Teoria dei numeri (2013-2014)

– First draft –

Ph. ELLIA

Upgrade 24/5/2014

26 Dicembre 2013

Indice

Parte I

Teoria elementare.

1

Introduzione storica.

La necessità di contare e misurare sono senz'altro all'origine dell'aritmetica e della geometria. Per quanto riguarda l'aritmetica prenderemo come punto di partenza i Pitagorici lasciando agli storici il compito di indagare su quanto sia successo prima.

1.1 Gli Antichi Greci: Pitagora, Euclide e Diofante.

Pitagora.

Si hanno poche certezze storiche sulla vita di Pitagora (600 prima di Cristo circa). Il famoso teorema che gli viene attribuito era già noto dai Babilonesi. La cosa forse più sicura che si può attribuire a Pitagora è la scoperta di intervalli e quindi di una scala musicale. Per i Pitagorici la matematica ha un aspetto mistico. Per esempio due numeri, n, m, sono *amicabili* (o amici) se la somma dei divisori di n (n escluso) è uguale a m e se la somma dei divisori di m (escluso m) è uguale a n. Per esempio 220 e 284 sono amicabili . Un numero amicabile con se stesso è un *numero perfetto*. Quindi 6 è un numero perfetto.

Per i Pitagorici "tutto è numero" cioè proporzioni, come gli intervalli musicali. In termini moderni tutti i numeri erano razionali. Ma questa credenza andò in frantumi quando uno di loro scoprì che un numero molto "naturale", la diagonale di un quadrato di lato uno (cioè $\sqrt{2}$, come segue proprio dal teorema di Pitagora) non era razionale!

Euclide.

Gli Elementi di Euclide (300 prima di Cristo circa) segnano la nascita della matematica come l'unica scienza ipotetico-deduttiva. Per quanto riguarda l'aritmetica, negli Elementi troviamo la nozione di numero primo, l'algoritmo

di Euclide, la divisione euclidea, il Teorema Fondamentale dell'Aritmetica e la dimostrazione del fatto che l'insieme dei numeri primi è infinito. Inoltre troviamo la dimostrazione del fatto che se $n = 2^{p-1}(2^p - 1)$ e se $2^p - 1$ è primo, allora n è perfetto. Eulero dimostrerà poi che ogni numero perfetto pari è necessariamente di questa forma.

Diofante.

Diofante (250 dopo Cristo circa) è il primo a considerare soluzioni intere (o in numeri razionali) di equazioni a più incognite. Le soluzioni proposte sembrano più il frutto di considerazioni ad hoc che di un metodo generale. La rilettura dell'opera di Diofante da parte di Fermat segna la nascita della teoria moderna dei numeri. L'aritmetica (o geometria aritmetica) diofantea è, oggi, quella branca della teoria dei numeri che si occupa di trovare soluzioni intere di equazioni polinomiali.

1.2 Fermat (1601-1665).

Il padre fondatore della teoria dei numeri "moderna" è senza alcun dubbio Pierre de Fermat (1601-1665, la data di nascita non è certa).

Fermat fa parte di una "banda dei quattro": Girard Desargues (1591-1661), René Descartes (1596-1650) e Blaise Pascal (1623-1662). Desargues era un architetto, Descartes (Cartesio) era un soldato di mestiere, matematico e filosofo, Pascal un matematico, filosofo e religioso. Fermat, la cui famiglia faceva parte della piccola borghesia, aveva una carica al Parlamento di Toulouse (Tolosa). Il suo mestiere di tranquillo funzionario gli ha lasciato il tempo di dedicarsi al suo passatempo favorito: la matematica. Dopo vari contributi importanti in analisi (metodo delle tangenti, calcolo infinitesimale), teoria delle probabilità (di cui, insieme a Pascal, gettò le basi), fisica (ottica: principio di Fermat), verso il 1635, dietro l'impulso del Padre Mersenne, iniziò a interessarsi alla teoria dei numeri. Il suo approccio tuttavia fu veramente originale in quanto, contrariamente ai suoi contemporanei, cercò di sviluppare metodi *propri* all'aritmetica, che non fossero delle semplici applicazioni dell'analisi o della geometria a questioni aritmetiche. Purtroppo, a parte il *metodo della discesa infinita*, non abbiamo idea dei metodi usati da Fermat per scoprire i suoi teoremi. Infatti malgrado una corrispondenza abbondante con vari scienziati, Fermat ha lasciato un'unica dimostrazione completa (il caso $n = 4$ dell'equazione di Fermat). Il suo modo di procedere, emblematico di quell'epoca, consisteva nel lanciare delle sfide sotto forma di problemi (di cui evidentemente conosceva la soluzione) o di enunciare, senza dimostrazioni, dei risultati. Dopotutto tutti questi signori facevano matematica per puro diletto. Un'altra fonte importante di informazioni, oltre alla corrispondenza, ci è

pervenuta sotto forma di annotazioni (48) che Fermat aveva posto in margine al suo volume delle opere di Diofante. Dopo la morte di Fermat, suo figlio pubblicò le sue opere complete tra cui queste annotazioni. La seconda è il famoso "teorema di Fermat".

Ecco una lista, non esaustiva, dei risultati enunciati da Fermat. Come abbiamo già detto Fermat non ha mai pubblicato alcuna dimostrazione di questi risultati (tranne il caso $n = 4$ dell'equazione di Fermat), ma non vi sono dubbi che, almeno nella maggior parte dei casi, avesse effettivamente una dimostrazione.

(F1) Per ogni intero a e ogni primo p: $a^p \equiv a \pmod{p}$, ossia se $(a, p) = 1$, $a^{p-1} \equiv 1 \pmod{p}$. Questo enunciato è noto come il *piccolo teorema di Fermat.*

(F2) *(Teorema dei due quadrati):* Un numero primo dispari, p, si scrive come la somma di due quadrati se e solo se $p \equiv 1 \pmod{4}$. Più generalmente un intero n si scrive come la somma di due quadrati se e solo se i primi $\equiv 3 \pmod{4}$ che compaiono nella sua fattorizzazione, compaiono con un esponente pari.

(F3) *(Teorema dei quattro quadrati):* Ogni intero naturale si scrive come la somma di (al più) quattro quadrati.

(F4) Sia p un primo dispari. Allora:

$$p = x^2 + 2y^2, x, y \in \mathbb{N} \Leftrightarrow p \equiv 1, 3 \pmod{8}$$

$$p = x^2 + 3y^2, x, y \in \mathbb{N} \Leftrightarrow p = 3 \text{ o } p \equiv 1 \pmod{3}$$

(F5) *(Caso $n = 3$ dell'equazione di Fermat):* Se x, y, z sono degli interi tali che: $x^3 + y^3 = z^3$, allora $xyz = 0$.

(F6) L'equazione $x^4 + y^4 = z^2$ non ha soluzioni non banali in numeri interi (questo include il caso $n = 4$ dell'equazione di Fermat).

(F7) L'unica soluzione in numeri interi dell'equazione $x^3 = y^2 + 2$ è $x = 3, y = 5$.

(F8) Se D non è un quadrato, l'equazione $x^2 - Dy^2 = 1$ ha un'infinità di soluzioni intere (questa equazione è nota come l'equazione di Pell).

(F9) ogni numero si scrive come la somma di al più tre numeri triangolari (cioè numeri della forma $n(n + 1)/2$).

(F10) Ogni intero della forma $2^{2^n} + 1$ è primo.

Sappiamo oggi che tutte queste affermazioni, tranne l'ultima, sono vere.

I problemi (F2), (F4) sono casi particolari del seguente problema generale: fissato $n \in \mathbb{N}$, quali sono i primi p che si possono scrivere nella forma $x^2 + ny^2$? Questo problema porterà, con i contributi di Eulero, Lagrange, Legendre e Gauss alla teoria delle forme quadratiche intere, alla legge di reciprocità quadratica e dopo (Hilbert, Artin ed altri) alla teoria del campo di classe (*class field theory*). Il problema (F7) (e anche (F3)) ha a che fare con l'aritmetica delle curve ellittiche. Per quanto riguarda (F1), uno dei risultati fondamentali della teoria dei numeri, è il primo test di primalità (ed è proprio per questo che Fermat l'ha fatto in connessione alle sue ricerche sui primi di Mersenne e i numeri perfetti).

L'affermazione più famosa di Fermat non è nella lista precedente. Nel 1637 Fermat scisse nel margine della sua copia delle opere di Diofante la sua famosa nota che si può riassumere nel modo seguente: *Ho trovato una bellissima dimostrazione del fatto che l'equazione* $x^n + y^n = z^n$ (+) *non ha soluzioni intere non banali se* $n \geq 3$*, ma il margine è troppo stretto perché io possa riportarla qui.* Dopo la morte di Fermat suo figlio pubblicò tutti gli scritti di suo padre, note comprese e fu così che l'affermazione di Fermat divenne, per la prima volta, di dominio pubblico. Infatti durante tutta la sua vita, Fermat non menzionò mai nella sua corrispondenza il caso generale dell'equazione (+), ma si limitò ai casi $n = 3, 4$.

L'affermazione di Fermat, nota come congettura di Fermat o ultimo teorema di Fermat (in inglese FLT: Fermat's Last Theorem) è rimasta irrisolta per più di 300 anni. Per risolverla i più grandi matematici hanno inventato teorie nuove, in particolare la teoria degli ideali e la teoria algebrica dei numeri nascono proprio da tentativi per dimostrare l'ultimo teorema di Fermat. Finalmente nel 1995 Wiles, con l'aiuto di Taylor, riuscì a portare a termine un programma iniziato da vari matematici e a dimostrare (tra tante altre cose) la congettura di Fermat. A conferma della difficoltà e ricchezza del problema, la soluzione è arrivata da una parte del tutto inaspettata: la teoria delle curve ellittiche.

Ci si chiede ancora se Fermat avesse o credesse veramente di avere una dimostrazione di FLT. La risposta più ovvia mi sembra la seguente: quando nel 1637 Fermat scrisse la sua famosa nota, iniziava ad interessarsi di teoria dei numeri. Il fatto che non menzionò mai pubblicamente il caso generale del problema lascia pensare che, continuando i suoi studi, si fosse accorto che la sua "bellissima" dimostrazione non era del tutto a posto. L'unica dimostrazione che abbiamo di Fermat è quella del caso $n = 4$ e molto probabilmente sapeva risolvere anche il caso $n = 3$ ed infatti questi due casi sono menzionati nella sua corrispondenza. Visto il carattere di Fermat, se avesse creduto di avere una dimostrazione del caso generale, l'avrebbe detto. Non sentì il bisogno di

correggere la sua famosa nota, semplicemente perché era privata e forse non ha mai immaginato che sarebbe diventa di dominio pubblico. Ecco come nascono le grandi scoperte!

1.3 Eulero (1707-1783)

Eulero venne a conoscenza dei risultati di Fermat tramite il suo amico Goldbach. In una lettera del 1729 Goldbach informa Eulero del 'risultato' di Fermat secondo cui $2^{2^n}+1$ è sempre primo. A questo punto Eulero inizia la lettura delle opere di Fermat e rimane colpito da quello che trova. Nel 1730 scrive a Goldbach che il 'teorema' di Fermat sui quattro quadrati è un *non inelegans theorema*. Nel 1732 Eulero trova un contr'esempio all'affermazione di Fermat mostrando che 641 divide $2^{2^5}+1$. Nei 51 anni rimanenti della sua vita, una delle preoccupazioni maggiori di Eulero sarà di dimostrare tutte le affermazioni di Fermat. Nella maggior parte dei casi ci è riuscito, ma non sempre! Eulero ha generalizzato il piccolo teorema di Fermat, dimostrato il caso $n=3$ dell'equazione di Fermat, dimostrato il teorema dei due quadrati (ma non quello dei quattro quadrati, dimostrato poi da Lagrange) e anche (F4). Nel corso delle sue ricerche sulla rappresentazione dei primi nella forma x^2+ny^2, Eulero ha 'intravisto' la *legge di reciprocità quadratica*, ma non è riuscito a formalizzarla bene e tanto meno a dimostrarla. Un altro contributo fondamentale di Eulero alla teoria dei numeri è l'introduzione delle funzioni ζ, Γ. Eulero è famoso per le sue doti di "calcolatore" spregiudicato. Non esita a scrivere che $1-1+1-1+1-....=\frac{1}{2}$ e cose simili! L'opera matematica di Eulero ha una molle impressionante, in tutti i settori della matematica. In teoria dei numeri il suo contributo è enorme. Un secolo dopo Fermat, Eulero ha rimesso in moto la teoria dei numeri. Molte delle sue intuizioni saranno portate a termine da Lagrange (col quale ha avuto una fitta corrispondenza ma che non ha mai incontrato!).

1.4 Lagrange (1736-1813)

Lagrange (italiano di nascita, tedesco per necessità e francese per scelta) ha dato vari contributi importanti alla teoria dei numeri. In qualche modo è stato il "rifinitore" di Fermat e Eulero (riguardo a vari problemi, ma non tutti). Ha dimostrato il teorema dei quattro quadrati (F3), ha risolto (F8) ("equazione di Pell") e sopratutto ha gettato le basi della teoria delle forme quadratiche intere. Lagrange è stato il primo ad accorgersi che forme "congruenti" (come diciamo oggi) rappresentavano gli stesi interi e quindi ad intraprendere una

classificazione delle forme quadratiche intere modulo "congruenza", un punto di vista molto moderno. Oltre ai suoi lavori in teoria dei numeri Lagrange ha lasciato il segno in tanti altri campi della matematica e della fisica. Per esempio la sua famosa memoria sulla risoluzione delle equazioni algebriche ha aperto la strada a Galois.

1.5 Legendre (1752-1833)

Legendre viene ricordato oggi soprattutto per il simbolo di Legendre $\left(\frac{n}{p}\right)$ e anche per essere stato il primo a formulare in modo chiaro ed inequivocabile la legge di reciprocità quadratica. Legendre pensava di avere dimostrato la legge di reciprocità quadratica, ma la sua dimostrazione usava il teorema di Dirichlet sui primi in una progressione aritmetica (risultato molto più difficile della legge di reciprocità quadratica). Legendre ha comunque dato altri contributi notevoli alla teoria dei numeri.

1.6 Gauss (1777-1855)

Se Fermat era il "principe dei dilettanti" (ma alla sua epoca tutti i matematici erano "dilettanti"), Gauss è il "principe dei matematici". Nel 1801 Gauss pubblica le *Disquisitiones arithmeticae* che si può considerare come un vero spartiacque nella storia della teoria dei numeri. L'opera, oltre a raccogliere in modo organico risultati già noti, introduce molte novità. La prima parte per esempio è dedicata ad una trattazione abbastanza completa delle congruenze (viene addirittura introdotta, per la prima volta, la notazione $a \equiv b \pmod{n}$). Poi i paragrafi sulle forme quadratiche (*composizione, teoria del genere, calcolo del class number di campi quadratici*, prima dimostrazione della legge di reciprocità quadratica) e quelli sui polinomi ciclotomici (e conseguente costruzione con la riga e il compasso del poligono regolare con 17 lati) segnano la nascita della teoria dei numeri "moderna". Il tentativo di capire e generalizzare questi risultati porterà alla teoria di Galois e alla teoria algebrica dei numeri. Gauss riteneva che la legge di reciprocità quadratica fosse il "gioiello" della matematica (ben più importante del teorema fondamentale dell'algebra, un altro suo risultato importante). Nel corso della sua vita ne diede varie dimostrazioni. Anche se la teoria dei numeri è rimasta sempre nel suo cuore (*la matematica è la regina delle scienze e la teoria dei numeri è la regina della matematica*), Gauss nel restante della sua lunga vita non ha pubblicato molto in teoria dei numeri. Scritti trovati dopo la sua morte mostrano però che aveva in serbo altri risultati interessanti (per esempio la teoria dei campi finiti, che sarà fatta

poi da Galois). Per concludere osserviamo che Gauss non conosceva la nozione di gruppo (anche se ha usato il gruppo delle classi!) e non si è mai interessato alla congettura di Fermat, problema che trovava artificiale, non naturale.

Dopo Gauss l'accelerazione, soprattutto ad opera della scuola tedesca è notevole. Dedekind (1831-1916), allievo di Gauss, getta le basi della teoria algebrica dei numeri. Importanti contributi sono dovuti a Kronecker (1823-1891), Kummer (1810-1893), Eisenstein (1823-1852), Minkowski (1864-1909). Nel frattempo Dirichlet (1805-1859) introduce metodi analitici, ma è soprattutto Riemann (1826-1866), un altro allievo di Gauss, ad usare metodi analitici complessi ed ad aprire orizzonti nuovi. La congettura di Riemann è tuttora IL problema aperto della matematica. Lo studio dei lavori e dei metodi di Riemann porteranno Hadamard (1865-1963) e de La Vallée Poussin (1866-1962) a dimostrare (1896), in modo indipendente, il teorema dei numeri primi.

A questo punto possiamo chiudere in bellezza questa breve introduzione con i contributi di Hilbert (1862-1943), uno degli ultimi matematici "universali". Nel 1897 Hilbert pubblica, dietro commissione della Società Matematica Tedesca, il volume *Theorie der algebraischen Zahlkoerper*, meglio noto come il *Zahlbericht*. Questo libro rimarrà per decenni il testo di riferimento della teoria dei numeri. Con questo testo e lavori annessi Hilbert sistema la teoria algebrica dei numeri e la "class field theory". Altri contributi importanti di Hilbert riguardano il problema di Waring.

Dopo Hilbert l'accelerazione è stata ancora maggiore e sono successe tante cose, possiamo riassumerle dicendo che la teoria dei numeri è stata prima elementare, poi algebrica e analitica, adesso è anche geometrica.

2

Il teorema fondamentale dell'aritmetica.

2.1 Divisori di un numero, numeri primi.

Il teorema fondamentale dell'aritmetica, la cui dimostrazione si trova negli *Elementi* di Euclide, afferma che ogni numero naturale si scrive, in modo essenzialmente unico, come un prodotto di numeri primi. Contrariamente al *teorema fondamentale dell'algebra*, il risultato di Euclide è veramente fondamentale e mette in evidenza l'importanza dei numeri primi.

Per iniziare considereremo solo numeri positivi, cioè elementi di $\mathbb{N}$. Se $a, b \in \mathbb{N}$, $b \neq 0$ si dice che b divide a (in simboli $b \mid a$) se esiste $c \in \mathbb{N}$ tale che $a = bc$. Ovviamente 1 divide ogni numero e ogni numero $n > 1$ ha almeno due divisori: 1 e n (i divisori banali).

Definizione 2.1. *Un intero $p \in \mathbb{N}$ è un numero primo se e solo se $p > 1$ e gli unici divisori di p sono quelli banali (1 e p).*

Da questa definizione (che non è quella giusta, come vedremo più avanti) risulta che i numeri primi sono gli "atomi" dei numeri: non si possono dividere in numeri più piccoli. I numeri primi ≤ 20 sono $2, 3, 5, 7, 11, 13, 17, 19$. Chiaramente 2 è l'unico numero primo pari.

I divisori di un numero vanno a coppia: se $b \mid n$, allora $n = ab$ e anche $a \mid n$. Quindi se $Div(n) = \{d_1 = 1, d_2, ..., d_r = n\}$ sono tutti i divisori di n con $d_1 < d_2 < ... < d_r = n$, abbiamo $d_1.d_r = n = d_2.d_{r-1}$, ecc... Quindi i divisori sono "simmetrici" rispetto a $\sqrt{n}$. Infatti se $n = ab$, con $a \leq b$, allora $a \leq \sqrt{n}$ e $b \geq \sqrt{n}$. Abbiamo uguaglianza se e solo se n è un quadrato ($a = b = \sqrt{n}$). In altre parole $\#(Div(n))$ è dispari se e solo se n è un quadrato. Cogliamo l'occasione per definire due funzioni aritmetiche importanti:

Definizione 2.2. *Sia $n > 1$ un intero e sia $Div(n) = \{1 = d_1, d_2, ..., d_r = n\}$ l'insieme dei suoi divisori. Si definisce $\tau(n) = \#Div(n)$ e $\sigma(n) = 1 + d_2 + ... + d_{r-1} + n$ (funzione somma dei divisori).*

Vedere l'Esercizio 7 per le proprietà di base di queste funzioni, per ora osserviamo:

Lemma 2.3. *Con le notazioni precedenti d_2 è primo.*

Dimostrazione. Se d_2 non è primo allora $d_2 = cd$, con $1 < c \leq d < d_2$. Siccome $d_2 \mid n$, anche $c \mid n$, quindi si avrebbe un divisore di n più piccolo di d_2 e > 1, contro la definizione di d_2. □

Corollario 2.4. *Sia $n \in \mathbb{N}$, $n > 1$, allora esiste p primo tale che $p \mid n$. Ossia ogni naturale $n > 1$, ammette un divisore primo.*

Dimostrazione. Se n è primo abbiamo finito. Se n non è primo $Div(n) = \{d_1 = 1, d_2, ..., d_r = n\}$ e d_2, $1 < d_2 < n$, è un divisore primo (Lemma 2.3) di n. □

Quindi il più piccolo divisore > 1 di un numero è sempre un numero primo. Con questa osservazione possiamo subito concludere che l'insieme dei numeri primi è infinito:

Teorema 2.5. (Euclide)
L'insieme dei numeri primi è infinito.

Dimostrazione. Supponiamo che l'insieme dei numeri primi, P, sia finito: $P = \{2 = p_1, 3 = p_2, ..., p_k\}$, $p_1 < ... < p_k$. Sia $N = p_1...p_k + 1$ e sia d_2 il più piccolo divisore > 1 di N (d_2 è ben definito perché $N > 1$). Se $d_2 = N$, allora per il Lemma 2.3, N è primo. Ma questo non è possibile perché $N > p_k$. Quindi $d_2 = p_i$ per un qualche i, $1 \leq i \leq k$. Ma anche questo non è possibile perché:

$$\frac{N}{p_i} = \frac{p_1...p_i...p_k}{p_i} + \frac{1}{p_i}$$

il primo termine è un intero, mentre il secondo, $1/p_i$, non lo è. Quindi abbiamo un assurdo e P è infinito. □

Questa dimostrazione è essenzialmente quella di Euclide. Esistono innumerevoli varianti della dimostrazione di Euclide (cf Esercizio 5 per una di queste). Esiste però una dimostrazione radicalmente diversa, dovuta a Eulero (cf 2.45), all'origine della teoria analitica dei numeri.

Possiamo anche dimostrare facilmente "la prima metà" del Teorema Fondamentale. La dimostrazione usa il principio del minimo : *ogni sotto insieme non vuoto $X \subset \mathbb{N}$ ammette un elemento minimo, x_0. Cioè $\exists x_0 \in X$ tale che $\forall x \in X, x \geq x_0$.*

Il principio del minimo è equivalente al principio di induzione.

Proposizione 2.6. *Ogni numero $n > 1$ si scrive come un prodotto di numeri primi.*

Dimostrazione. Sia $S = \{n > 1 \mid n$ non si scrive come un prodotto di numeri primi $\}$. Se $S \neq \emptyset$, S ammette un elemento minimo, m. Sia d_2 il più piccolo divisore > 1 di m: $m = d_2 a$. Non può essere $m = d_2$ perché d_2 è primo. Quindi $1 < a < m$. Siccome $a \notin S$ e $a > 1$, a si scrive come un prodotto di primi e quindi anche $m = d_2 a$ si scrive come un prodotto di primi, contraddizione. Quindi S è vuoto. □

Rimane la parte difficile: l'unicità della fattorizzazione, bisogna mostrare che se $n = p_1 ... p_t = q_1 ... q_r$, con i p_i, q_j primi, allora $t = r$ e (dopo eventuale riordino degli indici) $p_i = q_i, \forall i$. Si potrebbe essere tentati di procedere così: supponiamo $p_1 < ... < p_t$ e $q_1 < ... < q_r$. Allora $p_1 = q_1 = d_2$ il più piccolo divisore > 1 di n, dividendo per d_2 abbiamo $p_2 ... p_t = q_2 ... q_r$ e andando avanti così si conclude. Sfortunatamente non c'è niente che ci garantisca che il numero primo d_2 debba comparire in ogni fattorizzazione di n. Ci manca ancora un ingrediente per potere affermarlo e questo ingrediente è il famoso lemma di Euclide (detto anche lemma di Gauss, perché è stato Gauss il primo a metterlo in evidenza e a darne una dimostrazione limpida): se un numero primo divide un prodotto, allora divide uno dei fattori: se p primo allora: $p \mid ab \Rightarrow p \mid a$ o $p \mid b$. Con questo risultato è chiaro che deve essere $p_1 = q_1 = d_2$. Il lemma di Euclide *sembra* intuitivamente chiaro: $6 \mid 3.4$ ma $6 \nmid 3$ e $6 \nmid 4$, questo perché 6 si divide in due parti $6 = 2.3$, una parte va a dividere 4 e l'altra 3, ma questo non può succedere con un numero primo che è appunto "indivisibile" o "irriducibile" e quindi deve "entrare" tutto in uno dei due fattori.

Per mostrare che la questione è più sottile di quello che sembra consideriamo l'esempio seguente (dovuto a Hilbert): sia H l'insieme dei numeri della forma $4k + 1$; $H = \{1, 5, 9, 13, ...\}$. Osserviamo che il prodotto di due numeri in H è ancora in H: $(4k + 1)(4m + 1) = 4(4km + k + m) + 1$. Diciamo che un numero $n \in H$ è H-primo se $n > 1$ e i suoi divisori (in H) sono solo quelli banali. Quindi $5, 9, 13, 17, 21$ sono H-primi, mentre $25 = 5.5$ non lo è. Il Lemma 2.3 e la Proposizione 2.6 sono ancora validi in H, con le stesse dimostrazioni. Quindi ogni numero (> 1) di H si scrive come un prodotto di H-primi. Ma $441 = 21^2 = 9.49$ ammette due fattorizzazioni distinte come prodotto di H-primi! La "vera" fattorizzazione è $441 = 3^2.7^2$, ma né 3, né 7 appartengono ad H. Quindi il problema è che H non è *abbastanza grande* (in particolare non è un gruppo additivo). Nulla ci garantisce, a priori, che $\mathbb{N}$ lo sia!

Tornando al nostro teorema ci sono vari modi di concludere, alcuni "elementari", altri meno. Nella prossima sezione vedremo la prima dimostrazione, cioè quella di Euclide.

—— .. ——

Esercizi.

Esercizio 1 *Sia* $Div(n) = \{1 = d_1, d_2, ..., d_r, d_{r+1} = n\}$ *l'insieme dei divisori dell'intero* n *con* $d_1 < d_2 < ... < d_r < n$. *Mostrare che se* $d_2 > \sqrt[3]{n}$, *allora* $n = d_2$ *(quindi* n *è primo) o* d_r *è primo. Dare un esempio di un tale* n.

Esercizio 2 *Siano* $n, a, b \in \mathbb{N}$ *con* $n = ab$. *Mostrare che* $(a + b)/2 \geq \sqrt{n}$. *Quindi se* $a < \sqrt{n} < b$, $|\sqrt{n} - a| < |\sqrt{n} - b|$ *(*a *è più vicino a* $\sqrt{n}$ *di* b*).*

Esercizio 3 *Il problema della fattorizzazione di un numero in fattori primi o comunque come prodotto di numeri più piccoli è molto difficile ed importante. Infatti la crittografia moderna si basa sul fatto che, generalmente, è praticamente impossibile fattorizzare, in un tempo ragionevole, anche usando un computer, un numero molto grande. Fermat a suo tempo aveva escogitato il seguente metodo di fattorizzazione. Se* $n = x^2 - y^2$, *allora* $n = (x+y)(x-y)$.Nel seguito n indica un numero dispari *(è facile vedere che un numero è pari e dividerlo per l'opportuna potenza di due per renderlo dispari).*

1. *Viceversa mostrare che se* $n = ab$ *(*n <u>dispari</u>*), allora* n *si scrive come la differenza di due quadrati.*
2. *Sia* $r \in \mathbb{N}$, $r > (n + 1)/2$, *mostrare che* $r^2 - n$ *non è mai un quadrato.*
3. *Sia* k *il più piccolo intero* $\geq \sqrt{n}$. *Mostrare che se per* $k \leq k+t < (n+1)/2$, *nessun numero* $(k + t)^2 - n$ *è un quadrato allora* n *è primo, altrimenti abbiamo trovato una fattorizzazione non banale di* n.
4. *Mostrare che questo procedimento è più efficace del metodo brutale che consiste nel vedere se esiste un divisore (primo)* d *con* $d \leq \sqrt{n}$, *solo se* n *ha due divisori "vicini" (cioè entrambi vicini a* $\sqrt{n}$*).*
5. *In particolare mostrare che se* n *è il prodotto di due* primi gemelli *(cioè primi della forma* $(p, p + 2)$ *come* $(3, 5), (5, 7), (11, 13), ...$*), il metodo di Fermat trova subito la fattorizzazione di* n.
6. *Fattorizzare* 899 *e* 287, *con il metodo di Fermat e poi con il metodo "brutale".*

Esercizio 4 *Siano* $a, n > 1$ *degli interi positivi.*
(i) Se $N = a^n - 1$ *è primo, allora* $a = 2$ *e* n *è primo (cioè* $N = 2^p - 1$ *è un primo di Mersenne).*
(ii) Se $N = a^n + 1$ *è primo, allora* a *è pari e* n *è una potenza di* 2 *(i primi casi (*$a = 2$*) corrispondono ai numeri di Fermat* $F_n = 2^{2^n} + 1$*).*
(iii) Mostrare che esistono degli interi $a > 2$ *tali che* $a^n + 1$ *sia primo per un qualche* $n > 1$.
(iv) Determinare il più piccolo intero $a > 2$ *tale che* $a^4 + 1$ *sia primo (usare*

un computer!?).
(v) Mostrare che se $2^p - 1$ *è primo, allora* $N = 2^{p-1}(2^p - 1)$ *è un numero perfetto (cioè* $\sigma(N) = 2N$*).*
Osservazione: *si congettura che esistano infiniti primi della forma* $n^2 + 1$ *e che l'insieme dei primi di Mersenne sia infinito, mentre si congettura che* $F_k := 2^{2^k} + 1$ *è primo* $\Leftrightarrow k \leq 4$.

Esercizio 5 *Mostrare che ogni divisore di* $n! + 1$ *è* $> n$*. Concludere che l'insieme dei numeri primi è infinito (questa dimostrazione è dovuta a Hermite).*

2.2 La dimostrazione di Euclide.

La dimostrazione del Teorema Fondamentale usa sostanzialmente un unico fatto: il principio del minimo. Ovviamente non è così che Euclide presenta le cose. Anzi bisognerà aspettare Fermat, col suo *metodo di discesa infinita*, per vedere questo principio usato nelle dimostrazioni.

Il principio del minimo serve due volte: per mostrare l'esistenza di una fattorizzazione (Proposizione 2.6) e per definire la divisione euclidea. Con la divisione euclidea, che è ormai lo strumento fondamentale, si mostra l'esistenza di un massimo comune divisore, inoltre si vede che se $d = (a, b)$, allora $d = au + bv, u, v \in \mathbb{Z}$. Con questo ultimo fatto si mostra facilmente il Lemma di Euclide e quindi l'unicità della fattorizzazione.

Proposizione 2.7. (Divisione euclidea)
Siano $a, b \in \mathbb{N}$ con $b \neq 0$, esistono degli interi $q, r \in \mathbb{N}$ tali che $a = bq + r, 0 \leq r < b$. La coppia (q, r) è univocamente determinata.
Più generalmente se $a, b \in \mathbb{Z}$, $b \neq 0$, esiste un'unica coppia di interi (q, r) tale che $a = bq + r, 0 \leq r < |b|$.

Dimostrazione. Supponiamo $a, b \in \mathbb{N}$, $b \neq 0$. Se $a < b$, $a = 0.b + a$. Supponiamo $a \geq b$. Sia $S = \{n = a - bm \mid n \geq 0\}$. L'insieme S è non vuoto (perché $a - b \in S$). Per il principio del minimo ammette un elemento minimo, sia r questo elemento. Abbiamo $a = qb + r$ e $r < b$ perché altrimenti $a - (q + 1)b = r - b \in S$ con $r - b < r$, contro la definizione di r. Si verifica facilmente l'unicità di (q, r).

Se a o b è negativo basta aggiustare i segni e modificare eventualmente il resto. Per esempio se $a < 0$, $b > 0$: $-a = bq + r$, $a = (-q)b - r = (-q - 1)b + (b - r)$. I dettagli sono lasciati al lettore. □

Un massimo comune divisore (MCD) di due interi a, b è un intero d che divide sia a che b e tale che se $c \mid a$ e $c \mid b$, allora $c \mid d$. Il MCD è determinato a meno del segno, si usa considerare quello positivo e si scrive $(a, b) = d$; a e b sono *primi tra di loro* se $(a, b) = 1$.

Proposizione 2.8. *Siano $a, b \in \mathbb{Z}$ due interi non nulli, allora il loro MCD esiste e se $d = (a, b)$, si ha $d = au + bv$, $u, v \in \mathbb{Z}$.*

Dimostrazione. Sia $S = \{am + bn \mid m, n \in \mathbb{Z}, am + bn > 0\}$. L'insieme $S \subset \mathbb{N}$ è non vuoto ($|a| = ea + b.0$ con $e \pm 1$ a seconda del segno di a appartiene ad S). Sia d il suo elemento minimo. Per definizione $d = au + bv$ per opportuni interi. Per la divisione euclidea: $a = dq + r$, $0 \leq r < d$. Abbiamo $r = 0$, altrimenti $r = a - dq = a - (au + bv)q = a(1 - uq) + b(-vq) \in S$, contro la minimalità di d. Quindi $d \mid a$. Nello stesso modo $d \mid b$. Se c divide a e b, allora $c \mid d = au + bv$. □

L'algoritmo di Euclide fornisce un modo, i casi concreti, per determinare (a, b). Nella relazione $d = au+bv$, u o v possono essere negativi (è sicuramente il caso se $(a, b) = 1$) e non so come se la sbrogliasse Euclide (gli Antichi Greci non conoscevano i numeri negativi ma evidentemente sapevano sottrarre numeri positivi!).

Finalmente abbiamo:

Lemma 2.9. (Lemma di Euclide)
Se $a \mid bc$ e $(a, b) = 1$, allora $a \mid c$. In particolare se p è primo e $p \mid ab$, allora $p \mid a$ o $p \mid b$.
Più generalmente se $p \mid a_1...a_n$, allora esiste i tale che $p \mid a_i$.

Dimostrazione. Se $(a, b) = 1$ allora $au + bv = 1$, moltiplicando per c: $acu + bcv = c$, siccome a divide il membro di sinistra ($a \mid a$ e $a \mid bc$), abbiamo $a \mid c$. L'ultima parte si dimostra per induzione su n. Il caso $n = 2$ è stato appena fatto, supponiamo l'asserto vero per gli interi $< n$. Abbiamo $p \mid a_1.(a_2...a_n)$. Se $p \mid a_1$, abbiamo finito, altrimenti $p \mid a_2...a_n$ e si conclude per induzione. □

A questo punto abbiamo tutto quello che serve:

Teorema 2.10. (Teorema Fondamentale)
Ogni intero $n > 1$ si scrive come un prodotto di numeri primi e questa fattorizzazione è unica a meno dell'ordine dei fattori.

Dimostrazione. Abbiamo già visto l'esistenza della fattorizzazione (Proposizione 2.6). Mostriamo l'unicità per induzione su n. Il caso $n = 2$ è chiaro. Sia $n = p_1...p_t = q_1...q_r$. Abbiamo $p_1 \mid q_1...q_r$, quindi $p_1 \mid q_i$ per un qualche i, siccome p_1, q_i sono primi, questo implica $p_1 = q_i$. Riordinando gli indici possiamo assumere $i = 1$. Abbiamo $n/p_1 = p_2...p_t = q_2...q_r$ e si conclude per induzione. □

Il punto cruciale è quindi il Lemma di Euclide, che come vedremo più avanti, non è altro che la *buona* definizione di numero primo.

—— .. ——

Esercizi.

Esercizio 6 *Sia p un numero primo e siano $a, b \in \mathbb{N}$.*
(1) Se $0 < a < p$ e $0 < b < p$, mostrare che $p \nmid ab$.
(2) Dedurre da (1) che se $p \mid ab$ allora $p \mid a$ o $p \mid b$ (lemma di Euclide).
Osservazione: Questo fornisce una dimostrazione alternativa del Teorema Fondamentale dell'Aritmetica.

Esercizio 7 *Siano $\sigma(n) = 1 + d_2 + ... + n$ ($Div(n) = \{1, d_2, ..., d_r, n\}$) e $\tau(n) = \#Div(n)$.*
(i) Calcolare $\sigma(p^r), \tau(p^r)$, dove p è un numero primo.
(ii) Se $(m, n) = 1$, allora $\sigma(mn) = \sigma(m)\sigma(n)$, $\tau(mn) = \tau(m).\tau(n)$.
Osservazione: *Una funzione definita su $\mathbb{N}^*$ (a valori in $\mathbb{R}$ o $\mathbb{C}$) è detta* funzione aritmetica*. Una funzione aritmetica f è detta* moltiplicativa *se $(m, n) = 1 \Rightarrow f(mn) = f(m)f(n)$. Una funzione aritmetica moltiplicativa è completamente determinata dai valori $f(p^a), p$ primo, $a \in \mathbb{N}$. Le funzioni σ, τ sono moltiplicative.*
(iii) Sia $s(n) = \sigma(n) - n$ (la somma dei divisori, escluso il numero). La funzione aritmetica s è moltiplicativa?
(iv) Mostrare che $\tau(n) < 2\sqrt{n}$ e $\sigma(n) \leq \dfrac{n(n-1)}{2} + 1$ ($n \neq 2$).
(v) Mostrare che $\sigma(n)$ è dispari se e solo se n è un quadrato o due volte un quadrato. Cosa potete dire della parità di $\tau(n)$?

Esercizio 8 *Siano f, g due funzioni aritmetiche. La loro convoluzione, $f * g$, è definita da: $(f * g)(n) = \sum_{d|n} f(d).g(n/d)$.*
(i) Mostrare che $f * g = g * f$ e che $f * (g * h) = (f * g) * h$.
(ii) Sia e la funzione aritmetica definita da: $e(1) = 1$, $e(n) = 0$ se $n > 1$. Mostrare che $f * e = f$.
(iii) Sia u la funzione aritmetica definita da $u(n) = 1, \forall n$ e sia Id l'identità ($Id(n) = n, \forall n$). Mostrare che: $Id * u = \sigma$, $u * u = \tau$.
*(iv) Sia μ la funzione aritmetica (*funzione di Moebius*) definita nel modo seguente: $\mu(1) = 1$ e se $n > 1$, con fattorizzazione in primi: $n = \prod_{i=1}^{k} p_i^{a_i}$, allora:*

$$\mu(n) = \begin{cases} 0 \text{ se esiste } j \mid a_j > 1 \\ (-1)^k \text{ se } a_i = 1, \forall i \end{cases}$$

Mostrare che μ è moltiplicativa e che $\mu * u = e$, cioè:

$$\sum_{d|n} \mu(d) = \begin{cases} 1 \text{ se } n = 1 \\ 0 \text{ se } n > 1 \end{cases}$$

(v) Mostrare il Teorema di inversione di Moebius:

$$f(n) = \sum_{d|n} g(d) \Leftrightarrow g(n) = \sum_{d|n} f(d)\mu(n/d).$$

Esercizio 9 *Scopo di questo esercizio è di migliorare la stima di $\sigma(n)$ dell'Esercizio 7. Sia*

$$H_n := 1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{n} = \sum_{k=1}^{n} \frac{1}{k}$$

H_n è l'n-esimo numero armonico.
(i) Mostrare che $H_n - 1 < \log n < H_{n-1}$ (usare $\log n = \int_1^n \frac{1}{x} dx$).
(ii) Dedurre da (i) che: $\sigma(n) < n \log n + n$.
(iii) Si ricorda (notazione di Landau) che $f(x) << g(x)$ quando $x \to +\infty$ se esiste una costante C e un x_0 tali che: $x > x_0 \Rightarrow f(x) \leq Cg(x)$. Mostrare che: $\sigma(n) << n \log n$ (quando $n \to +\infty$).

Esercizio 10 *Un intero $n > 1$ è* abbondante *se $s(n) > n$,* diffetoso *se $s(n) < n$ e* perfetto *se $s(n) = n$ (come al solito $s(n) = \sigma(n) - n$). Queste definizioni risalgono all'Antichità.*
(i) Determinare il più piccolo numero difettoso pari (risp. dispari).
(ii) Determinare il più piccolo numero abbondante pari. Con l'aiuto di un computer determinare il più piccolo numero abbondante dispari.
(iii) Mostrare che se δ è perfetto o abbondante e se $\delta \mid n$, $\delta < n$, allora n è abbondante.
(iv) Secondo voi tra i numeri interi (risp. interi pari, dispari) ci sono più numeri abbondanti o più numeri difettosi?

2.3 Divisibilità in un anello integro.

Anche se la dimostrazione del Teorema Fondamentale ha un sapore squisitamente aritmetico s'inquadra in un contesto algebrico più generale che ci sarà utile nel seguito. Vale dunque la pena vedere l'algebra dietro questa dimostrazione.

Nel seguito indicheremo con A un anello *integro, commutativo*, si dice anche che A è un *dominio*. Se a, b sono due elementi non nulli di A si dice che a divide b (in simboli $a \mid b$) se esiste $c \in A$ tale che $ac = b$. Questo è equivalente a richiedere $(b) \subset (a)$, dove $(x) = \{tx \mid t \in A\}$ è l'ideale principale generato da x.

Definizione 2.11. *In un dominio A:*

1. *un elemento $e \in A$ è un'*unità *se e è invertibile ($\exists e'$ t.c. $ee' = 1$)*
2. *a e b sono* associati *se $a = be$ dove e è un'unità (si scrive $a \sim b$)*
3. *$q \in A$ è* irriducibile *se q non è un'unità e se $q = ab \Rightarrow a$ o b è un'unità.*
4. *$p \in A$ è* primo *se p non è un'unità e se $p \mid ab \Rightarrow p \mid a$ o $p \mid b$. Quest'ultima condizione è equivalente a richiedere che (p) sia un ideale primo (cioè che $A/(p)$ sia un anello integro).*

Esempio 2.12. Le unità di $\mathbb{Z}$ sono ± 1; le unità di $k[X]$ (k un campo) sono gli elementi di k^*. In $\mathbb{Z}$ 2 e -2 sono associati.

Osservazione 2.13. La definizione data di numero primo (Definizione 2.1) è in realtà la definizione di elemento *irriducibile*: se $p = ab$, allora $a \mid p$ quindi $a = 1$ (risp. p) e $b = p$ (risp. 1), cioè a o b è un'unità. Il Lemma di Euclide dice che in $\mathbb{Z}$ un elemento irriducibile è primo.

Osservazione 2.14. In un anello integro un elemento primo è sempre irriducibile (il viceversa non è sempre vero, Esercizio 11).

Definizione 2.15. *Un dominio A è:*

1. principale *(PID* principal ideal domain*) se ogni ideale $I \subset A$ è della forma $I = (a)$ (i.e. generato da un unico elemento).*
2. fattoriale *(UFD* unique factorization domain*) se ogni elemento ammette un'unica (modulo ordine dei fattori ed associati) fattorizzazione in elementi irriducibili.*

Cerchiamo di capire meglio cos'è un anello fattoriale. Intanto osserviamo che:

Lemma 2.16. *In un anello integro A: $(a) = (b) \Leftrightarrow a \sim b$ (a e b sono associati).*

Dimostrazione. Esercizio 11. □

Definizione 2.17. *Un anello integro A è* principalmente noetheriano *se ogni successione crescente di ideali principali è stazionaria.*

La terminologia (forse non ottimale) non è usuale.

Lemma 2.18. *Sia A un anello integro principalmente neotheriano.*

1. *Ogni $a \in A$, $a \neq 0$, a non unità, ammette un divisore irriducibile.*
2. *Ogni $a \in A$, $a \neq 0$, a non unità, si scrive come un prodotto di elementi irriducibili.*

Dimostrazione. (1) Se a è irriducibile, abbiamo finito. Se a non è irriducibile allora $a = xy$, dove x, y non sono delle unità. Se x è irriducibile abbiamo finito. Altrimenti $x = a_1 d_1$, a_1, d_1 non unità, quindi $a = a_1 d_1 y$. Abbiamo $a_1 \mid x \mid a$, cioè $(a) \subset (x) \subset (a_1)$. Se a_1 non è irriducibile allora $a_1 = a_2 d_2$, a_2, d_2 non unità e $(a) \subset (x) \subset (a_1) \subset (a_2)$. Andando avanti così se a_i non è irriducibile $a_i = a_{i+1} d_{i+1}$, a_{i+1}, d_{i+1} non unità e $(a) \subset (x) \subset (a_1) \subset ... \subset (a_i) \subset (a_{i+1}) \subset$ .... Siccome A è principalmente noetheriano esiste n tale $(a_n) = (a_{n+1})$. Per il Lemma 2.16, $a_n = \varepsilon a_{n+1}$, ε un'unità. Quindi $\varepsilon a_{n+1} = a_n = d_{n+1} a_{n+1}$. Segue che $a_{n+1}(d_{n+1} - \varepsilon) = 0$. Siccome A è integro e $a_{n+1} \neq 0$ (perché $a \neq 0$), abbiamo $d_{n+1} = \varepsilon$, contro l'ipotesi. Questo mostra che a_n è irriducibile.
(2) Se a è irriducibile abbiamo finito, altrimenti per (1), a ammette un divisore irriducibile proprio, q_1: $a = d_1 q_1$. Se d_1 è irriducibile abbiamo finito, altrimenti d_1 ammette un divisore irriducibile q_2: $d_1 = d_2 q_2$. Andando avanti così otteniamo: $(a) \subset (d_1) \subset (d_2) \subset$ .... Siccome A è principalmente noetheriano, esiste n tale che $(d_n) = (d_{n+1})$. Quindi $d_{n+1} = \varepsilon d_n$ e da $d_n = d_{n+1} q_{n+1}$ segue che q_{n+1} è invertibile: assurdo. Quindi d_n è irriducibile e a si scrive come prodotto di elementi irriducibili. □

Questa è esattamente la dimostrazione standard del fatto che ogni intero si scrive come un prodotto di primi, l'ipotesi "principalmente noetheriano" fa la parte del principio del minimo.

Passiamo adesso alla seconda parte del Teorema Fondamentale cioè l'unicità della fattorizzazione:

Proposizione 2.19. *Sia A un anello integro. Sono equivalenti:*

1. *A è principalmente noetheriano e ogni elemento irriducibile è primo*
2. *Ogni $a \in A$, $a \neq 0$, a non invertibile si scrive come un prodotto di elementi primi*
3. *A è fattoriale (i.e. ogni $a \neq 0$, non unità, si scrive in modo <u>unico</u> come prodotto di irriducibili).*

Dimostrazione. (1) $\Rightarrow$ (2): Segue dal Lemma 2.18 visto che ogni irriducibile è primo.
(2) $\Rightarrow$ (3): Siccome ogni primo è irriducibile, basta mostrare l'unicità della fattorizzazione (a meno di unità). Sia $p_1...p_r = q_1...q_s$, dove i p_i sono primi e dove i q_j sono irriducibili. Siccome $p_1 \mid q_1...q_s$, p divide uno dei fattori, diciamo $dp = q_j$. Siccome q_j è irriducibile questo implica d unità cioè $p \sim q_j$ e si conclude nel solito modo. (Osservare che ogni irriducibile q è primo: q si scrive come un prodotto di primi, quindi ha un divisore primo $q = pd$ e q irriducibile implica d unità, quindi q è primo).
(3) $\Rightarrow$ (1): Mostriamo che ogni elemento irriducibile q è primo. Sia $q \mid ab$. Quindi $qd = ab$. Ogni elemento ha una fattorizzazione unica in irriducibili: $d = l_1...l_t$, $a = q_1...q_r$, $b = Q_1...Q_k$. Quindi: $q.\prod l_i = \prod q_j.\prod Q_g$. Per unicità deve essere $q = q_{j_0}$ o $q = Q_{g_0}$, cioè $q \mid a$ o $q \mid b$.

Mostriamo che A è principalmente noetheriano: sia $(a_1) \subset (a_2) \subset ... \subset (a_n) \subset ....$ Sia $a_1 = q_1...q_n$ la fattorizzazione di a_1 in irriducibili (=primi), i q_i non necessariamente distinti. Abbiamo $a_2 \mid a_1$, quindi ogni primo nella fattorizzazione di a_2 compare in quella di a_1, inoltre se l'inclusione è stretta $a_1 \neq a_2$ e quindi a_2 ha $< n$ fattori nella sua fattorizzazione. Andando avanti così arriviamo ad un a_i con un unico fattore nella sua fattorizzazione, cioè a_i primo. Abbiamo $a_i = a_{i+1}d$. Siccome a_i è irriducibile a_{i+1} o d è un'unità. Nel primo caso $(a_{i+1}) = A$ e quindi $(a_j) = A$ se $j > i$; nel secondo caso $(a_i) = (a_{i+1})$. Ripetendo il ragionamento vediamo che: $(a_n) = (a_i)$ se $n > i$ oppure esiste j tale $(a_n) = A$ se $n > j$. La successione è comunque stazionaria. □

Osservazione 2.20. Un anello A è fattoriale $\Leftrightarrow$ ogni elemento non nullo, non invertibile ammette una fattorizzazione in elementi primi. Non si richiede *l'unicità* della fattorizzazione. Se invece vogliamo caratterizzare un anello fattoriale tramite l'esistenza di una fattorizzazione in irriducibili, bisogna richiedere l'unicità.

In un anello fattoriale: primo $\Leftrightarrow$ irriducibile.

Si potrebbe essere tentati di pensare che un anello noetheriano è fattoriale, ma questo non è vero (Esercizio 12).

Dimostrare il Teorema Fondamentale per un anello A torna a dimostrare che A è fattoriale. A priori questo non è una cosa facile. Per quanto riguarda $\mathbb{Z}$ (o $k[x]$) si usa il seguente giro:

A euclideo $\Rightarrow$ A principale $\Rightarrow$ A fattoriale.

In un anello principale le nozioni di elemento primo e irriducibile sono equivalenti:

Lemma 2.21. *Se A è principale (PID) e $p \in A$, le seguenti affermazioni sono equivalenti:*

1. p è primo
2. p è irriducibile
3. (p) è massimale.

Dimostrazione. (1) $\Rightarrow$ (2): se $p = ab$, allora $p \mid a$ o $p \mid b$ perché p è primo. Diciamo $a = pc$. Allora $p = pcb$, ossia $p(1 - cb) = 0$, siccome A è integro e $p \neq 0$, $cb = 1$ e b è un'unità. Quindi p è irriducibile.

(2) $\Rightarrow$ (3): sia $(p) \subset I$ dove I è un ideale di A. Abbiamo $I = (b)$ perché A è principale. Quindi $p = bc$. Siccome p è irriducibile b o c è un'unità. Se b è invertibile $1 = b^{-1}b \in I$ e $I = A$; se c è invertibile $b = c^{-1}p \in (p)$ e $I = (p)$. Quindi (p) è massimale.

(3) $\Rightarrow$ (1): Se (p) è massimale $A/(p)$ è un campo quindi in particolare un anello integro e quindi (p) è primo. □

Corollario 2.22. *Un anello principale è fattoriale (PID $\Rightarrow$ UFD).*

Dimostrazione. Un anello principale è ovviamente noetheriano (perché ogni ideale è finitamente generato, da un elemento), quindi principalmente noetheriano. Inoltre ogni irriducibile è primo (Lemma 2.21. Si conclude con la Proposizione 2.19. □

Osservazione 2.23. Abbiamo usato la caratterizzazione ben nota degli anelli noetheriani: sia A un anello commutativo, sono equivalenti:

1. ogni ideale $I \subset A$ è finitamente generato
2. ogni successione crescente di ideali è stazionaria
3. ogni collezione non vuota di ideali ammette un elemento massimale (per l'inclusione)

Osservazione 2.24. Si ricorda inoltre che:
A fattoriale $\Rightarrow A[X]$ fattoriale
A noetheriano $\Rightarrow A[X]$ noetheriano.
Quindi $k[X_1, ..., X_n]$ (k un campo) è fattoriale e noetheriano ma non principale se $n > 1$.

Definizione 2.25. *Un anello integro A è* euclideo *se esiste $f : A^* \to \mathbb{N}$ tale che per ogni $a, b \in A$, $b \neq 0$, esistano $q, r \in A$ tali che $a = bq + r$, con $r = 0$ o $f(r) < f(b)$.*

Osservazione 2.26. Certi autori richiedono inoltre che si abbia $f(b) \leq f(ab)$.

Proposizione 2.27. *Un anello euclideo è principale.*

Dimostrazione. Sia $I \subset A$ un ideale dell'anello euclideo A. Sia $X = \{f(a) \mid a \in I, a \neq 0\}$. Allora $X \subset \mathbb{N}$ è non vuoto ($I \neq (0)$) e quindi ammette un elemento minimo n_0. Sia $a \in I$ con $f(a) = n_0$. Se $b \in I$, allora $b = aq + r$. Abbiamo $r = b - aq \in I$, quindi per minimalità $r = 0$ e $b = aq$, pertanto $I = (a)$. □

Con questi risultati abbiamo una dimostrazione "algebrica" del Teorema Fondamentale dell'aritmetica, dall'esistenza della divisione euclidea otteniamo:

Corollario 2.28. *L'anello $\mathbb{Z}$ è euclideo, quindi principale e fattoriale. Un elemento è primo se e solo se è irriducibile (lemma di Euclide) e ogni elemento si scrive in modo unico (a meno di unità) come un prodotto di elementi primi.*

Ovviamente, ed è questo l'interesse di questo approccio, le stesse conclusioni valgono per ogni anello euclideo (per esempio $k[x]$).

—— .. ——

Esercizi.

Esercizio 11 *Sia A un anello integro.*
(i) Se $p \in A$ è primo, allora p è irriducibile.
(ii) Mostrare che $(a) = (b) \Leftrightarrow a \sim b$ (a e b sono associati).
(iii) Siano $a \sim b$. Allora a è primo (risp. irriducibile) se e solo se b lo è.

Esercizio 12 *Mostrare che $A = k[x, y, z]/(x^2 - yz)$ è un anello noetheriano integro non fattoriale.*
Mostrare che $B = k[X_1, ..., X_n, ...]$ è un anello fattoriale non noetheriano.

Esercizio 13 *Sia $\omega = i\sqrt{5}$ e sia $A = \{a + \omega b \mid a, b \in \mathbb{Z}\}$. In altri termini $A = \mathbb{Z}[\sqrt{-5}]$.*

1. *Mostrare che A è un sotto anello di $\mathbb{C}$.*
2. *Se $\alpha = a + \omega b \in A$ si definisce $N(\alpha) = a^2 + 5b^2 = (a + \omega b)(a - \omega b)$ (si dice che N è la* norma *di A). Mostrare che $\forall \alpha, \beta \in A$: $N(\alpha\beta) = N(\alpha)N(\beta)$.*
3. *Mostrare che 2 è irriducibile in A (usare la norma).*
4. *Nello stesso modo vedere che 3, $1 - \omega$, $1 + \omega$ sono irriducibili.*
5. *Osservare che $6 = 2 \cdot 3 = (1 - \omega) \cdot (1 + \omega)$. Concludere che A non è fattoriale.*
6. *Mostrare che $2 \mid (1 + \omega)^2$, ma $2 \nmid 1 + \omega$. Concludere che 2 è irriducibile ma non primo.*

Esercizio 14 *Sia $n > 1$ un intero. Si ricorda che n è* perfetto *se e solo se $\sigma(n) = 2n$, dove σ è la funzione "somma dei divisori" (cf Esercizio 7).*

1. *Mostrare che $\sigma(n) - n$ divide n se e solo se n è primo o n è perfetto.*
2. *Sia n un numero perfetto pari. Quindi $n = 2^{m-1}q$, con q dispari. Mostrare che $(2^m - 1)(\sigma(q) - q) = q$.*
3. *Concludere che ogni numero perfetto pari è della forma $n = 2^{p-1}(2^p - 1)$, dove $q = 2^p - 1$ è primo (e quindi p è primo, cf Esercizio 4).*

Questo risultato è dovuto a Eulero. Insieme al risultato di Euclide (Esercizio 4 punto (v)) questo mostra che la ricerca dei numeri perfetti pari si riconduce a quella dei primi di Mersenne, cioè i primi della forma $2^p - 1$. Al giorno d'oggi (3-3-2014) si conoscono 48 primi di Mersenne, il più grande è $2^{57\,885\,161} - 1$ e ha $17\,425\,170$ cifre. Si congettura che non esista nessun numero perfetto dispari.

Esercizio 15 *Se $n > 1$ è un intero si pone $h(n) := \sigma(n)/n$. Inoltre se $n = \prod_{i=1}^{k} p_i^{a_i}$ è la fattorizzazione in numeri primi ($p_i \neq p_j$ se $i \neq j$), si pone $\omega(n) =$*

k.

(1) Se p è primo, mostrare che $h(p^a) < p/(p-1)$.

(2) Sia n un numero perfetto pari. Osservare che $\omega(n) = 2$.

(3) Sia n un numero perfetto dispari. Mostrare che $\omega(n) > 2$.

2.4 Distribuzione dei numeri primi: un assaggio.

2.4.1 Generalità.

Il teorema di Euclide afferma che l'insieme dei numeri primi è infinito, ma non dice nulla su "quanto" sia grande questa infinità e su come siano distribuiti i numeri primi.

Nel seguito indicheremo con $p_1 = 2, p_2 = 3, ..., p_n, ...$ la successione crescente dei numeri primi. Quindi p_n è l'n-esimo numero primo. Dalla dimostrazione di Euclide risulta che $p_n \leq p_1 p_2 ... p_{n-1} + 1$. Questa osservazione porta alla seguente stima:

Lemma 2.29. *Se p_n è l'n-esimo numero primo, allora $p_n \leq 2^{2^{n-1}}$.*

Dimostrazione. Esercizio 16. □

Per studiare la distribuzione dei numeri primi si introduce la funzione $\pi(x)$:

Definizione 2.30. *La funzione $\pi : \mathbb{R}_{>0} \to \mathbb{N}$ è definita da $\pi(x) = \#\{p \mid p$ primo, $p \leq x\}$.*

Una prima stima di $\pi(x)$:

Lemma 2.31. *Con le notazioni precedenti, per $x \geq 2$:*

$$\pi(x) > \frac{\log(\log x)}{\log 2} > \log(\log x).$$

Dimostrazione. Sia $x \geq 2$. Esiste un intero positivo l tale che $2^{2^{l-1}} \leq x < 2^{2^l}$. Per il Lemma 2.29, $p_l \leq 2^{2^{l-1}}$. Quindi $\pi(x) \geq l$. Prendendo il logaritmo nella disuguaglianza $x < 2^{2^l}$, viene: $2^l > \log x / \log 2$. Riprendendo ancora il logaritmo: $l \log 2 > \log(\log x / \log 2)$. Siccome $\log 2 > 0$: $\pi(x) \geq l > [\log(\log x) - \log(\log 2)] / \log 2$. Siccome $\log 2 < 1$, $\log(\log 2) < 0$, quindi: $\pi(x) \geq l > \log(\log x)/\log 2 > \log(\log x)$. □

Questa stima può essere migliorata senza troppe difficoltà:

Lemma 2.32. *Per $x \geq 2$, abbiamo:*

$$\pi(x) \geq \frac{\log x}{2 \log 2}$$

Inoltre se p_n è l'n-esimo numero primo, allora: $4^n \geq p_n, n \geq 1$.

Dimostrazione. Sia $x \geq 1$ un intero e sia $2 = p_1 < p_2 < ... < p_j \leq x$ (quindi $\pi(x) = j$). Se $n \leq x$ è un intero scriviamolo nella forma $n = l^2 m$, dove m è senza fattori quadrati. Quindi $m = p_1^{\varepsilon_1} ... p_j^{\varepsilon_j}$, con $\varepsilon_i \in \{0, 1\}$.

Siccome $l^2 \leq n \leq x$, abbiamo $l \leq \sqrt{x}$. Ci sono quindi al più $\sqrt{x}$ possibilità per scegliere l. D'altra parte ci sono al più 2^j possibilità per m (a seconda dei valori degli ε_i). Siccome ci sono x valori possibili per n, concludiamo che: $x \leq 2^j \sqrt{x}$. Cioè: $2^j \geq \sqrt{x}$ $(*)$. Pertanto $j \log 2 \geq \log x/2$ e quindi $\pi(x) = j \geq \log x/(2 \log 2)$.

Se in $(*)$ prendiamo $x = p_n$, allora $j = n$ e $2^n \geq \sqrt{p_n}$, quindi $4^n = 2^{2n} \geq p_n$. □

2.4.2 Le stime di Tchebyshev.

Nel 1850 il matematico russo Tchebyshev (o Chebyshev), ha dimostrato, con metodi elementari, limiti molto precisi per $\pi(x)$. Più precisamente Tchebyshev ha dimostrato:

$$c_1 \frac{x}{\log x} \leq \pi(x) \leq c_2 \frac{x}{\log x} \tag{2.1}$$

per $x \geq 10$, dove $c_1 \simeq 0,921292$ e dove $c_2 = 6c_1/5 \simeq 1,1055$.

Mostriamo adesso una versione più debole delle stime originali di Tchebyshev, ma la cui dimostrazione, sempre nello stile di Tchebyshev, è più facile:

Teorema 2.33. (Tchebyshev)
Per $x \geq 2$:

$$\left(\frac{3 \log 2}{8}\right) \frac{x}{\log x} \leq \pi(x) \leq (6 \log 2) \frac{x}{\log x}.$$

Osservazione 2.34. Abbiamo $\log 2 \simeq 0,69314$. Quindi $3 \log 2/8 \simeq 0,256$, mentre $6 \log 2 \simeq 4,159$.

La dimostrazione, seppure elementare, è più digeribile, se spezzetta in vari lemma.

Si ricorda che $\lfloor x \rfloor$ indica la parte intera di x.

Lemma 2.35. *Sia p un numero primo e sia $v_p(n!)$ l'esponente di p nella fattorizzazione in numeri primi di $n!$. Allora:*

$$v_p(n!) = \sum_{k \geq 1} \lfloor \frac{n}{p^k} \rfloor.$$

Dimostrazione. La dimostrazione è per induzione su n. Per $n = 1$, l'enunciato è vero in quanto $\lfloor \frac{1}{p^k} \rfloor = 0$, $\forall p, \forall k$.

Supponiamo l'enunciato vero per n e sia $n + 1 = p^u m$, con $p \nmid m$. Siccome $(n + 1)! = n!(n + 1)$, viene $v_p((n + 1)!) = v_p(n!) + u$. Quindi, per ipotesi di induzione, $v_p(n + 1)!) = \sum_{k\geq 1} \lfloor \frac{n}{p^k} \rfloor + u$. Adesso $\sum_{k\geq 1} \lfloor \frac{n}{p^k} \rfloor + u = \sum_{k=1}^{u} \left(\lfloor \frac{n}{p^k} \rfloor + 1 \right) + \sum_{k>u} \lfloor \frac{n}{p^k} \rfloor$.

Per concludere basta osservare (cf Esercizio 17) che $\lfloor \frac{n}{p^k} \rfloor + 1 = \lfloor \frac{n+1}{p^k} \rfloor$, se $k \leq u$, mentre se $k > u$: $\lfloor \frac{n}{p^k} \rfloor = \lfloor \frac{n+1}{p^k} \rfloor$. □

Lemma 2.36. *Per $n > 1$, $\binom{2n}{n}$ divide $\prod_{p<2n} p^{r_p}$, dove r_p è l'unico intero tale che: $p^{r_p} \leq 2n < p^{r_p+1}$.*

Dimostrazione. Per via del Lemma 2.35 l'esponente con il quale p compare nella fattorizzazione di $\binom{2n}{n}$ è $v_p((2n)!) - v_p((n!)^2) = v_p((2n)!) - 2v_p(n!) = \sum_{k\geq 1} \left(\lfloor \frac{2n}{p^k} \rfloor - 2\lfloor \frac{n}{p^k} \rfloor \right)$. Si verifica facilmente che $\forall y \in \mathbb{R}$: $\lfloor 2y \rfloor - 2\lfloor y \rfloor \in \{0, 1\}$. Siccome $\lfloor \frac{2n}{p^k} \rfloor = 0$ se $k > r_p$ segue che $\sum_{k\geq 1} \left(\lfloor \frac{2n}{p^k} \rfloor - 2\lfloor \frac{n}{p^k} \rfloor \right) \leq r_p$, pertanto $p \mid \prod_{p<2n} p^{r_p}$. □

La prima metà del teorema 2.33:

Proposizione 2.37. *Per $x \geq 2$ si ha:*

$$\pi(x) > \frac{3 \log 2}{8} \frac{x}{\log x}.$$

Dimostrazione. Con le notazioni del Lemma 2.36, abbiamo:

$$\prod_{p<2n} p^{r_p} \leq \prod_{p<2n} 2n = (2n)^{\pi(2n)} \tag{2.2}$$

Siccome, sempre per il Lemma 2.36, $\binom{2n}{n} \mid \prod_{p<2n} p^{r_p}$, segue che:

$$\binom{2n}{n} \leq (2n)^{\pi(2n)} \tag{2.3}$$

Abbiamo: $(1 + 1)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k}$ e $\binom{2n}{n} \geq \binom{2n}{k}, 0 \leq k \leq 2n$ (Esercizio 18). Segue che:

$$(2n + 1)\binom{2n}{n} \geq \sum_{k=0}^{2n} \binom{2n}{k} = 2^{2n}$$

Quindi:

$$\binom{2n}{n} \geq \frac{2^{2n}}{2n+1} \tag{2.4}$$

D'altra parte: $\dfrac{2^{2n}}{2n+1} > 2^n$, se $n \geq 3$ (Esercizio 18). Combinando (2.3), (2.4), viene, se $n \geq 3$:

$$(2n)^{\pi(2n)} > 2^n$$

Quindi: $\pi(2n) > \dfrac{n \log 2}{\log 2n} = \left(\dfrac{\log 2}{2}\right)\left(\dfrac{2n}{\log 2n}\right)$.

Sia $x \geq 8$ e sia n l'unico intero tale che: $2n \leq x < 2n+2$. Chiaramente $n \geq 3$. Abbiamo: $2n > x - 2 \geq 3x/4$ (perché $x \geq 8$). La funzione $f(y) = y/\log y$ è crescente per $y > e$ (Esercizio 19). Quindi per $x \geq 8$:

$$\pi(x) \geq \pi(2n) > \left(\frac{\log 2}{2}\right)\left(\frac{2n}{\log 2n}\right) \geq \left(\frac{\log 2}{2}\right)\left(\frac{3x/4}{\log(3x/4)}\right)$$

Siccome

$$\left(\frac{\log 2}{2}\right)\left(\frac{3x}{4\log(3x/4)}\right) > \left(\frac{3\log 2}{2.4}\right)\left(\frac{x}{\log x}\right)$$

otteniamo:

$$\pi(x) > \left(\frac{3\log 2}{8}\right)\left(\frac{x}{\log x}\right)$$

per $x \geq 8$. Per $2 \leq x < 8$, si verifica la limitazione direttamente (Esercizio 19). □

Per la seconda parte del teorema abbiamo prima:

Lemma 2.38. *Si ha:*

$$\prod_{n<p\leq 2n} p \mid \binom{2n}{n}$$

e quindi:

$$\prod_{n<p\leq 2n} p < 2^{2n}.$$

Dimostrazione. Esercizio 20. □

Inoltre:

Lemma 2.39. *Abbiamo:*

$$\frac{n^{\pi(2n)}}{n^{\pi(n)}} \leq \prod_{n<p\leq 2n} p.$$

Dimostrazione. Esercizio 21. □

La seconda metà del Teorema 2.33:

Proposizione 2.40. *Per $x \geq 2$ abbiamo:*

$$\pi(x) < (6\log 2)\frac{x}{\log x} \cdot$$

Dimostrazione. Per i Lemma 2.38 e 2.39:

$$\frac{n^{\pi(2n)}}{n^{\pi(n)}} \leq 2^{2n}$$

Prendendo il logaritmo:

$$\pi(2n)\log n - \pi(n)\log(\frac{n}{2}.2) < 2n\log 2$$

Quindi:

$$\pi(2n)\log n - \pi(n)\log\frac{n}{2} < 2n\log 2 + \pi(n)\log 2 \leq 3n\log 2$$

Sia $g(n) = \pi(2n)\log(n)$. Abbiamo appena visto che:

$$g(n) - g(\frac{n}{2}) < (3\log 2).n$$

Prendiamo $n = 2^i$, $k \geq i \geq 2$:

$$g(2^k) - g(2^{k-1}) < (3\log 2).2^k$$
$$g(2^{k-1}) - g(2^{k-2}) < (3\log 2).2^{k-1}$$
$$\dots$$
$$g(4) - g(2) < (3\log 2).2^2$$

Sommando tutto:

$$g(2^k) < (3\log 2)(2^k + 2^{k-1} + ... + 2^2) + g(2)$$

Abbiamo $g(2) = \pi(4)\log 2 = 2\log 2 < 3\log 2$ e quindi:

$$\pi(2^{k+1})\log 2^k < (3\log 2)(2^k + ... + 2^2 + 1) < (3\log 2)2^{k+1}$$

Quindi:

$$\pi(2^{k+1}) < (6\log 2)\frac{2^k}{\log 2^k}$$

Per $x \geq 2$ sia $k \geq 1$ tale che $2^k \leq x < 2^{k+1}$. Se $x \geq 4$, allora $k \geq 2$ e $2^k \geq 4 > e$ e quindi (Esercizio 19): $2^k/\log 2^k \leq x/\log x$. In conclusione abbiamo, se $x \geq 4$:

$$\pi(x) \leq \pi(2^{k+1}) < (6\log 2)\frac{x}{\log x}$$

Si verifica poi direttamente questa disuguaglianza per $2 \leq x < 4$. □

Il Teorema 2.33 è dimostrato.

2.4.3 Il postulato di Bertrand.

Nel 1845 Joseph Bertrand dimostrò che per ogni intero n, $n \leq 6.10^6$, l'intervallo $[n, 2n]$ contiene un numero primo. Bertrand poi congetturò che questo dovesse essere vero per ogni intero n. Questo fu dimostrato da Tchebyshev nel 1850.

Lemma 2.41. *Per ogni $n \in \mathbb{N}$:*

$$\prod_{p \leq n} p \leq 4^n \ .$$

Dimostrazione. Procediamo per induzione su n. I casi $n = 1, 2$ sono chiari. Sia $n \geq 3$ e supponiamo l'asserto vero per k, $k < n$. Osserviamo che basta considerare il caso in cui n è dispari (perché $\prod_{p \leq n-1} p = \prod_{p \leq n} p$ se n è pari). Sia dunque $n = 2m + 1$. Abbiamo:

$$\prod_{m < p \leq 2m+1} p \mid \binom{2m+1}{m} \tag{2.5}$$

Inoltre:

$$\binom{2m+1}{m} \leq \frac{1}{2}(2^{2m+1}) = 4^m \tag{2.6}$$

Questo segue da:

$$(1+1)^{2m+1} = \sum_{k=0}^{2m+1} \binom{2m+1}{k} \geq \binom{2m+1}{m} + \binom{2m+1}{m+1} = 2\binom{2m+1}{m}$$

Usando l'ipotesi di induzione, (2.5) e (2.6), viene:

$$\prod_{p \leq 2m+1} p = \left(\prod_{p \leq m+1} p \right) \left(\prod_{m+1 < p \leq 2m+1} p \right) \leq 4^{m+1}.4^m = 4^{2m+1}.$$

□

Lemma 2.42. *Se $n \geq 3$ e se p è un primo tale che $2n/3 < p \leq n$, allora:*

$$p \nmid \binom{2n}{n} \ .$$

Dimostrazione. Abbiamo che p e $2p$ sono gli unici multipli di $p \leq 2n$ (perché $2n < 3p$). Quindi $p^2 \parallel (2n)!$. D'altra parte $p \mid n!$ perché $p \leq n$. Siccome

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$$

vediamo che $p \nmid \binom{2n}{n}$ (altrimenti si avrebbe $p^3 \mid (2n)!$). □

Possiamo ora dimostrare il risultato principale:

Teorema 2.43. (Postulato di Bertrand)
Per ogni intero $n > 0$, l'intervallo $[n, 2n]$ contiene un numero primo.

Dimostrazione. L'enunciato è vero per $n = 1, 2, 3$. Supponiamo, per assurdo, che sia falso per un qualche $n \geq 4$.

In queste condizioni ogni fattore primo, p, di $\binom{2n}{n}$ è $\leq 2n/3$. Infatti se $2n/3 < p \leq n$, $p \nmid \binom{2n}{n}$ per il Lemma 2.42, quindi $p > n$ o $p \leq 2n/3$. Nel primo caso, siccome $p \mid (2n)!$, $p \leq 2n$ e pertanto $p \in [n, 2n]$, contrariamente all'ipotesi.

Sia $p^\alpha \parallel \binom{2n}{n}$. Con le notazioni del Lemma 2.36, abbiamo $\alpha \leq r_p$ e quindi $p^\alpha \leq p^{r_p} \leq 2n$. In particolare se $\alpha \geq 2$, $p \leq \sqrt{2n}$.

Considerando tutti i fattori primi di $\binom{2n}{n}$ otteniamo:

$$\binom{2n}{n} \leq \left(\prod_{p \leq 2n/3} p \right) \left(\prod_{p \leq \sqrt{2n}} p^{r_p - 1} \right)$$

Abbiamo:

$$\prod_{p \leq \sqrt{2n}} p^{r_p - 1} \leq (2n)^{\pi(\sqrt{2n})} \leq (2n)^{\sqrt{2n}}$$

Abbiamo usato: $p^{r_p} \leq 2n$ e $\pi(x) \leq x$. D'altra parte per il Lemma 2.41, $\prod_{p \leq 2n/3} p \leq 4^{2n/3}$. Combinando tutto:

$$\binom{2n}{n} \leq 4^{2n/3} . (2n)^{\sqrt{2n}} \tag{2.7}$$

D'altra parte

$$\binom{2n}{n} \geq \frac{2^{2n}}{2n+1}$$

(cf dimostrazione della Proposizione 2.37). Segue che:

$$\frac{2^{2n}}{2n+1} \leq 4^{2n/3} . (2n)^{\sqrt{2n}}$$

e quindi

$$2^{2n/3} < (2n)^{2+\sqrt{2n}}$$

Prendendo il logaritmo:

$$\frac{2n}{3} \log 2 < (2 + \sqrt{2n}) \log(2n)$$

Poniamo $y = \sqrt{2n}$, allora l'ultima disuguaglianza si scrive:

$$f(y) := \frac{y^2 \log 2}{3} - 2(y+2)\log y < 0$$

Mostriamo adesso, con un banale studio di funzioni, che $f(y) > 0$ se $y \geq 32$. Questo implicherà $y < 32$, ossia $n < 521$.

Abbiamo $f'(y) = (2y \log 2)/3 - 2(1 + \frac{2}{y}) - 2\log y$. Per $y \geq 32 = 2^5$, $f'(y) > g(y) := (2y \log 2)/3 - 4 - 2\log y$. Abbiamo $g'(y) = (2\log 2)/3 - 2/y$. Si verifica che $g'(y) > 0$ se $y \geq 32$. D'altra parte: $g(32) = (34 \log 2)/3 - 4 > 0$. Concludiamo che per $y \geq 32$, $f'(y) > 0$. Siccome $f(32) > 0$, viene $f(y) > 0$ per $y \geq 32$.

Abbiamo quindi $n < 521$. Per concludere basta verificare l'enunciato per questi valori di n. Siccome 2, 3, 5, 7, 13, 23, 43, 83, 163, 317 e 557 sono primi, si vede facilmente che l'enunciato è sempre vero. □

2.4.4 Eulero e la funzione ζ.

Sia Eulero che Gauss e Legendre avevano intuito, cioè congetturato, che: $\pi(x) \sim x/\log x$, cioè $\lim_{x\to+\infty} \dfrac{\pi(x)}{x/\log x} = 1$. Le stime di Tchebyshev sono insufficienti per mostrare questo risultato.

Questo enunciato noto come il *Teorema dei numeri primi* è stato dimostrato, indipendentemente da de la Vallée-Poussin e Hadamard nel 1896. La loro dimostrazione riprende idee della famosa memoria di Riemann (del 1859). In quella memoria Riemann riprende ed estende al dominio complesso un'idea geniale di Eulero. Vediamo di cosa si tratta.

Sia $s \in \mathbb{R}$, sappiamo che la serie $\displaystyle\sum_{n\geq 1} \frac{1}{n^s}$ è convergente per $s > 1$ e divergente per $s \leq 1$. In particolare per $s = 1$, abbiamo la serie armonica: $\displaystyle\sum_{n\geq 1} \frac{1}{n}$, che serve spesso nei corsi di analisi come primo esempio non banale di serie divergente.

Per $s \in \mathbb{R}$, $s > 1$, poniamo con Eulero:

$$\zeta(s) := \sum_{n\geq 1} \frac{1}{n^s}$$

Eulero, il calcolatore geniale e spregiudicato, mostra allora:

Lemma 2.44. *Per $s \in \mathbb{R}, s > 1$:*

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}}.$$

Dimostrazione. Abbiamo:

$$\zeta(s) - \frac{1}{2^s}\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{5^s} + ... - \frac{1}{2^s} - \frac{1}{4^s} - \frac{1}{6^s} - \frac{1}{8^s} - \frac{1}{10^s}...$$

Cioè:

$$\zeta(s) - \frac{1}{2^s}\zeta(s) = \sum_{n \text{ dispari}} \frac{1}{n^s}$$

Quindi abbiamo tolto dalla sommatoria i multipli di 2. Adesso togliamo i multipli di 3 a quel che rimane. Osserviamo che: $(\zeta(s) - \frac{1}{2^s}\zeta(s)) - \frac{1}{3^s}(\zeta(s) - \frac{1}{2^s}\zeta(s)) = \zeta(s)(1 - \frac{1}{2^s})(1 - \frac{1}{3^s})$. Quindi abbiamo:

$$\zeta(s)(1 - \frac{1}{2^s})(1 - \frac{1}{3^s}) = 1 + \frac{1}{5^s} + \frac{1}{7^s} + ... = \sum_{n|(n,6)=1} \frac{1}{n^s}$$

Infatti $(n, 6) = 1 \Leftrightarrow n$ non è multiplo di 2 o di 3.

Andiamo avanti così togliendo i multipli di $5, 7, ..., p < x$, cioè togliendo i multipli dei primi $< x$. Otteniamo:

$$\left(\prod_{p<x}\left(1 - \frac{1}{p^s}\right)\right).\zeta(s) = \sum_{n|(n,P_x)=1} \frac{1}{n^s}$$

dove $P_x := \prod_{p<x} p$.

Quando $x \to +\infty$, per il Teorema Fondamentale dell'aritmetica, il membro di destra tende a 1, quindi:

$$\prod_{p}\left(1 - \frac{1}{p^s}\right).\zeta(s) = 1 \tag{2.8}$$

Siccome $\zeta(s) = \sum_{n\geq 1} 1/n^s < \infty$ $(s > 1)$, otteniamo la relazione cercata. □

Vi sentite a disagio? E' normale, è un calcolo di Eulero!

Un altro modo di presentare le cose, più nello stile di Eulero: per $x < 1$:

$$\frac{1}{1-x} = 1 + x + x^2 + ...$$

In realtà "formalmente" questa uguaglianza è sempre vera, ma per $x < 1$ la serie $\sum x^n$ è convergente. Quindi:

$$\frac{1}{1 - \frac{1}{p^s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + ...$$

Pertanto:

$$\prod_{p<x}\left(\frac{1}{1 - \frac{1}{p^s}}\right) = \prod_{p<x}\left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + ...\right) = \sum_{n\in L_x} \frac{1}{n^s}$$

dove L_x è l'insieme degli n tali che ogni divisore primo di n sia $< x$. Per l'ultima uguaglianza bisogna maneggiare dei prodotti infiniti, cosa un pochino delicata... (ma nello stile di Eulero).

Quando $x \to +\infty$, per il Teorema Fondamentale dell'aritmetica, viene:

$$\prod_p \frac{1}{1-p^{-s}} = \sum_{n\geq 1} \frac{1}{n^s}$$

Formalmente tutto questo sembra funzionare per ogni s, è ben quello che doveva pensare Eulero!

Comunque sia abbiamo:

Corollario 2.45. *L'insieme dei numeri primi è infinito.*

Dimostrazione. Per il Lemma 2.44, per $s > 1$:

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s} = \prod_p \frac{1}{1-p^{-s}}$$

Se l'insieme dei numeri primi è finito, il prodotto $\prod_p \frac{1}{1-p^{-1}}$ è sicuramente un numero finito. Quindi prendendo il limite quando $s \to 1$ per valori superiori si dovrebbe avere $\sum_{n\geq 1} \frac{1}{n} < +\infty$. Ma questo è assurdo perché la serie armonica è divergente! □

In conclusione l'insieme dei numeri primi è infinito perché la serie armonica è divergente! Riemann ha capito che per avere maggiori informazioni sulla distribuzione dei primi bisognava estendere la funzione ζ al dominio complesso (ed è per questo che si dice "la ζ di Riemann" e non la ζ di Eulero), ha poi mostrato che la distribuzione dei primi era legata alla distribuzione degli zeri della funzione ζ. Hadamard e de la Vallée Poussin, tramite una prima stima sulla distribuzione degli zeri della ζ hanno dimostrato il Teorema dei Numeri Primi. Dirichlet invece ha ripreso l'idea di Eulero e l'ha adattata per mostrare il suo famoso teorema sui primi nelle progressioni aritmetiche.

—— .. ——

Esercizi.

Esercizio 16 *Dimostrare il Lemma 2.29.*

Esercizio 17 *Sia p un numero primo e sia $n > 1$ un intero. Sia $n+1 = p^u m$, dove $p \nmid m$. Mostrare che:*
(a) $\lfloor \frac{n}{p^k} \rfloor + 1 = \lfloor \frac{n+1}{p^k} \rfloor$, *se* $k \leq u$
(b) $\lfloor \frac{n}{p^k} \rfloor = \lfloor \frac{n+1}{p^k} \rfloor$, *se* $k > u$.

Esercizio 18 *(a) Mostrare che* $\binom{2n}{n} \geq \binom{2n}{k}$, $0 \leq k \leq 2n$.
Chi è il più grande tra i coefficienti binomiali $\binom{2n+1}{k}$*?*
(b) Mostrare che: $\frac{2^{2n}}{2n+1} \geq 2^n$, *se* $n \geq 3$.
(c) Mostrare direttamente la disuguaglianza:

$$\binom{2n}{n} > 2^n.$$

Esercizio 19 *(a) Mostrare che la funzione $f(y) = y/\log y$ è crescente per $y > e$.*
(b) Verificare (con l'aiuto di un computer?) che per $2 \leq x < 8$:

$$\pi(x) > \left(\frac{3\log 2}{8}\right)\left(\frac{x}{\log x}\right).$$

Esercizio 20 *Dimostrare il lemma 2.38.*

Esercizio 21 *Dimostrare il Lemma 2.39.*

Esercizio 22 *Mostrare che $p_n < 2^n + 1$ (p_n denota l'n-esimo numero primo).*

Esercizio 23 *(a) Sia n il prodotto di k numeri interi consecutivi: $n = (m+1)...(m+k)$. Mostrare che $k! \mid n$.*
(b) Mostrare che $\forall N > 0$ esiste un intervallo di lunghezza N che non contiene alcun numero primo. Perché questo non contraddice il postulato di Bertrand?

3

Congruenze.

Le congruenze (o aritmetica modulare) erano note, in qualche modo, a Fermat ed ai suoi contemporanei (piccolo teorema di Fermat, teorema di Eulero), ma è stato Gauss, nella prima parte delle famose *Disquisitiones Aritmeticae* ([4]), il primo a definirle rigorosamente, a fare uno studio completo delle proprietà di base ed a introdurre le notazioni (sempre in uso).

3.1 Il teorema cinese del resto.

Nel seguito n denoterà un intero > 1 e p un primo positivo.

Definizione 3.1. *Due elementi $a, b \in \mathbb{Z}$ sono congrui modulo n (in simboli: $a \equiv b \pmod{n}$) se e solo se $n \mid a - b$. In altri termini a e b sono congrui modulo n se hanno lo stesso resto nella divisione per n.*

Proposizione 3.2. *La relazione di congruenza modulo n è una relazione d'equivalenza su $\mathbb{Z}$, l'insieme quoziente si nota $\mathbb{Z}/n\mathbb{Z}$ o anche $\mathbb{Z}_n$.*

L'addizione e la moltiplicazione passano al quoziente e con le operazioni indotte $(\mathbb{Z}_n, +, .)$ è un anello commutativo.

L'anello $\mathbb{Z}_n$ è un campo se e solo se $n = p$ è un numero primo.

Dimostrazione. Ricordiamo velocemente la dimostrazione dell'ultima affermazione. L'anello finito $\mathbb{Z}_n$ è un campo se e solo se è integro. Infatti in questo caso $\forall x \in \mathbb{Z}_n, x \neq 0$, la moltiplicazione per x è iniettiva, quindi suriettiva, pertanto esiste $a \in \mathbb{Z}_n$ tale che $ax = 1$.

Se n non è primo $n = ab, 1 < a, b < n$, quindi $a.b \equiv 0 \pmod{n}$, con $a, b \not\equiv 0 \pmod{n}$ e $\mathbb{Z}_n$ non è integro.

Se $n = p$ è primo $a.b \equiv 0 \pmod{p} \Rightarrow p \mid ab$ e quindi $p \mid a$ o $p \mid b$, cioè $a \equiv 0 \pmod{p}$ o $b \equiv 0 \pmod{p}$. Quindi $\mathbb{Z}_p$ è integro. □

Nel seguito indicheremo con $\overline{a}$ o $a \pmod n$ (o anche semplicemente a se non c'è rischio di confusione), la classe di $a \in \mathbb{Z}$ modulo n.

I resti (o residui) possibili nella divisione per n sono $0, 1, 2, ..., n-1$, quindi possiamo scrivere: $\mathbb{Z}_n = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$. Questa non è l'unica rappresentazione possibile, per esempio abbiamo anche $\mathbb{Z}_3 = \{-1, 3, 4\}$.

Definizione 3.3. *L'insieme di interi* $\{a_1, ..., a_n\}$ *è un* sistema completo di residui modulo n *se:*

- $i \neq j \Rightarrow a_i \not\equiv a_j \pmod n$
- $\forall a \in \mathbb{Z}, \exists i$ *tale che* $a \equiv a_i \pmod n$.

Quindi $\{0, 1, ..., n-1\}$ e $\{1, 2, ..., n\}$ sono dei sistemi completi di residui modulo n.

Lemma 3.4. *Se* $\{a_1, ..., a_n\}$ *è un sistema completo di residui modulo* n *e se* $(k, n) = 1$, *allora anche* $\{ka_1, ..., ka_n\}$ *è un sistema completo di residui modulo* n.

Dimostrazione. Esercizio 24. □

Il gruppo additivo $(\mathbb{Z}_n, +)$ è ciclico e $\overline{x}$ è un generatore se e solo se $(x, n) = 1$, cioè se e solo se $\overline{x}$ è invertibile (per la moltiplicazione). L'insieme degli elementi invertibili di $\mathbb{Z}_n$ si nota U_n: è il gruppo (moltiplicativo) delle *unità* di $\mathbb{Z}_n$. Come vedremo, in generale, questo gruppo non è ciclico.

Teorema 3.5. (Teorema cinese del resto)
Sia $n = \prod_{i=1}^{r} p_i^{a_i}$ *la fattorizzazione in numeri primi dell'intero* n, *allora esiste un isomorfismo di anelli:*

$$\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^{r} \mathbb{Z}/p_i^{a_i}\mathbb{Z}$$

In particolare:

$$U_n \simeq \prod_{i=1}^{r} U_{p_i^{a_i}}$$

qui U_n *indica il gruppo (moltiplicativo) delle unità dell'anello* $\mathbb{Z}/n\mathbb{Z}$.

Dimostrazione. Sia $f : \mathbb{Z} \to \prod_1^r \mathbb{Z}/p_i^{a_i}\mathbb{Z} : x \to (x \pmod{p_1^{a_1}}, ..., x \pmod{p_r^{a_r}})$. Si verifica facilmente che f è un morfismo d'anelli. Il Ker di f è l'insieme degli x tali che $p_i^{a_i} \mid x, \forall i$, è quindi l'insieme dei multipli di n, cioè nZ. Otteniamo quindi un morfismo iniettivo: $\overline{f} : \mathbb{Z}/n\mathbb{Z} \to \prod_1^r \mathbb{Z}/p_i^{a_i}\mathbb{Z}$. Un'applicazione iniettiva tra due insiemi finiti della stessa cardinalità è biiettiva, quindi $\overline{f}$ è un isomorfismo. □

In particolare se $(n,m)=1$, allora $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ e $U_{mn} \simeq U_n \times U_m$.

La versione "classica" del Teorem cinese del resto:

Teorema 3.6. (Teorema cinese del resto)
Siano $n_1,...,n_k$ degli interi due a due primi tra di loro (cioè $(n_i,n_j)=1$ per ogni $(i,j), i \neq j$), allora il sistema:

$$\begin{cases} x \equiv c_1 \pmod{n_1} \\ \cdots \\ x \equiv c_k \pmod{n_k} \end{cases}$$

ammette una soluzione. Inoltre se x e x' sono due soluzioni, allora $x \equiv x' \pmod{n}$, dove $n = n_1...n_k$.

Dimostrazione. Sia $n = n_1...n_k$, allora $\mathbb{Z}/n\mathbb{Z} \simeq \prod_1^k \mathbb{Z}/n_i\mathbb{Z}$ tramite $g(\overline{x}) = (x \pmod{n_1}, ..., x \pmod{n_k})$. Quindi esiste uno ed un unico $\overline{y}$ la cui immagine è $(c_1 \pmod{n_1}, ..., c_k \pmod{n_k})$. □

Questo risultato riflette un fenomeno molto semplice ma importante. Supponiamo di avere due sequenze $a_1,...,a_n,\ b_1,...,b_m$ e scriviamole una sopra l'altra in modo ciclico:

$$\begin{array}{cccccccccccc} a_1 & \cdots & \cdots & \cdots & a_n & a_1 & \cdots & \cdots & \cdots & a_n \\ b_1 & \cdots & b_m & b_1 & \cdots & b_m & b_1 & \cdots & b_m & b_1 \end{array}$$

otteniamo così delle coppie $\begin{matrix} a_i \\ b_j \end{matrix}$. Il problema è di capire quando capiterà la prima coppia ripetuta:

$$\begin{array}{cccccccccc} a_1 & \cdots & a_i & \cdots & \cdots & a_n & \cdots & \cdots & a_i \\ b_1 & \cdots & b_j & \cdots & \cdots & \cdots & \cdots & \cdots & b_j \end{array}$$

Intanto la prima coppia ripetuta sarà senz'altro $\begin{matrix} a_1 \\ b_1 \end{matrix}$. Infatti prima di $\begin{matrix} a_i \\ b_j \end{matrix}$ c'è $\begin{matrix} a_{i-1} \\ b_{j-1} \end{matrix}$ e quindi se $i > 1$, $\begin{matrix} a_{i-1} \\ b_{j-1} \end{matrix}$ è la prima coppia ripetuta ($n \geq m$). Quindi per la prima coppia ripetuta avremo:

$$\begin{matrix} \overbrace{a_1...a_n \cdots a_1...a_n}^{r} \\ \underbrace{b_1...b_m \cdots b_1...b_m}_{s} \end{matrix}$$

quindi $rn = sm$ "per la prima volta", cioè $k = rn = sm$ è il minore comune multiplo di n e m. Se $(n,m)=1$, allora $mcm(n,m) = nm$.

In altri termini se un evento E_1 si produce ciclicamente ogni n anni (per esempio il passaggio di una cometa) e se l'evento E_2 si ripete ciclicamente ogni m anni e se quest'anno entrambi gli eventi si sono prodotti, allora, se $(n, m) = 1$, bisognerà aspettare nm anni affinché questo accada ancora. Questo ragionamento era usato dagli astronomi (cinesi) dell'antichità.

—— .. ——

Esercizi.

Esercizio 24 *Dimostrare il Lemma 3.4.*

Esercizio 25 *Siano $n_1, ..., n_k \in \mathbb{N}$ due a due primi tra di loro. Mostrare che se $n_i \mid m, \forall i$, allora $n_1...n_k \mid m$.*

Esercizio 26 *(i) Mostrare che un quadrato è congruo a 0 o a 1 modulo 4.*
(ii) Caratterizzare gli interi $n > 1$ per i quali esiste una partizione di $X_n = \{1, 2, ..., n\}$ in due sotto insiemi I, J ($I \cup J = X_n$, $I \cap J = \emptyset$, I e J non vuoti) di modo che:

$$\sum_{i \in I} i = \sum_{j \in J} j$$

(iii) Dire se esiste una tale partizione per $n = 2014$.

Esercizio 27 *Un repunit (*repeated units*) è un numero le cui cifre sono tutte uguali a 1. Nel seguito r_n indica il repunit con n cifre ($r_2 = 11, r_3 = 111$, ecc...).*
(i) Mostrare che $r_n = (10^n - 1)/9$.
(ii) Mostrare che se r_n è primo allora n è primo.
(iii) Dare un esempio di un primo p tale che r_p non sia primo.

Esercizio 28 *(i) Mostrare che un quadrato è congruo a $0, 1$ o 4 modulo 8.*
(ii) Trovare infiniti interi che non si scrivono come somma di al più tre quadrati.
(iii) Determinare il più piccolo intero che non si scrive come somma di al più tre quadrati.

Esercizio 29 *Sia p un numero primo.*
(i) Determinare le soluzioni (in $\mathbb{Z}_{p^n}$) dell'equazione $x^2 \equiv x \pmod{p^n}$.
(ii) Determinare le soluzioni (in $\mathbb{Z}_{p^n}$) dell'equazione $x^2 \equiv 1 \pmod{p^n}$ (può essere utile osservare che l'MCD di $x - 1$ e $x + 1$ è 1 o 2).
(iii) Sia $m = 2^a p_1^{a_1} ... p_r^{a_r}$ (p_i primi dispari distinti). Determinare (in funzione della fattorizzazione di m) il numero di soluzioni dell'equazione $x^2 \equiv 1 \pmod{m}$.

Esercizio 30 *Trovare il più piccolo intero positivo n tale che $n \equiv 4 \pmod{7}$, $n \equiv 6 \pmod{9}$ e $n \equiv 1 \pmod{10}$.*

3.2 I teoremi di Fermat, Eulero e Wilson.

Il piccolo teorema di Fermat e la sua generalizzazione data da Euler, anche se facili da dimostrare, sono sicuramente dei risultati fondamentali. Il teorema di Wilson interviene in varie questioni e ha il merito di essere il primo test di primalità.

Teorema 3.7. (Il piccolo teorema di Fermat)
Sia p un numero primo. Se $a \in \mathbb{Z}$ è primo con p, allora: $a^{p-1} \equiv 1 \pmod{p}$.
In particolare $x^p \equiv x \pmod{p}$, per ogni intero x.

Ricordiamo la seguente:

Definizione 3.8. *La funzione di Eulero $\varphi : \mathbb{N}^* \to \mathbb{N}$ è definita da: $\varphi(n) = \#\{m \mid 1 \leq m \leq n \text{ e } (m,n) = 1\}$.*
In particolare $\#(U_n) = \varphi(n)$.

Siccome, ovviamente $\varphi(p) = p - 1$, il piccolo teorema di Fermat è un caso particolare del seguente teorema:

Teorema 3.9. (Eulero)
Se $(a,n) = 1$, allora $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Dimostrazione. Se $(a,n) = 1$, allora $\overline{a} \in U_n$, il gruppo delle unità. Siccome $\#(U_n) = \varphi(n)$, per il teorema di Lagrange, l'ordine di $\overline{a}$ divide $\varphi(n)$ e quindi $\overline{a}^{\varphi(n)} = 1$ in U_n. □

Il piccolo teorema di Fermat fornisce una condizione necessaria affinché un numero n sia primo: se esiste a con $(a,n) = 1$ e $a^{n-1} \not\equiv 1 \pmod{n}$, allora n non è primo. Ma questa condizione non è sufficiente (Esercizi 35, 36). Il teorema di Wilson fornisce invece una condizione necessaria e sufficiente (ma non molto comoda nella pratica):

Teorema 3.10. (Wilson)
Un intero $n > 1$ è primo se e solo se: $(n-1)! \equiv -1 \pmod{n}$.

Dimostrazione. Se n non è primo, allora $n = ab, 1 < a \leq b < n$ e $(n-1)! = 1.2...a...b...(n-1) \equiv 0 \pmod{n}$. Rimane da vedere che se $n = p$ è primo allora $1.2....(p-1) \equiv -1 \pmod{p}$. Nel campo $\mathbb{Z}_p$, ogni elemento non nullo, x, ha un inverso: $x.x^{-1} \equiv 1 \pmod{p}$. Abbiamo $x = x^{-1}$ se e solo se $x^2 - 1 = 0$. Il polinomio $X^2 - 1$ ha esattamente due radici nel campo $\mathbb{Z}_p$: ± 1. Siccome $p - 1 \equiv -1 \pmod{p}$, $1.2...(p-1) \equiv 2.3...(p-2)(-1) \pmod{p}$. Gli elementi di $2, 3, ..., p-2$ vanno a coppia $x.x^{-1}$, quindi $2.3....(p-2) \equiv 1 \pmod{p}$, pertanto $(p-1)! \equiv -1 \pmod{p}$. □

Questa dimostrazione è dovuta a Gauss.

———— .. ————

Esercizi.

Esercizio 31 (Il piccolo teorema di Fermat)
Sia p un numero primo. Sia a un intero primo con p. Mostrare che $(p-1)! \equiv a.2a.3a...(p-1)a \pmod{p}$ (cf Esercizio 24). Concludere che $a^{p-1} \equiv 1 \pmod{p}$.
Concludere che per ogni intero b, $b^p \equiv b \pmod{p}$.

Esercizio 32 (Il piccolo teorema di Fermat)
Ancora un'altra dimostrazione del piccolo teorema di Fermat.

1. *Sia p un numero primo, mostrare che se $1 \leq k < p$, il coefficiente binomiale $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ è divisibile per p.*
2. *Sia p un numero primo fissato. Mostrare per induzione su n, che $n^p \equiv n \pmod{p}, \forall n \in \mathbb{N}$ (usare la formula del binomio per calcolare $(n+1)^p$).*
3. *Concludere che $\forall n \in \mathbb{Z}$, $n^p \equiv n \pmod{p}$.*

Esercizio 33 *Sia $M_p = 2^p - 1$ il numero di Mersenne corrispondente al primo $p > 2$.*
(i) Mostrare che se un primo q divide M_p, allora $p \mid q-1$ (considerare l'ordine di $2 \pmod{q}$).
(ii) Concludere che ogni divisore primo di M_p è della forma $2kp+1, k \geq 1$.
(iii) Mostrare che M_{11} e M_{23} non sono primi.
Ai tempi di Fermat si sapeva che M_p era primo per $p = 2, 3, 5, 7, 13, 17, 19$ e che M_{11} era composito. E' stato Fermat a trovare che M_{23} non è primo (ed è proprio nel corso di queste ricerche che ha trovato il suo "piccolo teorema").

Esercizio 34 *Sia $s > 1$ un intero. Se $a \geq 1$ è un intero si pone $B_a = s^a - 1$.*
(i) Sia $a = bq + r, 0 \leq r < b$ la divisione euclidea di a per b. Mostrare che $B_a = QB_b + B_r$ (osservare che $B_a = B_r B_{qb} + B_{qb} + B_r$).
(ii) Mostrare che $(B_a, B_b) = B_d$, dove $d = (a, b)$.
(iii) Prima di dimostrare il suo piccolo teorema, Fermat aveva dimostrato il caso particolare: $p \mid 2^p - 2$ se p è primo. Usare questa versione del piccolo teorema e (ii) per ritrovare il fatto (Esercizio 33) che ogni divisore primo di M_p ($p > 2$) è della forma $2pk + 1$.
(iv) Viceversa dedurre che $p \mid 2^p - 2$ se p è primo dal fatto che ogni divisore primo di M_p, $p > 2$, è della forma $2kp + 1$.

Esercizio 35 *Gli Antichi Cinesi credevano che un intero dispari n fosse primo se e solo se $n \mid 2^n - 2$ (ossia se e solo se $2^{n-1} \equiv 1 \pmod{n}$).*
(i) Siano p, q due primi distinti e sia a un intero. Mostrare che se $a^p \equiv a \pmod{q}$ e $a^q \equiv a \pmod{p}$, allora $a^{pq} \equiv a \pmod{pq}$.

(ii) Osservare che $2^{10} = 31 \times 33 + 1$ *e che* $341 = 11 \times 31$. *Dedurne che* $2^{341} \equiv 2 \pmod{341}$. *Gli interi dispari compositi,* n, *tali che* $2^n \equiv 2 \pmod{n}$ *si chiamano* pseudo-primi *(relativamente alla base 2). Quindi* 341 *è un pseudo-primo.*
(iii) Determinare i tre più piccoli pseudo-primi.

Esercizio 36 *Per vedere se un intero (dispari)* n *è o meno primo possiamo usare il teorema di Fermat: se* n *è primo allora* $2^{n-1} \equiv 1 \pmod{n}$. *Quindi se* $2^{n-1} \not\equiv 1 \pmod{n}$, *allora* n *non è primo. L'esistenza di pseudo primi (Esercizio 35) mostra che alcuni numeri compositi supereranno questo test con successo. Possiamo però fare un altro test cambiando base: invece di 2 possiamo prendere* a, $(a, n) = 1$, *e vedere se* $a^{n-1} \equiv 1 \pmod{n}$. *Un* pseudo primo relativamente alla base a *è un intero composito dispari* n, $(a, n) = 1$, *tale che* $a^{n-1} \equiv 1 \pmod{n}$.
(i) Calcolare $7^{340} \pmod{341}$ *e concludere che* 341 *è composito.*
Anche se questo tipo di test non può mostrare che un dato n *è primo, è naturale chiedersi se per ogni composito* n *esiste una base* a, $(a, n) = 1$, *tale che* $a^{n-1} \not\equiv 1 \pmod{n}$. *La risposta è no! Un* numero di Carmichael *è un numero composito dispari* n *tale che per ogni* a, $(a, n) = 1$, *si abbia:* $a^{n-1} \equiv 1 \pmod{n}$.
(ii) Mostrare che $n = 561 = 3 \times 11 \times 17$ *è un numero di Carmichael.*

Esercizio 37 *Abbiamo già visto (Esercizio 4) che se* $2^n + 1$ *è primo, allora* n *è una potenza di* 2. *Sia quindi* $F_n = 2^{2^n} + 1$ *(*numeri di Fermat*). Fermat aveva osservato che* F_0, F_1, F_2, F_3 *e* F_4 *sono primi.*
(i) Verificare questa affermazione.
Aveva poi "annunciato" che F_n *è primo per ogni* n. *Questa è l'unica affermazione di Fermat che si è rilevata (completamente) sbagliata. Nel 1732 Eulero ha mostrato che* F_5 *è composito.*
(ii) Osservando che $641 = 2^7 \times 5 + 1 = 5^4 + 2^4$, *mostrare che* $641 \mid F_5$.

Osservazione: *Abbiamo* $F_5 = 4\,294\,967\,297$, *non è un numero "enorme" ma ai tempi di Fermat era un numero intrattabile. Oggi si sa che* $F_6, ..., F_{32}$ *e tanti altri numeri di Fermat sono compositi. Lo statuto di* F_{33} *è ancora aperto. In certi casi si sa che* F_n *è composito ma non si conosce nessun suo fattore primo. Per esempio c'è un premio di 500* \$ *per chi trova un fattore primo di* F_{14}. *Alcuni pensano che* F_n *sia composito per ogni* $n > 4$.

Esercizio 38 *Mostrare che se* $n > 5$ *e* $k \geq 1$, *l'equazione (in* n, k*)* $(n-1)! + 1 = n^k$, *non ha soluzioni.*

3.3 Il gruppo delle unità modulo n.

Il gruppo additivo $(\mathbb{Z}_n, +)$ è ciclico, per quanto riguarda U_n la situazione non è così chiara. Un primo problema naturale consiste nel determinare gli interi n tali che U_n sia un gruppo ciclico. Osserviamo che se U_n è ciclico allora esiste $x \in U_n$ di ordine $\varphi(n) = \#(U_n)$, quindi $x^{\varphi(n)} \equiv 1 \pmod{n}$ e $x^k \not\equiv 1 \pmod{n}$ se $k < \varphi(n)$. In questo caso per ogni $a \in U_n$, esiste i tale che $a \equiv x^i \pmod{n}$.

Definizione 3.11. *Un elemento $x \in U_n$ è una* radice primitiva (mod n) *se x ha ordine $\varphi(n)$ (cioè x è un generatore di U_n e pertanto U_n è ciclico, isomorfo a $\mathbb{Z}/\varphi(n)$).*

Osservazione 3.12. Le radici primitive modulo n non esistono sempre. Per esempio $U_8 = \{1, 3, 5, 7\}$ e $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$, quindi ogni elemento ($\neq 1$) ha ordine 2, U_8 non è ciclico; dalla classificazione dei gruppi $U_8 \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$.

Il comportamento della funzione di Eulero è piuttosto irregolare, ma abbiamo:

Proposizione 3.13. *Sia $\varphi(n)$ la funzione di Eulero, allora:*

1. *Se $n = \prod p_i^{a_i}$ è la fattorizzazione di n in fattori primi, allora $\varphi(n) = \prod \varphi(p_i^{a_i})$.*
2. *la funzione di Eulero è moltiplicativa: se $(m, n) = 1$, allora $\varphi(mn) = \varphi(m).\varphi(n)$.*
3. *Se p è primo, $\varphi(p^a) = p^a - p^{a-1} = p^a(1 - \frac{1}{p})$*
4. *Per ogni intero $m > 1$, $\varphi(m) = m.\prod_{p|m}(1 - \frac{1}{p})$ (il prodotto è fatto sui primi distinti che dividono m)*

Dimostrazione. (1) Segue dal Teorema 3.5: $\varphi(n) = \#(U_n) = \#(\prod U_{p_i^{a_i}}) = \prod \varphi(p_i^{a_i})$.
(2) Segue da (1).
(3) Sia $1 \leq n \leq p^a$, allora $(n, p^a) = 1 \Leftrightarrow p \nmid n$. I multipli di p minori di p^a, sono i $kp \leq p^a$, ce ne sono p^{a-1} ($1 \leq k \leq p^{a-1}$). Quindi $\varphi(p^a) = p^a - p^{a-1} = p^a(1 - 1/p)$.
(4) Da (1): $\varphi(n) = \prod \varphi(p_i^{a_i})$. Usando (3): $\varphi(n) = \prod p_i^{a_i}(1 - \frac{1}{p_i}) = n \prod (1 - \frac{1}{p_i})$. □

Un'altra proprietà interessante della funzione di Eulero:

Lemma 3.14. *Per ogni intero n:* $\sum_{d|n} \varphi(d) = n$

Dimostrazione. Esercizi 40, 41. □

Passiamo adesso allo studio dei gruppi U_n, cioè, visto il Teorema 3.5, allo studio dei gruppi U_{p^a}. Bisogna distinguere a seconda della parità di p.

- U_{2^a} $(p = 2)$.

Abbiamo $U_2 = \{1\}$ (elementi invertibili di $\mathbb{Z}_2 = \{0, 1\}$) e $U_4 = \{1, 3\} \simeq \mathbb{Z}_2$. Quindi U_{2^a} è ciclico se $1 \leq a \leq 2$.

Vediamo che U_{2^a} non è ciclico se $a \geq 3$. Osserviamo che $\#(U_{2^a}) = \varphi(2^a) = 2^{a-1}$. Inoltre se $\overline{n} \in U_{2^a}$, n è dispari.

Lemma 3.15. *Se n è un intero dispari e se $a \geq 3$, allora:*

$$n^{2^{a-2}} \equiv 1 \pmod{2^a}.$$

Dimostrazione. Il lemma è vero per $a = 3$ (Osservazione 3.12). Procediamo per induzione su a. Sia quindi $n^{2^{a-2}} = 1 + t2^a$. Elevando al quadrato: $n^{2^{a-1}} = 1 + 2^{a+1}t + t^2 2^{2a} \equiv 1 \pmod{2^{a+1}}$. □

Corollario 3.16. *Il gruppo U_{2^a} è ciclico se e solo se $1 \leq a \leq 2$.*

Osservazione 3.17. Si può dimostrare (cf Esercizio 46) che $U_{2^a} \simeq \mathbb{Z}_2 \times \mathbb{Z}_{2^{a-2}}$, se $a \geq 3$.

- U_{p^a}, $p \geq 3$.

Ricordiamo il seguente risultato di algebra:

Teorema 3.18. *Sia K un campo. Ogni sotto gruppo finito del gruppo moltiplicativo K^* è ciclico.*

Corollario 3.19. *Se p è primo, $U_p \simeq \mathbb{F}_p^\times$ è ciclico di ordine $p - 1$. Ci sono esattamente $\varphi(p - 1)$ radici primitive modulo p.*

Dimostrazione. Dal Teorema 3.18 se p è primo, U_p è ciclico, di ordine $p - 1$, quindi isomorfo al gruppo additivo $\mathbb{Z}_{p-1}$ e ha quindi $\varphi(p-1)$ generatori, cioè ci sono $\varphi(p - 1)$ radici primitive modulo p. □

Osserviamo che non si conosce nessuna procedura "veloce" per determinare il più piccolo intero g, $1 \leq g \leq p - 1$, tale che g sia una radice primitiva (mod p). Molto spesso 2 funziona, ma non sempre (Esercizio 44).

Mostriamo che esiste un intero g che è radice primitiva (mod p^a), per ogni $a > 0$. Questo mostrerà che U_{p^a} è ciclico, per ogni $a > 0$.

Lemma 3.20. *Sia g una radice primitiva $\pmod{p^a}$, allora uno solo dei due casi seguenti può prodursi:*
(a) g è radice primitiva $\pmod{p^{a+1}}$
(b) $g^{\varphi(p^a)} \equiv 1 \pmod{p^{a+1}}$.

Dimostrazione. Sia m l'ordine di $g \pmod{p^{a+1}}$, quindi $g^m \equiv 1 \pmod{p^{a+1}}$ e $m \mid \varphi(p^{a+1})$. Abbiamo anche $g^m \equiv 1 \pmod{p^a}$. Quindi $\varphi(p^a) \mid m$. In conclusione: $\varphi(p^a) \mid m \mid \varphi(p^{a+1}) = p\varphi(p^a)$. Quindi $m = p\varphi(p^a) = \varphi(p^{a+1})$ (caso (a)), oppure $m = \varphi(p^a)$ (caso (b)). □

Teorema 3.21. *Sia g una radice primitiva $\pmod{p}$ tale che $g^{p-1} = 1 + pm$ con $p \nmid m$. Allora g è radice primitiva $\pmod{p^a}$, $\forall a > 0$.*

Dimostrazione. Mostriamo per induzione su a che:

$$g^{\varphi(p^a)} = 1 + m_a p^a, \text{ con } p \nmid m_a, \forall a > 0 \tag{3.1}$$

Il caso $a = 1$ segue dall'ipotesi. Supponiamo (3.1) vero per a. Abbiamo:

$$\left(g^{\varphi(p^a)}\right)^p = (1 + m_a p^a)^p$$

Per la formula del binomio:

$$(1 + m_a p^a)^p = \sum_{i=0}^{p} \binom{p}{i} m_a^i p^{ia} = 1 + m_a p^{a+1} + p^{2a} t$$

dove $t = \sum_{i=2}^{p} \binom{p}{i} m_a^i p^{a(i-2)}$. Ponendo $m_{a+1} = m_a + p^{a-1}t$. Abbiamo $(1 + m_a p^a)^p = 1 + m_{a+1} p^{a+1}$, dove $p \nmid m_{a+1}$ (perché $p \nmid m_a$).

Per concludere basta osservare che:

$$\left(g^{\varphi(p^a)}\right)^p = g^{p\varphi(p^a)} = g^{\varphi(p^{a+1})}.$$

Abbiamo quindi dimostato (3.1).

Mostriamo per induzione su a che g è radice primitiva $\pmod{p^a}, \forall a$. Il caso $a = 1$ è vero per ipotesi. Supponiamo che g sia radice primitiva $\pmod{p^a}$. La relazione (3.1) implica: $g^{\varphi(p^a)} \not\equiv 1 \pmod{p^{a+1}}$, quindi per il Lemma 3.20, g è radice primitiva $\pmod{p^{a+1}}$. □

Se $p = 2$ l'unica radice primitiva mod 2 è 1 e non esiste nessun m dispari tale che $1 = 1 + 2m$.

Rimane da mostrare che esiste effettivamente una radice primitiva $\pmod{p}$, g, con $g^{p-1} = 1 + pm, p \nmid m$ quando $p > 2$.

Proposizione 3.22. *Esiste una radice primitiva $\pmod{p}$, g, tale che $g^{p-1} = 1 + pm$, con $p \nmid m$.*

Pertanto esiste, g, radice primitiva $\pmod{p}$ tale che g sia radice primitiva $\pmod{p^a}, \forall a > 0$.

Dimostrazione. Sia g una radice primitiva $\pmod p$, quindi $g^{p-1} = 1 + pm$. Se $p \nmid m$, abbiamo finito. Altrimenti sia $g_1 = g + p$. Allora $g_1 \equiv g \pmod p$, quindi anche g_1 è una radice primitiva $\pmod p$. Abbiamo:

$$g_1^{p-1} = (g+p)^{p-1} = g^{p-1} + (p-1)pg^{p-2} + p^2k = 1 + pm + (p-1)pg^{p-2} + p^2k$$

$$1 + p[g^{p-2} + m + pk] = 1 + pm_1$$

dove $m_1 = g^{p-2} + m + pk$. Siccome p divide m e pk, ma non divide g^{p-2}, $p \nmid m_1$.

L'ultima affermazione segue dal Teorema 3.21. □

Corollario 3.23. *Sia p un numero primo dispari, allora U_{p^a} e U_{2p^a} sono ciclici per ogni $a > 0$.*

Dimostrazione. Siccome $(2, p^a) = 1$, $U_{2p^a} \simeq U_2 \times U_{p^a} \simeq U_{p^a}$. Si conclude con la Proposizione 3.22. □

Il risultato finale:

Teorema 3.24. *Sia $n > 1$ un intero, allora U_n è ciclico se e solo se $n = 2, 4, p^a, 2p^a$, dove p è un primo dispari e $a > 0$.*

Dimostrazione. Abbiamo già visto che se $n = 2, 4, p^a$ o $2p^a$, allora U_n è ciclico (Corollari 3.16, 3.23). Mostriamo che questi sono gli unici valori possibili. Se $n = \prod_1^r p_i^{a_i}$, allora $U_n \simeq \prod_1^r U_{p_i^{a_i}}$ (Teorema 3.5). Ogni gruppo $U_{p_i^{a_i}}$ ha ordine pari uguale a $\varphi(p_i^{a_i})$, tranne se $p_i = 2, a_i = 1$ e in tal caso $U_{p_i^{a_i}} = U_2 = \{1\}$. Quindi basta mostrare che se G, H sono due gruppi di ordine $2r, 2s$, allora $G \times H$ non è ciclico. Se $(x, y) \in G \times H$, $(x, y)^{2rs} = (x^{2rs}, y^{2rs}) = (1, 1)$. Quindi ogni elemento ha ordine $\leq 2rs < 4rs$ e $G \times H$ non è ciclico. □

Esercizi.

Esercizio 39 *Sia p un numero primo. Mostrare (senza usare la teoria dei gruppi, ma solo il teorema di Fermat) che se $d \mid p-1$, l'equazione $x^d \equiv 1 \pmod p$ ha esattamente d soluzioni.*

Esercizio 40 *Sia G un gruppo ciclico di ordine n ($G \simeq (\mathbb{Z}_n, +)$). Mostrare che se $d \mid n$ esiste uno ed un unico sotto gruppo, H, ciclico di G di ordine d; H ha $\varphi(d)$ generatori. Ogni elemento di G genera un sotto gruppo ciclico.*
(i) Mostrare che $\sum_{d|n} \varphi(d) = n$.
(ii) Sia p un numero primo e $d \mid p-1$. In $\mathbb{F}_p^\times$ ci sono esattamente $\varphi(d)$ elementi il cui ordine è d.

Esercizio 41 *(i) Mostrare che la funzione $f(n) = \sum_{d|n} \varphi(d)$ è moltiplicativa (cf Esercizio 8).*
(ii) Calcolare $f(p^a)$ e concludere che $\sum_{d|n} \varphi(d) = n$.

Esercizio 42 *Sia p un primo. Mostrare che l'equazione $x^2 \equiv -1 \pmod p$ ha una soluzione se e solo se $p = 2$ o $p \equiv 1 \pmod 4$.*

Esercizio 43 *Sia g una radice primitiva mod. p. Allora ogni $a \in \mathbb{F}_p^\times$ si scrive: $a \equiv g^t \pmod p$. L'esponente t si chiama* l'indice *di a relativamente a g e si nota $ind_g(a)$. L'indice è definito mod. $\varphi(p)$.*
(i) Mostrare che: $ind_g(ab) \equiv ind_g(a) + ind_g(b) \pmod{p-1}$. In particolare $ind_g(a^n) \equiv n.ind_g(a) \pmod{p-1}$.
(ii) Un procedimento semplice per fare una "tabella degli indici". Fare una tabella con due righe, nella seconda riga scrivere i numeri $1, 2, ..., p-1$ (in questo ordine). Nella prima riga (prima colona) scrivere g, poi al posto successivo (prima riga, seconda colona) scrivere $g^2 \pmod p$, andare avanti con le potenze successive di g (al posto $(1, p-1)$ c'è 1). L'indice di un elemento della prima riga è l'elemento della seconda riga che gli sta sotto (cioè che è nella stessa colona).

Esempio: $p = 17, g = 3$:

a	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1
$ind_3(a)$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Quindi, per esempio, $ord_3(11) = 7$, cioè $11 \equiv 3^7 \pmod{17}$, ecc... Ovviamente tutto questo è valido per ogni n per i quali esistono delle radici primitive.
(iii) Mostrare che a è radice primitiva mod. p se e solo se $(ind_g(a), \varphi(p)) = 1$. Determinare le radici primitive mod. 17, 18.

Esercizio 44 *Determinare i primi $p < 200$ tali che 2 sia radice primitiva modulo p.*

Esercizio 45 *Sia a un intero il cui ordine mod. p^k è n e il cui ordine mod. p^{k-1} è m (p primo, $k \geq 2$).*
(i) Mostrare: $a^n \equiv 1 \pmod{p^{k-1}}$ e $a^{mp} \equiv 1 \pmod{p^k}$.
(ii) Concludere che $n = m$ o $n = mp$.
(iii) Mostrare che l'ordine di 3 mod. 2^k, $k \geq 3$, è 2^{k-2}.

Esercizio 46 *(i) Mostrare che l'ordine di 5 in U_{2^a} è 2^{a-2} per ogni $a \geq 3$.*
(ii) Mostrare che $\forall n \geq 1, 5^n \not\equiv -1 \pmod{2^a}, \forall a \geq 3$.
(iii) Dedurre da quanto precede che $U_{2^a} \simeq \mathbb{Z}_2 \times \mathbb{Z}_{2^{a-2}}$.

Esercizio 47 (Il teorema di Carmichael)
Dal teorema di Fermat se $(a,p) = 1$, $a^{p-1} \equiv 1 \pmod{p}$. Inoltre siccome esistono radici primitive modulo p, esiste a tale che $ord_p(a) = p-1$. Quindi l'esponente $p-1$ è, in un certo senso, il "migliore" possibile. Cosa succede se invece di p prendiamo un modulo m non primo? Per il teorema di Eulero, se $(a,m) = 1$, allora $a^{\varphi(m)} \equiv 1 \pmod{m}$.
(i) Mostrare che modulo 8 ogni elemento invertibile ha ordine due. Quindi $\varphi(2^3) = 4$ non è l'esponente "migliore".
(ii) La funzione λ di Carmichael è definita nel modo seguente:

$$\lambda(2) = 1, \lambda(4) = 2, \lambda(2^\alpha) = \varphi(2^\alpha)/2$$
$$\lambda(p^\alpha) = \varphi(p^\alpha), p \text{ primo dispari}$$
$$Se\ m = 2^\alpha p_1^{\alpha_1} ... p_n^{\alpha_n}, \lambda(m) = mcm\{\lambda(2^\alpha), \lambda(p_1^{\alpha_1}), ..., \lambda(p_n^{\alpha_n})\}$$

Mostrare che se $(a,m) = 1$, allora $a^{\lambda(m)} \equiv 1 \pmod{m}$ (teorema di Carmichael).
(iii) Per $m = 2^6 \times 3^3 \times 5 \times 7$, calcolare $\lambda(m)$ e $\varphi(m)$.
(iv) Mostrare che per ogni m esiste un a, $(a,m) = 1$, tale che l'ordine di a in U_m sia proprio $\lambda(m)$. In conclusione $\lambda(m)$ è l'esponente "migliore".

Esercizio 48 (Numeri di Carmichael)
Un numero di Carmichael è un intero composito dispari n tale che se $(a,n) = 1$, allora $a^{n-1} \equiv 1 \pmod{n}$ (cioè n supera tutti i tests di Fermat anche se non primo, cf Esercizio 36).
(i) Mostrare che n è un numero di Carmichael se e solo se: n è un prodotto di primi distinti: $n = p_1 p_2 ... p_k$ ($p_i \neq p_j$ se $i \neq j$) tali che $(p_i - 1) \mid (n-1)$, $\forall i$.
(ii) Con le notazioni di (i) mostrare che $k \geq 3$.
(iii) Ritrovare il fatto che $n = 561$ è un numero di Carmichael (Esercizio 36).
(iv) Determinare i primi tre numeri di Carmichael.

Osservazione: *E' stato dimostrato nel 1994 che esistono infiniti numeri di Carmichael ([1]).*

4

Il teorema dei due quadrati.

Quali sono gli interi $n \in \mathbb{N}$ che si scrivono come la somma di due quadrati: $n = x^2 + y^2$, $x, y \in \mathbb{N}$?

Si vede facilmente che $0 = 0^2 + 0^2, 1 = 1^2 + 0^2, 2 = 1^2 + 1^2$, $4 = 2^2 + 2^2$, $5 = 2^2 + 1^2$, $8 = 2^2 + 2^2$, $9 = 3^2 + 0^2$, $10 = 3^2 + 1^2$, $13 = 2^2 + 3^2$ sono tutti e soli i numeri ≤ 13 che si scrivono come somma di due quadrati. In particolare $3, 6, 7, 11, 12$ non si scrivono come somma di due quadrati. Cosa hanno in comune questi numeri? Un esame attento di ulteriori esempi ci può fare indovinare la risposta:
Un intero n si scrive come la somma di due quadrati se e solo se ogni primo $\equiv 3 \pmod 4$ che divide n compare con un esponente pari nella fattorizzazione di n in fattori primi.

Questo enunciato, noto come il *teorema dei due quadrati* era già stato menzionato, senza dimostrazione, da vari autori prima di Fermat.

Nella sua corrispondenza Fermat afferma di avere dimostrato il teorema dei due quadrati (e anche quelli dei tre e quattro quadrati). Afferma che il teorema è conseguenza del seguente risultato: *un numero primo dispari, p, è somma di due quadrati se e solo se $p \equiv 1 \pmod 4$* e che quest'ultimo risultato si può dimostrare con il metodo della *discesa infinita*. Bisognerà aspettare Eulero per avere la prima dimostrazione completa (secondo la traccia lasciata da Fermat) del teorema dei due quadrati.

4.1 La dimostrazione di Fermat-Eulero.

La dimostrazione di Eulero-Fermat funziona più o meno così. Per prima cosa abbiamo l'identità di Diofante (detta anche identità di Brahmagupta, Fibonacci, Viète, ...):

Lemma 4.1. *Se due interi sono somma di due quadrati allora anche il loro prodotto è somma di due quadrati. Più precisamente se* $n = a^2 + b^2$ *e se* $m = c^2 + d^2$*, allora:*

$$nm = (a^2 + b^2)(c^2 + d^2) = (ac \pm bd)^2 + (ad \mp bc)^2$$

Dimostrazione. Basta svolgere. □

Questa identità ci porta a studiare il problema per i numeri primi: quali sono i primi, $p > 2$, che si scrivono come somma di due quadrati? Una prima osservazione:

Lemma 4.2. *Se* p *è un numero primo dispari che si scrive come la somma di due quadrati, allora* $p \equiv 1 \pmod 4$.

Dimostrazione. Un numero primo dispari è congruo a 1 o 3 (mod 4). D'altra parte un quadrato è congruo a 0 o 1 (mod 4). Quindi la somma di due quadrati è congrua a 0, 1 o 2, modulo quattro. □

Più generalmente ci si può chiedere, dato un numero primo p, se esiste un multiplo di p che si scrive come la somma di due quadrati. Posta in questi termini la risposta è sempre positiva perché: $((m^2+n^2)p).p = (mp)^2+(np)^2$. Per evitare questa tautologia si richiede che uno (e quindi entrambi) dei quadrati non sia divisibile per p. Quindi ci chiediamo se esiste un multiplo di p, mp, tale che $mp = x^2 + y^2$, con $p \nmid x$ e $p \nmid y$, cioè se esistono $x, y \not\equiv 0 \pmod p$ tali che $x^2 + y^2 \equiv 0 \pmod p$. Osserviamo che dividendo per l'inverso di y^2 nel campo $\mathbb{F}_p$, questo è equivalente a cercare a tale che $a^2 + 1 \equiv 0 \pmod p$ e questo è ancora equivalente a chiedersi se $a^2 \equiv -1 \pmod p$, cioè se -1 è un quadrato (mod p). Questo è un caso particolare della *legge di reciprocità quadratica*. Per ora abbiamo (cf Esercizio 42):

Lemma 4.3. *Sia* p *un numero primo dispari, allora l'equazione* $x^2 + y^2 \equiv 0 \pmod p$ *ha una soluzione non banale (i.e. con* $x \not\equiv 0$ *e* $y \not\equiv 0$*) se e solo se* $p \equiv 1 \pmod 4$.
In altri termini: -1 *è un quadrato modulo* $p \Leftrightarrow p \equiv 1 \pmod 4$.

Dimostrazione. La dimostrazione che segue usa il Teorema di Wilson (3.10) (forse noto a Fermat?): se p è primo $(p-1)! \equiv -1 \pmod p$.

Mostriamo che se $p = 4k + 1$, allora -1 è un quadrato modulo p. Per $1 \le i \le 2k$, abbiamo: $(4k + 1 - i) + i = 4k + 1 = p \equiv 0 \pmod p$, quindi $4k + 1 - i \equiv -i \pmod p$. Questo è più apparente scrivendo:

$$\begin{array}{cccc} 1 & 2 & \cdots & 2k \\ 4k & 4k-1 & \cdots & 2k+1 \end{array}$$

Quindi: $(-1)(-2)...(-2k) \equiv 4k(4k-1)...(2k+1) \pmod{p}$. Moltiplicando per $2k!$: $(2k!)^2 \equiv (4k)! = (p-1)! \equiv -1 \pmod{p}$. In conclusione se $p = 4k+1$, allora: $(2k!)^2 \equiv -1 \pmod{p}$.

Se $p = 4k+3$ e se $a^2 \equiv -1 \pmod{p}$, allora $(a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$. Siccome $(p-1)/2 = 2k+1$, viene: $a^{p-1} \equiv -1 \pmod{p}$. Usando il piccolo teorema di Fermat: $a \equiv -1 \pmod{p}$; ma in questo caso $a^2 \equiv 1 \pmod{p}$, siccome $-1 \not\equiv 1 \pmod{p}$, perché p è dispari, abbiamo una contraddizione. □

Un'altra dimostrazione, più moderna:

Dimostrazione. Sia $p = 4k+1$. Il gruppo moltiplicativo $\mathbb{F}_p^\times$ è ciclico, di ordine $4k$. Quindi contiene un elemento, x, di ordine 4 (cf Esercizio 40). Abbiamo $(x^2-1)(x^2+1) = x^4-1 \equiv 0 \pmod{p}$, quindi $x^2-1 \equiv 0 \pmod{p}$ o $x^2+1 \equiv 0 \pmod{p}$. Il primo caso non è possibile (x avrebbe ordine due), quindi $x^2 \equiv -1 \pmod{p}$.

Sia $p = 4k+3$ e supponiamo di avere $x^2 + y^2 \equiv 0 \pmod{p}$ con $x \not\equiv 0$ e $y \not\equiv 0$. Moltiplicando per y^{-2} (l'inverso di y^2 nel campo $\mathbb{F}_p$), abbiamo $u^2 \equiv -1 \pmod{p}$, con $u^2 = x^2y^{-2}$ in $\mathbb{F}_p$. Quindi $u^4 \equiv 1 \pmod{p}$ e u ha ordine 4. Questo è impossibile perché $4 \nmid p-1 = 4k+2 = \#(\mathbb{F}_p^\times)$. □

Per la prima parte del Lemma si può anche ragionare così:
Per il piccolo teorema di Fermat, se $(x,p) = 1$, $x^{p-1} \equiv 1 \pmod{p}$. *Se* $p = 4n+1$, *abbiamo quindi* $x^{p-1} - 1 = (x^{2n}-1)(x^{2n}+1) \equiv 0 \pmod{p}$. *Quindi* $p \mid x^{2n}-1$ *o* $p \mid x^{2n}+1$. *Quindi basta trovare* $0 < a < p$ *tale che* $p \nmid a^{2n}-1$. *Il polinomio* $X^{2n}-1$ *ha al più* $2n < 4n = \#(\mathbb{F}_p^\times)$, *quindi un tale* a *esiste.*

Quindi se $p \equiv 1 \pmod{4}$ esiste un intero $m > 0$ tale che $mp = x^2+1$, cioè un multiplo di p si scrive come la somma di due quadrati. L'idea è di usare un argomento di *discesa* e di mostrare che se $m > 1$, allora esiste un altro intero r, $1 \le r < m$, tale che rp si scriva come somma di due quadrati. Se $r > 1$ si ripete il ragionamento e siccome non si può "scendere" indefinitamente in $\mathbb{N}$ (principio del minimo), si arriverà a $r = 1$.

Teorema 4.4. (Eulero)
Un numero primo dispari, p, si scrive come la somma di due quadrati se e solo se $p \equiv 1 \pmod{4}$.

Dimostrazione. Rimane da mostrare che ogni primo $p \equiv 1 \pmod{4}$ si scrive come la somma di due quadrati. Abbiamo visto che esiste un intero $m > 0$ tale che $mp = x^2+1$. Possiamo assumere $x > 0$. Se $x > p$, allora $x = kp + x', 0 < x' < p$ e $-1 \equiv x^2 \equiv x'^2 \pmod{p}$. Inoltre se $x' \ge (p+1)/2$, allora $y = p - x'$ verifica $0 < y < p/2$ e $y^2 \equiv x'^2 \equiv -1 \pmod{p}$. In conclusione possiamo assumere $0 < x < p/2$. Questo implica: $m = (x^2+1)/p < p$.

Quindi esiste m, $0 < m < p$, tale che $mp = x^2 + y^2$. Per concludere la dimostrazione per "discesa", basta mostrare che se $m > 1$, allora esiste r, $0 < r < m$, tale che rp si scriva come la somma di due quadrati.
Siano $u, v, -m/2 \leq u, v \leq m/2$ tali che $u \equiv x \pmod{m}$ e $v \equiv y \pmod{m}$. Allora $u^2 + v^2 \equiv x^2 + y^2 \equiv 0 \pmod{m}$. Pertanto $u^2 + v^2 = rm$. Se $m > 1$, allora $r \neq 0$, perché altrimenti $u = v = 0$, quindi $m \mid x$ e $m \mid y$ e dalla relazione $mp = x^2 + y^2$ risulterebbe che $m \mid p$, cioè $m = 1$.
Inoltre $r = (u^2 + v^2)/m < m$. Abbiamo:

$$(mp)(rm) = (x^2 + y^2)(u^2 + v^2) = (xu + yv)^2 + (xv - yu)^2 \quad (*)$$

dove l'ultima uguaglianza segue dal Lemma 4.1. Siccome $u \equiv x \pmod{m}$ e $y \equiv v \pmod{m}$, $xu+yv \equiv x^2+y^2 \equiv 0 \pmod{m}$; nello stesso modo $xv-yu \equiv 0 \pmod{m}$. Quindi la relazione $(*)$ si scrive: $m^2rp = (ma)^2 + (mb)^2$, da cui: $rp = a^2 + b^2$, con $1 \leq r < m$ e questo conclude la dimostrazione. □

Per concludere la dimostrazione del teorema generale useremo il seguente (vedere però l'Esercizio 49):

Lemma 4.5. *Siano $n = a^2 + b^2$ un intero somma di due quadrati ($a, b \geq 0$) e sia $p = c^2 + d^2$ un primo somma di due quadrati. Se $p \mid n$, allora anche n/p è somma di due quadrati.*

Dimostrazione. Se $p \mid n$, allora p divide anche $d^2n - b^2p = d^2(a^2 + b^2) - b^2(c^2 + d^2) = (ad)^2 - (bc)^2 = (ad + bc)(ad - bc)$. Siccome p è primo $p \mid ad + bc$ o $p \mid ad - bc$.

Se $ad - bc = ep$, allora $np = (a^2 + b^2)(c^2 + d^2) = (ad - bc)^2 + (ac + bd)^2$ (Lemma 4.1) $= e^2p^2 + (ac + bd)^2$. Quindi $p \mid ac + bd$: $ac + bd = pf$. Pertanto $np = e^2p^2 + f^2p^2$ e $n/p = e^2 + f^2$.

Se $ad + bc = ep$, si procede in modo analogo usando $(a^2 + b^2)(c^2 + d^2) = (ad + bc)^2 + (ac - bd)^2$ (Lemma 4.1). □

Nella fattorizzazione in fattori primi di un intero n possiamo distinguere tre tipi di fattori primi:

- il primo 2
- i primi $\equiv 1 \pmod{4}$
- i primi $\equiv 3 \pmod{4}$

Teorema 4.6. (Teorema dei due quadrati)
Sia $n > 1$ un intero e sia

$$n = 2^t p_1^{a_1} \ldots p_r^{a_r} q_1^{b_1} \ldots q_s^{b_s}, \;\; p_i \equiv 1, q_j \equiv 3 \pmod{4}$$

la sua fattorizzazione in fattori primi, allora n si scrive come la somma di due quadrati se e solo se b_j è pari per ogni $j, 1 \leq j \leq s$.

Dimostrazione. Per il Teorema 4.4 ogni p_i si scrive come una somma di due quadrati, così come anche 2 $(= 1^2 + 1^2)$. Quindi per il Lemma 4.1, $m = 2^t p_1^{a_1} ... p_r^{a_r}$ si scrive come la somma di due quadrati: $m = a^2 + b^2$. Se tutti i b_j sono pari: $q_1^{b_1} ... q_s^{b_s} = c^2$. Quindi $n = (a^2 + b^2)c^2 = (ac)^2 + (bc)^2$.

Osserviamo intanto che un prodotto di un quadrato con primi distinti, tutti $\equiv 3 \pmod 4$ non è mai la somma di due quadrati. Infatti se $D^2.q_1...q_s = x^2 + y^2$ $(q_i \neq q_j$ se $i \neq j)$, allora $x^2 + y^2 \equiv 0 \pmod{q_1}$ e dal Lemma 4.3, segue che $x = q_1 x_1, y = q_1 y_1$, quindi $q_1(x_1^2 + y_1^2) = D^2.q_2...q_s$ e $q_1 \mid D^2$, cioè $q_1 \mid D$: $D = q_1 D_1$ e viene: $x_1^2 + y_1^2 = D_1^2.q_1...q_s$. Quindi $q_1 \mid x_1^2 + y_1^2$ e possiamo ricominciare. Quando abbiamo esaurito tutti i fattori primi uguali a q_1 di D, arriviamo a: $q_1(x_l^2 + y_l^2) = D_{l-1}^2.q_2...q_s$, con $(q_1, D_{l-1}) = 1$ e siccome $q_1 \nmid q_j$ se $j > 1$, abbiamo un assurdo.

Supponiamo adesso che alcuni b_j siano dispari, siccome $q^{2b'+1} = (q^{b'})^2.q$, possiamo scrivere: $n = 2^t p_1^{a_1} ... p_r^{a_r} Q^2 q_{j_1} ... q_{j_k}$, dove i q_{j_i} corrispondono ai b_j dispari. Per il Lemma 4.5, dividendo successivamente per $2, p_1, ..., p_r$ il numero di volte necessario e usando il Teorema 4.4, se n è somma di due quadrati, allora anche $Q^2.q_{j_1}...q_{j_k}$ è somma di due quadrati, in contraddizione con quanto appena visto. □

Questa dimostrazione, davvero ingegnosa, è comunque *elementare*, cioè usa solo strumenti elementari: piccolo teorema di Fermat, identità algebriche, proprietà di base dei numeri primi.

———— .. ————

Esercizi.

Esercizio 49 *Una presentazione alternativa della dimostrazione del Teorema 4.4. Sia p un primo congruo a 1 mod.4. Come nel testo esiste un multiplo di p somma di due quadrati: $N = mp = a^2 + b^2$, con $0 < a, b < p/2$.*
(i) Possiamo assumere $(a, b) = 1$. I divisori primi di m sono tutti $< (p/2)$ e nessuno di loro è congruo a 3 mod. 4. Quindi per ipotesi di induzione possiamo assumere che sono tutti somma di due quadrati.
(ii) Concludere la dimostrazione applicando ripetutamente il Lemma 4.5

Esercizio 50 *Se $N = x^2 + y^2$ $(*)$ diremo che (x, y) (prendendo x, y positivi) è una "rappresentazione" (come somma di due quadrati) di N. Una rappresentazione è "propria" se $(x, y) = 1$.*
(i) Mostrare che N ammette una rappresentazione propria se e solo se i suoi fattori primi dispari sono tutti congrui a 1 mod. 4.
(ii) Mostrare che se N ammette una rappresentazione propria, allora N non è multiplo di 4.
(iii) Se $N = 2M$, M dispari, esiste una corrispondenza biunivoca tra le rappresentazioni di N e quelle di M. In questa corrispondenza le rappresentazioni proprie si corrispondono.
Se $(x, y) = d$, $x'd = x, y'd = y$, allora $N = d^2N'$ e (x', y') è una rappresentazione propria di N'. In conclusione per le questioni riguardanti le rappresentazioni ci si può limitare alle rappresentazioni proprie di interi dispari.

Esercizio 51 *Se $N = a^2+b^2$, $M = c^2+d^2$, allora, per il Lemma 4.1, NM ha due "rappresentazioni" (cf Esercizio 50) che diremo ottenute da (a, b) e (c, d) "per composizione".*
(i) Osservare la seguente formulazione del Lemma 4.5: Sia (a, b) una rappresentazione di N e sia (c, d) una rappresentazione del primo p. Se $p \mid N$, allora N/p ha una rappresentazione (x, y) tale che (a, b) si ottenga per composizione di (c, d) con (x, y).
(ii) Mostrare che un primo p congruo a 1 mod. 4 ammette un'unica (a meno dell'ordine dei termini) rappresentazione (necessariamente propria).

Esercizio 52 *Si ricorda che un intero n è perfetto se $\sigma(n) = 2n$ (cf Esercizi 10, 14, 15). Sia N un numero perfetto dispari (se mai ne esiste uno!) e sia $N = p_0^{a_0} ... p_n^{a_n}$ la sua fattorizzazione in primi.*
(i) Osservare che $2N = \sigma(N) = \prod_{i=0}^{n}(1 + p_i + ... + p_i^{a_i})$ e concludere che esiste un unico indice j, $0 \le j \le n$, tale che a_j sia dispari.
(ii) Riordinando semmai gli indici possiamo assumere $j = 0$. Poniamo $p_0 =$

$q, a_0 = 2t+1$. *Quindi* $N = q^{2t+1}.\prod_{i=1}^{n} p_i^{2\alpha_i}$. *Mostrare che* $q \equiv 1 \pmod 4$.
(iii) Mostrare che t *è pari. In conclusione un numero perfetto dispari è della forma:* $N = q^{4b+1}.\prod p_i^{2\alpha_i}$, *con* $q \equiv 1 \pmod 4$. *Questo risultato è dovuto a Eulero.*
(iv) Concludere che un numero perfetto non è mai un quadrato perfetto (La perfezione ha i suoi limiti!).
(v) Mostrare che un numero perfetto pari non si scrive come la somma di due quadrati. Cosa potete dire nel caso dispari?

Esercizio 53 *Scopo di questo esercizio è dimostrare che se* N *è un numero perfetto dispari, allora* $N > 10^4$.

Abbiamo visto (Esercizio 52) che un numero perfetto dispari è della forma $N = q^{4b+1}.\prod p_i^{2a_i}$, *con* $q \equiv 1 \pmod 4$. *Il primo* q *si chiama "primo speciale" o di Eulero.*
(i) Mostrare che $(q+1)/2 \mid N$.
(ii) Mostrare che se $3 \nmid N$, *allora* $q \geq 13$. *Concludere che se* $N < 10^4$, *allora* $3 \mid N$ *(Usare l'Esercizio 15).*
(iii) Mostrare che se $N < 10^4$ *è un numero perfetto dispari, allora* $3^2 \parallel N$ *e* $13 \mid N$.
(iv) Mostrare che se $N < 10^4$ *è un numero perfetto dispari allora* $q = 13$.
(v) Concludere che se N *è un numero perfetto dispari allora* $N > 10^4$.
Osservazione: *Si congettura che non esista alcun numero perfetto dispari e si sa che un numero perfetto dispari è* $> 10^{1500}$.

4.2 L'anello degli interi di Gauss e il teorema dei due quadrati.

Gauss oltre ad introdurre e studiare sistematicamente le congruenze fu uno dei primi ad usare i numeri complessi in aritmetica. In particolare studiò le proprietà aritmetiche di quello che si chiama oggi *l'anello degli interi di Gauss*, $\mathbb{Z}[i]$. Non è quindi sorprendente che Dedekind (allievo di Gauss) riuscì, usando l'anello degli interi di Gauss, a dare una dimostrazione più "concettuale" del Teorema dei due quadrati.

Nel seguito indichiamo con A l'insieme $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}, i^2 = -1\}$; chiaramente $(A, +, .)$ è un sotto anello di $\mathbb{C}$, quindi integro. Per le nozioni relative alla divisione (elementi primi, irriducibili, unità ecc...) rimandiamo alla Sezione 2.3.

Osserviamo subito che i primi di $\mathbb{Z}$ non sono necessariamente primi (o irriducibili) in A: $(1 + i)(1 - i) = 2$ e $1 \pm i$ non è un'unità (perché?).

Lo strumento fondamentale per studiare l'anello A è la *norma*.

Definizione 4.7. *Sia $\alpha = a + ib \in A$. Il coniugato di α è $\overline{\alpha} = a - ib$ e la norma di α è $N(\alpha) = \alpha.\overline{\alpha} = a^2 + b^2$.*

La norma di α non è nient'altro che il quadrato del modulo di α considerato come numero complesso.

Le osservazioni fondamentali sono:

- la norma è moltiplicativa: $N(\alpha.\beta) = N(\alpha).N(\beta)$
- $\alpha \mid N(\alpha) = \alpha\overline{\alpha}$
- $N(\alpha) \in \mathbb{N}$.

Questo ci permette subito di determinare le unità di A:

Lemma 4.8. *L'elemento $\alpha \in \mathbb{Z}[i]$ è un'unità se e solo se $N(\alpha) = 1$. Le unità di $\mathbb{Z}[i]$ sono esattamente: $\pm 1, \pm i$.*

Dimostrazione. Se α è un'unità allora $\alpha\beta = 1$ per un certo β, quindi $N(\alpha).N(\beta) = N(1) = 1$. Quindi un'unità ha norma uno. Viceversa sia $\alpha = a + ib$, con $N(\alpha) = a^2 + b^2 = 1$, allora $a = \pm 1$ e $b = 0$ o $a = 0$ e $b = \pm 1$. Quindi $\alpha = \pm 1, \pm i$ che sono chiaramente delle unità. □

Mostriamo adesso che A è un anello euclideo.

Proposizione 4.9. *Siano $\alpha, \gamma \in \mathbb{Z}[i]$, $\gamma \neq 0$, allora esistono $\delta, \rho \in \mathbb{Z}[i]$ tali che: $\alpha = \gamma.\delta + \rho$, con $0 \leq N(\rho) < N(\gamma)$.*

Dimostrazione. Abbiamo $\alpha/\gamma = (\alpha\overline{\gamma})/(\gamma.\overline{\gamma}) = r + si$, con $r, s \in \mathbb{Q}$. Siano $m, n \in \mathbb{Z}$ tali che $|r-m| \leq 1/2$, $|s-n| \leq 1/2$ e poniamo $\delta = m+in$. Abbiamo $\delta \in \mathbb{Z}[i]$. Abbiamo, con un abuso di notazioni, $N(\alpha/\gamma - \delta) = N((r-m) + i(s-n)) = |r-m|^2 + |s-n|^2 \leq 1/4 + 1/4 = 1/2$. Sia $\rho = \alpha - \gamma.\delta$. Allora $\rho \in \mathbb{Z}[i]$ e:

$$N(\rho) = N(\gamma(\alpha/\gamma - \delta)) = N(\gamma).N(\alpha/\gamma - \delta) \leq N(\gamma)/2 < N(\gamma)$$

In conclusione: $\alpha = \gamma.\delta + \rho$, con $0 \leq N(\rho) < N(\gamma)$. □

Osservazione 4.10. Osserviamo che nel caso di $\mathbb{Z}[i]$, la coppia (δ, ρ) non è univocamente determinata (Esercizio 54).

Sappiamo (Sezione 2.3) che ogni anello euclideo è un P.I.D. che, in un P.I.D., le nozioni di elemento primo, elemento irriducibile sono equivalenti, finalmente ogni P.I.D. è fattoriale (U.F.D.). In conclusione ogni elemento di $\mathbb{Z}[i]$ si scrive come un prodotto di elementi primi e questa fattorizzazione è unica a meno dell'ordine dei fattori e della moltiplicazione per unità.

Rimane da capire chi sono i primi di $\mathbb{Z}[i]$. Dei candidati "naturali" sono i numeri interi primi (cioè i primi di $\mathbb{Z}$), ma abbiamo già visto che un primo p non rimane sempre primo in $\mathbb{Z}[i]$ ($2 = (1+i)(1-i)$, $5 = (2+i)(2-i)$). Torneremo più avanti su questo argomento. Per il momento abbiamo:

Proposizione 4.11. *Sia p un primo con $p \equiv 1 \pmod 4$, allora p si scrive come la somma di due quadrati.*

Dimostrazione. Esiste un primo $\pi \in \mathbb{Z}[i]$ che divide p: $p = \alpha\pi$. Quindi $p^2 = N(p) = N(\alpha)N(\pi)$. Se α non è un'unità, allora $N(\alpha) > 1$ (Lemma 4.8) e pertanto $p = N(\alpha) = N(\pi)$. Se $\pi = x + iy$, allora $N(\pi) = x^2 + y^2 = p$ e p si scrive come la somma di due quadrati.

Rimane quindi da mostrare che α non è un'unità.

Siccome $p \equiv 1 \pmod 4$, -1 è un quadrato $\pmod p$ (Lemma 4.3), quindi esistono k, m tali che $kp = m^2 + 1 = (m+i)(m-i)$. Siccome $\pi \mid p$ e π è primo, $\pi \mid m+i$ o $\pi \mid m-i$, cioè $\pi \mid m \pm i$.

Se α è un'unità: $\pi = p\alpha^{-1}$ e quindi $p \mid \pi$. Segue pertanto che $p \mid m \pm i$ (attenzione: dall'uguaglianza $kp = (m+i)(m-i)$ non si può concludere a priori che $p \mid m \pm i$, perché non sappiamo che p è primo; infatti non lo è!). Abbiamo quindi $(a+ib)p = m \pm i$, cioè $pb = \pm 1$, ma questo è assurdo. Quindi α non è un'unità. □

Possiamo anche portare un piccolo complemento (cf Esercizio 51). Iniziamo con la seguente osservazione:

Lemma 4.12. *Sia $\alpha \in \mathbb{Z}[i]$, se $N(\alpha) = p$, p primo, allora α è primo.*

Dimostrazione. Sia $\alpha = \beta.\gamma$, allora $p = N(\alpha) = N(\beta).N(\gamma)$, quindi deve essere $N(\beta) = 1$ o $N(\gamma) = 1$, cioè (Lemma 4.8), β o γ è un'unità. Pertanto α è irriducibile, quindi primo. □

Proposizione 4.13. *Ogni primo $p \equiv 1 \pmod 4$ si scrive, in modo unico, come somma di due quadrati.*

Dimostrazione. Rimane da mostrare l'unicità. Se $p = \pi \prod_i \pi_i$ è la fattorizzazione in fattori primi, allora ogni π_i ha norma p, quindi $p = \pi\pi_1$. Ma $N(\pi) = \pi\overline{\pi} = N(\overline{\pi}) = p$ e anche $\overline{\pi}$ è primo (Lemma 4.12). In conclusione la fattorizzazione di p è: $p = \pi.\overline{\pi}$. Adesso se $p = a^2 + b^2$, allora $\xi = a + ib$ è primo (perché $N(\xi) = p$, Lemma 4.12), quindi per unicità della fattorizzazione $\xi \sim \pi$. Cioè $\xi = \pm\pi$ o $\xi = \pm i\pi$ (Lemma 4.8) pertanto $a = \pm x$, $b = \pm y$ o $a = \mp y$, $b = \pm x$ e la decomposizione è unica (a meno dell'ordine dei termini). □

Questa dimostrazione è senz'altro più facile (e più concettuale) di quella di Eulero-Fermat!

Possiamo riassumere il risultato nel modo seguente: un primo $p \equiv 3 \pmod 4$ rimane primo in $\mathbb{Z}[i]$ (si dice che p è *inerte*), mentre un primo $p \equiv 1 \pmod 4$ non rimane primo in $\mathbb{Z}[i]$ ma si fattorizza $p = \pi\overline{\pi}$ (si dice che p *si decompone*).

La morale della storia è che per quanto riguarda il problema di determinare i primi p che si scrivono nella forma $x^2 + ny^2$ conviene lavorare in $\mathbb{Z}[i\sqrt{n}] = \mathbb{Z}[\sqrt{-n}]$. Bisogna quindi studiare le proprietà aritmetiche di questi anelli (sono principali? chi sono le unità? quali primi p sono inerti (risp. si decompongono)?).

Esercizi.

Esercizio 54 *Mostrare con un esempio che il quoziente e il resto della divisione in $\mathbb{Z}[i]$ non sono univocamente determinati.*

Esercizio 55 *Segue dal teorema dei due quadrati che l'equazione diofantea $x^2 + y^2 = z^2$ $(*)$ ha (infinite) soluzioni.*
(i) Dividendo per l'MCD possiamo assumere $(x, y, z) = 1$. Segue che x, y, z sono due a due primi tra di loro. Mostrare che si può assumere x, z dispari e y pari.
(ii) Mostrare che $(z - x, z + x) = 2$. Porre $y = 2y', z + x = 2x', z - x = 2z'$ e concludere che le soluzioni di $(*)$ sono (a meno dell'ordine dei termini) tutte della forma: $x = d(u^2 - v^2)$, $y = 2duv$, $z = d(u^2 + v^2)$, dove u e v sono primi tra di loro.

Esercizio 56 *Trovare il più piccolo intero $x > 0$ tale che $2x^2 = y^2 + z^2$ con $y \neq z$.*

Esercizio 57 *Scopo dell'Esercizio è mostrare che l'equazione $z^2 = x^4 + y^4$ non ha soluzioni intere con $xyz \neq 0$.*
(i) Possiamo assumere x, y, z due a due primi tra diloro. Per l'Esercizio 55 possiamo assumere $x^2 = u^2 - v^2$, $y^2 = 2uv$, $z = u^2 + v^2$, con $(u, v) = 1$. Mostrare che $4 \mid y^2$, u è dispari e $v = 2v'$ è pari.
(iii) Mostrare che u e v' sono dei quadrati ($u = a^2, v' = b^2$).
(iv) Mostrare che $u = c^2 + d^2$, $(c, d) = 1$.
(v) Mostrare che c, d sono anche loro dei quadrati ($c = m^2, d = k^2$).
(vi) Osservare che $u = a^2 = m^4 + k^4$ e concludere ("per discesa") la dimostrazione.

Come corollario segue che l'equazione "di Fermat" $x^4 + y^4 = z^4$ non ammette nessuna soluzione non banale (cioè con $xyz \neq 0$). Questo è l'unico risultato enunciato da Fermat di cui abbiamo una dimostrazione completa dello stesso Fermat.

4.3 Il teorema dei quattro quadrati.

Il teorema dei quattro quadrati, enunciato da Fermat, fu dimostrato per la prima volta da Lagrange. Oggi ci sono varie dimostrazioni di questo risultato (con o senza i quaternioni), vediamone una "elementare" e simile a quella di Euler per i due quadrati.

Lemma 4.14. *Se gli interi m, n sono somma di quattro quadrati, anche il loro prodotto è somma di quattro quadrati. Più precisamente: se $m = a^2 + b^2 + c^2 + d^2$ e $n = e^2 + f^2 + g^2 + h^2$, allora:*

$$mn = (ae + bf + cg + dh)^2 + (af - be + ch - dg)^2 +$$

$$+(ag - bh - ce + df)^2 + (ah + bg - cf - de)^2.$$

Dimostrazione. Basta svolgere. □

A questo punto basta mostrare che ogni numero primo è somma di (al più) quattro quadrati. Siccome $2 = 1^2 + 1^2 + 0^2 + 0^2$, possiamo assumere p dispari.

Lemma 4.15. *Sia p un primo dispari. Esiste un intero k, $0 < k < p$, tale che $kp = x^2 + y^2 + 1$, per opportuni interi x, y.*

Dimostrazione. Mostriamo che esistono x, y con $0 \leq x, y < p/2$ tali che $x^2 + y^2 + 1 \equiv 0 \pmod{p}$. Sia $S = \{0^2, 1^2, ..., (\frac{p-1}{2})^2\}$ e sia $T = \{-1 - 0^2, -1 - 1^2, ..., -1 - (\frac{p-1}{2})^2\}$. In altri termini $S = \{x^2 \mid 0 \leq x \leq (p-1)/2\}$, mentre $T = \{-1-y^2 \mid 0 \leq y \leq (p-1)/2\}$. Chiaramente $S \cap T = \emptyset$, perché $x^2 = -1-y^2$ implica $x^2+y^2 = -1$ che non ha soluzioni in $\mathbb{R}$. D'altra parte se indichiamo con $\overline{S}$ l'insieme delle classi degli elementi di S modulo p, allora $\#(\overline{S}) = (p+1)/2$ perché $x^2 \equiv y^2 \pmod{p}$ è equivalente a $x^2 - y^2 \equiv (x-y)(x+y) \equiv 0 \pmod{p}$ e quindi $x \equiv \pm y \pmod{p}$. Ma questo non è possibile visto che $x, y < p/2$. Nello stesso modo $\#(\overline{T}) = (p+1)/2$. Siccome $\#(S \cup T) = p + 1$, per il principio dei cassetti (*pigeonhole principle*), esistono $x^2 \in S$, $-1 - y^2 \in T$ tali che $x^2 \equiv -1 - y^2 \pmod{p}$. Quindi $x^2 + y^2 + 1 = kp$. Siccome $x^2 + y^2 + 1 \leq 2(\frac{p-1}{2})^2 + 1 < p^2$, abbiamo $k < p$. □

Proposizione 4.16. *Ogni numero primo si scrive come la somma di (al più) quattro quadrati.*

Dimostrazione. Abbiamo già visto il caso $p = 2$. Sia p un primo dispari. Sia $Q = \{k \mid k \in \mathbb{N}, 0 < k < p$, e kp si scrive come la somma di quattro quadrati $\}$. Per il Lemma 4.15, $Q \neq \emptyset$ ($kp = x^2 + y^2 + 1^2 + 0^2$ con $k < p$). Quindi per il principio del minimo Q ha un elemento minimo m. Mostriamo, con il metodo della discesa infinita, che $m = 1$. Quindi supponiamo $m > 1$ e mostriamo che Q contiene un elemento più piccolo di m.

Sia $mp = x^2 + y^2 + z^2 + w^2$.

-Se m è pari, x, y, z, w sono tutti pari o tutti dispari o due sono pari e due sono dispari. Riordinando semmai i termini possiamo assumere $x \equiv y \pmod 2$ e $z \equiv w \pmod 2$. Quindi $(x \pm y)/2$ e $(z \pm w)/2$ sono degli interi. Abbiamo:

$$(\frac{x-y}{2})^2 + (\frac{x+y}{2})^2 + (\frac{z-w}{2})^2 + (\frac{z+w}{2})^2 = \frac{m}{2}p$$

quindi $m/2 \in Q$, contro la minimalità di m.

-Sia $m > 1$ dispari. Siano a, b, c, d tali che $a \equiv x \pmod m$, $b \equiv y \pmod m$, $c \equiv z \pmod m$, $d \equiv w \pmod m$, con $-m/2 < a, b, c, d < m/2$ (osservare che se $m = 2k + 1$, $\{-k, ..., -1, 0, 1, ..k\}$ è un sistema completo di residui modulo m). Abbiamo:

$$a^2 + b^2 + c^2 + d^2 \equiv x^2 + y^2 + z^2 + w^2 \equiv mp \equiv 0 \pmod m$$

Quindi $a^2+b^2+c^2+d^2 = km$ per un qualche intero k. Siccome $0 \leq a^2+b^2+c^2+d^2 < 4(m/2)^2 = m^2$, abbiamo $0 \leq k < m$. Se $k = 0$, allora $a = b = c = d = 0$. Questo implica $x \equiv y \equiv z \equiv w \equiv 0 \pmod m$ e questo a sua volta implica $m^2 \mid mp$, cioè $m = p$ ($m > 1$ per ipotesi), ma questo non è possibile perché $m < p$ per definizione. Quindi $0 < k < m$. Abbiamo:

$$(x^2 + y^2 + z^2 + w^2)(a^2 + b^2 + c^2 + d^2) = m^2kp$$

Per il Lemma 4.14, viene:

$$A^2 + B^2 + C^2 + D^2 = m^2kp$$

con $A = ax + by + cz + dw$, $B = bx - ay + dz - cw$, $C = cx - dy - az + bw$, $D = dx+cy-bz-aw$. Ma, per definizione di a, b, c, d: $A \equiv x^2+y^2+z^2+w^2 \equiv 0 \pmod m$, $B \equiv yx - xy + wz - zw \equiv 0 \pmod m$, $C \equiv zx - wy - xz + yw \equiv 0 \pmod m$ e $D \equiv wx + zy - yz - xw \equiv 0 \pmod m$. Quindi $A = mA'$, cioè $A^2 = m^2A'^2$, nello stesso modo m^2 divide B^2, C^2, D^2 e viene: $A'^2 + B'^2 + C'^2 + D'^2 = kp$, con $k < m$, contro la minimalità di m. □

Adesso si conclude facilmente:

Teorema 4.17. (Lagrange)
Ogni intero si scrive come la somma di (al più) quattro quadrati.

Dimostrazione. Se $n > 1$ sia $n = \prod p_i^{a_i}$ la sua fattorizzazione in numeri primi. Per la Proposizione 4.16, ogni p_i si scrive come una somma di quattro quadrati. Si conclude con il Lemma 4.14. I casi $n = 0, 1$ sono evidenti ($0 = 0^2, 1 = 1^2$).
□

Il Lemma 4.15 potrebbe fare pensare che bastano tre quadrati. Non è così: 7 non si scrive come la somma di (al più) tre quadrati (Esercizio 28) (ma $7 = 2^2 + 1^2 + 1^2 + 1^2$). Però abbiamo $2 \times 7 = 14 = 2^2 + 3^2 + 1$.

A questo punto è naturale chiedersi quali siano gli interi che si scrivono come somma di tre quadrati. Abbiamo:

Teorema 4.18. (Gauss)
Un intero n si scrive come la somma di tre quadrati se e solo se non è della forma $4^a(8m + 7)$.

La dimostrazione di questo risultato è più complicata di quelle dei teoremi dei due o quattro quadrati perché il prodotto di due numeri somme di tre quadrati non è necessariamente un numero somma di tre quadrati (contrariamente a quanto avviene nel caso di due, quattro quadrati).

———— ·· ————

Esercizi.

Esercizio 58 *Mostrare con un esempio che il prodotto di due numeri somme di tre quadrati non si scrive necessariamente come somma di tre quadrati.*

Esercizio 59 *In una lettera a Mersenne del 1636 Fermat "annuncia" i teoremi dei due, tre, quattro quadrati e il seguente risultato:*

Ogni numero si scrive come la somma di tre numeri triangolari. $(*)$

Si ricorda che n è triangolare se è della forma: $n = k(k+1)/2$.
(i) Dedurre da $(*)$ che ogni numero congruo a 3 mod. 8 si scrive come la somma di tre quadrati.
(ii) Usando (i) osservare che $n = 8m+4$ si scrive come somma di quattro quadrati. Se $8m+4 = x_1^2 + ... + x_4^2$, gli x_i hanno tutti la stessa parità. Se sono dispari usare

$$\left(\frac{x_1+x_2}{2}\right)^2 + \left(\frac{x_1^2-x_2^2}{2}\right)^2 = \frac{x_1^2+x_2^2}{2}$$

per concludere che $4m+2$ e poi $2m+1$ è somma di quattro quadrati. Concludere che ogni numero dispari si scrive come somma di quattro quadrati.
(iii) Con un ragionamento analogo a quello di (ii) mostrare che se $2m+1$ è somma di quattro quadrati, allora lo sono anche $4m+2, 4m+6$. Concludere che $(*)$ implica il teorema dei quattro quadrati.
(iv) Mostrare che $(*)$ è equivalente a sapere che ogni $n \equiv 3 \pmod 8$ si scrive come somma di tre quadrati.

Esercizio 60 *Mostrare che il teorema dei tre quadrati (Teorema 4.18) implica il teorema dei quattro quadrati (considerare $n - 4^a$).*

5

La legge di reciprocità quadratica.

5.1 Introduzione.

Il teorema dei due quadrati si può interpretare come un risultato sulle forme binarie quadratiche: quali sono gli interi rappresentati dalla forma x^2+y^2? Più generalmente ci si può chiedere, con Eulero, quali sono gli interi rappresentati dalla forma quadratica $x^2 + ay^2$ (a un intero positivo o negativo). Eulero si accorse subito che il problema è moltiplicativo: cioè se $n = t^2 + ak^2$ e se $m = u^2 + av^2$, allora anche mn è della forma $x^2 + ay^2$ per opportuni x, y (Esercizio 61). Questo riconduce il problema a determinare i primi p che si possono scrivere nella forma $x^2 + ay^2$. Chiaramente se $p = x^2 + ay^2$, allora $p \mid x^2 + ay^2$. Quindi un primo problema (più facile) consiste nel determinare i primi p tali che un loro multiplo si scriva nella forma $x^2 + ay^2$; è esattamente quello che abbiamo fatto nel caso dei due quadrati ($a = 1$). Ovviamente la cosa è interessante se $p \nmid x$ (al fine di evitare le soluzioni banali $(x^2p+ay^2p)p = (xp)^2 + a(yp)^2$). In altri termini ci chiediamo se la congruenza $x^2 + ay^2 \equiv 0 \pmod{p}$ ha delle soluzioni non banali. Se $p \mid a$, la congruenza si riduce a $x^2 \equiv 0 \pmod{p}$, e quindi $x \equiv 0 \pmod{p}$. In conclusione il nostro problema diventa: per quali primi p, con $(a, p) = 1$, la congruenza $x^2 + ay^2 \equiv 0 \pmod{p}$ ammette soluzioni non banali (i.e. con $xy \not\equiv 0 \pmod{p}$)?

Osserviamo che se $x^2 + ay^2 \equiv 0 \pmod{p}$, con $xy \not\equiv 0 \pmod{p}$, allora $x^2 \equiv -ay^2 \pmod{p}$ e moltiplicando per $(y^{-1})^2$, si ottiene: $-a \equiv (xy^{-1})^2 \pmod{p}$, cioè $-a$ è un quadrato modulo p. Viceversa se $-a \equiv b^2 \pmod{p}$, allora $mp = b^2 + a.1^2$ e mp si scrive nella forma $x^2 + ay^2$. Quindi $x^2 + ay^2 \equiv 0 \pmod{p} \Leftrightarrow -a$ è un quadrato modulo p.

Bisognerebbe quindi vedere per tutti i primi, p, che non dividono a se $-a$ è o meno un quadrato modulo p. In effetti Eulero ha trovato un criterio (Teorema 5.2) in questo senso, ma questo criterio non è soddisfacente anche perché bisognerebbe applicarlo per infiniti primi! Ma Eulero, il calcolatore

geniale, si era accorto di un fenomeno molto particolare: per due primi dispari, p, q, c'è un legame tra il fatto che p sia o meno un quadrato modulo q e il fatto che q sia o meno un quadrato modulo p. Questo legame, che è proprio la *legge di reciprocità quadratica*, fu formulato chiaramente per la prima da Legendre nel 1785. Diciamo che il *carattere quadratico* di $p \pmod q$ è 1 se p è un quadrato modulo q e -1 se p non è un quadrato modulo q. Allora:

(Legge di reciprocità quadratica) Siano p, q due primi dispari. Allora p e q hanno lo stesso carattere quadratico tranne se sono entrambi congrui a $3 \pmod 4$ e in tal caso i caratteri sono opposti.

Più precisamente Legendre introduce il seguente simbolo (simbolo di Legendre) $\left(\frac{p}{q}\right)$ per indicare il carattere quadratico di p modulo q (Definizione 5.4), con questa notazione la legge di reciprocità quadratica diventa:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)}{2} \cdot \frac{(q-1)}{2}}.$$

Ci sono poi due complementi (Proposizione 5.6, Proposizione 5.10) che trattano il caso di -1 e 2:

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}, \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

In realtà il simbolo di Legendre $\left(\frac{a}{p}\right)$ viene definito per ogni $a \in \mathbb{Z}$, $(a, p) = 1$, p primo dispari, per rappresentare il carattere quadratico di $a \pmod p$ (1 se $a \equiv \square \pmod p$, -1 altrimenti). Grazie al criterio di Eulero il carattere quadratico è moltiplicativo (Proposizione 5.5), quindi se $a = \prod p_i$, $\left(\frac{a}{q}\right) = \prod \left(\frac{p_i}{q}\right)$. Ma grazie alla legge di reciprocità quadratica e ai complementi possiamo calcolare $\left(\frac{p_i}{q}\right)$ in funzione di $\left(\frac{q}{p_i}\right)$. Quindi per sapere se a è un quadrato modulo q, basta trovare il carattere quadratico di q modulo p_i dove i p_i sono i primi che dividono a. Vediamo con un esempio come questo ci può aiutare nel nostro problema iniziale. Sia a trovare i primi $p > 3$ tali che un loro multiplo sia della forma $x^2 + 6y^2$ con $xy \not\equiv 0 \pmod p$. Come abbiamo visto questo torna a vedere se -6 è o meno un quadrato modulo p, cioè a calcolare $\left(\frac{-6}{p}\right)$. Abbiamo:

$$\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)$$

$$= (-1)^{(p-1)/2}.(-1)^{(p^2-1)/8}.\left(\frac{3}{p}\right)$$

Adesso: $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{(p-1)/2}$, quindi $\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right)$. Finalmente:

$$\left(\frac{-6}{p}\right) = (-1)^{(p^2-1)/8}\left(\frac{p}{3}\right)$$

Adesso

$$(-1)^{(p^2-1)/8} = \begin{cases} 1 \text{ se } p \equiv 1,7 \pmod 8 \\ -1 \text{ se } p \equiv 3,5 \pmod 8 \end{cases}$$

Osservare che questo esaurisce tutte le possibilità perché p è un primo dispari. D'altra parte i quadrati modulo 3 sono $0^2 = 0$, $1^2 = 1$, $2^2 = 4 \equiv 1 \pmod 3$, quindi:

$$\left(\frac{p}{3}\right) = \begin{cases} 1 \text{ se } p \equiv 1 \pmod 3 \\ -1 \text{ se } p \equiv 2 \pmod 3 \end{cases}$$

Questo esaurisce tutti i casi per $p > 3$ primo.

In conclusione, se $p > 3$ è primo:

$$\left(\frac{-6}{p}\right) = 1 \text{ se } p \equiv 1,7 \pmod 8 \text{ e } p \equiv 1 \pmod 3$$

$$\text{oppure se } p \equiv 3,5 \pmod 8 \text{ e } p \equiv 2 \pmod 3.$$

In conclusione se $p > 3$ è primo, un multiplo di p è della forma $x^2 + 6y^2$ se e solo se $p \equiv 1, 5, 7, 11 \pmod{24}$.

Una volta che sappiamo quali sono i primi tali che un loro multiplo sia della forma $x^2 + ay^2$, con un argomento di discesa (come nel teorema dei due quadrati), possiamo sperare di determinare gli interi rappresentati dalla forma $x^2 + ay^2$, risolvendo completamente il nostro problema iniziale. Questo mostra la potenza della legge di reciprocità quadratica, indovinata da Eulero, formulata da Legendre e dimostrata da Gauss.

Infatti il primo a proporre una dimostrazione della legge di reciprocità quadratica fu Legendre, ma la sua dimostrazione assumeva un risultato ben più profondo, il teorema di Dirichlet sui i primi in una progressione aritmetica:

Teorema 5.1. (Dirichlet)
Se $(a, b) = 1$, *esistono infiniti primi della forma* $ax + b$.

Questo teorema dall'apparenza innocua è uno dei più profondi risultati della teoria dei numeri e fu dimostrato da Dirichlet solo nel 1837. La dimostrazione di Legendre era quindi incompleta. La prima dimostrazione della legge di reciprocità quadratica fu data da Gauss nelle *Disquisitiones* ([4]),

per Gauss questo era il teorema "fondamentale", il gioiello della matematica (ben più importante del teorema "fondamentale dell'algebra"), quello che gli faceva dire che "l'aritmetica è la regina della matematica", tanto è vero che Gauss, nel corso della sua vita, diede ben otto diverse dimostrazioni della legge di reciprocità quadratica. Al giorno d'oggi sono state elencate ben 200 dimostrazioni, più o meno diverse, della legge di reciprocità quadratica, che risulta, dopo il teorema di Pitagora, il risultato "più" dimostrato della matematica. I tentativi di generalizzare questo risultato (a leggi di reciprocità cubiche, biquadratiche ecc...) sono all'origine della teoria algebrica dei numeri. Al momento il risultato più generale riguardo a questa questione sono le leggi di reciprocità di Emil Artin.

5.2 Il criterio di Eulero.

Come abbiamo visto un problema centrale è quello di sapere determinare se un dato intero a è o meno un quadrato modulo p ($(a,p) = 1$). Un primo risultato in questa direzione è il seguente criterio dovuto a Eulero:

Teorema 5.2. (Eulero)
Sia q un numero primo e a un intero con $(a,q) = 1$. Allora:

$$a \text{ è un quadrato} \pmod q \Leftrightarrow a^{(q-1)/2} \equiv 1 \pmod q.$$

Dimostrazione. ($\Rightarrow$) Se $a \equiv b^2 \pmod q$, allora $a^{(q-1)/2} \equiv b^{q-1} \equiv 1 \pmod q$, per il piccolo teorema di Fermat.

($\Leftarrow$) Mostriamo la contrapposta: se a non è un quadrato $\pmod q$, allora $a^{(q-1)/2} \not\equiv 1 \pmod q$ (e quindi $a^{(q-1)/2} \equiv -1 \pmod q$). L'equazione $X^{(q-1)/2} - 1 \equiv 0 \pmod q$ ha al più $(q-1)/2$ soluzioni nel campo $\mathbb{F}_q$. Se $x \in \{1, 2, ...(q-1)/2\}$, allora $y = x^2$ verifica $y^{(q-1)/2} = x^{q-1} \equiv 1 \pmod q$. Osserviamo che se $x, x' \in \{1, 2, ..., (q-1)/2\}$ allora $x^2 \not\equiv x'^2 \pmod q$, perché altrimenti si avrebbe $x^2 - x'^2 = (x - x')(x + x') \equiv 0 \pmod q$, ma $x + x' \not\equiv 0 \pmod q$ perché $x + x' \leq q - 1$, quindi $x = x'$.

In conclusione $P(X) = X^{(q-1)/2} - 1$ ha tutte le sue radici in $\mathbb{F}_q$ e ogni sua radice è un quadrato. Quindi se $a \neq \square \pmod q$, a non è radice di $P(X)$ e $a^{(q-1)/2} \not\equiv 1 \pmod q$. □

Osservazione 5.3. Abbiamo anche $a \neq \square \pmod q \Leftrightarrow a^{(q-1)/2} \equiv -1 \pmod q$. Infatti per il piccolo Fermat $(a^{(q-1)/2})^2 \equiv 1 \pmod q$, quindi $a^{(q-1)/2}$ è radice dell'equazione $X^2 \equiv 1 \pmod q$, le cui radici sono ± 1.

Introduciamo adesso il simbolo di Legendre:

Definizione 5.4. (Il simbolo di Legendre.)
Sia q un numero primo dispari *e $n \in \mathbb{Z}$, $n \neq 0 \pmod q$, il simbolo di Legendre $\left(\frac{n}{q}\right)$ è definito da:*

$$\left(\frac{n}{q}\right) = \begin{cases} 1 \text{ se } n = \square \pmod q \\ -1 \text{ se } n \neq \square \pmod q \end{cases}$$

Dal criterio di Eulero segue che il simbolo di Legendre è moltiplicativo:

Proposizione 5.5. *Sia q un numero primo dispari e siano due interi n_1, n_2, con $n_1.n_2 \not\equiv 0 \pmod q$, allora:*

$$\left(\frac{n_1.n_2}{q}\right) = \left(\frac{n_1}{q}\right)\left(\frac{n_2}{q}\right).$$

Dimostrazione. Per il criterio di Eulero $\left(\frac{n_1}{q}\right).\left(\frac{n_2}{q}\right) \equiv n_1^{(q-1)/2}.n_2^{(q-1)/2} \equiv (n_1 n_2)^{(q-1)/2} \equiv \left(\frac{n_1 n_2}{q}\right)$. □

Questa proposizione riconduce il calcolo del simbolo di Legendre al caso in cui n è un numero primo (positivo o negativo). Per limitarsi al caso in cui n è un primo (positivo) dispari (legge di reciprocità quadratica), bisogna conoscere $\left(\frac{-1}{q}\right)$ e $\left(\frac{2}{q}\right)$ (i *complementi alla legge di reciprocità quadratica*). Abbiamo già visto il caso -1 (Lemma 4.3), ma rivediamolo alla luce del criterio di Eulero:

Proposizione 5.6. *Sia q un numero primo dispari, allora:*

$$\left(\frac{-1}{q}\right) = \begin{cases} 1 \text{ se } q \equiv 1 \pmod 4 \\ -1 \text{ se } q \equiv 3 \pmod 4 \end{cases}$$

Dimostrazione. Per il criterio di Eulero, abbiamo $\left(\frac{-1}{q}\right) \equiv (-1)^{(q-1)/2} \pmod q$. Se $q = 4m+1$, viene $(-1)^{2m} = 1$; invece se $q = 4m+3$, viene $(-1)^{2m+1} = -1$. □

Il caso $n = 2$ è più contorto e sarà dimostrato nella sezione successiva (Proposizione 5.10).

5.3 Dimostrazione della legge di reciprocità quadratica.

In questa sezione, dopo il lemma di Gauss e il secondo complemento, presentiamo due dimostrazioni della legge di reciprocità. La prima, un po' macchinosa,

segue le linee tracciate da Eulero. La seconda, molto più compatta ed elegante è dovuta essenzialmente a Eisenstein. La prima dimostrazione estende al caso generale il lemma di Gauss (comunque fondamentale per entrambe le dimostrazioni), mentre la seconda sembra piovere giù dal cielo!

Sia $p > 2$ un numero primo e poniamo $P := (p-1)/2$, allora $-P, ..., -1, 0, 1, ..., P$ è un sistema completo di residui mod p, cioè $\mathbb{Z}_p = \{0, \pm 1, ..., \pm P\}$.

Lemma 5.7. (Gauss)
Sia $p > 2$ un primo e sia a un intero tale che $(a, p) = 1$. Consideriamo i P numeri: $a, 2a, 3a, ..., Pa$. Per ogni k, $1 \leq k \leq P$, $ka \equiv \pm x \pmod{x}$, con $x \in \{1, 2, ..., P\}$. Sia ν il numero di interi negativi così ottenuti, allora:

$$a^{(p-1)/2} \equiv (-1)^{\nu} \pmod{p}.$$

Dimostrazione. Osserviamo che se $1 \leq k, t \leq P$, $k \neq t$, allora $ka \not\equiv ta \pmod{p}$ (visto che a è invertibile mod p si dovrebbe avere $k \equiv t \pmod{p}$). Se $ka \equiv -ta \pmod{p}$, allora $a(k+t) \equiv 0 \pmod{p}$, ma questo è impossibile perché a è invertibile e $2 \leq k + t \leq 2P = (p-1)$.

Quindi quando riduciamo mod p i P numeri $a, 2a, 3a, ..., Pa$, con dei rappresentanti x, $-P \leq x \leq P$, ogni elemento di $\{1, 2, 3, ..., P\}$ compare una e una sola volta con un segno ben determinato, cioè:

$$\{a, 2a, ..., Pa\} \equiv \{\varepsilon_1.1, \varepsilon_2.2, ..., \varepsilon_P.P\} \ \ \varepsilon_i \in \{-1, 1\}, \forall i$$

Pertanto:

$$a(2a)...(Pa) \equiv (\varepsilon_1.1)(\varepsilon_2 2)...(\varepsilon_P P) \pmod{p}$$

Semplificando per $P!$ viene:

$$a^{(p-1)/2} = a^P \equiv \varepsilon_1.\varepsilon_2...\varepsilon_P = (-1)^{\nu} \pmod{p}.$$

□

Per il criterio di Eulero (Teorema 5.2) otteniamo:

Corollario 5.8. *Con le notazioni precedenti:*

$$\left(\frac{a}{p}\right) = 1 \Leftrightarrow \nu \text{ è pari.}$$

Vediamo come questo risultato ci permette di calcolare $\left(\frac{2}{p}\right)$. Il seguente lemma ci sarà utile anche nel seguito:

Lemma 5.9. *Siano $\alpha < \beta$ due numeri reali e sia $s, t \in \mathbb{N}$. Sia $I =]\alpha, \beta[$, $J =]\alpha + 2s, \beta + 2s + 2t[$. Sia $i(I)$ il numero di interi contenuti nell'intervallo I. Allora $i(J) = i(I) + 2t$, in particolare $i(I) \equiv i(J) \pmod{2}$.*

Dimostrazione. Esercizio 62. □

Torniamo adesso al problema di calcolare $\left(\frac{2}{p}\right)$ usando il Lemma 5.7. Consideriamo quindi i numeri: $2, 4, 6, ..., 2P = p-1$. Quando riduciamo mod p con dei rappresentanti tra $-P$ e P, quelli che avranno dei rappresentanti negativi sono i multipli di 2 tali che $P < 2n \leq 2P = p-1$. Siccome n è intero questa disuguaglianza è equivalente a: $p/2 < 2n < p$, cioè: $p/4 < n < p/2$. Dobbiamo quindi trovare la *parità* del numero di interi nell'intervallo $J =]p/4, p/2[$.

Poniamo $p = 8k + r$ con $r \in \{1, 3, 5, 7\}$. Abbiamo $J =]2k + r/4, 4k + r/2[$. Per il Lemma 5.9 la parità di $i(J)$ è uguale alla parità di $i(I)$ dove $I =]r/4, r/2[$. Siccome il numero di interi in I è 0 se $r = 1$, 1 se $r = 3, 5$, 2 se $r = 7$, otteniamo: $i(J)$ è pari $\Leftrightarrow p \equiv 1, 7 \pmod 8$. Per il Lemma di Gauss segue che:

Proposizione 5.10. ("Secondo complemento")
Abbiamo:

$$\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \pmod 8$$

cioè 2 *è un quadrato mod* p *se e solo se* $p \equiv 1, 7 \pmod 8$.

Esattamente nello stesso modo si dimostra che: $\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \pmod{12}$ $(p > 3)$. Per questo si procede così: si considera $3, 6, 9, ..., 3P = 3(p-1)/2$. Nella riduzione mod p con rappresentanti tra $-P$ e P avremo dei termini negativi per i multipli di 3 tali che: $P < 3n < p$. Infatti i $(p-1)/2$ successivi $p+1, ..., p+P = (3p-1)/2$ hanno tutti rappresentanti positivi e $3(p-1)/2 < (3p-1)/2$.

Quindi dobbiamo trovare la parità di $i(J)$ dove $J =]p/6, p/3[$. Dividiamo p per $12 = 4 \times 3$: $p = 12k + r$, $0 < r < 12$, quindi $J =]2k + r/6, 4k + r/3[$. Per il Lemma 5.9 la parità di $i(J)$ è la stessa di quella di $i(I)$ dove $I =]r/6, r/3[$. I resti possibili sono $r = 1, 5, 7, 11$. Nel secondo e terzo caso caso $i(I) = 1$, nel primo $i(I) = 0$, nell'ultimo $i(I) = 2$ e il risultato segue.

Se analizziamo queste dimostrazioni (casi $a = 2, 3$ del calcolo di $\left(\frac{a}{p}\right)$) vediamo che abbiamo seguito lo schema seguente:
-determinare la parità del numero di "termini negativi" è equivalente a conoscere la parità del numero di multipli di a che si trovano nell'intervallo $]p/2, p[$, cioè $p/2 < an < p$, quindi $p/2a < n < p/a$. Pertanto dobbiamo determinare la parità di $i(J)$ dove $J =]p/2a, p/a[$.
-si divide p per $4a$: $p = 4ak + r, 0 < r < 4a$. Allora $J =]2k + r/2a, 4k + r/a[$. Per il Lemma 5.9 basta determinare la parità di $i(I)$ dove $I =]r/2a, r/a[$. *In particolare se* p, q *sono due primi che hanno lo stesso resto nella divisione per*

$4a$, allora: $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$. Eulero ha anche osservato che la stessa conclusione è valida se i resti sono r e $4a - r$.

In effetti sulla base di numerosi calcoli Eulero era arrivato a questa conclusione: $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) \Leftrightarrow p$ e q hanno lo stesso resto nella divisione per $4a$ o hanno resti "opposti" (r e $4a - r$); negli altri casi: $\left(\frac{a}{p}\right) . \left(\frac{a}{q}\right) = -1$.

Questo enunciato è, come vedremo, equivalente alla legge di reciprocità quadratica. (Quindi in realtà Eulero è stato il primo ad enunciarla). La dimostrazione del caso generale secondo le linee precedenti si complica dal fatto che i "termini negativi" non sono necessariamente in un unico intervallo, ma rimane comunque elementare. Vediamo come funziona.

Si tratta quindi di determinare la parità del numero di multipli di a, $\leq aP$, che ridotti mod p tra $-P$ e P sono negativi. Se prendiamo un multiplo di p, cp, i successivi $(p-1)/2 = P$ numeri, $cp+1, cp+2, ..., cp+P$ sono congrui a $1, 2, ..., P$ mod. p. I successivi P numeri: $cp+P+1, ..., cp+2P$ sono congrui a $-P, -P+1, ..., -1$ ($P+1 = p-P$). Il numero successivo è $cp+2P+1 = (c+1)p$ e si ricomincia. Siamo quindi interessati ai multipli di a contenuti in intervalli del tipo $\tilde{J} = [cp+(p+1)/2, (c+1)p-1] = [(2c+1)p/2+1/2, (c+1)p-1]$. Gli interi contenuti in $\tilde{J}$ sono gli stessi di quelli contenuti in $J =](2c+1)p/2, (c+1)p[$. Siccome siamo interessati ai multipli $\leq aP$, $cp + 2P \leq aP$, cioè $c + 1 \leq a/2$ e l'ultimo intervallo da considerare sarà per $c + 1 = a/2$ se a è pari ($c + 1 = (a-1)/2$ se a è dispari).

In conclusione dobbiamo determinare la parità, ν, del numero di multipli di a contenuti negli intervalli:

$$]p/2, p[,]3p/2, 2p[,]5p/2, 3p[, ...,](2b-1)p/2, bp[, ...,](2B-1)p/2, Bp[$$

dove $B = a/2$ se a è pari e $B = (a-1)/2$ se a è dispari.

Se $\nu \equiv 0 \pmod 2$, allora $\left(\frac{a}{p}\right) = 1$, altrimenti $\left(\frac{a}{p}\right) = -1$.

Dividiamo p per $4a$: $p = 4ak + r, 0 < r < 4a$.
Abbiamo:

$$an \in](2b-1)p/2, bp[\Leftrightarrow \ n \in]4kb - 2k + \frac{r}{2a}(2b-1), 4kb + \frac{r}{a}b[:= J_b$$

Stiamo quindi cercando la parità del numero di interi contenuti negli intervalli J_b, $1 \leq b \leq B$. Cioè $\nu \equiv i(J_1) + ... + i(J_B) \pmod 2$.

Sia $I_b =]\frac{r}{2a}(2b-1), \frac{r}{a}b[$. Per il Lemma 5.9, $i(I_b) = i(J_b)$. Quindi $\nu \equiv i(I_1) + ... + i(I_B) \pmod 2$. Per b e a fissati $i(I_b)$ dipende solo da r. Siccome B dipende solo da a, concludiamo che, fissato a, $\nu \pmod 2$ dipende solo da r. Questo dimostra:

Lemma 5.11. *Se p, q sono due primi dispari, con $(a,p) = (a,q) = 1$, che hanno lo stesso resto nella divisione per $4a$, allora:*

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

Vediamo adesso che se p ha resto r e q ha resto $4a-r$, allora $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$. Per quanto visto prima questo torna a mostrare che la parità del numero di interi negli intervalli:

$$I_b =]\frac{r}{2a}(2b-1),\ \frac{r}{a}b[,\ 1 \le b \le B$$

è la stessa di quella del numero di interi negli intervalli:

$$T_b =]\frac{(4a-r)}{2a}(2b-1),\ \frac{(4a-r)}{a}b[,\ 1 \le b \le B$$

Abbiamo $T_b =]4b-2-\frac{r}{2a}(2b-1),\ 4b-\frac{r}{a}b[:=]X, Y[$. Sia $\tilde{T}_b =]4b-Y, 4b-X[$. Allora $\tilde{T}_b =]\frac{r}{a}b,\ 2+\frac{r}{2a}(2b-1)[$. Chiaramente $i(T_b) = i(\tilde{T}_b)$.

Adesso:

$$I_b \cup \tilde{T}_b =]\frac{r}{2a}(2b-1),\ 2+\frac{r}{2a}(2b-1)[\setminus \{\frac{r}{a}b\}$$

Osserviamo che sotto le nostre ipotesi rb/a e $r(2b-1)/2a$ non sono interi. Infatti se $rb/a = m$, allora $bp = 4akb + br = a(4kb+m)$ e siccome $(a,p) = 1$ segue che $a \mid b$, assurdo perché $b < a$. Nello stesso modo si vede che $r(2b-1)/2a$ non è intero. Abbiamo quindi:

$$i(I_b) + i(\tilde{T}_b) = i(]\frac{r}{2a}(2b-1),\ 2+\frac{r}{2a}(2b-1)[)$$

Se α non è intero si ha chiaramente $i(]\alpha,\ 2+\alpha[) = 2$ (mentre $i(]n,\ n+2[) = 1$). In conclusione: $i(I_b) + i(T_b) = i(I_b) + i(\tilde{T}_b) = 2$, pertanto:

$$\sum_{b=1}^{B} i(I_b) \equiv \sum_{b=1}^{B} i(T_b) \pmod 2.$$

Questo dimostra:

Lemma 5.12. *Siano p, q due numeri primi dispari e sia a un intero tale che $(a,p) = (a,q) = 1$. Se p ha resto r nella divisione per $4a$ e se q ha resto $4a-r$ nella divisione per $4a$, allora:*

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

Il Lemma 5.11 e il Lemma 5.12 dimostrano l'affermazione fatta da Eulero e sono equivalenti alla legge di reciprocità quadratica:

Teorema 5.13. (Legge di reciprocità quadratica)
Siano p, q due primi > 2, allora:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)}{2} \cdot \frac{(q-1)}{2}}.$$

Dimostrazione. Osserviamo che se $p = 4k + 1$, allora $(p-1)/2$ è pari, mentre se $p = 4j + 3$, $(p-1)/2$ è dispari. Quindi $(-1)^{\frac{(p-1)}{2} \cdot \frac{(q-1)}{2}} = -1 \Leftrightarrow p \equiv q \equiv 3 \pmod 4$.

i) Supponiamo $p \equiv q \pmod 4$. Possiamo assumere $p > q$. Sia $p - q = 4a$. Quindi $p = q + 4a$ e p è un quadrato mod q se solo se $4a$ lo è cioè $(4 = 2^2)$ se e solo se a è un quadrato mod q:

$$\left(\frac{p}{q}\right) = \left(\frac{4a+q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right)$$

Nello stesso modo:

$$\left(\frac{q}{p}\right) = \left(\frac{p-4a}{p}\right) = \left(\frac{-4a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right)$$

Siccome $p \equiv q \pmod{4a}$, $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$, per il Lemma 5.11. Quindi $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right)$. Siccome $\left(\frac{-1}{p}\right) = 1 \Leftrightarrow p \equiv 1 \pmod 4$, abbiamo il risultato cercato ($p \equiv q \pmod 4$ per ipotesi).

ii) Supponiamo $p \not\equiv q \pmod 4$. In questo caso $p \equiv -q \pmod 4$. Poniamo $p + q = 4a$. Abbiamo:

$$\left(\frac{p}{q}\right) = \left(\frac{4a-q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right)$$

Nello stesso modo:

$$\left(\frac{q}{p}\right) = \left(\frac{4a-p}{p}\right) = \left(\frac{4a}{p}\right) = \left(\frac{a}{p}\right)$$

Siccome $p \equiv -q \pmod{4a}$, abbiamo $\left(\frac{a}{q}\right) = \left(\frac{a}{p}\right)$ (Lemma 5.12. Quindi $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1 = (-1)^{\frac{(p-1)(q-1)}{4}}$. □

5.3.1 Seconda dimostrazione.

La dimostrazione che segue, molto sintetica e elegante, è essenzialmente dovuta a Eisenstein (allievo di Gauss).

Lemma 5.14. *Sia $p > 2$ un primo e $n > 0$ un intero dispari con $(n, p) = 1$. Sia:*

$$M = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{2n}{p} \rfloor + \cdots + \lfloor \frac{Pn}{p} \rfloor$$

dove $P = (p-1)/2$. Allora $\left(\frac{n}{p}\right) = (-1)^M$.

Dimostrazione. Per $1 \leq i \leq P$ dividiamo in per p: $in = p\lfloor \frac{in}{p} \rfloor + r_i$, $0 < r_i < p$. Sommando queste P equazioni viene:

$$n(1 + 2 + \cdots + P) = pM + r_1 + \cdots + r_P$$

Chiaramente $in \equiv r_i \pmod{p}$. Quando riduciamo modulo p $r_1, ..., r_P$ otteniamo P elementi distinti e dal Lemma di Gauss (Lemma 5.7) sappiamo che ν tra loro sono $> P$. Se $r_j > P$ lo rimpiazziamo con $r_j - p$, il cui valore assoluto è $p - r_j$. Abbiamo quindi $\{1, 2, ..., P\} = \{r_i, -r_j + p\}$. Siccome $x \equiv -x \pmod 2$, viene: $1 + 2 + \cdots + P \equiv r_1 + r_2 + \cdots r_P + p\nu \pmod 2$. Per differenza tra questa relazione e la precedente otteniamo:

$$(1 + 2 + \cdots + P)(n - 1) \equiv p(M - \nu) \pmod 2$$

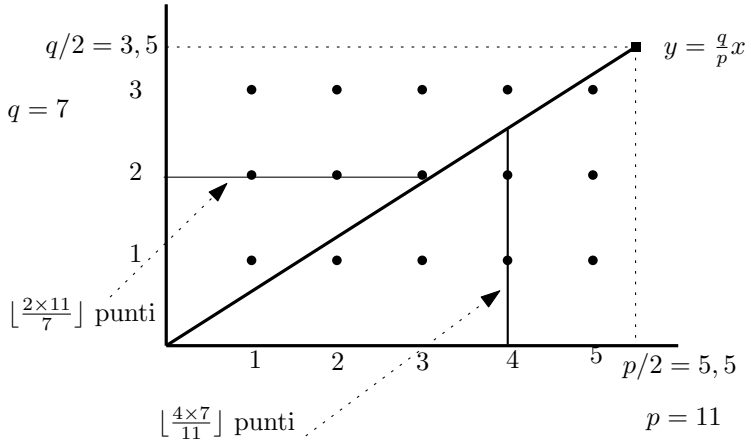
Siccome n, p sono dispari, $M \equiv \nu \pmod 2$ e si conclude con il Lemma 5.7. □

Passiamo ora alla dimostrazione della legge di reciprocità quadratica:

Dimostrazione (della legge di reciprocità quadratica).
Nel piano (x, y) consideriamo i punti a coordinate intere (x, y), $1 \leq x \leq (p-1)/2$, $1 \leq y \leq (q-1)/2$. Notiamo I l'insieme dei punti così ottenuti. Ovviamente $\#(I) = (p-1)/2.(q-1)/2$.

Sia R il rettangolo di vertici $(0, 0), (0, q/2), (p/2, 0), (p/2, q/2)$. La diagonale di R ha equazione $y = (q/p)x$ e non contiene nessun punto di I. Infatti se $py = qx$ con x, y interi, allora $p \mid x$ e $q \mid y$.

Il disegno qui sotto rappresenta la situazione nel caso $p = 11, q = 7$.



Per $1 \leq k \leq (p-1)/2$ la retta $x = k$ contiene i punti $(k,1),(k,2),...,(k,\lfloor \frac{kq}{p} \rfloor)$, cioè $\lfloor \frac{kq}{p} \rfloor$ punti di I. Quindi ci sono

$$M = \sum_{k=1}^{(p-1)/2} \lfloor \frac{kq}{p} \rfloor$$

punti di I sotto la diagonale. Per il Lemma 5.14 con $n = q$: $\left(\frac{q}{p}\right) = (-1)^M$.

Con lo stesso ragionamento ci sono

$$N = \sum_{j=1}^{(q-1)/2} \lfloor \frac{jp}{q} \rfloor$$

punti di I sopra la diagonale (considerare le rette $y = j, 1 \leq j \leq (q-1)/2$). Per il Lemma 5.14 con $n = p$: $\left(\frac{p}{q}\right) = (-1)^N$. Siccome $N + M = \frac{(p-1)}{2}\frac{(q-1)}{2} = \#(I)$, abbiamo:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{N+M} = (-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}}.$$

□

Esercizi.

Esercizio 61 *Mostrare che se* $m = t^2 + ak^2$, $n = u^2 + av^2$ *allora anche* mn *si scrive nella forma* $x^2 + ay^2$ *(tutti i numeri considerati sono interi positivi o negativi).*

Esercizio 62 *Siano* $x, y > 0$ *due numeri reali e sia* $I =]x,\ y[$. *Determinare in funzione di* x, y, $i(I)$, *il numero di interi contenuti in* I.
Dimostrare il Lemma 5.9.

Esercizio 63 *(i) Sia* p *un primo,* $p \equiv 3 \pmod 4$. *Si assume* $q = 2p+1$ *primo. Mostrare che* 2 *non è radice primitiva modulo* q.
(ii) Sia p *un primo tale che* $q = 4p + 1$ *sia anch'esso primo. Osservare che* $ord_q(2) \mid 4p$ *e concludere che* 2 *è radice primitiva modulo* q.

Esercizio 64 *(i) Dimostrare che esistono infiniti primi della forma* $p = 4k+1$ *(considerare* $(n!)^2 + 1$*).*
(ii) Dimostrare che esistono infiniti primi della forma $8r - 1$ *(considerare* $Q = (4p_1 \cdots p_k)^2 - 2$ *dove i* $p_i \equiv -1 \pmod 8$*).*

Esercizio 65 *(i) Il secondo complemento si può enunciare:*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

(ii) Sia p *un primo congruo a* $3 \pmod 4$ *tale che* $q = 2p + 1$ *sia anch'esso primo. Mostrare che* $q \mid 2^p - 1$. *Quindi il numero di Mersenne* $M_p = 2^p - 1$ *non è primo.*
(iii) Verificare (con un computer) che se $p = 1\,122\,659$, *allora* M_p *e* M_{2p+1} *non sono primi.*

Esercizio 66 *Sia* $F_n = 2^{2^n} + 1$ *l'ennesimo numero di Fermat.*
(i) Mostrare che ogni F_n *è primo o pseudo primo (relativamente alla base 2) (cf Esercizio 35).*
Osservazione: *Forse è per questo motivo che Fermat credeva che* F_n *fosse sempre primo?*
(ii) Mostrare che se p *è un divisore primo di* F_n, *allora* $p = 1+k2^{n+1}$ *(mostrare che* $ord_p(2) = 2^{n+1}$*).*
(iii) Con le notazioni del punto (ii) mostrare che k *è pari (considerare* $\left(\frac{2}{p}\right)$*).*
Quindi ogni divisore primo di F_n *è della forma* $1 + t.2^{n+2}$.
(iv) Per esempio se $n = 5$ *ogni divisore primo di* F_5 *è della forma* $p = 1 + 128.t$. *Per* $t = 5$ *viene* $p = 641$. *Nel 1732 Eulero ha mostrato che:* $F_5 =$

$641 \times 6\,700\,417$ *(cf Esercizio 37). Sia* $N := 6\,700\,417$. *Ogni divisore primo di* N *è della forma* $p = 1 + 128t$ *(perché?). Verificare che* $(1 + 128.21)^2 > N$. *Quindi un divisore primo di* N *è della forma* $1 + 128t$ *con* $1 \leq t \leq 20$. *Verificare che gli unici primi in questa lista sono:* $257(t = 2)$, $641(t = 5)$, $769(t = 6)$, $1153(t = 9)$ *e* $1409(t = 11)$. *Concludere che* N *è primo. Quindi la fattorizzazione di* F_5 *è:* $F_5 = 641 \times N$ *(questo risultato è dovuto a Eulero).*

Parte II

Teoria algebrica.

6

Campi di numeri.

In questo capitolo ricordiamo alcuni risultati di algebra sulle estensioni di campi, definiamo i campi di numeri (estensioni finite di $\mathbb{Q}$) e i relativi anelli degli interi. Il fatto fondamentale è che un campo di numeri è completamente determinato dal suo anello degli interi.

6.1 Estensioni, numeri algebrici.

Se L è un campo e se $K \subset L$ è un sotto campo si dice che L è un'estensione di K (in simboli: L/K).

Definizione 6.1. *Sia L/K un'estensione di K. Un elemento $\alpha \in L$ è algebrico su K se α è radice di un polinomio a coefficienti in K.*

L'estensione L/K è algebrica se ogni $\alpha \in L$ è algebrico su K.

Sia L/K un'estensione e $\alpha \in L$. Abbiamo un morfismo di anelli $\varphi : K[X] \to K[\alpha] \subset L : P(X) \to P(\alpha)$. Per definizione α è algebrico su K se e solo se φ non è iniettivo. In questo caso $Ker(\varphi)$ è un ideale $I \subset K[X]$. Siccome $K[X]$ è un PID (Sezione 2.3), $I = (M)$. Il polinomio M è univocamente determinato modulo un elemento non nullo di K (un'unità di $K[X]$). In particolare esiste uno ed un unico polinomio monico, $M_\alpha(X)$ tale che $I = (M_\alpha)$. Il polinomio M_α è irriducibile su K. Infatti sia $M_\alpha(X) = P(X)Q(X)$ con $P(X), Q(X) \in K[X]$, allora $M_\alpha(\alpha) = 0 = P(\alpha)Q(\alpha)$ implica $P(\alpha) = 0$ o $Q(\alpha) = 0$. Se $P(\alpha) = 0$, allora $P \in I = (M_\alpha)$, cioè $M_\alpha \mid P$ e questo implica che Q è una costante (cioè un'unità di $K[X]$), quindi $M_\alpha(X)$ è irriducibile su K.

Definizione 6.2. *Con le notazioni precedenti il polinomio $M_\alpha(X) \in K[X]$ è il* polinomio minimo *dell'elemento algebrico $\alpha \in L$.*

Abbiamo:

Lemma 6.3. *Sia L/K un'estensione di campi e sia $\alpha \in L$. Sono equivalenti:*

1. *α è algebrico su K*
2. *$K[\alpha] = K(\alpha)$*
3. *$\dim_K(K[\alpha]) < \infty$ (infatti $\dim_K(K[\alpha]) = \deg(M_\alpha)$).*

Dimostrazione. (1) $\Rightarrow$ (2): Siccome φ è ovviamente suriettiva su $K[\alpha]$, abbiamo $K[X]/(M_\alpha) \simeq K[\alpha]$. Siccome M_α è irriducibile, $K[X]/(M_\alpha) = K[\alpha]$ è un campo (Lemma 2.21). Quindi $K[\alpha]$ è un campo che contiene K e α, quindi $K(\alpha) \subset K[\alpha]$, l'altra inclusione è ovvia quindi $K(\alpha) = K[\alpha]$.

(2) $\Rightarrow$ (1): $\alpha^{-1} \in K(\alpha) = K[\alpha]$, quindi $\alpha^{-1} = a_n\alpha^n + ... + a_1\alpha + a_0$, moltiplicando per α si vede che il polinomio $P(X) = a_nX^{n+1} + ... + a_0X - 1 \in K[X]$ verifica $P(\alpha) = 0$.

(1) $\Rightarrow$ (3): Abbiamo $M_\alpha(\alpha) = 0 = \alpha^n + ... + a_1\alpha + a_0$ $(a_i \in K, \forall i)$. Allora $B = (1, \alpha, ..., \alpha^{n-1})$ è una base del K-spazio vettoriale $K[\alpha]$. Infatti i vettori di B sono linearmente indipendenti: se $\sum_{i=0}^{n-1} \lambda_i\alpha^i = 0$, allora $P(X) = \sum_{i=0}^{n-1} \lambda_iX^i \in K[X]$ verifica $P(\alpha) = 0$, ma questo è impossibile perché $\deg(P) < n = \deg(M_\alpha)$. Siccome $\alpha^n = -a_0 - ... - a_{n-1}\alpha^{n-1}$, per induzione si ha $< 1, \alpha, ..., \alpha^{n-1} >= K[\alpha]$. In particolare $\dim_K(K[\alpha]) = \deg(M_\alpha)$.

(3) $\Rightarrow$ (1): Se $n = \dim_K(K[\alpha])$ allora $1, \alpha, ..., \alpha^n$ sono linearmente dipendenti e esistono $\lambda_i \in K$ non tutti nulli tali che: $\sum_{i=0}^{n} \lambda_i\alpha^i = 0$ e $P(X) = \sum_{i=0}^{n} \lambda_iX^i \in K[X]$ verifica $P(\alpha) = 0$. □

Definizione 6.4. *L/K è* finita *se $[L : K] := \dim_K(L) < \infty$.*

Abbiamo:

Lemma 6.5. *Ogni estensione finita è algebrica.*

Sia $K \subset L \subset F$ una torre di estensioni, se due delle tre quantità $[L : K], [F : L], [F : K]$ sono finite allora anche la terza lo è e:

$$[F : K] = [F : L].[L : K]$$

Finalmente:

Proposizione 6.6. *Sia L/K un'estensione e sia*
$F := \{\alpha \in L \mid \alpha$ è algebrico su $K\}$. Allora:

1. *F è un sottocampo di L e si ha $K \subset F \subset L$*
2. *Se $\alpha \in L$ è algebrico su F, allora $\alpha \in F$*
3. *Se L è algebricamente chiuso anche F lo è.*

Dimostrazione. (1) Chiaramente $K \subset F$ perché se $\alpha \in K$, $X - \alpha \in K[X]$. Sia $\alpha \in L$, $\alpha \neq 0$ con

$$a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0,\ a_i \in K, \forall i$$

Dividendo per α^n (cioè moltiplicando per $(\alpha^{-1})^n$):

$$a_n + \cdots + a_1(\frac{1}{\alpha})^{n-1} + a_0(\frac{1}{\alpha})^n = 0$$

e quindi anche $\alpha^{-1} \in F$. Rimane da vedere che se $\alpha, \beta \in F$ allora anche $\alpha + \beta$ e $\alpha\beta$ sono in F. Siccome β è algebrico su $K(\alpha)$ (perché radice di un polinomio a coefficienti in K) $[K(\alpha, \beta) : K(\alpha)] < \infty$ (Lemma 6.3), osservare che $K(\alpha, \beta) = K(\alpha)(\beta)$). Nello stesso modo, siccome α è algebrico su K: $[K(\alpha) : K] < \infty$. Segue dal Lemma 6.5 che: $[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)][K(\alpha) : K] < \infty$. Pertanto $K(\alpha, \beta)/K$ è algebrica ((1) del Lemma 6.5). Quindi $\alpha + \beta$, $\alpha\beta \in K(\alpha, \beta)$ sono algebrici su K.

(2) Sia α radice di $P(X) = a_nX^n + ... + a_1X + a_0$ con $a_i \in F$. L'estensione $K(a_n, ..., a_0)/K$ è algebrica finita. Infatti ogni a_i è algebrico su K (perché $a_i \in F$), inoltre $K(a_1, a_0) = K(a_0)(a_1)$, quindi $K(a_0, a_1)/K$ è algebrica finita e procedendo per induzione si ottiene il risultato.

Adesso $P(X) \in K'[X]$ ($K' := K(a_n, ..., a_0)$). Quindi α è algebrico su K', cioè $[K'(\alpha) : K'] < \infty$ (Lemma 6.3). Segue che $[K'(\alpha) : K] = [K'(\alpha) : K'][K' : K] < \infty$, quindi α è algebrico su K, cioè $\alpha \in F$.

(3) Sia $P(X) \in F[X]$ con $\deg(P) \geq 1$. Se L è algebricamente chiuso, esiste $\alpha \in L$ tale che $P(\alpha) = 0$. Quindi α è algebrico su F. Per il passo (2), $\alpha \in F$. Quindi ogni polinomio non costante a coefficienti in F ha una radice in F: F è algebricamente chiuso. □

Esempio 6.7 (Esempio base).
Consideriamo l'estensione $\mathbb{Q} \subset \mathbb{C}$. Un numero complesso algebrico su $\mathbb{Q}$ si chiama (più semplicemente) un *numero algebrico* (chi l'avrebbe mai detto ;-). Per esempio i è un numero algebrico. Per la Prop. 6.6 l'insieme dei numeri algebrici è un campo e siccome $\mathbb{C}$ è algebricamente chiuso, questo campo è algebricamente chiuso (e contiene $\mathbb{Q}$): questo campo è $\overline{\mathbb{Q}}$, la chiusura algebrica di $\mathbb{Q}$. Se $z \in \mathbb{C} \setminus \overline{\mathbb{Q}}$ allora z è un *numero trascendente*. Siccome e, π sono trascendenti, $\overline{\mathbb{Q}} \neq \mathbb{C}$ (d'altra parte $\overline{\mathbb{Q}}$ è numerabile mentre $\mathbb{C}$ non lo è).

L'estensione $\overline{\mathbb{Q}}/\mathbb{Q}$ è algebrica (per definizione), infinita (per ogni $n \geq 1$ esiste un polinomio $p(x) \in \mathbb{Z}[x]$, irriducibile su $\mathbb{Q}$ di grado n: usare il criterio di Eisenstein). quindi non tutte le estensioni algebriche sono finite!

Le estensioni $\mathbb{C}/\mathbb{Q}$, $\mathbb{R}/\mathbb{Q}$ non sono algebriche (esistono numeri trascendenti), l'estensione $\mathbb{C}/\mathbb{R}$ è algebrica finita ($\mathbb{C} = \mathbb{R}(i)$, $[\mathbb{C} : \mathbb{R}] = 2$).

Definizione 6.8. *Un* campo di numeri (number field) *è un'estensione finita di* $\mathbb{Q}$.

Se K *è un campo di numeri, il* grado *di* K *è* $[K : \mathbb{Q}]$. *Un campo* quadratico *è un campo di numeri di grado due.*

6.2 Interi algebrici.

Come si fa a distinguere un elemento di $\mathbb{Z}$ in $\mathbb{Q}$?

Lemma 6.9. *Sia* $z \in \mathbb{Q}$ *allora* $z \in \mathbb{Z} \Leftrightarrow z$ *è radice di un polinomio monico a coefficienti in* $\mathbb{Z}$.

Dimostrazione. Esercizio. □

Osservare che ogni $z \in \mathbb{Q}$ è radice di un polinomio a coefficienti in $\mathbb{Z}$.

Definizione 6.10. *Un elemento* $z \in \mathbb{C}$ *è un* intero algebrico *se* z *è radice di un polinomio monico a coefficienti in* $\mathbb{Z}$.

Si nota $\mathcal{O}$ *l'insieme degli interi algebrici. Chiaramente* $\mathcal{O} \subset \overline{\mathbb{Q}}$.

Più generalmente:

Definizione 6.11. *Sia* R *un anello e* $A \subset R$ *un sotto anello. Un elemento* $b \in R$ *è* intero *su* A *se esiste un polinomio monico* $P(x) \in A[x]$ *tale che* $P(b) = 0$.

Non è chiaro a priori che la somma e il prodotto di due elementi interi sia ancora un elemento intero.

Lemma 6.12. *Siano* $A \subset R$ *due anelli. Siano* $u_1, ..., u_n \in R$. *Sono equivalenti:*

1. $u_1, ..., u_n$ *sono interi su* A
2. *L'anello* $A[u_1, ..., u_n]$ *dei polinomi in* $u_1, ..., u_n$ *a coefficienti in* A *è finitamente generato come* A*-modulo*
3. *Esiste un anello* B*, finitamente generato come* A*-modulo tale che* $A[u_1, ..., u_n] \subset B \subset R$.

Dimostrazione. (1) $\Rightarrow$ (2): Se $n = 1$ ($u = u_1$). Per ipotesi $u^n + a_{n-1}u^{n-1} + ... + a_0 = 0$, $a_i \in A$. Quindi $u^n = -(a_{n-1}u^{n-1} + ... + a_0)$ e vediamo che u^k, $k \geq n$ si esprime come combinazione lineare di $1, u, ..., u^{n-1}$ a coefficienti in A.

Adesso procediamo per induzione su n. Siccome u_n è intero su $C = A[u_1, ..., u_{n-1}]$, $C[u_n] = A[u_1, ..., u_n]$ è un C-modulo finitamente generato.

Per ipotesi di induzione C è un A-modulo finitamente generato. Pertanto $C[u_n] = A[u_1, ..., u_n]$ è un A-modulo finitamente generato.

(2) $\Rightarrow$ (3): chiaro.

(3) $\Rightarrow$ (1): Basta mostrare che ogni elemento $u \in B$ è intero su A. Siano $b_1, ..., b_k$ dei generatori di B, siccome u e b_i sono in B e B è un anello, anche $ub_i \in B$, quindi: per ogni i: $ub_i = \sum_j a_{ij}b_j$, cioè $0 = \sum_j (\delta_{ij}u - a_{ij})b_j$, $1 \leq i \leq k$. In forma matriciale $A. \begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix} = 0$, dove $A = (\delta_{ij}u - a_{ij})$. Dalla relazione $A^c A = \det A.I_n$ (A^c la trasposta della matrice dei cofattori), viene $\det A.b_i = 0, \forall i$, questo implica $\det A = 0$ (perché 1 è combinazione dei b_i). Adesso $\det A$ è un polinomio monico in u a coefficienti in A, quindi u è intero su A. □

Corollario 6.13. *Sia $A \subset R$ un'estensione di anelli. L'insieme, $\overline{A}$, degli elementi di R interi su A è un sotto anello di R.*

Dimostrazione. Siano $x, y \in R$ interi su A. Abbiamo $A[x + y] \subset B = A[x, y]$, $A[xy] \subset B$ e si conclude con il Lemma 6.12. □

La nozione di elemento intero è molto importante in teoria dei numeri (e anche in geometria algebrica), questo giustifica la seguente

Definizione 6.14. *Sia $A \subset R$ un'estensione di anelli. Con le notazioni del Corollario 6.13, l'anello $\overline{A}$ si chiama la chiusura integrale di A in R. Se $\overline{A} = A$ si dice che A è integralmente chiuso in R.*
Sia A un anello integro. La chiusura integrale, $\overline{A}$, di A nel suo campo dei quozienti si chiama la normalizzazione *di A. L'anello integro A è* integralmente chiuso *se A è integralmente chiuso nel suo campo dei quozienti (cioè A è uguale alla sua normalizzazione).*

Per esempio $\mathbb{Z}$ è integralmente chiuso.

Tornando agli interi algebrici abbiamo:

Proposizione 6.15. *L'insieme $\mathcal{O}$ è un anello integro il cui campo dei quozienti è $\overline{\mathbb{Q}}$.*

Dimostrazione. Rimane da vedere che $\overline{\mathbb{Q}}$ è il campo dei quozienti di $\mathcal{O}$. Sia $\mathcal{K}$ il campo dei quozienti $\mathcal{O}$. Chiaramente $\mathcal{K} \subset \overline{\mathbb{Q}}$ (perché $\mathcal{K}$ è contenuto in ogni campo contenente $\mathcal{O}$).

Viceversa vediamo che $\overline{\mathbb{Q}} \subset \mathcal{K}$. Sia $z \in \overline{\mathbb{Q}}$ vogliamo vedere $z = u/v, u, v \in \mathcal{O}$. Mostriamo che esiste $k \in \mathbb{Z}$ tale che $kz \in \mathcal{O}$. Per definizione z è radice di un polinomio a coefficienti in $\mathbb{Q}$, quindi (dopo avere ridotto allo stesso denominatore) di un polinomio a coefficienti in $\mathbb{Z}$: $a_n z^n + a_{n-1} z^{n-1} ... + a_1 z + a_0 = 0$. Moltiplicando per a_n^{n-1} si conclude ($a_{n-1} z \in \mathcal{O}$). □

La situazione $\mathcal{O} \subset \overline{\mathbb{Q}}$ generalizza quella ben nota $\mathbb{Z} \subset \mathbb{Q}$.

Definizione 6.16. *Sia K un campo di numeri. Si pone $\mathcal{O}_K := K \cap \mathcal{O}$, quindi $\mathcal{O}_K$ è l'insieme degli elementi di K che sono interi su $\mathbb{Z}$; $\mathcal{O}_K$ è un anello il cui campo dei quozienti è K.*

L'anello $\mathcal{O}_K$ è l'anello degli interi di K.

Il fatto che $\mathcal{O}_K$ sia un anello è chiaro. Se $\mathcal{K}$ è il campo dei quozienti di $\mathcal{O}_K$, allora chiaramente $\mathcal{K} \subset K$. Se $z \in K$, allora $z \in \overline{\mathbb{Q}}$ e dalla dimostrazione precedente esiste $n \in \mathbb{Z}$ tale che $nz \in \mathcal{O}$, quindi $nz \in \mathcal{O} \cap K = \mathcal{O}_K$.

In particolare l'anello degli interi $\mathcal{O}_K$ determina completamente il campo K: lo studio di K si riconduce a quello di $\mathcal{O}_K$.

6.3 $\mathbb{Q}$-immersioni, estensioni di Galois.

Ricordiamo il Teorema dell'elemento primitivo:

Teorema 6.17. (Teorema dell'elemento primitivo)
Sia L/K un'estensione finita con $ch(K) = 0$. Allora esiste $\alpha \in L$ tale che $L = K(\alpha)$.

In queste condizioni $[L : K] = \deg(M_\alpha(X))$ dove $M_\alpha(X)$ è il polinomio minimo di α su K.

Sia K un campo di numeri, per il Teorema dell'elemento primitivo esiste $z \in K$ tale che $K = \mathbb{Q}(z)$. Il polinomio minimo, $M(x) \in \mathbb{Q}[x]$, di z su $\mathbb{Q}$ ha grado $n = [K : \mathbb{Q}]$. Siccome $M(x)$ è irriducibile, le sue radici (in $\overline{\mathbb{Q}}$) sono distinte (perché?).

Definizione 6.18. *Una $\mathbb{Q}$ immersione di K è un morfismo di campi $\sigma : K \to \overline{\mathbb{Q}}$ tale che $\sigma|\mathbb{Q} = Id$. Si nota $Mor_{\mathbb{Q}}(K)$ l'insieme delle $\mathbb{Q}$-immersioni di K.*

Siccome $K = \mathbb{Q}(z)$, σ è completamente determinata da $\sigma(z)$. Siccome $M(z) = 0$ e $\sigma|\mathbb{Q} = Id$, $M(\sigma(z)) = 0$, quindi $\sigma(z)$ è una radice di M (diversa da z se $\sigma \neq Id$), anzi vediamo che $Mor_{\mathbb{Q}}(K)$ è in biiezione con le radici di M, in particolare:

$$\boxed{\#Mor_{\mathbb{Q}}(K) = deg(M) = dim_{\mathbb{Q}}(K)} \tag{6.1}$$

In generale $\sigma(K) \neq K$. Tra i $\mathbb{Q}$-morfismi $\varphi : K \to \overline{\mathbb{Q}}$ ci sono quelli che verificano: $\varphi(K) \subset K$: un tale $\mathbb{Q}$-morfismo è un $\mathbb{Q}$-automorfismo di K. Infatti

l'applicazione $\varphi : K \to K$ è $\mathbb{Q}$-lineare (perché φ è un $\mathbb{Q}$-morfismo), ma φ è iniettivo (come ogni morfismo di campi); siccome $dim_{\mathbb{Q}}(K) < \infty$ l'endomorfismo φ del $\mathbb{Q}$-spazio vettoriale K, essendo iniettivo è anche suriettivo.

Denotando con $Aut_{\mathbb{Q}}(K)$ l'insieme degli $\mathbb{Q}$-automorfismi di K, abbiamo quindi $Aut_{\mathbb{Q}}(K) \subset Mor_{\mathbb{Q}}(K)$. Se $K = \mathbb{Q}(u)$, gli elementi di $Mor_{\mathbb{Q}}(K)$ corrispondono alle radici del polinomio minimo, $M(X) \in \mathbb{Q}[X]$, di u; gli elementi di $Aut_{\mathbb{Q}}(K)$ corrispondono invece alle radici di $M(X)$ *appartenenti a* K.
(Questa descrizione non è molto canonica perché ci sono tanti elementi primitivi, ma è molto comoda!)

In particolare:

$$\boxed{\#Aut_{\mathbb{Q}}(K) \leq dim_{\mathbb{Q}}(K)} \tag{6.2}$$

Definizione 6.19. *Con le notazioni precedenti $Aut_{\mathbb{Q}}(K)$ è il* gruppo di Galois *dell'estensione $K/\mathbb{Q}$.*
L'estensione $K/\mathbb{Q}$ è di Galois (o galoisienne*) se $Aut_{\mathbb{Q}}(K) = Mor_{\mathbb{Q}}(K)$, cioè se $\sigma(K) = K$, $\forall \sigma \in Mor_{\mathbb{Q}}(K)$.*

—— .. ——

Esercizi.

Esercizio 67 *Mostrare che* $\alpha = \dfrac{\sqrt{2}}{3}$ *è un numero algebrico ma non è un intero algebrico (cioè* $\alpha \in \overline{\mathbb{Q}} \setminus \mathcal{O}$*).*

Esercizio 68 *Mostrare che l'estensione* $\overline{\mathbb{Q}}/\mathbb{Q}$ *è algebrica, infinita.*

Esercizio 69 *Mostrare che un anello fattoriale è integralmente chiuso (quindi* $\mathbb{Z}, k[X]$ *sono integralmente chiusi).*

Esercizio 70 *Sia* $A \subset B$ *un'estensione di anelli. Si dice che* B *è intero su* A *se ogni elemento di* B *è intero su* A*.*
Sia $A \subset B \subset C$ *una torre di estensioni di anelli. Mostrare che se* C *è intero su* B *e se* B *è intero su* A*, allora* C *è intero su* A*.*

Esercizio 71 *Sia* K *un campo quadratico (estensione di grado due di* $\mathbb{Q}$*).*
(i) Mostrare che ogni elemento $\alpha \in K \setminus \mathbb{Q}$ *è primitivo (i.e.* $K = \mathbb{Q}(\alpha)$*). Più generalmente se* $L/\mathbb{Q}$ *è un'estensione di grado* p *(*p *primo) ogni elemento di* $L \setminus \mathbb{Q}$ *è primitivo.*
(ii) Sia $\alpha \in K$ *un elemento primitivo. Mostrare che* α *è radice di un'equazione* $ax^2 + bx + c = 0$*, con* $a, b, c \in \mathbb{Z}$*. Concludere che* $K = \mathbb{Q}(\sqrt{d})$*, dove* $d \in \mathbb{Z}$ *è senza fattori quadrati.*
(iii) Mostrare che ogni estensione di grado due è di Galois.
(iv) Mostrare con un esempio che esistono estensioni di grado tre non di Galois.

7

Norma, traccia, basi intere e discriminante.

7.1 Norma e traccia.

In questa sezione $K/\mathbb{Q}$ indica un campo di numeri di grado n ($[K:\mathbb{Q}]=n$). Indicheremo con $\sigma_i : K \hookrightarrow \overline{\mathbb{Q}}$ le n $\mathbb{Q}$-immersioni di K in $\overline{\mathbb{Q}}$.

Definizione 7.1. *Se $z \in K$ i* coniugati *(relativamente a K) di z sono $\sigma_1(z), ..., \sigma_n(z)$.*

I campi coniugati di K sono i campi $\sigma_i(K) \subset \overline{\mathbb{Q}}$.

Se z è primitivo ($K = \mathbb{Q}(z)$), allora i coniugati di z sono le radici del suo polinomio minimo $M_z(x)$. Infatti se $M_z(x) = x^n + a_{n-1}x^{n-1} + ... + a_0$, allora $\sigma_i(z^n + a_{n-1}z^{n-1} + ... + a_0) = 0 = \sigma(z)^n + a_{n-1}(\sigma_i(z))^{n-1} + ... + a_0$, quindi ogni $\sigma_i(z)$ è radice di $M_z(x)$. Inoltre $\sigma_i(z) \neq \sigma_j(z)$ se $i \neq j$ (infatti $(1, z, ..., z^{n-1})$ è una base di $K/\mathbb{Q}$).

Se z non è primitivo si considera $\mathbb{Q} \subset \mathbb{Q}(z) \subset K$. Chiaramente z è primitivo per $\mathbb{Q}(z)$ e se $r = [\mathbb{Q}(z) : \mathbb{Q}]$, $M_z(x)$ ha grado r, con $rt = n$ dove $t = [K : \mathbb{Q}(z)]$. In questa situazione abbiamo: $\prod_{i=1}^{n}(x - \sigma_i(z)) = (M_z(x))^t$. Per vederlo consideriamo un'altra interpretazione del polinomio $P_z(x) = \prod(x - \sigma_i(z))$.

Osserviamo che l'applicazione $m_z : K \to K : x \to zx$ è un endomorfismo del $\mathbb{Q}$-spazio vettoriale K.

Lemma 7.2. *Sia $K/\mathbb{Q}$ un campo di numeri con $[K:\mathbb{Q}] = n$ e siano $\sigma_i : K \hookrightarrow \overline{\mathbb{Q}}$ le n $\mathbb{Q}$-immersioni di K in $\overline{\mathbb{Q}}$. Allora per ogni $z \in K$, il polinomio caratteristico di m_z è $P_z(x) = \prod_{i=1}^{n}(x - \sigma_i(z))$*

Dimostrazione. Supponiamo z primitivo (cioè $K = \mathbb{Q}(z)$). In questo caso il polinomio minimo ha grado n: $M_z(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$, $a_i \in \mathbb{Q}$.

Abbiamo $z^n + a_{n-1}z^{n-1} + ... + a_0 = 0$ e $B = (1, z, ..., z^{n-1})$ è una base del $\mathbb{Q}$-spazio vettoriale K. Rispetto a questa base la matrice di m_z è data da:

$$M = mat(m_z; B, B) = \begin{pmatrix} 0 & 0 & \cdots & \cdots & -a_0 \\ 1 & 0 & \cdots & \cdots & -a_1 \\ 0 & 1 & \cdots & \cdots & -a_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

E' un esercizio classico di algebra lineare (Esrcizio 72) verificare che il polinomio minimo di M è proprio $M_z(x)$. Quindi $Tr(z) = -a_{n-1}$ e $N(z) = (-1)^n a_0$. Adesso i coefficienti di $M_z(x)$ sono le funzioni simmetriche elementari delle sue radici: se $M_z(x) = \prod_{i=1}^{n}(x - r_i)$ (fattorizzazione in $\overline{\mathbb{Q}}$), allora $-a_{n-1} = r_1 + \cdots + r_n$ e $(-1)^n a_0 = r_1...r_n$. Rimane da osservare che le radici di $M_z(x)$ sono i coniugati di z: $r_i = \sigma_i(z)$ e il risultato segue.
Se z non è primitivo consideriamo $\mathbb{Q} \subset \mathbb{Q}(z) \subset K$. Se $B = (w_i)$ è una base di $\mathbb{Q}(z)/\mathbb{Q}$ e se $(v_1, ..., v_t)$ è una base di $K/\mathbb{Q}(z)$, allora $C = (w_i v_j)$ è una base di $K/\mathbb{Q}$. Nella base $C = (v_1 w_1, ..., v_1 w_r; v_2 w_1, ..., v_t w_r)$ la matrice di m_z è una matrice diagonale a blocchi dove ogni blocco è $M = mat(m'_z; B, B)$, dove m'_z è la restrizione a $\mathbb{Q}(z)$ di m_z. Quindi $P_z(x) = (P'_z(x))^t$, dove $P'_z(x)$ è il polinomio caratteristico di m'_z. Per la prima parte della dimostrazione $P'_z(x) = M_z(x)$. □

In conclusione i coniugati (relativamente a K) di $z \in K$ sono le radici del polinomio minimo $M_z(x)$, ognuna ripetuta $t = [K : \mathbb{Q}(z)]$ volte.

Definizione 7.3. *La norma (risp. la traccia, il polinomio caratteristico) dell'elemento $z \in K$ è il determinante (risp. la traccia, il polinomio caratteristico) dell'endomorfismo m_z. Indicheremo con $N_{K/\mathbb{Q}}(z)$, $Tr_{K/\mathbb{Q}}(z)$ (o più semplicemente $N(z), Tr(z)$ se non c'è rischio di confusione) la norma e la traccia di $z \in K$.*
Dal Lemma 7.2 risulta:

$$N(z) = \prod \sigma_i(z),\ Tr(z) = \sum \sigma_i(z).$$

Chiaramente $N(z), Tr(z) \in \mathbb{Q}$ per ogni $z \in K$. Se z è intero si può dire qualcosa di più:

Lemma 7.4. *Se $z \in \mathcal{O}_K$, allora il polinomio minimo, $M_z(x)$, di z è a coefficienti in $\mathbb{Z}$, pertanto $N_{K/\mathbb{Q}}(z), Tr_{K/\mathbb{Q}}(z) \in \mathbb{Z}$.*

Dimostrazione. Osserviamo che se $z \in \mathcal{O}_K$, allora $\sigma_i(z) \in \mathcal{O}$. Infatti se $Q(z) = z^m + a_{m-1}z^{m-1} + ... + a_0 = 0$, $a_i \in \mathbb{Z}$, allora $Q(\sigma_i(z)) = 0$.

Se $M_z(x) = x^r + b_{r-1}x^{r-1} + .. + b_0$ è il polinomio minimo, a priori $b_i \in \mathbb{Q}$. I coefficienti b_i sono dati dalle funzioni simmetriche elementari delle radici: $b_{r-1} = -(\sigma_1(z) + ... + \sigma_r(z))$, ..., $b_0 = (-1)^r\sigma_1(z)...\sigma_r(z)$. Siccome $\mathcal{O}$ è un anello, $b_i \in \mathcal{O}$, $\forall i$. Quindi $b_i \in \mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$. □

Il fatto che $N(z), Tr(z)$ siano degli interi non implica in generale $z \in \mathcal{O}_K$ (è vero però se K è un campo quadratico).

7.2 Discriminante.

Se $x_1, ..., x_n \in K$ ($n = [K : \mathbb{Q}]$) possiamo associare agli x_i (e ai loro coniugati relativamente a K) il loro discriminante $disc(x_1, ..., x_n)$; è un numero razionale che ha varie proprietà interessanti per esempio $disc(x_1, ..., x_n) \neq 0 \Leftrightarrow x_1, ..., x_n$ sono linearmente indipendenti su $\mathbb{Q}$. Se $x_i \in \mathcal{O}_K$, $\forall i$, allora $disc(x_1, ..., x_n) \in \mathbb{Z}$. Finalmente questa nozione ci servirà a definire un importante invariante di K (il *discriminate* di $K/\mathbb{Q}$ appunto).

Definizione 7.5. *Siano $x_1, ..., x_n \in K$, il discriminante degli n elementi $x_1, ..., x_n$ è: $disc(x_1, ..., x_n) := (\det(A))^2$, dove $A = (\sigma_i(x_j)$.*

Osservare che (per via del quadrato) il discriminante non dipende dall'ordine degli x_i, σ_j.

Abbiamo:

Lemma 7.6. *Con le notazioni della Definizione 7.5 abbiamo:*

$$disc(x_1, ..., x_n) = \det(Tr(x_i x_j)).$$

In particolare $disc(x_1, ..., x_n) \in \mathbb{Q}$ e se $x_i \in \mathcal{O}_K$, $\forall i$, $disc(x_1, ..., x_n) \in \mathbb{Z}$.

Dimostrazione. Sia $A = (\sigma_i(x_j))$. Abbiamo $\det({}^tAA) = (\det A)^2 = disc(x_i)$. Se ${}^tAA = (a_{ij})$, $a_{ij} = (i-$esima riga di ${}^tA \mid j$-esima colona di $A) = (i$-esima colona di $A \mid j$-esima colona di $A) = \sigma_1(x_i)\sigma_1(x_j) + ... + \sigma_n(x_i)\sigma_n(x_j)$ $= \sigma_1(x_ix_j) + ... + \sigma_n(x_ix_j) = Tr(x_ix_j)$.
L'ultima affermazione segue dal Lemma 7.4. □

Se $z \in K$ è un elemento primitivo, allora $1, z, ..., z^{n-1}$ formano una base di $K/\mathbb{Q}$ e abbiamo (con $z_i = \sigma_i(z)$):

$$disc(1, z, ..., z^{n-1}) = \begin{vmatrix} 1 & z_1 & z_1^2 & \cdots & z_1^{n-1} \\ 1 & z_2 & z_2^2 & \cdots & z_2^{n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & z_n & z_n^2 & \cdots & z_n^{n-1} \end{vmatrix}^2 = \prod_{i<j}(z_i - z_j)^2 \neq 0$$

L'ultima uguaglianza viene dal calcolo del determinante di Vandermonde (Esercizio 74). Si ricorda che se $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, il discriminate di $P(x)$ è $disc(P) = \prod_{i<j}(\alpha_i - \alpha_j)^2$, dove $\alpha_1, ..., \alpha_n$ sono le radici (nel campo di spezzamento) di $P(x)$. Quindi P non ha radici multiple $\Leftrightarrow disc(P) \neq 0$. Il discriminante di un polinomio è anche uguale (a meno del segno) al risultante di P con la sua derivata, precisamente: $(-1)^{n(n-1)/2} disc(P) = Res(P, P')$.

In conclusione se z è primitivo e se $B = (1, z, ..., z^{n-1})$ è la base di "potenze" associata, $disc(1, z, ..., z^{n-1})$ non è altro che il discriminante del polinomio minimo di z.

Consideriamo la forma bilineare simmetrica $\tau : K \times K \to \mathbb{Q} : (x, y) \to Tr(xy)$. Se z è un elemento primitivo e se $B = (1, z, ..., z^{n-1})$, la matrice di τ rispetto a B è: $M = mat_B(\tau) = (Tr(z^i z^j))$. Per il Lemma 7.6, $\det(M) = disc(1, z, ..., z^{n-1})$, quindi per quanto appena visto: $\det(M) = \prod_{i<j}(z_i - z_j)^2 \neq 0$. Questo mostra che la forma bilineare τ è non degenere.

Corollario 7.7. *Siano $x_1, ..., x_n \in K$. Allora $disc(x_1, ..., x_n) \neq 0 \Leftrightarrow (x_1, ..., x_n)$ è una base del $\mathbb{Q}$-spazio vettoriale K.*

Dimostrazione. Se $B = (x_1, ..., x_n)$ è una $\mathbb{Q}$-base di K, allora $\det(mat_B(\tau)) \neq 0$, quindi $disc(x_1, ..., x_n) \neq 0$.

Supponiamo gli x_i dipendenti: $c_1x_1 + \cdots + c_nx_n = 0$, $c_i \in \mathbb{Q}$, non tutti nulli. Abbiamo $\sigma_i(c_1x_1 + \cdots + c_nx_n) = 0 = c_1\sigma_i(x_1) + \cdots + c_n\sigma_i(x_n)$. Quindi i vettori colonna della matrice $A = (\sigma_i(x_j))$ sono dipendenti. Quindi $\det(A) = 0$, ossia $disc(x_1, ..., x_n) = 0$. □

7.3 Basi intere.

L'anello degli interi di K, $\mathcal{O}_K$, è un $\mathbb{Z}$-modulo. Scopo di quanto segue è mostrare che $\mathcal{O}_K$ è un $\mathbb{Z}$-modulo libero di rango n. Più generalmente se $I \subset \mathcal{O}_K$ è un ideale non nullo (quindi un gruppo abeliano) mostriamo che I è un $\mathbb{Z}$-modulo libero di rango n. Segue allora che $\mathcal{O}_K$ è un anello noetheriano.

Definizione 7.8. *Una* base intera *di $\mathcal{O}_K$ è una base di $\mathcal{O}_K$ come $\mathbb{Z}$-modulo. Quindi $\alpha_1, ..., \alpha_n \in \mathcal{O}_K$ è una base intera se ogni $\beta \in \mathcal{O}_K$ si scrive, in modo unico: $\beta = b_1\alpha_1 + \cdots + b_n\alpha_n$, con $b_i \in \mathbb{Z}$, $\forall i$.*

Osserviamo (Esercizio 75) che una base intera è automaticamente una base del $\mathbb{Q}$-spazio vettoriale K, quindi deve necessariamente essere costituita da $n = [K : \mathbb{Q}]$ elementi.

Lemma 7.9. *Sia $I \subset \mathcal{O}_K$ un ideale non nullo. Allora esiste $c \neq 0$, $c \in I \cap \mathbb{Z}$.*

Dimostrazione. Sia $\alpha \in I$ un elemento non nullo e sia $M_\alpha(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$ il suo polinomio minimo. Abbiamo $M_\alpha(x) \in \mathbb{Z}[x]$ (Lemma 7.4). Dalla relazione $\alpha^m + b_{m-1}\alpha^{m-1} + \cdots + b_1\alpha + b_0 = 0$ segue che $b_0 \in I$. Finalmente siccome $M_\alpha(x)$ è irriducibile $b_0 \neq 0$. □

Lemma 7.10. *Sia $I \subset \mathcal{O}_K$ un ideale non nullo. Allora esistono $\alpha_1, ..., \alpha_n \in I$ ($n = [K : \mathbb{Q}]$), tali che che $disc(\alpha_1, ..., \alpha_n) \neq 0$.*

Dimostrazione. Sia $(\omega_1, ..., \omega_n)$ una base del $\mathbb{Q}$-spazio vettoriale K. Abbiamo $disc(\omega_1, ..., \omega_n) \neq 0$ (Corollario 7.7). Per il Lemma 7.9 esiste $c \in I \cap \mathbb{Z}$, $c \neq 0$. Poniamo $\alpha_i = c\omega_i$. Abbiamo $\alpha_i \in I$. Siccome $(c\omega_1, ..., c\omega_n)$ è ancora una base di K su $\mathbb{Q}$, per il Corollario 7.7, $disc(\alpha_1, ..., \alpha_n) \neq 0$. □

Arriviamo adesso al nostro risultato principale:

Proposizione 7.11. *Sia K un campo di numeri di grado n (cioè $n = [K : \mathbb{Q}]$). Sia $I \subset \mathcal{O}_K$ un ideale non nullo. Allora esiste una base intera di I.*

Dimostrazione. Per il Lemma 7.13 esistono $\alpha_1, ..., \alpha_n \in I$ tali che $disc(\alpha_1, ..., \alpha_n) \neq 0$. Siccome $\alpha_i \in I \subset \mathcal{O}_K$, $disc(\alpha_1, ..., \alpha_n) \in \mathbb{Z}$ (Lemma 7.6). Quindi $|disc(\alpha_1, ..., \alpha_n)|$ è un intero > 0. Sia $S = \{|disc(\alpha_1, ..., \alpha_n)| \mid disc(\alpha_1, ..., \alpha_n) \neq 0, \alpha_i \in I, \forall i\}$. Siccome $S \subset \mathbb{N}$ è un insieme non vuoto, ammette un elemento minimo: $|disc(\gamma_1, ..., \gamma_n)|$. Dalla condizione $disc(\gamma_1, ..., \gamma_n) \neq 0$ segue che $(\gamma_1, ..., \gamma_n)$ è una base di K su $\mathbb{Q}$ (Corollario 7.7).
Sia $\alpha \in I$, allora $\alpha = b_1\gamma_1 + \cdots + b_n\gamma_n$, con $b_i \in \mathbb{Q}$. Dobbiamo mostrare che $b_i \in \mathbb{Z}$.
Se uno dei $b_i \notin \mathbb{Z}$, riordinano semmai gli indici possiamo assumere $b_1 \notin \mathbb{Z}$. Quindi esiste $n \in \mathbb{Z}$ tale che $n < b_1 < n + 1$.

Sia $\beta = \alpha - n\gamma_1$. Abbiamo $\beta \in I$, $\beta = (b_1 - n)\gamma_1 + b_2\gamma_2 + \cdots + b_n\gamma_n$. Pertanto: $\sigma_i(\beta) = (b_1 - n)\sigma_i(\gamma_1) + \cdots + b_n\sigma_i(\gamma_n)$, $1 \leq i \leq n$. In altri termini $(b_1 - n, b_2, ..., b_n)$ è soluzione del sistema lineare:

$$\begin{cases} \sigma_1(\beta) &= (b_1 - n)\sigma_1(\gamma_1) + b_2\sigma_1(\gamma_2) \cdots + b_n\sigma_1(\gamma_n) \\ \sigma_2(\beta) &= (b_1 - n)\sigma_2(\gamma_1) + b_2\sigma_2(\gamma_2) \cdots + b_n\sigma_2(\gamma_n) \\ \cdots \quad & \cdots \qquad\qquad\qquad\qquad\qquad\qquad \cdots \\ \sigma_n(\beta) &= (b_1 - n)\sigma_n(\gamma_1) + b_2\sigma_n(\gamma_2) \cdots + b_n\sigma_n(\gamma_n) \end{cases}$$

La matrice dei coefficienti di questo sistema è $A = (\sigma_i(\gamma_j))$. Sia A' la matrice ottenuta da A rimpiazzando la prima colonna con la trasposta di $(\sigma_1(\beta), ..., \sigma_n(\beta))$. Per la formula di Cramer: $b_1 - n = \det(A')/\det(A)$. Quindi $(b_1 - n)^2 = disc(\beta, \gamma_2, ..., \gamma_n)/disc(\gamma_1, \gamma_2, ..., \gamma_n)$. Siccome $b_1 - n < 1$, questo contraddice la minimalità di $|disc(\gamma_1, ..., \gamma_n)|$. Quindi $b_i \in \mathbb{Z}$, $\forall i$. □

Per una dimostrazione alternativa di questa Proposizione vedere l'Esercizio 76.

Una conseguenza importante:

Corollario 7.12. *Sia K un campo di numeri. L'anello degli interi di K, $\mathcal{O}_K$, è un anello noetheriano.*

Dimostrazione. Se $I \subset \mathcal{O}_K$ dalla Proposizione 7.11 I è generato da $[K : \mathbb{Q}]$ elementi come $\mathbb{Z}$-modulo, quindi è finitamente generato. □

Un altro fatto importante:

Lemma 7.13. *Sia $I \subset \mathcal{O}_K$ un ideale. Se $B = (\alpha_1, ..., \alpha_n)$, $B' = (\beta_1, ..., \beta_n)$ sono due basi intere di I, allora $disc(\alpha_1, ..., \alpha_n) = disc(\beta_1, ..., \beta_n)$.*

Dimostrazione. Dal Lemma 7.6, $disc(\alpha_1, ..., \alpha_n)$ è il determinante della matrice nella base $B = (\alpha_1, ..., \alpha_n)$ della forma bilineare $\tau(v, w) = Tr(vw)$. Se $A = mat_B(\tau)$ e $A' = mat_{B'}(\tau)$, allora $A =^t PA'P$ dove $P = mat(Id; B, B')$. Quindi $\det(A) = \det(P)^2 . \det(A')$. Siccome P è la matrice di passaggio tra due basi del $\mathbb{Z}$-modulo libero I, P è una matrice invertibile a coefficienti in $\mathbb{Z}$, quindi $\det(P) = \pm 1$. Pertanto $\det(A) = \det(A')$. □

Vediamo così che il discriminante di una base intera è un invariante di I. In particolare se $I = (1) = \mathcal{O}_K$, abbiamo un invariante di $\mathcal{O}_K$ (e quindi di K):

Definizione 7.14. *Il discriminante di un ideale $I \subset \mathcal{O}_K$ è il discriminante, d_I, di una base intera di I.*
Il discriminante di $\mathcal{O}_K$ (o di K) è il discriminate, D_K, di una base intera di $\mathcal{O}_K$.

7.4 Anello degli interi dei campi quadratici.

Se K è un campo quadratico ($[K : \mathbb{Q}] = 2$), allora ogni elemento $\alpha \in K \setminus \mathbb{Q}$ è primitivo (cioè $K = \mathbb{Q}(\alpha)$). Il polinomio minimo $M_\alpha(x) \in \mathbb{Q}[x]$ è irriducibile di grado due. Riducendo allo stesso denominatore vediamo che α è radice di un polinomio di grado due a coefficienti interi: $ax^2 + bx + c = 0$, $a, b, c \in \mathbb{Z}$. Quindi $\alpha = (-b \pm \sqrt{b^2 - 4ac})/2a$. Possiamo quindi rimpiazzare α con $\sqrt{\delta}$, $\delta = b^2 - 4ac$. Scrivendo $\delta = a^2 d$ dove d è senza fattori quadrati otteniamo: $K = \mathbb{Q}(\sqrt{d})$ dove $d \in \mathbb{Z}$, d senza fattori quadrati. In particolare $d \not\equiv 0 \pmod 4$. Quindi ogni $\alpha \in K$ è della forma $\alpha = r + s\sqrt{d}$, $r, s \in \mathbb{Q}$ e α è primitivo se e solo se $s \neq 0$.

Se $d > 0$, $K \subset \mathbb{R}$ e si dice che K è *reale*, se $d < 0$ $K \not\subset \mathbb{R}$ e si dice che K è *immaginario*.

Se α è primitivo il suo polinomio minimo è $X^2 - Tr(\alpha)X + N(\alpha)$, le cui radici sono $\alpha = r + s\sqrt{d}$ e $\overline{\alpha} = r - s\sqrt{d}$. Quindi $\overline{\alpha}$ è il coniugato di α.

D'altra parte è chiaro che $K/\mathbb{Q}$ è di Galois e le due $\mathbb{Q}$-immersioni sono Id e il coniugo: $K \to K : r + s\sqrt{d} \to r - s\sqrt{d}$.

Se $d < 0$, si tratta del coniugato nel senso dei numeri complessi. La *norma* di α è $N(\alpha) = \alpha.\overline{\alpha} = r^2 - ds^2 \in \mathbb{Q}$. Se $d < 0$, $N(\alpha) > 0, \forall \alpha \neq 0$; se $d > 0$ la norma prende valori positivi e valori negativi.

La *traccia* di α è $Tr(\alpha) = \alpha + \overline{\alpha} = 2r \in \mathbb{Q}$.
Osserviamo: $\alpha \in \mathcal{O}_K \Leftrightarrow N(\alpha) \in \mathbb{Z}$ e $Tr(\alpha) \in \mathbb{Z}$ (confrontare con il Lemma 7.4 e l'osservazione successiva).

Proposizione 7.15. *Sia $K = \mathbb{Q}(\sqrt{d})$ un campo quadratico, allora:*

- *Se $d \equiv 2$ o $3 \pmod 4$, $\mathcal{O}_K = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} = \mathbb{Z} + \sqrt{d}.\mathbb{Z}$*
- *Se $d \equiv 1 \pmod 4$, $\mathcal{O}_K = \{\dfrac{a + b\sqrt{d}}{2} \mid a, b \in \mathbb{Z}, a \equiv b \pmod 2\}$.*

Dimostrazione. Sia $\alpha \in \mathcal{O}_K$, riducendo allo stesso denominatore abbiamo $\alpha = (a + b\sqrt{d})/c$. Possiamo assumere $(a, b, c) = 1$ perché se p divide a, b e c allora si semplifica per p. Finalmente possiamo anche assumere $c > 0$.

Come già visto $Tr(\alpha) = 2a/c \in \mathbb{Z}$ e $N := N(\alpha) = (a^2 - db^2)/c^2 \in \mathbb{Z}$.

Abbiamo $(a, c) = 1$. Infatti se $p \mid a$ e $p \mid c$ da $c^2 N = a^2 - db^2$ segue che $p \mid db^2$ ma siccome d non ha fattori quadrati, questo implica $p \mid b$, contro l'ipotesi $(a, b, c) = 1$.

Da $(a, c) = 1$ e $2a/c \in \mathbb{Z}$ segue che $c = 1$ o $c = 2$. Se $c = 1$, $\alpha \in \mathbb{Z} + \sqrt{d}.\mathbb{Z}$.
Se $c = 2$ allora $a^2 - db^2 = 4N$ e quindi $a^2 - db^2 \equiv 0 \pmod 4$.

- Se a, b sono entrambi pari allora $2 \mid a, b, c$, contro l'ipotesi $(a, b, c) = 1$
- Se a è pari e b è dispari: $a^2 - db^2 \equiv -d \pmod 4$ quindi $d \equiv 0 \pmod 4$, contro l'ipotesi che d è senza fattori quadrati.
- Se a è dispari e b è pari: $a^2 - db^2 \equiv 1 \equiv 0 \pmod 4$, assurdo.
- Se a, b sono entrambi dispari, allora $a^2 - db^2 \equiv 1 - d \equiv 0 \pmod 4$, cioè $d \equiv 1 \pmod 4$.

Questo mostra che se $d \not\equiv 1 \pmod 4$ (quindi $d \equiv 2, 3 \pmod 4$), allora $c = 1$ e quindi $\mathcal{O}_K = \mathbb{Z} + \sqrt{d}.\mathbb{Z}$.

Se $d \equiv 1 \pmod 4$ e se $c = 2$ allora necessariamente a, b sono dispari. Viceversa se $\alpha = (a + b\sqrt{d})/2$ con a, b dispari, allora $Tr(\alpha) = a \in \mathbb{Z}$ e $N(\alpha) = (a^2 - db^2)/4 \in \mathbb{Z}$ perché $a^2 - db^2 \equiv 0 \pmod 4$. Quindi se $\alpha \in \mathcal{O}_K$ o $c = 1$ o $c = 2$ e a, b sono dispari. Se $c = 1$ possiamo comunque scrivere $\alpha = (2a + 2b\sqrt{d})/2$.
Quindi $\mathcal{O}_K = \{\dfrac{a + b\sqrt{d})}{2} \mid a, b \in \mathbb{Z}, a \equiv b \pmod 2\}$. □

Da questa descrizione risulta:

Corollario 7.16. *Sia $K = \mathbb{Q}(\sqrt{d})$ un campo quadratico. Sia*

$$\omega = \begin{cases} \sqrt{d} & \text{se } d \equiv 2,3 \pmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{se } d \equiv 1 \pmod 4 \end{cases}$$

allora $(1, \omega)$ è una base intera del $\mathbb{Z}$-modulo libero di rango due $\mathcal{O}_K$.

Abbiamo anche:

Corollario 7.17. *Sia $K = \mathbb{Q}(\sqrt{d})$ un campo quadratico. Il discriminante di K è dato da:*

$$D_K = \begin{cases} 4d & \text{se } d \equiv 2,3 \pmod 4 \\ d & \text{se } d \equiv 1 \pmod 4 \end{cases}$$

In particolare $D_K \equiv 0, 1 \pmod 4$.

Dimostrazione. Prendiamo la base intera $(1, \omega)$ dove $\omega = \sqrt{d}$ se $d \equiv 2, 3 \pmod 4$, $\omega = (1 + \sqrt{d})/2$ se $d \equiv 1 \pmod 4$. Per definizione (7.14) $D_K = disc(1, \omega)$ e per il Lemma 7.6:

$$D_K = \begin{vmatrix} Tr(1) & Tr(\omega) \\ Tr(\omega) & Tr(\omega^2) \end{vmatrix}$$

e si conclude facilmente. □

Osservazione 7.18. Questo è un fatto generale: il discriminante di un campo di numeri è sempre congruo a 0 o 1 modulo 4 (Esercizio 80).

Esercizi.

Esercizio 72 *Sia* $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in k[x]$. *Mostrare che il polinomio caratteristico della matrice*

$$M = \begin{pmatrix} 0 & 0 & \cdots & \cdots & -a_0 \\ 1 & 0 & \cdots & \cdots & -a_1 \\ 0 & 1 & \cdots & \cdots & -a_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

è proprio $P(x)$.

Esercizio 73 *Sia* $K/\mathbb{Q}$ *un campo di numeri. Si pone* $Tr = Tr_{K/\mathbb{Q}}$, $N = N_{K/\mathbb{Q}}$. *Siano* $\alpha, \beta \in K, a \in \mathbb{Q}$. *Dimostrare che:*
(i) $Tr : K \to \mathbb{Q} : \alpha \to Tr(\alpha)$ *è un'applicazione* $\mathbb{Q}$*-lineare con* $Tr(a) = n.a$ $(n = [K : \mathbb{Q}])$.
(ii) $N(\alpha\beta) = N(\alpha).N(\beta)$, $N(a) = a^n$, $N(a\alpha) = a^nN(\alpha)$.

Esercizio 74 *(Il determinante di Vandermonde)*
Sia $\delta(a_1, ..., a_n) = \det A$ *dove:*

$$A = A(a_1, ..., a_n) := \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ \vdots & \vdots & & \vdots \\ a_1^{n-1} & a_2^{n-1} & \cdots & a_n^{n-1} \end{pmatrix}$$

Si tratta di mostrare:

$$\delta(a_1, ..., a_n) = \prod_{1 \le i < j \le n} (a_j - a_i) \quad (*)$$

1. *Se* $f(x) = x^{n-1} + b_{n-2}x^{n-2} + ... + b_0$, *mostrare che:*

$$\delta(a_1, ..., a_n) = \begin{vmatrix} 1 & 1 & \cdots & \cdots & 1 \\ a_1 & a_2 & \cdots & \cdots & a_n \\ \vdots & \vdots & & \vdots & \vdots \\ a_1^{n-2} & a_2^{n-2} & \cdots & \cdots & a_n^{n-2} \\ f(a_1) & f(a_2) & \cdots & \cdots & f(a_n) \end{vmatrix}$$

2. *Dimostrare* $(*)$ *per induzione su* $n \ge 2$ *usando (1) e un* f *opportuno.*

Esercizio 75 *Sia K un campo di numeri e $\alpha \in K$. Mostrare che esiste $0 \neq m \in \mathbb{Z}$ tale che $m\alpha \in \mathcal{O}_K$. Concludere che una base intera di $\mathcal{O}_K$ è una base del $\mathbb{Q}$-spazio vettoriale K.*
Il viceversa non è vero: dare un esempio di una $\mathbb{Q}$-base di K fatta da interi algebrici che non sia una base intera.

Esercizio 76 *Scopo dell'Esercizio è dare una dimostrazione alternativa della Proposizione 7.11.*
(i) Sia E un k-spazio vettoriale e $f : E \times E \to k$ una forma bilineare simmetrica non degenere. Sia $B = (e_i)$ una base di E. Mostrare che esiste una base (v_i) di E tale che $f(e_i, v_j) = \delta_{ij}$.
(ii) Sia K un campo di numeri di grado n e sia $I \subset \mathcal{O}_K$ un ideale. Sia $(w_1, ..., w_n)$ una base di $K/\mathbb{Q}$. Esiste $0 \neq c \in \mathbb{Z}$ tale che $\alpha_i = cw_i \in I$. Per (i) esiste una $\mathbb{Q}$-base (γ_i) tale che $Tr(\alpha_i\gamma_j) = \delta_{ij}$. Se $\alpha \in I$, $\alpha = \sum a_i\gamma_i$, $a_i \in \mathbb{Q}$. Mostrare che $a_i \in \mathbb{Z}, \forall i$.
(iii) Per (ii), $I \subset \gamma_1\mathbb{Z} + \cdots + \gamma_n\mathbb{Z}$. Dedurne che I è un $\mathbb{Z}$-modulo libero di rango $m \leq n$ (usare il teorema di struttura dei moduli su un PID).
(iv) Per (iii) esiste $B = (\beta_1, ..., \beta_m)$, $\mathbb{Z}$-base di I. Mostrare che B è una base di $K/\mathbb{Q}$. Quindi $m = n$ e B è una base intera di I.

Esercizio 77 *Sia z un elemento primitivo di $K/\mathbb{Q}$ di polinomio minimo $M(x)$. Scopo dell'esercizio è mostrare che:*

$$disc(1, z, ..., z^{n-1}) = (-1)^{n(n-1)/2} N_{K/\mathbb{Q}}(M'(z))$$

dove $M'(x)$ è la derivata di $M(x)$.
(i) Sia $M(x) = \prod(x - z_i)$, dove $z_1 = z, ..., z_n$ sono i coniugati di z. Mostrare che $M'(z_j) = \prod_{i/i\neq j} (z_j - z_i)$.
(ii) Mostrare che $N(M'(z)) = \prod_{j=1}^{n} M'(z_j)$ ($N = N_{K/\mathbb{Q}}$).
(iii) Concludere che

$$N(M'(z)) = \prod_{i,j=1, i\neq j}^{n} (z_j - z_i) = (-1)^{n(n-1)/2} \prod_{1\leq i<j\leq n} (z_i - z_j)^2.$$

Esercizio 78 *Sia ξ una radice primitiva p-esima dell'unità (p primo). Quindi ξ è radice di $x^p - 1 = (x - 1)(x^{p-1} + \cdots + x + 1)$. Quindi ξ è radice di $\Phi_p(x) := x^{p-1} + \cdots + x + 1$.*
(i) Mostrare che $\Phi_p(x) \in \mathbb{Z}[x]$ è irriducibile (considerare $\Phi_p(x+1)$). Concludere che $K = \mathbb{Q}(\xi)$ ha grado $\varphi(p) = p - 1$ e che $B = (1, \xi, \xi^2, ..., \xi^{p-2})$ è una

$\mathbb{Q}$-base di K. Osservare che $\xi^i \in \mathcal{O}_K$.
(ii) I coniugati di ξ sono $\sigma_i(\xi) = \xi^i$, $i = 1, ..., p-1$. In particolare $\mathbb{Q}(\xi)/\mathbb{Q}$ è di Galois.
(iii) Mostrare che $Tr(\xi^i) = -1$, $Tr(1-\xi^i) = p$ $(1 \leq i \leq p-1)$ e $N(1-\xi) = p$.
(iv) Mostrare che $(1-\xi)\mathcal{O}_K \cap \mathbb{Z} = (p)$.
(v) Sia $\alpha \in \mathcal{O}_K$ e sia $\sigma_i \in Aut_{\mathbb{Q}}(K)$ definito da $\sigma_i(\xi) = \xi^i$. Mostrare che $\sigma_i(\alpha(1-\xi)) \in (1-\xi)\mathcal{O}_K$. Concludere che $Tr(\alpha(1-\xi)) \in (1-\xi)\mathcal{O}_K$.
(vi) Sia $\alpha \in \mathcal{O}_K$. Quindi $\alpha = a_0 + a_1\xi + \cdots + a_{p-2}\xi^{p-2} \in \mathcal{O}_K$, $a_i \in \mathbb{Q}$. Mostrare che $Tr(\alpha(1-\xi)) = a_0 p$ e concludere che $a_0 \in \mathbb{Z}$.
(vii) Osservare che $\xi^{-1} \in \mathcal{O}_K$, quindi $\alpha_1 = (\alpha - a_0)\xi^{-1} = a_1 + a_2\xi + \cdots + a_{p-2}\xi^{p-3} \in \mathcal{O}_K$. Ripetendo il ragionamento precedente mostrare che $a_1 \in \mathbb{Z}$. Concludere che $a_i \in \mathbb{Z}, \forall i$.

Questo mostra che $B = (1, \xi, \xi^2, ..., \xi^{p-2})$ è una base intera di $\mathcal{O}_K$ e quindi che $\mathcal{O}_K = \mathbb{Z}[\xi]$.

Esercizio 79 *Questo esercizio è una continuazione dell'Esercizio 78. Usando l'Esercizio 77, mostrare che:*

$$D_K := \prod_{1 \leq i < j \leq p-1} (\xi^i - \xi^j)^2 = (-1)^{(p-1)/2} p^{p-2}$$

dove $K = \mathbb{Q}(\xi)$, ξ radice primitiva p-esima dell'unità.

Esercizio 80 (Relazione di Stickelberger)
Sia $K/\mathbb{Q}$ un campo di numeri di grado n. Se $(\omega_1, ..., \omega_n)$ è una base intera, allora per definizione $D_K = disc(\omega_1, ..., \omega_n) = (det(\sigma_i(\omega_j)))^2$, dove $\sigma_1, ..., \sigma_n$ sono le n $\mathbb{Q}$-immersioni di K in $\overline{\mathbb{Q}}$.

Se $M = (a_{ij})$ è una matrice $n \times n$

$$\det(M) = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{\sigma(1),1} ... a_{\sigma(n),n} = P - N$$

dove $P = \sum_{\sigma | \varepsilon(\sigma) = 1} a_{\sigma(1),1} ... a_{\sigma(n),n}$ e dove $N = \sum_{\sigma | \varepsilon(\sigma) = -1} a_{\sigma(1),1} ... a_{\sigma(n),n}$.

D'ora in poi P, N sono definiti, con le notazioni precedenti da: $\det(\sigma_i(\omega_j)) = P - N$, *dove (ω_i) è una base intera.*
(i) Mostrare che $\sigma_i(P+N) = P+N$, $\sigma_i(PN) = PN$, $\forall i$.
(ii) Sia $\alpha \in K$ tale che $\sigma_i(\alpha) = \alpha, \forall i$. Mostrare che $\alpha \in \mathbb{Q}$. Concludere che $P+N, PN \in \mathbb{Q}$.
(iii) Mostrare che $P+N$ e PN sono interi algebrici $(\in \mathcal{O})$. Dedurne: $P+N, PN \in \mathbb{Z}$.
(iv) Concludere che $D_K \equiv 0, 1 \pmod 4$ (relazione di Stickelberger).

8

Il teorema di fattorizzazione di Dedekind.

Come abbiamo già visto (Esercizio 13) l'anello degli interi $\mathcal{O}_K$ di un campo di numeri non è sempre un anello a fattorizzazione unica (UFD), questo fatto fu osservato per la prima volta da Kummer nel corso delle sue ricerche sull'equazione di Fermat. Per ovviare a questo inconveniente Kummer ha introdotto la nozione di *numeri ideali*, questa nozione rivisitata poi da Dedekind ha dato luogo alla nozione di ideale di un anello. In termini moderni il teorema di Dedekind afferma che ogni ideale $I \subset \mathcal{O}_K$ si scrive in modo unico (a meno dell'ordine dei fattori) come un prodotto di ideali primi. Quindi anche se la fattorizzazione unica non è più vera per i numeri $\alpha \in \mathcal{O}_K$ e comunque vera per gli ideali (cioè per i numeri "ideali" $(\alpha) \subset \mathcal{O}_K$).

In realtà il teorema di Dedekind è un teorema di *algebra* valido per tutta una categoria di anelli (anelli di Dedekind appunto). Inizieremo quindi col definire la nozione di anello di Dedekind, mostreremo che ogni anello di interi $\mathcal{O}_K$ è un anello di Dedekind per poi dimostrare il teorema di fattorizzazione.

8.1 Anelli di Dedekind, anelli degli interi.

Iniziamo con la definizione:

Definizione 8.1. *Un anello integro A è di Dedekind se:*

1. *A è integralmente chiuso*
2. *A è noetheriano*
3. *ogni ideale primo non nullo è massimale*

Quindi per esempio $\mathbb{Z}$ è un anello di Dedekind. Scopo di quanto segue è mostrare che l'anello, $\mathcal{O}_K$, degli interi di un campo di numeri K è un anello di Dedekind.

Lemma 8.2. *L'anello degli interi di un campo di numeri è integralmente chiuso.*

Dimostrazione. Sia K un campo di numeri e $\alpha \in K$ intero su $\mathcal{O}_K$. Siccome $\mathcal{O}_K$ è intero su $\mathbb{Z}$, α è intero su $\mathbb{Z}$ (Esercizio 70). Quindi $\alpha \in \mathcal{O} \cap K = \mathcal{O}_K$. □

Lemma 8.3. *Sia K un campo di numeri e $I \subset \mathcal{O}_K$ un ideale non nullo, allora:*
(i) $I \cap \mathbb{Z} \neq \{0\}$
(ii) $\#(\mathcal{O}_K/I) < +\infty$.
(iii) Se I è primo, allora I è massimale.

Dimostrazione. (i) E' il Lemma 7.9.
(ii) Sia $0 \neq c \in I \cap \mathbb{Z}$. Allora $c.\mathcal{O}_K \subset I \subset \mathcal{O}_K$. Pertanto $\mathcal{O}_K/I \subset \mathcal{O}_K/c.\mathcal{O}_K$. Sia $\mathcal{O}_K = \omega_1\mathbb{Z} + ... + \omega_n\mathbb{Z}$ dove $(\omega_1, ..., \omega_n)$ è una base intera, allora $\mathcal{O}_K/c.\mathcal{O}_K \simeq (\mathbb{Z}/c\mathbb{Z})^n$ e $\#(\mathcal{O}_K/I)$ è finito.
(iii) Se I è primo $\mathcal{O}_K/I$ è integro. Siccome ogni anello integro finito è un campo, $\mathcal{O}_K/I$ è un campo e quindi I è massimale. □

A questo punto abbiamo raggiunto il nostro scopo:

Corollario 8.4. *L'anello degli interi di un campo di numeri è un anello di Dedekind.*

Dimostrazione. Sia K un campo di numeri. Allora $\mathcal{O}_K$ è noetheriano (Corollario 7.12), integralmente chiuso (Lemma 8.2) e ogni ideale primo è massimale (Lemma 8.3). □

8.2 Dimostrazione del teorema di fattorizzazione.

Ricordiamo il seguente risultato di algebra:

Lemma 8.5. *Sia A un anello integro noetheriano. Se I è un ideale non nullo di A, allora esistono degli ideali primi $\mathfrak{p}_1, ..., \mathfrak{p}_r$ tali che $\mathfrak{p}_1...\mathfrak{p}_r \subset I$.*

Dimostrazione. Nel caso contrario la famiglia degli ideali che non contiene un tale prodotto è non vuota. Siccome A è noetheriano tale famiglia ammette un elemento massimale, J, per l'inclusione. Chiaramente J non è primo quindi esistono $x, y \in A$ tali che $xy \in J$, $x \notin J$ e $y \notin J$. Abbiamo $J \subset J + (x)$ e $J \subset J + (y)$, inclusioni strette. Per massimalità di J, $J + (x)$ e $J + (y)$ contengono ognuno un prodotto di ideali primi. Siccome $xy \in J$, $(J + (x)).(J + (y)) \subset J$, quindi J contiene un prodotto di ideali primi: contraddizione. □

Proposizione 8.6. *Sia A un anello di Dedekind e sia $\mathfrak{p} \subset A$ un ideale primo. Sia $\mathfrak{p}^{-1} := \{x \in K \mid x\mathfrak{p} \subset A\}$ (K il campo dei quozienti di A). Per ogni ideale $I \subset A$:*

$$I\mathfrak{p}^{-1} = \{\sum a_i x_i \mid a_i \in I, x_i \in \mathfrak{p}^{-1}\} \neq I.$$

Dimostrazione. Mostriamo per iniziare che $\mathfrak{p}^{-1} \neq A$.

Sia $0 \neq a \in \mathfrak{p}$. Per il Lemma 8.5 (a) contiene un prodotto di ideali primi, prendiamo un prodotto di lunghezza r minimale: $\mathfrak{p}_1...\mathfrak{p}_r \subset (a) \subset \mathfrak{p}$. Esiste i tale $\mathfrak{p}_i \subset \mathfrak{p}$. Altrimenti $\forall i, \exists a_i \in \mathfrak{p}_i \setminus \mathfrak{p}$, ma $a_1..a_r \in \mathfrak{p}$ e $\mathfrak{p}$ è primo quindi $a_j \in \mathfrak{p}$ per qualche j: contraddizione. Siccome $\mathfrak{p}_i$ è massimale $\mathfrak{p}_i = \mathfrak{p}$. Possiamo assumere $i = 1$. Quindi $\mathfrak{p}_2...\mathfrak{p}_r \not\subset (a)$ ed esiste $b \in \mathfrak{p}_2...\mathfrak{p}_r$ tale che $b \notin aA$. Quindi $a^{-1}b \notin A$. Abbiamo $b\mathfrak{p} \subset (a)$ (perché $\mathfrak{p}\mathfrak{p}_2...\mathfrak{p}_r \subset (a)$), quindi $a^{-1}b\mathfrak{p} \subset A$, cioè $a^{-1}b \in \mathfrak{p}^{-1}$ e quindi $\mathfrak{p}^{-1} \neq A$.

Siano $\alpha_1, ..., \alpha_n$ dei generatori di I. Se $I\mathfrak{p}^{-1} = I$, per ogni $x \in \mathfrak{p}^{-1}$: $x\alpha_i = \sum_j a_{ij}\alpha_j$, $a_{ij} \in A$. Sia M la matrice di coefficienti $(\delta_{ij}x - a_{ij})$. Allora: $M.(\alpha_1, ..., \alpha_n)^t = 0$. Usando la relazione $M^c M = \det M.I_n$ (M^c è la trasposta della matrice dei cofattori) vediamo che $d = \det M$ verifica $d\alpha_i = 0, \forall i$, quindi $d = 0$. Questo implica che x è radice del polinomio caratteristico di M: $\det(\delta_{ij}X - a_{ij}$, questo è un polinomio monico a coefficienti in A, quindi x è intero su A, pertanto $x \in A$. Segue che $\mathfrak{p}^{-1} \subset A$, siccome chiaramente $A \subset \mathfrak{p}^{-1}$, viene $\mathfrak{p}^{-1} = A$ in contraddizione col primo punto della dimostrazione. □

Osserviamo subito alcune conseguenze di questa proposizione. Intanto introduciamo una definizione che rafforzerà l'analogia tra ideali (*numeri ideali*) e numeri:

Definizione 8.7. *Siano $I, J \subset A$ due ideali di un anello. L'ideale I divide J ($I \mid J$) se esiste un ideale $M \subset A$ tale che $IM = J$.*

Osserviamo che $I \mid J$ implica $J \subset I$ (perché $IM \subset I$ essendo I un ideale). In $\mathbb{Z}$ abbiamo: $n \mid m \Leftrightarrow (m) \subset (n)$. Vedremo presto che in un anello di Dedekind: $I \mid J \Leftrightarrow J \subset I$, intanto abbiamo:

Corollario 8.8. *Con le notazioni precedenti, se $\mathfrak{p}$ è primo, $\mathfrak{p}\mathfrak{p}^{-1} = A$.*
Se $I \subset A$ è un ideale qualsiasi e se $\mathfrak{p}$ è primo, abbiamo $\mathfrak{p} \mid I \Leftrightarrow I \subset \mathfrak{p}$. In particolare vale il Lemma di Euclide: se $\mathfrak{p} \mid IJ$, allora $\mathfrak{p} \mid I$ o $\mathfrak{p} \mid J$.

Dimostrazione. Infatti siccome $A \subset \mathfrak{p}^{-1}$, $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1}$. D'altra parte, per definizione, $\mathfrak{p}\mathfrak{p}^{-1} \subset A$. Quindi $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1} \subset A$. Siccome $\mathfrak{p}$ è massimale e $\mathfrak{p} \neq \mathfrak{p}\mathfrak{p}^{-1}$ (Proposizione 8.6), abbiamo $\mathfrak{p}\mathfrak{p}^{-1} = A$.

Se $\mathfrak{p} \mid I$ cioè se $\mathfrak{p}J = I$ per un qualche ideale J, siccome $\mathfrak{p}J \subset \mathfrak{p}$, abbiamo $I \subset \mathfrak{p}$.

Viceversa se $I \subset \mathfrak{p}$, allora $\mathfrak{p}^{-1}I \subset \mathfrak{p}^{-1}\mathfrak{p} = A$, quindi $J = \mathfrak{p}^{-1}I$ è un ideale e $\mathfrak{p}J = \mathfrak{p}\mathfrak{p}^{-1}I = A.I = I$, quindi $\mathfrak{p} \mid I$.
Se $\mathfrak{p} \mid IJ$, allora $IJ \subset \mathfrak{p}$ e questo implica $I \subset \mathfrak{p}$ o $J \subset \mathfrak{p}$ (cioè $\mathfrak{p} \mid I$ o $\mathfrak{p} \mid J$). □

Adesso possiamo dimostrare il teorema di fattorizzazione:

Teorema 8.9. (Dedekind)
Sia A un anello di Dedekind, allora ogni ideale non banale $I \subset A$ si scrive in modo unico come prodotto di ideali primi.

Dimostrazione. Sia $\mathcal{F} = \{I \mid I \subset A$ ideale non banale $(I \neq \{0\}, A)$ che non si scrive come un prodotto di ideali primi $\}$. Se la famiglia $\mathcal{F}$ è non vuota ammette un elemento massimale, J, per l'inclusione (perché?). Esiste un ideale massimale $\mathfrak{p}$ tale $J \subset \mathfrak{p}$. Siccome $A \subset \mathfrak{p}^{-1}$, $J \subset J\mathfrak{p}^{-1}$. Quindi $J \subset J\mathfrak{p}^{-1} \subset \mathfrak{p}\mathfrak{p}^{-1} \subset A$. Siccome $\mathfrak{p}\mathfrak{p}^{-1} = A$ (Corollario 8.8), abbiamo $J \subset J\mathfrak{p}^{-1} \subset A$. Per la Proposizione 8.6, $J \neq J\mathfrak{p}^{-1}$. Abbiamo $J\mathfrak{p}^{-1} \neq \mathfrak{p}\mathfrak{p}^{-1} = A$ perché J è strettamente contenuto in $\mathfrak{p}$. Per massimalità di J l'ideale $J\mathfrak{p}^{-1}$ ammette una fattorizzazione: $J\mathfrak{p}^{-1} = \mathfrak{p}_1...\mathfrak{p}_r$. Quindi $J = J\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}_1...\mathfrak{p}_r\mathfrak{p}$, in contraddizione con l'ipotesi, quindi $\mathcal{F} = \emptyset$. Questo mostra l'esistenza della fattorizzazione.

Per l'unicità si ragiona come in $\mathbb{Z}$ usando l'analogo del Lemma di Euclide (Corollario 8.8). □

Esercizi.

Esercizio 81 *Mostrare che un anello principale è di Dedekind.*
Dare un esempio di un anello fattoriale (UFD) che non sia di Dedekind.

Esercizio 82 *Sia A un anello di Dedekind e $I \subset A$ un ideale (intero). Scopo dell'esercizio è mostrare che I può essere generato da al più due elementi (uno dei quali scelto arbitrariamente).*
(i) Sia $a \in I$, $a \neq 0$, mostrare che l'ideale frazionario $(a)I^{-1} = J$ è intero.
(ii) Si ricorda che in ogni anello commutativo R vale il teorema cinese dei resti*: se I_i, $1 \leq i \leq n$, sono ideali tali che $I_i + I_j = (1)$, $i \neq j$, allora $\cap I_i = \prod I_i$ e $R/I_1 ... I_n \simeq \prod_{i=1}^{n} (R/I_i)$.*
Sia adesso $J = \mathfrak{p}_1^{a_1} ... \mathfrak{p}_r^{a_r}$ un ideale intero qualsiasi. Mostrare che esiste $b \in A$ tale che $b \notin \mathfrak{p}_i I$, $\forall i$. (Sia $\mathfrak{p}_i^{n_i} \parallel I$, considerare $b_i \in \mathfrak{p}_i^{n_i} \setminus \mathfrak{p}_i^{n_i+1}$.)
(iii) Sia J un ideale intero qualsiasi, mostrare che esiste $b \in A$ tali che J e $(b)I^{-1}$ siano primi tra di loro.
(iv) Mostrare che per ogni $a \in I$, $a \neq 0$, esiste b tale che $I = (a, b)$.

Esercizio 83 *Se $K = \mathbb{Q}(\sqrt{-5})$, allora $\mathcal{O}_K = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$.*
Siano $\mathfrak{p} = (2, 1 + \sqrt{-5})$, $\mathfrak{q} = (3, 1 + \sqrt{-5})$, $\mathfrak{r} = (3, 1 - \sqrt{-5})$.
(i) Mostrare che $\mathfrak{p}$ è massimale. Determinare una base intera di $\mathfrak{p}$. Mostrare che $\mathfrak{q}$, $\mathfrak{r}$ sono massimali e $\mathfrak{q} \neq \mathfrak{r}$.
(ii)Mostrare che $(2) = \mathfrak{p}^2$, $(3) = \mathfrak{q}\mathfrak{r}$, $\mathfrak{p}\mathfrak{q} = (1 + \sqrt{-5})$, $\mathfrak{p}\mathfrak{r} = (1 - \sqrt{-5})$.
(iii) In $\mathcal{O}_K$: $6 = 2.3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ sono due fattorizzazioni distinte.
(iv) La fattorizzazione in ideali primi dell'ideale (6) è:

$$(6) = \mathfrak{p}^2 \mathfrak{q}\mathfrak{r}$$

Quindi le due fattorizzazioni di 6 si possono vedere raggruppando in modi diversi i fattori: $(6) = (2)(3) = (\mathfrak{p}^2)(\mathfrak{q}\mathfrak{r})$, o $(6) = (1 + \sqrt{-5})(1 - \sqrt{-5}) = (\mathfrak{p}\mathfrak{q})(\mathfrak{p}\mathfrak{r})$.

9

Il gruppo delle classi.

Si definisce il gruppo delle classi di un anello di Dedekind A (in due modi, la prima definizione può sembrare artificiale, ma è più comoda per lavorare, la seconda è più naturale). Il gruppo delle classi misura in qualche modo quanto A si scosti dall'essere principale, cioè non a fattorizzazione unica (Lemma 9.7).

Si introduce poi il concetto molto importante di norma di un ideale (uno strumento potente quanto la norma degli elementi).

Finalmente si dimostra che il gruppo delle classi di un anello di interi algebrici è finito. Osserviamo che questo è un risultato di natura *aritmetica*: esistono anelli di Dedekind il cui gruppo delle classi non è finito.

9.1 Ideali frazionari e gruppo delle classi.

Se $n \in \mathbb{Z}$ è un intero non nullo, n non è necessariamente invertibile in $\mathbb{Z}$ ma lo è nel campo dei quozienti $\mathbb{Q}$. In modo analogo un ideale I di un anello di Dedekind ha un inverso nell'insieme degli ideali frazionari.

Definizione 9.1. *Sia A un anello integro e sia K il suo campo dei quozienti. Un ideale frazionario di A è un sotto A-modulo di K, I, tale che esista $d \in A$ con $I \subset d^{-1}A$ (cioè $dI \subset A$).*

Osservare che dI è un ideale di A. Se $x \in I$ allora $x = a/d, a \in A$: gli elementi di I hanno d come denominatore comune. Un ideale (usuale) $I \subset A$ è un ideale frazionario con $d = 1$, si dice allora che I è un *ideale intero* (come in $\mathbb{Z}$ e $\mathbb{Q}$ abbiamo gli interi e le frazioni).

Si definisce il prodotto di due ideali frazionari come nel caso "intero". Se J_K indica l'insieme degli ideali frazionari abbiamo:

Proposizione 9.2. *L'insieme J_K è un gruppo abeliano per la moltiplicazione degli ideali frazionari. Il gruppo J_K viene chiamato il gruppo degli ideali di A. L'inverso dell'ideale frazionario I è:*

$$I^{-1} := \{x \in K \mid xI \subset A\}.$$

Dimostrazione. Abbiamo chiaramente l'associatività e la commutatività, inoltre $I.(1) = I, \forall I \in J_K$. Il problema è l'inverso, iniziamo con gli ideali interi.

Se $\mathfrak{p}$ è un ideale intero primo, abbiamo già visto (Corollario 8.8) che $\mathfrak{p}\mathfrak{p}^{-1} = (1)$. Se I è un ideale intero qualsiasi allora $I = \mathfrak{p}_1 ... \mathfrak{p}_r$ (Teorema 8.9) e $I^{-1} = \mathfrak{p}_1^{-1} ... \mathfrak{p}_r^{-1}$.

Sia adesso I un ideale frazionario con $dI \subset A, d \in A$. Mostriamo che: $(dI)^{-1} = d^{-1}I^{-1}$.
$d^{-1}I^{-1} \subset (dI)^{-1}$: sia $x \in I^{-1}$, allora $\forall y \in I \ \frac{x}{d}dy = xy \in A$, quindi $d^{-1}x \in (dI)^{-1}$.
$(dI)^{-1} \subset d^{-1}I^{-1}$: sia $z \in (dI)^{-1}$, allora $\forall y \in I$, $zdy \in A$. Abbiamo $z = (zd)/d$ e $zd \in I^{-1}$, quindi $z \in d^{-1}I^{-1}$.

Se I è frazionario con $dI \subset A$, allora $J = dI$ è intero e il suo inverso è $(dI)^{-1}$. Da quanto precede $(dI)^{-1} = d^{-1}I^{-1}$. Quindi $(d^{-1}I^{-1})(dI) = (1)$. Ma $(d^{-1}I^{-1})(dI) = I^{-1}I$, quindi $I^{-1}I = (1)$. □

La fattorizzazione può essere estesa agli ideali frazionari:

Teorema 9.3. *Sia A un anello di Dedekind. Ogni ideale frazionario I di A si scrive in modo unico come un prodotto di ideali primi interi:*

$$I = \prod \mathfrak{p}_i^{n_i},\ n_i \in \mathbb{Z}$$

Inoltre se I, J sono due ideali frazionari: $I \mid J \Leftrightarrow J \subset I$.

Dimostrazione. Segue dal Teorema di fattorizzazione di Dedekind perché se I è un ideale frazionario con $dI \subset A$, allora $I = (dI).(d)^{-1}$ è un quoziente di due ideali interi, ognuno di questi ideali si fattorizza in modo unico. Inoltre due quozienti di ideali interi $J/M = J'/M'$ portano alla stessa fattorizzazione.

Basta mostrarlo per gli ideali interi: se $I = \prod p_i^{a_i}$, allora $J \mid I \Leftrightarrow J = \prod p_i^{b_i}$ con $b_i \leq a_i \Leftrightarrow I \subset J$. □

Segue che J_K è il gruppo abeliano libero sull'insieme degli ideali primi interi di A.

L'insieme degli ideali principali $x.A$ per $x \in K^*$ forma un sotto gruppo di J_K. Osserviamo che $x.A = y.A \Leftrightarrow x$ e y sono associati, cioè esiste $a \in A$ invertibile tale che $x = ay$. Infatti abbiamo $x = by$ e $ax = y, a, b \in A$, quindi $x = bax$ ossia $x(1 - ab) = 0$ quindi $ab = 1$. Il viceversa è chiaro.

Definizione 9.4. *Il gruppo degli ideali principali P_K è $K^*/A^\times$ dove $A^\times$ indica il gruppo degli elementi invertibili (o* unità*) di A.*

Il gruppo delle classi *di K (o A) è $Cl_K := J_K/P_K$.*

Il gruppo delle classi Cl_K misura "quanti" ideali non principali esistono, cioè quanto A si scosta dall'essere principale, questo è forse più chiaro con la presentazione della Sezione 9.2.

9.2 Il gruppo delle classi: take two.

Un'altra presentazione del gruppo delle classi di un anello di Dedekind A con campo dei quozienti K.

Sia $\mathcal{I}$ l'insieme degli ideali (interi) di A. Su $\mathcal{I}$ si definisce la seguente relazione: $I \sim J \Leftrightarrow \exists\, a, b \in A$ tali che: $(a)I = (b)J$. Abbiamo chiaramente che $\sim$ è riflessiva e simmetrica, per la transitività: se $(a)I = (b)J$ e $(c)J = (d)M$, allora $(ac)I = (bd)M$. Infatti se $x \in I$, $ax = bj$, $cj = dm$, quindi $acx = bcj = bdm$, quindi $(ac)I \subset (bd)M$; nello stesso modo si ottiene l'inclusione inversa.

Quindi $\sim$ è una relazione d'equivalenza su $\mathcal{I}$.

Lemma 9.5. *Con le notazioni precedenti: $I \sim (1) \Leftrightarrow I$ è principale.*

Dimostrazione. Chiaramente ogni ideale principale è equivalente a (1). Viceversa se $I \sim (1)$, abbiamo $(a)I = (b)(1) = (b)$, quindi $b = az$ con $z \in I$. Mostriamo che $I = (z)$. Abbiamo $(z) \subset I$ perché $z \in I$. Viceversa se $x \in I$, $ax = bu$ per un qualche $u \in A$, cioè $ax = azu$, quindi $a(x - zu) = 0$, siccome A è integro e $a \neq 0$, $x = zu$, pertanto $I \subset (z)$. □

Il prodotto degli ideali passa al quoziente, cioè se $\overline{I}$ indica la classe di I nell'insieme quoziente $\mathcal{I}/\sim$, abbiamo: $\overline{I}.\overline{J} = \overline{IJ}$. Infatti se $I \sim I'$, $J \sim J'$, bisogna mostrare che $\overline{I'J'} = \overline{IJ}$. Sia $(a)I' = (b)I, (c)J' = (d)J$ e sia $\sum x_i y_i \in IJ, x_i \in I, y_i \in J$, allora $bd\sum x_i y_i = \sum bx_i dy_i = \sum ax_i' cy_i' = ac\sum x_i' y_i'$, quindi $(bd)IJ \subset (ac)I'J'$, nello stesso modo si ottiene l'inclusione inversa e quindi $IJ \sim I'J'$.

Proposizione 9.6. *Sia A un anello di Dedekind, il prodotto induce su $\mathcal{I}/\sim$ una struttura di gruppo e $\varphi : Cl_K \to \mathcal{I}/\sim$: $[I] \to \overline{dI}$ è un isomorfismo di gruppi (qui se I è un ideale frazionario, $d \in A$ è tale che $dI \subset A$ e $[I]$ indica la classe di I in Cl_K).*

Dimostrazione. Vediamo intanto che $(\mathcal{I}/\sim, .)$ è un gruppo. L'unica cosa da mostrare è l'esistenza del simmetrico. Sia $I \in \mathcal{I}$, abbiamo $I.I^{-1} = (1)$, dove I^{-1} è l'ideale frazionario $\{x \in K \mid xI \subset A\}$ (Proposizione 9.2). Siccome I^{-1}

è frazionario esiste $d \in A$ tale $J = dI^{-1}$ sia un ideale di A. Quindi $IJ = (d)$. Per il Lemma 9.5, $\overline{IJ} = \overline{(1)}$, quindi $\overline{J}$ è l'inverso di $\overline{I}$.

Mostriamo adesso che $\varphi : Cl_K \to \mathcal{I}/\sim: [I] \to \overline{dI}$ è un isomorfismo di gruppi.

L'applicazione φ è ben definita: intanto la scelta del denominatore è ininfluente: se $dI = J$, $d'I = J'$, allora $(d')J = (d)J'$ quindi $\overline{J} = \overline{J'}$. Siano adesso I, J due ideali frazionari: $I = dI.(d)^{-1}$, $J = tJ.(t)^{-1}$. Se $[I] = [J]$, allora $IJ^{-1} = (x) = (mn^{-1})$, dove $x = m/n \in K$. Abbiamo: $IJ^{-1} = dI.(d)^{-1}.J^{-1} = (mn^{-1})$, quindi: $dI.(n) = J.(dm) = tJ.(t)^{-1}.(dm)$; finalmente: $dI.(nt) = tJ.(dm)$, quindi $dI \sim tJ$ ossia $\overline{dI} = \overline{tJ}$.

L'applicazione φ è un morfismo di gruppi e chiaramente suriettiva. Finalmente φ è iniettiva perché $\varphi([I]) = \overline{(1)}$ implica $dI = (a)$ cioè $I = (x)$ con $x = a/d$. □

Questa presentazione del gruppo delle classi Cl_K (o Cl_A) che utilizza solo gli ideali di A mostra che il gruppo delle classi misura quanto A si scosti dall'essere principale e quindi quanto venga a mancare la fattorizzazione unica:

Lemma 9.7. *Un anello di Dedekind è fattoriale (UFD) se e solo se è principale.*

Dimostrazione. Abbiamo già visto che un anello principale è fattoriale. Sia quindi A un anello di Dedekind fattoriale e mostriamo che A è principale. Basta mostrare che ogni ideale primo $\mathfrak{p}$ è principale. Sia $0 \neq a \in \mathfrak{p}$ e sia $a = p_1...p_r$ la sua fattorizzazione in elementi primi. Siccome $\mathfrak{p}$ è primo, da $a = p_1...p_r \in \mathfrak{p}$, segue che esiste i tale che $p_i \in \mathfrak{p}$. Quindi $(p_i) \subset \mathfrak{p}$. L'ideale (p_i) è primo (se $ab \in (p_i)$, $p_i \mid ab$, quindi $p_i \mid a$ o $p_i \mid b$, cioè $a \in (p_i)$ o $b \in (p_i)$). In un anello di Dedekind ogni ideale primo è massimale, quindi $(p_i) = \mathfrak{p}$. □

9.3 Norma di un ideale.

Abbiamo visto che se K è un campo di numeri e se $I \subset \mathcal{O}_K$ è un ideale, allora $\#(\mathcal{O}_K/I)$ è finito (Lemma 8.3). Questo giustifica la seguente:

Definizione 9.8. *Sia $I \subset \mathcal{O}_K$ dove K è un campo di numeri allora la* norma *dell'ideale I è: $N(I) := \#(\mathcal{O}_K/I)$.*

Se $\mathfrak{p} \subset \mathcal{O}_K$ è un ideale primo non nullo, $\mathfrak{p} \cap \mathbb{Z}$ è un ideale non nullo (Lemma 7.9) ovviamente primo. Se $\mathfrak{p} \cap \mathbb{Z} = (p)$, $(p) \subset \mathfrak{p}$ e $\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_K/(p)$. Osserviamo che p è l'unico numero primo contenuto in $\mathfrak{p}$; si dice che $\mathfrak{p}$ è *sopra* p (e p sotto $\mathfrak{p}$). Quindi ogni ideale primo $\mathfrak{p}$ sta sopra un unico numero primo p (ma un numero primo p può stare sotto diversi ideali primi).

Siccome $\mathfrak{p}$ è massimale, $\mathcal{O}_K/\mathfrak{p}$ è un campo (finito). Siccome $\mathcal{O}_K/(p)$ è un $\mathbb{F}_p = \mathbb{Z}/(p)$-modulo, la caratteristica di $\mathcal{O}_K/\mathfrak{p}$ è p, quindi $\#(\mathcal{O}_K/\mathfrak{p}) =: N(\mathfrak{p}) = p^f$.

Lemma 9.9. *Sia K un campo di numeri e sia $\mathfrak{p} \subset \mathcal{O}_K$ un ideale primo, allora $N(\mathfrak{p}^e) = N(\mathfrak{p})^e$.*

Dimostrazione. La dimostrazione è per induzione su e, il caso $e = 1$ è chiaro.

Abbiamo $\mathfrak{p} \supset \mathfrak{p}^2 \supset ... \supset \mathfrak{p}^n \supset ...$ con $\mathfrak{p}^i \neq \mathfrak{p}^{i+1}$ (unicità della fattorizzazione).

Osserviamo che $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ è un $k := \mathcal{O}_K/\mathfrak{p}$-spazio vettoriale, inoltre la sua dimensione è uno.

Vediamo questo ultimo punto: sia $F \subset \mathfrak{p}^i/\mathfrak{p}^{i+1}$ un k sotto-spazio vettoriale. Sia $\overline{a} \in F$ un elemento non nullo, quindi $a \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$. Sia $I = (a)+\mathfrak{p}^{i+1}$, allora $\mathfrak{p}^i \supset I \supset \mathfrak{p}^{i+1}$, $I \neq \mathfrak{p}^{i+1}$. Mostriamo che $I = \mathfrak{p}^i$. Se non fosse così $I' = I\mathfrak{p}^{-i}$ sarebbe un divisore proprio di $\mathfrak{p} = \mathfrak{p}^{i+1}\mathfrak{p}^{-i}$ (se $\mathfrak{p}^i \neq I$, $I' \neq (1)$ e $I' \mid \mathfrak{p}$ perché $\mathfrak{p}^{i+1} \subset I$ quindi $I \mid \mathfrak{p}^{i+1}$, $I' = I\mathfrak{p}^{-i}$). Quindi $F = \mathfrak{p}^i/\mathfrak{p}^{i+1}$, cioè $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ non ha sotto spazi propri, quindi ha dimensione uno.

Si conclude con la successione di $k = \mathcal{O}_K/\mathfrak{p}$-spazi vettoriali

$$0 \to \mathfrak{p}^i/\mathfrak{p}^{i+1} \to \mathcal{O}_K/\mathfrak{p}^{i+1} \to \mathcal{O}_K/\mathfrak{p}^i \to 0$$

□

Lemma 9.10. *Siano I, J due ideali frazionari dell'anello di Dedekind A. Il massimo comune divisore (M.C.D.) di I e J è $I + J$; il minimo comune multiplo (m.c.m.) è $I \cap J$. In particolare se $\mathfrak{p}, \mathfrak{q}$ sono due ideali interi primi distinti $\mathfrak{p} + \mathfrak{q} = (1)$.*

Dimostrazione. Siccome $I \subset I + J$, $I + J \mid I$, nello stesso modo $I + J \mid J$. Se $M \mid I$ e $M \mid J$, allora $I \subset M$ e $J \subset M$, quindi $I + J \subset M$ e $M \mid I + J$, pertanto $(I, J) = I + J$.
Nello stesso modo si mostra che $I \cap J$ è il m.c.m. di I e J.
L'ultima affermazione segue dalla fattorizzazione unica. □

Proposizione 9.11. *Sia K un campo di numeri e $I \subset \mathcal{O}_K$ un ideale. Se $I = \prod \mathfrak{p}_i^{e_i}$, allora $N(I) = \prod N(\mathfrak{p}_i)^{e_i}$.*

In particolare se $I, J \subset \mathcal{O}_K$ sono due ideali: $N(IJ) = N(I).N(J)$ e se $I \mid J$ allora $N(I) \mid N(J)$.

Dimostrazione. Per il Teorema cinese dei resti: $\mathcal{O}_K/I \simeq \prod \mathcal{O}_K/\mathfrak{p}_i^{e_i}$, si conclude con il Lemma 9.9. □

Il risultato seguente è molto utile nella pratica:

Corollario 9.12. *Se $N(I) = p$, p un numero primo, allora l'ideale I è primo.*

Dimostrazione. Esercizio 84.

Proposizione 9.13. *Sia K un campo di numeri e $I \subset \mathcal{O}_K$ un ideale, allora I divide l'ideale principale $N(I).\mathcal{O}_K$.*

Per ogni intero $m > 0$, l'insieme degli ideali $I \subset \mathcal{O}_K$ con $N(I) = m$ è finito.

Dimostrazione. Abbiamo $m = N(I) = \#(\mathcal{O}_K/I)$, quindi se $\alpha \in \mathcal{O}_K$, l'ordine di $\overline{\alpha}$ in $\mathcal{O}_K/I$ divide m (teorema di Lagrange), quindi $m\alpha \in I$, pertanto $(m) \subset I$, quindi $I \mid (m)$.

Sia $m > 0$ un intero. Abbiamo visto che se $N(I) = m$, allora $I \mid (m)$, ma l'ideale (m) ha un numero finito di divisori (considerare la fattorizzazione di (m) in ideali primi). □

Prima di dimostrare i prossimi risultati ricordiamo un risultato di algebra:

Proposizione 9.14. *Sia A un anello principale e sia M un A-modulo libero di rango n. Sia $N \subset M$ un sotto A-modulo. Allora N è libero di rango $m \leq n$. Inoltre esiste una base $(e_1, ..., e_n)$ di M e degli elementi $d_1, ..., d_m \in A$, tali che $(d_1e_1, ..., d_me_m)$ sia una base di N. I d_i possono essere scelti di modo che $d_i \mid d_{i+1}$.*

Si ricorda che se $I \subset \mathcal{O}_K$ è un ideale, il discriminante di I, d_I, è il discriminante di una qualsiasi basi intera di I.

Lemma 9.15. *Sia $I \subset \mathcal{O}_K$ un ideale non nullo, allora:*

$$N(I)^2 = \frac{d_I}{D_K}$$

dove d_I è il discriminante di I e dove D_K è il discriminante di K.

Dimostrazione. Sia $(\alpha_1, ..., \alpha_n)$ una base intera di $\mathcal{O}_K$. Siccome $I \subset \mathcal{O}_K$ è un $\mathbb{Z}$ sotto modulo libero di rango n, per la Proposizione 9.14, esistono degli interi $d_i \in \mathbb{Z}$, tali che $(d_1\alpha_1, ..., d_n\alpha_n)$ sia una base intera di I.

Segue che $\mathcal{O}_K/I \simeq \prod \mathbb{Z}/d_i\mathbb{Z}$ (isomorfismo di $\mathbb{Z}$-moduli). Quindi $N(I) = \#(\mathcal{O}_K/I) = |d_1...d_n|$.

D'altra parte

$$d_I = disc(d_1\alpha_1, ..., d_n\alpha_n) = \det(\sigma_i(d_j\alpha_j))^2 = (d_1...d_n)^2 \det(\sigma_i(\alpha_j))^2$$

$$= (d_1...d_n)^2 disc(\alpha_1, ..., \alpha_n) = (d_1...d_n)^2 D_K$$

cioè $d_I = N(I)^2.D_K$. □

Il lemma che segue è molto utile:

Lemma 9.16. *Sia $\alpha \in \mathcal{O}_K$, allora $N(\alpha.\mathcal{O}_K) = |N(\alpha)|$.*

Dimostrazione. Sia $(\alpha_1, ..., \alpha_n)$ una base intera di $\mathcal{O}_K$. Allora $(\alpha\alpha_1, ..., \alpha\alpha_n)$ è una base intera dell'ideale (α).

Per il Lemma 9.15: $N((\alpha))^2 = \dfrac{disc(\alpha\alpha_1, ..., \alpha\alpha_n)}{D_K}$.

Abbiamo $disc(\alpha\alpha_j) = \det(\sigma_i(\alpha\alpha_j))^2 = \det(\sigma_i(\alpha)\sigma_i(\alpha_j))^2$. Siccome:

$$(\sigma_i(\alpha)\sigma_i(\alpha_j)) = \begin{pmatrix} \sigma_1(\alpha) & & \\ & \ddots & \\ & & \sigma_n(\alpha) \end{pmatrix} \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \cdots & \sigma_1(\alpha_n) \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ \sigma_n(\alpha_1) & & & \sigma_n(\alpha_n) \end{pmatrix}$$

viene $disc(\alpha\alpha_j) = (\prod \sigma_i(\alpha))^2 \det(\sigma_i(\alpha_j)^2 = N(\alpha)^2 D_K$. Quindi $N((\alpha))^2 = N(\alpha)^2$. Siccome $N((\alpha)) > 0$, $N((\alpha)) = |N(\alpha)|$. □

9.4 Il gruppo delle classi è finito (Dirichlet).

Abbiamo tutto in mano per mostrare che il gruppo delle classi $Cl_K = \mathcal{I}/\sim$ è finito, questo sarà una conseguenza di:

Proposizione 9.17. *Per ogni campo di numeri K esiste $\mu \in \mathbb{R}$ (che dipende solo da K) tale che per ogni ideale $I \subset \mathcal{O}_K$ esista $\alpha \in I$ con*

$$|N(\alpha)| \leq \mu.N(I).$$

Infatti con questa proposizione otteniamo subito:

Corollario 9.18. *Ogni classe di $Cl_K = \mathcal{I}/\sim$ contiene un ideale I con $N(I) \leq \mu$ (lo stesso μ della Proposizione 9.17).*

Dimostrazione. Sia $J \subset \mathcal{O}_K$ un ideale qualsiasi e sia $b \in \mathcal{O}_K$ tale che $bJ^{-1} \subset \mathcal{O}_K$. Per la Proposizione 9.17 esiste $a \in bJ^{-1}$ tale che: $|N(a)| \leq \mu.N(bJ^{-1})$ $(*)$. Sia $I = (ab^{-1})J$, abbiamo $(b)I = (a)J$ quindi $I \sim J$. Abbiamo: $(a) = (ab^{-1})J.(bJ^{-1}) = I.(bJ^{-1})$. Quindi $N((a)) = N(I).N(bJ^{-1})$ (Proposizione 9.11). D'altra parte $N((a)) = |N(a)|$ (Lemma 9.16). Quindi abbiamo: $|N(a)| = N(I).N(bJ^{-1})$. Combinando con $(*)$: $N(I) \leq \mu$. □

Teorema 9.19. (Dirichlet)
Per ogni campo di numeri K il gruppo delle classi Cl_K è finito.

Dimostrazione. Per la Proposizione 9.13 esistono un numero finito di ideali $J_1, ..., J_k$ con $N(J_i) \leq \mu$, per il Corollario 9.18, il numero delle classi è finito. □

Definizione 9.20. *Sia K un campo di numeri, il numero delle classi (*class number*) è $h_K := \#(Cl_K)$. L'anello degli interi di K, $\mathcal{O}_K$, è principale (e quindi fattoriale) se e solo se $h_K = 1$.*

Rimane da dimostrare la Proposizione 9.17.

Dimostrazione (della Proposizione 9.17).
Sia $(\alpha_1, ..., \alpha_n)$ una base intera di $\mathcal{O}_K$ e sia $I \subset \mathcal{O}_K$. Prendiamo $t \in \mathbb{N}$ tale che: $t^n \leq N(I) < t^{n+1}$. Sia $S = \{\sum_{i=1}^{n} d_i\alpha_i \mid d_i \in \mathbb{N}, 0 \leq d_i \leq t\}$. Siccome $\#(S) = t^{n+1} > N(I) = \#(\mathcal{O}_K/I)$, per il principio dei cassetti, esistono $\alpha, \beta \in S$, $\alpha \neq \beta$, tali che $\gamma = \alpha - \beta = \sum_i a_i\alpha_i \in I$. Osserviamo che $|a_i| \leq t$. Abbiamo:

$$N(\gamma) = \prod_{i=1}^{n} \sigma_i(\sum_{j=1}^{n} a_j\alpha_j) = \prod_{i=1}^{n}(\sum_{j=1}^{n} a_j\sigma_i(\alpha_j))$$

Prendendo il valore assoluto in $\mathbb{C}$ ($|z| := \sqrt{z\overline{z}}$ dove $\overline{z}$ è il coniugato complesso di $z \in \mathbb{C}$):

$$|N(\gamma)| = \prod_{i=1}^{n}(|\sum_{j=1}^{n} a_j\sigma_i(\alpha_j)|) \leq \prod_{i=1}^{n}(\sum_{j=1}^{n} |a_i|.|\sigma_i(\alpha_j)|) \leq \prod_{i=1}^{n}(\sum_{j=1}^{n} t.|\sigma_i(\alpha_j)|)$$

Quindi $|N(\gamma)| \leq t^n.\mu$, dove $\mu = \prod_{i=1}^{n}(\sum_{j=1}^{n} |\sigma_i(\alpha_j)|)$. Siccome $t^n \leq N(I)$, abbiamo la relazione cercata: $|N(\gamma)| \leq \mu N(I)$. □

La dimostrazione del Teorema 9.19 è completa. Vediamo con un esempio come (in certi casi) si può rendere effettivi gli argomenti della dimostrazione precedente.

Esempio 9.21. Se $K = \mathbb{Q}(\sqrt{d})$ con $d > 0$, $d \equiv 2, 3 \pmod 4$, abbiamo $\mu = 1 + d + 2\sqrt{d}$. Per esempio se $d = 2$, $\mu = 5, 8...$ e ogni classe contiene un ideale I con $N(I) \leq 5$.

Abbiamo $N((\sqrt{2})) = |N(\sqrt{2})| = 2$, quindi $(\sqrt{2})$ è primo (Corollario 9.12). Siccome $(2) = (\sqrt{2})^2$ questa è la fattorizzazione dell'ideale (2). Se $N(I) = 2$ allora I è primo e $I \mid (2)$ (Proposizione 9.13), quindi $I = (\sqrt{2})$. Questo mostra che l'unico ideale di norma 2 è $(\sqrt{2})$.

Se $N(I) = 4$, allora $I \mid (4) = (\sqrt{2})^4$, quindi $I = (\sqrt{2})^a$ e $N(I) = 2^a$ cioè $I = (2)$.

Si vede poi che gli ideali $(3), (5)$ sono primi (Esercizio 86). Se $N(I) = 3$, $I \mid (3)$, quindi $I = (3)$ e $N(I) = 9$, contraddizione: non esiste nessun ideale di norma 3. Nello stesso modo non esiste nessun ideale di norma 5.

In conclusione gli ideali di norma ≤ 5 sono: $(1), (2), (\sqrt{2})$; sono tutti principali quindi $h_k = 1$ e $\mathcal{O}_K$ è principale ($K = \mathbb{Q}(\sqrt{2})$).

Osservazione 9.22. E' possibile ottenere una limitazione migliore nella Proposizione 9.17 (Teorema di Minkowski, 11.16).

Esercizi.

Esercizio 84 *Sia $I \subset \mathcal{O}_K$ un ideale con $N(I) = p$, p primo. Mostrare che I è un ideale primo.*

Esercizio 85 *Sia $I = (2, 1 + \sqrt{-5}) \subset \mathcal{O}_K$, $K = \mathbb{Q}(\sqrt{-5})$. Determinare d_I e quindi $N(I)$. Se non lo avete già fatto nell'Esercizio 83 ritrovate questo risultato direttamente. Concludere che I è primo.*

Esercizio 86 *Mostrare che gli ideali (3), (5) di $\mathbb{Z}[\sqrt{2}]$ sono ideali primi.*

Esercizio 87 *Sia K un campo di numeri e $\mathfrak{p} \subset \mathcal{O}_K$ un ideale primo.*
(i) Mostrare che $N(\mathfrak{p}) \geq 2$. Dare un esempio dove l'uguaglianza è raggiunta.
(ii) Concludere che per ogni ideale proprio $I \subset \mathcal{O}_K$, $N(I) > 1$.

Esercizio 88 *Sia $K/\mathbb{Q}$ un campo di numeri di grado n ($[K : \mathbb{Q}] = n$). Se $p \in \mathbb{N}$ è un numero primo, l'ideale $p.\mathcal{O}_K =: (p)$ non è necessariamente primo in $\mathcal{O}_K$. Per il teorema di fattorizzazione abbiamo però: $(p) = \mathfrak{p}_1^{e_1} ... \mathfrak{p}_g^{e_g}$.*

Quindi $\mathfrak{p}_i \mid (p)$, cioè $(p) \subset \mathfrak{p}_i$.
(i) Mostrare che $N(\mathfrak{p}_i) = p^{f_i}$.
(ii) Concludere che $\sum_{i=1}^{g} e_i f_i = n$ (si dice che f_i è il grado *di $\mathfrak{p}_i$ e e_i è* l'indice di ramificazione *di $\mathfrak{p}_i$). In particolare $g \leq n$.*
(iii) Se K è un campo quadratico ($n = 2$) abbiamo le seguenti possibilità:

- *$g = 2$, $e_1 = e_2 = 1$, $f_1 = f_2 = 1$, $(p) = \mathfrak{p}_1.\mathfrak{p}_2$, $\mathfrak{p}_1 \neq \mathfrak{p}_2$, $N(\mathfrak{p}_i) = p$. In questo caso si dice che p è* decomposto.
- *$g = 1$, $e = 2$, $f = 1$: $(p) = \mathfrak{p}$, con $N(\mathfrak{p}) = p^2$; in questo caso l'ideale (p) è ("rimane") primo; si dice che p è* inerte.
- *$g = 1, e = 1, f = 2$: $(p) = \mathfrak{p}^2$, $N(\mathfrak{p}) = p$; in questo caso si dice che p è* ramificato.

Sia $\sigma : K \to K : x + y\sqrt{d} \to x - y\sqrt{d}$ il coniugo. Sia p un primo non inerte: $(p) = \mathfrak{p}_1\mathfrak{p}_2$. Mostrare che $\sigma(\mathfrak{p}_1) = \mathfrak{p}_2$. In particolare se (p) è ramificato $(p) = \mathfrak{p}^2$, allora $\sigma(\mathfrak{p}) = \mathfrak{p}$. Per esempio 2 è ramificato in $\mathbb{Q}(\sqrt{-5})$ mentre 3 non lo è (cf Esercizio 83).

10

Il teorema delle unità di Dirichlet.

Due elementi α, β di $\mathcal{O}_K$ sono associati se e solo se $(\alpha) = (\beta)$. Quindi quando consideriamo gli ideali (usando per esempio il teorema di fattorizzazione) ignoriamo le unità. Alcune proprietà aritmetiche (o la risoluzione di equazioni diofantee) dipendono invece dalle unità di $\mathcal{O}_K$. L'insieme delle unità di $\mathcal{O}_K$ è un gruppo moltiplicativo che denoteremo con U_K.

10.1 Il sotto gruppo W_K delle radici dell'unità.

Ricordiamo intanto una caratterizzazione delle unità:

Lemma 10.1. *Sia $\alpha \in \mathcal{O}_K$, allora α è un'unità $\Leftrightarrow N(\alpha) = \pm 1$.*

Dimostrazione. Se $\alpha \in \mathcal{O}_K$ è un'unità allora esiste $\beta \in \mathcal{O}_K$ tale $\alpha\beta = 1$. Quindi $N(\alpha)N(\beta) = 1$, quindi $N(\alpha)$ è un intero invertibile, pertanto $N(\alpha) = \pm 1$.

Viceversa supponiamo $N(\alpha) = \pm 1$. Sia $\beta = \prod_{\sigma \neq Id} \sigma(\alpha)$ il prodotto dei coniugati di α per $\sigma \neq Id$. Per definizione della norma: $N(\alpha) = \alpha\beta$. Quindi $\alpha\beta = \pm 1$. Ogni $\sigma(\alpha) \in \mathcal{O}$, quindi $\beta \in \mathcal{O}$. Siccome $\beta = N(\alpha)/\alpha$, $\beta \in K$. Segue che $\beta \in \mathcal{O}_K$. Quindi α è invertibile in $\mathcal{O}_K$. □

Se $\xi \in \mathbb{C}$ è una radice dell'unità (cioè $\xi^m = 1$ per un qualche m), allora $\xi \in \mathcal{O}$. Se $\xi \in K$, allora $\xi \in \mathcal{O}_K$. Siccome $\xi^{m-1} = \xi^{-1}$, $\xi^{-1} \in \mathcal{O}_K$ e $\xi \in U_K$: *ogni radice dell'unità contenuta in K è un'unità di $\mathcal{O}_K$*. Siccome $\pm 1 \in K$, ci sono sempre almeno due radici dell'unità in K.

Definizione 10.2. *Indicheremo con $W_K \subset U_K$ il sotto gruppo costituito da radici dell'unità.*

Mostriamo che W_K è finito, ciclico.

Proposizione 10.3. *Sia $c \in \mathbb{R}$, $c > 0$. Sia K un campo di numeri di grado n e indichiamo con σ_i, $1 \leq i \leq n$, le n $\mathbb{Q}$-immersioni di K in $\overline{\mathbb{Q}}$. Sia $C = \{\alpha \in \mathcal{O}_K \mid |\sigma_i(\alpha)| < c, \forall i\}$. Allora C è un insieme finito.*

Dimostrazione. Siano $s_1 = X_1 + \cdots + X_n$, ..., $s_n = X_1 ... X_n$ gli n polinomi simmetrici elementari in n variabili. Sia T l'insieme dei polinomi monici, di grado $\leq n$, i cui coefficienti siano interi a con $|a| \leq c'$, dove c' è un numero reale sufficientemente grande.

Se $|\sigma_i(\alpha)| \leq c$, allora $|s_k(\sigma_1(\alpha), ..., \sigma_n(\alpha))| \leq c'$. Siccome i $s_k(\sigma_1(\alpha), ..., \sigma_n(\alpha))$ sono i coefficienti del polinomio caratteristico di α e siccome $\alpha \in \mathcal{O}_K$, $s_k(\sigma_1(\alpha), ..., \sigma_n(\alpha)) \in \mathbb{Z}$. Quindi α è radice di un polinomio in T. Siccome T è chiaramente un insieme finito, c'è un numero finito di possibilità per α. □

Corollario 10.4. *Con le notazioni della Proposizione 10.3, un elemento $\alpha \in K$ è una radice dell'unità se e solo se $\alpha \in \mathcal{O}_K$ e $|\sigma_i(\alpha)| = 1$, $i = 1, ..., n$.*

Dimostrazione. Se $\alpha \in K$ è una radice dell'unità abbiamo già visto che $\alpha \in \mathcal{O}_K$. Abbiamo $\alpha^m = 1$ per un qualche m, quindi $(\sigma_i(\alpha))^m = 1$. Pertanto $|\sigma_i(\alpha)| = 1$.

Viceversa, per la Proposizione 10.3 c'è un numero finito di elementi di $\mathcal{O}_K$ tali che $|\sigma_i(\alpha)| = 1, \forall i$. Inoltre se α è un tale elemento anche $\alpha^2, ..., \alpha^r, ...$ verificano $|\sigma_i(\alpha^r)| = 1, \forall i$. Quindi esistono $r, t, r \neq t$ tali che $\alpha^t = \alpha^r$, segue che $\alpha^{r-t} = 1$. □

Finalmente abbiamo:

Proposizione 10.5. *Il gruppo moltiplicativo W_K è ciclico, finito, di ordine pari.*

Dimostrazione. Per la Proposizione 10.3 e il Corollario 10.4, W_K è finito. Se t è l'ordine di W_K, ogni elemento $\alpha \in W_K$ verifica $\alpha^t = 1$, quindi W_K è contenuto nel gruppo ciclico delle radici t-esime dell'unità, pertanto W_K è ciclico. Finalmente siccome $\pm 1 \in W_K$, l'ordine di W_K è pari. □

10.2 Il teorema delle unità di Dirichlet.

Sia K un campo di numeri di grado n e siano $\sigma_1, ..., \sigma_n$ le n $\mathbb{Q}$-immersioni di K in $\overline{\mathbb{Q}}$. I campi $\sigma_i(K) \subset \overline{\mathbb{Q}}$ sono i (campi) *coniugati* di K.

Definizione 10.6. *Un campo coniugato di K, $\sigma_i(K)$, è detto* reale *se $\sigma_i(K) \subset \mathbb{R}$, altrimenti $\sigma_i(K)$ è detto* immaginario *(o non reale).*

Il morfismo σ_i è detto reale (risp. immaginario) se $\sigma_i(K)$ è reale (risp. immaginario).

Se $z = x + iy$ è un numero complesso il suo coniugato (complesso) è $\tau(z) = \overline{z} = x - iy$. Siccome $\tau : \mathbb{C} \to \mathbb{C}$ è un $\mathbb{R}$-morfismo di campi, se K è un campo di numeri $\tau(K)$ è un coniugato (algebrico) di K. In particolare $\tau \circ \sigma_i = \sigma_j$. Se σ_i è reale, $\tau \circ \sigma_i = \sigma_i$, invece se $\sigma_i(K)$ è immaginario, $\tau \circ \sigma_i \neq \sigma_i$. Possiamo quindi ordinare i campi coniugati di K nel modo seguente:

$\sigma_1(K), ..., \sigma_{r_1}(K)$ sono reali $(r_1 \geq 0)$

$\sigma_{r_1+1}(K), ..., \sigma_{r_1+r_2}(K)$ sono immaginari e $\sigma_{r_1+r_2+i}(K) = \tau(\sigma_{r_1+i}(K))$, $1 \leq i \leq r_2$, dove $n = r_1 + 2r_2$.

Gli interi r_1, r_2 sono invarianti importanti del campo di numeri K.

Possiamo adesso enunciare il teorema delle unità di Dirichlet:

Teorema 10.7. (Teorema delle unità di Dirichlet.)
Sia K un campo di numeri di grado n. Sia U_K il gruppo delle unità di $\mathcal{O}_K$, allora:

$$U_K \simeq W_K \times C_1 \times ... \times C_r$$

dove W_K è il sottogruppo delle radici dell'unità appartenenti a K e dove ogni C_i è un gruppo infinito ciclico. Inoltre $r = r_1 + r_2 - 1$.

Dimostreremo questo teorema per i campi quadratici nella prossima sezione. La dimostrazione del caso generale non è delle più semplici e si rimanda a [6]. Nella pratica determinare il gruppo delle unità può essere un problema molto difficile.

10.3 Radici dell'unità nei campi quadratici.

Sia $K = \mathbb{Q}(\sqrt{d})$ un campo quadratico ($d \in \mathbb{Z}$ senza fattori quadrati). Se $d < 0$, $r_1 = 0, r_2 = 1$ e $r_1 + r_2 - 1 = 0$, quindi dal Teorema 10.7 abbiamo $U_K = W_K$. In effetti abbiamo:

Proposizione 10.8. *Sia $K = \mathbb{Q}(\sqrt{d})$ con $d < 0$, allora $U_K = W_K$.*
Più precisamente $U_K = \{\pm 1\}$ tranne che nei due casi seguenti:

- $d = -1$

In questo caso $U_K = \{\pm 1, \pm i\}$

- $d = -3$

In questo caso $U_K = \{\pm 1, \frac{1 \pm i\sqrt{3}}{2}, \frac{-1 \pm i\sqrt{3}}{2}\}$.

Dimostrazione. Se $d \equiv 2,3 \pmod 4$, $\mathcal{O}_K = \{\alpha = a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$. Per il Lemma 10.1 α è un'unità se e solo se $N(\alpha) = a^2 - b^2 d = \pm 1$. Siccome $d < 0$, questo si riduce a $a^2 - b^2 d = 1$ le cui uniche soluzioni sono chiaramente $a = \pm 1, b = 0$ e $a = 0$, $b = \pm 1$ se $d = -1$.

Se $d \equiv 1 \pmod 4$, $\mathcal{O}_K = \{\alpha = \dfrac{a + b\sqrt{d}}{2} \mid a, b \in \mathbb{Z}, a \equiv b \pmod 2\}$. Come prima α è un'unità se e solo se $N(\alpha) = 1$, cioè se e solo se $a^2 - b^2 d = 4$. Chiaramente le uniche soluzioni sono $a = \pm 2, b = 0$ e $a = \pm 1, b = \pm 1$ se $d = -3$. □

Il caso $d > 0$ è più interessante, abbiamo $r_1 = 2, r_2 = 0, r_1 + r_2 - 1 = 1$, quindi dal Teorema di Dirichlet (10.7), $U_K \simeq W_K \times C_1$, dove C_1 è ciclico infinito. Ci sono quindi infinite unità che non sono radici dell'unità. Intanto abbiamo:

Lemma 10.9. *Sia $K = \mathbb{Q}(\sqrt{d})$ con $d > 0$. Allora $W_K = \{\pm 1\}$.*

Dimostrazione. Esercizio 90. □

Rimane quindi da determinare le unità non banali. Come prima α è un'unità se solo se $N(\alpha) = \pm 1$. Se $d \equiv 2,3 \pmod 4$, $\alpha = a + b\sqrt{d}$ e $N(\alpha) = \pm 1 \Leftrightarrow a^2 - b^2 d = \pm 1$. Se $d \equiv 1 \pmod 4$, l'equazione diventa $a^2 - b^2 d = \pm 4$.

La ricerca delle unità dei campi quadratici reali è strettamente legata alla risoluzione dell'equazione detta di Pell. In una lettera del 1657 Fermat lanciò una sfida ai matematici inglesi, con lo scopo di interessarli allo studio dell'aritmetica: si trattava di dimostrare che l'equazione

$$x^2 - dy^2 = 1 \tag{10.1}$$

con $d \in \mathbb{N}$, non quadrato, ammette sempre un'infinità di soluzioni $(x, y) \in \mathbb{N}^2$ e di risolverla per alcuni valori di d. Salterà fuori poi che le scelte di Fermat ($d = 149, 109, 433$) non erano affatto casuali. Dopo varie partenze false ($(x = 1, y = 0)$ è sempre soluzione; soluzioni in numeri razionali) i matematici inglesi Wallis e Brouncker riuscirono a produrre soluzioni per alcuni valori di d, ma non riuscirono a dare una regola generale. La questione fu poi ripresa da Eulero, che per un errore di trascrizione attribuì il problema al matematico inglese Pell, il quale non si è mai occupato della questione! (Si diventa famosi anche così...). Eulero mostrò che se esiste una soluzione non banale (con $y > 0$), allora ne esiste un'infinità. Finalmente è stato Lagrange a mostrare, usando le frazioni continue, che l'equazione di Pell, come viene chiamata oggi, ammette sempre un'infinità di soluzioni.

L'equazione di Pell è importante perché si ritrova in svariati problemi di teoria dei numeri e perché racchiude ancora qualche mistero non risolto.

10.4 Frazioni continue ed equazione di Pell.

Si tratta quindi di mostrare che l'insieme delle soluzioni di (10.1) ($d \in \mathbb{N}$, non quadrato) è infinito. Abbiamo $x^2 - dy^2 = (x + y\sqrt{d})(x - y\sqrt{d})$, quindi le soluzioni dell'equazione di Pell sono gli $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ tali che $N(\alpha) = 1$. Se $N(\alpha) = 1$, allora $N(\alpha^n) = 1$, quindi se abbiamo una soluzione non banale (con $b \neq 0$), l'equazione ha infinite soluzioni.

Osserviamo che se $(x - y\sqrt{d})(x + y\sqrt{d}) = 1$, allora:

$$x - y\sqrt{d} = \frac{1}{x + y\sqrt{d}}$$

Se x e y sono molto grandi $1/(x + y\sqrt{d})$ è molto piccolo e quindi $x \sim y\sqrt{d}$, cioè $\frac{x}{y} \sim \sqrt{d}$; cioè il numero razionale x/y fornisce una buona approssimazione del numero (irrazionale) $\sqrt{d}$. Era noto agli algebristi italiani del Medio-Evo che il metodo delle *frazioni continue* permetteva una buona approssimazione dei radicali, ma la teoria non era sufficientemente sviluppata. Fu Lagrange il primo a fare uno studio sistematico della teoria delle frazioni continue e quindi a mostrare che l'equazione di Pell ha sempre un'infinità di soluzioni, come affermato da Fermat.

Sia ξ un numero reale qualsiasi. Indichiamo con $\lfloor \xi \rfloor$ la parte intera di ξ, cioè il più grande intero $n \leq \xi$. Se $\lfloor \xi \rfloor = a$, allora $\xi = a + \varepsilon$, con $\varepsilon < 1$, quindi $\xi = a + (1/\alpha)$, dove $\alpha > 1$. Adesso possiamo ripetere questo procedimento con α al posto di ξ, più precisamente:

$$\begin{aligned} \xi = \xi_0 &= a_0 + (1/\xi_1);\ \xi_1 > 1 \\ \xi_1 &= a_1 + (1/\xi_2);\ \xi_2 > 1 \\ \xi_2 &= a_2 + (1/\xi_3);\ \xi_3 > 1 \\ &\dots \\ \xi_n &= a_n + (1/\xi_{n+1});\ \xi_{n+1} > 1 \\ &\dots \end{aligned} \tag{10.2}$$

Osserviamo che gli a_i sono degli interi, $a_0 \in \mathbb{Z}$ è un intero positivo o negativo, mentre $a_n \geq 1$ se $n \geq 1$. Il procedimento finisce se $\xi_N = a_N$ per qualche intero N. In questo caso $\xi_{N-1} = a_{N-1} + (1/a_N) \in \mathbb{Q}$ e risalendo fino alla prima equazione vediamo che $\xi \in \mathbb{Q}$. Quindi se ξ è irrazionale, il procedimento non si ferma mai.

Definizione 10.10. *La successione di interi (a_n) è lo sviluppo in frazione continue del numero reale ξ. Si usa indicare questa situazione con la notazione:* $\xi = [a_0; a_1, a_2, ..., a_n, ...]$.

Per esempio se $\xi = \sqrt{2}$, abbiamo $\sqrt{2} = 1 + (\sqrt{2} - 1) = 1 + (1/(1 + \sqrt{2}))$, quindi $\xi_1 = 1 + \sqrt{2} = 2 + (\sqrt{2} - 1)$ e vediamo che $\sqrt{2} = [1; 2, ..., 2, ..] = [1; \overline{2}]$; quindi la frazione continua di $\sqrt{2}$ è periodica ($\overline{2} := 2, 2, ..., 2, ...$). Se invece $\xi = 11/6$, abbiamo $11/6 = 1 + 5/6 = 1 + 1/(6/5)$, poi $6/5 = 1 + 1/5$ e $5 = 5$; quindi $11/6 = [1; 1, 5]$. In effetti:

$$\frac{11}{6} = 1 + \frac{1}{6/5} = \frac{1}{1 + \frac{1}{5}}$$

In modo analogo si potrebbe scrivere:

$$\sqrt{2} = \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cdots}}}}}}$$

Qui si spiega la terminologia di frazione continue (o continuate); questa scrittura, classica, oltre che ad essere scomoda, confonde e fa venire il mal di testa, perciò non la useremo più.

Tornando al caso generale (10.2), abbiamo $\xi_n = a_n + (1/\xi_{n+1}) = \dfrac{a_n \xi_{n+1} + 1}{\xi_{n+1}}$, questa equazione ("funzione fratta") si può scrivere in forma matriciale:

$$\begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \xi_{n+1} \\ 1 \end{pmatrix} = \begin{pmatrix} \xi_n \\ 1 \end{pmatrix}$$

Si verifica facilmente che la matrice della composizione di due funzioni fratte è il prodotto delle due matrici corrispondenti. Quindi se poniamo

$$A_n = \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix}$$

abbiamo:

$$\begin{pmatrix} \xi_0 \\ 1 \end{pmatrix} = A_0 . A_1 ... A_n \begin{pmatrix} \xi_{n+1} \\ 1 \end{pmatrix}$$

Lemma 10.11. *Con le notazioni precedenti sia $T_n := A_0 A_1 ... A_n$, allora:*

$$T_n = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix}$$

dove p_n, q_n sono definiti induttivamente, per $n \geq 0$, dalle relazioni:

$$p_n = a_n p_{n-1} + p_{n-2}$$
$$q_n = a_n q_{n-1} + q_{n-2}$$

con $p_{-2} = 0, q_{-2} = 1$, $p_{-1} = 1, q_{-1} = 0$. In particolare $p_0 = a_0, q_0 = 1$, $p_1 = a_0 a_1 + 1$, $q_1 = a_1$. Inoltre:

$$\xi = \frac{p_n \xi_{n+1} + p_{n-1}}{q_n \xi_{n+1} + q_{n-1}}.$$

Dimostrazione. Induzione su n. □

I numeri razionali p_n/q_n sono i *convergenti* di ξ, mentre gli a_n sono i *quozienti parziali*. Si può mostrare che $\lim_{n\to+\infty} \frac{p_n}{q_n} = \xi$ (in effetti la successione (p_{2n}/q_{2n}) è crescente e tende a ξ per valori inferiori, mentre (p_{2n+1}/q_{2n+1}) è decrescente e tende a ξ per valori superiori); questo dà un senso alla scrittura $\xi = [a_0; a_1, ..., a_n, ...]$. Il risultato che ci serve:

Lemma 10.12. *Sia ξ un numero reale irrazionale. Se p_n/q_n è un convergente di ξ, allora: $|\xi - \frac{p_n}{q_n}| \leq \frac{1}{q_n^2}$.*

Dimostrazione. Abbiamo $\xi = (p_n\xi_{n+1} + p_{n-1})/(q_n\xi_{n+1} + q_{n-1})$ e quindi $q_n\xi - p_n = (q_n p_{n-1} - p_n q_{n-1})/(q_n\xi_{n+1} + q_{n-1}) = (-1)^n/(q_n\xi_{n+1} + q_{n-1})$. In altri termini: $\xi - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n(q_n\xi_{n+1} + q_{n-1})}$. Quindi $|\xi - \frac{p_n}{q_n}| = \frac{1}{q_n(q_n\xi_{n+1} + q_{n-1})} < \frac{1}{q_n^2}$ (perché $\xi_{n+1} > 1, q_{n-1} \geq 0$). □

Abbiamo $q_0 = 1$, $q_1 = a_1 \geq 1$ e $q_n = a_n q_{n-1} + q_{n-2} > q_{n-1}$ se $n \geq 2$. In particolare $q_n \geq n$. Vediamo quindi che i convergenti forniscono una buona approssimazione di ξ.

Proposizione 10.13. *Sia $d \in \mathbb{N}$ un intero non quadrato. Se p_n/q_n è un convergente di $\xi = \sqrt{d}$, allora $p_n^2 - dq_n^2 = k$, dove $k \in \mathbb{Z}$ verifica $|k| < 1 + 2\sqrt{d}$. In particolare esiste $k \in \mathbb{Z}$, con $|k| < 1 + 2\sqrt{d}$ tale che l'equazione $x^2 - dy^2 = k$ abbia un'infinità di soluzioni intere.*

Dimostrazione. Dal Lemma 10.12 abbiamo:

$$|\frac{p_n}{q_n} - \sqrt{d}| < \frac{1}{q_n^2}$$

Quindi $|p_n - q_n\sqrt{d}| < \frac{1}{q_n}$ $(*)$. Inoltre $\frac{p_n}{q_n} - \sqrt{d} < \frac{1}{q_n^2}$, pertanto $\frac{p_n}{q_n} < \frac{1}{q_n^2} + \sqrt{d} \leq \sqrt{d} + 1$ $(**)$.

Adesso $|p_n^2 - q_n^2 d| = |(p_n - q_n\sqrt{d})(p_n + q_n\sqrt{d})| < \dfrac{|p_n + q_n\sqrt{d}|}{q_n}$ per $(*)$. Siccome $p_n + q_n\sqrt{d} \geq 0$ (questo torna a mostrare che $p_n > 0$ se $n \geq 1$ e questo segue da $p_n = a_n p_{n-1} + p_{n-2}, p_0 = a_0 = \lfloor \xi \rfloor$, $p_1 = a_0 a_1 + 1$ con $a_i = \lfloor \xi_i \rfloor$, dove $\xi_i > 1$ se $i \geq 1$), usando $(**)$: $|p_n^2 - q_n^2 d| < \dfrac{p_n + q_n\sqrt{d}}{q_n} = \dfrac{p_n}{q_n} + \sqrt{d} \leq 2\sqrt{d} + 1$. La parte finale segue dal fatto che ci sono infiniti convergenti (distinti, Esercizio **??**) ma solo un numero finito di $k \in \mathbb{Z}$ con $|k| < 2\sqrt{d} + 1$. □

Osservazione 10.14. Osserviamo che ci sono quattro elementi di $\mathbb{Z}[\sqrt{d}]$ che hanno le stesse componenti a meno del segno: infatti $\alpha = a + b\sqrt{d}$, $\overline{\alpha} = a - b\sqrt{d}$, $-\alpha = -a - b\sqrt{d}$ e $-\overline{\alpha} = -a + b\sqrt{d}$ sono tutti e soli gli elementi con componenti $\pm a, \pm b$; questi quattro elementi hanno tutti la stessa norma. In particolare uno di loro a tutte e due le componenti ≥ 0. Se $a \geq 0, b \geq 0$ e $N(\alpha) = 1$ i quattro numeri sono α, $\overline{\alpha} = 1/\alpha$, $-\alpha$, $-1/\alpha$ e abbiamo $\alpha \geq 1, 0 < 1/\alpha \leq 1$, $-\alpha \leq -1$ e $-1 \leq -1/\alpha < 0$. Quindi le soluzioni non banali positive (con $x, y > 0$) dell'equazione di Pell-Fermat corrispondono agli $\alpha > 1$ con $N(\alpha) = 1$.

Se $k \in \mathbb{Z}$, definiamo su $\mathbb{Z}[\sqrt{d}]$ le relazione $\alpha \equiv \beta \pmod{k} \Leftrightarrow k \mid \alpha - \beta$. Si verifica facilmente che $\equiv \pmod{k}$ è una relazione d'equivalenza. Siccome $k \mid \alpha = a + b\sqrt{d} \Leftrightarrow k \mid a$ e $k \mid b$, vediamo che l'insieme quoziente $\mathbb{Z}[\sqrt{d}]/\equiv \pmod{k} \simeq \mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$, in particolare questo insieme quoziente è finito.

Teorema 10.15. (Lagrange)
Sia $d \in \mathbb{N}$ un intero non quadrato, allora l'equazione di Pell-Fermat $x^2 - dy^2 = 1$, ha sempre un'infinità di soluzioni intere.

Dimostrazione. Dalla Proposizione 10.13 segue che esiste $k \in \mathbb{Z}$ tale che l'equazione $x^2 - dy^2 = k$ abbia un'infinità di soluzioni. Siccome l'insieme quoziente $\mathbb{Z}[\sqrt{d}]/\equiv \pmod{k}$ è finito, esiste una classe d'equivalenza che contiene un'infinità di soluzioni, quindi possiamo trovare due soluzioni α_1, α_2 con $\alpha_1 \equiv \alpha_2 \pmod{k}$ e $\alpha_1 \neq \alpha_2$. Quindi $\alpha_i = a_i + b_i\sqrt{d}$, $N(\alpha_i) = k$ e $k \mid \alpha_1 - \alpha_2$. Quindi $k \mid (\alpha_1 - \alpha_2)\overline{\alpha}_2$ e siccome $\alpha_2\overline{\alpha}_2 = k$, abbiamo $k \mid \alpha_1\overline{\alpha}_2$. Sia $k\beta = \alpha_1\overline{\alpha}_2$. Allora $N(k\beta) = N(\alpha_1\overline{\alpha}_2) = \alpha_1\overline{\alpha}_2.\overline{\alpha}_1\alpha_2 = k^2$. Siccome $N(k\beta) = k^2 N(\beta)$, segue che $N(\beta) = 1$ e quindi β è una soluzione dell'equazione di Pell-Fermat. Sia $\beta = x + y\sqrt{d}$. Possiamo assumere $x \geq 0$ e $y \geq 0$ (Osservazione 10.14). Se $y = 0$, abbiamo $N(\beta) = x^2 = 1$, quindi $\beta = 1$. In questo caso $\alpha_1\overline{\alpha}_2 = k = \alpha_2\overline{\alpha}_2$ e quindi $\alpha_1 = \alpha_2$, contro l'ipotesi. Pertanto $y > 0$. Adesso come già osservato $N(\beta^n) = (N(\beta))^n = 1$ e quindi anche β^n è soluzione, $\forall n \in \mathbb{N}$. Siccome $\beta > 1$ (Osservazione 10.14), $\beta < \beta^2 < ... < \beta^n < ...$ e l'equazione di Pell-Fermat ha un'infinità di soluzioni intere. □

Siamo quindi arrivati, anche se per vie traverse, a mostrare che la nostra equazione ha un'infinità di soluzioni intere. Cerchiamo adesso di capire come

sono fatte queste soluzioni. Tutte le soluzioni $\alpha = x + y\sqrt{d}$ con $x, y > 0$, verificano $\alpha > 1$ (Osservazione 10.14). Tra queste c'è ne una minimale, $\alpha_0 = x_0 + y_0\sqrt{d}$ (è quella con y_0 minimale). Quindi α_0 è la più piccola soluzione > 1:

Definizione 10.16. *Con le notazioni precedenti α_0 è la* soluzione fondamentale *dell'equazione di Pell-Fermat.*

La soluzione fondamentale (o minimale) fornisce tutte le soluzioni:

Teorema 10.17. *Ogni soluzione, $\alpha = u + v\sqrt{d}$, dell'equazione di Pell-Fermat $x^2 - dy^2 = 1$ è della forma $u + v\sqrt{d} = \pm(x_0 + y_0\sqrt{d})^n$ per un qualche $n \in \mathbb{Z}$, dove $\alpha_0 = x_0 + y_0\sqrt{d}$ è la soluzione fondamentale.*

Dimostrazione. Abbiamo già visto (Osservazione 10.14) che i quattro numeri $\pm\alpha, \pm 1/\alpha$ danno quattro soluzioni che differiscono solo per il segno di u e v. Quindi basta mostrare che se $\alpha > 1$, allora $\alpha = \alpha_0^n$ per un qualche $n \in \mathbb{N}$. Siccome $\alpha > 1$, $\alpha \geq \alpha_0$, quindi esiste $n \in \mathbb{N}$ tale che: $\alpha_0^n \leq \alpha < \alpha_0^{n+1}$. Sia $\alpha/\alpha_0^n = \beta$, allora $\beta \in \mathbb{Z}[\sqrt{d}]$ perché α_0 essendo un'unità è invertibile, inoltre $N(\beta) = 1$ (perché $\alpha/\alpha_0^n = \alpha(\frac{1}{\alpha_0})^n = \alpha\overline{\alpha}_0^n$). Quindi β è una soluzione positiva ($\beta = \alpha/\alpha_0^n \geq 1$) dell'equazione. Siccome $\alpha_0 = \alpha_0^{n+1}/\alpha_0^n > \beta = \alpha/\alpha_0^n$, l'unica possibilità è $\beta = 1$, ossia $\alpha = \alpha_0^n$. □

Riassumendo per risolvere l'equazione $x^2 - dy^2 = 1$, $d \in \mathbb{N}$, d non quadrato si inizia a scrivere la tabella dello sviluppo di $\sqrt{d}$ in frazione continue e ad ogni passo si calcola $p_n^2 - dq_n^2$. Da quanto visto finora ad un certo punto troveremo una soluzione non banale dell'equazione. La prima soluzione trovata sarà quella fondamentale (perché la successione (q_n) è crescente) e quindi (Teorema 10.17) ci darà tutte le soluzioni. Non è chiaro però *quando* incontreremo questa soluzione. Tutto quello che possiamo dire è che fissato d, il procedimento è finito. Infatti lo sviluppo di $\sqrt{d}$ è periodico, più precisamente si può dimostrare ([3]):

Proposizione 10.18. *Sia $d \in \mathbb{N}$ un intero che non è un quadrato e sia $\xi = \sqrt{d}$, la frazione continua di $\sqrt{d}$ è periodica più precisamente:*

$$\sqrt{d} = [a_0; \overline{a_1, ..., a_h}], \text{ dove } a_h = 2a_0 \text{ e dove } a_i = a_{h-i}, i = 1, ..., h-1.$$

Inoltre $p_n^2 - dq_n^2 = \pm 1$ se e solo se $n = kh - 1$ per un qualche $k > 0$ e in questo caso: $p_n^2 - dq_n^2 = (-1)^{kh}$.

Il problema è che non si sa nulla sul periodo che può essere anche abbastanza lungo, in effetti le soluzioni fondamentali delle equazioni di Pell hanno un comportamento imprevedibile.

10.5 Unità dei campi quadratici.

Sia $K = \mathbb{Q}(\sqrt{d})$ un campo quadratico reale. Supponiamo $d \equiv 2, 3 \pmod 4$. Un elemento $u = a + b\sqrt{d}$ $(a, b \in \mathbb{Z})$ è un'unità di $\mathcal{O}_K$ se e solo se: $N(\alpha) = a^2 - b^2 d = \pm 1$. Le unità di norma 1 sono esattamente le soluzioni dell'equazione di Pell $x^2 - dy^2 = 1$.

Le unità di norma negativa sono le soluzioni dell'equazione "anti-Pelliana": $x^2 - dy^2 = -1$. Quest'ultima equazione non ha sempre soluzioni: una condizione necessaria è che -1 sia un quadrato mod. d, ma questa condizione non è sufficiente (Esercizio 94). Se esiste una soluzione l'insieme delle soluzioni ha una struttura analoga a l'insieme delle soluzioni dell'equazione di Pell: esiste una soluzione fondamentale γ (soluzione positiva minimale) e ogni altra soluzione è della forma $\gamma^{2n+1}, n \in \mathbb{Z}$. Inoltre $\gamma^2 = \alpha_0$ dove α_0 è la soluzione fondamentale dell'equazione di Pell corrispondente. Questo segue essenzialmente dal fatto che se $\beta = a + b\sqrt{d}$ verifica $N(\beta) = -1$, allora $N(\beta^2) = 1$.

Segue dalla Proposizione 10.18 che esistono unità di norma -1 se e solo se il periodo, h, dello sviluppo in frazioni continue di $\sqrt{d}$ è dispari. Tranne alcuni casi particolari non c'è modo di determinare a priori la parità di tale periodo. Se l'equazione anti-Pelliana ammette soluzioni, l'unità fondamentale u_0 (la più piccola unità > 1) ha norma -1.

Se $d \equiv 1 \pmod 4$, $\alpha = (a + b\sqrt{d})/2 \in \mathcal{O}_K$ (a, b con la stessa parità) è un'unità se e solo se $a^2 - b^2 d = \pm 4$. Osserviamo che se $x^2 - y^2 d = 1$ è una soluzione dell'equazione di Pell, allora $(2x)^2 - d(2y)^2 = 4$. Esistono quindi infinite unità non banali. Possiamo concludere:

Teorema 10.19. *Sia $K = \mathbb{Q}(\sqrt{d})$ un campo quadratico reale ($d > 0$ senza fattori quadrati). Il gruppo delle unità U_K è isomorfo a $\{\pm 1\} \times C_1$, dove $C_1 = \langle u_0 \rangle$ è il gruppo ciclico (moltiplicativo) infinito generato dall'unità fondamentale (cioè $u_0 = inf\,\{u \in \mathcal{O}_K \mid N(u) = \pm 1, u > 1\}$).*

Dimostrazione. Da quanto precede sappiamo che esistono (infinite) unità non banali. Se u è un'unità, $u, 1/u, \overline{u}, 1/\overline{u}$ sono unità e uno di questi numeri è necessariamente > 1.

Mostriamo che esiste una più piccola unità > 1. Per questo basta mostrare che per ogni numero reale $c > 1$ esiste un numero finito di unità, u, con $1 < u < c$. Abbiamo $N(u) = u\overline{u} = \pm 1$, quindi $1/c < \overline{u} < 1$ o $-1 < \overline{u} < -1/c$, quindi $|\overline{u}| < c$ e si conclude con la Proposizione 10.3.

Sia quindi u_0 la più piccola unità > 1. Mostriamo che ogni unità positiva, u, è una potenza di u_0. Esiste un intero n tale che $u_0^n \leq u < u_0^{n+1}$. Siccome u/u_0^n è un'unità con $1 \leq u/u_0^n < u_0$, viene $u = u_0^n$. In modo analogo ogni unità negativa è della forma $-u_0^n$ per un qualche $n \in \mathbb{Z}$. □

Questo risultato, insieme alla Proposizione 10.8, conclude la dimostrazione del Teorema delle unità di Dirichlet nel caso quadratico.

.. .. ..

Esercizi.

Esercizio 89 *Sia* $\theta = \dfrac{1+i\sqrt{3}}{2}$. *Risulta dalla Proposizione 10.8 che* θ *è un'unità di* $\mathcal{O}_K$, $K = \mathbb{Q}(\sqrt{-3})$, *anzi* θ *è una radice* n*-esima dell'unità contenuta in* K. *Determinare* n *e il polinomio minimo di* θ.

Esercizio 90 *Dimostrare che* $W_K = \{\pm 1\}$ *se* K *è un campo quadratico reale (Lemma 10.9).*

Esercizio 91 *Sia* ξ *una radice primitiva* p*-esima dell'unità (*p *primo* > 2*). Sia* $K = \mathbb{Q}(\xi)$. *Sappiamo che* W_K *è un gruppo ciclico. Sia* w *il suo ordine.*
(i) Mostrare che $2p \mid w$ *(considerare* $-\xi$*).*
(ii) Concludere che $W_K = \{1, \xi, ..., \xi^{p-1}, -1, -\xi, ..., -\xi^{p-1}\}$.

Esercizio 92 *Sia* $u_0 = a + b\sqrt{d}$ *l'unità fondamentale di* $\mathbb{Q}(\sqrt{d})$ *(*$d > 0$*). Osservare che* $a >, b > 0$ *e* $b = min\ \{y > 0 \mid x^2 - dy^2 = \pm 1\}$. *Determinare l'unità fondamentale di* $\mathbb{Q}(\sqrt{d})$ *per* $d = 2, 3, 5, 6, 7, 10, 13$.

Esercizio 93 *Determinare tutti gli interi* n *tali che lo sviluppo in frazioni continue di* $\sqrt{n}$ *abbia* $h \leq 2$ *(*h *la lunghezza del periodo), più precisamente mostrare che:*
(a) $\sqrt{n} = (a_0; \overline{2a_0}) \Leftrightarrow n = a^2 + 1$ *(caso* $h = 1$*)*
(b) $\sqrt{n} = (a_0; \overline{a_1, 2a_0}) \Leftrightarrow n = a^2r^2 + a (a > 1)$ *o* $n = t^2a^2 + 2t$ *(caso* $h = 2$*). (Hint: usare la Proposizione 10.18).*

Sia (u, v) *la soluzione fondamentale dell'equazione* $x^2 - dy^2 = 1$, *con* $d = a^2r^2 + a$. *Mostrare che, a seconda di* a, r, *può essere sia* $u > d$ *che* $u < d$.

Esercizio 94 *Mostrare che* -1 *è un quadrato modulo* 34.
Mostrare che l'equazione $x^2 - 34y^2 = -1$ *non ha soluzioni intere.*

Esercizio 95 *Per* $n \geq 1$, *si pone* $T_n = \dfrac{n(n+1)}{2}$ *(*T_n *è l'*n*-esimo numero triangolare). Determinare tre numeri triangolari che siano dei quadrati, cioè determinare tre coppie* (n, m) *di interi positivi tali che* $\dfrac{n(n+1)}{2} = m^2$ *(ricondursi ad un'equazione di Pell).*

11

Campi quadratici.

Se $K = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ senza fattori quadrati allora (Proposizione 7.15):

- Se $d \equiv 2$ o $3 \pmod 4$, $\mathcal{O}_K = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} = \mathbb{Z} + \sqrt{d}.\mathbb{Z}$
- Se $d \equiv 1 \pmod 4$, $\mathcal{O}_K = \{\frac{a + b\sqrt{d}}{2} \mid a, b \in \mathbb{Z}, a \equiv b \pmod 2\}$.

  Inoltre se
$$\omega = \begin{cases} \sqrt{d} & \text{se } d \equiv 2, 3 \pmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{se } d \equiv 1 \pmod 4 \end{cases}$$
allora $(1, \omega)$ è una base intera (Corollario 7.16). Finalmente, per quanto riguarda il discriminante D_K, abbiamo (Corollario 7.17):
$$D_K = \begin{cases} 4d & \text{se } d \equiv 2, 3 \pmod 4 \\ d & \text{se } d \equiv 1 \pmod 4 \end{cases}$$

Scopo di questo capitolo è di studiare più in dettaglio le proprietà dei campi quadratici $\mathbb{Q}(\sqrt{d})$.

11.1 Decomposizione, ramificazione dei primi nei campi quadratici.

Sia $p \in \mathbb{N}$ un numero primo, se K è un campo di numeri, l'ideale $p.\mathcal{O}_K$, che noteremo anche (p), non è necessariamente primo in $\mathcal{O}_K$, ma per il teorema di fattorizzazione abbiamo
$$(p) = \mathfrak{p}_1^{e_1} ... \mathfrak{p}_g^{e_g} \tag{11.1}$$

Scopo di questa sezione è di studiare questa fattorizzazione (o decomposizione), nel caso in cui K sia un campo quadratico.

Nella fattorizzazione (11.1) abbiamo $\mathfrak{p}_i \mid (p)$, quindi $(p) \subset \mathfrak{p}_i$, cioè $p \in \mathfrak{p}_i$ e pertanto $\mathfrak{p}_i \cap \mathbb{Z} = (p)$, quindi $\mathbb{Z}/(p) \subset \mathcal{O}_K/\mathfrak{p}_i$ e il campo $\mathcal{O}_K/\mathfrak{p}_i$ è un estensione di $\mathbb{F}_p = \mathbb{Z}/(p)$, pertanto $N(\mathfrak{p}_i) = p^{f_i}$.

Definizione 11.1. *Con le notazioni precedenti e_i è l'indice di ramificazione di $\mathfrak{p}_i$ e f_i è il grado di $\mathfrak{p}_i$.*

Esiste una relazione notevole tra gli interi e_i, f_i, g e $n = [K : \mathbb{Q}]$ (cf Esercizio 88):

Proposizione 11.2. *Sia K un campo di numeri di grado n (cioè $[K : \mathbb{Q}] = n$) e sia*

$$(p) = \mathfrak{p}_1^{e_1} ... \mathfrak{p}_g^{e_g}$$

la fattorizzazione dell'ideale (p) in ideali primi ($p \in \mathbb{N}$ un numero primo). Allora:

$$\sum_{i=1}^{g} e_i f_i = n.$$

Dimostrazione. Come visto prima abbiamo $N(\mathfrak{p}_i) = p^{f_i}$, quindi:

$$N((p)) = \prod_{i=1}^{g} (N(\mathfrak{p}_i))^{e_i} = \prod_{i=1}^{g} p^{e_i f_i} = p^{\sum_{i=1}^{g} e_i f_i}$$

(abbiamo usato la Proposizione 9.11). D'altra parte $N((p)) = |N(p)| = p^n$ (Lemma 9.16) e il risultato segue. □

Se K è un campo quadratico ($n = 2$) abbiamo le seguenti possibilità:

- $g = 2$, $e_1 = e_2 = 1$, $f_1 = f_2 = 1$, $(p) = \mathfrak{p}_1.\mathfrak{p}_2$, $\mathfrak{p}_1 \neq \mathfrak{p}_2$, $N(\mathfrak{p}_i) = p$. In questo caso si dice che p è *decomposto*.
- $g = 1$, $e = 2$, $f = 1$: $(p) = \mathfrak{p}$, con $N(\mathfrak{p}) = p^2$; in questo caso l'ideale (p) è ("rimane") primo; si dice che p è *inerte*.
- $g = 1, e = 1, f = 2$: $(p) = \mathfrak{p}^2$, $N(\mathfrak{p}) = p$; in questo caso si dice che p è *ramificato*.

Possiamo dare ancora una precisazione. Indichiamo con $\sigma : K \to K$ il coniugo (nel caso reale $\sigma(x + y\sqrt{d} = x - y\sqrt{d}$, nel caso complesso σ è il coniugo dei numeri complessi). L'applicazione σ è un $\mathbb{Q}$-automorfismo del campo K (in effetti $K/\mathbb{Q}$ è di Galois). Abbiamo $\sigma(\mathcal{O}_K) = \mathcal{O}_K$ e se $I \subset \mathcal{O}_K$ è un ideale (risp. un ideale primo) anche $\sigma(I)$ è un ideale (risp. un ideale primo).

Lemma 11.3. *Sia K un campo quadratico e sia $(p) = \mathfrak{p}_1\mathfrak{p}_2$ dove p è un numero primo. Allora $\mathfrak{p}_2 = \sigma(\mathfrak{p}_1)$.*

Dimostrazione. Supponiamo $\mathfrak{p}_1 \neq \mathfrak{p}_2$. Abbiamo $\mathfrak{p}_1 \cap \mathbb{Z} = \mathfrak{p}_2 \cap \mathbb{Z} = (p)$. Siccome $\sigma(\mathcal{O}_K) = \mathcal{O}_K$ ($K/\mathbb{Q}$ è di Galois), segue che $(p) = \sigma(p) = \sigma(\mathfrak{p}_1)\sigma(\mathfrak{p}_2)$. Per unicità della fattorizzazione $\sigma(\mathfrak{p}_1) = \mathfrak{p}_2$ o $\mathfrak{p}_1$. Nel primo caso abbiamo finito. Supponiamo $\mathfrak{p}_1 = \sigma(\mathfrak{p}_1) \neq \mathfrak{p}_2$. Sia $\alpha \in \mathfrak{p}_2, \alpha \notin \mathfrak{p}_1$. Abbiamo $a = N(\alpha) = \alpha\sigma(\alpha) \in \mathfrak{p}_2 \cap \mathbb{Z} = \mathfrak{p}_1 \cap \mathbb{Z}$. Quindi $\alpha\sigma(\alpha) \in \mathfrak{p}_1$, siccome $\mathfrak{p}_1$ è primo e $\alpha \notin \mathfrak{p}_1$, questo implica $\sigma(\alpha) \in \mathfrak{p}_1 = \sigma(\mathfrak{p}_1)$, cioè $\alpha \in \mathfrak{p}_1$ e abbiamo un assurdo.

Se $(p) = \mathfrak{p}^2$, allora $(p) = \sigma((p)) = \sigma(\mathfrak{p})^2$ e per unicità della fattorizzazione $\sigma(\mathfrak{p}) = \mathfrak{p}$. □

Vediamo adesso che la fattorizzazione di (p), p primo dispari in $\mathcal{O}_K$, $K = \mathbb{Q}(\sqrt{d})$ dipende da due fatti: (i) se p divide o meno il discriminante D_K, (ii) se d è o meno un quadrato modulo p.

Useremo il fatto seguente:

Lemma 11.4. *Sia K un campo quadratico e sia p un numero primo. Se $(p) = IJ$, allora I e J sono ideali primi.*

Dimostrazione. Infatti $N(I) = N(J) = p$ e si conclude con il Corollario 9.12. □

Proposizione 11.5. *Sia $K = \mathbb{Q}(\sqrt{d})$ (d intero senza fattori quadrati) e sia p un numero primo dispari, allora:*

1. *Se $p \nmid D_K$ e se $\left(\frac{d}{p}\right) = 1$, allora $(p) = \mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{p}_1 \neq \mathfrak{p}_2$. Cioè p è* decomposto. *Più precisamente $(p) = (p, a + \sqrt{d})(p, a - \sqrt{d})$ ($0 \leq a \leq p-1$).*
2. *Se $p \nmid D_K$ e se d non è un quadrato modulo p, allora (p) è primo (p è* inerte*).*
3. *Se $p \mid D_K$, $(p) = \mathfrak{p}^2$, con $\mathfrak{p} = (p, \sqrt{d})$ (p è* ramificato*).*

Dimostrazione. (1) Sia $d \equiv a^2 \pmod{p}$. Abbiamo $(p, a + \sqrt{d})(p, a - \sqrt{d}) = (p)(p, a + \sqrt{d}, a - \sqrt{d}, (a^2 - d)/p) = (p)J$. Ma $J = (1)$ perché $p, 2a \in J$ e p e $2a$ sono primi tra di loro ($p \nmid 2a$ perché $a < p$ e p è dispari). Quindi $(p) = (p, a + \sqrt{d})(p, a - \sqrt{d})$. Abbiamo $(p, a + \sqrt{d}) \neq (p, a - \sqrt{d})$, infatti se $I = (p, a + \sqrt{d}) = (p, a - \sqrt{d})$, allora $2a, p \in I$, ma $(p, 2a) = 1$ quindi $I = (1)$ e $(p) = I^2 = (1)$: assurdo.

(2) Sia $\mathfrak{p} \mid (p)$. Se $N(\mathfrak{p}) = p$, l'inclusione $\mathbb{Z} \hookrightarrow \mathcal{O}_K$ induce un isomorfismo $\mathbb{Z}/p\mathbb{Z} \to \mathcal{O}_K/\mathfrak{p}$. Quindi esiste $a \in \mathbb{Z}$ tale che $a \equiv \sqrt{d} \pmod{\mathfrak{p}}$, quindi $a^2 \equiv d \pmod{\mathfrak{p}}$ e $a^2 \equiv d \pmod{p}$, contro l'ipotesi. Quindi se $\mathfrak{p} \mid (p)$, $N(\mathfrak{p}) = p^2$, cioè $\mathfrak{p} = (p)$.
(2) *(Dimostrazione alternativa:)* Supponiamo $(p) = \mathfrak{p}\mathfrak{q}$. Esiste $\alpha \in \mathfrak{p}$ tale che $p \nmid \alpha$. Infatti altrimenti si avrebbe $\mathfrak{p} \subset (p)$ e quindi $(p) = \mathfrak{p}$ (abbiamo $(p) \subset \mathfrak{p}$ perché $\mathfrak{p} \mid (p)$).

Abbiamo $(\alpha) \subset \mathfrak{p}$ quindi $\mathfrak{p} \mid (\alpha)$ e pertanto $p = N(\mathfrak{p}) \mid N((\alpha)) = |N(\alpha)|$.

Se $\alpha = a + b\sqrt{d}$ ($d \equiv 2, 3 \pmod 4$), $N(\alpha) = a^2 - db^2$; se $\alpha = (a + b\sqrt{d})/2$ ($d \equiv 1 \pmod 4$), $N(\alpha) = (a^2 - db^2)/4$. In ogni caso $p \mid a^2 - db^2$. Quindi $a^2 \equiv db^2 \pmod p$. Abbiamo $p \nmid b$ (altrimenti $p \mid a$ e $p \mid \alpha$). Quindi b è invertibile modulo p e $d \equiv (ab^{-1})^2 \pmod p$, contro l'ipotesi.

(3) Siccome p è dispari $p \mid D_K \Rightarrow p \mid d$, ($D_K = 4d$ se $d \equiv 2, 3 \pmod 4$, $D_K = d$ se $d \equiv 1 \pmod 4$) quindi $d/p \in \mathbb{Z}$. Abbiamo $(p, \sqrt{d})^2 = (p)(p, d/p, \sqrt{d})$. Adesso $(p, d/p) = 1$ perché d è senza fattori quadrati, quindi $(p, \sqrt{d})^2 = (p)$. □

Rimane da fare il caso $p = 2$. Osserviamo che $2 \nmid D_K \Leftrightarrow d \equiv 1 \pmod 4$ (infatti se $d \equiv 2, 3 \pmod 4$, $D_k = 4d$; se $d \equiv 1 \pmod 4$, $d = D_k$ è dispari). Inoltre se $d \equiv 1 \pmod 4$, allora $d \equiv 1, 5 \pmod 8$.

Proposizione 11.6. *Abbiamo i casi seguenti:*

1. *Se* $2 \nmid D_K$ *e* $d \equiv 1 \pmod 8$, *allora* (2) *è* decomposto*:* $(2) = \mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{p}_1 \neq \mathfrak{p}_2$. *Più precisamente* $\mathfrak{p}_1 = (2, \omega)$, $\mathfrak{p}_2 = (2, \overline{\omega})$
2. *Se* $2 \nmid D_K$ *e* $d \equiv 5 \pmod 8$ *allora* (2) *è primo, cioè* 2 *è* inerte
3. *Se* $2 \mid D_K$, *allora* $(2) = \mathfrak{p}^2$, *dove* $\mathfrak{p} = (2, \sqrt{d})$ *se* $d \equiv 2 \pmod 4$ *e* $\mathfrak{p} = (2, 1 + \sqrt{d})$ *se* $d \equiv 3 \pmod 4$. *In questo caso* 2 *è* ramificato.

Dimostrazione. (1) Sia $d \equiv 1 \pmod 8$. Abbiamo $(2, (1 + \sqrt{d})/2)(2, (1 - \sqrt{d})/2) = (2)(2, (1-\sqrt{d})/2, (1+\sqrt{d})/2, (1-d^2)/8)$. Osserviamo che $1-d^2 \equiv 0 \pmod 8$, quindi $(1 - d^2)/8 \in \mathbb{Z}$, inoltre $1 = (1 + \sqrt{d})/2 + (1 - \sqrt{d})/2$, quindi $(2, (1 + \sqrt{d})/2)(2, (1 - \sqrt{d})/2) = (2)$.

(2) Sia $d \equiv 5 \pmod 8$. Supponiamo $(2) = \mathfrak{pq}$. Quindi $N(\mathfrak{p}) = 2$. Mostriamo che questo conduce ad un assurdo. Sia $\alpha \in \mathfrak{p}$ tale che $2 \nmid \alpha$ (un tale α esiste altrimenti $(2) = \mathfrak{p}$). Abbiamo $2 \mid N(\alpha)$. Se $\alpha = (a+b\sqrt{d})/2$ con $a \equiv b \pmod 2$, allora $N(\alpha) = (a^2-db^2)/4$ e quindi $8 \mid a^2-db^2$. Pertanto $0 \equiv a^2-db^2 \equiv a^2-5b^2 \pmod 8$. Se a e b sono dispari, viene (il quadrato di un numero dispari è congruo a 1 modulo 8) $0 \equiv 4 \pmod 8$: assurdo. Quindi $a = 2a', b = 2b'$ e $\alpha = a' + b'\sqrt{d}$. Abbiamo $a'^2 \equiv db'^2 \pmod 2$, siccome d è dispari, a' e b' hanno la stessa parità. Se sono entrambi pari, allora $2 \mid \alpha$: assurdo. Se sono entrambi dispari, $\alpha = 2\overline{a} + 1 + 2\overline{b}\sqrt{d} + \sqrt{d} = 2\overline{a} + 2\overline{b}\sqrt{d} + 2\omega$ e $2 \mid \alpha$: assurdo. Questo mostra che se $\mathfrak{p} \mid (2)$, allora $N(\mathfrak{p}) = 4$, quindi $(p) = \mathfrak{p}$.

(3) Sia $d \equiv 2 \pmod 4$, allora $(2, \sqrt{d})^2 = (4, 2\sqrt{d}, d)$. Siccome $d = 4k + 2$, $2 = d - 4k \in (2, \sqrt{d})^2$, l'altra inclusione è chiara (d è pari), quindi $(2) = (2, \sqrt{d})^2$.
Se $d \equiv 3 \pmod 4$: $(2, 1+\sqrt{d})^2 = (4, 2+2\sqrt{d}, 1+d+2\sqrt{d})$. Abbiamo $d = 4k+3$ quindi: $-4k + (1 + d + 2\sqrt{d}) - (2 + 2\sqrt{d}) = 2$ e $(2) = (2, 1 + \sqrt{d})^2$. □

11.2 Il teorema di Minkowski.

Il teorema di Minkowski fornisce una stima migliore del class number di quella fornita ottenuta nella dimostrazione della Proposizione 9.17. Si tratta di un risultato generale che dimostreremo solo nel caso quadratico. La dimostrazione generale è analoga solo i calcoli sono più complicati.

Definizione 11.7. *Un reticolo $\Gamma \subset \mathbb{R}^n$ è un $\mathbb{Z}$-modulo libero di rango n cioè $\Gamma = \{m_1 v_1 + ... + m_n v_n \mid m_i \in \mathbb{Z}\}$ dove $v_1, ..., v_n$ sono n vettori di $\mathbb{R}^n$ linearmente indipendenti su $\mathbb{R}$.*

In particolare un reticolo è un sotto gruppo discreto di $\mathbb{R}^n$; viceversa si può mostrare che ogni sotto gruppo discreto di $\mathbb{R}^n$ è un reticolo.

Vediamo adesso come associare un reticolo di $\mathbb{R}^2$ ad ogni campo quadratico.

Il caso reale: Se $K = \mathbb{Q}(\sqrt{d})$ con $d > 0$, allora K ha due $\mathbb{Q}$-immersioni che sono anche degli automorfismi di K ($K/\mathbb{Q}$ è di Galois) e sono l'identità e σ il coniugo: se $z = x + y\sqrt{d}$, $\sigma(z) = x - y\sqrt{d} =: \overline{z}$. Sia $\varphi : K \to \mathbb{R}^2 : z \to (z, \overline{z})$. Abbiamo quindi $\varphi(\mathcal{O}_K) \subset \mathbb{R}^2$, si verifica che φ è un morfismo iniettivo di gruppi. In particolare $\Gamma_K = \varphi(\mathcal{O}_K)$ è un reticolo (perché $\mathcal{O}_K$ è un $\mathbb{Z}$-modulo libero di rango due). Più precisamente Γ_K è generato da $\varphi(1) = (1, 1) =: v_1$ e $\varphi(\omega) = (\omega, \overline{\omega}) =: v_2$. Per esempio se $d \equiv 2, 3 \pmod 4$, una base di Γ_K è $v_1 = (1, 1)$, $v_2 = (\sqrt{d}, -\sqrt{d})$.

Osservazione 11.8. C'è una piccola trappola: due vettori di $\mathbb{R}^2$ linearmente indipendenti su $\mathbb{Z}$ non sono necessariamente indipendenti su $\mathbb{R}$, ma nel nostro caso si vede chiaramente che (v_1, v_2) è una base di $\mathbb{R}^2$.

Il caso complesso: Se $K = \mathbb{Q}(\sqrt{d})$ con $d < 0$, allora $K = \mathbb{Q}(i\sqrt{-d})$, ci sono ancora due $\mathbb{Q}$-immersioni (automorfismi di K) che sono l'identità e σ il coniugo: se $z = x + iy\sqrt{-d}$, $\sigma(z) = x - y\sqrt{-d} = \overline{z}$ (è il coniugo dei numeri complessi). Questa volta si definisce $\varphi : K \to \mathbb{C} \simeq \mathbb{R}^2 : z = x + yi\sqrt{-d} \to z$. Il reticolo $\varphi(\mathcal{O}_K)$ è generato da $\varphi(1) = (1, 0) =: v_1$ e da $\varphi(\omega) = \omega =: v_2$. Per esempio se $d \equiv 2, 3 \pmod 4$, $v_1 = (1, 0)$, $v_2 = (0, \sqrt{-d})$.

Se $I \subset \mathcal{O}_K$ è un ideale, allora I è $\mathbb{Z}$-sotto modulo libero di rango due e quindi anche $\varphi(I) \subset \mathbb{R}^2$ è un reticolo, indicheremo questo reticolo con Γ_I.

Osservazione 11.9. Per quanto riguarda Γ_I, rispetto all'Osservazione 11.8, la dimostrazione del Lemma 11.11 mostra che Γ_I è effettivamente un reticolo (i.e. è generato da due vettori $\mathbb{R}$-indipendenti).

Il gruppo quoziente $\mathbb{R}^2/\Gamma \simeq \mathbb{C}/\Gamma$ è un toro, ossia una curva ellittica. Quindi ad ogni campo quadratico corrisponde una curva ellittica.

Definizione 11.10. *Sia $\Gamma \subset \mathbb{R}^n$ un reticolo di base $B = (v_1, ..., v_n)$ allora $P_B = \{\sum \lambda_i v_i \mid 0 \leq \lambda_i < 1\}$ è il parallelogramma fondamentale di Γ. Il volume di Γ è $vol(\Gamma) = |\det(v_1, ..., v_n)|$.*

Nel caso $n = 2$, il volume di Γ è l'area del parallelogramma costruito su v_1, v_2. Il volume non dipende dalla $\mathbb{Z}$-base scelta. Se (w_i) è un'altra base del $\mathbb{Z}$-modulo Γ la matrice di cambiamento di base è una matrice invertibile a coefficienti in $\mathbb{Z}$, quindi il suo determinante vale ± 1 e non altera il volume. In conclusione il volume è un invariante del reticolo.

Nel seguito parleremo di "misura" (o area, volume) di sottinsiemi $X \subset \mathbb{R}^n$. Useremo questo termine in senso intuitivo (per essere rigorosi bisognerebbe parlare di misura di Lebesgue) senza porci il problema di sapere se X è effettivamente "misurabile" (perché questo sarà sempre verificato nei casi considerati!). Indicando con $\mu(X)$ la misura di X, nel caso di un reticolo Γ abbiamo $vol(\Gamma) = \mu(P_B) = |\det(v_1, ..., v_n)|$. Useremo inoltre le seguenti proprietà: una traslazione non cambia la misura: $\mu(X) = \mu(v+X)$, un'omotetia invece sì: $\mu(\lambda X) = \lambda^n \mu(X)$. Finalmente se $(X_i)_{i \in I}$ sono disgiunti $\mu(\cup_i X_i) = \sum_i \mu(X_i)$.

Detto ciò abbiamo:

Lemma 11.11. *Sia K un campo quadratico e sia $\Gamma_K \subset \mathbb{R}^2$ il reticolo associato. Allora:*

1. *Abbiamo $vol(\Gamma_K) = 2^{-s}\sqrt{|D_K|}$, dove $s = 1$ nel caso complesso e $s = 0$ nel caso reale e dove D_K è il discriminante di K.*
2. *Se $I \subset \mathcal{O}_K$ è un ideale e se Γ_I è il reticolo associato, $vol(\Gamma_I) = vol(\Gamma_K).N(I)$.*

Dimostrazione. (1) Facciamo il caso reale. Se $d \equiv 2, 3 \pmod 4$, $\omega = \sqrt{d}$ e $D_K = 4d$. Per definizione $vol(\Gamma_K)$ è il valore assoluto del determinante $\begin{vmatrix} 1 & \omega \\ 1 & \overline{\omega} \end{vmatrix}$.
Quindi $vol(\Gamma_K) = |\omega - \overline{\omega}| = 2\sqrt{d} = \sqrt{D_K}$.
Se $d \equiv 1 \pmod 4$, $\omega = (1 + \sqrt{d})/2$, $D_K = d$ e abbiamo ancora $vol(\Gamma_K) = |\omega - \overline{\omega}| = \sqrt{d} = \sqrt{D_K}$.
Il caso complesso è simile ed è lasciato al lettore.

(2) Se $I \subset \mathcal{O}_K$ è un ideale, esiste una base intera (e_1, e_2) di $\mathcal{O}_K$ e degli interi a, b $(a \mid b)$ tali che (ae_1, be_2) sia una base intera di I (Teorema **??**). Abbiamo $vol(\Gamma_I) = |\det(ae_1, be_2)| = |ab|.|\det(e_1, e_2)| = |ab|.vol(\Gamma_K)$. D'altra parte $\mathcal{O}_K/I \simeq (\mathbb{Z}e_1 \oplus \mathbb{Z}e_2)/(\mathbb{Z}ae_1 \oplus \mathbb{Z}be_2) \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. Quindi $N(I) = ab$ e il risultato segue. □

Dopo questi preliminari possiamo entrare nel vivo dell'argomento:

Lemma 11.12. (Minkowski)
Sia $\Gamma \subset \mathbb{R}^2$ un reticolo e sia $S \subset \mathbb{R}^2$ tale che $\mu(S) > vol(\Gamma)$. Allora esistono $x, y \in S$, $x \neq y$ tali che $x - y \in \Gamma$.

Dimostrazione. Sia (e_1, e_2) una base di Γ e sia $P = \{ue_1 + ve_2 \mid 0 \leq u, v < 1\}$ il parallelogramma fondamentale. L'insieme S è l'unione disgiunta dei sottinsiemi $S \cap (h + P), h \in \Gamma$. Quindi $\mu(S) = \sum_{h\in\Gamma} \mu(S \cap (h + P))$. Abbiamo $\mu(S \cap (h + P)) = \mu((-h + S) \cap P)$ (la misura è invariante per traslazioni). I sottinsiemi $(-h + S) \cap P$ non possono essere tutti disgiunti perché si avrebbe $vol(\Gamma) = \mu(P) \geq \sum_{h\in\Gamma} \mu((-h + S) \cap P)) = \sum_{h\in\Gamma} \mu(S \cap (h + P)) = \mu(S)$, contro l'ipotesi $\mu(S) > vol(\Gamma)$. Quindi esistono $h, h' \in \Gamma$, $h \neq h'$ tali che $((-h + S) \cap P) \cap ((-h' + S) \cap P) \neq \emptyset$. Quindi abbiamo $-h + x = -h' + y$ con $x, y \in S$. Pertanto $x - y = h - h' \in \Gamma$ e $x \neq y$ perché $h \neq h'$. □

Prima di enunciare il risultato principale ci serve una definizione:

Definizione 11.13. *Un sotto insieme $S \subset \mathbb{R}^n$ è simmetrico rispetto all'origine se: $x \in S \Rightarrow -x \in S$. Inoltre S è convesso se $x, y \in S \Rightarrow [x, y] \subset S$, dove $[x, y] = \{\lambda x + (1 - \lambda)y \mid 0 \leq \lambda \leq 1\}$ è il segmento di retta individuato da x e y.*

Teorema 11.14. (Minkowski)
Sia $\Gamma \subset \mathbb{R}^2$ un reticolo e sia $S \subset \mathbb{R}^2$ un sotto insieme convesso e simmetrico rispetto all'origine. Si assume che una delle seguenti condizioni sia verificata:

1. *$\mu(S) > 4.vol(\Gamma)$*
2. *$\mu(S) \geq 4.vol(\Gamma)$ e S è compatto.*

Allora $\Gamma \cap S$ contiene un punto diverso dall'origine.

Dimostrazione. (1) Sia $S' = \frac{1}{2}S$. Abbiamo $\mu(S') = \frac{1}{4}\mu(S) > vol(\Gamma)$. Per il Lemma 11.12, esistono $x, y \in S'$, $x \neq y$ tali che $x - y \in \Gamma$. Abbiamo $x - y = \frac{1}{2}(2x - 2y), 2x, 2y \in S$. Per simmetria $-2y \in S$, per convessità $\frac{1}{2}(2x - 2y) \in S$, quindi $x - y \in S \cap \Gamma$ e $x - y \neq 0$.
(2) Per $m \in \mathbb{N}, m > 0$, sia $S_m = (1 + \frac{1}{m})S$. Per la prima parte $S_m \cap \Gamma$ contiene un punto, x_m, diverso dall'origine. L'insieme $\{x_m\}$ è finito perché compatto e discreto ($\{x_m\} \subset 2S \cap \Gamma$). Quindi esiste un punto, x, di questo insieme che appartiene a S_m per infiniti m: $x \in \cap_{m\in I} S_m := \Sigma$, quindi x appartiene alla chiusura: $x \in \overline{\Sigma} = S$. □

Vediamo adesso come usare questo risultato. Sia $K = \mathbb{Q}(\sqrt{d})$ un campo quadratico reale ($d > 0$). L'immersione in $\mathbb{R}^2$ è data da $\varphi : K \to \mathbb{R}^2 : \alpha \to (\alpha, \overline{\alpha})$, dove $\alpha = x + y\sqrt{d}$, $\overline{\alpha} = x - y\sqrt{d}$. La norma di α è $N(\alpha) = \alpha.\overline{\alpha}$. Se $x = (x_1, x_2) \in \mathbb{R}^2$, poniamo $N(x) = x_1x_2$.

Sia $A = \{x = (x_1, x_2) \mid |x_1| \leq 1, |x_2| \leq 1\}$. Se $x \in A$, $|N(x)| \leq 1$, chiaramente (fare un disegno) $\mu(A) = 4$ e A è convesso e simmetrico rispetto

all'origine. Sia $\Gamma \subset \mathbb{R}^2$ un reticolo. Sia $S := tA$ con $t^2 = vol(\Gamma)$. Allora $\mu(S) = 4t^2 = 4.vol(\Gamma)$ e per il Teorema 11.14, esiste $x \in S \cap \Gamma$, $x \neq 0$. Abbiamo $x = (tx_1, tx_2)$ e quindi $|N(x)| = t^2|x - 1x_2| \leq t^2 = vol(\Gamma)$, quindi Γ contiene un punto non nullo con $|N(x)| \leq vol(\Gamma)$. Se $\Gamma = \Gamma_I$, dove $I \subset \mathcal{O}_K$ è un ideale, viene: $|N(x)| \leq \sqrt{|D_K|}.N(I)$, cioè possiamo prendere $\mu = \sqrt{|D_K|}$ nella Proposizione 9.17. Se $d \equiv 2, 3 \pmod 4$, viene $\mu = 2\sqrt{d}$; è un bel miglioramento rispetto alla limitazione precedente ($1 + d + 2\sqrt{d}$, Osservazione **??**). Ma si può fare meglio:

Teorema 11.15. *Sia K un campo quadratico, se $I \subset \mathcal{O}_K$ è un ideale, allora esiste $\alpha \in I$, $\alpha \neq 0$ con $|N(\alpha)| \leq \mu_M.N(I)$.*

In particolare ogni classe di Cl_K contiene un ideale I con:

$$N(I) \leq \mu_M.$$

dove $\mu_M := \frac{1}{2}(\frac{4}{\pi})^s\sqrt{|D_K|}$, con $s = 0$ se K è reale e $s = 1$ se K è complesso.

Dimostrazione. (i) Iniziamo col caso reale. Si ragiona come prima ma prendendo $A = \{x = (x_1, x_2) \mid |x_1| + |x_2| \leq 2\}$. Abbiamo $\mu(A) = 8$ e A è simmetrico rispetto all'origine e convesso (fare un disegno). Se $x \in A$ allora $|N(x)| \leq 1$, questo segue dal teorema della media geometrica: $\sqrt{ab} \leq \frac{a+b}{2}$, se $a \geq 0, b \geq 0$ (equivalente a dire che $(a - b)^2 \geq 0$). Se Γ è un reticolo sia t tale che $t^2 = vol(\Gamma)/2$, allora se $S = tA$, $\mu(S) = 8t^2 = 4vol(\Gamma)$ e $\Gamma \cap S$ contiene un punto non nullo x. Abbiamo $|N(x)| = t^2|x_1|.|x_2| \leq t^2 = vol(\Gamma)/2$ e questo permette di concludere.

(ii) Sia K complesso, l'immersione $\varphi : K \to \mathbb{C} \simeq \mathbb{R}^2$ è data da $\varphi(x + iy\sqrt{-d}) = (x, y\sqrt{-d})$ e la norma è $N(\alpha) = \alpha.\overline{\alpha}$, dove $\overline{\alpha}$ è il coniugato complesso. La norma è $N(\alpha) = |\alpha|^2$ (dove $|z| = \sqrt{z\overline{z}}$ è il modulo del numero complesso z). Quindi se $x = (x_1, x_2) \in \mathbb{R}^2$, poniamo $N(x) = x_1^2 + x_2^2$.

Sia $A = \{x = (x_1, x_2) \mid \sqrt{x_1^2 + x_2^2} \leq 1\}$. Chiaramente A è convesso e simmetrico rispetto all'origine con $\mu(A) = \pi$. Sia Γ un reticolo e sia t tale che $t^2\pi = 4.vol(\Gamma)$. Allora $tA \cap \Gamma$ contiene un punto x diverso dall'origine. Abbiamo $N(x) = t^2(x_1^2 + x_2^2) \leq t^2 = \frac{4}{\pi}.vol(\Gamma)$. In particolare, visto che $vol(\Gamma_I) = \frac{1}{2}\sqrt{|D_K|}.N(I)$, otteniamo che I contiene un elemento non nullo x con $|N(x)| \leq \frac{2}{\pi}\sqrt{|D_K|}.N(I)$. □

Questo risultato è un caso particolare del teorema di Minkowski sui campi di numeri:

Teorema 11.16. (Minkowski)
Sia K un campo di numeri e $I \subset \mathcal{O}_K$ un ideale, allora esiste $x \in I$, $x \neq 0$ con $|N(x)| \leq \mu_M.N(I)$ e ogni classe di Cl_K contiene un ideale I con $N(I) \leq \mu_M$ dove:

$$\mu_M := \frac{n!}{n^n}.(\frac{4}{\pi})^s.\sqrt{|D_K|}$$

qui $n = [K : \mathbb{Q}]$ e s è il numero di $\mathbb{Q}$-immersioni complesse di K (si ha $r + 2s = n$ dove r è il numero di $\mathbb{Q}$-immersioni reali: $K \to \mathbb{R}$).

La dimostrazione del caso generale è completamente analoga a quella del caso quadratico, solo più complicata nei conti. Prima si dimostra che $vol(\Gamma_K) = \sqrt{|D_K|}/2^s$ e $vol(\Gamma_I) = vol(\Gamma_K).N(I)$. Poi si considera il dominio $A = \{x = (x_1, ..., x_n) \mid |x_1|+...+|x_r|+2(\sqrt{x_{r+1}^2 + x_{r+2}^2}+...+\sqrt{x_{n-1}^2 + x_n^2}) \leq n\}$. Si mostra che $\mu(A) = \frac{n^n}{n!}2^r(\frac{\pi}{2})^s$. Poi bisogna vedere che A è convesso e simmetrico rispetto all'origine. Finalmente si verifica che $|N(x)| \leq 1$ se $x \in A$ usando il teorema della media geometrica: $\sqrt[n]{a_1...a_n} \leq (a_1 + ... + a_n)/n$ $(a_i \geq 0)$ (qui $N(x) = x_1...x_r(x_{r+1}^2 + x_{r+2}^2)...(x_{n-1}^2 + x_n^2)$) (vedere [5], [6], [7] per complementi).

11.3 Ideali primitivi, normalizzati, calcolo del class number.

Sia K un campo quadratico e $\mathfrak{p} \subset \mathcal{O}_K$ un ideale primo, allora $\mathfrak{p} \cap \mathbb{Z} = (p)$, p primo e a seconda della decomposizione di p abbiamo $(p) = \mathfrak{p}^2$ (p ramificato), $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ (p decomposto, qui $\overline{\mathfrak{p}}$ è l'ideale coniugato di $\mathfrak{p}$), $(p) = \mathfrak{p}$ (p inerte). In particolare se $I = \mathfrak{p}J$ e se p è inerte, allora $I = (p)J$ e $I \sim J$ cioè I e J rappresentano la stessa classe nel gruppo delle classi Cl_K. Osserviamo che $N(J) < N(I)$. Quindi ogni ideale è equivalente ad un ideale i cui (ideali) fattori primi non stiano sopra numeri primi inerti. Cioè se $\mathcal{R} = \{p \in \mathbb{N} \mid p \text{ primo ramificato}\}$, $\mathcal{I} = \{p \in \mathbb{N} \mid p \text{ primo inerte}\}$, $\mathcal{D} = \{p \in \mathbb{N} \mid p \text{ primo decomposto}\}$, allora ogni ideale è equivalente ad un ideale del tipo

$$I = \prod_{q \in \mathcal{R}} \mathfrak{q}^{e_q}. \prod_{p \in \mathcal{D}} \mathfrak{p}^{e_p}\overline{\mathfrak{p}}^{e'_p}$$

Possiamo ulteriormente "ridurre" I: tenuto conto che $\mathfrak{q}^2 = (q)$, I è equivalente ad un ideale (di norma più piccola) con $e_q = 0$ o 1. In modo analogo visto che $\mathfrak{p}\overline{\mathfrak{p}} = (p)$ possiamo assumere che solo uno dei due compaia (cioè $e_p e'_p = 0$).

Definizione 11.17. *Un ideale I è* primitivo $\Leftrightarrow$ *per ogni primo $p \in \mathbb{N}$, $(p) \nmid I$.*

Possiamo riassumere quanto detto prima nel seguente lemma:

Lemma 11.18. *Un ideale I è primitivo se e solo se:*

$$I = \prod_{q \in \mathcal{R}} \mathfrak{q}^{e_q}. \prod_{p \in \mathcal{D}} \mathfrak{p}^{e_p}\overline{\mathfrak{p}}^{e'_p},\ 0 \leq e_q \leq 1, e_p, e'_p \geq 0, e_p.e'_p = 0 \tag{11.2}$$

Ogni ideale I è equivalente ad un ideale primitivo J con $N(J) \leq N(I)$.

Per il teorema di Minkowski (Teorema 11.15) ogni classe di Cl_K contiene un ideale con $N(I) \leq \mu_M$, dove $\mu_M = \frac{1}{2}(\frac{4}{\pi})^s\sqrt{|D_K|}$, $s = 0$ nel caso reale, $s = 1$ nel caso complesso. Ricordiamo che se $K = \mathbb{Q}(\sqrt{d})$, allora $D_K = 4d$ se $d \equiv 2, 3 \pmod 4$, mentre $D_K = d$ se $d \equiv 1 \pmod 4$.

Definizione 11.19. *Un ideale I è normalizzato se $N(I) \leq \mu_M$. Si indica con $\mathcal{N}$ l'insieme degli ideali primitivi normalizzati e con $N(\mathcal{N}) = \{N(I) \mid I \in \mathcal{N}\}$.*

Corollario 11.20. *Ogni classe contiene un ideale primitivo normalizzato.*

Dimostrazione. Segue dal teorema di Minkowski e dal Lemma 11.18. □

Quindi la determinazione di Cl_K si riduce a quella di $\mathcal{N}$ e per studiare $\mathcal{N}$ si userà $N(\mathcal{N})$.

Riassumendo le tappe per calcolare il class number sono le seguenti:

- Vedere quali sono i primi di $\mathcal{R}$, $\mathcal{D}$
- Determinare l'insieme $\mathcal{N}$ degli ideali primitivi normalizzati e l'insieme $N(\mathcal{N})$ delle loro norme
- Per ogni coppia $I, J \in \mathcal{N}$ vedere se $I \sim J$

Questo procedimento permette di accelerare il calcolo del class number. Facciamo un esempio.

Sia $d > 0$ (caso reale).

La costante di Minkowski è

$$\mu_M = \sqrt{D_K}/2 = \begin{cases} \sqrt{d} & \text{se } d \equiv 2, 3 \pmod 4 \\ (\sqrt{d})/2 & \text{se } d \equiv 1 \pmod 4 \end{cases}$$

Sia $\theta := \lfloor \mu_M \rfloor$ (parte intera).

- $\theta = 1$

In questo caso $\sqrt{D_K} < 4$, $D_K < 16$, cioè $4d < 16$ ossia $d < 4$ se $d \equiv 2, 3 \pmod 4$ e $d < 16$ se $d \equiv 1 \pmod 4$. Quindi $d \in \{2, 3, 5, 13\}$ con i relativi discriminanti $D_K \in \{8, 12, 5, 13\}$. In questo caso $N(\mathcal{N}) = \{1\}$ e quindi necessariamente l'unico ideale primitivo normalizzato è (1). Quindi $h = 1$ e $\mathcal{O}_K$ è principale.

Chiaramente all'aumentare di μ questo approccio diventa presto impraticabile. Un metodo "elementare" alternativo consiste nell'utilizzare la teoria delle forme quadratiche intere, argomento che per mancanza di tempo non abbiamo trattato. Con questo approccio Gauss ha osservato che spesso e volentieri si ha $h_K = 1$ nel caso reale, mentre nel caso non reale questa eventualità sembra molto rara. Più precisamente Gauss ([4]) ha congetturato:

Conjecture 11.21. (Gauss.)
(i) Si ha $\lim_{d\to-\infty} h(d) = \infty$ (qui $h(d) = h_K$ dove $K = \mathbb{Q}(\sqrt{d}), d < 0$).
(ii) Gli unici campi quadratici non reali con $h_K = 1$ si ottengono per $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$.
(iii) Esistono infiniti campi quadratici reali con $h_K = 1$.

La parte (i) è stata dimostrata nel 1934 da Heilbronn, la parte (ii) è stata dimostrata da Heegner (1952), ma la dimostrazione fu giudicata incompleta e poi da Stark nel 1967. Il punto (iii) *è ancora un problema aperto*. Tutti i risultati sono stati ottenuti con metodi analitici, esiste infatti una formula analitica del class number che esprime h_K in funzione di vari invarianti di K e di una certa funzione L di K. Nel caso reale purtroppo uno degli invarianti è $\log u$ dove u è l'unità fondamentale, il cui comportamento, come abbiamo visto, è altamente imprevedibile. Ma questo è un'altra storia...

That's all folks!

———— .. ————

Esercizi.

Esercizio 96 *Sia* $K = \mathbb{Q}(\sqrt{-6})$.
(i) Mostrare che $-2, 3, \sqrt{-6}$ *sono irriducibili. Osservare che* $-6 = -2.3 = \sqrt{-6}.\sqrt{-6}$.
(ii) Osservare che per il teorema di Minkowski ogni classe di Cl_K *contiene un ideale* I *con* $N(I) \leq 3, 1$....
(iii) Osservare che i primi $2, 3$ *sono ramificati e concludere che* $h_K = 2$.

Esercizio 97 *Sia* $K = \mathbb{Q}(\sqrt{-31})$.
(i) per il teorema di Minkowski ogni classe contiene un ideale I, *con* $N(I) \leq 3$.
(ii) Non esistono ideali di norma 3.
(iii) Abbiamo che 2 *è decomposto in* K: $(2) = \mathfrak{p}\overline{\mathfrak{p}}$; $\mathfrak{p}$ *e* $\overline{\mathfrak{p}}$ *sono gli unici ideali di norma* 2. *Determinare* $\mathfrak{p}$ *e mostrare che* $\mathfrak{p}$ *non è principale.*
(iv) Mostrare che $\mathfrak{p}^2$ *non è principale.*
(v) Osservare che $8 = (1 + \sqrt{-31})/2.(1 - \sqrt{-31})/2$ *e concludere che* $\mathfrak{p}^3$, $\overline{\mathfrak{p}}^3$ *sono principali.*
(vi) Concludere che $h_K = 3$.

Esercizio 98 *Sia* p *un primo congruo a* 5 *modulo* 12. *Si pone* $K = \mathbb{Q}(\sqrt{-p})$.
(i) Mostrare che 3 *è decomposto in* K. *Quindi* $(3) = \mathfrak{p}\overline{\mathfrak{p}}$.
(ii) Mostrare che se $p > 3^n$, *allora* $\mathfrak{p}$ *ha ordine almeno* n *in* Cl_K. *Quindi* $h_K \geq n$.

Esercizio 99 *Sia* K *un campo quadratico e* $I \subset \mathcal{O}_K$ *un ideale. Con* $\overline{I} = \sigma(I)$ *si indica l'ideale coniugato. Mostrare che* $I.\overline{I} = (N(I).\mathcal{O}_K)$ *(se* $I\overline{I} \cap \mathbb{Z} = n\mathbb{Z}$ *mostrare che* $I.\overline{I} = (n.\mathcal{O}_K)$*).*

Esercizio 100 *Sia* K *un campo quadratico e sia* $I \subset \mathcal{O}_K$ *un ideale. Con* $\overline{I} = \sigma(I)$ *si indica l'ideale coniugato. Sia* $D_K = p_1^a p_2 ... p_t$ *la fattorizzazione in primi di* D_K *dove* $p_1 = 2, a = 0, 2$ *o* 3. *Mostrare che se* $I = \overline{I}$ *allora* I *si scrive in modo unico come* $I = r\mathfrak{p}_1^{a_1} ... \mathfrak{p}_t^{a_t}$ *dove* $r \in \mathbb{N}$, $0 \leq a_i \leq 1$ *e dove* $(p_i) = \mathfrak{p}_i^2, i = 1, ..., t$.

Esercizio 101 *Sia* K *un campo quadratico. Il gruppo delle classi* $Cl_K =: \mathcal{C}$ *è* J_K/P_K *dove* J_K *è l'insieme degli ideali frazionari e* P_K *l'insieme degli ideali frazionari principali* $(\{\alpha\mathcal{O}_K \mid \alpha \in K^*\})$. *Due ideali frazionari sono equivalenti* $(I \sim J)$ *se hanno la stessa classe in* $\mathcal{C}$: $[I] = [J]$.

Sia P_+ *l'insieme degli ideali principali frazionari con* $N(\alpha) > 0$.
(i) Mostrare che P_+ *è un gruppo. Osservare che se* $K = \mathbb{Q}(\sqrt{d})$, $d < 0$, $P_+ = P_K$.
(ii) Il gruppo quoziente $J_K/P_+ =: \mathcal{C}_+$ *si chiama il gruppo delle classi ristrette*

*(*narrow class group*); si indica con h_+ la sua cardinalità. Due ideali frazionari sono strettamente equivalenti ($I \approx J$) se $I = (x.\mathcal{O}_K).J$ con $N(x) > 0$, $x \in K$. Mostrare che: (1) Se $d < 0$, $I \sim J \Leftrightarrow I \approx J$.*
(2) Se $d > 0$ e se l'unità fondamentale ε_0 ha norma -1, allora $I \sim J \Leftrightarrow I \approx J$.
(3) Se $d > 0$ e se l'unità fondamentale ha norma +1 allora ogni classe di equivalenza dà luogo a due classi di equivalenza stretta (perché $I \not\approx (\sqrt{d}).I$).
(iii) Concludere che c'è una successione esatta di gruppi abeliani:

$$1 \to \langle \sqrt{d} \rangle \to \mathcal{C}_+ \to \mathcal{C} \to 1$$

dove $\langle \sqrt{d} \rangle = \{1, [(\sqrt{d})]_+\}$.

Quindi: $h_+ = 2h$ se e solo se $d > 0$ e l'unità fondamentale ha norma $+1$; in tutti gli altri casi $h_+ = h$.
(iv) Si può mostrare che $2^{t-1} \mid h_+$ dove t è il numero di primi ramificati (cioè $\omega(|D_K|)$, il numero di primi distinti che dividono $|D_K|$). Prendendo per buono questo risultato mostrare che se $d > 0$, $h = 1$ e l'unità fondamentale ha norma -1, allora $K = \mathbb{Q}(\sqrt{d})$ con $d = p$ un primo $\equiv 1 \pmod 4$ oppure $d = 2$.

Bibliografia

1. Alford, W.R.-Granville, A.-Pomerance, C.: *There are infinitely many Carmichael numbers*, Annals of Math., **140**, 703-722 (1994)
2. Borevich Z.I.-Shafarevich, I.: *Number theory*, Academic Press (1966)
3. Coppel, W.A.: *Number theory, an introduction to mathematics*, Universitext, Springer
4. Gauss, C. F.: *Disquisitiones Aritmeticae*
5. Marcus, D.A.: Number fields, Universitext, Springer (1977)
6. Ribenboim, P.: *Algebraic numbers*, Wiley-Interscience (1972)
7. Samuel, P.: *Théorie algébrique des nombres*, Hermann (1967)