Proprietà fondamentali di $\mathbb{Z}[i]$, $\mathbb{Z}[x]$, $\mathbb{Z}_p[x]$ e $\mathbb{Q}[x]$

Gabriel Antonio Videtta

3 gennaio 2023

Indice

1 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. 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 1.2. 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. Sia p un numero primo tale che $p \equiv 1 \pmod 4$. Allora p è riducibile in $\mathbb{Z}[i]$.

Dimostrazione. Per il *Lemma 1.2*, 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 (*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*, p è riducibile in $\mathbb{Z}[i]$. In quanto riducibile in $\mathbb{Z}[i]$, per il *Lemma 1.1*, p è allora somma di due quadrati. □

Teorema 1.2. 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. 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.* Al contrario i primi p congrui a -1 in modulo 4 sono irriducibili, per il *Teorema 1.2*, da cui la tesi. □

Teorema 1.3. $z \in \mathbb{Z}[i]$ è irriducibile se e solo se z è un associato di un $k \in \mathbb{Z}$ tale che $k \equiv -1 \pmod 4$, 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*, $q_i \equiv -1 \pmod 4$.

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 $k \in \mathbb{Z}$ e $k \equiv -1 \pmod 4$, per il *Teorema 1.2*, k 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 (*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:

$$|z_1|\,|z_2| = |z_1 z_2|\,. \tag{1}$$

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), 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 1.1. 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 $65 = 5 \cdot 13 = (2 \cdot 3 - 1 \cdot 2)^2 + (2 \cdot 2 + 1 \cdot 3)^2 = 4^2 + 7^2$.

2 Irriducibilità in $\mathbb{Z}[x]$ e in $\mathbb{Q}[x]$

2.1 Criterio di Eisenstein e proiezione in $\mathbb{Z}_p[x]$

Prima di studiare le irriducibilità in $\mathbb{Z}$, si guarda alle irriducibilità nei vari campi finiti $\mathbb{Z}_p$, con p primo. Questo metodo presenta un vantaggio da non sottovalutare: in $\mathbb{Z}_p$ per ogni grado n esiste un numero finito di polinomi monici[2] – in particolare, p^n – e quindi per un polinomio di grado d è sufficiente controllare che questo non sia prodotto di tali polinomi monici per $1 \leq n < d$.

In modo preliminare, si definisce un omomorfismo fondamentale.

[2]Si prendono in considerazione solo i polinomi monici dal momento che vale l'equivalenza degli associati: se a divide b, allora tutti gli associati di a dividono b. $\mathbb{Z}_p$ è infatti un campo, e quindi $\mathbb{Z}_p[x]$ è un anello euclideo.

Definizione 2.1. Sia il seguente l'**omomorfismo di proiezione** da $\mathbb{Z}$ in $\mathbb{Z}_p$:

$$\hat{\pi}_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x],\ a_n x^n + \ldots + a_0 \mapsto [a_n]_p\, x^n + \ldots + [a_0]_p.$$

Osservazione. Si dimostra facilmente che $\hat{\pi}$ è un omomorfismo di anelli. Innanzitutto, $\hat{\pi}(1) = [1]_p$. Vale chiaramente la linearità:

$$\begin{aligned}\hat{\pi}_p(a_n x^n + \ldots + a_0) + \hat{\pi}_p(b_n x^n + \ldots + b_0) = [a_n]_p\, x^n + \ldots + [b_n]_p\, x^n + \ldots = \\ = [a_n + b_n]_p\, x^n + \ldots = \hat{\pi}_p(a_n x^n + \ldots + a_0 + b_n x^n + \ldots + b_0).\end{aligned}$$

Infine vale anche la moltiplicatività:

$$\begin{aligned}\hat{\pi}_p(a_n x^n + \ldots + a_0)\hat{\pi}_p(b_n x^n + \ldots + b_0) = ([a_n]_p\, x^n + \ldots)([b_n]_p\, x^n + \ldots) = \\ = \sum_{i=0}^{n} \sum_{j+k=i} [a_j]_p\, [b_k]_p\, x^i = \sum_{i=0}^{n} \sum_{j+k=i} [a_j b_k]_p\, x^i = \hat{\pi}_p\left(\sum_{i=0}^{n} \sum_{j+k=i} a_j b_k x^i\right) = \\ = \hat{\pi}_p\left((a_n x^n + \ldots + a_0)(b_n x^n + \ldots + b_0)\right).\end{aligned}$$

Prima di enunciare un teorema che si rivelerà importante nel determinare l'irriducibilità di un polinomio in $\mathbb{Z}[x]$, si enuncia una definizione che verrà ripresa anche in seguito

Definizione 2.2. Un polinomio $a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$ si dice **primitivo** se $\mathrm{MCD}(a_n, \ldots, a_0) = 1$.

Teorema 2.1. Sia p un primo. Sia $f(x) = a_n x^n + \ldots \in \mathbb{Z}[x]$ primitivo. Se $p \nmid a_n$ e $\hat{\pi}_p(f(x))$ è irriducibile in $\mathbb{Z}_p[x]$, allora anche $f(x)$ lo è in $\mathbb{Z}[x]$.

Dimostrazione. Si dimostra la tesi contronominalmente. Sia $f(x) = a_n x^n + \ldots \in \mathbb{Z}[x]$ primitivo e riducibile, con $p \nmid a_n$. Dal momento che $f(x)$ è riducibile, esistono $g(x)$, $h(x)$ non invertibili tali che $f(x) = g(x)h(x)$.

Si dimostra che $\deg g(x) \geq 1$. Se infatti fosse nullo, $g(x)$ dovrebbe o essere uguale a ± 1 – assurdo, dal momento che $g(x)$ non è invertibile, $\lightning$ – o essere una costante non invertibile. Tuttavia, nell'ultimo caso, risulterebbe che $f(x)$ non è primitivo, poiché $g(x)$ dividerebbe ogni coefficiente del polinomio. Analogamente anche $\deg h(x) \geq 1$.

Si consideri ora $\hat{\pi}_p(f(x)) = \hat{\pi}_p(g(x))\hat{\pi}_p(h(x))$. Dal momento che $p \nmid a_n$, il grado di $f(x)$ rimane costante sotto l'operazione di omomorfismo, ossia $\deg \hat{\pi}_p(f(x)) = \deg f(x)$.

Inoltre, poiché nessuno dei fattori di $f(x)$ è nullo, $\deg f(x) = \deg g(x) + \deg h(x)$. Da questa considerazione si deduce che anche i gradi di $g(x)$ e $h(x)$ non devono calare, altrimenti si avrebbe che $\deg \hat{\pi}_p(f(x)) < \deg f(x)$, $\lightning$. Allora $\deg \hat{\pi}_p(g(x)) = \deg g(x) \geq 1$, $\deg \hat{\pi}_p(h(x)) = \deg h(x) \geq 1$.

Poiché $\deg \hat{\pi}_p(g(x))$ e $\deg \hat{\pi}_p(h(x))$ sono dunque entrambi non nulli, $\hat{\pi}_p(g(x))$ e $\hat{\pi}_p(h(x))$ non sono invertibili[3]. Quindi $f(x)$ è prodotto di non invertibili, ed è dunque riducibile.

□

Teorema 2.2 (*Criterio di Eisenstein*)**.** Sia p un primo. Sia $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$ primitivo tale che:

(1) $p \nmid a_n$,

(2) $p \mid a_i$, $\forall\, i \neq n$,

(3) $p^2 \nmid a_0$.

Allora $f(x)$ è irriducibile in $\mathbb{Z}[x]$.

Dimostrazione. Si ponga $f(x)$ riducibile e sia pertanto $f(x) = g(x)h(x)$ con $g(x)$ e $h(x)$ non invertibili. Analogamente a come visto per il *Teorema 2.1*, si desume che $\deg g(x)$, $\deg h(x) \geq 1$.

Si applica l'omomorfismo di proiezione in $\mathbb{Z}_p[x]$:

$$\hat{\pi}_p(f(x)) = \underbrace{[a_n]_p}_{\neq 0} x_n,$$

da cui si deduce che $\deg \hat{\pi}_p(f(x)) = \deg f(x)$.

Dal momento che $\hat{\pi}_p(f(x)) = \hat{\pi}_p(g(x))\hat{\pi}_p(h(x))$ e che $\mathbb{Z}_p[x]$, in quanto campo, è un dominio, necessariamente sia $\hat{\pi}_p(g(x))$ che $\hat{\pi}_p(h(x))$ sono dei monomi.

Inoltre, sempre in modo analogo a come visto per il *Teorema 2.1*, sia $\deg \hat{\pi}_p(g(x))$ che $\deg \hat{\pi}_p(h(x))$ sono maggiori o uguali ad 1.

Combinando questo risultato col fatto che questi due fattori sono monomi, si desume che $\hat{\pi}_p(g(x))$ e $\hat{\pi}_p(h(x))$ sono monomi di grado positivo. Quindi p deve dividere entrambi i termini noti di $g(x)$ e $h(x)$, e in particolare p^2 deve dividere il loro prodotto, ossia a_0. Tuttavia questo è un assurdo, ↯. □

Osservazione. Si consideri $x^k - 2$, per $k \geq 1$. Per il *Criterio di Eisenstein*, considerando come primo $p = 2$, si verifica che $x^k - 2$ è sempre irriducibile. Pertanto, per ogni grado di un polinomio esiste almeno un irriducibile – a differenza di come invece avviene in $\mathbb{R}[x]$ o in $\mathbb{C}[x]$.

Teorema 2.3. Sia $f(x) \in \mathbb{Z}[x]$ primitivo e sia $a \in \mathbb{Z}$. Allora $f(x)$ è irriducibile se e solo se $f(x + a)$ è irriducibile.

Dimostrazione. Si dimostra una sola implicazione, dal momento che l'implicazione contraria consegue dalle stesse considerazioni poste studiando prima $f(x + a)$ e poi $f(x)$.

[3]Si ricorda che $\mathbb{Z}_p[x]$ è un anello euclideo. Pertanto, non avere lo stesso grado dell'unità equivale a non essere invertibili.

Sia $f(x) = a(x)b(x)$ riducibile, con $a(x)$, $b(x) \in \mathbb{Z}[x]$ non invertibili. Come già visto per il *Teorema 2.1*, $\deg a(x)$, $\deg b(x) \geq 1$.

Allora chiaramente $f(x+a) = g(x+a)h(x+a)$, con $\deg g(x+a) = \deg g(x) \geq 1$, $\deg h(x+a) = \deg h(x) \geq 1$. Pertanto $f(x+a)$ continua a essere riducibile, da cui la tesi. □

Esempio 2.1. Si consideri $f(x) = x^{p-1} + \ldots + x^2 + x + 1 \in \mathbb{Z}[x]$, dove tutti i coefficienti del polinomio sono 1. Si verifica che:

$$f(x+1) = \frac{(x+1)^p - 1}{x} = p + \binom{p}{2}x + \ldots + x^{p-1}.$$

Allora, per il *Criterio di Eisenstein* con p, $f(x+1)$ è irriducibile. Pertanto anche $f(x)$ lo è.

2.2 Alcuni irriducibili di $\mathbb{Z}_2[x]$

Tra tutti gli anelli $\mathbb{Z}_p[x]$, $\mathbb{Z}_2[x]$ ricopre sicuramente un ruolo fondamentale, dal momento che è il meno costoso computazionalmente da analizzare, dacché $\mathbb{Z}_2$ consta di soli due elementi. Pertanto si computano adesso gli irriducibili di $\mathbb{Z}_2[x]$ fino al quarto grado incluso, a meno di associati.

Sicuramente x e $x+1$ sono irriducibili, dal momento che sono di primo grado. I polinomi di secondo grado devono dunque essere prodotto di questi polinomi, e pertanto devono avere o 0 o 1 come radice: si verifica quindi che $x^2 + x + 1$ è l'unico polinomio di secondo grado irriducibile.

Per il terzo grado vale ancora lo stesso principio, per cui $x^3 + x^2 + 1$ e $x^3 + x + 1$ sono gli unici irriducibili di tale grado. Infine, per il quarto grado, i polinomi riducibili soddisfano una qualsiasi delle seguenti proprietà:

- 0 e 1 sono radici del polinomio,
- il polinomio è prodotto di due polinomi irriducibili di secondo grado.

Si escludono pertanto dagli irriducibili i polinomi non omogenei – che hanno sicuramente 0 come radice –, e i polinomi con 1 come radice, ossia x^4+x^3+x+1, $x^4+x^3+x^2+1$, e x^4+x^2+x+1. Si esclude anche $(x^2+x+1)^2 = x^4+x^2+1$. Pertanto gli unici irriducibili di grado quattro sono $x^4+x^3+x^2+x+1$, x^4+x^3+1, $x^4 + x + 1$.

Tutti questi irriducibili sono raccolti nella seguente tabella:

- (grado 1) x, $x+1$,
- (grado 2) $x^2 + x + 1$,
- (grado 3) $x^3 + x^2 + 1$, $x^3 + x + 1$,
- (grado 4) $x^4 + x^3 + x^2 + x + 1$, $x^4 + x^3 + 1$, $x^4 + x + 1$.

Esempio 2.2. Il polinomio $51x^3 + 11x^2 + 1 \in \mathbb{Z}[x]$ è primitivo dal momento che $\mathrm{MCD}(51, 11, 1) = 1$. Inoltre, poiché $\hat{\pi}_2(51x^3 + 11x^2 + 1) = x^3 + x + 1$ è irriducibile, si deduce che anche $51x^3 + 11x^2 + 1$ lo è per il *Teorema 2.1*.

2.3 Teorema delle radici razionali e lemma di Gauss

Si enunciano in questa sezione i teoremi più importanti per lo studio dell'irriducibilità dei polinomi in $\mathbb{Q}[x]$ e in $\mathbb{Z}[x]$, a partire dai due teoremi più importanti: il classico *Teorema delle radici razionali* e il *Lemma di Gauss*, che si pone da ponte tra l'analisi dell'irriducibilità in $\mathbb{Z}[x]$ e quella in $\mathbb{Q}[x]$.

Teorema 2.4 (*Teorema delle radici razionali*)**.** Sia $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$. Abbia $f(x)$ una radice razionale. Allora, detta tale radice $\frac{p}{q}$, già ridotta ai minimi termini, questa è tale che:

(i.) $p \mid a_0$,

(ii.) $q \mid a_n$.

Dimostrazione. Poiché $\frac{p}{q}$ è radice, $f\left(\frac{p}{q}\right) = 0$, e quindi si ricava che:

$$a_n \left(\frac{p}{q}\right)^n + \ldots + a_0 = 0 \implies a_n p^n = -q(\ldots + a_0 q^{n-1}).$$

Quindi $q \mid a_n p^n$. Dal momento che $\mathrm{MCD}(p, q) = 1$, si deduce che $q \mid a_n$.

Analogamente si ricava che:

$$a_0 q^n = -p(a_n p^{n-1} + \ldots).$$

Pertanto, per lo stesso motivo espresso in precedenza, $p \mid a_0$, da cui la tesi. □

Teorema 2.5 (*Lemma di Gauss*)**.** Il prodotto di due polinomi primitivi in $\mathbb{Z}[x]$ è anch'esso primitivo.

Dimostrazione. Siano $g(x) = a_m x^m + \ldots + a_0$ e $h(x) = b^n x^n + \ldots + b_0$ due polinomi primitivi in $\mathbb{Z}[x]$. Si assuma che $f(x) = g(x)h(x)$ non sia primitivo. Allora esiste un p primo che divide tutti i coefficienti di $f(x)$.

Siano a_s e b_t i più piccoli coefficienti non divisibili da p dei rispettivi polinomi. Questi sicuramente esistono, altrimenti p dividerebbe tutti i coefficienti, e quindi o $g(x)$ o $h(x)$ non sarebbe primitivo, ↯.

Si consideri il coefficiente di x^{s+t} di $f(x)$:

$$c_{s+t} = \sum_{j+k=s+t} a_j b_k = \underbrace{a_0 b_{s+t} + a_1 b_{s+t-1} + \ldots}_{\equiv 0 \pmod p} + a_s b_t + \underbrace{a_{s+1} b_{t-1} + \ldots}_{\equiv 0 \pmod p},$$

dal momento che $p \mid c_{s+t}$, si deduce che p deve dividere anche $a_s b_t$, ossia uno tra a_s e b_t, che è assurdo, ↯. Quindi $f(x)$ è primitivo.

□

Teorema 2.6 (*Secondo lemma di Gauss*)**.** Sia $f(x) \in \mathbb{Z}[x]$. Allora $f(x)$ è irriducibile in $\mathbb{Z}[x]$ se e solo se $f(x)$ è irriducibile in $\mathbb{Q}[x]$ ed è primitivo.

Dimostrazione. Si dimostrano le due implicazioni separatamente.

($\implies$) Si dimostra l'implicazione contronominalmente, ossia mostrando che se $f(x)$ non è primitivo o se è riducibile in $\mathbb{Q}[x]$, allora $f(x)$ è riducibile in $\mathbb{Z}[x]$.

Se $f(x)$ non è primitivo, allora $f(x)$ è riducibile in $\mathbb{Z}[x]$. Sia quindi $f(x)$ primitivo e riducibile in $\mathbb{Q}[x]$, con $f(x) = g(x)h(x)$, $g(x)$, $h(x) \in \mathbb{Q}[x] \setminus \mathbb{Q}[x]^*$.

Si descrivano $g(x)$ e $h(x)$ nel seguente modo:

$$g(x) = \frac{p_m}{q_m}x^m + \ldots + \frac{p_0}{q_0}, \quad \text{MCD}(p_i, q_i) = 1 \ \forall\, 0 \leq i \leq m,$$

$$h(x) = \frac{s_n}{t_n}x^n + \ldots + \frac{s_0}{t_0}, \quad \text{MCD}(s_i, t_i) = 1 \ \forall\, 0 \leq i \leq n.$$

Si definiscano inoltre le seguenti costanti:

$$\alpha = \frac{\text{mcm}(q_m, \ldots, q_0)}{\text{MCD}(p_m, \ldots, p_0)}, \quad \beta = \frac{\text{mcm}(t_n, \ldots, t_0)}{\text{MCD}(s_n, \ldots, s_0)}.$$

Si verifica che sia $\hat{g}(x) = \alpha g(x)$ che $\hat{h}(x) = \beta h(x)$ appartengono a $\mathbb{Z}[x]$ e che entrambi sono primitivi. Pertanto $\hat{g}(x)\hat{h}(x) \in \mathbb{Z}[x]$.

Si descriva $f(x)$ nel seguente modo:

$$f(x) = a_k x^k + \ldots + a_0, \quad \text{MCD}(a_k, \ldots, a_0) = 1.$$

Sia $\alpha\beta = \frac{p}{q}$ con $\text{MCD}(p, q) = 1$, allora:

$$\hat{g}(x)\hat{h}(x) = \alpha\beta f(x) = \frac{p}{q}(a_k x^k + \ldots + a_0),$$

da cui, per far sì che $\hat{g}(x)\hat{h}(x)$ appartenga a $\mathbb{Z}[x]$, q deve necessariamente dividere tutti i coefficienti di $f(x)$. Tuttavia $f(x)$ è primitivo, e quindi $q = \pm 1$. Pertanto $\alpha\beta = \pm p \in \mathbb{Z}$.

Infine, per il *Lemma di Gauss*, $\alpha\beta f(x)$ è primitivo, da cui $\alpha\beta = \pm 1$. Quindi $f(x) = \pm\hat{g}(x)\hat{h}(x)$ è riducibile.

($\impliedby$) Se $f(x)$ è irriducibile in $\mathbb{Q}[x]$ ed è primitivo, sicuramente $f(x)$ è irriducibile anche in $\mathbb{Z}[x]$. Infatti, se esiste una fattorizzazione in irriducibili in $\mathbb{Z}[x]$, essa non include alcuna costante moltiplicativa dal momento che $f(x)$ è primitivo, e quindi esisterebbe una fattorizzazione in irriducibili anche in $\mathbb{Q}[x]$. $\square$