

ALGEBRA
2011/12

CARANTI, DE
GRAAF,
MATTAREI &
SALA

CORSI DI
ALGEBRA

I CORSI OFFERTI

QUALCHE DETTAGLIO
SUI CORSI

LAUREA
TRIENNALE

LAUREA TRIENNALE

LAUREA
MAGISTRALE

LAUREA
MAGISTRALE IN
MATEMATICA

LAUREA
MAGISTRALE IN
INGEGNERIA DELLE
TELECOMUNICAZIONI

CORSI E PIANI DI STUDIO DI ALGEBRA A.A. 2011/12

Andrea Caranti Willem de Graaf Sandro Mattarei
Massimiliano Sala

Dipartimento di Matematica
Università degli Studi di Trento
`science.unitn.it/~caranti`

Trento, 18 maggio 2011

PIANO DELLA PRESENTAZIONE

CORSI DI
ALGEBRA

I CORSI OFFERTI

QUALCHE DETTAGLIO
SUI CORSI

LAUREA
TRIENNALE

LAUREA TRIENNALE

LAUREA
MAGISTRALE

LAUREA
MAGISTRALE IN
MATEMATICA

LAUREA
MAGISTRALE IN
INGEGNERIA DELLE
TELECOMUNICAZIONI

1 CORSI DI ALGEBRA

I corsi offerti

Qualche dettaglio sui corsi

2 LAUREA TRIENNALE

Algebra Computazionale e Crittografia

3 DUE SOLUZIONI PER LA LAUREA MAGISTRALE

Laurea Magistrale in Matematica

Laurea Magistrale in Ingegneria delle
Telecomunicazioni

CORSI DI ALGEBRA

Corso	Sem.	Docente
Teoria di Galois	1	de Graaf
Teoria dei Numeri e Crittografia	2	Mattarei
Teoria dei Gruppi	2	Mattarei
Computational Algebra	1	de Graaf
Discrete Fourier Analysis	N.A.	Mattarei
Finite Fields and Symm. Cryptography	2	Mattarei
Coding Theory	1	Sala

- I primi tre corsi (in italiano) sono per la Triennale.
- Gli altri (in inglese) sono per la Magistrale.
- I corsi sono **indipendenti**.
- Sono tutti da 6 CFU, tranne Coding Theory che è da 12.
- Più avanti segnalerò piani di studio **consigliati**.

TEORIA DI GALOIS

- Tenuto da Willem de Graaf nel primo semestre.
- Adatto a tutti gli orientamenti: didattico, generale, e anche interdisciplinare. (I *telecomunicatori* lo riconoscono come *Complementi di trasmissione numerica!*)

L'equazione di secondo grado

$$x^2 + bx + c = 0$$

ammette le radici

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

TEORIA DI GALOIS

Formule *simili* a

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

(cioè che contengono le quattro operazioni, e simboli di radice) esistono anche per le equazioni di terzo e quarto grado.

L'equazione

$$x^3 + px + q = 0$$

ha radici

$$x = \frac{1}{\sqrt[3]{2}} \cdot \left(\sqrt[3]{-q + \sqrt{-q^2 + \frac{4}{27}p^3}} + \sqrt[3]{-q - \sqrt{-q^2 + \frac{4}{27}p^3}} \right)$$

TEORIA DI GALOIS

- Ma **non esistono** formule che contengano solo le quattro operazioni, e simboli di radice per le equazioni dal quinto grado in su. (Ruffini, Abel, Galois.)
- In questo corso vediamo un metodo generale, dovuto a Galois, per trovare le formule per il terzo e quarto grado, e per vedere che non esistono dal quinto grado in su.
- Si fa teoria dei campi e teoria dei gruppi.
- E' per la Triennale.

TEORIA DEI NUMERI E CRITTOGRAFIA

- Tenuto da Sandro Mattarei nel secondo semestre.
- Raccomandato per la Triennale.
- Riprende gli argomenti di crittografia trattati nel primo corso di Algebra: RSA, testa o croce per telefono.
- Ha da un lato un aspetto **teorico**. Questo riguarda soprattutto la Teoria dei Numeri interi, numeri primi, ecc.
- Ha poi un aspetto **applicativo**.
- Si parla ad esempio dell'algorithmo ufficialmente adottato per la **firma digitale** e dell'idea che ha avuto Phong Q. Nguyen (Eurocrypt 2004!) per mostrare che l'implementazione in GNU Privacy Guard 1.2.3 era **insicura!**

TEORIA DEI GRUPPI

- Tenuto da Sandro Mattarei su base semestrale nel secondo semestre.
- E' per la Triennale.
- Molti gruppi hanno origine come insiemi di simmetrie, ovvero automorfismi, di una certa struttura matematica (figura geometrica, spazio vettoriale, spazio topologico, varietà differenziabile, struttura algebrica quale anello o campo, ecc.).
- Uno stesso gruppo può apparire come gruppo di simmetrie in contesti diversi. La teoria delle *azioni* permette di analizzare e confrontare queste varie incarnazioni di un gruppo.

TEORIA DEI GRUPPI

- Lo studio delle azioni serve anche a ricavare informazioni sulla stessa struttura interna dei gruppi. Un esempio illustrativo di varie idee e tecniche su gruppi ed azioni sarà quello dei *gruppi delle simmetrie dei solidi platonici*. Capiremo, ad esempio, cosa legghi un dodecaedro alle equazioni di quinto grado.
- Studieremo, fra l'altro, un'applicazione delle azioni a certi problemi di conteggio non risolvibili facilmente in modo diretto. Ad esempio, quanti sono i grafi distinti con un dato numero di nodi.
- Spesso la struttura di cui si studiano le simmetrie è uno spazio vettoriale, o vi si può associare uno spazio vettoriale. In un tale contesto le azioni si chiamano *rappresentazioni lineari*, che sono l'oggetto di una teoria molto ricca con tante applicazioni. Ne vedremo le basi.

COMPUTATIONAL ALGEBRA

CORSI DI
ALGEBRA

I CORSI OFFERTI

QUALCHE DETTAGLIO
SUI CORSI

LAUREA
TRIENNALE

LAUREA TRIENNALE

LAUREA
MAGISTRALE

LAUREA
MAGISTRALE IN
MATEMATICA

LAUREA
MAGISTRALE IN
INGEGNERIA DELLE
TELECOMUNICAZIONI

- Tenuto da Willem de Graaf nel primo semestre.
- E' un seguito di Teoria di Galois, ed è per la Magistrale
- L'avvento dei calcolatori ha stimolato un interesse per i *metodi effettivi*. Non ci basta più dire “esiste un vettore tale che...”. Vogliamo essere in grado di *trovare* il vettore in questione, e trovarlo *in tempo ragionevole*.
- Willem de Graaf è un vero esperto di metodi computazionali, su cui ha anche scritto un libro.

FINITE FIELDS AND SYMMETRIC CRYPTOGRAPHY

- Tenuto da Sandro Mattarei nel secondo semestre, ad anni alterni con *Discrete Fourier Analysis*. Si tiene nel 2011/12.
- Il Governo Americano ha ufficialmente adottato il sistema di crittografia simmetrica Rijndael come Advanced Encryption Standard (AES).
- AES ha una forte struttura matematica.
- Uno dei punti chiave di AES consiste nel prendere il campo finito E con $2^8 = 256$ elementi, e considerare la funzione

$$f : E \rightarrow E \quad \text{che manda} \quad x \mapsto x^{-1}$$

- Nel corso (ri)vedremo la teoria dei campi finiti, descriveremo AES, e ne proveremo la resistenza ad *attacchi crittanalitici*.

DISCRETE FOURIER ANALYSIS

- Tenuto da Sandro Mattarei ad anni alterni con *Finite Fields and Symmetric Cryptography*. Dunque nel 2012/13.
- Teoria
 - Legge di reciprocità quadratica
 - Gruppi e loro rappresentazioni
- Pratica
 - DFT: Discrete Fourier Transform
 - FFT: Fast Fourier Transform
- Applicazioni:
 - “[The FFT] also dominates the search for offshore oil.” (Terras, *Fourier Analysis on Finite Groups and Applications*, p. 151.)
 - Progetto di soffitti per sale da concerto.
 - Analisi delle coalizioni nelle votazioni alla Corte Suprema
 - Codici a correzione d'errore

CODING THEORY

- 12 crediti, laurea Magistrale, primo semestre.
- Tenuto da Max Sala.
- Riprende gli argomenti di Teoria dei Codici discussi durante la seconda unità di Algebra.
- Tratta di codici effettivamente usati in pratica: segnali ferroviari, codici nelle memorie Flash, codici nei CD. . .
- Utilizza vari strumenti algebrici, quali potenze nei campi finiti, resti quadratici, ecc., ma anche metodi al confine tra algebra e geometria, come basi di Groebner, teoria delle curve su campi finiti. . .

ALGEBRA COMPUTAZIONALE E CRITTOGRAFIA

- Per chi lo desidera, è anche possibile scegliere nell'ambito della **Laurea Triennale** un piano di studio di **Algebra Computazionale e Crittografia**
- Si suggerisce di seguire i corsi di
 - Teoria di Galois,
 - Teoria dei Numeri e Crittografia
 - Teoria dei Gruppi
- e poi un corso tratto dal Corso di Laurea in **Ingegneria della Telecomunicazioni**:
 - Comunicazioni elettriche (12 CFU)

ALGEBRA COMPUTAZIONALE, CRITTOGRAFIA, CODICI

CORSI DI
ALGEBRA

I CORSI OFFERTI

QUALCHE DETTAGLIO
SUI CORSI

LAUREA
TRIENNALE

LAUREA TRIENNALE

LAUREA
MAGISTRALE

LAUREA
MAGISTRALE IN
MATEMATICA

LAUREA
MAGISTRALE IN
INGEGNERIA DELLE
TELECOMUNICAZIONI

Corso	CFU
Computational Algebra	6
Coding Theory	12
Finite Fields and Symmetric Cryptography	6
Discrete Fourier Analysis	6
Stochastic Processes (primo modulo)	6
Un altro corso in MAT/06-09	6
Liberi	9
Lingua	3
Stage	12
Tesi	18

ALGEBRA COMPUTAZIONALE, CRITTOGRAFIA, CODICI

Si suggeriscono 36 CFU a scelta fra i seguenti:

Corso	CFU
Elliptic Curves and Cryptography	6
Integral Transforms	6
Communication systems	12
Digital signal processing	6
Multimedia signal processing and comm.	6
Data hiding	6

STAGE

- C'è la possibilità di svolgere *stage* presso aziende nel settore.
- In genere presso la stessa azienda si fa la tesi. Dunque complessivamente 30 CFU, cioè un semestre.
- Ovviamente occorre pensarci per tempo.

PROSEGUIRE A INGEGNERIA

- Al termine della Laurea triennale c'è anche la possibilità di iscriversi alla [Laurea Magistrale in Ingegneria della Telecomunicazioni](#).
- Lo hanno già fatto quattro studenti.
- I *telecomunicatori* (Ingegneri delle Telecomunicazioni) sono molto contenti di avere studenti con un forte curriculum matematico, e alla fine si è ingegneri a tutti gli effetti.
- Se siete interessati, parlatene con me, o con uno degli studenti che lo hanno già fatto.