

DIARIO DEL CORSO DI TEORIA DEI NUMERI E CRITTOGRAFIA

SANDRO MATTAREI

A.A. 2008/09

(42 ore complessive di lezione)

PRIMA SETTIMANA. LEZIONE DI MARTEDÍ 17 FEBBRAIO 2009 (DUE ORE)

Rappresentazione di numeri interi, razionali e reali rispetto a una base arbitraria b .

Conversione da base b a base 10. Conversione da base 10 a base b .

Numeri periodici in base b . Caratterizzazione del periodo.

LEZIONE DI MERCOLEDÍ 18 FEBBRAIO 2009 (DUE ORE)

Complessità computazionale: operazioni bit.

Complessità (computazionale) dell'addizione (e della sottrazione) e della moltiplicazione.

La notazione “ O maiuscola”. Algoritmi a tempo polinomiale e non.

Un algoritmo piú rapido per la moltiplicazione. Cenno alla *Fast Fourier Transform*.

Complessità della divisione con resto. Complessità della conversione fra basi diverse.

SECONDA SETTIMANA. LEZIONE DI MARTEDÍ 24 FEBBRAIO 2009 (DUE ORE)

Complessità del calcolo del fattoriale (e cenno all'approssimazione di Stirling).

L'algoritmo di Euclide e la sua complessità.

LEZIONE DI MERCOLEDÍ 25 FEBBRAIO 2009 (DUE ORE)

L'algoritmo di Euclide esteso, nelle diverse varianti, e la sua complessità. Precisione della costante nella stima; i numeri di Fibonacci. Studio degli interi u e v tali che $au + bv = (a, b)$. Interpretazioni geometriche.

TERZA SETTIMANA. LEZIONE DI MARTEDÍ 3 MARZO 2009 (DUE ORE)

Gli invertibili nell'anello degli interi modulo m . Calcolo di inversi modulo m e risoluzione di congruenze. Loro complessità.

La funzione di Eulero e come si calcola.

Ripasso di teoria dei gruppi: i sottogruppi (e gli ideali) di \mathbb{Z} ; laterali e teorema di Lagrange; gruppo quoziente.

Date: Versione finale, 3 aprile 2009.

LEZIONE DI GIOVEDÌ 5 MARZO 2009 (TRE ORE)

Ripasso di teoria degli anelli: ideali e anello quoziente; il teorema fondamentale sugli omomorfismi (o primo teorema sugli omomorfismi); il teorema di corrispondenza (o secondo teorema sugli omomorfismi, o talvolta anche terzo).

Elementi invertibili e ideali massimali. Anelli locali.

Il Teorema cinese dei resti. Dimostrazione non costruttiva (mediante il lemma dei cassetti) e dimostrazione costruttiva. Risoluzione di sistemi di congruenze.

Equivalenza computazionale fra la fattorizzazione di $n = pq$ ed il calcolo della sua funzione di Eulero.

Algoritmo di Bombelli per estrarre le radici quadrate di numeri interi o reali (quello imparato alla scuola media), e sua complessità.

LEZIONE DI VENERDÌ 6 MARZO 2009 (DUE ORE)

Complessità della fattorizzazione negli interi usando il metodo delle divisioni per tentativi, in diverse varianti. Confronto con le complessità dei metodi moderni. Enunciato del teorema dei numeri primi.

Il Teorema di Eulero-Fermat. Il Piccolo Teorema di Fermat (con tre dimostrazioni: con i gruppi, per induzione, combinatoria con le “collane di perline”).

Rafforzamento del teorema di Eulero Fermat, nel caso speciale in cui $n = pq$. Esponente di un gruppo. La funzione di Carmichael.

QUARTA SETTIMANA. LEZIONE DI LUNEDÌ 9 MARZO 2009 (DUE ORE)

Teorema di Dirichlet sui primi contenuti in una progressione aritmetica (enunciati). Densità di un insieme di numeri naturali in uno che lo contiene.

Dimostrazione elementare dell'esistenza di infiniti primi $\not\equiv 1 \pmod{m}$.

Ordine di una potenza in un gruppo. Generatori ed automorfismi di un gruppo ciclico.

Applicazione del teorema di Dirichlet al numero di generatori (del gruppo moltiplicativo) di un campo con p elementi.

Divisori primi di numeri della forma $a^n - 1$.

LEZIONE DI MARTEDÌ 10 MARZO 2009 (DUE ORE)

Esempio di fattorizzazione di numeri della forma $a^n - 1$. Primi di Mersenne e di Fermat.

Divisori primi di numeri della forma $1 + a + a^2 + \dots + a^{q-1}$. Caso speciale del teorema di Dirichlet: per q primo, esistono infiniti primi $\equiv 1 \pmod{q}$.

La formula $\sum_{d|n} \varphi(d) = n$. Ogni sottogruppo moltiplicativo finito di un campo è ciclico.

LEZIONE DI MERCOLEDÌ 11 MARZO 2009 (DUE ORE)

Generatori di un campo finito. Esempi. La congettura di Artin.

Ordine del prodotto di due elementi in un gruppo: se essi commutano e hanno ordini coprimi, allora il loro prodotto ha ordine il prodotto degli ordini.

QUINTA SETTIMANA. LEZIONE DI MARTEDÍ 17 MARZO 2009 (DUE ORE)

La crittografia in generale. Esempi di crittografia a chiave segreta: mappe affini su $\mathbb{Z}/N\mathbb{Z}$. Analisi di frequenza.

Altri esempi di crittografia a chiave segreta: mappe affini su $\mathbb{Z}/N^k\mathbb{Z}$; mappe affini su $(\mathbb{Z}/N\mathbb{Z})^k$; elevamento a potenza in un campo finito.

Firme autenticate.

LEZIONE DI GIOVEDÍ 19 MARZO 2009 (TRE ORE)

Il metodo RSA. Generalizzazione del teorema di Eulero-Fermat nel caso in cui n è libero da quadrati. Sua falsità altrimenti.

Varie osservazioni sul metodo RSA, fra cui: necessità di avere $\mathcal{P} \neq \mathcal{C}$; basta che le chiavi e e d siano inverse modulo $[p-1, q-1]$.

Rischi connessi all'uso del Teorema cinese dei resti nell'implementazione della firma RSA in una smartcard.

Firme autenticate nel metodo RSA.

Calcolo di potenze modulo m , complessità dei vari metodi. L'algoritmo "eleva al quadrato e moltiplica".

Un gruppo abeliano di ordine mn , con $(m, n) = 1$, è prodotto diretto (interno) di un sottogruppo di ordine m ed uno di ordine n . Risultato piú generale sull'ordine del prodotto di due elementi in un gruppo.

LEZIONE DI VENERDÍ 19 MARZO 2009 (DUE ORE)

La struttura di $U(\mathbb{Z}/n\mathbb{Z})$: riduzione al caso $n = p^\alpha$.

Se p è un primo dispari, $1+p$ ha ordine $p^{\alpha-1}$ modulo p^α . Il numero 5 ha ordine $2^{\alpha-2}$ modulo 2^α .

SESTA SETTIMANA. LEZIONE DI MARTEDÍ 24 MARZO 2009 (DUE ORE)

Il gruppo $U(\mathbb{Z}/p^\alpha\mathbb{Z})$ è ciclico se $p > 2$, mentre è prodotto diretto di due gruppi ciclici, di ordini 2 e $2^{\alpha-2}$, se $p = 2$.

Se un intero g è un generatore modulo p , allora almeno uno fra g e $g(1+p)$ (o, equivalentemente, uno fra g e $g+p$) è una radice primitiva modulo p^α . Se g è una radice primitiva modulo p^2 allora è anche una radice primitiva modulo p^α per ogni α .

LEZIONE DI GIOVEDÍ 26 MARZO 2009 (TRE ORE)

Una migliore garanzia di sicurezza del metodo RSA: algoritmo (probabilistico) per fattorizzare $n = pq$ conoscendo un multiplo di $[p-1, q-1]$.

Il logaritmo discreto. Lo scambio di chiavi di Diffie-Hellmann.

Il metodo di Massey-Omura. Il metodo di El-Gamal.

LEZIONE DI VENERDÍ 27 MARZO 2009 (DUE ORE)

Algoritmo di Silver-Pohlig-Hellman per il calcolo del logaritmo discreto in un campo finito.

SETTIMA SETTIMANA. LEZIONE DI MARTEDÍ 31 MARZO 2009 (DUE ORE)

Resti quadratici modulo p . Esempi di grafi della mappa elevamento al quadrato modulo p . Simbolo di Legendre. La caratterizzazione di Eulero. La formula per il simbolo di Legendre $\left(\frac{2}{p}\right)$ (senza dimostrazione).

Algoritmo di Tonelli e Shanks per l'estrazione di radici quadrate modulo p (inizio).

LEZIONE DI GIOVEDÍ 2 APRILE 2009 (TRE ORE)

Algoritmo di Tonelli e Shanks per l'estrazione di radici quadrate modulo p (conclusione).

Test di primalità (probabilistici). Pseudoprimi. Numeri di Carmichael e loro caratterizzazione.

Pseudoprimi forti e test di Miller-Rabin. Conseguenza: nel metodo RSA $p - 1$ e $q - 1$ non devono avere un fattore comune grande.

LEZIONE DI VENERDÍ 3 APRILE 2009 (DUE ORE)

Numeri smooth e powersmooth. Fattorizzazione: il metodo $p - 1$ di Pollard. Conseguenza: nel metodo RSA ciascuno fra $p - 1$ e $q - 1$ deve avere almeno un fattore primo grande.