DISMA Dipartimento di Scienze Matematiche G. L. Lagrange

Algebra e Geometria: proposte di prove finali

Incontro di presentazione

19 febbraio 2026

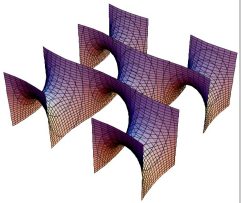
Politecnico di Torino

Geometria Differenziale

Usa tecniche dal calcolo differenziale, dal calcolo integrale e dall'algebra (multi)lineare per studiare problemi geometrici

Debora Impera - debora.impera@polito.it

Aspetti della teoria delle superfici minime in $\mathbb{R}^3$:

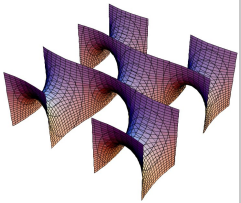


Problema: Costruire esempi di superfici minime

- Rappresentazione di Weierstrass per superfici minime
- Costruzione di superfici minime periodiche

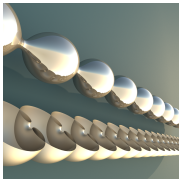
Debora Impera - debora.impera@polito.it

Aspetti della teoria delle superfici minime in $\mathbb{R}^3$:



Problema: Costruire esempi di superfici minime

- Rappresentazione di Weierstrass per superfici minime
- Costruzione di superfici minime periodiche



Problema: Classificazione di superfici minime e a curvatura media costante con determinate proprietà

- Il teorema di Delaunay
- Il teorema di Alexandrov

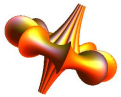
Emilio Musso - emilio.musso@polito.it

Nel piano iperbolico valgono tutte le usuali proprietà della geometria euclidea, tranne il postulato delle rette parallele, che viene modificato nel modo seguente:

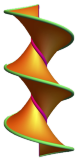
data una retta e un punto esterno ad essa, esistono almeno due rette passanti per quel punto che non la intersecano.

Problema: È possibile realizzare il piano iperbolico come superficie regolare dello spazio euclideo?

- Il teorema di Hilbert e la non immergibilità del piano iperbolico nello spazio euclideo



Esistono tuttavia immersioni isometriche di porzioni del piano iperbolico nello spazio euclideo: le superfici pseudosferiche.



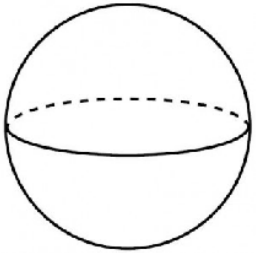
MATHEMATICA → rappresentare superfici pseudosferiche di rotazione.

Francesco Pediconi - francesco.pediconi@polito.it

Domanda: Che legame c'è tra curvatura e topologia?

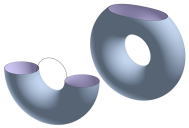
- Il Teorema di Bonnet

Il Teorema di Bonnet è un risultato classico di fondamentale importanza nella teoria delle superfici lisce e fornisce uno dei primi esempi del legame profondo tra curvatura e topologia. Più nello specifico, il teorema afferma che se la curvatura Gaussiana di una superficie completa è positiva e uniformemente staccata da zero, allora la superficie è compatta.



Michele Rimoldi - michele.rimoldi@polito.it

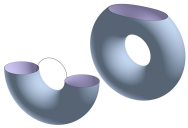
Domanda: È possibile studiare proprietà topologiche e geometriche di una superficie usando proprietà di particolari funzioni differenziabili su di essa?



- Aspetti introduttivi della teoria di Morse su superfici

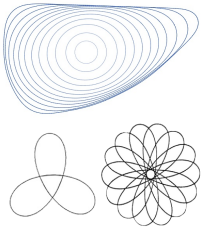
Michele Rimoldi - michele.rimoldi@polito.it

Domanda: È possibile studiare proprietà topologiche e geometriche di una superficie usando proprietà di particolari funzioni differenziabili su di essa?



- Aspetti introduttivi della teoria di Morse su superfici

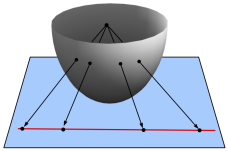
Domanda: Sia data una curva piana semplice e chiusa, che si muova in ogni punto in direzione normale alla curva stessa, con velocità pari alla curvatura della curva in tale punto. Quali tipi di comportamento possiamo aspettarci?



- Curve shortening flow: aspetti analitici e geometrici
- Classificazione di curve che si contraggono omoteticamente lungo il CSF

Giovanni Manno - giovanni.manno@polito.it

Domanda: La sfera e il piano non sono varietà isometriche. Eppure, geodetiche della sfera (pezzi di equatori) vengono mandate in geodetiche del piano (segmenti) tramite la proiezione. In un certo senso hanno le stesse geodetiche.



- Geometria delle equazioni differenziali

Le geodetiche sono soluzioni di equazione differenziali ordinarie. Cosa si può dire per le equazioni a derivate parziali (PDEs)? Lo studio di questo problema ha applicazioni che spaziano dalla geometria proiettiva alla relatività.

Geometria Algebrica

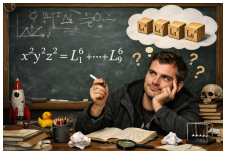
Studia e classifica le varietà geometriche che sono definite come l'insieme di soluzioni di un insieme di polinomi in diverse variabili.

Monomi come somme di potenze

Scrivere il monomio xyz come una somma di cubi può sembrare un'inutile complicazione, ma in realtà è utile quanto diagonalizzare una matrice quadrata. Di quanti monomi abbiamo bisogno? Ne bastano 4.

Sorprendentemente conosciamo la risposta per il suo quadrato, $(xyz)^2$, solo usando coefficienti complessi, non reali.

Domanda: Cosa succede se dobbiamo usare solo coefficienti reali?

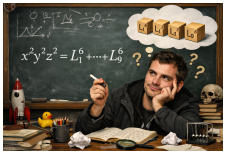


- Monomi come somme di potenze

Scrivere il monomio xyz come una somma di cubi può sembrare un'inutile complicazione, ma in realtà è utile quanto diagonalizzare una matrice quadrata. Di quanti monomi abbiamo bisogno? Ne bastano 4.

Sorprendentemente conosciamo la risposta per il suo quadrato, $(xyz)^2$, solo usando coefficienti complessi, non reali.

Domanda: Cosa succede se dobbiamo usare solo coefficienti reali?



Il prodotto righe per colonne non è l'unico modo di moltiplicare due matrici, ne esistono molti. Ad esempio il prodotto di Hadamard che semplicemente moltiplica elemento per elemento. La stessa operazione si può effettuare su oggetti geometrici, come curve e superfici. Il risultato non è però sempre ovvio.

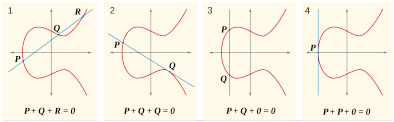
E.g. due curve posso dare come risultato una superficie, una curva, ma anche un punto.

Domanda: Come possiamo predire la dimensione del risultato?

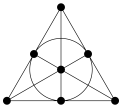
- Prodotti di Hadamard di matrici e di varietà

Juan Pons-Llopis - juan.ponsllopis@polito.it

- Curve ellittiche e gruppi abeliani



- Geometria proiettiva su campi finiti



- Rappresentazioni di gruppi finiti

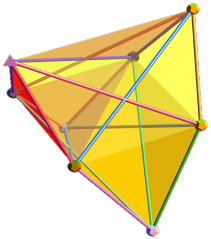
Emanuele Ventura - emanuele.ventura@polito.it

Una Grassmanniana è una varietà differenziabile (e algebrica) i cui punti sono i sottospazi vettoriali di una data dimensione in uno spazio vettoriale. Lo spazio proiettivo è il primo esempio di Grassmanniana.

Problema: studiarne la costruzione e le proprietà geometriche fondamentali

- La geometria delle Grassmanniane

  - Fondamentale importanza in geometria algebrica reale e complessa, con profondi legami alla combinatoria e alla fisica teorica.
  - Le Grassmanniane reali positive hanno un ruolo cruciale in certe teorie quantistiche dei campi.



Francesco Malaspina - francesco.malaspina@polito.it

- Questioni di topologia generale, topologia algebrica, logica, geometria algebrica, geometria proiettiva, algebra commutativa, algebra omologica, spazi vettoriali topologici
- Etnomatematica: con possibilità di esperienze didattiche in Africa. Ci sarà un incontro con un ospite dell'associazione SAMI (Supporting African Maths Initiative) il 3 marzo in cui verranno date maggiori informazioni.

Thank you for your attention

Politecnico
di Torino

CrypTO

Crittografia e Teoria dei Numeri

Prove finali del gruppo di Crittografia e Teoria dei Numeri

CrypTO
https://crypto.polito.it

Danilo Bazzanella danilo.bazzanella@polito.it
Antonio Di Scala antonio.discala@polito.it
Carlo Sanna carlo.sanna@polito.it

Politecnico di Torino

DISMA

"We the Cypherpunks are dedicated to building anonymous systems. We are defending our **privacy** *with* **cryptography**, *with anonymous mail forwarding systems, with digital signatures, and with electronic money."*

Eric Hughes,
A Cypherpunk's Manifesto

"La Matematica é la regina delle Scienze, la Teoria dei Numeri é la regina della matematica."

Carl Friedrich Gauss

La prova finale in **Crittografia o Teoria dei Numeri** può essere utile per scegliere con maggiore consapevolezza il vostro percorso di studi alla laurea magistrale:

Percorso di studi in CRITTOGRAFIA E SICUREZZA

Laurea Magistrale in Ingegneria Matematica

INSEGNAMENTO	CFU	ANNO	PERIODO
Reti di calcolatori	8	1	1
Processi stocastici e Dinamiche su network	12	1	1
Sicurezza dei sistemi informativi	6	1	1
Modelli Statistici	6	1	1
Calcolatori elettronici	8	1	2
Model Order Reduction and Machine Learning	6	1	2
Crittografia	6	1	2
Blockchain e Criptoeconomia	6	1	2
Machine Learning for Mathematical Engineering	6	1	2

INSEGNAMENTO	CFU	ANNO	PERIODO
Management and content delivery for Smart Networks	12	2	1
AI and Cybersecurity	6	2	1
Advanced Cryptography	6	2	1
Networks and cloud technologies security	12	2	1,2
Post-Quantum Cryptography	6	2	2
Tesi	16	2	2

SECONDA LAUREA

Laureandosi in Ingegneria Matematica con il percorso di studi in **"Crittografia e Sicurezza"** è possibile ottenere una **SECONDA LAUREA** in **Cybersecurity** o in **Ingegneria Informatica** sostenendo solo 5 esami e la tesi:

INSEGNAMENTO	CFU
Offensive Security	6
Threat Intelligence and Incident Management	6
Data protection, Privacy and Anonymity	6
Advanced Information systems security oppure Security verification and testing	8
Cybersecurity laws and regulations oppure Technology and Innovation Management in Cybersecurity	6
Tesi	22

Possibili argomenti per la prova finale di **Crittografia o Teoria dei Numeri**

- La crittografia in Bitcoin
- Crittografia Post-Quantum
- Test di primalità e algoritmi di fattorizzazione
- Algebra e Teoria dei Numeri per le applicazioni crittografiche
- Successione di Fibonacci e applicazioni
- Curve ellittiche
- Frazioni Continue
- Teoria dei Codici
- Funzioni Hash
- Approfondimenti sulla storia della Teoria dei Numeri
- Protocolli di commitment
- Protocolli di Check-sum (somme di controllo)
- Risoluzione di sistemi polinomiali applicati alla crittografia
- ...

Per ulteriori informazioni:

- Responsabile gruppo: **danilo.bazzanella@polito.it**
- Sito web del gruppo: **https://crypto.polito.it**

CrypTO

Crittografia e Teoria dei Numeri

Grazie per l'attenzione

Politecnico di Torino

1859

DISMA