IL TEOREMA FONDAMENTALE DELL'ARITMETICA: FATTORIZZAZIONE IN NUMERI PRIMI.

PH. ELLIA

Indice

Introduzione

Questi appunti sono un'introduzione elementare al mondo affascinante della teoria dei numeri (aritmetica). Come indicato nel titolo l'obbiettivo è di dare una (in realtà tre) dimostrazione completa del teorema fondamentale dell'aritmetica: *Ogni numero naturale si scrive in modo sostanzialmente unico come un prodotto di numeri primi.* Strada facendo toccheremo altri argomenti (divisori di un numero, numeri perfetti, l'infinità dei numeri primi,...). I prerequisiti sono minimi: uno studente del primo anno dovrebbe leggere (e capire!)

questi appunti senza difficoltà (e questo dovrebbe valere, tranne forse per la Sezione 7, anche per uno studente, bravo, dell'ultimo anno del liceo).

1. Divisori di un numero.

In questa parte ci occuperemo esclusivamente di numeri naturali positivi ("numeri" nel seguito) cioè degli elementi di $\mathbb{N}^* = \{1, 2, 3, ..., n, ...\}$.

Definizione 1.1. *Il numero $a \in \mathbb{N}^*$ divide il numero $n \in \mathbb{N}^*$ se esiste $b \in \mathbb{N}^*$ tale che: $n = ab$.*

Si nota $a \mid n$ (a divide n). Ogni numero n ha sempre due divisori banali: 1 e se stesso: $n = 1.n$.

Osservazione 1.2. *Questo è un caso particolare della divisone euclidea : dati due numeri a, b esiste un'unica coppia di numeri (q, r) tale che: $b = aq + r$ con $0 \leq r < a$. Infatti mostriamo prima l'esistenza. Se $a > b$ basta prendere $q = 0$, $r = b$. Se $a \leq b$, si considera $b - a$ al posto di b: se $a > b - a$, allora $b = a + (b - a)$ ($q = 1$, $r = b - a$); se $a \leq b - a$, si considera $b - 2a$ e si ripete il ragionamento. A un certo punto si avrà: $a > b - qa$ e quindi $b = qa + r$, $0 \leq r < a$ (con $r = b - qa$).*

Mostriamo adesso l'unicità: se $b = aq + r = aq' + r'$ con, diciamo, $q > q'$, allora $r < r'$ e: $a(q - q') = r' - r$, ma $a(q - q') \geq a$ mentre $r' - r < a$: assurdo. Questo mostra l'unicità.

Dato un numero n possiamo considerare l'insieme, $Div(n)$, dei suoi divisori: $Div(n) = \{a \in \mathbb{N}^* \mid a \text{ divide } n\}$. Osserviamo che i divisori di n sono simmetrici rispetto a $\sqrt{n}$, più precisamente:

Lemma 1.3. *Siano a, b divisori di n: $n = ab$. Se $a \leq b$, allora: $a \leq \sqrt{n}$ e $b \geq \sqrt{n}$.*

Dimostrazione. Mostriamo che $a \leq \sqrt{n}$. Se, per assurdo, $a > \sqrt{n}$, allora $b \geq a > \sqrt{n}$ e quindi: $n = ab > (\sqrt{n})^2 = n$, assurdo, quindi $a \leq \sqrt{n}$.
Mostriamo che $b \geq \sqrt{n}$. In caso contrario: $a \leq b < \sqrt{n}$ e $n = ab < (\sqrt{n})^2$: assurdo. □

Quindi ad ogni divisore $\leq \sqrt{n}$ ne corrisponde uno $\geq \sqrt{n}$. L'uguaglianza si verifica se e solo se n è un quadrato (per es. $4 = 2.2$). L'insieme $Div(n)$ è ovviamente un insieme finito e la sua cardinalità (indicata con $\#Div(n)$) è in generale un numero pari ($\#Div(n)$ è un numero dispari se e solo se n è un quadrato).

Per esempio: $Div(6) = \{1, 2, 3, 6\}$, mentre $Div(16) = \{1, 2, 4, 8, 16\}$.

Riguardo ai divisori di un numero facciamo una piccola parentesi con un problema che risale all'antichità:

Definizione 1.4. *Un numero n è perfetto se la somma dei suoi divisori è uguale a $2n$.*

I primi numeri perfetti sono: 6 e 28. Infatti: $6 = 1+2+3$, $28 = 1+2+4+7+14$ (n è perfetto se è uguale alla somma dei suoi divisori tranne n stesso). Si conoscono solo un numero finito di numeri perfetti, tutti quelli noti sono pari, e finiscono con 6 o 8, ma nessuno è ancora riuscito a dimostrare che l'insieme dei numeri perfetti è infinito (o finito?), che ogni numero perfetto deve essere pari e terminare con 6 o 8 (o che queste affermazioni sono false).

Possiamo però osservare una piccola proprietà dei numeri perfetti che tira in ballo solo la risoluzione dell'equazione del secondo grado:

Lemma 1.5. *Se n è perfetto e $\#Div(n) = 4$, allora $n = 6$.*

Dimostrazione. Sia $Div(n) = \{1, a, b, n\}$, con $a \leq b$. Se n è perfetto allora: $n = 1 + a + b$. Siccome $n = ab$, abbiamo: $ab = n$ e $a + b = n - 1$. Quindi a, b sono le soluzioni dell'equazione: $X^2 - (n-1)X + n = 0$. In particolare:

$$a = \frac{n - 1 - \sqrt{n^2 - 6n + 1}}{2}$$

Siccome a deve essere un intero, questo implica che $\sqrt{n^2 - 6n + 1}$ è un intero. Si verifica facilmente che per $n \geq 8$: $n - 4 < \sqrt{n^2 - 6n + 1} < n - 3$. Quindi per $n \geq 8$, $\sqrt{n^2 - 6n + 1} \notin \mathbb{N}$. Adesso basta controllare che l'unico numero perfetto ≤ 7 è 6 per concludere. □

Già che ci siamo, mostriamo che non esiste nessun numero perfetto n con $\#Div(n) = 3$. Se $Div(n) = \{1, a, n\}$ e se n è perfetto allora: $n = a + 1 = a^2$, quindi $a(a-1) = 1$: impossibile se $a \in \mathbb{N}$.

La dimostrazione del Lemma 1.5 è un'applicazione divertente della formula risolutiva dell'equazione del secondo grado e del fatto che le radici, a, b di $X^2 - sX + p = 0$ verificano: $s = a + b$, $p = ab$.

2. Numeri primi: definizioni.

Iniziamo con una definizione:

Definizione 2.1. *Un numero $p \in \mathbb{N}^*$ è primo se: $p > 1$ e se gli unici divisori di p sono quelli banali (cioè 1 e p). In altre parole p è primo se e solo se $\#Div(p) = 2$.*

Per esempio i numeri primi minori di 10 sono: $2, 3, 5, 7$.

Il numero 1 non viene considerato primo perché è invertibile: ogni numero n è divisibile per 1.

I numeri primi, come vedremo fra poco, sono i *mattoni* che permettono di costruire tutti gli altri numeri (almeno da un punto di vista moltiplicativo).

2.1. **Fare la lista dei numeri primi.** La domanda fondamentale è: *come fare per decidere se un numero dato, n, è primo o no?*. La risposta a questa domanda è molto difficile e comunque *time consuming*. Un primo approccio consiste nel fare la lista dei numeri primi $\leq n$ e guardare se n è o meno in quella lista. Cerchiamo di fare la lista dei numeri primi ≤ 20.

Su un foglio di carta scriviamo i numeri da 1 a 20. Sbarriamo il numero 1 il quale, per definizione, non è primo. Il numero 2 è primo (è l'unico numero primo pari!): tracciamo un cerchio intorno al numero 2. Dopodiché sbarriamo tutti i multipli di 2 (cioè tutti i numeri pari tra 4 e 20 compreso: di sicuro non sono numeri primi). Il numero più basso né sbarrato, né accerchiato è il numero 3. Lo accerchiamo e sbarriamo tutti i suoi multipli (che di sicuro non sono numeri primi in quanto divisibili per 3): 6 è già sbarrato in quanto multiplo di 2, sbarriamo 9, 12 è già sbarrato, sbarriamo 15, ecc... Fatto ciò il numero più basso, né cerchiato, né sbarrato, è il numero 5: lo accerchiamo

e sbarriamo i suoi multipli (in realtà 10, 15, 20 sono già sbarrati in quanto multipli di 2 o 3). Fatto ciò il numero più basso né sbarrato, né cerchiato è il numero 7: lo accerchiamo e sbarriamo i suoi multipli (in realtà 14, l'unico multiplo di 7 minore di 20 è già sbarrato in quanto multiplo di 2). A questo punto i numeri cerchiati sono $2, 3, 5, 7$ e i numeri né cerchiati, né sbarrati (≤ 20) sono: $11, 13, 17, 19$. Andando avanti così vediamo che i numeri primi ≤ 20 sono: $2, 3, 5, 7, 11, 13, 17, 19$ (osservare che se $n \geq 11$, ogni multiplo di n è > 20).

Questo procedimento è noto come il crivello di Erastotene. (Esercizio: usando il crivello di Erastotene, fare la lista dei numeri primi ≤ 100). Questo metodo è sostanzialmente un metodo costruttivo per fare la lista dei numeri primi $< N$, N dato.

Tornando alla nostra domanda di partenza (come fare a decidere se un dato numero n è primo o no?) possiamo procedere in un altro modo (*brute force method*): proviamo a dividere n per tutti i numeri m, $2 \leq n - 1$: se $\forall m$ la divisione non è possibile, allora n è primo; se $\exists m$ per cui la divisione è possibile ($n = mt, t \in \mathbb{N}^*$), allora n non è primo.

Possiamo migliorare questo procedimento "brutale": in realtà, per vedere che n è primo, basta verificare che nessun numero ≥ 2 e $\leq \sqrt{n}$ divide n. Infatti se $m \mid n$ e $m > \sqrt{n}$, allora $n = mt$ con $t \leq \sqrt{n}$ (cf Lemma 1.3), ma $t \mid n$ e $t \leq \sqrt{n}$.

Un algoritmo *semi-brutale* per testare se un dato numero n è o meno primo è quindi il seguente:

(1) Prendere il numero n
(2) Calcolare $N = \sqrt{n}$
(3) Per ogni numero m, $2 \leq m \leq N$, calcolare il resto della divisione $\frac{n}{m}$; se per un qualche m questo resto è zero, allora n non è primo. Se questo resto è diverso da zero per ogni m, $2 \leq m \leq N$, allora n è primo.

A questo punto viene naturale chiederci "quanti" sono i numeri primi, in particolare sono in numero finito (e in questo caso l'algoritmo precedente è

piuttosto banale), oppure no? Il teorema seguente si trova negli *Elementi* di Euclide:

Teorema 2.2. *L'insieme dei numeri primi è infinito.*

Per dimostrare questo teorema useremo il seguente:

Lemma 2.3. *Ogni numero $n > 1$ è divisibile per un numero primo.*

Dimostrazione. Se n è primo abbiamo finito. Se n non è primo, esiste d_1, $1 < d_1 < n$ che divide n: $n = d_1 q_1$. Se d_1 è primo, abbiamo finito. Se d_1 non è primo, esiste d_2, $1 < d_2 < d_1 < n$ che divide d_1 e quindi che divide n. Otteniamo così una successione di divisori di n: $1 < d_i < ... < d_2 < d_1 < n$. Questo procedimento non può continuare indefinitamente perché ci sono solo $n-2$ numeri (strettamente compresi) tra 1 e n, quindi si arriverà necessariamente ad un divisore d_i di n che sarà un numero primo. □

Dimostrazione del Teorema 2.2.
Supponiamo (per assurdo) che l'insieme, P, dei numeri primi sia finito: $P = \{p_1 = 2, p_2 = 3, ..., p_n\}$. Sia $N = p_1.p_2...p_n + 1$. Allora N non è divisibile per nessun numero primo (perché $N/p_i = \frac{p_1...p_i...p_n}{p_i} + \frac{1}{p_i} = p_1...p_{i-1}p_{i+1}...p_n + \frac{1}{p_i} \notin \mathbb{N}$). Questo è assurdo perché contraddice il Lemma 2.3. □

Questa dimostrazione è un esempio classico di dimostrazione per assurdo.

Ci sono varie altre dimostrazioni del Teorema 2.2. Vediamone, per ora, un'altra. Iniziamo col:

Lemma 2.4. *Sia $n > 1$ un intero e siano $1 = d_1 < d_2 < ... < d_{r-1} < d_r = n$ i suoi divisori. Allora d_2 è un numero primo (cioè il più piccolo divisore > 1 di un numero è sempre un numero primo).*

Dimostrazione. Se d_2 non è primo, allora $d_2 = ab$ con $1 < a \leq b < d_2$. Ma $a \mid d_2$ e $d_2 \mid n$ implica $a \mid n$, in contraddizione con la definizione di d_2. □

Invece il più grande divisore non banale (d_{r-1}) non è necessariamente un numero primo (considerare $n = 8$).

Un'altra dimostrazione del teorema 2.2 (Hermite).

Poniamo $n! = 1.2.3...(n-1).n$ (n fattoriale), per esempio $3! = 6$, $4! = 24$ ecc...

Sia p_n il più piccolo divisore > 1 di $n!+1$. Abbiamo $p_n > n$ (perché se $k < n$: $\frac{n!+1}{k} = \frac{1.2...(k-1).k.(k+1)...n}{k} + \frac{1}{k} \notin \mathbb{N}$). Per il Lemma 2.4, p_n è primo. Quindi per ogni n esiste un numero primo $p_n > n$. Pertanto l'insieme dei numeri primi è infinito. □

Questa dimostrazione è particolarmente interessante perché si può dimostrare che se p è un numero primo, allora $p \mid (p-1)! + 1$ (teorema di Wilson), ovvero p è il più piccolo divisore non banale di $(p-1)! + 1$. Quindi se applichiamo il procedimento di Hermite per tutti gli interi n, questo ci darà la lista di tutti i numeri primi.

3. Il metodo di dimostrazione per induzione.

L'importanza dei numeri primi deriva dal seguente:

Teorema 3.1 (Teorema fondamentale dell'aritmetica)**.** *Ogni numero $n > 1$ si scrive in modo (sostanzialmente unico) come un prodotto di numeri primi.*

Per esempio: $15 = 3.5$, $60 = 2^2.3.5$ ecc... In altri termini con i numeri primi si possono ottenere tutti gli altri numeri; i numeri primi sono i "mattoni" (*gli atomi*) dell'aritmetica.

Per dimostrare il Teorema 3.1 useremo il procedimento di dimostrazione per induzione. Questo procedimento rispecchia la natura dei numeri naturali ed essenzialmente si basa sulla seguente proprietà di $\mathbb{N}$: ogni sottinsieme (non vuoto) $X \subset \mathbb{N}$, ha un più piccolo elemento (cioè: $\exists m \in X$ tale che $\forall n \in X, n \geq m$). Osserviamo che questa proprietà non è più vera su $\mathbb{Q}$ (e quindi a fortiori su $\mathbb{R}$, $\mathbb{C}$; per quanto riguarda $\mathbb{Z}$ prendere $X = \mathbb{Z}$!): $X = \{\frac{1}{n} \mid n \in \mathbb{N}^*\}$ non ammette un più piccolo elemento.

In effetti si può cercare di definire i naturali con gli assiomi di Peano, partendo dal "simbolo" 0 e dalla nozione di successore (+1):

(1) Ogni numero ha un successore
(2) 0 non è il successore di nessun numero
(3) due numeri distinti non possono avere lo stesso successore

(4) Sia F un insieme di numeri verificante le seguenti condizioni: (a) $0 \in F$, (b) se un numero appartiene ad F, allora anche il suo successore appartiene ad F. Allora $\mathbb{N} = F$ (allora ogni numero appartiene ad F).

Se indichiamo con $x + 1$ il successore di x, la condizione 4. si legge: $[0 \in F$ e $(x \in F \Rightarrow x + 1 \in F] \Rightarrow F = \mathbb{N}$.

La condizione 4. è il principio di induzione. Notiamo che questi assiomi non bastano a definire $\mathbb{N}$ perché usano un termine non definito, quello di "insieme". Oggigiorno la nozione di numero (naturale, relativo, razionale, reale, complesso) segue dalla nozione di insieme; una rigorosa definizione della nozione di insieme richiede argomentazioni sofisticate di logica matematica (non ogni "collezione" di "oggetti" è un insieme: la collezione di tutti gli insiemi non è un insieme, ma un'altra cosa (*l'insieme degli insiemi non è un insieme*). Questo è il famoso paradosso di Russel: in un villaggio c'è un barbiere. Il barbiere fà la barba solo ed esclusivamente a quelli che non si fanno la barba loro stessi. Chi fa la barba al barbiere? Se il barbiere si fà la barba c'è una contraddizione perché il barbiere fà la barba solo a quelli che non si fanno la barba loro stessi. Se il barbiere non si fà la barba, cè una contraddizione perché il barbiere fà la barba a quelli che non si fanno la barba.

In conclusione queste questioni sono molto delicate e vanno prese con le pinze, comunque, nella definizione più accettata al giorno d'oggi degli assiomi della matematica (modello di Zermelo-Frankel con assioma della scelta) la regola 4. (principio di induzione) è contemplata, anzi è uno dei principi di base.

Tornando al metodo di dimostrazione per induzione, l'idea è la seguente: sia $P(n)$ una proprietà (formula, enunciato, ecc...) che dipende da $n \in \mathbb{N}$. Per dimostrare $P(n)$ per ogni $n \in \mathbb{N}$ basta:

(1) Dimostrare $P(0)$
(2) mostrare che *se* $P(n)$ è vera, *allora* anche $P(n + 1)$ è vera.

Infatti se indichiamo con F l'insieme degli n per i quali $P(n)$ è vera; per l'assioma 4. di Peano, si ha immediatamente che $F = \mathbb{N}$.
Infatti, per 1., $P(0)$ è vera. Per 2., siccome $P(0)$ è vera, anche $P(1)$ è vera.

Per 2. ancora, siccome $P(1)$ è vera, anche $P(2)$ è vera, e, andando avanti così è chiaro che $P(n)$ è vera per ogni n. L'assiome 4. di Peano non fa altro che *zippare* in una sola riga questo procedimento ricorsivo infinito.

Possiamo rappresentarci questo procedimento con la seguente immagine: $\mathbb{N}$ è una scala a pioli: c'è il piolo 0, poi il piolo 1, ecc... L'unico inconveniente di questa scala è di essere infinita! L'induzione ci dice che per essere sicuri di percorrere questa scala infinita senza tralasciare nessun piolo basta:

(1) mettere il piede sul piolo 0
(2) quando si è messo il piede su un piolo, metterlo poi su quello successivo.

Osserviamo alcune variazioni del metodo di dimostrazione per induzione:

(a) Il caso iniziale non deve necessariamente essere 0: per dimostrare $P(n)$ per $n \geq k_0$ basta dimostrare il caso iniziale $P(k_0)$ e poi mostrare il passo di induzione: $P(n) \Rightarrow P(n+1), n \geq k_0$.

(b) L'ipotesi di induzione nel passo di induzione si può formulare nel modo seguente: $P(m)$ è vera per ogni m tale che $k_0 \leq m \leq n$.

Facciamo un esempio di applicazione del metodo di dimostrazione per induzione.

Sia $S(n) = 1 + 2 + 3 + ... + n$ la somma dei primi n numeri. Si tratta di trovare *e dimostrare* una formula per $S(n)$.

Un quadrato $n \times n$ contiene n^2 elementi. Ci sono n elementi sulla diagonale. Per simmetria, il numero di elementi sopra la diagonale è uguale al numero di elementi sotto la diagonale, quindi questo numero è: $(n^2 - n)/2$ ("elementi totali meno elementi sulla diagonale, diviso due"). Adesso $1 + 2 + 3 + ... + n$ è uguale al numero di elementi sulla diagonale più il numero di elementi sotto la diagonale (infatti sulla prima riga c'è un elemento, sulla seconda due, sulla terza tre, ecc... fino all'ultima riga che consta di n elementi (fare un disegno)). Quindi $S(n) = (n^2 - n)/2 + n$ (elementi sotto la diagonale più elementi sulla diagonale). In conclusione $S(n) = n(n+1)/2$.

Questa dimostrazione è perfetta ma una persona (un matematico) particolarmente pignola potrebbe obiettare che in qualche modo si fa uso di una "figura", che l'espressione "per simmetria" non è perfettamente definita ecc...

Tutte queste obiezioni possono essere superate ma, adesso che conosciamo la formula, possiamo fare di meglio: possiamo dimostrarla per induzione!

(1) Il caso iniziale $S(1) = \frac{1.2}{2} = 1$ è verificato.
(2) Il passo di induzione: mostriamo che se la formula è vera per n ($S(n) = \frac{n(n+1)}{2}$), allora è vera anche per $n+1$ ($S(n+1) = \frac{(n+1)(n+2)}{2}$). Abbiamo:

$$S(n+1) = 1 + 2 + 3 + ... + n + (n+1)$$

$$= (1 + 2 + 3 + ... + n) + (n+1) = S(n) + (n+1)$$

Per ipotesi di induzione, $S(n) = \frac{n(n+1)}{2}$, quindi $S(n+1) = \frac{n(n+1)}{2} + (n+1)$, cioè: $S(n+1) = \frac{(n+1)(n+2)}{2}$.

La nostra formula è dimostrata per ogni n.

Osserviamo che per dimostrare la formula per induzione bisogna prima conoscerla!

Per concludere osserviamo la seguente dimostrazione, molto facile, della nostra formula: scriviamo i numeri 1, 2,..., n prima in ordine crescente e poi in ordine decrescente e facciamo la somma:

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

Concludiamo che $2S(n) = n(n+1)$, cioè: $S(n) = n(n+1)/2$.

Col primo metodo, meno formale, abbiamo scoperto (e anche dimostrato) la formula. Col metodo per induzione ne abbiamo dato una dimostrazione formale, rigorosa. Questo riflette esattamente il modo di lavorare del matematico: c'è una prima parte intuitiva in cui si indovina, si scopre la soluzione e poi una seconda parte più formale, tecnica, in cui si verifica se l'intuizione era giusta. Per illustrare meglio questo procedimento cerchiamo di scoprire e dimostrare una formula per:

$$Q(n) = 1^2 + 2^2 + 3^3 + ... + n^2.$$

Da dove iniziare? La formula che dà $S(n)$ è un polinomio del secondo grado in n. Tirando ad indovinare si può immaginare che la formula per $Q(n)$ sia un polinomio del terzo grado in n. Insisto sul fatto che questa è solo una supposizione, un tirare ad indovinare. Supponiamo quindi che $Q(n) = an^3 + bn^2 + cn + d$. Come fare a trovare a, b, c, d? Dando dei valori, per esempio: $Q(0) = 0 = d$, $Q(1) = 1 = a + b + c + d$, $Q(2) = 5 = 8a + 4b + 2c + d$, $Q(3) = 14 = 27a + 9b + 3c + d$. Abbiamo un sistema di quattro equazioni in quattro incognite che con un pò di fortuna sarà un sistema di Cramer. Infatti risolvendo troviamo:$a = 1/3$, $b = 1/2$, $c = 1/6$, $d = 0$. Se abbiamo indovinato bene la formula dovrebbe essere: $Q(n) = \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6} = \frac{n(n+1)(2n+1)}{6}$. Come esserne sicuri? Basta provare a dimostrare la formula per induzione! Ragionando come prima:

$$Q(n+1) = Q(n) + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2$$
$$= \frac{(n+1)[n(2n+1) + 6(n+1)]}{6}$$
$$= \frac{(n+1)(2n^2+7n+6)}{6} = \frac{(n+1)(n+2)[2(n+1)]}{6}$$

e questo è la nostra formula con $n+1$ al posto di n; la formula è dimostrata per ogni n.

Come ultimo esempio di applicazione, dimostriamo che la derivata di $f_n(x) = x^n$ è nx^{n-1}.

Il caso iniziale ($n = 1$) segue immediatamente dalla definizione di derivata:

$$f_1'(x) = \lim_{h\to 0} \frac{f_1(x+h) - f_1(x)}{h} = 1$$

Per il passo d'induzione useremo la formula per derivare un prodotto: $(uv)' = u'v + uv'$. Quindi ($u = x$,$v = x^{n-1}$): $f_n'(x) = x^{n-1} + x.(x^{n-1})'$. Per ipotesi di induzione $(x^{n-1})' = (n-1)x^{n-2}$, quindi: $f_n'(x) = x^{n-1} + (n-1)x^{n-1} = nx^{n-1}$ e la formula è dimostrata per ogni n.

4. Il teorema fondamentale dell'aritmetica: prima dimostrazione.

Tornando al teorema sulla fattorizzazione in numeri primi, dobbiamo dimostrare due cose:

(1) *L'esistenza:* ogni numero $n > 1$ si scrive come un prodotto di numeri primi.
(2) *L'unicità:* la fattorizzazione $n = p_1^{a_1}...p_r^{a_r}$ è unica (a meno dell'ordine dei fattori).

Iniziamo con l'esistenza.

Proposizione 4.1. *Ogni numero $n > 1$ si scrive come un prodotto di numeri primi.*

Dimostrazione. Procediamo per induzione su n. Il caso iniziale $n = 2$ è verificato (2 è primo).

Passo di induzione: supponiamo la proposizione vera per ogni intero m, $2 \leq m \leq n$ (ipotesi di induzione) e mostriamola per $n + 1$. Se $n + 1$ è primo, allora $n + 1$ si scrive ovviamente come un prodotto di numeri primi. Se $n + 1$ non è primo, allora ammette un divisore primo (Lemma 2.3): $n + 1 = p.t$ con p primo e $2 \leq t \leq n$. Per ipotesi di induzione, t si scrive come un prodotto di numeri primi: $t = p_1.p_2...p_r$, quindi $n + 1 = p.p_1.p_2...p_r$ si scrive anche lui come un prodotto di numeri primi. □

Mostriamo adesso l'unicità. La dimostrazione che segue (tratta da [1]) *non* è la dimostrazione usuale (che vedremo più avanti). Iniziamo con un lemma:

Lemma 4.2. *Sia n un intero che si scrive in modo unico (a meno dell'orine dei fattori) come prodotto di numeri primi:*

$$n = p_1 p_2 ... p_r \quad (*)$$

Se q è un numero primo che divide n, allora $q = p_i$ per qualche i (cioè q compare nella fattorizzazione $(*)$).

Dimostrazione. Abbiamo $n = qm$. Per la Prop. 4.1, m si scrive come un prodotto di numeri primi: $m = q_1 q_2 ... q_t$. Quindi $n = pq_1 ... q_t$. Per unicità quest'ultima fattorizzazione è $(*)$, quindi $p = p_i$ per qualche i. □

Possiamo adesso dimostrare il nostro teorema:

Teorema 4.3 (Teorema fondamentale dell'aritmetica)**.**
Ogni intero $n > 1$ si scrive in modo unico (a meno dell'ordine dei fattori) come un prodotto di numeri primi.

Dimostrazione. Procediamo per induzione su n. Il caso iniziale $n = 2$ è chiaro (2 è primo).

Passo di induzione: supponiamo l'asserto dimostrato per ogni numero $< n$ e mostriamo che vale anche per n. Se n è primo, abbiamo finito. Sia quindi n composito. Supponiamo di avere due fattorizzazioni diverse di n:

$$n = p_1 p_2 ... p_r = q_1 q_2 ... q_t$$

Siccome n non è primo $r, t > 1$. Osserviamo che: $p_i \neq q_j$, $\forall i, j$, $(+)$. Infatti se, per esempio, $p_1 = q_1$, allora $n/p_1 = p_2 ... p_r = q_2 ... q_t$, ma siccome $n/p_1 < n$, per ipotesi di induzione n/p_1 ammette una ed un'unica fattorizzazione, quindi $r = t$ e (dopo eventuale riordino degli indici): $p_i = q_i, \forall i$.

Possiamo assumere $p_1 < p_2 ... < p_r$, $q_1 < q_2 ... < q_t$. Quindi $p := p_1 \leq \sqrt{n}$ e $q := q_1 \leq \sqrt{n}$. Siccome $p \neq q$, $pq < n$. Consideriamo il numero $m = n - pq$. Abbiamo $m < n$ e anche $m > 1$ (altrimenti $n = 1 + pq$ in contraddizione con $p \mid n$). Per ipotesi di induzione, m ammette una ed un'unica fattorizzazione in numeri primi:

$$m = n - pq = P_1 ... P_s$$

Siccome $p \mid n$ e $p \mid pq$ segue che $p \mid m$. Per il Lemma 4.2, $p = P_i$ per qualche i, diciamo $p = P_1$. Nello stesso modo $q \mid m$ e quindi, diciamo: $q = P_2$. Quindi $m = pqP_3 ... P_s$. Siccome $m = n - pq$, $n = pq + pqP_3 ... P_s$ e quindi $pq \mid n = pp_2 ... p_r$. Questo implica che $q \mid n' = p_2 ... p_r$. Siccome $1 < n' < n$, per ipotesi di induzione, n' ammette una ed un'unica fattorizzazione. Per il Lemma 4.2 segue che $q = p_j$ per qualche $j > 1$. Siccome $q = q_1$ questo contraddice $(+)$. Pertanto la fattorizzazione di n è unica. □

Questa dimostrazione, piuttosto ingegnosa, è relativamente semplice e usa soltanto l'induzione e le quattro operazioni di base. Si osserverà l'uso della sottrazione ($m = n - pq$) che sembra inevitabile in ogni dimostrazione del teorema.

Il teorema mostra che i numeri primi sono i mattoni, gli atomi dell'aritmetica: tutti gli altri numeri si ottengono (tramite moltiplicazione) dai numeri primi.

Osservazione 4.4. *Nella fattorizzazione possono esserci fattori ripetuti, in questo caso, di solito, si usa la notazione esponenziale (p^r), si può anche convenire di scrivere i fattori in ordine crescente ($p_1 < p_2 < ... < p_r$), seguendo queste convenzioni la fattorizzazione si scrive: $n = p_1^{\alpha_1}.p_2^{\alpha_2}...p_r^{\alpha_r}$ $(*)$, $p_i \neq p_j$ se $i \neq j$ e $p_1 < p_2 < ... < p_r$. Con queste convenzioni la fattorizzazione $(*)$ è unica.*

Per esempio: $180 = 2^2.3^2.5$.

5. Prime conseguenze del teorema di fattorizzazione.

Vediamo adesso come ricavare dalla fattorizzazione informazioni sui divisori di un numero (il loro numero e la loro somma). Un'altra conseguenza è il famoso (e utilissimo) lemma di Gauss . Vedremo, nella prossima sezione, un'altra dimostrazione del teorema fondamentale, basata proprio sul lemma di Gauss.

5.1. Numero e somma dei divisori.

Conoscendo la fattorizzazione di un numero possiamo ricavare il numero dei suoi divisori e la loro somma:

Proposizione 5.1. *Sia $n > 1$ un intero e $n = p_1^{a_1}p_2^{a_2}...p_r^{a_r}$ la sua fattorizzazione in numeri primi.*

1. *Se $d \mid n$, allora $d = p_1^{\alpha_1}...p_r^{\alpha_r}$, con $0 \leq \alpha_i \leq a_i$ (per convenzione $b^0 = 1$).*
2. *Abbiamo $d(n) = \#Div(n) = (a_1 + 1)(a_2 + 1)...(a_r + 1)$.*
3. *Se $\sigma(n)$ indica la somma dei divisori di n (1 e n compresi), allora:*

$$\sigma(n) = (1 + p_1 + p_1^2 + ... + p_1^{a_1})(1 + p_2 + p_2^2 + ...p_2^{a_2})...(1 + p_r + p_r^2 + ... + p_r^{a_r}).$$

Dimostrazione. (1) Se $d = 1$ (resp. $d = n$) basta prendere $\alpha_i = 0, \forall i$ (risp. $\alpha_i = a_i, \forall i$). Supponiamo quindi $1 < d < n$. Abbiamo $n = dm$. Siano $d = q_1^{b_1}...q_t^{b_t}$, $m = P_1^{c_1}...P_s^{c_s}$ le fattorizzazioni di d, m in fattori primi. Allora $n = q_1^{b_1}...q_t^{b_t}.P_1^{c_1}...P_s^{c_s}$ è una fattorizzazione di n in numeri primi. Per unicità:

$$q_1^{b_1}...q_t^{b_t}.P_1^{c_1}...P_s^{c_s} = p_1^{a_1}p_2^{a_2}...p_r^{a_r}$$

con ogni q_j, P_l uguale a qualche p_i, la conclusione segue.

(2) Ci sono a_i+1 possibilità per scegliere α_i con $0 \leq \alpha_i \leq a_i$. La conclusione segue da (1).

(3) Svolgendo il prodotto $(1 + p_1 + p_1^2 + ... + p_1^{a_1})...(1 + p_r + p_r^2 + ... + p_r^{a_r})$, otteniamo la somma di tutti i possibili termini $p_1^{\alpha_1}...p_r^{\alpha_r}$, con $0 \leq \alpha_i \leq a_i$, ossia la somma di tutti i divisori. □

Quindi, per esempio, $28 = 2^2.7$, cioè $a_1 = 2, a_2 = 1$ con le notazioni precedenti. Quindi 28 ha $3.2 = 6$ divisori $(1, 2, 4, 7, 14, 28)$, la cui somma è: $\sigma(28) = (1+2+2^2)(1+7) = 7.8 = 56$. In particolare $\sigma(28) = 2.28$ e quindi 28 è un numero perfetto (cf Def. 1.4). Questo è un caso particolare di una situazione più generale:

Proposizione 5.2 (Euclide)**.**
Sia p un numero primo. Se $p+1 = 2^k$, allora $n = p.2^{k-1}$ è un numero perfetto.

Dimostrazione. Abbiamo $1 + 2 + ... + 2^{k-1} = 2^k - 1 = p$. Per la Prop. 5.1:

$$\sigma(n) = (1 + 2 + ... + 2^{k-1})(1 + p) = p(p + 1) = p.2^k = 2.(2^{k-1}p) = 2n.$$

□

Osservazione 5.3. *Eulero ha dimostrato che ogni numero perfetto* pari *è della forma $2^{k-1}.p$ con p primo, $p + 1 = 2^k$. Quindi la ricerca dei numeri perfetti pari è equivalente a quella dei numeri primi p tali che $p + 1$ sia una potenza di due.*

5.2. **Il lemma di Gauss.** Il lemma di Gauss (il cui enunciato si trova anche negli Elementi di Euclide, ma con una dimostrazione incompleta) viene generalmente dimostrato prima del Teorema fondamentale.

Lemma 5.4 (Gauss)**.**
Siano a, b degli interi e p un numero primo. Se $p \mid ab$, allora $p \mid a$ o $p \mid b$.

Dimostrazione. Siano $a = q_1...q_r$, $b = p_1...p_t$ le fattorizzazioni di a, b in numeri primi. Abbiamo $mp = ab$, quindi se $m = P_1...P_s$ è la fattorizzazione di m:

$$p.P_1...P_s = q_1...q_r.p_1...p_t$$

Per unicità deve essere $p = p_i$ o $p = q_j$ per opportuni indici i, j. □

Ovviamente se p non è primo il risultato è falso: $6 \mid 12 = 3.4$ ma 6 non divide né 3, né 4. Infatti $6 = 2.3$ con 2 che divide 4 e 3 che divide 3. Quindi 6 si spezza in due fattori primi e ognuno di loro va a dividere uno dei fattori. Un numero primo "non si spezza" in due.

Più generalmente abbiamo:

Lemma 5.5. *Sia p un numero primo. Se p divide $a_1.a_2...a_n$ allora p divide uno degli a_i.*

Dimostrazione. Procediamo per induzione sul numero n dei fattori. Il caso iniziale $n = 2$ è precisamente il Lemma 5.4.

Supponiamo l'asserto vero per $n - 1$ fattori (ipotesi di induzione). Sia $p \,|\, a_1.a_2...a_n = b.a_3...a_n$ $(b = a_1.a_2)$. Quindi p divide un prodotto di $n - 1$ fattori, quindi per l'ipotesi di induzione, p divide uno degli a_i, $3 \leq i \leq n$ e in questo caso abbiamo finito; altrimenti p divide $b = a_1.a_2$ e per il caso iniziale (Lemma 5.4), p divide a_1 o p divide a_2. □

Per estendere il Lemma di Gauss introduciamo la seguente:

Definizione 5.6. *Il massimo comune divisore (MCD) di due interi, m, n è il più grande intero d tale che: $d \mid m$ e $d \mid m$. Si nota $(m, n) = d$.*

I due interi m, n sono primi tra di loro *se* $(m, n) = 1$.

Se $m = p_1^{a_1}...p_r^{a_r}$, $b = q_1^{b_1}...q_s^{b_s}$ sono le fattorizzazioni di m e n, il massimo comune divisore si ottiene prendendo i primi che compaiono in entrambe le fattorizzazioni, con l'esponente più basso, e facendone il prodotto. Per esempio se $n = 2^2.3^3.5$ e $m = 2^4.3^2.7$, allora $(m, n) = 2^2.3^2$.

Due interi sono primi tra di loro se e solo se non esiste nessun primo che li divide entrambi. Abbiamo:

Lemma 5.7. *Se $a \mid m.n$ e se a e m sono primi tra di loro, allora $a \mid n$.*

Dimostrazione. Siccome $(a, m) = 1$, i primi della fattorizzazione di a non compaiono nella fattorizzazione di m, pertanto compaiono in quella di n, cioè $a \mid n$. □

Il minimo comune multiplo (mcm) di due interi n, m è il più piccolo intero a tale che $n \mid a$ e $m \mid a$. Il minimo comune multiplo si ottiene prendendo tutti i primi che compaiono in entrambe le fattorizzazioni, con l'esponente più grande. Per esempio se $a = 2^2.3^3.5$ e $b = 2^3.3^2.7$, il mcm è: $2^3.3^3.5.7$.

6. Un'altra dimostrazione del teorema fondamentale.

Proponiamo adesso una dimostrazione alternativa del Teorema Fondamentale. L'esistenza si dimostra come prima (cf Prop. 4.1). Per l'unicità si tratta di dimostrare *prima* il lemma di Gauss (senza usare ovviamente il Teorema Fondamentale!).

Lemma 6.1. *Sia p un numero primo. Se p divide ab, allora p divide a o p divide b.*

Dimostrazione. Sia $p_1 = 2, p_2 = 3, ..., p_n, ...$ la successione dei numeri primi. Mostriamo per induzione su n l'asserzione $G(n)$: se p_n divide un prodotto, allora p_n divide uno dei fattori.

Caso iniziale: $n = 1$ dobbiamo vedere: $p_1 = 2 \mid ab \Rightarrow 2 \mid a$ o $2 \mid b$; cioè se il prodotto ab è pari, uno dei due fattori è pari. Questo è chiaro perché il prodotto di due numeri dispari è dispari $((2t+1)(2m+1) = 2(2mt+t+m)+1)$.

Passo di induzione: per semplificare la scrittura poniamo $p_n = p$. L'ipotesi di induzione è: se q è un numero primo con $q < p$ e se q divide un prodotto di due numeri, allora q divide uno dei due fattori.

Vogliamo mostrare che questo implica $G(n) : p \mid ab \Rightarrow p \mid a$ o $p \mid b$.

Abbiamo quindi $ab = pd$ $(*)$. Facciamo la divisione euclidea (Osservazione 1.2) di a (risp. b) per p:

$$a = pm + r,\ b = pt + s,\ \ 0 \leq r, s < p \ \ (**)$$

Se $r = 0 (p \mid a)$ o $s = 0 (p \mid b)$ abbiamo finito.

Supponiamo quindi $r \geq 1$ e $s \geq 1$ $(+)$; per concludere la dimostrazione basta mostrare che questo conduce ad un assurdo.

Abbiamo $ab = (pm + r)(pt + s) = p(pmt + ms + rt) + rs$, combinando con $(*)$:

$$rs = p\beta \text{ con } \beta = d - ms - rt - pmt \quad (++)$$

Se $r = s = 1$, allora $1 = p\beta$, ma questo è assurdo perché $p \geq 2$ e $\beta \geq 1$. Possiamo quindi assumere che uno tra r e s è maggiore di 1, diciamo $r > 1$. Sia q un divisore primo di r (Lemma 2.3): $r = qa_1$ con $2 \leq q \leq r$, $1 \leq a_1 < r$ (NB: $a_1 < r$ perché q, in quanto primo, è ≥ 2). Inserendo in $(++)$:

$$qa_1 s = p\beta \quad (@)$$

Quindi q divide $p\beta$ e siccome $q \leq r < p$, per ipotesi di induzione, possiamo concludere che $q \mid p$ o $q \mid \beta$. Non può essere $q \mid p$ perché p è primo e $p > q$. Quindi $q \mid \beta$: $q\beta_1 = \beta$, $1 \leq \beta_1 < \beta$. Combinando con $(@)$ viene:

$$a_1 s = p\beta_1 \text{ con } 1 \leq a_1 < s \text{ e } 1 \leq \beta_1 < \beta \quad (@@)$$

Se $a_1 = 1$ allora $s = p\beta_1$, ma questo è assurdo perché $s < p$.

Se $a_1 > 1$, sia q_1 un divisore primo di a_1 (2.3): $q_1 a_2 = a_1$, $2 \leq q_1 \leq a_1$, $1 \leq a_2 < a_1$. Ripetendo il ragionamento precedente, viene:

$$a_2 s = p\beta_2 \text{ con } 1 \leq a_2 < a_1 < s \text{ e } 1 \leq \beta_2 < \beta_1 < \beta$$

Procedendo in questo modo otteniamo una successione strettamente decrescente di numeri: $1 \leq a_i < a_{i-1} < ... < a_1 < s$ con $a_i s = p\beta_i$. Siccome c'è un numero finito di numeri tra 1 e s, si arriverà inevitabilmente a un indice j con $a_j = 1$. Si avrà allora: $a_j s = s = p\beta_j$; ma questo è assurdo perché $s < p$. Il lemma è dimostrato. □

Ancora una volta osserviamo che questa dimostrazione (che può essere semplificata con considerazioni più avanzate sul MCD) usa solo l'induzione e le quattro operazioni.

Esattamente come in 6.1 si dimostra che se un numero primo divide un prodotto, allora divide uno dei fattori. A questo punto possiamo dimostrare l'unicità:

Lemma 6.2. *Due fattorizzazioni in numeri primi del numero n differiscono solo per l'ordine dei fattori.*

Dimostrazione. Ancora una volta procediamo per induzione su n. Il caso iniziale $n = 2$ è chiaro.

Sia adesso $n = p_1.p_2...p_r = q_1.q_2...q_m$ due fattorizzazioni di n. Il numero primo p_1 divide il prodotto $q_1.q_2...q_m$, per il Lemma 6.1, p_1 divide uno dei q_i. Riordinando gli indici possiamo assumere che p_1 divide q_1. Siccome q_1 è primo (e $p_1 \geq 2$ perché primo), questo implica $p_1 = q_1$. Abbiamo $\frac{n}{p_1} = p_2...p_r = q_2...q_m$. Siccome $\frac{n}{p_1} < n$, per ipotesi di induzione: $r = m$ e, dopo avere eventualmente riordinato gli indici: $p_i = q_i$, $2 \leq i \leq r$. Quindi le due fattorizzazioni di n sono uguali (a meno dell'ordine dei fattori). □

7. Divisibilità: algebra e aritmetica.

Le idee e il linguaggio dell'algebra permettono di semplificare e generalizzare i ragionamenti dell'aritmetica elementare. Vediamo adesso come usando le strutture algebriche (gruppi, anelli, ideali) è possibile esprimere quanto fatto prima.

Nel seguito si assumono note le nozioni di gruppo, anello (commutativo). In particolare $(\mathbb{Z}, +, .)$ è un anello commutativo, integro ($m.n = 0 \Rightarrow m = 0$ o $n = 0$), cioè un *dominio*.

Si ricorda inoltre:

Definizione 7.1. *Sia A un anello commutativo. Un sotto insieme $I \subset A$ è un ideale se $(I, +)$ è un sottogruppo di $(A, +)$ e se $a \in A$, $x \in I \Rightarrow ax \in I$.*

Per esempio se $a \in \mathbb{N}$ e se indichiamo con (a) l'insieme dei multipli di a: $(a) = \{na \mid n \in \mathbb{Z}\}$, allora si verifica facilmente che (a) è un ideale di $\mathbb{Z}$.

In realtà, grazie alla divisione euclidea, si ha che *ogni* ideale di $\mathbb{Z}$ è di questa forma:

Teorema 7.2. *Ogni ideale di $\mathbb{Z}$ è della forma (a) per un qualche $a \in \mathbb{N}$.*

Dimostrazione. Sia $I \subset \mathbb{Z}$ un ideale. Se $I = \{0\}$, abbiamo finito, nel caso contrario sia $n \in I$, $n \neq 0$. Possiamo assumere $n > 0$ (perché $n \in I \Rightarrow -n \in I$).

Quindi $I_+ = \{n \in I \mid n > 0\}$ è non vuoto. Abbiamo $I_+ \subset \mathbb{N}$. Sia a il più piccolo elemento di I_+. Se $n \in I_+$ facciamo la divisione euclidea di n per a: $n = aq + r$ con $0 \leq r < a$. Per le proprietà di un ideale $n - aq \in I$, quindi $r \in I$. Se $r > 0$, $r \in I_+$, ma questo è impossibile ($r < a$). Quindi $r = 0$ e $n = aq$. Quindi ogni elemento di I_+ è un multiplo di a.

Se $m \in I$, $m < 0$, allora $-m \in I_+$, quindi $-m = at$, cioè $m = a(-t)$. Questo mostra $I = (a)$. □

Questa dimostrazione usa una proprietà fondamentale di $\mathbb{N}$: "ogni sotto insieme, non vuoto, di $\mathbb{N}$ ha un più piccolo elemento".

In un anello (commutativo) A l'insieme dei multipli di $a \in A$, cioè $(a) = \{ax \mid x \in A\}$ è sempre un ideale di A; (a) è l'ideale *generato* da a, un tale ideale (generato da un unico elemento) si dice *principale*. Il teorema 7.2 dice che in $\mathbb{Z}$, ogni ideale è principale; in altre parole $\mathbb{Z}$ è un dominio (anello integro) ad ideali principali (ogni ideale è generato da un unico elemento). Secondo la terminologia (anglosassone) vigente: $\mathbb{Z}$ è un P.I.D. (*principal ideal domain*). I P.I.D. sono una classe molto importante di anelli.

Osservazione 7.3. *Siano $a, b \in \mathbb{N}^*$. Allora $a \mid b \Leftrightarrow (b) \subset (a)$. Infatti se $a \mid b$, $aq = b$ e a è un multiplo di b, cioè $a \in (b)$. Viceversa se $(b) \subset (a)$, allora $b \in (a)$, cioè $b = qa$.*

Definizione 7.4. *Sia A un anello commutativo e siano I, J due ideali di A. Si pone $I + J = \{x + y \mid x \in I, y \in J\}$. Allora $I + J$ è un ideale di A.*

Lemma 7.5. *L'ideale $I + J$ è il più piccolo ideale contenente $I \cup J$. Cioè $I + J$ è l'intersezione di tutti gli ideali contenenti $I \cup J$.*

Dimostrazione. Sia R un ideale contenente $I \cup J$, basta mostrare che $I + J \subset R$. Sia $x + y \in I + J$, $x \in I, y \in J$. Abbiamo $x \in I \subset I \cup J$, $y \in J \subset I \cup J$. Quindi $x, y \in R$. Siccome R è un ideale, $x + y \in R$. Pertanto $I + J \subset R$. □

Proposizione 7.6. *Siano $a, b \in \mathbb{N}^*$. L'ideale $(a) + (b)$ di $\mathbb{Z}$ è principale, quindi $(a) + (b) = (d)$. Allora d è il massimo comune divisore di a e b ($d = (a, b)$).*

Quindi se $d = (a, b)$, esistono $x, y \in \mathbb{Z}$ tali che $d = ax + by$.

In particolare se a e b sono primi tra di loro ($(a, b) = 1$), esistono $x, y \in \mathbb{Z}$, tali che $ax + by = 1$.

Dimostrazione. Chiaramente $(a) \subset (a) + (b) = (d)$ ($(a) = \{ax + b0\}$), quindi $d \mid a$. Nello stesso modo $(b) \subset (d)$, quindi $d \mid b$. Pertanto $d \mid a$ e $d \mid b$.

Sia m che divide sia a che b. Quindi $(a) \subset (m)$ e $(b) \subset (m)$. Questo implica $(a) \cup (b) \subset (m)$, quindi (Lemma 7.5), $(a) + (b) = (d) \subset (m)$ e quindi $m \mid d$, in particolare $m \leq d$, segue che d è il M.C.D. di a e b. □

Questa Proposizione viene spesso citata come "lemma di Bezout" .

Possiamo adesso dimostrare il lemma di Gauss:

Lemma 7.7. *Sia p un numero primo, se $p \mid ab$, allora $p \mid a$ o $p \mid b$.*

Dimostrazione. Se $p \mid a$, abbiamo finito, altrimenti a e p sono primi tra di loro (gli unici divisori di p sono 1 e p), quindi per la Prop. 7.6 esistono $x, y, \in \mathbb{Z}$ tali che $ax + py = 1$. Moltiplicando per b: $abx + pyb = b$. Siccome $p \mid ab$ e ovviamente $p \mid p$, segue che $p \mid b$. □

Adesso come nella Sezione 6, possiamo dimostrare l'unicità della fattorizzazione in numeri primi, ottenendo cosí una terza dimostrazione del Teorema fondamentale.

Per concludere mostriamo un procedimento "effettivo" (algoritmo di Euclide) per trovare il M.C.D. di a e b.

Supponiamo $b \geq a$. Facciamo la divisione euclidea di b per a: $b = aq_0 + r_0$, $0 \leq r_0 < a$. L'osservazione cruciale è la seguente: se d divide a e b, allora d divide r_0 (e a).

Se m divide a e r_0, allora m divide b (e a).

Quindi i divisori comuni di (b, a) sono gli stessi dei divisori comuni di (a, r_0). Ma $a \leq b$ e $r_0 < a$.

Adesso ripetiamo il procedimento dividendo a per r_0:

$$a = r_0 q_1 + r_1, \;\; 0 \leq r_1 < r_0$$

Abbiamo rimpiazzato (a, r_0) con (r_0, r_1), dove $0 \leq r_1 < r_0 < a$. Questo procedimento deve necessariamente terminare dopo un numero finito di volte e terminerà con una divisione esatta: $r_{m-1} = r_m q_{m+1}$. A questo punto i divisori comuni di a e b sono i divisori comuni di r_{m-1} e r_m, ma siccome $r_m \mid r_{m-1}$, sono i divisori di r_m e il più grande di loro è r_m. Quindi $(a, b) = r_m$, cioè l'ultimo resto non nullo nelle divisioni successive.

Per esempio se $b = 1800 = 2^3.3^2.5^2$ e $a = 84 = 2^2.3.7$, abbiamo:

$$1800 = 21.84 + 36$$

e $(1800, 84) \to (84, 36)$

$$84 = 2.36 + 12$$

e $(84, 36) \to (36, 12)$

$$36 = 3.12$$

Quindi $(1800, 84) = 12$ (come si vede dalla fattorizzazione in numeri primi).

Dalla prima equazione: $36 = 1800 - 21.84$, dalla seconda: $12 = 84 - 2.36$, quindi $12 = 84 - 2.(1800 - 21.84) = 43.84 - 2.1800$ e ritroviamo l'espressione $d = ax + by$ della Prop. 7.6.

Questo è un fatto generale: dalla prima divisione $b = aq_0 + r_0$, si ricava: $r_0 = b - aq_0$, cioè r_0 è combinazione lineare di a e b. Dalla seconda divisione: $r_1 = a - r_0 q_1$. Usando l'espressione precedente di r_0, possiamo scrivere r_1 nella forma $ax + by$. Andando avanti cosí anche l'ultimo resto non nullo (cioè il M.C.D.) si scriverà nella forma $ax + by$.

8. Conclusione.

Abbiamo visto i primi, fondamentali, risultati sui numeri primi: l'insieme dei numeri primi è infinito, ogni numero è divisibile per un numero primo, il lemma di Gauss, il teorema della fattorizzazione in numeri primi (teorema fondamentale dell'aritmetica).

Per dimostrare questi risultati abbiamo usato solo le cose seguenti: proprietà elementari delle quattro operazioni e il metodo di dimostrazione per induzione (e anche quello della dimostrazione per assurdo, in particolare per l'infinità dei numeri primi).

Questa osservazione ci deve fare riflettere sull'importanza dell'induzione. A questo proposito ricordiamo le parole di Poincaré: "La matematica consiste essenzialmente in dimostrazioni. Ogni dimostrazione consiste in una serie di sillogismi. Per esempio: *Ogni uomo è mortale. Socrate è un uomo. Quindi Socrate è mortale.* A guardarci bene questo sillogismo non è un granché: all'inizio sappiamo che *tutti* gli uomini sono mortali e, alla fine, concludiamo *solo* che Socrate è mortale, non abbiamo imparato molto! Quindi, visto che la matematica non è altro che un vasto cumulo di tali sillogismi, come fa la matematica a non essere solo una grande trivialità?"

Per Poincaré la risposta sta nella nozione d'infinito: la matematica si occupa di collezioni infinite di oggetti (i numeri naturali, i punti di una retta). Ma com'è possibile questo, visto che una dimostrazione (o una definizione) consta necessariamente di un numero finito di parole? Secondo Poincaré è proprio l'induzione che, "zippando" in poche righe un'infinità di sillogismi, rende questa trattazione possibile. A pensarci bene la nozione di infinito non è così scontata come potrebbe sembrare...

Bibliografia

[1] Davenport, H.: *The higher arithmetic*, Cambridge Univ. Press (sixth edition) (1992)

[2] Hardy, G. H.-Wright E. M.: *An introduction to the theory of numbers*, Oxford Univ. Press (fifth edition) (1979)

Index

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