

# DIARIO DEL CORSO DI ALGEBRA

A.A. 2010/11

DOCENTE: ANDREA CARANTI

## LEZIONE 1. MERCOLEDÍ 15 SETTEMBRE 2010 (2 ORE)

Presentazione del corso.

Esercizio: cosa succede a moltiplicare per  $2, 3, 4, \dots$  il numero

$052631578947368421$ ,

e perché?

Divisibilità fra interi. Proprietà riflessiva e transitiva. Non vale la proprietà simmetrica. Determinazione delle coppie  $(a, b)$  tali che  $a$  divide  $b$  e  $b$  divide  $a$ .

Divisione con resto non negativo. Unicità di quoziente e resto.

## LEZIONE 2. GIOVEDÍ 16 SETTEMBRE 2010 (2 ORE)

Divisione con dividendo e/o divisore negativo.

Criterio di divisibilità in base all'annullarsi del resto.

Massimo comun divisore: definizione elementare. Problema: non esiste il MCD di 0 e 0. Modalità di calcolo: l'approccio mediante la fattorizzazione fallisce con numeri "grandi": provare con numeri dell'ordine di grandezza di  $10^{200}$ , tenendo presente che l'Universo ha  $13.7 \cdot 10^9$  anni.

Definizione ufficiale. Esistenza e costruzione mediante l'algoritmo di Euclide (inizio).

## LEZIONE 3. LUNEDÍ 20 SETTEMBRE 2010 (2 ORE)

Algoritmo di Euclide. L'algoritmo di Euclide su due numeri grandi all'incirca  $N$  termina in al più  $2 \cdot \log_2(N)$  passi. Il grafico di  $y = 2^x$ .

Assioma di estensione e di specificazione. Paradosso di Russell.

## LEZIONE 4. MARTEDÍ 21 SETTEMBRE 2010 (2 ORE)

La necessità della dimostrazione di esistenza.

Unicità del massimo comun divisore.

Algoritmo di Euclide esteso per esprimere il massimo comun divisore di due numeri come loro combinazione lineare: i due metodi.

Lemmi aritmetici.

## LEZIONE 5. MERCOLEDÌ 22 SETTEMBRE 2010 (2 ORE)

Applicazione dei lemmi aritmetici: il minimo comune multiplo (formula  $(a, b) \cdot [a, b] = a \cdot b$ , e interpretazione in termini di *fattori comuni e non comuni*).

Altra applicazione: tutte le combinazioni per esprimere il massimo comun divisore come combinazione lineare.

Congruenze. Esempi: le congruenze modulo 0, 1, 2, 3. Essere congrui vuol dire avere lo stesso resto. Dunque la congruenza è una relazione di equivalenza.

## LEZIONE 6. GIOVEDÌ 23 SETTEMBRE 2010 (2 ORE)

La congruenza è una relazione di equivalenza: dimostrazione diretta.

Classi rispetto a una relazione di equivalenza, e loro proprietà.

Relazioni di equivalenza e partizioni. Le classi formano una partizione.

Classi di congruenza (o resto) modulo un intero  $n$ .

## LEZIONE 7. LUNEDÌ 27 SETTEMBRE 2010 (2 ORE)

Modulo  $n$  ci sono esattamente  $n$  classi resto, che sono  $[0], [1], \dots, [n-1]$ . Notazione  $\mathbf{Z}/n\mathbf{Z}$ . Si può calcolare con le classi resto. La prova del nove.

## LEZIONE 8. MARTEDÌ 28 SETTEMBRE 2010 (2 ORE)

Criteri di divisibilità per 9, 3, 11, 2, 4, 7.

Un'applicazione: trovare i numeri interi positivi il cui prodotto delle cifre faccia un numero della forma  $111\dots 1$ .

## LEZIONE 9. MERCOLEDÌ 29 SETTEMBRE 2010 (2 ORE)

Criterio di divisibilità per 13.

Inversi in un anello. Inversi in  $\mathbf{Z}/n\mathbf{Z}$ . Calcolo degli inversi in  $\mathbf{Z}/n\mathbf{Z}$  mediante l'algoritmo di Euclide esteso.

Divisori dello zero. Divisori dello zero in  $\mathbf{Z}/n\mathbf{Z}$ .

Dunque  $[a] \in \mathbf{Z}/n\mathbf{Z}$  è invertibile se e solo se  $(a, n) = 1$ , e l'inverso si trova mediante l'algoritmo di Euclide esteso. Se invece  $(a, n) > 1$ , allora  $[a]$  è un divisore dello zero.

## LEZIONE 10. GIOVEDÌ 30 SETTEMBRE 2010 (2 ORE)

Il problema della buona definizione. Buona definizione di somma e prodotto fra le classi resto.

Lemma dei cassetti.

In un anello finito (commutativo, con unità) gli elementi sono o invertibili o divisori dello zero.

## LEZIONE 11. LUNEDÌ 4 OTTOBRE 2010 (2 ORE)

Gruppi: notazione neutra, additiva e moltiplicativa.

Monoidi, lemma sugli inversi, gli elementi invertibili di un monoide formano un gruppo. Esempi.

## LEZIONE 12. MARTEDÍ 5 OTTOBRE 2010 (2 ORE)

Il gruppo delle classi invertibili modulo  $n$ . Funzione di Eulero. Valore della funzione di Eulero per la potenze di un primo. Potenze, regole delle potenze. Il caso in cui tutte le potenze sono distinte.

Principio del minimo intero. Il caso in cui le potenze non sono distinte: periodo (o ordine) di un elemento.

## LEZIONE 13. MERCOLEDÍ 6 OTTOBRE 2010 (2 ORE)

Periodo di un elemento in un gruppo. Eguaglianza di due potenze. Periodi dello sviluppo di frazioni come numeri decimali. Il periodo di un elemento divide l'ordine del gruppo. (Dimostrazione solo nel caso commutativo.)

## LEZIONE 14. GIOVEDÍ 7 OTTOBRE 2010 (2 ORE)

Il gioco del tris.

Il primo teorema di isomorfismo fra insiemi.

Un'applicazione: potenze in un gruppo.

## LEZIONE 15. LUNEDÍ 11 OTTOBRE 2010 (2 ORE)

Il logaritmo come esempio di isomorfismo.

Teorema cinese dei resti. La funzione di Eulero è moltiplicativa nel senso della teoria dei numeri.

## LEZIONE 16. MARTEDÍ 12 OTTOBRE 2010 (2 ORE)

Un prodotto di anelli come anello.

Ancora sul teorema cinese.

Il calcolo della funzione di Eulero richiede la fattorizzazione.

Sistemi di congruenze (inizio).

## LEZIONE 17. MERCOLEDÍ 13 OTTOBRE 2010 (3 ORE)

Prima provetta intermedia.

## LEZIONE 18. GIOVEDÍ 14 OTTOBRE 2010 (2 ORE)

L'algoritmo di Euclide e la suriettività nel teorema cinese in forma geometrica.

Sistemi di congruenze.

Eulero-Fermat: test di primalità.

## LEZIONE 19. LUNEDÍ 18 OTTOBRE 2010 (2 ORE)

Sistemi di più congruenze: due congruenze equivalgono a una.

Numeri di Carmichael, test di primalità probabilistici e deterministici.

Crittografia simmetrica, cifrario di Cesare.

## LEZIONE 20. MARTEDÍ 19 OTTOBRE 2010 (2 ORE)

Rappresentazione dei numeri interi non negativi rispetto a una base  $B > 1$  arbitraria.

RSA.

## LEZIONE 21. MERCOLEDÍ 20 OTTOBRE 2010 (2 ORE)

RSA. Calcolo delle potenze.

## LEZIONE 22. GIOVEDÍ 21 OTTOBRE 2010 (2 ORE)

Polinomi. Grado: grado della somma e del prodotto.

Divisione fra polinomi. Regola di Ruffini.

## LEZIONE 23. LUNEDÍ 25 OTTOBRE 2010 (2 ORE)

Un polinomio di grado  $n$  a coefficienti in un campo  $F$  ha al più  $n$  radici in  $F$ .

Massimo comun divisore fra polinomi, e razionalizzazione.

Quadrati in  $F = \mathbf{Z}/p\mathbf{Z}$ . Se  $p$  è dispari, ci sono  $(p-1)/2$  quadrati non nulli in  $F$ .

## LEZIONE 24. MARTEDÍ 26 OTTOBRE 2010 (2 ORE)

I quadrati non nulli in  $F = \mathbf{Z}/p\mathbf{Z}$ , con  $p$  dispari, sono le radici del polinomio  $x^{(p-1)/2} - 1$ .

Come calcolare le radici quadrate modulo  $p$ , se  $p \equiv 3 \pmod{4}$ .

$-1$  è un quadrato modulo il numero primo dispari  $p$  se e solo se  $p \equiv 1 \pmod{4}$ .

Come trovare una radice quadrata con un metodo probabilistico.

## LEZIONE 25. MERCOLEDÍ 27 OTTOBRE 2010 (2 ORE)

Testa o croce per telefono: radici quadrate modulo il prodotto di due numeri primi dispari distinti.

## LEZIONE 26. GIOVEDÍ 28 OTTOBRE 2010 (2 ORE)

Ripasso di RSA e di testa o croce per telefono.

## LEZIONE 27. MARTEDÍ 2 NOVEMBRE 2010 (2 ORE)

Costruzione formale dei polinomi come funzioni sui naturali quasi ovunque nulle, con la somma per componenti, e il prodotto di convoluzione.

La valutazione è un morfismo di anelli.

## LEZIONE 28. MERCOLEDÍ 3 NOVEMBRE 2010 (3 ORE)

Seconda provetta intermedia.

## LEZIONE 29. GIOVEDÌ 4 NOVEMBRE 2010 (2 ORE)

Sottoanelli, estensioni. Il più piccolo sottoanello  $F[\alpha]$  che contiene  $F$  e  $\alpha$ : esistenza e forma.

Esempi:  $\mathbf{Z}[i]$  e  $\mathbf{Z}[\sqrt{2}]$ : irrazionalità di  $\sqrt{2}$ .

Norme, domini euclidei. Esempi: interi, polinomi,  $\mathbf{Z}[i]$  (solo norma).

## LEZIONE 30. LUNEDÌ 8 NOVEMBRE 2010 (2 ORE)

Aritmetica nei domini: unità, elementi associati.

Norme e domini euclidei. Una unità ha norma 1. In un dominio euclideo, un elemento di norma 1 è una unità. Norme speciali.

Gli interi di Gauss sono un dominio euclideo.

Elementi primi e irriducibili.

## LEZIONE 31. MARTEDÌ 9 NOVEMBRE 2010 (2 ORE)

Diverse definizioni di elemento irriducibile.

Un primo è irriducibile.

Un esempio in  $A = \mathbf{Z}[i\sqrt{5}]$ . Dall'eguaglianza

$$6 = 2 \cdot 3 = (1 + i\sqrt{5}) \cdot (1 - i\sqrt{5})$$

segue che 2 è irriducibile in  $A$ , ma non è primo.

In un dominio euclideo, gli irriducibili sono primi.

In un dominio dotato di una norma speciale, ogni elemento si può scrivere come prodotto di irriducibili.

## LEZIONE 32. MERCOLEDÌ 10 NOVEMBRE 2010 (2 ORE)

Sostanziale unicità della fattorizzazione in irriducibili in un dominio in cui gli irriducibili sono primi (p. es. in un dominio euclideo).

Se una norma è speciale, un elemento che abbia per norma un numero primo è irriducibile.

I primi di  $\mathbf{Z}$  in  $\mathbf{Z}[i]$ . 2 si scrive come prodotto  $2 = (1+i)(1-i)$  di due irriducibili associati. I numeri primi  $p \equiv 3 \pmod{4}$  restano irriducibili in  $\mathbf{Z}[i]$ . I numeri primi  $p \equiv 1 \pmod{4}$  si scrivono come prodotto di due irriducibili, ovvero  $p$  si scrive come somma di due quadrati: algoritmo.

## LEZIONE 33. GIOVEDÌ 11 NOVEMBRE 2010 (2 ORE)

Fattorizzazione dei primi  $p \equiv 1 \pmod{4}$  in  $\mathbf{Z}[i]$ , ovvero, come scriverli come somma di due quadrati.

Terne pitagoriche.

## LEZIONE 34. LUNEDÌ 15 NOVEMBRE 2010 (2 ORE)

Terne pitagoriche primitive.

Estensioni semplici. Elementi trascendenti e algebrici.

## LEZIONE 35. MARTEDÌ 16 NOVEMBRE 2010 (2 ORE)

Polinomio minimo. Isomorfismo fra l'estensione semplice  $F[\alpha]$  e l'anello  $F[x]/R$ , ove  $R$  è la congruenza modulo il polinomio minimo di  $\alpha$  su  $F$ . Un altro esempio di razionalizzazione in  $\mathbf{Q}[\sqrt[4]{2}]$ .

Il polinomio minimo di  $\sqrt{2}$  su  $\mathbf{Q}$  è  $x^2 - 2$ . Un esempio di polinomio minimo non irriducibile. Se un polinomio monico che si annulla su  $\alpha$  è irriducibile, allora è il polinomio minimo di  $\alpha$ . Se siamo in un dominio, i polinomi minimi sono irriducibili.

## LEZIONE 36. MERCOLEDÌ 17 NOVEMBRE 2010 (2 ORE)

Irriducibilità di polinomi di grado basso.

Polinomi minimi su  $\mathbf{Q}$  di  $\sqrt{2}$  e  $\sqrt[3]{2}$ .

Estensioni come spazi vettoriali. La dimensione di  $F[\alpha]$ , con  $\alpha$  algebrico su  $F$ , è il grado del polinomio minimo di  $\alpha$  su  $F$ .

## LEZIONE 37. GIOVEDÌ 18 NOVEMBRE 2010 (2 ORE)

Calcolo del polinomio minimo di  $\sqrt{2} + \sqrt{3}$  su  $\mathbf{Q}$ . Formula dei gradi (solo enunciato).

Cenni alle costruzioni mediante riga e compasso.

## LEZIONE 38. LUNEDÌ 22 NOVEMBRE 2010 (2 ORE)

Calcolo del polinomio minimo di  $\sqrt{3} + \sqrt{5}$  su  $\mathbf{Q}$ .

Come trovare una estensione in cui esiste una radice di un polinomio dato (inizio).

## LEZIONE 39. MARTEDÌ 23 NOVEMBRE 2010 (2 ORE)

Come trovare una estensione in cui esiste una radice di un polinomio dato.

Campo di spezzamento di un polinomio.

## LEZIONE 40. MERCOLEDÌ 24 NOVEMBRE 2010 (3 ORE)

Terza provetta intermedia.

## LEZIONE 41. GIOVEDÌ 25 NOVEMBRE 2010 (2 ORE)

Caratteristica di un anello. La caratteristica di un dominio è zero, o un numero primo. Un campo finito ha ordine una potenza  $q$  di un numero primo, e i suoi elementi sono le radici del polinomio  $x^q - x$ .

## LEZIONE 42. LUNEDÌ 29 NOVEMBRE 2010 (2 ORE)

Esistenza di un campo finito di ogni ordine  $p^n$ , come insieme della radici del polinomio  $x^{p^n} - x$  nel suo campo di spezzamento.

Lemmi: numeri primi e coefficienti binomiali, criterio della derivata per le radici multiple.

## LEZIONE 43. MARTEDÍ 30 NOVEMBRE 2010 (2 ORE)

Costruzione di un campo finito di ordine  $p^n$  come estensione  $\mathbf{F}_p[\alpha]$  del campo  $\mathbf{F}_p$  con  $p$  elementi mediante una radice  $\alpha$  di un polinomio monico, di grado  $n$ , irriducibile in  $\mathbf{F}_p[x]$ .

Esempi: campi di ordine 4, 9, 8. Radici degli altri polinomi irriducibili. Auto-morfismo di Frobenius.

## LEZIONE 44. MERCOLEDÍ 1 DICEMBRE 2010 (2 ORE)

Campi di ordine 8 e 16.

## LEZIONE 45. GIOVEDÍ 2 DICEMBRE 2010 (2 ORE)

Ancora sul campo di ordine 16, e i polinomi minimi dei suoi elementi.  
Costruzione del campo con 8 elementi mediante il polinomio  $x^3 + x^2 + 1$ .  
Codici a rivelazione e correzione di errori. Il codice fiscale.

## LEZIONE 46. LUNEDÍ 6 DICEMBRE 2010 (2 ORE)

Codici lineari e binari.

Il codice a ripetizione due volte rivela un errore.

Il codice a ripetizione tre volte corregge un errore.

Distanza di Hamming: proprietà. Distanza 1.

## LEZIONE 47. MARTEDÍ 7 DICEMBRE 2010 (2 ORE)

Distanza minima di un codice: caso di un codice lineare.

Un codice rivela un errore se ha distanza minima almeno 2, e ne corregge uno se ha distanza minima almeno 3. Il caso di RIP-2 e RIP-3.

Matrice di un codice, e matrice di controllo di parità.

Codice a controllo di parità.

## LEZIONE 48. GIOVEDÍ 9 DICEMBRE 2010 (2 ORE)

Matrici  $G$  del codice, e matrici  $G$  di controllo di parità, per RIP-2, RIP-3 e il codice di controllo di parità.

Codifica: si moltiplica un vettore per la matrice  $G$ .

Decodifica: si moltiplica il vettore ricevuto per  $H^t$ .

## LEZIONE 49. LUNEDÍ 13 DICEMBRE 2010 (2 ORE)

Decodifica mediante la sindrome. Codice di Hamming [7, 4].

## LEZIONE 50. MARTEDÍ 14 DICEMBRE 2010 (2 ORE)

Il codice di Hamming [7, 4] con l'altro polinomio.

Il codice di Hamming è ciclico: descrizione degli elementi.

Il codice di Hamming in generale.

Un codice BCH che corregge due errori.

## LEZIONE 51. MERCOLEDÌ 15 DICEMBRE 2010 (2 ORE)

Il codice di Hamming [15, 11] basato sul campo con 16 elementi.

Sottogruppi di un gruppo: definizioni alternative.

Teorema di Lagrange. Corollario: il periodo di un elemento di un gruppo finito divide l'ordine del gruppo.

Sottogruppi di  $\mathbf{Z}$ .

## LEZIONE 52. GIOVEDÌ 16 DICEMBRE 2010 (2 ORE)

Relazioni (di equivalenza) compatibili su un anello.

Ideali. Ogni relazione compatibile è una congruenza modulo un ideale.

Primo teorema di isomorfismo per anelli.

## LEZIONE 53. LUNEDÌ 20 DICEMBRE 2010 (2 ORE)

Ancora sul primo teorema di isomorfismo per anelli, enunciato in termini di ideali.

Primo teorema di isomorfismo fra gruppi: sottogruppi normali.

## LEZIONE 54. MARTEDÌ 21 DICEMBRE 2010 (2 ORE)

Due applicazioni del codice di Hamming:

- Cappelli rossi e cappelli blu.
- Sette domande, una menzogna.

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

*E-mail address:* [caranti@science.unitn.it](mailto:caranti@science.unitn.it)

*URL:* <http://science.unitn.it/~caranti/>