ESTRATTO

Terence Tao

Risolvere problemi matematici

Il mio punto di vista

scienza express edizioni

3. Esempi in algebra e analisi

> Non si può fuggire alla sensazione... che queste formule matematiche abbiano un'esistenza indipendente e un'intelligenza propria... che siano più sagge di noi, più sagge perfino dei loro scopritori... che ricaviamo da esse più di quanto abbiamo originariamente messo in esse.
>
> Heinrich Hertz,
> citato da F. J. Dyson

L'algebra è ciò che la maggior parte delle persone associa alla matematica. In un certo senso, questo è giustificato. La matematica è lo studio degli oggetti astratti, numerici, logici o geometrici, che segue da un insieme di diversi assiomi scelti attentamente. E l'algebra di base riguarda la più semplice cosa importante che può soddisfare la definizione di matematica qui sopra. Ci sono solo circa una dozzina di postulati, ma questo è sufficiente per rendere il sistema magnificamente simmetrico. La mia identità algebrica preferita, per fare un esempio, è

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + 3 + \cdots + n)^2.$$

Questo significa, in particolare, che la somma dei primi n cubi è sempre un quadrato; per esempio $1 + 8 + 27 + 64 + 125 = 225 = 15^2$.

Tuttavia, c'è più di un'algebra. L'algebra è lo studio dei numeri con l'operazione di addizione, sottrazione, moltiplicazione e divisione. L'algebra delle matrici, per esempio, fa più o meno lo stesso, ma con gruppi di numeri invece di usarne solo uno. Altre algebre usano tutti i tipi di operazione e tutti i tipi di "numeri", ma esse, a volte sorprendentemente, tendono ad avere gran parte delle stesse proprietà dell'algebra normale. Per esempio, una matrice quadrata A può, sotto speciali condizioni, soddisfare l'equazione algebrica

$$(I - A)^{-1} = I + A + A^2 + A^3 + \cdots .$$

L'algebra è la fondazione di base di una gran parte della matematica applicata. Molti problemi di meccanica, economia, chimica, elettronica, ottimizzazione e così via sono risolti dall'algebra e dal calcolo differenziale, che è una forma avanzata di algebra. In effetti l'algebra è così importante che la gran parte dei suo segreti sono stati scoperti; per questo essa può essere inserita in modo sicuro nei programmi della scuola superiore. Tuttavia, un po' di gemme possono essere ancora trovate qua e là.

3.1 Analisi di funzioni

Anche l'analisi è un soggetto pesantemente esplorato, ed è tanto generale quanto l'algebra: in sostanza, l'analisi è lo studio delle funzioni e delle loro proprietà. Più complicate sono le proprietà, più "alta" è l'analisi. La più bassa forma di analisi è lo studio delle funzioni che soddisfano semplici proprietà algebriche, per esempio possiamo considerare una funzione $f(x)$ tale che

$$\begin{array}{l} f \text{ è continua, } f(0) = 1 \text{ e } f(m+n+1) = f(m) + f(n) \\ \text{per tutti i numeri reali } m,\, n \end{array} \tag{9}$$

e quindi dedurre proprietà della funzione. Per esempio, in questo caso, c'è esattamente una funzione f che soddisfa le proprietà qui sopra, cioè la funzione $f(x) = 1 + x$; lasciamo questo come esercizio. Questi problemi sono un buon modo per imparare come pensare matematicamente, perché c'è un solo dato o due da usare e quindi dovrebbe esserci una direzione chiara da seguire. È una specie di "matematica tascabile" dove al posto di tre dozzine di assiomi e innumerevoli migliaia di teoremi, si può usare solo una manciata di "assiomi" (ovvero i dati). Nonostante questo, ci può comunque riservare delle sorprese.

Esercizio 3.1. Sia f una funzione reale di variabile reale che soddisfa la condizione (9). Dimostrare che $f(x) = 1 + x$ per tutti i numeri reali x. (Suggerimento: dimostrarlo prima per gli interi x, poi per i razionali e quindi per i reali.)

Problema 3.1. (Greitzer 1978, pag. 19). (*) Supponiamo che f sia una funzione che manda interi positivi in interi positivi tale che $f(n+1) > f(f(n))$ per ogni numero intero positivo n. Si dimostri che $f(n) = n$ per ogni intero positivo n.

Questa equazione sembra insufficiente a dimostrare ciò che vogliamo. Dopotutto, come può una disuguaglianza dimostrare un'uguaglianza? Altri problemi di questo tipo (come l'Esercizio 3.1) coinvolgono *equazioni* funzionali e sono più facili da maneggiare, perché è possibile applicare diverse sostituzioni o simili, e gradualmente manipolare i dati originali per dar loro una forma maneggevole. Questo problema sembra completamente diverso.

Tuttavia, se la domanda viene letta attentamente, vediamo che la funzione assume valori interi, a differenza della maggior parte dei problemi che coinvolgono equazioni funzionali, che solitamente assumono valori reali. Un modo immediato di capitalizzare questo fatto è rendere la diseguaglianza "più forte":

$$f(n+1) \geq f(f(n)) + 1. \tag{10}$$

Ora vediamo cosa possiamo dedurre. Il metodo standard per trattare queste equazioni consiste nel sostituire valori adeguati al posto delle variabili, quindi cominciamo con $n = 1$:

$$f(2) \geq f(f(1)) + 1$$

Questo non ci dice molto di $f(2)$ o $f(1)$ a prima vista, ma il $+1$ nel membro di destra suggerisce che $f(2)$ non può essere troppo piccolo. In effetti, dato che f prende valori interi positivi, $f(f(1))$ deve essere almeno 1. Quindi $f(2)$ è almeno 2. Ora dobbiamo dimostrare che $f(2)$ è proprio 2, quindi potremmo essere sulla pista giusta. (Cerchiamo sempre di usare tattiche che avvicinino all'obiettivo, a meno che tutti gli approcci diretti disponibili non siano esauriti. Solo allora dovremmo pensare di procedere lateralmente, o, occasionalmente, all'indietro).

Quindi, possiamo dimostrare che $f(3)$ è almeno 3? Beh, possiamo usare (10) di nuovo per ottenere $f(3) \geq f(f(2)) + 1$. Usando lo stesso argomento usato poco fa, possiamo dire che $f(3)$ è almeno 2. Ma possiamo dire qualcosa di più forte? Prima abbiamo detto che $f(f(1))$ era almeno 1. Forse $f(f(2))$ è almeno 2. (Infatti, dato che "segretamente" sappiamo che $f(n)$ dovrebbe alla fine essere uguale a n, sappiamo che $f(f(2))$ *è* 2, ma non possiamo ancora usare questo fatto, dato che non possiamo in realtà usare ciò che stiamo cercando di dimostrare.) Seguendo questa linea di pensiero possiamo applicare (10) ancora:

$$f(3) \geq f(f(2)) + 1 \geq f(f(f(2) - 1)) + 1 + 1 \geq 3.$$

Qui abbiamo inserito nella nostra formula $f(2)-1$ al posto di n. Questo funziona perché sappiamo già che $f(2)-1$ è almeno 1.
Quindi pare che possiamo dedurre che $f(n) \geq n$. Dato che abbiamo usato il fatto che $f(2)$ era almeno 2 per dimostrare che $f(3)$ è almeno 3, la dimostrazione generale puzza di induzione.
L'induzione non è altro che un piccolo trucco. Consideriamo il caso successivo, ovvero dimostrare che $f(4) \geq 4$. Da (10) sappiamo che $f(4) \geq f(f(3))+1$. Sappiamo già che $f(3) \geq 3$, quindi ci piacerebbe dimostrare che $f(f(3)) \geq 3$, per poter concludere che $f(f(3))+1 \geq 4$. Per farlo vorremmo avere a disposizione un fatto della forma "se $n \geq 3$, allora $f(n) \geq 3$". Il modo più semplice per fare questo è inserire questa informazione nell'induzione che stiamo cercando di dimostrare. Più precisamente, dimostreremo:

Lemma 3.1.1. $f(m) \geq n$ per tutti gli $m \geq n$.

Procediamo per induzione su n.

1. *Passo base* $n = 1$. Questo è ovvio: sappiamo già per ipotesi che $f(m)$ è un intero positivo, quindi $f(m)$ è almeno 1.

2. *Passo induttivo.* Assumiamo che il lemma funzioni per n e cerchiamo di dimostrare che $f(m) \geq n+1$ per tutti gli $m \geq n+1$. Beh, per tutti gli $m \geq n+1$, possiamo usare (10) per ottenere $f(m) \geq f(f(m-1))+1$. Ora $m-1 \geq n$, quindi $f(m-1) \geq n$ (per ipotesi induttiva). Possiamo andare oltre: dato che $f(m-1) \geq n$, allora, di nuovo per l'ipotesi induttiva, otteniamo che $f(f(m-1)) \geq n$. Pertanto, $f(m) \geq f(f(m-1))+1 \geq n+1$ e l' ipotesi induttiva è dimostrata.

Se specializziamo il Lemma 3.1.1 al caso $m = n$, otteniamo il nostro sotto-obiettivo:

$$f(n) \geq n \text{ per tutti gli interi positivi } n. \tag{11}$$

E ora? Beh, come in tutti i problemi con equazioni funzionali, una volta che abbiamo un nuovo risultato, dovremmo giocarci un po' e ricombinarlo con i risultati precedenti. Il nostro unico risultato precedente è (10), quindi possiamo inserire la nostra nuova equazione in (10). L'unico risultato utile che otteniamo è

$$f(n+1) \geq f(f(n))+1 \geq f(n)+1$$

che segue una volta che sostituiamo n con $f(n)$ in (11). In altre parole,

$$f(n+1) > f(n).$$

Questa formula è molto utile: significa che f è una funzione crescente! (non era ovvio da (10), vero?) Ciò significa che $f(m) > f(n)$ se e solo se $m > n$ e quindi che la nostra equazione originale

$$f(n+1) > f(f(n))$$

può essere riformulata come

$$n+1 > f(n).$$

E questa, insieme alla (11), dimostra ciò che volevamo.

Problema 3.2. (Australian Mathematics Competition 1984, pag. 7). Supponiamo che f sia una funzione definita sugli interi positivi che assume valori interi con le seguenti proprietà:

(a) $f(2) = 2$

(b) $f(mn) = f(m)f(n)$ per tutti gli interi positivi m e n

(c) $f(m) > f(n)$ se $m > n$.

Trovare $f(1983)$ (con motivazione, naturalmente).

Ora dobbiamo trovare un valore particolare di f. Il migliore modo è cercare di valutare tutta la funzione f, non solamente $f(1983)$ (in ogni caso 1983 è solo l'anno in cui il problema è stato proposto). Questo significa ovviamente assumere che ci sia un'unica soluzione di f. Ma è implicito nella domanda il fatto che c'è un solo possibile valore di $f(1983)$ (altrimenti ci sarebbe più di una risposta), e data l'ordinarietà di 1983 potremmo ragionevolmente congetturare che ci sia un'unica soluzione per f.
Ora, quali sono le proprietà di f? Sappiamo che $f(2) = 2$. Un'applicazione ripetuta di (b) ci porta a stabilire che $f(4) = f(2)f(2) = 4$, $f(8) = f(4)f(2) = 8$ ecc... Quindi, una semplice induzione mostra che $f(2^n) = 2^n$ per ogni n. Dunque $f(x) = x$ quando x è una potenza di 2. Forse $f(x) = x$ per tutti gli x. Mettendo questa funzione nelle condizioni (a), (b) e (c), vediamo che funziona: $f(x) = x$ è una soluzione di (a), (b) e (c). Quindi, se pensiamo che ci sia una sola soluzione per f, allora deve essere questa. Quindi potremmo voler dimostrare il problema più generale, ma più chiaro:

> La sola funzione dagli interi positivi agli interi che soddisfi (a), (b) e (c) è la funzione identità (cioè $f(n) = n$ per ogni n).

Dobbiamo quindi dimostrare che se f soddisfa (a), (b) e (c), allora $f(1) = 1$, $f(2) = 2$, $f(3) = 3$ e così via. Proviamo innanzitutto a dimostrare che $f(1) = 1$ (con le equazioni funzionali dovremmo prima provare esempi piccoli per avere un'"idea" del problema). Beh, da (c) sappiamo che $f(1) < f(2)$, e sappiamo che $f(2) = 2$, quindi $f(1)$ è meno di 2. E da (b) otteniamo (con $n = 1$ e $m = 2$)

$$f(2) = f(1)f(2).$$

Dunque $2 = 2f(1)$. Questo significa che $f(1)$ deve essere uguale a 1, come desiderato. Abbiamo ora che $f(1) = 1$ e $f(2) = 2$. Cosa possiamo dire di $f(3)$? (a) non è di aiuto e (b) ci dà solamente $f(3)$ in funzione di altri numeri come $f(6)$ o $f(9)$, che allo stesso modo non è di grande aiuto. (c) porta a

$$f(2) < f(3) < f(4).$$

Ma $f(2)$ è 2 e $f(4)$ è 4, quindi

$$2 < f(3) < 4.$$

Ma l'unico intero tra 2 e 4 è 3. Quindi $f(3)$ deve essere 3.
Questo ci dà un indizio: $f(3)$ è 3 solo perché deve essere un intero (notate come questo sia simile al problema precedente, $f(n + 1) > f(f(n))$?). Senza questa restrizione, $f(3)$ avrebbe potuto essere $2,1$ o $3,5$ o qualunque altro valore tra 2 e 4. Vediamo se possiamo usare questo indizio più spesso.
Sappiamo già che $f(4) = 4$; proviamo a individuare il valore di $f(5)$. Usando (c) nella speranza di fare ciò che abbiamo fatto con $f(3)$, otteniamo che

$$f(4) < f(5) < f(6).$$

Ora $f(4)$ è 4. Ma cosa possiamo dire di $f(6)$? Niente panico: 6 è 2 per 3, quindi $f(6) = f(2)f(3) = 2 \times 3 = 6$. Quindi, $f(5)$ è compreso tra 4 e 6, e deve essere 5. Sembra procedere bene. Abbiamo ora calcolato tutti i valori di $f(n)$ fino a $n = 6$. Dato che sembriamo affidarci a risultati passati per raggiungere quelli nuovi, la dimostrazione generale puzza fortemente di induzione. E dato che non stiamo usando solo un risultato precedente, ma molti risultati precedenti, probabilmente abbiamo bisogno dell'induzione *forte*.

Lemma 3.1.2. $f(n) = n$ per ogni n.

Dimostrazione. Usiamo l'induzione forte. Innanzitutto controlliamo il passo base: $f(1) = 1$? Sì, lo abbiamo già mostrato. Assumiamo quindi che $m \geq 2$ e che $f(n) = n$ per tutti gli n più piccoli di m. Vogliamo dimostrare che $f(m) = m$.

Guardando un po' di esempi vedremo presto che dobbiamo considerare due casi: m pari e m dispari.

Caso 1: m è pari. In questo caso possiamo scrivere $m = 2n$ per qualche intero n. n è minore di m, quindi per l'ipotesi induttiva forte $f(n) = n$. Perciò $f(m) = f(2n) = f(2)f(n) = 2n = m$, come desiderato.

Caso 2: m è dispari. Qui scriviamo $m = 2n + 1$. Per (c), $f(2n) < f(m) < f(2n+2)$. Per induzione forte $f(2n) = 2n$ e $f(n+1) = n+1$ dato che $n+1$ e $2n$ sono più piccoli di m. Ora, grazie a (b), $f(2n + 2) = f(2)f(n + 1) = 2(n + 1) = 2n + 2$, quindi la nostra disuguaglianza diventa

$$2n < f(m) < 2n + 2$$

e quindi $f(m) = 2n + 1 = m$, come desiderato. Quindi, in ogni caso, vale l'ipotesi induttiva.
Dunque per induzione forte $f(n)$ deve valere per forza n. Pertanto, per rispondere al nostro problema, $f(1983)$ deve essere 1983, e questo è quanto. □

Esercizio 3.2. Si dimostri che il Problema 3.2 può ancora essere risolto se sostituiamo (a) con la condizione più debole
(a') $f(n) = n$ per almeno un intero $n \geq 2$.

Esercizio 3.3. (*) Si dimostri che il Problema 3.2 può essere ancora risolto se ammettiamo che $f(n)$ sia un numero reale, piuttosto che solamente un intero. (Suggerimento: prima cerchiamo di dimostrare che $f(3) = 3$, confrontando $f(2^n)$ con $f(3^m)$ per vari interi n e m.) Per una sfida aggiuntiva, risolvere il Problema 3.2 con questa assunzione e con (a) rimpiazzata da (a').

Esercizio 3.4. (1986 International Mathematical Olympiad, Q5). (**) Si trovino tutte le funzioni f a valori reali non negativi definite sui reali non negativi (se ce ne sono), tali che

(a) $f(xf(y))f(y) = f(x + y)$ per tutti i reali non negativi x, y;

(b) $f(2) = 0$;

(c) $f(x) \neq 0$ per ogni $0 \leq x < 2$.

(Suggerimento: la prima condizione riguarda il prodotto di valori della funzione, e le altre due riguardano il fatto che una funzione prenda il valore 0 (o diverso da 0). Ora, cosa possiamo dire quando un prodotto fa 0?)

3.2 Polinomi

Molti problemi di algebra riguardano i polinomi in una o più variabili, quindi prendiamoci un'attimo di pausa per richiamare alcune definizioni e risultati su questi polinomi.
Un *polinomio in una variabile* è una funzione, chiamiamola $f(x)$, della forma

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$$

o, per essere più formali,

$$f(x) = \sum_{i=0}^{n} a_i x^i.$$

Gli a_i sono costanti (in questo libro saranno sempre numeri reali) e assumiamo che a_n sia diverso da 0. Chiamiamo n il *grado* di f.
I polinomi in più variabili, diciamo tre variabili per esempio, non hanno la stessa bella forma dei polinomi monodimensionali, ma sono comunque abbastanza utili. In ogni caso, $f(x, y, z)$ è un polinomio in tre variabili se ha la forma

$$f(x, y, z) = \sum_{k,l,m} a_{k,l,m} x^k y^l z^m,$$

dove $a_{k,l,m}$ sono costanti (reali), la somma varia tra i k, l e m non negativi tali che $k + l + m \leq n$ e assumiamo che almeno uno degli $a_{k,l,m}$ diversi da 0 soddisfi $k + l + m = n$. Anche in questo caso chiamiamo n il *grado* di f; i polinomi di grado 2 sono detti *quadratici*, di grado 3 *cubici* e così via... Se il grado è 0, allora il polinomio è detto *banale* o *costante*. Se tutti gli $a_{k,l,m}$ non nulli soddisfano $n = k + l + m$, allora f è detto *omogeneo*. I polinomi omogenei hanno la proprietà che

$$f(tx_1, tx_2, ..., tx_m) = t^m f(x_1, x_2, ..., x_m)$$

per tutti gli $x_1, ..., x_m, t$. Per esempio, $x^2y + z^3 + xz$ è un polinomio di tre variabili (x, y e z) e ha grado 3. Non è omogeneo, perché il termine xz ha grado 2.
Un polinomio f con m variabili si dice *fattorizzato* nei due polinomi p e q se $f(x_1, ..., x_m) = p(x_1, ..., x_m)q(x_1, ..., x_m)$ per tutti gli $x_1, ..., x_m$; p e q sono detti *fattori* di f. Si dimostra facilmente che il grado di un polinomio è uguale alla somma dei gradi dei fattori. Un polinomio è *irriducibile* se non può essere fattorizzato in fattori non banali.
Le *radici* di un polinomio $f(x_1, ..., x_m)$ sono i valori di $(x_1, ..., x_m)$ che danno un valore zero, cosicché $f(x_1, ..., x_m) = 0$. I polinomi di una variabile possono avere tante radici quanto il loro grado; in effetti se si tiene conto delle molteplicità e

delle radici complesse, i polinomi di una variabile hanno sempre esattamente tante radici quante il loro grado. Per esempio, le radici di un polinomio quadratico $f(x) = ax^2 + bx + c$ sono date dalla ben nota formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Le cubiche e i polinomi di quarto grado hanno anch'essi delle formule per il calcolo delle loro radici, ma sono molto più intricate e non molto utili nella pratica. Non appena si arriva ai polinomi di quinto grado o maggiore, non ci sono per niente formule elementari! E i polinomi di due o più variabili sono ancora peggio; tipicamente ci sono un numero infinito di radici.

Le radici di un fattore sono un sottoinsieme delle radici del polinomio originale; questa può essere un'informazione utile per decidere se un polinomio divide un altro oppure no. In particolare, $x - a$ divide $f(x)$ se e solo se $f(a) = 0$, dato che a è radice di $x - a$. In particolare, per ogni polinomio $f(x)$ di una variabile e ogni numero naturale t, $x - t$ divide $f(x) - f(t)$.

Affrontiamo dunque qualche problema sui polinomi.

Problema 3.3. (Australian Mathematics Competition 1987, pag. 13). Siano a, b, c numeri reali tali che

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = \frac{1}{a+b+c} \tag{12}$$

con tutti i denominatori diversi da 0. Dimostrare che

$$\frac{1}{a^5} + \frac{1}{b^5} + \frac{1}{c^5} = \frac{1}{(a+b+c)^5}. \tag{13}$$

A prima vista questo problema sembra semplice. È data esattamente un'unica informazione, quindi dovrebbe essere una sequenza lineare di passi logici a portarci al risultato voluto. Beh, un tentativo iniziale di dedurre la seconda equazione dalla prima potrebbe consistere nell'elevare entrambi i membri di (12) alla quinta potenza, il che ci porta a qualcosa di simile al risultato desiderato, ma con un'accozzaglia di termini confusi nel membro sinistro. Non sembra che ci siano altre manipolazioni ovvie. Questo è quanto, riguardo all'approccio diretto.

A un secondo sguardo, la prima equazione sembra sospetta, come una di quelle equazioni che gli studenti delle scuole superiori sono avvertiti di non usare perché di solito sono ingannevoli. Questo ci dà il nostro primo vero indizio: la prima equazione dovrebbe limitare un bel po' a, b e c. Potrebbe valere la pena di reinterpretare l'equazione (12).

Un denominatore comune sembra essere un buon punto di partenza. Combinando i tre reciproci nel membro di sinistra otteniamo

$$\frac{ab+bc+ca}{abc} = \frac{1}{a+b+c}$$

e, moltiplicando a croce, otteniamo

$$ab^2 + a^2b + a^2c + ac^2 + b^2c + bc^2 + 3abc = abc. \tag{14}$$

A questo punto potremmo pensare alle varie disuguaglianze da usare qui: Cauchy-Schwarz, media aritmetica-media geometrica ecc. (Hardy 1975, pagg. 33-34). Questo non sarebbe male se a, b e c fossero vincolati ad essere positivi, ma non c'è una simile restrizione: in effetti la condizione non può valere se a, b e c sono positivi, dato che $\frac{1}{a+b+c}$ sarebbe più piccolo di tutti e tre i reciproci del membro di sinistra di (12).

Dato che (14) è equivalente a (12) ed è algebricamente più semplice ((14) non contiene reciproci), potremmo cercare di dedurre (13) da (14). Ancora una volta l'approccio diretto non è possibile. Di solito l'unico altro modo per dedurre un'equazione da alcune altre è dimostrare un risultato intermedio o fare qualche sostituzione utile. (Ci sono alternative più esotiche, come considerare (12) come un profilo della funzione $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} - \frac{1}{a+b+c}$ e quindi usare l'analisi per trovare la forma e le proprietà di tale profilo, ma è meglio restare prima sulle opzioni semplici.)

Le sostituzioni non sembrano opportune: le equazioni (12) e (14) sono abbastanza semplici così come sono e le sostituzioni non le renderebbero molto più semplici. Quindi proveremo a indovinare e a dimostrare un risultato intermedio. Il miglior tipo di risultato intermedio è una parametrizzazione, dato che essa può essere sostituita direttamente nell'equazione desiderata. Un modo di parametrizzare è risolvere in una delle variabili, per esempio a. L'equazione (14) non si risolve facilmente in a (a meno che non vogliamo usare la formula per le equazioni di secondo grado). L'equazione (12) si risolve per a e possiamo dimostrare il problema risolvendo per a, b e c a turno e deducendo un risultato intermedio (che per inciso è equivalente al risultato che mostrerò qui sotto. Ma doveva accadere, no?). Ma proverò una strada differente.

Se fallisce una parametrizzazione, si potrebbe semplicemente riformulare (14) in una forma migliore. Le soluzioni di (14) sono sostanzialmente le radici del polinomio $a^2b + b^2a + b^2c + c^2b + c^2a + a^2c + 2abc$. Il migliore modo per trattare con le radici dei polinomi consiste nel fattorizzarli (e viceversa). Quali sono i fattori? Dato che sappiamo che (14) deve implicare in qualche modo (13), dovremmo essere abbastanza fiduciosi nel fatto che ci sia una qualche forma maneggevole di (14) che ci

condurrà a (13) e l'unica forma maneggevole di un polinomio è una scomposizione in fattori. Ma per trovare quali siano, dobbiamo fare degli esperimenti. Il polinomio è omogeneo, quindi dovrebbero esserlo anche i suoi fattori. Il polinomo è simmetrico, perciò i fattori dovrebbero essere reciprocamente simmetrici. Il polinomio è cubico, pertanto dovrebbe esserci un fattore lineare. Dovremmo ora provare fattori della forma $a+b$, $a-b$, $a+b+c$, $a+b-c$ e così via. (Anche cose come $a+2b$ potrebbero funzionare, ma non sono così "carine" e in ogni caso le si può provare in seguito.) Diventa presto evidente (dal Teorema di fattorizzazione) che $a+b$ e, similmente, $b+c$ e $c+a$ sono radici della cubica. È facile verificare che (14) è fattorizzabile in $(a+b)(b+c)(c+a)$. Questo significa che la (12) è vera se e solo se $a+b=0$, $b+c=0$ o $c+a=0$. Il trucco consiste nel sostituire ognuna di queste possibilità in (13).

Esercizio 3.5. Fattorizzare $a^3+b^3+c^3-3abc$.

Esercizio 3.6. Trovare tutti gli interi a, b, c, d tali che $a+b+c+d=0$ e $a^3+b^3+c^3+d^3=24$. (Suggerimento: non è difficile indovinare *alcune* soluzioni di queste equazioni, ma per dimostrare che le abbiamo trovate *tutte*, sostituiamo la prima equazione nella seconda e fattorizziamo.)

La fattorizzazione di polinomi, o la sua impossibilità, è una parte affascinante della matematica. Il seguente problema è istruttivo, perché utilizza quasi tutti i trucchi presenti nel libro per trovare una soluzione.

Problema 3.4. (**) Dimostrare che nessun polinomio della forma $f(x) = (x-a_1)^2(x-a_2)^2\cdots(x-a_n)^2+1$, dove $a_1, ..., a_n$ sono tutti interi, può essere fattorizzato in due polinomi non banali, ognuno a coefficienti interi.

Questo è un enunciato piuttosto generale: ci dice per esempio che il polinomio

$$(x-1)^2(x+2)^2+1 = x^4+2x^3-3x^2-4x+5$$

non può essere fattorizzato in altri polinomi a coefficienti interi. Come possiamo dimostrarlo?
Beh, supponiamo che $f(x)$ sia fattorizzabile in due polinomi non banali a coefficienti interi, $p(x)$ e $q(x)$. Allora $f(x) = p(x)q(x)$ per tutti gli x. Bell'affare. Ma ricordiamo che f ha questa proprietà speciale: è una specie di quadrato più uno. Come possiamo usare questo fatto? Beh, potremmo dire che $f(x)$ è sempre positivo (o addirittura che $f(x) \geq 1$), ma questo non ci dice molto su $p(x)$ e $q(x)$ tranne il

fatto che hanno lo stesso segno. Tuttavia abbiamo un altro dato; f non è solo un vecchio quadrato qualsiasi più uno; il quadrato è il quadrato di una combinazione di fattori lineari. Possiamo usare questi $(x - a_i)$ a nostro vantaggio?
Beh, il migliore fattore che potremmo avere è 0, perché questo renderebbe l'intera espressione 0. (In realtà, ci sono anche casi in cui avere 0 è l'ultima cosa che uno vorrebbe, perché si potrebbe desiderare di semplificare quel fattore.) $(x - a_i)$ è 0 quando x è a_i, quindi abbiamo un'idea: mettiamo un a_i al posto di x. Otteniamo

$$f(a_i) = \cdots (a_i - a_i)^2 \cdots + 1 = 1$$

Tornando a $p(x)$ e $q(x)$, questo risultato significa che

$$p(a_i)q(a_i) = 1.$$

Cosa significa questo? Assai poco, a meno che non si ricordi che p e q hanno coefficienti interi e che gli a_i sono anch'essi interi. Il risultato è che $p(a_i)$ e $q(a_i)$ sono ambedue interi. Abbiamo dunque due interi in cui prodotto è 1. Questo può accadere solo quando gli interi sono entrambi 1 o entrambi -1. In breve,

$$p(a_i) = q(a_i) = \pm 1 \text{ per ogni } i = 1, ..., n.$$

Si dovrebbe stare un po' attenti con la notazione $\pm$ qui; sappiamo che $p(a_1)$ e $q(a_1)$, per esempio, sono uguali uno all'altro, ma $p(a_1)$ e $p(a_2)$ potrebbero avere lo stesso segno o segno opposto, per quello che sappiamo finora.
Abbiamo trovato, più o meno, i valori di $p(a_1), ..., p(a_n)$ e $q(a_1), ..., q(a_n)$, quindi ogni polinomio è "appeso" ad n punti. Ma i polinomi di coefficiente direttore 1 hanno tanti gradi di libertà quanto il loro grado. Ora, dato che $pq = f$, il grado di p più il grado di q è uguale al grado di f, che è $2n$. Questo significa che uno dei polinomi, diciamo p, ha grado al più n. In sintesi, abbiamo un polinomio di grado n ma costretto a passare per n punti dati. Possiamo sperare che questo conduca a una contraddizione, che è quello che cerchiamo.
Cosa sappiamo di un polinomio che ha grado al più n? Beh, che ha al massimo n radici. Sappiamo qualcosa delle radici di p? Beh, p è un fattore di f, quindi le radici di p sono anche radici di f. Quali sono le radici di f? Non ce ne sono! (Beh, nessuna sulla retta reale, almeno.) f è sempre positivo (in effetti, è sempre almeno 1), e quindi non può avere radici. Questo significa che a sua volta p non può avere radici. Cosa significa quando un polinomio non ha radici? Significa che non attraversa mai lo 0, cioè che non cambia mai segno. In altre parole, p è sempre positivo o sempre negativo. Questo ci dà due casi, ma possiamo risparmiare un po' di lavoro osservando che un caso implica l'altro. Infatti se