Aritmetica 2017-2018

Esercizi

1 02.10.2017

1.1 Induzione

- Sia r un numero reale tale che $r + 1/r$ è un intero. Allora per ogni intero $n \geq 1$ si ha che $r^n + 1/r^n$ è intero.
- Dimostrare che i numeri di Fibonacci ($F_0 = 0, F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3$) soddisfano l'uguaglianza
$$F_n^2 = F_{n+1}F_{n-1} + (-1)^{n+1}$$
- Sia D_n il numero di modi di coprire una griglia $2 \times n$ con tesserine 2×1. Allora $D_1 = 1$, $D_2 = 2$, $D_3 = 3$... e D_n?

1.2 Calcolo combinatorio

- Il totocalcio è un gioco al quale per ognuna di 13 partite si sceglie uno fra $\{1, 2, X\}$. Quante possibili schedine del totocalcio posso giocare? Qual è la probabilità di fare 13? Qual è la probabilità di fare almeno 12? Qual è la probabilità di fare esattamente 12? Qual è la probabilità di fare 0? Dimostrare che la probabilità di fare esattamente k, per $0 \leq k \leq 13$, è $\binom{13}{k} \left(\frac{2}{3}\right)^{13-k} \left(\frac{1}{3}\right)^k$.
- Sia X un insieme con 100 elementi. Quante coppie di sottoinsiemi (A, B) di X esistono tali che $\#(A \cap B) = 30$? E quante coppie esistono tali che $\#(A \cup B) = 30$?

1.3 Qualche problema extra, per chi si vuole esercitare

- Dimostrare che $4^n + 15n - 1$ è divisibile per 9 per ogni n intero positivo.
- Dimostrare che per ogni intero positivo n si ha $n! \geq n^{n/2}$.

2 04.10.2017

- (Principio di inclusione-esclusione) Quanti sono i numeri interi $1 \leq n \leq 1000$ che non sono divisibili né per 2, né per 3, né per 5?
- (Funzioni surgettive) Ci sono 3 scatole (una tonda, una quadrata, e una rettangolare) e sette palline colorate (di sette colori diversi). Quanti modi esistono di piazzare le palline nelle scatole in modo che ogni scatola contenga almeno una pallina?
- (Dal compito del 20 luglio 2015) Determinare il numero di terne ordinate di numeri interi positivi (x, y, z) tali che $xyz = 10^{100}$, e il numero di terne per le quali $x^2yz = 10^{100}$.
- Qual è la probabilità di fare 6 al superenalotto?
- Quanti sono i modi di distribuire le carte a bridge [52 carte distribuite in gruppi da 13 fra 4 giocatori distinguibili]?
- Quante persone servono per far sì che con probabilità $\geq 50\%$ due abbiano lo stesso compleanno? E per essere *sicuri* che due abbiano lo stesso compleanno?
- Dimostrare che per $0 \leq k \leq m \leq n$ si ha

$$\binom{n}{m}\binom{m}{k} = \binom{n}{k}\binom{n-k}{m-k}$$

- Dimostrare che

$$\sum_{l=0}^{k} \binom{n}{l}\binom{n}{k-l} = \binom{2n}{k}$$

(Indicazione: se fra $2n$ persone vogliamo sceglierne k, il numero di modi è il lato destro dell'uguaglianza. Ma se queste $2n$ persone fossero n uomini ed n donne, cosa rappresenterebbe il lato sinistro?)

2.1 Challenges

- Dimostrare che per ogni $n \geq 1$ si ha

$$\sum_{k=0}^{n} k\binom{n}{k} = n \cdot 2^{n-1}$$

(Indicazione: quante squadre si possono formare avendo a disposizione n persone, se supponiamo di voler inoltre scegliere un capitano fra i membri della squadra?)

- Dimostrare che il numero di modi di scrivere un intero positivo n come somma (non ordinata!) di interi non-negativi e ognuno $\leq k$ è uguale al numero di modi di scrivere n come somma (non ordinata!) di al più k interi non-negativi.

  Per esempio, il numero di modi di scrivere 5 come somma di al più due parti sono solo 3, 5, $4+1$, e $3+2$ (ricordiamo che in questo problema l'ordine non conta). Questo è anche il numero di modi di scrivere 5 come somma di parti ognuna ≤ 2: infatti 5 si scrive come $1+1+1+1+1$, come $2+1+1+1$, e come $2+2+1$.

3 11.10.2017

- (Dal primo compitino di Aritmetica del 2014) Determinare il numero di sottoinsiemi di $\{1, 2, \ldots, 100\}$ costituiti di tre elementi la cui somma sia 100.
- (Da un compito di Aritmetica dell'anno accademico 2005-2006) Determinare il numero delle terne ordinate (a, b, c) tali che esattamente due fra a, b, c sono pari, esattamente uno fra a, b, c è multiplo di 3, e $1 \leq a, b, c \leq 60$.
- Trovare il numero di divisori positivi di un intero positivo $n = p_1^{e_1} \cdots p_k^{e_k}$.

  Risposta: $(e_1 + 1) \cdots (e_k + 1)$.
- Sia n un intero positivo. Il numero di divisori positivi di n è *dispari* se e solo se n è un quadrato perfetto.
- Trovare una soluzione dell'equazione diofantea

$$173x + 132y = 1$$

- Descrivere *tutte* le soluzioni dell'equazione diofantea

$$173x + 132y = 1$$

- Quante soluzioni intere hanno le equazioni $x^2 - y^2 = 1002$, $x^2 - y^2 = 2^{40}$, $x^2 - y^2 = 3^{40}$?

3.1 Extra

- Quanti sono gli anagrammi di MAMMALUCCO?
- Risolvere l'equazione diofantea[1] $xy + 3x + 3y = 2017$.
- (Problema di Frobenius, o delle monete ($\star$)) Siano a, b interi positivi fra loro coprimi. Qual è il più grande intero positivo N per cui l'equazione

$$ax + by = N$$

  non ha soluzione intere *positive*?
- Dimostrare che, per ogni $n \geq 1$, i numeri di Fibonacci F_n e F_{n+1} sono primi fra loro.

[1] ovvero si cercano solo le soluzioni intere

4 12.10.2017

4.1 Teoria: la φ di Eulero

Definizione 1. *Per $n \geq 1$ si pone*

$$\varphi(n) = \#\left\{m \in \mathbb{N} \;\middle|\; 1 \leq m \leq n, (m,n) = 1\right\}.$$

Ecco alcune proprietà di questa funzione:

- Se
$$n = p_1^{e_1} \cdots p_k^{e_k},$$
allora
$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_k}\right) = p_1^{e_1-1}(p_1-1)\cdots p_2^{e_2-1}(p_2-1)\cdots p_k^{e_k-1}(p_k-1).$$
- La funzione φ è *moltiplicativa*, ovvero: se m, n sono interi positivi primi fra loro si ha $\varphi(mn) = \varphi(m)\varphi(n)$.
- Si ha che $\varphi(n)$ è dispari se e solo se $n = 1$ o $n = 2$.
- Vale la formula
$$\sum_{d|n} \varphi(d) = n.$$

4.2 Esercizi

- Determinare tutte le soluzioni dell'equazione $\varphi(n) = 2$ e dell'equazione $\varphi(n) = 12$.
- Sia p un primo ed n un intero positivo. Determinare l'esponente di p nella fattorizzazione di $n!$
- ($\star$) Sia $\mathcal{F}_n$ l'n-simo *insieme di Farey*, ovvero l'insieme delle frazioni fra 0 e 1 con denominatore $\leq n$, ordinate per grandezza. Per esempio,
$$\mathcal{F}_5 = \left\{\frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}\right\}.$$
Dimostrare che se $\frac{a}{b} < \frac{c}{d}$ sono due elementi consecutivi di $\mathcal{F}_n$, allora $\dfrac{c}{d} - \dfrac{a}{b} = \dfrac{1}{bd}$.

  Dimostrazione. L'equazione $ay - bx = 1$ ha infinite soluzioni, ma solo una con $0 \leq n - b < y \leq n$. Vogliamo dimostrare che questa soluzione è $(x, y) = (c, d)$. Se non lo fosse, siccome $0 < y \leq n$, la frazione x/y sarebbe in $\mathcal{F}_n$; inoltre,
$$\frac{x}{y} = \frac{a}{b} + \frac{1}{by} > \frac{a}{b}.$$
Siccome $a/b < c/d$ sono adiacenti, questo implica $\frac{x}{y} > \frac{c}{d} > \frac{a}{b}$. Ma allora
$$\frac{1}{by} = \frac{x}{y} - \frac{a}{b} = \left(\frac{x}{y} - \frac{c}{d}\right) + \left(\frac{c}{d} - \frac{a}{b}\right) \geq \frac{1}{dy} + \frac{1}{bd},$$
da cui (moltiplicando per bdy e ricordando $y > n - b$)
$$d \geq b + y > b + (n - b) = n,$$
assurdo perché $\frac{b}{d} \in \mathcal{F}_n$.

4.3 Extra

- Sia n un intero positivo tale che $2^n - 1$ è primo: dimostrare che allora n stesso è un numero primo. Cosa si può dire se $2^n + 1$ è primo?
- Dimostrare che se x, y sono interi positivi si ha $\mathrm{GCD}(x, y) \cdot \mathrm{lcm}(x, y) = xy$.

  Nota. GCD e lcm stanno rispettivamente per *greatest common divisor* and *least common multiple*, ovvero *massimo comun divisore* e *minimo comune multiplo*.
- Quante sono le terne ordinate (a, b, c) di interi positivi tali che $abc = 144$? Come cambia la risposta se si considerano terne di interi eventualmente negativi?
- Sia $f(x)$ un polinomio a coefficienti interi. Supponiamo che esistano quattro interi distinti a, b, c, d tali che $f(a) = f(b) = f(c) = f(d) = 5$. Dimostrare che, se k è intero, $f(k) \neq 8$.
- (Da un compito di Aritmetica dell'anno accademico 2005-2006) Dimostrare che per ogni n intero positivo si ha
$$\varphi(n) \geq \frac{n}{\omega(n) + 1},$$
dove $\omega(n)$ è il numero di fattori primi distinti di n.

5 18.10.2017

5.1 Congruenze, teorema cinese del resto

- Risolvere le congruenze

$$7x \equiv 6 \pmod{21}, \quad 3x \equiv 6 \pmod{21}, \quad 5x \equiv 3 \pmod{48}$$

- Consideriamo i sistemi di congruenze

$$\begin{cases} x \equiv 132 \pmod{125} \\ x \equiv 3 \pmod{100} \end{cases}$$

e

$$\begin{cases} x \equiv 132 \pmod{125} \\ x \equiv 7 \pmod{100} \end{cases}$$

Determinare se esistono soluzioni e, in tal caso, trovarle tutte.

- Siano a, b due interi positivi tra loro relativamente primi. Utilizzando il teorema cinese del resto, dedurre che i sistemi

$$\begin{cases} x \equiv 1 \pmod{a} \\ x \equiv 0 \pmod{b} \end{cases}$$

e

$$\begin{cases} x \equiv 0 \pmod{a} \\ x \equiv 1 \pmod{b} \end{cases}$$

ammettono soluzione, unica modulo ab. Sia x_a una soluzione al primo sistema e x_b una soluzione al secondo. Siano m, n due interi. Dimostrare che le soluzioni al sistema

$$\begin{cases} x \equiv m \pmod{a} \\ x \equiv n \pmod{b} \end{cases}$$

sono $x \equiv mx_a + nx_b \pmod{ab}$. Trovare x_a, x_b nel caso concreto $a = 13, b = 5$.

- (Dallo scritto del 28 giugno 2006) Determinare, in funzione del parametro intero a, le soluzioni del sistema

$$\begin{cases} (6a-1)x \equiv 1 \pmod{21} \\ x \equiv a \pmod{35} \end{cases}$$

- Determinare tutti gli interi x che soddisfano la congruenza $(x+1)(x+2) \equiv 0 \pmod{24}$.

5.2 Extra

- Dimostrare che l'equazione diofantea $x^4 - 4y^3 = 11$ non ammette soluzioni (indicazione: cosa succede se consideriamo quest'equazione modulo 4?)
- Dimostrare che la φ di Eulero è una funzione moltiplicativa sfruttando il Teorema Cinese del Resto.
- Dimostrare il *Teorema di Wilson*: p è un numero primo se e solo se $(p-1)! \equiv -1 \pmod{p}$.
- Dimostrare che, per ogni intero positivo N, esistono N interi consecutivi ognuno dei quali è composto. Dimostrare che esistono N interi consecutivi nessuno dei quali è una potenza perfetta (un intero positivo n si dice *potenza perfetta* se è della forma $n = a^b$ con a, b interi positivi e $b \geq 2$).

6 25.10.2017

6.1 Congruenze lineari, polinomiali, esponenziali, ...

- Determinare le ultime due cifre di 13^{39^5}. Determinare il resto nella divisione di $5^{5^{17}}$ per 13.
- Dimostrare (senza fare conti espliciti) che l'ordine di 9 modulo 11 è 5. Risolvere l'equazione $9^x \equiv 4 \pmod{11}$.
- Trovare tutti gli interi x tali che $x^x \equiv 3 \pmod{5}$.
- Determinare le soluzioni dell'equazione $x^3 + 5 \equiv 0 \pmod{7 \cdot 8 \cdot 11}$.
- Sia p un numero primo tale che $2^{2^{30}} \equiv -1 \pmod{p}$ (esiste?). Determinare l'ordine di 2 modulo p.

6.2 Extra

- (Compito settembre 2015) Determinare le soluzioni intere del sistema

$$\begin{cases} x^3 \equiv 8 \pmod{1000} \\ x \equiv 2 \pmod{3} \\ 0 \leq x < 3001 \end{cases}$$

- (Compitino novembre 2014) Determinare per quali valori del parametro $a \in \mathbb{Z}$ il sistema

$$\begin{cases} x^{27} \equiv x^2 \pmod{16} \\ x^{27} \equiv x^2 \pmod{9} \\ 2^{x-1} \equiv 4 \pmod{11} \end{cases}$$

  è risolubile e determinarne le soluzioni.

- (Compito luglio 2015) Determinare al variare di $a \in \mathbb{Z}$ le soluzioni intere del sistema

$$\begin{cases} 7ax \equiv a \pmod{49} \\ x^a \equiv 1 \pmod{3} \end{cases}$$

7 30.10.2017

7.1 Ancora congruenze; soluzioni di $x^k \equiv a \pmod m$

- Determinare, al variare di $k \in \mathbb{N}$, le soluzioni del sistema

$$\begin{cases} x^k \equiv x \pmod 7 \\ x^3 \not\equiv x \pmod 7 \end{cases}$$

- Per quali valori interi di a il seguente sistema ammette soluzioni?

$$\begin{cases} ax \equiv 4 \pmod{25} \\ x^2 + a \equiv 0 \pmod{15} \end{cases}$$

  Determinarne le soluzioni per $a = -1$.

- Dimostrare che $x^2 \equiv y^2 \pmod p$ implica $x \equiv \pm y \pmod p$. Dedurre che se p è un primo dispari il numero delle classi di resto $a \in \mathbb{Z}/p\mathbb{Z}$ per le quali l'equazione $x^2 \equiv a \pmod p$ ha soluzione è $\frac{p-1}{2} + 1$. Queste classi di resto sono dette *residui quadratici modulo p*.

- Sia x un intero tale che $x^2 \equiv 25 \pmod{3 \cdot 5 \cdot 7 \cdot 11}$. Quante possibilità ci sono per $x \pmod{3 \cdot 5 \cdot 7 \cdot 11}$?

- Sia p un primo tale che $3 \nmid p - 1$. Dimostrare che $x^3 \equiv y^3 \pmod p$ implica $x \equiv y \pmod p$. Consideriamo allora la funzione

$$\begin{array}{rccc} f: & (\mathbb{Z}/p\mathbb{Z})^\times & \to & (\mathbb{Z}/p\mathbb{Z})^\times \\ & x & \mapsto & x^3. \end{array}$$

  Dimostrare che f è iniettiva. Dedurre che è surgettiva. Convincersi che quanto dimostrato implica il seguente fatto: per ogni classe di resto $a \in \mathbb{Z}/p\mathbb{Z}$ l'equazione $x^3 \equiv a \pmod p$ ha soluzione, e questa soluzione è unica modulo p.

- Più generalmente, supponiamo che m sia un intero positivo e che k sia un intero tale che $(k, \varphi(m)) = 1$. Dimostrare che, se a è un intero coprimo con m, allora l'equazione

$$x^k \equiv a \pmod m$$

  ammette soluzione, unica modulo m.

- Esempio: consideriamo l'equazione $x^7 \equiv 2 \pmod{17}$. Dimostrare che questa equazione ammette un'unica soluzione modulo 17 e determinarla.

- Esempio: l'ipotesi $(k, \varphi(m)) = 1$ è necessaria! Determinare le soluzioni dell'equazione $x^5 \equiv 1 \pmod{25}$.

- Siano p un primo dispari e n un intero positivo. Dimostrare che l'ordine moltiplicativo di $1 + p$ modulo p^n è p^{n-1}.

7.2 Extra

- Determinare l'ordine moltiplicativo di 3 modulo 125.

8 01.11.2017

8.1 Una miscellanea di esercizi

- Trovare una *formula chiusa* per le seguenti successioni per ricorrenza:
  1. $a_{n+1} = 5a_n - 6a_{n-1}$, $a_0 = 2$, $a_1 = 5$
  2. $a_{n+1} = 4(a_n - a_{n-1})$, $a_0 = 0$, $a_1 = 2$
  3. $a_{n+1} = 3a_n + 2$, $a_0 = 2$
- Sia a un intero non divisibile per 3 e sia x_n la successione per ricorrenza data da

$$\begin{cases} x_0 = 1 \\ x_1 = a \\ x_{n+1} = 5x_n + 3x_{n-1} \end{cases}$$

  Dimostrare che $(x_{n+1}, x_n) = 1$ per ogni $n \geq 1$.
- Risolvere $x^2 - x + 43 \equiv 0 \pmod{55}$.
- Determinare tutti i numeri naturali $n \leq 120$ tali che $(n, \varphi(n)) = 3$.
- Determinare il numero di coppie ordinate $(x, y) \in \mathbb{Z}/100\mathbb{Z} \times \mathbb{Z}/100\mathbb{Z}$ tali che $xy \equiv 0 \pmod{100}$
- Siano

$$A = \{f : \{1, \dots, 5\} \to \{1, \dots, 100\} \mid f(i) < f(i+1) \ \forall\, i = 1, 2, 3, 4\};$$
$$B = \{f \in A \mid \exists i \text{ con } f(i+1) > f(i) + 1\};$$
$$C = \{f \in A \mid f(i+1) > f(i) + 1 \ \forall\, i = 1, 2, 3, 4\}.$$

  Determinare le cardinalità di A, B, C.

8.2 Extra

- Sia a_n la successione definita da

$$\begin{cases} a_0 = 2 \\ a_1 = 3 \\ a_2 = 5 \\ a_{n+1} = a_n - a_{n-1} + 2a_{n-2} \quad \text{per } n \geq 2 \end{cases}$$

  Dimostrare che $a_n < a_{n+1}$ per ogni $n \geq 0$.
- Sia $x = \{1, 2, \dots, 100\}$.
  1. Determinare il numero di sottoinsiemi di due elementi di X la somma dei cui elementi sia divisibile per 4.
  2. Determinare il numero di sottoinsiemi di cardinalità 3 di X che non contengono due numeri consecutivi.

9 15.11.2017

9.1 Gruppi: primi esercizi

- Sia $f : G \to H$ un omomorfismo di gruppi. Dimostrare che f è iniettivo se e solo se $\ker f = \{\mathrm{id}_G\}$.
- Sia G un gruppo finito e H un sottoinsieme con la proprietà che $h_1, h_2 \in H \Rightarrow h_1 \cdot h_2 \in H$. Dimostrare che H è un sottogruppo.
- Dimostrare che un gruppo (finito) di ordine pari ha un numero dispari di elementi di ordine 2.
- Descrivere (a meno di isomorfismo) tutti i gruppi di ordine 6.
- Siano m, n due interi positivi, $G_1 = \mathbb{Z}/m\mathbb{Z}$ e $G_2 = \mathbb{Z}/n\mathbb{Z}$. Quanti sono gli omomorfismi da G_1 a G_2? Come sono fatti? Quanti sono gli omomorfismi da G_1 a $\mathbb{Z}$? E quanti sono gli omomorfismi da $\mathbb{Z}$ a G_1?

9.2 Extra

- Sia G un gruppo. Dimostrare che l'applicazione

$$\begin{array}{rccc} f: & G & \to & G \\ & x & \mapsto & x^2 \end{array}$$

  è un omomorfismo se e solo se G è abeliano.
- Classificare (a meno di isomorfismo) i gruppi di ordine 10 (simile al caso $|G| = 6$), $2p$ con p primo (praticamente della stessa difficoltà), 8 (non facilissimo. La risposta è che ci sono 5 gruppi di ordine 8 a meno di isomorfismo, di cui tre abeliani e due non abeliani. Uno dei non abeliani è D_4. Ma l'altro?)
- (difficile) Sia G un gruppo finito di ordine non divisibile per 3. Supponiamo che per ogni $a, b \in G$ si abbia $(ab)^3 = a^3b^3$. Dimostrare che G è abeliano.

10 16.11.2017

- Abbiamo dimostrato il *primo teorema di omomorfismo*:

  Teorema. *Sia $f : G \to H$ un omomorfismo di gruppi.*

  1. *Sia K un sottogruppo normale di G contenuto in $\ker f$. Esiste un unico omomorfismo di gruppi $f_K : G/K \to H$ tale che, detta π_K la proiezione canonica $\pi_K : G \to G/K$, si abbia*
  $$f = f_K \circ \pi_K.$$
  Inoltre, l'immagine di f_K coincide con l'immagine di f.
  2. *Nel caso particolare $K = \ker f$, l'omomorfismo f_K è iniettivo, e si ha dunque*
  $$\operatorname{Im} f = \operatorname{Im} f_K \cong \frac{G}{K} = \frac{G}{\ker f},$$
  ovvero: ***l'immagine di un omomorfismo di gruppi è isomorfa al quoziente del gruppo di partenza per il nucleo dell'omomorfismo.***

- Siano G_1, G_2 gruppi, H_1, H_2 sottogruppi di G_1, G_2 rispettivamente. Sia inoltre $f : G_1 \to G_2$ un omomorfismo di gruppi.
  1. $f(H_1)$ è un sottogruppo di G_2?
  2. $f^{-1}(H_2)$ è un sottogruppo di G_1?
  3. Supponiamo che H_1 sia un sottogruppo normale di G_1. E' vero che $f(H_1)$ è un sottogruppo normale di G_2?
  4. Supponiamo che H_2 sia un sottogruppo normale di G_2. E' vero che $f^{-1}(H_2)$ è un sottogruppo normale di G_1?

11 22.11.2017

- Sia n un intero positivo. Per ogni intero positivo d determinare il numero di elementi di ordine d in $\mathbb{Z}/n\mathbb{Z}$.
- (173) Sia G un gruppo, p un numero primo, e H, K due sottogruppi normali di G di indice p, distinti e tali che $H \cap K = \{e\}$.
  1. Dimostrare che G è isomorfo a $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.
  2. Determinare il numero di sottogruppi di G di ordine p.
- (135) Sia $G = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$.
  1. Quanti sono gli elementi di G di ordine 60?
  2. Quanti sono i sottogruppi ciclici di G di ordine 30?
  3. Quanti sono gli omomorfismi iniettivi $f : \mathbb{Z}/12\mathbb{Z} \to G$?
- (143) Sia G un gruppo abeliano e sia H il suo sottoinsieme formato da tutti gli elementi di ordine finito.
  1. Dimostrare che H è un sottogruppo di G, e mostrare con un esempio che H può essere infinito.
  2. Dimostrare che ogni elemento di G/H diverso dall'identità ha ordine infinito.
  3. Dimostrare che il nucleo di ogni omomorfismo $G \to \mathbb{Z}$ contiene H.
  4. Dimostrare che G/H è isomorfo a G se e solo se H è banale.

12 29.11.2017

- Sia G un sottogruppo finitamente generato di $(\mathbb{Q}, +)$. Dimostrare che G è ciclico.
- Siano K, H sottogruppi di un gruppo abeliano G. Poniamo $m = [G : K], n = [G : H]$ e $d = [G : K \cap H]$.
  1. Dimostrare che $d \mid mn$.
  2. Dimostrare che $d = mn$ se e solo se $G = K + H$.
- Sia G un gruppo abeliano finito, denotato additivamente, e siano p un numero primo ed a un numero naturale tali che $p^a || \#G$.
  1. Dimostrare che $H = \{x \in G \mid p^a x = 0\}$ è un sottogruppo di G.
  2. Dimostrare che G/H non ha elementi di ordine p.
  3. Dimostrare che $\#H = p^a$.
- Sia G un gruppo. Il **centro** di G è il sottoinsieme

  $$Z(G) = \{g \in G : \forall h \in G, hg = gh\},$$

  ovvero il sottoinsieme costituito da quegli elementi che commutano con tutti gli elementi di G. Dimostrare che il centro è un sottogruppo. Qual è il centro di $\mathbb{Z}$? Di S_3? Di D_6 (il gruppo diedrale su 6 elementi)?
- Siano G un gruppo e H un suo sottogruppo. Il **centralizzatore** e **normalizzatore** di H sono rispettivamente gli insiemi

  $$Z_G(H) = \{g \in G : gh = hg \quad \forall h \in H\}$$

  e

  $$N_G(H) = \{g \in G : ghg^{-1} \in H \quad \forall h \in H\}.$$

  Dimostrare che $Z_G(H), N_G(H)$ sono sottogruppi di G.
- Dato il polinomio $x^5 + x^4 + x^3 + x^2 + x + 1$, trovarne la fattorizzazione in irriducibili in $\mathbb{C}[x]$, $\mathbb{Z}[x]$, $\mathbb{Z}/13\mathbb{Z}[x]$, $\mathbb{Z}/5\mathbb{Z}[x]$.

12.1 Extra

- (185) Sia G un gruppo abeliano e per ogni $k \in \mathbb{N}$ poniamo $G^k = \{g^k \mid g \in G\}$.
  1. Dimostrare che G^k è un sottogruppo di G per ogni k.
  2. Supponendo che G sia finito di cardinalità n, caratterizzare gli interi k tali che $G^k = G$.
  3. Dare un esempio di un gruppo G per cui $G^k \neq G$ per ogni $k > 1$.
  4. Dare un esempio di un gruppo non banale G per cui $G^k = G$ per ogni $k \geq 1$.

13 06.12.2017

- Determinare tutti i polinomi irriducibili di grado ≤ 3 in $\mathbb{F}_2[x]$. Fattorizzare $x^4 + x^2 + 1$ in $\mathbb{F}_2[x]$.
- Consideriamo il polinomio $f(x) = x^3 + nx + 1$ con n intero. Dimostrare che se $n \geq 3$ o se n è dispari, allora $f(x)$ è irriducibile in $\mathbb{Q}[x]$.
- Qual è la fattorizzazione di $x^4 - 2x^3 + x - 1$ in $\mathbb{Q}[x]$?
- Sia p un numero primo. Dimostrare che il polinomio $1 + x + x^2 + \cdots + x^{p-1}$ è irriducibile in $\mathbb{Q}[x]$.
- Dimostrare che $x^n - 2$ è irriducibile in $\mathbb{Z}[x]$. Qual è la sua fattorizzazione in $\mathbb{Q}[x]$? In $\mathbb{C}[x]$? In $\mathbb{R}[x]$ quando $n = 5$?
- Sia $f(x) = x^3 - 5x^2 + 7x - 3$. Consideriamo l'anello $A = \mathbb{F}_5[x]/(f(x))$. Determinare: la cardinalità di A; il numero di elementi invertibili in A; il numero di divisori di 0 in A; il numero di elementi nilpotenti in A.

13.1 Extra

- Determinare la fattorizzazione di $x^3 - 1$ in $\mathbb{Z}[x]$ e in $\mathbb{Z}/p\mathbb{Z}[x]$ per p primo (la risposta dipende da p).

14 14.12.2017

- Sia p un numero primo e K il campo di spezzamento del polinomio $x^p - a \in \mathbb{Q}[x]$. Determinare il grado $[K : \mathbb{Q}]$. Identificare un campo $L \subseteq K$ tale che $[L : \mathbb{Q}] = p - 1$.
- Sia K un campo di caratteristica diversa da 2 e siano $\alpha, \beta \in K^\times$. Dimostrare che $K(\sqrt{\alpha}) = K(\sqrt{\beta})$ se e solo se esiste $\gamma \in K$ tale che $\alpha = \beta\gamma^2$.
- Sia $f(x) \in \mathbb{Q}[x]$ un polinomio irriducibile di grado 3. Supponiamo che $f(x)$ abbia esattamente una radice reale. Dimostrare che il campo di spezzamento di $f(x)$ su $\mathbb{Q}$ ha grado 6.
- Sia $\alpha \in \mathbb{C}$ una radice del polinomio $x^4 + 2x^2 + 2$. Calcolare il polinomio minimo di α^2 e quello di $\frac{1}{\alpha+2}$ su $\mathbb{Q}$.
- Determinare il campo di spezzamento di $x^4 - 25$ su $\mathbb{Q}$.
- Sia $\alpha = \sqrt{2 + \sqrt{7}} \in \mathbb{C}$.
  1. Determinare il grado di $\mathbb{Q}(\alpha)$ su $\mathbb{Q}$.
  2. Sia $g(x)$ il polinomio minimo di α. Determinare il grado del campo di spezzamento di $g(x)$ su $\mathbb{Q}$.
- Determinare il grado del campo di spezzamento di $x^4 + 3x^2 + 1$ su $\mathbb{Q}$.
- ($\star\star$) Mostrare (con un esempio) che esistono polinomi a coefficienti razionali di grado 3 il cui campo di spezzamento ha grado 3 su $\mathbb{Q}$.