Math 261 — Fall 2022
Number Theory
https://sites.aub.edu.lb/kmakdisi/
Problem set 8, due Friday, November 4 at the beginning of class

Exercise 8.1: a) By trial and error, or otherwise, write each of 23 and 29 as a sum of four squares.

b) Use your answer to part a) to write $667 = 23 \times 29$ as a sum of four squares.

Exercise 8.2: The Hurwitz integral quaternions, part I.

a) Define $R' = \{(a + bi + cj + dk)/2 \mid a, b, c, d \in \mathbf{Z}, \quad a \equiv b \equiv c \equiv d \pmod 2\} \subset \mathbf{H}$. Show that R' is a subring of $\mathbf{H}$, i.e., it is closed under addition, subtraction, and multiplication. Also show that the norm of an element of R' belongs to $\mathbf{Z}$, i.e., there is no denominator. (R' is called the ring of Hurwitz integral quaternions; the naive ring $R = \{a + bi + cj + dk \mid a, b, c, d \in \mathbf{Z}\}$ does not behave as nicely as R'.)

b) Show that the units of R' are precisely the elements of norm 1, and list them all. (There are 24 units. If you know some group theory, try to study the structure of the group of units — e.g., what orders do its elements have? What subgroups can you find?)

c) Show that for all $\alpha \in R'$, there exists a unit $u \in R'$ such that $\alpha u \in R$, the naive ring. Hint: if $\alpha \in R$, this is easy. If $\alpha \in R' - R$, show that there exists a unit $w \in R'$, with $w \notin R$, and a naive integer $\gamma \in R$, such that $\alpha = w + 2\gamma$. Then try $u = \overline{w}$.

d) Deduce that every norm of an element of R' is a sum of four squares. Explain why this means that the four square theorem will follow once we can show that for every prime $p \in \mathbf{Z}$ with $p \geq 3$, we can find an element $\alpha \in R'$ with $N(\alpha) = p$.

Exercise 8.3: The Hurwitz integral quaternions, part II. The ring R' is the same as in the previous exercise.

a) Show that given $h \in \mathbf{H}$, there exists $q \in R'$ such that $q - h = x + yi + zj + wk$ with $|x| \leq 1/4$, and $|y|, |z|, |w| \leq 1/2$. Show that this implies $N(q - h) < 1$. Hint: first subtract an integral multiple of $(1 + i + j + k)/2$, then integral multiples of i, j, k.

b) Show that given $\alpha, \beta \in R'$, with $\beta \neq 0$, then there exist $q, r \in R'$ with $\alpha = q\beta + r$ and $N(r) < N(\beta)$. (What would fail if we used R instead of R'?)

c) Show that given nonzero $\gamma, \delta \in R'$, the set (culture: the "left ideal") $I = \{s\gamma + t\delta \mid s, t \in R'\}$ contains a nonzero element β with smallest norm, and that in fact $I = \{q\beta \mid q \in R'\}$. This is analogous to what we know for $\mathbf{Z}$ and $\mathbf{Z}[i]$, except that one has to be careful with the order of multiplication.

d) Deduce from the above that $N(\beta)$ is a divisor (in $\mathbf{Z}$) of both $N(\gamma)$ and $N(\delta)$.

Exercise 8.4: The Hurwitz integral quaternions, part III. We continue with the same situation as in the previous two exercises.

a) Let $p \in \mathbf{Z}$ be a prime with $p \geq 3$. We have seen in class that there exists $\gamma \in R'$ (in fact, $\gamma \in R$) of the form $\gamma = 1 + c_1 i + c_2 j$, with $N(\gamma)$ divisible by p. Apply part (c) of the previous exercise to this γ and to $\delta = p$, to deduce the existence of $s_1, t_1 \in R'$ with $\gamma = s_1\beta$ and $p = t_1\beta$.

b) Show from the last equality in part (a) that the resulting β must have $N(\beta) \in \{1, p, p^2\}$. Our goal is now to show that the norm of β is neither 1 nor p^2.

c) Suppose in this part that $N(\beta) = p^2$. We will look for a contradiction. Show that if $N(\beta) = p^2$, then t_1 is a unit in R'. Use this fact to write γ in the form ϵp for some $\epsilon \in R'$. (Be careful about noncommutativity of R'! However, note conveniently that $p \in \mathbf{Z}$, so p does commute with all the elements of R'.) Show however that γ cannot be of the form ϵp with $\epsilon \in R'$. This is the desired contradiction. (Be careful of the "denominator" 2 in elements of R'.)

d) Suppose in this part that $N(\beta) = 1$. Then deduce a contradiction as follows: β is a unit, so (looking back at the definition of I and doing some algebra) show that it is possible to find $s', t' \in R'$ such that $1 = s'\gamma + t'p$. Now multiply by $\overline{\gamma}$ on the right to obtain $\overline{\gamma} = s'\gamma\overline{\gamma} + t'p\overline{\gamma}$. Show (being careful as usual about commutativity) that this implies the existence of $\epsilon' \in R'$ such that $\overline{\gamma} = \epsilon' p$. Deduce a contradiction similarly to part (c).

The above shows that $N(\beta) = p$, and then, from the previous exercises, that p is in fact a sum of four squares. This completes the proof of the four square theorem.