

equazioni diofantee

PROPOSIZIONE 1 Siano a, b, c interi con $a, b \neq 0$. Allora l'equazione

$$ax + by = c \quad (1)$$


ha soluzioni intere se, e solo se, c é multiplo di un massimo comune divisore d di a e b .

DIM. Se (\bar{x}, \bar{y}) é una soluzione intera della (1), d divide

$$a\bar{x} + b\bar{y} = c,$$

perché d divide sia a che b . Viceversa, se é $c = kd$, con $k \in \mathbb{Z}$, e $d = ma + nb$, risulta

$$c = kd = k(ma + nb) = a(km) + b(kn)$$


e $(\bar{x}, \bar{y}) = (km, kn)$ é una soluzione intera della (1). 

PROPOSIZIONE 2 Nell'ipotesi che l'equazione (1) abbia una soluzione intera (h, k) , sia d un massimo comune divisore di a e b e sia $a = da_1$, $b = db_1$. Allora le soluzioni intere della (1) sono tutte e sole quelle del tipo

$$(h + nb_1, k - na_1), \quad n \in \mathbb{Z}. \quad (2)$$

DIM. É immediato verificare che una coppia del tipo (2) é una soluzione intera della (1). Supponiamo, dunque, che (\bar{x}, \bar{y}) sia una soluzione intera della (1) e osserviamo che, in queste ipotesi, si ha:

$$a(\bar{x} - h) = b(k - \bar{y}) \Rightarrow a_1(\bar{x} - h) = b_1(k - \bar{y})$$

e, poiché a_1 e b_1 sono coprimi, abbiamo che a_1 divide $k - \bar{y}$ e b_1 divide $\bar{x} - h$. Ne segue che esiste un intero n per cui $(\bar{x}, \bar{y}) = (h + nb_1, k - na_1)$ e l'asserto é completamente provato. 

DEFINIZIONE 3 Un elemento $u \in \mathbb{Z}$ si dice *invertibile* se esiste un intero u' tale che $uu' = 1$. ◇

OSSERVAZIONE 4 Gli elementi invertibili in \mathbb{Z} sono 1 e -1 . ◇

DEFINIZIONE 5 Un elemento $a \in \mathbb{Z}$ si dice *irriducibile* se é diverso da 0, 1, -1 e i suoi unici divisori sono quelli banali, cioè 1, -1 , a , $-a$. ◇

ESERCIZIO 6 Provare che un intero a , diverso da 0, 1, -1 , é irriducibile se, e solo se, vale la seguente proprietá:

$$a = bc, \text{ con } b, c \in \mathbb{Z} \Rightarrow b \text{ oppure } c \text{ invertibile.}$$

DEFINIZIONE 7 Un elemento $p \in \mathbb{Z}$ si dice *primo* se é diverso da 0, 1, -1 e se ogni qualvolta divide un prodotto ab , con $a, b \in \mathbb{Z}$, allora divide uno almeno dei fattori. ◇

ESERCIZIO 8 Provare che un intero a é irriducibile (risp. primo) se, e solo se, $-a$ é irriducibile (risp. primo).

PROPOSIZIONE 9 Un numero intero é primo se, e soltanto se, é irriducibile.

DIM. Sia p un primo e supponiamo $p = ab$. Poiché $p|ab$, abbiamo che $p|a$ o $p|b$, cioè $a = ph$ o $b = pk$, con $h, k \in \mathbb{Z}$. Ne segue che $p = phb$ o $p = pak$, cioè $hb = 1$ o $ak = 1$ e quindi b , oppure a , é invertibile. Abbiamo cosí che p é irriducibile.

Sia p un irriducibile e sia $p|ab$. Posto $ph = ab$, supponiamo che p non divida a . Allora é $MCD(a, p) = 1$ ed esistono due interi m, n tali che $ma + np = 1$. Risulta, dunque, $mab + npb = b$ e, dividendo p il primo membro di questa uguaglianza, deve dividere b . Abbiamo cosí che p é primo. ◇

ESERCIZIO 10 Sia p un primo che divide il prodotto $a_1 a_2 \cdots a_k$. Allora p divide almeno uno dei fattori a_1, a_2, \dots, a_k .

teorema fondamentale dell'aritmetica

TEOREMA 11 (teorema fondamentale dell'aritmetica) *Ogni intero $n \geq 2$ può essere fattorizzato nella forma $n = p_1 p_2 \cdots p_k$, ove p_1, p_2, \dots, p_k sono primi positivi (non necessariamente distinti) e tale fattorizzazione è unica, a meno dell'ordine dei fattori.*

DIM. • Sia X l'insieme degli interi $n \geq 2$ che non ammettono una fattorizzazione in primi positivi. Se assumiamo $X \neq \emptyset$, possiamo considerare il minimo m di X .

• L'intero m non è primo (altrimenti $m \notin X$) e quindi è $m = ab$, con $1 < a, b < m$. Ne segue che $a, b \notin X$.

• Gli interi a, b , sono fattorizzabili in primi positivi e da ciò segue che m è fattorizzabile in primi; un assurdo.

• Sia Y l'insieme degli interi $n \geq 2$ che ammettono fattorizzazioni distinte in primi, a meno dell'ordine dei fattori. Se $Y \neq \emptyset$, possiamo considerare il minimo m di Y e due sue diverse fattorizzazioni del tipo desiderato $m = p_1 p_2 \cdots p_k$ e $m = p'_1 p'_2 \cdots p'_l$.

• $p_1 \mid m = p'_1 p'_2 \cdots p'_l \Rightarrow p_1$ divide almeno uno dei p'_j .

Non è restrittivo supporre che $p_1 \mid p'_1$ e da ciò segue $p_1 = p'_1$. Così abbiamo che l'intero $\frac{m}{p_1} \geq 2$ è minore di m e possiede due distinte fattorizzazioni del tipo desiderato

$$\frac{m}{p_1} = p_2 p_3 \cdots p_k = p'_2 p'_3 \cdots p'_l,$$

un assurdo.



teorema fondamentale dell'aritmetica

COROLLARIO 12 Ogni intero $n \geq 2$ può essere scritto nella forma


$$n = p_1^{h_1} p_2^{h_2} \cdots p_k^{h_k},$$

ove p_1, p_2, \dots, p_k sono primi positivi distinti e tale scrittura è unica, a meno dell'ordine dei fattori.


COROLLARIO 13 Sia m un intero tale che $|m| \geq 2$. Allora m possiede una fattorizzazione in primi. Inoltre, se

$$m = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l,$$

con $p_1, p_2, \dots, p_k, q_1, q_2, \dots, q_l$ primi, allora si ha $k = l$ ed esiste una permutazione σ di $\{1, 2, \dots, k\}$ tale che $p_j = \pm q_{\sigma(j)}$, per ogni $j = 1, 2, \dots, k$.

OSSERVAZIONE 14 E' da notare che, se si ammettesse che 1 e -1 fossero primi, il teorema fondamentale dell'aritmetica sarebbe falso. 

TEOREMA 15 (teorema di Euclide) L'insieme P dei numeri primi è infinito.

DIM. Si supponga che $P = \{p_1, p_2, \dots, p_t\}$ sia finito e si ponga $n = 1 + p_1 p_2 \cdots p_t$. Poiché $|n| \geq 2$, esiste un primo p_i che divide n . Ne segue che p_i divide $n - p_1 p_2 \cdots p_t = 1$, un assurdo. 

crivello di Eratostene

ESERCIZIO 16 Sia a un intero maggiore di 2. Provare che, se a non é divisibile per alcun intero n tale che $2 \leq n \leq \sqrt{a}$, allora a é primo. Provare inoltre che, se a non é divisibile per alcun primo positivo minore o uguale di \sqrt{a} , allora a é primo.

ESERCIZIO 17 Sia a un intero maggiore di 2 e si consideri la successione $Pr(a)$ di interi costruita con il seguente algoritmo (crivello di Eratostene):

1. scrivere la successione crescente degli interi da 2 ad a ;
 2. cancellare dalla successione tutti gli interi maggiori di 2 che sono multipli di 2;
 3. se nella nuova successione non vi sono interi maggiori di 2 e minori o uguali di \sqrt{a} terminare l'algoritmo (altrimenti andare al passo successivo);
 4. detto p_1 l'intero che compare dopo 2 nella nuova successione (chi é?), cancellare tutti gli interi maggiori di p_1 che sono multipli di p_1 ;
 5. se nella nuova successione non vi sono interi maggiori di p_1 e minori o uguali di \sqrt{a} terminare l'algoritmo (altrimenti andare al passo successivo);
 6. detto p_2 l'intero che compare dopo p_1 nella nuova successione (chi é?), cancellare tutti gli interi maggiori di p_2 che sono multipli di p_2 ;
- continuare con la stessa regola fino a quando l'algoritmo termina

Provare che $Pr(a)$ é la successione dei numeri primi che sono minori o uguali di a .

distribuzione dei primi

OSSERVAZIONE 18 Uno dei problemi piú interessanti che pone il teorema di Euclide é quello di studiare la distribuzione dei numeri primi nell' insieme dei numeri naturali; in altre parole, si tratta di trovare una formula per il numero $\pi(m, n)$ dei primi p tali che $m \leq p \leq n$. Se si dá uno sguardo ai termini iniziali della successione dei primi positivi, si intuisce che, tranne qualche eccezione, i numeri primi diventano gradualmente piú sporadici.

Osserviamo che la successione $(\pi(n) = \pi(2, n))$ é crescente e che il teorema di Euclide dice che

$$\lim_{n \rightarrow +\infty} \pi(n) = +\infty.$$

Un risultato interessante al riguardo é che la successione $(\pi(n))$ tende asintoticamente all'infinito come la successione $(n/\log n)$, nel senso che

$$\lim_{n \rightarrow +\infty} \frac{\pi(n)}{n/\log n} = 1.$$

A tutt' oggi é aperto il problema del calcolo di una formula esplicita di $\pi(m, n)$. 

ESERCIZIO 19 *Provare che, per ogni intero $n > 1$, la successione finita*

$$n! + 2, n! + 3, \dots, n! + n$$

non contiene numeri primi. Dedurne che, per ogni intero positivo n , esistono due primi consecutivi p, q tali che $q - p \geq n$.

ESERCIZIO 20 *Provare che, se n é un intero maggiore di 1 e p un primo positivo, allora non esiste alcun numero razionale y tale che $y^n = p$.*

primi di Mersenne

ESERCIZIO 21 Provare che, se a, b sono interi positivi risulta

$$2^{ab} - 1 = (2^a - 1)(2^{(b-1)a} + 2^{(b-2)a} + \dots + 2^a + 1).$$

Dedurre che, se $2^h - 1$ é un primo positivo, allora h é un primo. Trovare inoltre il piú piccolo primo positivo p tale che $2^p - 1$ non é un primo.

OSSERVAZIONE 22 I primi della forma $m_p = 2^p - 1$ si chiamano *primi di Mersenne*, dal nome di uno dei matematici che li studi6. E' aperto il problema di stabilire se esistono o meno infiniti primi di Mersenne.

Al momento (febbraio 2000) si conoscono solo trentotto primi di Mersenne, precisamente quelli corrispondenti ai seguenti valori di p : 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593. L'ultimo di questi é il piú grande numero primo conosciuto ed é stato scoperto il *1 giugno 1999* nell'ambito di un'organizzazione amatoriale di nome *GIMPS* (The GREAT Internet Mersenne Prime Search), che si occupa di trovare nuovi primi di Mersenne e pu6 essere contattata via internet attraverso il seguente indirizzo:

<http://www.mersenne.org>.

Su questo sito web si trovano anche molte informazioni sui numeri di Mersenne e, piú in generale, sui numeri primi di forme particolari.



primi di Fermat

ESERCIZIO 23 *Provare che, se $2^h + 1$ é primo, allora h non puó avere fattori dispari, cioè deve essere una potenza di 2.*

OSSERVAZIONE 24 I numeri della successione

$$f_n = (2^{2^n} + 1)$$

si chiamano *numeri di Fermat*, dal nome del matematico che li introdusse. I cinque termini iniziali della successione sono

$$f_0 = 3, f_1 = 5, f_2 = 17, f_3 = 257, f_4 = 65537$$

e risultano primi; per questo motivo lo stesso Fermat congetturó che erano primi tutti i termini della successione. Fu *L.Euler* a provare la falsitá della congettura trovando che

$$f_5 = 4294976297$$

si decompone nel prodotto dei due primi 641 e 6700417.

Il problema di stabilire se un numero di Fermat é primo (*primo di Fermat*) é molto difficile; ancora oggi

$$f_0, f_1, f_2, f_3, f_4$$

sono gli unici primi di Fermat noti e non si sa se i primi di Fermat sono in numero finito o infinito.

E' noto, per esempio, che i numeri da f_6 a f_{23} non sono primi e f_{24} é il piú piccolo numero di Fermat per cui non si sa se é primo.

