Corsi e Piani di Studio di Algebra
A.A. 2012/13

Andrea Caranti Willem de Graaf Sandro Mattarei
Massimiliano Sala

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

Trento, 24 maggio 2012

Piano della presentazione

PIANO DELLA PRESENTAZIONE

CORSI DI ALGEBRA

CORSI DI ALGEBRA

Corso	Sem.	Docente
Teoria di Galois	2	de Graaf

CORSI DI ALGEBRA

Corso	Sem.	Docente
Teoria di Galois	2	de Graaf
Teoria Algebrica dei Numeri	2	Mattarei

CORSI DI ALGEBRA

Corso	Sem.	Docente
Teoria di Galois	2	de Graaf
Teoria Algebrica dei Numeri	2	Mattarei
Teoria dei Gruppi	N.A.	Mattarei

CORSI DI ALGEBRA

Corso	Sem.	Docente
Teoria di Galois	2	de Graaf
Teoria Algebrica dei Numeri	2	Mattarei
Teoria dei Gruppi	N.A.	Mattarei

CORSI DI ALGEBRA

Corso	Sem.	Docente
Teoria di Galois	2	de Graaf
Teoria Algebrica dei Numeri	2	Mattarei
Teoria dei Gruppi	N.A.	Mattarei
Computational Algebra	2	de Graaf

CORSI DI ALGEBRA

Corso	Sem.	Docente
Teoria di Galois	2	de Graaf
Teoria Algebrica dei Numeri	2	Mattarei
Teoria dei Gruppi	N.A.	Mattarei
Computational Algebra	2	de Graaf
Discrete Fourier Analysis	2	Mattarei

CORSI DI ALGEBRA

Corso	Sem.	Docente
Teoria di Galois	2	de Graaf
Teoria Algebrica dei Numeri	2	Mattarei
Teoria dei Gruppi	N.A.	Mattarei
Computational Algebra	2	de Graaf
Discrete Fourier Analysis	2	Mattarei
Finite Fields and Symm. Cryptography	N.A.	Mattarei

CORSI DI ALGEBRA

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

CORSI DI ALGEBRA

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

CORSI DI ALGEBRA

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

- I corsi in italiano sono per la Triennale.

CORSI DI ALGEBRA

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

- I corsi in italiano sono per la Triennale.
- I corsi in inglese sono per la Magistrale.

CORSI DI ALGEBRA

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

- I corsi in italiano sono per la Triennale.
- I corsi in inglese sono per la Magistrale.
- I corsi sono *indipendenti*.

CORSI DI ALGEBRA

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

- I corsi in italiano sono per la Triennale.
- I corsi in inglese sono per la Magistrale.
- I corsi sono *indipendenti*.
- Sono tutti da 6 CFU, tranne Coding Theory che è da 12.

CORSI DI ALGEBRA

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

- I corsi in italiano sono per la Triennale.
- I corsi 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*.

PIANO DELLA PRESENTAZIONE

TEORIA DI GALOIS

Tenuto da Willem de Graaf nel secondo semestre.

L'equazione di secondo grado

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

ha soluzioni

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

L'equazione di terzo grado

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

ha soluzioni

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

TEORIA DI GALOIS

Tenuto da Willem de Graaf nel secondo semestre.

L'equazione di secondo grado

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

ha soluzioni

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

L'equazione di terzo grado

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

ha soluzioni

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

TEORIA DI GALOIS

Tenuto da Willem de Graaf nel secondo semestre.
L'equazione di secondo grado

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

ha soluzioni

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

L'equazione di terzo grado

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

ha soluzioni

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

TEORIA DI GALOIS

Tenuto da Willem de Graaf nel secondo semestre.
L'equazione di secondo grado

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

ha soluzioni

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

L'equazione di terzo grado

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

ha soluzioni

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

TEORIA DI GALOIS

Tenuto da Willem de Graaf nel secondo semestre.
L'equazione di secondo grado

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

ha soluzioni

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

L'equazione di terzo grado

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

ha soluzioni

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

TEORIA DI GALOIS

Tenuto da Willem de Graaf nel secondo semestre.
L'equazione di secondo grado

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

ha soluzioni

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

L'equazione di terzo grado

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

ha soluzioni

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

TEORIA DI GALOIS

- Ci sono formule anche per il quarto grado.
- 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 DI GALOIS

- Ci sono formule anche per il quarto grado.
- 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 DI GALOIS

- Ci sono formule anche per il quarto grado.
- 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 DI GALOIS

- Ci sono formule anche per il quarto grado.
- 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 DI GALOIS

- Ci sono formule anche per il quarto grado.
- 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 DI GALOIS

- Ci sono formule anche per il quarto grado.
- 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 DI GALOIS

- Ci sono formule anche per il quarto grado.
- 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 GRUPPI (CHE PERÒ TACE)

- Tenuto da Sandro Mattarei nel secondo semestre.
- Gruppi importanti nascono come gruppi di simmetrie (o automorfismi) di una certa struttura matematica. Strutture di origine diversa possono anche avere lo stesso gruppo di simmetrie, o gruppi correlati.
- La teoria delle azioni permette di
  - analizzare e confrontare queste varie incarnazioni di un gruppo, ma anche
  - ricavare informazioni sulla struttura interna del gruppo.
- Fra gli esempi di applicazioni, vedremo i *gruppi di simmetrie dei solidi platonici,* scoprendo cosa lega un dodecaedro alle equazioni algebriche di quinto grado.
- Se la struttura di cui si studiano le simmetrie è anche uno spazio vettoriale, le *azioni* sono *rappresentazioni lineari*. Ne accenneremo l'inizio della teoria.

TEORIA DEI GRUPPI (CHE PERÒ TACE)

- Tenuto da Sandro Mattarei nel secondo semestre.
- Gruppi importanti nascono come gruppi di simmetrie (o automorfismi) di una certa struttura matematica. Strutture di origine diversa possono anche avere lo stesso gruppo di simmetrie, o gruppi correlati.
- La teoria delle azioni permette di
  - analizzare e confrontare queste varie incarnazioni di un gruppo, ma anche
  - ricavare informazioni sulla struttura interna del gruppo.
- Fra gli esempi di applicazioni, vedremo i *gruppi di simmetrie dei solidi platonici,* scoprendo cosa lega un dodecaedro alle equazioni algebriche di quinto grado.
- Se la struttura di cui si studiano le simmetrie è anche uno spazio vettoriale, le *azioni* sono *rappresentazioni lineari*. Ne accenneremo l'inizio della teoria.

TEORIA DEI GRUPPI (CHE PERÒ TACE)

- Tenuto da Sandro Mattarei nel secondo semestre.
- Gruppi importanti nascono come gruppi di simmetrie (o automorfismi) di una certa struttura matematica. Strutture di origine diversa possono anche avere lo stesso gruppo di simmetrie, o gruppi correlati.
- La teoria delle azioni permette di
  - analizzare e confrontare queste varie incarnazioni di un gruppo, ma anche
  - ricavare informazioni sulla struttura interna del gruppo.
- Fra gli esempi di applicazioni, vedremo i *gruppi di simmetrie dei solidi platonici,* scoprendo cosa lega un dodecaedro alle equazioni algebriche di quinto grado.
- Se la struttura di cui si studiano le simmetrie è anche uno spazio vettoriale, le *azioni* sono *rappresentazioni lineari*. Ne accenneremo l'inizio della teoria.

TEORIA DEI GRUPPI (CHE PERÒ TACE)

- Tenuto da Sandro Mattarei nel secondo semestre.
- Gruppi importanti nascono come gruppi di simmetrie (o automorfismi) di una certa struttura matematica. Strutture di origine diversa possono anche avere lo stesso gruppo di simmetrie, o gruppi correlati.
- La teoria delle azioni permette di
  - analizzare e confrontare queste varie incarnazioni di un gruppo, ma anche
  - ricavare informazioni sulla struttura interna del gruppo.
- Fra gli esempi di applicazioni, vedremo i *gruppi di simmetrie dei solidi platonici,* scoprendo cosa lega un dodecaedro alle equazioni algebriche di quinto grado.
- Se la struttura di cui si studiano le simmetrie è anche uno spazio vettoriale, le *azioni* sono *rappresentazioni lineari*. Ne accenneremo l'inizio della teoria.

TEORIA DEI GRUPPI (CHE PERÒ TACE)

- Tenuto da Sandro Mattarei nel secondo semestre.
- Gruppi importanti nascono come gruppi di simmetrie (o automorfismi) di una certa struttura matematica. Strutture di origine diversa possono anche avere lo stesso gruppo di simmetrie, o gruppi correlati.
- La teoria delle azioni permette di
  - analizzare e confrontare queste varie incarnazioni di un gruppo, ma anche
  - ricavare informazioni sulla struttura interna del gruppo.
- Fra gli esempi di applicazioni, vedremo i *gruppi di simmetrie dei solidi platonici,* scoprendo cosa lega un dodecaedro alle equazioni algebriche di quinto grado.
- Se la struttura di cui si studiano le simmetrie è anche uno spazio vettoriale, le *azioni* sono *rappresentazioni lineari*. Ne accenneremo l'inizio della teoria.

TEORIA DEI GRUPPI (CHE PERÒ TACE)

- Tenuto da Sandro Mattarei nel secondo semestre.
- Gruppi importanti nascono come gruppi di simmetrie (o automorfismi) di una certa struttura matematica. Strutture di origine diversa possono anche avere lo stesso gruppo di simmetrie, o gruppi correlati.
- La teoria delle azioni permette di
  - analizzare e confrontare queste varie incarnazioni di un gruppo, ma anche
  - ricavare informazioni sulla struttura interna del gruppo.
- Fra gli esempi di applicazioni, vedremo i *gruppi di simmetrie dei solidi platonici,* scoprendo cosa lega un dodecaedro alle equazioni algebriche di quinto grado.
- Se la struttura di cui si studiano le simmetrie è anche uno spazio vettoriale, le *azioni* sono *rappresentazioni lineari*. Ne accenneremo l'inizio della teoria.

TEORIA DEI GRUPPI (CHE PERÒ TACE)

- Tenuto da Sandro Mattarei nel secondo semestre.
- Gruppi importanti nascono come gruppi di simmetrie (o automorfismi) di una certa struttura matematica. Strutture di origine diversa possono anche avere lo stesso gruppo di simmetrie, o gruppi correlati.
- La teoria delle azioni permette di
  - analizzare e confrontare queste varie incarnazioni di un gruppo, ma anche
  - ricavare informazioni sulla struttura interna del gruppo.
- Fra gli esempi di applicazioni, vedremo i *gruppi di simmetrie dei solidi platonici,* scoprendo cosa lega un dodecaedro alle equazioni algebriche di quinto grado.
- Se la struttura di cui si studiano le simmetrie è anche uno spazio vettoriale, le *azioni* sono *rappresentazioni lineari*. Ne accenneremo l'inizio della teoria.

TEORIA ALGEBRICA DEI NUMERI

- Tenuto da Sandro Mattarei nel secondo semestre.
- Storicamente ha fra le sue motivazioni l'ambizione di dimostrare l'*Ultimo Teorema di Fermat*: per $n > 2$ non esistono interi $x, y, z \neq 0$ tali che $x^n + y^n = z^n$.
- Per $n = 2$ tutte le soluzioni si possono ottenere sfruttando la fattorizzazione unica in $\mathbf{Z}[i]$.
- In modo analogo si dimostra che non ci sono soluzioni per $n = 3, 5, 7, 11, \ldots$ ma il metodo fallisce per $n = 23$, perché in $\mathbf{Z}[e^{2\pi i/23}]$ non vale la fattorizzazione unica!
- Studieremo, in particolare,
  - gli anelli di interi algebrici nelle estensioni finite di $\mathbf{Q}$,
  - se in essi valga o meno la fattorizzazione unica,
  - una misura di quanto ci si allontani (il *class group*),
  - quali siano (gli ideal)i primi in tali anelli e come si relazionino con i primi in $\mathbf{Z}$, ...

TEORIA ALGEBRICA DEI NUMERI

- Tenuto da Sandro Mattarei nel secondo semestre.
- Storicamente ha fra le sue motivazioni l'ambizione di dimostrare l'*Ultimo Teorema di Fermat*: per $n > 2$ non esistono interi $x, y, z \neq 0$ tali che $x^n + y^n = z^n$.
- Per $n = 2$ tutte le soluzioni si possono ottenere sfruttando la fattorizzazione unica in $\mathbf{Z}[i]$.
- In modo analogo si dimostra che non ci sono soluzioni per $n = 3, 5, 7, 11, \ldots$ ma il metodo fallisce per $n = 23$, perché in $\mathbf{Z}[e^{2\pi i/23}]$ non vale la fattorizzazione unica!
- Studieremo, in particolare,
  - gli anelli di interi algebrici nelle estensioni finite di $\mathbf{Q}$,
  - se in essi valga o meno la fattorizzazione unica,
  - una misura di quanto ci si allontani (il *class group*),
  - quali siano (gli ideal)i primi in tali anelli e come si relazionino con i primi in $\mathbf{Z}$, ...

TEORIA ALGEBRICA DEI NUMERI

- Tenuto da Sandro Mattarei nel secondo semestre.
- Storicamente ha fra le sue motivazioni l'ambizione di dimostrare l'*Ultimo Teorema di Fermat*: per $n > 2$ non esistono interi $x, y, z \neq 0$ tali che $x^n + y^n = z^n$.
- Per $n = 2$ tutte le soluzioni si possono ottenere sfruttando la fattorizzazione unica in $\mathbf{Z}[i]$.
- In modo analogo si dimostra che non ci sono soluzioni per $n = 3, 5, 7, 11, \ldots$ ma il metodo fallisce per $n = 23$, perché in $\mathbf{Z}[e^{2\pi i/23}]$ non vale la fattorizzazione unica!
- Studieremo, in particolare,
  - gli anelli di interi algebrici nelle estensioni finite di $\mathbf{Q}$,
  - se in essi valga o meno la fattorizzazione unica,
  - una misura di quanto ci si allontani (il *class group*),
  - quali siano (gli ideal)i primi in tali anelli e come si relazionino con i primi in $\mathbf{Z}$, ...

TEORIA ALGEBRICA DEI NUMERI

- Tenuto da Sandro Mattarei nel secondo semestre.
- Storicamente ha fra le sue motivazioni l'ambizione di dimostrare l'*Ultimo Teorema di Fermat*: per $n > 2$ non esistono interi $x, y, z \neq 0$ tali che $x^n + y^n = z^n$.
- Per $n = 2$ tutte le soluzioni si possono ottenere sfruttando la fattorizzazione unica in $\mathbf{Z}[i]$.
- In modo analogo si dimostra che non ci sono soluzioni per $n = 3, 5, 7, 11, \ldots$ ma il metodo fallisce per $n = 23$, perché in $\mathbf{Z}[e^{2\pi i/23}]$ non vale la fattorizzazione unica!
- Studieremo, in particolare,
  - gli anelli di interi algebrici nelle estensioni finite di $\mathbf{Q}$,
  - se in essi valga o meno la fattorizzazione unica,
  - una misura di quanto ci si allontani (il *class group*),
  - quali siano (gli ideal)i primi in tali anelli e come si relazionino con i primi in $\mathbf{Z}$, ...

TEORIA ALGEBRICA DEI NUMERI

- Tenuto da Sandro Mattarei nel secondo semestre.
- Storicamente ha fra le sue motivazioni l'ambizione di dimostrare l'*Ultimo Teorema di Fermat*: per $n > 2$ non esistono interi $x, y, z \neq 0$ tali che $x^n + y^n = z^n$.
- Per $n = 2$ tutte le soluzioni si possono ottenere sfruttando la fattorizzazione unica in $\mathbf{Z}[i]$.
- In modo analogo si dimostra che non ci sono soluzioni per $n = 3, 5, 7, 11, \ldots$ ma il metodo fallisce per $n = 23$, perché in $\mathbf{Z}[e^{2\pi i/23}]$ non vale la fattorizzazione unica!
- Studieremo, in particolare,
  - gli anelli di interi algebrici nelle estensioni finite di $\mathbf{Q}$,
  - se in essi valga o meno la fattorizzazione unica,
  - una misura di quanto ci si allontani (il *class group*),
  - quali siano (gli ideal)i primi in tali anelli e come si relazionino con i primi in $\mathbf{Z}$, ...

TEORIA ALGEBRICA DEI NUMERI

- Tenuto da Sandro Mattarei nel secondo semestre.
- Storicamente ha fra le sue motivazioni l'ambizione di dimostrare l'*Ultimo Teorema di Fermat*: per $n > 2$ non esistono interi $x, y, z \neq 0$ tali che $x^n + y^n = z^n$.
- Per $n = 2$ tutte le soluzioni si possono ottenere sfruttando la fattorizzazione unica in $\mathbf{Z}[i]$.
- In modo analogo si dimostra che non ci sono soluzioni per $n = 3, 5, 7, 11, \ldots$ ma il metodo fallisce per $n = 23$, perché in $\mathbf{Z}[e^{2\pi i/23}]$ non vale la fattorizzazione unica!
- Studieremo, in particolare,
  - gli anelli di interi algebrici nelle estensioni finite di $\mathbf{Q}$,
  - se in essi valga o meno la fattorizzazione unica,
  - una misura di quanto ci si allontani (il *class group*),
  - quali siano (gli ideal)i primi in tali anelli e come si relazionino con i primi in $\mathbf{Z}$, ...

TEORIA ALGEBRICA DEI NUMERI

- Tenuto da Sandro Mattarei nel secondo semestre.
- Storicamente ha fra le sue motivazioni l'ambizione di dimostrare l'*Ultimo Teorema di Fermat*: per $n > 2$ non esistono interi $x, y, z \neq 0$ tali che $x^n + y^n = z^n$.
- Per $n = 2$ tutte le soluzioni si possono ottenere sfruttando la fattorizzazione unica in $\mathbf{Z}[i]$.
- In modo analogo si dimostra che non ci sono soluzioni per $n = 3, 5, 7, 11, \ldots$ ma il metodo fallisce per $n = 23$, perché in $\mathbf{Z}[e^{2\pi i/23}]$ non vale la fattorizzazione unica!
- Studieremo, in particolare,
  - gli anelli di interi algebrici nelle estensioni finite di $\mathbf{Q}$,
  - se in essi valga o meno la fattorizzazione unica,
  - una misura di quanto ci si allontani (il *class group*),
  - quali siano (gli ideal)i primi in tali anelli e come si relazionino con i primi in $\mathbf{Z}$, ...

TEORIA ALGEBRICA DEI NUMERI

- Tenuto da Sandro Mattarei nel secondo semestre.
- Storicamente ha fra le sue motivazioni l'ambizione di dimostrare l'*Ultimo Teorema di Fermat*: per $n > 2$ non esistono interi $x, y, z \neq 0$ tali che $x^n + y^n = z^n$.
- Per $n = 2$ tutte le soluzioni si possono ottenere sfruttando la fattorizzazione unica in $\mathbf{Z}[i]$.
- In modo analogo si dimostra che non ci sono soluzioni per $n = 3, 5, 7, 11, \ldots$ ma il metodo fallisce per $n = 23$, perché in $\mathbf{Z}[e^{2\pi i/23}]$ non vale la fattorizzazione unica!
- Studieremo, in particolare,
  - gli anelli di interi algebrici nelle estensioni finite di $\mathbf{Q}$,
  - se in essi valga o meno la fattorizzazione unica,
  - una misura di quanto ci si allontani (il *class group*),
  - quali siano (gli ideal)i primi in tali anelli e come si relazionino con i primi in $\mathbf{Z}$, ...

TEORIA ALGEBRICA DEI NUMERI

- Tenuto da Sandro Mattarei nel secondo semestre.
- Storicamente ha fra le sue motivazioni l'ambizione di dimostrare l'*Ultimo Teorema di Fermat*: per $n > 2$ non esistono interi $x, y, z \neq 0$ tali che $x^n + y^n = z^n$.
- Per $n = 2$ tutte le soluzioni si possono ottenere sfruttando la fattorizzazione unica in $\mathbf{Z}[i]$.
- In modo analogo si dimostra che non ci sono soluzioni per $n = 3, 5, 7, 11, \ldots$ ma il metodo fallisce per $n = 23$, perché in $\mathbf{Z}[e^{2\pi i/23}]$ non vale la fattorizzazione unica!
- Studieremo, in particolare,
  - gli anelli di interi algebrici nelle estensioni finite di $\mathbf{Q}$,
  - se in essi valga o meno la fattorizzazione unica,
  - una misura di quanto ci si allontani (il *class group*),
  - quali siano (gli ideal)i primi in tali anelli e come si relazionino con i primi in $\mathbf{Z}$, ...

COMPUTATIONAL ALGEBRA

- Tenuto da Willem de Graaf nel secondo 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.

COMPUTATIONAL ALGEBRA

- Tenuto da Willem de Graaf nel secondo 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.

COMPUTATIONAL ALGEBRA

- Tenuto da Willem de Graaf nel secondo 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.

COMPUTATIONAL ALGEBRA

- Tenuto da Willem de Graaf nel secondo 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.

COMPUTATIONAL ALGEBRA

- Tenuto da Willem de Graaf nel secondo 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.

COMPUTATIONAL ALGEBRA

- Tenuto da Willem de Graaf nel secondo 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.

COMPUTATIONAL ALGEBRA

- Tenuto da Willem de Graaf nel secondo 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.

COMPUTATIONAL ALGEBRA

- Tenuto da Willem de Graaf nel secondo 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*. *Non* si tiene nel 2012/13, si terrà in forma lievemente rivista nel 2013/14.

FINITE FIELDS AND SYMMETRIC CRYPTOGRAPHY

- Tenuto da Sandro Mattarei nel secondo semestre, ad anni alterni con *Discrete Fourier Analysis*. *Non* si tiene nel 2012/13, si terrà in forma lievemente rivista nel 2013/14.
- Il Governo Americano ha ufficialmente adottato il sistema di crittografia simmetrica Rijndael come Advanced Encryption Standard (AES).

FINITE FIELDS AND SYMMETRIC CRYPTOGRAPHY

- Tenuto da Sandro Mattarei nel secondo semestre, ad anni alterni con *Discrete Fourier Analysis*. *Non* si tiene nel 2012/13, si terrà in forma lievemente rivista nel 2013/14.
- Il Governo Americano ha ufficialmente adottato il sistema di crittografia simmetrica Rijndael come Advanced Encryption Standard (AES).
- AES ha una forte struttura matematica.

FINITE FIELDS AND SYMMETRIC CRYPTOGRAPHY

- Tenuto da Sandro Mattarei nel secondo semestre, ad anni alterni con *Discrete Fourier Analysis*. *Non* si tiene nel 2012/13, si terrà in forma lievemente rivista nel 2013/14.
- 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

FINITE FIELDS AND SYMMETRIC CRYPTOGRAPHY

- Tenuto da Sandro Mattarei nel secondo semestre, ad anni alterni con *Discrete Fourier Analysis*. *Non* si tiene nel 2012/13, si terrà in forma lievemente rivista nel 2013/14.
- 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

$$f : E \to E$$

FINITE FIELDS AND SYMMETRIC CRYPTOGRAPHY

- Tenuto da Sandro Mattarei nel secondo semestre, ad anni alterni con *Discrete Fourier Analysis*. *Non* si tiene nel 2012/13, si terrà in forma lievemente rivista nel 2013/14.
- 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

$$f : E \to E \qquad \text{che manda}$$

FINITE FIELDS AND SYMMETRIC CRYPTOGRAPHY

- Tenuto da Sandro Mattarei nel secondo semestre, ad anni alterni con *Discrete Fourier Analysis*. *Non* si tiene nel 2012/13, si terrà in forma lievemente rivista nel 2013/14.
- 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

$$f : E \to E \qquad \text{che manda} \qquad x \mapsto x^{-1}$$

FINITE FIELDS AND SYMMETRIC CRYPTOGRAPHY

- Tenuto da Sandro Mattarei nel secondo semestre, ad anni alterni con *Discrete Fourier Analysis*. *Non* si tiene nel 2012/13, si terrà in forma lievemente rivista nel 2013/14.
- 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

$$f : E \to E \qquad \text{che manda} \qquad x \mapsto x^{-1}$$

- 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*. Si tiene 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

DISCRETE FOURIER ANALYSIS

- Tenuto da Sandro Mattarei ad anni alterni con *Finite Fields and Symmetric Cryptography*. Si tiene 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

DISCRETE FOURIER ANALYSIS

- Tenuto da Sandro Mattarei ad anni alterni con *Finite Fields and Symmetric Cryptography*. Si tiene 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

Discrete Fourier Analysis

- Tenuto da Sandro Mattarei ad anni alterni con *Finite Fields and Symmetric Cryptography*. Si tiene 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

DISCRETE FOURIER ANALYSIS

- Tenuto da Sandro Mattarei ad anni alterni con *Finite Fields and Symmetric Cryptography*. Si tiene 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

DISCRETE FOURIER ANALYSIS

- Tenuto da Sandro Mattarei ad anni alterni con *Finite Fields and Symmetric Cryptography*. Si tiene 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

DISCRETE FOURIER ANALYSIS

- Tenuto da Sandro Mattarei ad anni alterni con *Finite Fields and Symmetric Cryptography*. Si tiene 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

Discrete Fourier Analysis

- Tenuto da Sandro Mattarei ad anni alterni con *Finite Fields and Symmetric Cryptography*. Si tiene 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

Discrete Fourier Analysis

- Tenuto da Sandro Mattarei ad anni alterni con *Finite Fields and Symmetric Cryptography*. Si tiene 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

Discrete Fourier Analysis

- Tenuto da Sandro Mattarei ad anni alterni con *Finite Fields and Symmetric Cryptography*. Si tiene 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

Discrete Fourier Analysis

- Tenuto da Sandro Mattarei ad anni alterni con *Finite Fields and Symmetric Cryptography*. Si tiene 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

Discrete Fourier Analysis

- Tenuto da Sandro Mattarei ad anni alterni con *Finite Fields and Symmetric Cryptography*. Si tiene 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

CRYPTOGRAPHY

- Un *nuovo* corso da 6 crediti, tenuto da Sala nel primo semestre.
- È un corso misto laboratorio-lezione: a ogni due ore di lezione si affiancano 2/3 ore in laboratorio, in cui si riprendono i temi.
- Gli argomenti di base trattati sono:
  - la crittografia nella teoria dell'informazione,
  - crittografia simmetrica,
  - crittografia pubblica,
  - hash function,
  - (pseudo)-randomicità,
  - approfondimento teorico: dalla crittografia a chiave pubblica a RSA e Diffie Helmann.
- La programmazione nel laboratorio sarà incentrata su tematiche attualissime, che vengono effettivamente richieste come sviluppo/ricerca all'Università dalle aziende!

CRYPTOGRAPHY

- Un *nuovo* corso da 6 crediti, tenuto da Sala nel primo semestre.
- È un corso misto laboratorio-lezione: a ogni due ore di lezione si affiancano 2/3 ore in laboratorio, in cui si riprendono i temi.
- Gli argomenti di base trattati sono:
  - la crittografia nella teoria dell'informazione,
  - crittografia simmetrica,
  - crittografia pubblica,
  - hash function,
  - (pseudo)-randomicità,
  - approfondimento teorico: dalla crittografia a chiave pubblica a RSA e Diffie Helmann.
- La programmazione nel laboratorio sarà incentrata su tematiche attualissime, che vengono effettivamente richieste come sviluppo/ricerca all'Università dalle aziende!

CRYPTOGRAPHY

- Un *nuovo* corso da 6 crediti, tenuto da Sala nel primo semestre.
- È un corso misto laboratorio-lezione: a ogni due ore di lezione si affiancano 2/3 ore in laboratorio, in cui si riprendono i temi.
- Gli argomenti di base trattati sono:
  - la crittografia nella teoria dell'informazione,
  - crittografia simmetrica,
  - crittografia pubblica,
  - hash function,
  - (pseudo)-randomicità,
  - approfondimento teorico: dalla crittografia a chiave pubblica a RSA e Diffie Helmann.
- La programmazione nel laboratorio sarà incentrata su tematiche attualissime, che vengono effettivamente richieste come sviluppo/ricerca all'Università dalle aziende!

CRYPTOGRAPHY

- Un *nuovo* corso da 6 crediti, tenuto da Sala nel primo semestre.
- È un corso misto laboratorio-lezione: a ogni due ore di lezione si affiancano 2/3 ore in laboratorio, in cui si riprendono i temi.
- Gli argomenti di base trattati sono:
  - la crittografia nella teoria dell'informazione,
  - crittografia simmetrica,
  - crittografia pubblica,
  - hash function,
  - (pseudo)-randomicità,
  - approfondimento teorico: dalla crittografia a chiave pubblica a RSA e Diffie Helmann.
- La programmazione nel laboratorio sarà incentrata su tematiche attualissime, che vengono effettivamente richieste come sviluppo/ricerca all'Università dalle aziende!

CRYPTOGRAPHY

- Un *nuovo* corso da 6 crediti, tenuto da Sala nel primo semestre.
- È un corso misto laboratorio-lezione: a ogni due ore di lezione si affiancano 2/3 ore in laboratorio, in cui si riprendono i temi.
- Gli argomenti di base trattati sono:
  - la crittografia nella teoria dell'informazione,
  - crittografia simmetrica,
  - crittografia pubblica,
  - hash function,
  - (pseudo)-randomicità,
  - approfondimento teorico: dalla crittografia a chiave pubblica a RSA e Diffie Helmann.
- La programmazione nel laboratorio sarà incentrata su tematiche attualissime, che vengono effettivamente richieste come sviluppo/ricerca all'Università dalle aziende!

CRYPTOGRAPHY

- Un *nuovo* corso da 6 crediti, tenuto da Sala nel primo semestre.
- È un corso misto laboratorio-lezione: a ogni due ore di lezione si affiancano 2/3 ore in laboratorio, in cui si riprendono i temi.
- Gli argomenti di base trattati sono:
  - la crittografia nella teoria dell'informazione,
  - crittografia simmetrica,
  - crittografia pubblica,
  - hash function,
  - (pseudo)-randomicità,
  - approfondimento teorico: dalla crittografia a chiave pubblica a RSA e Diffie Helmann.
- La programmazione nel laboratorio sarà incentrata su tematiche attualissime, che vengono effettivamente richieste come sviluppo/ricerca all'Università dalle aziende!

CRYPTOGRAPHY

- Un *nuovo* corso da 6 crediti, tenuto da Sala nel primo semestre.
- È un corso misto laboratorio-lezione: a ogni due ore di lezione si affiancano 2/3 ore in laboratorio, in cui si riprendono i temi.
- Gli argomenti di base trattati sono:
  - la crittografia nella teoria dell'informazione,
  - crittografia simmetrica,
  - crittografia pubblica,
  - hash function,
  - (pseudo)-randomicità,
  - approfondimento teorico: dalla crittografia a chiave pubblica a RSA e Diffie Helmann.
- La programmazione nel laboratorio sarà incentrata su tematiche attualissime, che vengono effettivamente richieste come sviluppo/ricerca all'Università dalle aziende!

CRYPTOGRAPHY

- Un *nuovo* corso da 6 crediti, tenuto da Sala nel primo semestre.
- È un corso misto laboratorio-lezione: a ogni due ore di lezione si affiancano 2/3 ore in laboratorio, in cui si riprendono i temi.
- Gli argomenti di base trattati sono:
  - la crittografia nella teoria dell'informazione,
  - crittografia simmetrica,
  - crittografia pubblica,
  - hash function,
  - (pseudo)-randomicità,
  - approfondimento teorico: dalla crittografia a chiave pubblica a RSA e Diffie Helmann.
- La programmazione nel laboratorio sarà incentrata su tematiche attualissime, che vengono effettivamente richieste come sviluppo/ricerca all'Università dalle aziende!

CRYPTOGRAPHY

- Un *nuovo* corso da 6 crediti, tenuto da Sala nel primo semestre.
- È un corso misto laboratorio-lezione: a ogni due ore di lezione si affiancano 2/3 ore in laboratorio, in cui si riprendono i temi.
- Gli argomenti di base trattati sono:
  - la crittografia nella teoria dell'informazione,
  - crittografia simmetrica,
  - crittografia pubblica,
  - hash function,
  - (pseudo)-randomicità,
  - approfondimento teorico: dalla crittografia a chiave pubblica a RSA e Diffie Helmann.
- La programmazione nel laboratorio sarà incentrata su tematiche attualissime, che vengono effettivamente richieste come sviluppo/ricerca all'Università dalle aziende!

CRYPTOGRAPHY

- Un *nuovo* corso da 6 crediti, tenuto da Sala nel primo semestre.
- È un corso misto laboratorio-lezione: a ogni due ore di lezione si affiancano 2/3 ore in laboratorio, in cui si riprendono i temi.
- Gli argomenti di base trattati sono:
  - la crittografia nella teoria dell'informazione,
  - crittografia simmetrica,
  - crittografia pubblica,
  - hash function,
  - (pseudo)-randomicità,
  - approfondimento teorico: dalla crittografia a chiave pubblica a RSA e Diffie Helmann.
- La programmazione nel laboratorio sarà incentrata su tematiche attualissime, che vengono effettivamente richieste come sviluppo/ricerca all'Università dalle aziende!

CRYPTOGRAPHY

- Un *nuovo* corso da 6 crediti, tenuto da Sala nel primo semestre.
- È un corso misto laboratorio-lezione: a ogni due ore di lezione si affiancano 2/3 ore in laboratorio, in cui si riprendono i temi.
- Gli argomenti di base trattati sono:
  - la crittografia nella teoria dell'informazione,
  - crittografia simmetrica,
  - crittografia pubblica,
  - hash function,
  - (pseudo)-randomicità,
  - approfondimento teorico: dalla crittografia a chiave pubblica a RSA e Diffie Helmann.
- La programmazione nel laboratorio sarà incentrata su tematiche attualissime, che vengono effettivamente richieste come sviluppo/ricerca all'Università dalle aziende!

CRYPTOGRAPHY

- Un *nuovo* corso da 6 crediti, tenuto da Sala nel primo semestre.
- È un corso misto laboratorio-lezione: a ogni due ore di lezione si affiancano 2/3 ore in laboratorio, in cui si riprendono i temi.
- Gli argomenti di base trattati sono:
  - la crittografia nella teoria dell'informazione,
  - crittografia simmetrica,
  - crittografia pubblica,
  - hash function,
  - (pseudo)-randomicità,
  - approfondimento teorico: dalla crittografia a chiave pubblica a RSA e Diffie Helmann.
- La programmazione nel laboratorio sarà incentrata su tematiche attualissime, che vengono effettivamente richieste come sviluppo/ricerca all'Università dalle aziende!

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...

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...

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...

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...

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...

PIANO DELLA PRESENTAZIONE

I CORSI

- I corsi di algebra disponibili sono
  - Teoria di Galois,
  - Teoria dei Numeri e Crittografia
  - (Teoria dei Gruppi)
- e poi se si ha intenzione di proseguire nella Laurea Magistrale si consiglia un corso tratto dal Corso di Laurea in *Ingegneria della Telecomunicazioni:*
  - Comunicazioni elettriche (12 CFU)

I CORSI

- I corsi di algebra disponibili sono
  - Teoria di Galois,
  - Teoria dei Numeri e Crittografia
  - (Teoria dei Gruppi)
- e poi se si ha intenzione di proseguire nella Laurea Magistrale si consiglia un corso tratto dal Corso di Laurea in *Ingegneria della Telecomunicazioni:*
  - Comunicazioni elettriche (12 CFU)

I CORSI

- I corsi di algebra disponibili sono
  - Teoria di Galois,
  - Teoria dei Numeri e Crittografia
  - (Teoria dei Gruppi)
- e poi se si ha intenzione di proseguire nella Laurea Magistrale si consiglia un corso tratto dal Corso di Laurea in *Ingegneria della Telecomunicazioni:*
  - Comunicazioni elettriche (12 CFU)

I CORSI

- I corsi di algebra disponibili sono
  - Teoria di Galois,
  - Teoria dei Numeri e Crittografia
  - (Teoria dei Gruppi)
- e poi se si ha intenzione di proseguire nella Laurea Magistrale si consiglia un corso tratto dal Corso di Laurea in *Ingegneria della Telecomunicazioni:*
  - Comunicazioni elettriche (12 CFU)

I CORSI

- I corsi di algebra disponibili sono
  - Teoria di Galois,
  - Teoria dei Numeri e Crittografia
  - (Teoria dei Gruppi)
- e poi se si ha intenzione di proseguire nella Laurea Magistrale si consiglia un corso tratto dal Corso di Laurea in *Ingegneria della Telecomunicazioni:*
  - Comunicazioni elettriche (12 CFU)

I CORSI

- I corsi di algebra disponibili sono
  - Teoria di Galois,
  - Teoria dei Numeri e Crittografia
  - (Teoria dei Gruppi)
- e poi se si ha intenzione di proseguire nella Laurea Magistrale si consiglia un corso tratto dal Corso di Laurea in *Ingegneria della Telecomunicazioni:*
  - Comunicazioni elettriche (12 CFU)

Piano della presentazione

ALGEBRA COMPUTAZIONALE, CRITTOGRAFIA, CODICI

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 fra i corsi seguenti.

Corso	**CFU**
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 azienza si fa la tesi. Dunque complessivamente 30 CFU, cioè un semestre.
- Ovviamente occorre pensarci per tempo.

STAGE

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

STAGE

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

STAGE

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

RIASSUMENDO

Laurea Triennale

- Si possono scegliere questi corsi:
  - Teoria di Galois
  - Teoria Algebrica dei Numeri
  - (Teoria dei Gruppi)

Laurea Magistrale

- Si può scegliere di proseguire con l'orientamento di *Computational Algebra, Cryptography, Coding Theory*.
- O comunque scegliere a piacere fra i corsi di
  - Computational Algebra
  - Discrete Fourier Analysis
  - (Finite Fields and Symmetric Cryptography)
  - Coding Theory

RIASSUMENDO

Laurea Triennale

- Si possono scegliere questi corsi:
  - Teoria di Galois
  - Teoria Algebrica dei Numeri
  - (Teoria dei Gruppi)

Laurea Magistrale

- Si può scegliere di proseguire con l'orientamento di *Computational Algebra, Cryptography, Coding Theory*.
- O comunque scegliere a piacere fra i corsi di
  - Computational Algebra
  - Discrete Fourier Analysis
  - (Finite Fields and Symmetric Cryptography)
  - Coding Theory

RIASSUMENDO

Laurea Triennale

- Si possono scegliere questi corsi:
  - Teoria di Galois
  - Teoria Algebrica dei Numeri
  - (Teoria dei Gruppi)

Laurea Magistrale

- Si può scegliere di proseguire con l'orientamento di *Computational Algebra, Cryptography, Coding Theory*.
- O comunque scegliere a piacere fra i corsi di
  - Computational Algebra
  - Discrete Fourier Analysis
  - (Finite Fields and Symmetric Cryptography)
  - Coding Theory

RIASSUMENDO

Laurea Triennale

- Si possono scegliere questi corsi:
  - Teoria di Galois
  - Teoria Algebrica dei Numeri
  - (Teoria dei Gruppi)

Laurea Magistrale

- Si può scegliere di proseguire con l'orientamento di *Computational Algebra, Cryptography, Coding Theory*.
- O comunque scegliere a piacere fra i corsi di
  - Computational Algebra
  - Discrete Fourier Analysis
  - (Finite Fields and Symmetric Cryptography)
  - Coding Theory

RIASSUMENDO

Laurea Triennale

- Si possono scegliere questi corsi:
  - Teoria di Galois
  - Teoria Algebrica dei Numeri
  - (Teoria dei Gruppi)

Laurea Magistrale

- Si può scegliere di proseguire con l'orientamento di *Computational Algebra, Cryptography, Coding Theory*.
- O comunque scegliere a piacere fra i corsi di
  - Computational Algebra
  - Discrete Fourier Analysis
  - (Finite Fields and Symmetric Cryptography)
  - Coding Theory

RIASSUMENDO

Laurea Triennale

- Si possono scegliere questi corsi:
  - Teoria di Galois
  - Teoria Algebrica dei Numeri
  - (Teoria dei Gruppi)

Laurea Magistrale

- Si può scegliere di proseguire con l'orientamento di *Computational Algebra, Cryptography, Coding Theory*.
- O comunque scegliere a piacere fra i corsi di
  - Computational Algebra
  - Discrete Fourier Analysis
  - (Finite Fields and Symmetric Cryptography)
  - Coding Theory

RIASSUMENDO

Laurea Triennale

- Si possono scegliere questi corsi:
  - Teoria di Galois
  - Teoria Algebrica dei Numeri
  - (Teoria dei Gruppi)

Laurea Magistrale

- Si può scegliere di proseguire con l'orientamento di *Computational Algebra, Cryptography, Coding Theory*.
- O comunque scegliere a piacere fra i corsi di
  - Computational Algebra
  - Discrete Fourier Analysis
  - (Finite Fields and Symmetric Cryptography)
  - Coding Theory

RIASSUMENDO

Laurea Triennale

- Si possono scegliere questi corsi:
  - Teoria di Galois
  - Teoria Algebrica dei Numeri
  - (Teoria dei Gruppi)

Laurea Magistrale

- Si può scegliere di proseguire con l'orientamento di *Computational Algebra, Cryptography, Coding Theory*.
- O comunque scegliere a piacere fra i corsi di
  - Computational Algebra
  - Discrete Fourier Analysis
  - (Finite Fields and Symmetric Cryptography)
  - Coding Theory

RIASSUMENDO

Laurea Triennale

- Si possono scegliere questi corsi:
  - Teoria di Galois
  - Teoria Algebrica dei Numeri
  - (Teoria dei Gruppi)

Laurea Magistrale

- Si può scegliere di proseguire con l'orientamento di *Computational Algebra, Cryptography, Coding Theory*.
- O comunque scegliere a piacere fra i corsi di
  - Computational Algebra
  - Discrete Fourier Analysis
  - (Finite Fields and Symmetric Cryptography)
  - Coding Theory

RIASSUMENDO

Laurea Triennale

- Si possono scegliere questi corsi:
  - Teoria di Galois
  - Teoria Algebrica dei Numeri
  - (Teoria dei Gruppi)

Laurea Magistrale

- Si può scegliere di proseguire con l'orientamento di *Computational Algebra, Cryptography, Coding Theory*.
- O comunque scegliere a piacere fra i corsi di
  - Computational Algebra
  - Discrete Fourier Analysis
  - (Finite Fields and Symmetric Cryptography)
  - Coding Theory

RIASSUMENDO

Laurea Triennale

- Si possono scegliere questi corsi:
  - Teoria di Galois
  - Teoria Algebrica dei Numeri
  - (Teoria dei Gruppi)

Laurea Magistrale

- Si può scegliere di proseguire con l'orientamento di *Computational Algebra, Cryptography, Coding Theory*.
- O comunque scegliere a piacere fra i corsi di
  - Computational Algebra
  - Discrete Fourier Analysis
  - (Finite Fields and Symmetric Cryptography)
  - Coding Theory

RIASSUMENDO

Laurea Triennale

- Si possono scegliere questi corsi:
  - Teoria di Galois
  - Teoria Algebrica dei Numeri
  - (Teoria dei Gruppi)

Laurea Magistrale

- Si può scegliere di proseguire con l'orientamento di *Computational Algebra, Cryptography, Coding Theory*.
- O comunque scegliere a piacere fra i corsi di
  - Computational Algebra
  - Discrete Fourier Analysis
  - (Finite Fields and Symmetric Cryptography)
  - Coding Theory