Sums of Two Squares

A Complete Treatment

December 2025

1 The Ring of Gaussian Integers

Definition 1.1. The ring of Gaussian integers is $\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}$, where $i^2 = -1$.

Definition 1.2. The norm function $N : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$ is defined by $N(a + bi) := a^2 + b^2$.

Lemma 1.3 (Multiplicativity of the Norm). For all $\alpha, \beta \in \mathbb{Z}[i]$, we have $N(\alpha\beta) = N(\alpha)N(\beta)$.

Proof. Let $\alpha = a + bi$ and $\beta = c + di$. Then $\alpha\beta = (ac - bd) + (ad + bc)i$, and direct computation yields $N(\alpha\beta) = (ac - bd)^2 + (ad + bc)^2 = (a^2 + b^2)(c^2 + d^2) = N(\alpha)N(\beta)$. ∎

Corollary 1.4 (Unit Characterisation). The units of $\mathbb{Z}[i]$ are precisely the elements of norm 1, namely $\{1, -1, i, -i\}$.

Proof. If $\alpha\beta = 1$, then $N(\alpha)N(\beta) = 1$ with $N(\alpha), N(\beta) \in \mathbb{Z}_{\geq 0}$, forcing $N(\alpha) = 1$. Conversely, $a^2 + b^2 = 1$ with $a, b \in \mathbb{Z}$ implies $(a, b) \in \{(\pm 1, 0), (0, \pm 1)\}$. ∎

---

2 Euclidean Structure

Theorem 2.1. The ring $\mathbb{Z}[i]$ is a Euclidean domain with respect to the norm N.

Proof. Let $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$. We must find $q, r \in \mathbb{Z}[i]$ such that $\alpha = \beta q + r$ with $N(r) < N(\beta)$.

Consider $\alpha/\beta \in \mathbb{C}$. Write $\alpha/\beta = x + yi$ with $x, y \in \mathbb{R}$. Choose integers m, n such that $|x - m| \leq 1/2$ and $|y - n| \leq 1/2$. Set $q := m + ni$ and $r := \alpha - \beta q$.

Then $r/\beta = (\alpha/\beta) - q = (x - m) + (y - n)i$, whence $N(r/\beta) = (x - m)^2 + (y - n)^2 \leq 1/4 + 1/4 = 1/2 < 1$. Multiplicativity of the norm gives $N(r) = N(r/\beta) \cdot N(\beta) < N(\beta)$. ∎

Corollary 2.2. The ring $\mathbb{Z}[i]$ is a principal ideal domain and hence a unique factorisation domain. In particular, an element of $\mathbb{Z}[i]$ is irreducible if and only if it is prime.

---

3 Quadratic Residues and Euler's Criterion

Lemma 3.1 (Euler's Criterion). Let p be an odd prime and let a be an integer with $p \nmid a$. Then

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p},$$

where $\left(\frac{a}{p}\right)$ denotes the Legendre symbol, equal to 1 if a is a quadratic residue modulo p and -1 otherwise.

Proof. The multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p - 1$. Let g be a generator and write $a \equiv g^k \pmod{p}$ for some integer k. Then $a^{(p-1)/2} \equiv g^{k(p-1)/2} \pmod{p}$.

We claim $g^{(p-1)/2} = -1$ in $(\mathbb{Z}/p\mathbb{Z})^\times$. Indeed, $(g^{(p-1)/2})^2 = g^{p-1} = 1$, so $g^{(p-1)/2}$ has order dividing 2. Since g has order exactly $p-1$, we have $g^{(p-1)/2} \neq 1$, so $g^{(p-1)/2}$ has order exactly 2. In $(\mathbb{Z}/p\mathbb{Z})^\times$, the equation $x^2 = 1$ has exactly two solutions, namely $x = \pm 1$, and only -1 has order 2. Hence $g^{(p-1)/2} = -1$.

Therefore $a^{(p-1)/2} \equiv (-1)^k \pmod{p}$.

Now a is a quadratic residue if and only if $a = (g^{k/2})^2$ for some integer, which occurs if and only if k is even. Thus $\left(\frac{a}{p}\right) = 1$ if and only if k is even, i.e., $\left(\frac{a}{p}\right) = (-1)^k$. ∎

Corollary 3.2. Let p be an odd prime. Then -1 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod{4}$.

Proof. By Lemma 3.1, $(-1)^{(p-1)/2} \equiv \left(\frac{-1}{p}\right) \pmod{p}$. Both sides lie in $\{-1, 1\}$, and since $p > 2$, the integers -1 and 1 are incongruent modulo p. Hence congruence implies equality: $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

Thus -1 is a quadratic residue if and only if $(p-1)/2$ is even, which holds if and only if $4 \mid (p-1)$. ∎

---

4 Classification of Primes in $\mathbb{Z}[i]$

Definition 4.1. An element $\pi \in \mathbb{Z}[i]$ is irreducible if π is a non-unit and whenever $\pi = \alpha\beta$, at least one of α, β is a unit. By Corollary 2.2, irreducibility and primality coincide in $\mathbb{Z}[i]$.

Theorem 4.2 (Trichotomy for Rational Primes). Let p be a prime in $\mathbb{Z}$. Exactly one of the following holds:

(i) $p = 2$: The prime 2 ramifies as $2 = -i(1+i)^2$, where $1+i$ is prime in $\mathbb{Z}[i]$.
(ii) $p \equiv 1 \pmod{4}$: The prime p splits as $p = \pi\bar{\pi}$ for some prime $\pi \in \mathbb{Z}[i]$, where π and $\bar{\pi}$ are non-associate.
(iii) $p \equiv 3 \pmod{4}$: The prime p remains prime in $\mathbb{Z}[i]$.

Proof of (i). We have $(1+i)(1-i) = 1 - i^2 = 2$. Moreover, $1 - i = (1+i)(-i)$, since $(1+i)(-i) = -i - i^2 = -i + 1 = 1 - i$. Thus $2 = (1+i)(1-i) = (1+i)\cdot(1+i)(-i) = -i(1+i)^2$.

Since $N(1+i) = 1^2 + 1^2 = 2$ is prime in $\mathbb{Z}$, any factorisation $1+i = \alpha\beta$ would yield $N(\alpha)N(\beta) = 2$, forcing one of $N(\alpha), N(\beta)$ to equal 1. By Corollary 1.4, that factor is a unit, so $1+i$ is irreducible. By Corollary 2.2, it is therefore prime in $\mathbb{Z}[i]$. ∎

Proof of (iii). Suppose $p \equiv 3 \pmod{4}$ and $p = \alpha\beta$ for some $\alpha, \beta \in \mathbb{Z}[i]$ with α, β non-units. Taking norms, $N(\alpha)N(\beta) = N(p) = p^2$. Since α, β are non-units, Corollary 1.4 gives $N(\alpha) > 1$ and $N(\beta) > 1$. The only factorisation of p^2 into integers greater than 1 is $p \cdot p$, so $N(\alpha) = N(\beta) = p$.

Writing $\alpha = a + bi$, we have $a^2 + b^2 = p$. Now for any integer m, we have $m^2 \equiv 0 \pmod 4$ if m is even, and $m^2 \equiv 1 \pmod 4$ if m is odd. Hence $a^2 + b^2 \equiv 0, 1,$ or $2 \pmod 4$, according to the parities of a and b. But $p \equiv 3 \pmod 4$, a contradiction.

Thus p admits no factorisation into non-units; that is, p is irreducible in $\mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is a UFD (Corollary 2.2), irreducibility implies primality. Hence p is prime in $\mathbb{Z}[i]$. ■

Proof of (ii). Let $p \equiv 1 \pmod 4$. By Corollary 3.2, there exists $a \in \mathbb{Z}$ with $a^2 \equiv -1 \pmod p$, so $p \mid (a^2 + 1)$ in $\mathbb{Z}$.

In $\mathbb{Z}[i]$, we have $a^2 + 1 = (a + i)(a - i)$. Suppose, for contradiction, that p were prime in $\mathbb{Z}[i]$. Since $p \mid (a + i)(a - i)$ and p is prime, we would have $p \mid (a + i)$ or $p \mid (a - i)$.

Suppose $p \mid (a + i)$. By definition of divisibility in $\mathbb{Z}[i]$, this means $a + i = p\gamma$ for some $\gamma = c + di \in \mathbb{Z}[i]$. Comparing real and imaginary parts: $a = pc$ and $1 = pd$. The second equation requires $d \in \mathbb{Z}$ with $pd = 1$, which is impossible since $p > 1$. By identical reasoning, $p \nmid (a - i)$.

This contradicts the primality assumption, so p is not prime in $\mathbb{Z}[i]$. By Corollary 2.2, prime and irreducible are equivalent in $\mathbb{Z}[i]$. Since p is not prime, it is not irreducible, and hence admits a non-trivial factorisation $p = \alpha\beta$ where α, β are non-units.

Taking norms: $N(\alpha)N(\beta) = p^2$. Since $N(\alpha), N(\beta) > 1$ (by Corollary 1.4), we must have $N(\alpha) = N(\beta) = p$.

We now show α is irreducible. Suppose $\alpha = \gamma\delta$ for some $\gamma, \delta \in \mathbb{Z}[i]$. Then $N(\gamma)N(\delta) = N(\alpha) = p$. Since p is prime in $\mathbb{Z}$, either $N(\gamma) = 1$ or $N(\delta) = 1$. By Corollary 1.4, that factor is a unit. Hence α is irreducible, and by Corollary 2.2, α is prime in $\mathbb{Z}[i]$.

Set $\pi := \alpha$. We have $N(\pi) = p$. For any $\zeta \in \mathbb{Z}[i]$, we have $N(\bar{\zeta}) = N(\zeta)$, so $N(\bar{\pi}) = p$. Thus $\bar{\pi}$ is also irreducible by the same argument, hence prime in $\mathbb{Z}[i]$. Now $\pi\bar{\pi} = N(\pi) = p$, giving the desired factorisation.

It remains to show π and $\bar{\pi}$ are not associates. Write $\pi = a + bi$. The associates of π are $u\pi$ for $u \in \{1, -1, i, -i\}$:

- $1 \cdot \pi = a + bi$
- $(-1) \cdot \pi = -a - bi$
- $i \cdot \pi = i(a + bi) = ai + bi^2 = -b + ai$
- $(-i) \cdot \pi = -i(a + bi) = -ai - bi^2 = b - ai$

For $\bar{\pi} = a - bi$ to be associate to π, we require $a - bi \in \{a + bi, -a - bi, -b + ai, b - ai\}$. Comparing:

- $a - bi = a + bi \implies -b = b \implies b = 0$
- $a - bi = -a - bi \implies a = -a \implies a = 0$
- $a - bi = -b + ai \implies a = -b$ and $-b = a \implies a = -b$

- $a - bi = b - ai \implies a = b$ and $-b = -a \implies a = b$

Thus $\bar{\pi}$ is associate to π if and only if $b = 0$, $a = 0$, $a = b$, or $a = -b$.

Since $p = a^2 + b^2$ is an odd prime:

- $b = 0 \implies p = a^2$. A prime cannot be a perfect square: if $p = a^2$ with $a \in \mathbb{Z}$, then either $|a| = 1$ (giving $p = 1$, not prime) or $|a| > 1$ (making p composite). Contradiction.
- $a = 0 \implies p = b^2$. Same reasoning yields a contradiction.
- $a = b \implies p = 2a^2$. Since p is odd, this is impossible.
- $a = -b \implies p = 2a^2$. Same contradiction.

Hence none of these cases occur, and $\pi, \bar{\pi}$ are non-associate Gaussian primes. ∎

---

5 The Main Theorem

Theorem 5.1 (Fermat–Euler). An odd prime p is expressible as $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$ if and only if $p \equiv 1 \pmod 4$.

Proof. The equation $p = x^2 + y^2$ holds if and only if $p = N(x + yi)$ for some $x + yi \in \mathbb{Z}[i]$.

($\Leftarrow$) Suppose $p \equiv 1 \pmod 4$. By Theorem 4.2(ii), $p = \pi\bar{\pi}$ where $\pi = x + yi$ is a Gaussian prime. Then $p = N(\pi) = x^2 + y^2$.

($\Rightarrow$) Suppose $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$. We show $p \equiv 1 \pmod 4$.

For any integer m, we have $m^2 \equiv 0 \pmod 4$ if m is even, and $m^2 \equiv 1 \pmod 4$ if m is odd. The possible values of $x^2 + y^2$ modulo 4 are therefore:

- $0 + 0 = 0$ (both even)
- $0 + 1 = 1$ (one even, one odd)
- $1 + 0 = 1$ (one odd, one even)
- $1 + 1 = 2$ (both odd)

Thus $x^2 + y^2 \equiv 0, 1,$ or $2 \pmod 4$. Since p is an odd prime, $p \not\equiv 0 \pmod 4$ and $p \not\equiv 2 \pmod 4$. Hence $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$.

The case $p \equiv 3 \pmod 4$ is ruled out because 3 is not among $\{0, 1, 2\}$. Therefore $p \equiv 1 \pmod 4$. ∎

---

6 Uniqueness of Representation

Theorem 6.1. If $p \equiv 1 \pmod 4$, the representation $p = x^2 + y^2$ with $x, y > 0$ is unique up to the interchange of x and y.

Proof. Suppose $p = a^2 + b^2 = c^2 + d^2$ with $a, b, c, d > 0$. Then

$$p = (a + bi)(a - bi) = (c + di)(c - di).$$

Each factor $a + bi, a - bi, c + di, c - di$ has norm p. Since p is prime in $\mathbb{Z}$, any Gaussian integer ζ with $N(\zeta) = p$ is irreducible: if $\zeta = \gamma\delta$, then $N(\gamma)N(\delta) = p$ forces one factor to have norm 1, hence to be a unit by Corollary 1.4. By Corollary 2.2, irreducibility implies primality in $\mathbb{Z}[i]$.

By Theorem 4.2(ii), $p = \pi\bar{\pi}$ is the unique factorisation of p into non-associate Gaussian primes (up to units and ordering).

Now $a + bi$ is prime in $\mathbb{Z}[i]$ and divides $p = \pi\bar{\pi}$. Since primes dividing a product must divide one of the factors, either $(a + bi) \mid \pi$ or $(a + bi) \mid \bar{\pi}$.

Case: Suppose $(a + bi) \mid \pi$. Then $\pi = (a + bi)\varepsilon$ for some $\varepsilon \in \mathbb{Z}[i]$. Taking norms: $p = N(a + bi) \cdot N(\varepsilon) = p \cdot N(\varepsilon)$, so $N(\varepsilon) = 1$ and ε is a unit by Corollary 1.4. Hence $a + bi$ and π are associates.

We now determine that $a - bi$ is associate to $\bar{\pi}$. Conjugation $\sigma : \mathbb{Z}[i] \to \mathbb{Z}[i]$ defined by $\sigma(\alpha) = \bar{\alpha}$ is a ring automorphism: it satisfies $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$ and $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$. Consequently, if $\alpha \mid \beta$ in $\mathbb{Z}[i]$, then $\sigma(\alpha) \mid \sigma(\beta)$. From $\pi = (a + bi)\varepsilon$, applying σ yields $\bar{\pi} = (a - bi)\bar{\varepsilon}$. Since ε is a unit, so is $\bar{\varepsilon}$ (as $N(\bar{\varepsilon}) = N(\varepsilon) = 1$). Hence $a - bi$ and $\bar{\pi}$ are associates.

The case $(a + bi) \mid \bar{\pi}$ yields, by the same reasoning, $a + bi \sim \bar{\pi}$ and $a - bi \sim \pi$.

Invariance of coordinate pairs. We show that if $\alpha \sim \beta$ (associates), then $\{|\operatorname{Re}(\alpha)|, |\operatorname{Im}(\alpha)|\} = \{|\operatorname{Re}(\beta)|, |\operatorname{Im}(\beta)|\}$.

Let $\pi = x + yi$. The associates of π are $u\pi$ for $u \in \{1, -1, i, -i\}$:

- $1 \cdot \pi = x + yi$
- $(-1) \cdot \pi = -x - yi$
- $i \cdot \pi = -y + xi$
- $(-i) \cdot \pi = y - xi$

In each case, the unordered pair of absolute values of real and imaginary parts is $\{|x|, |y|\}$. Hence this pair is invariant under multiplication by units.

Conclusion. Since $a + bi$ is associate to either π or $\bar{\pi}$, and both $\pi = x + yi$ and $\bar{\pi} = x - yi$ yield the pair $\{|x|, |y|\} = \{x, y\}$ (as $x, y > 0$ by construction in Theorem 4.2(ii)), we have $\{a, b\} = \{x, y\}$. The same reasoning applied to $c + di$ gives $\{c, d\} = \{x, y\}$.

Therefore $\{a, b\} = \{c, d\}$, which is the claimed uniqueness. ■

---

7 Generalisation Framework

The method generalises to norms of quadratic rings. For a squarefree integer $d < 0$, consider the imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$ with ring of integers $\mathcal{O}_K$.

Remark 7.1. The structure of $\mathcal{O}_K$ depends on d modulo 4: if $d \equiv 2$ or $3 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$; if $d \equiv 1 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}[(1+\sqrt{d})/2]$.

Principle 7.2. A prime p is represented by the norm form of $\mathcal{O}_K$ if and only if:

1. p splits or ramifies in $\mathcal{O}_K$, and
2. the prime ideals above p are principal.

For $\mathbb{Z}[i]$, every ideal is principal (the class number is 1), so condition (2) is automatically satisfied. For rings with class number greater than 1, the analysis requires ideal class groups.

Example 7.3. The form $x^2 + 5y^2$ corresponds to the maximal order $\mathbb{Z}[\sqrt{-5}]$ of $\mathbb{Q}(\sqrt{-5})$, since $-5 \equiv 3 \pmod 4$. This ring has class number 2. The representability of primes by $x^2 + 5y^2$ is governed by the splitting behaviour in the Hilbert class field of $\mathbb{Q}(\sqrt{-5})$. (For nonmaximal orders, the appropriate object is the ring class field rather than the Hilbert class field.)

---

8 Connection to Cyclotomic Theory

The ring $\mathbb{Z}[i] = \mathbb{Z}[\zeta_4]$ is the ring of integers of the 4th cyclotomic field $\mathbb{Q}(\zeta_4)$, where $\zeta_4 = i$ is a primitive 4th root of unity with minimal polynomial $\Phi_4(x) = x^2 + 1$.

Theorem 8.1. Let p be a prime with $p \nmid n$. The prime p splits completely in $\mathbb{Q}(\zeta_n)$ if and only if $p \equiv 1 \pmod n$.

For $n = 4$, the extension $\mathbb{Q}(i)/\mathbb{Q}$ has degree $\varphi(4) = 2$. In a quadratic extension, "splits completely" and "splits" coincide (as opposed to remaining inert or ramifying). Thus p splits in $\mathbb{Q}(i)$ if and only if $p \equiv 1 \pmod 4$, recovering our criterion from Theorem 4.2.

The cyclotomic perspective unifies the treatment: the factorisation of $x^n - 1$ into cyclotomic polynomials $\Phi_d(x)$ governs the arithmetic of roots of unity, and congruence conditions on primes control their splitting behaviour in cyclotomic fields.