SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Lukrecija Roić

ABC SLUTNJA

Diplomski rad

Voditelj rada:
izv. prof. dr. sc. Filip Najman

Zagreb, Veljača, 2018.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Zahvaljujem svima koji su bili uz mene tijekom mog obrazovanja.

Sadržaj

Sadržaj **iv**

Uvod **1**

1 Nastanak ABC slutnje **2**

2 Iskaz ABC slutnje **3**
2.1 Radikal broja 3
2.2 ABC slutnja 6

3 Forme ABC slutnje **7**
3.1 Druge verzije ABC slutnje 7

4 Posljedice ABC slutnje **10**
4.1 Fermatov posljedni teorem 10
4.2 Catalanova slutnja 12
4.3 Fermat-Catalanova slutnja 13
4.4 Rothov teorem 15
4.5 Wieferichovi i Ne-Wieferichovi prosti brojevi 17
4.6 Pillai-ova slutnja 19
4.7 Hallova slutnja 21
4.8 Erdős-Woodsova slutnja 22
4.9 Waring-HIlbertov teorem 23
4.10 Još neke posljedice ABC slutnje 24

5 Generalizacije ABC slutnje **26**
5.1 ABC slutnja za polinome 26
5.2 ABC slutnja za binarne oblike 27
5.3 ABC slutnja za n cijelih brojeva 27
5.4 Bakerova ABC slutnja za cijele brojeve 28

5.5 Hu-Yangova verzija ABC slutnje za cijele brojeve 29

6 Pokušaj dokaza ABC slutnje **30**

Bibliografija **31**

Uvod

Teorija brojeva je grana matematike koja proučava svojstva brojeva te njihove međusobne odnose. Ponajprije proučava svojstva skupa prirodnih, cijelih i ponekad racionalnih brojeva. Potječe od pitogorejaca, a u Europi su je unaprijedili poznati matematičari poput P. Fermat, L. Euler i J.-L. Lagrange. Modernu teoriju brojeva zasnovao je C. F. Gauss. Na prvi pogled može se činiti da se radi o najjednostavnijoj grani matematike, no to nije tako. U teoriji brojeva su vrlo česti iznimno jednostavno formulirani problemi koje je teško dokazati i koji godinama, čak i stoljećima te ostaju nerazrješeni. Takve neriješene probleme nazivamo slutnje.

Neki vrlo poznati problemi su tek nedavno dokazani su: Posljedni Fermatov problem, Dorabellina šifra, Poincareova slutnja...
I danas postoje mnogobrojni problemi koji nisu riješeni, a za neke od njih nude se i također visoke novčane nagrade. Neki od tih problema su: ABC slutnja, Bealova slutnja, Kromatski broj ravnine, Collatzova slutnja, Problem diskretnog logaritma, Goldbachova slutnja, Grimmova slutnja, Legendreova slutnja..

U ovom radu tema će biti ABC slutnja. Cilj ovog rada je detaljno opisati ABC slutnju te sve njezine verzije. Također u ovom radu će biti objašnjeno zašto je ABC slutnja toliko bitna za matematiku te kolika je važnost njezinih posljedica te će biti opisan pokušaj njezinog dokazivanja. ABC slutnja je vrlo jasnog i jednostavnog iskaza, iako još nije dokazana. Kaže se da je ona najvažniji neriješeni problem u Diofantovoj analizi.

Poglavlje 1

Nastanak ABC slutnje

ABC slutnju su prvi put izrekli u 20. stoljeću matematičari Joseph Oesterlé i David Wiliam Masser u Bonnu 1985.g. Oesterlé je francuski matematičar rođen 1954.g. te se proslavio ABC slutnjom, član je udruge francuskih matematičara "Bourbaki". Masser je rođen 1948.g. Doktorirao je na sveučilištu Cambridge te sada radi kao profesor na sveučilištu u Baselu, Švicarska. Oesterlé i Masser su došli do ABC slutnje potaknuti proučavanjem određenih teza o polinomima i proučavanjem Szpirove slutnje.

Slutnja 1.0.1 (Szpirova slutnja)**.** *Za svaki $\varepsilon > 0$ postoji konstanta $C(\varepsilon)$ takva da za svaku eliptičku krivulju E koja je definirana nad $\mathbb{Q}$ sa minimalnom diskriminantom Δ i kondukto-rom f, imamo:*

$$|\Delta| \leq C(\varepsilon) \cdot f^{6+\varepsilon}.$$

Što je točno dovelo Massera i Oesterla do ABC slutnje?
Oesterlé je bio zainteresiran za novu Sziporovu slutnju koja uključuje varijanate eliptičkih krivulja nad $\mathbb{Q}$. Masser je čuo Oesterlévo predavanje o Szpirovoj slutnji i htio ju je formulirati bez upućivanja na eliptičke krivulje. On je bio djelomično inspiriran novim elementarnim teoremom o polinomima koji je analogan ABC slutnji. Još prije je otkriveno da ABC slutnja sadrži i Fermatov posljedni teorem, no to nije bila izvorna motivacija za slutnju. Prva pojava ABC slutnje je bila Masserov doprinos za listu problema na Rothovom 60. rođendanskom skupu.

Poglavlje 2

Iskaz ABC slutnje

2.1 Radikal broja

Radikal broja

Definicija 2.1.1 (Radikal broja)**.** *Za svaki pozitivan cijeli broj* $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_n^{\alpha_n}$*, radikal je* $\operatorname{rad} n = p_1 \cdot p_2 \cdot ... \cdot p_n$*.*

Primjer 2.1.2. *Neki radikali brojevi:*

- $\operatorname{rad}(1) = 1$,
- $\operatorname{rad}(45) = \operatorname{rad}(3^2 \cdot 5) = 3 \cdot 5 = 15$,
- $\operatorname{rad}(252) = \operatorname{rad}(2^2 \cdot 3^2 \cdot 7) = 2 \cdot 3 \cdot 7 = 45$,
- $\operatorname{rad}(100000) = \operatorname{rad}(10^5) = 10$,
- $\operatorname{rad}(4320) = \operatorname{rad}(2^5 \cdot 3^2 \cdot 5^2) = 2 \cdot 3 \cdot 5 = 30$,
- $\operatorname{rad}(a^m) = \operatorname{rad}(a)$ *(za kvadratno slobodan a).*

Napomena 2.1.3. *Nije poznat način kako izračunati radikal bez faktoriziranja n. Još posebnije, nije poznato je li radikal od prostoga broja n jednak* $\operatorname{rad}(n) = n$ *bez faktoriziranja.*

Najveća zajednička mjera

Definicija 2.1.4 (Najveća zajednička mjera)**.** *Najveća zajednička mjera (ili najveći zajednički djelitelj) brojeva* $n_1, n_2, ..., n_k$ *jest broj m koji ima svojstva:*
1. m *je djelitelj svakog od brojeva* $n_1, n_2, ..., n_k$

2. m je naveći broj s tim svojstvom.
Najveću zajedničku mjeru označavamo s $\mathrm{M}(n_1, n_2, ..., n_k)$.

Za brojeve kojima je najveća zajednička mjera jednaka 1, kažemo da su relativno prosti. Euklidov algoritam služi nam kako bismo našli najveću zajedničku mjeru više brojeva.

EUKLIDOV ALGORITAM:
Svojstvo najveće zajedničke mjere:
U postupku dijeljenja prirodnih brojeva (dijelimo broj a brojem b i dobivamo ostatak r) $a = q \cdot b + r$, vrijedi: $\mathrm{M}(a, b) = \mathrm{M}(b, r)$.

Primjer 2.1.5. *Određivanje najveće zajedničke mjere Euklidovim algoritmom.*

$\mathrm{M}(616, 585) =$ *?*
$616 : 585 = 1$ *i ostatak 31*
$\mathrm{M}(616, 585) = \mathrm{M}(585, 31)$
$585 : 31 = 18$ *i ostatak 27*
$\mathrm{M}(585, 31) = \mathrm{M}(31, 27)$
31:27 = 1 i ostatak 4
$\mathrm{M}(31, 27) = \mathrm{M}(27, 4)$
27:4 = 6 i ostatak 3
$\mathrm{M}(27, 4) = \mathrm{M}(4, 3)$
4:3 = 1 i ostatak 1
$\mathrm{M}(4, 3) = \mathrm{M}(3, 1)$
3:1 = 3 i ostatak 0.
$\mathrm{M}(3, 1) = 1.$
$\mathrm{M}(616, 585) = \mathrm{M}(585, 31) = \mathrm{M}(31, 27) = \mathrm{M}(27, 4) = \mathrm{M}(4, 3) = \mathrm{M}(3, 1) = 1.$

Radikali od a, b i $a + b$

Teorem 2.1.6 (Teorem o radikalima)**.** *Među svim a,b gdje je* $\mathrm{M}(a, b) = n$, $\mathrm{rad}(ab(a + b)) = \prod_{p|ab(a+b)} p$ *poprima neku određenu vrijednost samo konačno mnogo puta. [3]*

Primjer 2.1.7. *Svi primjeri za* $\mathrm{rad}(ab(a + b)) = 30$ *gdje je* $\mathrm{M}(a, b) = 1$.

- $2 + 3 = 5$,
- $1 + 5 = 6$,
- $3 + 5 = 8$,
- $4 + 5 = 9$,

- $1 + 9 = 10$,
- $1 + 15 = 16$,
- $1 + 24 = 25$,
- $9 + 16 = 25$,
- $2 + 25 = 27$,
- $1 + 80 = 81$,
- $3 + 125 = 128$.

Analogan problem možemo promatrati za polinome.
Započnimo s konačnim skupom u $\mathbb{C}$, pronađimo $f(t)$ i $g(t)$ bez zajedničkih korijena u $\mathbb{C}$ td. korijeni od $f(t)$, $g(t)$ i $f(t) + g(t)$ su skup.

ABC trojke

Definicija 2.1.8 (ABC trojka)**.** *Trojka tri cijela pozitivna broja (a,b,c) takva da vrijedi* $a + b = c$ *i* $\mathrm{M}(a, b, c) = 1$ *(ekvivalentno* $\mathrm{M}(a, b) = 1$*) zove se ABC trojka.*

Primjer 2.1.9. *Primjeri (a,b,c) trojki su:* $(1, 8, 9)$, $(8, 25, 33)$, $(19, 12, 31)$, $(1, 2^n - 1, 2^n)$.

ABC trojke s posebnim svojstvom

Postoje ABC trojke koje imaju i svojstvo da je

$$c > \mathrm{rad}(abc).$$

Takve ABC trojke su vrlo rijetke.

Od svih 3044 ABC trojki (a, b, c) takvih da je $1 \leq a \leq b \leq 100$, samo 7 ABC trojki imaju svojstvo da je $c > \mathrm{rad}(abc)$:
(1,1,1), (1,8,9), (1,48,49), (1,63,64), (1,80,81), (5,27,32), (32,49,81).

- $(5, 27, 32) \rightarrow \mathrm{rad}(5 \cdot 27 \cdot 32) = \mathrm{rad}(5 \cdot 3^3 \cdot 2^5) = 5 \cdot 3 \cdot 2 = 30 < 32 = c$,
- $(1, 63, 64) \rightarrow \mathrm{rad}(1 \cdot 63 \cdot 64) = \mathrm{rad}(1 \cdot 3^2 \cdot 7 \cdot 2^6) = 1 \cdot 3 \cdot 7 \cdot 2 = 42 < 64 = c$.

No, postoji beskonačno mnogo takvih trojki ako broj c teži u beskonačnost.
[8]

Propozicija 2.1.10. *ABC trojki sa svojstvom da je* $c > \text{rad}(abc)$ *ima beskonačno mnogo.*

Dokaz. Uzmimo $k \geq 1$, $a = 1$, $c = 3^{2^k}$ i $b = c - 1$

Lema 2.1.11. 2^{k+2} *dijeli* $3^{2^k} - 1$.

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

$$rad((3^{2^k} - 1) \cdot 3^{2^k}) \leq \frac{3^{2^k} - 1}{2^{k+1}} \cdot 3 < 3^{2^k}.$$

Stoga je $(1, 3^{2^k} - 1, 3^{2^k})$ ABC trojka koja ima svojstvo $c > \text{rad}(abc)$.

Budući da to vrijedi za svaki $k \geq 1$, dokazali smo takvih trojki ima beskonačno mnogo. □

2.2 ABC slutnja

Sada možemo izreći ABC slutnju.

Slutnja 2.2.1 (ABC slutnja)**.** *Za svaki* $\varepsilon > 0$*, postoji samo konačno mnogo ABC trojki* (a, b, c) *za koje vrijedi*

$$c > \text{rad}(abc)^{1+\varepsilon}.$$

Netočno je da $c < \text{rad}(abc)^{1+0}$ za sve osim konačno mnogo abc trojki, kao što smo i vidjeli. Ako se tvrdnja pokaže za neki ε_0, onda je automatski točno i za $\varepsilon > \varepsilon_0$. "The ABC@home projekt" je pretraživao abc trojke. Pronašli su 3 koje zadovoljavaju $c < \text{rad}(abc)^{1.6}$, 13 koje zadovoljavaju $c < \text{rad}(abc)^{1.5}$ te 234 njih koje zadovoljavaju $c < \text{rad}(abc)^{1.4}$. To uključuje sve primjere od $c > \text{rad}(abc)$ gdje c ima do 20 znamenki. [5]

Poglavlje 3

Forme ABC slutnje

Slutnja koja smo izrekli već u prethodnom poglavlju je bila prva verzija ABC slutnje. [3]

Slutnja 3.0.1 (ABC slutnja I.)**.** *Za svaki $\varepsilon > 0$, postoji samo konačno mnogo ABC trojki za koje vrijedi:*

$$c > \mathrm{rad}(abc)^{1+\varepsilon}.$$

Ovu verziju nazivamo slabom formom ABC slutnje.
Verzija koja je ekvivalentna prethodnoj verziji je:

Slutnja 3.0.2 (ABC slutnja II.)**.** *Za svaki $\varepsilon > 0$, postoji konstanta $k_\varepsilon > 0$, takva da za sve ABC trojke vrijedi:*

$$c < k_\varepsilon \,\mathrm{rad}(abc)^{1+\varepsilon}.$$

3.1 Druge verzije ABC slutnje

U definiciji za ABC trojke, vrijedi da je $a + b = c$ i $\mathrm{M}(a, b, c) = 1$. No, zamijenimo sada "$a, b > 0$" s "$a, b, c \neq 0$" te za $n < 0$ postavimo $\mathrm{rad}(n) = \mathrm{rad}(|n|)$. Sada ABC slutnja izgleda ovako:

Slutnja 3.1.1. *Za svaki $\varepsilon > 0$, postoji samo konačno mnogo ABC trojki (a, b, c) za koje vrijedi:*

$$\max(|a|, |b|, |c|) > \mathrm{rad}(abc)^{1+\varepsilon}.$$

Verzija koja je ekvivalentna prethodnoj verziji je:

Slutnja 3.1.2. *Za svaki $\varepsilon > 0$, postoji konstanta $k_\varepsilon > 0$, takva da za sve ABC trojke (a,b,c) vrijedi:*

$$\max(|a|, |b|, |c|) < k_\varepsilon \,\mathrm{rad}(abc)^{1+\varepsilon}.$$

Sada možemo izreći logaritamsku formu ABC slutnje:

Slutnja 3.1.3. *Za svaki $\varepsilon > 0$, ali za samo konačno mnogo ABC trojki vrijedi:*

$$\frac{\log \max(|a|, |b|, |c|)}{\log \operatorname{rad}(abc)} \geq 1 + \varepsilon.$$

Verzija slutnje gdje je rad(abc) ograničen odozdo:

Slutnja 3.1.4. *Za svaki $\varepsilon > 0$, ali za samo konačno mnogo ABC trojki (a, b, c) vrijedi:*

$$\operatorname{rad}(abc) > \max(|a|, |b|, |c|)^{1-\varepsilon}.$$

Kvaliteta ABC trojki

Kvaliteta ABC trojki (a, b, c) q definira se kao

$$q(a, b, c) = \frac{\log c}{\log(\operatorname{rad}(abc))}.$$

Najveća poznata jednakost među ABC trojkama dolazi iz:

$$2 + 3^{100} \cdot 109 = 23^5 \Rightarrow \frac{\log c}{\log(\operatorname{rad}(abc))} \approx 1.6299.$$

[3]

Što je manji radikal u usporedbi s c, veća je kvaliteta trojke.
Sada možemo izreći treću verziju ABC slutnje:

Slutnja 3.1.5 (ABC slutnja III.)**.** *Za svaki $\varepsilon > 0$, postoji samo konačno mnogo ABC trojki za koje vrijedi:*

$$q(a, b, c) > 1 + \varepsilon.$$

Tablica 3.1: 20 trojki najveće kvalitete

	a	b	c	q	Autor:
1.	2	$3^{10} \cdot 109$	23^5	1.62991	E.R.
2.	11^2	$3^2 \cdot 5^6 \cdot 7^3$	$2^{21} \cdot 23$	1.62599	B.W.
3.	$19 \cdot 1307$	$7 \cdot 29^2 \cdot 31^8$	$2^8 \cdot 3^{22} \cdot 5^4$	1.62349	J.B-J.B
4.	283	$5^{11} \cdot 13^2$	$2^8 \cdot 3^8 \cdot 17^3$	1.58076	J.B-J.B, A.N
5.	1	$2 \cdot 3^7$	$5^4 \cdot 7$	1.56789	B.W.
6.	7^3	3^{10}	$2^{11} \cdot 29$	1. 54708	B.W.
7.	$7^2 \cdot 41^2 \cdot 311^3$	$11^{16} \cdot 13^2 \cdot 79$	$2 \cdot 3^3 \cdot 5^{23} \cdot 953$	1.54443	A.N.
8.	5^3	$2^9 \cdot 3^{17} \cdot 13^2$	$11^5 \cdot 17 \cdot 31^3 \cdot 137$	1.53671	P.M-H.R
9.	$13 \cdot 19^6$	$2^{30} \cdot 5$	$3^{13} \cdot 11^2 \cdot 31$	1.52700	A.N.
10.	$3^{18} \cdot 23 \cdot 2269$	$17^3 \cdot 29 \cdot 31^8$	$2^{10} \cdot 5^2 \cdot 7^{15}$	1.52216	A.N.
11.	$13^{10} \cdot 37^2$	$3^7 \cdot 19^5 \cdot 71^4 \cdot 223$	$2^{26} \cdot 5^{12} \cdot 1873$	1.5094	T.D,
12.	$2^7 \cdot 23^8$	$19^9 \cdot 857^2$	$3^{22} \cdot 13 \cdot 47^2 \cdot 263$	1.5033	T.S. -M.H.
13.	239	$5^8 \cdot 17^3$	$2^{10} \cdot 37^4$	1.5028	J.B. - J.B. -A.N.
14.	$5^2 \cdot 7937$	17^{13}	$2^{18} \cdot 3^7 \cdot 13^2$	1.4976	B.-W.
15.	$2^2 \cdot 11$	$3^2 \cdot 13^{10} \cdot 17 \cdot 151 \cdot 4423$	$5^9 \cdot 139^6$	1.4924	A.N.
16.	73	$2^{13} \cdot 7^7 \cdot 941^2$	$3^{16} \cdot 103^3 \cdot 127$	1.4916	A.N.
17.	2^{24}	$11^7 \cdot 19 \cdot 29^2$	$3^{11} \cdot 5^3 \cdot 7^3 \cdot 41$	1.4892	A.N.
18.	11^2	$3^9 \cdot 13$	$2^{11} \cdot 5^3$	1.4889	B.-W.
19.	37	2^{15}	$3^8 \cdot 5$	1.4829	B.-W.
20.	$5^{14} \cdot 19$	$2^5 \cdot 3, \cdot 7^{13}$	$11^7 \cdot 37^2 \cdot 353$	1.4813	A.N.

Poglavlje 4

Posljedice ABC slutnje

ABC slutnja je važna zbog mnogobrojnih generalizacija i značajnih posljedica koje bi njeno dokazivanje uzrokovalo. Kad bi se ABC slutnja dokazala, dokazali bi se i mnogi dosad neriješeni problemi u matematici.

ABC slutnja ima veliki broj posljedica. To uključuje i poznate rezultate i slutnjama za koje daje uvjetni dokaz. Sama slutnja ostaje od interesa za ostale slutnje koje će dokazati, zajedno s brojnim poveznicama s dubokim pitanjima u teoriji brojeva. [6] [10]

4.1 Fermatov posljednji teorem

Teorem 4.1.1 (Fermatov posljedni teorem)**.** *Ne postoje prirodni brojevi $a, b,$ i c takvi da je $a^n + b^n = c^n$ gdje je n prirodan broj veći od 2.*

Matematičar iz 17. stoljeća Pierre de Fermat pisao je o ovom teoremu 1637. godine u svojoj kopiji poznate Diofantove Aritmetike: ”Otkrio sam zaista nevjerovatan dokaz ovog teorema koji ne može stati na marginu ove strane”. (Latinski: ”Cuius rei demonstrationem mirabilem sane detexi hanc marginis exiguitas non caperet.”)

Bez obzira na to, nijedan korektan dokaz nije pronađen sljedećih 357 godina. Teorem je konačno dokazao Andrew Wiles 1995. godine. Andrew Wiles je na stotinjak stranica koristeći iznimno napredne matematičke tehnike (iz područja teorije brojeva i algebarske geometrije), koje ni mnogi profesionalni matematičari ne bi mogli u cjelini pratiti, dokazao posljednji ili veliki Fermatov teorem kojeg je Pierre de Fermat iskazao. Zapravo, Wiles je dokazao tzv. teorem o modularnosti (engl. modularity theorem), a već je prije Wilesa bilo poznato da ako taj teorem vrijedi, onda vrijedi i Fermatov veliki teorem. Wiles je dokaz predao 1994. Najavio ga je zapravo 1993., no tada je otkrio određene ”rupe” u dokazu, koje je ”pokrpao” sa svojim bivšim studentom Richardom Taylorom te se konačni dokaz treba djelomice priznati i Tayloru. [3]

Ova tvrdnja je značajna jer su svi drugi Fermatovi teoremi bili utemeljeni, bilo pomoću dokaza koje je on dao, ili pomoću dokaza koji su pronađeni kasnije. Teorem nije posljednji kojeg je Fermat dao, nego posljednji kojeg je trebalo dokazati.

Teorem se općenito smatrao matematičkom slutnjom koja je isprovocirala najveći broj netočnih matematičkih dokaza.

Fermatov posljednji teorem za polinome

Pretpostavimo da $f(t)^n + g(t)^n = h(t)^n$ gdje f, g, h nisu nula i nisu svi konstante. Želimo pokazati da je $n < 3$. Bez smanjenja općenitosti f, g, h su relativno prosti.

Prema Mason-Stothersovom teoremu:

$$\deg f^n, \deg g^n, \deg h^n \leq \deg(\mathrm{rad}(f^n g^n h^n)) - 1 = \deg(\mathrm{rad}(fgh)) - 1.$$

Prema tome:

$$n \deg f, n \deg g, n \deg h \leq \deg(fgh) - 1.$$

Zbrojimo:

$$n(\deg(fgh)) \leq 3(\deg(fgh) - 1) < 3 \deg(fgh).$$

Prema tome, $n < 3$ i to je kraj.

Fermatov posljednji teorem i ABC slutnja

Wiles je 1994. pokazao da ABC slutnja povlači Fermatov posljedni teorem. Pretpostavimo da $a^n + b^n = c^n$ kada je $n \geq 3$ i $a, b, c \epsilon \mathbb{Z}^+$ i $\mathrm{M}(a, b) = 1$. Pretpostavimo da je ABC slutnja dokazana za neki ε:

$$\max(|a|, |b|, |c|) \leq k_\varepsilon \, \mathrm{rad}(abc)^{1+\varepsilon}$$

za svaku abc trojku (a, b, c).

Koristeći ABC slutnju (a^n, b^n, c^n):

$$\begin{aligned} c^n &< k_\varepsilon \, \mathrm{rad}(a^n b^n c^n)^{1+\varepsilon} \\ c^n &= k_\varepsilon rad(abc)^{1+\varepsilon} \\ c^n &\leq k_\varepsilon (abc)^{1+\varepsilon} \\ c^n &\leq k_\varepsilon c^{3(1+\varepsilon)} \quad / : c^{3(1+\varepsilon)} \\ c^{n-3(1+\varepsilon)} &\leq k_\varepsilon \quad / \tfrac{1}{n-3(1+\varepsilon)}. \end{aligned}$$

Za $n > 3(1+\varepsilon)$

$$c < k_\varepsilon^{\frac{1}{n-3(1+\varepsilon)}} < 2, \text{ za dovoljno veliki n,}$$

pa je n ograničen odozgo. Ako ABC slutnja vrijedi za neke $\varepsilon < \frac{1}{3}$ onda za sve $n \geq 4 > 3(1+\varepsilon)$ imamo $c < k_\varepsilon^{\frac{1}{n-3(1+\varepsilon)}}$.
Fermatov posljednji teorem onda slijedi nakon provjere za preostale eksponente.

Ako je $k_1 = 1$ onda ABC slutnja povlači Fermatov posljednji teorem za $n > 6$. [3]

4.2 Catalanova slutnja

Slutnja 4.2.1 (Catalanova slutnja 1843.g.)**.** *Jedina rješenja jednadžbe* $x^p - y^q = 1$*, za prirodne brojeve* x, y, p, q *su* $3^2 - 2^3 = 1$.

Povijest problema seže barem od Gersonida, koji je 1343. godine pokazao poseban slučaj slutnje gdje je (x, y) ograničen na $(2, 3)$ ili $(3, 2)$. Prvi značajan napredak nakon što je Catalan izrekao svoju slutnju dogodio se 1850. kada se Victor-Amédée Lebesgue bavio slučajem y = 2.

Godine 1976. Robert Tijdeman primijenio je Bakerovu metodu iz teorije transcendencije kako bi uspostavio vrezultate koji ograničavaju x, y u smislu p, q da bi se dobila učinkovita gornja granica za x, y, p, q. Ovo je razriješilo Catalanovu slutnju za sve osim konačnog broja slučajeva. Ipak, konačni izračun potreban za dovršenje dokaza teorema bio je predugačak. [9]
Catalanovu slutnju je dokazao Preda Mihăilescu u travnju 2002., pa se sada ponekad zove Mihăilescuov teorem.

Mihailescu je dokazao da jednadžba $x^p - y^q = 1$ nema rješenja u skupu cijelih brojeva različitim od nule i za relativno proste brojeve p i q. Ovo zajedno s rezultatima Lesbegua (1850) i KO Chaoa (1865) dokazuje slutnju.

Catalanova slutnja za polinome

Dokažimo Catalanovu slutnju za polinome.
Pretpostavimo:
$f(t)^p - g(q)^q = 1$ gdje su $p, q \geq 2$. Tada su f, g relativno prosti. Ako f ili g nisu konstante, prema Mason-Stothersovom teoremu s trojkom $(f(t)^p, -g(t)^q, 1)$:

$$\deg f^p, \deg g^q \leq \deg(\text{rad}(f^p g^q)) - 1 = \deg(\text{rad}(fg)) - 1$$

pa je

$$p \deg f, q \deg g < \deg f + \deg g.$$

Stoga imamo:

$$\deg f < \frac{\deg g}{p-1}, \deg g < \frac{\deg g}{(p-1)(q-1)}.$$

Ovo povlači da su f i g nultog stupnja, odnosno da su f i g su konstante.

ABC slutnja povlači Catalanovu slutnju

ABC slutnja povlači Catalanovu slutnju do na konačno izuzetaka. Pretpostavimo $x^p - y^q = 1$ u $\mathbb{N}$ gdje su $p, q \geq 2$. Tada $p \neq q$ i $M(x, y) = 1$. ABC slutnja za ABC trojku $(y^q, 1, x^p)$ povlači:

$$\begin{aligned} x^p < k_\varepsilon \operatorname{rad}(x^p y^q)^{1+\varepsilon} &= k_\varepsilon \operatorname{rad}(xy)^{1+\varepsilon} \\ &\leq k_\varepsilon (xy)^{1+\varepsilon}. \end{aligned}$$

Budući da je $y^q < x^p$, onda je $y < x^{\frac{p}{q}}$, pa dobivamo:

$$x^p < k_\varepsilon (x^{1+p/q})^{(1+\varepsilon)} = k_\varepsilon x^{p(1/p+1/q)(1+\varepsilon)}.$$

Imamo : $\dfrac{1}{p} + \dfrac{1}{q} \leq \dfrac{1}{2} + \dfrac{1}{3} = \dfrac{5}{6}$ pa je

$$x^p < k_\varepsilon x^{\frac{5}{6}(1+\varepsilon)} \Rightarrow x^{\frac{p(1-5\varepsilon)}{6}} < k_\varepsilon.$$

Ako je $0 < \varepsilon < \dfrac{1}{5}$ onda možemo ograničiti x i y s p, q i ε:

$$x < k_\varepsilon^{\frac{6}{p(1-5\varepsilon)}} \text{ i } y < x^{\frac{p}{q}} < k_\varepsilon^{\frac{6}{q(1-5\varepsilon)}}.$$

Za $p, q \geq 0$, dobivamo $x, y < 2$ pa su p i q ograničene.

4.3 Fermat-Catalanova slutnja

Fermat-Catalanova slutnja je dobila ime zato što kombinira ideje od Fermatovog posljednjeg teorema i Catalanove slutnje. Slutnju je izrekao Brun 1914. godine.[2]

Slutnja 4.3.1. *Jednakost $x^p + y^q = z^r$ ima konačan skup rješenja (x,y,z,p,q,r) u pozitivnim cijelim brojevima takvima da je* $\mathrm{M}(x, y, z) = 1$ *i* $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$.

Poznato je 10 rješenja, to su:
$1 + 2^3 = 3^2$ (Catalan)
$2^5 + 7^2 = 3^4$

$7^3 + 13^2 = 2^9$
$2^7 + 17^3 = 71^2$
$3^5 + 11^4 = 122^2$
$17^7 + 76271^3 = 21063928^2$
$1414^3 + 2213459^2 = 65^7$
$9262^3 + 15312283^2 = 113^7$
$43^8 + 96222^3 = 30042907^2$
$33^8 + 1549034^2 = 15613^3$
Posljednja 5 rješenja pronašli su F. Beukers i D. Zagier.

Ako se pronađe potpuni niz rješenja za Fermat-Catalanovu slutnju i dokaz se pokaže potpunim, Catalanova slutnja bi bila poseban slučaj. Fermat-Catalanova slutnja bi značila da postoji samo konačno mnogo rješenja.
Fermat-Catalanova slutnja, zajedno s eksplicitnim popisom rješenja, također bi dokazala Fermatov posljednji teorem.

Bealova slutnja

Slutnja 4.3.2 (Bealova slutnja)**.** *Jednadžba $x^p + y^q = z^r$ nema rješenja za relativno proste x, y, z i $p, q, r \geq 3$.*

Fermat-Catalanova slutnja bi značila da postoji samo konačno mnogo rješenja. Ako nijedna od rješenja za Fermat-Catalan problem ne daje kontraprimjer Bealovoj slutnji, to bi dokazalo Bealovu slutnju.
Bealova nagrada, uz potporu AMS-a, bit će dana za dokaz da vrijedi ili ne vrijedi činjenica da ne postoji rješenje za Fermat-Catalanovu jednadžbu s relativno prostim cijelim brojevima (x, y, z) i $p, q, r \geq 3$. Sve je počelo davne 1997., kada je Beal ponudio 5.000 dolara za dokaz slutnje. Zatim je 2000. godine nagradu podigao na 100.000 dolara sve do sada kada je ona dostigla milijun dolara.

ABC slutnja povlači Fermat-Catalanovu slutnju - Tijademan(1988)

Možemo reći da za proste brojeve (p, q, r) zapravo uvijek imamo:

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq \frac{41}{42}.$$

Primijenimo ABC slutnju za $\varepsilon = \frac{1}{84}$ i $(a, b, c) = (x^p, y^q, z^r)$ te to povlači

$$z^{r(1-2\varepsilon)} > xyz \geq rad(x^p y^q z^r) > K(\varepsilon) z^{r(1-\varepsilon)}.$$

Slučaj kada je (p, q, r) **fiksan - Darmon i Granville (1995)**

Za svaku trojku za koju vrijedi $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$ postoji samo konačno mnogo relativno prostih (x, y, z) za Fermat-Catalanovu slutnju. [7]

Slučaj kada je $(p, q, 2)$ **i** $(p, q, 3)$ **- Darmon i Granville (1997)**

Fermat-Catalanova jednadžba nema rješenja za relativno proste pozitivne cijele brojeve za $p = q \geq 3$ i $r = 3$. [7]

4.4 Rothov teorem

Roth je dokazao da za iracionalan $\alpha \epsilon \mathbb{R}$, beskonačno mnogo racionalnih brojeva $\frac{a}{b}$ gdje su a i b relativno prosti zadovoljava :

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^2}.$$

Primjer: $\left|\pi - \frac{22}{7}\right| \approx .0012 \approx \frac{1}{800} < \frac{1}{49}$.

Teorem 4.4.1 (Rothov teorem)**.** *Ako je α algebarski iracionalan realan broj onda za svaki $\varepsilon > 0$ nejednakost*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{|b|^{2+\varepsilon}}$$

ima samo konačno mnogo racionalnih rješenja.
Ekvivalnentno, za sve racionalne brojeve $\frac{a}{b}$

$$\left|\alpha - \frac{a}{b}\right| > \frac{C_{\alpha,\varepsilon}}{|b|^{2+\varepsilon}}.$$

U matematici, Rothov teorem je temeljni rezultat diofantnske aproksimacije algebarskih brojeva. Teorem pokazuje da određeni algebarski broj α ne mora imati previše racionalnih aproksimacija broja, koji su "vrlo dobri". Više od pola stoljeća značenje "vrlo dobrog" objasnilo je niz matematičara, počevši od Josipa Liouvillea 1844. godine i nastavljajući radom Axel Thuea (1909.), Carl Ludwig Siegela (1921.), Freeman Dysona (1947.) i Klaus Rotha (1955.).

Klaus Roth je njemački matematičar koji je za ovaj rezultat 1958. dobio Fieldsovu medalju. [2]
Osnovni nedostatak metode Thuea, Siegela i Rotha je u tome što ne daje granicu na veličinu nazivnika q racionalnih rješenja od navedene jednadžba ili, ekvivalentno tome, ne daje eksplicitnu konstantu. Ova je metoda stoga neefektivna, ne omogućava nam pronalaženje svih rješenja od navedene jednadžbe.

Rothov teorem i ABC slutnja

Prisjetimo se verzije ABC slutnje za "donje granicu" od rad(abc): Za svaki $\varepsilon > 0$, ali za samo konačno mnogo ABC trojki vrijedi

$$\text{rad}(abc) > \max(|a|, |b|, |c|)^{1-\varepsilon}$$

Dakle, svi relativno prosti cijeli brojevi a i b, koji nisu takvi da je $a + b = 0$ zadovoljavaju

$$\text{rad}(ab(a+b)) > c_\varepsilon max(|a|, |b|)^{1-\varepsilon}.$$

Za homogene $f(x, y) \epsilon\, \mathbb{Z}[x, y]$ s neponovljenim linearnim faktorima,

$$\text{rad}(f(a, b)) > C_{r\varepsilon} \max(|a|, |b|)^{\deg f - 2 - \varepsilon}.$$

ABC slutnja je specijalan slučaj za $f(x, y) = xy(x + y)$ s stupnjem polinoma f jednak 3. Idemo probati $f(x, y) = x^d - 2y^d$ s $d \geq 2$.
Za racionalne brojeve $\frac{a}{b}$(u skraćenoj formi);

$$f(a, b) \neq 0 \text{ p}a\ |a^d - 2b^d| > C_{d\varepsilon} \max(|a|, |b|)^{d-2-\varepsilon} \geq |b|^d \frac{C_{d\varepsilon}}{\max(|a|, |b|)^{2+\varepsilon}}.$$

Podijelimo izraz s $|b|^d$, pa dobivamo:

$$|(\frac{a}{b})^d - 2| > \frac{C_d}{\max(|a|, |b|)^{2+\varepsilon}}.$$

Ako je $\frac{a}{b}$ jako blizu $\sqrt[d]{2}$, onda vrijedi $t^d - 2 = 0 \Rightarrow a \approx \sqrt[d]{2}$.
Onda vrijedi:

$$|\frac{a}{b} - \sqrt[d]{2}|d(\sqrt[d]{2})^{d-1} > \frac{C_{d\varepsilon}}{(\sqrt[d]{2}|b|)^{2+\varepsilon}}.$$

To je Roth za $\sqrt[d]{2}$!
ABC slutnja povlači cijeli Rothov teorem. Ako se dokaže ABC slutnja, onda će se dokazati i Rothov teorem.

Dobra aproksimacija racionalnih brojeva

Primjer 4.4.2. *Neka je* $\alpha = \sqrt[5]{2} \approx 1.1486$. *Usporedimo*

$$|\sqrt[5]{2} - \tfrac{1148}{1000}| \gg \tfrac{1}{1000^2},$$
$$|\sqrt[5]{2} - \tfrac{309}{269^2}| \gg \tfrac{1}{269^2}.$$

Razlomci (potpuno skraćeni) zadovoljavaju $|\alpha - \frac{a}{b}| < \frac{1}{b^2}$, *po redoslijedu gdje je nazivnik sve veći* $b > 1$ *(nađeno pomoću "verižnih razlomaka"):*

$$\frac{7}{6}, \frac{8}{7}, \frac{15}{13}, \frac{23}{20}, \frac{31}{27}, \frac{54}{47}, \frac{85}{74}, \frac{139}{121}, \frac{224}{195}, \frac{309}{269}, \cdots$$

Neka je $\frac{a_i}{b_i}$ *(potpuno skraćen) razlomak takav da vrijedi* $|\sqrt[5]{2} - \frac{a}{b}| < \frac{1}{b_i^2}$ *gdje je* $b_1 < b_2 < b_3 < \cdots$.
Namjestimo $|\sqrt[5]{2} - \frac{a}{b}| = \frac{1}{(b_i)^{2+\varepsilon i}}$ *gdje je* $\varepsilon_i > 0$.

Pa ε_i *nije konstanta,ali ide prema nuli. Tako, za svaki* $\varepsilon > 0$, *samo konačno mnogo puta vrijedi* $|\sqrt[5]{2} - \frac{a}{b}| < \frac{1}{b^{2+\varepsilon}} < \frac{1}{b^2}$.

To je poseban primjer Rothovog teorema. [9]

Dobra aproksimacija racionalnih brojeva i ABC slutnja

Elkies i Langevin pokazali su da slaba verzija ABC slutnje implicira da za svaki $\varepsilon > 0$ da je $\mathrm{rad}(a^5 - 2b^5) > \max(|a|, |b|^{3-\varepsilon})$ za sve ali konačno mnogo relativno prostih a i b. To ustvari implicira Rothov teorem za $\alpha = \sqrt[5]{2}$, $|\sqrt[5]{2} - \frac{a}{b}| < \frac{1}{b^{2+\varepsilon}}$ konačno mnogo za svaki ε.

Algebarsko polje brojeva i ABC slutnja - Bombieri (1994)

1994. godine Enrico Bombieri pokazao da ABC slutnju povlači Theu-Siegel-Rothov teorem o Diophantskom aproksimacijom algebraskim brojevima.
ABC slutnja implicira da u nejednakosti $|\alpha - \frac{p}{q}| < \frac{1}{q^{2+\varepsilon}}$ u Theu-Siegel-Rothovom teoremu možemo zamijeniti eksponent ε s $k(\log q)^{-1/2}(\log\log q)^{-1}$ gdje k ovisi jedino α.

4.5 Wieferichovi i Ne-Wieferichovi prosti brojevi

Wieferich prost broj je prosti broj p, takav da p^2, dijeli $2^{p-1} - 1$, stoga povezuje ove proste brojeve s Fermatovim malim teoremom. Svaki neparni prosti broj p, dijeli $2^{p-1} - 1$. Wieferichove proste brojeve prvi put su opisali Arthur Wieferich 1909. godine u djelima koja se odnose na Fermatov posljednji teorem, a tada su oba Fermatova teorema bila već dobro poznata matematičarima. Prvi Wieferichovi prosti brojevi su 1093, 3511, .

Ne-Wieferichov prost broj je broj koji zadovoljava $2^{p-1} \not\equiv 1(\mod p^2)$.

Ne-Wieferichovi prosti brojevi i ABC slutnja

Silverman je 1988. pokazao da, ako se vrijedi ABC slutnja, tada postoje beskonačno mnogo ne-Wieferichovih prostih brojeva. Točnije, on je dokazao da ABC slutnja povlači postojanje konstante koja je ovisna samo o α tako da broj ne-Wieferichovih prostih brojeva je veći od $\log X$ za bazu α za sve $\alpha \geqslant 2$. Za svaki $\alpha \geqslant 2$ i za svaki fiksiran $k \geqslant 2$ te za proste brojeve p koji su manji od ili jednaki od varijable X vrijedi da je $\alpha^{p-1} \not\equiv 1(\mod p^2)$ i $p \equiv 1 \pmod{k}$. Numerički dokazi pokazuju da je veoma malo prostih brojeva u određenom intervalu koji su Wieferichovi prosti brojevi. Skup Wieferichovih prostih brojeva i skup ne-Wieferichovih prostih brojeva, ponekad označen W2 i W2c, su komplementarni skupovi, pa ako je jedan od njih pokazan konačnim, drugi bi nužno morao biti beskonačan, jer oba su pravi podskupovi skupa prostih brojeva. Kasnije je pokazano da postojanje beskonačno mnogih ne-Wieferichovih prostih brojeva slijedi iz slabije forme ABC slutnje. [8]

Teorem 4.5.1. *Ako su α i k cijeli brojevi jedan veći od drugoga i to povlači abc slutnju, tada postoji beskonačno mnogo prostih brojeva p takvi da $a^{p-1} \not\equiv 1(\mod p^2)$ i $p \equiv 1 \pmod{k}$.*

Dokaz. Neka je $\varepsilon < \dfrac{\Phi(k)}{3k}$. Označimo s p_n n-ti prosti broj koji je relativno prost s k i faktoriziran izraz $a^{p_n k} - 1 = C_{p_n k} D_{p_n k}$.

Zapišimo:

$$a^{p_n k} = (a^{p_n k} - 1) + 1,$$

tada ABC slutnja povlači

$$a^{p_n k} \ll_\varepsilon (\operatorname{rad}(a^{p_n k}(a^{p_n k} - 1)))^{1+\frac{\varepsilon}{2}},$$

pa je

$$a^{p_n k} - 1 \ll_\varepsilon (\operatorname{rad}(aC_{p_n k} D_{p_n k}))^{1+\frac{\varepsilon}{2}}$$

i na taj način dobivamo:

$$C_{p_n k} D_{p_n k} \ll_\varepsilon ((aC_{p_n k} D_{p_n k}))^{1+\frac{\varepsilon}{2}},$$

$\operatorname{rad}(D_{p_n k}) \leq (D_{p_n k})^{\frac{1}{2}}$. To povlači

$$(D_{p_n k})^{\frac{1}{2}} \ll_{\varepsilon,a} (aC_{p_n k} D_{p_n k})^{\frac{\varepsilon}{2}},$$

pa je $D_{p_n k} \ll_{\varepsilon,a} (a(a^{p_n k} - 1))^{\varepsilon}$ te zaključujemo da je

$$(D_{p_nk)} \ll_{\varepsilon,a} a^{p_nk_\varepsilon}.$$

Pa je

$$a^{p_nk-1} <_{\varepsilon,a} C_{p_nk}a^{p_nk_\varepsilon}, C_{p_nk} >_{\varepsilon,a} a^{p_nk(1-\varepsilon)}.$$

Neka je $C'_{p_nk} = ((C_{p_nk}, \Phi_{p_nk(a)})iD'_{p_nk} = ((D_{p_nk}, \Phi_{p_nk(a)})$ pa je $C'_{p_nk}D'_{p_nk} = \Phi_{p_nk(a)}$.
Po propoziciji :

Propozicija 4.5.2. *Za sve cijele brojeve $a \geq 2$ i $n > 2$, $|\Phi_n(a)| \geq \frac{1}{2}a^{\Phi}(n)$*

vrijedi

$$a^{p_nk_\varepsilon C'_{p_nk}} \gg \Phi_{p_nk}(a) \geqslant \frac{1}{2}a^{\Phi}(p_nk),$$

te zbog našeg izbora za ε i Rossovog teorema koji glasi:

Teorem 4.5.3 (Rossov teorem)**.** *N-ti prosti broj je strogo veći od $n \log n$.*

vrijedi

$$C'_{p_nk} \gg a^{\Phi(p_nk-p_nk_\varepsilon} \gg a^{\frac{\Phi(p_nk)}{2}} \gg a^{nlogn}.$$

Ako je C'_{p_nk} produkt različitih prostih brojeva.

$$\lim_{n\to\infty} |\text{prosti brojevi p} : p|C'_{p_jk}, j \leq n| = \infty.$$

Svaki prosti broj dijeli C'_{p_nk} i također dijeli $\Phi_{p_nk(a)}$ stoga je kongruentan s 1 modulo p_nk. Također znamo da ako p dijeli C'_{p_nk} onda $a^{p-1} \not\equiv 1(\mod p^2)$. Postoji beskonačno mnogo prostih brojeva p takvih da $a^{p-1} \not\equiv 1(\mod p^2)$ i $p \equiv 1 \pmod{k}$. □

4.6 Pillai-ova slutnja

Savršene potencije

Definicija 4.6.1. *Savršene potencije su pozitivni cijeli brojevi forme a^b gdje su a i b pozitivni cijeli brojevi gdje je $b \geqslant 2$.*

Primjer 4.6.2. *Primjeri savršenih potencija:*
Niz savršenih potencija: 1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 81, 100, 121, 125, 128, 144, 169, 196, 216, 225, 243, 256, 289, 324, 343, 361, 400, 441, 484, 512, 529, 576, 625, 676, 729, 784, 841, 900, 961, 1000, 1024, 1089, 1024, 1089, 1156, 1225, 1296, 1331, 1369, 1444, 1521, 1600, 1681, 1728, 1764, . . .

Kvadrati :
1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196,...
Kubovi :
1, 8, 27, 64, 125, 216, 343, 512, 729, 1 000, 1 331,...

Skoro pa jednake savršene potencije

- Razlika 1 : (8, 9)
- Razlika 2 : (25, 27),...
- Razlika 3 : (1, 4), (125, 128),...
- Razlika 4 : (4, 8), (32, 36), (121, 125),...
- Razlika 5 : (4, 9), (27, 32),...

Iskaz Pillai-ove slutnje - 1945

Slutnja 4.6.3. *Neka je k pozitivan cijeli broj. Jednadžba*

$$x^p - y^q = k,$$

gdje su nepoznanice x, y, p *i* q *cijeli brojevi, svi* $\geqslant 2$*, ima samo konačno mnogo rješenja* (x, y, p, q).

Pillaijeva slutnja odnosi se na razliku savršenih potencija : to je otvoreni problem koji je početno predložio S. S. Pillai, koji je pretpostavljao da praznine u nizu savršenih potencija imaju tendenciju da budu beskonačne. To je ekvivalentno navođenju da se svaki pozitivni cijeli broj pojavljuje samo konačno mnogo puta kao razlika savršenih potencija: općenitije, 1931. Pillai je pretpostavljao da za fiksne pozitivne cjeline A, B i C jednadžba $Ax^p - By^q = C$. Ta jednadžba ima samo beskonačno mnoga rješenja (x, y, p, q) s $(p, q) \neq (2, 2)$. Pillai su pokazali da razlika $|Ax^p - By^q| \gg x^{\lambda p}$ za bilo koji λ manji od 1, ravnomjerno u p i q.

Slučaj kad je $k = 1$ **- Cassels, Tijdeman, Langevin i Mignotte**

Jednadžba $|x^p - y^q| = 1$ nema cjelobrojna rješenja (x, y, p, q) s $p, q > 1$ i $\max(x^p, y^q) > \exp\exp\exp\exp(730)$.

PIllai-ova slutnja i ABC slutnja

Ne postoji vrijednost za $k \geq 2$ za koju se zna da Pillai-ova jednadžba $x^p - y^q = k$ ima samo konačno mnogo rješenja.

Pillai-ova slutnja kao posljedica ABC slutnje glasi:
Ako je $x^p \neq y^q$, tada

$$|x^p - y^q| \geq c(\varepsilon) \max x^p, y^{qk-\varepsilon} \quad \text{s} \quad k = 1 - \frac{1}{p} - \frac{1}{q}.$$

4.7 Hallova slutnja

Marshall Hall formulirao je originalnu formu Hallove slutnje 1970. godine. Hallovu slutnju smo u ovom radu već spominjali na samom početku. [10]

Slutnja 4.7.1. *Za svaki $\varepsilon > 0$, postoji konstanta $c(\varepsilon) > 0$ sa svojstvom da ako su x i y prirodni brojevi takvi da je $x^3 - y^2 \neq 0$, onda je*

$$|x^3 - y^2| > c(\varepsilon) x^{\frac{1}{2}-\varepsilon}.$$

Poznato je da Hallova slutnja slijedi iz ABC slutnje (postoji i jača verzija Hallove slutnje koja je ekvivalentna s ABC slutnjom).

Hallova slutnja i ABC slutnja

Dokazat ćemo da slaba Hallova slutnja slijedi iz odgovarajuće slabe ABC slutnje.

Teorem 4.7.2. *Pretpostavimo da je f rastuća te da zadovoljava*

$$f(2k) \leq k \text{ i } f(3k) \leq k, \text{ za } k \epsilon N.$$

Tada slaba ABC slutnja s ovom funkcijom f povlači slabu Hallovu slutnju.

Dokaz. Za prirodne brojeve x i y za koje vrijedi $x^2 \neq y^3$ te neka je $d = \mathrm{M}(x^2, y^3)$ onda je

$$a = \tfrac{1}{d}|x^2 - y^3| \text{ i } b = \tfrac{1}{d} \min(x^2 - y^3).$$

Tada je $a + b = c$ i $\mathrm{M}(a, b) = 1$.

Budući da f nije padajuća zbog djeljivosti m/n slijedi

$$r_f(m) \leq r_f(m)$$

osim toga pretpostavka teorema podrazumijeva

$$r_f(x^2) \leq x \text{ i} \leq r_f(y^3) \leq y.$$

Stoga

$$r_f(\tfrac{1}{d}x^2) \leqslant r_f(x^2) \leqslant x$$

i

$$r_f(\tfrac{1}{d}y^3) \leqslant r_f(y^3) \leqslant y.$$

Stoga $r_f(b)r_f(c) \leqslant xy$.

Iz slabe forme ABC slutnje dobivamo, za neki $C_1(\varepsilon) > 0$.

$$c \leqslant C_1(\varepsilon)r_f(abc)^{1+\varepsilon} \leqslant C_1\varepsilon(xy|x^2 - y^3|)^{1+\varepsilon}.$$

i stoga

$$x^2 \leqslant C_1(\varepsilon)(xy|x^2 - y^{3|})^{1+\varepsilon},\ y^3 \leqslant C_1(\varepsilon)(xy|x^2 - y^{3|})^{1+\varepsilon}.$$

Množenjem tih dviju nejednadžbi dobivamo:

$$x^3y^3 \leqslant C_1(\varepsilon)^2(xy|x^2 - y^{3|})^{2+2\varepsilon}.$$

i otuda

$$|x^2 - y^3|^{2+2\varepsilon} \geqslant C_2(\varepsilon)x^{-2\varepsilon}y^{1-2\varepsilon}.$$

Za $x \leqslant y^2$ slijedi da

$$|x^2 - y^3|^{2+2\varepsilon} \geqslant C_2(\varepsilon)y^{1-6\varepsilon}.$$

Stoga

$$|x^2 - y^3| \geqslant C_3(\varepsilon)y^{\frac{1}{2}-\varepsilon'},$$

s $\varepsilon' = \frac{7}{2(1+\varepsilon)} \cdot \varepsilon$.

Ako je $x > y^2$ onda očito imamo

$$|x^2 - y^3| > y^4 - y^3 > y > y^{\frac{1}{2}-\varepsilon}$$

za $y > 1$. □

4.8 Erdős-Woodsova slutnja

Postoji beskonačno mnogo parova pozitivnih cijelih brojeva (x, y) gdje je $x < y$ takvi da x i y imaju isti radikal, i u isto vrijeme $x + 1$ i $y + 1$ imaju također isti radikal.

Doista, za $k \geq 1$, par brojeva (x, y) s

$$x = 2^k - 2 = 2(2^{k-1} - 1) \text{ i } y = (2^k - 1)^2 - 1 = 2^{k+1}(2^{k-1} - 1)$$

zadovoljava uvjet, ako je

$$x + 1 = 2^k - 1 \text{ i } y + 1 = (2^k - 1)^2.$$

Postoji jedan poznati primjer, $(x, y) = (75, 1215)$ pa je

$$75 = 3 \cdot 5^2 \text{ i } 1215 = 3^5 \cdot 5 \text{ s } \text{rad}(75) = \text{rad}(1215) = 3 \cdot 5 = 15,$$

dok je

$$76 = 2^2 \cdot 19 \text{ i } 1215 = 2^6 \cdot 19 \text{ s } \text{rad}(76) = \text{rad}(1216) = 2 \cdot 19 = 38.$$

Nije poznato postoje je li daljnji primjeri. Ne zna se ni postoje li dva različita broja x, y takva da

$$\text{rad}(x) = \text{rad}(y),\ \text{rad}(x + 1) = \text{rad}(y + 1) \text{ i } \text{rad}(x + 2) = \text{rad}(y + 2).$$

Slutnja 4.8.1. *Postoji apsolutna konstanta k takva da, ako su x i y pozitivni cijeli brojevi zadovoljava*

$$\text{rad}(x + i) = \text{rad}(y + i)$$

za $i = 0, 1, ..., k - 1$ *i* $x = y$.

ABC slutnja i Erdős-Woodsova slutnja - 1996

Već 1975. godine Langevin je proučavao radikal od $n(n + k)$ gdje je $\text{M}(n, k) = 1$ koristeći donje granice linearne forme u logaritmima za algebarske brojeve (Bakerova metoda). Langevin je dokazao da ova slutnja proizlazi iz ABC slutnje.

4.9 Waring-HIlbertov teorem

U teoriji brojeva, Waringov problem postavlja pitanje ima li svaki prirodni broj k pridruženi pozitivni cijeli broj tako da svaki prirodni broj predstavlja sumu od najviše prirodnih brojeva na eksponent k. Na primjer, svaki prirodni broj je zbroj najviše 4 kvadrata, 9 kubova ili 19 potencija s eksponentom 4. Waringov problem predložio je Edward Waring 1770. godine, nakon čega je dobio naziv po njemu. Njegov afirmativni odgovor, poznat kao Hilbert-Waringov teorem, izrekao je Hilbert 1909. godine. Waringov problem ima svoju klasifikaciju predmeta matematike "Waringov problem i varijante". [9]

Teorem 4.9.1. *Waring-HIlbertov teorem*

Za svaki k postoji $g(k)$ *takav da je svaki pozitivan cijeli broj zbroj od najvećih k-tih eksponenata od* $g(k)$.

Slutnja o g(k)

Slutnja 4.9.2 (J.A. Euler (1772))**.** *Za svaki $k \geq 1$, $g(k) \geq l(k)$ gdje je*

$$l(k) = 2^k + \lfloor (3/2)^k \rfloor - 2.$$

Doista, cijeli broj $2\lfloor (3/2)^k \rfloor - 1$ je manji od 3^k pa mora biti napisano tako da se mogu pojaviti samo 1 ili 2 kao k.

Slutnja 4.9.3 (Bretshneiderova slutnja (1853))**.** *$g(k) = l(k)$ za svaki $k \geq 2$.*

Procjene o g(k) za k= 2,3,4,...

$g(2) = 4 \Rightarrow$ *Lagrange*(1770)
g(3) = 9$\Rightarrow$ *Kempner*(1912)
g(4) = 19$\Rightarrow$ *Balusubramanian*, *Dress*, *Deshouillers*(1986)
g(5) = 37$\Rightarrow$ *ChenJingrum*(1964)
g(6) = 73$\Rightarrow$ *Pillai*(1940)
g(7) = 143$\Rightarrow$ *Dickson*(1936)

Dovoljan uvjet - Dickson, Pillai (1936) Ako je k takav da je $2^k(3/2)^k + \lfloor (3/2)^k \rfloor \leq 2^k - 2$ tada Bretscneiderova slutnja vrijedi za k.

Teorem 4.9.4 (Mahlerov teorem)**.** *Uvjet od Dicksona i Pillai je istinit za konačan skup cijelih brojeva k.*

Waring-HIlbertov teorem i ABC slutnja

Rasprava između Davida i Waldschmidta je dovela do dokaza Mahlerovog rezultata kao posljedica ABC slutnje. Laishram je to dokazao Bretschneiderovom slutnjom koja slijedi iz Bakerove eksplicitna verzije ABC slutnje. Isti autor je dokazao niz eksplicitnih rezultata u zajedničkom radu s Shoreyjem.

4.10 Još neke posljedice ABC slutnje

Preostale posljedice ABC slutnje:
• Langova slutnja: niže granice za visine, broj točaka integrala na eliptičkim krivuljama. (Frey 1987) (Hindry, Silverman 1988)
• Brojevi koji nisu cjelobrojni kvadrati brojeva i potencije koje nisu cjelobrojne su vrijednosti polinoma. (Browkin, Filaseta, Greaves, Schinzel 1995)
• Granice za redoslijed grupe Tate-Shafarevich. (Goldfeld, Szpiro 1995)
• Frey je 1987. godine dokazao ekvivalentnost između više slutnje i ABC slutnje, dok je

Mai i Murty 1996. dokazali jednakost s stupnjem slutnje.
• Slutnja abc za ciklotomsko algebrasko polje brojeva K implicira Greenbergovu slutnju za beskonačno. mnogo prostih brojeva p: Iwasawove invarijante $\lambda_{p(K)}$ i $\mu_p(K)$ nestaju. (Ichimura pomoću leme od Sumide 1998)
• Jaka ABC slutnja implicira Dresslerovu slutnju: između dva pozitivna cijela broja koji ima iste proste faktori, uvijek postoji prost broj. (Cochrane i Dressler, 1999)
• Uniformna abc slutnja za algebraska polja brojeva implicira nižu granicu za broj klase imaginarnih kvadratnih polja (Granville i Stark 2000), a Mahler je pokazao da to implicira da povezana L-funkcija nema Siegelovih nula.

Poglavlje 5

Generalizacije ABC slutnje

5.1 ABC slutnja za polinome

Neka je $f(t)$ polinom (s kompleksnim koeficijentima) te neka je rad(f) produkt prostih faktora od f.

Primjer 5.1.1. *Ako je* $f(t) = t-3t^3+3t^5-t^7 = t(1-t)^3(1+t)^3$ *onda je* $\text{rad}(f) = t(t-1)(t+1) = t^3 - t$.

Polinomi imaju specijalno svojstvo da se radikal može odrediti drugačije:

$$\text{rad}(f) = \frac{f(t)}{M((f(t), f'(t))}.$$

Teorem 5.1.2 (Stothers(1981) - Mason(1983))**.** *Ako* $f(t)+g(t) = h(t)$, *s* $f, g, h \neq 0$ *relativno prosti i nisu sve konstante, onda je*

$$\max(\deg f, \deg g, \deg h) \leq \deg(rad(fgh)) - 1. \tag{5.1}$$

Usporedimo ovaj teorem s logaritamskom formom ABC slutnje:

$$\max(\log|a|, \log|b|, \log|c|) < (1+\varepsilon)\log \text{rad}(abc) + \log k_\varepsilon.$$

Dokaz. Ni f ni g nisu konstante, te je $f + g = h$. Podijelimo ovaj izraz s f. Dobivamo $1 + \frac{g}{f} = \frac{h}{f}$ te kada deriviramo dobivamo: $\frac{fg' - gf'}{f^2} = \frac{fh' - hf'}{f^2} \Rightarrow fg' - gf' = fh' - hf'$. Lijeva strana je djeljiva s M(f, f') i M(g, g') i desna strana je djeljiva s M(h, h'). M(f, f'), M(g, g') i M(h, h') su relativno prosti te zato vrijedi:

$$\text{M}(f, f')\,\text{M}(g, g')\,\text{M}(h, h')|(fg' - gf'),$$

$$\deg(\mathrm{M}(f, f')\,\mathrm{M}(g, g')\,\mathrm{M}(h, h')) \leq \deg f + \deg g - 1. \tag{5.2}$$

Za $\mathrm{rad}(f) = \dfrac{f}{M(f, f')}$, $\deg(\mathrm{M}(f, f')) = \deg f - \deg(\mathrm{rad}(f))$. Također isto vrijedi i za g i h.

Lijeva strana nejednakosti (5.2) jednaka je $\deg f + \deg g + \deg h - \deg(\mathrm{rad}(fgh))$.

Zamijenimo ovo s nejednakosti i oduzimanjem $\deg f$ i $\deg g$ te dobivamo:

$$\deg h \leq \deg(\mathrm{rad}(fgh)) - 1.$$

Micanjem uvjeta iz originala $f + g = h$ dobivamo slično

$$\deg f, \deg g \leq \deg(\mathrm{rad}(fgh)) - 1$$

i to je kraj dokaza. □

5.2 ABC slutnja za binarne oblike

Neka je $F(x, y)$ homogeni polinom s cjelobrojnim koeficijentima i bez ponavljanja linearnih faktora. Za svaki $\varepsilon > 0$, postoji konstanta k_ε takva da za sve relativno proste brojeve m i n vrijedi:

$$\max(|m|, |n|) \leq k_{\varepsilon,F}(\mathrm{rad}(mnF(m, n))^{\deg(F)+\varepsilon}.$$

Obrnuto, ova slutnja povlači ABC slutnju kada je $F(X, Y) = X + Y$. [9]

5.3 ABC slutnja za n cijelih brojeva

Browkin-Brzezinskeva n-slutnja

1994. godine, Browkin i Brzezinski predložili su sljedeću slutnju: [4]
Za $n \geq 3$, neka $a_1, a_2, ..., a_n \epsilon \ \mathbb{Z}$ zadovoljavaju tri uvjeta:
(i) $\mathrm{M}(a_1, a_2, ..., a_n) = 1$,
(ii) $a_1 + a_2 + ... + a_n = 0$,
(iii) Nijedna podsuma od $a_1, a_2, ..., a_n$ nije jednaka nuli.
Prva formulacija:

Slutnja 5.3.1 (n-slutnja)**.** *Za svaki $\varepsilon > 0$, postoji konstanta $k_{n,\varepsilon}$ koja ovisi o n i o ε takva da za sve cijele brojeve $a_1, a_2, ..., a_n$, $a_1 + a_2 + ... + a_n = 0$, $\mathrm{M}(a_1, ..., a_n) = 1$ vrijedi:*

$$\max(|a_1|, ..., |a_n|) < k_{n,\varepsilon}(rad(a_1 \times ... \times a_n))^{2n-5+\varepsilon}.$$

Druga fomulacija:

Slutnja 5.3.2. *Definiramo kvalitetu od* $a_1 + a_2 + ... + a_n$ *kao*

$$q(a_1, a_2, ..., a_n) = \frac{\log(\max(|a_1|, |a_2|, ..., |a_n|)}{\log(\text{rad}(|a_1| \cdot |a_2| \cdot .... \cdot |a_n|)}.$$

Pa n-slutnja navodi da $\limsup q(a_1, a_2, ..., a_n) = 2n - 5$.

Vojtova snažna n-slutnja

1998. godine je Vojta predložio snažniju varijantu n slutnje:

Postoje dvije različite formulacije ove snažne n slutnje.

Za $n \geq 3$, neka $a_1, a_2, ..., a_n \epsilon \ \mathbb{Z}$ zadovoljavaju tri uvjeta:

(i) $a_1, a_2, ..., a_n$ su relativno prosti u parovima,

(ii) $a_1 + a_2 + ... + a_n = 0$,

(iii) Nijedna podsuma od $a_1, a_2, ..., a_n$ nije jednaka nuli.

Prva formulacija:

Slutnja 5.3.3 (Snažna n-slutnja)**.** *Za svaki* $\varepsilon > 0$*, postoji konstanta* $k_{n,\varepsilon}$ *koja ovisi o n i o* ε *takva da za sve cijele brojeve* $a_1, a_2, ..., a_n,\ a_1 + a_2 + ... + a_n = 0,\ \text{M}(a_1, ..., a_n) = 1$ *vrijedi:*

$$\max(|a_1|, ..., |a_n|) \leq k_{n,\varepsilon}(\text{rad}(a_1 \times ... \times a_n))^{1+\varepsilon}.$$

Druga fomulacija:

Slutnja 5.3.4. *Definiramo kvalitetu od* $a_1 + a_2 + ... + a_n$ *kao*

$$q(a_1, a_2, ..., a_n) = \frac{\log(\max(|a_1|, |a_2|, ..., |a_n|)}{\log(rad(|a_1| \cdot |a_2| \cdot .... \cdot |a_n|)}.$$

Snažna n-slutnja navodi da $\limsup q(a_1, a_2, ..., a_n) = 1$.

5.4 Bakerova ABC slutnja za cijele brojeve

Alan Baker je engleski matematičar koji je dobio Fieldsovu medalju, u dobi od 31 godine. Njegovi su interesi bili u teoriji brojeva, transcendenciji, logaritamskim formama, efektivnim metodama, diofantskoj geometriji i diofantskoj analizi. [1]

Godine 2012. postao je član Američkog matematičkog društva.
1996. godine Alan Baker predložio je verziju ABC slutnje povezanu s teorijom linearnih formi u logaritmima.

Slutnja 5.4.1. *Za svaki ε, postoji konstanta $k_\varepsilon > 0$ takva da za svaku trojku pozitivnih cijelih brojeva a, b, c koji zadovoljavaju $a + b = c$ i $\mathrm{M}(a, b) = 1$ imamo:*

$$c \leq k_\varepsilon(\varepsilon^\omega \operatorname{rad}(abc))^{1+\varepsilon}$$

gdje ω označava broj različitih prostih faktora od abc.

Ova slutnja bi dala najbolje donje granice koje se mogu dobiti u teoriji linearnih formi u logaritmima.

5.5 Hu-Yang-ova verzije ABC slutnje za cijele brojeve

Neka je a cijeli broj različit od nule s faktorizacijom $|a| = p_j^{i_1} ... p_n^{i_n}$ gdje su $p_1, ..., p_n$ različiti prosti brojevi. Odredimo k-radikal da bude: $r_k(a) = \prod_{p_j|a}(p_j)^{\min(i_j,k)}$.
2002. Hu i Yang predlažu sljedeću slutnju:

Slutnja 5.5.1. *Neka su $a_i, i = 0, ..., k$ cijeli brojevi različiti od nule bez zajedničkih faktora i bez odgovarajućih podsuma jednakih nuli takvi da*

$$a_0 + ... + a_k = 0.$$

Tada za $\varepsilon > 0$, postoji konstanta $C(k, \varepsilon)$ takva da je

$$\max |a_i| < C(k, \varepsilon)R(a_0...a_k)^{i+\varepsilon}$$

gdje je $R(a_0...a_k) = \prod_i r_{k-1}(a_i)$.

Ako je $k = 2$, onda to odgovara ABC slutnji.

Poglavlje 6

Pokušaj dokaza ABC slutnje

Vidjeli smo da je ABC slutnja ekvivalentna proširenjima nekoliko najvažnijih teorema u teoriji brojeva: Rothov Theorem, Bakerov teorem i Wilesov teorem. Dokazivanje abc slutnje bi stoga imalo izuzetan utjecaj na naše razumijevanje teorije brojeva.

Dokaz od 500 stranica objavio je Shinichi Mochizuki iz Sveučilišta Kyoto u Japanu 2012. Shinichi Mochizuki je japanski matematičar rođen 29. ožujka 1969. godine koji se bavi teorijom brojeva. Matematičari su bili uzbuđeni dokazom, ali su se trudili uhvatiti u koštac s Mochizukijevom "Inter-universal Teichmüller teorijom" (IUT), sasvim novim područjem matematike koju je razvio tijekom desetljeća kako bi se riješio problem. Sastanak 2016. godine na Sveučilištu u Oxfordu u Velikoj Britaniji s ciljem proučavanja IUT-a završio je neuspjehom, dijelom zato što Mochizuki ne želi pojednostaviti njegov rad kako bi ga lakše shvatio, te zbog sukoba između načina japanske i zapadne kulture proučavanja matematike. 2012. godine Shinichi Mochizuki objavio je seriju od četiri preprinta o Inter-universal Teichmuller Theory koja se potom primjenjuje za dokazivanje nekoliko poznatih slutnji u teoriji brojeva, uključujući Szpirovu slutnju, hiperboličku Vojtinu pretpostavku i ABC slutnju. Teorija se mnogo razlikuje od bilo koje standardne teorije i ide dobro izvan opsega aritmetičke geometrije. Razvijen je tijekom dva desetljeća s posljednja četiri IUT članka zauzimajući prostor od preko 500 stranica i korištenjem mnogih njegovih prethodno objavljenih radova.

Kada je istaknuta pogreška u jednom od članaka Vesselin Dimitrov i Akshay Venkatesh u listopadu 2012, Mochizuki je objavio komentar na svojoj web stranici priznajući pogrešku, navodeći da neće utjecati na rezultat, i obećavajući ispravljenu verziju u bliskoj budućnosti.

Bibliografija

[1] Alan Baker, *Logarithmic forms and the abc-conjecture*, Journal of sNumber Theory (1998).

[2] Razvan Barbulescu i Michel Waldschmidt, *The abc conjecture and some of its consequences*.

[3] Frits Beukers, *The ABC-conjecture*, 2005, `http://www.staff.science.uu.nl/~beuke106/ABCpresentation.pdf`.

[4] Jerzy Browkin i Juliusz Brzeziński, *Some remarks on the abc-conjecture*, American Mathematical Society (1994).

[5] Brian Conrad, *The ABC conjecture*.

[6] Dorian Goldfeld, *Modular Forms, Elliptic Curves, and the ABC Conjecture*, A Panorama of Number Theory Or The View from Baker's Garden, Cambridge University Press, 2002.

[7] Andrew Granville i Thomas J. Tucker, *It's As Easy As abc*, Notices of the American Mathematical Society (2002).

[8] Hester Graves i M. Ram Murty, *The abc conjecture and non-Wieferich primes in arithmetic progressions*, Journal of Number Theory (2013).

[9] Michel Waldschmidt, *Lecture on the abc conjecture and some of its consequences*, 2014.

[10] _____, *On the abc Conjecture and some of its consequences*.

Sažetak

ABC slutnju su prvi put izrekli u 20. stoljeću matematičari Joseph Oesterlé i David Wiliam Masser u Bonnu 1985.g. Oesterlé i Masser su došli do ABC slutnje potaknuti proučavanjem određenih teza o polinomima i proučavanjem Szpirove slutnje. ABC slutnja kaže da za svaki $\varepsilon > 0$ postoji samo konačno mnogo trojki relativno prostih prirodnih brojeva a, b, c za koja vrijedi $a + b = c$ i za koje je produckt prostih faktora od a, b, c veći od $c^{1+\varepsilon}$. ABC trojkom nazivamo relativno proste brojeve a,b za koje vrijedi $a + b = c$, dok produkt prostih faktora nekog broja nazivamo radikal. Što je manji radikal u usporedbi s c, veća je kvaliteta trojke. Prvu verziju ABC slutnje nazivamo slaba verzija ABC slutnje, te nakon te verzije su nastale još mnoge verzije. ABC slutnja je važna zbog mnogobrojnih generalizacija i značajnih posljedica koje bi njeno dokazivanje uzrokovalo. Kad bi se ABC slutnja dokazala, dokazali bi se i mnogi dosad neriješeni problemi u matematici. Neke od posljedica: Fermatov posljedni teorem, Catalanova slutnja, Fermat-Catalanova slutnja, Rothov teorem, Hallova slutnja te mnoge druge. Neke od generalizacija: ABC slutnja za polinome, za binarne oblike, za n cijelih brojeva, Bakerova ABC slutnja za cijele brojeve... Za ABC slutnju se još ne zna je li dokazana. Dokaz od 500 stranica objavio je Shinichi Mochizuki iz Sveučilišta Kyoto u Japanu 2012. Shinichi Mochizuki je japanski matematičar rođen 29. ožujka 1969. godine koji se bavi teorijom brojeva. Matematičari su bili uzbuđeni dokazom, ali su se trudili uhvatiti u koštac s Mochizukijevom ”Inter-universal Teichmüller teorijom” (IUT), sasvim novim područjem matematike koju je razvio tijekom desetljeća kako bi se riješio problem.

Summary

The abc conjecture is a conjecture in number theory, first proposed by Joseph Oesterlé and David Masser (1985). It is stated in terms of three positive integers, a, b and c (hence the name) that are relatively prime and satisfy $a + b = c$. If rad denotes the product of the distinct prime factors of abc, the conjecture essentially states that rad is usually not much smaller than c. In other words: if a and b are composed from large powers of primes, then c is usually not divisible by large powers of primes. The abc conjecture has a large number of consequences and generalizations. These include both known results (some of which have been proven separately since the conjecture has been stated) and conjectures for which it gives a conditional proof. While an earlier proof of the conjecture would have been more significant in terms of consequences, the abc conjecture itself remains of interest for the other conjectures it would prove, together with its numerous links with deep questions in number theory. Some of consequences are: Fermat last theorem, Catalan's conjecture, Fermat-Catalan's conjecture, Roth's conjecture, Hall's conjecture and others. In August 2012, Shinichi Mochizuki released a series of four preprints on Inter-universal Teichmuller Theory which is then applied to prove several famous conjectures in number theory, including Szpiro's conjecture, the hyperbolic Vojta's conjecture and the abc conjecture. Mochizuki calls the theory on which this proof is based "inter-universal Teichmüller theory (IUT)". The theory is radically different from any standard theory and goes well outside the scope of arithmetic geometry. It was developed over two decades with the last four IUT papers occupying the space of over 500 pages and using many of his prior published papers.

Životopis

Lukrecija Roić rođena je 07.02.1992. godine u Zagrebu. Pohađala je Osnovnu školu "Grof Janko Drašković" te II. gimnaziju u Zagrebu. Obrazovanje je nastavila na Matematičkom odsjeku Prirodoslovno matematickog fakulteta u Zagrebu, na kojem upisuje preddiplomski studij 2010. godine te nakon toga diplomski studij Matematika; smjer nastavnički 2014. godine. Od 2016. godine aktivno radi na dva učilišta gdje predaje mateamatiku. Završila je diplomski studij u veljači 2018. godine.