ESERCIZI DI TEORIA DEI NUMERI

A. BERNARDI

1. Secondo foglio di esercizi

Gli esercizi sembrano molti ma quelli della prima sezione sono banali; li ho messi per farvi lavorare con un esempio a mio avviso istruttivo ma allo stesso tempo molto semplice. Gli esercizi significativi sono quelli della seconda sezione.

1.1. **Un esercizio istruttivo.** Per $d \geq 1, d \in \mathbb{N}$, poniamo

$$A_d = \mathbb{Z}[\sqrt{-d}] = \mathbb{Z}[i\sqrt{d}] = \{a + ib\sqrt{d} \;\; a, b \in \mathbb{Z}\}.$$

Si verifica facilmente che A_d è un sottoanello di $\mathbb{C}$ e quindi è integro (non occorre che lo mostriate).

Definition 1. Per $z = a + ib\sqrt{d} \in A_d$ si definisce la norma di z come

$$N(z) = z\overline{z} = a^2 + db^2.$$

Esercizio 1. La norma è moltiplicativa.

Cerchiamo tramite una serie di esercizi di determinare le unità di A_d.

Esercizio 2. Un elemento $z \in A_d$ è invertibile se e solo se $N(z) = 1$. Le unità di A_d sono ± 1 se $d > 1$; ± 1 e $\pm i$ se $d = 1$.

Esercizio 3. Ogni elemento non nullo di A_d ammette una fattorizzazione in prodotto di irriducibili.

Esercizio 4. L'elemento 2 è irriducibile in A_d se $d \geq 3$. Per $d \geq 3$, A_d non è un UFD.

Esercizio 5. Per $d = 1, 2$ l'anello A_d è euclideo.

Definition 2. Sia A un anello commutativo integro. Due elementi $x, y \in A$ si dicono *estranei tra loro* se esistono $u, v \in A$ t.c. $xu + yv = 1$.

Esercizio 6. Se due elementi sono estranei tra loro sono anche primi tra loro. Il viceversa non è sempre vero.

Esercizio 7. Mostrare che la definizione di MCD come il più grande divisore comune tra due elementi non è ben posta in $\mathbb{Z}[\sqrt{-5}]$.

Non c'è una buona teoria della divisibilità in $\mathbb{Z}[\sqrt{-d}]$ se $d \geq 3$.

Vediamo insieme un esempio classico. Nel 1847 Lamé annunciò di aver trovato una dimostrazione della congettura di Fermat. La sua idea era la seguente (facciamo il caso $n = 3$ per semplicità):

Possiamo scrivere

$$x^3 + y^3 = z^3$$

nella forma $x^3 - z^3 = -y^3$ e poi

$$\left(\frac{x}{z}\right)^3 - 1 = -\left(\frac{y}{z}\right)^3. \tag{1}$$

Adesso $X^3-1=(X-1)(X^2+X+1)=(X-1)(X-j)(X-j^2)$ dove $j=\frac{-1+i\sqrt{3}}{3}$ è una radice primitiva terza dell'unità. Quindi $\left(\frac{x}{z}\right)^3-1=\left(\frac{x}{z}-1\right)\left(\frac{x}{z}-j\right)\left(\frac{x}{z}-j^2\right)$. Moltiplichiamo per z^3 otteniamo $x^3-z^3=(x-z)(x-jz)(x-j^2z)$, quindi l'equazione (1) diventa

$$(x-z)(x-jz)(x-j^2z)=-y^3.$$

Esercizio 8. Adesso se abbiamo degli interi a_i tali che $a_1a_2a_3=t^3$ e se $(a_i,a_j)=1$, possiamo concludere che a_i è un cubo per ogni i.

Quindi Lamé conclude che ogni $x-1$, $x-jz$, $x-j^2z$ è un cubo.

Esercizio 9. Concludere sotto queste ipotesi con un metodo di discesa infinita una contraddizione.

Subito vari matematici tra cui Loiouville (che aveva suggerito l'uso dei numeri complessi a Lamé) sollevarono dubbi: il fatto è che non si sta più lavorando negli interi, ma con dei numeri della forma $n+jm$, $n,m\in\mathbb{Z}$ e per questi "nuovi" numeri (cioè per l'anello $\mathbb{Z}[j]$) il teorema fondamentale dell'aritmetica non è dimostrato, In effetti Kummee aveva già percorso questa strada dimostrato alcuni anni prima che per i numeri del tipo $n+\zeta m$, ζ radice n-esima dell'unità, il teorema fondamentale non era sempre vero (cioè $\mathbb{Z}[\zeta]$) non è sempre fattoriale).

La dimostrazione di Lamé era quindi COMPLETAMENTE SBAGLIATA!

Gli sforzi di Kummer per capire come si poteva rimediare sono all'origine dell'algebra moderna (teoria degli ideali) e della teoria dei numeri.

1.2. **Esercizi significativi.**

Esercizio 10. Sia $M_p=2^p-1$ il numero di Mersenne corrispondente al primo $p>2$.

(1) Mostrare che se un primo q divide M_p, allora $p\mid(q-1)$.
(2) Concludere che ogni divisore primo di M_p è della forma $2kp+1$, $k\geq 1$.
(3) Mostrare che M_{11} e M_{23} non sono primi.

Esercizio 11. Sia G un gruppo ciclico di ordine n.

(1) Mostrare che se $d\mid n$ allora esiste uno ed un solo sottogruppo H ciclico di G di ordine d. Inoltre H ha $\varphi(d)$ generatori. Ogni elemento di G genera un sottogruppo ciclico.
(2) Dimostrare poi che per ogni intero n si ha che $\sum_{d|n}\varphi(d)=n$.
(3) Infine mostrare che se p è un numero primo e $d\mid(p-1)$ allora in $\mathbb{F}_p^\times$ ci sono esattamente $\varphi(d)$ elementi il cui ordine è d.

Esercizio 12. La funzione λ di Carmichael è definita nel modo seguente:

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

(1) Mostrare che se $(a,m)=1$ allora $a^{\lambda(m)}\equiv 1\pmod m$ (Teorema di Carmichael).
(2) Per $m=2^6\times 3^3\times 5\times 7$, calcolare $\lambda(m)$ e $\varphi(m)$.
(3) Mostrare che per ogni m esiste un a relativamente primo con m tale che l'ordine di a in U_m sia $\lambda(m)$.
(4) Con questi risultati, come si può "migliorare" il teorema di Eulero che afferma che se $(a,m)=1$ allora $a^{\varphi(m)}\equiv 1\pmod m$?

Esercizio 13. Se $N=x^2+y^2$ diremo che (x,y) (con $x,y\geq 0$) è una *rappresentazione* di N. Diremo poi che è propria se $(x,y)=1$.

(1) Mostrare che se N ammette una rappresentazione propria allora i suoi fattori primi dispari sono congrui a 1 (mod 4).
(2) Mostrare che se N ammette una rappresentazione propria, allora N non è multiplo di 4.

(3) 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.

(4) Mostrare che un primo $p \equiv 1 \pmod 4$ ammette un'unica (a meno di ordine dei termini) rappresentazioni (propria).

Esercizio 14. L'equazione diofantea

$$x^2 + y^2 = z^2 \tag{2}$$

ha infinite soluzioni (si veda come conseguenza del teorema dei 2 quadrati).

(1) Possiamo assumere che $(x, y, z) = 1$. Segue che x, y, z sono a due a due primi tra loro. Mostrare che si può assumere x, z dispari e y pari.

(2) Mostrare che $(z - x, z + x) = 2$. Porre $y = 2y'$, $z + x = 2x'$, $z - x = 2z'$ e concludere che le soluzioni di (2) sono tutte della forma $x = d(u^2 - v^2)$, $y = 2duv$, $z = d(u^2 + v^2)$, dove $(u, v) = 1$.

Esercizio 15. In una lettere a Mersenne del 1637 Fermat "annuncia" i teoremi dei 2,3 4 quadrati e il seguente:

Ogni numero si scrive come la somma di 3 numeri triangolari.[1]

(1) Dedurre da questa affermazione di Fermat che ogni numero congruo a 3 mod 8 si scrive come somma di 3 quadrati.

(2) Usando il punto (1) osservare che $n = 8m + 4$ si scrive come somma di 4 quadrati. Se $8m + 4 = x_1^2 + \cdots + x_4^2$, gli x_i hanno tutti la stessa parità. Se sono dispari usare

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

per concludere che $4m+2$ e $2m+1$ sono somma di 4 quadrati. Concludere che ogni numero dispari si scrive come somma di 4 quadrati.

(3) Con un ragionamento analogo a quello del punto (2) mostrare che se $2m+1$ è somma di 4 quadrati allora lo son anche $4m+2$, $4m+6$. Concludere che l'enunciato di Fermat implica il teorema dei 4 quadrati.

(4) Mostrare che l'enunciato di Fermat è equivalente a sapere che ogni $n \equiv 3 \pmod 8$ si scrive come somma di 3 quadrati.

Esercizio 16.

(1) Dimostrare che esistono infiniti primi della forma $4k + 1$.[2]

(2) Dimostrare che esistono infiniti primi della forma $8r - 1$.[3]

Esercizio 17.

(1) Sia p un primo congruo a 3 (mod 4) t.c. $q = 2p + 1$ sia anch'esso primo. Mostrare che $q \mid 2^p - 1$. Quindi il numero di Mersenne $M_p = 2^p - 1$ non è primo.

(2) Verificare che se $p = 1122659$ allora M_p e M_{2p+1} NON sono primi. [4]

---

[1] Un numero triangolare è della forma $n = \frac{(k+1)k}{2} = \binom{k+1}{2}$.

[2] Suggerimento: Considerare $(n!)^2 + 1$.

[3] Suggerimento: Considerare $Q = (4p_1 \cdots p_k)^2 - 2$ dove i $p_i \equiv -1 \pmod 8$.

[4] Da fare col computer!