

Anello dei polinomi a coefficienti in un campo

(184)

Tutti i discorsi fatti per polinomi a coefficienti reali valgono per polinomi a coefficienti in un campo qualsiasi, poiché vi si opera con le consuete regole del calcolo letterale.

In particolare, se chiamiamo K il campo, l'anello $K[x]$ è un dominio di integrità in cui è definito l'algoritmo della divisione (basato unicamente sulla possibilità di invertire tutti gli elem. di K^* e sul concetto di grado, che è un numero naturale, non ha nulla a che vedere con il campo).

Verrà quindi anche il teor. di Ruffini:

$$a \in K \text{ è una radice di } p(x) \in K[x] \Leftrightarrow p(x) = (x-a) \cdot q(x)$$

Si olterà poi la nozione di polinomio riducibile (\Rightarrow si può scrivere come prodotto di due polinomi entrambi di grado minore del pol. dato) e irriducibile, e attraverso l'algoritmo euclideo delle divisioni successive (che permette di trovare MCD e mcm di 2 polinomi) si potrà garantire che un polinomio $p(x)$ è irriducibile se e solo se è primo, cioè tale che

$$p(x) \mid a(x)b(x) \text{ e } p(x) + a(x) \Rightarrow p(x) \mid b(x).$$

e che ogni polinomio di $K[x]$ può essere fattorizzato in modo esenzialmente unico come prodotto di polinomi irriducibili.

Esercizio 1. Determinare quoziente e resto della divisione
tra i due polinomi di $\mathbb{Z}_5[x]$: $p(x) = x^4 + 2x + 3$
e $d(x) = 2x^2 + 2$, ove i "numeri" 2, 3... denotano
le classi di resto che hanno quei numeri per
rappresentanti

$$\begin{array}{r} x^4 \\ -3x^4 - x^2 \\ \hline 4x^2 \quad +2x + 3 \\ -4x^2 \quad - \quad 4 \\ \hline 2x + 4 \end{array}$$

$$\left| \begin{array}{r} 2x^2 + 2 \\ \hline 3x^2 + 2 \end{array} \right.$$

In \mathbb{Z}_5 :

$$\begin{aligned} 2^{-1} &= 3 \\ 4^{-1} &= 4 \\ -1 &\equiv 4 \pmod{5} \end{aligned}$$

In $\mathbb{Z}_5[x]$ $x^4 + 2x + 3 = (2x^2 + 2)(3x^2 + 2) \rightarrow \frac{2x + 4}{\text{quoziente}} \text{ Resto}$

Esercizio 2. In $\mathbb{Z}_3[x]$ si consideri il polinomio
 $p(x) = x^4 + 2x + 2$. Quanti fattori di 1° grado
ha? E' riducibile?

$p(x)$ avrà un fattore di 1° grado della forma $x+a \Leftrightarrow$ (TEOR. di RUFFINI) $p(-a)=0$. Visto che $a \in \mathbb{Z}_3$, si devono testare 3 elementi:

$$p(0) = 0+0+2 \neq 0 \Rightarrow x \text{ non è un fattore di } p(x)$$

$$p(1) = 1+2+2 = 2 \neq 0 \Rightarrow (x-1) = (x+2) \text{ non è un fattore di } p(x)$$

$$p(2) = 1+1+2 = 1 \neq 0 \Rightarrow (x-2) = (x+1) \text{ non è un fattore di } p(x)$$

Gli altri polinomi di grado 1 sono i prodotti di questi per 2 e quindi non sono neppure questi fattori di $p(x)$, che quindi non ha fattori di 1° grado.

Per escludere che $p(x)$ sia riducibile, però, non basta!

E' ovvio che $p(x)$ non ha fattori di grado 3 irriducibili (altrimenti dovrebbe averne di grado 1). Ma potrebbe essere prodotto di 2 polinomi irriducibili di 2° grado.

I pol. di 2° grado sono 18: di essi ci saranno irriducibili (RUFFINI!!!)

$$x^2+x+2, \quad x^2+2x+2, \quad x^2+1 \text{ e i loro prodotti per 2}$$

I restanti 12 ($x(x+1), x(x+2), (x+1)(x+2), x^2, (x+1)^2, (x+2)^2$ e i loro prodotti per 2) sono riducibili.

$$\begin{array}{r}
 x^4 & + 2x + 2 \\
 -x^4 - x^3 - 2x^2 \\
 \hline
 2x^3 + x^2 + 2x + 2 \\
 -2x^3 - 2x^2 - x \\
 \hline
 2x^2 + x + 2 \\
 -2x^2 - 2x + 2 \\
 \hline
 2x + 1
 \end{array}$$

$$\begin{array}{c|cc}
 & x^2 + x + 2 & \\
 & \hline
 & x^2 + 2x + 2
 \end{array}$$

$$\mathbb{Z}_3[x]$$

$$2^{-1} = 2$$

$$\Rightarrow p(x) = (x^2 + x + 2)(x^2 + 2x + 2) + \underbrace{2x + 1}_{\text{resto}}$$

nella divisione di $p(x)$ tanto per $x^2 + x + 2$ che per $x^2 + 2x + 2$

$$\begin{array}{r}
 x^4 & + 2x + 2 \\
 -x^4 - x^2 \\
 \hline
 2x^2 + 2x + 2 \\
 -2x^2 \\
 \hline
 2x
 \end{array}$$

$$\begin{array}{c|cc}
 & x^2 + 1 & \\
 & \hline
 & x^2 + 2
 \end{array}$$

$$\Rightarrow p(x) = (x^2 + 1)(x^2 + 2) + \underbrace{2x}_{\text{resto}}$$

Quindi il polinomio $x^4 + 2x + 2$ è irriducibile in $\mathbb{Z}_3[x]$.

Esercizio 3. In $(\mathbb{Z}_2[x], +, \cdot)$

- quanti sono i polinomi di 2° grado?
- quali di essi sono irriducibili?
- sviluppare e trovare $(x+1)^2$, $(x+1)^4$, $(x+1)^8$. Che cosa posso dire di $(x+1)^{2^n}$ con $n \geq 1$?
- i coefficienti del polinomio sono: $1 \cdot 2 \cdot 2 = 4 \Rightarrow x^2 + x + 1$, $x^2 + x$, $x^2 + 1$, x^2 sono i polinomi di 2° grado.
- $x^2 + x = x(x+1)$, $x^2 = x \cdot x$, $x^2 + 1 = (x+1)^2$. Tuttavia $x^2 + x + 1$ è irriducibile poiché, essendo di 2° grado, se fosse riducibile avrebbe un fattore di grado 1, ma ciò non succede poiché il suo valore in $x=0, x=1$ è $\neq 0$.
- $(x+1)^2 = x^2 + 1$
 $(x+1)^4 = ((x+1)^2)^2 = (x^2 + 1)^2 = x^4 + 1$
 $(x+1)^8 = ((x+1)^4)^2 = x^8 + 1$
 $(x+1)^{2^n} = x^{2^n} + 1$.

INVECE: $(x+1)^3 = (x+1)^2 \cdot (x+1) = (x^2 + 1)(x+1) = x^3 + x^2 + x + 1$,

Esercizio 4. Considerare l'anello quoziante

$$A = \frac{\mathbb{Z}_2[x]}{I} \quad \text{ove}$$

- i) I è l'ideale dei multipli di $x^2 + 1$ in $\mathbb{Z}_2[x]$
- ii) I è " " " " " $x^2 + x + 1$ in $\mathbb{Z}_2[x]$

Per ciascuno dei due casi dire:

- 1) quanti elementi ha A ;
- 2) come sono fatti tali elementi;
- 3) quali elementi sono invertibili e quali sono divisori di zero;
- 4) se $(A, +)$ è isomorfo a $(\mathbb{Z}_4, +)$.

Che cosa si può dedurre da tutto ciò?

1) Sono ④ poiché i laterali di I sono in entrambi i casi individuati dai possibili resti nelle divisioni per un polinomio di 2° grado

\Rightarrow polinomi di grado ≤ 1 di $\mathbb{Z}_2[x]$
Le possibili scelte dei coefficienti sono 2·2.

2) $I+0 = I$, $I+1$, $I+x$, $I+(x+1)$

3) i) (I è lo zero), $I+1$ è invertibile; $I = (x^2+1)\mathbb{Z}_2[x]$

$$(I+x)^2 = I+x^2 = I+1 : I+x \text{ è invertibile}$$

$$(I+x+1)^2 = I+(x+1)^2 = I+(x^2+1) = I : I+(x+1) \text{ è}$$

L'anello è isomorfo a \mathbb{Z}_4 ? d'inciso delle
zero

ii) $I = (x^2+x+1)\mathbb{Z}_2[x]$

$I+1$ è invertibile

$$(I+x)^2 = I+x^2 = I+(x+1)$$

$$(I+(x+1))^2 = I+(x^2+1) = I+x$$

$$(I+x)(I+x+1) = I+x^2+x = I+1 \Rightarrow I+x \text{ e } I+(x+1)$$

sono uno l'inv.
dell'altro.

CAMPO di
ordine 4



199
b12

i) ii) $\frac{\mathbb{Z}_2[x]}{(x^2+x+1)}$ è un campo \Rightarrow non c'è l'anno zero a \mathbb{Z}_4 , che ha divisori dello zero.

ii) $I = (x^2+1)$. La tavola dell'addizione in $\frac{\mathbb{Z}_2[x]}{I}$ è

$+$	I	$I+1$	$I+x$	$I+(1+x)$
I	I	$I+1$	$I+x$	$I+(1+x)$
$I+1$	I	I	$I+(1+x)$	$I+x$
$I+x$	I	I	I	$I+1$
$I+(1+x)$	I	I	I	I

mentre in \mathbb{Z}_4 è:

$+$	[0]	[1]	[2]	[3]
[0]	[0]			
[1]		[2]		
[2]			[0]	
[3]				[2]

In particolare si vede che per ogni laterale $I+a$ si ha $(I+a)+(I+a)=I$, mentre risp. +

In particolare non è vero che per ogni classe di resto $[a]$ si abbia $[a]+[a]=[0]$

Quindi i due gruppi additivi non sono isomorfi \Rightarrow non lo sono neanche gli anelli

Verificare che il gruppo additivo di $\frac{\mathbb{Z}_2[x]}{(x^2+1)}$ è isomorfo al gruppo triangolo, sgr di S_4 : $\{ \text{id}, (12)(34), (13)(24), (14)(23) \}$.

Domanda: $\frac{\mathbb{Z}_2[x]}{(x^2)}$ può essere isomorfo a \mathbb{Z}_4 ?

Matrici a coeff. in un campo K ; spazi vettoriali
sul K ; sistemi lineari a coeff. in K .

(198)

Non cambia nulla rispetto a quanto visto in \mathbb{R} .

Ad es. se $K = \mathbb{Z}_5$ (e quindi i numeri rappresentano le classi di resto mod 5)

$$\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} + \begin{pmatrix} 4 & 1 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 4+4 & 1+1 \\ 0+1 & 0+4 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 0 & 4 \end{pmatrix}$$

$$\left| \begin{pmatrix} 4 & 1 \\ 2 & 3 \end{pmatrix} \right| = 2 - 2 = 0 \quad \Rightarrow \quad \begin{pmatrix} 4 & 1 \\ 2 & 3 \end{pmatrix} \text{ è una matrice singolare}$$

$$\text{Infatti } \begin{pmatrix} 4 \\ 2 \end{pmatrix} = -\begin{pmatrix} 1 \\ 3 \end{pmatrix}$$

Quindi l'applicazione lineare $f: K^2 \rightarrow K^2$ definita da $f\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 4 & 1 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$ trasforma i 2 vettori della base $\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ in 2 vettori dipendenti.

$$\text{Il suo nucleo } \ker f = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \mid 4x+y=0 \right\} = \left\{ \begin{pmatrix} k \\ k \end{pmatrix}, k \in K \right\}$$

ha dimensione 1;

l'immagine $\text{Im } f = \left\{ \begin{pmatrix} 2k \\ k \end{pmatrix}, k \in K \right\}$ ha dimensione 1

e la preimmagine di $\begin{pmatrix} 2k \\ k \end{pmatrix}$ (con R fissato in K) è data da

$$\ker f + \left\{ \begin{pmatrix} 3k \\ 0 \end{pmatrix}, k \in K \right\} = \left\{ \begin{pmatrix} k+3R \\ k \end{pmatrix}, k \in K \right\}$$

I suoi autovettori si trovano con l'eq. caratteristica:

$$\left| \begin{matrix} 4-\lambda & 1 \\ 2 & 3-\lambda \end{matrix} \right| = 0 \quad \text{cioè} \quad \lambda^2 - 2\lambda = 0 \quad \begin{cases} \lambda = 0 \\ \lambda = 2 \end{cases}$$

da cui, autovettori relativi a $\lambda = 0$: $\begin{pmatrix} k \\ k \end{pmatrix}, k \in K^*$ mentre per $\lambda = 2$ gli autovettori sono le coppie ordinate non nulle $\begin{pmatrix} x \\ y \end{pmatrix}$ t.c. $(4-2)x+y=0 \Leftrightarrow y=3x$ cioè hanno la forma $\begin{pmatrix} h \\ 3h \end{pmatrix}, h \in K^*$.

Digressione sui metodi per calcolare il determinante di una matrice $n \times n$

198
bis

- ① Metodo di Laplace: fisso una riga (o una colonna) e calcolo la somma dei prodotti di ciascun elemento della riga (o colonna) per il corrispondente complemento algebrico.

Ad es.

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 1 & 0 \\ 1 & 0 & 0 \end{vmatrix} = 1 \cdot (-1)^{3+1} \begin{vmatrix} 2 & 3 \\ 1 & 0 \end{vmatrix} + 0 + 0 = 2 \cdot 0 - 3 \cdot 1 = -3$$

(se $K = \mathbb{Z}_5$: $-3 = 2$... ma non mi importa in questo contesto)

DIFETTO DEL METODO DI LAPLACE : complessità computazionale

Il numero di prodotti da calcolare in una matrice $n \times n$ è $n!$

Infatti supponiamo di calcolare il det. per righe successive. Ciascuno degli n elem. della prima riga porta con sé tutti i prodotti contenuti in ciascuno degli n minori di ordine $n-1$ complementari. Per calcolare i minori fisso la loro 1^a riga (la 2^a delle matrice iniziale): $n-1$ elem. ciascuno dei quali porta con sé i prodotti contenuti in ciascuno degli $n-1$ minori complementari ecc. Fino ad arrivare alla penultima riga su cui si trovano matrici di ordine 2 e ogni el della 1^a riga porta con sé 1 solo prodotto:

$$n \cdot (n-1) \cdot \dots \cdot 2 \cdot 1$$

Vedi esempio per $n=4$.

$$\begin{vmatrix} a & b & c & d \\ a' & b' & c' & d' \\ a'' & b'' & c'' & d'' \\ a''' & b''' & c''' & d''' \end{vmatrix} = a \begin{vmatrix} b' & c' & d' \\ b'' & c'' & d'' \\ b''' & c''' & d''' \end{vmatrix} - b \begin{vmatrix} a' & c' & d' \\ a'' & c'' & d'' \\ a''' & c''' & d''' \end{vmatrix} +$$

$$+ c \begin{vmatrix} a' & b' & d' \\ a'' & b'' & d'' \\ a''' & b''' & d''' \end{vmatrix} - d \begin{vmatrix} a' & b' & c' \\ a'' & b'' & c'' \\ a''' & b''' & c''' \end{vmatrix} =$$

Sviluppando il 1° adolenuolo, per gli altri i.e. n° di prodotti è lo stesso:

$$a \begin{vmatrix} b' & c' & d' \\ b'' & c'' & d'' \\ b''' & c''' & d''' \end{vmatrix} = a \left(b' \begin{vmatrix} c'' & d'' \\ c''' & d''' \end{vmatrix} - c' \begin{vmatrix} b'' & d'' \\ b''' & d''' \end{vmatrix} + d' \begin{vmatrix} b'' & c'' \\ b''' & c''' \end{vmatrix} \right) =$$

Siamo arrivati alle ultime 2 righe!

$$= a \underbrace{\left(b'c''d''' - b'd''c''' \right)}_2 - \underbrace{\left(c'b''d''' - c'd''b''' \right)}_2 + \underbrace{\left(d'b''c''' - d'c''b''' \right)}_2$$

$\frac{1}{2}$ per ciascuno degli elementi della 1a riga
 \Rightarrow Totale 6 prodotti

Mindi se ho 4 adolenuoli fatti così: $4 \cdot 6$ prodotti

Questo da un lato dice che il metodo di Laplace non è computazionalmente conveniente, dall'altro dice che è considerato metodo di SARRUS, valido per matrici 3×3 , non vale se $n > 3$:

Metodo di Sarrus per il calcolo di

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 1 & 0 \\ 1 & 0 & 0 \end{vmatrix} : \quad \begin{array}{ccc|cc} 1 & 2 & 3 & 1 & 2 \\ 4 & 1 & 0 & 4 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{array}$$

Sommare i prodotti sulle linee verdi e sottrarre i prodotti nelle linee rosse

aggiunge

Ma se la matrice è 4×4 il metodo porta 8 e non 24 prodotti!

$$\begin{array}{cccc} a & b & c & d \\ a' & b' & c' & d' \\ a'' & b'' & c'' & d'' \\ a''' & b''' & c''' & d''' \end{array}$$

⑨ metodo di GAUSS di triangolazione della matrice (basato sulla multilinearità del determinante)

E' un modo per far venire fuori un po' di elem.=0 sistematicamente

$$\left| \begin{array}{cccc} 1 & 0 & 1 & 3 \\ 2 & 1 & 3 & 1 \\ 4 & -1 & 3 & 5 \\ 0 & 2 & 1 & 1 \end{array} \right| = \text{faccio comparire } 0 \text{ in posizione (2,1) e (3,1)} \\ \text{sommando a 2^a e 3^a riga un opportuno multiplo della 1^a}$$

$$= \left| \begin{array}{cccc} 1 & 0 & 1 & 3 \\ 2-2 & 1-0 & 3-2 & 1-6 \\ 4-4 & -1-0 & 3-4 & 5-12 \\ 0 & 2 & 1 & 1 \end{array} \right| = \left| \begin{array}{cccc} 1 & 0 & 1 & 3 \\ 0 & 1 & 1 & -5 \\ 0 & -1 & -1 & -7 \\ 0 & 2 & 1 & 1 \end{array} \right| = \text{faccio comparire } 0 \text{ in posiz. (3,2) e (4,2)} \\ \text{sommando a 3^a e 4^a riga} \\ \text{multiplo della 2^a}$$

$$= \left| \begin{array}{cccc} 1 & 0 & 1 & 3 \\ 0 & 1 & 1 & -5 \\ 0 & -1+1 & -1+1 & -7-5 \\ 0 & 2-2 & 1-2 & 1+10 \end{array} \right| = \left| \begin{array}{cccc} 1 & 0 & 1 & 3 \\ 0 & 1 & 1 & -5 \\ 0 & 0 & \textcircled{0} & -12 \\ 0 & 0 & -1 & 11 \end{array} \right| = \text{!! Sceambio 3^a - 4^a riga}$$

$$= \left| \begin{array}{cccc} 1 & 0 & 1 & 3 \\ 0 & 1 & 1 & -5 \\ 0 & 0 & -1 & 11 \\ 0 & 0 & 0 & -12 \end{array} \right| = -1 \cdot 1 \cdot (-1) \cdot (-12) = -12$$

Quanti prodotti ho dovuto fare? 8, ma con un'altra matrice sarebbero potuti essere $4 \times 3 = 12$, nel 1° passo, $3 \times 2 = 6$ nel 2° passo, nessuno nel 3°, ma in realtà sarebbero potuti essere 2×1 . In fine 1 prodotto di 4 elem. lungo la diagonale. C'è, maleducata che vada

$4 \times 3 + 3 \times 2 + 2 \times 1 = 20$ prodotti di coppie di elementi e 1 prodotto di 4 elementi (che conta per 3 prodotti di coppie) $\Rightarrow 23$ prodotti di coppie

Contro i 24×3 prodotti di coppie del metodo di Laplace. Se i prodotti sono più costosi va molto meglio!

Digressione sui legami tra sistemi lineari

(198-V)

(e loro soluzioni) e applicazioni lineari (e laterali del nucleo).

1) un sist. lin. di m eq. in $\underbrace{x_1, \dots, x_n}_{\text{a var.}}$

nel campo K si rappresenta come una equazione matriciale:

$$A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \quad A \in M_{m \times n}(K)$$

2) la corrispondenza $f: K^n \rightarrow K^m$ definita

$$f \left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \right) = A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

è un'applicazione lineare.

3) dire che il sistema (1) non ha soluzione SIGNIFICA che $\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \notin f(K^n) =$ immagine di f e quindi IMPLICA che f non è suriettiva

• dire che il sist. (1) ha soluzione $\begin{pmatrix} \bar{x}_1 \\ \vdots \\ \bar{x}_n \end{pmatrix}$ significa che $\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in f(K^n)$

Tutte e sole le soluzioni del sistema (1) sono le preimmagini di $\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$.

Visto che f è un omomorfismo dei gruppi additivi di K^n e K^m , tali preimmagini sono gli elementi del laterale $\ker f + \begin{pmatrix} \bar{x}_1 \\ \vdots \\ \bar{x}_n \end{pmatrix}$ (e la soluzione è unica se $\ker f = \{0\}$)

Le soluz. del sistema (1) si possono pensare alternate sommando a una sol particolare tutte quelle del sistema $A\bar{x} = 0$.

E quelli di polinomi o di matrici a coefficienti
in un anello?

(199)

Là si rischia molto.

Ad esempio la matrice di $M_2(\mathbb{Z})$:

$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ ha determinante diverso da zero,
ma la matrice non è invertibile in $M_2(\mathbb{Z})$
... bisogna che il determinante sia INVERTIBILE
perché una matrice di $M_2(\mathbb{Z})$ sia invertibile.

Ad es.

$A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ è invertibile in $M_2(\mathbb{Z})$

$$\left(\begin{array}{cc|cc} 2 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array} \right) \rightsquigarrow \left(\begin{array}{cc|cc} 1 & 1 & 0 & 1 \\ 2 & 1 & 1 & 0 \end{array} \right) \rightsquigarrow \left(\begin{array}{cc|cc} 1 & 1 & 0 & 1 \\ 0 & -1 & 1 & -2 \end{array} \right) \rightsquigarrow$$
$$\left(\begin{array}{cc|cc} 1 & 1 & 0 & 1 \\ 0 & 1 & -1 & 2 \end{array} \right) \rightsquigarrow \left(\begin{array}{cc|cc} 1 & 0 & 1 & -1 \\ 0 & 1 & -1 & 2 \end{array} \right)$$

$$A^{-1} = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}$$

Però $\mathbb{Z}[x]$ è ancora un dominio di integrità.

Tuttavia $\mathbb{Z}_4[x]$, che non è un dominio di integrità poiché il quadrato del polinomio 2 dà il polinomio nullo, ha polinomi di grado > 0 che sono invertibili, ad es.

$$(1+2x)^2 = 1 + 4x + 4x^2 = 1$$

cioè $1+2x$ è inverso di se stesso.

Il teorema del quoziente e del resto vale tanto in $\mathbb{Z}[x]$ che in $\mathbb{Z}_4[x]$ Solo se il divisore ha coefficiente direttore invertibile. Ecc.