Esercizi sui polinomi (tratti dalle tracce di esame)

Traccia del 25 settembre 2020

(a) Nel gruppo moltiplicativo $\mathbb{Z}_{101}^*$, che è ciclico, e il cui ordine è 100, esiste un elemento di periodo 50 (generatore dell'unico sottogruppo H di ordine 50). Allora, per ogni $\alpha \in H$, in virtù del Teorema di Lagrange, si ha che $\alpha^{50} = \overline{1}$. Pertanto, per ogni $\alpha \in H$,

$$\overline{f}(\alpha) = \sum_{i=0}^{100} \left(\alpha^{50}\right)^i = \overline{101} = \overline{0}.$$

Quindi i 50 elementi di H sono radici di $\overline{f}(X)$ in $\mathbb{Z}_{101}$.

(b)

- *Primo metodo:*

Il termine noto del polinomio $\overline{f}(X)$ è $\overline{1}$, quindi lo zero di $\mathbb{Z}_5$ non è certamente sua radice.
Effettuiamo la seguente distinzione fra gli esponenti di X: i multipli di 50 con fattore pari sono multipli di 4, quelli con fattore dispari sono congrui a 50, e quindi a 2, modulo 4.
Sia $\alpha \in \mathbb{Z}_5^*$. Sapendo, per Lagrange, che $\alpha^4 = \overline{1}$, si ha allora quanto segue:

$$\overline{f}(\alpha) = \overline{1} + \sum_{i=1}^{50} \alpha^{50 \cdot 2i} + \sum_{i=0}^{49} \alpha^{50 \cdot (2i+1)} = \overline{1} + \overline{50} + \overline{50}\alpha^2 = \overline{1} \neq \overline{0}.$$

In conclusione, l'insieme delle radici di $\overline{f}(X)$ in $\mathbb{Z}_5$ è vuoto.

- *Secondo metodo:*

Sia $\alpha \in \mathbb{Z}_5^*$. Si ha, per il Piccolo Teorema di Fermat, $\alpha^{50} = \left(\left(\alpha^5\right)^5\right)^2 = \alpha^2$. Dunque $\overline{f}(\alpha) = \sum_{i=0}^{100} \left(\alpha^2\right)^i$. In base ad una nota identità aritmetica, si ha quindi:

$$\alpha^{202} - \overline{1} = \left(\alpha^2\right)^{101} - \overline{1} = \left(\alpha^2 - \overline{1}\right)\overline{f}(\alpha),$$

ove, sempre per il Piccolo Teorema di Fermat, $\alpha^{202} = \left(\alpha^{25}\right)^8 \alpha^2 = \alpha^8 \alpha^2 = \left(\alpha^5\right)^2 = \alpha^2$. Quindi si ha:

$$\alpha^2 - \overline{1} = \left(\alpha^2 - \overline{1}\right)\overline{f}(\alpha).$$

Pertanto, se α è radice, allora $\alpha^2 - \overline{1} = \overline{0}$. Ma ciò avviene se e solo se $\alpha \in \{\overline{1}, -\overline{1}\}$. Tuttavia, in tal caso, $\overline{f}(\alpha) = \overline{101} = \overline{1} \neq \overline{0}$. Ciò prova che $\overline{f}(X)$ non possiede radici in $\mathbb{Z}_5$.

Traccia dell'11 settembre 2020

(a) Il polinomio $f(X)$ ha sempre $\overline{p-1} = -\overline{1}$ come radice, visto che, in base al Piccolo Teorema di Fermat, $(-\overline{1})^{p+2} = (-\overline{1})^3 = -\overline{1}$. Questa è anche l'unica radice se $p = 2$, in quanto in tal caso $f(X) = X^4 + \overline{1} = (X + \overline{1})^4$.
(Per ogni $a(X), b(X) \in \mathbb{Z}_p[X]$,

$$(a(X) + b(X))^{p^2} = ((a(X) + b(X))^p)^p = \left(a(X)^p + b(X)^p\right)^p = a(X)^{p^2} + b(X)^{p^2},$$

e, come si stabilisce per induzione, vale l'analoga proprietà per ogni esponente che sia una potenza di

p).
Sia ora $p > 2$.
In generale, $\alpha \in \mathbb{Z}_p$ è radice se e solo se $\left(\alpha^{p+2} = \right)\alpha^3 = -\overline{1}$. In tal caso $\alpha^6 = \overline{1}$, e quindi, nel gruppo moltiplicativo $\mathbb{Z}_p^*$, $o(\alpha)$ divide 6. Però $o(\alpha)$ non è 1 (dato che $\overline{1}$ non è radice di $f(X)$), né 3. E se $o(\alpha) = 2$, allora $\alpha = -\overline{1}$, radice già trovata. Quindi le radici di $f(X)$ distinte da $-\overline{1}$, se ne esistono, sono tutti e soli gli elementi di $\mathbb{Z}_p^*$ aventi periodo 6. Questi elementi esistono (nel gruppo ciclico $\mathbb{Z}_p^*$, di ordine $p-1$) se e solo se $6|p-1$. Quattro valori di p siffatti sono $7,\ 13,\ 19,\ 31$. Per ciascuno di tali valori di p, il numero delle radici distinte è dunque $1 + \varphi(6) = 3$.

(b) Sia $\alpha \in \mathbb{Z}_p$. Allora, tenendo conto del Piccolo Teorema di Fermat, α è radice di $g(X)$ se e solo se $\alpha^{8436} = \overline{1}$. In tal caso $\alpha \in \mathbb{Z}_p^*$, e dunque $\alpha^{p-1} = \overline{1}$. Pertanto l'uguaglianza voluta sarà verificata da ognuno dei $p-1$ elementi di $\mathbb{Z}_p^*$ se $p-1$ sarà un divisore di 8436. Due valori di p siffatti, e maggiori di 100, sono 149 e 229.

Traccia del 17 febbraio 2020

(a) Si ha $f(X)(X-\overline{1}) = X^{p-1} - \overline{1}$, polinomio decomponibile nel prodotto $\prod_{\alpha \in \mathbb{Z}_p^*}(X-\alpha)$. Ne consegue che $f(X) = \prod_{\alpha \in \mathbb{Z}_p^* \setminus \{\overline{1}\}}(X-\alpha)$. Quindi le radici di $f(X)$ in $\mathbb{Z}_p$ sono tutti e soli gli elementi distinti da $\overline{0}$ e $\overline{1}$.

(b) Si ha $g(X) = X^{p-1} - \overline{1} + X + \overline{1}$. Per quanto osservato al punto (a), $f(X)$ divide $X^{p-1} - \overline{1}$. Ora, se $p = 3$, allora $f(X) = X + \overline{1}$, e quindi $f(X)$ divide $g(X)$, e dunque il resto è $\overline{0}$. Se invece $p > 3$, allora $\deg f(X) = p - 2 > 1$, pertanto il resto è $X + \overline{1}$.

Traccia del 31 gennaio 2020

(a) Si noti anzitutto che $\overline{0}$ è radice del fattore di $f(X)$ corrispondente ad $\alpha = \overline{0}$. Sia ora $\beta \in \mathbb{Z}_p^*$. Allora $\beta^{p-1} = \overline{1}$, e quindi β è radice del fattore di $f(X)$ corrispondente ad $\alpha = -\overline{1} - \beta^2$. Se ne deduce che ogni elemento di $\mathbb{Z}_p$ è radice di $f(X)$.

(b) Alla luce di (a), il polinomio $X^{p-1} - \overline{1} = \prod_{\alpha \in \mathbb{Z}_p^*}(X-\alpha)$ divide $f(X)$ ed è dunque il massimo comune divisore cercato.

Traccia del 15 gennaio 2020

(a) Si ha

$$f(X) = X^{3p} + X^{2p} - X^p - \overline{1} = \left(X^3 + X^2 - X - \overline{1}\right)^p = \left((X+\overline{1})(X^2-\overline{1})\right)^p =$$
$$(X+\overline{1})^{2p}(X-\overline{1})^p$$

Le radici di $f(X)$ in $\mathbb{Z}_p$ sono dunque:

- se $p = 2,$ una sola, $\alpha = \overline{1}$, di molteplicità 6;
- se $p > 2,$ due, ossia $\alpha_1 = \overline{1}$, di molteplicità $p,$ e $\alpha_2 = -\overline{1}$, di molteplicità $2p$.

(b) Sia $g(X) = X^{3p} - X^{2p} - X^p + \overline{1}$. Allora

$$g(X) = \left(X^3 - X^2 - X + \overline{1}\right)^p = \left((X-\overline{1})\left(X^2-\overline{1}\right)\right)^p = (X-\overline{1})^{2p}(X+\overline{1})^p.$$

Confrontando le fattorizzazioni di $f(X)$ e $g(X)$ si ricava

$$\mathrm{MCD}(f(X), g(X)) = (X+\overline{1})^p(X-\overline{1})^p = \left(X^2-\overline{1}\right)^p = X^{2p} - \overline{1} \text{ se } p \neq 2.$$

Se invece $p = 2,$ allora $f(X) = g(X) = \mathrm{MCD}(f(X), g(X))$.

Traccia del 15 novembre 2019

Ogni radice razionale di $f(X)$ è intera. Si osservi che, per ogni intero $a,$ la somma $a^n + a^m$ è un intero pari. Quindi, se $p > 2$, non vi sono radici. Sia allora $p = 2$. Se $n = m$, allora $f(X) = 2X^n + 2$ non ha radici se n è pari, altrimenti ha come unica radice -1. Supponiamo allora che sia $n > m$. Se l'intero a è radice, allora $a^m\left(a^{n-m}+1\right) = -2$. Quindi a è un divisore negativo di 2. Se $a = -1$, allora il primo membro è uguale a $(-1)^m\left((-1)^{n-m}+1\right)$, ove $n-m$ è pari, mentre m è dispari (e quindi n è dispari). In tutti questi casi -1 è radice. Se invece $a = -2,$ allora $m = 1$. Ma il numero tra parentesi non può essere 1. Quindi l'uguaglianza non è verificata.
In conclusione, si hanno radici razionali (una sola radice, pari a -1) se e solo se $p = 2$ ed n, m sono entrambi dispari.

Traccia del 25 settembre 2019

(a) Esiste, nel gruppo moltiplicativo (ciclico) $\mathbb{Z}_p^*$, un elemento α di periodo $p-1$. Dunque le potenze α^i, con $0 \leq i \leq p-2$, sono tutti i $p-1$ elementi del gruppo. Pertanto

$$f(\alpha) = \sum_{i=0}^{p-2} \alpha^i = \sum_{i=1}^{p-1} [i]_p = \left[\sum_{i=1}^{p-1} i\right]_p = \left[\frac{p(p-1)}{2}\right]_p = [0]_p,$$

in quanto, essendo p dispari, il numero $\dfrac{p-1}{2}$ è intero.

(b) Un calcolo del tutto analogo al precedente mostra che $[1]_p$ è radice di $g(X)$.

Traccia del 10 settembre 2019

(a) Sia $\alpha \in \mathbb{Z}_p$. Allora, alla luce del Piccolo Teorema di Fermat,

$$f(\alpha) = \alpha^{2p^2} - \overline{2}\alpha^{p^2} - \alpha^p + \overline{2} = \alpha^2 - \overline{2}\alpha - \alpha + \overline{2} = \alpha^2 - \overline{3}\alpha + \overline{2} = (\alpha-\overline{1})(\alpha-\overline{2}).$$

Quindi α è radice di $f(X)$ se e solo se $\alpha \in \{\overline{1}, \overline{2}\}$.

(b) Poiché, per il Piccolo Teorema di Fermat, $\overline{2}^p = \overline{2}$ e $\overline{-3}^p = \overline{-3}$, si ha

$$g(X) = X^{2p} - \overline{3}X^p + \overline{2} = X^{2p} + \left(\overline{-3}^p X^p\right) + \overline{2}^p = \left(X^2 - \overline{3}X \ + \overline{2}\right)^p = ((X-\overline{1})(X-\overline{2}))^p.$$

D'altra parte

$f(X) = h(X)^p$,

ove $h(X) = X^{2p} - \overline{2}X^p - X + \overline{2}$ ha radici $\overline{1}$ e $\overline{2}$, sempre distinte. Ciò prova che $\ell(X) = (X-\overline{1})(X-\overline{2})$ divide $h(X)$. Ne consegue che $g(X) = \ell(X)^p$ divide $f(X)$. Pertanto $\mathrm{MCD}(f(X),\ g(X)) = g(X)$.

<u>Traccia del 5 luglio 2019</u> (v. anche Eserciziario N.3)

(a) Sia $\alpha \in \mathbb{Z}_p$ radice di $f(X)$. Allora $\alpha \in \mathbb{Z}_p^*$, e quindi $\alpha^{p-1} = \overline{1}$. Ora

$$f(\alpha) = \left(\alpha^{p!}\right)^2 + \alpha^{p!} + \overline{1}.$$

Quindi α è radice di $f(X)$ se e solo se l'elemento a secondo membro è nullo. Si noti che i primi due addendi sono potenze di α^{p-1}, e quindi sono entrambi pari a $\overline{1}$. Pertanto $f(\alpha) = \overline{3}$. Questo è $\overline{0}$, e lo è per ogni $\alpha \in \mathbb{Z}_p^*$, se e solo se $p = 3$. Negli altri casi non vi sono radici in $\mathbb{Z}_p$.

(b) Analogamente a sopra si ricava che $\overline{0}$ non è radice, mentre, per ogni $\alpha \in \mathbb{Z}_p^*$, $g(\alpha) = \overline{6}$. Quindi $g(X)$ ha radici se e solo se $p = 2$ oppure $p = 3$; nel primo caso l'unica radice è $\overline{1}$, nel secondo caso vi sono due radici, $\overline{1}$ e $\overline{2}$.