189-235A: Basic Algebra I
Assignment 8
Due: Wednesday, November 20

Section 9.1: 6, 22, 24, 30.

Section 9.2: 12, 13, 15, 32.

Section 9.3: 9, 11.

11. In class, we showed that the ring $\mathbf{Z}[i]$ is a Euclidean domain, and hence, a unique factorization domain. We concluded that every prime which is congruent to 1 mod 4 is a sum of two integer squares. In this question, we will prove the following theorem due to Lagrange:
Every positive integer can be written as a sum of 4 *integer squares.*
(For example, $2 = 1^2 + 1^2 + 0^2 + 0^2, 7 = 2^2 + 1^2 + 1^2 + 1^2$, etc.)

a) Verify Lagrange's theorem empirically, by expressing 23 and 107 as a sum of four squares.

b) Recall the ring of Hurwitz integer quaternions:

$$R = \{a + bi + cj + dk\},$$

where a, b, c, d are either all integers or halves of odd integers, and i, j, k satisfy

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

In a previous assignment, you showed that R is a (non-commutative!) ring with identity, and that the "quaternionic norm" $\delta : R \longrightarrow \{0, 1, 2, \ldots\}$ defined by:

$$\delta(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$$

satisfies $\delta(r_1 r_2) = \delta(r_1)\delta(r_2)$ for all $r_1, r_2 \in R$. Using the quaternionic norm, show that if a and b are two integers which are sums of 4 squares, then their product ab is also a sum of four squares. Hence it is enough to prove that every odd prime p is a sum of four squares, to prove Lagrange's theorem.

From now on, fix an odd prime p.

c) Show that there exists x and y in $\mathbf{Z}_p$ such that $x^2 + y^2 + 1 = 0$ in $\mathbf{Z}_p$. (Hint: note that the expressions of the form x^2 and $-1 - y^2$ each take on exactly $(p+1)/2$ distinct values in $\mathbf{Z}_p$.) Conclude that there exist integers a and b such that $a^2 + b^2 + 1 = pm$, with $m < p$.

d) A (non-commutative) integral domain R is said to be Euclidean if there is a function $\delta : R \longrightarrow \{0, 1, 2, \ldots\}$ such that

1. $\delta(a) \leq \delta(ab)$ for all $a, b \neq 0$.
2. For all $a, b \in R$, there exist q and r so that
$$a = qb + r, \quad \text{with } \delta(r) < \delta(b).$$

This is an extension of the notion of Euclidean domain, to the context of non-commutative rings. Show that the ring R of integral Hurwitz quaternions is Euclidean. (Hint: the proof uses an idea similar to the proof given in class that $\mathbf{Z}[i]$ is Euclidean.)

e) A *left ideal* in a non-commutative ring R is a subset $I \subset R$ which is closed under subtraction, and under left multiplication by elements of R: i.e., for all $r \in R$ and $x \in I$, rx belongs to I.

A left ideal is said to be principal if it is generated by a single element a: i.e., it consists of all multiples xa of a by some $x \in R$ (on the left).

If R is a Euclidean ring (in the sense of d), show that every left ideal in R is principal, by mimicking the proof given in class for commutative rings.

f) Show that p is the quaternionic norm of an element γ of R. (Hint: Let I be the left ideal of R generated by p and by $1 + ai + bj$, where a, b are as the integers obtained in part c. I.e., I is the set of elements of the form $xp + y(1 + ai + bj)$, where x and y belong to R. Let γ be a generator of I.)

g) Find all the units in R. Show that the element γ obtained in part f) has an associate whose coefficients are integers. Deduce the Lagrange four squares theorem.