This week, we will continue to investigate the irreducible elements of \( \mathbb{Z}[i] \) and eventually characterize the integers which are sums of two squares. Last week, we showed that prime integers that are congruent to 3 mod 4 can not be written as sums of two squares and therefore are irreducible in \( \mathbb{Z}[i] \). Now we have to analyze the more difficult case of when \( p \equiv 1 \mod 4 \).

**Exercise 1.**
(a) Find an integer \( a \) such that \( a^4 \equiv 1 \mod 5 \) but \( a^k \not\equiv 1 \mod 5 \) for any \( 0 \leq k \leq 3 \).
(b) Find an integer \( a \) such that \( a^{16} \equiv 1 \mod 17 \) but \( a^k \not\equiv 1 \mod 17 \) for any \( 0 \leq k \leq 15 \).

It turns out that this is always possible. If \( p \) is any prime integer, then there exists some \( 0 \leq a \leq p-1 \) such that \( a^{p-1} \equiv 1 \mod p \) but \( a^k \not\equiv 1 \mod p \) for any \( 0 \leq k \leq p-2 \). Such an \( a \) is called a primitive root mod \( p \).

Another fact: we know that if \( x \) is an integer such that \( x^2 = 1 \), then \( x = 1 \) or \( -1 \). This is also true mod \( p \), i.e. if \( x \) is an integer such that \( x^2 \equiv 1 \mod p \), then \( x \equiv 1 \) or \( -1 \mod p \). Using these two facts, prove the following.

**Exercise 2.** If \( p \equiv 1 \mod 4 \), prove that there is some integer \( n \) such that \( p \) divides \( n^2 + 1 \) (Hint: this is equivalent to showing that some \( n \) satisfies \( n^2 \equiv -1 \mod p \). Let \( a \) be a primitive root mod \( p \) and proceed).

**Exercise 3.** (CHALLENGE). Prove that if \( p \) is a prime integer and \( a \neq 0 \mod p \), then \( a^{p-1} \equiv 1 \mod p \) (Hint: compare the two sets \( \{1, 2, 3, \ldots, p-1\} \) and \( \{a, 2a, 3a, \ldots, (p-1)a\} \)). This result is known as Fermat’s little theorem.

Now we are ready to analyze the case when \( p \equiv 1 \mod 4 \).

**Exercise 4.** The purpose of this exercise is to prove that if \( p \equiv 1 \mod 4 \), then \( p \) factors as \( p = (a + bi)(a - bi) \) where \( a + bi \) is an irreducible element of \( \mathbb{Z}[i] \).

(a) Factor \( n^2 + 1 \) in the Gaussian integers for any integer \( n \).
(b) Let \( p \) be a prime integer congruent to 1 mod 4 and let \( n \) be any integer. Show that \( p \) does not divide \( n + i \) via a contradiction argument. (Hint: What can we say about \( p \) and \( n - i \)?)
(c) By the claim above, \( p \) divides \( n^2 + 1 \) for some integer \( n \). Prove that \( p \) is not irreducible.
(d) Show that \( p \) factors as \( p = (a + bi)(a - bi) \) for integers \( a, b \). (Hint: Exercise 8(a))
(e) Show that \( a + bi \) and \( a - bi \) are irreducible Gaussian integers. (Hint: Use the norm)
We are now ready to write down all irreducible elements of \( \mathbb{Z}[i] \). As a recap of what we have done, there are three classes of irreducible elements in the Gaussian integers.

1. We know that \( 1 + i \) is irreducible via the norm.
2. We showed that prime integers congruent to 3 mod 4 are irreducible.
3. Finally, we showed that when \( p \) is a prime integer congruent to 1 mod 4, the distinct irreducible factors \( a + bi \) and \( a - bi \) of \( p = a^2 + b^2 \) are irreducible.

We want to show that these are all the irreducible elements of the Gaussian integers.

**Exercise 5.** Assume that \( \alpha = a + bi \) is an irreducible element of \( \mathbb{Z}[i] \).

(a) Prove that \( \alpha \) divides \( N(\alpha) \).

(b) Conclude that \( \alpha \) divides some prime integer. (Hint: \( N(\alpha) \) is an integer that might not be prime)

(c) Conclude that \( \alpha \) must be an element of our list.

Now, finally, we are able to prove a complete characterization of which positive integers are sums of two squares. The following theorem was first proved by Fermat.

**Theorem 1.** Let \( n \) be a positive integer. Write the prime factorization of \( n \) as

\[
    n = 2^k \cdot p_1^{\ell_1} \cdots p_k^{\ell_k} \cdot q_1^{f_1} \cdots q_d^{f_d}
\]

where \( p_1, \ldots, p_k \) are distinct primes congruent to 1 mod 4 and \( q_1, \ldots, q_d \) are distinct primes congruent to 3 mod 4. Then \( n \) is the sum of two squares if and only if all of the \( f_j \) are even.

**Exercise 6.** Prove the above theorem.

(a) Prove that \( n \) is the sum of two squares if and only if there is some Gaussian integer \( \gamma = A + Bi \) such that \( N(\gamma) = n \).

(b) Prove that if \( \alpha \) is irreducible in \( \mathbb{Z}[i] \), then \( N(\alpha) \) is equal to 2, a prime congruent to 1 mod 4, or the square of a prime congruent to 3 mod 4.

(c) Suppose \( n = N(\gamma) \) for some \( \gamma \in \mathbb{Z}[i] \). Show that each \( f_j \) must be even (Hint: factor \( \gamma = \alpha_1 \cdots \alpha_m \) as a product of irreducible Gaussian integers. Take the norm and use part (b)).

(d) Suppose that each \( f_j \) is even. Show that there exist irreducible Gaussian integers \( \alpha_1, \ldots, \alpha_m \) such that \( N(\alpha_1) \cdots N(\alpha_m) = n \) (Hint: Exercise 8(c)).

(e) Explain why parts (a)-(d) together complete the proof of the theorem.