

Congettura 1 Sia $k > 1$ un numero reale. Allora esistono solo un numero finito di terne (a, b, c) di numeri naturali che soddisfano $a + b = c$, $(a, b, c) = 1$ e $c > \text{rad}(abc)^k$, dove $\text{rad}(n)$ per $n \in \mathbb{N}$ è il prodotto dei fattori primi distinti di n .

Questa congettura è molto importante, perchè spiega qualcosa dei nostri numeri naturali. Alcuni famosi teorema possono essere dimostrati facilmente partendo da essa, se è vera. Per esempio, il teorema di Catalan, di Fermat, la congettura di Fermat-Catalan (Super Fermat), la congettura di Schinzel-Tijdeman etc. Al contrario, non ci sono molti teoremi sulla supposizione, ma ce ne è uno di Granville.

Definizione 2 Definiamo $\text{pow}(n)$ come

$$\text{pow}(n) = \log n / \log \text{rad}(n).$$

Adesso siamo pronti per il teorema.

Teorema 3 (Granville) Sia $a \geq 1$. Allora

$$\lim_{n \rightarrow \infty} \frac{\log \#\{n \leq N \mid \text{pow}(n) \geq a\}}{\log N} = 1/a$$

DIMOSTRAZIONE. Primo di tutto, proviamo un limite inferiore:

Se $a \in \mathbb{Z}_{>0}$, è vero che

$$\#\{n \leq N : \text{pow}(n) \geq a\} \geq \lfloor N^{1/a} \rfloor.$$

Infatti ogni numero n minore di $N^{1/a}$ a potenza a è un proprio una a -potenza, e per questi numeri $\text{pow}(n) \geq a$. E naturalmente $\log N^{1/a} / \log N = 1/a$.

Se $a \notin \mathbb{Z}_{>0}$, sia $k \in \mathbb{N}_{>0}$ tale che $k < a \leq k + 1$. Prendiamo i numeri di forma $n = t^k u^{k+1}$ con $u, t \in \mathbb{Z}_{>0}$ e con t senza quadrati. Allora $\text{rad}(n) \leq tu$. Ci sono due condizione per n nell'insieme indicato sopra: $n \leq N$ e $\text{rad}(n)^a \leq n$. Quindi la prima condizione diventa $t^k u^{k+1} \leq N$ e la seconda diventa $(tu)^a \leq n = t^k u^{k+1}$, ovvero, $t^{a-k} \leq u^{k+1-a}$, o anche $t^k \leq u^{(k+1-a)k/(a-k)}$. Queste due condizioni, insieme, danno $u^{1/\gamma} \leq N$ con

$$\gamma := \frac{1}{(k+1) + (k+1-a)k/(a-k)}$$

e quindi

$$\#\{n \leq N : \text{pow}(n) \geq a\} \geq \sum_{0 < u \leq N^\gamma} \#\{t : 0 < t \leq (u^{k+1-a})^{1/(a-k)}, t \text{ senza quadrati}\}.$$

Abbiamo bisogno che t sia senza quadrati, altrimenti conteremmo nel secondo membro più di una volta, sbagliando.

Questa diseguaglianza è proprio il limite inferiore perchè abbiamo considerato n particolari, del tipo prodotto di due potenze.

Il numero $\#\{t : 0 < t \leq u^{(k+1-a)/(a-k)}, t \text{ senza quadrati}\}$ è più o meno uguale a $cu^{(k+1-a)/(a-k)}$ per qualsiasi costante c . Quindi

$$\#\{n \leq N : \text{pow}(n) \geq a\} \simeq c \int_1^{N^\gamma} u^{(k+1-a)/(a-k)} du \simeq c' u^{(k+1-a)/(a-k)+1} \Big|_1^{N^\gamma} = c' N^{1/a}$$

Questa conclude la prova del limite inferiore.

Ora, proviamo il limite superiore. È vero che

$$\#\{n \leq N : \text{pow}(n) \geq a\} = \#\{n \leq N : \text{rad}(n) \leq N^{1/a}\} \leq \sum_{n=1}^{\infty} \left(\frac{N^{1/a}}{\text{rad}(n)} \right)$$

Il lato a destra non converge, ma usiamo un trucco per farla convergere:

$$\#\{n \leq N : \text{rad}(n) \leq N^{1/a}\} \leq \sum_{n=1}^{\infty} \left(\frac{N^{1/a}}{\text{rad}(n)} \frac{N}{n} \right)$$

che ancora non converge, però per ogni $\epsilon > 0$

$$\#\{n \leq N : \text{rad}(n) \leq N^{1/a}\} \leq \sum_{n=1}^{\infty} \left(\left(\frac{N^{1/a}}{\text{rad}(n)} \right)^{1+\epsilon} \left(\frac{N}{n} \right)^\epsilon \right) = N^{1/a(1+\epsilon)+\epsilon} f(\epsilon)$$

e questa converge! Infatti

$$f(\epsilon) = \sum_{n=1}^{\infty} \left(\frac{1}{\text{rad}(n)} \right)^{1+\epsilon} \frac{1}{n^\epsilon} = \prod_{p \text{ primo}} \left(1 + \frac{1}{p^{1+\epsilon}} (1/p^\epsilon + 1/p^{2\epsilon} + \dots) \right)$$

L'ultima uguaglianza segue per mezzo del contare. Inoltre

$$1/p^\epsilon + 1/p^{2\epsilon} + \dots = 1/(p^\epsilon - 1) \leq 1/(2^\epsilon - 1)$$

e perciò $f(\epsilon)$ è limitata da

$$f(\epsilon) \leq \prod_{p \text{ primo}} (1 + 1/(2^\epsilon - 1) \cdot 1/p^{1+\epsilon}).$$

Poichè la serie

$$\sum_{p \text{ primo}} 1/(2^\epsilon - 1) \cdot 1/p^{1+\epsilon}$$

è finita, il prodotto sopra è anch'esso finito, passando ai logaritmi, e quindi la funzione $f(\epsilon)$ è finita. Adesso abbiamo:

$$\frac{\log \#\{n \leq N : \text{rad}(n) \leq N^{1/a}\}}{\log N} \leq 1/a(1 + \epsilon) + \epsilon + \frac{\log f(\epsilon)}{\log N}.$$

Passando al limite su ϵ nel limite superiore si ha:

$$\lim_{\epsilon \rightarrow 0} \limsup_{N \rightarrow \infty} \frac{\log \#\{n \leq N : \text{rad}(n) \leq N^{1/a}\}}{\log N} \leq 1/a.$$

Il teorema è provato. \square

Il prossimo teorema è usato nel progetto di ABC@Home, anzi con questo teorema è possibile costruire un algoritmo per contare il numero di terne abc. Cominciamo con descrivere l'algoritmo:

Algoritmo 4 Algoritmo per trovare tutte le terne di numeri naturali (a, b, c) con $a + b = c$, $(a, b, c) = 1$ e con $q > 1$:

1. Scriviamo una lista ordinata dei primi minori di N
2. Con questi primi, calcoliamo dei numeri $r < N$ senza quadrati: prima numeri p_1^i con $\text{rad} = p_1$, poi numeri $p_1^i p_2^j$ con $\text{rad} = p_1 p_2$, etc.
3. Per ogni r , con lo stesso procedimento usato per trovare r , creiamo un numero s tale che $rs < N^a$ e $(r, s) = 1$.
4. Se $r > s$, allora $r + s = c$, $s = a$, $r = b$, o analogamente $a = r - s$, $b = s$, $c = r$.
5. Controlliamo se $(a, b, c) = 1$ e se $q > 1$

Definizione 5 Definiamo order in questo modo: per ogni paio di funzioni f e g nello stesso anello con co-dominio R , $f = \text{order}(g)$ se e solo se per ogni $\epsilon > 0$ e $\epsilon \in R$ abbiamo $f = O(g^{1+\epsilon})$.

Teorema 6 Il numero di terne abc con qualità almeno q e con $c < N$ è al massimo $\text{order}(N^{2q/3})$.

DIMOSTRAZIONE. Siano a, b, c una terna abc, e $\{x, y, z\}$ tali che $\text{rad}(x) \leq \text{rad}(y) \leq \text{rad}(z)$. Supponiamo inoltre che $\text{rad}(x)\text{rad}(y) = \text{rad}(xy) \leq N^{2q/3}$. Per x e y , il numero z può essere $x - y$ o $x + y$ se $x > y$. Allora il numero di terne abc è al massimo due volte il numero di coppie (x, y) tali che $0 < x, y \leq N$ e $\text{rad}(xy) < N^{2q/3}$, e tale numero è $\text{order}(N^{2q/3})$ in virtù del seguente lemma.

Lemma 1 Per ogni $a \geq 1$:

$$\lim_{N \rightarrow \infty} \frac{\log \#\{(x, y) \in \mathbb{N}^2 : 0 < x, y < N, \text{rad}(xy) < N^a\}}{\log N} = a$$

DIMOSTRAZIONE. Sia $S \in \mathbb{Z}_{>0}$ un numero fissato e per $1 \leq k \leq S$ definiamo

$$R_k = \{(x, y) \in \mathbb{N}^2 : 0 < x, y \leq N, \text{rad}(x) \leq N^{ka/S}, \text{rad}(y) < N^{(S-k+1)a/S}\}.$$

Dal teorema di Granville, la grandezza di R_k è come $\text{order}(N^{a(1+1/S)})$ se $N \rightarrow \infty$. L'insieme di cui vogliamo sapere la cardinalità è contenuto nell'unione R di ogni R_k e anche R ha una grandezza come $\text{order}(N^{a(1+1/S)})$. Poichè S è fissato, e poichè questo è vero per ogni S , possiamo considerare come $\text{order} N^{a/S}$. Il lemma è provato. \square

Il teorema è provato. \square

Questo teorema ci dà qualche informazione necessaria per sapere qualcosa sul nostro algoritmo.

Corollario 1 *I primi quattro passi dell'algorithmo sopracitato per trovare tutte le terne con $c < N$ e con qualità almeno q ha complessità $\text{order}(N^{2q/3})$.*

DIMOSTRAZIONE. Il primo passo costa $O(N^{2q/3} \log N^{2q/3})$. Il secondo passo costa una moltiplicazione per ogni numero, e dal teorema di Granville ci sono $\text{order}N^{2q/3}$ quei numeri. Il terzo passo è più o meno il Lemma sopra ed anche questo costa $\text{order}(N^{2q/3})$. Il quarto passo è una costante per ogni risultato. \square

Per il progetto ABC@Home abbiamo preso $N = 10^{18}$ e $q = 1$. Un'ultima domanda rimane, che sarà ϵ nel nostro caso? Chissà.