MAU23101 Introduction to number theory
4 - Sums of squares

Nicolas Mascot
mascotn@tcd.ie
Module web page

Michaelmas 2020–2021
Version: October 20, 2021

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Main goal of this chapter

Theorem (Obvious)

An integer $n = \prod_j p_j^{v_j} \in \mathbb{N}$ *is a square iff.* v_j *is even for all* j.

Example

$2020 = 2^2 5^1 101^1$ is not a square.

Main goal of this chapter

Theorem

An integer $n = \prod_j p_j^{v_j} \in \mathbb{N}$ *is a sum of 2 squares iff.* v_j *is even whenever* $p_j \equiv -1 \bmod 4$.

Example

$2019 = 3^1 673^1$ is not a sum of 2 squares.
$3 \times 2019 = 3^2 673^1 = 36^2 + 69^2$.
$2020 = 2^2 5^1 101^1 = 24^2 + 38^2$.
$3^2 = 3^2 + 0^2$.

Main goal of this chapter

Theorem

An integer $n = \prod_j p_j^{v_j} \in \mathbb{N}$ *is a sum of 2 squares iff.* v_j *is even whenever* $p_j \equiv -1 \bmod 4$.

Theorem (Legendre)

An integer $n \in \mathbb{N}$ *is a sum of 3 squares iff. it is* *<u>not</u>* *of the form* $4^a(8b+7)$, $a, b \in \mathbb{Z}_{\geqslant 0}$.

So n is not a sum of 3 squares iff. $v_2(n)$ is even and $\frac{n}{2^{v_2(n)}} \equiv -1 \bmod 8$.

Example

$60 = 2^2 \times 15$ is not a sum of 3 squares.

$30 = 2^1 \times 15 = 5^2 + 2^2 + 1^2$. $44 = 2^2 \times 11 = 6^2 + 2^2 + 2^2$.

Main goal of this chapter

Theorem

An integer $n = \prod_j p_j^{v_j} \in \mathbb{N}$ *is a sum of 2 squares iff.* v_j *is even whenever* $p_j \equiv -1 \bmod 4$.

Theorem (Legendre)

An integer $n \in \mathbb{N}$ *is a sum of 3 squares iff. it is not of the form* $4^a(8b+7)$, $a, b \in \mathbb{Z}_{\geqslant 0}$.

Theorem (Lagrange)

Every $n \in \mathbb{N}$ *is a sum of 4 squares.*

Example

$60 = 6^2 + 4^2 + 2^2 + 2^2$.

Waring's problem (not examinable)

Theorem (Hilbert, 1909)

For each $k \in \mathbb{N}$, there exists $m \in \mathbb{N}$ such that every $n \in \mathbb{N}$ is the sum of m k^{th} powers.

For each k, the smallest possible m is denoted by $g(k)$.

Theorem

- $g(2) = 4$ *(Lagrange, 1770)*
- $g(3) = 9$ *(Wieferich - Kempner, ~1910)*
- $g(4) = 19$ *(Balasubramanian - Dress - Deshouillers, 1986)*
- $g(5) = 37$ *(Chen, 1964)*
- $\ldots$

Gaussian integers

Gaussian integers

Definition

The set of *Gaussian integers* *is*

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C},$$

where $i \in \mathbb{C}$ *is such that* $i^2 = -1$.

Proposition

$\mathbb{Z}[i]$ *is a* *ring*: *whenever* $\alpha, \beta \in \mathbb{Z}[i]$, *we also have*

$$\alpha + \beta,\ \alpha - \beta,\ \alpha\beta \in \mathbb{Z}[i].$$

Proof.

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

□

Gaussian integers

Definition

The set of Gaussian integers is

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C},$$

where $i \in \mathbb{C}$ is such that $i^2 = -1$.

Proposition

$\mathbb{Z}[i]$ is a ring: whenever $\alpha, \beta \in \mathbb{Z}[i]$, we also have

$$\alpha + \beta, \ \alpha - \beta, \ \alpha\beta \in \mathbb{Z}[i].$$

Remark

$\mathbb{Z}[i] = \{P(i) \mid P(x) \in \mathbb{Z}[x]\}$, whence the notation $\mathbb{Z}[i]$.

The norm

Definition

The norm of $\alpha = a + bi \in \mathbb{Z}[i]$ is

$$N(\alpha) = \alpha\overline{\alpha} = a^2 + b^2.$$

Remark

$N(\alpha) \geqslant 0$, with equality only if $\alpha = 0$.
If $n \in \mathbb{Z} \subset \mathbb{Z}[i]$, then $N(n) = n^2$.

Proposition

For all $\alpha, \beta \in \mathbb{Z}[i]$, $N(\alpha\beta) = N(\alpha)N(\beta)$.

Lemma

An integer $n \in \mathbb{N}$ is a sum of 2 squares iff. it is the norm of a Gaussian integer.

Units

Definition

A Gaussian integer $\alpha \in \mathbb{Z}[i]$ is a unit if it is invertible in $\mathbb{Z}[i]$, meaning there exists $\beta \in \mathbb{Z}[i]$ such that $\alpha\beta = 1$. The set of units of $\mathbb{Z}[i]$ is denoted by $\mathbb{Z}[i]^\times$.

Proposition

Let $\alpha \in \mathbb{Z}[i]$. Then α is a unit iff. $N(\alpha) = 1$.

Proof.

If $\alpha\beta = 1$, then $1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta)$.
Conversely, if $N(\alpha) = 1$, then $\alpha\beta = 1$ for $\beta = \overline{\alpha} \in \mathbb{Z}[i]$. □

Units

Definition

A Gaussian integer $\alpha \in \mathbb{Z}[i]$ *is a* unit *if it is invertible in* $\mathbb{Z}[i]$*, meaning there exists* $\beta \in \mathbb{Z}[i]$ *such that* $\alpha\beta = 1$*. The set of units of* $\mathbb{Z}[i]$ *is denoted by* $\mathbb{Z}[i]^\times$*.*

Proposition

Let $\alpha \in \mathbb{Z}[i]$*. Then* α *is a unit iff.* $N(\alpha) = 1$*.*

Corollary

$$\mathbb{Z}[i]^\times = \{1, -1, i, -i\}.$$

Remark

We could say that in $\mathbb{Z}$, the units are 1 and -1; hence the term “unit”.

Arithmetic with the Gaussian integers

Euclidean division

Theorem

Let $\alpha, \beta \in \mathbb{Z}[i]$ *with* $\beta \neq 0$. *There exists* $\gamma, \rho \in \mathbb{Z}[i]$ *such that*

$$\alpha = \beta\gamma + \rho \quad \text{and} \quad N(\rho) < N(\beta).$$

Euclidean division

Proof.

Compute $\alpha/\beta = x + yi \in \mathbb{C}$. Let $m, n \in \mathbb{Z}$ such that

$$|x-m| \leqslant \frac{1}{2} \quad \text{and} \quad |y-n| \leqslant \frac{1}{2},$$

and set $\gamma = m + ni$, $\rho = \alpha - \beta\gamma$. Then $\gamma, \rho \in \mathbb{Z}[i]$, and $\alpha = \beta\gamma + \rho$.

Extend the norm to all of $\mathbb{C}$ by $N(\alpha) = \alpha\overline{\alpha}$. Then

$$\frac{N(\rho)}{N(\beta)} = \frac{N(\alpha-\beta\gamma)}{N(\beta)} = N\left(\frac{\alpha}{\beta} - \gamma\right) = N((x+yi)-(m+ni))$$
$$= (x-m)^2 + (y-n)^2 \leqslant \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2},$$

so $N(\rho) \leqslant \frac{1}{2} N(\beta) < N(\beta)$. □

Euclidean division

Theorem

Let $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$. There exists $\gamma, \rho \in \mathbb{Z}[i]$ such that

$$\alpha = \beta\gamma + \rho \quad \text{and} \quad N(\rho) < N(\beta).$$

Example

Let $\alpha = 8 + i$, $\beta = 2 + 3i$. Then

$$\frac{\alpha}{\beta} = \frac{8+i}{2+3i} = \frac{(8+i)(2-3i)}{(2+3i)(2-3i)} = \frac{19}{13} - \frac{22}{13}i \approx 1 - 2i,$$

so we set $\gamma = 1 - 2i$ and $\rho = \alpha - \beta\gamma = 2i$.
We can check that $N(\rho) = 4 < N(\beta) = 13$.

Remark

In general, the pair (γ, ρ) is not unique. But it will not matter for what we have in mind!

Consequences of Euclidean division: gcd

Definition

Let $\alpha, \beta \in \mathbb{Z}[i]$. We say that $\alpha \mid \beta$ if there exists $\gamma \in \mathbb{Z}[i]$ such that $\beta = \alpha\gamma$.

Lemma (Important)

For all $\alpha \in \mathbb{Z}[i]$, we have $\alpha \mid N(\alpha)$.
If $\alpha \mid \beta$ in $\mathbb{Z}[i]$, then $N(\alpha) \mid N(\beta)$ in $\mathbb{Z}$.

Consequences of Euclidean division: gcd

Definition

We say that $\alpha, \beta \in \mathbb{Z}[i]$ are associate if $\alpha \mid \beta$ and $\beta \mid \alpha$.

Lemma

α, β are associate $\iff \beta = \upsilon\alpha$ for some $\upsilon \in \mathbb{Z}[i]^\times$.

Proof.

$\Leftarrow$: If $\beta = \upsilon\alpha$, then $\alpha \mid \beta$, and also $\alpha = \upsilon^{-1}\beta$ so $\beta \mid \alpha$.

$\Rightarrow$: $\beta = \xi\alpha$ and $\alpha = \eta\beta$ for some $\xi, \eta \in \mathbb{Z}[i]$, so $\alpha = \xi\eta\alpha$.
If $\alpha \neq 0$ then $\xi\eta = 1$ so $\xi, \eta \in \mathbb{Z}[i]^\times$.
If $\alpha = 0$ then $\beta = \xi\alpha = 0$ so also OK. □

Consequences of Euclidean division: gcd

Definition

Let $\alpha, \beta, \gamma \in \mathbb{Z}[i]$. We say that γ is a gcd of α, β if for all $\delta \in \mathbb{Z}[i]$, $\quad \delta \mid \gamma \Longleftrightarrow \delta \mid \alpha$ *and* $\delta \mid \beta$.

Alternatively, a gcd is a common divisor whose norm is as large as possible.

Theorem

Gcd's exist, can be found by the Euclidean algorithm, and are unique up to multiplication by units.

Consequences of Euclidean division: gcd

Theorem

Gcd's exist, can be found by the Euclidean algorithm, and are unique up to multiplication by units.

Proof.

If $\alpha = \beta\gamma + \rho$, then $\mathrm{Div}(\alpha, \beta) = \mathrm{Div}(\beta, \rho) \rightsquigarrow$ Gcd's exist and can be found by Euclidean algorithm.
Uniqueness: suppose α, β are not both 0, and let γ, γ' be two gcd's. Then $\gamma \mid \gamma'$ and $\gamma' \mid \gamma$. □

Corollary

Given α, β, the elements of $\mathbb{Z}[i]$ of the form $\alpha\xi + \beta\eta$ ($\xi, \eta \in \mathbb{Z}[i]$) are exactly the multiples of $\gcd(\alpha, \beta)$.

Gauss's lemma: if $\alpha \mid \beta\gamma$ and $\gcd(\alpha, \beta) = 1$, then $\alpha \mid \gamma$.

Consequences of Euclidean division: factorisation

Definition (Gaussian primes)

An element $\pi \in \mathbb{Z}[i]$ is irreducible if $\pi \notin \mathbb{Z}[i]^\times$ and whenever $\pi = \alpha\beta$, then one of α, β is a unit.

Example

If $N(\alpha)$ is a prime number, then α is irreducible.
Indeed, if $\alpha = \beta\gamma$, then $N(\alpha) = N(\beta)N(\gamma)$.

⚠ The converse is not true!

Consequences of Euclidean division: factorisation

Theorem

Every nonzero $\alpha \in \mathbb{Z}[i]$ may be factored as

$$\alpha = \upsilon \pi_1 \cdots \pi_r$$

with $\upsilon \in \mathbb{Z}[i]^\times$ and the π_j irreducible.

If $\alpha = \upsilon' \pi'_1 \cdots \pi'_s$, then $r = s$ and each π'_j is associate to a π_k.

Proof.

Euclid's lemma holds in $\mathbb{Z}[i]$. □

Example

$2 = (-i)(1+i)^2 = i(1-i)^2$.
$1 \pm i$ is irreducible since it has norm 2 which is prime. These are the same factorisations since $1+i = i(1-i)$.

Classification of the Gaussian primes

Decomposition of prime numbers in $\mathbb{Z}[i]$

Theorem

Let $p \in \mathbb{N}$ be prime.

- *(Split case) If $p \equiv +1 \bmod 4$, then $p = \pi\overline{\pi}$ for some irreducible $\pi \in \mathbb{Z}[i]$ of norm p, and $\pi, \overline{\pi}$ are not associate.*
- *(Inert case) If $p \equiv -1 \bmod 4$, then p remains irreducible in $\mathbb{Z}[i]$.*
- *(Special case) $2 = (1+i)(1-i) = (-i)(1+i)^2$.*

Example

$3 \in \mathbb{Z}[i]$ is an irreducible whose norm $N(3) = 3^2$ is composite.

$5 = (2+i)(2-i)$.

Decomposition of prime numbers in $\mathbb{Z}[i]$

Lemma

Let $p \in \mathbb{N}$ be prime, and suppose p becomes reducible in $\mathbb{Z}[i]$. Then p factors as $p = \pi\overline{\pi}$, where $\pi \in \mathbb{Z}[i]$ is irreducible of norm p; besides $\pi = a + bi$ is such that a, b are coprime in $\mathbb{Z}$.

Lemma

If $p \equiv -1 \bmod 4$, then p is irreducible in $\mathbb{Z}[i]$.

Lemma

If $p \equiv +1 \bmod 4$, then p splits in $\mathbb{Z}[i]$.

Lemma

Suppose $p = \pi\overline{\pi}$. If $\overline{\pi}$ and π are associate, then $p = 2$.

Decomposition of prime numbers in $\mathbb{Z}[i]$

Lemma

Let $p \in \mathbb{N}$ be prime, and suppose p becomes reducible in $\mathbb{Z}[i]$. Then p factors as $p = \pi\overline{\pi}$, where $\pi \in \mathbb{Z}[i]$ is irreducible of norm p; besides $\pi = a + bi$ is such that a, b are coprime in $\mathbb{Z}$.

Proof.

We have $p = \upsilon\pi_1 \cdots \pi_r$ where $r \geqslant 2$. Then

$$p^2 = N(p) = N(\upsilon)N(\pi_1)\cdots N(\pi_r),$$

so $r = 2$ and $N(\pi_1) = N(\pi_2) = p$. Thus $\pi_1\overline{\pi_1} = p$.

Write $\pi_1 = a + bi$, $a, b \in \mathbb{Z}$. If $d \mid a, b$, then $d \mid \pi_1$,
so $d^2 = N(d) \mid N(\pi_1) = p$, so $d = \pm 1$. □

Decomposition of prime numbers in $\mathbb{Z}[i]$

Lemma

If $p \equiv -1 \bmod 4$*, then* p *is irreducible in* $\mathbb{Z}[i]$*.*

Proof.

Suppose p becomes reducible in $\mathbb{Z}[i]$. Then $p = \pi\overline{\pi}$, where $\pi = a + bi$ is such that $a^2 + b^2 = p$ and $\gcd(a, b) = 1$.

We cannot have both $p \mid a$ and $p \mid b$; WLOG $p \nmid a$.
Then $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, so $c = b/a \in \mathbb{Z}/p\mathbb{Z}$ satisfies $c^2 + 1 = 0$, whence $\left(\frac{-1}{p}\right) = +1$; contradiction since $p \equiv -1 \bmod 4$. □

Decomposition of prime numbers in $\mathbb{Z}[i]$

Lemma

If $p \equiv +1 \bmod 4$*, then* p *splits in* $\mathbb{Z}[i]$*.*

Proof.

Since $p \equiv 1 \bmod 4$, we have $\left(\frac{-1}{p}\right) = +1$, so there exists $c \in \mathbb{Z}$ such that $c^2 + 1 = kp$ for some $k \in \mathbb{Z}$.
Then $kp = (c+i)(c-i)$, so $p \mid (c+i)(c-i)$ in $\mathbb{Z}[i]$.
If p were irreducible, then Euclid's lemma would force $p \mid (c \pm i)$; then $\frac{c}{p} \pm \frac{1}{p} i \in \mathbb{Z}[i]$, absurd. □

Decomposition of prime numbers in $\mathbb{Z}[i]$

Lemma

Suppose $p = \pi\overline{\pi}$. If $\overline{\pi}$ and π are associate, then $p = 2$.

Proof.

Write $\pi = a + bi$; then $\gcd(a, b) = 1$ so $au + bv = 1$ for some $u, v \in \mathbb{Z}$.
As $\pi \mid (\pi + \overline{\pi}) = 2a$ and $\pi \mid -i(\pi - \overline{\pi}) = 2b$, we have

$$\pi \mid (2au + 2bv) = 2.$$

Therefore $p = N(\pi) \mid N(2) = 4$. □

Classification of Gaussian primes

Proposition

Up to associates, we have seen all the irreducibles of $\mathbb{Z}[i]$ in the previous theorem.

Proof.

Let $\pi \in \mathbb{Z}[i]$ be irreducible. Then $\pi \mid N(\pi) \in \mathbb{N}$ which is a product of prime numbers. By Euclid's lemma, π divides one of these prime numbers. □

Classification of Gaussian primes

Proposition

Up to associates, we have seen all the irreducibles of $\mathbb{Z}[i]$ in the previous theorem.

Corollary

Let $\pi \in \mathbb{Z}[i]$ be irreducible. Then either

- $N(\pi) = 2$, *and then π is associate to $1+i$, or*
- $N(\pi)$ *is a prime* $p \equiv +1 \bmod 4$, *and π is associate to exactly one of π' and $\overline{\pi'}$, where $p = \pi'\overline{\pi'}$, or*
- $N(\pi) = q^2$ *where* $q \equiv -1 \bmod 4$ *is prime, and π is associate to q.*

Practical factoring in $\mathbb{Z}[i]$

Example (Factor $\alpha = 27 + 39i$)

We know that $\alpha = \upsilon\pi_1 \cdots \pi_r$ with $\upsilon \in \mathbb{Z}[i]^\times$ and the π_j irreducible. Besides, $\alpha \mid N(\alpha) = 27^2 + 39^2 = 2250 = 2 \times 3^2 \times 5^3$. So $\alpha = \upsilon\pi_2\pi_{3^2}\pi_5\pi_5'\pi_5''$ where $N(\pi_n) = n$.

We already know that we can take $\pi_2 = 1 + i$ and $\pi_{3^2} = 3$.

We have $5 = \pi\overline{\pi}$, $\pi = 2 + i$; so each of π_5, π_5', π_5'' may be taken to be exactly one of $2 + i, 2 - i$.
If some were $2 + i$ and some were $2 - i$, then we would have $5 = (2 + i)(2 - i) \mid \alpha$, absurd. So it's either all $2 + i$ or all $2 - i$.
We compute $\alpha/(2 + i) = \frac{93}{5} + \frac{51}{5} \notin \mathbb{Z}[i]$
(or $\alpha/(2 - i) = 3 + 21i \in \mathbb{Z}[i]$), so it's $2 - i$.

Finally $\upsilon = \frac{\alpha}{(1+i)3(2-i)^3} = i$, whence the complete factorisation

$$\alpha = i(1 + i)3(2 - i)^3.$$

Conclusion and complements

Sums of 2 squares

Theorem

An integer $n = \prod_j p_j^{v_j} \in \mathbb{N}$ *is a sum of 2 squares iff.* v_j *is even whenever* $p_j \equiv -1 \bmod 4$.

Proof.

$\Rightarrow$: If n is a sum of 2 squares, then $n = N(\alpha)$ for some $\alpha \in \mathbb{Z}[i]$. Factor $\alpha = \upsilon \pi_1 \cdots \pi_r$. Then we have $n = N(\alpha) = N(\pi_1) \cdots N(\pi_r)$, and for each j, $N(\pi_j)$ is either 2, or $p \equiv +1 \bmod 4$, or q^2 where $q \equiv -1 \bmod 4$. So $v_q(n)$ must be even for each $q \equiv -1 \bmod 4$.

$\Leftarrow$: Suppose $n = 2^a \prod_{p_j \equiv +1 \bmod 4} p_j^{b_j} \prod_{q_j \equiv -1 \bmod 4} q_j^{2c_j}$. Then letting

$$\alpha = (1+i)^a \prod_{p_j \equiv +1 \bmod 4} \pi_j^{b_j} \prod_{q_j \equiv -1 \bmod 4} q_j^{c_j}$$ where $p_j = \pi_j \overline{\pi_j}$,

we have $N(\alpha) = n$. □

Sums of 2 squares

Theorem

An integer $n = \prod_j p_j^{v_j} \in \mathbb{N}$ *is a sum of 2 squares iff.* v_j *is even whenever* $p_j \equiv -1 \bmod 4$.

Remark

Let $m, n \in \mathbb{N}$. If both m and n are sums of 2 squares, then so is mn.

Proof 1.

$$(a^2 + b^2)(A^2 + B^2) = (aA - bB)^2 + (aB + bA)^2.$$

□

Proof 2.

$$N(\alpha)N(\beta) = N(\alpha\beta).$$

□

Algebraic number theory (not examinable)

Instead of $\mathbb{Z}[i]$, we could have introduced

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}.$$

Then, letting $N(a+b\sqrt{2}) = (a+b\sqrt{2})(a-b\sqrt{2}) = a^2 - 2b^2$, studying the decomposition of prime numbers in $\mathbb{Z}[\sqrt{2}]$ would give information on which integers are of the form $a^2 - 2b^2$. However, beware that there is not always a Euclidean division, and thus not always unique factorisation!

Counter-example

In $\mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$, we have

$$6 = 2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$

and all 4 factors are irreducible, yet non-associate.
$\rightsquigarrow$ Integers of the form $a^2 + 5b^2$ are more difficult to characterise!

Sums of 4 squares (not examinable)

Introduce the quaternionic order

$$\mathcal{O} = \{a + bI + cJ + dK \mid a, b, c, d \in \mathbb{Z}\}$$

$$IJ = -JI = K,\ JK = -KJ = I,\ KI = -IK = J,\ \ I^2 = J^2 = K^2 = -1.$$

Given $\alpha = a + bI + cJ + dK \in \mathcal{O}$, define $\overline{\alpha} = a - bI - cJ - dK$ and

$$N(\alpha) = \alpha\overline{\alpha} = a^2 + b^2 + c^2 + d^2.$$

Then we have $N(\alpha\beta) = N(\alpha)N(\beta)$.

Possible interpretation:

$$I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},\ N(\alpha) = \det \alpha.$$

We find that every prime $p \in \mathbb{N}$ splits in $\mathcal{O}$.

$\rightsquigarrow$ Every integer is a sum of 4 squares.

Sums of 4 squares (not examinable)

Remark

Let $m, n \in \mathbb{N}$. If both m and n are sums of 4 squares, then so is mn.

Proof 1.

$$(a^2+b^2+c^2+d^2)(A^2+B^2+C^2+D^2) =$$
$$(aA-bB-cC-dD)^2+(aB+bA+cD-dC)^2$$
$$+(aC-bD+cA+dB)^2+(aD+bC-cD+dA)^2. \qquad \square$$

Proof 2.

$$N(\alpha)N(\beta) = N(\alpha\beta). \qquad \square$$

Sums of 3 squares

The set of sums of 3 squares is not closed under multiplication!

Counter-example

$2 = 1^2 + 1^2 + 0^2$, and $14 = 3^2 + 2^2 + 1^2$; and yet

$$2 \times 14 = 28 = 4 \times 7 \neq x^2 + y^2 + z^2.$$

This explains why proofs of the theorem for 3 squares are less nice.