PROBLEMI RISOLTI ED IRRISOLTI IN TEORIA DEI NUMERI.

PH. ELLIA

Indice

Date: June 9, 2013.

1. Pitagora, Euclide, Diofante.

1.1. **Pitagora.**

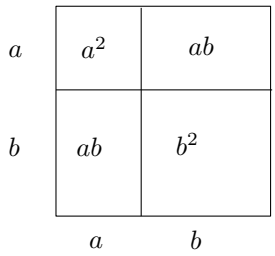
Pitagora (600 anni prima di Cristo circa):

- *Tutto è numero.* Numeri interi o frazioni ("rapporti")
- musica ((12, 8, 6): 12/6 = 2 ottava, 8/6=4/3 quarta, 12/8=3/2 quinta)
- Il teorema di Pitagora
- Rappresentazione geometrica dei numeri (numeri triangolari)

1.2. **Numeri "geometrici".**

Gli Antichi Greci non avevano il nostro sistema di numerazione, per loro i numeri misuravano grandezze geometriche, o meglio rapporti tra grandezze geometriche. Per dare un'idea ecco come (forse?) dimostravano l'identità algebrica $(a+b)^2 = a^2 + b^2 + 2ab$.

$(a+b)^2 = a^2 + b^2 + 2ab$



Vediamo adesso come calcolavano la somma $t_n = 1 + 2 + 3 + ... + n$. Consideriamo una tabella $n \times n$. La tabella contiene n^2 entrate. Consideriamo le seguenti entrate

$$\begin{array}{c} 1 \\ 2 \\ 3 \\ \vdots \\ n \end{array} \begin{pmatrix} \mathbf{0} & & & & \\ 0 & \mathbf{0} & & & \\ 0 & 0 & \mathbf{0} & & \\ \vdots & & & & \\ 0 & 0 & 0 & \cdots & \mathbf{0} \end{pmatrix}$$

I tondini sulla diagonale (in grassetto) più quelli sotto la diagonale rappresentano esattamente la somma $t_n = 1 + 2 + 3 + ... + n$. Sulla diagonale abbiamo n tondini (perché ogni riga interseca la diagonale in un unico punto, quindi ci sono altrettanto punti sulla diagonale che il numero di righe). Se togliamo la diagonale dalla tabella rimangono $n^2 - n$ entrate: quelle sotto la diagonale (S_t) e quelle sopra la diagonale (S_p). Per simmetria $S_t = S_p$, quindi $n^2 - n = S_t + S_p = 2S_t$, pertanto $S_t = (n^2 - n)/2$. Quindi i tondini sulla diagonale più quelli sotto la diagonale sono $n + (n^2 - n)/2 = n(n + 1)/2$. In conclusione:

$$t_n = n(n + 1)/2 \tag{1}$$

Un numero della forma $n(n+1)/2$ si chiama un *numero triangolare* (il perché si evince dalla figura).

Tutto questo è molto ingegnoso ma ecco un'altra dimostrazione più veloce: scriviamo i nostri numeri da 1 a n su una riga e riscriviamoli sulla riga sotto ma nell'ordine opposto e facciamo le somme per colonne:

$$\begin{array}{ccccc} 1 & 2 & 3 & \cdots & n \\ n & n-1 & n-2 & \cdots & 1 \\ - & - & - & \cdots & - \\ n+1 & n+1 & n+1 & \cdots & n+1 \end{array}$$

Abbiamo n pacchetti la cui somma vale sempre $n + 1$, quindi $2t_n = n(n + 1)$, ossia $t_n = n(n + 1)/2$.

Conoscendo t_n possiamo calcolare $s_n = 1^2 + 2^2 + 3^2 + ... + n^2$. Infatti se riprendiamo la nostra figura vediamo che:

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ \vdots \\ n-1 \\ n \end{array} \quad \overbrace{}^{n-1} \quad \left(\begin{array}{cccccc} \mathbf{0} & \times & \times & \times & \cdots & \times \\ 0 & \mathbf{0} & \times & \times & & \vdots \\ 0 & 0 & \mathbf{0} & \times & \times & \vdots \\ \vdots & & & & & \\ \vdots & & & & & \times \\ 0 & 0 & 0 & 0 & \cdots & \mathbf{0} \end{array} \right) \left\{ \begin{array}{c} \\ \\ \\ \\ \\ n-1 \end{array} \right.$$

Le crocette sono il triangolo (rovesciato) corrispondente a $t_{n-1} = 1 + 2 + ... + (n-1)$. Concludiamo che

$$n^2 = t_n + t_{n-1} \tag{2}$$

(con $t_0 := 0$). Quindi $1^2 + 2^2 + ... + n^2 = (t_1 + ... + t_n) + (t_1 + ... + t_{n-1})$. Ponendo $T_n = t_1 + ... + t_n$, abbiamo $s_n = T_n + T_{n-1}$. Rimane da calcolare T_n.

Possiamo rappresentare T_n col seguente triangolo:

$$\begin{array}{ccccccccccc} & & & & & & 1 & & & & \\ & & & & & 1 & + & 2 & & & \\ & & & & 1 & + & 2 & + & 3 & & \\ & & & \cdots & & & & & & \cdots & \\ & & 1 & + & 2 & & & & & + & n \end{array}$$

Riprendiamo la stessa figura ma scriviamo ogni riga in senso opposto (cioè iniziando dalla fine):

$$\begin{array}{ccccccccccc} & & & & & & 1 & & & & \\ & & & & & 2 & + & 1 & & & \\ & & & & 3 & + & 2 & + & 1 & & \\ & & & \cdots & & & & & & \cdots & \\ & & n & + & & & & & & + & 1 \end{array} \tag{3}$$

Adesso facciamo la "somma" dei due triangoli, coefficiente per coefficiente. Come abbiamo visto nella dimostrazione "veloce" della formula per t_n, tutti i coefficienti della seconda riga saranno uguali a $3 = 2 + 1$, quelli della terza a

$4 = 3 + 1$, quelli della k-esima a $k + 1$ perché:

$$\begin{array}{ccccccc} 1 & & 2 & & 3 & \cdots & k \\ k & & k-1 & & k-2 & \cdots & 1 \\ - & & - & & - & \cdots & - \\ k+1 & & k+1 & & k+1 & \cdots & k+1 \end{array}$$

Concludiamo che $2T_n$ è rappresentato dal triangolo:

$$\begin{array}{ccccccccccc} & & & & & 2 & & & & & \\ & & & & 3 & + & 3 & & & & \\ & & & 4 & + & 4 & + & 4 & & & \\ & & \cdots & & & & & & \cdots & & \\ & (n+1) & + & & & & & & + & (n+1) & \end{array}$$

Adesso consideriamo ancora un altro modo di scrivere T_n: prendiamo il triangolo in (3) e lo facciamo girare di 120^o (oppure considerare le diagonali):

$$\begin{array}{ccccccccccc} & & & & & n & & & & & \\ & & & & (n-1) & + & (n-1) & & & & \\ & & & (n-2) & + & (n-2) & + & (n-2) & & & \\ & & \cdots & & & & & & & \cdots & \\ & 1 & + & & & & & & & + & 1 \end{array}$$

Anche qui tutti i termini della k-esima riga sono uguali e valgono $n + 1 - k$.

Sommando i due ultimi triangoli otteniamo che $3T_n$ è rappresentato da

$$\begin{array}{ccccccccccc} & & & & & (n+2) & & & & & \\ & & & & (n+2) & + & (n+2) & & & & \\ & & & (n+2) & + & (n+2) & + & (n+2) & & & \\ & & \cdots & & & & & & & \cdots & \\ & (n+2) & + & & & & & & & + & (n+2) \end{array}$$

Infatti nel primo triangolo gli elementi della riga k valgono tutti $k + 1$, nel secondo valgono tutti $n+1-k$, quindi facendo la somma $k+1+n+1-k = n+2$.

Concludiamo che $3T_n = (n+2)t_n = n(n+1)(n+2)/2$. Si ricava poi facilmente:

$$s_n := 1^2 + 2^2 + ... + n^2 = n(n+1)(2n+1)/6 \tag{4}$$

Rispetto ai quadrati osserviamo le seguenti figure:

$1+3+5=3^2$: $\begin{matrix} \bullet & \bullet & \bullet \\ \times & \times & \bullet \\ \bullet & \times & \bullet \end{matrix}$ $1+3+5+7=4^2$: $\begin{matrix} \times & \times & \times & \times \\ \bullet & \bullet & \bullet & \times \\ \times & \times & \bullet & \times \\ \bullet & \times & \bullet & \times \end{matrix}$

Vediamo così che:

$$1 + 3 + 5 + ... + (2n-1) = n^2 \tag{5}$$

Cioè la somma dei primi n numeri dispari è uguale a n^2.

Adesso osserviamo che:

$$\begin{aligned} 1^3 &= 1 \\ 2^3 &= 3+5 \\ 3^3 &= 7+9+11 \\ 4^3 &= 13+15+17+19 \end{aligned}$$

Quindi $1^3 + 2^3 = 1 + 3 + 5 = 3^2$, $1^3 + 2^3 + 3^3 = 1 + 3 + 5 + 7 + 9 + 11 = 6^2$, $1^3 + 2^3 + 3^3 + 4^3 = 1 + 3 + ... + 19 = 10^2$. Quindi 1^3 è la somma del primo numero dispari, 2^3 è la somma dei successivi 2 numeri dispari, 3^3 è la somma dei successivi 3 numeri dispari, ecc... *se le cose vanno avanti così*, n^3 è la somma di n numeri dispari, l'ultimo dei quali è il k-esimo numero dispari dove $k = 1 + 2 + 3 + ... + n = t_n$. Wow!

1^3	$=$	1	1 primo numero dispari
2^3	$=$	$3+5$	2 numeri dispari successivi
3^3	$=$	$7+9+11$	3 numeri dispari successivi
4^3	$=$	$13+15+17+19$	4 numeri dispari successivi
$\cdots$	$\cdots$	$\cdots$	$\cdots$
n^3	$=$	$\bullet + \bullet + \bullet + \bullet + \cdots + \bullet$	n numeri dispari successivi

Sommando tutto: $1^3+2^3+...+n^3$ è la somma dei primi $1+2+3+...+n=t_n$ numeri dispari, cioè:

$$1^3+2^3+3^3+...+n^3=1+3+5+...+(2t_n-1) \tag{6}$$

Usando (5) viene:

$$1^3+2^3+3^3+...+n^3=(t_n)^2=n^2(n+1)^2/4 \tag{7}$$

Ossia la somma dei primi n cubi è uguale al quadrato della somma dei primi n numeri!! Spettacolare!!

■ **Attenzione:** La dimostrazione della formula (7) è **incompleta**, infatti abbiamo supposto, ma *non dimostrato*, che l'ennesimo cubo era la somma di n numero dispari successivi l'ultimo dei quali era il t_n-esimo numero dispari (cf "se le cose vanno avanti così"). Ma adesso che abbiamo un'idea di cosa sia la formula, possiamo provare a dimostrarla per *induzione*. Cioè mostriamo che la formula è vera per $n=1$: $1^3=1^2.2^2/4=1$, fatto. Adesso mostriamo che se la formula è vera per $n-1$, allora è vera anche per n: $1^3+2^3+...+(n-1)^3+n^3=[1^3+2^3+...+(n-1)^3]+n^3=\frac{(n-1)^2n^2}{4}+n^3$; abbiamo usato che la formula è vera per $n-1$. Adesso: $\frac{(n-1)^2n^2}{4}+n^3=\frac{(n-1)^2n^2+4n^3}{4}=\frac{n^2[(n-1)^2+4n]}{4}=\frac{n^2(n+1)^2}{4}$, che è proprio la nostra formula, che è quindi vera anche per n.

Riassumendo, la formula è vera per $1(=n-1)$, quindi è vera per $n=2$; essendo vera per 2 è vera anche per 3 ecc... e la nostra formula è vera per ogni n. Un altro modo di vederlo è il seguente: sia $X=\{n \mid$ la formula è falsa per $n\}$. Se X non è vuoto, ha un più piccolo elemento $n_0>1$ ($n_0\in X$ e $\forall n\in X, n\geq n_0$). In particolare $n_0-1\geq 1$ e la formula è vera per n_0-1 (perché $n_0-1\notin X$). Questo porta a un assurdo perché sappiamo che se la formula è vera per n_0-1, allora lo è anche per n_0. Concludiamo che X è vuoto.

Il metodo di dimostrazione per induzione (da usare solo per proprietà $P(n), n\in\mathbb{N}$) è uno degli strumenti più potenti della matematica.

1.3. **Divisori di un numero, numeri perfetti.**

I Pitagorici classificavano i numeri in tre categorie: i numeri *difettivi, abbondanti e perfetti*. Un numero è difettivo (risp. abbondante) se la somma dei suoi divisori (escluso il numero stesso) è inferiore (risp. superiore) al numero. Per esempio i divisori di 8 sono $Div(8) = \{1, 2, 4, 8\}$ e $1 + 2 + 4 = 7 < 8$, 8 è difettivo. Si verifica facilmente che 12 è abbondante.

Un numero intero n è *perfetto* se è uguale alla somma dei suoi divisori (escluso se stesso). Se indichiamo con $\sigma(n)$ la somma di tutti i divisori di n, n è perfetto se $\sigma(n) = 2n$. Per esempio i divisori di 6 sono $Div(6) = \{1, 2, 3, 6\}$ e $\sigma(6) = 1 + 2 + 3 + 6 = 2 \times 6$. Il prossimo numero perfetto è 28. I successivi sono: 496, 8128.

Questi numeri sono tutti pari e terminano alternativamente per 6 e per 8.

Il problema seguente risale ai Pitagorici:

Problema 1.

- *Esiste un numero perfetto dispari?*
- *Esistono infiniti numeri perfetti?*

Come vedremo questo problema (oggi noto come *the oldest open problem in mathematics*) è, in parte, all'origine di notevoli sviluppi in teoria dei numeri e non solo...

1.4. **Euclide.**

Euclide (300 anni circa prima di Cristo):

Gli *Elementi* di Euclide segnano la nascita della matematica come scienza ipotetico-deduttiva: cioè si parte da una serie di assiomi ("veri") e con ragionamenti logici si dimostrano teoremi. Usando gli assiomi e i teoremi dimostrati si prova a dimostrare teoremi nuovi.

La fisica, la chimica, la biologia ecc... sono *scienze sperimentali*; la matematica non è una scienza sperimentale. Questo spiega che la matematica degli Antichi Greci sia ancora valida, mentre la fisica dell'antichità (o del Medio-Evo) è essenzialmente obsoleta.

1.5. **Divisione euclidea e massimo comune divisore.**

Divisione euclidea:

Siano due interi $b > a > 0$, allora possiamo dividere ("divisione con resto") b per a: $b = aq + r, 0 \leq r < a$. Infatti abbiamo $b - a > 0$ se $b - a < a$ si pone $r = b - a$, altrimenti si considera $b - 2a$: $b - 2a > 0$, se $b - 2a < a$ si pone $r = b - 2a$, altrimenti si considera $b - 3a$ ecc... In altri termini se q è il numero massimo di volte che a "sta" in b, allora $b - qa \geq 0$ e $r = b - qa < a$ (altrimenti a ci starebbe ancora un'altra volta ;-). Questa è la *divisione euclidea*.

Osservazione 1.1. *Nel seguito considereremo solo numeri interi positivi ($n \in \mathbb{N} = \{0, 1, 2, ...\}$), ma la divisione euclidea può essere definita anche con numeri interi negativi.*

Massimo comune divisore.

Definizione 1.2. *Se a, b sono due interi positivi il massimo comune divisore (MCD), m, di a, b è, come indica il nome, il più grande divisore comune a a e b: $m \mid a$ e $m \mid b$, inoltre se $d \mid a$ e $d \mid b$, allora $d \leq m$. Si nota $m = (a, b)$ (o anche $MCD(a, b)$).*

Due interi a, b sono primi tra di loro *se $(a, b) = 1$.*

In altri termini se $Div(n)$ indica l'insieme dei divisori di n, il MCD (a, b) è il più grande elemento dell'insieme $Div(a) \cap Div(b)$; è ben definito perché $Div(a) \cap Div(b)$ è un insieme finito, non vuoto (contiene sempre 1).

Sia $I = \{ax + by \mid x, y \in \mathbb{Z}\}$ ($\mathbb{Z} := \{... - 2, -1, 0, 1, 2, ...\}$ è l'insieme degli interi positivi o negativi) e sia $I_+ = \{z \in I \mid z > 0\}$. Osserviamo che I_+ è non vuoto: $a, b \in I_+$. Sia $M = au + bv$ il più piccolo elemento di I_+. Se $z \in I_+$, la divisione euclidea fornisce: $z = Mq + r, 0 \leq r < M$. Abbiamo $r = z - Mq = ax + by - q(au + bv) = a(x - qu) + b(y - qv) \in I$. Se $r \neq 0$, allora $r \in I_+$, ma questo contraddice la minimalità di M, quindi $r = 0$ e $z = qM$. Quindi ogni elemento di I_+ è un multiplo di M. Se $z \in I$, $z < 0$, allora $-z \in I_+$, $-z = bM$ per un qualche b e $z = -bM$, quindi ogni elemento di I è un multiplo di M. Mostriamo che $M = (a, b)$.

Intanto siccome $a, b \in I$, a, b sono multipli di M, cioè $M \mid a$ e $M \mid b$. Sia d un divisore comune a a, b. Siccome $M = au + bv$ e siccome $d \mid a$ e $d \mid b$, viene $d \mid M$, in particolare $d \leq M$. Pertanto $M = (a, b)$. La cosa importante per il seguito è:

Lemma 1.3. (Lemma di Bézout.)
Siano a, b due interi positivi e sia $M = (a, b)$ il loro MCD, allora esistono degli interi (positivi o negativi) u, v tali che: $M = au + bv$.

1.6. **L'algoritmo di Euclide.**

Quanto visto prima mostra l'esistenza della relazione (fondamentale) $M = au + bv$ ma non permette di calcolare M e tanto meno di trovare degli interi u, v soddisfacenti la relazione. L'algoritmo di Euclide colma queste lacune.

Dati due numeri $a, b\,(a < b)$ si procede come segue: si divide b per a

$$b = aq_0 + a_1,\ 0 \leq a_1 < a =: a_0$$

Se $a_1 \neq 0$, si divide $a = a_0$ per a_1 e si procede così fino ad ottenere un resto nullo:

$$\begin{aligned}
b &= a_0q_0 + a_1, && 0 < a_1 < a_0\\
a_0 &= a_1q_1 + a_2, && 0 < a_2 < a_1\\
a_1 &= a_2q_2 + a_3, && 0 < a_3 < a_2\\
&\cdots \quad\quad \cdots &&\\
a_{n-3} &= a_{n-2}q_{n-2} + a_{n-1} &&\\
a_{n-2} &= a_{n-1}q_{n-1} + a_n, && 0 < a_n < a_{n-1}\\
a_{n-1} &= a_nq_n &&
\end{aligned}$$

In queste condizioni il MCD di a e b è a_n, l'ultimo resto non nullo, si nota $(a, b) = a_n$.

Perché siamo sicuri che avremo un resto nullo?

Se guardiamo gli a_i abbiamo: $a = a_0 > a_1 > a_2 > a_3 > \cdots > a_{n-1} > a_n > 0$, gli a_i sono tutti numeri interi compresi tra a e 0 e quindi il procedimento non può continuare all'infinito senza raggiungere zero.

Vediamo che a_n divide a e b:

$a_n \mid a_{n-1}$ (ultima equazione), quindi divide a_{n-2} (penultima equazione). Adesso siccome a_n divide a_{n-1} e a_{n-2}, divide anche a_{n-3}. Procedendo di questo passo arriviamo a a_n divide a_2 e a_1, quindi divide $a = a_0$ e finalmente $a_n \mid b$.

Finalmente vediamo che a_n è il più grande divisore comune di a e b:

Se d divide $a = a_0$ e b, allora divide a_1 (prima equazione), poi se divide a_0 e a_1 divide a_2 ecc... si arriva a $d \mid a_{n-2}$ e $d \mid a_{n-1}$, quindi $d \mid a_n$, pertanto $d \leq a_n$.

Se i puntini e gli ecc... vi danno fastidio, rifate i ragionamenti con un piccolo numero di passi, per esempio:

$$\begin{aligned} b &= a_0 q_0 + a_1, \quad 0 < a_1 < a_0 \\ a_0 &= a_1 q_1 + a_2, \quad 0 < a_2 < a_1 \\ a_1 &= a_2 q_2 + a_3, \quad 0 < a_3 < a_2 \\ a_2 &= a_3 q_3 + a_4, \quad 0 < a_4 < a_3 \\ a_3 &= a_4 q_4 \end{aligned}$$

Ritroviamo il Lemma 1.3:

Lemma 1.4. *Siano a, b due interi e sia $m = (a, b)$, allora esistono due interi (positivi o negativi) u, v, tali che $au + bv = m$.*

Dimostrazione. Abbiamo $a_n = a_{n-2} - a_{n-1}q_{n-1} = f(a_{n-2}, a_{n-1})$. L'equazione successiva ci permette di esprimere a_{n-1} in funzione di a_{n-3}, a_{n-2}, quindi a_n si esprime (linearmente) in funzione di a_{n-2}, a_{n-3}. L'equazione successiva ci darà a_{n-2} in funzione di a_{n-3}, a_{n-4} e così via fino ad arrivare a $a_n = ea_0 + fa_1$. Ma $a_1 = b - a_0 q_0$, quindi $a_n = (e - fq_0)a_0 + fb$, visto che $a = a_0$ questa è l'espressione cercata. □

Esempio 1.5. *Per trovare l'M.C.D. di* 70 *e* 6*:*

$$70 = 6.11 + 4$$

$$6 = 4.1 + 2$$

$$4 = 2.2$$

Quindi $(70, 6) = 2$. *Inoltre* $2 = 6 - 4$, $4 = 70 - 6.11$, *quindi* $2 = 6 - 70 + 6.11 = 6.12 - 70.1$.

Osservazione 1.6. *Gli interi u, v del Lemma 1.4 non sono univocamente determinati. Infatti sia g un divisore comune a a, b, $au + bv = m$; allora $(u + k\frac{b}{g})a + (v - k\frac{a}{g})b = g$. Per esempio $(a, b) = (6, 70)$, allora $g = 2$ e abbiamo visto che $(u = 12, v = -1)$ soddisfa le condizioni e $(12 + k\frac{70}{2}).6 + (-1 - k\frac{6}{2}).70 = 2$. Per $k = 1$, viene:* $47 \times 6 - 4 \times 70 = 2$.

1.7. **Il teorema fondamentale dell'aritmetica.**

Euclide definisce per la prima volta la nozione di numero primo:

Definizione 1.7. *Un intero $p > 1$ è primo se i suoi unici divisori sono* 1 *e p.*

Il numero 1 (unità) ha uno statuto speciale: 1 divide ogni numero ($1.n = n$).

I numeri primi ≤ 20 sono: $2, 3, 5, 7, 11, 13, 17, 19$.

Un intero (> 1) e sia primo, sia composto. Se n non è primo allora $n = ab, 1 < a, b < n$. I numeri primi sono gli *atomi* dei numeri (non possono essere divisi). Vediamo adesso che ogni numero è "composto" (in modo unico) da numeri primi.

Lemma 1.8 (Lemma di Euclide)**.**
Se $a \mid bc$ e se $(a, b) = 1$, allora $a \mid c$.
In particolare se p è primo e se $p \mid ab$, allora $p \mid a$ o $p \mid b$.

Dimostrazione. Siccome $(a, b) = 1$, abbiamo $au + bv = 1$, moltiplicando per c: $acu + bcv = c$. Siccome $a \mid acu$ e $a \mid bcv$, a divide il membro di sinistra, quindi $a \mid c$.

Se $p \mid a$, abbiamo finito. Altrimenti $(a, p) = 1$ (perché gli unici divisori di p sono 1 e p), per quanto appena visto $p \mid b$. □

Sia $n > 0$ un intero e sia $Div(n) = \{1 = d_1, d_2, ..., d_{r-1}, d_r = n\}$, l'insieme dei suoi divisori con $1 < d_2 < d_3 < \cdots < d_{r-1} < d_r$. Con queste notazioni necessariamente d_2 è primo (se $a \mid d_2$ è un divisore non banale $1 < a < d_2$, allora $a \mid n$, contro la minimalità di d_2).

Quindi:

Lemma 1.9. *Ogni numero intero $n > 1$ ammette un divisore primo.*

Proposizione 1.10. *Ogni numero $n > 1$ si scrive come un prodotto di numeri primi.*

Dimostrazione. Sia $m > 1$ il più piccolo numero che non si scrive come un prodotto di primi. In particolare m non è primo, quindi $m = ab, 1 < a, b < m$. Siccome $a < m$, a si scrive come un prodotto di primi: $a = p_1...p_r$. Nello stesso modo $b = q_1...q_t$. Segue che $m = ab = p_1...p_r q_1...q_t$ si scrive come un prodotto di primi: assurdo. □

Teorema 1.11 (Il teorema fondamentale dell'aritmetica)**.**
Ogni numero intero $n > 1$ si scrive in modo unico (a meno dell'ordine dei fattori) come un prodotto di numeri primi.
La scrittura $n = p_1^{a_1} p_2^{a_2}...p_r^{a_r}$ con p_i primo $\forall i$, $p_1 < p_2 < ... < p_r$ è unica.

Dimostrazione. Abbiamo già visto che ogni numero si scrive come un prodotto di primi, rimane da vedere che questa scrittura è unica (a meno dell'ordine dei fattori). Sia $n = p_1...p_r = q_1...q_t$, p_i, q_j primi. Allora $p_1 \mid q_1.(q_2...q_t)$, quindi (Lemma 1.8) $p_1 \mid q_1$ o $p_1 \mid q_2...q_t$. Nel secondo caso $p_1 \mid q_2.(q_3...q_t)$, quindi $p_1 \mid q_2$ o $p_1 \mid q_3.(q_4...q_t)$. Andando avanti così vediamo che p_1 divide uno dei q_j. Riordinando semmai gli indici possiamo assumere $p_1 \mid q_1$. Siccome p_1 e q_1 sono primi, questo implica $p_1 = q_1$. Semplificando per p_1 abbiamo: $p_2...p_r = q_2...q_t$. Ripetendo il procedimento con p_2 e successivamente con gli altri p_i, vediamo che $r = t$ e (dopo riordino degli indici) $p_i = q_i$ per ogni i. □

Quindi per esempio: $60 = 2^2.3.5$, $140 = 2^2.5.7$, ecc...

I numeri primi sono i "mattoni" dell'aritmetica. A questo punto è naturale chiedersi se l'insieme dei numeri primi è o meno infinito.

1.8. **La ripartizione dei numeri primi e problemi connessi.**

Il primo risultato in merito risale a Euclide:

Teorema 1.12 (Euclide)**.**
L'insieme dei numeri primi è infinito.

Dimostrazione. Indichiamo con $n!$ (n fattoriale) il prodotto $1.2.3....n$. Consideriamo $n!+1 = 1.2.3...n+1$. Se $1 < d \leq n$, allora $d \nmid n!+1$. Infatti $\frac{n!+1}{d} = \frac{1.2...d...n}{d} + \frac{1}{d}$; il primo termine è un intero (si può semplificare per d), ma il secondo termine $\frac{1}{d}$ non è un intero. Per il Lemma 1.9, $n!+1$ ammette un divisore primo, p. Per quanto visto $p > n$. Quindi per ogni n, esiste p primo con $p > n$, pertanto l'insieme dei numeri primi è infinito. □

Osservazione 1.13. *Questa non è la dimostrazione di Euclide, Euclide ragiona per assurdo: se $\{p_1, ..., p_r\}$ è l'insieme di tutti i numeri primi, allora $N = p_1...p_r + 1$ non ammette nessun divisore primo, in contraddizione con il Lemma 1.9; assurdo, quindi l'insieme dei numeri primi è infinito.*

Problema 2. *Come si fa a vedere se un dato numero n è o meno primo?*

Un metodo brutale consiste nel vedere se esiste un numero più piccolo di n che lo divide, quindi si prova con $2, 3, 4, 5$ ecc... fino a $n-1$. Se nessuno di questi numeri divide n allora n è primo. Si può migliorare questo approccio brutale con la seguente osservazione: se $n = ab$ con $a \leq b$, allora $a \leq \sqrt{n}$ e $b \geq \sqrt{n}$. Infatti se $a > \sqrt{n}$, allora $\sqrt{n} < a \leq b$ e $ab > (\sqrt{n})^2 = n$: assurdo. Quindi $a \leq \sqrt{n}$. Nello stesso modo $b \geq \sqrt{n}$. Quindi i divisori di n sono *simmetrici* rispetto a $\sqrt{n}$. In particolare n ha un numero dispari di divisori se e solo se n è un quadrato.

Quindi se n non ha nessun divisore non banale $\leq \sqrt{n}$, allora n è primo. Quindi basta provare gli interi nell'intervallo $[2, \sqrt{n}]$.

Si può ancora migliorare se $2 \nmid n$ (cioè se n è dispari) allora nessun numero pari può dividere n e basta provare con quelli dispari. Se $3 \nmid n$, allora nessun multiplo di 3 può dividere n e possiamo cancellare dalla lista i multipli (dispari) di 3 $(9, 15, ...)$. Il prossimo numero da provare è 5. Se $5 \nmid n$, possiamo cancellare i multipli di 5, ecc... Questo procedimento noto come crivello di Erastotene, serve anche a fare la lista dei numeri primi $\leq N$ dove N è un numero dato (provate a fare la lista dei primi ≤ 50).

Come vedremo più avanti il sapere determinare se un numero è o meno primo è un problema fondamentale con applicazioni pratiche alla crittografia.

L'insieme dei numeri primi è infinito, ma quanto? Cioè se $\pi(x) = \#\{p \mid p \leq x, p \text{ primo } \}$ (quindi la funzione $\pi(x)$ conta il numero di primi $\leq x$), cosa possiamo dire sull'ordine di grandezza di $\pi(x)$? Abbiamo:

Teorema 1.14. (Il teorema dei numeri primi.)
Con le notazioni precedenti: $\pi(x) \sim \dfrac{x}{\log(x)}$ *quando* x *tende a* $+\infty$.
Cioè $\lim_{x\to+\infty} \dfrac{\pi(x).\log(x)}{x} = 1$.

Questo teorema è stato dimostrato, in modo indipendente, da Hadamard e de la Vallée-Poussin nel 1896. La dimostrazione usa tecniche sofisticate di analisi complessa. La congettura di Riemann, forse il problema aperto più importante di tutta la matematica, permetterebbe di avere una stima migliore su $\pi(x)$.

Per quanto riguarda la distribuzione dei numeri primi va notato anche il seguente risultato:

Teorema 1.15. ("Postulato di Bertrand", teorema di Tchebycheff)
Per ogni $n \geq 1$, *l'intervallo* $[n, 2n]$ *contiene un numero primo.*

Osservare che esistono intervalli arbitrariamente grandi che non contengono nessun numero primo. Per esempio $I_k = [k! + 2, k! + k]$ non contiene nessun numero primo. Infatti se $n \in I_k$, allora $n = k! + t$ con $2 \leq t \leq k$, abbiamo $t \mid k! = 1.2...t...k$ e $t \mid t$, quindi $t \mid n$. Siccome $1 < t < n$, n non è primo. Questo fatto non contraddice il Teorema 1.15.

Quanto possono essere vicini due numeri primi? Siccome 2 è l'unico numero primo pari, l'unica coppia di primi consecutivi è $(2, 3)$. Possiamo cercare coppie di primi la cui differenza è due, per esempio $(3, 5), (5, 7), (11, 13)$; due primi p, q con $q = p+2$ vengono chiamati *primi gemelli*. Un problema aperto famoso è la seguente:

Congettura 1. *Esistono infiniti primi gemelli.*

Poche settimane fa il matematico Yitang Zhang ha annunciato di avere dimostrato che esistono infiniti primi p, q con $q - p \leq 70.000.000$. Anche se

70.000.000 è molto più grande di 2 (non sono gemelli, neanche cugini ma parenti lontanissimi ;-), questo risultato, se confermato, sarebbe il primo progresso importante verso la congettura dei primi gemelli.

Abbiamo $2^2+1=5$, $4^2+1=17$, $6^2+1=37$, tutti primi (ma $8^2+1=65$ non è primo). Da cui il:

Problema 3. *Esistono infiniti primi della forma n^2+1?*

Se non vado errato gli esperti pensano che la risposta sia affermativa, ma nessuno sa come dimostrarlo.

Abbiamo $4=2+2$, $6=3+3$, $8=3+5$, $10=5+5=3+7$... La famosa congettura di Goldbach afferma che:

Congettura 2. (Goldbach)
Ogni numero pari >2 si scrive come la somma di due numeri primi.

Poche settimane fa Helfgott ha annunciato la dimostrazione della congettura "ternare" di Goldbach: ogni numero dispari >5 si scrive come la somma di tre primi ($7=2+2+3$, $9=3+3+3$, $11=3+5+3$ ecc...)

1.9. **Euclide e i numeri perfetti.**

Il fatto seguente era noto dall'antichità: se $a\neq 1$, $S_n=1+a+a^2+...+a^n$, allora $S_n=(a^{n+1}-1)/(a-1)$.

Infatti $aS_n=a+a^2+...+a^{n+1}$, quindi $aS_n-S_n=a^{n+1}-1$, da cui il risultato.

Riguardo ai numeri perfetti Euclide dimostra:

Teorema 1.16. *Se 2^k-1 è un numero primo allora $n=2^{k-1}(2^k-1)$ è un numero perfetto.*

Dimostrazione. Abbiamo $n=p2^{k-1}$, quindi, visto che p è primo, i divisori di n sono $1,2,2^2,..,2^{k-1},p,2p,...,2^{k-2}p,2^{k-1}p=n$. Sia $S=1+2+2^2+...+2^{k-1}$. Abbiamo $S=2^k-1$. La somma di tutti i divisori di n è $S(1+p)=(2^k-1)(2^k)=2.2^{k-1}(2^k-1)=2n$, quindi n è perfetto. □

A questo punto si pone il problema di sapere quand'è che $2^k - 1$ è un numero primo.

Lemma 1.17. *Sia a un intero, se $a^n - 1$ è un numero primo, allora $a = 2$ e n è un numero primo.*

Dimostrazione. Si ricorda l'identità: $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + ... + a + 1)$. Se $a > 2$, $a - 1$ è un divisore non banale di $a^n - 1$.
Se n non è primo, $n = kd$, $1 < k, d < n$ e $a^n = (a^k)^d$. Ponendo $b = a^k$, abbiamo $a^n - 1 = b^d - 1$. Siccome $b - 1 \mid b^d - 1$ e siccome $b > 2$ (perché $a \geq 2, k > 1$), $a^n - 1$ ha un divisore non banale. □

Vediamo quindi che affinché $2^k - 1$ sia primo è *necessario* che k sia primo. In effetti gli esempi noti fin qua sono tutti del tipo $2^{p-1}(2^p - 1)$ con p primo:

- $p = 2$: $2^1(2^2 - 1) = 6$
- $p = 3$: $2^2(2^3 - 1) = 28$
- $p = 5$: $2^4(2^5 - 1) = 496$
- $p = 7$: $2^6(2^7 - 1) = 8128$

La condizione che p sia primo *non è sufficiente*: $2^{11} - 1 = 2\,047 = 23 \times 89$, quindi per $p = 11$, $2^{p-1}(2^p - 1)$ non è perfetto.

Osservazione 1.18. *Tutti questi numeri perfetti sono triangolari, infatti $n = 2^{p-1}(2^p - 1) = P(P+1)/2 = t_P$ dove $P = 2^p - 1$.*

A questo punto:

Problema 4. *Un numero perfetto pari è necessariamente della forma $2^{p-1}(2^p - 1)$?*

1.10. **Diofante.**

Diofante è l'ultimo matematico dell'Antica Grecia (circa 300 dopo Cristo).

Diofante cerca soluzioni intere (o razionali) di equazioni polinomiali. Per esempio si pone il problema di trovare triangoli rettangoli i cui lati abbiano come misura dei numeri interi. Per il teorema di Pitagora questo torna a

cercare $(x, y, z) \in \mathbb{N}^3$ tali che $x^2 + y^2 = z^2$. Una tale terna è chiamata *terna pitagorica*. Per esempio $(3, 4, 5)$ è una terna pitagorica. Come vedremo questo problema avrà un'influenza notevole sullo sviluppo della teoria dei numeri.

L'opera di Diofante ci è pervenuta solo in parte ed è stata tradotta e diffusa nel Medio-Evo prima dai matematici arabi e poi da quelli europei.

Oggi c'è tutta una branca della teoria dei numeri che si chiama *geometria diofantea* in onore di Diofante.

2. Fermat (1601-1665).

Fermat è senza dubbi il padre fondatore della teoria dei numeri moderna. Uomo di legge di mestiere, faceva matematica per hobby (e per questo viene chiamato *il principe dei dilettanti*), le sue contribuzioni sono molteplici (teoria delle probabilità con Pascal, calcolo infinitesimale "metodo della tangente", ottica) ma è sopratutto in teoria dei numeri che Fermat ha dato i suoi contributi più importanti, anche se in un modo un pò particolare...

2.1. **Il lascito di Fermat.**

Ecco una lista, non esaustiva, dei risultati enunciati da Fermat. 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.

(1) Per ogni intero a e ogni primo p: $p \mid a^p - a$, quindi se $p \nmid a$, $p \mid a^{p-1} - 1$. Questo enunciato è noto come il *piccolo teorema di Fermat*.
(2) *(Teorema dei due quadrati):* Ogni numero primo della forma $4k + 1$ si scrive, in modo unico, come la somma di due quadrati.
(3) *(Teorema dei quattro quadrati):* Ogni intero naturale si scrive come la somma di (al più) quattro quadrati.
(4) *(Caso $n = 3$ dell'equazione di Fermat):* Se x, y, z sono degli interi tali che: $x^3 + y^3 = z^3$, allora $xyz = 0$.
(5) L'unica soluzione in numeri interi dell'equazione $x^3 = y^2 + 2$ è $x = 3, y = 5$.
(6) 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).

(7) Se D non è un quadrato, l'equazione $x^2 - Dy^2 = 1$ ha un'infinità di soluzioni intere (oggi questa equazione è nota come l'equazione di Pell).
(8) ogni numero primo della forma $3k + 1$ si può scrivere come $x^2 + 3y^2$. Ogni primo della forma $8k + 1$ o $8k + 3$ si può scrivere nella forma $x^2 + 2y^2$.
(9) ogni numero si scrive come la somma di al più tre numeri triangolari (cioè numeri della forma $n(n + 1)/2$).
(10) Ogni intero della forma $2^{2^n} + 1$ è primo.

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

2.2. **La congettura di Fermat.**

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, diventando uno dei problemi aperti più affascinante e difficile della matematica:

Congettura 3 (Congettura di Fermat)**.**
Sia n un intero con $n > 2$. Se a, b, c sono degli interi tali che $a^n + b^n = c^n$, allora $abc = 0$.

Quindi contrariamente al caso $n = 2$ delle terne pitagoriche, considerato da Diofante, in cui ci sono infinite soluzioni non banali, se $n > 2$, secondo questa congettura, non ci dovrebbero essere soluzioni (tranne quelle banali del tipo $a^n + 0^n = a^n$).

La congettura di Fermat è stata dimostrata nel 1995 da Wiles (più di tre secoli dopo!).

2.3. **Fermat e i numeri perfetti, primi di Mersenne.**

Sotto l'impulso del prete Mersenne, Fermat si mise a studiare il problema dei numeri perfetti. Come abbiamo già visto, Euclide aveva mostrato che se $2^p - 1$ è un numero primo, allora $2^{p-1}(2^p - 1)$ è perfetto.

Definizione 2.1. *Per ogni intero $n > 1$ poniamo $M_n := 2^n - 1$.*
Un numero primo q è detto di Mersenne se $q = M_n$ per un qualche n (sappiamo allora che necessariamente $n = p$ è primo). Finalmente indichiamo con Mn l'ennesimo primo di Mersenne.

Quindi

- $M1 = M_2 = 3$
- $M2 = M_3 = 7$
- $M3 = M_5 = 31$
- $M4 = M_7 = 127$

Ma $M_{11} = 2^{11} - 1 = 2\,047 = 23 \times 89$ non è primo. I primi quattro primi di Mersenne erano noti dall'antichità, i successivi tre nel Medio-Evo, sono:

- $M5 = M_{13} = 8\,191$
- $M6 = M_{17} = 131\,071$
- $M7 = M_{19} = 524\,287$.

Ovviamente ad ogni primo di Mersenne, M_p, corrisponde un numero perfetto pari: $P = 2^{p-1}M_p$ (ma a priori ce ne potrebbero essere altri di pari e a fortiori di dispari).

Problema 5. *Come si fa a capire se M_p è primo o no?*

Nel 1640 Fermat annuncia questi due teoremi:

Teorema 2.2. *Ogni divisore primo, q, di M_p è della forma $q = 2kp + 1$, $k \in \mathbb{N}$.*

Teorema 2.3. *Sia p un numero primo, allora $p \mid 2^p - 2$.*

In realtà questi due teoremi sono equivalenti! Per vederlo si usa:

Lemma 2.4. *Sia $s > 1$ un intero. Per $n \in \mathbb{N}$ si pone $B_n = s^n - 1$. Allora se $g = (a, b)$, $(B_a, B_b) = B_g$.*
In particolare se a e b sono primi tra di loro, il massimo comune divisore di B_a, B_b è $s - 1$.

Dimostrazione. Mostriamo che se $a = bq + c$, allora $B_a = QB_b + B_c$. Questo permette di concludere perché mostra che quando facciamo l'algoritma di Euclide per trovare (a, b), possiamo "riportare" i calcoli nell'algoritma per trovare (B_a, B_b), quindi se g è l'ultimo resto non nullo nell'algoritmo di (a, b), in quello di (B_a, B_b) sarà B_g.
Abbiamo:

$$\begin{aligned} s^a - 1 &= (s^c - 1)(s^{bq} - 1) + (s^{bq} - 1) + (s^c - 1) \\ &= (s^{bq+c} - 1) \\ &= \left[((s^c - 1) + 1)\frac{(s^{bq} - 1)}{s^b - 1}\right].(s^b - 1) + (s^c - 1) \end{aligned}$$

Siccome $s^b - 1 \mid s^{bq} - 1$ (perché $b \mid bq$), $Q = \left[((s^c - 1) + 1)\frac{s^{bq}-1)}{s^b-1}\right]$ è un intero e abbiamo: $B_a = QB_b + B_c$. □

Mostriamo adesso che i Teoremi 2.2 e 2.3 sono equivalenti:

Dimostrazione.

Teorema 2.2 implica Teorema 2.3:

Osserviamo che il prodotto di due numeri della forma $2kp + 1$ è ancora un numero della stessa forma: $(2kp + 1)(2sp + 1) = 4ksp^2 + 2kp + 2sp + 1 = 2(2ksp + k + s)p + 1$. Quindi dal Teorema 2.2 segue che ogni divisore di M_p è della forma $2kp + 1$ (ogni divisore è un prodotto di divisori primi). In particolare anche M_p è della forma $2kp + 1$, cioè: $2^p - 1 = 2kp + 1$ e quindi $2^p - 2 = 2kp$ e $p \mid 2^p - 2$.

Teorema 2.3 implica Teorema 2.2:

Sia q un divisore primo di $M_p = 2^p - 1$ (in particolare q è dispari). Per il Teorema 2.3, $q \mid 2^q - 2 = 2(2^{q-1} - 1)$. Siccome $q \nmid 2$, $q \mid 2^{q-1} - 1$ (Lemma 1.8). Sia G l'M.C.D. di $2^p - 1$ e $2^{q-1} - 1$. Abbiamo $G > 1$ (perché q divide entrambi i numeri). Per il Lemma 2.4, $G = 2^g - 1$ dove $g = (p, q - 1)$ è l'M.C.D. di p e $q - 1$. Siccome $G > 1$, anche $g > 1$ e l'unica possibilità è $g = p$ (perché p è

primo). Quindi $p \mid q-1$: $tp = q-1$, ossia $tp+1 = q$. Se t è dispari, q è pari: impossibile, quindi $t = 2k$ e $q = 2kp+1$. □

Quindi per dimostrare il Teorema 2.2 basta dimostrare il teorema 2.3. Pochi mesi dopo Fermat annuncia un risultato ancora più generale:

Teorema 2.5 (Il piccolo teorema di Fermat)**.**
Se p è un primo, allora per ogni intero a, $p \mid a^p - a$.

Ovviamente il Teorema 2.3 è il caso particolare $p = 2$ del piccolo teorema di Fermat. Quindi il piccolo teorema di Fermat, risultato fondamentale della teoria dei numeri, nasce dalle ricerche di Fermat sui numeri perfetti.

Per vedere se $M_{11} = 2\,047$ è o meno primo basta vedere se è divisibile per $2.k.11+1, k = 1, 2, 3...$ e si vede subito che $23 \mid 2\,047$. Per $M_{23} = 8\,388\,607$, Fermat ha trovato che $47 \mid M_{23}$. Per $M_{29} = 536\,870\,911$, dobbiamo cercare dei divisori della forma $58k+1$, ossia $59, 117, 175, 233$. Si vede che $59 \nmid M_{29}$, è inutile provare con 117 e 175 perché non sono primi (il più piccolo divisore > 1 di un numero è primo) e poi si vede che $233 \mid M_{23}$. Il prossimo da vedere è $M_{31} = 2\,147\,483\,647$. Osserviamo che $\sqrt{M_{31}} = 46\,340, 9...$, quindi dobbiamo cercare se i numeri della forma $62k+1 \leq 46\,340$, $k = 1, 2, ...$ dividono o meno M_{31}, si vede che $1 \leq k \leq 747 \sim (46\,339)/62$, certo tra questi basta provare quelli primi ma bisogna essere in grado di capire quali lo sono. Oggi con i computers non è un problema, ma dovendo fare i calcoli a mano è un'altra cosa!

3. Il piccolo teorema di Fermat.

Il piccolo teorema di Fermat è un risultato fondamentale della teoria dei numeri per molteplici motivi, uno dei quali è che serve come test di primalità.

3.1. **Test di primalità e numeri di Carmichael.**

Dato un intero a se riusciamo a trovare un intero n tale che a non divida $n^a - n$, allora possiamo concludere che a non è primo e questo *senza neanche conoscere un divisore di a!* In realtà si può mostrare che basta provare per n

tale che $1 \leq n < a$. Per esempio $2^6 - 2 = (2^3)^2 - 2 = 62$, $6 \nmid 62$, quindi 6 non è primo. Sembra complicato ma il fatto è che con un computer questo tipo di calcoli ("modulo a") sono molto veloci.

E se $a \mid n^a - n$ per ogni intero n, possiamo concludere che a è primo? La risposta è negativa, ci sono dei "falsi" primi, cioè dei numeri che si comportano come dei primi per il piccolo teorema di Fermat ma che non sono primi. Il più piccolo di questi numeri (detti *numeri di Carmichael*) è $561 = 3 \times 11 \times 17$. I numeri di Carmichael sono piuttosto rari. Si può dimostrare che n è un numero di Carmichael se e solo se: n non è divisibile per il quadrato di un numero primo (cioè la fattorizzazione in primi di n è della forma $n = \prod p_1...p_r$, $p_i \neq p_j$ se $i \neq j$ e $r > 1$) e se per ogni divisore primo, p di n, $p - 1$ divide $n - 1$. Per esempio $2, 10$ e 16 dividono 560. E' stato dimostrato solo nel 1994 che esistono infiniti numeri di Carmichael.

Anche se l'esistenza dei numeri di Carmichael distrugge definitivamente la possibilità di usare il piccolo teorema di Fermat per dimostrare che un dato numero è primo, rimane che il piccolo teorema di Fermat (generalizzato e modificato) è un ottimo strumento per testare la primalità di un numero.

3.2. **Dimostrazione del piccolo teorema di Fermat.**

Con un po' di conoscenze in algebra (gruppi finiti) la dimostrazione del piccolo teorema di Fermat è banale (= una riga!). Senza scomodare l'algebra si può usare la formula del binomio:

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i} \tag{8}$$

dove:

$$\binom{n}{k} := \frac{n!}{k!(n-k)!} = \frac{(n-k+1)...n}{1.2...k}$$

Si ricorda che per convenzione $0! = 1$. I numeri $\binom{n}{k}$ si chiamano *coefficienti binomiali* e sono esattamente il numero di sotto insiemi con k elementi di un insieme con n elementi. In particolare sono numeri interi. Questo viene dal fatto che per sviluppare $(x+y)^n = (x+y)(x+y)...(x+y)$, se ci pensate bene, si procede così: in ogni pacchetto $(x+y)$ si sceglie o x o y in tutti i modi possibili. Per esempio per avere $x^{n-1}y$ si sceglie sempre x tranne una volta,

in quanti modi è possibile fare questa scelta? Esattamente n perché ci sono n pacchetti. Quindi il coefficiente di $x^{n-1}y$ in $(x+y)^n$ è $n = \binom{n}{1}$. Quale sarà il coefficiente di $x^{n-2}y^2$? Bisogna vedere in quanto modi posso scegliere due volte y. Se indichiamo con $\{P_1, P_2, ..., P_n\}$ gli n pacchetti $(x+y)$, scegliere due volte y torna a scegliere due pacchetti cioè un sotto insieme di due elementi di $\{P_1, ..., P_n\}$ un insieme con n elementi.

Rimane da vedere che il numero di sotto insiemi con k elementi di un insieme con n elementi è dato da $\binom{n}{k}$: questo si dimostra per doppia induzione su n e k.

Se non avete voglia di farlo potete dimostrare la formula (8) per induzione su n scrivendo che $(x+y)^n = (x+y)^{n-1}.(x+y)$.

Per dimostrare il piccolo teorema di Fermat abbiamo bisogno del:

Lemma 3.1. *Se p è un numero primo e se $1 \leq k < p$, allora $p \mid \binom{p}{k}$.*

Dimostrazione. Abbiamo $\binom{p}{i} = \frac{(p-i+1)...p}{1.2...i}$. Abbiamo $(1.2...i, p) = 1$, infatti se un primo divide p e $i!$, questo primo è necessariamente p, quindi $p \mid 1.2...i$ e questo implica $p \mid k$ per un qualche k, $1 \leq k \leq i$ e questo è impossibile perché $k \leq i < p$. Quindi nessun divisore del denominatore può cancellare il p al numeratore, pertanto $p \mid \binom{p}{i}$. □

Dimostrazione del piccolo teorema di Fermat.

Mostriamo per induzione su n che $p \mid n^p - n$. Se $n = 1$, $1^p - 1 = 0$ è divisibile per p. Supponiamo l'asserto vero per n e mostriamolo per $n+1$. Per la formula del binomio:

$$(n+1)^p = n^p + \sum_{i=1}^{p-1} \binom{p}{i} n^i + 1$$

Quindi:

$$(n+1)^p - (n+1) = (n^p - n) + \sum_{i=1}^{p-1} \binom{p}{i} n^i$$

Per ipotesi di induzione $p \mid n^p - n$, per il Lemma 3.1, $p \mid \binom{p}{i}$ se $1 \leq i < p$, quindi $p \mid (n+1)^p - (n+1)$ e l'asserto è dimostrato per $n+1$. □

4. Euler (1707-1783).

Il matematico svizzero Leonhard Euler (Eulero in italiano) ha ripreso sistematicamente le affermazioni di Fermat cercando di dimostrarle. Il più delle volte c'è riuscito, ma non sempre! In particolare Eulero ha dimostrato una forma più generale del piccolo teorema di Fermat.

Per quanto riguarda i numeri perfetti Euler ha dimostrato due risultati che sono tutt'ora, qualitativamente parlando, i migliori risultati noti.

Teorema 4.1 (Euler)**.** *Ogni numero perfetto pari è della forma* $2^{p-1}(2^p-1)$ *con* p *primo.*

Questo risolve il Problema 4 e grazie a questo risultato, la ricerca dei numeri perfetti pari è equivalente a quella dei numeri primi di Mersenne.

Teorema 4.2 (Euler)**.** *Se* n *è un numero perfetto dispari allora la sua fattorizzazione in numeri primi è della forma:*

$$n = q^{4b+1}.\prod p_i^{2a_i}$$

dove q *è un primo della forma* $4k+1$.

Questa è solo una piccolissima, minuscola, parte della produzione matematica di Euler.

5. Oggi.

5.1. **I numeri perfetti oggi.**

Per quanto riguarda i numeri perfetti ci sono stati pochi progressi tranne che dallo stato, un po' incerto di "problema", si è passato a quello più deciso di congettura:

Congettura 4 ("The oldest open problem in mathematics")**.**
Non esiste nessun numero perfetto dispari.

Congettura 5. *Esiste un'infinità di numeri perfetti pari (questo è equivalente a dire che esistono infiniti primi di Mersenne).*

Lo stato dell'arte è il seguente: se esiste un numero perfetto dispari n, allora $n > 10^{1500}$ (dimostrato nel 2012 col computer). Si conoscono 48 primi di Mersenne quindi 48 numeri perfetti. In particolare si conosce Mn fino a $n = 42$, l'ultimo (il 48-esimo) primo di Mersenne scoperto (gennaio 2013) ha più di 17 milioni di cifre e corrisponde al primo 57.885.161, cf www.mersenne.org (o GIMPS)).

L'interesse nei numeri di Mersenne è dovuto alla *crittografia*.

5.2. **La congettura di Fermat è ormai il teorema di Wiles.**

Nel 1847 il matematico francese Lamé annunciò di avere 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 $(x/z)^3 - 1 = -(y/z)^3$. Adesso $X^3 - 1 = (X - 1)(X^2 + X + 1) = (X - 1)(X - j)(X - j^2)$ dove $j = (-1 + i\sqrt{3})/2$ è una radice primitiva terza dell'unità. Quindi $(x/z)^3 - 1 = ((x/z) - 1)((x/z) - j)((x/z) - j^2)$. Moltiplicando per z^3: $x^3 - z^3 = (x - z)(x - jz)(x - j^2z)$. In definitiva la nostra equazione diventa: $(x - z)(x - jz)(x - j^2z) = -y^3$. 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. Infatti se $t = \prod p_i$ è la fattorizzazione in numeri primi, quella di t^3 è $t^3 = \prod p_i^3$. Quindi $a_1a_2a_3 = \prod p_i^3$. Ogni p_i divide uno e uno solo degli a_j (perchè gli a_i sono due a due primi tra di loro) e quindi lo divide al cubo, cioè nella fattorizzazione di a_j ogni fattore primo compare al cubo, pertanto a_j è un cubo.

Quindi Lamé conclude che ogni $x - 1, x - jz, x - j^2z$ è un cubo e da questo deriva una contraddizione. Subito vari matematici tra cui Liouville (che aveva suggerito l'uso dei numeri complessi a Lamé) sollevano dubbi: il fatto è che non si sta più lavorando con degli interi, ma con dei numeri della forma $n+jm$ n, m interi e per questi "nuovi" numeri il teorema fondamentale dell'aritmetica non è dimostrato! In effetti il matematico tedesco Kummer aveva già dimostrato, alcuni anni prima, che per numeri del tipo $n+\zeta m$, ζ radice n-esima dell'unità, il teorema fondamentale non era sempre vero! 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 algebrica dei numeri. Kummer riusci a dimostrare che per i primi soddisfacenti una certa condizione aritmetica la congettura di Fermat era vera. Per vari anni (inizio '900 inoltrato) le ricerche su Fermat erano centrate, senza grande successo, sui metodi derivanti dai lavori di Kummer.

La chiave per Fermat arrivò in modo inaspettato. Nel 1982 il matematico tedesco Frey ebbe questa idea per lo meno strana: supponiamo di avere una soluzione non banale di Fermat: $a^p + b^p = c^p$ (basta considerare p primo dispari) e consideriamo la curva di equazione $y^2 = x(x - a^p)(x + b^p)$. Questa è una *curva ellittica*. La teoria delle curve ellittiche era già ben sviluppata e Frey si accorse che una tale curve doveva avere delle proprietà aritmetiche così straordinarie che alla fine... non doveva esistere.

Infatti seguendo questa via e dopo gli sforzi e contributi di vari matematici (Serre, Mazur, Ribet tra altri), Wiles riuscì nel 1995 (con un aiutino da parte di Taylor) a portare a termine la dimostrazione della congettura di Fermat. I metodi introdotti da Wiles portarono dopo alla dimostrazione completa della congettura di Taniyama-Shimura-Weil, risultato ben più importante per i matematici della congettura di Fermat!

5.3. **Crittografia, curve ellittiche, internet.**

La crittografia moderna ("a chiave pubblica") si basa su un'idea molto semplice: è molto difficile, praticamente impossibile fattorizzare in numeri primi, in un tempo ragionevole, un numero molto molto grande; anche usando computers molto potenti!

Per convincervi di questo fatto visitate il sito www.mersenne.org dedicato alla ricerca dei primi di Mersenne. Viceversa dato un numero molto grande se si conosce un suo fattore primo ("la chiave"), allora la fattorizzazione diventa possibile. In sostanza il messaggio (=il numero molto grande o meglio la sua fattorizzazione) può essere reso pubblico, tutti sanno cosa bisogna fare, ma solo chi ha la chiave può leggere il messaggio. Questa è l'idea di base, in realtà si complica un pochino la situazione usando, per esempio, la generalizzazione di Eulero del piccolo teorema di Fermat.

Per questi motivi questioni squisitamente di teoria dei numeri come tests di primalità, metodi di fattorizzazione sono alla base della crittografia moderna. Inaspettatamente, ancora una volta, la teoria delle curve ellittiche (sì, la stessa che è servita a dimostrare Fermat!) gioca un ruolo importante in crittografia.

All'inizio (anni '90 del secolo scorso) la rete Internet era riservata agli organismi istituzionali (università, enti di governo ecc...), nessuno aveva Internet a casa. Verso la fine degli anni '90 si inizio a intravedere la possibilità di sviluppare l'E-commerce, questo grazie anche ai progressi teorici e computazionali in crittografia. Questa fu la molle che spinse i grandi investitori ad investire fiumi di denaro per connettere il mondo intero e portare Internet in tutte le case. Possiamo dire che il World Wide Web esiste anche grazie al piccolo teorema di Fermat e alla teoria delle curve ellittiche!

Si potrebbe anche aggiungere che i nostri computers non sono altro che la realizzazione di macchine immaginate, pensate secoli fa da vari matematici (Pascal, Babbagge, Turing, von Neumann per citarne solo alcuni), ma questa è un'altra storia!

5.4. **Conclusione.**

Abbiamo visto che esiste un filo continuo che parte da Pitagora, i numeri perfetti, le terne pitagoriche, passa per Fermat, il suo piccolo teorema e la sua "congettura" per arrivare alla teoria delle curve ellittiche, la ricerca di grandi numeri primi (di Mersenne), la crittografia e Internet.

Questo è solo un esempio di come funziona la ricerca di base: si sviluppa con problemi suoi, interni, che visti da fuori sembrano futili, inutili e poi, quando meno te lo aspetti, salta fuori l'applicazione "pratica" che sconvolge il mondo.

Per concludere diciamo che ci sono ancora tanti problemi aperti, congetture irrisolte in teoria dei numeri. Negli ultimi trent'anni sono stati risolti alcune congetture molto importanti:

- La congettura di Mordell (Faltings 1983). Questo risultato, troppo tecnico da essere enunciato qui, implica tra altre cose che per ogni $n > 3$ l'equazione di Fermat ha un numero finito di soluzioni.
- La congettura di Fermat (Wiles 1995).

- Due quadrati non possono essere consecutivi (cioè differire di 1), ma un quadrato e un cubo? Più generalmente quali sono le potenze consecutive di numeri interi? In termini diofantei, quali sono le soluzioni in numeri interi dell'equazione:

$$x^n - y^k = 1 \tag{9}$$

  Abbiamo $3^2 - 2^3 = 1$, nel 1844 Eugène Catalan congetturò che questa era *l'unica soluzione* in interi positivi. La congettura di Catalan è stata dimostrata nel 2003 da Preda Mihailescu.

Rimane però ancora molto da fare, la congettura di Goldbach, quella dei primi gemelli, quelle sui numeri perfetti, miriade di altre congetture, problemi senza parlare dei problemi "top" la cui formulazione è troppo tecnica per essere esposta qui: *la congettura di Riemann, la congettura* abc e *la congettura di Birch-Swinnerton-Dyer*.

Ci sono anche questioni "meno serie" (ma molto difficili) come il problema del $3x+1$ (potete scaricare il software Aritmetica 1.0 dal sito www.unife.it/philippe.ellia (sezione Altro) per vedere di cosa si tratta).

Dipartimento di Matematica, 35 via Machiavelli, 44100 Ferrara
E-mail address: phe@unife.it