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

## §1.1 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[1] – 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.

**Definizione 1.1.1.** 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

[1] 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 1.1.2.** 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 1.1.3**

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 $\pm 1$ – 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[2]. Quindi $f(x)$ è prodotto di non invertibili, ed è dunque riducibile. □

**Teorema 1.1.4** (*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 $\mathbb{Z}[x]$.

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

*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 1.1.3*, 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 1.1.3*, 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, $\lightning$. $\square$

**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 1.1.5**

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 $f(x)$.

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 1.1.3*, $\deg a(x)$, $\deg b(x) \geq 1$.

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. $\square$

**Esempio 1.1.6**
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.

## §1.2 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 1.2.1**

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 1.1.3*.

## §1.3 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 1.3.1** (*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. $\square$

**Teorema 1.3.2** (*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, $\lightning$.

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, $\lightning$. Quindi $f(x)$ è primitivo.

□

**Teorema 1.3.3** (*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:

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

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

Si definiscano inoltre le seguenti costanti:

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

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:

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

Sia $\alpha\beta = \frac{p}{q}$ con $\mathrm{MCD}(p, q) = 1$, 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.

($\Longleftarrow$) 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 $\mathbb{Q}[x]$. $\square$