# L'anello $\mathbb{Z}[i]$ e sue applicazioni

Marco Damele

12 gennaio 2024

# Capitolo 1

# L'anello degli interi di Gauss.

## 1.1 Definizione di $\mathbb{Z}[i]$ e norma.

Nel seguito $\mathbb{C}$ è considerato munito delle operazioni usuali di somma e prodotto.

**Definizione 1.** *L'insieme degli interi di Gauss è l'insieme:*

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

*e un generico elemento di $\mathbb{Z}[i]$ è detto intero di Gauss.*

**Proposizione 1.** *$\mathbb{Z}[i]$ è un sottoanello di $\mathbb{C}$.*

*Dimostrazione.* Banalmente $(\mathbb{Z}[i], +)$ è un sottogruppo di $\mathbb{C}$ dato che, se $a + ib$ e $c + id$ sono elementi di $\mathbb{Z}[i]$, allora $(a + ib) + (c + id) = (a + c) + i(b + d) \in \mathbb{Z}[i]$ e $-(a + ib) = -a + i(-b) \in \mathbb{Z}[i]$. Inoltre $(a + ib)(c + id) = (ac - bd) + i(ad + bc) \in \mathbb{Z}[i]$ e poi $1_{\mathbb{C}} = 1 + i0 \in \mathbb{Z}[i]$. $\square$

Segue dunque immediatamente dalla proposizione anteriore che $(\mathbb{Z}[i],+,\cdot)$ è un dominio di integrità (anello commutativo unitario in cui $ab = 0$ implica $a = 0$ o $b = 0$). La prima domanda cui siamo interessati a rispondere è: quali sono le unità di $\mathbb{Z}[i]$ (cioè gli elementi invertibili di $\mathbb{Z}[i]$ rispetto al prodotto $\cdot$)? Per farlo cogliamo l'occasione per definire un oggetto importante, la norma di un intero di Gauss.

**Definizione 2.** *Se $\alpha = a + ib \in \mathbb{Z}[i]$, è detta norma di $\alpha$ il numero naturale $N(\alpha) = a^2 + b^2$.*

Con un calcolo diretto si mostra che l'applicazione $N\colon \mathbb{Z}[i] \longrightarrow \mathbb{N}$ è moltiplicativa: $\forall \alpha, \gamma \in \mathbb{Z}[i]$, $N(\alpha\gamma) = N(\alpha)N(\gamma)$. Questo fatto ci permette di dimostrare in maniera agevole la seguente proposizione.

**Proposizione 2.** *Le unità di $\mathbb{Z}[i]$ sono $1$, $-1$, $i$, $-i$.*

*Dimostrazione.* Ovviamente $1$, $-1$, $i$ e $-i$ sono unità di $\mathbb{Z}[i]$. Mostriamo che sono le uniche. Sia $\alpha = a + ib$ un'unità di $\mathbb{Z}[i]$ e sia $\gamma$ il suo inverso moltiplicativo, quindi $\alpha\gamma = 1$. Allora $N(\alpha\gamma) = 1$ da cui $N(\alpha)N(\gamma) = 1$ ovvero $N(\alpha) = 1$. Segue che $a^2 + b^2 = 1$ e quindi le quattro possibilità: $a = 1$, $b = 0$, che portano ad $\alpha = 1$; $a = -1$, $b = 0$, che portano ad $\alpha = -1$; $a = 0$, $b = 1$, che portano ad $\alpha = i$; e l'ultima, $a = 0$, $b = -1$, che porta ad $\alpha = -i$. $\square$

## 1.2 $\mathbb{Z}[i]$ è un dominio euclideo.

In $\mathbb{Z}$ vale la proprietà notevole che ogni intero si scrive in maniera unica (a meno di moltiplicare per 1 o $-1$) come prodotto di potenze di primi distinti. Ci si domanda se tale proprietà valga anche in $\mathbb{Z}[i]$. Come vedremo tra poco tale proprietà è rispettata. Diamo inanzitutto la definizione di primo in $\mathbb{Z}[i]$:

**Definizione 3.** *$\alpha \in \mathbb{Z}[i] \backslash \{0, 1, -1, i, -i\}$ è detto primo se $p = ab$ implica che $a$ è un'unità oppure $b$ è un'unità.*

**Osservazione 1.** *In generale se $p$ è un primo di $\mathbb{Z}$ non è necessariamente primo in $\mathbb{Z}[i]$. Si pensi ad esempio a 5, che è primo in $\mathbb{Z}$ ma non in $\mathbb{Z}[i]$, dato che $5 = (1-2i)(1+2i)$. Anche 2 è primo in $\mathbb{Z}$ ma non in $\mathbb{Z}[i]$ dato che $2 = (1-i)(1+i)$. Ci sono tuttavia primi di $\mathbb{Z}$ che sono primi anche in $\mathbb{Z}[i]$. Ad esempio 3 è un primo sia in $\mathbb{Z}$ che in $\mathbb{Z}[i]$. Per vedere questo fatto ragioniamo per assurdo. Supponiamo che $3 = ab$ con $a, b \in \mathbb{Z}[i]$ e $a$, $b$ non unità di $\mathbb{Z}[i]$ e quindi $N(a), N(b) > 1$. Abbiamo che $9 = N(3) = N(a)N(b)$ da cui $N(a) = 3$ e $N(b) = 3$. Se quindi $a = x + iy$ abbiamo $x^2 + y^2 = 3$, da cui $y^2 = 3 - x^2$. Deduciamo che $x \in \{-1, 0, 1\}$. Se $x = -1$ o $x = 1$ troviamo $y^2 = 2$ che è assurdo essendo 2 primo in $\mathbb{Z}$; se $x = 0$ troviamo $y^2 = 3$ che è assurdo essendo 3 primo in $\mathbb{Z}$. Più avanti dimostreremo che se $p$ è un primo di $\mathbb{Z}$ tale che $p = 3 \pmod 4$, allora $p$ è primo in $\mathbb{Z}[i]$.*

Per stabilire se un intero di Gauss è primo risulta utile anche la seguente:

**Proposizione 3.** *Sia $\alpha \in \mathbb{Z}[i]$. Se $N(\alpha)$ è primo in $\mathbb{Z}$, allora $\alpha$ è primo in $\mathbb{Z}[i]$.*

*Dimostrazione.* Supponiamo che $\alpha = ab$ con $a, b$ interi di Gauss. Siccome $N(\alpha) = N(a)N(b)$ e $N(\alpha)$ è primo deduciamo che uno tra $N(a)$ e $N(b)$ vale 1 e quindi che uno tra $a$ e $b$ è un'unità. $\square$

**Osservazione 2.** *Il viceversa non è vero. Se $\alpha$ è primo in $\mathbb{Z}[i]$, non necessariamente $N(\alpha)$ è primo in $\mathbb{Z}$. Si pensi ad esempio a 3 che è primo in $\mathbb{Z}[i]$ ma ha norma 9.*

**Definizione 4.** *Siano $\alpha, \beta \in \mathbb{Z}[i]$. Diciamo che $\alpha$ divide $\beta$ e scriviamo $\alpha \mid \beta$ se $\beta = \alpha\gamma$ per qualche $\gamma \in \mathbb{Z}[i]$.*

**Osservazione 3.** *Osserviamo che se $\alpha, \beta \in \mathbb{Z}[i]$ tali che $\alpha \mid \beta$, allora $N(\alpha) \mid N(\beta)$. Infatti $\beta = \alpha\gamma$ con $\gamma \in \mathbb{Z}[i]$, da cui segue che $N(\beta) = N(\alpha)N(\gamma)$ e quindi $N(\alpha)$ divide $N(\beta)$.*

Ricordiamo allora la nozione di massimo comun divisore:

**Definizione 5.** *Siano $\alpha, \beta \in \mathbb{Z}[i]$ non nulli. Un massimo comun divisore di $\alpha$ e $\beta$ è un elemento $d \in \mathbb{Z}[i]$ tale che $d \mid \alpha$, $d \mid \beta$ e $d$ ha norma massimale.*

**Osservazione 4.** *Osserviamo che se $\alpha$ e $\beta$ ammettono come massimo comun divisore $d$ allora anche $-d$, $id$, $-id$ sono massimi comun divisori per $\alpha$ e $\beta$. In effetti questi sono gli unici massimi comun divisori di $\alpha$ e $\beta$. Infatti se $d$ e $d'$ sono due massimi comun divisori, allora $d$ divide $d'$ (mostrarlo per esercizio) quindi $d' = dk$ con $k$ intero di Gauss. Segue che $N(d') = N(d)N(k) = N(d')N(k)$ da cui $N(k) = 1$ e quindi $k$ è un'unità.*

**Definizione 6.** *Siano $\alpha, \beta \in \mathbb{Z}[i]$ non nulli. Essi sono detti coprimi, e scriviamo $(\alpha, \beta) = 1$, se 1 è un massimo comun divisore di $\alpha$ e $\beta$.*

Enunciamo un teorema, dovuto a Bezout, che si dimostra in maniera analoga a a quanto si fa in $\mathbb{Z}$.

**Teorema 1.** *Siano* $\alpha, \beta \in \mathbb{Z}[i]$ *non nulli e* $d$ *un massimo comun divisore tra* $\alpha$ *e* $\beta$. *Allora esistono* $x, y \in \mathbb{Z}[i]$ *tali che* $d = \alpha x + \beta y$. *Inoltre* $\alpha$ *e* $\beta$ *sono coprimi se e solo se esistono* $x, y \in \mathbb{Z}[i]$ *tali che* $1 = \alpha x + \beta y$.

Ricordiamo la seguente:

**Definizione 7.** *Sia* $R$ *un dominio di integrità.* $R$ *è detto dominio euclideo se esiste una funzione (detta funzione euclidea)* $\delta\colon R \setminus \{0\} \longrightarrow \mathbb{N}$ *tale che:*

$$\forall a, b \in R : b \neq 0,\ \exists c, r \in R : a = cb + r,\ \text{con } \delta(r) < \delta(b) \vee r = 0.$$

**Teorema 2.** $\mathbb{Z}[i]$ *è un dominio euclideo.*

*Dimostrazione.* Mostriamo che $N\colon\ \mathbb{Z}[i] \setminus \{0\} \longrightarrow \mathbb{N}$ è una funzione euclidea. Siano $a, b \in \mathbb{Z}[i] : b \neq 0$. Se $b$ divide $a$ allora $a = cb$ per qualche $c \in \mathbb{Z}[i]$, e quindi la tesi è soddisfatta con $c$ ed $r = 0$. Se invece $b$ non divide $a$ allora esiste $x + iy \in \mathbb{Z}[i]$ tale che $N(ab^{-1} - (x + iy)) \leq \sqrt{2}/2 < 1$, dove $b^{-1}$ è l'inverso moltiplicativo di $b$ in $\mathbb{C}$. Poniamo allora $c = x + iy$ e $r = a - cb$. Sia ora $M\colon\ \mathbb{C} \longrightarrow \mathbb{N},\ z = m + in \longmapsto m^2 + n^2$. Similmente a come si fa per $N$ si mostra che $M$ è moltiplicativa e banalmente $N$ ristretta a $\mathbb{Z}[i]$ coincide con $N$. Adesso $c$ ed $r$ sono elementi di $\mathbb{Z}[i]$ tali che $a = cb + r$ e poiché $M(rb^{-1}) = M(ab^{-1} - c) = M(ab^{-1} - (x + iy)) \leq \sqrt{2}/2 < 1$ si trova $N(r) = M(r) < M(b) = N(b)$. $\square$

Ricordando che i domini euclidei sono domini a fattorizzazione unica, abbiamo il seguente corollario:

**Corollario 1.** $\mathbb{Z}[i]$ *è un dominio a fattorizzazione unica (UFD). Ovvero, se* $\alpha \in \mathbb{Z}[i] \setminus \{0, 1, -1, i, -i\}$, *allora esistono* $p_1, \ldots, p_n$ *primi di* $\mathbb{Z}[i]$ *tali che:*

$$\alpha = p_1 \cdots p_n.$$

*Inoltre, se* $q_1, \ldots, q_m$ *sono primi di* $\mathbb{Z}[i]$ *tali che* $\alpha = q_1 \cdots q_m$, *allora* $n = m$ *e* $\forall i = 1, \ldots, n\ \exists j \in \{1, \ldots, n\}$ *tale che* $p_i = uq_j$ *per qualche unità* $u$ *di* $\mathbb{Z}[i]$.

**Esercizio 1.2.1.** *Nel prossimo capitolo faremo ampio uso dei seguenti fatti che lasciamo come stimolanti esercizi per il lettore (alcuni sono immediati).*

1. *Provare che, se* $\alpha \in \mathbb{Z}[i]$, *allora* $N(\alpha) = 0 \pmod 2 \iff 1 + i \mid \alpha$.
2. *Se* $\alpha, \beta \in \mathbb{Z}[i]$ *con* $N(\beta) \mid N(\alpha)$, *è vero che* $\beta \mid \alpha$?
3. *Se* $\alpha, \beta \in \mathbb{Z}[i]$ *con* $N(\beta) = N(\alpha)$, *è vero che* $\beta = u\alpha$ *per qualche unità* $u$ *di* $\mathbb{Z}[i]$?
4. *Se* $\alpha, \beta \in \mathbb{Z}[i]$ *con* $(N(\beta), N(\alpha)) = 1$, *provare che* $(\alpha, \beta) = 1$.
5. *Siano* $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ *con* $(\alpha, \beta) = 1$ *e* $\alpha \mid \beta\gamma$. *Provare che* $\alpha \mid \gamma$.
6. *Siano* $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ *con* $(\alpha, \beta) = 1$, $\alpha \mid \gamma$ *e* $\beta \mid \gamma$. *Provare che* $\alpha\beta \mid \gamma$.
7. *Se* $\alpha \in \mathbb{Z}[i] \setminus \{0\}$ *e* $d \mid \alpha$ *e* $N(d) = N(\alpha)$, *provare che* $d = u\alpha$ *per qualche unità* $u$ *di* $\mathbb{Z}[i]$.

8. *Se* $\alpha \in \mathbb{Z}[i]$ *e* $u$ *unità allora* $(\alpha, u) = 1$.

9. *Se* $\alpha, \beta \in \mathbb{Z}[i]$ *ammettono un'unita come massimo comun divisore, allora sono coprimi.*

10. *Fattorizzare in primi* $3 + 4i$ *e* $2319 + 1694i$.

11. *Se* $\alpha, \beta \in \mathbb{Z}[i]$ *e* $d$ *è un loro massimo comun divisore, allora* $d \mid \alpha + \beta$, $d \mid \alpha - \beta$ *e* $d \mid \alpha\beta$.

12. *Provare che* $1 + i$ *è primo.*

13. *Se* $u \in \mathbb{Z}[i]$ *è un'unità, dimostrare che esiste* $v \in \mathbb{Z}[i]$ *tale che* $u = v^3$.

# Capitolo 2

# Applicazioni alle equazioni diofantee.

Per noi un'equazione diofantea è un'equazione della forma $P(x_1, \ldots, x_n) = 0$, essendo $P(x_1, \ldots, x_n)$ un polinomio a coefficienti interi in $n$ incognite. Ovvero formalmente $P(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$. Risolvere l'equazione diofantea $P(x_1, \ldots, x_n) = 0$ significa trovare tutti gli interi $a_1, \ldots, a_n$ tali che $P(a_1, \ldots, a_n) = 0$. Generalmente, risolvere un'equazione diofantea non è affatto semplice. Si pensi alla celebre equazione diofantea proposta da Fermat: $x^n + y^n = z^n$ con $n$ naturale maggiore di 2. Prima di essere completamente risolta, si sono dovuti attendere più di 300 anni. Con la teoria sviluppata per l'anello degli interi di Gauss $\mathbb{Z}[i]$, possiamo risolvere alcune equazioni diofantee che a prima acchito possono sembrare ostiche.

## 2.1 Le terne Pitagoriche.

La prima equazione diofantea che vogliamo studiare è $x^2 + y^2 = z^2$. Ovvero vogliamo determinare tutte le terne di interi $(A, B, C)$ soluzioni dell'equazione $x^2+y^2 = z^2$, ovvero tali che $A^2 + B^2 = C^2$. Banalmente le terne $(0, k, k)$ e $(k, 0, k)$, al variare di $k$ in $\mathbb{Z}$, sono soluzione. Tuttavia esistono anche altre terne di soluzioni, come $(3, 4, 5)$. Vogliamo determinarle tutte nel caso $(A, B) = 1$. Sebbene ci siano vari metodi per farlo, noi useremo il fatto che $\mathbb{Z}[i]$ è un dominio a fattorizzazione unica. Per lo studio più dettagliato sulle terne pitagoriche si rimanda il lettore alle note "L'ultimo teorema di Fermat nel caso $n = 4k$" che si trova nei file PDF del gruppo Facebook "Problemi di Matematica".

**Teorema 3.** *Se $A, B, C$ sono interi tali che $A^2 + B^2 = C^2$ e $(A, B) = 1$, allora esistono $m, n$ interi tali che $A = m^2 - n^2$, $B = 2mn$, $C = m^2 + n^2$ oppure $A = 2mn$, $B = m^2 - n^2$, $C = m^2 + n^2$. Viceversa, per ogni $m, n \in \mathbb{Z}$, si ha $(m^2 - n^2)^2 + (2mn)^2 = (m^2 + n^2)^2$.*

*Dimostrazione.* Abbiamo $(A - iB)(A + iB) = C^2$. Ma $A - iB$ e $A + iB$ sono coprimi in $\mathbb{Z}[i]$. Infatti, sia $d$ un massimo comun divisore tra essi. Proviamo che $d$ è unità. Poiché $d \mid A - iB$ e $d \mid A + iB$, allora $d$ divide la loro somma e la loro differenza: $d \mid 2A$ e $d \mid i2B$ e quindi $d \mid 2A$ e $d \mid 2B$ (poiché $(d, i) = 1$). Se proviamo che $(d, 2) = 1$ allora $d \mid A$ e $d \mid B$ ed essendo $A$ e $B$ coprimi in $\mathbb{Z}$ (e quindi coprimi anche in $\mathbb{Z}[i]$) si avrebbe $d$ unità. Sia $M$ un massimo comun divisore tra $d$ e 2, e supponiamo per assurdo che $M$ non sia un unità. Abbiamo che $M \mid 2 = -i(1 + i)^2$ quindi $M \mid (1 + i)^2$ (poiché $(M, -i) = 1$). Adesso vediamo che $1 + i$ divide $M$. Di fatto sia $R$ un massimo comun divisore tra $M$ e $1 + i$. Se $R$ è un'unità, allora $(M, 1 + i) = 1$, e segue che $M \mid 1 + i$. Se invece $R$ non è unità allora, poiché $R$ divide $1 + i$ si avrebbe $1 + i = uR$, e quindi $R = v(1 + i)$ con $v$ unità. Allora $1 + i$ divide $R$, da cui segue che $N(R)$ è pari. Tuttavia $R$ divide $M$ quindi

$N(R)$ divide $N(M)$, da cui segue che $N(M)$ è pari, ma $M$ divide $d$ quindi $N(d)$ è pari ma $d$ divide $C^2$, quindi $N(d)$ divide $N(C^2) = C^4$, da cui segue che $C^4$ è pari, e quindi $C$ è pari. Allora, essendo $A$ e $B$ coprimi in $\mathbb{Z}$, si ha che $A = 1 \pmod 2$e $B = 1 \pmod 2$, da cui $A^2 = 1 \pmod 4$ e $B^2 = 1 \pmod 4$, da cui segue che $C^2 = 2 \mod 4$, che è assurdo perché i quadrati modulo 4 sono solo 0 e 1. Conseguentemente $R$ è unità e quindi $M$ divide $1+i$. Allora non essendo $M$ unità, si ha che $M = h(1+i)$ con $h$ unità e si perviene quindi all'assurdo che $C$ è pari. Conseguentemente $M$ è unità e quindi $(d, 2) = 1$ e cioè $d$ è unità. Quindi $A - iB$ e $A + iB$ sono coprimi in $\mathbb{Z}[i]$. Adesso, siccome $A - iB$ e $A + iB$ sono coprimi e il loro prodotto è un quadrato per il fatto che $\mathbb{Z}[i]$ è UFD esiste un unità $u$ e due interi $c, d$ tali che $A + iB = u(m + in)^2 = u(m^2 - n^2 + i2mn)$. Di conseguenza, identificando parte reale e immaginaria se:

1. $u = 1$: troviamo $A = m^2 - n^2$, $B = 2mn$, $C = m^2 + n^2$;
2. $u = -1$: troviamo $A = n^2 - m^2$, $B = 2(-m)n$, $C = m^2 + n^2$;
3. $u = i$: troviamo $A = 2(-m)n$, $B = m^2 - n^2$, $C = m^2 + n^2$;
4. $u = -i$: troviamo $A = 2mn$, $B = n^2 - m^2$, $C = m^2 + n^2$.

In ogni caso esistono sempre due interi $c, d$ tali che $A = c^2 - d^2$, $B = 2cd$, $C = c^2 + d^2$, oppure $A = 2cd$, $B = c^2 - d^2$, $C = c^2 + d^2$. Il viceversa del teorema è immediato. □

## 2.2 Una cubica

Un'equazione diofantea simile alla precedente è la seguente: $x^2 + y^2 = z^3$. Anche per questa, usiamo la fattorizzazione unica di $\mathbb{Z}[i]$ per ricavare tutte le terne primitive cioè quelle per cui $(x, y) = 1$.

**Teorema 4.** *Se $a, b, c$ sono interi tali che $a^2 + b^2 = c^3$ con $(a, b) = 1$, allora esistono $m, n$ interi tali che $a = m^3 - 3mn^2$, $b = 3m^2n - n^3$, $c = m^2 + n^2$. Viceversa per ogni $m, n \in \mathbb{Z}$, $(m^3 - 3mn^2)^2 + (3m^2n - n^3)^2 = (m^2 + n^2)^3$.*

*Dimostrazione.* Il viceversa della dimostrazione è immediato. Adesso osserviamo che $c$ è dispari. Infatti $a$ e $b$ sono coprimi, quindi non possono essere entrambi pari. Se fossero entrambi dispari avremmo che $c^3 = 2 \pmod 8$, che è assurdo. Segue che (a meno di scambiare i nomi) $a$ è pari e $b$ è dispari. Segue che $c$ è dispari. Adesso $(a-ib)(a+ib) = c^3$. Tuttavia $a - ib$ e $a + ib$ sono coprimi. Infatti se $d$ è un massimo comun divisore di $a - ib$ e $a + ib$, allora $d$ divide $2a$, $d$ divide $2b$ e $d$ divide $c^3$. Quindi $N(d)$ divide $4a^2$, $4b^2$ e $c^6$. Segue che $N(d)$ è dispari quindi $N(d)$ divide $a^2$ e $N(d)$ divide $b^2$. Ma poiché $a$ e $b$ sono coprimi segue che $N(d)$ è 1 quindi $d$ è unità. Adesso siccome $\mathbb{Z}[i]$ è UFD e ogni unità è il cubo di un intero di Gauss si ha che $a + ib = (m + in)^3$ con $m, n$ interi. Uguagliando parte reale e immaginaria si trova $a = m^3 - 3mn^2$, $b = 3m^2n - n^3$, $c = m^2 + n^2$. □

## 2.3 Un'equazione di Mordell.

Le equazioni di Mordell sono equazioni diofantee della forma $y^2 = x^3 + k$, con $k$ intero non nullo. Si è dimostrato che il numero di soluzioni intere di tale equazione è un numero finito per ogni $k$. Studiamo il caso $k = -1$ usando la fattorizzazione unica di $\mathbb{Z}[i]$.

**Teorema 5.** *L'unica soluzione intera dell'equazione di Mordell $y^2 = x^3 - 1$ è $(1, 0)$.*

*Dimostrazione.* Ovviamente $(1, 0)$ è soluzione. Viceversa mostriamo che se $(x, y)$ è soluzione allora $x = 1$ e $y = 0$. Di fatto $x^3 = (y - i)(y + i)$. Vediamo che $y - i$ e $y + i$ sono coprimi. Sia $d$ un massimo comun divisore tra essi. Allora $d$ divide $2i = (1 + i)^2$ quindi $(1 + i)^2 = \gamma d$ per qualche $\gamma \in \mathbb{Z}[i]$. Per il fatto che $\mathbb{Z}[i]$ è UFD e $1 + i$ è primo, abbiamo che $d$ è unità oppure $d = 1 + i$ oppure $d = (1 + i)^2$. Se per assurdo $d$ non è unità, allora $1 + i$ divide $d$ e quindi $1 + i$ divide $x^3$. Segue che 2 divide $x^6$ e quindi $x$ è pari allora $y^2 + 1 = 0 \pmod 4$ che è assurdo. Quindi $d$ è unità. Allora esistono $m, n$ interi tali che $y + i = (m + in)^3$. Uguagliando parte reale e immaginaria ricaviamo che $y = m(m^2 - 3n^2)$ e $1 = n(3m^2 - n^2)$. Quindi se $n = 1$ si trova $3m^2 = 2$ che è assurdo, quindi $n = -1$ che porta a $m = 0$ e quindi la soluzione $(1, 0)$. □

Usando l'anello $\mathbb{Z}[i]$, Lebesgue ha dimostrato che per ogni naturale $> 1$ l'equazione $y^2 = x^d - 1$ non ha soluzioni con $x, y$ non nulli.

**Esercizio 2.3.1.** *Per i temerari consiglio i seguenti esercizi, un po' più complicati dei precedenti.*

1. *Risolvere l'equazione diofantea $x^2 + 4 = y^3$.*

2. *Risolvere l'equazione diofantea $x^2 + 9 = y^5$.*

3. *Siano $a, b, c, d$ naturali positivi tali che $a^2 + b^2 = cd$: Provare che esistono $x, y, z, w, t$ interi tali che:*

$$a = t(xz - yw),\ b = t(xw + yz),\ c = t(x^2 + y^2),\ d = t(z^2 + w^2).$$

4. *Provare che se $a$ e $b$ sono naturali positivi tali che $ab = c^2 + 1$ per qualche intero $c$ non nullo, allora $a$ e $b$ sono somma di due quadrati.*

5. *Provare che se $p$ è un primo di $\mathbb{Z}$ della forma $4k+1$, allora è somma di due quadrati.*

6. *Risolvere l'equazione diofantea dovuta a Euler: $4xy - x - y = z^2$.*

7. *Trovare tutti i triangoli rettangoli diofantei di $\mathbb{R}^4$, cioè tutte le quaterne $(A, B, C, D)$ di interi tali che $A^2 + B^2 + C^2 = D^2$.*

# Capitolo 3

# Somma di quadrati.

**Teorema 6.** *Sia $p \in \mathbb{Z}$ un primo tale che $p = a^2 + b^2$ con $a, b \in \mathbb{Z}$. Se $p = c^2 + d^2$ con $c, d \in \mathbb{Z}$ allora:*

$a = c \wedge b = d \vee a = -c \wedge b = -d \vee a = d \wedge b = c \vee a = -d \wedge b = -c \vee a = -c \wedge b = d \vee a = -c \wedge b = d \vee a = -d \wedge b = c \vee a = d \wedge b = -c$.

*Dimostrazione.* Abbiamo che, essendo $p$ primo, $a + ib$, $a - ib$, $c + id$, e $c - id$ hanno norma $p$ e quindi sono primi. Poiché poi $(a + ib)(a - ib) = (c + id)(c - id)$, per il fatto che $\mathbb{Z}[i]$ è un dominio a fattorizzazione unica, abbiamo che $a + ib = u(c + id)$ oppure $a + ib = u(c - id)$ per qualche unità $u$. Considerando tutti i possibili casi ($u = 1$, $-1$, $i$, $-i$) si perviene alla conclusione del teorema. $\square$

Possiamo riassumere il teorema precedente dicendo che, se un primo di $\mathbb{Z}$ si scrive come somma di due quadrati $p = a^2 + b^2$, allora c'è un unico modo per fare ciò (a meno, come dice il teorema, di cambiare segno ad $a$ e $b$). Tale proprietà non è pero vera per interi generici. Ad esempio 50 si scrive come $25 + 25 = 5^2 + 5^2$, ma anche come $1^2 + 7^2$. Come applicazione del teorema vediamo il seguente esempio.

**Esempio 1.** *Consideriamo il quinto numero di Fermat: $F_5 = 2^{2^5} + 1 = 4294967297$. Fermat pensava che $F_5$ fosse primo, tuttavia Euler ha trovato che si può scrivere come somma di due quadrati in due modi diversi: $2^{2^5} + 1 = (2^{16})^2 + 1^2 = 62264^2 + 20449^2$. Consegue che $F_5$ non è primo (abbiamo dimostrato che non è primo senza necessariamente trovare un suo divisore non banale!). Sempre Euler trovò che un divisore non banale di $F_5$ era 641.*

Il nostro prossimo obbiettivo è quello di determinare tutti i primi di $\mathbb{Z}$ che sono primi in $\mathbb{Z}[i]$. In parte ci dà la risposta il seguente teorema.

**Teorema 7.** *Sia $p \in \mathbb{Z}^+$ un primo. Allora $p$ è primo in $\mathbb{Z}[i]$ se e solo se $p$ non è somma di due quadrati.*

*Dimostrazione.* Se $p$ è primo in $\mathbb{Z}[i]$ e per assurdo $p = a^2 + b^2$ allora $p(a - ib)(a + ib)$ e quindi $p$ non è primo in $\mathbb{Z}[i]$, assurdo. Se invece $p$ non è somma di due quadrati supponiamo che $p = \alpha\gamma$ con $\alpha, \gamma \in \mathbb{Z}[i]$ non unità. Allora $p^2 = N(\alpha)N(\gamma)$, da cui segue che $N(\alpha) = p$ e quindi se $\alpha = a + ib$ troviamo $p = a^2 + b^2$ che è assurdo. $\square$

La condizione non essere somma di due quadrati non è di facile verifica. Per questo ci viene in soccorso il seguente importante teorema (che ci dice quando un primo di $\mathbb{Z}$ è somma di due quadrati.)

**Teorema 8.** *Sia $p \in \mathbb{Z}^+$ un primo. Allora $p$ è somma di due quadrati $\iff$ $p = 1 \pmod 4$ oppure $p = 2$.*

*Dimostrazione.* Se $p = a^2 + b^2$ e $p \neq 2$, proviamo che $p = 1 \pmod 4$. Se per assurdo così non fosse, essendo $p$ dispari, si avrebbe $p = 3 \pmod 4$ quindi $a^2 + b^2 = 3 \pmod 4$. Seguirebbe che, senza perdere generalità, $a^2 = 1 \pmod 4$ e $b^2 = 2 \pmod 4$, che è assurdo perché i quadrati mod 4 sono 0 e 1. Viceversa, supponiamo che $p = 2$ o $p = 1 \pmod 4$ e proviamo che è somma di due quadrati. Ovviamente 2 soddisfa tale proprietà in quanto $2 = 1^2 + 1^2$. Supponiamo ora che $p = 1 \pmod 4$, diciamo $p - 1 = 4k$ con $k$ naturale non nullo. Consideriamo il polinomio $X^{p-1} - 1 = (X^{(p-1)/2} - 1)(X^{(p-1)/2} + 1) \in \mathbb{Z}_p[X]$. Per il piccolo teorema di Fermat il polinomio $X^{p-1} - 1$ ha $p - 1$ radici in $\mathbb{Z}_p$, mentre il polinomio $X^{(p-1)/2} - 1$ ha al più $(p-1)/2$ radici in $\mathbb{Z}_p$. Segue che il polinomio $X^{(p-1)/2} + 1$ ha almeno una radice in $\mathbb{Z}_p$. Quindi esiste $c \in \mathbb{Z}$ tale che $c^{(p-1)/2} = -1 \pmod p$ e quindi esiste un intero $m$ tale che $m^2 = -1 \pmod p$. Segue che $p \mid m^2 + 1$, cioè $m^2 + 1 = pn$ con $n$ intero e quindi $(m - i)(m + i) = pn$. Supponiamo per assurdo che $p$ non sia somma di due quadrati. Allora per il teorema precedente $p$ è primo in $\mathbb{Z}[i]$. Allora $p \mid m + i$ oppure $p \mid m - i$, da cui segue che esiste qualche intero di Gauss $g$ tale che $m + i = gp$ oppure $m - i = gp$. Ma questo è assurdo in entrambi i casi, perché porterebbe a $p = 1$. Quindi $p$ è somma di due quadrati. □

Segue che:

**Teorema 9.** *Sia $p \in \mathbb{Z}^+$ un primo. Allora $p$ è primo in $\mathbb{Z}[i]$ $\iff$ $p = 3 \pmod 4$.*

**Esercizio 3.0.1.**

*Provare che un intero $n > 1$ è somma di due quadrati $\iff$ $\forall p$, $p$ primo tale che $p \mid n$ e $p = 3 \pmod 4$, allora $p$ compare nella fattorizzazione di $n$ un numero pari di volte.*