

# DIARIO DELL'UNITÀ DIDATTICA DI CAMPI FINITI E CRITTOGRAFIA SIMMETRICA

A.A. 2008/09

DOCENTE: ANDREA CARANTI

## LEZIONE 1. LUNEDÌ 3 NOVEMBRE 2008 (2 ORE)

Campo dei quozienti di un dominio. Numeri razionali, funzioni razionali.

Caratteristica di un anello con unità. Caratteristica zero: se i multipli dell'unità sono distinti fra loro, allora l'anello contiene  $\mathbf{Z}$ , e se è un campo contiene  $\mathbf{Q}$ .

Caso in cui i multipli dell'unità non sono distinti.

Caratteristica positiva  $t$ : l'anello contiene  $\mathbf{Z}/t\mathbf{Z}$ . Se l'anello è un dominio,  $t$  è un numero primo, dunque il dominio contiene il campo  $\mathbf{F}_t = \mathbf{Z}/t\mathbf{Z}$ .

## LEZIONE 2. MARTEDÌ 4 NOVEMBRE 2008 (2 ORE)

Un dominio finito è un campo. Cenno al teorema di Wedderburn.

Un campo finito  $E$  contiene un campo  $\mathbf{F}_p$ , con  $p$  primo, e se ha grado  $n$  su di esso, allora  $|E| = p^n$ . Il campo di ordine  $p^n$  è il campo di spezzamento di  $x^{p^n} - x$  su  $\mathbf{F}_p$ .

Definizione alternativa della funzione di Eulero.

## LEZIONE 3. MERCOLEDÌ 5 NOVEMBRE 2008 (2 ORE)

La funzione definita mediante  $\sum_{d|n} \varphi(d) = n$  è proprio la funzione di Eulero.

Numero di elementi di ordine  $n$  in un gruppo ciclico di ordine  $n$ . Un gruppo ciclico di ordine  $n$  ha uno e un solo sottogruppo di ordine  $d$ , per ogni divisore  $d$  di  $n$ , e questo sottogruppo è ciclico. Numero di elementi di ordine  $d$  in un gruppo ciclico di ordine  $n$ . Ne segue di nuovo la formula  $\sum_{d|n} \varphi(d) = n$ .

Il gruppo moltiplicativo di un campo finito è ciclico. Un campo finito di caratteristica  $p$  è estensione semplice di  $\mathbf{F}_p$ . Dunque su  $\mathbf{F}_p$  ci sono polinomi irriducibili di ogni grado.

Il gruppo di Galois  $\text{Gal}(E/\mathbf{F}_p)$  è ciclico, generato dall'isomorfismo di Frobenius.

## LEZIONE 4. LUNEDÌ 10 NOVEMBRE 2008 (2 ORE)

Corrispondenza di Galois e sottocampi di un campo finito. Approccio elementare.

Il polinomio  $x^{p^n} - x$  è il prodotto di tutti i polinomi monici irriducibili in  $\mathbf{F}_p[x]$  di grado un divisore di  $n$ .

Funzione di Moebius: formula definitoria, esistenza e unicità, formula in termini di una fattorizzazione.

Prodotto di convoluzione: polinomi.

## LEZIONE 5. MARTEDÍ 11 NOVEMBRE 2008 (2 ORE)

Prodotto di convoluzione: polinomi.

Formula di inversione di Moebius. Applicazione: la funzione di Eulero.

Numero di polinomi irriducibili di dato grado sul campo con un numero primo di elementi. Inclusione-esclusione.

## LEZIONE 6. MERCOLEDÍ 12 NOVEMBRE 2008 (2 ORE)

Ancora su inclusione-esclusione. Numero di polinomi primitivi.

Un sottogruppo moltiplicativo finito di un campo è ciclico.

Su ogni campo finito ci sono polinomi irriducibili di grado qualsiasi.

Crittografia simmetrica: lo schema di Shannon.

## LEZIONE 7. LUNEDÍ 17 NOVEMBRE 2008 (2 ORE)

Cifrari classici: Cesare, Vigenere. One-time pad.

Analisi delle frequenze.

Schema generale di AES.

## LEZIONE 8. MARTEDÍ 18 NOVEMBRE 2008 (2 ORE)

Funzioni lineari ed affini. Gruppo diedrale: il prodotto di due involuzioni può avere periodo arbitrario.

## LEZIONE 9. MERCOLEDÍ 19 NOVEMBRE 2008 (2 ORE)

Crittanalisi chosen plaintext e given plaintext delle funzioni lineari ed affini. Crittanalisi differenziale. Eulero-Mascheroni.

Funzioni lineari su un campo finito, duale.

## LEZIONE 10. LUNEDÍ 24 NOVEMBRE 2008 (2 ORE)

La traccia. Di nuovo le funzioni lineari su un campo finito.

Distanza di due funzioni booleane. Correlazione. Distanza dalle funzioni affini.

Funzioni cappuccio. Prodotto hermitiano.

## LEZIONE 11. MARTEDÍ 25 NOVEMBRE 2008 (2 ORE)

Le parità formano un sistema ortonormale.

## LEZIONE 12. MERCOLEDÍ 26 NOVEMBRE 2008 (2 ORE)

Eguaglianza di Parseval. Distanza dell'inversione dalle funzioni affini.

## LEZIONE 13. LUNEDÍ 1 DICEMBRE 2008 (2 ORE)

Il polinomio di AES: irriducibilità.

Codici lineari. Singleton bound.

## LEZIONE 14. MARTEDÍ 2 DICEMBRE 2008 (2 ORE)

Codici lineari. Matrice generatrice e matrice di controllo di parità. Distanza minima in termini di colonne linearmente indipendenti di quest'ultima.

Codici Reed-Solomon. Il codice usato in AES.

## LEZIONE 15. MERCOLEDÍ 3 DICEMBRE 2008 (2 ORE)

Codici Reed-Solomon. Il codice usato in AES.

AES: inizio.

## LEZIONE 16. MARTEDÍ 9 DICEMBRE 2008 (2 ORE)

AES: descrizione delle componenti.

Crittanalisi della Big Bad Box.

## LEZIONE 17. MERCOLEDÍ 10 DICEMBRE 2008 (2 ORE)

Crittanalisi differenziale e AES: il comportamento dell'inversione.

## LEZIONE 18. LUNEDÍ 15 DICEMBRE 2008 (2 ORE)

Crittanalisi differenziale troncata.

Crittanalisi differenziale di AES.

## LEZIONE 19. MARTEDÍ 16 DICEMBRE 2008 (2 ORE)

Valutazione della didattica.

Il teorema delle 25 S-box attive su 4 rounds, per la resistenza di AES alla crittanalisi differenziale.

## LEZIONE 20. MERCOLEDÍ 17 DICEMBRE 2008 (2 ORE)

AES non ha backdoors basate sulla crittanalisi differenziale troncata.

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DEGLI STUDI DI TRENTO, VIA SOMMARIVE  
14, 38050 POVO (TRENTO)

*E-mail address:* caranti@science.unitn.it