Math 361

March 1, 2023

Quiz

1. Let R be a ring, and let M be an R-module. What does it mean to say the M is *Noetherian*.

2. Suppose that $0 \to M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \to 0$ is a short exact sequence of R-modules. What can we say about the Noetherian condition in this setting?

3. State the Hilbert basis theorem.

Today

- FDs versus UFD
- Euclidean domains
- Application.

Factorization

Let R be a ring.

Factorization

Let R be a ring.

- $u \in R$ is a *unit* if it divides 1, i.e., if it has a multiplicative inverse.

Factorization

Let R be a ring.

- $u \in R$ is a *unit* if it divides 1, i.e., if it has a multiplicative inverse.
- $r \in R$ is *irreducible* if it is

Factorization

Let R be a ring.

- $u \in R$ is a *unit* if it divides 1, i.e., if it has a multiplicative inverse.
- $r \in R$ is *irreducible* if it is nonzero,

Factorization

Let R be a ring.

- $u \in R$ is a *unit* if it divides 1, i.e., if it has a multiplicative inverse.
- $r \in R$ is *irreducible* if it is nonzero, not a unit,

Factorization

Let R be a ring.

- $u \in R$ is a *unit* if it divides 1, i.e., if it has a multiplicative inverse.
- $r \in R$ is *irreducible* if it is nonzero, not a unit, and $r = st \Rightarrow s$ or t is a unit.

Factorization

Let R be a ring.

- $u \in R$ is a *unit* if it divides 1, i.e., if it has a multiplicative inverse.
- $r \in R$ is *irreducible* if it is nonzero, not a unit, and $r = st \Rightarrow s$ or t is a unit.
- $p \in R$ is *prime* if it is

Factorization

Let R be a ring.

- $u \in R$ is a *unit* if it divides 1, i.e., if it has a multiplicative inverse.
- $r \in R$ is *irreducible* if it is nonzero, not a unit, and $r = st \Rightarrow s$ or t is a unit.
- $p \in R$ is *prime* if it is nonzero,

Factorization

Let R be a ring.

- $u \in R$ is a *unit* if it divides 1, i.e., if it has a multiplicative inverse.
- $r \in R$ is *irreducible* if it is nonzero, not a unit, and $r = st \Rightarrow s$ or t is a unit.
- $p \in R$ is *prime* if it is nonzero, not a unit,

Factorization

Let R be a ring.

- $u \in R$ is a *unit* if it divides 1, i.e., if it has a multiplicative inverse.
- $r \in R$ is *irreducible* if it is nonzero, not a unit, and $r = st \Rightarrow s$ or t is a unit.
- $p \in R$ is *prime* if it is nonzero, not a unit, and whenever $p|(ab)$,

Factorization

Let R be a ring.

- $u \in R$ is a *unit* if it divides 1, i.e., if it has a multiplicative inverse.
- $r \in R$ is *irreducible* if it is nonzero, not a unit, and $r = st \Rightarrow s$ or t is a unit.
- $p \in R$ is *prime* if it is nonzero, not a unit, and whenever $p|(ab)$, either $p|a$ or $p|b$.
- In a domain, prime $\Rightarrow$ irreducible.

Factorization

Let R be a ring.

- $u \in R$ is a *unit* if it divides 1, i.e., if it has a multiplicative inverse.
- $r \in R$ is *irreducible* if it is nonzero, not a unit, and $r = st \Rightarrow s$ or t is a unit.
- $p \in R$ is *prime* if it is nonzero, not a unit, and whenever $p|(ab)$, either $p|a$ or $p|b$.
- In a domain, prime $\Rightarrow$ irreducible. In a PID, the converse holds.

Factorization

$r \in R$ has a *factorization into irreducibles* if there exists a unit u and irreducibles $p_1, \ldots, p_k$ such that

$$r = up_1 \cdots p_k.$$

Factorization

$r \in R$ has a *factorization into irreducibles* if there exists a unit u and irreducibles $p_1, \ldots, p_k$ such that

$$r = up_1 \cdots p_k.$$

The factorization of r is *unique* if whenever

$$r = vq_1 \cdots q_\ell$$

with v a unit and $q_1, \ldots, q_\ell$ irreducible,

Factorization

$r \in R$ has a *factorization into irreducibles* if there exists a unit u and irreducibles $p_1, \ldots, p_k$ such that

$$r = up_1 \cdots p_k.$$

The factorization of r is *unique* if whenever

$$r = vq_1 \cdots q_\ell$$

with v a unit and $q_1, \ldots, q_\ell$ irreducible, then $k = \ell$ and up to a permutation of the indices $p_i = u_i q_i$ for some unit u_i for all i.

Factorization

$r \in R$ has a *factorization into irreducibles* if there exists a unit u and irreducibles $p_1, \ldots, p_k$ such that

$$r = up_1 \cdots p_k.$$

The factorization of r is *unique* if whenever

$$r = vq_1 \cdots q_\ell$$

with v a unit and $q_1, \ldots, q_\ell$ irreducible, then $k = \ell$ and up to a permutation of the indices $p_i = u_i q_i$ for some unit u_i for all i.

The ring R is a *factorization domain* (FD) is each nonzero element has a factorization into irreducibles.

Factorization

$r \in R$ has a *factorization into irreducibles* if there exists a unit u and irreducibles $p_1, \ldots, p_k$ such that

$$r = up_1 \cdots p_k.$$

The factorization of r is *unique* if whenever

$$r = vq_1 \cdots q_\ell$$

with v a unit and $q_1, \ldots, q_\ell$ irreducible, then $k = \ell$ and up to a permutation of the indices $p_i = u_i q_i$ for some unit u_i for all i.

The ring R is a *factorization domain* (FD) is each nonzero element has a factorization into irreducibles.

The ring R is a *unique factorization domain* (UFD) if each nonzero element $r \in R$ has a unique factorization into irreducibles.

Factorization

We have seen that every Noetherian domain is an FD.

Factorization

We have seen that every Noetherian domain is an FD. In particular, the ring of integers in a number field is an FD.

Factorization

We have seen that every Noetherian domain is an FD. In particular, the ring of integers in a number field is an FD.

Theorem. Let R be an FD.

Factorization

We have seen that every Noetherian domain is an FD. In particular, the ring of integers in a number field is an FD.

Theorem. Let R be an FD. Then R is a UFD if and only if every irreducible in R is prime.

Factorization

We have seen that every Noetherian domain is an FD. In particular, the ring of integers in a number field is an FD.

Theorem. Let R be an FD. Then R is a UFD if and only if every irreducible in R is prime.

Proof. See Theorems 4.14 in our text.

Factorization

We have seen that every Noetherian domain is an FD. In particular, the ring of integers in a number field is an FD.

Theorem. Let R be an FD. Then R is a UFD if and only if every irreducible in R is prime.

Proof. See Theorems 4.14 in our text.

Example. In $\mathbb{Z}[\sqrt{-5}]$, we have

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Factorization

We have seen that every Noetherian domain is an FD. In particular, the ring of integers in a number field is an FD.

Theorem. Let R be an FD. Then R is a UFD if and only if every irreducible in R is prime.

Proof. See Theorems 4.14 in our text.

Example. In $\mathbb{Z}[\sqrt{-5}]$, we have

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

$\mathbb{Z}[\sqrt{-5}]$ is an FD but not a UFD.

Euclidean domains

Euclidean domains. A domain R is a *Euclidean domain* if

Euclidean domains

Euclidean domains. A domain R is a *Euclidean domain* if there exists a function

$$d \colon R \setminus \{0\} \to \mathbb{N}$$

such that for all $a, b \in R \setminus \{0\}$,

Euclidean domains

Euclidean domains. A domain R is a *Euclidean domain* if there exists a function

$$d \colon R \setminus \{0\} \to \mathbb{N}$$

such that for all $a, b \in R \setminus \{0\}$,

1. $a|b$ implies $d(a) \leq d(b)$, and

Euclidean domains

Euclidean domains. A domain R is a *Euclidean domain* if there exists a function

$$d \colon R \setminus \{0\} \to \mathbb{N}$$

such that for all $a, b \in R \setminus \{0\}$,

1. $a|b$ implies $d(a) \leq d(b)$, and
2. there exist $q, r \in R$ such that

$$a = qb + r$$

with $r = 0$ or $d(r) < d(b)$.

Euclidean domains

Euclidean domains. A domain R is a *Euclidean domain* if there exists a function

$$d\colon R \setminus \{0\} \to \mathbb{N}$$

such that for all $a, b \in R \setminus \{0\}$,

1. $a|b$ implies $d(a) \leq d(b)$, and
2. there exist $q, r \in R$ such that

$$a = qb + r$$

with $r = 0$ or $d(r) < d(b)$.

Examples. $\mathbb{Z}$ with $d(n) = |n|$,

Euclidean domains

Euclidean domains. A domain R is a *Euclidean domain* if there exists a function

$$d\colon R \setminus \{0\} \to \mathbb{N}$$

such that for all $a, b \in R \setminus \{0\}$,

1. $a|b$ implies $d(a) \leq d(b)$, and
2. there exist $q, r \in R$ such that

$$a = qb + r$$

with $r = 0$ or $d(r) < d(b)$.

Examples. $\mathbb{Z}$ with $d(n) = |n|$, and $K[x]$ for a field K with $d(f) = \deg(f)$.

Euclidean domains

Proposition. Every Euclidean domain is a PID.

Euclidean domains

Proposition. Every Euclidean domain is a PID.

Proof. Let R, d be a Euclidean domain, and let $I \subseteq R$ be an ideal.

Euclidean domains

Proposition. Every Euclidean domain is a PID.

Proof. Let R, d be a Euclidean domain, and let $I \subseteq R$ be an ideal. If $I = (0)$, there is nothing to prove. So suppose $I \neq (0)$.

Euclidean domains

Proposition. Every Euclidean domain is a PID.

Proof. Let R, d be a Euclidean domain, and let $I \subseteq R$ be an ideal. If $I = (0)$, there is nothing to prove. So suppose $I \neq (0)$. Among the nonzero elements of I choose one, a, with minimal value $d(a)$.

Euclidean domains

Proposition. Every Euclidean domain is a PID.

Proof. Let R, d be a Euclidean domain, and let $I \subseteq R$ be an ideal. If $I = (0)$, there is nothing to prove. So suppose $I \neq (0)$. Among the nonzero elements of I choose one, a, with minimal value $d(a)$. We now show that $I = (a)$.

Euclidean domains

Proposition. Every Euclidean domain is a PID.

Proof. Let R, d be a Euclidean domain, and let $I \subseteq R$ be an ideal. If $I = (0)$, there is nothing to prove. So suppose $I \neq (0)$. Among the nonzero elements of I choose one, a, with minimal value $d(a)$. We now show that $I = (a)$.

Given $b \in I$ we write

$$b = qa + r$$

with either $r = 0$ or $d(r) < d(a)$.

Euclidean domains

Proposition. Every Euclidean domain is a PID.

Proof. Let R, d be a Euclidean domain, and let $I \subseteq R$ be an ideal. If $I = (0)$, there is nothing to prove. So suppose $I \neq (0)$. Among the nonzero elements of I choose one, a, with minimal value $d(a)$. We now show that $I = (a)$.

Given $b \in I$ we write

$$b = qa + r$$

with either $r = 0$ or $d(r) < d(a)$. Note that $r = b - qa \in I$.

Euclidean domains

Proposition. Every Euclidean domain is a PID.

Proof. Let R, d be a Euclidean domain, and let $I \subseteq R$ be an ideal. If $I = (0)$, there is nothing to prove. So suppose $I \neq (0)$. Among the nonzero elements of I choose one, a, with minimal value $d(a)$. We now show that $I = (a)$.

Given $b \in I$ we write

$$b = qa + r$$

with either $r = 0$ or $d(r) < d(a)$. Note that $r = b - qa \in I$. Therefore, by minimality of $d(a)$, it cannot be the case that $d(r) < d(a)$.

Euclidean domains

Proposition. Every Euclidean domain is a PID.

Proof. Let R, d be a Euclidean domain, and let $I \subseteq R$ be an ideal. If $I = (0)$, there is nothing to prove. So suppose $I \neq (0)$. Among the nonzero elements of I choose one, a, with minimal value $d(a)$. We now show that $I = (a)$.

Given $b \in I$ we write

$$b = qa + r$$

with either $r = 0$ or $d(r) < d(a)$. Note that $r = b - qa \in I$. Therefore, by minimality of $d(a)$, it cannot be the case that $d(r) < d(a)$. Therefore, $r = 0$ and $b = qa$. Hence, $b \in (a)$. $\square$

Quadratic fields

Theorem. Let $m \in \mathbb{Z}_{<0}$ be a negative integer, and let $K = \mathbb{Q}(\sqrt{m})$. Then $\mathfrak{O}_K$ is Euclidean exactly when

Quadratic fields

Theorem. Let $m \in \mathbb{Z}_{<0}$ be a negative integer, and let $K = \mathbb{Q}(\sqrt{m})$. Then $\mathfrak{O}_K$ is Euclidean exactly when

$$d = -1, -2, -3, -7, -11.$$

Quadratic fields

Theorem. Let $m \in \mathbb{Z}_{<0}$ be a negative integer, and let $K = \mathbb{Q}(\sqrt{m})$. Then $\mathfrak{O}_K$ is Euclidean exactly when

$$d = -1, -2, -3, -7, -11.$$

In these cases, one may use the norm as the Euclidean function ($d(\alpha) := N(\alpha)$ for all $\alpha \in \mathfrak{O}_K$).

Quadratic fields

Theorem. Let $m \in \mathbb{Z}_{<0}$ be a negative integer, and let $K = \mathbb{Q}(\sqrt{m})$. Then $\mathfrak{O}_K$ is Euclidean exactly when

$$d = -1, -2, -3, -7, -11.$$

In these cases, one may use the norm as the Euclidean function ($d(\alpha) := N(\alpha)$ for all $\alpha \in \mathfrak{O}_K$).

Theorem. The ring of integers of $\mathbb{Q}(\sqrt{m})$, for positive m, is Euclidean with respect to the (absolute value of the) norm function if and only if

$$m = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 55, 73.$$

Quadratic fields

Theorem. Let $m \in \mathbb{Z}_{<0}$ be a negative integer, and let $K = \mathbb{Q}(\sqrt{m})$. Then $\mathfrak{O}_K$ is Euclidean exactly when

$$d = -1, -2, -3, -7, -11.$$

In these cases, one may use the norm as the Euclidean function ($d(\alpha) := N(\alpha)$ for all $\alpha \in \mathfrak{O}_K$).

Theorem. The ring of integers of $\mathbb{Q}(\sqrt{m})$, for positive m, is Euclidean with respect to the (absolute value of the) norm function if and only if

$$m = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 55, 73.$$

Result from 2000: $\mathbb{Z}[14]$ is Euclidean (but not with respect to the norm function).

Quadratic fields

Theorem. Let $m \in \mathbb{Z}_{<0}$ be a negative integer, and let $K = \mathbb{Q}(\sqrt{m})$. Then $\mathfrak{O}_K$ is Euclidean exactly when

$$d = -1, -2, -3, -7, -11.$$

In these cases, one may use the norm as the Euclidean function ($d(\alpha) := N(\alpha)$ for all $\alpha \in \mathfrak{O}_K$).

Theorem. The ring of integers of $\mathbb{Q}(\sqrt{m})$, for positive m, is Euclidean with respect to the (absolute value of the) norm function if and only if

$$m = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 55, 73.$$

Result from 2000: $\mathbb{Z}[14]$ is Euclidean (but not with respect to the norm function). Full list is an open problem.

Application

Theorem. The only integer solutions to

$$y^2 + 4 = z^3$$

are $(y, z) = (\pm 11, 5)$ and $(y, z) = (\pm 2, 2)$.

Application

Theorem. The only integer solutions to

$$y^2 + 4 = z^3$$

are $(y, z) = (\pm 11, 5)$ and $(y, z) = (\pm 2, 2)$.

Proof. See Theorem 4.22 in our text.

Application

Theorem. The only integer solutions to

$$y^2 + 4 = z^3$$

are $(y, z) = (\pm 11, 5)$ and $(y, z) = (\pm 2, 2)$.

Proof. See Theorem 4.22 in our text. We will do the case where y is odd.

Application

Theorem. The only integer solutions to

$$y^2 + 4 = z^3$$

are $(y, z) = (\pm 11, 5)$ and $(y, z) = (\pm 2, 2)$.

Proof. See Theorem 4.22 in our text. We will do the case where y is odd.

Factor the equation in $\mathbb{Z}[i]$:

$$(2 + iy)(2 - iy) = z^3.$$

Application

Theorem. The only integer solutions to

$$y^2 + 4 = z^3$$

are $(y, z) = (\pm 11, 5)$ and $(y, z) = (\pm 2, 2)$.

Proof. See Theorem 4.22 in our text. We will do the case where y is odd.

Factor the equation in $\mathbb{Z}[i]$:

$$(2 + iy)(2 - iy) = z^3.$$

The proof proceeds in two steps:

Application

Theorem. The only integer solutions to

$$y^2 + 4 = z^3$$

are $(y, z) = (\pm 11, 5)$ and $(y, z) = (\pm 2, 2)$.

Proof. See Theorem 4.22 in our text. We will do the case where y is odd.

Factor the equation in $\mathbb{Z}[i]$:

$$(2 + iy)(2 - iy) = z^3.$$

The proof proceeds in two steps:

- First show that $2 + iy$ and $2 - yi$ are relatively prime in $\mathbb{Z}[i]$.

Application

Theorem. The only integer solutions to

$$y^2 + 4 = z^3$$

are $(y, z) = (\pm 11, 5)$ and $(y, z) = (\pm 2, 2)$.

Proof. See Theorem 4.22 in our text. We will do the case where y is odd.

Factor the equation in $\mathbb{Z}[i]$:

$$(2 + iy)(2 - iy) = z^3.$$

The proof proceeds in two steps:

- First show that $2 + iy$ and $2 - yi$ are relatively prime in $\mathbb{Z}[i]$.
- Consider the implication for a perfect cube $z^3 = (2 + iy)(2 - iy) = y^2 + 4$.

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

If $a + bi$ divides both $2 + iy$ and $2 - iy$, then it divides their sum and difference:

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

If $a + bi$ divides both $2 + iy$ and $2 - iy$, then it divides their sum and difference:

$$4 = (a + bi)\gamma \quad \text{and} \quad 2iy = (a + bi)\mu,$$

for some $\gamma, \mu \in \mathbb{Z}[i]$.

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

If $a + bi$ divides both $2 + iy$ and $2 - iy$, then it divides their sum and difference:

$$4 = (a + bi)\gamma \quad \text{and} \quad 2iy = (a + bi)\mu,$$

for some $\gamma, \mu \in \mathbb{Z}[i]$.

Take norms:

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

If $a + bi$ divides both $2 + iy$ and $2 - iy$, then it divides their sum and difference:

$$4 = (a + bi)\gamma \quad \text{and} \quad 2iy = (a + bi)\mu,$$

for some $\gamma, \mu \in \mathbb{Z}[i]$.

Take norms:

$$16 = (a^2 + b^2)N(\gamma)$$

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

If $a + bi$ divides both $2 + iy$ and $2 - iy$, then it divides their sum and difference:

$$4 = (a + bi)\gamma \quad \text{and} \quad 2iy = (a + bi)\mu,$$

for some $\gamma, \mu \in \mathbb{Z}[i]$.

Take norms:

$$16 = (a^2 + b^2)N(\gamma) \quad \text{and} \quad 4y^2 = (a^2 + b^2)N(\mu)$$

where $N(\gamma), N(\mu) \in \mathbb{Z}$.

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

If $a + bi$ divides both $2 + iy$ and $2 - iy$, then it divides their sum and difference:

$$4 = (a + bi)\gamma \quad \text{and} \quad 2iy = (a + bi)\mu,$$

for some $\gamma, \mu \in \mathbb{Z}[i]$.

Take norms:

$$16 = (a^2 + b^2)N(\gamma) \quad \text{and} \quad 4y^2 = (a^2 + b^2)N(\mu)$$

where $N(\gamma), N(\mu) \in \mathbb{Z}$.

$16 = (a^2 + b^2)N(\gamma) \Rightarrow a^2 + b^2$ is a power of 2.

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

If $a + bi$ divides both $2 + iy$ and $2 - iy$, then it divides their sum and difference:

$$4 = (a + bi)\gamma \quad \text{and} \quad 2iy = (a + bi)\mu,$$

for some $\gamma, \mu \in \mathbb{Z}[i]$.

Take norms:

$$16 = (a^2 + b^2)N(\gamma) \quad \text{and} \quad 4y^2 = (a^2 + b^2)N(\mu)$$

where $N(\gamma), N(\mu) \in \mathbb{Z}$.

$16 = (a^2 + b^2)N(\gamma) \Rightarrow a^2 + b^2$ is a power of 2.
Then $4y^2 = (a^2 + b^2)N(\mu) \Rightarrow a^2 + b^2 \in \{1, 2, 4\}$.

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

We have seen: if $a + bi$ divides both $2 + iy$ and $2 - iy$, then $a^2 + b^2 \in \{1, 2, 4\}$.

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

We have seen: if $a + bi$ divides both $2 + iy$ and $2 - iy$, then $a^2 + b^2 \in \{1, 2, 4\}$.

Case 1. $a^2 + b^2 = 1$

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

We have seen: if $a + bi$ divides both $2 + iy$ and $2 - iy$, then $a^2 + b^2 \in \{1, 2, 4\}$.

Case 1. $a^2 + b^2 = 1 \Rightarrow a + bi = \pm 1, \pm i$.

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

We have seen: if $a + bi$ divides both $2 + iy$ and $2 - iy$, then $a^2 + b^2 \in \{1, 2, 4\}$.

Case 1. $a^2 + b^2 = 1 \Rightarrow a + bi = \pm 1, \pm i$. So in this case $a + bi$ is a unit, hence not prime.

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

We have seen: if $a + bi$ divides both $2 + iy$ and $2 - iy$, then $a^2 + b^2 \in \{1, 2, 4\}$.

Case 1. $a^2 + b^2 = 1 \Rightarrow a + bi = \pm 1, \pm i$. So in this case $a + bi$ is a unit, hence not prime.

Case 2. $a^2 + b^2 = 2$

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

We have seen: if $a + bi$ divides both $2 + iy$ and $2 - iy$, then $a^2 + b^2 \in \{1, 2, 4\}$.

Case 1. $a^2 + b^2 = 1 \Rightarrow a + bi = \pm 1, \pm i$. So in this case $a + bi$ is a unit, hence not prime.

Case 2. $a^2 + b^2 = 2 \Rightarrow a + bi = \pm(1 \pm i)$.

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

We have seen: if $a + bi$ divides both $2 + iy$ and $2 - iy$, then $a^2 + b^2 \in \{1, 2, 4\}$.

Case 1. $a^2 + b^2 = 1 \Rightarrow a + bi = \pm 1, \pm i$. So in this case $a + bi$ is a unit, hence not prime.

Case 2. $a^2 + b^2 = 2 \Rightarrow a + bi = \pm(1 \pm i)$. These four solution differ by a unit factor: $\pm 1, \pm i$.

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

We have seen: if $a + bi$ divides both $2 + iy$ and $2 - iy$, then $a^2 + b^2 \in \{1, 2, 4\}$.

Case 1. $a^2 + b^2 = 1 \Rightarrow a + bi = \pm 1, \pm i$. So in this case $a + bi$ is a unit, hence not prime.

Case 2. $a^2 + b^2 = 2 \Rightarrow a + bi = \pm(1 \pm i)$. These four solution differ by a unit factor: $\pm 1, \pm i$. So it suffices to consider the case $a + bi = 1 + i$.

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

We have seen: if $a + bi$ divides both $2 + iy$ and $2 - iy$, then $a^2 + b^2 \in \{1, 2, 4\}$.

Case 1. $a^2 + b^2 = 1 \Rightarrow a + bi = \pm 1, \pm i$. So in this case $a + bi$ is a unit, hence not prime.

Case 2. $a^2 + b^2 = 2 \Rightarrow a + bi = \pm(1 \pm i)$. These four solution differ by a unit factor: $\pm 1, \pm i$. So it suffices to consider the case $a + bi = 1 + i$. Then

$$2 + iy = (1 + i)(s + ti) = (s - t) + (s + t)i,$$

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

We have seen: if $a + bi$ divides both $2 + iy$ and $2 - iy$, then $a^2 + b^2 \in \{1, 2, 4\}$.

Case 1. $a^2 + b^2 = 1 \Rightarrow a + bi = \pm 1, \pm i$. So in this case $a + bi$ is a unit, hence not prime.

Case 2. $a^2 + b^2 = 2 \Rightarrow a + bi = \pm(1 \pm i)$. These four solution differ by a unit factor: $\pm 1, \pm i$. So it suffices to consider the case $a + bi = 1 + i$. Then

$$2 + iy = (1 + i)(s + ti) = (s - t) + (s + t)i,$$

implies $s - t = 2$ and $s + t = y$.

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

We have seen: if $a + bi$ divides both $2 + iy$ and $2 - iy$, then $a^2 + b^2 \in \{1, 2, 4\}$.

Case 1. $a^2 + b^2 = 1 \Rightarrow a + bi = \pm 1, \pm i$. So in this case $a + bi$ is a unit, hence not prime.

Case 2. $a^2 + b^2 = 2 \Rightarrow a + bi = \pm(1 \pm i)$. These four solution differ by a unit factor: $\pm 1, \pm i$. So it suffices to consider the case $a + bi = 1 + i$. Then

$$2 + iy = (1 + i)(s + ti) = (s - t) + (s + t)i,$$

implies $s - t = 2$ and $s + t = y$. That's not possible since y is odd.

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

Case 3. $a^2 + b^2 = 4$

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

Case 3. $a^2 + b^2 = 4 \Rightarrow a + bi = \pm 2, \pm 2i$.

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

Case 3. $a^2 + b^2 = 4 \Rightarrow a + bi = \pm 2, \pm 2i$. Again, these solutions all differ by a factor of a unit.

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

Case 3. $a^2 + b^2 = 4 \Rightarrow a + bi = \pm 2, \pm 2i$. Again, these solutions all differ by a factor of a unit. Consider the case $a + bi = 2$.

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

Case 3. $a^2 + b^2 = 4 \Rightarrow a + bi = \pm 2, \pm 2i$. Again, these solutions all differ by a factor of a unit. Consider the case $a + bi = 2$. However, 2 is not prime in $\mathbb{Z}[i]$:

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

Case 3. $a^2 + b^2 = 4 \Rightarrow a + bi = \pm 2, \pm 2i$. Again, these solutions all differ by a factor of a unit. Consider the case $a + bi = 2$. However, 2 is not prime in $\mathbb{Z}[i]$:

$$2 = (1 + i)(1 - i).$$

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

Case 3. $a^2 + b^2 = 4 \Rightarrow a + bi = \pm 2, \pm 2i$. Again, these solutions all differ by a factor of a unit. Consider the case $a + bi = 2$. However, 2 is not prime in $\mathbb{Z}[i]$:

$$2 = (1 + i)(1 - i).$$

So 2 divides the product of $1 + i$ and $1 - i$.

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

Case 3. $a^2 + b^2 = 4 \Rightarrow a + bi = \pm 2, \pm 2i$. Again, these solutions all differ by a factor of a unit. Consider the case $a + bi = 2$. However, 2 is not prime in $\mathbb{Z}[i]$:

$$2 = (1 + i)(1 - i).$$

So 2 divides the product of $1 + i$ and $1 - i$. But 2 does not divide $1 \pm i$ since $N(2) = 4$ does not divide $N(1 \pm i) = 2$.

$2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$

Case 3. $a^2 + b^2 = 4 \Rightarrow a + bi = \pm 2, \pm 2i$. Again, these solutions all differ by a factor of a unit. Consider the case $a + bi = 2$. However, 2 is not prime in $\mathbb{Z}[i]$:

$$2 = (1 + i)(1 - i).$$

So 2 divides the product of $1 + i$ and $1 - i$. But 2 does not divide $1 \pm i$ since $N(2) = 4$ does not divide $N(1 \pm i) = 2$.

Thus, we have shown that $2 + iy$ and $2 - iy$ are relatively prime in $\mathbb{Z}[i]$.

Implications

We have $(2 + yi)(2 - iy) = z^3$ with $z \in \mathbb{Z}$ and where $2 + iy$ and $2 - iy$ are relatively prime.

Implications

We have $(2 + yi)(2 - iy) = z^3$ with $z \in \mathbb{Z}$ and where $2 + iy$ and $2 - iy$ are relatively prime.

Consider the factorization of z in $\mathbb{Z}[i]$.

Implications

We have $(2 + yi)(2 - iy) = z^3$ with $z \in \mathbb{Z}$ and where $2 + iy$ and $2 - iy$ are relatively prime.

Consider the factorization of z in $\mathbb{Z}[i]$. We must be able to group the factors so that $z = \alpha\beta$ in $\mathbb{Z}[i]$ where α is relatively prime to $2 - iy$ and β is relatively prime to $2 + iy$.

Implications

We have $(2 + yi)(2 - iy) = z^3$ with $z \in \mathbb{Z}$ and where $2 + iy$ and $2 - iy$ are relatively prime.

Consider the factorization of z in $\mathbb{Z}[i]$. We must be able to group the factors so that $z = \alpha\beta$ in $\mathbb{Z}[i]$ where α is relatively prime to $2 - iy$ and β is relatively prime to $2 + iy$. Therefore,

$$2 + iy = u\alpha^3 \quad \text{and} \quad 2 - iy = v\beta^3$$

for some units u and v.

Implications

We have $(2 + yi)(2 - iy) = z^3$ with $z \in \mathbb{Z}$ and where $2 + iy$ and $2 - iy$ are relatively prime.

Consider the factorization of z in $\mathbb{Z}[i]$. We must be able to group the factors so that $z = \alpha\beta$ in $\mathbb{Z}[i]$ where α is relatively prime to $2 - iy$ and β is relatively prime to $2 + iy$. Therefore,

$$2 + iy = u\alpha^3 \quad \text{and} \quad 2 - iy = v\beta^3$$

for some units u and v.

Every unit in $\mathbb{Z}[i]$ is a cube. (Check.)

Implications

We have $(2+yi)(2-iy) = z^3$ with $z \in \mathbb{Z}$ and where $2+iy$ and $2-iy$ are relatively prime.

Consider the factorization of z in $\mathbb{Z}[i]$. We must be able to group the factors so that $z = \alpha\beta$ in $\mathbb{Z}[i]$ where α is relatively prime to $2-iy$ and β is relatively prime to $2+iy$. Therefore,

$$2+iy = u\alpha^3 \quad \text{and} \quad 2-iy = v\beta^3$$

for some units u and v.

Every unit in $\mathbb{Z}[i]$ is a cube. (Check.) Therefore, we have

$$2+iy = (a+bi)^3$$

for some $a, b \in \mathbb{Z}$.

Implications

We have $(2+yi)(2-iy) = z^3$ with $z \in \mathbb{Z}$ and where $2+iy$ and $2-iy$ are relatively prime.

Consider the factorization of z in $\mathbb{Z}[i]$. We must be able to group the factors so that $z = \alpha\beta$ in $\mathbb{Z}[i]$ where α is relatively prime to $2-iy$ and β is relatively prime to $2+iy$. Therefore,

$$2+iy = u\alpha^3 \quad \text{and} \quad 2-iy = v\beta^3$$

for some units u and v.

Every unit in $\mathbb{Z}[i]$ is a cube. (Check.) Therefore, we have

$$2+iy = (a+bi)^3$$

for some $a, b \in \mathbb{Z}$. Take conjugates to get

$$2-iy = (a-bi)^3.$$

Implications

Add the equations $2 + iy = (a + bi)^3$ and $2 - iy = (a - bi)^3$:

$$4 = (a + bi)^3 + (a - bi)^3$$

Implications

Add the equations $2 + iy = (a + bi)^3$ and $2 - iy = (a - bi)^3$:

$$4 = (a + bi)^3 + (a - bi)^3 = 2a(a^2 - 3b^2).$$

Implications

Add the equations $2 + iy = (a + bi)^3$ and $2 - iy = (a - bi)^3$:

$$4 = (a + bi)^3 + (a - bi)^3 = 2a(a^2 - 3b^2).$$

Hence, $2 = a(a^2 - 3b^2)$.

Implications

Add the equations $2 + iy = (a + bi)^3$ and $2 - iy = (a - bi)^3$:

$$4 = (a + bi)^3 + (a - bi)^3 = 2a(a^2 - 3b^2).$$

Hence, $2 = a(a^2 - 3b^2)$.

Possible solutions:

Implications

Add the equations $2 + iy = (a + bi)^3$ and $2 - iy = (a - bi)^3$:

$$4 = (a + bi)^3 + (a - bi)^3 = 2a(a^2 - 3b^2).$$

Hence, $2 = a(a^2 - 3b^2)$.

Possible solutions: $a = 1, b = \pm 1$, and $a = 2, b = \pm 1$.

Implications

Add the equations $2 + iy = (a + bi)^3$ and $2 - iy = (a - bi)^3$:

$$4 = (a + bi)^3 + (a - bi)^3 = 2a(a^2 - 3b^2).$$

Hence, $2 = a(a^2 - 3b^2)$.

Possible solutions: $a = 1, b = \pm 1$, and $a = 2, b = \pm 1$.

Next, note that

$$z^3 = (2+iy)(2-iy) = (a+bi)^3(a-bi)^3 = ((a+bi)(a-bi))^3 = (a^2+b^2)^3.$$

Implications

Add the equations $2 + iy = (a + bi)^3$ and $2 - iy = (a - bi)^3$:

$$4 = (a + bi)^3 + (a - bi)^3 = 2a(a^2 - 3b^2).$$

Hence, $2 = a(a^2 - 3b^2)$.

Possible solutions: $a = 1, b = \pm 1$, and $a = 2, b = \pm 1$.

Next, note that

$$z^3 = (2+iy)(2-iy) = (a+bi)^3(a-bi)^3 = ((a+bi)(a-bi))^3 = (a^2+b^2)^3.$$

So $z = a^2 + b^2$.

Implications

Add the equations $2 + iy = (a + bi)^3$ and $2 - iy = (a - bi)^3$:

$$4 = (a + bi)^3 + (a - bi)^3 = 2a(a^2 - 3b^2).$$

Hence, $2 = a(a^2 - 3b^2)$.

Possible solutions: $a = 1, b = \pm 1$, and $a = 2, b = \pm 1$.

Next, note that

$$z^3 = (2+iy)(2-iy) = (a+bi)^3(a-bi)^3 = ((a+bi)(a-bi))^3 = (a^2+b^2)^3.$$

So $z = a^2 + b^2$. Plugging in possible values for a and b give $z = 2, 5$.

Implications

Add the equations $2 + iy = (a + bi)^3$ and $2 - iy = (a - bi)^3$:

$$4 = (a + bi)^3 + (a - bi)^3 = 2a(a^2 - 3b^2).$$

Hence, $2 = a(a^2 - 3b^2)$.

Possible solutions: $a = 1, b = \pm 1$, and $a = 2, b = \pm 1$.

Next, note that

$$z^3 = (2+iy)(2-iy) = (a+bi)^3(a-bi)^3 = ((a+bi)(a-bi))^3 = (a^2+b^2)^3.$$

So $z = a^2 + b^2$. Plugging in possible values for a and b give $z = 2, 5$.

To finish the case where y is odd, solve $y^2 + 4 = z^3$ in these cases.