DIARIO DEL CORSO DI ALGEBRA A

A.A. 2017/18

DOCENTE: ANDREA CARANTI

Nota. La descrizione di lezioni non ancora svolte si deve intendere come una previsione/pianificazione.

Lezione 1. martedí 20 febbraio 2018 (2 ore)

Presentazione del corso.

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

$$142857,$$

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. Determinazione delle coppie (x, y) di interi tali che $xy = 1$.

Divisione con resto non negativo. Il caso del dividendo negativo. Il caso del divisore negativo. Unicità di quoziente e resto.

Ruolo di ± 1 e 0 nella divisibilità. Se a divide b e c, allora divide anche $b \pm c$.

Lezione 2. giovedí 22 febbraio 2018 (2 ore)

Criterio di divisibilità in base all'annullarsi del resto.

Modalità di calcolo del MCD: l'approccio mediante la fattorizzazione fallisce con numeri "grandi".

Provare con

$$1\,000\,000\,014\,000\,000\,049 \qquad \text{e} \qquad 1\,200\,000\,049\,400\,000\,287.$$

Massimo comun divisore (MCD): definizione elementare. Problema: non esiste il MCD di 0 e 0.

Problema col metodo di calcolo mediante la fattorizzazione. Provare con numeri dell'ordine di grandezza di 10^{200}, tenendo presente che l'Universo ha $13.7 \cdot 10^9$ anni, che il più potente calcolatore attuale fa (approssimativamente) 33.86 petaflops, cioè $33.86 \cdot 10^{15}$ operazioni al secondo, e che la popolazione mondiale è di poco più di $7 \cdot 10^9$ abitanti.

Definizione formale del MCD fra due interi a, b. Il MCD di 0 e 0 è 0.

Paradosso di Russell.

Assioma di specificazione.

Sono equivalenti: d è il massimo comun divisore fra a e b, e $\mathfrak{D}(a) \cap \mathfrak{D}(b) = \mathfrak{D}(d)$. (Qui $\mathfrak{D}(c) = \{\, x \in \mathbf{Z} : x \mid c \,\}$.)

Date: Trento, A. A. 2017/18.

Lezione 3. martedí 27 febbraio 2018 (2 ore)

"Unicità" del massimo comun divisore.

Esistenza e costruzione del MCD mediante l'algoritmo di Euclide: si comincia con il fatto che il MCD fra 0 e b è b.

Notazione $\gcd(a, b)$ per il MCD.

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

Teorema di Bézout. Algoritmo di Euclide (cosiddetto) esteso per esprimere il massimo comun divisore d di due numeri a, b come loro combinazione lineare $ax + by = d$, con $x, y \in \mathbf{Z}$.

Lezione 4. giovedí 1 marzo 2018 (2 ore)

Esempi dei due metodi per Bézout.

Se $\gcd(a, b) = 1$, allora a e b si dicono coprimi, o primi fra loro, o relativamente primi.

a e b sono coprimi se e solo se esistono $x, y \in \mathbf{Z}$ tali che $ax + by = 1$.

Lemmi aritmetici.

Applicazione dei lemmi aritmetici: il minimo comune multiplo, la formula

$$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = a \cdot b,$$

e interpretazione in termini di *fattori comuni e non comuni*.

Applicazione dei lemmi aritmetici: tutte le combinazioni per esprimere il massimo comun divisore come combinazione lineare.

Induzione e assiomatica degi numeri naturali (inizio).

Lezione 5. martedí 6 marzo 2018 (2 ore)

Principio di induzione forte e principio del minimo intero.

Ancora sulla divisione con resto: dimostrazione per induzione, o meglio con il principio del minimo intero.

Congruenze. Basta considerare le congruenze modulo numeri non negativi. Le congruenze modulo $0, 1$.

La congruenza è una relazione di equivalenza: cenno alla dimostrazione diretta.

Essere congrui vuol dire avere lo stesso resto, dunque la congruenza è una relazione di equivalenza.

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

Lemma: se R è una relazione di equivalenza sull'insieme $A \neq \emptyset$, e $[a] = \{ x \in A : xRa \}$ è la classe di $a \in A$, allora per ogni $a \in A$ si ha $a \in [a]$, e per $a, b \in A$ sono equivalenti:

(1) aRb,
(2) $a \in [b]$,
(3) $[a] \subseteq [b]$,
(4) $[a] = [b]$.

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

Lezione 6. giovedí 8 marzo 2018 (2 ore)

Classi di congruenza (o resto) modulo un intero n. Le classi modulo 2 e 3.

Lemma: n divide a se e solo se $a \equiv 0 \pmod{n}$ se e solo se $[a] = [0]$ in $\mathbf{Z}/n\mathbf{Z}$.

Per $n > 0$ e $a \in \mathbf{Z}$ si ha $[a] = \{\, a + nq : q \in \mathbf{Z} \,\}$.

Se $n > 0$, e $0 \leq r < n$, allora per $a \in \mathbf{Z}$ sono equivalenti: r è il resto della divisione di a per n, e $[a] = [r]$.

Modulo n ci sono esattamente n classi modulo n, che sono $[0], [1], \ldots, [n-1]$, cioè esattamente le classi dei possibili resti della divisione per n. Per $a \in \mathbf{Z}$ e $0 \leq r < n$, si ha che $a \in [r]$ se e solo se r è il resto della divisione di a per n.

Notazione $\mathbf{Z}/n\mathbf{Z}$. Si può calcolare con le classi resto.

Gruppi, anelli.

Lezione 7. martedí 13 marzo 2018 (2 ore)

La prova del nove, ovvero criterio di divisibilità per 9.

Criteri di divisibilità per 11 e 7.

Esercizio proposto: trovare i numeri interi positivi il cui prodotto delle cifre faccia un numero della forma $111\ldots1$.

Per $n \geq 2$, gli elementi invertibili in $\mathbf{Z}/n\mathbf{Z}$ sono le classi a tali che $\gcd(a, n) = 1$. (Inizio)

Lezione 8. giovedí 15 marzo 2018 (2 ore)

Elementi invertibili in un anello.

Per $n \geq 2$, gli elementi invertibili in $\mathbf{Z}/n\mathbf{Z}$ sono le classi a tali che $\gcd(a, n) = 1$: algoritmo di Euclide per trovare gli inversi.

Divisori dello zero (anche detti 0-divisori) in un anello commutativo. Se $A \neq \{\, 0 \,\}$, lo 0 è uno 0-divisore.

Sono equivalenti, per un anello commutativo $A \neq \{\, 0 \,\}$: l'unico 0-divisore è 0, e in A vale la legge di annullamento del prodotto. Definizione di dominio.

Per $n \geq 2$, se $\gcd(a, n) > 1$, allora $[a]$ è uno 0-divisore in $\mathbf{Z}/n\mathbf{Z}$. Dicotomia invertibili/0-divisori in $\mathbf{Z}/n\mathbf{Z}$, per $n \geq 2$. Si noti che in $\mathbf{Z}$ gli elementi invertibili sono $1, -1$, e l'unico *o*-divisore è 0, mentre tutti gli altri elementi non sono né l'uno né l'altro.

Se n è primo, allora $\mathbf{Z}/n\mathbf{Z}$ è un dominio.

Lezione 9. martedí 20 marzo 2018 (2 ore)

(Lezione tenuta da Simone Ugolini)

In un anello commutativo con unità un elemento non può essere 0-divisore e invertibile. In un anello commutativo si può semplificare per un non 0-divisore. $\mathbf{Z}/n\mathbf{Z}$ è un dominio se e solo se n è primo. Definizione di campo. Un campo è un dominio ma non vale necessariamente il viceversa. Se n è primo, allora $\mathbf{Z}/n\mathbf{Z}$ è un campo. Lemma dei Cassetti. In un anello finito commutativo con unità vale la dicotomia invertibile/0-divisore. Un dominio finito è un campo. Buona definizione delle operazioni in $\mathbf{Z}/n\mathbf{Z}$. $\mathbf{Z}/n\mathbf{Z}$ è un anello (cenni).

Lezione 10. giovedí 22 marzo 2018 (2 ore)

(Lezione tenuta da Simone Ugolini)

Definizione di operazione (binaria), di elemento neutro e di elemento simmetrico. Elemento neutro e elemento simmetrico, se esistono, sono unici. Semigruppi, monoidi, gruppi. Notazione neutra, additiva e moltiplicativa per un monoide.ă Lemma sugli inversi in un monoide. Linsieme degli elementi invertibili di un monoide è un gruppo. Esempi: gruppo degli invertibili di $\mathbf{Z}/n\mathbf{Z}$, $M_n(\mathbf{K})$ con $\mathbf{K}$ campo, $M_n(\mathbf{Z})$. Composizione di funzioni. Inversa destra e sinistra. Inversa destra e sinistra, se esistono, non sono necessariamente uniche.

Lezione 11. martedí 27 marzo 2018 (2 ore)

Inversa destra e sinistra corrispondono a funzioni iniettive e suriettive.

Gruppo simmetrico delle funzioni invertibili (biiettive) su un insieme.

Lezione 12. mercoledí 28 marzo 2018 (3 ore)

Prima prova intermedia.

Lezione 13. giovedí 29 marzo 2018 (2 ore)

(Lezione tenuta da Simone Ugolini)

Il gruppo $U(\mathbf{Z}/n\mathbf{Z})$ delle classi invertibili modulo n. Funzione di Eulero. Valore della funzione di Eulero su piccoli numeri, sui numeri primi, e sulle potenze di un numero primo. La funzione di Eulero è moltiplicativa nel senso della teoria dei numeri (solo enunciato). Il caso in cui $n = pq$ è il prodotto di due numeri primi distinti: cenno al principio di inclusione/esclusione. Se n è il prodotto di due numeri primi distinti, calcolare $\varphi(n)$ equivale a fattorizzare n. Calcolo della φ di Eulero data la fattorizzazione di n.

La funzione $f : \mathbf{Z} \to \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ che manda x in $([x]_m, [x]_n)$. La funzione f non è necessariamente suriettiva. Esempi.

Sistemi di due congruenze

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

Il sistema ha soluzione se e solo se $\gcd(m, n) \mid ab$. Come trovare una soluzione. Come trovare tutte le soluzioni: se il sistema $x \equiv a \mod m$ $x \equiv b \mod n$ ha una soluzione x_0, allora le soluzioni sono tutti e soli gli x tali che $x \equiv x_0 \mod \operatorname{lcm}(m, n)$. Esempi di sistemi di congruenze.

Lezione 14. giovedí 5 aprile 2018 (2 ore)

Diagonali e sistemi di congruenze.

Teorema cinese dei resti: se $\gcd(m, n) = 1$, la funzione $\mathbf{Z}/mn\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ data da $[x]_{mn} \mapsto ([x]_m, [x]_n)$ è ben definita e biiettiva.

Corollario: la funzione di Eulero è moltiplicativa nel senso della teoria dei numeri.

Primo teorema di isomorfismo fra insiemi. (Inizio)

Lezione 15. martedí 10 aprile 2018 (2 ore)

Primo teorema di isomorfismo fra insiemi. (Inizio)

Ogni relazione di equivalenza R è della forma: *aRb se e solo se a e b hanno la stessa immagine sotto una opportuna funzione.*

Applicazione del primo teorema di isomorfismo fra insiemi: prima forma del Teorema Cinese dei resti: la biiezione $\mathbf{Z}/mn\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ data da $[x]_{mn} \mapsto ([x]_m, [x]_n)$.

Il gioco dei 9 numeri come esempio di isomorfismo.

Logaritmo. Tavole dei logaritmi.

Morfismi e isomorfismo di gruppi: unità, inversi (inizio). Trasporto di struttura (cenno).

Lezione 16. giovedí 12 aprile 2018 (2 ore)

Morfismi e isomorfismo di gruppi: unità, inversi (fine). Perché si può semplificare.

A^B come insieme delle funzioni $B \to A$. Il caso di A^n. A^0 ha un'unico elemento, la funzione vuota.

Un gruppo ha tre operazioni, una binaria, una unaria, una zeraria.

Morfismi di gruppi: basta richiedere che sia preservata l'operazione binaria.

Morfismi e isomorfismi di anelli: zero, opposti, eventuale unità, eventuali inversi.

Prodotto diretto di gruppi: unità, inversi.

Prodotto diretto di anelli: zero, opposti, unità, inversi.

Seconda forma del Teorema Cinese dei Resti: la funzione

$$\mathbf{Z}/mn\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$$
$$[x]_{mn} \mapsto ([x]_m, [x]_n)$$

è un isomorfismo di anelli con unità.

Lezione 17. martedí 17 aprile 2018 (2 ore)

Nel gruppo delle matrici invertibili 2×2 a coefficienti reali si ha

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

dunque in un gruppo in generale da $ba = ac$ non si può dedurre $b = c$.

Il Teorema Cinese dei Resti come isomorfismo di anelli.

Di nuovo: la funzione di Eulero è moltiplicativa nel senso della teoria dei numeri.

Sottogruppi.

L'immagine di un morfismo è un sottogruppo.

La relazione di equivalenza R indotta da un morfismo di gruppi $f : A \to B$ è compatibile con l'operazione, e quindi l'operazione su A/R data da $[x][y] = [xy]$ è ben definita, e fa di A/R un gruppo. La funzione $\pi : A \to A/R$ che manda $a \mapsto [a]$ è un morfismo di gruppi.

Primo teorema di isomorfismo per gruppi.

Primo Teorema di Isomorfismo per anelli.

Lezione 18. giovedí 19 aprile 2018 (2 ore)

Applicazione del Primo Teorema di Isomorfismo per anelli: il teorema cinese.

Potenze e multipli. Definizione ricorsiva e dimostrazioni per induzione. (Cenno agli assiomi di Peano.)

Regole delle potenze. Un esempio di dimostrazione.

Applicazione del primo teorema di isomorfismo al morfismo $f : \mathbf{Z} \to G$ che manda $x \mapsto a^x$, ove G è un gruppo (scritto in forma moltiplicativa), e $a \in G$. Si ha che $f : \mathbf{Z} \mapsto \langle\, a \,\rangle = \{\, a^x : x \in \mathbf{Z} \,\}$ è un morfismo suriettivo.

Se f è iniettivo, allora $f : \mathbf{Z} \to \langle\, a \,\rangle$ è un isomorfismo.

Se invece f non è iniettivo, col principio del minimo intero si vede che esiste m che sia il più piccolo intero positivo x tale che $a^x = 1$. In tal caso si ha

$$\begin{cases} a^x = 1 & \text{se e solo se } m \mid x \\ a^x = a^y & \text{se e solo se } x \equiv y \pmod{m} \end{cases}$$

e il primo teorema di isomorfismo per i gruppi ci dice che $g : \mathbf{Z}/m\mathbf{Z} \to \langle\, a \,\rangle$ tale che $[x] \mapsto a^x$ è un isomorfismo.

Lezione 19. martedí 24 aprile 2018 (2 ore)

Multipli: regole.

Esempio: il periodo di [3] in $U(\mathbf{Z}/7\mathbf{Z})$.

Se G è un gruppo finito, e $a \in G$, allora l'ordine di a divide l'ordine di G. Dimostrazione solo nel caso commutativo.

Teorema di Eulero-Fermat e Piccolo Teorema di Fermat.

Applicazione: numeri decimali periodici.

Lezione 20. giovedí 26 aprile 2018 (2 ore)

Crittografia. Il cifrario di Cesare. Esempi:

- `LCJKCXXMBCJAYKKGLBGLMQRPYTGRY`
- `UGFWVQKPSWGNECHHGKQPQPRGPUCXQ`
- `CGMZFUBUMFFUEBADOTUPMXMHMDQ`

Scrittura di un numero in base $B > 1$: algoritmo.

Albergo di Hilbert.

Lezione 21. giovedí 3 maggio 2018 (2 ore)

Crittografia a chiave pubblica: RSA.

Calcolo delle potenze.

Criteri probabilistici e deterministici di primalità.

Lezione 22. venerdí 4 maggio 2018 (3 ore)

Seconda prova intermedia.

Lezione 23. martedí 8 maggio 2018 (2 ore)

Stime del numero di interi coprimi.
Due esempi di RSA.
Polinomi: grado, grado della somma e del prodotto

Lezione 24. giovedí 10 maggio 2018 (2 ore)

L'anello dei polinomi a coefficienti in un dominio è un dominio — grado del prodotto.

Proprietà universale dell'anello dei polinomi. Valutazione di un polinomio in un elemento.

Aritmetica nei domini. Divisibilità: proprietà.

Divisione con resto fra polinomi

Lezione 25. lunedí 14 maggio 2018 (2 ore)

Divisione con resto fra polinomi, MCD, algoritmo di Euclide.

Un esempio di razionalizzazione con l'algoritmo di Euclide esteso.

Radici di un polinomio e regola di Ruffini. In un dominio, un polinomio non nullo può avere al massimo tante radici distinte quanto il suo grado.

L'immagine $v_\alpha(A[x]) = A[\alpha]$ del morfismo di valutazione è il più piccolo sottoanello che contenga A e α.

Inizio del caso $\mathbf{Z}[\alpha]$, ove $\alpha \in \mathbf{C} \setminus \mathbf{Q}$ è radice di un polinomio $x^2 + b_1 x + b_0 \in \mathbf{Z}[x]$.

Lezione 26. giovedí 17 maggio 2018 (2 ore)

Il caso $\mathbf{Z}[\alpha]$, ove $\alpha \in \mathbf{C} \setminus \mathbf{Q}$ è radice di un polinomio $x^2 + b_1 x + b_0 \in \mathbf{Z}[x]$.

Elementi primi e irriducibili in un dominio.

I primi sono irriducibili.

Lezione 27. martedí 22 maggio 2018 (2 ore)

Norme e norme speciali. Esempi. Unità in $\mathbf{Z}[i]$ e $\mathbf{Z}[\sqrt{-5}]$.

Gli irriducibili non sono necessariamente primi. L'esempio

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

mostra che 2 (e anche $3, 1 \pm \sqrt{-5}$) sono irriducibili, ma non primi, in $\mathbf{Z}[\sqrt{-5}]$.

Lezione 28. giovedí 24 maggio 2018 (2 ore)

Non esiste il MCD in $\mathbf{Z}[\sqrt{-5}]$.

Unicità della fattorizzazione.

L'unicità della fattorizzazzione equivale al fatto che gli irriducibili sono primi.

Domini euclidei. $\mathbf{Z}$ come dominio euclideo: non vale più l'unicità di quoziente e resto.

La norma di un dominio euclideo è speciale.

Lezione 29. martedí 29 maggio 2018 (2 ore)

In un dominio euclideo si può calcolare il GCD con l'algoritmo di Euclide e valgono i lemmi aritmetici.

In un dominio euclideo gli irriducibili sono primi.

$\mathbf{Z}[i]$ è un dominio euclideo. Esempio di divisione con resto e della non unicità di quoziente e resto. 2 non è irriducibile $\mathbf{Z}[i]$.

Se un primo dispari è somma di due quadrati, allora è congruo a 1 modulo 4.

Lezione 30. giovedí 31 maggio 2018 (1 ora)

Terne pitagoriche.

Lezione 31. venerdí 1 giugno 2018 (3 ore)

Terza prova intermedia.

Dipartimento di Matematica, Università degli Studi di Trento, via Sommarive 14, 38123 Trento

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

URL: http://www.science.unitn.it/∼caranti/