Homework is due at the beginning of class. No late homework will be accepted. You may collaborate on the homework, but your final write-up must be done on your own and should reflect your own understanding of the problem. Write the names of any students you collaborated with on your assignment, and cite any help you get.

(All solutions must be supported with a proof, a counterexample, or a detailed computation, as appropriate. Simple Yes/No answers are unacceptable, even if the question is phrased in those terms. Solutions should be written in complete sentences and paragraphs.)

- Reading assignment: Chapters 10.1-10.5.
- Textbook exercises: Exercises 10.2, 10.3, 10.4, 10.5, 10.6, 10.7, 10.8, 10.9, 10.13, 10.14.

**Problem 1.**

1. Show that the congruence
   \[(x^2 - 2)(x^2 - 3)(x^2 - 6) \equiv 0 \pmod{p}\]
   has a solution for every prime \(p\).
2. What is the smallest prime \(p\) such that the above congruence has 6 distinct solutions?

**Problem 2.** Show that a positive integer \(n\) is a difference of two squares if and only if \(n\) is not congruent to 2 mod 4.

**Problem 3.** Do the following parts for each \(n \in \{45, 61, 65\}\).

1. Factor \(n\) into primes in the Gaussian integers \(\mathbb{Z}[i]\).
2. What are all the essentially distinct ways in which \(n\) can be written as a sum of two squares?

**Problem 4.** Show that if \(h, k\) are nonnegative integers then \(n := 4^h(8k + 7) \notin S_3\), i.e. \(n\) is not a sum of three squares.

**Problem 5.** The Hamiltonian integers are a ring \(\mathbb{H}\) consisting of numbers of the form
\[\{a + bi + cj + dk : a, b, c, d \in \mathbb{Z}\}\]
where the addition and multiplication are defined as in §10.5 of the text. The conjugate of a Hamiltonian integer \(q = a + bi + cj + dk \in \mathbb{H}\) is
\[\overline{q} := a - bi - cj - dk,\]
and the norm is defined by
\[N(q) = a^2 + b^2 + c^2 + d^2.\]
Thus, the set \(S_4\) of sums of four squares consists precisely of the norms of Hamiltonian integers.

1. Prove that \(\overline{q_1 q_2} = \overline{q_1} \cdot \overline{q_2}\) for any \(q_1, q_2 \in \mathbb{H}\).
2. Prove that \(N(q) = q \cdot \overline{q}\) for any \(q \in \mathbb{H}\).
3. Prove that \(N(q_1 \cdot q_2) = N(q_1) \cdot N(q_2)\) for any \(q_1, q_2 \in \mathbb{H}\).
4. Prove that \(S_4\) is closed under multiplication.