove: For any positive integer  $k$ , there exists a positive integer  $n$  such that none of the  $k+1$  integers  $n, n+1, \dots, n+k$  are sums of two squares.

4.4)\* Which positive integers  $z$  can be the length of the hypotenuse of a right triangle with integer legs? (An honest triangle: each of the legs must have positive length!)

Let  $p$  be an odd prime. An integer  $n$  is said to be a **quadratic residue mod  $p$**  if  $p \nmid n$  and  $n \equiv x^2 \pmod{p}$  for some  $x \in \mathbb{Z}$ . The same terminology applies to an element  $n \in \mathbb{Z}/p\mathbb{Z}$ .

4.5) Show that precisely half of the elements of  $(\mathbb{Z}/p\mathbb{Z})^\times$  are quadratic residues. (Hint: for  $x \in \mathbb{Z}/p\mathbb{Z}$ ,  $x^2 = y^2 \iff x = \pm y$ .)

4.6) For each prime  $p$ ,  $3 \leq p \leq 103$ , compute all quadratic residues modulo  $p$ .<sup>1</sup>

4.7)a) For which primes  $p$  in the above range is 2 a quadratic residue modulo  $p$ ? Do you see a pattern here similar to  $-1$  is a square mod  $p$  iff  $p \equiv 1 \pmod{4}$ ? (Hint: look modulo 8.)

b) Same as part a) but with  $-2$  instead of 2.

c) Same as part b) but with  $-3$  instead of  $-2$ . (Hint: look modulo 3.)

d) Same as part c) but with 3 instead of  $-3$ . (Hint: look modulo something.)

e) Same as part d) but with 5 instead of 3. (Hint: look modulo something.)

For  $a \in \mathbb{Z}$  and  $p$  an odd prime, the **Legendre symbol**  $\left(\frac{a}{p}\right)$  is defined to be 0 if  $p \mid a$ , 1 if  $\gcd(a, p) = 1$  and  $a$  is a quadratic residue mod  $p$  and  $-1$  if  $\gcd(a, p) = 1$  and  $a$  is a quadratic nonresidue mod  $p$ .

---

<sup>1</sup>Suggestion: a handheld calculator and/or a short computer program will save you lots of time.

4.8) Evaluate the following Legendre symbols using your solution to 4.6):

$$\left(\frac{5}{29}\right), \left(\frac{29}{5}\right), \left(\frac{61}{89}\right), \left(\frac{89}{61}\right), \left(\frac{59}{103}\right), \left(\frac{103}{59}\right).$$

Let  $R$  be an integral domain with fraction field  $F$ .  $R$  is said to be **integrally closed** if every element  $x \in F$  which satisfies a monic polynomial with  $R$ -coefficients is already an element of  $R$ . Note that Theorem 5 on page 4 of the handout on irrational numbers says precisely that  $\mathbb{Z}$  is integrally closed.

4.9) Show that any unique factorization domain is integrally closed. (Suggestion: the argument for  $R = \mathbb{Z}$  can be adapted with little change to this general case.)

4.10) Suppose  $0, 1 \neq D$  is a squarefree integer with  $D \equiv 1 \pmod{4}$ . Show that the element  $\tau_D := \frac{1+\sqrt{D}}{2}$  is an element of  $\mathbb{Q}[\sqrt{D}]$  which is integral over  $\mathbb{Z}[\sqrt{D}]$  but not an element of  $\mathbb{Z}[\sqrt{D}]$ . Conclude that  $\mathbb{Z}[\sqrt{D}]$  is not a UFD. (Suggestion: just compute the unique monic quadratic polynomial  $P(t) \in \mathbb{Q}[t]$  satisfied by  $\tau_D$  and observe that it has  $\mathbb{Z}$ -coefficients.)

4.11) Let  $D$  be squarefree, different from  $0, 1$ . Put  $F = \mathbb{Q}(\sqrt{D})$ . Furthermore, if  $D \equiv 1 \pmod{4}$ , put  $\mathbb{Z}_F = \mathbb{Z}[\tau_D] = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ , whereas if  $D \equiv 2, 3 \pmod{4}$  (since  $D$  is squarefree,  $D \equiv 0 \pmod{4}$  is impossible) put  $\mathbb{Z}_F = \mathbb{Z}[\sqrt{D}]$ .

a) Show that if  $D \equiv 1 \pmod{4}$ ,  $\mathbb{Z}_F = \{a + b\tau_D \mid a, b \in \mathbb{Z}\}$ .

b) Let  $\zeta_3 = e^{\frac{2\pi i}{3}}$ . Show that when  $D = -3$ ,  $\mathbb{Z}_F = \mathbb{Z}[\zeta_3]$ .

c) Let  $N : F \rightarrow \mathbb{Q}^{\geq 0}$  be the usual norm map,  $N(x + y\sqrt{D}) = |x^2 - Dy^2|$ . Show that  $N(\mathbb{Z}_F) \subset \mathbb{N}$ . (We know this already unless  $D \equiv 1 \pmod{4}$ .)

d)\*\* Show that  $\mathbb{Z}_F$  is integrally closed. (This is not really so difficult, but it requires a few facts about integral elements and extensions that you probably won't know unless you have taken a graduate algebra class.)

Comment: The upshot of this is that when  $D \equiv 1 \pmod{4}$ , the ring  $\mathbb{Z}[\sqrt{D}]$  is "too small" to have a fighting chance at being a UFD.

4.12) Let  $D < 0$  be a squarefree integer which is  $1 \pmod{4}$ , and  $F = \mathbb{Q}(\sqrt{D})$ .

a) Show that  $N$  is a Euclidean norm on  $\mathbb{Z}_F$  if and only if  $D = -3$  or  $D = -7$ , and conclude that  $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}] = \mathbb{Z}[\zeta_3]$  and  $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$  are UFDs.

b)\* What two results about representation of integers by binary quadratic forms (i.e., by a homogeneous quadratic polynomial in two variables, like  $x^2 - Dy^2$ ) does part a) imply?