UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

CORSO DI LAUREA MAGISTRALE IN MATEMATICA

TESI DI LAUREA

PERIODICITÀ IN SERIE FORMALI DI LAURENT

RELATORE: Prof. Alberto Facchini

LAUREANDA: Beatrice Stivanello

Mat. 1130746

23 Febbraio 2018

Introduzione

Nel lavoro [1] pubblicato sull'American Mathematical Monthly, A. Facchini e G. Simonetta hanno dimostrato la somiglianza tra il comportamento dei monoidi ciclici finiti e il comportamento della rappresentazione decimale dei numeri razionali. In entrambi i casi si ha una periodicità a partire da un certo punto in poi. La motivazione di questa somiglianza nel comportamento deriva dal fatto che le cifre decimali di un numero razionale sono effettivamente gli elementi di un monoide ciclico finito in un monoide di classi resto di interi. In questa tesi, che è di natura elementare, ma originale, vediamo com'è possibile ottenere risultati simili nel caso in cui, invece di numeri razionali, si considerino funzioni razionali a coefficienti in un campo $\Bbbk$. L'analogia si dimostra essere molto buona ed è dovuta al fatto che sia $\mathbb{Z}$ che $\Bbbk[x]$ sono domini euclidei. È necessario infatti eseguire divisioni euclidee. Un'altra cosa che si è notato essere fondamentale per avere la periodicità da un certo punto in poi è il fatto che tutti i quozienti propri di $\mathbb{Z}$ sono finiti. Ci è stato quindi indispensabile supporre che ogni quoziente proprio di $\Bbbk[x]$ fosse finito; equivalentemente possiamo supporre che il campo $\Bbbk$ sia finito. Ciononostante questa ipotesi può essere indebolita a un campo $\Bbbk$ di caratteristica p ed estensione algebrica del suo sottocampo fondamentale $\mathbb{F}_p$.

Abbiamo poi trattato i criteri di divisibilità di Pascal tra numeri interi e, inoltre, alcuni curiosi fenomeni riguardanti i divisori interi dei numeri della forma $99\ldots900\ldots0$. Tali numeri sono quelli che compaiono quando da un numero razionale scritto in forma periodica si vuol risalire ad una

sua forma come quoziente di due interi: al denominatore va scritto un numero del tipo $99\ldots900\ldots0$, con tanti 9 quante sono le cifre del periodo e tanti 0 quante sono le cifre dell'antiperiodo. L'analogo dei numeri del tipo $99\ldots900\ldots0$, nel nostro caso di quozienti di polinomi, risultano essere i polinomi del tipo $x^{a+b} - x^b = x^a(x^b - 1)$. Si noti la somiglianza coi numeri $99\ldots900\ldots0 = 10^a(10^b - 1)$.

In questa tesi trattiamo queste relazioni in modo approfondito. Nel primo capitolo sono ripresi alcuni risultati e alcune definizioni di Algebra relative ai monoidi ciclici e alle loro proprietà. Il secondo capitolo è dedicato alla relazione tra i monoidi ciclici finiti e i numeri razionali, ed è basato sull'articolo [1]. Infine, il terzo capitolo consiste nella parte originale della tesi e in esso è trattata la relazione tra monoidi ciclici e quozienti di polinomi.

Indice

Capitolo 1

Monoidi ciclici

1.1 Rappresentazione di monoidi ciclici

Iniziamo con alcune nozioni ben note relative ai monoidi.

Definizione 1.1. Un **monoide** $(M, \cdot)$ è un insieme M dotato di un'operazione $\cdot$ che soddisfa le seguenti proprietà:

(a) associatività: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ per ogni $a, b, c \in M$;

(b) identità: esiste un elemento $e \in M$ tale che $e \cdot a = a \cdot e = a$ per ogni $a \in M$.

In un monoide moltiplicativo $(M, \cdot)$ l'identità e si indica solitamente con 1 o 1_M. In un monoide additivo $(M, +)$, l'identità si indica con 0 o 0_M.

Sia M un monoide, un **sottomonoide** N di M è un sottoinsieme $N \subset M$ chiuso rispetto all'operazione $\cdot$ di M e tale che $1_M \in N$.

Definizione 1.2. Sia X un sottoinsieme di un monoide M. L'intersezione di tutti i sottomonoidi di M che contengono l'insieme X è un sottomonoide di M, in particolare è il più piccolo sottomonoide di M contenente X. È detto il **sottomonoide di M generato da X** e lo si denota con $\langle X \rangle$. Si ha

$$\langle X \rangle = \{1_M, x_1 \dots x_n \mid n \in \mathbb{N}^*, x_1, \dots, x_n \in X\}.$$

Se $X = \{a\}$ ha un solo elemento, il sottomonoide $\langle a \rangle$ è detto **ciclico** e si scrive nella forma

$$\langle a \rangle = \{a^n \mid n \in \mathbb{N}\}.$$

Sappiamo che i gruppi ciclici sono isomorfi a $\mathbb{Z}/n\mathbb{Z}$ per qualche $n \in \mathbb{N}^*$ e che possono essere rappresentati nel modo seguente:

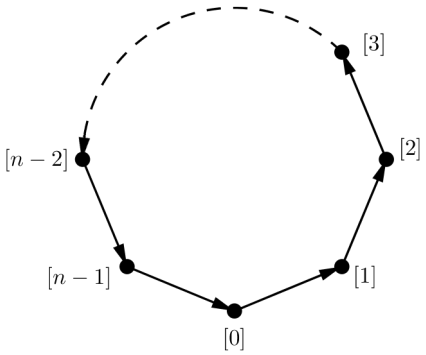


Figura 1.1: Il gruppo ciclico $\mathbb{Z}/n\mathbb{Z}$

I monoidi ciclici finiti si comportano in modo diverso, ed è quello che presenteremo in questo capitolo.

Lemma 1.1. *Sia M un monoide ciclico finito, $M = \langle a \rangle$. Allora M è isomorfo a $C_{t,\ell} = \{1, a, \ldots, a^{t+\ell-1} \mid a^{t+k} = a^{t+\ell+k}$ per ogni $k \geq 0\}$, con $\ell \geq 1$.*

Si può quindi dire che i monoidi ciclici finiti sono "periodici a partire da un certo punto in poi".

L'insieme dei numeri naturali $\mathbb{N}$ è un monoide sia rispetto all'addizione che alla moltiplicazione. Vedremo che ogni monoide ciclico finito M è isomorfo a un monoide quoziente additivo $\mathbb{N}/\sim_{t,\ell}$ per qualche parametro $t, \ell \in \mathbb{N}$, $\ell \geq 1$. La relazione di equivalenza $\sim_{t,\ell}$ su $\mathbb{N}$ è definita da: per ogni $x, y \in \mathbb{N}$,

$$x \sim_{t,\ell} y \text{ se } \begin{cases} x = y, \text{ o} \\ x \geq t,\ y \geq t \text{ and } x \equiv y \mod \ell. \end{cases}$$

È possibile mostrare che le relazioni di equivalenza del tipo $\sim_{t,\ell}$ sono tutte le congruenze nel monoide additivo $\mathbb{N}$ diverse dalla relazione di uguaglianza $=$, ovvero sono tutte le relazioni di equivalenza $\sim$ di $\mathbb{N}$ tali che $x \sim y \Rightarrow x + z \sim y + z$ per ogni $x, y, z \in \mathbb{N}$.

Notazione: Sia $\sim$ una relazione di equivalenza su un insieme A. Indichiamo con $[a]_\sim$ la classe di equivalenza di a modulo $\sim$. Quindi $[a]_\sim$ è l'insieme di tutti gli elementi $b \in A$ tali che $b \sim a$.

Il quoziente di $\mathbb{N}$ rispetto alla relazione di equivalenza $\sim_{t,\ell}$ è

$$\mathbb{N}/\!\sim_{t,\ell} = \{[0]_{\sim_{t,\ell}}, [1]_{\sim_{t,\ell}}, \ldots, [t+\ell-1]_{\sim_{t,\ell}}\},$$

dove gli elementi $[0]_{\sim_{t,\ell}}$, $[1]_{\sim_{t,\ell}}$, $\ldots$, $[t+\ell-1]_{\sim_{t,\ell}}$ di $\mathbb{N}/\!\sim_{t,\ell}$ sono a due a due distinti. L'insieme $\mathbb{N}/\!\sim_{t,\ell}$, rispetto all'operazione indotta dall'addizione su $\mathbb{N}$, è un monoide ciclico generato dalla classe di equivalenza $[1]_{\sim_{t,\ell}}$. Gli elementi di $\mathbb{N}/\!\sim_{t,\ell}$ sono:

$$\begin{aligned}
&[0]_{\sim_{t,\ell}} = \{0\},\\
&[1]_{\sim_{t,\ell}} = \{1\},\\
&[2]_{\sim_{t,\ell}} = \{2\},\\
&\vdots\\
&[t-2]_{\sim_{t,\ell}} = \{t-2\},\\
&[t-1]_{\sim_{t,\ell}} = \{t-1\},\\
&[t]_{\sim_{t,\ell}} = \{t, t+\ell, t+2\ell, \ldots\},\\
&[t+1]_{\sim_{t,\ell}} = \{t+1, t+1+\ell, t+1+2\ell, \ldots\},\\
&\vdots\\
&[t+\ell-2]_{\sim_{t,\ell}} = \{t+\ell-2, t+\ell-2+\ell, t+\ell-2+2\ell, \ldots\},\\
&[t+\ell-1]_{\sim_{t,\ell}} = \{t+\ell-1, t+\ell-1+\ell, t+\ell-1+2\ell, \ldots\}.
\end{aligned}$$

La struttura del quoziente $\mathbb{N}/\!\sim_{t,\ell}$ è periodica a partire da $[t]_{\sim_{t,\ell}}$ in poi, ovvero consiste in un ciclo di lunghezza ℓ preceduto da una coda di

lunghezza t che parte da $[0]_{\sim_{t,\ell}}$ e si può rappresentare nella forma:

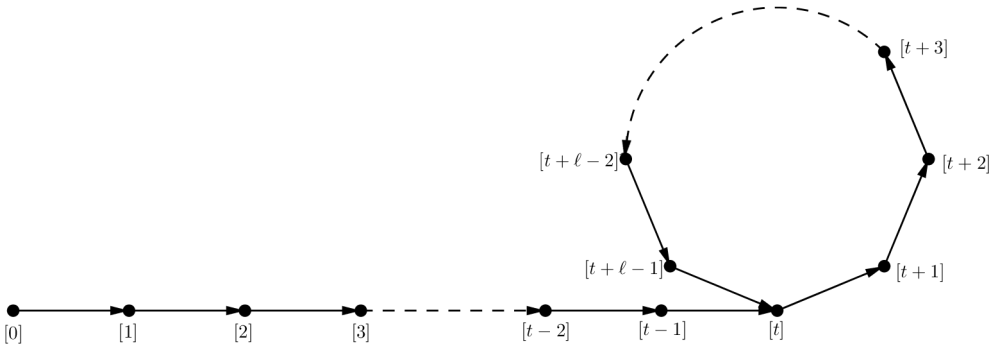


Figura 1.2: Il monoide ciclico $\mathbb{N}/\sim_{t,\ell}$

1.2 Classi laterali di monoidi modulo sottomonoidi ciclici

Il resto di questo capitolo e il capitolo successivo si basano sull'articolo [1] di A. Facchini e G. Simonetta.

Sia M un monoide e sia N un sottomonoide di M. Dato $x \in M$, possiamo considerare la **classe laterale sinistra** $xN = \{xn \mid n \in N\}$ di x modulo N. Si noti che le classi laterali sinistre modulo N non formano una partizione di M, come succede invece per i gruppi.

Sia M un monoide finito e sia $N = \langle y \rangle$ il sottomonoide ciclico generato da $y \in N$. In questo caso si ha $xN = \{xy^k \mid k \in \mathbb{N}\}$ per ogni $x \in M$. Consideriamo la mappa $f : \mathbb{N} \to M$, definita da $f(k) = xy^k$ per ogni $k \in \mathbb{N}$. L'immagine della mappa f è la classe laterale sinistra di x modulo il sottomonoide ciclico $\langle y \rangle = \{y^k \mid k \in \mathbb{N}\}$ di M generato da y.

Siano A e B due insiemi, consideriamo la mappa $f : A \to B$, allora esiste una relazione di equivalenza $\sim_f$ su A definita, per ogni $a, a' \in A$, da $a \sim_f a'$ se $f(a) = f(a')$. Questa relazione è detta la **relazione di equivalenza su A associata a f**.

Lemma 1.2. *Sia M un monoide moltiplicativo finito e siano $x, y \in M$. Sia $f : \mathbb{N} \to M$ la mappa definita da $f(k) = xy^k$, per ogni $k \in \mathbb{N}$. Allora la relazione di equivalenza $\sim_f$ associata a f è una delle equivalenze $\sim_{t,\ell}$, per opportuni $t, \ell \in \mathbb{N}$, con $\ell \geq 1$.*

Dimostrazione. Sia $s \in \mathbb{N}$ il più piccolo intero tale che $xy^t = xy^s$ per un opportuno $t \in \mathbb{N}$, $t < s$. Sia $\ell = s - t$. Per come abbiamo scelto s, gli elementi $x, xy, \ldots, xy^{s-1}$ sono tutti distinti e, in particolare, t e ℓ sono univocamente determinati. Per ogni $k \geq 0$, $xy^{t+k} = xy^{t+\ell+k}$, perché $xy^t = xy^s$ e $s = t + \ell$, ovvero, per ogni $k \geq 0$, $f(t + k) = f(t + \ell + k)$. Da cui, $[t + k]_{\sim_f} \supseteq \{t + k, t + k + \ell, t + k + 2\ell, \ldots\} = [t + k]_{\sim_{t,\ell}}$, dunque $i \sim_{t,\ell} j \Rightarrow i \sim_f j$. Viceversa, supponiamo $xy^i = xy^j$, cioè $f(i) = f(j)$. Esistono $i' < t + \ell$ e $j' < t + \ell$ tali che $i' \sim_{t,\ell} i$ e $j' \sim_{t,\ell} j$. Per quanto visto sopra, $xy^{i'} = xy^i = xy^j = xy^{j'}$. Poiché $i', j' < s$, per la minimalità di s, si ha $i' = j'$. Dunque $i \sim_{t,\ell}$. □

La classe laterale $x\langle y\rangle$ può quindi essere rappresentata da un ciclo con una coda, come nella Figura 1.2.

Esempio 1.1. Sia $M = \mathbb{Z}/14\mathbb{Z}$. Consideriamo $y = \overline{10} = 10 + 14\mathbb{Z}$. Si ha $\langle y\rangle = \{\overline{1}, \overline{10}, \overline{2}, \overline{6}, \overline{4}, \overline{12}, \overline{8}\}$. Vediamo le classi laterali $x\langle y\rangle$ al variare di $x \in \mathbb{Z}/14\mathbb{Z}$.

$$
\begin{array}{lll}
x\langle y\rangle\colon & x = \overline{0}, & x\langle y\rangle = \{\overline{0}\} \\
& x = \overline{3}, & x\langle y\rangle = \{\overline{3}, \overline{2}, \overline{6}, \overline{4}, \overline{12}, \overline{8}, \overline{10}\} \\
& x = \overline{2}, & x\langle y\rangle = \{\overline{2}, \overline{6}, \overline{4}, \overline{12}, \overline{8}, \overline{10}\} \\
& x = \overline{7}, & x\langle y\rangle = \{\overline{7}, \overline{0}\}
\end{array}
$$

Queste classi laterali possono essere rappresentate nel seguente modo:

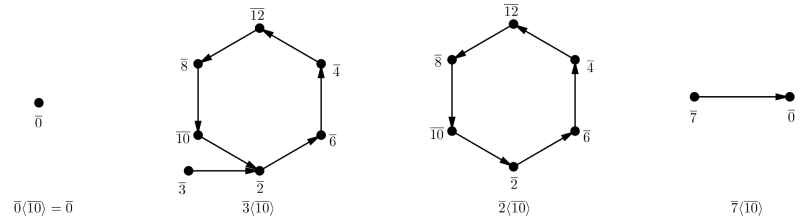


Figura 1.3: Le classi laterali di $\langle\overline{10}\rangle$

Nelle ipotesi del Lemma 1.2, diciamo che $\sim_{t,\ell}$ è il **tipo di periodicità** della classe laterale xN di x modulo N. In particolare, per $x = 1$, definiamo allo stesso modo il tipo di periodicità del monoide ciclico $N = \langle y \rangle$. Chiaramente si ha $N \cong \mathbb{N}/\sim_{t,\ell}$.

Come abbiamo detto, le congruenze del monoide additivo $\mathbb{N}$ sono le relazioni di equivalenza $\sim_{t,\ell}$, con $t \geq 0$ e $l \geq 1$, e l'uguaglianza $=$. Possiamo definire un ordine parziale sull'insieme $\mathrm{Cong}(\mathbb{N})$, ponendo

$$\sim \leq \simeq \text{ se, per ogni } n, m \in \mathbb{N},\ n \sim m \Rightarrow n \simeq m.$$

Allora l'elemento minimo di $\mathrm{Cong}(\mathbb{N})$ è l'uguaglianza $=$, e l'elemento massimo è la congruenza banale $\sim_{0,1}$. Inoltre, $\sim_{t,\ell} \leq \sim_{t',\ell'}$ se e solo se $t' \leq t$ e $\ell' \mid \ell$. Concludiamo quindi che l'insieme $\mathrm{Cong}(\mathbb{N})$ è un reticolo.

Lemma 1.3. *Sia $N = \langle y \rangle$ un sottomonoide ciclico di un monoide finito M. Siano $a, s \in M$. Allora il tipo di periodicità della classe laterale aN è minore o uguale al tipo di periodicità della classe laterale saN.*

Dimostrazione. Consideriamo la mappa $f : \mathbb{N} \to M$, definita come $f(k) = ay^k$ per ogni $k \in \mathbb{N}$, e la mappa $g : M \to M$, definita come $g(z) = sz$ per ogni $z \in M$. Allora la mappa $g \circ f : \mathbb{N} \to M$ è definita come $g \circ f(k) = say^k$ per ogni $k \in \mathbb{N}$. Per le relazioni di equivalenza associate alle funzioni, si ha $\sim_f \leq \sim_{g \circ f}$, ovvero $n \sim_f m \Rightarrow n \sim_{g \circ f} m$ per ogni $m, n \in \mathbb{N}$. □

Lemma 1.4. *Se una successione $r_0, r_1, \ldots$ è periodica di periodo $\ell \geq 1$ ed periodica di periodo $\ell' \geq 1$, allora è periodica di periodo* $\mathrm{mcd}(\ell, \ell')$.

Dimostrazione. Se ℓ divide ℓ' o se ℓ' divide ℓ è ovvio. Supponiamo allora che ℓ non divida ℓ' e che ℓ' non divida ℓ. Sia $\ell'' = \mathrm{mcd}(\ell, \ell')$, per l'identità di Bézout, esistono due interi $a, b \in \mathbb{Z}$ tali che $\ell'' = a\ell + b\ell'$. Poiché $\ell'' < \ell, \ell'$, allora $a < 0$ o $b < 0$. Possiamo assumere $b < 0$, dunque $a > 0$. Allora, per ogni $n, k \geq 0$, $r_{n+k\ell''} = r_{n+ka\ell+kb\ell'}$, ma $r_{n+ka\ell+kb\ell'} = r_{n+ka\ell}$, per la periodicità in ℓ', e $r_{n+ka\ell} = r_n$, per la periodicità in ℓ. Quindi $r_{n+k\ell''} = r_n$, la sequenza è periodica di periodo ℓ''. □

Da questo Lemma seguono due risultati.

Corollario 1.5. *Se una successione $r_0, r_1, \ldots$ è periodica di periodo ℓ a partire da r_t in poi, e periodica di periodo ℓ' a partire da $r_{t'}$ in poi, allora è anche periodica di periodo ℓ'' a partire da $r_{t''}$ in poi, dove $t'' = \min\{t, t'\}$ e $\ell'' = \mathrm{mcd}(\ell, \ell')$.*

Corollario 1.6. *Se una successione $r_0, r_1, \ldots$ è periodica da un certo punto in poi, allora esistono due interi "minimi" $t \geq 0$ e $\ell \geq 1$ tali che la sequenza sia periodica di periodo ℓ a partire da r_t in poi. Inoltre, per ogni altra coppia di interi $t' \geq 0$ e $\ell' \geq 1$, si ha che la sequenza è periodica di periodo ℓ' da $r_{t'}$ in poi se e solo se $t \leq t'$ e $\ell \mid \ell'$.*

Capitolo 2

Numeri razionali, numeri reali, periodicità

2.1 Rappresentazione decimale di un reale

Un numero reale positivo α può essere rappresentato in notazione decimale come

$$\alpha = d_N \dots d_1 d_0, d_{-1} d_{-2} \dots,$$

dove $d_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ per ogni $i \leq N$. Equivalentemente,

$$\alpha = \sum_{i=0}^{N} d_i 10^i + \sum_{i=1}^{\infty} d_{-i} 10^{-i},$$

dove $\sum_{i=0}^{N} d_i 10^i$ è la **parte intera** di α e $\sum_{i=1}^{\infty} d_{-i} 10^{-i}$ è la **parte frazionaria** di α.

Proposizione 2.1. *Un numero reale positivo scritto in notazione decimale $\alpha = d_N \dots d_1 d_0, d_{-1} d_{-2} \dots$, è razionale se e solo se le cifre d_i si ripetono periodicamente a partire da un certo indice in poi.*

Dimostrazione.

($\Leftarrow$) Supponiamo che la sequenza $d_N, \dots, d_0, d_{-1}, \dots$ sia periodica a partire da un certo indice in poi, ovvero supponiamo che, dopo d_{-t}, le

cifre $d_{-t-1}, \ldots, d_{-t-\ell}$ si ripetano ciclicamente. Lo scriviamo nella forma

$$\alpha = d_N \ldots d_0, d_{-1} \ldots d_{-t} \overline{d_{-t-1} \ldots d_{-t-\ell}}$$

con $t \geq 0$ e $\ell \geq 1$. Allora possiamo calcolare

$$\alpha \cdot 10^t = (d_N \ldots d_1 d_0 d_{-1} \ldots d_{-t}) + 0, \overline{d_{-t-1} \ldots d_{-t-\ell}}$$

e

$$\begin{aligned} \alpha \cdot 10^{t+\ell} &= (d_N \ldots d_1 d_0 d_{-1} \ldots d_{-t-\ell}) + 0, \overline{d_{-t-\ell-1} \ldots d_{-t-2\ell}} \\ &= (d_N \ldots d_1 d_0 d_{-1} \ldots d_{-t-\ell}) + 0, \overline{d_{-t-1} \ldots d_{-t-\ell}}. \end{aligned}$$

Da cui si ha

$$\begin{aligned} \alpha 10^{t+\ell} - \alpha 10^t = &(d_N \ldots d_1 d_0 d_{-1} \ldots d_{-t-\ell}) + \\ &- (d_N \ldots d_1 d_0 d_{-1} \ldots d_{-t}) \end{aligned}$$

e questo è un intero che possiamo chiamare $A \in \mathbb{Z}$. Allora

$$\begin{aligned} &\alpha 10^{t+\ell} - \alpha 10^t = A \\ &\Rightarrow \alpha = \frac{A}{10^{t+\ell} - 10^t} \in \mathbb{Q} \end{aligned}$$

($\Rightarrow$) Sia $\alpha = \frac{m}{n} \in \mathbb{Q}$, con $m, n \in \mathbb{N}^*$. Vogliamo scrivere α in notazione decimale. Procediamo induttivamente.
Passo zero: tramite divisione Euclidea, dividiamo m per n e troviamo $m = a_0 n + r_0$, con $a_0, r_0 \in \mathbb{Z}$ e $0 \leq r_0 < n$
Consideriamo ora $10r_0$, poiché $r_0 < n$, allora $10r_0 < 10n$, dunque il quoziente di $10r_0$ per n è un numero naturale minore di 10.
Passo uno: dividiamo $10r_0$ per n e troviamo $10r_0 = a_1 n + r_1$, con $0 \leq a_1 < 10$ e $0 \leq r_1 < n$.
Iterando, arriviamo al Passo i: dividiamo $10r_{i-1}$ per n e troviamo $10r_{i-1} = a_i n + r_i$, con $0 \leq a_i < 10$ e $0 \leq r_i < n$.
Otteniamo allora che

$$\alpha = \frac{m}{n} = a_0 + \frac{r_0}{n} = a_0 + \frac{a_1}{10} + \frac{r_1}{10n} = \cdots = a_0 + \sum_{i=1}^{\infty} a_i 10^{-i},$$

quindi la rappresentazione decimale della parte frazionaria di α è $,a_1a_2\ldots$. Dobbiamo dimostrare che la sequenza di cifre $a_1, a_2, \ldots$ è periodica da un certo punto in poi.
Ora, per quanto visto, $m \equiv r_0 \mod n$ e $10r_{i-1} \equiv r_i \mod n$ per ogni $i \geq 1$, allora $r_i \equiv m10^i \mod n$ per ogni $i \geq 0$. Allora le classi $\overline{r_0}, \overline{r_1}, \ldots$ di congruenza modulo n sono elementi della classe laterale $\overline{m}\langle\overline{10}\rangle$ in $\mathbb{Z}/n\mathbb{Z}$. Per cui, come abbiamo visto, gli elementi $\overline{r_i} \in \mathbb{Z}/n\mathbb{Z}$ sono periodici da un certo punto in poi. Dato che $0 \leq r_i < 0$ per ogni $i \geq 0$, allora $r_i = \overline{r_i}$ in $\mathbb{Z}/n\mathbb{Z}$, dunque anche la sequenza $r_0, r_1, \ldots$ è periodica da un certo punto in poi. Ma $10r_{i-1} = a_in + r_i$ per ogni $i \geq 1$, quindi anche la sequenza $a_1, a_2, \ldots$ è periodica da un certo punto in poi.

□

La dimostrazione prova che i numeri razionali $\alpha \in (0, 1)$ possono essere rappresentati come un ciclo con una coda.

Esempio 2.1. Sia $\alpha = \frac{122241}{222220} \in \mathbb{Q}$. Il numero razionale α ha rappresentazione decimale $\alpha = 0,55\overline{00900}$ e può essere rappresentato nel modo seguente:

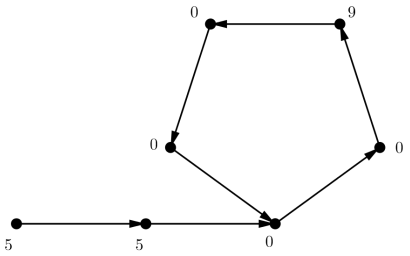


Figura 2.1: Rappresentazione del numero razionale $\alpha = \frac{122241}{222220}$

Definizione 2.1. Sia α un numero razionale positivo. Se $t \geq 0$ e $\ell \geq 1$ sono i più piccoli interi per cui α può essere scritto nella forma

$$\alpha = d_N d_{N-1} \ldots d_1 d_0, a_1 a_2 \ldots a_t \overline{a_{t+1} a_{t+2} \ldots a_{t+\ell}},$$

diremo che la congruenza $\sim_{t,\ell}$ di $\mathbb{N}$ è il **tipo di periodicità** di α. Quindi $t \geq 0$ e $\ell \geq 1$ sono i più piccoli interi tali che

$$\text{per ogni } i, j \in \mathbb{N},\ i \sim_{t,\ell} j \Rightarrow a_{i+1} = a_{j+1}.$$

La congruenza $\sim_{t,\ell}$ è la più grande congruenza in $\mathbb{N}$ con questa proprietà, ovvero, la parte frazionaria di α non può essere scritta in notazione decimale con meno di $t + \ell$ cifre.

Teorema 2.2. *Sia $\sim_{t,\ell}$ il tipo di periodicità di $\alpha = \frac{m}{n}$, con $m, n \in \mathbb{N}^*$, $t \geq 0$ e $\ell \geq 1$. Allora la mappa $f : \mathbb{N} \to \mathbb{Z}/n\mathbb{Z}$, definita da $f(k) = \overline{m} \cdot \overline{10}^k$ per ogni $k \in \mathbb{N}$, ha come immagine la classe laterale $\overline{m}\langle\overline{10}\rangle$ di $\overline{m}$ modulo il sottomonoide ciclico di $\mathbb{Z}/n\mathbb{Z}$ generato da $\overline{10}$ e la relazione di equivalenza associata a f è $\sim_{t,\ell}$. In particolare, esiste una biiezione canonica tra $\mathbb{N}/\sim_{t,\ell}$ e $\overline{m}\langle\overline{10}\rangle$, in modo tale che il tipo di periodicità di $\overline{m}\langle\overline{10}\rangle$ coincide con il tipo di periodicità di α.*

Dimostrazione. Banalmente si vede che l'immagine della mappa f è la classe laterale $\overline{m}\langle\overline{10}\rangle$, per definizione.
Quindi dobbiamo solo mostrare che la relazione di equivalenza associata a f è la relazione $\sim_{t,\ell}$. Come nella dimostrazione della Proposizione 2.1, con la divisione euclidea, otteniamo le cifre $a_1, a_2, \ldots$ della parte frazionaria di α, con $m = a_0 n + r_0$ e $10r_{i-1} = a_i n + r_i$ per ogni $i \geq 1$, da cui si vede che $r_i \equiv m10^i \mod n$ per ogni $i \geq 0$. Dunque $f(i) = \overline{m} \cdot \overline{10}^i = \overline{r_i}$ per ogni $i \geq 0$.

Per mostrare che $\sim_{t,\ell}$ è la relazione di equivalenza associata a f, dimostriamo che tutti gli $r_0, \ldots, r_{t+\ell-1}$ sono distinti e che $r_{t+k} = r_{t+\ell+k}$ per ogni $k \geq 0$.

Mostriamo che gli $r_0, \ldots, r_{t+\ell-1}$ sono tutti distinti. Per assurdo, supponiamo esistano $0 \leq i < j \leq t + \ell - 1$ tali che $r_i = r_j$. Allora, per come sono definite la sequenza delle cifre $a_1, a_2, \ldots$ e quella dei resti $r_0, r_1, \ldots$, segue che $a_{i+1} = a_{j+1}$ e $r_{i+1} = r_{j+1}$. Iterando si trova che $a_{i+k} = a_{j+k}$ per ogni $k \geq 0$. Allora la congruenza $\sim_{i,j-i}$ è tale che, per ogni $s, u \in \mathbb{N}$, $s \sim_{i,j-i} u \Rightarrow a_{s+1} = a_{u+1}$. Per la minimalità di t e ℓ si ha che $t \leq i$ e $\ell \leq j - i$, da cui $t + \ell \leq j$ e questa è una contraddizione.

Proviamo ora che $r_{t+k} = r_{t+\ell+k}$ per ogni $k \geq 0$. Abbiamo

$$\alpha = \frac{m}{n} = d_N d_{N-1} \dots d_1 d_0, a_1 a_2 \dots a_t \overline{a_{t+1} \dots a_{t+\ell}}.$$

Allora

$$\alpha \cdot 10^{t+k} = d_N d_{N-1} \dots d_1 d_0 a_1 \dots a_{t+k}, \overline{a_{t+k+1} \dots a_{t+\ell+k+1}}$$

e

$$\begin{aligned} \alpha \cdot 10^{t+\ell+k} &= d_N d_{N-1} \dots d_1 d_0 a_1 \dots a_{t+\ell+k}, \overline{a_{t+\ell+k+1} \dots a_{t+2\ell+k+1}} \\ &= d_N d_{N-1} \dots d_1 d_0 a_1 \dots a_{t+\ell+k}, \overline{a_{t+k+1} \dots a_{t+\ell+k+1}}, \end{aligned}$$

da cui si ha che

$$\begin{aligned} \alpha 10^{t+\ell+k} - \alpha 10^{t+k} = d_N d_{N-1} \dots d_1 d_0 a_1 \dots a_{t+\ell+k} + \\ - d_N d_{N-1} \dots d_1 d_0 a_1 \dots a_{t+k}. \end{aligned}$$

Chiamiamo A l'intero ottenuto, $A \in \mathbb{Z}$. Allora

$$m10^{t+\ell+k} - m10^{t+k} = nA.$$

Poiché, come abbiamo visto, $r_i \equiv m10^i \mod n$, si ha

$$r_{t+\ell+k} - r_{t+k} \equiv m10^{t+\ell+k} - m10^{t+k} = nA \equiv 0 \mod n,$$

allora $r_{t+\ell+k} \equiv r_{t+k} \mod n$, ma $r_i < n$ per ogni $i \geq 0$, da cui otteniamo che, per ogni $k \geq 0$, vale

$$r_{t+\ell+k} = r_{t+k}.$$

□

Questo Teorema determina il collegamento tra la rappresentazione decimale dei numeri razionali e le classi laterali di monoidi ciclici.

2.2 Criteri di divisibilità

In questa sezione vogliamo studiare le proprietà dei razionali del tipo $\frac{1}{n}$, dove $n \geq 2$ è un intero. Usiamo la stessa notazione della precedente sezione: $\sim_{t,\ell}$ è il tipo di periodicità di $\frac{1}{n}$, $10r_{i-1} = a_i n + r_i$ con $0 \leq r_i < n$ per ogni $i \geq 1$ e $r_0 = 1$, e $r_i \equiv 10^i \mod n$ per ogni $i \geq 0$. In questo caso particolare, la mappa considerata nel Teorema 2.1 è un omomorfismo di monoidi, segue quindi che esiste un isomorfismo canonico tra il monoide $\mathbb{N}/\sim_{t,\ell}$ e il sottomonoide ciclico $\langle\overline{10}\rangle$ del monoide moltiplicativo $\mathbb{Z}/n\mathbb{Z}$.

Proposizione 2.3. *Sia $n \geq 2$ un intero e siano $r_0, r_1, r_2, \ldots$ i resti delle divisioni euclidee di $1, 10, 10^2, \ldots$ per n. Allora la successione $r_0, r_1, r_2, \ldots$ ha le seguenti proprietà:*

(a) la successione è periodica da un certo punto in poi, con lo stesso tipo di periodicità $\sim_{t,\ell}$ di $\frac{1}{n}$;

(b) (Teorema di Pascal) *un intero positivo $m = d_N \ldots d_0 \in \mathbb{Z}$, scritto in notazione decimale, è divisibile per n se e solo se $\sum_{i=0}^{N} r_i d_i$ è divisibile per n.*

Dimostrazione.

(a) Abbiamo visto che le seguenti affermazioni sono equivalenti:
   (1) $r_i = r_j$;
   (2) $\overline{r_i} = \overline{r_j}$ in $\mathbb{Z}/n\mathbb{Z}$;
   (3) $\overline{10}^i = \overline{10}^j$ in $\mathbb{Z}/n\mathbb{Z}$;
   (4) $i \sim_{t,\ell} j$, perché il monoide ciclico $\langle\overline{10}\rangle$ e $\mathbb{N}/\sim_{t,\ell}$ sono isomorfi.

   E da questo segue naturalmente la tesi del punto (a).

(b) Poiché $r_i \equiv 10^i \mod n$ per ogni $i \geq 0$, si ha

$$m = \sum_{i=0}^{N} d_i 10^i \equiv \sum_{i=0}^{N} d_i r_i \mod n.$$

   Da cui segue che m è divisibile per n ($m \equiv 0 \mod n$) se e solo se $\sum_{i=0}^{N} d_i r_i$ lo è ($\sum_{i=0}^{N} d_i r_i \equiv 0 \mod n$).

□

La Proposizione 2.3 determina i Criteri di divisibilità di un intero m per n. Questo procedimento è utile perché, a partire da $m = d_N \dots d_0$, otteniamo un intero $m' = \sum_{i=0}^{N} r_i d_i$ che, generalmente, è più piccolo di m, e quindi più facile da analizzare. Nel caso questo numero fosse ancora troppo grande, è possibile reiterare il procedimento applicandolo a m' al fine di ottenere un numero ancora più piccolo, e così via.

In questo risultato si vede anche che la sequenza dei resti $r_0, r_1, \dots$ ha la stessa struttura di monoide ciclico delle cifre della parte frazionaria di $\frac{1}{n}$, e del sottomonoide ciclico $\langle \overline{10} \rangle$ di $\mathbb{Z}/n\mathbb{Z}$.

Esempio 2.2. Vediamo i Criteri di divisibilità in alcuni casi particolari.

Casi $n = 2, 5, 10$: In questi tre casi la sequenza dei resti è $1, 0, 0, \dots$. Quindi un intero positivo $m = d_N \dots d_0$, scritto in notazione decimale, è divisibile per 2, 5 o 10 se e solo se $\sum_{i=0}^{N} r_i d_i = d_0$ è divisibile per 2, 5 o 10, rispettivamente. Il tipo di periodicità di $\frac{1}{2} = 0,5\overline{0}$, $\frac{1}{5} = 0,2\overline{0}$ e $\frac{1}{10} = 0,1\overline{0}$ è $\sim_{1,1}$.
Casi $n = 4, 8$: Se $n = 4$, la sequenza dei resti è $1, 2, 4, 0, 0, \dots$, se $n = 8$ la sequenza dei resti è $1, 2, 4, 0, 0, \dots$. Quindi un intero positivo $m = d_N \dots d_0$, scritto in notazione decimale, è divisibile per 4 se e solo se $\sum_{i=0}^{N} r_i d_i = d_0 + 2d_1$ è divisibile per 4, ed è divisibile per 8 se e solo se $\sum_{i=0}^{N} r_i d_i = d_0 + 2d_1 + 4d_2$ è divisibile per 8. Nella sequenza dei resti ogni elemento può essere sostituito con un altro a lui congruente modulo n. Se $n = 4$, $10 \equiv 2 \mod 4$ quindi $d_0 + 2d_1$ è divisibile per 4 se e solo se $d_0 + 10d_1$ lo è, ovvero se e solo se $d_1 d_0$, scritto in notazione decimale, lo è. Analogamente, per $n = 8$, si ha $10 \equiv 2 \mod 8$ e $100 \equiv 4 \mod 8$, quindi m è divisibile per 8 se e solo se $d_2 d_1 d_0$, scritto in notazione decimale, lo è. Il tipo di periodicità di $\frac{1}{4} = 0,25\overline{0}$ è $\sim_{2,1}$ e quello di $\frac{1}{8} = 0,125\overline{0}$ è $\sim_{3,1}$.
Casi $n = 3, 9$: In questi due casi, la sequenza dei resti è $1, 1, 1 \dots$. Quindi un intero positivo $m = d_N \dots d_0$, scritto in notazione decimale, è divisibile per 3 o per 9 se e solo se $\sum_{i=0}^{N} r_i d_i = \sum_{i=0}^{N} d_i$ è divisibile per 3 o 9. Il tipo di periodicità di $\frac{1}{3} = 0,\overline{3}$ e di $\frac{1}{9} = 0,\overline{1}$ è $\sim_{0,1}$.
Caso $n = 11$: Per $n = 11$, la sequenza dei resti è $1, 10, 1, 10, \dots$. Sostituiamo i resti uguali a 10 con $-1 \equiv 10 \mod 11$. Quindi un intero

positivo $m = d_N \dots d_0$, scritto in notazione decimale, è divisibile per n se e solo se $\sum_{i=0}^{N} r_i d_i = \sum_{i=0}^{N} (-1)^i d_i$ è divisibile per 11, ovvero se e solo se $d_0 + d_2 + d_4 + \cdots \equiv d_1 + d_3 + d_5 + \dots \mod 11$. Il tipo di periodicità di $\frac{1}{11} = 0,\overline{09}$ è $\sim_{0,2}$.

Casi $n = 6, 12$: Se $n = 6$, la sequenza dei resti è $1, 4, 4, 4, \dots$, se $n = 12$ la sequenza dei resti è $1, 10, 4, 4, 4, \dots$. Quindi un intero positivo $m = d_N \dots d_0$, scritto in notazione decimale, è divisibile per 6 se e solo se $\sum_{i=0}^{N} r_i d_i = d_0 + 4\sum_{i=1}^{N} d_i$ è divisibile per 6, ed è divisibile per 12 se e solo se $\sum_{i=0}^{N} r_i d_i = d_0 - 2d_1 + 4\sum_{i=2}^{N} r_i d_i$ è divisibile per 12. Il tipo di periodicità di $\frac{1}{6} = 0,1\overline{6}$ è $\sim_{1,1}$ e quello di $\frac{1}{12} = 0,08\overline{3}$ è $\sim_{2,1}$.

Caso $n = 7$: In questo caso la sequenza dei resti è periodica e ripete periodicamente le cifre $1, 3, 2, 6, 4, 5$, possiamo sostituire alcuni resti con numeri congruenti modulo 7: la sequenza è $1, 3, 2, -1, -3, -2$. Quindi un intero positivo $m = d_N \dots d_0$, scritto in notazione decimale, è divisibile per 7 se e solo se è divisibile per 7 anche il numero $\sum_{i=0}^{N} r_i d_i = d_0 + 3d_1 + 2d_2 - d_3 - 3d_4 - 2d_5 + d_6 + \dots$. Il tipo di periodicità di $\frac{1}{7} = 0,\overline{142857}$ è $\sim_{0,6}$.

2.3 Numeri della forma $99\dots900\dots0$

Sia $\alpha = \frac{1}{n} \in \mathbb{Q}$, con $n \in \mathbb{N}^*$. Per quanto visto nella dimostrazione della Proposizione 2.1, possiamo scrivere

$$\frac{1}{n}(10^{t+\ell} - 10^t) = A$$

per qualche $A \in \mathbb{Z}$, dunque

$$nA = 10^{t+\ell} - 10^t = \underbrace{99\dots9}_{\ell \text{ volte}}\underbrace{00\dots0}_{t \text{ volte}}.$$

Pertanto, ogni intero $n \geq 2$ divide un intero della forma $99\dots900\dots0$.

Proposizione 2.4. *Sia $n \geq 2$ un intero e sia $\sim_{t,\ell}$ il tipo di periodicità di $\frac{1}{n}$. Allora*

(a) $\underbrace{99\ldots9}_{\ell\ volte}\underbrace{00\ldots0}_{t\ volte}$ *è il più piccolo intero della forma* $9\ldots90\ldots0$ *divisibile per* n*;*

(b) per ogni $a \geq 1$*,* $b \geq 0$*, l'intero* n *divide* $\underbrace{99\ldots9}_{a\ volte}\underbrace{00\ldots0}_{b\ volte}$ *se e solo se* $\ell \mid a$ *e* $t \leq b$*.*

Dimostrazione. Siano $a \geq 1$ e $b \geq 0$ interi. Allora n divide

$$\underbrace{99\ldots9}_{a\,\text{volte}}\underbrace{00\ldots0}_{b\,\text{volte}} = (10^a - 1)10^b = 10^{a+b} - 10^b$$

se e solo se $10^{a+b} \equiv 10^b \mod n$, ovvero se e solo se $\overline{10}^{a+b} = \overline{10}^b$ nel monoide moltiplicativo $\mathbb{Z}/n\mathbb{Z}$. Dato che il sottomonoide ciclico di $\mathbb{Z}/n\mathbb{Z}$ generato da $\langle\overline{10}\rangle$ è isomorfo a $\mathbb{N}/\sim_{t,\ell}$, allora $\overline{10}^{a+b} = \overline{10}^b$ in $\mathbb{Z}/n\mathbb{Z}$ se e solo se $t \leq b$ e $\ell \mid a$. E questo prova il punto (b).

La dimostrazione del punto (a) segue da quanto visto, infatti l'intero $\underbrace{99\ldots9}_{\ell\,\text{volte}}\underbrace{00\ldots0}_{t\,\text{volte}}$ è il più piccolo tra i numeri $\underbrace{9\ldots9}_{a\,\text{volte}}\underbrace{0\ldots0}_{b\,\text{volte}}$ con $t \leq b$ e $\ell \mid a$. □

Esempio 2.3. Sia $n = 14$. Si ha $\frac{1}{14} = 0,0\overline{714285}$, quindi $\frac{1}{n}$ ha tipo di periodicità $\sim_{1,6}$ e dunque le cifre decimali della parte frazionaria possono essere rappresentate come nella Figura 2.2 a sinistra, ovvero con una coda di lunghezza 1 e un ciclo di lunghezza 6. La sequenza dei resti $r_0, r_1, \ldots$ segue lo stesso schema delle cifre decimali, questa è infatti costituita da 1 e da $10, 2, 6, 4, 12, 8$ che si ripetono ciclicamente, può essere rappresentata come nella Figura 2.2 a destra.

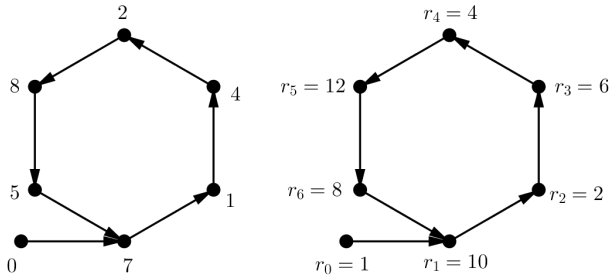


Figura 2.2: Rappresentazione del numero $\frac{1}{14}$ e della sequenza dei resti.

Inoltre, per la Proposizione 2.4, 14 divide 9999990, infatti $9999990 = 14 \cdot 714285$, e questo è il più piccolo intero di questa forma divisibile per 14.

Osservazione 1. Il numero m tale che $\underbrace{99\ldots9}_{\ell \text{ volte}}\underbrace{00\ldots0}_{t \text{ volte}}$ sia uguale a mn è $m = a_1 \ldots a_{t+\ell} - a_1 \ldots a_t$.
Infatti, se $mn = 10^{t+\ell} - 10^t$ e $\frac{1}{n} = 0, a_1 \ldots a_t\overline{a_{t+1} \ldots a_{t+\ell}}$, allora

$$m = (10^{t+\ell} - 10^t) \cdot 0, a_1 \ldots a_t\overline{a_{t+1} \ldots a_{t+\ell}} = a_1 \ldots a_{t+\ell} - a_1 \ldots a_t.$$

Possiamo riassumere alcuni dei risultati visti nella seguente Proposizione:

Proposizione 2.5. *Siano $t \geq 0$ e $\ell \geq 1$ interi. Un razionale positivo $\alpha \in \mathbb{Q}^+$ ha tipo di periodicità $\sim_{t,\ell}$ se e solo se α può essere scritto nella forma $\alpha = \frac{m}{n}$, dove:*

(1) m è un intero positivo;
(2) $n = \underbrace{99\ldots9}_{\ell \text{ volte}}\underbrace{00\ldots0}_{t \text{ volte}}$;
(3) $t \geq 1$ se m non è multiplo di 10;
(4) per ogni fattore primo p di ℓ, m non è multiplo di

$$\frac{10^\ell - 1}{10^{\frac{\ell}{p}} - 1} = \frac{\overbrace{99\ldots9}^{\ell \text{ volte}}}{\underbrace{99\ldots9}_{\frac{\ell}{p} \text{ volte}}}.$$

Osservazione 2. Sia $c = \frac{\ell}{p}$. La rappresentazione decimale di $\frac{10^\ell - 1}{10^c - 1}$ è

$$\frac{10^\ell - 1}{10^c - 1} = \sum_{i=0}^{p-1} 10^{ci} = \underbrace{1\underbrace{0\,0\ldots0}_{c-1 \text{ zeri}}1\underbrace{0\,0\ldots0}_{c-1 \text{ zeri}}1\underbrace{0\,0\ldots0}_{c-1 \text{ zeri}}\ldots1\underbrace{0\,0\ldots0}_{c-1 \text{ zeri}}}_{p-1 \text{ blocchi della forma } 100\ldots0}1$$

con $p-1$ blocchi della forma $100\ldots0$, ognuno dei quali con $c-1$ zeri, e termina con un ultimo 1.

Dimostrazione.

($\Rightarrow$) Sia $\alpha \in \mathbb{Q}^+$ un razionale positivo con tipo di periodicità $\sim_{t,\ell}$, con $t \geq 0$ e $\ell \geq 1$ i più piccoli interi tali che la rappresentazione decimale della parte frazionaria di α sia $,a_1a_2 \dots a_t\overline{a_{t+1}a_{t+2} \dots a_{t+\ell}}$. Abbiamo visto nella dimostrazione della dimostrazione della Proposizione 2.1 che si può scrivere $\alpha = \frac{m}{10^{t+\ell}-10^t}$, con $m \in \mathbb{Z}$. E questo prova i punti (1) e (2).
Sia $t \geq 1$, per assurdo, supponiamo m sia un multiplo di 10. Allora $m = 10m'$, per un opportuno $m' \in \mathbb{N}$, dunque

$$\alpha = \frac{m}{10^{t+\ell} - 10^t} = \frac{m'}{10^{t+\ell-1} - 10^{t-1}}.$$

Per cui la parte frazionaria di α, in notazione decimale, può essere scritta con $t-1$ cifre prima delle cifre periodiche, e questo contraddice la minimalità di t.
Infine, sia p un fattore primo di ℓ. Poniamo $c = \frac{\ell}{p}$. Per assurdo supponiamo m sia un multiplo di $\frac{10^\ell-1}{10^c-1}$, ovvero

$$m = m'\frac{10^\ell - 1}{10^c - 1},$$

per qualche intero $m' \in \mathbb{N}$. Si ha quindi

$$\alpha = \frac{m}{10^{t+\ell} - 10^t} = \frac{m'}{(10^c - 1)10^t}.$$

Allora α ha tipo di periodicità $\sim_{t,c'}$, ma $\sim_{t,c'} \geq \sim_{t,c} > \sim_{t,\ell}$, che è una contraddizione per la minimalità di t ed ℓ.

($\Leftarrow$) Sia $\alpha = \frac{m}{n} \in \mathbb{Q}$, con $m, n \in \mathbb{N}^*$ che soddisfano le proprietà (1)-(4). Per dimostrare che il tipo di periodicità di α è $\sim_{t,\ell}$, per il Teorema 2.2, dobbiamo provare che il tipo di periodicità della classe laterale $\overline{m}\langle\overline{10}\rangle$ del monoide moltiplicativo $\mathbb{Z}/n\mathbb{Z}$ è $\sim_{t,\ell}$. Ora $n = 10^{t+\ell} - 10^t$ divide $m(10^{t+\ell} - 10^t)$, quindi la sequenza $\overline{m}\overline{10}^i$ in $\mathbb{Z}/n\mathbb{Z}$ è periodica di periodo ℓ a partire da $\overline{m}\overline{10}^t$ in poi. Per assurdo, supponiamo che la periodicità non sia $\sim_{t,\ell}$, per il Corollario 1.6, ci sono due possibilità: o la sequenza è periodica partire da $\overline{m}\overline{10}^{t-1}$, oppure la

sequenza è periodica di periodo d, con $d \mid \ell$ e $d < \ell$. Nel primo caso, $t \geq 1$ e n divide $m(10^{t+\ell-1} - 10^{t-1})$, per cui 10 divide m, ma questo contraddice il punto (3). Nel secondo caso, assumiamo la sequenza $\overline{m10}^i$ sia periodica di periodo d da $\overline{m10}^t$ in poi. Se p è un divisore primo di $c = \frac{\ell}{d}$, allora esiste $\ell' \in \mathbb{N}$ tale che $p\ell' = \frac{\ell}{d}$. Perciò c è un multiplo di d, la sequenza è periodica di periodo c a partire da $\overline{m10}^t$ in poi. Quindi n divide $m(10^{t+c} - 10^t)$, per cui $\frac{10^\ell - 1}{10^c - 1}$ divide m. E questo contraddice la proprietà (4).

□

2.3.1 Fattori primi e periodicità

Scomponiamo un intero $n \geq 2$ in fattori primi. Poiché stiamo lavorando in base 10, si può pensare che i primi 2 e 5 abbiano una rilevanza diversa rispetto agli altri. Scriviamo la fattorizzazione nel modo seguente:

$$n = 2^{e_2} 5^{e_5} \prod_{p \in P} p^{e_p},$$

dove e_2 e e_5 sono interi non-negativi, P è un insieme finito di numeri primi diversi da 2 e 5, e e_p è un intero positivo, per ogni $p \in P$.

Proposizione 2.6. *Sia $n \geq 2$ un intero e sia $\sim_{t,\ell}$ il tipo di periodicità di $\frac{1}{n}$. Allora $t = \max\{e_2, e_5\}$ e ℓ è un divisore di* $\operatorname{mcm}\{\, p^{e_p} - p^{e_p - 1} \mid p \in P \,\}$.

Dimostrazione. Ricordiamo che gli interi $t \geq 0$ e $l \geq 1$ sono tali che il sottomonoide ciclico $\langle \overline{10} \rangle$ di $\mathbb{Z}/n\mathbb{Z}$ è isomorfo al monoide $\mathbb{N}/\sim_{t,\ell}$.

Per il Teorema Cinese del Resto, si ha l'isomorfismo canonico

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/2^{e_2}\mathbb{Z} \times \mathbb{Z}/5^{e_5}\mathbb{Z} \times \prod_{p \in P} \mathbb{Z}/p^{e_p}\mathbb{Z}.$$

Da cui, $10^i \equiv 10^j \mod n$ se e solo se la congruenza $10^i \equiv 10^j$ è soddisfatta modulo 2^{e_2}, modulo 5^{e_5} e modulo p^{e_p} per ogni $p \in P$.

Ovviamente, $10^{i-j} \equiv 0 \mod 2^{e_2}$ se e solo se $i - j \geq e_2$, cioè $10^i \equiv 10^j \mod 2^{e_2}$, se e solo se $i \sim_{e_2,1} j$. Analogamente, $10^i \equiv 10^j \mod 5^{e_5}$ se e solo se $i \sim_{e_5,1} j$.

Per $p \in P$, ovvero per un primo p coprimo con 10, la classe di 10 è invertibile in $\mathbb{Z}/p^{e_p}\mathbb{Z}$. Poiché il gruppo degli elementi invertibili è un gruppo ciclico di ordine $p^{e_p} - p^{e_p-1}$, se $i \equiv j \mod p^{e_p} - p^{e_p-1}$ allora $10^i \equiv 10^j \mod p^{e_p}$, da cui segue la tesi. □

Osservazione 3. Sia $n = 2^{e_2}5^{e_5}\prod_{p\in P} p^{e_p}$, come prima, e $t = \max\{e_2, e_5\}$. Poniamo $c := \prod_{p\in P}(p^{e_p} - p^{e_p-1})$. Per la Proposizione 2.6, $\frac{1}{n}$ può essere scritto, in notazione decimale, come $0, a_1a_2\ldots a_t\overline{a_{t+1}\ldots a_{t+c}}$, e la sequenza dei resti $r_0, r_1, \ldots$ consiste in t interi distinti $r_0 = 1, r_1, \ldots, r_{t-1}$ e c interi che si ripetono periodicamente. Inoltre n divide il numero $\underbrace{99\ldots9}_{c\text{volte}}\underbrace{00\ldots0}_{t\text{volte}}$.

Vogliamo mostrare che esiste una relazione tra il gruppo moltiplicativo $\mathbb{Q}^+$ e il reticolo $\mathrm{Cong}(\mathbb{N})$ delle congruenze in $\mathbb{N}$. Il gruppo moltiplicativo $\mathbb{Q}^+$ è un gruppo abeliano parzialmente ordinato rispetto all'ordine $\preceq$, definito da $\alpha \preceq \beta$ se $\frac{\beta}{\alpha} \in \mathbb{N}^*$, per ogni $\alpha, \beta \in \mathbb{Q}^+$. Dunque $(\mathbb{Q}^+, \preceq)$ è un reticolo, infatti se $\alpha, \beta \in \mathbb{Q}^+$, $\alpha = \frac{m}{n}$ e $\beta = \frac{m'}{n'}$, con $m, n, m', n' \in \mathbb{N}^*$, allora

$$\alpha \vee \beta = \frac{\mathrm{mcm}\{m, m'\}}{n} \qquad \text{e} \qquad \alpha \wedge \beta = \frac{\mathrm{mcd}\{m, m'\}}{n}.$$

L'ordine parziale indotto da $\preceq$ sul sottomonoide $\mathbb{N}^*$ di $\mathbb{Q}^+$ è l'ordine parziale di divisibilità $|$.

Consideriamo la funzione $F : \mathbb{Q}^+ \to \mathrm{Cong}(\mathbb{N})$, definita da $F(\alpha) = \sim_{t,\ell}$, dove $\sim_{t,\ell}$ è il tipo di periodicità di α. Mostriamo che F è un morfismo di insiemi parzialmente ordinati, ovvero è una mappa crescente. Siano $\alpha, \beta \in \mathbb{Q}^+$, con $\alpha \preceq \beta$, allora $\alpha = \frac{m}{n}$ e $\beta = \frac{ms}{n}$, per $m, n, s \in \mathbb{N}^*$. Il tipo di periodicità $\sim_{t,\ell}$ di α è lo stesso della classe laterale $\overline{m}\langle\overline{10}\rangle$ di $\mathbb{Z}/n\mathbb{Z}$, e il tipo di periodicità $\sim_{t',\ell'}$ di β è lo stesso della classe laterale $\overline{ms}\langle\overline{10}\rangle$ di $\mathbb{Z}/n\mathbb{Z}$. Dunque, per il Lemma 1.3, $\sim_{t,\ell} \leq \sim_{t',\ell'}$.

Da questo segue che, per un fissato elemento $\alpha \in \mathbb{Q}^+$, gli elementi $\beta \in \mathbb{Q}^+$ tali che $\alpha \preceq \beta$, ovvero $\beta = s\alpha$ per un qualche $s \in \mathbb{N}^*$, hanno solo un numero finito di possibili tipi di periodicità. Infatti, come abbiamo

visto, $\sim_{t,\ell} \leq \sim_{t',\ell'}$ se e solo se $t' \leq t$ e $\ell' \mid \ell$ e, ovviamente, c'è solo un numero finito di possibilità per t' e ℓ'. Si osservi che la funzione F non è un morfismo di reticoli. Per esempio, consideriamo $\frac{1}{2}, \frac{1}{5} \in \mathbb{Q}^+$, si ha $\frac{1}{2} \vee \frac{1}{5} = \frac{\text{mcm}\{2,5\}}{10} = 1$, $F(\frac{1}{2}) = \sim_{1,1}$, $F(\frac{1}{5}) = \sim_{1,1}$, ma $F(1) = \sim_{0,1}$.

Osservazione 4. I risultati di questo capitolo fanno riferimento alla notazione decimale, ovvero al fatto che è stata usata la base $b = 10$. Gli stessi risultati possono essere estesi ad ogni altra base $b \geq 2$, considerando il sottomonoide $\langle \overline{b} \rangle$ generato da b in $\mathbb{Z}/n\mathbb{Z}$, e le conseguenti sequenze della forma $\overline{m}\overline{b}^i$.

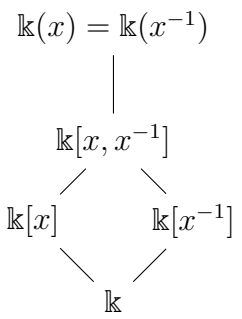
Capitolo 3

Polinomi, serie formali, periodicità

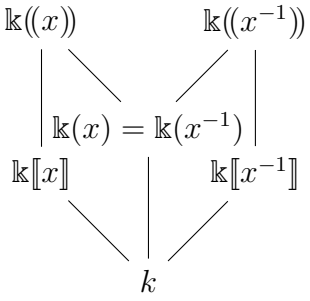
Passiamo ora alla parte originale della tesi. Vogliamo vedere come i risultati dell'articolo [1], presentati nei precedenti due capitoli, possano essere estesi sostituendo l'anello $\mathbb{Z}$ con l'anello $\Bbbk[x]$ dei polinomi a coefficienti in un campo $\Bbbk$.

3.1 Relazione tra quozienti di polinomi e serie formali di Laurent

Sia $\Bbbk$ un campo. Consideriamo gli anelli di polinomi in x e in x^{-1} a coefficienti in $\Bbbk$: $\Bbbk[x]$ e $\Bbbk[x^{-1}]$. Si hanno le seguenti relazioni di inclusione:



Se completiamo rispetto alle topologie (x)-adica e (x^{-1})-adica, otteniamo il diagramma:



Definizione 3.1. Sia $\Bbbk$ un campo. Consideriamo l'anello $\Bbbk[\![x]\!]$ delle serie formali a coefficienti in $\Bbbk$. Il suo campo delle frazioni è l'**anello $\Bbbk(\!(x)\!)$ delle serie formali di Laurent**, ovvero delle serie del tipo

$$f(x) = a_{-n}x^{-n} + \cdots + a_0 + \sum_{i=1}^{\infty} a_i x^i \ , \ a_i \in \Bbbk \ , \ n \in \mathbb{N}.$$

Proposizione 3.1. *Sia $\Bbbk$ un campo finito. Un quoziente di polinomi $\alpha(x) = \frac{m(x)}{n(x)}$, con $m(x), n(x) \in \Bbbk[x]$, $n(x) \neq 0$, può essere scritto come serie di Laurent in x^{-1}, ovvero come elemento di $\Bbbk(\!(x^{-1})\!)$. Inoltre, i coefficienti della serie trovata sono periodici a partire da un certo punto in poi.*

Dimostrazione. Sia $\alpha(x) = \frac{m(x)}{n(x)}$, con $m(x), n(x) \in \Bbbk[x]$, $n(x) \neq 0$. Per scrivere $\alpha(x)$ come serie di Laurent procediamo induttivamente.
Passo zero: tramite divisione Euclidea, dividiamo $m(x)$ per $n(x)$ e troviamo $m(x) = a_0(x)n(x)+r_0(x)$, con $a_0(x), r_0(x) \in \Bbbk[x]$ e $\delta(r_0(x)) < \delta(n(x))$, dove $\delta(p(x))$ indica il grado in x del polinomio p.
Consideriamo ora $xr_0(x)$, ovviamente $\delta(xr_0(x)) \leq \delta(n(x))$, dunque il quoziente di $xr_0(x)$ per $n(x)$ è un elemento del campo $\Bbbk$.
Passo uno: dividiamo $xr_0(x)$ per $n(x)$ e troviamo $xr_0(x) = a_1 n(x)+r_1(x)$, con $a_1 \in \Bbbk$, $r_1(x) \in \Bbbk[x]$ e $\delta(r_1(x)) < \delta(n(x))$.
Iterando, arriviamo al Passo i: dividiamo $xr_{i-1}(x)$ per $n(x)$ e troviamo $xr_{i-1}(x) = a_i n(x) + r_i(x)$, con $a_i \in \Bbbk$, $r_i(x) \in \Bbbk[x]$ e $\delta(r_i(x)) < \delta(n(x))$.

Otteniamo allora

$$\alpha(x) = \frac{m(x)}{n(x)} = a_0(x) + \frac{r_0(x)}{n(x)} = a_0(x) + \frac{a_1}{x} + \frac{r_1(x)}{xn(x)} = \cdots = a_0(x) + \sum_{i=1}^{\infty} a_i x^{-i}$$

e questo è proprio un elemento di $\Bbbk((x^{-1}))$.

La periodicità dei coefficienti della serie trovata segue dalla definizione degli stessi. I coefficienti sono infatti i quozienti delle divisioni euclidee effettuate. Dal momento che in ogni divisione i resti hanno grado strettamente minore del grado di $n(x)$ e poiché il campo $\Bbbk$ è finito, allora esiste solo un numero finito di possibili resti, ovvero ci sono $|\Bbbk|^{\delta(n(x))}$ possibilità. Ad un certo punto si avrà necessariamente $r_i(x) = r_j(x)$ per qualche $i, j \in \mathbb{N}, i \neq j$. Ne segue allora che $a_{i+1} = a_{j+1}$ e, per la ricorsività, si ha che $a_{i+1+p} = a_{j+1+p}$ per ogni $p \geq 0$. □

Corollario 3.2. *Sia $\Bbbk$ un campo finito. Un quoziente $\alpha(x) = \frac{m(x)}{n(x)}$, con $m(x), n(x) \in \Bbbk[x]$, $n(x) \neq 0$, può essere scritto come serie di Laurent in x, ovvero come elemento di $\Bbbk((x))$. Inoltre, i coefficienti della serie trovata sono periodici a partire da un certo punto in poi.*

Dimostrazione. Sia $\alpha(x) = \frac{m(x)}{n(x)} = \frac{x^a p(x)}{x^b q(x)}$, con $a, b \in \mathbb{Z}$ e $p(x), q(x) \in \Bbbk[x]$, con termine noto non nullo. Possiamo scrivere

$$\alpha(x) = x^{a-b} \frac{x^{\delta(p(x))} m'\left(\frac{1}{x}\right)}{x^{\delta(q(x))} n'\left(\frac{1}{x}\right)}.$$

Applichiamo una sostituzione: $y = \frac{1}{x}$ e consideriamo la frazione $\frac{m'(y)}{n'(y)}$. Procediamo induttivamente come nella dimostrazione precedente.
Passo zero: dividiamo $m'(y)$ per $n'(y)$ e troviamo $m'(y) = b_0(y)n'(y) + r_0(y)$, con $b_0(y), r_0(y) \in \Bbbk[y]$ e $\delta(r_0(y)) < \delta(n'(y))$.
Consideriamo ora $yr_0(y)$, ovviamente $\delta(yr_0(y)) \leq \delta(n'(y))$, dunque il quoziente di $yr_0(y)$ per $n'(y)$ è un elemento del campo $\Bbbk$.
Passo uno: dividiamo $yr_0(y)$ per $n'(y)$ e troviamo $yr_0(y) = b_1 n'(y) + r_1(y)$, con $b_1 \in \Bbbk$, $r_1(y) \in \Bbbk[y]$ e $\delta(r_1(y)) < \delta(n'(y))$.
Iterando, arriviamo al Passo i: dividiamo $yr_{i-1}(y)$ per $n'(y)$ e troviamo $yr_{i-1} = b_i n'(y) + r_i(y)$, con $b_i \in \Bbbk$, $r_i(y) \in \Bbbk[y]$ e $\delta(r_i(y)) < \delta(n'(y))$.

Otteniamo allora

$$\frac{m'(y)}{n'(y)} = b_0(y) + \frac{r_0(y)}{n'(y)} = b_0(y) + \frac{b_1}{y} + \frac{r_1(y)}{yn'(y)} = \cdots = b_0(y) + \sum_{i=1}^{\infty} b_i y^{-i}.$$

Da cui, risostituendo $x = \frac{1}{y}$, si ha

$$\alpha(x) = x^z \left(b_0(x^{-1}) + \sum_{i=1}^{\infty} b_i x^i \right) \ , \ z \in \mathbb{Z}$$

e questo è proprio un elemento di $\Bbbk(\!(x)\!)$.

La periodicità dei coefficienti segue come nella Proposizione 3.1. □

Esempio 3.1. Consideriamo il polinomio $\alpha(x) = \frac{1}{1-x}$. Studiamone lo sviluppo in serie formale di Laurent come elemento di $\Bbbk(\!(x^{-1})\!)$ e come elemento di $\Bbbk(\!(x)\!)$.

Svolgiamo i calcoli come nella precedenti dimostrazioni.

Vediamo prima lo svolgimento in $\Bbbk(\!(x^{-1})\!)$. Abbiamo $m(x) = 1$ e $n(x) = 1 - x$.

Passo zero: dividiamo 1 per $1 - x$ e troviamo $1 = 0 \cdot (1 - x) + 1$, con $a_0(x) = 0$ e $r_0(x) = 1$.
Passo uno: dividiamo x per $1 - x$ e troviamo $x = -1 \cdot (1 - x) + 1$, con $a_1 = -1$ e $r_1(x) = 1$.
Poiché $r_1(x) = 1 = r_0(x)$, la divisione seguente è uguale, e, iterando, si ha $r_i(x) = 1$ e $a_i = -1$ per ogni $i \geq 1$.
Dunque

$$\frac{1}{1-x} = 0 + \frac{1}{1-x} = 0 - \frac{1}{x} + \frac{1}{x(1-x)} = \cdots = -\sum_{i=1}^{\infty} x^{-i} \in \Bbbk(\!(x^{-1})\!).$$

Studiamo ora lo svolgimento in $\Bbbk(\!(x)\!)$.

Innanzitutto scriviamo

$$\frac{1}{1-x} = \frac{1}{x\left(\frac{1}{x} - 1\right)}$$

dunque, applicando la sostituzione $y = \frac{1}{x}$, si ha $m'(y) = 1$ e $n'(y) = y - 1$.
Passo zero: dividiamo 1 per $y - 1$ e troviamo $1 = 0 \cdot (y - 1) + 1$, con $b_0(y) = 0$ e $r_0(y) = 1$.
Passo uno: dividiamo y per $y - 1$ e troviamo $y = 1 \cdot (y - 1) + 1$, con $b_1 = 1$ e $r_1(y) = 1$.
Poiché $r_1(y) = 1 = r_0(y)$, la divisione seguente è uguale, e, iterando, si ha $r_i(y) = 1$ e $b_i = 1$ per ogni $i \geq 1$.
Dunque

$$\frac{m'(y)}{n'(y)} = 0 + \frac{1}{y-1} = 0 + \frac{1}{y} + \frac{1}{y(y-1)} = \cdots = \sum_{i=1}^{\infty} y^{-i}$$

e sostituendo nuovamente $x = \frac{1}{y}$ otteniamo

$$\alpha(x) = x^{-1}(x + x^2 + x^3 + \dots) = 1 + x + x^2 + \cdots = \sum_{i=0}^{\infty} x^i \in \Bbbk(\!(x)\!)$$

che è proprio la serie geometrica che ci aspettavamo.

Corollario 3.3. *La periodicità dei coefficienti della serie definita nella Proposizione 3.1 vale per un campo $\Bbbk$ se e solo se il campo $\Bbbk$ è un campo di caratteristica p algebrico sul suo campo fondamentale $\mathbb{F}_p$.*

Osservazione 5. Se $\Bbbk$ ha caratteristica p ed è algebrico su $\mathbb{F}_p$, allora la Proposizione 3.1 vale perchè $\Bbbk$ è unione diretta di campi finiti, in quanto

$$\Bbbk \subset \overline{\mathbb{F}}_p = \bigcup_{n \geq 1} \mathbb{F}_{p^n}.$$

Il sottocampo di $\Bbbk$ generato dai coefficienti di $m(x)$ e $n(x)$ è finitamente generato e dunque finito.
Negli altri casi la periodicità non vale:

- Se $\Bbbk$ non è algebrico.

  Esempio 3.2. Abbiamo visto che $\frac{1}{1-x} = 1 + x + x^2 + \dots$, quindi si ha $\frac{x}{x-1} = \frac{1}{1-\frac{1}{x}} = 1 + x^{-1} + x^{-2} + \dots$.

Sia ora τ un numero trascendente su $\mathbb{F}_p$ e consideriamo l'estensione trascendente $\mathbb{F}_p(\tau)$ di $\mathbb{F}_p$. Consideriamo il quoziente $\frac{\frac{1}{\tau}x}{\frac{1}{\tau}x-1}$, si ha

$$\frac{\frac{1}{\tau}x}{\frac{1}{\tau}x-1} = 1 + \tau x^{-1} + \tau^2 x^{-2} + \tau^3 x^{-3} + \dots$$

questa serie ha come coefficienti $\tau, \tau^2, \tau^3, \dots$, che sono tutti distinti in $\mathbb{F}_p(\tau)$. Infatti, se così non fosse, ovvero se $\tau^r = \tau^s$ per qualche $r \neq s$, allora τ sarebbe radice del polinomio $x^r - x^s \in \mathbb{F}_p[x]$ e dunque sarebbe algebrico.

- Se $\mathbb{k}$ ha caratteristica 0.

Esempio 3.3. Consideriamo il quoziente $\frac{1}{1-2x^{-1}}$, si ha

$$\frac{1}{1-2x^{-1}} = 1 + 2x^{-1} + 4x^{-2} + 8x^{-3} + \dots$$

questa serie ha come coefficienti $1, 2, 4, 8, \dots$ che sono tutti distinti.

Il viceversa dei risultati visti vale anche nel caso generale di un campo $\mathbb{k}$ qualsiasi.

Proposizione 3.4. *Sia $\mathbb{k}$ un campo. Sia $\alpha(x) = d_n x^n + \dots + d_0 + \sum_{i=1}^{\infty} a_i x^{-i} \in \mathbb{k}(\!(x^{-1})\!)$ una serie di Laurent con i coefficienti periodici da un certo punto in poi, ovvero esistono $t, \ell \in \mathbb{N}$, $\ell \geq 1$, tali che $a_{j+\ell} = a_j$ per ogni $j \geq t$. Allora $\alpha(x)$ può essere scritto come quoziente di polinomi $\alpha(x) = \frac{m(x)}{n(x)}$, con $m(x), n(x) \in \mathbb{k}[x]$, $n(x) \neq 0$.*

Dimostrazione. Sia $\alpha(x) = d_n x^n + \dots + d_0 + \sum_{i=1}^{\infty} a_i x^{-i} \in \mathbb{k}(\!(x^{-1})\!)$ tale che esistono $t, \ell \in \mathbb{N}$, $\ell \geq 1$, per cui $a_{j+\ell} = a_j$ per ogni $j \geq t$.

Allora possiamo calcolare

$$\begin{aligned}\alpha(x)\cdot x^t &= d_n x^{n+t} + \cdots + d_0 x^t + \sum_{i=1}^{\infty} a_i x^{t-i} \\ &= d_n x^{n+t} + \cdots + d_0 x^t + a_1 x^{t-1} + \cdots + a_t + a_{t+1}x^{-1} + \\ &\quad + a_{t+2}x^{-2} + \cdots + a_{t+\ell}x^{-\ell} + a_{t+\ell+1}x^{-\ell-1} + \dots \\ &= d_n x^{n+t} + \cdots + d_0 x^t + a_1 x^{t-1} + \cdots + a_t + a_{t+1}x^{-1} + \\ &\quad + a_{t+2}x^{-2} + \cdots + a_t x^{-\ell} + a_{t+1}x^{-\ell-1} + \dots\end{aligned}$$

e

$$\begin{aligned}\alpha(x)\cdot x^{t+\ell} &= d_n x^{n+t+\ell} + \cdots + d_0 x^{t+\ell} + \sum_{i=1}^{\infty} a_i x^{t+\ell-i} \\ &= d_n x^{n+t+\ell} + \cdots + d_0 x^{t+\ell} + a_1 x^{t+\ell-1} + \cdots + a_t x^{\ell} + \\ &\quad + a_{t+1}x^{\ell-1} + \cdots + a_{t+\ell} + a_{t+\ell+1}x^{-1} + \dots \\ &= d_n x^{n+t+\ell} + \cdots + d_0 x^{t+\ell} + a_1 x^{t+\ell-1} + \cdots + a_t x^{\ell} \\ &\quad + a_{t+1}x^{\ell-1} + \cdots + a_t + a_{t+1}x^{-1} + \dots.\end{aligned}$$

Da cui si ha che

$$\begin{aligned}\alpha(x)x^{t+\ell} - \alpha(x)x^t = {} & d_n x^{n+t+\ell} + \cdots + d_0 x^{t+\ell} + \\ & - d_n x^{n+t} - \cdots - d_0 x^t + \\ & + a_1 x^{t+\ell-1} + \cdots + a_{t-1}x^{\ell+1} + \\ & - a_1 x^{t-1} - \cdots - a_{t-1}x + \\ & + a_t x^{\ell} + \cdots + a_{t+\ell-1}x,\end{aligned}$$

e questo è un polinomio a coefficienti in $\Bbbk$, diciamo $p(x) \in \Bbbk[x]$. Allora

$$\begin{aligned}&\alpha(x)x^{t+\ell} - \alpha(x)x^t = p(x) \\ &\Rightarrow \alpha(x) = \frac{p(x)}{x^{t+\ell} - x^t} \in \Bbbk(x)\end{aligned}$$

□

Possiamo riassumere i risultati trovati nel seguente Teorema.

Teorema 3.5. *Sia $\Bbbk$ un campo di caratteristica p algebrico su $\mathbb{F}_p$. Una serie di Laurent $\alpha(x) = a_{-n}x^{-n} + \cdots + a_0 + \sum_{i=1}^{\infty} a_i x^i \in \Bbbk(\!(x)\!)$ è un elemento di $\Bbbk(x)$, ovvero può essere scritta come quoziente di due polinomi $\alpha(x) = \frac{m(x)}{n(x)}$, con $m(x), n(x) \in \Bbbk[x]$, $n(x) \neq 0$, se e solo se i suoi coefficienti a_i si ripetono periodicamente da un certo punto in poi.*

3.1.1 Periodicità in serie formali di Laurent

Consideriamo un campo $\Bbbk$ di caratteristica p algebrico su $\mathbb{F}_p$. Come abbiamo visto, la periodicità dei coefficienti delle serie di Laurent si trova nei coefficienti dei termini in x^i per le serie di $\Bbbk(\!(x)\!)$ e nei coefficienti dei termini in x^{-i} per le serie di $\Bbbk(\!(x^{-1})\!)$, $i \geq 0$. D'ora in poi considereremo solo serie con $a_0(x) = 0$ e $b_0(x) = 0$, ovvero quozienti del tipo

$$\alpha(x) = \frac{m(x)}{n(x)} \begin{cases} \in \Bbbk(\!(x)\!) & \text{con } \delta(m(x)) < \delta(n(x)) \\ \in \Bbbk(\!(x^{-1})\!) & \text{con } \delta(m(x)) > \delta(n(x)). \end{cases}$$

Definizione 3.2. Sia $\alpha(x) \in \Bbbk(x)$ e siano $t \geq 0$ e $\ell \geq 1$ i più piccoli interi per cui $\alpha(x)$ può essere scritto nella forma

$$\alpha(x) = a_0(x) + a_1 x^{-1} + \cdots + a_t x^{-t} + \overline{a_{t+1}x^{-t-1} + \cdots + a_{t+\ell}x^{-t-\ell}},$$

dove la parte barrata indica la sequenza dei coefficienti che si ripetono periodicamente. Diciamo che la congruenza $\sim_{t,\ell}$ è il **tipo di periodicità** di $\alpha(x)$. Equivalentemente, $t \geq 0$ e $\ell \geq 1$ sono i più piccoli interi tali che

$$\text{per ogni } i, j \in \mathbb{N},\ i \sim_{t,\ell} j \Rightarrow a_{i+1}(x) = a_{j+1}(x).$$

Esempio 3.4. Calcoliamo lo sviluppo in serie di Laurent del quoziente

$$\alpha(x) = \frac{x^3 + x^2 + 1}{x^7 - x^2} \in \Bbbk(x).$$

Divisioni:
$$\begin{aligned}
a_0 &= 0 \quad r_0(x) = x^3 + x^2 + 1 \\
a_1 &= 0 \quad r_1(x) = x^4 + x^3 + x \\
a_2 &= 0 \quad r_2(x) = x^5 + x^4 + x^2 \\
a_3 &= 0 \quad r_3(x) = x^6 + x^5 + x^3 \\
a_4 &= 1 \quad r_4(x) = x^6 + x^4 + x^2 \\
a_5 &= 1 \quad r_5(x) = x^5 + x^3 + x^2 \\
a_6 &= 0 \quad r_6(x) = x^6 + x^4 + x^3 \\
a_7 &= 1 \quad r_7(x) = x^5 + x^4 + x^2 = r_2(x)
\end{aligned}$$

Dunque $t = 2$ e $\ell = 5$, il suo sviluppo in serie di Laurent è

$$\begin{aligned}
\alpha(x) &= x^{-4} + x^{-5} + x^{-7} + x^{-9} + x^{-10} + x^{-12} + x^{-14} + x^{-15} + \dots \\
&= \overline{0 \cdot x^{-3} + 1 \cdot x^{-4} + 1 \cdot x^{-5} + 0 \cdot x^{-6} + 1 \cdot x^{-7}} \in \Bbbk(\!(x^{-1})\!).
\end{aligned}$$

e può essere rappresentato nel modo seguente

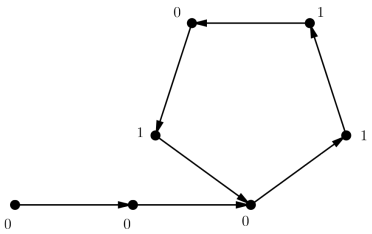


Figura 3.1: Rappresentazione del quoziente $\alpha(x) = \frac{x^3+x^2+1}{x^7-x^2}$

Teorema 3.6. *Sia $\sim_{t,\ell}$ il tipo di periodicità del quoziente di polinomi $\alpha(x) = \frac{m(x)}{n(x)}$, con $m(x), n(x) \in \Bbbk[x]$, $n(x) \neq 0$, e $t \geq 0$, $\ell \geq 1$. Allora la mappa $f : \mathbb{N} \to \Bbbk[x]/(n(x))$, definita da $f(k) := \overline{m(x)} \cdot \overline{x}^k$ per ogni $k \in \mathbb{N}$, ha come immagine la classe laterale $\overline{m(x)}\langle\overline{x}\rangle$ di $\overline{m(x)}$ modulo il sottomonoide del monoide ciclico generato da $\overline{x}$, e $\sim_{t,\ell}$ è la relazione di equivalenza associata ad f. In particolare, c'è una biiezione canonica tra $\mathbb{N}/\sim_{t,\ell}$ e la classe laterale $\overline{m(x)}\langle\overline{x}\rangle$, quindi il tipo di periodicità della classe laterale $\overline{m(x)}\langle\overline{x}\rangle$ coincide con il tipo di periodicità di $\alpha(x) = \frac{m(x)}{n(x)}$.*

Dimostrazione. Si prova facilmente che l'immagine della mappa f è la classe laterale $\overline{m(x)}\langle\overline{x}\rangle$.

Perciò dobbiamo solo mostrare che la relazione di equivalenza associata a f è la relazione $\sim_{t,\ell}$. Come nella dimostrazione della Proposizione 3.1, con la divisione euclidea tra polinomi, otteniamo i coefficienti $a_1, a_2, \ldots$ di $\alpha(x)$, con $m(x) = a_0(x)n(x) + r_0(x)$ e $xr_{i-1} = a_i n(x) + r_i(x)$ per ogni $i \geq 1$, da cui si vede che $r_i(x) \equiv x^i m(x) \mod n(x)$ per ogni $i \geq 0$. Dunque, $f(i) = \overline{m(x)} \cdot \overline{x}^i = \overline{r_i}$ per ogni $i \geq 0$.

Per mostrare che $\sim_{t,\ell}$ è la relazione di equivalenza associata a f, basta dimostrare che tutti gli $r_0(x), \ldots, r_{t+\ell-1}(x)$ sono distinti e che $r_{t+k}(x) = r_{t+\ell+k}(x)$ per ogni $k \geq 0$.

Mostriamo che gli $r_0(x), \ldots, r_{t+\ell-1}(x)$ sono tutti distinti. Per assurdo, supponiamo esistano $0 \leq i < j \leq t + \ell - 1$ tali che $r_i(x) = r_j(x)$. Allora, per come sono definiti i resti $r_0(x), r_1(x), \ldots$ e i coefficienti $a_1, a_2, \ldots$ della serie di Laurent associata, si ha $a_{i+1} = a_{j+1}$ e $r_{i+1}(x) = r_{j+1}(x)$. Iterando, segue che $a_{i+k} = a_{j+k}$ e $r_{i+k}(x) = r_{j+k}(x)$ per ogni $k \geq 0$. Dunque la relazione $\sim_{i,j-i}$ è tale che, per ogni $s, u \in \mathbb{N}$, $s \sim_{i,j-i} u \Rightarrow a_{s+1} = a_{u+1}$. Per la minimalità di t e ℓ, si ha che $t \leq i$ e $\ell \leq j - i$, da cui $t + \ell \leq j$ e questa è una contraddizione.

Vediamo ora che $r_{t+k}(x) = r_{t+\ell+k}(x)$ per ogni $k \geq 0$. Abbiamo

$$\frac{m(x)}{n(x)} = d_N x^N + \cdots + d_0 + a_1 x^{-1} + \cdots + a_t x^{-t} + \overline{a_{t+1}x^{-t-1} + \cdots + a_{t+\ell}x^{-t-\ell}}.$$

Allora

$$\alpha(x) \cdot x^{t+k} = d_N x^{N+t+k} + \cdots + a_{t+k} + \overline{a_{t+k+1}x^{-1} + \cdots + a_{t+\ell+k+1}x^{-t-\ell-1}}$$

e

$$\begin{aligned}\alpha(x) \cdot x^{t+\ell+k} &= d_N x^{N+t+\ell+k} + \cdots + a_{t+\ell+k} + \\ &\quad + \overline{a_{t+\ell+k+1}x^{-1} + \cdots + a_{t+2\ell+k+1}x^{-t-2\ell-1}} \\ &= d_N x^{N+t+\ell+k} + \cdots + a_{t+\ell+k} + \\ &\quad + \overline{a_{t+k+1}x^{-1} + \cdots + a_{t+\ell+k+1}x^{-t-\ell-1}}.\end{aligned}$$

Da cui si ha

$$\alpha(x)x^{t+\ell+k} - \alpha(x)x^{t+k} = d_N x^{N+t+\ell+k} + \cdots + a_{t+\ell+k} - d_N x^{N+t+k} - \cdots - a_{t+k}.$$

Chiamiamo $p(x)$ il polinomio ottenuto, $p(x) \in \Bbbk[x]$.

Allora

$$m(x)x^{t+\ell+k} - m(x)x^{t+k} = n(x)p(x).$$

Poiché, come abbiamo visto, $r_i(x) \equiv x^i m(x) \mod n(x)$, si ha

$$r_{t+\ell+k}(x) - r_{t+k}(x) \equiv m(x)x^{t+\ell+k} - m(x)x^{t+k} = n(x)p(x) \equiv 0 \mod n(x)$$

allora $r_{t+\ell+k}(x) \equiv r_{t+k}(x) \mod n(x)$, ma $\delta(r_i(x)) < \delta(n(x))$ per ogni $i \geq 0$, da cui otteniamo che, per ogni $k \geq 0$, vale

$$r_{t+\ell+k}(x) = r_{t+k}(x).$$

□

Come nel caso dei numeri razionali visto precedentemente, questo Teorema ci dà la connessione tra i polinomi frazionari e le classi laterali di monoidi ciclici.

3.2 Divisibilità di polinomi

In questa sezione vogliamo studiare le proprietà dei polinomi frazionari del tipo $\frac{1}{n(x)}$, dove $n(x) \in \Bbbk[x]$, $n(x) \neq 0$. Usiamo la stessa notazione della precedente sezione: $\sim_{t,\ell}$ è il tipo di periodicità di $\frac{1}{n(x)}$, $xr_{i-1}(x) = a_i n(x) + r_i(x)$, con $\delta(r_i(x)) < \delta(n(x))$ per ogni $i \geq 1$ e $r_0(x) = 1$, e $r_i(x) \equiv x^i \mod n(x)$ per ogni $i \geq 0$. In questo caso particolare, la mappa considerata nel Teorema 3.6 è un omomorfismo di monoidi, segue quindi che esiste un isomorfismo canonico tra il monoide $\mathbb{N}/\sim_{t,\ell}$ e il sottomonoide ciclico $\langle \overline{x} \rangle$ del monoide moltiplicativo $\Bbbk[x]/(n(x))$.

3.2.1 Criteri di divisibilità per polinomi

Sia $m(x) = a_0 + a_1 x + \cdots + a_n x^n \in \Bbbk[x]$ un polinomio. Sappiamo che x divide $m(x)$ se e solo se il suo termine noto è nullo, ovvero se e solo se $a_0 = 0$. Più in generale, x^s divide $m(x)$ se e solo se $a_0 = a_1 = \cdots = a_{s-1} = 0$.

Similmente, $x-1$ divide $m(x)$ se e solo se $\sum_{i=0}^{n} = 0$, e $x+1$ divide $m(x)$ se e solo se $\sum_{i=0}^{n}(-1)^i a_i = 0$.

Questi semplici fatti seguono dal Teorema di Ruffini.

Teorema 3.7 (Teorema di Ruffini)**.** *Siano $p(x) \in \Bbbk[x]$ e $a \in \Bbbk$. Allora a è radice di $p(x)$ se e solo se il polinomio $x-a$ divide $p(x)$ nell'anello $\Bbbk[x]$.*

Dimostrazione. Supponiamo $a \in \Bbbk$ sia radice di $p(x)$. Dividiamo $p(x)$ per $x-a$ e otteniamo $p(x) = q(x)(x-a) + r(x)$, con $q(x), r(x) \in \Bbbk[x]$ e $\delta(r(x)) < \delta(x-a)$. Ma $\delta(x-a) = 1$, quindi $\delta(r(x)) = 0$, ovvero $r(x) = r$ è un elemento di $\Bbbk$. Si ha dunque $p(x) = q(x)(x-a) + r$, con $q(x) \in \Bbbk[x]$ e $r \in \Bbbk$. Poiché a è radice del polinomio $p(x)$, si ha $0 = p(a) = q(a)(a-a) + r = r$. Segue che $p(x) = q(x)(x-a)$, cioè $x-a$ divide $p(x)$.

Viceversa, supponiamo che $x-a$ divida $p(x)$, allora $p(x) = q(x)(x-a)$ per un opportuno $q(x) \in \Bbbk[x]$. Allora $p(a) = q(a)(a-a) = 0$, ovvero a è radice di $p(x)$. □

Un altro modo per provare gli esempi visti sopra è il seguente Criterio di divisibilità per polinomi. Questo criterio è l'equivalente del Criterio di divisibilità di Pascal per i numeri interi visto nella Sezione 2.2.

Proposizione 3.8. *Sia $\Bbbk$ un campo di caratteristica p algebrico su $\mathbb{F}_p$. Sia $n(x) \in \Bbbk[x]$, $n(x) \neq 0$, un polinomio e siano $r_0(x), r_1(x), \ldots$ i resti delle divisioni di $1, x, \ldots$ per $n(x)$. Allora la sequenza $r_0(x), r_1(x), \ldots$ ha le seguenti proprietà:*

(a) la successione è periodica da un certo punto in poi, con lo stesso tipo di periodicità $\sim_{t,\ell}$ di $\frac{1}{n(x)}$;

(b) (Teorema di Pascal) *un polinomio $m(x) = d_N x^N + \cdots + d_1 x + d_0 \in \Bbbk[x]$ è divisibile per $n(x)$ se e solo se $\sum_{i=0}^{N} r_i(x) d_i = 0$.*

Dimostrazione.

(a) Abbiamo visto che le seguenti affermazioni sono equivalenti:
   (1) $\overline{r_i(x)} = \overline{r_j(x)}$;
   (2) $\overline{r_i(x)} = \overline{r_j(x)}$ in $\Bbbk[x]/(n(x))$;
   (3) $\overline{x}^i = \overline{x}^j$ in $\Bbbk[x]/(n(x))$;

(4) $i \sim_{t,\ell} j$, perché il monoide ciclico $\langle \overline{x} \rangle$ e $\mathbb{N}/\sim_{t,\ell}$ sono isomorfi. E da questo segue naturalmente la tesi del punto (a).

(b) Abbiamo visto che $r_i(x) \equiv x^i \mod n(x)$, dunque

$$m(x) = \sum_{i=0}^{N} d_i x^i \equiv \sum_{i=0}^{N} d_i r_i(x) \mod n(x).$$

Da cui si ha che $m(x)$ è divisibile per $n(x)$ se lo è $\sum_{i=0}^{N} d_i r_i(x)$, ma questo polinomio, per la definizione dei resti $r_i(x)$, ha grado strettamente minore di $n(x)$, quindi l'unica possibilità è che la somma sia nulla, ovvero che $\sum_{i=0}^{N} d_i r_i(x) = 0$.

□

Esempio 3.5. Sia $\Bbbk = \mathbb{F}_5$, consideriamo $n(x) = x^5 - x^3 \in \Bbbk[x]$ e sia $m(x) = x^{10} + x^9 - 2x^8 + x^7 + x^6 - x^5 - x^3 \in \Bbbk[x]$. Vogliamo vedere che $n(x) \mid m(x)$ con il criterio della Proposizione 3.8. Studiamo la periodicità di $\frac{1}{n(x)}$.

Divisioni:
$$\begin{aligned} a_0 &= 0 \quad r_0(x) = 1 \\ a_1 &= 0 \quad r_1(x) = x \\ a_2 &= 0 \quad r_2(x) = x^2 \\ a_3 &= 0 \quad r_3(x) = x^3 \\ a_4 &= 0 \quad r_4(x) = x^4 \\ a_5 &= 1 \quad r_5(x) = x^3 = r_3(x) \end{aligned}$$

Dunque $t = 3$ e $\ell = 2$, ovvero $\frac{1}{n(x)}$ ha tipo di periodicità $\sim_{3,2}$. Abbiamo visto che $n(x) \mid m(x)$ se e solo se $\sum_{i=0}^{10} d_i r_i(x) = 0$, si ha

$$\begin{aligned} \sum_{i=0}^{10} d_i r_i(x) &= 0 \cdot 1 + 0 \cdot x + 0 \cdot x^2 + (-1) \cdot x^3 + 0 \cdot x^4 + (-1) \cdot x^3 + \\ &\quad + 1 \cdot x^4 + 1 \cdot x^3 + (-2) \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^4 \\ &= -x^3 - x^3 + x^4 + x^3 - 2x^4 + x^3 + x^4 = 0 \end{aligned}$$

e quindi la condizione del Criterio di divisibilità è soddisfatta.

3.2.2 Radici di polinomi e divisibilità

Possiamo ridurci a un caso particolare con i polinomi di primo grado. Sia $m(x) = d_N x^N + \cdots + d_1 x + d_0 \in \Bbbk[x]$, se α è una radice di $m(x)$, allora, per il Teorema di Ruffini, il polinomio $n(x) = x - \alpha$ divide $m(x)$ in $\Bbbk[x]$. Come nel caso di un polinomio $n(x)$ qualsiasi, dobbiamo studiare il tipo di periodicità $\sim_{t,\ell}$ di $\frac{1}{x-\alpha}$:

$$\frac{1}{x-\alpha} = -\frac{1}{\alpha}\cdot\frac{1}{1-\frac{x}{\alpha}} = -\frac{1}{\alpha}\left(-\frac{\alpha}{x} - \frac{\alpha^2}{x^2} - \frac{\alpha^3}{x^3} + \dots\right) = \frac{1}{x} + \frac{\alpha}{x^2} + \frac{\alpha^2}{x^3} + \dots$$

Se $\alpha = 0$, allora

$$\frac{1}{x-0} = \frac{1}{x} + \frac{0}{x^2} + \frac{0}{x^3} + \cdots = \frac{1}{x}$$

dunque $\frac{1}{x}$ ha tipo di periodicità $\sim_{1,1}$. Per cui l'unico resto che si ottiene è $r_0(x) = 1$, allora $m(x)$ è divisibile per x se e solo se $\sum_{i=0}^{N} r_i(x)d_i = d_0 r_0(x) = d_0 \cdot 1 = d_0 = 0$, vale a dire, se e solo se ha termine noto nullo, come ci si aspetta.

Se $\alpha = 1$, allora

$$\frac{1}{x-1} = \frac{1}{x} + \frac{1}{x^2} + \frac{1}{x^3} + \frac{1}{x^4} + \dots$$

dunque $\frac{1}{x-1}$ ha tipo di periodicità $\sim_{0,1}$. Tutti i resti che si ottengono sono $r_i(x) = 1$ per ogni $i \geq 0$, allora $m(x)$ è divisibile per $x - 1$ se e solo se $\sum_{i=0}^{N} r_i(x)d_i = \sum_{i=0}^{N} d_i = 0$, se e solo se la somma dei coefficienti di $m(x)$ è nulla.

Se $\alpha = -1$, allora

$$\frac{1}{x+1} = \frac{1}{x} - \frac{1}{x^2} + \frac{1}{x^3} - \frac{1}{x^4} + \dots$$

dunque $\frac{1}{x+1}$ ha tipo di periodicità $\sim_{0,2}$. Per cui i resti che si ottengono sono $r_{2i}(x) = 1$ e $r_{2i+1}(x) = -1$ per ogni $i \geq 0$, allora $m(x)$ è divisibile per $x + 1$ se e solo se $\sum_{i=0}^{N} r_i(x)d_i = \sum_{i=0}^{N} (-1)^i d_i = 0$, cioè se e solo se

la somma alternata dei coefficienti di $m(x)$ è nulla.

In generale, sia $\alpha \neq 0$, allora

$$\frac{1}{x-\alpha} = \frac{1}{x} + \frac{\alpha}{x^2} + \frac{\alpha^2}{x^3} + \frac{\alpha^3}{x^4} + \dots$$

dunque $\frac{1}{x-\alpha}$ ha tipo di periodicità $\sim_{0,\ell}$, dove ℓ è l'ordine di α in $\Bbbk$.

3.3 Polinomi della forma $x^{a+b} - x^b$

Sia $\Bbbk$ un campo di caratteristica p algebrico su $\mathbb{F}_p$ e sia $\alpha(x) = \frac{1}{n(x)} \in \Bbbk(x)$, per quanto visto nella dimostrazione della Proposizione 3.4, possiamo scrivere

$$\frac{1}{n(x)}\left(x^{t+\ell} - x^t\right) = p(x)$$

per qualche $p(x) \in \Bbbk[x]$, dunque

$$x^{t+\ell} - x^t = n(x)p(x).$$

Pertanto, ogni polinomio $n(x) \in \Bbbk[x]$, $n(x) \neq 0$, divide un polinomio del tipo $x^{a+b} - x^b$, con $a, b \in \mathbb{N}$.

Proposizione 3.9. *Sia $n(x) \in \Bbbk[x]$, $n(x) \neq 0$, e sia $\sim_{t,\ell}$ il tipo di periodicità di $\frac{1}{n(x)}$. Allora*

(a) $x^{t+\ell} - x^t$ è il più piccolo polinomio della forma $x^{a+b} - x^b$ divisibile per $n(x)$;

(b) per ogni $a \geq 1$, $b \geq 0$, il polinomio $n(x)$ divide il polinomio $x^{a+b} - x^b$ se e solo se $\ell \mid a$ e $t \leq b$.

Dimostrazione. Siano $a \geq 1$ e $b \geq 0$, il polinomio $n(x)$ divide $x^{a+b} - x^b$ se e solo se $x^{a+b} \equiv x^b \mod n(x)$, ovvero, se e solo se $\overline{x}^{a+b} = \overline{x}^b$ in $\Bbbk[x]/(n(x))$. Come abbiamo visto nel Teorema 3.6, il monoide ciclico generato da $\overline{x}$ in $\Bbbk[x]/(n(x))$ è isomorfo a $\mathbb{N}/\sim_{t,\ell}$, segue quindi che $\overline{x}^{a+b} = \overline{x}^b$ in $\Bbbk[x]/(n(x))$ se e solo se $t \leq b$ e $\ell \mid a$. E questo prova il punto (b).

La dimostrazione di (a) segue da quanto visto poiché $x^{t+\ell} - x^t$ è il più piccolo polinomio della forma $x^{a+b} - x^b$ con $t \leq a$ e $\ell \mid b$. □

Osservazione 6. L'ordine su $\Bbbk[x]$ considerato nella dimostrazione precedente è la relazione di divisibilità.

$(\Bbbk[x], |)$ soddisfa le seguenti proprietà: per ogni $p(x), q(x), r(x) \in \Bbbk[x]$,

- Riflessività: $p(x) \mid p(x)$
- Transitività: $p(x) \mid q(x)$ e $q(x) \mid r(x) \Rightarrow p(x) \mid r(x)$

Non soddisfa l'antisimmetria: $p(x) \mid q(x)$ e $q(x) \mid p(x) \not\Rightarrow p(x) = q(x)$. Per esempio: sia $\Bbbk = \mathbb{F}_5$ e siano $p(x) = x + 1$ e $q(x) = 2x + 2$, ovviamente $p(x) \neq q(x)$, ma $p(x) \mid q(x)$ e $q(x) \mid p(x)$, infatti $q(x) = 2p(x)$ e $p(x) = 3q(x)$.

La relazione di divisibilità, dunque, è un preordine parziale in $\Bbbk[x]$.

Esempio 3.6. Sia $\Bbbk = \mathbb{F}_3$, consideriamo $n(x) = x^4 + x^2 \in \Bbbk[x]$ e calcoliamo il tipo di periodicità di $\frac{1}{n(x)}$.

Divisioni:
$$\begin{aligned} a_0 &= 0 & r_0(x) &= 1 \\ a_1 &= 0 & r_1(x) &= x \\ a_2 &= 0 & r_2(x) &= x^2 \\ a_3 &= 0 & r_3(x) &= x^3 \\ a_4 &= 1 & r_4(x) &= -x^2 \\ a_5 &= 0 & r_5(x) &= -x^3 \\ a_6 &= -1 & r_6(x) &= x^2 = r_2(x) \end{aligned}$$

Dunque $t = 2$ e $\ell = 4$, ovvero $\frac{1}{n(x)}$ ha tipo di periodicità $\sim_{2,4}$.

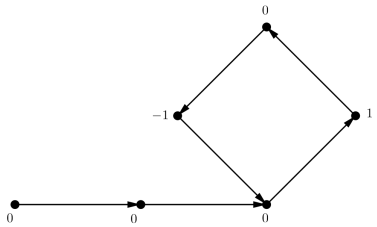


Figura 3.2: Rappresentazione del quoziente $\frac{1}{x^4+x^2}$.

Lo sviluppo in serie di Laurent è:

$$\begin{aligned} \frac{1}{x^4+x^2} &= 0 + \frac{0}{x} + \frac{0}{x^2} + \frac{0}{x^3} + \frac{1}{x^4} + \frac{0}{x^5} - \frac{1}{x^6} + \frac{0}{x^7} + \frac{1}{x^8} + \frac{0}{x^9} - \frac{1}{x^{10}} + \dots \\ &= x^{-4} - x^6 + x^{-8} - x^{-10} + x^{-12} - x^{-14} + \dots \\ &= \overline{0 \cdot x^{-3} + 1 \cdot x^{-4} + 0 \cdot x^{-5} - 1 \cdot x^{-6}}. \end{aligned}$$

Da cui

$$\frac{1}{x^4+x^2}\cdot x^2 = x^{-2} - x^{-4} + x^{-6} - x^{-8} + x^{-10} - x^{-12} + \dots$$

e

$$\frac{1}{x^4+x^2}\cdot x^6 = x^2 - 1 + x^{-2} - x^{-4} + x^{-6} - x^{-8} + \dots$$

Otteniamo

$$\begin{aligned}&\frac{1}{x^4+x^2}\left(x^6-x^2\right) = x^2-1\\ &\Leftrightarrow x^6 - x^2 = (x^4+x^2)(x^2-1)\end{aligned}$$

Dunque $n(x) \mid x^6 - x^2$.

Siano $a = 8$ e $b = 3$, si ha $t \leq b$ e $\ell \mid a$, consideriamo quindi il polinomio $x^{11}-x^3$. Poiché a e b soddisfano le ipotesi della Proposizione 3.9, $n(x)$ divide questo polinomio. Si ha infatti $x^{11}-x^3 = (x^4+x^2)(x^7-x^5+x^3-x)$.

Sia $\Bbbk$ un campo di caratteristica p algebrico su $\mathbb{F}_p$, possiamo riassumere alcuni dei risultati visti nella seguente Proposizione:

Proposizione 3.10. *Siano $t \geq 0$ e $\ell \geq 1$. Un polinomio frazionario $\alpha(x) \in \Bbbk(x)$ ha periodicità $\sim_{t,\ell}$ se e solo se $\alpha(x)$ può essere scritto nella forma $\frac{m(x)}{n(x)}$, dove:*

(1) $m(x) \in \Bbbk[x]$;
(2) $n(x) = x^{t+\ell} - x^t$;
(3) $t \geq 1$, se $m(x)$ non è divisibile per x;
(4) per ogni primo p che divide ℓ, $m(x)$ non è un multiplo di $\frac{x^\ell-1}{x^{\frac{\ell}{p}}-1}$.

Osservazione 7. Sia p un primo che divide ℓ, poniamo $c = \frac{\ell}{p}$, il quoziente del punto (4) può essere scritto come prodotto di polinomi ciclotomici:

$$\frac{x^\ell - 1}{x^c - 1} = \frac{\prod_{d\mid\ell}\Phi_d}{\prod_{d'\mid c}\Phi_{d'}} = \prod_{\substack{d\mid\ell\\ d\nmid c}}\Phi_d.$$

Equivalentemente si ha

$$\frac{x^\ell - 1}{x^c - 1} = \sum_{i=0}^{p-1} x^{ci} = 1 + x^c + \cdots + x^{c(p-1)}.$$

Dimostrazione.

($\Rightarrow$) Sia $\alpha(x) \in \Bbbk(x)$ un polinomio frazionario con tipo di periodicità $\sim_{t,\ell}$, per cui $t \geq 0$ e $\ell \geq 1$ sono i più piccoli interi per cui lo sviluppo in serie di Laurent di $\alpha(x)$, può essere scritto nella forma

$$\alpha(x) = b(x) + a_1 x^{-1} + \cdots + a_t x^{-t} + \overline{a_{t+1}x^{-t-1} + \cdots + a_{t+\ell}x^{-t-\ell}},$$

con $b(x) \in \Bbbk[x]$ e $a_i \in \Bbbk$ per ogni $i \geq 1$. Come abbiamo visto nella Proposizione 3.4, si può scrivere $\alpha(x) = \frac{m(x)}{x^{t+\ell}-x^t}$ con $m(x) \in \Bbbk[x]$. E da questo seguono i punti (1) e (2) della tesi.
Proviamo il punto (3) per contraddizione: sia $t \geq 1$ e supponiamo che $m(x)$ sia divisibile per x, allora $m(x) = x \cdot m'(x)$, dunque possiamo scrivere

$$\alpha(x) = \frac{m(x)}{x^{t+\ell} - x^t} = \frac{m'(x)}{x^{t+\ell-1} - x^{t-1}},$$

ovvero la parte in x^{-1} di $\alpha(x)$ può essere scritta con $t-1$ termini non periodici e ℓ termini periodici. E questo contraddice la minimalità di t.
Infine, proviamo il punto (4). Sia p un divisore primo di ℓ e poniamo $c = \frac{\ell}{p}$. Per contraddizione, supponiamo $m(x)$ sia un multiplo di $\frac{x^\ell-1}{x^c-1}$, allora

$$m(x) = m'(x) \cdot \frac{x^\ell - 1}{x^c - 1}$$

con $m'(x) \in \Bbbk[x]$, otteniamo quindi

$$\alpha(x) = \frac{m(x)}{x^{t+\ell} - x^t} = \frac{m'(x)}{x^t(x^c - 1)},$$

dunque $\alpha(x)$ ha tipo di periodicità $\sim_{t,\ell'} \geq \sim_{t,c} \geq \sim_{t,\ell}$, che contraddice la minimalità di t ed ℓ.

($\Leftarrow$) Sia $\alpha(x) = \frac{m(x)}{n(x)} \in \Bbbk(x)$, con $m(x), n(x) \in \Bbbk[x]$ che soddisfano le proprietà (1)-(4). Vogliamo dimostrare che $\alpha(x)$ ha tipo di periodicità $\sim_{t,\ell}$, ovvero, per il Teorema 3.6, vogliamo dimostrare che la classe laterale $\overline{m(x)}\langle\overline{x}\rangle$ in $\Bbbk[x]/(n(x))$ ha tipo di periodicità $\sim_{t,\ell}$. Sappiamo che $n(x) = x^{t+\ell} - x^t$ divide $m(x)(x^{t+\ell} - x^t)$, quindi la successione $\overline{m(x)}\overline{x}^i$ è periodica di periodo ℓ da $\overline{m(x)}\overline{x}^t$ in poi. Dimostriamo per contraddizione che la periodicità è proprio $\sim_{t,\ell}$. Per quanto visto, ci sono solo due possibilità: o la successione $\overline{m(x)}\overline{x}^i$ è periodica a partire da $\overline{m(x)}\overline{x}^{t-1}$ in poi, oppure la successione ha periodo d, dove $d \mid \ell$ e $d < \ell$.
Nel primo caso, $t \geq 1$ e $n(x) \mid m(x)(x^{t+\ell-1} - x^{t-1})$, quindi x divide $m(x)$, ma questo contraddice la proprietà (3). Nel secondo caso, sia p un fattore primo di $c = \frac{\ell}{d}$, allora esiste $\ell' \in \mathbb{Z}$ tale che $p\ell' = \frac{\ell}{d}$. Segue che c è un multiplo di d, per cui la successione $\overline{m(x)}\overline{x}^i$ è periodica da $\overline{m(x)}\overline{x}^t$ in poi con periodo c. Allora, $n(x)$ divide $m(x)(x^{t+c} - x^t)$, ovvero $\frac{x^\ell - 1}{x^c - 1}$ divide $m(x)$, ma questo contraddice il punto (4).

□

3.3.1 Fattori irriducibili e periodicità

Sia $\Bbbk$ un campo finito di caratteristica p con q elementi. Un polinomio $n(x) \in \Bbbk[x]$, $n(x) \neq 0$, può essere scritto come prodotto di polinomi irriducibili in $\Bbbk[x]$. Poiché stiamo considerando polinomi in x, possiamo pensare che il polinomio irriducibile x abbia una rilevanza particolare rispetto agli altri, dunque scriviamo $n(x)$ nella forma

$$n(x) = \lambda x^{e_1} \prod_{i=2}^{r} p_i^{e_i}(x),$$

dove $\lambda \in \Bbbk^*$, $e_i \in \mathbb{N}$ e i polinomi $p_i(x) \in \Bbbk[x]$ sono monici e irriducibili per ogni $i = 2, \ldots, r$. Vogliamo studiare se esiste qualche relazione tra il tipo di periodicità $\sim_{t,\ell}$ di $\frac{1}{n(x)}$ e i suoi fattori irriducibili.

Proposizione 3.11. *Sia $n(x) \in \Bbbk[x]$, $n(x) \neq 0$, con $\sim_{t,\ell}$ tipo di periodicità di $\frac{1}{n(x)}$. Allora $t = e_1$ e ℓ divide* $\operatorname{mcm}\{q^{e_i d_i} - q^{(e_i-1)d_i} \mid i = 2, \dots, r\}$, *dove $d_i = \delta(p_i(x))$ per ogni $i = 2, \dots, r$.*

Dimostrazione. Ricordiamo che gli interi $t \geq 0$ e $\ell \geq 1$ sono tali che il sottomonoide ciclico $\langle \overline{x} \rangle$ del monoide $\Bbbk[x]/(n(x))$ è isomorfo al monoide $\mathbb{N}/\sim_{t,\ell}$.

Si ha l'isomorfismo canonico

$$\frac{\Bbbk[x]}{(n(x))} \cong \frac{\Bbbk[x]}{(x^{e_i})} \times \frac{\Bbbk[x]}{(p_2^{e_2}(x))} \times \cdots \times \frac{\Bbbk[x]}{(p_r^{e_r}(x))}.$$

Quindi $x^j \equiv x^k \mod n(x)$ se e solo se $p_i^{e_i}(x) \mid x^j - x^k$ in $\Bbbk[x]$ per ogni $i = 1, \dots, r$. Ovviamente, $x^{j-k} \equiv 0 \mod x^{e_1}$ se e solo se $j - k \geq e_1$, dunque $x^j \equiv x^k \mod x^{e_1}$ se e solo se $j \sim_{e_1,1} k$.

Consideriamo ora i polinomi $p_i^{e_i}(x)$, per $i = 2, \dots, r$. Per definizione, $p_i^{e_i}(x)$ è coprimo con x, dunque, per Bézout, $\overline{x}$ è invertibile nell'anello $\frac{\Bbbk[x]}{(p_i^{e_i}(x))}$. Studiamo quali sono gli elementi invertibili di quest'anello. Ogni elemento di $U\left(\frac{\Bbbk[x]}{(p_i^{e_i}(x))}\right)$ si scrive in modo unico come $\lambda + f(x) + (p_i^{e_i}(x))$, con $\lambda \in \Bbbk^*$ e $f(x) \in \frac{(p_i(x))}{(p_i^{e_i}(x))}$.
Il modulo $\frac{\Bbbk[x]}{(p_i(x))}$ è l'unico modulo semplice nell'anello locale $\frac{\Bbbk[x]}{(p_i^{e_i}(x))}$, a meno di isomorfismi. Sia $\delta(p_i(x)) = d_i$.
Allora $\left|\frac{\Bbbk[x]}{(p_i(x))}\right| = q^{d_i}$, quindi $\frac{(p_i(x))}{(p_i^2(x))}$ ha q^{d_i} elementi, poiché $\frac{\Bbbk[x]}{(p_i(x))} \to \frac{(p_i(x)}{(p_i^2(x))}$, definita da $f(x) + (p_i(x)) \mapsto p_i(x) \cdot f(x) + (p_i^2(x))$, è una biiezione; $\frac{(p_i(x))}{(p_i^3(x))}$ ha $q^{d_i} \cdot q^{d_i} = q^{2d_i}$ elementi, perché, per ogni sequenza esatta tra moduli finiti $0 \to A \to B \to C \to 0$, vale $|B| = |A| \cdot |C|$; analogamente $\frac{(p_i(x))}{(p_i^4(x))}$ ha $q^{d_i} \cdot q^{2d_i} = q^{3d_i}$ elementi, e, iterando, arriviamo a $\frac{(p_i(x))}{(p_i^{e_i}(x))}$ che ha $q^{(e_i-1)d_i}$ elementi.

Poiché $\frac{\Bbbk[x]}{(p_i^{e_i}(x))}$ è un anello locale artiniano, ogni suo elemento è invertibile o nilpotente. Gli elementi nilpotenti sono gli elementi di $\frac{(p_i(x))}{(p_i^{e_i}(x))}$, ci sono $q^{(e_i-1)d_i}$ elementi nilpotenti.
Da cui $\left|U\left(\frac{\Bbbk[x]}{(p_i^{e_i}(x))}\right)\right| = q^{e_i d_i} - q^{(e_i-1)d_i} = N$. Quindi l'ordine degli elementi di $U\left(\frac{\Bbbk[x]}{(p_i^{e_i}(x))}\right)$ divide N e si ha che, se $i \equiv j \mod N$, $x^i \equiv x^j$

mod $p_i^{e_i}(x)$. Allora ℓ divide $\mathrm{mcm}\{q^{e_i d_i} - q^{(e_i-1)d_i} \mid i = 2, \ldots, r\}$. $\square$

Si noti che ℓ può essere un divisore proprio di $\mathrm{mcm}\{q^{e_i d_i} - q^{(e_i+1)d_i} \mid i = 2, \ldots, r\}$. Per esempio, consideriamo $n(x) = x^5 - x^3 \in \mathbb{F}_5[x]$, si ha $\ell = 2$ ma $\mathrm{mcm}\{5^{e_i d_i} - 5^{(e_i+1)d_i} \mid i = 2, \ldots, r\} = 4$.

Osservazione 8. Sia $n(x) = \lambda x^{e_1} \prod_{i=2}^{r} p_i^{e_i}(x)$, con $\lambda \in \Bbbk^*$, $e_i \in \mathbb{N}$ per ogni $i = 1, \ldots, r$ e $p_i(x) \in \Bbbk[x]$ monici e irriducibili. Poniamo $t = e_1$ e $c = \prod_{i=2}^{r} (q^{e_i} - q^{e_i-1})$. Per la Proposizione 3.11, possiamo scrivere

$$\frac{1}{n(x)} = a_1 x^{-1} + \cdots + a_t x^{-t} + \overline{a_{t+1} x^{-t-1} + \cdots + a_{t+c} x^{-t-c}}.$$

La sequenza dei resti $r_0(x), r_1(x), \ldots$ consiste di t polinomi distinti e di c polinomi che si ripetono periodicamente, dunque, per la Proposizione 3.8, $n(x)$ divide il polinomio $x^{t+c} - x^t$.

In conclusione, i numeri razionali scritti in notazione decimale e gli sviluppi in serie di Laurent di quozienti di polinomi a coefficienti in un campo $\Bbbk$, di caratteristica p e algebrico su $\mathbb{F}_p$, hanno comportamenti simili. Entrambi sono "periodici da un certo punto in poi", ovvero si comportano in modo analogo ai monoidi ciclici. Questo particolare tipo di periodicità, come abbiamo visto, implica interessanti proprietà nei criteri di divisibilità tra numeri interi e tra polinomi a coefficienti in $\Bbbk$, e nello studio degli interi del tipo $99\ldots900\ldots0$ e dei polinomi della forma $x^{a+b} - x^b$. Come nel caso dei razionali in cui la base utilizzata ha una rilevanza particolare, nel caso dei polinomi la stessa rilevanza risiede nella variabile considerata.

Bibliografia

[1] A. Facchini e G. Simonetta, *Rational numbers, finite cyclic monoids, divisibility rules, and numbers of type* $99\ldots900\ldots0$, Amer. Math. Monthly 121 (2014), 471-485.

[2] A. Facchini, *Algebra e matematica discreta*, Decibel-Zanichelli, Padova, 2000.

[3] S. Lang, *Algebra*, Graduate Texts in Mathematics 211, Springer-Verlag, New York, 2002.

[4] N. Jacobson, *Basic Algebra I*, Second edition, Dover Publications Inc., New York, 1985.

[5] A. Facchini, *Introduction to Ring and Module Theory*, Edizioni Libreria Progetto Padova, 2015.

[6] M.F. Atiyah, I.G. McDonald, *Introduction to Commutative Algebra*, Addison-Wellsey Publishing Company, Reading (Mass.), 1969.

Ringraziamenti

Oggi si conclude il mio percorso universitario, un traguardo per me molto importante e vorrei ringraziare tutte le persone che mi sono state accanto nella corsa verso il suo raggiungimento.

Prima di tutto ringrazio il mio relatore, il Professor Alberto Facchini, per avermi proposto quest'interessante argomento e per il suo prezioso aiuto durante la stesura della tesi.

Un ringraziamento speciale va sicuramente alla mia famiglia, in particolare ai miei genitori e ai miei nonni, per avermi sostenuto e incoraggiato in tutti questi anni.

Proseguo poi con un enorme ringraziamento ai miei amici, in ordine alfabetico: Alberto, compagno di vintage; Alessandro, compagno di indecisioni e di pasta in bianco; Angela, compagna di gossip hollywoodiano; Claudia, compagna di avventure, risate ed "E-punto-Fermi" da sempre; Elena, compagna di Follie; Filippo, compagno di meme matematici; e Valeria, compagna di divertimenti e "ricerche scientifiche". Li ringrazio per avermi supportato (e sopportato), per aver ascoltato i miei deliri e per avermi sempre fatto ridere e star bene.

Infine vorrei ringraziare tutti gli insegnanti che ho incontrato nella mia carriera scolastica, in particolare la Professoressa Caldart e la Professoressa Gobbo che mi hanno trasmesso il loro entusiasmo per la Matematica.

E grazie a chiunque altro abbia dimenticato o non abbia inserito per motivi di spazio.

GRAZIE DI CUORE!