Irriducibili e corollari di aritmetica in $\mathbb{Z}[i]$

Come già dimostrato, $\mathbb{Z}[i]$ è un anello euclideo con la seguente funzione grado:

$$g : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{Z},\ a + bi \mapsto \|a + bi\|^2 .$$

A partire da questo preconcetto è possibile dimostrare un teorema importante in aritmetica, il *Teorema di Natale di Fermat*, che discende direttamente come corollario di un teorema più generale riguardante $\mathbb{Z}[i]$.

§1.1 Il teorema di Natale di Fermat e gli irriducibili in $\mathbb{Z}[i]$

Lemma 1.1.1

Sia p un numero primo riducibile in $\mathbb{Z}[i]$, allora p può essere scritto come somma di due quadrati in $\mathbb{Z}$.

Dimostrazione. Se p è riducibile in $\mathbb{Z}[i]$, allora esistono $a + bi$ e $c + di$ appartenenti a $\mathbb{Z}[i] \setminus \mathbb{Z}[i]^*$ tali che $p = (a + bi)(c + di)$.

Impiegando le proprietà dell'operazione di coniugio si ottiene la seguente equazione:

$$\overline{p} = p = (a - bi)(c - di) \implies p^2 = p\overline{p} = (a^2 + b^2)(c^2 + d^2).$$

Dal momento che $a + bi$ e $c + di$ non sono invertibili, i valori della funzione grado calcolati in essi sono strettamente maggiori del valore assunto nell'unità, ovverosia:

$$a^2 + b^2 > 1, \qquad c^2 + d^2 > 1.$$

Allora devono per forza valere le seguenti equazioni:

$$p = a^2 + b^2, \qquad p = c^2 + d^2,$$

da cui la tesi. □

Lemma 1.1.2

Sia p un numero primo tale che $p \equiv 1 \pmod 4$. Allora esiste un $x \in \mathbb{Z}$ tale che $p \mid x^2 + 1$.

Dimostrazione. Per il *Teorema di Wilson*, $(p-1)! \equiv -1 \pmod{p}$. Attraverso varie manipolazioni algebriche si ottiene:

$$-1 \equiv 1 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-1) \equiv 1 \cdots \frac{p-1}{2} \left(-\frac{p-1}{2}\right) \cdots (-1) \equiv$$

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

da cui con $x = \left(\frac{p-1}{2}\right)!$ si verifica la tesi. □

Teorema 1.1.3

Sia p un numero primo tale che $p \equiv 1 \pmod 4$. Allora p è riducibile in $\mathbb{Z}[i]$.

Dimostrazione. Per il *Lemma 1.1.2*, si ha che esiste un $x \in \mathbb{Z}$ tale che $p \mid x^2 + 1$. Se p fosse irriducibile, dacché $\mathbb{Z}[i]$ è un PID in quanto euclideo, p sarebbe anche un primo di $\mathbb{Z}[i]$. Dal momento che $x^2 + 1 = (x+i)(x-i)$, p dovrebbe dividere almeno uno di questi due fattori.

Senza perdità di generalità, si ponga che $p \mid (x+i)$. Allora $\exists\, a+bi \in \mathbb{Z}[i] \mid x+i = (a+bi)p$. Uguagliando le parti immaginarie si ottiene $bp = 1$, che non ammette soluzioni, ↯. Pertanto p è riducibile. □

Corollario 1.1.4 (*Teorema di Natale di Fermat*)

Sia p un numero primo tale che $p \equiv 1 \pmod 4$. Allora p è somma di due quadrati in $\mathbb{Z}$.

Dimostrazione. Per il *Teorema 1.1.3*, p è riducibile in $\mathbb{Z}[i]$. In quanto riducibile in $\mathbb{Z}[i]$, per il *Lemma 1.1.1*, p è allora somma di due quadrati. □

Teorema 1.1.5

Sia p un numero primo tale che $p \equiv -1 \pmod 4$. Allora p è irriducibile in $\mathbb{Z}[i]$.

Dimostrazione. Se p fosse riducibile in $\mathbb{Z}[i]$, per il *Teorema di Natale di Fermat* esisterebbero a e b in $\mathbb{Z}$ tali che $p = a^2 + b^2$. Dal momento che p è dispari, possiamo supporre, senza perdità di generalità, che a sia pari e che b sia dispari. Pertanto $a^2 \equiv 0 \pmod 4$ e $b^2 \equiv 1 \pmod 4$, dacché sono uno pari e l'altro dispari[1]. Tuttavia la congruenza $a^2 + b^2 \equiv 1 \equiv -1 \pmod 4$ non è mai soddisfatta, ↯. Pertanto p può essere solo irriducibile. □

[1] Infatti, $0^2 \equiv 0 \pmod 4$, $1^2 \equiv 1 \pmod 4$, $2^2 \equiv 4 \equiv 0 \pmod 4$, $3^2 \equiv 9 \equiv 1 \pmod 4$.

Osservazione. Si osserva che $2 = (1+i)(1-i)$. Dal momento che $\|1+i\|^2 = \|1-i\|^2 = 2 \neq 1$, si deduce che nessuno dei due fattori è invertibile. Pertanto 2 non è irriducibile.

Proposizione 1.1.6

Gli unici primi $p \in \mathbb{Z}$ irriducibili in $\mathbb{Z}[i]$ sono i primi p tali che $p \equiv -1 \pmod 4$.

Dimostrazione. Per l'osservazione precedente, 2 non è irriducibile in $\mathbb{Z}[i]$, così come i primi congrui a 1 in modulo 4, per il *Teorema 1.1.3*. Al contrario i primi p congrui a -1 in modulo 4 sono irriducibili, per il *Teorema 1.1.5*, da cui la tesi. □

Teorema 1.1.7

$z \in \mathbb{Z}[i]$ è irriducibile se e solo se z è un associato di un primo $p \in \mathbb{Z}$ tale che $p \equiv -1 \pmod 4$, o se $\|z\|^2$ è primo.

Dimostrazione. Si dimostrano le due implicazioni separatamente.

($\implies$) Sia $z \in \mathbb{Z}[i]$ irriducibile. Chiaramente $z \mid z\overline{z} = g(z)$. Dacché $\mathbb{Z}$ è un UFD, $g(z)$ può decomporsi in un prodotto di primi $q_1 q_2 \cdots q_n$. Dal momento che $\mathbb{Z}[i]$ è un PID, in quanto anello euclideo, z deve dividere uno dei primi della fattorizzazione di $g(z)$. Si assuma che tale primo sia q_i. Allora esiste un $w \in \mathbb{Z}[i]$ tale che $q_i = wz$.

Se $w \in \mathbb{Z}[i]^*$, si deduce che z è un associato di q_i. Dal momento che z è irriducibile, q_i, che è suo associato, è a sua volta irriducibile. Allora, per la *Proposizione 1.1.6*, $q_i \equiv -1 \pmod 4$.

Altrimenti, se w non è invertibile, si ha che $g(w) > g(1)$, ossia che $\|w\|^2 > 1$. Inoltre in quanto irriducibile, anche z non è invertibile, e quindi $g(z) > g(1) \implies \|z\|^2 > 1$. Dalla proprietà moltiplicativa del modulo si ricava $q_i^2 = \|q_i\|^2 = \|w\|^2 \|z\|^2$, da cui necessariamente consegue che:

$$\|w\|^2 = q_i, \quad \|z\|^2 = q_i,$$

attraverso cui si verifica l'implicazione.

($\impliedby$) Se $p \in \mathbb{Z}$ e $p \equiv -1 \pmod 4$, per il *Teorema 1.1.5*, p è irriducibile. Allora in quanto suo associato, anche z è irriducibile.

Altrimenti, se $\|z\|^2$ è un primo p, si ponga $z = ab$ con a e $b \in \mathbb{Z}[i]$. Per la proprietà moltiplicativa del modulo, $p = \|z\|^2 = \|ab\|^2 = \|a\|^2 \|b\|^2$. Tuttavia questo implica che uno tra $\|a\|^2$ e $\|b\|^2$ sia pari a 1, ossia che uno tra a e b sia invertibile, dacché $g(1) = 1$. Pertanto z è in ogni caso irriducibile. □

Infine si enuncia un'ultima identità inerente all'aritmetica, ma strettamente collegata a $\mathbb{Z}[i]$.

§1.2 L'identità di Brahmagupta-Fibonacci

Proposizione 1.2.1 (*Identità di Brahmagupta-Fibonacci*)
Il prodotto di due somme di quadrati è ancora una somma di quadrati. In particolare:

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2.$$

Dimostrazione. La dimostrazione altro non è che una banale verifica algebrica. Ciononostante è possibile risalire a questa identità in via alternativa mediante l'uso del modulo dei numeri complessi.

Siano $z_1 = a+bi$, $z_2 = c+di \in \mathbb{C}$. Allora, per le proprietà del modulo dei numeri complessi:

$$\|z_1\| \, \|z_2\| = \|z_1 z_2\| \, . \tag{1.1}$$

Computando il prodotto tra z_1 e z_2 si ottiene:

$$z_1 z_2 = (ac-bd) + (ad+bc)i,$$

da cui a sua volta si ricava:

$$\|z_1 z_2\| = \sqrt{(ac-bd)^2 + (ad+bc)^2},$$

assieme a:

$$\|z_1\| = \sqrt{a^2+b^2}, \quad \|z_2\| = \sqrt{c^2+d^2}.$$

Infine, da (1.1), elevando al quadrato, si deduce l'identità presentata:

$$\sqrt{a^2+b^2}\sqrt{c^2+d^2} = \sqrt{(ac-bd)^2+(ad+bc)^2} \implies (a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2.$$

□

Esempio 1.2.2

Si consideri $65 = 5 \cdot 13$. Dal momento che sia 5 che 13 sono congrui a 1 in modulo 4, sappiamo già si possono scrivere entrambi come somme di due quadrati. Allora, dall'*Identità di Brahmagupta-Fibonacci*, anche 65 è somma di due quadrati.

Infatti $5 = 2^2 + 1^2$ e $13 = 3^2 + 2^2$. Pertanto $65 = 5 \cdot 13 = (2 \cdot 3 - 1 \cdot 2)^2 + (2 \cdot 2 + 1 \cdot 3)^2 = 4^2 + 7^2$.