Proposizione: "Unicità della scomposizione in fattori primi.

"La scomposizione in fattori primi è unica. A parte permutazioni di fattori, un naturale può essere espresso come prodotto di primi in un solo modo".

Dimostrazione (Lindemann)

Chiamiamo numeri enormali i numeri che possono essere fattorizzati in prodotti di primi in più modi (a parte permutazioni).

Sia n il numero enormale più piccolo. Lo stesso primo p non può comparire in più fattorizzazioni di n.

Se, diversamente, p comparisse in più fattorizzazioni n/p sarebbe enormale; infatti $\frac{n}{p} < n$ ma così avendo per ogni abbiamo definito n.

Allora

$$n = p_1 p_2 p_3 \cdots = q_1 q_2 q_3 \cdots$$

dove i p_i e q_j sono primi e nessun p è uguale a q e nessun p è uguale a p.

Sia p_1 il minimo dei p. Allora

$p_1^2 \leq n$

Sia q_1 il minimo dei q. Allora

$q_1^2 \leq n$. Poiché $p_1 \neq q_1 \Rightarrow p_1 q_1 < n$

Poniamo $N = n - p_1 q_1$, $0 < N < n$

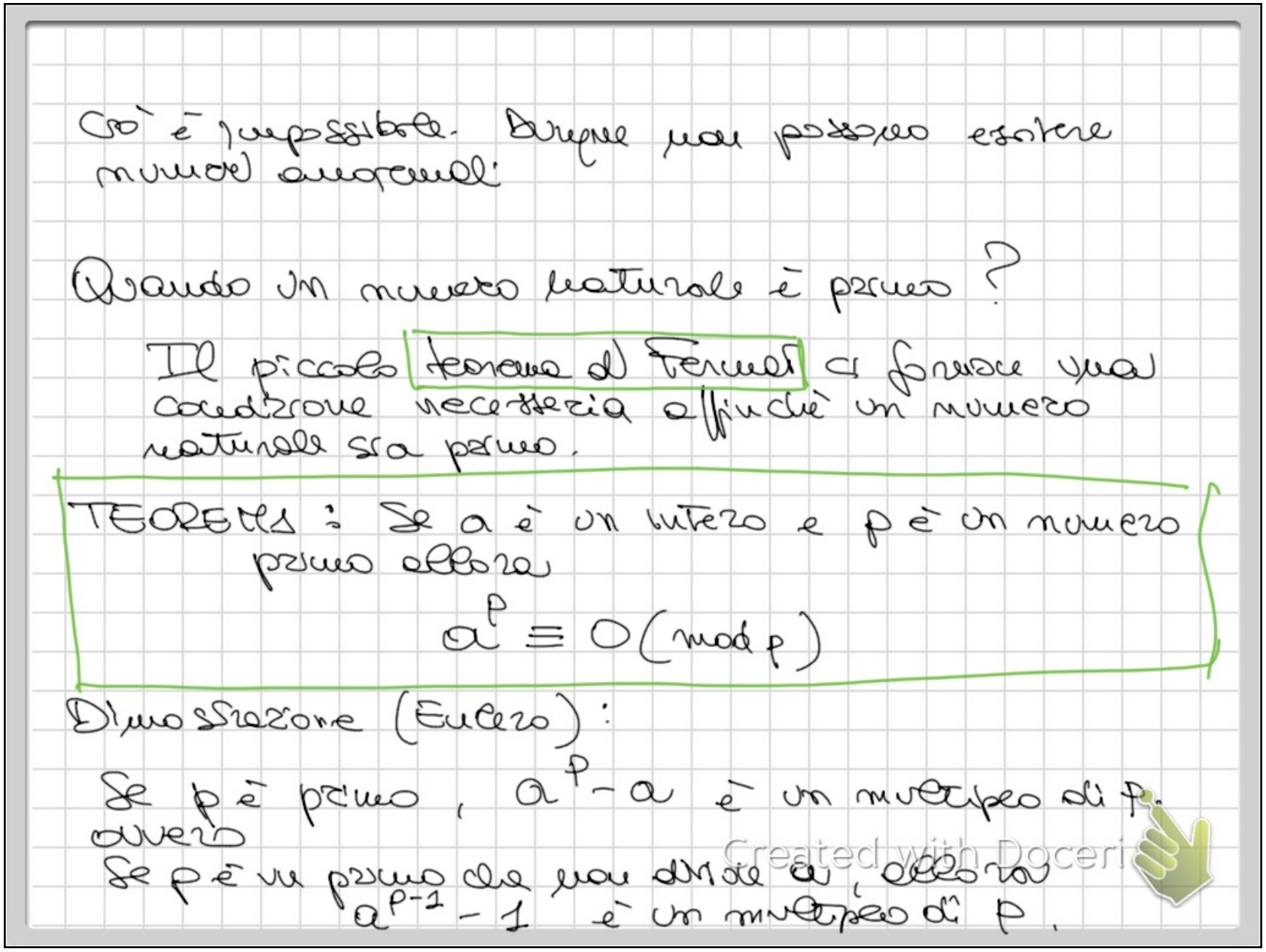
dunque N non è annullo.

$\frac{p_1}{n}$ $\frac{p_1}{N}$ $\frac{q_1}{n}$ $\frac{q_1}{N}$

p_1 e q_1 appaiono entrambi nella unica fattorizzazione di N $\frac{p_1 q_1}{N}$

Da ciò segue che $\frac{p_1 q_1}{n}$ e quindi $q_1 \mid n/p_1$

Ma n/p_1 è minore di n e dunque ammette una unica fattorizzazione $p_2 p_3 \cdots$ Dato che q_1 non è un p_i



Così è impossibile. Dunque non possono esistere numeri primi gemelli.

Quando un numero naturale è primo?

Il piccolo teorema di Fermat ci fornisce una condizione necessaria affinché un numero naturale sia primo.

TEOREMA: Se a è un intero e p è un numero primo allora

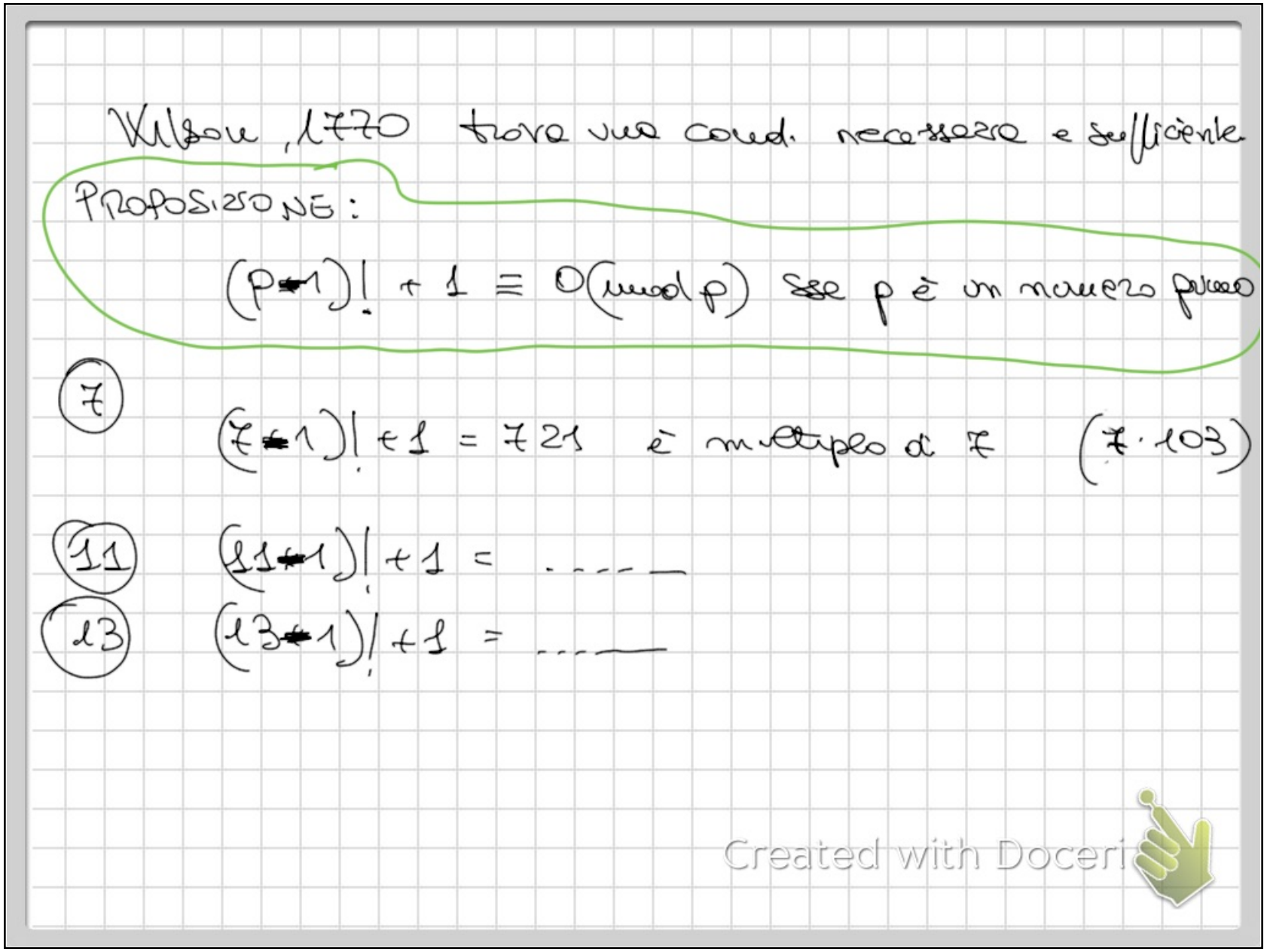
$$a^p \equiv 0 \pmod{p}$$

Dimostrazione (Eulero):

Se p è primo, $a^p - a$ è un multiplo di p.
ovvero
Se p è un primo che non divide a, allora
$a^{p-1} - 1$ è un multiplo di p.

Questa condizione è necessaria ma non sufficiente

Cioè tutti i numeri primi soddisfano questa espressione del piccolo teorema di Fermat, ma non tutti i numeri che soddisfano tale condizione sono primi.


Wilson, 1770 trova una cond. necessaria e sufficiente
PROPOSIZIONE:
$(p-1)! + 1 \equiv 0 \pmod{p}$ sse p è un numero primo
7
$(7-1)! + 1 = 721$ è multiplo di 7 $(7 \cdot 103)$
11
$(11-1)! + 1 =$ ....
13
$(13-1)! + 1 =$ ....
Created with Doceri

Euclide (libro IX, XX)

"I numeri primi sono sempre più di ogni assegnata quantità di primi".

Dimostrazione:

Sia $p_1, p_2, \dots, p_r$ una assegnata quantità di numeri primi

Poniamo $P = p_1 p_2 \cdots p_r + 1$. Sia p un numero primo che divide P

Ora p non può essere $p_1, p_2, \dots, p_r$ altrimenti p dividerebbe la differenza $P - 1$ ovvero

$p_1 - p_1 p_2 \cdots p_r$ ma ciò è impossibile.

Dunque questo p è diverso da $p_1, p_2, \dots, p_r$

(Provate a usare una dimostrazione moderna)

Teorema fondamentale dell'aritmetica

Ogni numero naturale maggiore di 1 o è un numero primo o si può esprimere come prodotto di numeri primi. Tale rappresentazione è unica, se si prescinde dall'ordine in cui compaiono i fattori.

Dimostrazione: Si parte dalla definizione di numero primo da cui si può dedurre che ogni numero maggiore o uguale a 2 o è un primo oppure ha un divisore che è un numero primo.
Per induzione

$n = 2$ è primo soddisfa l'enunciato

Supponiamo vero l'enunciato per tutti i numeri da 2 a n. e dimostriamo che vale anche per $n+1$.

Per $n+1$ abbiamo 2 possibilità o esso è primo oppure è divisibile per un numero compreso tra 2 e n.

Nel caso in cui $n+1$ sia divisibile per se stesso, per l'ipotesi induttiva, che a è primo oppure ha un divisore primo p.
In quest'ultimo caso p è anche un divisore di $n+1$
In ogni caso o $n+1$ è primo o è divisibile per un primo.

Ancora per induzione dimostro che la fattorizzazione è unica:

$n=2$ ho il caso banale perché 2 è primo e già fattorizzato

Supposo vera l'esistenza di una fattorizzazione per tutti i naturali compresi tra 2 e n.
Dimostro che è vero per $n+1$

Considero $n+1$, ho 2 casi possibili: o $n+1$ è primo oppure è divisibile per un primo p.
Nel secondo caso posso scrivere

$$m = \frac{n+1}{p} \qquad m < n+1$$

Quindi esiste

Una fattorizzazione di m - Perciò

$m+1 = m \cdot p$ cioè $m+1$ è fattorizzabile

Quindi l'esistenza di una fattorizzazione è dimostrata per ogni naturale n.

UNICITÀ Per assurdo supponiamo che esistano dei numeri scomponibili in fattori primi in più modi e sia m il più piccolo (per il principio del buon ordinamento).

Prendiamo 2 diverse fattorizzazioni

$$m = p_1 p_2 \cdots p_s$$

$$m = q_1 q_2 \cdots q_t$$

p_i e q_j sono primi tra di loro, cioè

$\forall i,j : p_i \neq q_j$.

Se infatti ci fosse un fattore identico $p_h = p_k$ possiamo ricondurci al caso indicato dividendo m per tale fattore e ottenendo un numero $m' < m$ che avrebbe anch'esso fattorizzazioni distinte.

A questo punto supponiamo che $p_1 \neq q_1$ e possiamo supporre

$$p_1 < q_1$$

Possiamo porre allora $n = (q_1 - p_1)\, q_2 \cdots q_t$

$n < m$

Dimostriamo che anche due diverse fattorizzazioni distinte

$q_1 - p_1$ — primo

non primo → lo possiamo fattorizzare

una delle nuove fattorizzazioni avrebbe p_1 tra i suoi fattori.

Ma p_1 è diverso da $q_2 q_3 \cdots q_t$ e quindi non può comparire nella fattorizzazione di $q_1 - p_1$.

Se ciò accadesse $q_1 - p_1 = p_1 u$

e dunque $q_1 = p_1(u+1)$ il che non è possibile. Possiamo affermare che $q_1 - p_1$ è primo

Se scriviamo

$$n = (q_1 - p_1) q_2 \cdots q_t =$$

$$= q_1 q_2 \cdots q_t - p_1 q_2 \cdots q_t = m - p_1 q_2 \cdots q_t =$$

$$= p_1 (p_2 \cdots p_s - q_2 \cdots q_t)$$

Otteniamo una fattorizzazione di n che ha p_1 come fattore e dunque è divisa da quella fornita in precedenza. Ciò è assurdo perché causa l'ipotesi che n sia il più piccolo intero con fattorizzazione prima distinta.

Concetto di cardinalità (vedere)

Proposizione: L'insieme $P \subseteq \mathbb{N}$ dei numeri naturali pari è equipotente a $\mathbb{N}$.

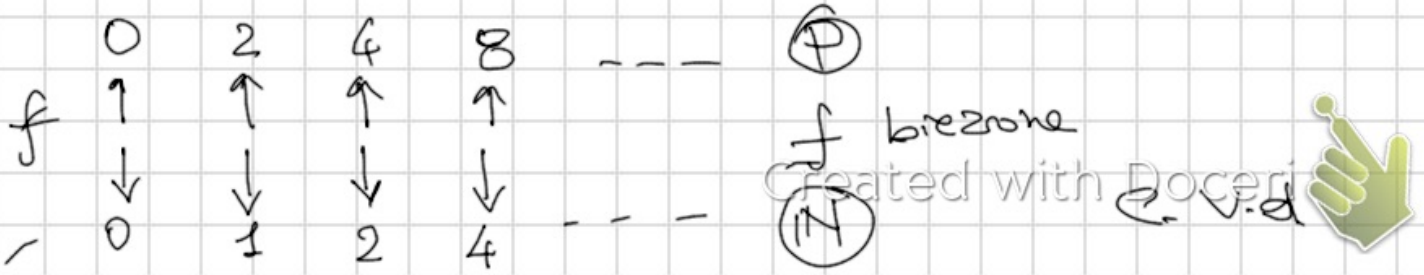
Dimostrazione: Sia P l'insieme di numeri pari

$$P = \{ m \in \mathbb{N} : m = 2n, n \in \mathbb{N} \}$$

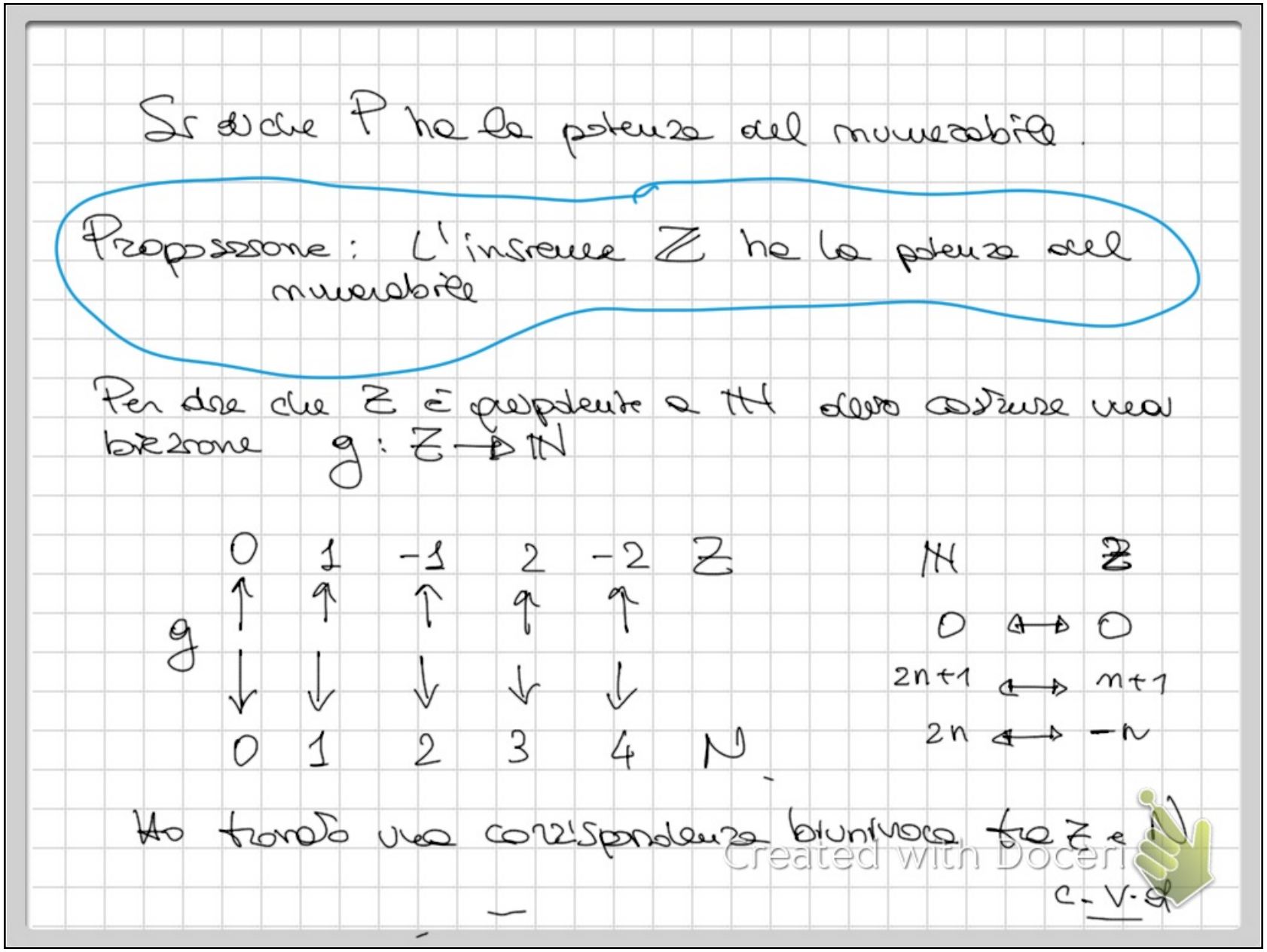
Devo individuare una funzione $f: P \to \mathbb{N}$ biettiva

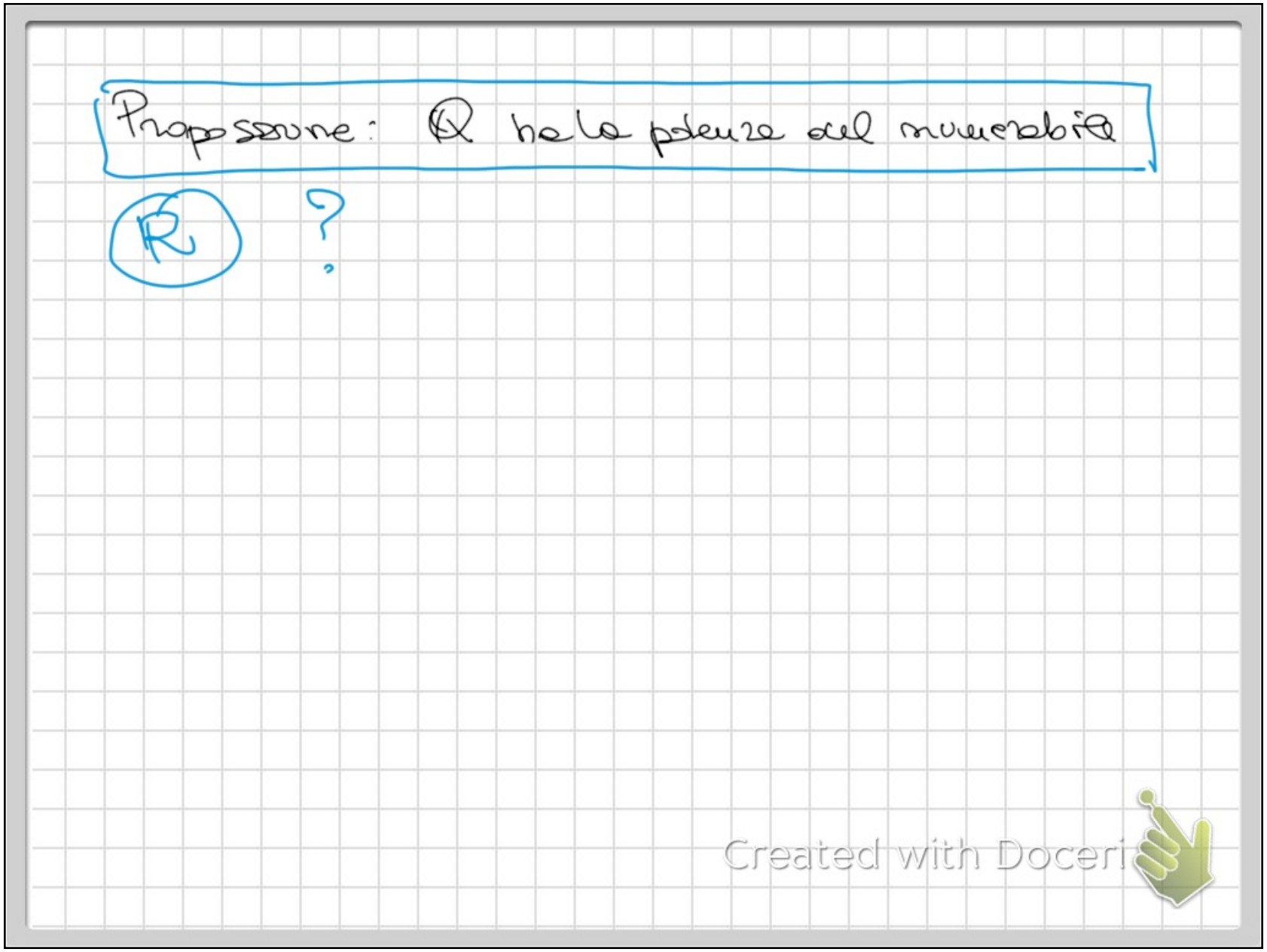
$$f: x \in P \to \frac{x}{2} \in \mathbb{N}$$

Questo che f è biettiva ovvero che gli elementi di P possono essere posti in corrispondenza con gli elementi di $\mathbb{N}$.



c.v.d.


Si dice P ha la potenza del numerabile.
Proposizione: L'insieme Z ha la potenza del numerabile
Per dire che Z è equipotente a N devo costruire una biezione g: Z → N
0 1 -1 2 -2 Z
g
0 1 2 3 4 N
N Z
0 ↔ 0
2n+1 ↔ n+1
2n ↔ -n
Ho trovato una corrispondenza biunivoca tra Z e N
Created with Doceri
C.V.D.


Proposizione: R ha la potenza del numerabile
R
?
Created with Doceri