ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ

Μια ανασκόπηση του 10ου Προβλήματος του Hilbert

Hilbert 1900

10. Entscheidung der Losbarkeit einer diophantischen Gleichung. Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlkoefficienten sei vorgelegt: man soll ein Verfahren angeben, nach welchen sich mittels einer endlichen Anzahl von Operationen entscheiden lässt, ob die Gleichung in ganzen rationalen Zahlen losbar ist.

Αλέξανδρος Συγκελάκης
(ags@math.uoc.gr)
Επιβλέπων Καθηγητής : Αθανάσιος Φειδάς

Ηράκλειο 2005

Μία ανασκόπηση της απόδειξης του $10^{ου}$ Προβλήματος του Hilbert

Αλέξανδρος Γ. Συγκελάκης *

29 Νοεμβρίου 2005

Περίληψη

Το 10^o πρόβλημα του Hilbert ήταν, όπως λέει και το όνομά του, το 10^o στη σειρά των 23ών προβλημάτων που έθεσε ο Hilbert στο Παγκόσμιο συνέδριο Μαθηματικών το 1900.Το πρόβλημα ήταν: «Να βρεθεί ενας υπολογιστικός αλγόριθμος[1], ο οποίος θα αποφαίνεται, εαν μία δοσμένη διοφαντική εξίσωση με ακέραιους συντελεστές έχει ή όχι λύση στους ακεραίους.» Ο Matiyasevič έδειξε με ένα αρθρο του το 1970, οτι τέτοιος αλγόριθμος **δεν** υπάρχει. Για την ακρίβεια των πραγμάτων, ολοκλήρωσε την προσπάθεια που είχαν ξεκινήσει νωρίτερα άλλοι Μαθηματικοί.

Ας κάνουμε όμως, μία σύντομη ιστορική αναδρομή στο Πρόβλημα, για να δούμε την δουλειά των υπολοίπων μαθηματικών που ασχολήθηκαν με το 10^o πρόβλημα του Hilbert, μέχρι τον Matiyasevič που ολοκλήρωσε την απόδειξη:

1900: Ο Hilbert θέτει το 10^o πρόβλημα, μεταξύ των 23ών συνολικά που έθεσε. «Προβλήματα, από την συζήτηση των οποίων, θα προκύψει πρόοδος της επιστήμης των Μαθηματικών»

1930: Εισάγεται η έννοια της Υπολογισιμότητας και των αλγορίθμων. Σε αυτό συντελούν οι K. Gödel, A. Church, Stephen Kleene, Alan Turing.

1931: Επινόηση από τον Alan Turing της Παγκόσμιας Μηχανής Turing και ανακάλυψη των βασικών άλυτων προβλημάτων.

1953: Ο Martin Davis, δείχνει ότι οι Φραγμένοι Ποσοδείκτες μπορούν να εξαλειφθούν, συνεπώς κάθε αναδρομικώς απαριθμήσιμο σύνολο S, μπορεί να οριστεί ως:

$$S = \{x|(\exists\ y)(\forall\ k)_{\leq y}(\exists\ y_1, \ldots, y_m)[P(k, x, y, y_1, \ldots, y_m) = 0]\}$$

1950: Εικασία της Julia Robinson: Υπάρχει Διοφαντικό σύνολο D τέτοιο ώστε:

1. $(u, v) \in D$ δίνει $v \leq u^u$
2. Για κάθε k, υπάρχει $(u, v) \in D$ τέτοιο ώστε $v > u^k$

*Τμήμα Μαθηματικών, Πανεπιστήμιο Κρήτης

[1]Με την σημερινή έννοια του όρου

1970: Ο Matiyasevič, αποδεικνύει την εικασία της Julia Robinson, χρησιμοποιώντας τους αριθμούς Fibonacci. Συγκεκριμένα,

$$(\tfrac{5}{4})^n < a_n < 2^{n-1} \ \ \forall n \geq 3,$$

όπου a_n, ο n-οστός αριθμός Fibonacci που ορίζεται αναδρομικά ως εξής:

$$a_1 = a_2 = 1 \text{ και } a_{n+1} = a_n + a_{n-1}.$$

Τότε η συνάρτηση a_{2n} είναι Διοφαντική και το σύνολο :

$$D = \{(u, v) | v = a_{2u} \wedge u \geq 2\},$$

ικανοποιεί τις συνθήκες στην εικασία της Julia Robinson.

1 Διοφαντικά Σύνολα και Συναρτήσεις (Diophantine Sets and Functions)

Περίληψη

Στο πρώτο αυτό μέρος της παρουσίασης, θα δώσουμε τους ορισμούς του **Διοφαντικού Συνόλου** και της **Διοφαντικής Συνάρτησης** με κάποια πολύ απλά παραδείγματα για να γίνουν κατανοητά, μια και με αυτά θα ασχοληθούμε στο σύνολο της παρουσίασης αυτής.

Ορισμός 1.1 *Ένα σύνολο S διατεταγμένων n-άδων θετικών ακεραίων αριθμών λέγεται **Διοφαντικό**, εαν υπάρχει πολυώνυμο $P(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m)$, με $m \geq 0$, με ακέραιους συντελεστές, ώστε $(x_1, x_2, \ldots, x_n) \in S$ αν-ν [2] υπάρχουν θετικοί ακέραιοι $y_1, y_2, \ldots, y_m$ για τους οποίους $P(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) = 0$.*

Από τη Λογική δανειζόμαστε τα σύμβολα «$\exists$» για το « για κάθε » και το « $\Longleftrightarrow$ » για το « αν-ν » και έτσι η σχέση μεταξύ του συνόλου S και του πολυωνύμου P, μπορεί να γραφεί σύντομα ως εξής :

$$(x_1, x_2, \ldots, x_n) \in S \iff (\exists\, y_1, y_2, \ldots, y_m)[P(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m)]$$

ή ισοδύναμα :

$$S = \{(x_1, x_2, \ldots, x_n) | (\exists\, y_1, y_2, \ldots, y_m)[P(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m)]\}$$

Τα παρακάτω σύνολα είναι Διοφαντικά:

Παράδειγμα 1.1

(i) *Το σύνολο των αριθμών που δεν είναι δυνάμεις του 2:*

[2] Έτσι θα συμβολίζουμε από εδώ και πέρα το «αν και μόνο αν»

$$x \in S \iff (\exists\, y, z)[x = y(2z+1)],$$

(ii) *Το σύνολο των σύνθετων αριθμών:*

$$x \in S \iff (\exists\, y, z)[x = (y+1)(z+1)],$$

(iii) *Το σύνολο* W *των* 3*-άδων* (x, y, z) *για τις οποίες* x/y *και* $x < z$*:*

$$x/y \iff (\exists\, u)(y = xu) \text{ και } x < z \iff (\exists\, v)(z = x + v)$$
$$\text{Συνεπώς, } (x, y, z) \in W \iff (\exists\, u, v)[(y - xu)^2 + (z - x - v)^2 = 0]$$ [3]

Ορισμός 1.2 *Μία συνάρτηση* f*,* n*-μεταβλητών καλείται* ***Διοφαντική****, εαν το σύνολο* $\{(x_1, x_2, \ldots, x_n, y) | y = f(x_1, x_2, \ldots, x_n)\}$ *είναι Διοφαντικό (δηλαδή είναι Διοφαντική εαν το γράφημά της είναι Διοφαντικό)*

Παράδειγμα 1.2 *Μία πολύ σημαντική Διοφαντική συνάρτηση είναι εκείνη που αναφέρεται στους τριγωνικούς αριθμούς, δηλαδή αριθμούς της μορφής:*

$$T(n) = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

Καθώς η $T(n)$ *είναι γνησίως αύξουσα συνάρτηση, για κάθε θετικό ακέραιο* z*, υπάρχει μοναδικό* $n \geq 0$ *ώστε*

$$T(n) < z \leq T(n+1) = T(n) + n + 1$$

συνεπώς κάθε z *μπορεί να γραφεί με μοναδικό τρόπο ως :*

$$z = T(n) + y, \text{ με } y \leq n + 1$$

Αφού όμως $y \leq n + 1$*, υπάρχει* $x \geq 1$ *τέτοιο ώστε* $y + x - 1 = n + 1$ *δηλαδή* $n = x + y - 2$*, οπότε το* z *γράφεται με μοναδικό τρόπο στη μορφή:*

$$z = T(x + y - 2) + y$$

[3] Ας σημειωθεί ότι η παραπάνω τεχνική μπορεί να γενικευθεί. Άρα για να ορίσουμε ένα Διοφαντικό σύνολο, μπορούμε να χρησιμοποιήσουμε το ισοδύναμο σύστημα $P_1 = 0, P_2 = 0, \ldots, P_k = 0$ πολυωνυμικών εξισώσεων αφού αυτό μπορεί να αντικατασταθεί από το ισοδύναμο με μία εξίσωση: $P_1^2 + P_2^2 + \cdots + P_k^2 = 0$

Εαν λοιπόν θέσουμε $x = L(z), y = R(z)$, και $P(x, y) = T(x + y - 2) + y$, τότε οι $L(z), R(z)$ και $P(x, y)$ είναι Διοφαντικές συναρτήσεις καθώς:

$$\begin{aligned} z = P(x,y) &\iff 2z = (x+y-2)(x+y-1) + 2y \\ x = L(z) &\iff (\exists\, y)[2z = (x+y-2)(x+y-1) + 2y] \\ y = R(z) &\iff (\exists\, x)[2z = (x+y-2)(x+y-1) + 2y] \end{aligned}$$

Η συνάρτηση $P(x, y)$ απεικονίζει το σύνολο των διατεταγμένων ζευγών θετικών ακεραίων ένα προς ένα στο σύνολο των θετικών ακεραίων. Αντίστροφα, για κάθε z, το διατεταγμένο ζεύγος που απεικονίζεται στο z μέσω της $P(x, y)$ είναι το $(R(z), L(z))$. Ας σημειωθεί ότι $L(z) \leq z$, και $R(z) \leq z$. Συνοψίζοντας, έχουμε το παρακάτω θεώρημα :

Θεώρημα 1.1 ***(Pairing Function Theorem)***

Υπάρχουν Διοφαντικές συναρτήσεις $P(x, y), L(z), R(z)$ τέτοιες ώστε:
(i) *Για κάθε $x, y, L(P(x, y)) = x, R(P(x, y)) = y$, και*
(ii) *Για κάθε $z, P(L(z), R(z)) = z, L(z) \leq z, R(z) \leq z$*

Ένα πολύ ενδιαφέρον επίσης παράδειγμα Διοφαντικής συνάρτησης, συσχετίζεται με το *Κινέζικο Θεώρημα Υπολοίπων* το οποίο αναφέρεται παρακάτω:

Ορισμός 1.3 *Οι αριθμοί $m_1, m_2, \ldots, m_N$ ονομάζονται* ***αποδεκτή ακολουθία σχετικά πρώτων****, εαν για $i \neq j$, έχουμε $(m_i, m_j) = 1$.*

Θεώρημα 1.2 (Κινέζικο Θεώρημα Υπολοίπων) *Έστω $a_1, a_2, \ldots, a_N$ τυχαίοι θετικοί ακέραιοι και έστω $m_1, m_2, \ldots, m_N$ μία αποδεκτή ακολουθία σχετικά πρώτων. Τότε υπάρχει x ώστε:*

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\cdots\cdots\cdots \\ x &\equiv a_N \mod m_N \end{aligned}$$

□

Εστω τώρα η συνάρτηση $S(i, u)$ η οποία ορίζεται ως εξής:

$$S(i, u) = w$$

όπου w είναι ο μοναδικός θετικός ακέραιος για τον οποίο:

$$\begin{aligned} w &\equiv L(u) \mod (1 + iR(u)) \\ w &\leq 1 + iR(u) \end{aligned}$$

δηλαδή ο w είναι το ελάχιστο θετικό υπόλοιπο της διαίρεσης του $L(u)$ με το $1 + iR(u)$. Τότε αποδεικνύεται το παρακάτω Θεώρημα(με χρήση του Κινέζικου Θεωρήματος Υπολοίπων καθώς επίσης και του Θεωρήματος 1.1):

Θεώρημα 1.3 ***(Sequence Number Theorem*** [4]***)*** *Υπάρχει μία Διοφαντική συνάρτηση $S(i, u) = w$ τέτοια ώστε:*

(i)$S(i, u) \leq u$, *και*

(ii) *Για κάθε ακολουθία $a_1, a_2, \ldots, a_N$, υπάρχει αριθμός u τέτοιος ώστε:*

$$S(i, u) = a_i, \text{ για } 1 \leq i \leq N.$$

Ένα πολύ όμορφο χαρακτηριστικό των Διοφαντικών συνόλων θετικών ακεραίων δίνεται από το παρακάτω θεώρημα:

Θεώρημα 1.4 *Ένα σύνολο S θετικών ακεραίων είναι Διοφαντικό, αν-ν υπάρχει πολυώνυμο P, τέτοιο ώστε το S να είναι* ***ακριβώς****, το σύνολο των* ***θετικών*** *ακεραίων του πεδίου τιμών του πολυωνύμου P.*

2 24 Βοηθητικά Λήμματα

Το δυσκολότερο κομμάτι της εργασίας, είναι να δείξουμε οτι η εκθετική συνάρτηση $h(n, k) = n^k$ είναι Διοφαντική. Αυτό θα ολοκληρωθεί στην επόμενη παράγραφο. Σε αυτό το κομμάτι θα επεκτείνουμε τις μεθόδους που χρειαζόμαστε, χρησιμοποιώντας την γνωστή **εξίσωση του Pell**:

$$\begin{array}{ccc} x^2 - dy^2 = 1 & , & \text{με } x, y \geq 0, \\ & \text{όπου} & \\ d = a^2 - 1 & , & \text{με } a > 1. \end{array} \tag{2.1}$$

Οι προφανείς λύσεις της παραπάνω είναι:

$$\begin{array}{ll} x = 1 & y = 1 \\ x = a & y = 1 \end{array}$$

Λήμμα 2.1 *Δεν υπάρχουν ακέραιοι x, y οι οποίοι να ικανοποιούν την εξίσωση (2.1), για τους οποίους*

$$1 < x + y\sqrt{d} < a + \sqrt{d}.$$

Λήμμα 2.2 *Έστω x, y και x', y' ακέραιοι οι οποίοι να ικανοποιούν την εξίσωση (2.1), και x'', y'' έτσι ώστε:*

$$x'' + y''\sqrt{d} = (x + y\sqrt{d})(x' + y'\sqrt{d}).$$

[4]Από εδώ και στο εξής, θα το χρησιμοποιούμε ως S.N.T.

Τότε οι x'', y'' ικανοποιούν επίσης την εξίσωση (2.1).

Ορισμός 2.1 *Έστω* $n \geq 0,\ a > 1$. *Τότε ορίζουμε* $x_n(a), y_n(a)$ *τέτοια ώστε*

$$x_n(a) + y_n(a)\sqrt{d} = (a + \sqrt{d})^n$$

Λήμμα 2.3 *Τα* x_n, y_n, *με τον τρόπο που ορίστηκαν παραπάνω ικανοποιούν την εξίσωση (2.1).*

Λήμμα 2.4 *Έστω* x, y *μή αρνητικές λύσεις της εξίσωσης (2.1). Τότε για κάποιο* n, *έχουμε* $x = x_n$ *και* $y = y_n$.

Λήμμα 2.5 $x_{m\pm n} = x_m x_n \pm d y_n y_m$ *και* $y_{m\pm n} = x_n y_m \pm x_m y_n$

Λήμμα 2.6 $y_{m\pm 1} = a y_m \pm x_m$ *και* $x_{m\pm 1} = a x_m \pm d y_m$

Λήμμα 2.7 $(x_n, y_n) = 1$

Λήμμα 2.8 y_n / y_{nk}

Λήμμα 2.9 $y_n / y_t \iff n/t$

Λήμμα 2.10 $y_{nk} \equiv k\, x_n^{k-1}\, y_n \mod (y_n)^3$

Λήμμα 2.11 $y_n^2 / y_{n y_n}$

Λήμμα 2.12 *Εαν* y_n^2 / y_t *τότε* y_n / t

Λήμμα 2.13 $x_{n+1} = 2a x_n - x_{n-1}$ *και* $y_{n+1} = 2a y_n - y_{n-1}$

Λήμμα 2.14 $y_n \equiv n \mod (a-1)$

Λήμμα 2.15 *Εαν* $a \equiv b \mod c$, *τότε για όλα τα* n *ισχύει,*

$$x_n(a) \equiv x_n(b), y_n(a) \equiv y_n(b) \mod c$$

Λήμμα 2.16 *Εαν το* n *είναι άρτιος, τότε και το* y_n *είναι άρτιος και οταν το* n *είναι περιττός, τότε και το* y_n *είναι περιττός.*

Λήμμα 2.17 $x_n(a) - y_n(a)(a-y) \equiv y^n \mod (2ay - y^2 - 1)$.

Λήμμα 2.18 *Για κάθε* n, *ισχύει* $y_{n+1} > y_n \geq n$.

Λήμμα 2.19 *Για κάθε* n, *ισχύει* $x_{n+1}(a) > x_n(a) \geq a^n$.

Λήμμα 2.20 $x_{2n\pm j} \equiv -x_j \mod x_n$.

Λήμμα 2.21 $x_{4n\pm j} \equiv x_j \mod x_n$.

Λήμμα 2.22 *Έστω* $x_i \equiv x_j \mod x_n$, *με* $i \leq j \leq 2n, n > 0$. *Τότε* $i = j$, *εκτός εαν* $a = 2, n = 1, i = 0$ *και* $j = 2$.

Λήμμα 2.23 *Έστω* $x_j \equiv x_i \mod x_n$, *με* $n > 0, 0 < i \leq n$ *και* $0 \leq j < 4n$. *Τότε είτε* $j = i$, *είτε* $j = 4n - i$.

Λήμμα 2.24 *Εαν* $0 < i \leq n$ *και* $x_j \equiv x_i \mod x_n$, *τότε* $j \equiv \pm i \mod 4n$.

3 Η εκθετική συνάρτηση είναι Διοφαντική

Έστω το σύστημα των Διοφαντικών εξισώσεων:

1. $x^2 - (a^2-1)y^2 = 1$
2. $u^2 - (a^2-1)v^2 = 1$
3. $s^2 - (b^2-1)t^2 = 1$
4. $v = ry^2$
5. $b = 1 + 4py = a + qu$
6. $s = x + cu$
7. $t = k + 4(d-1)y$
8. $y = k + e - 1$

Θεώρημα 3.1 *Για δοσμένα* $a,\ x,\ k,\ \ a > 1$, *το σύστημα των εξισώσεων* $(1)-(8)$, *έχει λύση ως προς τις υπόλοιπες μεταβλητές* $y,\ u,\ v,\ s,\ t,\ b,\ r,\ p,\ q,\ c,\ d,\ e$ *αν-ν* $x = x_k(a)$.

Απόδειξη: Ας θεωρήσουμε αρχικά, μία λύση του συστήματος $(1)-(8)$. Από την (5), έχουμε $b > a > 1$. Τότε οι $(1),(2),(3)$ δίνουν (Λήμμα 2.4) την ύπαρξη $i,j,n > 0$ τέτοιων ώστε

$$x = x_i(a),\ y = y_i(a),\ u = x_n(a),\ v = y_n(a),\ s = x_j(b),\ t = y_j(b).$$

Από την (4), $y \le v$ δηλαδή $i \le n$. Από τις $(5),(6)$ παίρνουμε τις ισοτιμίες

$$b \equiv a \mod x_n(a) \text{ και } x_j(b) \equiv x_i(a) \mod x_n(a)$$

και από το Λήμμα 2.15 παίρνουμε $x_j(b) \equiv x_j(a) \mod x_n(a)$.
Άρα, $x_i(a) \equiv x_j(a) \mod x_n(a)$.
Από το Λήμμα 2.24 έχουμε :

$$j \equiv \pm i \mod 4n \tag{3.1}$$

Από την άλλη, η εξίσωση (4) δίνει : $(y_i(a))^2/y_n(a)$
συνεπώς από το Λήμμα 2.12 παίρνουμε $y_i(a)/n$ και η (3.1) δίνει :

$$j \equiv \pm i \mod 4y_i(a). \tag{3.2}$$

Από την εξίσωση (5), $b \equiv 1 \mod 4y_i(a)$,
άρα από το Λήμμα 2.14,

$$y_j(b) \equiv j \mod 4y_i(a). \tag{3.3}$$

Από την εξίσωση (7),

$$y_j(b) \equiv k \mod 4y_i(a). \tag{3.4}$$

Συνδιάζοντας τις (3.2), (3.3), (3.4) παίρνουμε,

$$k \equiv \pm i \mod 4y_i(a). \tag{3.5}$$

Η εξίσωση (8) δίνει, $k \leq y_i(a)$
και από το Λήμμα 2.18, $i \leq y_i(a)$.
Συνεπώς, αφού οι αριθμοί

$$-2y + 1,\ -2y + 2,\ \ldots,\ -1,\ 0,\ 1,\ \ldots,\ 2y$$

αποτελούν ένα πλήρες σύστημα υπολοίπων modulo $4y = 4y_i(a)$, οι ανισότητες αυτές δείχνουν ότι η (3.5) δίνει $k = i$

$$\text{Άρα } x = x_i(a) = x_k(a).$$

Αντίστροφα τώρα, έστω $x = x_k(a)$ και ας πάρουμε $y = y_k(a)$ ώστε να ισχύει η (1). Έστω $m = 2ky_k(a)$ και έστω $u = x_m(a), v = y_m(a)$. Τότε ικανοποιείται η (2). Από τα Λήμματα 2.9 και 2.11 έχουμε y^2/v. Οπότε μπορούμε να διαλέξουμε κάποιο r ώστε να ικανοποιείται η (4). Επιπλέον, από το Λήμμα 2.16, ο v είναι άρτιος δηλαδή ο u είναι περιττός. Από το Λήμμα 2.7 $(u, v) = 1$ άρα $(u, v, 4y) = 1$. [5] Άρα από το Κινέζικο Θεώρημα Υπολοίπων μπορούμε να βρούμε

$$b_0 \equiv 1 \mod 4y$$
$$b_0 \equiv a \mod u.$$

Το $b_0 + 4juy$ θα ικανοποιεί επίσης τις παραπάνω ισοτιμίες συνεπώς μπορούν να βρεθούν b, p, q τα οποία να ικανοποιούν την (5). Η (3) ικανοποιείται θέτοντας $s = x_k(b), t = y_k(b)$. Αφού $b > a$ έχουμε $s = x_k(b) > x_k(a) = x$. Από το Λήμμα 2.15 (χρησιμοποιώντας την (5)), $s \equiv x \mod u$. Άρα μπορούμε να διαλέξουμε κάποιο c που να ικανοποιεί την (6). Από το Λήμμα 2.18, $t \geq k$ και από το Λήμμα 2.14, $t \equiv k \mod (b-1)$, συνεπώς χρησιμοποιώντας την (5), $t \equiv k \mod 4y$.Οπότε το d μπορεί να επιλεγεί ώστε να ικανοποιεί την (7). Χρησιμοποιώντας και πάλι το Λήμμα 2.18 έχουμε $y \geq k$, άρα η (8) ικανοποιείται εαν θέσουμε $e = y - k + 1$.

Πόρισμα 3.1 *Η συνάρτηση $g(z, k) = x_k(z + 1)$ είναι Διοφαντική.*

Απόδειξη: Με προσάρτηση της

$$a = z + 1 \tag{3.6}$$

[5] Εαν ο p είναι πρώτος διαιρέτης του u και του $4y$, τότε p/y διότι ο u είναι περιττός και συνεπώς αφού y/v έχουμε p/v

στο σύστημα των εξισώσεων $(1)-(8)$, από το παραπάνω θεώρημα, το σύστημα των (3.6), $(1)-(8)$ έχει λύση αν-ν $x = x_k(a) = g(z,k)$. Συνεπώς, μπορούμε να έχουμε ένα Διοφαντικό ορισμό της συνάρτησης g, με τον συνήθη τρόπο προσθέτοντας τα τετράγωνα των 9 πολυωνύμων.

Τελικά λοιπόν, μπορούμε να αποδείξουμε το εξής:

Θεώρημα 3.2 *Η εκθετική συνάρτηση $h(n,k) = n^k$ είναι Διοφαντική.*

Θα κάνουμε αρχικά χρήση μίας απλής ανισότητας:

Λήμμα 3.1 *Εαν $a > y^k$, τότε $2ay - y^2 - 1 > y^k$.*

Έπειτα θεωρούμε το σύστημα των εξισώσεων $(1)-(8)$ σε συνδιασμό με τις

1. $(x - y(a-n) - m)^2 = (f-1)^2(2an - n^2 - 1)^2$
2. $m + g = 2an - n^2 - 1$
3. $w = n + h = k + l$
4. $a^2 - (w^2-1)(w-1)^2 z^2 = 1$

Τότε το θεώρημα 3.2 προκύπτει άμεσα από το παρακάτω Λήμμα:

Λήμμα 3.2 *$m = n^k$ αν-ν το σύστημα των 12 εξισώσεων έχει λύση ως προς τις υπόλοιπες μεταβλητές του Θεωρήματος 3.1.*

4 Η Γλώσσα των Διοφαντικών Κατηγορημάτων

Στην προηγούμενη παράγραφο δείξαμε το Θεώρημα 3.2 και με τη βοήθειά του μπορούμε να παράγουμε νέες Διοφαντικές συναρτήσεις και σύνολα.

Παράδειγμα 4.1 *Ας θεωρήσουμε την συνάρτηση $h(u,v,w) = u^{v^w}$. Ισχυριζόμαστε ότι η h είναι Διοφαντική συνάρτηση διότι γράφεται:*

$$y = u^{v^w} \iff (\exists\, z)(y = u^z \wedge z = v^w),$$

όπου το $\wedge$ είναι το λογικό σύμβολο για το « ΚΑΙ ». Χρησιμοποιώντας το θεώρημα 3.2, υπάρχει ένα πολυώνυμο P τέτοιο ώστε:

$$\begin{aligned} y = u^z &\iff (\exists\, r_1, r_2, \ldots, r_n)[P(y,u,z,r_1,r_2,\ldots,r_n) = 0], \\ z = v^w &\iff (\exists\, s_1, s_2, \ldots, s_n)[P(z,v,w,s_1,s_2,\ldots,s_n) = 0]. \end{aligned}$$

Συνεπώς,

$$\begin{aligned} y = u^{v^w} \iff (\exists\, z, r_1, r_2, \ldots, r_n, s_1, s_2, \ldots, s_n [P^2(y,u,z,r_1,r_2,\ldots,r_n) + \\ P^2(z,v,w,s_1,s_2,\ldots,s_n) = 0]. \end{aligned}$$

Με αυτό τον τρόπο,έχοντας Διοφαντικά σύνολα και χρησιμοποιώντας τα λογικά σύμβολα $\exists$, $\wedge$ μπορούμε, να τα συνδιάσουμε και να παράγουμε παραστάσεις οι οποίες ορίζουν και πάλι ένα Διοφαντικό σύνολο.Οι παραστάσεις αυτές που προκύπτουν, λέγονται μερικές φορές και ***Διοφαντικά Κατηγορήματα***. Σε αυτή τη «γλώσσα», είναι αποδεκτό να χρησιμοποιούμε και το λογικό σύμβολο $\vee$ για το « Ή », αφού:

$$(\exists\, r_1, r_2, \ldots, r_n)[P_1 = 0] \vee (\exists\, s_1, s_2, \ldots, s_m)[P_2 = 0] \iff$$
$$(\exists\, r_1, r_2, \ldots, r_n, s_1, s_2, \ldots, s_m)[P_1 P_2 = 0]$$

Θεώρημα 4.1 *Οι παρακάτω συναρτήσεις είναι Διοφαντικές:*

1. $f(n,k) = \binom{n}{k}$
2. $g(n) = n!$
3. $h(a,b,y) = \prod_{k=1}^{y}(a+bk)$

Υπενθυμίζουμε ότι ακέραιο μέρος $[a]$, ενός ακεραίου a, είναι ο μεγαλύτερος ακέραιος ο οποίος δεν υπερβαίνει τον a. Συμβολικά:

$$[a] \leq a < [a] + 1.$$

Λήμμα 4.1 *Εαν* $0 < k \leq n$ *και* $u > 2^n$, *τότε* $\left[\frac{(n+1)^n}{u^k}\right] = \sum_{i=k}^{n} \binom{n}{i} u^{i-k}$

Λήμμα 4.2 *Εαν* $0 < k \leq n$ *και* $u > 2^n$, *τότε* $\left[\frac{(n+1)^n}{u^k}\right] \equiv \binom{n}{k} \mod u$

Λήμμα 4.3 *Η συνάρτηση* $f(n,k) = \binom{n}{k}$ *είναι Διοφαντική.*

Απόδειξη: Το παραπάνω Λήμμα ορίζει το $\binom{n}{k}$ ως τον μοναδικό θετικό ακέραιο, ισοϋπόλοιπο με τον $\left[\frac{(n+1)^n}{u^k}\right]$ modulo u και μικρότερο από u. Συνεπώς,

$$z = \binom{n}{k} \iff$$
$$(\exists\, u, v, w)(v = 2^n \ \wedge\ u > v \ \wedge\ w = \left[\frac{(n+1)^n}{u^k}\right] \ \wedge\ z \equiv w \mod u \ \wedge\ z < u).$$

Για να δούμε οτι η $f(n,k)$ είναι Διοφαντική αρκεί να δείξουμε οτι κάθε μία από τις παραπάνω παραστάσεις που χωρίζονται από το Λογικό σύμβολο $\wedge$, είναι Διοφαντικά κατηγορήματα. Η $v = 2^n$ είναι Διοφαντική από το Θεώρημα 3.2. Η ανισότητα $u > v$ είναι Διοφαντικό κατηγόρημα αφού $u > v \iff (\exists\, x)(u = v + x)$. Επίσης,

$$z \equiv w \mod u \wedge z < u \iff (\exists\, x, y)(w = z + (x-1)u \wedge u = z + y).$$

Τέλος,

$$w = \Big[\frac{(n+1)^n}{u^k}\Big]$$
$$\Longleftrightarrow$$
$$(\exists\, x, y, t)(t = u + 1 \wedge x = t^n \wedge w \leq \frac{x}{y} < w + 1),$$

και $w \leq \dfrac{x}{y} < w + 1 \iff wy \leq x < (w+1)y.$

Λήμμα 4.4 *Εαν* $r > (2x)^{x+1}$, *τότε* $x! = \Big[r^x / \binom{r}{x}\Big]$

Απόδειξη: Εαν $r > (2x)^{x+1}$, τότε

$$\begin{aligned} r^x / \binom{r}{x} &= \frac{r^x x!}{r(r-1)\cdots(r-x+1)} \\ &= x! \cdot \Big\{\frac{1}{(1-\frac{1}{r})\cdots(1-\frac{x-1}{r})}\Big\} \\ &< x! \cdot \frac{1}{(1-\frac{x}{r})^x} \end{aligned}$$

Επίσης έχουμε,

$$\begin{aligned} \frac{1}{1-\frac{x}{r}} &= 1 + \frac{x}{r} + (\frac{x}{r})^2 + \cdots \\ &= 1 + \frac{x}{r}\Big\{1 + \frac{x}{r} + (\frac{x}{r})^2 + \cdots\Big\} \\ &< 1 + \frac{x}{r}\Big\{1 + \frac{1}{2} + \frac{1}{4} + \cdots\Big\} \\ &= 1 + \frac{2x}{r} \end{aligned}$$

και,

$$\begin{aligned} \Big(1 + \frac{2x}{r}\Big)^x &= \sum_{j=0}^{x} \binom{x}{j} \Big(\frac{2x}{r}\Big)^j \\ &< 1 + \frac{2x}{r} \sum_{j=1}^{x} \binom{x}{j} \\ &< 1 + \frac{2x}{r} \cdot 2^x \end{aligned}$$

Συνεπώς,

$$\begin{aligned} r^x / \binom{r}{x} &< x! + \frac{2x}{r} \cdot x! \cdot 2^x \\ &< x! + \frac{2^{x+1} x^{x+1}}{r} \\ &< x! + 1. \end{aligned}$$

Λήμμα 4.5 *Η $n!$, είναι Διοφαντική συνάρτηση.*

Απόδειξη: $m = n! \iff (\exists\, r,s,t,u,v)\{s = 2x+1 \ \wedge\ t = x+1 \ \wedge\ r = s^t \ \wedge\ u = r^n \ \wedge\ v = \binom{r}{n} \ \wedge\ mv \le u < (m+1)v\}$.

Λήμμα 4.6 *Έστω $bq \equiv a \mod M$. Τότε,*

$$\prod_{k=1}^{y}(a+bk) \equiv b^y \cdot y! \cdot \binom{q+y}{y} \mod M.$$

Λήμμα 4.7 *Η συνάρτηση $h(a,b,y) = \prod_{k=1}^{y}(a+bk)$ είναι Διοφαντική.*

Απόδειξη: Από το Λήμμα 4.6, διαλέγω $M = b(a+by)^y + 1$. Τότε, $(M,b) = 1$ και $M > \prod_{k=1}^{y}(a+bk)$. Συνεπώς, η ισοτιμία $bq \equiv a \mod M$ είναι επιλύσιμη ως προς q, και άρα το $\prod_{k=1}^{y}(a+bk)$, ορίζεται να είναι ο μοναδικός αριθμός ο οποίος είναι ισοϋπόλοιπος modulo M με τον $b^y \cdot y! \cdot \binom{q+y}{y}$, και είναι επίσης $< M$

Άρα λοιπόν,

$$z = \prod_{k=1}^{y}(a+bk) \iff$$
$$(\exists\, M,p,q,r,s,t,u,v,w,x)\Big\{r = a+by \wedge s = r^y \wedge M = bs+1 \wedge bq = a+Mt \wedge$$
$$u = b^y \ \wedge\ v = y! \ \wedge\ z < M \ \wedge\ w = q+y \ \wedge\ x = \binom{w}{y} \ \wedge\ z + Mp = uvx\Big\}.$$

Χρησιμοποιώντας τις προηγούμενες παραστάσεις για την εκθετική συνάρτηση, για $v = y!$ και για $x = \binom{w}{y}$, παίρνουμε το ζητούμενο αποτέλεσμα.

Η απόδειξη λοιπόν του Θεωρήματος 4.1, έχει ολοκληρωθεί με την απόδειξη των Λημμάτων (4.3),(4.5) και (4.7).

5 *Φραγμένοι Ποσοδείκτες*

Η γλώσσα των Διοφαντικών κατηγορημάτων, επιτρέπει την χρήση των $\wedge, \vee, \exists$. Άλλα λογικά σύμβολα που χρησιμοποιούνται στη Λογική είναι:

- $\sim$, για το « ΟΧΙ »
- $\forall x$, για το « ΓΙΑ ΚΑΘΕ x »

- $\rightarrow$, για το « ΕΑΝ ... ΤΟΤΕ ... »

Όπως θα γίνει φανερό αργότερα, από τη χρήση αυτών των συμβόλων, μπορεί να οδηγηθούμε σε παραστάσεις που ορίζουν σύνολα τα οποία δεν είναι Διοφαντικά.

Ορίζουμε τους **υπαρξιακούς φραγμένους ποσοδείκτες**:

$$\text{« } (\exists\, y)_{\leq x} \ldots \text{ » το οποίο σημαίνει « } (\exists\, y)(y \leq x \ \wedge \ \ldots) \text{ »}$$

καθώς επίσης και τους **καθολικούς φραγμένους ποσοδείκτες**:

$$\text{« } (\forall y)_{\leq x} \ldots \text{ » το οποίο σημαίνει « } (\forall y)(y > x \ \vee \ \ldots) \text{ »}$$

Αυτοί οι τελεστές, μπορούν να προσαρτηθούν στη γλώσσα των Διοφαντικών κατηγορημάτων και τα σύνολα που ορίζονται από παραστάσεις αυτής της επεκτεταμένης γλώσσας, θα παραμείνουν Διοφαντικά. Έχουμε:

Θεώρημα 5.1 *Εαν P είναι ένα πολυώνυμο, και*

$$R = \{(y, x_1, \ldots, x_n) | (\exists\, z)_{\leq y} (\exists\, y_1, \ldots, y_m)[P(y, z, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0]\}$$

και,

$$S = \{(y, x_1, \ldots, x_n) | (\forall z)_{\leq y} (\exists\, y_1, \ldots, y_m)[P(y, z, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0]\},$$

τότε τα σύνολα R και S είναι Διοφαντικά.

Το ότι το R είναι Διοφαντικό, είναι τετριμμένο καθώς,

$$(y, x_1, \ldots, x_n) \in R \iff (\exists\, z, y_1, \ldots, y_m)(z \leq y \ \wedge \ P = 0).$$

Η απόδειξη του άλλου μισού του θεωρήματος, είναι πιο περίπλοκη. Θα εισάγουμε λοιπόν 2 βοηθητικά λήμματα, που θα βοηθήσουν στην απόδειξη.

Λήμμα 5.1 $(\forall k)_{\leq y} (\exists\, y_1, \ldots, y_m)[P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0]$
$$\iff$$
$$(\exists\, u)(\forall k)_{\leq y} (\exists\, y_1, \ldots, y_m)_{\leq u}[P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0].$$

Απόδειξη: Τό δεξί μέλος της ισοδυναμίας, τετριμμένα δίνει το αριστερό.

Για το αντίστροφο, ας υποθέσουμε ότι ισχύει το αριστερό μέλος για δοσμένα $y, x_1, \ldots, x_n$. Τότε για κάθε $k = 1, 2, \ldots, y$ υπάρχουν ορισμένοι αριθμοί $y_1^{(k)}, y_2^{(k)}, \ldots, y_m^{(k)}$ για τους οποίους:

$$P(y, k, x_1, \ldots, x_n, y_1^{(k)}, y_2^{(k)}, \ldots, y_m^{(k)}) = 0$$

Παίρνοντας το u να είναι το μέγιστο των $m \cdot y$ αριθμών

$$\{y_j^{(k)} | j = 1, \ldots, m; k = 1, 2, \ldots, y\}$$

προκύπτει οτι το δεξί μέλος της ισοδυναμίας είναι φανερό.

Λήμμα 5.2 *Έστω $Q(y, u, x_1, \ldots, x_n)$, ένα πολυώνυμο με τις ιδιότητες*

1. $Q(y, u, x_1, \ldots, x_n) > u$
2. $Q(y, u, x_1, \ldots, x_n) > y$
3. *Οι σχέσεις $k \leq y$ και $y_1, \ldots, y_m \leq u$ δίνουν*

$$|P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m)| \leq Q(y, u, x_1, \ldots, x_n)$$

Τότε,

$$(\forall k)_{\leq y}(\exists\, y_1, \ldots, y_m)_{\leq u}[P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0]$$
$$\Longleftrightarrow$$

$$\begin{aligned}
(\exists\, c, t, a_1, \ldots, a_m) \quad [\quad & 1 + ct = \prod_{k=1}^{y}(1 + kt) \\
\wedge \quad & t = Q(y, u, x_1, \ldots, x_n)! \\
\wedge \quad & 1 + ct / \prod_{j=1}^{u}(a_1 - j) \\
\wedge \quad & \cdots\cdots\cdots\cdots\cdots \\
\wedge \quad & 1 + ct / \prod_{j=1}^{u}(a_m - j) \\
\wedge \quad & P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_m) \equiv 0 \mod (1 + ct)].
\end{aligned}$$

Το σημαντικό στο Λήμμα αυτό, είναι οτι παρόλο που το δεξί μελος της ισοδυναμίας φαίνεται να είναι πιο πεπλεγμένο από το πρώτο, ωστόσο δεν περιέχει φραγμένους καθολικούς ποσοδείκτες.

Με τη βοήθεια λοιπόν αυτών των Λημμάτων, μπορούμε να ολοκληρώσουμε την απόδειξη του Θεωρήματος 5.1.

Αρχικά, βρίσκουμε ένα πολυώνυμο Q που να ικανοποιεί τα (1),(2),(3) του Λήμματος 5.1. Αυτό είναι εύκολο να γίνει :

Γράφουμε,

$$P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m) = \sum_{r=1}^{N} t_r$$

όπου κάθε t_r έχει τη μορφή,

$$t_r = |c| y^a k^b x_1^{q_1} x_2^{q_2} \cdots x_n^{q_n} y_1^{s_1} y_2^{s_2} \cdots y_m^{s_m}$$

για c θετικό ή αρνητικό ακέραιο. Θέτουμε

$$u_r = cy^{a+b}k^b x_1^{q_1}x_2^{q_2}\cdots x_n^{q_n}u^{s_1+s_2+\cdots+s_m} \text{ και έστω}$$
$$Q(y,u,x_1,\ldots,x_n) = u + y + \sum_{r=1}^{N} u_r.\ ^{6}$$

Τότε οι $(1),(2)$ και (3) του Λήμματος 5.1 ισχύουν. Ώστε:

$$(\forall k)_{\le y}(\exists\, y_1,\ldots,y_m)[P(y,k,x_1,\ldots,x_n,y_1,\ldots,y_m)=0]$$
$$\Longleftrightarrow$$

$$\begin{aligned}(\exists\, u,c,t,a_1,\ldots,a_m)\quad \Big[\quad & 1+ct=\prod_{k=1}^{y}(1+kt)\\ \wedge\quad & t=Q(y,u,x_1,\ldots,x_n)!\\ \wedge\quad & 1+ct/\prod_{j=1}^{u}(a_1-j)\\ \wedge\quad & \cdots\cdots\cdots\cdots\cdots\\ \wedge\quad & 1+ct/\prod_{j=1}^{u}(a_m-j)\\ \wedge\quad & P(y,c,x_1,\ldots,x_n,a_1,\ldots,a_m)\equiv 0 \mod (1+ct)\Big]\end{aligned}$$

$$\Longleftrightarrow$$

$$\begin{aligned}&(\exists\, u,c,t,a_1,\ldots,a_n,e,f,g_1,\ldots,g_m,h_1,\ldots,h_n,l)\Big[e=1+ct\\ \wedge\quad & e=\prod_{k=1}^{y}(1+kt)\ \wedge\ f=Q(y,u,x_1,\ldots,x_n)\ \wedge\ t=f!\\ \wedge\quad & g_1=a_1-u-1\ \wedge\ g_2=a_2-u-1\ \wedge\ \cdots\cdots\cdots\ \wedge\ g_m=a_m-u-1\\ \wedge\quad & h_1=\prod_{k=1}^{u}(g_1+k)\ \wedge\ h_2=\prod_{k=1}^{u}(g_2+k)\ \wedge\ \cdots\cdots\cdots\ \wedge\ h_m=\prod_{k=1}^{u}(g_m+k)\\ \wedge\quad & e/h_1\ \wedge\ e/h_2\ \wedge\ \cdots\cdots\ \wedge\ e/h_m\ \wedge\ l=P(y,c,x_1,\ldots,x_n,a_1,\ldots,a_n)\ \wedge\ e/l\Big]\end{aligned}$$

το οποίο, είναι Διοφαντικό από το Θεώρημα 4.1

6 *Αναδρομικές Συναρτήσεις*

Είδαμε οτι διάφορα σύνολα είναι Διοφαντικά, κάνοντας χρήση κάποιων τεχνασμάτων. Τώρα έχουμε πολύ ισχυρές μεθόδους για να δείξουμε οτι κάποιο σύνολο είναι Διοφαντικό. Η επεκτεταμένη μορφή των Διοφαντικών Κατηγορημάτων,

[6] Παρατηρούμε οτι η εύρεση του Q είναι κατασκευαστική, δηλαδή μπορούμε να κατασκευάσουμε ένα πολυώνυμο Q, που να ικανοποιεί τις ιδιότητες $(1),(2),(3)$ του Λήμματος 5.2.

με επιτρεπόμενη τη χρήση των φραγμένων ποσοδεικτών (κοίτα το Θεώρημα 5.1) και το S.N.T. (Θεώρημα 1.3), επιτρέπουν σε κάποιο να δείξει με άμεσο τρόπο, οτι σχεδόν οποιοδήποτε σύνολο θέλουμε, είναι Διοφαντικό.

Παρακάτω δίνουμε παραδείγματα άλλων δύο Διοφαντικών συνόλων:

Παράδειγμα 6.1 *Το σύνολο των πρώτων αριθμών:*

$$x \in P \iff x > 1 \wedge (\forall\, y, z)_{\leq x}[yz < x \vee yz > x \vee y = 1 \vee z = 1]$$

Ένας δεύτερος τρόπος να περιγράψουμε το σύνολο των πρώτων αριθμών είναι χρησιμοποιώντας το θεώρημα του Wilson [7].

Από το Θεώρημα 1.4, προκύπτει οτι υπάρχει κάποιο πολυώνυμο P, αναπαράστασης των πρώτων αριθμών το οποίο σημαίνει οτι ένας θετικός ακέραιος είναι πρώτος αν-ν ανήκει στο πεδίο τιμών του P [8]

Παράδειγμα 6.2 *Η συνάρτηση $g(y) = \prod_{k=1}^{y}(1+k)^2$. Εδώ χρησιμοποιούμε το S.N.T., για να «μεταφράσουμε» την ακολουθία $g(1), g(2), \ldots, g(y)$ σε ένα μόνο αριθμό u τέτοιο ώστε :*

$$S(i,u) = g(i), \quad i = 1, 2, \ldots, y$$

Συνεπώς,

$$\begin{aligned} z = g(y) \quad &\iff \quad (\exists\, u)\{S(1,u) = 2 \ \wedge\ (\forall\, k)_{\leq y}[k = 1 \ \vee\ (S(k,u) = (1+k^2)S(k-1,u))] \\ &\wedge \quad z = S(y,u)\} \\ &\iff \quad (\exists\, u)\{S(1,u) = 2 \ \wedge\ (\forall\, k)_{\leq y}[k = 1 \ \vee\ (\exists\, a,b,c)(a = k-1 \\ &\wedge \quad b = S(a,u) \ \wedge\ c = S(k,u) \ \wedge\ c = (1+k^2)b)] \ \wedge\ z = S(y,u)\} \end{aligned}$$

Γίνεται λοιπόν καθαρό τώρα, οτι οι μέθοδοι που έχουμε στη διάθεσή μας είναι γενικοί. Είναι τόσο ισχυροί που γεννιέται η ερώτηση: Πώς μπορεί κάθε «λογικό» σύνολο (ή συνάρτηση), να ξεφύγει από αυτές τις μεθόδους και άρα να μην είναι Διοφαντικό ;

Η ισχύς των μεθόδων που περιγράψαμε, μπορεί να δοκιμασθεί μελετώντας την κλάση όλων των *υπολογιστικών* ή *αναδρομικών* συναρτήσεων. Αυτές είναι οι συναρτήσεις οι οποίες μπορούν να υπολογισθούν με ένα πεπερασμένο [9] πρόγραμμα ή υπολογιστική μηχανή, η οποία υποθέτουμε οτι δεν έχει περιορισμούς όσον αφορά το πλήθος και το μέγεθος των αριθμών που θυμάται. Υπάρχουν και είναι διαθέσιμοι, πολλοί και ακριβείς ορισμοί αυτής της κλάσης[10]. Ένας από τους απλούστερους είναι ο ακόλουθος :

[7] Ένας αριθμός p είναι πρώτος, αν-ν $(p-1)! \equiv 1 \mod p$

[8] Υπάρχει τρόπος κατασκευής αυτού του πολυωνύμου και μπορεί να αναζητηθεί στο βιβλίο Diophantine representation of the set of prime numbers (Russian). Dokl. Akad. Nauk SSSR, 196 (1971) 770-773. Improved English translation with Addendum: Soviet. Math. Doklady, 12 (1971) 249-254.

[9] Δηλαδή μπορεί να γράψει, να διαβάσει κ.λ.π. πεπερασμένου πλήθους αριθμούς σε πεπερασμένο χρόνο.

[10] Όλοι είναι ισοδύναμοι μεταξύ τους.

Οι ***αναδρομικές συναρτήσεις*** είναι όλες εκείνες οι συναρτήσεις, που μπορούμε να πάρουμε από τις πρωταρχικές συναρτήσεις:

$$c(x) = 1$$
$$s(x) = x + 1$$
$$U_i^n(x_1, x_2, \ldots, x_n) = x_i, \quad 1 \leq i \leq n$$
$$S(i, u) \quad [11]$$

εφαρμόζοντας όσες φορές χρειάζεται, τις τρεις πράξεις: *σύνθεση*, *πρωταρχική αναδρομή* και *σχήμα ελαχιστοποίησης* οι οποίες ορίζονται παρακάτω:

Η ***σύνθεση***, παράγει την συνάρτηση

$$h(x_1, \ldots, x_n) = f(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n))$$

από τις δοσμένες συναρτήσεις $g_1, \ldots, g_m$ και $f(t_1, \ldots, t_m)$.

Η ***πρωταρχική αναδρομή***, παράγει την συνάρτηση $h(x_1, \ldots, x_n, z)$ η οποία ικανοποιεί τις εξισώσεις:

$$h(x_1, \ldots, x_n, 1) = f(x_1, \ldots, x_n)$$
$$h(x_1, \ldots, x_n, t+1) = g(t, h(x_1, \ldots, x_n, t)x_1, \ldots, x_n)$$

από τις δοσμένες συναρτήσεις f, g.

Όταν $n = 0$, η f γίνεται σταθερά και τότε η h παράγεται απευθείας από την g.

Με το ***σχήμα ελαχιστοποίησης***, παράγεται η συνάρτηση:

$$h(x_1, \ldots, x_n) = min_y[f(x_1, \ldots, x_n, y) = g(x_1, \ldots, x_n, y)]$$

από τις δοσμένες συναρτήσεις f, g, με την προϋπόθεση ότι οι f, g είναι τέτοιες ώστε για κάθε $x_1, \ldots, x_n$ υπάρχει τουλάχιστον ένα y που ικανοποιεί την εξίσωση: $f(x_1, \ldots, x_n, y) = g(x_1, \ldots, x_n, y)$ [12].

Το κύριο τότε αποτέλεσμα αυτού του άρθρου, είναι:

Θεώρημα 6.1 *Μία συνάρτηση είναι Διοφαντική αν-ν είναι αναδρομική.*

Για να ξεκινήσουμε την απόδειξη του παραπάνω θεωρήματος, θα δούμε κάποιες αναδρομικές συναρτήσεις:

1. Η $x + y$ είναι αναδρομική καθώς

$$x + 1 = s(x)$$
$$x + (t + 1) = s(x + t) = g(t, x + t, x),$$

όπου $g(u, v, w) = s(U_2^3(u, v, w))$.

[11] Η συνάρτηση αυτή είναι πλεονασμός καθώς μπορεί να παραχθεί από τις προηγούμενες τρεις.

[12] Δηλαδή η συνάρτηση h πρέπει να είναι παντού ορισμένη.

2. Η $x \cdot y$ είναι αναδρομική καθώς

$$x \cdot 1 = U_1^1(x)$$
$$x \cdot (t+1) = (x \cdot t) + x = g(t, x \cdot t, x),$$

όπου $g(u,v,w) = U_2^3(u,v,w) + U_3^3(u,v,w)$.

3. Για κάθε σταθερό k, η σταθερή συνάρτηση $c_k(x) = k$ είναι αναδρομική, καθώς η $c_1(x)$ είναι μία από τις πρωταρχικές συναρτήσεις και $c_{k+1}(x) = c_k(x) + c(x)$.

4. Κάθε πολυώνυμο $P(x_1, \ldots, x_n)$ με θετικούς ακέραιους συντελεστές, είναι αναδρομική συνάρτηση, καθώς μπορεί να εκφραστεί ως πεπερασμένη εφαρμογή προσθέσεων και πολλαπλασιασμών μεταβλητών και σταθερών $c(x)$. Για παράδειγμα:

$$2x^2y + 3xz^3 + 5 = c_2(x) \cdot x \cdot x \cdot y + c_3(x) \cdot x \cdot z \cdot z \cdot z + c_5(x).$$

Συνεπώς τα $(1), (2), (3)$ χρησιμοποιώντας την σύνθεση, δίνουν το αποτέλεσμα.

Τώρα είναι εύκολο να δείξουμε, οτι κάθε Διοφαντική συνάρτηση είναι αναδρομική:
Έστω f μία Διοφαντική συνάρτηση, και ας γράψουμε:

$$y = f(x_1, \ldots, x_n) \iff (\exists\, t_1, \ldots, t_m)[P(x_1, \ldots, x_n, y, t_1, \ldots, t_m) = Q(x_1, \ldots, x_n, y, t_1, \ldots, t_m)],$$

όπου P, Q είναι πολυώνυμα με θετικούς ακεραίους συντελεστές. Τότε από το S.N.T., έχουμε:

$$\begin{aligned} f(x_1, \ldots, x_n) &= S(1, min_u[P(x_1, \ldots, x_n, S(1,u), S(2,u), \ldots, S(m+1,u)) \\ &= Q(x_1, \ldots, x_n, S(1,u), S(2,u), \ldots, S(m+1,u))]). \end{aligned}$$

Αφού οι συναρτήσεις $P, Q, S(i,u)$ είναι αναδρομικές, είναι και η f (Χρησιμοποιώντας σύνθεση, και το σχήμα ελαχιστοποίησης).

Για το αντίστροφο: Η $S(i,u)$ είναι γνωστό ότι είναι Διοφαντική όπως επίσης (τετριμμένα) και όλες οι πρωταρχικές συναρτήσεις. Αρκεί λοιπόν να δείξουμε ότι οι Διοφαντικές συναρτήσεις είναι κλειστές ως προς τη σύνθεση, την πρωταρχική αναδρομή και το σχήμα ελαχιστοποίησης.

Σύνθεση: Εαν $h(x_1, \ldots, x_n) = f(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n))$ όπου οι συναρτήσεις $f, g_1, \ldots, g_m$ είναι Διοφαντικές, τότε και η h είναι Διοφαντική καθώς:

$$y = h(x_1, \ldots, x_n) \iff (\exists\, t_1, \ldots, t_m)[t_1 = g_1(x_1, \ldots, x_n) \wedge \ldots \wedge\ t_m = g_m(x_1, \ldots, x_n)\ \wedge\ y = f(t_1, \ldots, t_m)].$$

Πρωταρχική αναδρομή: Εαν,

$$h(x_1,\ldots,x_n,1) = f(x_1,\ldots,x_n)$$
$$h(x_1,\ldots,x_n,t+1) = g(t,h(x_1,\ldots,x_n,t),x_1,\ldots,x_n),$$

και οι f, g είναι Διοφαντικές [13]:

$$y = h(x_1,\ldots,x_n,z) \iff$$

$$\begin{aligned}(\exists\, u)\quad & \{(\exists\, v)[v = S(1,u)\ \wedge\ v = f(x_1,\ldots,x_n)]\\ \wedge\quad & (\forall\, t)_{\le z}[(t = z)\ \vee\ (\exists\, v)(v = S(t+1,u)\\ \wedge\quad & v = g(t,S(t,u),x_1,\ldots,x_n))]\ \wedge\ y = S(z,u)\}\end{aligned}$$

και συνεπώς χρησιμοποιώντας το Θεώρημα 5.1, η h είναι Διοφαντική.

Σχήμα ελαχιστοποίησης: Εαν,

$$h(x_1,\ldots,x_n) = \min_y[f(x_1,\ldots,x_n,y) = g(x_1,\ldots,x_n,y)],$$

όπου οι f, g είναι Διοφαντικές, τότε και η h είναι Διοφαντική καθώς,

$$y = h(x_1,\ldots,x_n) \iff$$

$$\begin{aligned}(\exists\, z)\quad & [z = f(x_1,\ldots,x_n,y)\ \wedge\ z = g(x_1,\ldots,x_n,y)]\\ \wedge\quad & (\forall\, t)_{\le y}[(t = y)\ \vee\ (\exists\, u,v)(u = f(x_1,\ldots,x_n,t)\\ \wedge\quad & v = g(x_1,\ldots,x_n,t)\ \wedge\ (u < v\ \vee\ v < u)].\end{aligned}$$

7 Καθολικό Διοφαντικό Σύνολο

Θα κάνουμε τώρα μία σαφή απαρίθμηση, όλων των Διοφαντικών συνόλων με θετικούς ακέραιους. Κάθε πολυώνυμο με θετικούς ακέραιους συντελεστές, μπορεί να κατασκευαστεί από το 1, καθώς επίσης και από μεταβλητές, με διαδοχικές προσθέσεις και πολλαπλασιασμούς. Ορίζω το αλφάβητο των μεταβλητών που χρησιμοποιώ:

$$x_0, x_1, x_2, x_3, \ldots$$

και κατόπιν, φτιάχνω την ακόλουθη απαρίθμηση όλων των πολυωνύμων που περιέγραψα παραπάνω (χρησιμοποιώντας «pairing functions»):

$$\begin{aligned}P_1 &= 1\\ P_{3i-1} &= x_{i-1}\\ P_{3i} &= P_{L(i)} + P_{R(i)}\\ P_{3i+1} &= P_{L(i)} \cdot P_{R(i)}\end{aligned}$$

με $P_i = P_i(x_0, x_1, \ldots, x_n)$, όπου ο n είναι τόσο μεγάλος ώστε όλες οι μεταβλητές που εμφανίζονται στο P_i, να συμπεριλαμβάνονται. [14]

Ας πάρουμε τώρα το σύνολο:

[13] Χρησιμοποιώντας το S.N.T. για να κωδικοποιήσουμε τους αριθμούς $h(x_1,\ldots,x_n,1), h(x_1,\ldots,x_n,2),\ldots,h(x_1,\ldots,x_n,z)$

[14] Προφανώς το P_i δεν εξαρτάται γενικά από όλες αυτές τις μεταβλητές.

$$D_n = \{x_0 | (\exists\, x_1, \ldots, x_n)[P_{L(n)}(x_0, x_1, \ldots, x_n) = P_{R(n)}(x_0, x_1, \ldots, x_n)]\}.$$

Εδώ, τα πολυώνυμα $P_{L(n)}$ και $P_{R(n)}$ δεν περιέχουν απαραίτητα όλες τις μεταβλητές $x_0, x_1, \ldots, x_n$ αλλά σίγουρα δεν περιέχουν άλλες.[15] Από τον τρόπο που έχει κατασκευαστεί η ακολουθία P_i, φαίνεται οτι η ακολουθία των συνόλων

$$D_1, D_2, D_3, D_4, \ldots,$$

περιέχει όλα τα Διοφαντικά σύνολα. Επιπλέον ισχύει:

Θεώρημα 7.1 ***(Θεώρημα της Πληρότητας)***

Το σύνολο $\{(n, x) | x \in D_n\}$ *είναι Διοφαντικό.*

Απόδειξη: Για άλλη μια φορά χρησιμοποιώντας το S.N.T., έχουμε τα εξής:

$$\begin{aligned} x \in D_n \quad \Longleftrightarrow \quad & (\exists\, u)\{S(1,u) = 1 \ \wedge \ S(2,u) = x \\ \wedge \quad & (\forall\, i)_{\leq n}[S(3i,u) = S(L(i),u) + S(R(i),u)] \\ \wedge \quad & (\forall\, i)_{\leq n}[S(3i+1,u) = S(L(i),u) \cdot S(R(i),u)] \\ \wedge \quad & S(L(n),u) = S(R(n),u)\} \end{aligned}$$

Είναι τώρα καθαρό οτι το κατηγόρημα δεξία από την ισοδυναμία είναι Διοφαντικό σύνολο, συνεπώς χρειάζεται μόνο να ελεγχθεί ο ισχυρισμός:

Έστω $x \in D_n$ για δοσμένα x, n. Τότε υπάρχουν αριθμοί $t_1, \ldots, t_n$ τέτοιοι ώστε: $P_{L(n)}(x, t_1, \ldots, t_n) = Q_{L(n)}(x, t_1, \ldots, t_n)$. Ας επιλέξουμε u (από το S.N.T.), τέτοιο ώστε:

$$S(j,u) = P_j(x, t_1, \ldots, t_n), \quad j = 1, 2, \ldots, 3n+2. \tag{7.1}$$

Ειδικότερα, $S(2,u) = x$ και $S(3i-1,u) = t_{i-1},\ i = 2, 3, \ldots, n+1$. Συνεπώς το δεξί μέλος της ισοδυναμίας ισχύει.

Αντίστροφα, ας πάρουμε το δεξί μέλος της (7.1) να ισχύει για δοσμένα n, x και έστω

$$t_1 = S(5,u), t_2 = S(8,u), \ldots, t_n = S(3n+2,u).$$

Τότε η (7.1) πρέπει να ισχύει. Καθώς $S(L(n),u) = S(R(n),u)$, πρέπει να είναι η περίπτωση όπου:

$$P_{L(n)}(x, t_1, \ldots, t_n) = P_{R(n)}(x, t_1, \ldots, t_n),$$

συνεπώς $x \in D_n$.

Αφού λοιπόν τα $D_1, D_2, \ldots,$ δίνουν μία απαρίθμηση όλων των Διοφαντικών συνόλων, είναι εύκολο να κατασκευάσουμε ένα σύνολο διαφορετικό από όλα αυτά και συνεπώς όχι Διοφαντικό.

[15] Ας θυμηθούμε οτι $L(n), R(n) \leq n$.

Αυτό είναι το:

$$V = \{n|\ n \notin D_n\}$$

Θεώρημα 7.2 *Το σύνολο* V ***δεν*** *είναι Διοφαντικό*

Απόδειξη: Είναι μία απλή εφαρμογή της διαγώνιας μεθόδου του Cantor. Εαν το V ήταν Διοφαντικό, τότε για κάποιο i, θα είχαμε $V = D_i$. Ανήκει όμως το i στο V; Έχουμε:

Αφού $V = D_i,\ i \in V \iff i \in D_i$.

Από την άλλη όμως, από τον τρόπο ορισμού του V, $i \in V \iff i \notin D_i$, άτοπο.

Θεώρημα 7.3 *Η συνάρτηση που ορίζεται από τις σχέσεις:*

$$g(n,x) = 1 \text{ , } \textit{εαν } x \notin D_n,$$
$$g(n,x) = 2 \text{ , } \textit{εαν } x \in D_n,$$

δεν είναι αναδρομική.

Απόδειξη: Εαν η συνάρτηση g, ήταν αναδρομική, τότε θα ήταν Διοφαντική (Θεώρημα 6.1) της μορφής:

$$y = g(n,x) \iff (\exists\ y_1, \ldots, y_m)[P(n,x,y,y_1,\ldots,y_m) = 0].$$

Τότε όμως, θα προέκυπτε ότι:

$$V = \{x|\ (\exists\ y_1, \ldots, y_m)[P(x,x,1,y_1,\ldots,y_m) = 0]\}$$

και το οποίο έρχεται σε αντίθεση με το Θεώρημα 7.2.

Κάνοντας χρήση του Θεωρήματος 7.1, έχουμε:

$$x \in D_n \iff (\exists\ z_1, \ldots, z_k)[P(n,x,z_1,\ldots,z_k) = 0].$$

όπου P είναι κάποιο καθορισμένο (εντούτοις όμως περίπλοκο), πολυώνυμο. Ας υποθέσουμε οτι υπήρχε ένας αλγόριθμος, που θα αποφαινόταν για την ύπαρξη ή όχι λύσεων μιας Διοφαντικής εξίσωσης, δηλαδή ένας αλγόριθμο για το 10^o πρόβλημα του Hilbert. Τότε για δοσμένα n, x, αυτός ο αλγόριθμος θα μπορούσε να χρησιμοποιηθεί για να εξετάσει εαν η εξίσωση:

$$P(n,x,z_1,\ldots,z_k) = 0,$$

έχει ή όχι λύση, δηλαδή εαν ισχύει ή δεν ισχύει ότι $x \in D_n$. Συνεπώς ο αλγόριθμος θα μπορούσε να χρησιμοποιηθεί για να υπολογίσει τη συνάρτηση $g(n,x)$. Από το γεγονός όμως ότι οι αναδρομικές συναρτήσεις είναι μόνο εκείνες για τις οποίες υπάρχει υπολογιστικός αλγόριθμος που τις υπολογίζει, η g θα έπρεπε να είναι αναδρομική. Αυτό όμως θα ερχόταν σε αντίθεση με το θεώρημα 7.3, και αυτό αποδεικνύει τελικά ότι:

Θεώρημα 7.4 ***Το*** 10^o ***Πρόβλημα του Hilbert είναι άλυτο!***

Αναφορές

[1] Αθανάσιος Φειδάς «Το $10^ο$ Πρόβλημα του Hilbert». Σημειώσεις από διάλεξη στο Πανεπιστήμιο Πάτρας.

[2] Martin Davis, «Hilbert's 10th problem is Unsolvable» . The American Mathematical Monthly, 80(3):233-269 [1973].

[3] Yuri Matiyasevič, Online Lecture and Lecture notes, http://www.pims.math.ca/science/2000/distchair/matiyasevich/lecture1/

[4] Martin Davis, Yuri Matiyasevič and Julia Robinson, «Hilberts 10th problem. Diophantine Equations: Positive aspects of a negative solution». The Proceedings of Symposia in Pure Mathematics, Volume 28: p.323-378 [1976].