Μια αλγεβρική απόδειξη της Εικασίας του Catalan

Μεταπτυχιακή εργασία

Γιώργος Παπαδημητρίου
Επιβλέπων: Νίκος Τζανάκης

Πανεπιστήμιο Κρήτης - Τμήμα Μαθηματικών & Εφαρμοσμένων Μαθηματικών
Οκτώβριος 2024

Εισαγωγή

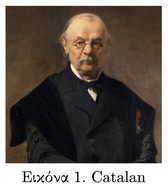
Το 1844 ο Βέλγος μαθηματικός Eugène Charles Catalan σε ένα σύντομο σημείωμά του προς το περιοδικό του Aug. Leop. Crelle ζητά τη δημοσίευση της εικασίας ότι ***το 8 και το 9 είναι το μόνο ζεύγος διαδοχικών τέλειων δυνάμεων,*** «ελπίζοντας ότι ίσως άλλοι θα έχουν την "τύχη" να αποδείξουν».
Ισοδύναμη διατύπωση της εικασίας: Μοναδική λύση της

$$x^n - y^m = 1, \;\; xy \neq 0, \;\; n, m \geq 2,$$

είναι η $(n, m, x, y) = (2, 3, \pm 3, 2)$.
Όπως συνήθως στις εκθετικές Διοφαντικές εξισώσεις, η μελέτη της παραπάνω εξίσωσης ανάγεται στην περίπτωση **πρώτων εκθετών**.

$$x^p - y^q = 1,$$

με τους x, y μη μηδενικούς ακέραιους και τους p, q πρώτους.
Οι περιπτώσεις $p = 2$ και $q = 2$ απαιτούν στοιχειώδεις μεθόδους και μελετήθηκαν από τους **Ko Chao** και **V.A. Lebesgue**.
Ιδιαίτερη δυσκολία και ενδιαφέρον παρουσιάζει η περίπτωση όπου οι p, q είναι και οι δύο περιττοί πρώτοι. Ο **Preda Mihăilescu** σε τρία άρθρα του μεταξύ των ετών 2003 και 2006 απέδειξε ότι η εξίσωση αυτή είναι αδύνατη, αποδεικνύοντας έτσι την εικασία.


Εικόνα 1. Catalan

Οι συνθήκες του Mihăilescu

Ο Mihăilescu απέδειξε τέσσερις πολύ ισχυρές συνθήκες οι οποίες πρέπει να ικανοποιούνται από τους x, y, p, q, αν αυτοί είναι λύση της εξίσωσης.
Αρχικά θα παρουσιάσουμε τις τέσσερις συνθήκες και θα δείξουμε πόσο απλά προκύπτει το θεώρημα από αυτές.

Θεώρημα (Πρώτη Συνθήκη - Σ1). *Αν $x^p - y^q = 1$, τότε*

$$p^2 \mid y, \quad q^2 \mid x, \quad q^{p-1} \equiv 1 \pmod{p^2}, \quad p^{q-1} \equiv 1 \pmod{q^2}.$$

Θεώρημα (Δεύτερη Συνθήκη - Σ2). *Αν $x^p - y^q = 1$, τότε*

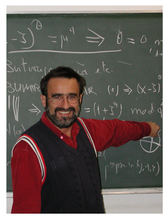
$$\min\{p, q\} > 11.$$

Θεώρημα (Τρίτη Συνθήκη - Σ3). *Αν $x^p - y^q = 1$, τότε*

$$p < 4q^2 \;\; \textit{και} \;\; q < 4p^2.$$

Θεώρημα (Τέταρτη Συνθήκη - Σ4). *Αν $x^p - y^q = 1$, τότε*

$$p \equiv 1 \pmod{q} \;\; \textit{ή} \;\; q \equiv 1 \pmod{p}.$$


Εικόνα 2. Mihăilescu

Η απόδειξη της εικασίας

Θεώρημα (P. Mihăilescu). *Αν οι p, q είναι περιττοί πρώτοι, τότε η εξίσωση $x^p - y^q = 1$ δεν έχει μη μηδενικές ακέραιες λύσεις.*
Λήμμα. *Αν (x, y, p, q) είναι λύση της $x^p - y^q = 1$, τότε $p \neq q$.*
Παρατήρηση. *Εφόσον οι p, q στην εξίσωση $x^p - y^q = 1$ είναι και οι δύο περιττοί, η εξίσωση γράφεται, επίσης, $(-y)^q - (-x)^p = 1$. Συνεπώς, ο ρόλος των ζευγαριών (x, p) και (y, q) στην εξίσωση είναι συμμετρικός. Επομένως, αφού $p \neq q$, μπορούμε να υποθέσουμε $p > q$.*
Απόδειξη του Θεωρήματος. Έστω (x, y, p, q) λύση της εξίσωσης. Από το Λήμμα, $p \neq q$. Από την **(Σ4)** $p \equiv 1 \pmod{q}$ ή $q \equiv 1 \pmod{p}$. Λόγω συμμετρίας (Παρατήρηση), έστω $p \equiv 1 \pmod{q}$. Από το Διωνυμικό Θεώρημα έχουμε ότι

$$p^q = (1 + (p-1))^q = 1 + \underbrace{\sum_{i=1}^{q} \binom{q}{i} (p-1)^i}_{\equiv 0 \pmod{q^2}},$$

άρα

$$p^q \equiv 1 \pmod{q^2}. \tag{1}$$

Από τη **(Σ1)**, είναι $p^{q-1} \equiv 1 \pmod{q^2}$, άρα

$$p^q \equiv p \pmod{q^2}. \tag{2}$$

Συνδυάζοντας τις (1) και (2) έχουμε τελικά $p \equiv 1 \pmod{q^2}$. Από τη **(Σ3)**, είναι $p < 4q^2$ άρα έχουμε τελικά

$$p = 1 + sq^2, \; s = 1, 2, 3.$$

Οι τιμές $s = 1$ και $s = 3$ δίνουν άρτιο p, οπότε απορρίπτονται, άρα $p = 1 + 2q^2$. Από τη **(Σ2)**, ο q είναι πρώτος > 3 , άρα $q^2 \equiv 1 \pmod{3}$, άρα $p \equiv 0 \pmod{3}$, άτοπο. □

Οι αποδείξεις των συνθηκών

Κύριο μέρος της εργασίας αυτής αποτέλεσε η λεπτομερής μελέτη των αποδείξεων των τεσσάρων συνθηκών. Οι αποδείξεις απαιτούν αρκετά σύνθετα μαθηματικά εργαλεία και εμφανίζουν ιδιαίτερη δυσκολία. Ένα αποτέλεσμα που αποδείχθηκε 40 χρόνια πριν τις εργασίες του Mihăilescu, το οποίο όμως έχει ενεργό ρόλο στην απόδειξη των συνθηκών είναι το ακόλουθο θεώρημα και οφείλεται στον **J.W.Cassels**.

Θεώρημα (Cassels, 1960). *Αν $x^p - y^q = 1$, τότε $p \mid y$ και $q \mid x$.*

Συμβολισμοί

- $\zeta = \zeta_p$, πρωταρχική p-ρίζα της μονάδας.
- $K = \mathbb{Q}(\zeta)$ και $K^+ = \mathbb{Q}(\zeta + \zeta^{-1})$.
- $\mathbb{Z}_K$, $\mathbb{Z}_{K^+}$ δακτύλιοι των ακεραίων των K και K^+ αντίστοιχα.
- $G = \mathrm{Gal(K/\mathbb{Q})} = \{\sigma_1, \sigma_2, \ldots, \sigma_{p-1}\}$, όπου $\sigma_k(\zeta) = \zeta^k$ και άρα $\sigma_{p-1} = \iota$.
- $G^+ = \mathrm{Gal}(K^+/\mathbb{Q})$
- $\mathrm{Cl}(K)$, $\mathrm{Cl}(K^+)$ οι αντίστοιχες ομάδες κλάσεων ιδεωδών.
- $h_p := |\mathrm{Cl}(K)|$ και $h_p^+ := |\mathrm{Cl}(K^+)|$.

Στις αποδείξεις εμφανίζεται μια αλγεβρική δομή η οποία αποτελεί "συνδυασμό" ενός δακτύλιου και μιας ομάδας. Έστω R ένας αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο και μια πεπεραμένη πολλαπλασιστική ομάδα H, όπου $H = \{h_1, \ldots, h_n\}$.
Ορίζουμε τον **δακτύλιο ομάδας**

$$R[H] = \left\{ \sum_{j=1}^{n} r_j h_j \,\middle|\, r_j \in R \right\}.$$

Ο $R[H]$ εφοδιασμένος με τις "φυσιολογικές" πράξεις είναι **ελεύθερο R-module** και **δακτύλιος**.
Σε ό,τι ακολουθεί $p > q$ περιττοί πρώτοι και x, y μη μηδενικοί ακέραιοι ώστε $x^p - y^q = 1$.

Απόδειξη Πρώτης Συνθήκης

Πρόταση 1. *Αν $x^p - y^q = 1$, τότε ισχύει η ισοδυναμία $q^2 \mid x \Leftrightarrow p^{q-1} \equiv 1 \pmod{q^2}$.*

Πρόταση 2. *Αν το $\theta \in \mathbb{Z}[G]$ μηδενίζει την $\mathrm{Cl}(K)$ (δηλαδή $[\mathfrak{a}]^\theta = [1]$ για κάθε ιδεώδες $\mathfrak{a}$ του K), τότε $(1 - \zeta x)^{(1-\iota)\theta}$ είναι q-δύναμη στο K.*

Πρόταση 3. *Αν υπάρχει $\theta \in \mathbb{Z}[G]$ που δεν διαιρείται από τον q (στον $\mathbb{Z}[G]$) και το $(1 - \zeta x)^\theta$ είναι q-δύναμη, τότε $q^2 \mid x$.*

Εξαιτίας της **Π3** και της συμμετρίας αρκεί να δείξουμε ότι $q^2 \mid x$. Από τις **Π1** και **Π2**, αρκεί να βρούμε $\Theta_S \in \mathbb{Z}[G]$ ώστε το Θ_S να μηδενίζει την $\mathrm{Cl}(K)$ και να μην διαιρείται από το q στον $\mathbb{Z}[G]$. Για την εύρεση του Θ_S χρησιμοποιούμε ένα γνωστό θεώρημα που οφείλεται στον **Stickelberger**.
Θεωρούμε το στοιχείο $\Theta = \frac{1}{p} \sum_{a=1}^{p-1} a\sigma_a^{-1} \in \mathbb{Q}[G]$ και ορίζουμε το **ιδεώδες του Stickelberger** $I_s := \Theta\mathbb{Z}[G] \cap \mathbb{Z}[G]$. Τα στοιχεία του είναι τα $\mathbb{Z}[G]$-πολλαπλάσια του Θ που ανήκουν στον $\mathbb{Z}[G]$.
Θεώρημα (Stickelberger, 1890). *Κάθε $\theta \in I_s$ μηδενίζει την ομάδα κλάσεων $\mathrm{Cl}(K)$ του K.*
Από το παραπάνω, είναι εύκολο να δούμε ότι το στοιχείο $\Theta_S = \sum_{a=1}^{p-1} a\sigma_a^{-1}$ έχει τις ζητούμενες ιδιότητες και αποδεικνύεται η **(Σ1)**

Απόδειξη Δεύτερης Συνθήκης

Η **(Σ2)** αποτελεί αμέσο πόρισμα του ακόλουθου θεωρήματος.
Θεώρημα (Mihăilescu). *Αν $x^p - y^q = 1$, τότε $p \mid h_q^-$ και $q \mid h_p^-$.*
Ο αριθμός h_p^- ορίζεται ως το πηλίκο h_p/h_p^+.
Λόγω συμμετρίας, έστω $q \leq 11$. Είναι γνωστό ότι $h_q = 1$ για κάθε πρώτο $q \leq 19$. Επομένως, έχουμε $p \nmid h_q^- = 1$ και άρα από το παραπάνω θεώρημα έχουμε άτοπο.

Απόδειξη Τρίτης Συνθήκης

Ορισμός. • $E := \{u(1-\zeta)^k \mid u \in U_K, \; k \in \mathbb{Z}\}$.
• $V := \{\alpha \in K^* \mid \alpha\mathbb{Z}_K = \mathfrak{b}^q\mathfrak{p}^k, \; \mathfrak{b}$ *κλασματικό ιδεώδες του* $\mathbb{Z}_K\}$.
• $S := V/(K^*)^q$ *και συμβολίζουμε με* $[v]$ *την κλάση του* $v \in V$ *στην* S.

Συμβολίζουμε με X τον μηδενιστή της $[x - \zeta] \in S$ στον $\mathbb{Z}[G]$. Ορίζουμε επίσης το $I = (1-\iota)I_s$, το οποίο αποδεικνύουμε ότι μηδενίζει την ομάδα S. Τέλος, για ένα $f = \sum_{t=1}^{p-1} a_t\sigma_t \in \mathbb{Z}[G]$ ορίζουμε **νόρμα** $\|f\| = \sum_{t=1}^{p-1} |a_t|$.
Η **(Σ3)** είναι συνέπεια των παρακάτω προτάσεων:

Πρόταση 1. *Έστω $\theta \in X \cap (1-\iota)\mathbb{Z}[G]$ μη μηδενικό, $\alpha \in K^*$ ώστε $(x-\zeta)^\theta = \alpha^q$ και $\|\theta\| \leq 3q/(p-1)$. Τότε είναι $|\mathrm{Arg}(\alpha)| > \frac{\pi}{q}$, όπου $\mathrm{Arg}(z) \in (-\pi, \pi]$.*

Πρόταση 2. *Έστω $q > 4p^2$. Τότε υπάρχει μη μηδενικό $\theta \in I$, με $\|\theta\| \leq 3q/(p-1)$ και $|\mathrm{Arg}(\alpha)| \leq \pi/q$, όπου το $\alpha \in K^*$ είναι εκείνο για το οποίο έχουμε $(x-\zeta)^\theta = \alpha^q$.*

Λόγω συμμετρίας, έστω $q > 4p^2$. Τότε, από την **Π2** έχουμε $0 \neq \theta \in I$ με "κατάλληλη" νόρμα ώστε $|\mathrm{Arg}(\alpha)| \leq \pi/q$. Όμως, το I μηδενίζει την S και $I \subseteq (1-\iota)\mathbb{Z}[G]$, άρα $\theta \in X \cap (1-\iota)\mathbb{Z}[G]$ και άρα από **Π1**, είναι $|\mathrm{Arg}(\alpha)| > \frac{\pi}{q}$, άτοπο.

Απόδειξη Τέταρτης Συνθήκης

Για την απόδειξη της τελευταίας συνθήκης ορίζουμε μια "ιδιαίτερη" ομάδα S_q και συμβολίζουμε με S^+ τα στοιχεία της S που είναι αναλλοίωτα από τον ι.

Θεώρημα 1. *Έστω ότι $x^p - y^q = 1$. Τότε, το υπο-module του S^+ που παράγεται από την κλάση $[x-\zeta]^{1+\iota}$ είναι ελεύθερο, δηλαδή*

$$\mathrm{Ann}_{\mathbb{F}_q[G^+]}([x-\zeta]^{1+\iota}) = 0.$$

Θεώρημα 2. *Αν $p \not\equiv 1 \pmod{q}$, τότε*

$$\mathrm{Ann}_{\mathbb{F}_q[G^+]}(S^+ \cap S_q) \neq 0.$$

Έστω $p \not\equiv 1 \pmod{q}$. Αποδεικνύεται ότι $[x-\zeta]^{1+\iota} \in S^+ \cap S_q$, άρα $0 \neq \mathrm{Ann}_{\mathbb{F}_q[G^+]}(S^+ \cap S_q) \subseteq \mathrm{Ann}_{\mathbb{F}_q[G^+]}([x-\zeta]^{1+\iota}) = 0$, άτοπο και έχουμε την **(Σ4)**.

Αναφορές

[1] Henri Cohen, *Number Theory Vol. I & II*, Graduate Texts in Mathematics **239** & **240**, Springer (2007).
[2] René Schoof, *Catalan's Conjecture*, Springer (2008).
[3] Y. F. Bilu, Y. Bugeaud, M. Mignotte, *The Problem of Catalan*, Springer (2014).