

Block Notes Matematico

La congettura abc

Rosario Turco, Maria Colonnese

Sommario

In ogni attività umana è necessario partire dall'abc, ovvero dalle cose più semplici, in modo da apprendere e dominare l'argomento; ma qui gli autori ci mostrano, invece, una delle più recenti congetture, la "congettura abc" proposta nel 1985 da J. Oesterlè e raffinata successivamente da D. W. Masser.

Oesterlè motivò la sua congettura a seguito di un lavoro di Szpiro riguardante le curve ellittiche; mentre Masser, sulla scia del Teorema di Mason sui polinomi, introdusse un'analogia congettura su \mathbb{Z} per i polinomi.

La congettura abc è semplice da formulare, ma è difficile da dimostrare; essa dimostrerebbe la forma debole dell'Ultimo Teorema di Fermat (UTF), un equivalente del Teorema di Fermat sui polinomi, il problema di Fermat asintotico, le condizioni di Wieferich, la congettura originale di Hall, la congettura di Szpiro, le coppie di Brown e i numeri forti o potenti, la congettura di Erdos-Mollin-Walsh, la congettura di Mordell, i risultati di Elkies, Bombieri e Granville.

Una sua soluzione positiva, cioè, porta come effetto domino alla soluzione di altre congetture. Su essa lo studio confluisce anche nel settore della computazione a forza bruta, per la ricerca di triple che soddisfano la congettura stessa.

L'articolo è soprattutto un tentativo per avvicinare il lettore alla congettura ed, inoltre, costituisce una breve esposizione delle principali informazioni disponibili sull'argomento.

Introduzione

Chiamiamo con \mathbf{P} l'insieme dei numeri primi.

Definizione

Per $n \in \mathbf{P}$, supponiamo $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_k^{e_k}$ dove i p_i sono numeri primi distinti e gli e_i numeri interi.

Si definisce *radicale di n* la quantità:

$$r(n) = p_1 \cdot p_2 \cdot \dots \cdot p_k$$

In altri termini il radicale di n è il prodotto dei suoi fattori privi di potenza.

Nota: nel seguito dell'articolo gcd indica il MCD e deg il grado di un polinomio. Inoltre useremo la notazione $x(t) \ll y(t)$ come equivalente a $x(t) = O(y(t))$, il che vuol dire che esiste un $C \in \mathbb{R}$, $C > 0$ tale che $x(t) \leq C y(t)$. Il simbolo \square indica, invece, la fine di una dimostrazione.

Congettura abc (formulazione di Oesterlè)

Se consideriamo triple non banali di numeri interi con $a, b, c > 0$ e tali che: $a + b = c$ e $\gcd(a, b) = 1$ allora è:

$$L = L(a, b, c) = \frac{\log \max(|a|, |b|, |c|)}{\log r(abc)} = \frac{\log c}{\log r(abc)}$$

e le funzioni L sono limitate.

Congettura abc (formulazione di Masser)

Per ogni $\varepsilon > 0$ esiste una costante universale positiva $\mu(\varepsilon)$ tale che:

$$\max(|a|, |b|, |c|) = c \leq \mu(\varepsilon) r(abc)^{1+\varepsilon}$$

Vediamo alcuni Lemmi utili per il prosieguo.

Lemma 1

Sotto le ipotesi della congettura abc, la funzione $r(n)$ è una funzione moltiplicativa.

Dim.

Questo è garantito da $\gcd(a, b) = 1$. \square

Lemma 2

Per tutti gli $n \in \mathbb{P}$, è sempre $r(n) \leq n$.

Dim.

E' una conseguenza della definizione di radicale. \square

Per il prosieguo occorre comprendere perché è importante la ε nella formulazione di Masser; a tal proposito useremo un esempio di Wojtek Jastrzebowski e Dan Spielman riportato da Serge Lang [1].

Lemma 3

Supponiamo che $a_n = 3^{2^n} - 1, b_n = 1, c_n = 3^{2^n}, n \in \mathbb{P}$. I tre valori sono scelti in modo da rispettare la congettura abc: $a_n + b_n = c_n$. Dimostriamo che $2^n \mid 3^{2^n} - 1$.

Dim.

Per $n=1$ è evidente che $2 \mid 3^2 - 1$.

Assumiamo che sia vero anche per induzione per $n = k$, cioè: $2^k \mid 3^{2^k} - 1$.

Ora possiamo scrivere che:

$$3^{2^{k+1}} - 1 = 3^{2^k \cdot 2} - 1 = (3^{2^k})^2 - 1 =$$

Per la differenza dei quadrati $a^2 - 1 = (a-1)(a+1)$ allora diventa:

$$= (3^{2^k} - 1)(3^{2^k} + 1)$$

Poiché per induzione è $2^k \mid 3^{2^k} - 1$ e $2 \mid 3^{2^k} + 1$ perché il termine a destra è pari, quindi è vero che $2^{k+1} \mid 3^{2^{k+1}} - 1$ e per induzione è vero che $2^n \mid 3^{2^n} - 1$. \square

Lemma 4

Nella congettura abc è necessario ε .

Dim.

Supponiamo $a_n = 3^{2^n} - 1, b_n = 1, c_n = 3^{2^n}, n \in \mathbb{P}$ e che *per assurdo* che esista un μ tale che $c_n \leq \mu \cdot r(a_n b_n c_n)$.

Ora dalla ipotesi per assurdo e dalla definizione della congettura abc nella formulazione di Masser si ha che:

$$\max(|a_n|, |b_n|, |c_n|) = c_n = 3^{2^n}$$

$$3^{2^n} \leq \mu \cdot r(a_n b_n c_n) =$$

$$= \mu \cdot r(|3^{2^n} - 1| \cdot 1 \cdot 3^{2^n}) =$$

Se sfruttiamo il Lemma 1 ed il concetto di radicale sul termine $1 \cdot 3^{2^n}$ otteniamo che:

$$= \mu \cdot 3 \cdot r(|3^{2^n} - 1|) =$$

$$= \mu \cdot 3 \cdot r\left(\frac{2^n |3^{2^n} - 1|}{2^n}\right) =$$

Se sfruttiamo il Lemma 3 ed il concetto di radicale si ha:

$$= \mu \cdot 3 \cdot 2 \cdot r\left(\frac{3^{2^n} - 1}{2^n}\right)$$

Per cui si è arrivati alla conclusione che:

$$3^{2^n} \leq \mu \cdot 3 \cdot 2 \cdot r\left(\frac{3^{2^n} - 1}{2^n}\right)$$

Moltiplicando entrambi i lati per 2^n e dividendo per , si ottiene che:

$$2^n \leq \mu \cdot 6 \cdot \frac{3^{2^n} - 1}{3^{2^n}}$$

Se si passa al limite $n \rightarrow \infty$ la disuguaglianza fallisce, cioè esiste una contraddizione! Quindi μ deve dipendere per forza da ε . \square

Ma in che modo μ dipende da ε ?

Lemma 5

Nella congettura abc $\mu(\varepsilon)$ varia inversamente a ε . [Non lo dimostriamo].

La congettura polinomiale abc

Definizione

Sia $p(t)$ un polinomio i cui coefficienti appartengono ad un *campo algebricamente chiuso*¹ di caratteristica 0^2 . Diciamo $n_0(p)$ il numero di zeri distinti di $p(t)$, ovvero il numero di zeri di molteplicità 1 del polinomio.

Nel seguito faremo notare la somiglianza tra Teorema di Mason e la congettura abc nella forma di Masser.

Teorema di Mason

Siano $a(t), b(t), c(t)$ tre polinomi i cui coefficienti appartengono ad un campo algebricamente chiuso di caratteristica 0. Supponiamo $a(t), b(t), c(t)$ relativamente primi tra loro e che $a(t) + b(t) = c(t)$; allora è:

$$\max \deg \{a(t), b(t), c(t)\} \leq n_0(a(t) \cdot b(t) \cdot c(t)) - 1$$

Dim.

$$a + b = c \Rightarrow \frac{a}{c} + \frac{b}{c} = 1 \quad \text{ora se poniamo } f = a/c, g = b/c, \text{ allora è: } f + g = 1$$

Differenziando si ottiene che:

$$f' + g' = 0 \text{ da cui è: } \frac{f'}{f} \cdot f + \frac{g'}{g} \cdot g = 0 \Rightarrow \frac{g'}{g} \cdot g = -\frac{f'}{f} \cdot f \quad \text{per cui è: } \frac{g}{f} = \frac{-f'}{g'}$$

Poiché $a = f \cdot c, b = g \cdot c$ allora da qui è: $\frac{b}{a} = \frac{g}{f}$ da cui è:

$$\frac{b}{a} = \frac{-f'}{g'} \quad (1)$$

Definiamo con $R(t)$ una funzione razionale con ρ_i le radici distinte del numeratore e del denominatore; allora è:

¹ Un campo F è detto algebricamente chiuso se ogni polinomio di grado almeno 1, a coefficienti in F , ha una radice in F (cioè un elemento x tale che il valore del polinomio in x è l'elemento neutro dell'addizione in F). Ad esempio, il campo dei numeri reali non è algebricamente chiuso, perché l'equazione polinomiale $3x^2 + 1 = 0$ non ha soluzioni nei reali, anche se entrambi i suoi coefficienti (3 e 1) sono reali. Al contrario, il campo dei numeri complessi è algebricamente chiuso: questo è ciò che afferma il teorema fondamentale dell'algebra.

Dato un campo F , l'affermazione " F è algebricamente chiuso" è equivalente ad ognuna delle seguenti:

- Ogni polinomio $p(x)$ di grado $n \geq 1$, a coefficienti in F , è decomponibile in fattori lineari. In altre parole, vi sono elementi k, x_1, x_2, \dots, x_n del campo F tali che $p(x) = k(x - x_1)(x - x_2) \cdots (x - x_n)$.
- Il campo F non possiede estensioni algebriche proprie.

² Il più piccolo intero positivo n tale che $n \cdot 1 = 0$; qui $n \cdot 1$ sta per la somma di n sommandi $1 + 1 + 1 + \dots + 1$. Se un tale intero non esiste si dice che la caratteristica del campo è zero. Ogni caratteristica diversa da zero è un numero primo. Ad es. i campi dei numeri razionali, dei numeri reali e dei numeri p -adici hanno caratteristica 0, mentre il campo finito \mathbb{Z}_p ha caratteristica p .

$$R(t) = \prod_i (t - \rho_i)^{q_i}$$

con $q_i \in \mathbb{Z}$ che rappresenta la molteplicità della radice ed è:

$$q_i = \begin{cases} > 0 \text{ se } t - \rho_i \text{ a numeratore} \\ < 0 \text{ se } t - \rho_i \text{ a denominatore} \end{cases}$$

Per cui è:

$$\begin{aligned} R'(t) &= \sum_i q_i \frac{R(t)}{(t - \rho_i)} \\ \frac{R'(t)}{R(t)} &= \sum_i \frac{q_i}{(t - \rho_i)} \end{aligned} \quad (2)$$

Il vantaggio della (2) è che la molteplicità delle radici è adesso 1.

Supponiamo che:

$$a(t) = \prod_i (t - \alpha_i)^{m_i} \quad b(t) = \prod_j (t - \beta_j)^{n_j} \quad c(t) = \prod_k (t - \gamma_k)^{r_k}$$

Usando la (1) e la (2) si ottiene:

$$\frac{b}{a} = -\frac{\frac{f'}{f}}{\frac{g'}{g}} = -\frac{\sum_i \frac{m_i}{(t - \alpha_i)} - \sum_k \frac{r_k}{(t - \gamma_k)}}{\sum_j \frac{n_j}{(t - \beta_j)} - \sum_k \frac{r_k}{(t - \gamma_k)}} \quad (3)$$

Un comune denominatore tra numeratore e denominatore della (3), con a, b, c relativamente primi, è:

$$D(t) = \prod_i (t - \alpha_i) \prod_j (t - \beta_j) \prod_k (t - \gamma_k)$$

Dove: $\deg(D(t)) = n_0(abc)$

Ora si osserva che se $b=0$ $\deg(\frac{f'}{f}) = -\infty$ se $a=0$ $\deg(\frac{g'}{g}) = -\infty$; mentre se né $a=0$ né $b=0$ allora

$\deg(\frac{f'}{f}) = \deg(\frac{g'}{g}) = -1$. Di conseguenza: $\deg(D \cdot \frac{f'}{f}) \leq n_0(abc) - 1$ e $\deg(D \cdot \frac{g'}{g}) \leq n_0(abc) - 1$

Dalla (1) si ottiene però: $\frac{b}{a} = \frac{-D \frac{f'}{f}}{D \frac{g'}{g}}$ che è equivalente a dire che $-a \cdot D \frac{f'}{f} = b \cdot D \frac{g'}{g}$

Poiché $\gcd(a,b)=1$ allora è:

$$a \mid D \frac{g'}{g} \Rightarrow \deg(a) \leq n_0(abc) - 1 \quad (4)$$

Analogamente si può dire che:

$$\deg(b) \leq n_0(abc) - 1 \quad (5)$$

Da qui è: $\deg(c) \leq \max \{ \deg(a), \deg(b) \}$ (6)

Da (4)(5)(6) si ottiene che: $\max \{ \deg(a), \deg(b), \deg(c) \} \leq n_0(a(t)b(t)c(t)) - 1$. \square

Corollario (Teorema di Fermat per i polinomi)

Siano $a(t), b(t), c(t)$ tre polinomi i cui coefficienti appartengono ad un campo algebricamente chiuso di caratteristica 0 e tali che almeno uno di grado > 0 ; allora

$$x(t)^n + y(t)^n = c(t)^n$$

Non ha soluzioni per $n \geq 3$.

Dim.

Dal Teorema di Mason si ha che:

$$\deg(x(t)^n) = n \cdot \deg(x(t)) \leq \deg(x(t)) + \deg(y(t)) + \deg(z(t)) - 1$$

Se nella parte sinistra a $x(t)$ aggiungiamo $y(t)$ e $z(t)$ otteniamo che:

$$n \cdot [\deg(x(t)) + \deg(y(t)) + \deg(z(t))] \leq 3[\deg(x(t)) + \deg(y(t)) + \deg(z(t))] - 3$$

Il che è in contrasto con $n \geq 3$. \square

Nel seguito esamineremo una serie di ulteriori conseguenze.

Congettura della forma debole del Teorema di Fermat (problema asintotico di Fermat)

Se è vero $\mu(\varepsilon)$ allora esiste un $N \in \mathbb{Z}$ tale che per $n > N$

$$x^n + y^n = z^n$$

Dove $\gcd(x, y, z) = 1$, ha solo soluzioni banali negli Interi.

Teorema

La congettura abc implica la congettura del problema asintotico di Fermat.

Dim.

Dalla congettura abc formulazione di Masser dovremmo scrivere che:

$$|x^n| \leq \mu\left(\frac{\varepsilon}{3}\right) r(xyz)^{1+\frac{\varepsilon}{3}}$$

$$|y^n| \leq \mu\left(\frac{\varepsilon}{3}\right) r(xyz)^{1+\frac{\varepsilon}{3}}$$

$$|z^n| \leq \mu\left(\frac{\varepsilon}{3}\right) r(xyz)^{1+\frac{\varepsilon}{3}}$$

Da cui:

$$|x^n| \cdot |y^n| \cdot |z^n| = |xyz|^n \ll (|xyz|^{1+\frac{\epsilon}{3}})^3 = |xyz|^{3+\epsilon}$$

Ora se $|xyz| > 1$ allora n è limitato; altrimenti $|xyz| \leq 1$ ed almeno uno degli interi è nullo. \square

Da notare il ruolo avuto da $\mu(\epsilon)$; in particolare la scelta di ϵ determina il valore di N .

Congetture classiche influenzate dalla congettura abc

In questa seconda parte esamineremo alcune congettura influenzate dalla congettura abc su cui non presenteremo dimostrazioni, che sono, invece, presenti in [2][4].

Condizione di Wieferich

Definizione

Un numero primo $p \in \mathbb{Z}$ soddisfa la condizione di Wieferich se e solo se $2^{p-1} \not\equiv 1 \pmod{p^2}$

Congettura infinità dei numeri primi di Wieferich

Esistono infiniti numeri primi che soddisfano la condizione di Wieferich.

Teorema

La congettura abc implica che è vera la congettura dell'infinità dei numeri primi di Wieferich.

Dim.

Vedi [2] e dimostrazione di Silverman.

Congettura originale di Hall

Siano u, v due numeri interi non nulli e relativamente primi tali che $u^3 - v^2 \neq 0$, allora è:

$$|u^3 - v^2| \gg |u|^{1/2-\epsilon}$$

Teorema

La congettura abc implica la congettura originale di Hall.

Dim.

Vedi [2], dimostrazione dovuta a Lang.

Richiamo teorico

Oesterlè sappiamo che si ispirò alla congettura di Szpiro. Ricordiamo che una equazione ellittica [3] di Weiestrass è della forma:

$$E: y^2 = x^3 - ux + v$$

dove $u, v \in \mathbb{Z}$.

Il discriminante di E è indicato con $\Delta = 16(4u^3 - 27v^2)$; mentre il discriminante del polinomio cubico è indicato con $D = 4u^3 - 27v^2$. Viene definita *conduttore di E*, per i primi $p \in \mathbb{Z}$, la quantità

$c(E) = \prod_p p^{f_p}$, dove

$$f_p = \begin{cases} 0 & \text{se la riduzione di } E \text{ è non singolare} \\ 1 & \text{se la riduzione di } E \text{ è moltiplicativa} \\ 2 + \delta_p & \text{se la riduzione di } E \text{ è additiva} \end{cases}$$

δp è una costante indipendente limitata della curva, con $\delta p = 0$ se $p \geq 5$.

In generale è $r(D) \leq c(E)$.

Congettura originale di Szpiro

Assumendo una equazione di Weierstrass con il discriminante D di un polinomio cubico e $c(E)$ il conduttore dell'equazione, allora è:

$$|D| \ll r(D)^{6+\varepsilon} \ll c(E)^{6+\varepsilon}$$

Teorema

La congettura abc implica la congettura originale di Szpiro.

Dim.

Vedi [2]. La dimostrazione sfrutta i risultati della prova della congettura di Hall; in particolare la congettura abc e la congettura di Szpiro sono equivalenti.

Definizione

Le coppie di interi che soddisfano il problema di Brocard $n! + 1 = m^2$ sono dette coppie di Brown.

Teorema

La congettura abc implica che esistono solo un numero finito di coppie di Brown.

Dim.

Vedi [4].

Definizione

Per $n \in \mathbb{P}$, n è detto numero potente se per ogni primo p che divide n , p^2 divide n .

Congettura Erdos-Mollin-Walsh

Non esistono tre numeri interi consecutivi potenti.

Teorema

La congettura abc implica che l'insieme di triple di interi consecutivi e potenti è finito.

Congettura di Mordell

Una curva di genus > 1 definita sopra un campo numerico K , ha solo molti e finiti punti razionali su K .

Teorema

La congettura abc per campi numerici implica la congettura di Mordell sopra un qualsiasi campo numerico.

Dim.

Vedi [5].

Teorema di Roth

Per $\epsilon > 0$, per ogni numero algebrico α l'ineguaglianza diofantea $|\alpha - \frac{p}{q}| < \frac{1}{q^{2+\epsilon}}$ ha soltanto un numero finito di soluzioni.

Teorema

La congettura abc implica che, per la condizione del Teorema di Roth $\left| \alpha - \frac{p}{q} \right| > \frac{1}{q^{2+\varepsilon}}$ per un numero finito di frazioni p/q in forma ridotta, dove $k = C(\alpha) \cdot (\log q)^{-1/2} \cdot (\log \log q)^{-1}$ per qualche costante $C(\alpha)$ dipende solo da α .

Dim.

Vedi [6].

Teorema

La congettura abc implica che per un polinomio $F(x)$ a coefficienti interi, senza radici ripetute e contenente 1, allora $F(n)$ è libero di quadrati per infiniti interi n .

Dim.

Vedi [7].

Le “Good triples”

Ritorniamo alla formulazione di Oesterlè della congettura abc. Il problema di Oesterlè era di vedere se le funzioni L sono limitate.

Teorema A

La congettura abc è valida se e solo se $\limsup \{L\} \leq 1$.

Dim. (Vedi [2])

Supponiamo vera la congettura, allora è:

$$L = L(a, b, c) = \frac{\log \max(|a|, |b|, |c|)}{\log r(abc)} \leq \frac{\log |\mu(\varepsilon) \cdot r(abc)^{1+\varepsilon}|}{\log r(abc)} = \frac{\log \mu(\varepsilon)}{\log r(abc)} + 1 + \varepsilon$$

Per $\varepsilon > 0$, fissiamo $k = \mu(\varepsilon)$.

Noi vogliamo che: $\frac{\log k}{\log r(abc)} \leq \varepsilon$, per un numero finito di triple (a, b, c) , il che è equivalente a:

$$\log r(abc) \geq \frac{\log k}{\varepsilon}$$

oppure a:

$$r(abc) \geq M := \exp\left(\frac{\log k}{\varepsilon}\right)$$

Questo risultato afferma che in base alla congettura abc esistono solo un numero finito di triple il cui radicale è limitato superiormente: $r(abc) \leq M$

Supponiamo adesso che $\limsup \{L\} \leq 1$. Ciò è vero se e solo se:

$$\limsup \left\{ \frac{\log c_n}{\log r(a_n b_n c_n)} \right\} \leq 1 \Rightarrow \frac{\log c_n}{\log r(a_n b_n c_n)} \leq 1 + \varepsilon \quad \text{per } n \text{ grandi}$$

Quindi per qualche $n > N$ risulta $c_n \leq r(a_n b_n c_n)^{1+\varepsilon}$

Scegliendo le costanti $\mu_i(\varepsilon)$ per ogni i tale che: $c_i \leq \mu_i(\varepsilon) \cdot r(abc)^{1+\varepsilon}$ allora $c_n \leq \mu_n(\varepsilon) \cdot r(abc)^{1+\varepsilon}$ per tutti gli n \square

In [2] si vede che se si considera l'esempio $a_n = 3^{2^n} - 1, b_n = 1, c_n = 3^{2^n}, n \in \mathbb{P}$ risulta $L_n > 1$ e come conseguenza si ottiene il seguente Teorema.

Teorema B

La congettura abc è valida se e solo se $\limsup \{L\} = 1$.

Definizione

Vengono definite “**good triples**” le triple (a,b,c) tali che $L > 1.4$.

Dal Teorema B si ottiene il seguente Corollario.

Corollario

Se la congettura abc è vera vi sono solo un numero finito di “good triples”.

Lista delle “good triples”

Fino al 2002 erano note solo 152, oggi sono circa 228 “good triples” (Vedi [2][8][9][10]).

Riferimenti

- [1] Lang, Serge - Old and New Conjectured Diophantine Equations. Bulletin of the American Mathematical Society Volume 23, Number 1, July 1990, 37-75.
- [2] Jeffrey Paul Whiler (august 2002) – A Thesis – The abc conjecture
- [3] Wikipedia http://en.wikipedia.org/wiki/Elliptic_curve
- [4] Overholt Marius - The Diophantine Equation $n! + 1 = m^2$ - Bull. Lond. Math. Soc. 25, No. 2, 104 (1993).
- [5] Elkies, Noam D. - abc Implies Mordell - Int. Math. Res. Not. 1991, No. 7, 99-109 (1991).
- [6] Bombieri, E. - Roth's Theorem and the abc Conjecture - Preprint (1994).
- [7] Granville, Andrew - ABC allows us to count squarefrees.- Int. Math. Res. Not. 1998, No. 19, 991-1009 (1998).
- [8] <http://www.math.leidenuniv.nl/~desmit/abc/?set=2> (Bart de Smith)
- [9] <http://www.math.unicaen.fr/~nitaj/abc.html>
- [10] http://en.wikipedia.org/wiki/Abc_conjecture

This document was created with Win2PDF available at <http://www.win2pdf.com>.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.