

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

A.A. 2007/08

DOCENTE: ANDREA CARANTI

LEZIONE 1. LUNEDÌ 5 NOVEMBRE 2007 (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.

LEZIONE 2. MARTEDÌ 6 NOVEMBRE 2007 (2 ORE)

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 $\mathbf{F}_t = \mathbf{Z}/t\mathbf{Z}$.

Un dominio finito contiene 1, ed 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 .

Un sottogruppo moltiplicativo finito di un campo è ciclico. (Inizio.)

LEZIONE 3. MERCOLEDÌ 7 NOVEMBRE 2007 (2 ORE)

Un sottogruppo moltiplicativo finito di un campo è ciclico.

I campi finiti sono estensioni semplici del campo con p elementi. Costruzione mediante un polinomio irriducibile.

Gruppo di Galois di un campo finito.

LEZIONE 4. LUNEDÌ 12 NOVEMBRE 2007 (2 ORE)

Corrispondenza di Galois: un campo di ordine p^n contiene un campo di ordine p^d se e solo se d divide n . Metodo elementare: $x^{p^d} - x$ divide $x^{p^n} - x$ se e solo se d divide n .

$x^{p^n} - x$ è il prodotto di tutti i polinomi monici e irriducibili di grado un divisore di n .

Funzione di Moebius: definizione ricorsiva, esistenza, unicità e proprietà moltiplicativa.

LEZIONE 5. MARTEDÌ 13 NOVEMBRE 2007 (2 ORE)

Convoluzioni e polinomi. Formula di inversione di Moebius. Applicazioni: la funzione di Eulero, il numero di polinomi irriducibili di grado dato su un campo finito. Interpretazione mediante prodotti e inversi di $x^{p^n} - x$. Inclusione-esclusione.

LEZIONE 6. MERCOLEDÌ 14 NOVEMBRE 2007 (2 ORE)

Ancora inclusione-esclusione: prodotto dei polinomi irriducibili di grado dato su un campo finito.

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

LEZIONE 7. LUNEDÌ 19 NOVEMBRE 2007 (2 ORE)

Un esempio di decifrazione di un testo crittato mediante una permutazione delle lettere.

Cifrari a chiave privata: lo schema di Shannon. Il polinomio di Rijndael.

LEZIONE 8. MARTEDÌ 20 NOVEMBRE 2007 (2 ORE)

Ancora sulla decifrazione di un testo crittato mediante permutazione.

Il polinomio di Rijndael è irriducibile.

Funzioni lineari: crittanalisi chosen plaintext e given plaintext. Probabilità di trovare una base in una successione casuale di vettori.

LEZIONE 9. MERCOLEDÌ 21 NOVEMBRE 2007 (2 ORE)

Funzioni affini: crittanalisi chosen plaintext e given plaintext. Gruppi diedrali: il prodotto di due elementi di ordine 2 può avere ordine arbitrario.

LEZIONE 10. LUNEDÌ 26 NOVEMBRE 2007 (2 ORE)

Funzioni booleane: *value vector*. Distanza di due funzioni booleane, correlazione. Funzioni cappuccio. Prodotto scalare (Hermitiano) di funzioni a valori complessi, definite su $V = \mathbf{F}_2^n$. Relazione con la correlazione. Minima distanza di una funzione booleana dalle funzioni affini.

LEZIONE 11. MARTEDÌ 27 NOVEMBRE 2007 (2 ORE)

Le parità sono un sistema ortonormale. Trasformata di Walsh. Formula di Parseval, e minorazione per il massimo della correlazione con una funzione affine.

LEZIONE 12. MERCOLEDÌ 28 NOVEMBRE 2007 (2 ORE)

Funzioni lineari su un campo finito, e da un campo finito nel campo primo. Traccia. Nonlinearità dell'inversione.

LEZIONE 13. LUNEDÌ 3 DICEMBRE 2007 (2 ORE)

Crittanalisi differenziale troncata. Sifting per verificare che un vettore sta in un sottospazio. Riduzione della complessità della forza bruta se si sa che la trasformazione rispetta la relazione che definisce le classi laterali rispetto a un sottospazio. Distribuzione delle differenze rispetto a una trasformazione non lineare.

LEZIONE 14. MARTEDÍ 4 DICEMBRE 2007 (2 ORE)

Ancora sulla riduzione della complessità.

Comportamento dell'inversione rispetto alla differenze. Equazioni di secondo grado in caratteristica due.

Codici lineari.

LEZIONE 15. MERCOLEDÍ 5 DICEMBRE 2007 (2 ORE)

Distanza per codici lineari e singleton bound. Codici Reed-Solomon. Matrici circolanti. Il codice usato da Rijndael.

LEZIONE 16. LUNEDÍ 10 DICEMBRE 2007 (2 ORE)

Matrici circolanti in caratteristica zero. Il codice usato da Rijndael ha distanza 5: tutti i minori di una certa matrice 4×4 sono diversi da zero. (Per quelli 3×3 si guarda l'inversa.) Dunque il codice ha distanza cinque, e corregge due errori a livello di bytes, e fino a nove consecutivi a livello di bits.

Big Bad Box.

LEZIONE 17. MARTEDÍ 11 DICEMBRE 2007 (2 ORE)

Crittanalisi della Big Bad Box. Interpolation attacks. Lo stato di AES. Bytes e words. Key schedule. AES ridotto a `SubBytes` e `AddRoundKey`: si può decrittare byte per byte. `ShiftRows` e `MixColumns`. Differenze.

LEZIONE 18. MERCOLEDÍ 12 DICEMBRE 2007 (2 ORE)

Valutazione della didattica.

Paradigma della crittanalisi differenziale.

Il passaggio critico per le differenze è `SubBytes`.

Un esempio di quattro rounds con 25 S-box attive.

LEZIONE 19. LUNEDÍ 17 DICEMBRE 2007 (2 ORE)

La strategia *wide trail* per quanto riguarda la crittanalisi differenziale e lineare.

LEZIONE 20. MARTEDÍ 18 DICEMBRE 2007 (2 ORE)

Il teorema del 25 sul numero di S-box attive su 4 round.

Una proprietà di AES rispetto alla crittanalisi differenziale troncata.

LEZIONE 21. MERCOLEDÍ 19 DICEMBRE 2007 (1 ORA)

I sottospazi di un campo finito di caratteristica due, chiusi rispetto all'inversione, sono sottoanelli, e dunque sottocampi.

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

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