Aritmetica 2019-2020

Esercizi

1 26.09.2019 – Induzione e complementi

- Dimostrare per induzione la formula chiusa per i numeri di Fibonacci,

$$F_n = \frac{\phi^n}{\sqrt{5}} - \frac{(1-\phi)^n}{\sqrt{5}} = \frac{\phi^n - (-\phi)^{-n}}{\sqrt{5}},$$

  dove $\phi = \dfrac{1+\sqrt{5}}{2}$.

- Cercare di capire come "indovinare" la formula chiusa qui sopra.

- 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 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.

- n automobili sono disposte (in modo del tutto arbitrario) in vari punti di una pista circolare lunga $60Km$. La i-esima automobile ha un carico di carburante pari a b_i litri. Si sa che ognuna di queste automobili percorre 20Km con ogni litro di carburante, ed inoltre che $\sum_{i=1}^{n} b_i \geq 3$ (ovvero *in totale* i serbatoi delle n automobili contengono almeno 3 litri di benzina). Quando un'automobile raggiunge un'altra, è possibile trasferire tutto il carburante dal serbatoio dell'una a quello dell'altra. Dimostrare che è possibile scegliere una macchina in modo che questa possa fare un giro completo della pista, ovvero percorrere 60Km tutti nel medesimo verso. Naturalmente il guidatore può fermarsi a rifornire il serbatoio da tutte le macchine che incontra sul suo cammino.

1.1 Problemi non discussi in classe

- 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?

- Dimostrare che per ogni intero $n \geq 14$ esistono interi non-negativi x, y tali che $n = 3x + 8y$.

- Dimostrare per induzione la formula del binomio di Newton,

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

2 02.10.2019

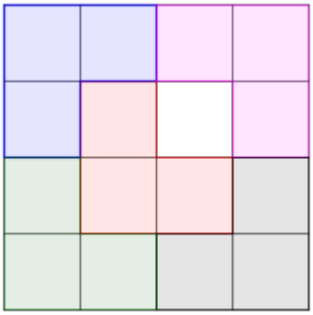
- ($\star$) Dimostrare per induzione che vale la disuguaglianza

$$\frac{1}{2} \cdot \frac{3}{4} \cdots \frac{2n-1}{2n} < \frac{1}{\sqrt{3n}}.$$

Nota. Questo è un esempio della situazione a cui alludevo durante la prima esercitazione: dimostrare questa disuguaglianza per induzione sembra molto difficile (forse impossibile?), ma si riesce facilmente a dimostrare per induzione una disuguaglianza *più forte* (quale?). Un altro esempio di questo fenomeno è dato nell'esercizio successivo.

- Un *tromino* è un pezzo a forma di L costituito da tre caselle, come in questa figura:  . Dimostrare che per ogni $n \geq 2$ esiste almeno un modo di ricoprire una griglia $2^n \times 2^n$ con tromini senza che ci siano sovrapposizioni, senza che alcuno dei pezzi esca dal bordo della griglia, e in modo che resti libera esattamente una casella, e più precisamente una delle 4 caselle centrali. I tromini possono essere ruotati in qualunque modo.

  Un ricoprimento valido per $n = 2$ è mostrato qui sotto, con unica casella scoperta in bianco:



2.1 Calcolo combinatorio

- Sia X un insieme finito. Dimostrare che

$$\#\{A \subseteq X : |A| \text{ è pari}\} = \#\{A \subseteq X : |B| \text{ è dispari}\}$$

A parole: il numero di sottoinsiemi di X di cardinalità pari è uguale al numero di sottoinsiemi di X di cardinalità dispari.

- **Stars & bars**: determinare il numero di soluzioni intere positive dell'equazione $x_1 + \cdots + x_k = n$ (dove k, n sono interi positivi fissati). Determinare il numero di soluzioni intere *non negative* della medesima equazione.

3 03.10.2019 – Conteggi standard

- **Principio di inclusione-esclusione**. Siano $A_1, \ldots, A_n$ sottoinsiemi di un insieme X. Dimostrare che

$$\begin{aligned} |A_1 \cup \cdots \cup A_n| &= \sum_{\substack{I \subseteq \{1,\ldots,n\} \\ I \neq \emptyset}} (-1)^{|I|+1} \left| \bigcap_{i \in I} A_i \right| \\ &= \sum_{j=1}^{n} (-1)^{j+1} \sum_{\substack{I \subseteq \{1,\ldots,n\} \\ |I|=j}} \left| \bigcap_{i \in I} A_i \right| \end{aligned}$$

- **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?

  Più generalmente: quante sono le funzioni surgettive da un insieme X a un insieme Y?

- **Anagrammi.** Quanti sono gli anagrammi distinti della parola CANE? E quelli di CASA? Di MAMMA? Trovare un formula generale.

- **Coefficienti multinomiali.** Abbiamo davanti a noi 30 biglie, numerate da 1 a 30. In quanti modi diversi è possibile colorare le biglie in modo che ce ne siano 12 rosse, 12 blu, 4 verdi e 2 gialle?

  Più generalmente: quanti sono i modi di mettere N oggetti in k scatole, in modo che la prima scatola contenga n_1 oggetti, la seconda n_2, ..., la k-esima n_k?

- Sia $X = \{1, \ldots, n\}$.

  1. Determinare il numero di terne ordinate (A, B, C) di sottoinsiemi di X, a due a due disgiunti, tali che $A \cup B \cup C = X$.
  2. Determinare il numero di terne ordinate (A, B, C) di sottoinsiemi di X tali che $A \cup B \cup C = X$.

- 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 $\#(A \cup B) = 30$?

4 10.10.2019

- Sia n un intero positivo. Determinare, in termini della fattorizzazione di n, il numero di divisori positivi di n.
- Consideriamo l'equazione diofantea $11x + 41y = 2$. Ammette soluzioni? Se sì, quante soluzioni rispettano $|x| \leq 100, |y| \leq 100$?
- Siano a, b interi positivi. Determinare il massimo comun divisore $(3^a - 1, 3^b - 1)$.
- Determinare, al variare di n fra gli interi, i possibili valori che può assumere $(n^3 + n + 3, 2n + 1)$.
- ($\star$) Sia $\mathcal{F}_n$ l'n-esimo *insieme di Farey*, ovvero l'insieme dei numeri razionali nell'intervallo $[0, 1]$ il cui denominatore è al più n. Siano $\frac{a}{b} < \frac{c}{d}$ due elementi "adiacenti" di $\mathcal{F}_n$, ovvero tali che non esista alcun $q \in \mathcal{F}_n$ con $\frac{a}{b} < q < \frac{c}{d}$. Dimostrare che $bc - ad = 1$.
- ($\star$) 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?)

5 14.10.2019

- Dimostrare che esistono infiniti numeri primi.
- Siano a, n interi positivi tali che $a^n - 1$ è primo. Cosa si può dire su a e su n? Similmente, supponiamo che $2^n + 1$ sia primo: cosa si può dire su n? Infine, ($\star$) supponiamo che $4^n + 2^n + 1$ sia primo: dimostrare che n è una potenza di 3.
- Sia $d = 2^3 \cdot 3^4 \cdot 5^5$, e sia D l'insieme dei divisori positivi di d. Sia infine N il prodotto di tutti gli elementi di D. Con quanti zeri termina la scrittura decimale di N?
- Sia $X = \{1, \ldots, 10\}$. Determinare il numero di funzioni $f : X \to X$ tali che $f(a)f(b)$ *non sia* un numero primo per alcuna scelta di $a \in X, b \in X$.
- Determinare quanti sono gli interi positivi minori o uguali a 1000 che non sono divisibili né per 2, né per 3, né per 5.
- Sia n un intero positivo. Determinare la fattorizzazione in primi di $n!$

- Determinare il numero di sottoinsiemi di $X = \{1, \dots, 100\}$ con esattamente 3 elementi la cui somma sia 100.
- 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?

6 Esercizi che non penso di trattare in classe

- 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?)
- 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 $\binom{13}{k}\left(\frac{2}{3}\right)^{13-k}\left(\frac{1}{3}\right)^{k}$.

7 17.10.2019 – Primi passi sulle congruenze

- Studiare le congruenze $3x \equiv 6 \pmod{21}$, $6x \equiv 7 \pmod{21}$, $5x \equiv 3 \pmod{48}$, $x^2 \equiv 0 \pmod{8}$, $x^2 \equiv 1 \pmod{21}$.
- Determinare se esistono soluzioni ai sistemi di congruenze
$$\begin{cases} x \equiv 141 \pmod{343} \\ x \equiv 20 \pmod{70} \end{cases} \quad \text{e} \quad \begin{cases} x \equiv 141 \pmod{343} \\ x \equiv 20 \pmod{71} \end{cases}$$
- (Metodo di interpolazione per risolvere i sistemi di congruenze). Trovare soluzioni modulo $13 \cdot 27$ ai sistemi di congruenze
$$\begin{cases} x \equiv 1 \pmod{13} \\ x \equiv 0 \pmod{27}, \end{cases} \quad \begin{cases} x \equiv 0 \pmod{13} \\ x \equiv 1 \pmod{27}, \end{cases} \quad \begin{cases} x \equiv 7 \pmod{13} \\ x \equiv 11 \pmod{27} \end{cases}$$

- Dimostrare che esistono 2019 interi positivi consecutivi nessuno dei quali è primo. Dimostrare che esistono 2019 interi positivi consecutivi nessuno dei quali è una potenza perfetta (si ricorda che un intero positivo è una *potenza perfetta* se è della forma a^b con a, b interi e $b \geq 2$).

8 24.10.2019

- Consideriamo la successione per ricorrenza data da

$$\begin{cases} a_1 = 3 \\ a_{n+1} = a_n^2 - a_n + 1 \quad \forall n \geq 1 \end{cases}$$

  Dimostrare che per ogni coppia di interi positivi (m, n) con $m \neq n$ si ha $(a_m, a_n) = 1$.

- Determinare il numero di divisori positivi di $3^{40}5^{25}$ che siano congrui ad 1 modulo 7.

- Sia p un numero primo maggiore di 2. Discutere la risolubilità della congruenza $ax^2 + bx + c \equiv 0 \pmod{p}$. Dimostrare in particolare che (a meno che $a = b = c = 0$) una tale equazione non può avere più di due soluzioni modulo p.

- Determinare il numero di soluzioni dell'equazione $x^2 \equiv 1 \pmod{p^k}$, dove p è numero primo (non necessariamente dispari, e $k \geq 1$). Dedurne una formula per il numero di soluzioni dell'equazione $x^2 \equiv 1 \pmod{n}$.

- Trovare tutti gli interi positivi n per cui $3^n \equiv 4 + n \pmod{10}$. Sia p un numero primo: determinare il numero di soluzioni modulo $p(p-1)$ della congruenza $3^n + 4 + n \equiv 0 \pmod{p}$.

- Risolvere le equazioni diofantee $x^2 - y^2 = 2018, x^2 - y^2 = 2020$ e $x^2 - y^2 = 3^{40}$.

9 28.10.2019

- (Inversi moltiplicativi e frazioni) Lavoriamo in $\mathbb{Z}/n\mathbb{Z}$. Siano b, d classi invertibili in $\mathbb{Z}/n\mathbb{Z}$. Verificare che:

  1. per ogni intero $k \geq 0$ si ha $(b^{-1})^k \equiv \left(b^k\right)^{-1} \pmod{n}$; questo ci permette di definire b^{-k} (con k positivo) come $(b^{-1})^k$, o anche come $(b^k)^{-1}$.
  2. Più generalmente, si ha $b^{-1}d^{-1} \equiv (bd)^{-1} \pmod{n}$. Questa uguaglianza può essere pensata come $\frac{1}{b} \times \frac{1}{d} \equiv \frac{1}{bd} \pmod{n}$.
  3. Per ogni $a, c \in \mathbb{Z}/n\mathbb{Z}$ si ha $b^{-1}a + d^{-1}b \equiv (bd)^{-1}(ad + bc) \pmod{n}$. Quest'ultima uguaglianza può essere pensata come $\frac{a}{b} + \frac{c}{d} \equiv \frac{ad+bc}{bd}$.

D'ora in poi scriveremo $\frac{1}{b}$ per b^{-1}: le verifiche precedenti mostrano che b^{-1} si comporta in tutto e per tutto come ci aspetteremmo si comportasse la frazione $\frac{1}{b}$.

- Dimostrare che se p è primo si ha $\frac{1}{b} \equiv b^{p-2} \pmod{p}$. Dedurne che se p è un primo maggiore di 3 si ha $p \mid 2^{p-2} + 3^{p-2} + 6^{p-2} - 1$.

- Verificare che la formula risolutiva per le equazioni di secondo grado funziona anche per risolvere congruenze quadratiche modulo p, dove p è un primo diverso da 2.

- Dare una nuova interpretazione del metodo di interpolazione per risolvere i sistemi di congruenze secondo le seguenti linee. Siano m, n interi coprimi. Il teorema cinese del resto fornisce un'applicazione bigettiva (fatta come?)

$$\varphi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

  Risolvere il sistema

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

  equivale a determinare $\varphi^{-1}((a, b))$. Osservare che se $\varphi(x_1) = (1, 0)$ e $\varphi(x_2) = (0, 1)$, allora $\varphi(ax_1 + bx_2) = (a, b)$. Notare infine che risolvere $\varphi(x_1) = (1, 0), \varphi(x_2) = (0, 1)$ equivale esattamente a risolvere i sistemi

$$\begin{cases} x \equiv 1 \pmod{m} \\ x \equiv 0 \pmod{n} \end{cases} \qquad \begin{cases} x \equiv 0 \pmod{m} \\ x \equiv 1 \pmod{n} \end{cases}$$

- Determinare in funzione di $a \in \mathbb{Z}$ le soluzioni del sistema

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

- ($\star$) Sia $p \equiv 3 \pmod{4}$. Dimostrare che la congruenza $x^2 + 1 \equiv 0 \pmod{p}$ non ha soluzioni.

  Indicazione. Supponiamo che x sia una soluzione. Cosa si può dire dell'ordine moltiplicativo modulo p di x?

- Risolvere il seguente sistema:

$$\begin{cases} 5^x \equiv 9 \pmod{16} \\ x^2 + 2x + 8 \equiv 0 \pmod{176} \end{cases}$$

- ($\star$) Sia $p = 32003$ (che è primo). Determinare le soluzioni della congruenza $x^3 \equiv 1754 \pmod{p}$.

  Indicazione. Si consiglia di iniziare determinando il *numero* di tali soluzioni).

10 31.10.2019

- (Congruenze modulo potenze di p, sollevamento delle soluzioni)
  1. Risolvere la congruenza $x^6 + x^2 + 12 \equiv 0 \pmod{16}$
  2. Risolvere la congruenza $x^2 \equiv 73 \pmod{81}$
  3. Sia p un primo dispari. Dimostrare che l'ordine moltiplicativo modulo p^n di $1 + p$ è p^{n-1}.
- Determinare le ultime due cifre del numero $13^{(39^5)}$.
- Contare il numero di soluzioni modulo 77 della congruenza $x^{27} \equiv x^{15} \pmod{77}$.
- Al variare di $a \in \mathbb{Z}$, determinare il numero di soluzioni del sistema

$$\begin{cases} ax \equiv 2 \pmod{12} \\ 9x \equiv a^2 + 2a - 3 \pmod{81} \end{cases}$$

- Determinare, in funzione dell'intero positivo a, le soluzioni del sistema di congruenze

$$\begin{cases} 3^x \equiv 7^a \pmod{11} \\ (a+3)x \equiv 2 \pmod{5} \end{cases}$$

- Risolvere la congruenza $x^{660} \equiv 1 \pmod{847}$
- Determinare gli interi positivi m per cui $\varphi(m) = 12$.

11 06.11.2019

11.1 Congruenze

- Dimostrare che se p è un primo congruo a 2 modulo 3, allora $x \mapsto x^3$ è iniettiva modulo p.
- Determinare le soluzioni modulo $7 \cdot 8 \cdot 11$ di $x^3 + 13 \equiv 0 \pmod{7 \cdot 8 \cdot 11}$.

11.2 Funzioni aritmetiche

- Determinare gli interi positivi n per cui $\varphi(n) = \frac{2}{5}n$.
- Per ogni intero positivo n, sia $\omega(n)$ il numero dei fattori primi distinti di n. Dimostrare che $\varphi(n) \geq \frac{n}{1+\omega(n)}$.

- Sia $d(n)$ la somma dei divisori positivi di n. Dimostrare che se a, b sono interi positivi tali che $(a, b) = 1$, allora $d(ab) = d(a)d(b)$. Generalizzazione: fissato $k \in \mathbb{N}$, sia
$$d_k(n) = \sum_{d|n, d>0} d^k.$$
Allora $d_k(ab) = d_k(a)d_k(b)$ se $(a, b) = 1$.

- Dimostrare che per ogni intero positivo n si ha $\varphi(n) + d(n) \leq n + 1$.

12 Esercizi che non penso di trattare in classe

- Al variare dell'intero a, contare le soluzioni modulo 77 della congruenza $x^{100} \equiv a \pmod{77}$.

- Dimostrare il **teorema di Wilson**: un intero positivo p è primo se e solo se $(p-1)! \equiv -1 \pmod{p}$.

- Determinare per quali valori di a il sistema
$$\begin{cases} x^{27} \equiv x^2 \pmod{144} \\ 10x \equiv a \pmod{25} \\ 2^{x-1} \equiv 4 \pmod{11} \end{cases}$$
ha soluzione, e in tali casi descrivere l'insieme delle soluzioni.

- Al variare di $a \in \mathbb{Z}$, risolvere il sistema
$$\begin{cases} 5^{x^2-1} \equiv 2^a \pmod{13} \\ x^3 \equiv 0 \pmod{64} \end{cases}$$

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

13 13.11.2019 – Gruppi I

- Siano $(G_1, \star)$ e $(G_2, *)$ due gruppi. Allora la funzione

$$\begin{array}{rccc} \cdot : & (G_1 \times G_2) \times (G_1 \times G_2) & \to & G_1 \times G_2 \\ & (g_1, g_2), (g_1', g_2') & \mapsto & (g_1 \star g_1', g_2 * g_2') \end{array}$$

  munisce l'insieme $G_1 \times G_2$ di una struttura di gruppo. Il gruppo ottenuto in questo modo si denota semplicemente $G_1 \times G_2$, ed è detto il **prodotto diretto** di G_1 e G_2.

- Identifichiamo il gruppo ciclico di ordine n al sottogruppo μ_n delle radici n-esime dell'unità in $\mathbb{C}^\times$. Dimostrare che $\mu_m \subseteq \mu_n$ se e solo se $m \mid n$. Dimostrare inoltre che $\bigcup_m \mu_m \subseteq \mathbb{C}^\times$ è un sottogruppo infinito di $(\mathbb{C}^\times, \cdot)$ ognuno dei cui elementi ha ordine finito.

- Verificare che il gruppo $((\mathbb{Z}/17\mathbb{Z})^\times, \cdot)$ è ciclico, e quindi isomorfo al gruppo $(\mathbb{Z}/16\mathbb{Z}, +)$.

- Sia G un gruppo e siano H, K due sottogruppi di G. Poniamo

$$HK := \{h \cdot k \mid h \in H, k \in K\}$$

  e similmente

$$KH := \{k \cdot h \mid k \in K, h \in H\}.$$

  Dimostrare che $HK = KH$ (come sottoinsiemi di G) se e soltanto se HK è un sottogruppo di G.

- Sia $(G, \cdot)$ un gruppo **finito** e H un sottoinsieme con la proprietà che $h_1, h_2 \in H \Rightarrow h_1 \cdot h_2 \in H$ (diciamo anche che H è **chiuso rispetto all'operazione**). Dimostrare che H è un sottogruppo di G.

  Trovare poi un controesempio a questa affermazione nel caso G sia infinito, ovvero, descrivere un gruppo infinito G e un sottoinsieme H chiuso rispetto all'operazione che **non** sia un sottogruppo di G.

- 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.

- Caso particolare del problema precedente: sia G un gruppo con la proprietà che $g^2 = \mathrm{id}_G$ per ogni $g \in G$. Dimostrare che G è abeliano.

14 14.11.2019 – Gruppi II

- Dimostrare che il centro di $G_1 \times G_2$ coincide (insiemisticamente) con il prodotto dei centri di G_1 e di G_2.
- Dimostrare che un gruppo (finito) di ordine pari ha un numero dispari di elementi di ordine 2. In particolare, questo dimostra che un gruppo di ordine pari ha (almeno) un elemento di ordine 2. Si tratta di un caso particolare del **teorema di Cauchy**: se G è un gruppo finito e $p \mid \#G$, allora G contiene un elemento di ordine p.
- Quanti sono gli elementi di ordine 8 nel gruppo $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$? E gli elementi di ordine 12? E quelli di ordine 16?
- Descrivere (a meno di isomorfismo) tutti i gruppi di ordine minore o uguale a 6.

15 Esercizi ancora da discutere

Un numero fra parentesi prima del testo di un esercizio indica un problema tratto dal libro di Chirivì, Del Corso, Dvornicich.

- 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?

- Sia G un gruppo. Poniamo

$$\mathrm{Aut}(G) := \{f : G \to G \mid f \text{ è un isomorfismo di gruppi}\}.$$

  Dimostrare che $\mathrm{Aut}(G)$, con l'operazione di composizione, è un gruppo. Determinare $\mathrm{Aut}(G)$ nei casi $G = \mathbb{Z}, G = \mathbb{Z}/n\mathbb{Z}$, e $(\star)$ $G = S_3$.

- Un gruppo abeliano è detto un *p-gruppo abeliano elementare* se è della forma $\mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z}$. Studiare i sottogruppi di un p-gruppo abeliano elementare.

- Sia G un gruppo e H un sottogruppo. Dimostrare che c'è una bigezione fra le classi laterali destre e sinistre di H in G.

- Sia G un gruppo e H un sottogruppo di indice 2. Dimostrare che H è normale in G.

- Definire il sottogruppo generato da un insieme.

- Sia G un sottogruppo finitamente generato di $(\mathbb{Q}, +)$. Dimostrare che G è ciclico.

- Sia G un gruppo finito. Dimostrare che il numero $s_d(G)$ dei sottogruppi di ordine d di G e il numero $e_d(G)$ degli elementi di ordine d di G sono legati dalla formula

$$s_d(G) = \frac{e_d(G)}{\varphi(d)}.$$

- Quanti sono gli omomorfismi da $\mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/32\mathbb{Z}$ a $\mathbb{Z}/4\mathbb{Z}$? Quanti sono i sottogruppi ciclici di $\mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/32\mathbb{Z}$ di ordine 8?

- Sia G un gruppo finito e α un automorfismo di G con la proprietà che $\alpha(x) = x$ se e soltanto se x è l'elemento neutro e di G.

  1. Mostrare che per ogni $g \in G$ esiste $x \in G$ tale che $g = x^{-1}\alpha(x)$.
  2. Dimostrare che se inoltre vale anche $\alpha(\alpha(x)) = x$ per ogni $x \in G$, allora si ha $\alpha(g) = g^{-1}$ per ogni g in G.

- (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 $f : \mathbb{Z}/12\mathbb{Z} \to G$?

Gli esercizi seguenti usano (in maniera più o meno sostanziale) la teoria che sarà discussa in classe nella settimana del 18 novembre. Non preoccupatevi se senza questi nuovi strumenti non riuscite a risolvere questi problemi! Anticipo alcuni fatti che possono essere utili:

1. (teorema di Lagrange) Se G è un gruppo finito di ordine n e g è un elemento di G, allora l'ordine di g divide n. Più generalmente, l'ordine di un sottogruppo divide l'ordine del gruppo.
2. (teorema di Cauchy per i gruppi abeliani) Sia G un gruppo abeliano finito e sia p un numero primo. Se $p \mid \#G$, allora G contiene un elemento di ordine p.

- (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.
- (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.
- Sia G un gruppo abeliano finito, denotato additivamente, e siano p un numero primo ed a un numero naturale tali che $p^a || \#G$ (cioè $p^a \mid \#G$, ma $p^{a+1} \nmid \#G$).
    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 $\#H = p^a$.
- (176) Sia G un gruppo e sia $\Delta = \{(x, x) | x \in G\}$.
    1. Dimostrare che Δ è un sottogruppo di $G \times G$.
    2. Dimostrare che Δ è normale in $G \times G$ se e solo se G è abeliano.
    3. Dimostrare che, se G è abeliano, $G \times G/\Delta$ è isomorfo a G.

- Sia G un gruppo finito e siano H, K due sottogruppi di G. Dimostrare che
$$|H \cdot K| = \frac{|H| \cdot |K|}{|H \cap K|}$$

- (183)
  1. Contare gli omomorfismi e gli omomorfismi iniettivi da $\mathbb{Z}/12\mathbb{Z}$ nel gruppo $\mathbb{Z}/4\mathbb{Z} \times S_3$.
  2. Descrivere tutti gli omomorfismi $\varphi : \mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \times S_3$ per cui $\varphi(\overline{10})$ ha ordine 3.

- 1. Siano G un gruppo e H, K due sottogruppi normali di G. Supponiamo che $H \cap K = \{e\}$: dimostrare che per ogni $h \in H$ e ogni $k \in K$ si ha $hkh^{-1}k^{-1} = e$.
  2. Sia p un numero primo. Determinare tutti i gruppi finiti G con la seguente proprietà: ogni elemento di G (tranne l'identità) ha ordine p, e per ogni $g \in G \setminus \{e\}$ si ha che $\langle g \rangle$ è normale in G, con $G/\langle g \rangle \cong \mathbb{Z}/p\mathbb{Z}$.

- Sia G un gruppo qualsiasi. Dimostrare che il centro $Z(G)$ di G è un sottogruppo normale di G. Supponiamo che il quoziente $G/Z(G)$ sia ciclico: dimostrare che allora G è abeliano (e quindi in tal caso $G/Z(G)$ è il gruppo banale con un elemento). Conseguenza: non esistono gruppi G per cui $|G/Z(G)|$ sia un numero primo.

- ($\star$) Sia G un gruppo finito **non abeliano** di ordine n. Dimostrare che
$$\#\{(x, y) \in G \times G : xy = yx\} \leq \frac{5}{8}n^2$$
e trovare un esempio in cui valga l'uguaglianza.

  Indicazione. Dimostrare che $|Z(G)| \leq \frac{1}{4}|G|$. Dimostrare inoltre che un elemento $g \in G \setminus Z(G)$ commuta con al più $\frac{1}{2}|G|$ elementi.

- (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.

- 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?)

  Per semplificarvi il lavoro, per questo esercizio potete usare il teorema di Cauchy per gruppi anche non commutativi (ma noi per ora lo dimostreremo solo nel caso abeliano).