CAPITOLO 3
POLINOMI

3.1 Definizione. Addizione e moltiplicazione tra polinomi

Si dicono polinomi *in una variabile*, espressioni del tipo $P(x) = a_0 + a_1x + ... + a_nx^n$, dove i coefficienti appartengono ad un determinato insieme numerico. In genere ci occuperemo di polinomi a coefficienti interi, con qualche accenno ai casi in cui i coefficienti appartengono all'insieme dei numeri reali, o all'insieme quoziente Z_n.

Un polinomio è scritto nella *forma canonica* dopo che i monomi simili sono stati tutti sommati tra loro, e si definisce *grado del polinomio* quello maggiore dei monomi che lo costituiscono.

Consideriamo *identici* due polinomi che hanno lo stesso grado, e gli stessi coefficienti corrispondenti.

I polinomi possono essere sommati o moltiplicati tra loro. Riprendiamo la regola in base alla quale queste operazioni possono essere eseguite. Siano $P(x) = a_0 + a_1x + ... + a_nx^n$ e $Q(x) = b_0 + b_1x + ... + b_mx^m$ due polinomi con, ad esempio, $n > m$. Risulta:

- $P(x) + Q(x) = (a_0 + b_0) + (a_1 + b_1)x + ... + (a_m + b_m)x^m + a_{m+1}x^{m+1} + ... + a_nx^n$;
- $P(x) \cdot Q(x) = a_nb_mx^{n+m} + (a_nb_{m-1} + a_{n-1}b_m)x^{n+m-1} + ... + a_0b_0$.

In queste ipotesi è chiaro il motivo per cui non viene assegnato il grado al *polinomio nullo* $P(x) \equiv 0$: se, per assurdo, fosse *d* il grado del polinomio nullo, per la regola di moltiplicazione risulterebbe ad esempio $0 = 0 \cdot x \Rightarrow d + 1 = d$, e ciò non è possibile.

E' possibile osservare un'interessante analogia tra l'insieme dei polinomi a coefficienti interi, che denotiamo con $Q[x]$, e quello dei numeri interi, dove per ogni elemento esiste l'opposto rispetto all'addizione, ma non il reciproco rispetto alla moltiplicazione. E' quindi necessario approfondire la questione legata alla *divisibilità* tra polinomi.

Divisibilità tra polinomi

Definizione. Si dice che il polinomio $A(x)$ è *divisibile* per il polinomio $B(x)$ se esiste un polinomio $Q(x)$, detto il *quoziente*, tale che $A(x) = Q(x)B(x)$.

Notiamo come questa definizione richiami quella analoga di divisibilità tra numeri interi.

L'analogia prosegue con la verifica delle seguenti proprietà:

- $D(x) \mid A(x), B(x) \Rightarrow D(x) \mid (A(x) + B(x))$;
- $D(x) \mid A(x) \Rightarrow D(x) \mid A(x)C(x)$;
- $D(x) \mid A(x) \;\; A(x) \mid B(x) \Rightarrow \;\; D(x) \mid B(x)$.

Questo "esame comparato" ci porta alla ricerca dell'analogo per i polinomi dei numeri primi.

Riducibilità tra polinomi

Definizione. Un polinomio si dice *riducibile* se ammette divisori diversi dalle costanti non nulle e da se stesso; in caso contrario si dice *irriducibile*.

I polinomi irriducibili costituiscono quindi l'analogo dei numeri primi.

E' importante notare che la riducibilità di un polinomio è legata all'insieme a cui appartengono i coefficienti. Ad esempio, il polinomio $A(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ è riducibile come polinomio a coefficienti reali, ma non lo è come polinomio a coefficienti interi.

Analogamente, il polinomio $A(x) = x^2 + 1$ non è riducibile come polinomio a coefficienti reali.

Infatti, per stabilire se, in generale, un polinomio di secondo grado è riducibile, occorre vedere se questo può essere scritto come *prodotto di due polinomi di primo grado*. Poniamo quindi $x^2 + 1 = (x + a)(x + b)$. Svolgendo il prodotto al membro di destra, ed uguagliando i coefficienti dei

polinomi ai due membri dell'uguaglianza, otteniamo: $x^2+1=x^2+(a+b)x+ab \Rightarrow \begin{cases} 1=1 \\ 0=a+b \\ 1=ab \end{cases}$,

chiaramente impossibile. Quindi, il polinomio $A(x)=x^2+1$ non è riducibile nell'insieme dei reali. Esiste un insieme in cui, tuttavia, il polinomio $A(x)=x^2+1$ è riducibile: il quoziente Z_2. Infatti, il sistema $\begin{cases} a+b=0 \\ ab=1 \end{cases}$ ha soluzioni $\begin{cases} a=1 \\ b=1 \end{cases}$ (vedi le tavole di composizione dell'addizione e della moltiplicazione in Z_2).

Strumenti molto utili per risolvere questioni legate alla riducibilità dei polinomi, sono rappresentati dai *prodotti notevoli*. Ne riportiamo alcuni, espressi in modo "opportuno".

$$\left(a^2x^2-b^2\right)=\left(ax-b\right)\left(ax+b\right),\ \left(a^3x^3-b^3\right)=\left(ax-b\right)\left(a^2x^2+abx+b^2\right),\ \left(ax+b\right)^n=\sum_{k=0}^{n}\binom{n}{k}a^kx^kb^{n-k}.$$

Esercizi

1. Scrivere il polinomio $x^{12}+x^6+1$ come prodotto di fattori (*fattorizzare*, cioè, il polinomio).
2. Dimostrare che in Z_n vale l'uguaglianza $x^2-ax+k=x^2-(a-n)x+n+k$.
3. Si determinino *a*, e *b* in modo tale che i polinomi x^3-2ax^2+bx+1 e $x^3+2bx^2+(a-1)x+1$ siano identici.
4. Eseguire nell'insieme dei polinomi $Z_7[x]$ il prodotto $\left(x^2-5x+1\right)(x+4)-(3-x^2)(6+x^3)$. A cosa corrisponde questo prodotto in $Z_5[x]$? Ed in $Z_3[x]$?.
5. Si trovi un insieme in cui il polinomio x^2+9 è riducibile.
6. Dato il polinomio $A(x)=ax^2+bx+c$, determinare *a*, *b*, *c* affinché $A(x+1)-A(x)=x$. Supponiamo inoltre che la variabile *x* possa assumere soltanto i valori "naturali" 1, 2, 3,…Si dimostri che dalle differenze $A(n+1)-A(n)$ è possibile ottenere la formula della *somma dei primi N numeri naturali*.
7. Si sfruttino le considerazioni dell'esercizio precedente per calcolare, a partire dal polinomio $A(x)=ax^3+bx^2+cx+d$, la somma dei quadrati dei primi N numeri naturali.
8. Si dica per quale valore di *h* il polinomio x^3-4x^2+4x+h è divisibile per $x+1$.
9. Si sviluppino i seguenti prodotti notevoli: $\left(a^3+b^3x^3\right)$, $\left(x+1\right)^7$.

Soluzioni

1. $x^{12}+x^6+1=\left(x^6+1\right)^2-x^6=\left[\left(x^6+1\right)-x^3\right]\left[\left(x^6+1\right)+x^3\right]$
2. $Z_n:\begin{cases} -a=-a+n=-(a-n) \\ k=k+n \end{cases}$.
3. $\begin{cases} -2a=2b \\ b=a-1 \end{cases} \Rightarrow \begin{cases} a=1/2 \\ b=-1/2 \end{cases}$.
4. $x^5-2x^3+5x^2-19x-14=\begin{cases} x^5-2x^3+5x^2+2x \quad (Z_7) \\ x^5-2x^3+x+1 \quad (Z_5) \\ x^5-2x^3+2x^2+2x+1 \quad (Z_3) \end{cases}$.

5. $\begin{cases} a+b=0 \\ ab=9 \end{cases}$ in Z_{10} risulta, ad esempio, $\begin{cases} 1+9=0 \\ 1\cdot 9=9 \end{cases}$.

6. $x=A(x+1)-A(x)=a(x+1)^2+b(x+1)+c-ax^2-bx-c=2ax+a+b \Rightarrow \begin{cases} 2a=1 \\ a+b=0 \end{cases} \Rightarrow \begin{cases} a=1/2 \\ b=-1/2 \end{cases}$

   Dalla somma delle $A(n+1)-A(n)=n$, otteniamo il valore della somma dei primi *n* numeri naturali: $A(n+1)-A(1)=\frac{(n+1)^2}{2}-\frac{n+1}{2}+c-\frac{1}{2}+\frac{1}{2}-c=\frac{n(n+1)}{2}$.

7. $x^2=A(x+1)-A(x)=3ax^2+(3a+2b)x+a+b+c \Rightarrow \begin{cases} 3a=1 \Rightarrow a=1/3 \\ 3a+2b=0 \Rightarrow b=-1/2 \\ a+b+c=0 \Rightarrow c=1/6 \end{cases}$. Da questo segue $A(n+1)-A(1)=\frac{(n+1)^3}{3}-\frac{(n+1)^2}{2}+\frac{n+1}{6}+d-\frac{1}{3}+\frac{1}{2}-\frac{1}{6}-d=\frac{n(n+1)(2n+1)}{6}$.

8. Posto $x^3-4x^2+4x+h=(x+1)(ax^2+bx+c) \Rightarrow h=9$.

9. $\left(a^3+b^3x^3\right)=\left(a+bx\right)\left(a^2-abx+b^2x^2\right)$,

   $(x+1)^7=\sum_{k=0}^{7}\binom{7}{k}x^k 1^{7-k}=1+7x+21x^2+35x^3+35x^4+21x^5+7x^6+x^7$.

3.2 Divisione con resto fra polinomi

Vediamo se le operazioni che hanno permesso, nel caso della divisione tra numeri interi, di determinare quoziente e resto, si possono adattare all'insieme dei polinomi. Ad esempio, abbiamo scritto "32 diviso 12 " nella forma $32=2\cdot 12+8$, dove 2 rappresentava il quoziente, e 8 il resto. Ora, quanto scritto può essere interpretato come il risultato di 2 (quoziente) sottrazioni successive:

$$\begin{array}{l} 32-12=20 \\ \underline{20-12=8} \\ 32+20-2\cdot 12=20+8 \Rightarrow 32=2\cdot 12+8 \end{array} \quad .$$

Proviamo ad applicare questo metodo al caso dei polinomi. Siano $A(x)=5x^4-3x^2+4x-2$ e $B(x)=5x^2-1$. Se dividiamo il monomio di grado massimo di $A(x)$ per quello di $B(x)$ otteniamo: $5x^4/5x^2=x^2$ e, quindi $A(x)-x^2B(x)=-2x^2+4x-2:=R_1(x)$. Ripetiamo il procedimento dividendo stavolta il monomio di grado massimo del resto venutosi a formare al passaggio precedente, $R_1(x)$, sempre per quello di $B(x)$: $R_1(x)-\left(-\frac{2}{5}\right)B(x):=4x-\frac{12}{5}:=R_2(x)$. Il processo si arresta quando il grado del polinomio resto che si viene a formare è *minore* di quello del polinomio divisore $B(x)$. Ricapitolando:

$$\begin{array}{l} A(x)-x^2B(x)=-2x^2+4x-2:=R_1(x) \\ \underline{R_1(x)-\left(-\frac{2}{5}\right)B(x)=4x-\frac{12}{5}:=R_2(x),\ \ \deg\left[R_2(x)\right]<\deg\left[B(x)\right]} \\ A(x)-\left(x^2-\frac{2}{5}\right)B(x)=4x-\frac{12}{5} \end{array} \quad .$$

Con questo procedimento sembra possibile determinare il resto *senza* effettuare la divisione che, tuttavia, poteva essere eseguita con il metodo usuale (che poggia su quanto appena visto):

$$\begin{array}{l|l} 5x^4-3x^2+4x-2 & \\ \underline{-5x^4+x^2} & \\ -2x^2+4x-2 & \dfrac{5x^2-1}{x^2-\dfrac{2}{5}}. \\ \underline{2x^2-\dfrac{2}{5}} & \\ 4x-\dfrac{12}{5}:=R(x) & \end{array}$$

Questo metodo di divisione può essere generalizzato, ed enunciato formalmente come teorema.

Teorema 1. *Siano* $A(x)$ *e* $B(x)$ *due polinomi tali che* $\deg[A(x)]=n\geq\deg[B(x)]=m$. *Allora è possibile sottrarre ad* $A(x)$ *un multiplo di* $B(x)$, *detto* $Q(x)$, *in modo da ottenere un polinomio* $R(x)$ *di grado inferiore a quello di* $A(x)$.

Dimostrazione. Si tratta di compiere il procedimento visto sopra: $A(x)-\dfrac{a_n}{b_m}x^{n-m}B(x):=R(x)$, e di iterarlo sostituendo ad ogni passo il dividendo con il resto che si viene così a formare, finché non si ottiene un resto di grado minore di quello del divisore.

Esercizi

10. Determinare il resto, senza eseguire la divisione, tra i polinomi $A(x)=3x^3+5x^2-x+2$ e $B(x)=x+2$.
11. Determinare *a*, *b* in modo tale che il polinomio $2x^4+ax^3+x^2+4x+b$ sia divisibile per x^2+x.

Soluzioni

$$\frac{3x^3}{x}=3x^2\Rightarrow A(x)-3x^2B(x)=-x^2-x+2:=R_1(x);$$

10. Si ha $\dfrac{-x^2}{x}=-x\Rightarrow R_1(x)-(-x)B(x)=x+2:=R_2(x);$.

$$\frac{x}{x}=1\Rightarrow R_2(x)-(1)B(x)=0\Rightarrow A(x)=(3x^2-x+1)(x+2)\Rightarrow R(x)=0$$

11. Si determina il resto: $R_3(x)=(a+1)x+b\Rightarrow R_3(x)=0\Leftrightarrow\begin{cases}a=-1\\ b=0\end{cases}$.

A questo punto è possibile enunciare un risultato che ricorda molto uno analogo relativo alla divisione tra interi.

Teorema 2. *Siano* $A(x)$ *e* $B(x)$ *due polinomi tali che* $B(x)\neq 0$. *Esiste un'unica coppia di polinomi* $Q(x),R(x)$ *tali che* $A(x)=B(x)\cdot Q(x)+R(x)$, *dove* $\deg[R(x)]<\deg[B(x)]\vee\deg[B(x)]=0$.

Dimostrazione. L'esistenza è una diretta applicazione del metodo visto nel teorema 1. Si dimostra quindi l'unicità, supponendo per assurdo l'esistenza di due coppie tali che

$\begin{matrix} A(x) = B(x)\cdot Q_1(x) + R_1(x) \\ A(x) = B(x)\cdot Q_2(x) + R_2(x) \end{matrix}$. Sottraendo membro a membro si ottiene l'uguaglianza $0 = B(x)\left[Q_1(x) - Q_2(x)\right] + \left[R_1(x) - R_2(x)\right]$. Se $\left[Q_1(x) - Q_2(x)\right]$ fosse diverso da zero, sarebbe un polinomio di grado *k*, quindi $B(x)\left[Q_1(x) - Q_2(x)\right]$ avrebbe grado $m+k$. Ora, per ipotesi, $\left[R_1(x) - R_2(x)\right]$ ha grado minore di *m*, quindi il membro di destra dell'uguaglianza $0 = B(x)\left[Q_1(x) - Q_2(x)\right] + \left[R_1(x) - R_2(x)\right]$ avrebbe grado $m+k$, e non potrebbe quindi essere uguale al polinomio nullo, membro di sinistra.

Analogamente al caso dei numeri interi, il polinomio $A(x)$ è divisibile per $B(x)$ *se e soltanto se* il resto $R(x)$ è uguale a zero. Sussiste al riguardo il seguente risultato.

3.3 Il teorema di Ruffini

Teorema 3. (Ruffini) *Il polinomio* $A(x)$ *è divisibile per* $(x-\alpha)$ *quando il resto* $R(x)$ *è uguale a zero, quindi se e solo se* $A(\alpha) = 0$. In questo caso si dice che α è una *radice* del polinomio.
Dimostrazione. $(\Rightarrow)$ $A(x)$ è divisibile *per* $(x-\alpha)$, allora $A(x) = (x-\alpha)Q(x) \Rightarrow A(\alpha) = (\alpha-\alpha)Q(\alpha) = 0$.
$(\Leftarrow)$ Viceversa, posto $A(x) = (x-\alpha)Q(x) + R(x)$, segue che $\deg\left[R(x)\right] < \deg\left[x-\alpha\right] = 1$, quindi il resto è una *costante,* per cui $A(x) = (x-\alpha)Q(x) + h$. Si giunge alla tesi facendo vedere che questa costante è 0: per ipotesi $A(\alpha) = 0$, allora $0 = A(\alpha) = (\alpha-\alpha)Q(\alpha) + h \Rightarrow h = 0$.

Tra le conseguenze del teorema di Ruffini consideriamo le seguenti.
Proposizione 1. Un polinomio di terzo grado è riducibile se e solo se ammette una radice.
Dimostrazione. $(\Rightarrow)$ Un polinomio di terzo grado riducibile può essere scritto nel prodotto di un polinomio di grado uno per un polinomio di grado due. La tesi segue dal fatto che un polinomio di grado uno ammette sempre una radice.
$(\Leftarrow)$ Viceversa, se il polinomio $A(x)$ ammette una radice α, può essere scritto nella forma $A(x) = (x-\alpha)Q(x)$, dove il quoziente è un polinomio di grado due.

Proposizione 2. Se α è una radice di un polinomio a coefficienti interi, allora α divide il termine noto.
Dimostrazione. $P(x) = a_0 + a_1 x + \ldots + a_n x^n \Rightarrow 0 = P(\alpha) \Rightarrow -a_0 = \alpha\left(a_1 + a_2 x + \ldots + a_n x^{n-1}\right) \Rightarrow \alpha \mid a_0$.

Esercizi

12. Trovare tutte le radici, intere o razionali, del polinomio $x^4 - 3x^3 - 2x^2 - 32$.
13. Tra i polinomi di secondo grado che divisi per $(x-1), (x-2)$ danno per resto 4, determinare quello che ha come radice $\alpha = 0$.
14. E' dato il polinomio $P_n(x) = x^n + 1$ sull'insieme degli interi. Per quali valori di *n* è riducibile? In tal caso, si dica quant'è il valore dei coefficienti del polinomio di grado massimo che si viene a determinare nella divisione.
15. Dividere il polinomio $x^{16} - 1$ per $x-1$, e determinare i coefficienti del polinomio quoziente.
16. Si trovino le intersezioni tra la parabola di vertice $V(2,2)$ passante per l'origine, e l'iperbole $xy = 12$.
17. Per quali valori di *k* la parabola di equazione $y = x^2 - 2x - 1$ interseca l'iperbole $xy = k$ in punti ad ascissa intera?
18. Sia $P(x)$ un polinomio e $Q(x) = P(x) + 1$. Dimostrare che $P(x)^{2n} + Q(x)^n - 1$ è divisibile per il prodotto $P(x)\cdot Q(x)$.
19. Dimostrare che un polinomio è divisibile per $(x-1)$ se la somma dei suoi coefficienti è zero.

20. Trovare tutte le radici di x^3-3x^2+2x in Z_6.

Soluzioni

12. Si osserva che $x=4$ e $x=-2$ sono radici del polinomio, quindi questo può essere scritto nella forma $x^4-3x^3-2x^2-32=(x-4)(x+2)(x^2-x+4)$, con l'ultimo fattore irriducibile in R.

13. $\begin{matrix} ax^2+bx+c=(ax+a+b)(x-1)+a+b+c \\ ax^2+bx+c=(ax+2a+b)+4a+2b+c \end{matrix} \Rightarrow \begin{cases} a+b+c=4 \\ 4a+2b+c=4 \end{cases} \Rightarrow \begin{cases} b=-3a \\ c=4+2a \end{cases}$. Il polinomio può quindi essere scritto nella forma $P(x)=ax^2-3ax+4+2a$. Imponendo $P(0)=0$ otteniamo il polinomio: $P(0)=0\Rightarrow 4+2a=0\Rightarrow a=-2\Rightarrow P(x)=-2x^2+6x$.

14. Il polinomio è riducibile se *n* è dispari. In tal caso $x=-1$ è una radice, quindi può essere diviso per il polinomio $x+1$; di conseguenza $P_n(x)=x^n+1=\left(a_0+a_1x+...+a_{n-1}x^{n-1}\right)(x+1)$. I coefficienti del polinomio quoziente di grado $n-1$ si determinano eseguendo la moltiplicazione dei fattori presenti al membro di destra, ed imponendo *l'unicità* della forma canonica: $x^n+1=a_0+(a_0+a_1)x+(a_1+a_2)x^2+...+(a_{n-2}+a_{n-1})x^{n-1}+a_{n-1}x^n$ da cui seguono le uguaglianze $a_0=1,\quad a_{n-1}=1\Rightarrow a_{n-2}=-1\Rightarrow a_{n-3}=1\Rightarrow ...\Rightarrow a_1=-1$, ottenute ponendo uguale a zero tutte le somme tra parentesi. Il quoziente è quindi $Q_{n-1}(x)=\sum_{k=0}^{n-1}(-1)^k x^k$.

15. $x^{16}-1=(x-1)(x+1)\left(x^2+1\right)\left(x^4+1\right)\left(x^8+1\right)$. Poiché $x=1$ è una radice del polinomio, non c'è in realtà bisogno di fare grandi calcoli: si procede, con qualche adattamento, come nell'esercizio precedente:
$x^{16}-1=\left(a_0+a_1x+...+a_{n-1}x^{n-1}\right)(x-1)=-a_0+(a_0-a_1)x+(a_1-a_2)x^2+...(a_{n-2}-a_{n-1})x^{n-1}+a_{n-1}x^n$
$a_0=1\Rightarrow a_1=a_2=...=a_{n-1}=1$

16. Si mette a sistema l'equazione della parabola $y-2=-\frac{1}{2}(x-2)^2\Rightarrow y=-\frac{x^2}{2}+2x$, con quella dell'iperbole, ottenendo l'equazione risolvente $x^3-4x^2+24=0$. Le soluzioni dell'equazione sono radici del polinomio $P(x)=x^3-4x^2+24$; poiché una di queste è $x=-2$, il polinomio può essere fattorizzato nel prodotto $x^3-4x^2+24=(x+2)\left(x^2-6x+12\right)$. Essendo il polinomio di secondo grado irriducibile nell'insieme dei numeri reali, l'unica intersezione tra la parabola e l'iperbole è rappresentata dal punto $(-2;-6)$.

17. Dall'equazione risolvente $x^3-2x^2-x-k=0$ e dalla divisibilità per $x=n\in Z$ otteniamo la fattorizzazione $x^3-2x^2-x-k=(x-n)\left(x^2+(n-2)x+n^2-2n-1\right)$, con resto zero $n\left[n(n-2)-1\right]-k=0\Rightarrow k=n\left[n(n-2)-1\right]$. Il valore (o i valori) di *k* dipendono da quelli di *n* che forniscono radici intere del polinomio di secondo grado nella fattorizzazione. Questi valori si ottengono imponendo che il discriminante dell'equazione associata al fattore di secondo grado sia non negativo: $-3n^2+4n+8\geq 0\Rightarrow \frac{2-2\sqrt{7}}{3}\leq n\leq \frac{2+\sqrt{7}}{3}\Rightarrow n=0,1$. Per $n=1$ otteniamo $k=-2$ e $x^3-2x^2-x+2=(x-1)\left(x^2-x-2\right)=(x-1)(x+1)(x-2)$. Per $n=0$ otteniamo $k=0$ e l'iperbole non esiste.

18. Posto $P(x) = Q(x) - 1$, poiché $Q(x)^n - 1$ è divisibile per $Q(x) - 1$ si ha
$P(x)^{2n} + Q(x)^n - 1 = P(x)^{2n} + Q(x)^n + P(x) - Q(x) = P(x)(P(x)^{2n-1} + 1) + Q(x)(Q(x)^{n-1} - 1)$.
Ora, poiché nel caso in cui *n* è dispari $x^n + 1$ è divisibile per $x + 1$, essendo $2n - 1$ dispari, allora $P(x)^{2n-1} + 1$ è divisibile per $P(x) + 1$, ovvero per $Q(x)$. In definitiva,
$P(x)^{2n} + Q(x)^n - 1 = P(x)(P(x)^{2n-1} + 1) + Q(x)(Q(x)^{n-1} - 1) =$
$P(x)A(x)Q(x) + Q(x)B(x)P(x) = Q(x)P(x)(A(x) + B(x))$.
19. Per il teorema di Ruffini, la divisibilità per $(x - 1)$ equivale a dire che $x = 1$ è una radice del polinomio, quindi $0 = P(1) = a_0 + a_1 + ... + a_n$.
20. $x^3 - 3x^2 + 2x = x(x^2 - 3x + 2)$. Una radice è evidentemente $x = 0$. Le altre possono essere individuate, per la proprietà conseguente al teorema di Ruffini, tra i divisori del termine noto, che sono in Z_6 , oltre a $x = 1$ e $x = 2$, anche $x = 4$ e $x = 5$, dal momento che $5 \cdot 4 = 20 \equiv 2_6$. Sostituendo questi valori nel polinomio di secondo grado e svolgendo i calcoli con le classi di resto modulo 6, si trova che le soluzioni sono 0, 1, 2, 4, 5.