

DIARIO DEL CORSO DI ALGEBRA A

A.A. 2021/22

DOCENTE: ANDREA CARANTI

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

LEZIONE 1. MERCOLEDÌ 2 MARZO 2022 (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.

Ruolo di ± 1 e 0 nella divisibilità.

LEZIONE 2. VENERDÌ 4 MARZO 2022 (2 ORE)

Unicità di quoziente e resto.

Criterio di divisibilità in base all'annullarsi del resto.

Se a divide b e c , allora divide anche $b \pm c$.

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

Provare con

1 000 000 014 000 000 049 e 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 .

Unicità (a meno del segno) del massimo comun divisore.

LEZIONE 3. MERCOLEDÌ 9 MARZO 2022 (2 ORE)

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

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

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

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

Grafico di $y = 2^x$:

- $2^{10} \approx 10^3$ cm = 10 m, questo edificio.
- $2^{20} \approx 10^6$ cm = 10 km, oltre l'Everest.
- $2^{40} \approx 10^{11}$ cm = 10^6 km, Terra-Luna sono meno di 400 000 km.
- $2^{50} \approx 10^{15}$ cm = 10^{10} km, Terra-Sole sono meno di $150 \cdot 10^6$ km.
- $2^{80} \approx 10^{24}$ cm = 10^{19} km, raggio della galassia $5 \cdot 10^{17}$ km.
- $2^{100} \approx 10^{30}$ cm = 10^{25} km, raggio dell'Universo osservabile $5 \cdot 10^{23}$ km.

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 $x, y \in \mathbf{Z}$.

Esempi dei due metodi per Bézout.

LEZIONE 4. VENERDÌ 11 MARZO 2022 (2 ORE)

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

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

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.

Assioma di specificazione. Assioma di estensione.

Paradosso di Russell.

Induzione e assiomatica dei numeri naturali.

Principio di induzione forte e principio del minimo intero.

LEZIONE 5. MERCOLEDÌ 16 MARZO 2022 (2 ORE)

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) $[a] = [b]$,
- (5) $[a] \cap [b] \neq \emptyset$.

Da relazioni di equivalenza a partizioni. Le classi formano una partizione.

LEZIONE 6. VENERDÌ 18 MARZO 2022 (2 ORE)

Da partizioni a relazioni di equivalenza. I due concetti si equivalgono.

Ogni relazione di equivalenza è del tipo “avere la stessa immagine sotto una funzione”.

Terzo concetto equivalente: funzione suriettiva.

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

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

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 $[a] = [r]$.

Notazione $\mathbf{Z}/n\mathbf{Z}$.

Modulo n ci sono esattamente n classi modulo n , che sono $[0], [1], \dots, [n-1]$, 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 .

Gruppi. Unicità dell'elemento neutro e dell'inverso.

LEZIONE 7. MERCOLEDÌ 23 MARZO 2022 (2 ORE)

Notazione neutra, additiva e moltiplicativa per i gruppi.

Anelli, anelli con unità.

Si può calcolare con le classi resto. Divisori dello zero, e elementi invertibili in un anello: esempi in $\mathbf{Z}/n\mathbf{Z}$.

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

Criterio di divisibilità per 11

LEZIONE 8. VENERDÌ 25 MARZO 2022 (2 ORE)

Criterio di divisibilità per 7.

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

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.

In un anello commutativo con unità un elemento non può essere 0-divisore e invertibile.

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 0-divisore è 0, mentre tutti gli altri elementi non sono né l'uno né l'altro.

Lemma dei Casseti — versione quantitativa.

LEZIONE 9. MERCOLEDÌ 30 MARZO 2022 (2 ORE)

Lemma dei Casseti — versione quantitativa.

In un anello commutativo si può semplificare per un non 0-divisore.

In un anello finito commutativo con unità vale la dicotomia invertibile/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.

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.

Un dominio finito è un campo. Buona definizione delle operazioni in $\mathbf{Z}/n\mathbf{Z}$.

Semigrupperi: elemento neutro e elemento simmetrico, se esistono, sono unici. Monoidi, gruppi.

Lemma sugli inversi in un monoide.

LEZIONE 10. VENERDÌ 1 APRILE 2022 (2 ORE)

L'insieme 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.

Inversa destra e sinistra corrispondono a funzioni iniettive e suriettive.

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

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.

LEZIONE 11. MERCOLEDÌ 6 APRILE 2022 (2 ORE)

(Lezione tenuta da Simone Ugolini)

Valore della funzione di Eulero 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 $f : \mathbf{Z} \rightarrow \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ 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 $\gcd(m, n) \mid a - b$. Come trovare una soluzione. Come trovare tutte le soluzioni: se il sistema $x \equiv a \pmod{m}$ $x \equiv b \pmod{n}$ ha una soluzione x_0 , allora le soluzioni sono tutti e soli gli x tali che $x \equiv x_0 \pmod{\text{lcm}(m, n)}$. Esempi di sistemi di congruenze.

Diagonali e sistemi di congruenze.

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

LEZIONE 12. VENERDÌ 8 APRILE 2022 (2 ORE)

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

Teorema di biiezione fra insiemi.

Applicazione del teorema di biezione fra insiemi: prima forma del Teorema Cinese dei resti: la biiezione $\mathbf{Z}/mn\mathbf{Z} \rightarrow \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ 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. Un cenno al trasporto di struttura.

LEZIONE 13. MERCOLEDÌ 13 APRILE 2022 (2 ORE)

Morfismi e isomorfismo di gruppi: unità, inversi. Cenno alla costruzione dei numeri naturali all'interno della teoria degli insiemi. Operazioni binarie, unarie, zerarie.

Anelli con e senza unità. Morfismi e isomorfismi di anelli. Un morfismo di anelli non porta necessariamente l'unità del primo (se c'è) in quella del secondo (esempio), ma questo vale se è suriettivo.

Inversi sotto (iso)morfismi di anelli.

Prodotto diretto di gruppi e di anelli.

Se $m, n \geq 2$ sono interi, e $\gcd(m, n) = 1$ allora la biiezione

$$\begin{aligned} f : \mathbf{Z}/mn\mathbf{Z} &\rightarrow \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z} \\ [x]_{mn} &\mapsto ([x]_m, [x]_n) \end{aligned}$$

del teorema cinese è un morfismo di anelli, e dunque un isomorfismo.

Nuova dimostrazione della moltiplicatività della funzione di Eulero.

LEZIONE 14. MERCOLEDÌ 20 APRILE 2022 (2 ORE)

(Lezione tenuta da Simone Ugolini)

Semigrupperi, morfismi e sottosemigrupperi.

Un sottosemigruppero H di un semigruppero G è un semigruppero rispetto alla restrizione dell'operazione del semigruppero G .

L'immagine di un morfismo di semigrupperi è un sottosemigruppero del codominio.

Se $f : A \rightarrow B$ è un morfismo suriettivo di semigrupperi allora la relazione R definita su A come xRy se e solo se $f(x) = f(y)$ è una relazione di equivalenza compatibile con l'operazione di semigruppero; inoltre, l'operazione $[x] \cdot [y] = [xy]$ è ben definita e induce su A/R una struttura di semigruppero. Sottogruppi.

Esempio: sottogruppi di $U(\mathbf{Z}/8\mathbf{Z})$. Un sottogruppo è un gruppo rispetto alle restrizioni delle operazioni del gruppo.

L'immagine di un morfismo di gruppi è un sottogruppo del codominio.

Primo teorema di isomorfismo per i gruppi.

LEZIONE 15. VENERDÌ 22 APRILE 2022 (2 ORE)

Sottoanelli. Un sottoanello è un anello rispetto alle (restrizioni delle) operazioni dell'anello.

Un sottoanello può avere una unità diversa da quella dell'anello.

L'immagine di un morfismo di anelli è un sottoanello del codominio.

Primo teorema di isomorfismo per gli anelli.

Ancora una volta il Teorema Cinese.

Potenze e multipli. Definizione ricorsiva e dimostrazioni per induzione. Regole delle potenze:

$$(1) a^{n+m} = a^n \cdot a^m,$$

$$(2) a^{nm} = (a^n)^m.$$

In generale non vale $(ab)^n = a^n b^n$.

LEZIONE 16. MERCOLEDÌ 27 APRILE 2022 (2 ORE)

Nei gruppi abeliani vale anche $(ab)^n = a^n b^n$.

Dato un gruppo G , e un elemento $a \in G$, la funzione

$$f : \mathbf{Z} \rightarrow G \\ n \mapsto a^n$$

è un morfismo, che ha per immagine il sottogruppo

$$\langle a \rangle = \{ a^n : n \in \mathbf{Z} \}.$$

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

Se f non è iniettivo, ci sono interi $x > y$ tali che $a^x = a^y$, dunque $x - y$ è un elemento dell'insieme

$$A = \{ n \in \mathbf{N} : n > 0 \text{ e } a^n = 1 \} \subseteq \mathbf{N}.$$

Dunque A è un sottoinsieme non vuoto dei numeri naturali, che ha quindi un minimo.

Il minimo m di A (nel caso in cui f non sia iniettiva) si dice periodo o ordine di a . Dunque m è definito da

| | | | |
|----|-------------------------|--------|------------|
| | $m > 0$, e $a^m = 1$ | | |
| se | $n > 0$, e $a^n = 1$, | allora | $m \leq n$ |

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 $\varphi : \mathbf{Z}/m\mathbf{Z} \rightarrow \langle a \rangle$ tale che $[x] \mapsto a^x$ è un isomorfismo.

Esempi: il periodo di $[10]$ in $U(\mathbf{Z}/11/\mathbf{Z})$ e $U(\mathbf{Z}/7/\mathbf{Z})$. Perché si chiama periodo.

Perché si chiama ordine: il sottogruppo $\langle a \rangle$ è il più piccolo sottogruppo che contenga a , e ha m elementi.

Periodo zero.

LEZIONE 17. VENERDÌ 29 APRILE 2022 (2 ORE)

Lemma: in un gruppo le traslazioni destre e sinistre sono biiezioni. Traslazioni destre.

Se G è un gruppo finito, allora l'ordine di ogni elemento divide l'ordine del gruppo. Dimostrazione solo nel caso di un gruppo abeliano (cioè commutativo).

Conseguenze: Eulero-Fermat, Piccolo Teorema di Fermat.

Un'applicazione: numeri decimali periodici.

LEZIONE 18. MERCOLEDÌ 4 MAGGIO 2022 (2 ORE)

Introduzione alla crittografia. Il cifrario di Cesare. Da lettere a numeri a classi resto.

Scrittura di un numero naturale in base $B > 1$: esistenza e unicità. Come condensare in un unico numero una successione finita di numeri $< B$.

L'albergo di Hilbert. Insiemi infiniti numerabili. \mathbf{Q} è numerabile.

LEZIONE 19. VENERDÌ 6 MAGGIO 2022 (2 ORE)

Ancora sul teorema che una unione numerabile di insiemi numerabili è numerabile.

Crittografia a chiave pubblica.

RSA:

- (1) scelta della chiave pubblica da parte di Bob;
- (2) come fa Alice a cifrare il messaggio usando la chiave pubblica;
- (3) come fa Bob a decifrare il messaggio, usando la sua chiave segreta.

Dato N noto, prodotto di due numeri primi ignoti, calcolare $\varphi(N)$ è equivalente a fattorizzare N .

Criteri probabilistici di primalità.

Calcolo delle potenze (modulo N). Il metodo che passa per scrivere l'esponente in base 2. Stima del numero di divisioni con resto/moltiplicazioni.

Un esempio di RSA.

LEZIONE 20. MERCOLEDÌ 11 MAGGIO 2022 (2 ORE)

(Complessità della scrittura in base 2.)

Un esempio di RSA.

Polinomi.

Grado di un polinomio, grado della somma e del prodotto. Proprietà universale dell'anello dei polinomi e morfismo di valutazione (inizio).

LEZIONE 21. VENERDÌ 13 MAGGIO 2022 (2 ORE)

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

Aritmetica nei domini. Divisibilità. Se A è un dominio, per $a, b \in A$ sono equivalenti

- (1) $a \mid b$ e $b \mid a$, e
- (2) $b = au$, con $u \in A$ invertibile (in A).

Un elemento invertibile di un dominio viene chiamato *una unità*.

Divisione con resto fra polinomi: si può fare quando il coefficiente direttore del divisore è invertibile. Massimo comun divisore, algoritmo di Euclide (esteso). Un esempio di razionalizzazione.

Radici di un polinomio. Regola di Ruffini: sono equivalenti, per un polinomio $a \in A[x]$ e $\alpha \in A$

- (1) α è una radice di a , ovvero $v_\alpha(a) = 0$, e
- (2) $x - \alpha \mid a$.

Numero di radici di un polinomio. Se A è un dominio, e $a \in A[x]$ ha grado n , allora a ha al più n radici distinte in A .

LEZIONE 22. MERCOLEDÌ 18 MAGGIO 2022 (2 ORE)

(Lezione tenuta da Simone Ugolini)

Se A è un dominio, gli elementi invertibili in $A[x]$ sono gli elementi invertibili in A .

Se $\alpha \in \mathbf{C} \setminus \mathbf{Q}$ è radice di un polinomio $x^2 + b_1x + b_0 \in \mathbf{Z}[x]$, allora $\mathbf{Z}[\alpha] = \{a_0 + a_1\alpha : a_i \in \mathbf{Z}\}$. Inoltre ogni elemento di $\mathbf{Z}[\alpha]$ si scrive in modo unico nella forma $a_0 + a_1\alpha$.

Elementi primi e irriducibili in un dominio. Formulazioni equivalenti dell'irriducibilità.

Le unità di $\mathbf{Z}[i]$ sono gli elementi il cui modulo complesso (al quadrato) è 1. Le unità sono dunque $1, -1, i, -i$.

LEZIONE 23. VENERDÌ 20 MAGGIO 2022 (2 ORE)

I primi sono irriducibili.

Norme. La norma di una unità è 1.

Norma del grado sui polinomi. Con questa norma, in $\mathbf{Z}[x]$ non tutti gli elementi di norma 1 sono unità. Una norma alternativa su $\mathbf{Z}[x]$.

Norme speciali: la norma di \mathbf{Z} è speciale.

La norma sul dominio $\mathbf{Z}[i]$ degli interi di Gauss.

Ancora sulle unità di $\mathbf{Z}[i]$: se $1 = N(a_0 + ia_1) = a_0^2 + a_1^2 = (a_0 + ia_1) \cdot (a_0 - ia_1)$, allora l'inverso di $a_0 + ia_1$ è il suo coniugato $a_0 - ia_1$.

La norma speciale su $\mathbf{Z}[\sqrt{-5}]$.

Un dominio A dotato di norma speciale è atomico, nel senso che ogni $a \in A$, $a \neq 0$, a non una unità, si scrive come prodotto di irriducibili.

Se un dominio A è dotato di una norma speciale, allora un elemento $a \in A$ tale che la sua norma sia un primo (in \mathbf{Z}) è irriducibile in A .

Cosa vuol dire per un elemento *non* essere irriducibile, ovvero essere riducibile.

LEZIONE 24. MERCOLEDÌ 25 MAGGIO 2022 (2 ORE)

(Essenziale) unicità della fattorizzazione in irriducibili. Definizione di dominio a fattorizzazione unica (UFD).

Teorema: se A è un dominio atomico, sono equivalenti

- (1) in A gli irriducibili sono primi, e
- (2) A è un dominio a fattorizzazione unica.

Dall'eguaglianza

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

segue che $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ sono irriducibili, ma non primi, in $\mathbf{Z}[\sqrt{-5}]$, e dunque che $\mathbf{Z}[\sqrt{-5}]$ non è un UFD.

Domini euclidei. Riguardando \mathbf{Z} come un dominio euclideo, quoziente e resto della divisione con resto non sono più unici.

In un dominio euclideo si può fare l'algoritmo di Euclide (esteso), e dunque esiste il massimo comun divisore, e valgono i lemmi aritmetici.

$\mathbf{Z}[i]$ è un dominio euclideo.

LEZIONE 25. VENERDÌ 27 MAGGIO 2022 (2 ORE)

La norma di un dominio euclideo è speciale, dunque un dominio euclideo è atomico.

In un dominio euclideo gli irriducibili sono primi, e dunque un dominio euclideo è un dominio a fattorizzazione unica.

Esempio di divisione con resto e di calcolo del MCD negli interi di Gauss: il massimo comun divisore è definito a meno di una unità.

I primi/irriducibili di $\mathbf{Z}[i]$ si trovano fra i divisori dei primi/irriducibili di \mathbf{Z} .

2 non è primo in $\mathbf{Z}[i]$.

I primi congrui a 3 modulo 4 sono irriducibili in $\mathbf{Z}[i]$. Se un primo dispari è somma di due quadrati, allora è congruo a 1 modulo 4. Ogni primo congruo a 1 modulo 4 si scrive come somma di due quadrati (solo enunciato). Irriducibili di $\mathbf{Z}[i]$.

Quadrati in $F = \mathbf{Z}/p\mathbf{Z}$. Se p è dispari, ci sono $(p-1)/2$ quadrati non nulli in F , e questi sono le radici del polinomio $x^{(p-1)/2} - 1$.

Se p è un primo dispari, e $a \not\equiv 0 \pmod{p}$, allora

$$a^{(p-1)/2} \equiv \begin{cases} 1 & \text{se } a \text{ è un quadrato, e} \\ -1 & \text{se } a \text{ non è un quadrato.} \end{cases}$$

LEZIONE 26. MERCOLEDÌ 1 GIUGNO 2022 (2 ORE)

(Lezione tenuta da Simone Ugolini)

-1 è un quadrato modulo il primo dispari p se $p \equiv 1 \pmod{4}$. Algoritmo probabilistico per trovare una radice quadrata di -1 modulo $p \equiv 1 \pmod{4}$.

Scrittura di un primo dispari $p \equiv 1 \pmod{4}$ come somma di due quadrati. Esempio.

Terne pitagoriche.

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DEGLI STUDI DI TRENTO, VIA SOMMARIVE
14, 38123 TRENTO

Email address: andrea.caranti@unitn.it

URL: <http://caranti.maths.unitn.it/>