I primi negli interi Gaussiani

Maurizio Cornalba

16 dicembre 2011

Sia $A = \mathbb{Z}[i]$ l'anello degli interi Gaussiani. Sappiamo che A è un dominio euclideo, e quindi a ideali principali e a fattorizzazione unica. La *norma* di un elemento $z = a + bi \in A$ è $N(z) = |z|^2 = a^2 + b^2$; si tratta di un intero non negativo. Lo scopo principale di queste note è di descrivere gli elementi primi o, che è lo stesso, irriducibili di A. Nel seguito, per evitare confusioni tra gli elementi primi di A e gli elementi primi di $\mathbb{Z}$, chiameremo spesso questi ultimi *primi razionali.*

Ricordiamo che un intero Gaussiano è una unità se e solo se la sua norma è 1, e che quindi le sole unità in A sono ± 1 e $\pm i$. Sia $z = a + ib$ un intero Gaussiano, e supponiamo che $N(z) = a^2 + b^2$ sia dispari. Allora a e b sono uno pari e uno dispari, cioè uno della forma $2h$ e l'altro della forma $2k + 1$. Quindi $N(z) = 4h^2 + 4k^2 + 4k + 1$ è congruo a 1 modulo 4.

Lemma 1. *Sia z un elemento primo di A. Allora $N(z)$ è uguale a 2, o è un numero primo congruo a 1 modulo 4, oppure è il quadrato di un numero primo associato a z.*

Dimostrazione. Sappiamo che $N(z) > 1$. Se $z \in \mathbb{Z}$, è evidentemente un primo razionale e $N(z) = z^2$. Se $z \notin \mathbb{Z}$ è evidente che anche $\overline{z}$ è primo. Se inoltre $N(z)$ non è un numero primo ci sono interi h e k strettamente maggiori di 1 tali che

$$z\overline{z} = N(z) = hk$$

Poiché A gode della proprietà di fattorizzazione unica z deve essere associato a uno dei fattori h e k, e $\overline{z}$ all'altro fattore. Ne segue in particolare che h e k sono numeri primi e che inoltre $h = |z| = |\overline{z}| = k$.

Se $N(z)$ è un primo dispari segue dall'osservazione immediatamente precedente l'enunciato che è congruo a 1 modulo 4. □

Lemma 2. *Sia z un elemento di A. Supponiamo che $N(z)$ sia un numero primo. Allora z è primo in A.*

Dimostrazione. Supponiamo che $z = uv$. Allora $N(z) = N(u)N(v)$. Dato che $N(z)$ è un numero primo uno tra $N(u)$ e $N(v)$ deve valere 1, e quindi uno tra u e v è una unità. □

Notiamo che $2 = N(1 - i) = (1 - i)(1 + i) = i(1 - i)^2$. Per il lemma precedente $(1 - i)$ è primo in A; inoltre $(1 + i)$ è associato a $(1 - i)$. Restano da esaminare i numeri primi dispari.

Lemma 3. *Ogni numero primo congruo a 3 modulo 4 è primo in A.*

Dimostrazione. Sia p un numero primo dispari. Supponiamo che ci siano interi Gaussiani v e w non invertibili, cioè di norma strettamente maggiore di 1, tali che $p = vw$. Allora $p^2 = N(p) = N(v)N(w)$. Per l'unicità della fattorizzazione in $\mathbb{Z}$, $p = N(v) = N(w)$. Ma in questo caso $p \equiv 1 \mod 4$, dato che è dispari e uguale alla norma di un intero Gaussiano. □

Lemma 4. *Se p è un numero primo congruo a 1 modulo 4 esiste un intero Gaussiano z tale che $p = N(z) = z\overline{z}$. Inoltre z e $\overline{z}$ sono primi non associati in A.*

Supponiamo di sapere che $p = N(z)$ per qualche z. Che z e $\overline{z}$ siano primi segue dal Lemma 2. Se z e $\overline{z}$ fossero associati dovrebbe essere $\overline{z} = \pm iz$, e quindi $\pm iz^2 = p$ sarebbe un numero reale. Se scriviamo $z = a + ib$, questo implicherebbe che $b = \pm a$, e dunque che $p = 2a^2$, il che è assurdo.

Resta da trovare un intero Gaussiano z la cui norma sia p. Ci servono un paio di semplici risultati di teoria dei gruppi.

Lemma 5. *Siano a e b due elementi di un gruppo abeliano G. Supponiamo che a abbia ordine finito h e b ordine finito k. Allora esiste un elemento di G il cui ordine è $\mathrm{mcm}(h,k)$.*

Dimostrazione. Siano
$$h = \prod_p p^{e_p}\,, \quad k = \prod_p p^{f_p}\,,$$
dove p varia tra tutti i numeri primi, le decomposizioni in fattori primi di h e k. Poniamo
$$u = \prod_{e_p > f_p} p^{e_p}\,, \quad v = \prod_{e_p \le f_p} p^{f_p}\,.$$
Notiamo che u e v sono primi fra loro, che
$$uv = \mathrm{mcm}(h,k)$$
e che esistono interi r e s tali che $h = ur$, $k = vs$. Dico che $g = a^r b^s$ ha ordine uv. In primo luogo $g^{uv} = (a^h)^v (b^k)^u = 1$. Inoltre a^r ha ordine u e b^s ha ordine v. Se $g^\ell = 1$, allora l'ordine di $(a^r)^\ell = (b^{-s})^\ell$ divide sia u che v. Dato che u è primo con v se ne deduce che $(a^r)^\ell = (b^s)^\ell = 1$, e quindi che u e v dividono ℓ. La conclusione è che ℓ è divisibile per uv, sempre perchè u e v sono coprimi. □

Lemma 6. *Sia G un gruppo abeliano finito. Supponiamo che per ogni intero positivo n esistano al più n elementi $g \in G$ tali che $g^n = 1$. Allora G è ciclico.*

Dimostrazione. Sia a un elemento di G di ordine massimo h. Sia b un altro elemento di G, e sia k il suo ordine. Se k non dividesse h il lemma precedente direbbe che esiste un elemento di ordine $\mathrm{mcm}(h,k) > h$, contro la definizione di a. Dunque $k \big| h$. Ma allora il gruppo $\langle a \rangle$ contiene esattamente k elementi g tali che $g^k = 1$, e dunque per ipotesi b deve essere uno di questi. Quindi $G = \langle a \rangle$. □

Corollario 1. *Sia R un dominio. Ogni sottogruppo finito del gruppo delle unità $R^\times$ è ciclico.*

Dimostrazione. Basta osservare che ogni sottogruppo finito di $R^\times$ soddisfa le ipotesi del Lemma 6 perché il polinomio $X^n - 1$ ha al più n radici in R per ogni n. □

Lemma 7. *Sia p un numero primo. Allora -1 è un quadrato in $\mathbb{Z}/(p)$ se e solo se $p = 2$ oppure $p \equiv 1 \mod 4$.*

Dimostrazione. Se $p = 2$, $1^2 = 1 = -1$. Se p è congruo a 1 modulo 4 il gruppo $\mathbb{Z}/(p)^\times$ ha ordine $p - 1 = 4k$. Dato che $\mathbb{Z}/(p)^\times$ è ciclico per il Corollario 1, il sottogruppo dei quadrati coincide con il nucleo dell'omomorfismo "elevamento alla $2k$-esima potenza", che contiene -1. Se invece p è congruo a 3 modulo 4, cioè se $p - 1$ è della forma $4k + 2$, ogni quadrato in $\mathbb{Z}/(p)^\times$ ha per ordine un divisore di $2k + 1$, e dunque un numero dispari. Quindi -1, che ha ordine pari, non può essere un quadrato. □

Ora siamo in grado di completare la dimostrazione del Lemma 4. Per ogni elemento $v \in A$ indichiamo con $[v]$ la classe di v in $A/(p)$. L'anello $A/(p)$ contiene come sottoanello $\mathbb{Z}/(p)$. Per il Lemma 7 c'è un intero n tale che $[n]^2 = (-[n])^2 = -1$. Si noti che $-[n] \neq [n]$ dato che $p \neq 2$. È chiaro che $[i]^2 = -1$ e anche che $[i] \neq \pm[n]$; infatti $i \pm n$ non è divisibile per p in A. Di conseguenza il polinomio $X^2 + 1$ ha almeno tre radici in A (in effetti quattro, se teniamo conto anche di $-[i]$), e quindi $A/(p)$ non è un dominio. Ne segue che p non è primo, cioè che esistono interi Gaussiani non invertibili v e w tali che $p = vw$. Passando alle norme se ne deduce che $p^2 = N(p) = N(v)N(w)$, e quindi che $p = N(z) = N(w)$. Questo completa la dimostrazione del Lemma 4.

Riassumendo, una lista completa di primi in A a due a due non associati è la seguente:

1. $1 - i$;
2. i numeri primi congrui a 3 modulo 4;
3. per ogni numero primo p congruo a 1 modulo 4, due interi Gaussiani z e $\overline{z}$ tali che $p = N(z) = z\overline{z}$.

I lemmi che abbiamo dimostrato provano il seguente risultato classico.

Proposizione 1. *Un numero primo è somma di due quadrati se e solo se è uguale a* 2 *o è congruo a* 1 *modulo* 4*.*

Più in generale, vale il risultato seguente.

Corollario 2. *Un numero intero $n > 1$ è somma di due quadrati se e solo se ogni primo congruo a* 3 *modulo* 4 *compare con esponente pari nella decomposizione di n in fattori primi.*

Dimostrazione. Ricordiamo innanzitutto che essere somma di quadrati equivale a essere la norma di un intero Gaussiano. Se

$$n = \prod_{p \equiv 3} p^{2h_p} \prod_{p \not\equiv 3} p^{k_p} \,,$$

dove tutte le congruenze sono intese modulo 4, allora

$$n = N\left(\prod_{p \equiv 3} p^{h_p} \prod_{p \not\equiv 3} z_p^{k_p} \right) \,,$$

dove $N(z_p) = p$ per p non congruo a 3 modulo 4. Viceversa supponiamo che $n = N(w)$. Sia

$$w = \prod_{p \equiv 3} p^{h_p} \prod_{N(z) \text{ primo}} z^{k_z}$$

la decomposizione in fattori primi di w, dove si intende che il secondo prodotto contiene un fattore per ogni classe di primi non razionali associati. Allora

$$n = \prod_{p \equiv 3} p^{2h_p} \prod_{N(z) \text{ primo}} N(z)^{k_z} \,.$$

La tesi segue ricordando che $N(z)$ non è mai congruo a 3 modulo 4. $\square$