Το 10ο πρόβλημα του Hilbert I

Το 1900 στο Παρίσι, ο David Hilbert έκανε μια ομιλία για τα 23 πιο σπουδαία μαθηματικά προβλήματα που κληρονομούσε ο 20ος αιώνας από τον 19ο. Το 10ο ήταν:

> *Απόφανση περί επιλυσιμότητας μιας Διοφαντικής εξίσωσης*

δηλαδή να ευρεθεί **αλγόριθμος** που δεδομένου ενός **πολυωνύμου με ακέραιους συντελεστές** να αποφασίζει αν έχει **ακέραιες ρίζες**.

Μία τέτοια εξίσωση

$$D(x_1, \ldots, x_n) = 0,$$

όπου D πολυώνυμο με ακέραιους συντελεστές λέγεται **Διοφαντική** προς τιμήν του Έλληνα (Αλεξανδρινού) μαθηματικού Διόφαντου, που έζησε τον 3ο αιώνα μ.Χ.

Έως το 1900, υπήρχαν μέθοδοι επίλυσης (θετικής ή αρνητικής) για διάφορες υποκατηγορίες των Διοφαντικών εξισώσεων, ο Hilbert όμως ζητούσε μία **καθολική μέθοδο**, δηλαδή αλγόριθμο απόφασης, για όλες τις Διοφαντικές εξισώσεις.

Το 10ο πρόβλημα του Hilbert II

Με χρήση του θεωρήματος Lagrange (κάθε φυσικός είναι άθροισμα τεσσάρων τετραγώνων), μπορεί να δείξει κανείς ότι τα εξής δύο προβλήματα απόφασης ανάγονται το ένα στο άλλο (είναι **ισοδύναμα** ως προς $\equiv_m$):

- Επιλυσιμότητα Διοφαντικής εξίσωσης με *ακεραίους*.
- Επιλυσιμότητα Διοφαντικής εξίσωσης με *φυσικούς*.

Θεώρημα (DMPR)

Το 10ο πρόβλημα του Hilbert είναι **μη επιλύσιμο**.

Και μάλιστα κατασκευαστικά:

Θεώρημα

Υπάρχει αλγόριθμος που, δεδομένου αλγορίθμου A που δήθεν επιλύει το 10ο πρόβλημα του Hilbert, κατασκευάζει Διοφαντική εξίσωση αντιπαράδειγμα.

Δηλαδή υπάρχει $\leqslant_m$-αναγωγή, άρα το πρόβλημα είναι RE-πλήρες.

Εικασία Davis I

Ας θεωρήσουμε οικογένειες από παραμετρικές Διοφαντικές εξισώσεις:

$$D(x_1, \ldots, x_m, a_1, \ldots, a_n) = 0,$$

- ακέραιοι συντελεστές
- παράμετροι $a_1, \ldots, a_n$
- άγνωστοι $x_1, \ldots, x_m$.

Για ποιες τιμές των παραμέτρων a_i έχει η D ακέραιες ρίζες;

Εικασία Davis II

Ορισμός

Διοφαντικό σύνολο:
$\{(a_1, \dots, a_n) \mid \exists (x_1, \dots, x_m) \colon D(x_1, \dots, x_m, a_1, \dots, a_n) = 0\}$,
όπου D: Διοφαντική εξίσωση με ακέραιους συντελεστές.

Παράβαλε *αναδρομικά αριθμήσιμο σύνολο:*

$$\{(a_1, \dots, a_n) \mid \exists (x_1, \dots, x_m) \colon f(x_1, \dots, x_m, a_1, \dots, a_n) = 0\},$$

όπου f: αναδρομική συνάρτηση.

Παρατήρηση

Αν η συνάρτηση D στο ορισμό του διοφαντικού συνόλου είναι ένα πολυώνυμο ως προς τους αγνώστους $x_1, x_2, \dots, x_m$ τότε το σύνολο ονομάζεται **πολυωνυμικά** διοφαντικό σύνολο.
Αν στη συνάρτηση D επιτρέπεται να υπάρχει άγνωστη μεταβλητή $(x_1, \dots, x_m)$ σε εκθέτη, τότε το σύνολο ονομάζεται **εκθετικά** διοφαντικό.

Εικασία Davis III

Παράδειγμα

NQ $= \{n \mid n$ όχι τέλειο τετράγωνο$\}$ είναι διοφαντικό σύνολο διότι
NQ $= \{d \mid \exists(x,y): x^2 - d(y+1)^2 - 1 = 0\}$ (εξίσωση του Pell).

Προφανώς κάθε Διοφαντικό σύνολο είναι (καταγράψιμο) αναδρομικά αριθμήσιμο.

Παρατήρηση

Και οι δύο κλάσεις D και RE είναι κλειστές ως προς ένωση και τομή όχι όμως ως προς συμπλήρωμα.

Εικασία Davis IV

Εικασία (Davis, 1950)

Κάθε αναδρομικά αριθμήσιμο σύνολο είναι διοφαντικό.

Martin Davis

Εικασία Davis V

Μία συνέπεια αυτής της εικασίας είναι ότι το σύνολο PRIMES είναι διοφαντικό, άρα περιγράφεται με μια πολυωνυμική εξίσωση! Το ίδιο ισχύει και για το σύνολο POWERS-OF-2.

Μια άλλη συνέπεια ("Davis Normal Form", παράβαλε KNF) είναι η ύπαρξη καθολικής (universal) Διοφαντικής εξίσωσης $[U_n(\underline{a}, k, \underline{y}) = 0]$ που περιγράφει (με index k) κάθε r.e. σύνολο:

$$\forall D, \exists k, \forall \underline{a}\ [\exists \underline{x} D(\underline{a}, \underline{x}) = 0 \leftrightarrow \exists \underline{y} (U_n(\underline{a}, k, \underline{y}) = 0]$$

Εικασία Davis VI

Ο Martin Davis απέδειξε αμέσως:

Θεώρημα (Davis Normal Form)

Κάθε r.e. σύνολο περιγράφεται:

$$\{\underline{a} | \exists z, \forall y \leqslant z, \exists \underline{x}\ p(\underline{a}, \underline{x}, y, z) = 0\}$$

δηλαδή το σύνολο των παραμέτρων $\underline{a}$ ώστε όλα τα πολυώνυμα

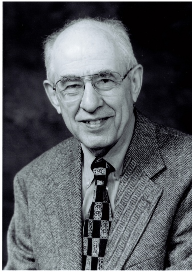
$$p(\underline{a}, \underline{x}, 0, z), p(\underline{a}, \underline{x}, 1, z), \ldots, p(\underline{a}, \underline{x}, z, z)$$

να έχουν ρίζα.

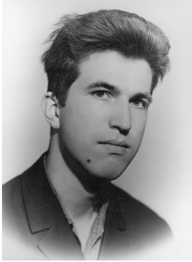
Το ζητούμενο τώρα ήταν να απαλειφθεί ο καθολικός ποσοδείκτης για να αποδειχτεί η εικασία Davis. Αυτό έγινε μετά από τουλάχιστον 20 χρόνια.

J. Robinson, H. Putnam, Y. Matiyasevich I

Julia Robinson



Hilary Putnam



Yuri Matiyasevich

J. Robinson, H. Putnam, Y. Matiyasevich II

Εικασία (J. Robinson)

Υπάρχει διοφαντικό σύνολο ζευγαριών D τέτοιο ώστε:

1. $(a, b) \in D : b \leqslant a^a$ *και*
2. $\forall k, \exists (a, b) \in D : b > a^k$

Ορισμός

Το σύνολο $D = \{(a, b, c) \mid a = b^c\}$ ονομάζεται **σχέση εκθετικής αυξητικότητας** ή σχέση Julia Robinson.
Παρατήρηση: Μέχρι την δεκαετία 1960 δεν ήταν γνωστό στους αριθμοθεωρητικούς αν υπάρχει τέτοιο σύνολο D.

Η Julia Robinson (μαθήτρια του Tarski στο Berkeley) που μελετούσε την διοφαντικότητα του συνόλου POWERS-OF-2 απέδειξε το 1950 ότι η εικασία J. Robinson *συνεπάγεται* ότι η σχέση εκθετικής αυξητικότητας είναι διοφαντικό σύνολο.

Εικασία (PAP)

Υπάρχουν αριθμητικές πρόοδοι πρώτων αριθμών, αυθαιρέτου μήκους.

J. Robinson, H. Putnam, Y. Matiyasevich III

O Davis μαζί με τον φιλόσοφο (Harvard) Hilary Putnam μελέτησαν εκθετικές διοφαντικές εξισώσεις (π.χ. $(x+1)^a + (y+1)^a = (z+1)^a$, Fermat: μόνον για $a = 1, 2$) και έδειξαν το 1959 ότι:

εικασία PAP + εικασία J. Robinson ⇒ εικασία Davis

Δυστυχώς η εικασία PAP δεν είχε αποδειχτεί τότε. Όμως η J. Robinson κατόρθωσε να αντικαταστήσει την εικασία PAP με κάτι σχετικό με το θεώρημα πρώτων αριθμών.

Παρατήρηση

Η εικασία PAP απεδείχθει το 2004 από τους Ben Green και Terence Tao και ως εκ τούτου είναι πλέον γνωστή με την ονομασία Θεώρημα Green-Tao.

J. Robinson, H. Putnam, Y. Matiyasevich IV

Έτσι, έχουμε:

Θεώρημα (DPR)

1. *Κάθε r.e. σύνολο είναι εκθετικά διοφαντικό.*
2. *Η εικασία J. Robinson είναι ισοδύναμη με: Κάθε r.e. σύνολο είναι (πολυωνυμικά) διοφαντικό.*

Παρατήρηση

Η εικασία J.R. είναι ισοδύναμη με: $\{(a, b, a^b)\}$ είναι (πολυωνυμικά) διοφαντικό.

Τέλος, ο (νεαρός, 22 ετών) Yuri Matiyasevich απέδειξε το 1970 την εικασία της J. Robinson. Έδειξε δηλαδή ότι υπάρχει σχέση που ορίζει ακριβώς την εκθετική αυξητικότητα της J. Robinson και μάλιστα η σχέση είναι

$$\{(a, b) \mid b = Fib_{2a}\}.$$

Χρησιμοποίησε μια ιδιότητα των αριθμών Fibonacci που αυτός απέδειξε:

$$Fib_n^2 | Fib_m \rightarrow Fib_n | m.$$

J. Robinson, H. Putnam, Y. Matiyasevich V

Παρατίθενται πιο ισχυρές παραλλαγές του θεωρήματος DMPR.

Θεώρημα

Υπάρχει Διοφαντική εξίσωση W με μία παράμετρο a: $W(a, \underline{x}) = 0$ έτσι ώστε το $\{a \mid \exists \underline{x} \in N^m : W(a, \underline{x}) = 0\}$ είναι μη επιλύσιμο.

Θεώρημα

Εκτός από την παραπάνω W υπάρχει αλγόριθμος που για κάθε αλγόριθμο f μας βρίσκει ένα a_f έτσι ώστε ο f να μην αποφασίζει σωστά αν η $W(a_f, \underline{x})$ έχει ρίζα.

Γενικεύσεις I

Παρατήρηση

Αν το 10ο πρόβλημα του Hilbert είχε θετική επίλυση για ακέραιους τότε θα είχε και για ρητούς. Τώρα όμως παραμένει ανοικτό το πρόβλημα για ρητούς.

- Το θεώρημα DMPR έδωσε "αρνητική" λύση στο διάσημο 10ο Πρόβλημα του Hilbert, είναι η πιο σημαντική εφαρμογή της Λογικής στα κλασικά μαθηματικά, και ώθησε τη δημιουργία μιας καινούριας ερευνητικής περιοχής: HTP, από το αγγλικό Hilbert's Tenth Problem.
- Τα βασικά προβλήματα της HTP είναι η αποκρισιμότητα των θεωριών για δομές που προκύπτουν με φυσικό τρόπο στην Άλγεβρα, τη Θεωρία Αριθμών και την Αλγεβρική Γεωμετρία.
- Χαρακτηριστικό της HTP είναι ότι οι αποδείξεις δεν είναι απλές, και τείνουν να χρησιμοποιούν αποτελέσματα και μεθόδους από κλασικά μαθηματικά, έξω από τη Λογική. Και όμως, τα αποτελέσματα Θεωρίας Αριθμών που απαιτούνται για την απόδειξη του DMPR είναι σχετικά απλά —κλασικές ιδιότητες της εξίσωσης Pell.
- Από την άλλη μεριά, το ανάλογο ερώτημα για τη δομή των ρητών αριθμών έχει αντισταθεί στις προσπάθειες πολλών διακεκριμένων μαθηματικών (από πολλούς, συναφείς κλάδους) και παραμένει το βασικό ανοικτό πρόβλημα αυτής της περιοχής:

  Υπάρχει αλγόριθμος που να αποφασίζει αν το τυχαίο πολυώνυμο με ρητούς συντελεστές έχει ρητές λύσεις;

Γενικεύσεις ΙΙ

- Έτσι η περιοχή HTP είναι ευλογημένη από ένα κλασικό θεώρημα (το DMPR), και ένα κεντρικό και (κατά γενική ομολογία) πολύ δύσκολο ανοικτό πρόβλημα και χαρακτηρίζεται από το γεγονός ότι είναι κάπου ανάμεσα στη Λογική, τη Θεωρία Αριθμών και την Αλγεβρική Γεωμετρία.