MATH 4400/6400 – Homework #3

posted February 10, 2023; due Feb. 20, by midnight

It is impossible to be a mathematician without being a poet in soul.
– Sofia Kovalevskaya

Directions. Give complete solutions, providing full justifications when appropriate. Your assignment must be stapled if it goes on beyond one page.

MATH 4400 problems

1. Let p be an odd prime, and let a be an integer not divisible by p. Prove that $\sqrt{a}$ exists in $\mathbf{Z}_p$ if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$.

   Hint. Revisit the argument for when $\sqrt{-1}$ exists in $\mathbf{Z}_p$. That is, pair nonzero elements of $\mathbf{Z}_p$ that multiply to a.

2. Prove the Division Algorithm in $\mathbf{Z}[\sqrt{2}]$: For every $\alpha, \beta \in \mathbf{Z}[\sqrt{2}]$ with $\beta \neq 0$, there are $\gamma, \rho \in \mathbf{Z}[\sqrt{2}]$ with $\alpha = \beta\gamma + \rho$ and $|N\rho| < |N\beta|$. Then do the same for $\mathbf{Z}[\sqrt{3}]$.

3. Show that the equation $2 \cdot 2 = (\sqrt{5}+1)(\sqrt{5}-1)$ exhibits a genuine failure of unique factorization in $\mathbb{Z}[\sqrt{5}]$. That is, show that all the factors involved are prime in $\mathbf{Z}[\sqrt{5}]$ and that the two factorizations cannot be made to agree with each other by reordering and introduction of unit factors.

4. Let $d \in \mathbf{Z}^+$ with $d \neq \square$. Suppose $a, b \in \mathbf{Q}$, and let $\eta = a + b\sqrt{d}$.

   (a) Expand $(x-\eta)(x-\tilde{\eta})$ in the form $x^2 - Ax - B$, expressing A and B in terms of a and b.

   (b) Show that if x_n, y_n are defined by $x_n + y_n\sqrt{d} = (a+b\sqrt{d})^n$, then for every positive integer n,
   $$x_{n+1} = Ax_n + Bx_{n-1}, \quad y_{n+1} = Ay_n + By_{n-1},$$
   where A and B are the numbers you found in part (a).

5. Let $d \in \mathbf{Z}^+$ with $d \neq \square$.

   (a) Suppose (as we will show in class is always the case) that there is a unit > 1 in $\mathbf{Z}[\sqrt{d}]$. Prove there is a smallest unit > 1 in $\mathbf{Z}[\sqrt{d}]$.

   (b) Let ϵ be the smallest unit > 1 in $\mathbf{Z}[\sqrt{d}]$. Show that the collection of units > 1 consists precisely of the elements ϵ^n, for $n \in \mathbf{Z}^+$.

   (c) Show that the collection of all units in $\mathbf{Z}[\sqrt{d}]$ consists precisely of the elements $\pm\epsilon^n$, where now n ranges over all of $\mathbf{Z}$.

   (d) With ϵ as in (b), show that if $N(\epsilon) = 1$, then every unit in $\mathbf{Z}[\sqrt{d}]$ has norm 1.

6. Find the smallest unit > 1 <u>of norm 1</u> in $\mathbf{Z}[\sqrt{99}]$. Then do the same for $\mathbf{Z}[\sqrt{101}]$. Justify your answers.

7. A number is called *pentagonal* if it has the form $\frac{1}{2}n(3n-1)$ for some integer n.[1]

[1] If you are curious about the name, draw some dot diagrams of nested pentagons and count the number of dots at each stage. If you get stuck, check out `https://en.wikipedia.org/wiki/Pentagonal_number`.

Consider the problem of finding all square pentagonal numbers, i.e., all positive integers n and m with $m^2 = \frac{1}{2}n(3n-1)$. The smallest n which gives rise to a solution is $n = 1$, corresponding to $m = 1$. The second smallest n is $n = 81$, corresponding to $m = 99$. Find, with proof, the third smallest n.

MATH 6400 problems

G1. Consider the sequence of primes $2, 3, 7, 43, 139, \ldots$ defined by the following procedure. Let $q_1 = 2$, and assuming q_j has been defined for $1 \le j \le k$, let q_{k+1} be the largest prime divisor of $1 + q_1 \cdots q_k$. Prove that the prime 5 does not appear in the sequence $\{q_i\}_{i=1}^{\infty}$.

G2. Show that if $p \equiv 1 \pmod 4$ is prime, then $\mathbf{Z}_p$ contains a fourth root of -4.