

## Aritmetica Crittografia E Codici

These are notes of my Discrete Mathematics lectures held for students in Communication and Electric Engineering at Sapienza, the University of Roma. Roughly, the course is composed of the following parts: 1. Elements of Number Theory 2. elements of modern algebra 3. elements of combinatorics 4. elements of graph theory My objective was to illustrate several topics in different areas of modern mathematics into which Discrete Mathematics can be subdivided. Moreover, I wanted to give an "experimental" approach to the study of the material by repeatedly inviting students, whenever possible or feasible, to use a computer and a computer algebra system to carry out experimentation. Given the great variety of possible topics it was difficult to select a single book containing everything I wanted to show and only that. I therefore consulted many different sources that are acknowledged in the bibliography and I recommend them for further study. Some sections written in smaller fonts can be skipped or skimmed in a first reading as they do not properly belong to a traditional course on Discrete Mathematics, but that I felt important enough to include here with the aim of stimulating the curiosity of inquiring young minds.

Aritmetica, crittografia e codici Springer Science & Business Media

A partire dagli studi sulla prospettiva degli artisti del Rinascimento, la geometria proiettiva si è sviluppata nei secoli successivi come disciplina autonoma che, oltre ad essere alla base della geometria algebrica classica, trova applicazioni in numerosi settori, dall'ingegneria alla computer vision, dall'architettura alla crittografia. La prima parte di questo testo contiene richiami, sintetici ma rigorosi, delle nozioni fondamentali di geometria proiettiva, in un linguaggio semplice e moderno. Ciò offre al lettore una rapida visione d'insieme della materia trattata e lo introduce alle tecniche e alle notazioni successivamente adoperate. Nella seconda parte sono presentati più di 200 problemi risolti, per molti dei quali si propongono più soluzioni alternative. Il livello di difficoltà è variabile: si spazia da esercizi di carattere calcolativo a problemi più impegnativi di carattere teorico, fino a veri e propri teoremi con dimostrazione guidata. La struttura del testo consente al lettore di utilizzare la risoluzione degli esercizi per impadronirsi delle nozioni e delle tecniche di base e per progredire nella conoscenza della materia fino allo studio di alcuni risultati classici.

46.7

The book collects over 120 exercises on different subjects of Mathematical Finance, including Option Pricing, Risk Theory, and Interest Rate Models. Many of the exercises are solved, while others are only proposed. Every chapter contains an introductory section illustrating the main theoretical results necessary to solve the exercises. The book is intended as an exercise textbook to accompany graduate courses in mathematical finance offered at many universities as part of degree programs in Applied and Industrial Mathematics, Mathematical Engineering, and Quantitative Finance. The purpose of the volume is to provide a support for a first course in Mathematics. The contents are organised to appeal especially to Engineering, Physics and Computer Science students, all areas in which mathematical tools play a crucial role. Basic notions and methods of differential and integral calculus for functions of one real variable are presented in a manner that elicits critical reading and prompts a hands-on approach to concrete applications. The layout has a specifically-designed modular nature, allowing the instructor to make flexible didactical choices when planning an introductory lecture course. The book may in fact be employed at three levels of depth. At the elementary level the student is supposed to grasp the very essential ideas and familiarise with the corresponding key techniques. Proofs to the main results befit the intermediate level, together with several remarks and complementary notes enhancing the treatise. The last, and farthest-reaching, level requires the additional study of the material contained in the appendices, which enable the strongly motivated reader to explore further into the subject. Definitions and properties are furnished with substantial examples to stimulate the learning process. Over 350 solved exercises complete the text, at least half of which guide the reader to the solution. This new edition features additional material with the aim of matching the widest range of educational choices for a first course of Mathematics.

Il libro nasce dall'esigenza di coniugare esperienze e capacità procedurali diverse provenienti da vari ambiti disciplinari, quali l'informatica e la statistica, al fine di ricercare ed individuare percorsi e relazioni legate alla conoscenza. In un contesto di business, la conoscenza scoperta può avere un valore strategico per le aziende perchè consente di aumentare i profitti, riducendo i costi oppure aumentando le entrate con il conseguente aumento del ROI. Il volume è rivolto sia a studenti universitari e ricercatori, che a professionisti e manager aziendali che vogliono approfondire gli aspetti algoritmici delle tecniche di Data mining: lo studio degli algoritmi e delle principali tecniche è essenziale per conoscere meglio come la tecnologia possa essere applicata ai diversi tipi di dati e quindi anche diverse problematiche di business. Il testo pone volutamente l'attenzione sugli aspetti procedurali e di calcolo della metodologia, differenziandosi dagli altri testi in italiano che inquadrano puramente il contesto statistico. Il materiale esposto può essere utile a quanti vogliono completare la loro formazione scientifica in questa disciplina.

Si parla di fumetti nel libro del 2004 con quella che sta diventando una tradizione con il fumetto stile Disney del 2003 e del grafico olandese Maurits Cornelis Escher, anzi si "vedono" alcune delle immagini che sono state realizzate in animazione. Si parla del sogno di un uomo, di Gaudì, della grande ambizione di ascendere verso il cielo con la cattedrale di Barcellona; di come quel sogno si stia realizzando. Di teatro, di cinema si parla, ovviamente. Dell'interessante spettacolo di Luca Viganò e del teatro di Genova su Evariste Galois. E anche della America's Cup, di come dei matematici abbiano contribuito alla vittoria della barca Svizzera nella più importante avventura velica del mondo. Si parla di guerra e di pace, un argomento che non cessa mai di essere attuale. Inoltre, un omaggio al matematico Ennio De Giorgi che avrebbe dovuto essere il primo oratore del primo convegno di "Matematica e cultura". Una avventura dunque nella matematica che continua...

Il testo intende essere di supporto ad un secondo insegnamento di Analisi Matematica secondo i principi dei nuovi Ordinamenti

Didattici. E' in particolare pensato per quei corsi di studio (quali ad esempio Ingegneria, Informatica, Fisica) in cui lo strumento matematico è ? parte significativa della formazione. I concetti e i metodi fondamentali del calcolo differenziale ed integrale di più variabili, le serie di funzioni e le equazioni differenziali ordinarie sono presentati con l'obiettivo primario di addestrare lo studente ad un loro uso operativo, ma critico. L'impostazione didattica del testo ricalca quella usata per l'Analisi I. La modalità di presentazione degli argomenti permette un uso flessibile e modulare del testo, in modo da rispondere alle diverse possibili scelte didattiche nell'organizzazione di un corso di Analisi Matematica. Numerosi esempi corredano e illustrano le definizioni e le proprietà di volta in volta enunciate. Viene fornito un cospicuo numero di esercizi, tutti con la relativa soluzione. Per oltre la metà di essi si delinea in modo completo il procedimento risolutivo.

Il presente volume intende fornire un'introduzione alla probabilità e alle sue applicazioni, senza fare ricorso alla teoria della misura, per studenti dei corsi di laurea scientifici (in particolar modo di matematica, fisica e ingegneria). Viene dedicato ampio spazio alla probabilità discreta, vale a dire su spazi finiti o numerabili. In questo contesto sono sufficienti pochi strumenti analitici per presentare la teoria in modo completo e rigoroso. L'esposizione è arricchita dall'analisi dettagliata di diversi modelli, di facile formulazione e allo stesso tempo di grande rilevanza teorica e applicativa, alcuni tuttora oggetto di ricerca. Vengono poi trattate le variabili aleatorie assolutamente continue, reali e multivariate, e i teoremi limite classici della probabilità, ossia la Legge dei Grandi Numeri e il Teorema Limite Centrale, dando rilievo tanto agli aspetti concettuali quanto a quelli applicativi. Tra le varie applicazioni presentate, un capitolo è dedicato alla stima dei parametri in Statistica Matematica. Numerosi esempi sono parte integrante dell'esposizione. Ogni capitolo contiene una ricca selezione di esercizi, per i quali viene fornita la soluzione sul sito Springer dedicato al volume.

The book represents a basic support for a master course in electromagnetism oriented to numerical simulation. The main goal of the book is that the reader knows the boundary-value problems of partial differential equations that should be solved in order to perform computer simulation of electromagnetic processes. Moreover it includes a part devoted to electric circuit theory based on ordinary differential equations. The book is mainly oriented to electric engineering applications, going from the general to the specific, namely, from the full Maxwell's equations to the particular cases of electrostatics, direct current, magnetostatics and eddy currents models. Apart from standard exercises related to analytical calculus, the book includes some others oriented to real-life applications solved with MaxFEM free simulation software.

Il volume potrà essere utile ai docenti che intendano svolgere un corso su questi argomenti, la cui presenza sempre più viene richiesta nei corsi di laurea di matematica, fisica, informatica, ingegneria.

Giorgio Balzarotti e Pier Paolo Lava - già autori di La sequenza dei numeri primi, Gli errori nelle dimostrazioni matematiche e 103 curiosità matematiche - si avventurano in questo volume alla scoperta di un nuovo approccio alla teoria dei numeri. Il concetto di derivata di un numero, concepito molto probabilmente per la prima volta da un matematico spagnolo pressochè sconosciuto, José Mingot Shelly, dopo essere stato ignorato per quasi un secolo, sta avendo una grande rinascita proprio in questi ultimi anni nei siti e nelle riviste del settore. L'idea di Mingot Shelly scaturisce da una similitudine con i più ostici concetti dell'analisi delle funzioni che il matematico spagnolo reinterpreta e applica ai numeri interi. Sotto forma di un gioco di aritmetica elementare, o meglio sulla base di una proprietà dei numeri interi, è sviluppato un ingegnoso metodo per affrontare i problemi ancora aperti della teoria dei numeri. Così, oggi, ci si accorge che il concetto di derivata di un numero è molto più che una semplice curiosità per i dilettanti della matematica. Balzarotti e Lava raccolgono e sviluppano in modo sintetico e originale molti dei risultati che si trovano nella letteratura matematica sull'argomento, in modo da rendere la brillante idea accessibile a tutti. Famose congetture sono riscritte utilizzando le derivate dei numeri e anche la formula che esprime l'ennesimo numero primo, chimera di tutti gli appassionati di teoria dei numeri, trova in questo contesto un naturale e accattivante enunciato.

This book offers readers a primer on the theory and applications of Ordinary Differential Equations. The style used is simple, yet thorough and rigorous. Each chapter ends with a broad set of exercises that range from the routine to the more challenging and thought-provoking. Solutions to selected exercises can be found at the end of the book. The book contains many interesting examples on topics such as electric circuits, the pendulum equation, the logistic equation, the Lotka-Volterra system, the Laplace Transform, etc., which introduce students to a number of interesting aspects of the theory and applications. The work is mainly intended for students of Mathematics, Physics, Engineering, Computer Science and other areas of the natural and social sciences that use ordinary differential equations, and who have a firm grasp of Calculus and a minimal understanding of the basic concepts used in Linear Algebra. It also studies a few more advanced topics, such as Stability Theory and Boundary Value Problems, which may be suitable for more advanced undergraduate or first-year graduate students. The second edition has been revised to correct minor errata, and features a number of carefully selected new exercises, together with more detailed explanations of some of the topics. A complete Solutions Manual, containing solutions to all the exercises published in the book, is available. Instructors who wish to adopt the book may request the manual by writing directly to one of the authors.

Questo volume fornisce una introduzione all'analisi dei sistemi dinamici discreti. La materia è presentata mediante un approccio unitario tra il punto di vista modellistico e quello di varie discipline che sviluppano metodi di analisi e tecniche risolutive: Analisi Matematica, Algebra Lineare, Analisi Numerica, Teoria dei Sistemi, Calcolo delle Probabilità. All'esame di un'ampia serie di esempi, segue la presentazione degli strumenti per lo studio di sistemi dinamici scalari lineari e non lineari, con particolare attenzione all'analisi della stabilità. Si studiano in dettaglio le equazioni alle differenze lineari e si fornisce una introduzione elementare alle trasformate Z e DFT. Un capitolo è dedicato allo studio di biforcazioni e dinamiche caotiche. I sistemi dinamici vettoriali ad un passo e le applicazioni alle catene di Markov sono oggetto di tre capitoli. L'esposizione è autocontenuta: le appendici tematiche presentano prerequisiti, algoritmi e suggerimenti per simulazioni al computer. Ai numerosi esempi proposti si affianca un gran numero di esercizi, per la maggior parte dei quali si fornisce una soluzione dettagliata. Il volume è indirizzato principalmente agli studenti di Ingegneria, Scienze, Biologia ed Economia. Questa terza edizione comprende l'aggiornamento di vari argomenti, l'aggiunta di nuovi esercizi e l'ampliamento della trattazione relativa alle matrici positive ed alle loro proprietà utili nell'analisi di sistemi, reti e motori di ricerca.

The book provides an introduction to Differential Geometry of Curves and Surfaces. The theory of curves starts with a discussion of possible definitions of the concept of curve, proving in particular the classification of 1-dimensional manifolds. We then present the classical local theory of parametrized plane and space curves (curves in n-dimensional space are discussed in the complementary material): curvature, torsion, Frenet's formulas and the fundamental theorem of the local theory of curves. Then, after a self-contained presentation of degree theory for continuous self-maps of the circumference, we study the global theory of



plane curves, introducing winding and rotation numbers, and proving the Jordan curve theorem for curves of class  $C^2$ , and Hopf theorem on the rotation number of closed simple curves. The local theory of surfaces begins with a comparison of the concept of parametrized (i.e., immersed) surface with the concept of regular (i.e., embedded) surface. We then develop the basic differential geometry of surfaces in  $R^3$ : definitions, examples, differentiable maps and functions, tangent vectors (presented both as vectors tangent to curves in the surface and as derivations on germs of differentiable functions; we shall consistently use both approaches in the whole book) and orientation. Next we study the several notions of curvature on a surface, stressing both the geometrical meaning of the objects introduced and the algebraic/analytical methods needed to study them via the Gauss map, up to the proof of Gauss' Teorema Egregium. Then we introduce vector fields on a surface (flow, first integrals, integral curves) and geodesics (definition, basic properties, geodesic curvature, and, in the complementary material, a full proof of minimizing properties of geodesics and of the Hopf-Rinow theorem for surfaces). Then we shall present a proof of the celebrated Gauss-Bonnet theorem, both in its local and in its global form, using basic properties (fully proved in the complementary material) of triangulations of surfaces. As an application, we shall prove the Poincaré-Hopf theorem on zeroes of vector fields. Finally, the last chapter will be devoted to several important results on the global theory of surfaces, like for instance the characterization of surfaces with constant Gaussian curvature, and the orientability of compact surfaces in  $R^3$ .

This book pursues the accurate study of the mathematical foundations of Quantum Theories. It may be considered an introductory text on linear functional analysis with a focus on Hilbert spaces. Specific attention is given to spectral theory features that are relevant in physics. Having left the physical phenomenology in the background, it is the formal and logical aspects of the theory that are privileged. Another not lesser purpose is to collect in one place a number of useful rigorous statements on the mathematical structure of Quantum Mechanics, including some elementary, yet fundamental, results on the Algebraic Formulation of Quantum Theories. In the attempt to reach out to Master's or PhD students, both in physics and mathematics, the material is designed to be self-contained: it includes a summary of point-set topology and abstract measure theory, together with an appendix on differential geometry. The book should benefit established researchers to organise and present the profusion of advanced material disseminated in the literature. Most chapters are accompanied by exercises, many of which are solved explicitly.

Questo volume intende presentare le nozioni fondamentali dell'aritmetica modulare, con particolare riguardo a quegli argomenti che costituiscono la base matematica della teoria dei codici e della crittografia. Non è richiesta al lettore una particolare conoscenza di nozioni di algebra o di teoria dei numeri, dal momento che tutte le definizioni ed i risultati necessari alla lettura sono riportati nel testo: è però utile una certa familiarità con il ragionamento matematico. Il contenuto del libro è organizzato nel modo seguente: nei primi 5 capitoli sono esposti gli elementi essenziali dell'aritmetica modulare, corredati dai principali algoritmi e da numerosi esercizi, sia svolti che proposti. I restanti 4 capitoli sono dedicati a complementi della teoria, in due direzioni essenzialmente diverse. Infatti, i Capitoli 6 e 7 intendono dare un'idea di come la teoria esposta venga utilizzata nella crittografia a chiave pubblica. I Capitoli 8 e 9 contengono invece un ulteriore approfondimento della teoria, e sono dedicati ad un'esposizione semplice, ma completa, della teoria dei campi finiti, anch'essa ampiamente utilizzata in crittografia e nella teoria dei codici. Infine, l'Appendice contiene alcuni cenni relativi alla complessità computazionale degli algoritmi, limitatamente a quanto è necessario alla comprensione del testo.

Nel volume vengono descritti e analizzati gli algoritmi di ottimizzazione non vincolata maggiormente noti e quelli studiati più di recente e proposti nella letteratura specialistica. Particolare attenzione viene data alle proprietà teoriche di convergenza degli algoritmi descritti e agli aspetti numerici e computazionali ad essi connessi. La stesura del testo tale da renderlo adatto sia a un lettore che intenda acquisire una preparazione di base delle metodologie di ottimizzazione non vincolata, sia a un lettore che abbia già competenze generali di ottimizzazione e che voglia approfondire specifici argomenti. I concetti matematici di base sono riportati nelle appendici con il fine di presentare una trattazione degli argomenti autocontenuta.

Gli Automi sono modelli matematici di macchine digitali di grande interesse sia dal punto di vista teorico che applicativo. La teoria degli Automi Finiti costituisce una delle parti fondamentali dell'Informatica Teorica. Questo volume fornisce, per la prima volta, nel panorama didattico italiano una trattazione matematicamente rigorosa della teoria degli Automi Finiti e delle macchine sequenziali generalizzate nell'ambito della teoria algebrica dei semigrupp. Il volume, la cui lettura presuppone solamente conoscenze elementari di algebra, si rivolge agli studenti sia dei corsi di laurea magistrale e specialistica che di master e di dottorato in Informatica, in Matematica, ed in Ingegneria. Il libro è anche uno strumento utilissimo per gli studiosi di Informatica e, in particolare, di Informatica Teorica, ai quali fornisce una trattazione completa e rigorosa della teoria algebrica degli Automi. Ogni capitolo ha una sezione di esercizi ed una di note bibliografiche. La risoluzione della maggior parte degli esercizi è riportata alla fine del volume.

Il libro introduce la teoria della misura e l'analisi funzionale con una coda di argomenti scelti. Contiene un'ampia gamma di esempi ed esercizi, per i quali si forniscono spesso suggerimenti generosi. È rivolto principalmente a studenti della laurea in Matematica e Ingegneria.

La finanza matematica ha visto un notevole sviluppo in tempi recenti, soprattutto per l'introduzione di strumenti finanziari atti a contenere il rischio nelle operazioni di mercato. Lo studio delle problematiche legate a tali strumenti richiede tecniche matematiche talvolta sofisticate e la maggior parte di queste tecniche sono legate alla teoria della Probabilità. Gli ambienti finanziari sono quindi divenuti uno sbocco professionale non solo per gli economisti, ma anche per i matematici ed in generale per i laureati delle discipline tecnico-scientifiche. Il presente libro è inteso come testo e nasce dall'esperienza d'insegnamento degli autori. Non esistono molti testi simili a livello internazionale ed il libro intende colmare tale lacuna. Benché concepito maggiormente per un corso di laurea triennale in matematica, esso dovrebbe adattarsi bene anche a corsi di tipo quantitativo per le facoltà di economia.

Le equazioni differenziali sono un argomento fondamentale non solo della matematica, ma anche della fisica,

dell'ingegneria e, in generale, di tutte le scienze. Questo volume intende fornire allo studente una panoramica di alcune tra le più interessanti e suggestive questioni relative alle equazioni differenziali ordinarie trattate da un punto di vista geometrico, aprendo uno sguardo verso l'analisi funzionale. Oltre ai risultati classici sulle equazioni lineari, molto spazio è dato ai problemi nonlineari che spesso non sono oggetto dei corsi istituzionali. L'esposizione è tenuta a un livello semplice in modo che il libro possa essere accessibile a studenti dell'ultimo anno della laurea triennale e della laurea magistrale, offrendo anche spunti per ulteriori approfondimenti.

Il testo è rivolto a studenti di ingegneria, matematica applicata e fisica ed è disegnato per corsi alle fine del triennio o all'inizio del biennio magistrale. obiettivo didattico è duplice: da un lato presentare ed analizzare alcuni classici modelli differenziali della Meccanica dei Continui, completati da esercizi svolti e da simulazioni numeriche, illustrate usando il metodo delle differenze finite; dall'altro introdurre la formulazione variazionale dei più importanti problemi iniziali/al bordo, accompagnate da simulazioni numeriche effettuate utilizzando il metodo degli elementi finiti. In ultima analisi, il percorso didattico è caratterizzato da una costante sinergia tra modello-teoria-simulazione numerica.

Questa è una raccolta di esercizi che illustra alcuni aspetti fondamentali della Finanza Matematica, in particolare della valutazione dei derivati. E' rivolta a studenti dei corsi di Laurea Magistrale, ma può essere utilizzata con successo anche nei corsi di Laurea del primo livello, da studenti che abbiano una adeguata formazione di tipo matematico (Corsi di Laurea in Matematica, Ingegneria). La risoluzione degli esercizi viene affrontata con l'utilizzo di metodi propri sia della Teoria della Probabilità (processi stocastici) che dell'Analisi Matematica (Equazioni alle Derivate Parziali).

Questo manuale è stato realizzato per permettere ai futuri studenti di Ingegneria di affrontare con successo i propri studi. Vengono presentati alcuni concetti di base in matematica, generalmente già appresi prima dell'ingresso all'Università. Si è constatato che non tutti gli studenti hanno una padronanza completa di questo insieme di nozioni fondamentali: perciò il presente manuale fornisce un utile supporto, sotto forma sia di esercizi sia di nozioni teoriche. Il futuro studente potrà scegliere i capitoli che più lo interessano, al fine di verificare la propria capacità a risolvere problemi quali i "Problemi di revisione", ricorrendo alle proprie abilità di ragionamento ed alle proprie conoscenze.

Questi sono appunti delle mie lezioni di Matematica Discreta per il corso di studi in Ingegneria Elettronica e Ingegneria delle Comunicazioni dell'Università di Roma, La Sapienza. È un corso facoltativo di 6 CFU. A grandi linee il corso si compone delle seguenti parti: Elementi di teoria dei numeri Elementi di algebra moderna Elementi di combinatoria Elementi di teoria dei grafi Mi sono proposto di illustrare alcune tematiche di diversi campi della matematica moderna in cui si può suddividere la Matematica Discreta. Data la varietà dei possibili argomenti è difficile indicare un singolo libro di testo che comprenda un po' di tutto ciò che volevo illustrare. Per questi appunti ho attinto perciò da varie fonti citate nella bibliografia a cui rinvio per approfondimenti. Il testo contiene anche numerosi esercizi svolti.

Durante la II guerra mondiale hanno avuto luogo numerosi risultati di rilievo nel campo della crittografia militare. Uno dei meno conosciuti è quello usato dal servizio di intelligence svedese, nei confronti del codice tedesco per le comunicazioni strategiche con i comandi dei paesi occupati nel nord Europa, le cui linee passavano per la Svezia. In tal modo, durante la fase più critica della guerra la direzione politica e militare svedese era in grado di seguire i piani e le disposizioni dei Tedeschi, venendo a conoscenza dei più arditi progetti per modificare la propria politica, tenendo la Svezia fuori dalla guerra. La violazione del codice tedesco è narrata in dettaglio, per la prima volta, con elementi che gli permettono di essere un'ottima introduzione al campo della crittografia, oltre che un ritratto vitale e umano della società del tempo: una disperata condizione bellica, l'intrigo politico e spionistico, il genio del matematico Arne Beurling, le difficoltà e i trucchi del mestiere, e il lavoro sistematico e oscuro di una folla di decrittatori.

Questo testo è espressamente concepito per i corsi brevi del nuovo ordinamento delle Facoltà di Ingegneria e di Scienze. Esso affronta tutti gli argomenti tipici della Matematica Numerica, spaziando dal problema di approssimare una funzione, al calcolo dei suoi zeri, delle sue derivate e del suo integrale definito fino alla risoluzione approssimata di equazioni differenziali ordinarie e di problemi ai limiti. Due capitoli sono inoltre dedicati alla risoluzione di sistemi lineari ed al calcolo degli autovalori di una matrice, mentre un capitolo iniziale conduce lo studente ad un rapido ripasso degli argomenti dell'Analisi Matematica di uso frequente nel volume e ad una introduzione al linguaggio Matlab. I vari argomenti sono volutamente affrontati a livello elementare ed i paragrafi che richiedono maggior impegno sono stati opportunamente contrassegnati. In questa quarta edizione il linguaggio Octave (di distribuzione gratuita) si affianca a MATLAB.

This book is designed as an advanced undergraduate or a first-year graduate course for students from various disciplines like applied mathematics, physics, engineering. It has evolved while teaching courses on partial differential equations during the last decade at the Politecnico of Milan. The main purpose of these courses was twofold: on the one hand, to train the students to appreciate the interplay between theory and modelling in problems arising in the applied sciences and on the other hand to give them a solid background for numerical methods, such as finite differences and finite elements.

Il testo intende essere di supporto ad un primo insegnamento di Analisi Matematica secondo i principi dei nuovi Ordinamenti Didattici. È in particolare pensato per Ingegneria, Informatica, Fisica. Il testo presenta tre diversi livelli di lettura. Un livello essenziale permette allo studente di cogliere i concetti indispensabili della materia e di familiarizzarsi con le relative tecniche di calcolo. Un livello intermedio fornisce le giustificazioni dei principali risultati e arricchisce l'esposizione mediante utili osservazioni e complementi. Un terzo livello di lettura, basato su numerosi riferimenti ad un testo virtuale disponibile in rete, permette all'allievo più motivato ed interessato di approfondire la sua preparazione sulla materia. Completano il testo numerosi esempi ed esercizi con soluzioni. La grafica accattivante, a 2 colori, fa di questo testo un punto di riferimento fondamentale per lo studio della disciplina.

Nato dall'esperienza dell'autore nell'insegnamento della topologia agli studenti del corso di Laurea in Matematica, questo libro contiene le nozioni fondamentali di topologia generale ed una introduzione alla topologia algebrica. La scelta degli argomenti, il loro ordine di presentazione e, soprattutto, il tipo di esposizione tiene conto delle tendenze attuali nell'insegnamento della topologia e delle novità nella struttura dei corsi di Laurea scientifici conseguenti all'introduzione del sistema 3+2. Questa seconda edizione, oltre a semplificare alcune dimostrazioni, presenta una sostanziale riscrittura della parte sui rivestimenti e l'aggiunta di ulteriori esempi; il numero complessivo di esercizi proposti stato portato a 500 ed il numero di quelli svolti a 120.

In this volume one finds basic techniques from algebra and number theory (e.g. congruences, unique factorization domains, finite fields, quadratic residues, primality tests, continued fractions, etc.) which in recent years have proven to be extremely useful for applications to cryptography and coding theory. Both cryptography and codes have crucial applications in our daily lives, and they are described here, while the complexity problems that arise in implementing the related numerical algorithms are also taken into due account. Cryptography has been developed in great detail, both in its classical and more recent aspects. In particular public key cryptography is extensively discussed, the use of algebraic geometry, specifically of elliptic curves over finite fields, is illustrated, and a final chapter is devoted to quantum cryptography, which is the new frontier of the field. Coding theory is not discussed in full; however a chapter, sufficient for a good introduction to the subject, has been devoted to linear codes. Each chapter ends with several complements and



with an extensive list of exercises, the solutions to most of which are included in the last chapter. Though the book contains advanced material, such as cryptography on elliptic curves, Goppa codes using algebraic curves over finite fields, and the recent AKS polynomial primality test, the authors' objective has been to keep the exposition as self-contained and elementary as possible. Therefore the book will be useful to students and researchers, both in theoretical (e.g. mathematicians) and in applied sciences (e.g. physicists, engineers, computer scientists, etc.) seeking a friendly introduction to the important subjects treated here. The book will also be useful for teachers who intend to give courses on these topics.

L'opera fornisce una introduzione alla geometria delle varietà differenziabili, illustrandone le principali proprietà e descrivendo le principali tecniche e i più importanti strumenti usati per il loro studio. Uno degli obiettivi primari dell'opera è di fungere da testo di riferimento per chi (matematici, fisici, ingegneri) usa la geometria differenziale come strumento; inoltre può essere usato come libro di testo per diversi corsi introduttivi alla geometria differenziale, concentrandosi su alcuni dei vari aspetti della teoria presentati nell'opera. Più in dettaglio, nell'opera saranno trattati i seguenti argomenti: richiami di algebra multilineare e tensoriale, spesso non presentati nei corsi standard di algebra lineare; varietà differenziali, incluso il teorema di Whitney; fibrati vettoriali, incluso il teorema di Frobenius e un'introduzione ai fibrati principali; gruppi di Lie, incluso il teorema di corrispondenza fra sottogruppi e sottoalgebre; coomologia di de Rham, inclusa la dualità di Poincaré e il teorema di de Rham; connessioni, inclusa la teoria delle geodetiche; e geometria Riemanniana, con particolare attenzione agli operatori di curvatura e inclusi teoremi di Cartan-Hadamard, Bonnet-Myers, e Synge-Weinstein. Come abitudine degli autori, il testo è scritto in modo da favorire una lettura attiva, cruciale per un buon apprendimento di argomenti matematici; inoltre è corredato da numerosi esempi svolti ed esercizi proposti.

La Matematica Numerica è elemento fondante del calcolo scientifico. Punto di contatto di diverse discipline nella matematica e nelle moderne scienze applicate, ne diventa strumento di indagine qualitativa e quantitativa. Scopo di questo testo è fornire i fondamenti metodologici della matematica numerica, richiamandone le principali proprietà, quali la stabilità, l'accuratezza e la complessità algoritmica. Nel contesto di ogni specifica classe di problemi vengono illustrati gli algoritmi più idonei, ne viene fatta l'analisi teorica e se ne verificano i risultati previsti implementandoli con l'ausilio di programmi in linguaggio MATLAB. Ogni capitolo è integrato da esercizi e temi svolti, questi ultimi corredati da programmi MATLAB. Il volume è indirizzato principalmente agli studenti delle facoltà scientifiche, con particolare attenzione ai corsi di laurea in Ingegneria, Matematica e Scienze dell'Informazione. L'enfasi posta sullo sviluppo di software lo rende interessante anche per ricercatori e utilizzatori delle tecniche del calcolo scientifico nei campi professionali più disparati. La quarta edizione contiene numerose integrazioni in quasi tutti i capitoli. Diverse sezioni sono inoltre state rivisitate con lo scopo di rendere più chiari concetti ed argomenti di considerevole complessità.

The purpose of the volume is to provide a support textbook for a second lecture course on Mathematical Analysis. The contents are organised to suit, in particular, students of Engineering, Computer Science and Physics, all areas in which mathematical tools play a crucial role. The basic notions and methods concerning integral and differential calculus for multivariable functions, series of functions and ordinary differential equations are presented in a manner that elicits critical reading and prompts a hands-on approach to concrete applications. The pedagogical layout echoes the one used in the companion text Mathematical Analysis I. The book's structure has a specifically-designed modular nature, which allows for great flexibility in the preparation of a lecture course on Mathematical Analysis. The style privileges clarity in the exposition and a linear progression through the theory. The material is organised on two levels. The first, reflected in this book, allows students to grasp the essential ideas, familiarise with the corresponding key techniques and find the proofs of the main results. The second level enables the strongly motivated reader to explore further into the subject, by studying also the material contained in the appendices. Definitions are enriched by many examples, which illustrate the properties discussed. A host of solved exercises complete the text, at least half of which guide the reader to the solution. This new edition features additional material with the aim of matching the widest range of educational choices for a second course of Mathematical Analysis.

Questo è un libro di testo sulla geometria differenziale di curve e superfici, adatto agli studenti universitari del secondo e terzo anno dei corsi di Laurea in Matematica, Fisica, Ingegneria e Informatica.

This short book, geared towards undergraduate students of computer science and mathematics, is specifically designed for a first course in mathematical logic. A proof of Gödel's completeness theorem and its main consequences is given using Robinson's completeness theorem and Gödel's compactness theorem for propositional logic. The reader will familiarize himself with many basic ideas and artifacts of mathematical logic: a non-ambiguous syntax, logical equivalence and consequence relation, the Davis-Putnam procedure, Tarski semantics, Herbrand models, the axioms of identity, Skolem normal forms, nonstandard models and, interestingly enough, proofs and refutations viewed as graphic objects. The mathematical prerequisites are minimal: the book is accessible to anybody having some familiarity with proofs by induction. Many exercises on the relationship between natural language and formal proofs make the book also interesting to a wide range of students of philosophy and linguistics.

Il presente testo di Meccanica Razionale è concepito in vista del rinnovamento dell'organizzazione e dei contenuti dei corsi offerti dalle Facoltà di Ingegneria, dove il ruolo della Meccanica Razionale non è solo quello di introdurre alla modellizzazione fisico-matematica rigorosa, ma anche di propedeuticità all'insegnamento di specifiche applicazioni ingegneristiche. In particolare, il testo introduce i concetti fondamentali a partire da esempi e problemi concreti, anche comuni ad altre discipline, in vista di sinergie didattiche a volte favorite dalla presenza di corsi integrati. Il libro possiede una impostazione il più possibile coerente con questa finalità, soprattutto in alcune sezioni tradizionalmente caratterizzate da una trattazione forse più astratta: dai vincoli al Principio dei lavori virtuali, dal Principio di d'Alembert alla Meccanica Analitica.

Mathematics of Computing -- Parallelism.

[Copyright: 2285b3db8712d19c7e8317a3905df31d](#)