# Scomposizione di un numero primo come somma di due quadrati

M. Alessandra De Angelis
Relatore : Prof. Andrea Loi

Università degli studi di Cagliari
Corso di laurea triennale in Matematica

31 Marzo 2015

Il nostro scopo è quello di dimostrare il seguente teorema dovuto a Pierre de Fermat :

*Se $p$ è un primo della forma $4n + 1$, allora $p = a^2 + b^2$, per opportuni interi $a$ e $b$.*

Per dimostrarlo abbiamo bisogno di introdurre alcuni concetti :

1) definizione e proprietà degli anelli euclidei;

2) definizione del dominio degli interi di Gauss.

## Definizione di anello euclideo

Un dominio d'integrità **R** (anello commutativo privo di divisori dello zero) è detto anello euclideo se è possibile definire una funzione

$$\delta : \mathbf{R} \setminus \{\mathbf{0}\} \longrightarrow \mathbb{Z}_+$$

che associa a ogni $a \neq 0$ con $a \in \mathbf{R}$, un intero non negativo $\delta(a)$ tale che per $a,b \in \mathbf{R}$ con $a \neq 0$ e $b \neq 0$ si abbia :

$$\delta(a) \leq \delta(ab) \qquad (1)$$

e inoltre $\exists\ t, r \in \mathbf{R}$ tali che

$$a = tb + r \qquad (2)$$

con $r = 0$ oppure $\delta(r) < \delta(b)$

## Osservazione (1)

A $\delta(0)$ non viene assegnato nessun valore.

## Lemma (1)

*In un anello euclideo* $\mathbf{R}$ *due qualunque elementi ammettono un massimo comune divisore* $d$*. Si ha inoltre che* $d = a\lambda + b\mu$ *per opportuni* $\lambda$ *e* $\mu$ *di* $\mathbf{R}$*.*

## Corollario (1)

*Un anello euclideo possiede un elemento unità.*

## Definizione (1)

*Sia* $\mathbf{R}$ *un anello commutativo con unità. Un elemento* $a \in \mathbf{R}$ *si dice invertibile se* $\exists\ b \in \mathbf{R}$ *tale che* $ab = 1$*.*

### Osservazione (2)

*Se* **R** *è un anello euclideo e* $b \neq 0$ *non è invertibile in* **R** *allora* $\delta(a) < \delta(ab)$.

### Lemma (2)

*Sia* **R** *un dominio di integrità con unità. Supponiamo che per due elementi* $a, b \in$ **R** *si abbia :* $a \mid b$ *e* $b \mid a$. *Allora* $a = ub$ *dove* $u$ *è un elemento invertibile in* **R**.
*Due elementi siffatti vengono detti* **associati**.

### Definizione (2)

*In un anello euclideo* **R** *un elemento non invertibile* $\pi$ *della forma* $\pi = ab$, *con* $a, b \in$ **R**, *si dice primo se* $a$ *oppure* $b$ *è invertibile.*

### Lemma (3)

*In un anello euclideo* $\mathbf{R}$ *ogni elemento o è invertibile oppure si può scrivere come prodotto di un numero finito di elementi primi di* $\mathbf{R}$ *.*

### Lemma (4)

*Se* $\pi$ *è primo in* $\mathbf{R}$ *e* $\pi \mid ab$*, con* $a, b \in \mathbf{R}$ *, allora* $\pi$ *divide* $a$ *oppure* $b$*.*

### Teorema (1)

*Sia* $\mathbf{R}$ *un anello euclideo e* $a \neq 0$ *un elemento non invertibile di* $\mathbf{R}$*. Supponiamo che* $a = \pi_1 \pi_2 ... \pi_n = \pi'_1 \pi'_2 ... \pi'_m$*, dove* $\pi_i$ *e* $\pi'_j$ *sono elementi primi di* $\mathbf{R}$*. Allora* $m = n$ *e ogni* $\pi_i$ *con* $1 \leq i \leq n$ *è associato a qualche* $\pi'_j$ *con* $1 \leq j \leq m$ *e viceversa.*

# Il dominio $\mathbb{J}[\mathrm{i}]$ degli interi di Gauss

$\mathbb{J}[\mathfrak{i}]$ è l'insieme dei numeri della forma $a + \mathfrak{i}b$ con a e b interi e $\mathfrak{i}$ l' unità immaginaria.
Con le usuali operazione di somma e moltiplicazione $(\mathbb{J}[\mathfrak{i}], +, \cdot)$ forma un dominio d'integrità detto *dominio degli interi di Gauss*.

## Teorema (2)

*( $\mathbb{J}[\mathfrak{i}]$,+,·) è un anello euclideo.*

**Dimostrazione :** Definiamo la funzione

$$\delta : \mathbb{J}[\mathfrak{i}] \setminus \{0\} \longrightarrow \mathbb{Z}_+$$

$$x \longmapsto \delta(x) = x\overline{x}$$

dove con $\overline{x}$ indichiamo il complesso coniugato di x.
Se $x = a + \mathfrak{i}b$, $x\overline{x} = a^2 + b^2$

1) Dimostriamo che $\delta(x) \leq \delta(xy) \; \forall \; y \neq 0$.
Osserviamo che $\delta(x) = a^2 + b^2 \geqslant 1$ in quanto somma di quadrati di due interi positivi non nulli.
Inoltre dalle proprietà dei numeri complessi discende che dati $x, y \in \mathbb{J}[\mathfrak{i}]$ si ha

$$\delta(xy) = \delta(x)\delta(y)$$

Unendo le due considerazioni troviamo

$$\delta(x) = \delta(x)1 \leq \delta(x)\delta(y) = \delta(xy)$$

2) Dimostriamo che dati $x, y \in \mathbb{J}[\mathfrak{i}]\ \exists\ t, r \in \mathbb{J}[\mathfrak{i}]$ tali che $y = tx + r$, con $r = 0$ oppure $\delta(r) < \delta(x)$.
Dimostriamolo prima in un caso particolare.
Consideriamo $y \in \mathbb{J}[\mathfrak{i}]$ e $x \in \mathbb{Z}$ della forma $y = a + \mathfrak{i}b$ e $x = n$ (ricordiamo che $\mathbb{Z}$ è un sottoanello di $\mathbb{J}[\mathfrak{i}]$).
Per l'algoritmo della divisione euclidea degli interi possiamo trovare due interi $\mathfrak{u}$ e $\mathfrak{s}$ tali che $a = \mathfrak{u}n + \mathfrak{u}_1$ e $b = \mathfrak{s}n + \mathfrak{s}_1$ dove $\mathfrak{u}_1$ e $\mathfrak{s}_1$ sono due interi tali che

$$|\mathfrak{u}_1| \leq \frac{n}{2} \text{ e } |\mathfrak{s}_1| \leq \frac{n}{2} \tag{3}$$

Si ha allora

$$\begin{aligned} y = a + \mathfrak{i}b &= \mathfrak{u}n + \mathfrak{u}_1 + \mathfrak{i}(\mathfrak{s}n + \mathfrak{s}_1) \\ &= (\mathfrak{u} + \mathfrak{i}\mathfrak{s})n + (\mathfrak{u}_1 + \mathfrak{i}\mathfrak{s}_1) \\ &= tn + r \end{aligned}$$

con $t = \mathfrak{u} + \mathfrak{i}\mathfrak{s}$ e $r = \mathfrak{u}_1 + \mathfrak{i}\mathfrak{s}_1$.

Poiché

$$\delta(r) = \delta(\mathfrak{u}_1 + \mathfrak{i}\mathfrak{s}_1)$$

per definizione di $\delta$ si ha

$$\delta(r) = \mathfrak{u}_1^2 + \mathfrak{s}_1^2$$

e per la (3) si conclude

$$\delta(r) \leq \frac{n^2}{4} + \frac{n^2}{4} \leq n^2 = \delta(n)$$

Dimostriamo il caso generale.
Supponiamo $x, y \in \mathbb{J}[\mathfrak{i}]$ con $x \neq 0$. Se consideriamo $\frac{y\overline{x}}{x\overline{x}}$, possiamo ricondurci al caso precedente ricordandoci che $x\overline{x}$ è un intero che chiameremo n.
Esisteranno allora $t, r \in \mathbb{J}[\mathfrak{i}]$ tali che $y\overline{x} = tn + r$ con $r = 0$ o $\delta(r) \leq \delta(n) = \delta(x\overline{x})$.

Abbiamo trovato che

$$\delta(r) = \delta(y\overline{x} - tx\overline{x}) = \delta(y - tx)\delta(\overline{x})$$

Ma

$$\delta(r) < \delta(x\overline{x}) \text{ con } \overline{x} \neq 0$$

per cui

$$\delta(y - tx) < \delta(x)$$

Se chiamiamo $r_0 = y - tx$ e $y = tx + r_0$ allora $t, r \in \mathbb{J}[\mathfrak{i}]$ sono gli elementi cercati.

$\square$

## Lemma (5)

*Sia $p$ un intero primo, e supponiamo che per un certo intero $c$ primo con $p$ si possano trovare due interi $x$ e $y$ tali che $x^2 + y^2 = cp$. Allora esistono due interi $a$ e $b$ tali che $p = a^2 + b^2$.*

**Dimostrazione :**

Per ipotesi p è primo in $\mathbb{Z}$. Supponiamo per assurdo che sia primo anche in $\mathbb{J}[\mathfrak{i}]$. Se scriviamo $cp = x^2 + y^2 = (x + \mathfrak{i}y)(x - \mathfrak{i}y)$, dal Lemma (4) sappiamo che

$$p \mid (x + \mathfrak{i}y) \text{ oppure } p \mid (x - \mathfrak{i}y)$$

Ma se questo è vero allora

$$p \mid x \text{ e } p \mid y$$

perciò

$$x = p\mathfrak{u} \text{ e } y = p\mathfrak{s}$$

Si ha allora

$$x + \mathfrak{i}y = p(\mathfrak{u} + \mathfrak{i}\mathfrak{s})$$

e dunque $p \mid (x - \mathfrak{i}y)$.
Allora $p^2 \mid (x + \mathfrak{i}y)(x - \mathfrak{i}y) = cp$
questo implica che

$$p^2 \mid c$$

contro l'ipotesi $(p, c) = 1$ .
Abbiamo fatto vedere che p non è primo in $\mathbb{J}[\mathfrak{i}]$. Segue che :

$$p = (a + \mathfrak{i}b)(g + \mathfrak{i}d)$$

dove $a + \mathfrak{i}b, g + \mathfrak{i}d \in \mathbb{J}[\mathfrak{i}]$ e nessuno dei due è invertibile. Questo vuol dire che $(a + \mathfrak{i}b)(a - \mathfrak{i}b) = a^2 + b^2 \neq 1$.
Infatti se $a + \mathfrak{i}b$ non è invertibile, per l'osservazione (2) si ha che

$$\delta(a - \mathfrak{i}b) < \delta((a - \mathfrak{i}b)(a + \mathfrak{i}b)) = \delta(a - \mathfrak{i}b)\delta(a + \mathfrak{i}b)$$

da cui si ricava

$$1 < \delta(a + \mathrm{i}b) = a^2 + b^2$$

Analogamente $g^2 + d^2 \neq 1$. Poiché $p \in \mathbb{Z}$ si ha

$$p = (a - \mathrm{i}b)(g - \mathrm{i}d)$$

perciò

$$p^2 = (a + \mathrm{i}b)(g + \mathrm{i}d)(a - \mathrm{i}b)(g - \mathrm{i}d) = (a^2 + b^2)(g^2 + d^2)$$

Quindi $(a^2 + b^2) \mid p^2$.
Si presentano tre possibilità :

1) $a^2 + b^2 = 1$ ma non può accadere perché $a + \mathrm{i}b$ non è invertibile;

2) $a^2 + b^2 = p^2$ ma questo implica $g^2 + d^2 = 1$ che per le stesse motivazioni del punto 1) non può accadere;

3) $a^2 + b^2 = p$ come volevasi dimostrare.

$\square$

I numeri primi dispari si dividono in due classi:

1)quelli che divisi per 4 danno resto 1, della forma $4n + 1$;

2) quelli che divisi per 4 danno resto 3, della forma $4n + 3$.

### Lemma (6)

*Se $p$ è un numero primo della forma $4n + 1$ allora la congruenza $x^2 \equiv_p -1$ ammette soluzione.*

**Dimostrazione :**
Definiamo un numero $x = 1 \cdot 2 \cdot ... \cdot \frac{p-1}{2}$. Essendo $p - 1 = 4n$ ,x è il prodotto di un numero pari di fattori. Quindi possiamo scrivere equivalentemente $x = (-1) \cdot (-2) \cdot ... \cdot (-\frac{p-1}{2})$.

Per il teorema di Wilson sappiamo che se p è un numero primo allora $p - k \equiv_p -k$ è vera e dunque

$$x^2 = 1 \cdot 2 \cdot \ldots \cdot \tfrac{p-1}{2} \cdot (-1) \cdot (-2) \cdot \ldots \cdot (-\tfrac{p-1}{2}) \equiv_p$$
$$1 \cdot 2 \cdot \ldots \cdot \tfrac{p-1}{2} \cdot \tfrac{p+1}{2} \cdot \ldots \cdot (p-1) \equiv_p (p-1)! \equiv_p -1$$

$\square$

## Teorema di Fermat

## Teorema (3)

*Se $p$ è un numero primo della forma $4n+1$ allora $p = a^2 + b^2$ per opportuni $a$ e $b$.*

**Dimostrazione :** Dal lemma (6) sappiamo che esiste $x \in \mathbb{J}[\mathfrak{i}]$ tale che $x^2 \equiv_p -1$ con $0 \leq x \leq (p-1)$.
Notiamo che l'intervallo può essere reso ancora più piccolo, infatti se

$$x > \tfrac{p}{2} \ \text{ allora } \ y = p - x \ \text{ verifica}$$

$$y^2 \equiv_p (p-x)^2 \equiv_p p^2 - 2xp + x^2 \equiv_p x^2 \equiv_p -1$$

con $\mid y \mid \leq \frac{p}{2}$ .

Ha senso quindi considerare $\mid x \mid \leq \frac{p}{2}$.
Lo stesso lemma ci dice anche che $x^2 + 1 \equiv_p 0$ quindi $x^2 + 1$ è un multiplo di p che indicheremo con cp. Abbiamo

$$cp = x^2 + 1 \leq \frac{p^2}{4} + 1 < p^2$$

Poiché in un anello euclideo non ci sono divisori dello zero otteniamo

$$c < p \text{ perciò p non divide c e dunque } (p, c) = 1$$

Siamo nelle ipotesi del lemma (5) e possiamo concludere

$$p = a^2 + b^2 \text{ per opportuni a e b.}$$

$\square$