Theorem 47.4. The function \( \nu(\alpha) = N(\alpha) \) for nonzero \( \alpha \in \mathbb{Z}[i] \) is a Euclidean norm in \( \mathbb{Z}[i] \) and so \( \mathbb{Z}[i] \) is a Euclidean domain.

**Proof.** For all \( \beta = b_1 + b_2 i \neq 0 \) in \( \mathbb{Z}[i] \) we have
\[
N(b_1 + b_2 i) = b_1^2 + b_2^2 = \mathbb{1}.
\]
Then for all \( \alpha, \beta \in \mathbb{Z}[i] \) where \( \alpha \neq 0 \neq \beta \) we have
\[
N(\alpha) \leq N(\alpha N(\beta)) \quad \text{since} \quad N(\beta) \geq 1
\]
\[
= N(\alpha \beta) \quad \text{By Lemma 47.2 (3)}
\]
so Condition 2 for a Euclidean norm in Definition 46.1 holds.
Theorem 47.4. (Continued)

**Theorem. 47.4.** The function \( \nu(\alpha) = N(\alpha) \) for nonzero \( \alpha \in \mathbb{Z}[i] \) is a Euclidean norm in \( \mathbb{Z}[i] \) and so \( \mathbb{Z}[i] \) is a Euclidean domain.

**Proof (Continued).** If \( \rho = 0 \) we are done. Otherwise, by construction of \( \sigma \) we have \( |r - q_1| \leq 1/2 \) and \( |s - q_2| \leq 1/2 \), so

\[
N(\alpha / \beta - \sigma) = N((r + si) - (q_1 + q_2 i)) = N((r - q_1) + (s - q_2)i) \leq \frac{1^2}{2} + \frac{1^2}{2} = \frac{1}{2}.
\]

Thus

\[
N(\rho) = N(\alpha - \beta \sigma) = N(\beta (\alpha / \beta - \sigma)) = N(\beta) N(\alpha / \beta - \sigma) \quad \text{By Lemma 47.2(3)}
\]

\[
\leq N(\beta) \cdot \frac{1}{2}
\]

So \( N(\rho) < N(\beta) \) and Condition 2 follows.

Theorem 47.7. (Continued)

**Theorem 47.7.** If \( D \) is an integral domain with a multiplicative norm \( N \), then \( N(1) = 1 \) and \( |N(u)| = 1 \) for every unit \( u \in D \). If, furthermore, every \( \alpha \) satisfying \( |N(\alpha)| = 1 \) is a unit in \( D \), then an element \( \pi \in D \) with \( |N(\pi)| = p \) for a prime \( p \in \mathbb{Z} \) is an irreducible of \( D \).

**Proof.** Let \( D \) be an integral domain with a multiplicative norm \( N \). Then \( N(1) = N((1)(1)) = N(1)N(1) \) and so \( N(1) \) is either 0 or 1. By Condition (1) we have that \( N(1) = 1 \). If \( u \in D \) is a unit then \( 1 = N(1) = N(uu^{-1}) = N(u)N(u^{-1}) \). Since \( N(u) \) is an integer then \( N(u) = \pm 1 \) and \( |N(u)| = 1 \).

Theorem 47.10. Fermat’s \( p = a^2 + b^2 \) Theorem

**Theorem 47.10.** Fermat’s \( p = a^2 + b^2 \) Theorem Let \( p \) be an odd prime in \( \mathbb{Z} \). Then \( p = a^2 + b^2 \) for integers \( a, b \in \mathbb{Z} \) if and only if \( p \equiv 1 \pmod{4} \).

**Proof.** First, suppose \( p = a^2 + b^2 \). Now \( a \) and \( b \) cannot both be even or both be odd since this would give \( p \) even (notice that we hypothesize an odd prime). If \( a = 2r \) (even) and \( b = 2s + 1 \) (odd), then

\[
a^2 + b^2 = 4r^2 + 4rs + 1 \equiv 1 \pmod{4}
\]

and \( p \equiv 1 \pmod{4} \).
Theorem 47.10. Fermat’s $p = a^2 + b^2$ Theorem (Continued)

Theorem 47.10. Fermat’s $p = a^2 + b^2$ Theorem Let $p$ be an odd prime in $\mathbb{Z}$. Then $p = a^2 + b^2$ for integers $a, b \in \mathbb{Z}$ if and only if $p \equiv 1 \pmod{4}$.

Proof. (Continued) Second, assume $p \equiv 1 \pmod{4}$. Now consider the multiplicative group of nonzero elements of $\mathbb{Z}_p$. This is a cyclic group and has order $p - 1$. Since 4 is a divisor of $p - 1$, then this cyclic group has an element $n$ of multiplicative order 4 (the multiplicative group is isomorphic to $U_{p-1}$ and $\exp(2\pi i (p-1)/4i)$ is of order 40. Then $n^2$ is of multiplicative order 2. So $n^2 = -1$ in $\mathbb{Z}_p$ (or $n^2 = p - 1$). So in $\mathbb{Z}$ we have $n^2 \equiv -1 \pmod{p}$ and $n^2 + 1 \in \mathbb{Z}$ is a multiple of $p$.

Theorem 47.10. Fermat’s $p = a^2 + b^2$ Theorem (Continued)

Theorem 47.10. Fermat’s $p = a^2 + b^2$ Theorem Let $p$ be an odd prime in $\mathbb{Z}$. Then $p = a^2 + b^2$ for integers $a, b \in \mathbb{Z}$ if and only if $p \equiv 1 \pmod{4}$.

Proof. (Continued) Viewing $p$ and $n^2 + 1$ in $\mathbb{Z}[i]$ we see that $p$ divides $n^2 + 1 = (n + 1)(n - 1)$. Assume $p$ is irreducible in $\mathbb{Z}[i]$. Then $p$ would have to divide either $n + 1$ or $n - 1$ by Lemma 45.13 (since $\mathbb{Z}$ is a PID — see p391). If $p$ divides $n + 1$, then $n + 1 \equiv p(a + bi)$ for some $a, b \in \mathbb{Z}$. But then we need $pb = 1$ (equating “imaginary parts”). An irreducible is, by definition, not a unit — since $p$ is irreducible by assumption, then $p$ is not a unit so $1 = pb$ is a contradiction. Similarly, if $p$ divides $n - 1$ then we need $-1 = pb$ or $1 \equiv p(-b)$, again a contradiction. These contradictions imply that the assumption that $p$ is irreducible in $\mathbb{Z}[i]$ is false, and $p$ is not irreducible.