Diario delle lezioni di Matematica Discreta 2018

AVVISO

Lunedì 26 febbraio 2018: Lezione annullata per neve

Mercoledì 28 febbraio 2018

Lezione 1: Una breve introduzione ai problemi e ai metodi della matematica discreta. Se si frequentano le lezioni assiduamente è sufficiente studiare sui miei *Appunti di Matematica Discreta (Esculapio ed. 2016).* In caso contrario, potrebbe essere necessario approfondire su alcuni dei seguenti testi consigliati:

a. Baldoni, Ciliberto, Piacentini Cattaneo: *Aritmetica, Crittografia e Codici,* Springer 2006
b. Biggs, *Discrete Mathematics*, Oxford, 2002
c. Brualdi, *Introductory Combinatorics*, Prentice Hall, 1999.
d. Cerasoli, Eugeni, Protasi, *Elementi di Matematica Discreta*, Zanichelli 1988
e. Knuth, *The art of Computer Programming,* Vol. I Addison Wesley, 1997
f. Graham, Knuth, Patashnik, *Concrete Mathematics,* Addison Wesley 1988
g. Schroeder, *Number Theory in Science and Communication*, Springer 2009

La lettura del testo di Schroeder è particolarmente consigliata per le motivazioni che fornisce allo studio della teoria dei numeri e della matematica discreta.

Numeri naturali. Principio di induzione e principio del buon ordinamento. Numeri perfetti. Numeri di Mersenne. (1.1-1.3 Appunti)

Paragrafi 1.1, 1.2 degli Appunti.

Esercizio. Trovare e dimostrare una formula per la somma delle quarte potenze di interi consecutivi.
Esercizio. Definire la seguente funzione sugli interi: se x è un intero dispari si prenda f(x)= (3x+1)/2; se invece x è pari si prenda x/2. Verificare che se x è un qualunque intero minore di 100 allora iterando questa procedura a partire da x e calcolando f(x), f(f(x)), f(f(f(x))), per un numero sufficiente di volte si ottiene sempre 1.

Lunedì 5 marzo 2018: Lezione annullata per elezioni politiche

Mercoledì 7 marzo 2018

Lezione 2:

Euclide (300 AC): Tutti i numeri della forma $2^{p-1}(2^p-1)$ sono perfetti purché 2^p-1 sia un numero primo (primo di Mersenne). Al momento si conoscono solo 49 numeri primi di Mersenne. L'ultimo, scoperto nel 2016, ha oltre 22 milioni di cifre. AGGIORNAMENTO!: il 3 gennaio 2018 è stato annunciato il 50esimo numero primo di Mersenne: ha oltre 23 milioni di cifre (vedere https://www.mersenne.org/)

Eulero (1747): Tutti i numeri perfetti pari devono essere necessariamente della forma $2^{p-1}(2^p-1)$.

Massimo comun divisore e identità di Bézout. Teorema fondamentale dell'aritmetica. Esistono infiniti numeri primi: dimostrazione di Euclide.

La dimostrazione di Euclide può essere adattata per dimostrare che esistono infiniti primi della forma 4n+3. Perché lo stesso ragionamento non funziona per dimostrare che esistono infiniti primi della forma 4n+1? (V. Appunti p.6)

Dimostrazione che la serie dei reciproci dei numeri primi diverge, da cui, come conseguenza, segue che i numeri primi sono infiniti.

Definizione di frazione continua e qualche calcolo semplice per scrivere frazioni come frazioni continue. Frazioni continue infinite. Il caso della frazione continua [1;1,1,1,1,1,…]. (Appunti 1.4,1.5)

Esercizi da provare:

1. Se ho due bottiglie di capacità di 2 e 3 litri e voglio riempire un secchio con esattamente n litri di acqua usando le due bottiglie, mi domando se si può fare per qualunque n? oppure solo per alcuni n?
2. Se le capacità sono 2 e 4?
3. Se ho capacità h e k (interi), quali n posso ottenere?
4. Esplorare se sia vero o meno che un numero naturale n è primo se e solo se n divide 2^n-2. Per esempio, abbiamo $2^7-2=126$ e $126=18x7$, mentre $2^6-2=62$ che non è un multiplo di 6.
5. Verificare che $2^{57}-2$ non è divisibile per 57
6. Verificare che $2^{64}-2$ non è divisibile per 64
7. Verificare che $2^{341}-2$ **è divisibile** per 341, pur non essendo 341 primo (341=11x31)
8. Esprimere $\sqrt{5}$ come frazione continua.
9. Calcolare MCD(6381,5163) usando le divisioni successive di Euclide.
10. Scrivere il MCD trovato nell'esercizio precedente mediante l'identità di Bézout.
11. Scrivere il numero razionale 6381/5163 come frazione continua usando una calcolatrice.
12. Scrivere 5163/6381 come frazione continua usando una calcolatrice.
13. Calcolare il valore della frazione continua [2;1,3,1,5,4].

Lunedì 12 marzo 2018

Lezione 3 e 4:

Svolgimento dell'esercizio di determinare e dimostrare una formula per la somma di quarte potenze. Definizione di congruenza e sue proprietà. Aritmetica modulare sugli insieme quoziente $\mathbf{Z}_n$. Strutture di anello e di campo in $\mathbf{Z}_n$. Elementi invertibili di $\mathbf{Z}_n$. L'anello $\mathbf{Z}_n$ è un campo se e solo se n è un numero primo.

Calcolo dell'elemento inverso mediante l'algoritmo delle divisioni successive e dell'identità di Bézout. Applicazione delle congruenze ai criteri di divisibilità.

Esercizi.

1. Costruire le tabelle additive e moltiplicative per l'anello $\mathbf{Z}_6$ e per il campo $\mathbf{Z}_7$.
2. Calcolare l'inverso, se esiste, di 7 modulo 228 (Risposta: -65 oppure 163)
3. Calcolare l'espressione di prima media: $51 \div \{12 + 3 \cdot [2 \cdot 18 - 9 \cdot (24 \div 6 - 2) \div 6] - 60\} + 7$ considerando però i numeri come elementi una volta di $\mathbf{Z}_7$ e un'altra di $\mathbf{Z}_6$.
4. Dimostrare che se un numero intero N ha una espressione in base 10 in modo che $N=10b+a_0$, dove a_0 è la cifra delle unità, allora N è congruo a a_0+3b modulo 7.
5. Guardare il video https://www.ted.com/talks/eduardo_saenz_de_cabezon_math_is_forever#t-569375
6. Per quanto riguarda il problema della somma di potenze di interi vedere https://www.maa.org/press/periodicals/convergence/sums-of-powers-of-positive-integers

Mercoledì 14 marzo 2018

Lezione 5

Piccolo Teorema di Fermat e sua dimostrazione. Se un numero p è primo allora $a^p \equiv a \pmod p$, quindi se a^n non è congruo ad a allora n non è primo. Tuttavia alcuni numeri composti passano questo test di primalità di Fermat, come ad esempio 341. Risulta infatti che 2^{341} è congruo a 2 modulo 341 pur non essendo primo (341=11 x 31). Tuttavia 3^{341} non è congruo a 3 modulo 341 e quindi si vede che 341 non è primo. Ci sono alcuni numeri tuttavia, come 561, che passano il test di Fermat qualunque intero prendiamo come base pur non essendo primi (541=3x11x17). Un numero del genere si dice numero di Carmichael o pseudo primo. Nel 1994 si è dimostrato che esistono infiniti numeri di Carmichael.

(Appunti 1.6)

Esercizi.

1. Calcolare la classe di congruenza di 2^{100} modulo 101
2. Calcolare la classe di congruenza di 2^{703} modulo 101
3. Calcolare le ultime due cifre di 873623^{47635}

Lunedì 19 marzo 2018

Lezione 6 e 7:

Svolgimento di alcuni esercizi della lezione precedente. Come calcolare la classe di congruenza modulo 7. Risoluzione di congruenze lineari. Alcune applicazioni delle congruenze. Sistemi di congruenze. Teorema cinese dei resti (CRT). Applicazioni del Teorema.

(Appunti 1.7)

Esercizi.

Alcune applicazioni delle congruenze e del Teorema cinese dei resti si trovano in

https://www.dropbox.com/sh/nyo718jzbyopzbw/AACm-ZbWQ6mWfZOkX1sevOz3a?dl=0

(questo link verrà rimosso entro qualche giorno)

Mercoledì 21 marzo 2018

Lezione 8

Metodo di risoluzione per sostituzione. Caso di moduli non coprimi. Definizione della funzione ϕ di Eulero e alcune sue proprietà.

(Appunti 1.8)

Esercizi.

1. Calcolare ϕ (2018).
2. Detto A_n, l'insieme dei numeri interi positivi minori di n e coprimi con n, stabilire una corrispondenza biunivoca "naturale" tra A_{21} e $A_7 x A_3$.

Lunedì 26 marzo 2018 (Aula 9)

Lezione 9 e 10:

Formula per il calcolo della funzione ϕ di Eulero. Teorema di Eulero che generalizza il Piccolo Teorema di Fermat.

Introduzione alla nozione di gruppo. Definizione e esempi. Gruppi numerici (**Z**, **Q**, **R**, **C**), gruppi di matrici, gruppi di permutazioni, gruppi diedrali. Ordine di un gruppo e ordine di un elemento. Gruppi ciclici. Enunciato del teorema di Lagrange e dimostrazione del teorema di Eulero.

(Appunti 2.1, 2.2)

Esercizi.

1. Determinare se l'operazione di sottrazione in **Z** è associativa.
2. Determinare se l'operazione su **R** definita da $a \times b = a+b+ab$ è associativa.
3. Sia G l'insieme dei numeri reali non nulli della forma $a+b\sqrt{2}$, dove a e b sono razionali. Dimostrare che G è un gruppo rispetto alla moltiplicazione.

4. Dimostrare che se g è un elemento di un gruppo allora l'insieme degli elementi del tipo g^n , al variare di n in **Z**, costituiscono un sottogruppo di G.
5. Altri esercizi.

Mercoledì 28 marzo 2018 (Aula 12)

Lezione 11:

Dimostrazione del teorema di Lagrange. Corollario: un gruppo di ordine p, p primo, è ciclico. Definizione di omomorfismo e isomorfismo. Isomorfismo tra $\mathbf{C}_n$, il gruppo delle radici n-esime dell'unità in **C**, e $\mathbf{Z}_n$. Classificazione dei gruppi ciclici. Definizione di anello e di campo. Esempi. Campi finiti $\mathbf{Z}_p$. Un esempio di campo con 9 elementi ottenuto prendendo un insieme di matrici di ordine 2 su $\mathbf{Z}_3$ (v. esercizio nel paragrafo 2.5 degli Appunti).

(Appunti 2.3, 2.4, 2.5)

Esercizio. Scrivere un esplicito isomorfismo tra $\mathbf{C}_6$ e $\mathbf{Z}_6$

Lunedì 2 aprile Vacanza: Buona Pasqua e Pasquetta.

Mercoledì 4 aprile

Lezione 12

Campi Finiti: due esempi diversi di campi finiti di ordine 9. Isomorfismo tra di essi. Teorema di classificazione dei campi finiti. Caratteristica di un campo. Costruzione di un campo finito con p^n elementi. Esempi: Campo con 9 elementi, con 8 elementi, con 25 elementi. Polinomi irriducibili.

Esercizio: Costruire un campo con 25 elementi ed uno con 16 elementi.

(Appunti 2.5, 2.6)

lunedì 9 aprile

Lezione 13 e 14

Esposizione/esercitazione sul Calendario Perpetuo.

Elementi primitivi di $\mathbf{F}_9$. Studio dell'irriducibilità di un polinomio di 4 grado. Costruzione di un campo con 16 elementi.

Primi elementi di crittografia. Definizione di cifrario come cinquina di oggetti. Alcuni cifrari classici. Cifrario di Cesare e sue generalizzazioni. Cifrario di Hill. Cifrario di permutazione. Cifrari monoalfabetici e polialfabetici. Cifrario di Vigénère.

Esercizi.

1. Usare il cifrario di Cesare per criptare il messaggio VENI VIDI VICI.
2. Usare il cifrario di Hill per criptare il messaggio ATTACCATE ALL'ALBA (ignorando l'apostrofo) mediante la matrice A=1,2//4,3 e il vettore b=(5,7).
3. Usare il cifrario di Vigénère per criptare il messaggio NELMEZZODELCAMMINDINOSTRAVITA con la chiave DANTE.
4. Decriptare la stringa seguente sapendo che è stata criptata usando lo stesso metodo dell'esercizio precedente.

```
HQHBRGIHLGLMZHEUIIXHHRYXWWEYEI
```

mercoledì 11 aprile

Lezione 15

Criptoanalisi del cifrario di Vigénère: test di Kasiski e Indice di coincidenza di Friedman. Diffie e Hellman: protocollo di scambio di chiavi.

Esercizi.

1. Analizzare la seguente stringa:
   ```
   DZTLLLZLLEEQAWEPTCEAANSORPZXDTVFTEECOCWBUYWBSDEKTLTXSDMBPZMPIOMSIOISATRAUPZFOEXLLP
   ECORKFAOY
   KIAWFLZRNUPPIALHBSEVXSLPFVLZBRDSFLXSKTPIJEYESALPIANYOAWEITCEPCPRAEGEKEWPXVLPIEQMKO
   LYKTZVOEY
   XBEOENUPWQAAEOTPMIMFVLNZRXRCMSAGEZHPEILLRZHPHBLAEPSPKDIPVL
   ```
   a. applicare a questa stringa il Test di Kasiski. Quali risultati anche parziali ottenete? (dopo qualche tentativo a mano necessario per capire il modo di procedere, vi suggerisco di utilizzare http://cs.colgate.edu/~chris/FSemWeb/tools/kasiski.html . Quale sembra essere la lunghezza più probabile della parola chiave?
   b. Quanto vale l'indice di coincidenza in questo caso? (http://cs.colgate.edu/~chris/FSemWeb/tools/coincidence.html)
   c. Quanto è lunga la parola chiave? (Nella pagina http://cs.colgate.edu/~chris/FSemWeb/tools/coincidence.html potete testare gli indici di coincidenza per varie prove di lunghezza, dovreste ottenere per lunghezza 2 i due indici 0.06 e 0.05, per lunghezza 3, 0.055, 0.041, 0.05, per lunghezza 4, 0.078, 0.081, 0.097, 0.062, per lunghezza 5 0.04, 0.039, 0.043, 0.044, 0.05,) Qual è la lunghezza più probabile?
   d. Qual è la parola chiave? (una volta determinata la lunghezza al punto precedente, usare http://cs.colgate.edu/~chris/FSemWeb/tools/vigenere-cracker.html e fare qualche prova)
   e. Qual è il messaggio in chiaro?

Avviso: *ai fini dell'assicurazione della qualità dei corsi di studio, come prescritto dalle indicazioni contenute nel sistema di Autovalutazione, Valutazione e Accreditamento (AVA), gli studenti, devono compilare il "Questionario on line delle opinioni studenti ", quando il corso ha raggiunto i 2/3 del suo sviluppo.*
A tal fine si chiede al Centro InfoSapienza di attivare le procedure telematiche per la Rilevazione Opinioni Studenti sugli insegnamenti del ***secondo semestre*** *per l'a.a.* ***2017-2018****. La rilevazione riguarda tutti gli insegnamenti che si concluderanno con un esame o una prova di idoneità. L'accesso ai questionari degli insegnamenti del secondo semestre resterà aperto fino al* ***28 febbraio 2019****.*
Si raccomanda vivamente affinché gli studenti frequentanti siano ***efficacemente sollecitati*** *a pronunciarsi sugli insegnamenti seguiti, in primo luogo dai docenti nel corso delle lezioni, una volta completata la metà o i*

due terzi delle lezioni e comunque prima della loro fine.
…

Al fine di una maggiore efficacia comunicativa, si raccomanda a Facoltà e/o Dipartimenti di:
*- segnalare anche **nei siti web** l'avvio della Rilevazione Opinioni Studenti 2017-2018 per gli insegnamenti del secondo semestre;*
*- sollecitare i docenti a fornire agli studenti indicazioni per compilare i questionari online e a informarli **sull'importanza dell'iniziativa** e sulle **garanzie di anonimato**.*

lunedì 16 aprile

Lezione 16 e 17

Sistemi a chiave pubblica. Sistema RSA: chiave pubblica e chiave privata. Autenticazione delle firme.

Cenni di teoria dei codici. Ridondanza. Codici a blocchi. Codice di ripetizione. Distanza di Hamming. Codici di tipo (n,M,d). La distanza minima d è legata al numero di errori che il codice può rilevare (al massimo d-1) o correggere (al massimo (d-1)/2). Problema principale della teoria dei codici e definizione di $A_q(n,d)$. Calcolo di $A_q(n,1)$, $A_q(n,n)$, $A_2(5,3)$. Concetto di equivalenza tra codici.

(Appunti 3.2, 3.3, 3.4, 4.1, 4.2)

mercoledì 18 aprile

Lezione 18

Svolgimento degli esercizi assegnati.

lunedì 23 aprile

lezione 19 e 20

Compito di esonero

lunedì 30 aprile

lezione 21 e 22

Codici binari. Un codice binario di tipo (n,M,d) esiste se e solo se ne esiste uno di tipo (n+1,M,d+1). Sfere. Disuguaglianza di Hamming. Codici perfetti.

Costruzione di un codice perfetto a partire dal piano di Fano: codice di Hamming di tipo [7,4]. Codici lineari. Matrice generatrice di un codice lineare. Peso di una parola.

(Appunti 4.3, 4.4, 4.5)

mercoledì 2 maggio

lezione 23

Codifica del codice di Hamming [7,4] mediante la matrice generatrice. Codici lineari equivalenti. Operazioni sulle righe e colonne di una matrice generatrice. Forma standard della matrice generatrice. Matrice di controllo di parità.

(Appunti 4.6)

lunedì 7 maggio

lezione 24 e 25

Come ottenere la matrice di controllo di parità a partire dalla matrice generatrice. Decodifica usando lo schieramento standard e usando la sindrome.

Come calcolare la distanza minima di un codice a partire dalle colonne della matrice H. Famiglia di codici di Hamming Ham(r,q).

Successioni definite per ricorrenza. Successione di Fibonacci e formula di Binet.

(Appunti 4.7, 4.8, 5.1, 5.2)

Esercizi: Nella cartella https://www.dropbox.com/sh/nyo718jzbyopzbw/AACm-ZbWQ6mWfZOkX1sevOz3a?dl=0

trovate degli appunti aggiornati sulla teoria dei codici, inclusi anche diversi esercizi svolti.

mercoledì 9 maggio

lezione 26

Tre dimostrazioni differenti della formula di Binet: metodo dello spazio vettoriale, metodo della matrice, metodo della funzione generatrice.

Generalizzazione alla risoluzione di ricorrenze lineari omogenee.

(Appunti 5.1, 5.2)

lunedì 14 maggio

lezione 27 e 28

Esercizi di risoluzione di ricorrenze. Caso delle radici multiple. Anello delle serie formali. Prodotto di convoluzione e composizione di serie.

Altri numeri definiti per ricorrenza. Successione dei numeri Catalan e loro funzione generatrice. Formula chiusa per i numeri di Catalan. Triangolazione di poligoni.

Esercizi: Nella cartella https://www.dropbox.com/sh/nyo718jzbyopzbw/AACm-ZbWQ6mWfZOkX1sevOz3a?dl=0

ho aggiunto qualche esercizio su una ricorrenza.

mercoledì 16 maggio

lezione 29

Partizioni di interi. Diagrammi di Ferrers. Funzione generatrice del numero p(n) delle partizioni. Teorema di Eulero sulle partizioni in parti dispari e in parti distinte: dimostrazione combinatoria e dimostrazione analitica. Coefficienti binomiali: alcune identità. Convoluzione di Vandermonde: dimostrazione analitica e combinatoria. Principio dei cassetti (Pigeonhole principle)

(Da Wikipedia: Si ritiene che il principio sia stato esplicitato per la prima volta da Dirichlet nel 1834 col nome *Schubfachprinzip* ("principio del cassetto"). In alcune lingue, (ad esempio il russo) questo principio è pertanto noto come il *principio di Dirichlet*, da non confondersi con il principio dello stesso nome sulle funzioni armoniche. In inglese, invece, si parla di *pigeonhole principle*, dove il "pigeonhole" si riferisce alle cassette postali aperte in uso in alcuni uffici e università.

Dirichlet published his works in both French and German, using either the German *Schubfach* (he wrote about distributing pearls), or the French *tiroir*. The strict original meaning of both corresponds to the English *drawer*, an *open-topped box that can be slid in and out of the cabinet that contains it*. These terms were morphed to the word *pigeonhole*, standing for a *small open space in a desk, cabinet, or wall for keeping letters or papers*, metaphorically rooted in the structures that house pigeons.

El **principio del palomar**, también llamado **principio de Dirichlet** o **principio de las cajas**, establece que si *n* palomas se distribuyen en *m* palomares, y si $n > m$, entonces al menos habrá un palomar con más de una paloma.)

lunedì 21 maggio

lezione 30 e 31

Definizione di grafo semplice. Alcuni grafi notevoli. Grafi bipartiti. Cammini euleriani. Matrice di adiacenza di un grafo. Circuiti hamiltoniani: teorema di Ore. Grafi bipartiti e abbinamenti (matchings). Colorazione di grafi e applicazioni. Handshaking lemma.

mercoledì 23 maggio:

Complementi ed esercizi sui grafi col prof. Vietri

lunedì 28 maggio Secondo compito d'esonero.