

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

Come indicato nel titolo l'obiettivo è di dare una dimostrazione del teorema fondamentale dell'aritmetica e far capire ai discenti l'importanza dei numeri primi, mattoni alla base della struttura dei numeri:

Ogni numero naturale si scrive in modo sostanzialmente unico come un prodotto di numeri primi.

1. Numeri primi: definizioni.

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.

I numeri primi, come vedremo fra poco, sono i mattoni che permettono di costruire tutti gli altri numeri

1.1. Fare la lista dei numeri primi

Come fare per decidere se un numero dato, n , è primo o no?.

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 .

Il Crivello di Erastotene.

Questo metodo è sostanzialmente un metodo costruttivo per fare la lista dei numeri primi $< N$, N dato.

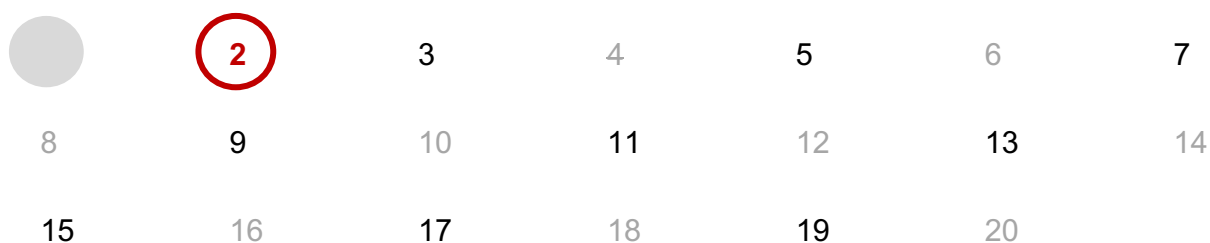
Su un foglio di carta scriviamo i numeri da 1 a 20.

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	

Sbarriamo il numero 1 il quale, per definizione, non è primo.

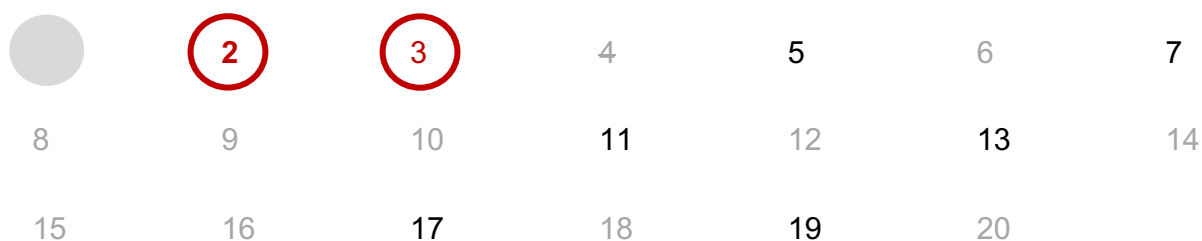
	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	

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).

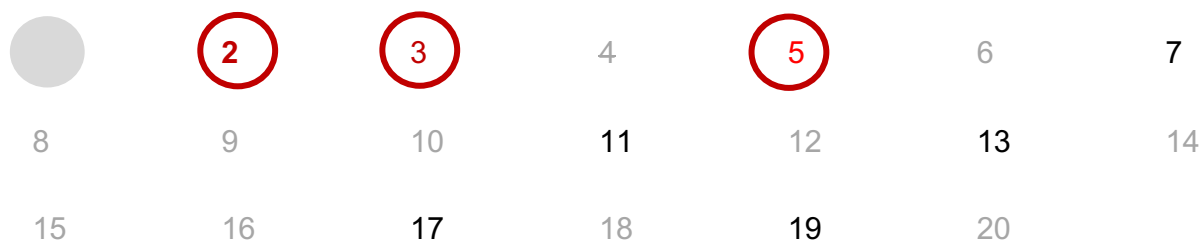


Il numero più basso né sbarrato, né accerchiato è il numero 3.

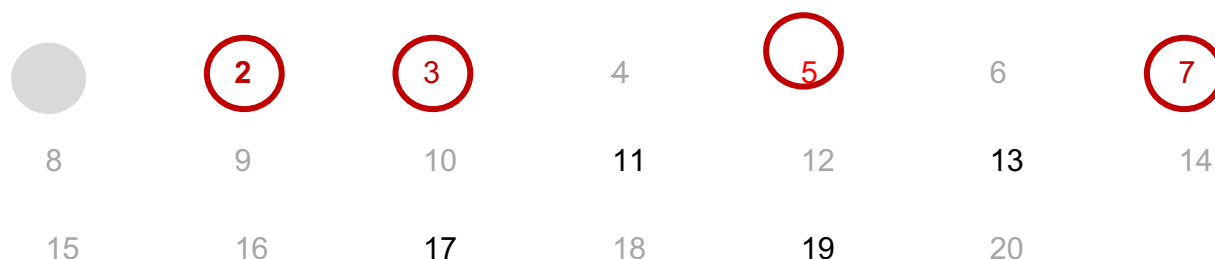
Lo accerchiamo e sbarriamo tutti i suoi multipli (che di sicuro non sono numeri primi in quanto divisibili per 3): 6 è già sbarrato in quanto multiplo di 2, sbarriamo 9, 12 è già sbarrato, sbarriamo 15, ecc...



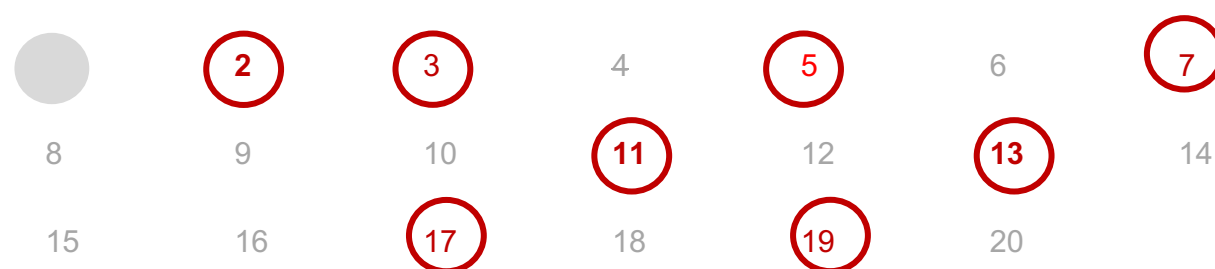
Fatto ciò il numero più basso, né cerchiato, né sbarrato, è il numero 5: lo accerchiamo e sbarriamo i suoi multipli (in realtà 10, 15, 20 sono già sbarrati in quanto multipli di 2 o 3).



Fatto ciò il numero più basso né sbarrato, né cerchiato è il numero 7: 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).

Esercizio: usando il crivello di Erastotene, fare la lista dei numeri primi ≤ 100 .

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 , $2 \leq m \leq n-1$: 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.

2. 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: $15 = 3 \cdot 5$, $60 = 2^2 \cdot 3 \cdot 5$. 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.

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 $N = F$ (allora ogni numero appartiene ad F).

Se indichiamo con $x+1$ il successore di x, la condizione 4. si legge:

$[0 \in F \text{ e } x \in F \Rightarrow x+1 \in F] \Rightarrow F = N$.

La condizione 4. è il principio di induzione.

Notiamo che questi assiomi non bastano a definire N perché usano un termine non definito, quello di "insieme".

Oggigiorno la nozione di numero (naturale, intero, 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**:

Questo è il famoso paradosso di Russel:

In un villaggio c'è un barbiere. Il barbiere fa 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 fa la barba c'è una contraddizione perché il barbiere fa la barba solo a quelli che non si fanno la barba loro stessi.

Se il barbiere non si fa la barba, c'è una contraddizione perché il barbiere fa 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 la regola 4. (principio di induzione) è uno dei principi di base.