Διοφαντικές εξισώσεις και το 10^o πρόβλημα του Hilbert

Διπλωματική εργασία

Σύψα Πολυνίκη
Μεταπτυχιακό πρόγραμμα λογικής και αλγορίθμων
$\mu\Pi\lambda\forall$

Μάρτιος 2002

Περιεχόμενα

1 Εισαγωγή

Το 1900, στο δεύτερο διεθνές συνέδριο Μαθηματικών που έγινε στο Παρίσι ο David Hilbert , μεγάλος μαθηματικός της εποχής, έθεσε εικοσιτρία προβλήματα που έμελλε να παίξουν σπουδαίο ρόλο στην εξέλιξη των μαθηματικών τον εικοστό αιώνα (βλέπε [4]).

Το δέκατο πρόβλημα ζητούσε μια διαδικασία που να ελέγχει την ύπαρξη ακεραίων ριζών, ενός πολυωνύμου με ακέραιους συντελεστές.

Το πρώτο βήμα για την απάντηση στο πρόβλημα έγινε τη δεκαετία του '30 με την εισαγωγή της θεωρίας αναδρομικών συναρτήσεων από τους Gödel, Turing, Post, Church και άλλους, και τη διατύπωση της θέσης Church-Turing που ταυτίζει τις αλγοριθμικά υπολογίσιμες συναρτήσεις με τις αναδρομικές.

Το επόμενο βήμα έγινε από τον Martin Davis (βλέπε [1]), που διατύπωσε μερικά χρόνια αργότερα την εικασία ότι οι κλάσεις των διοφαντικών και των αναδρομικά απαριθμητών συνόλων συμπίπτουν. Αυτό απαντούσε στο ερώτημα του Hilbert με τρόπο που ο ίδιος δεν θα μπορούσε να φανταστεί, δείχνοντας ότι δεν μπορεί να υπάρχει ο αλγόριθμος που ζητείτο.

Η δουλειά των J.Robinson, M.Davis και H.Putnam η οποία φαίνεται στο [3] έδειξε ότι η εικασία του M.Davis θα προέκυπτε αν η εκθετική συνάρτηση αποδεικνυόνταν διοφαντική. Ωστώσο η J.Robinson , το 1952 είχε ήδη αποδείξει ότι η διοφαντικότητα μιας συνάρτησης εκθετικής τάξης, θα οδηγούσε και στην διοφαντικότητα της εκθετικής συνάρτησης[10]. Το 1970 ο Y.Matiyasevich στο [7], απέδειξε τη διοφαντικότητα μιας συνάρτησης εκθετικής τάξης οδήγησε στην απόδειξη της εικασίας του M.Davis .

Στα επόμενα εισάγουμε την κλάση των διοφαντικών σχέσεων και δίνουμε σχετικά παραδείγματα.

Δίνουμε βασιζόμενοι στο [6], μια τροποποιημένη απόδειξη της διοφαντικής φύσης της εκθετικής συνάρτησης και χρησιμοποιούμε το αποτέλεσμα αυτό για να εμπλουτίσουμε την κλάση των διοφαντικών συναρτήσεων με τη διωνυμική, το παραγοντικό, καθώς επίσης και την κλάση των διοφαντικών σχέσεων με την Prime .

Χρησιμοποιώντας κατάλληλες διοφαντικές κωδικοποιήσεις και κάποια αριθμοθεωρητικά αποτελέσματα, αποδεικνύουμε την ύπαρξη καθολικής διοφαντικής εξίσωσης. Μετά, κάνοντας απαλοιφή του φραγμένου καθολικού ποσοδείκτη, δείχνουμε την ταύτιση της διοφαντικότητας και της ημιαναδρομικότητας. Δίνουμε έτσι αρνητική απάντηση στο ερώτημα του Hilbert.

Στο τελευταίο κεφάλαιο, βασιζόμενοι στο [5] αποδεικνύουμε την ύπαρξη καθολικής διοφαντικής εξίσωσης με συγκεκριμένη πολυπλοκότητα ως προς το βαθμό και το πλήθος των αγνώστων.

2 Αρχικοί ορισμοί

2.1 Το 10^o πρόβλημα του Hilbert ως πρόβλημα απόφασης

Ορισμός 2.1 *'Διοφαντική εξίσωση' είναι μια εξίσωση της μορφής*

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

όπου $D(x_1, \ldots, x_m)$ είναι πολυώνυμο με ακέραιους συντελεστές.

- *Βαθμός του αγνώστου x_i σε μια διοφαντική εξίσωση καλείται ο μέγιστος βαθμός του x_i στην εξίσωση.*
- *Βαθμός μονωνύμου σε μια διοφαντική εξίσωση καλείται το άθροισμα των βαθμών των διαφορετικών μεταβλητών που υπάρχουν στο μονώνυμο.*
- *(Ολικός) Βαθμός μια διοφαντικής εξίσωσης λέγεται ο μεγαλύτερος βαθμός των μονωνύμων της διοφαντικής εξίσωσης.*

Το 10^o πρόβλημα του Hilbert διατυπώνεται ως εξής:

Υπάρχει μια γενική μέθοδος που να αποφασίζει αν μια διοφαντική εξίσωση έχει λύση ή όχι στους ακεραίους;

Παρατήρηση 2.1

- *Το 10^o πρόβλημα του Hilbert είναι ένα πρόβλημα απόφασης*
- *Ένα πρόβλημα απόφασης αποτελείται από αριθμήσιμα πολλά στιγμιότυπα (στη συγκεκριμένη περίπτωση διοφαντικές εξισώσεις) στα οποία πρέπει να δοθεί μια απάντηση 'ΝΑΙ' ή 'ΟΧΙ'.*

  Σκοπός: να βρεθεί μια γενική μέθοδος που να χρησιμοποιείται για να λάβουμε απάντηση σε κάθε ένα από τα στιγμιότυπα.
- *Η επιλυσιμότητα ενός προβλήματος απόφασης μπορεί να δειχθεί με δύο τρόπους:*
  - *Άμεσα: Δίνοντας τη διαδικασία που ζητάμε.*

– *Έμμεσα: Ανάγοντας το δεδομένο πρόβλημα σε ένα άλλο του οποίου η επιλυσιμότητα έχει δειχθεί.*

- *Το ανεπίλυτο ενός προβλήματος απόφασης μπορεί να δειχθεί είτε άμεσα είτε ανάγοντας στο δεδομένο πρόβλημα ένα άλλο, του οποίου το ανεπίλυτο έχει δειχθεί.*

Η απάντηση στο 10^o πρόβλημα του Hilbert είναι αρνητική

2.2 Ένα πρόβλημα ανάλογο με το 10^o πρόβλημα του Hilbert

Στο 10^o πρόβλημα του Hilbert ρωτάμε για την ύπαρξη λύσεων των διοφαντικών εξισώσεων στους ακεραίους. Μπορούμε να θεωρήσουμε ένα παρόμοιο πρόβλημα στο οποίο θα ρωτάμε για την ύπαρξη λύσεων των διοφαντικών εξισώσεων στους φυσικούς.Έτσι έχουμε δύο προβλήματα τα οποία είναι διαφορετικά

ΠΡΟΒΛΗΜΑ A: Δεδομένης μιας διοφαντικής εξίσωσης να αποφασιστεί αν αυτή εχει λύση ή όχι στους ακεραίους.

ΠΡΟΒΛΗΜΑ B: Δεδομένης μιας διοφαντικής εξίσωσης να αποφασιστεί αν αυτή εχει λύση ή όχι στους φυσικούς.

Τα δύο προβλήματα είναι ισοδύναμα διότι το ένα ανάγεται στο άλλο.

- Το πρόβλημα A ανάγεται στο πρόβλημα B: Έστω $D(x_1, \ldots, x_m) = 0$ διοφαντική εξίσωση και ψάχνουμε για λύση στους ακεραίους. Θεωρούμε την εξίσωση $D(y_1 - z_1, \ldots, y_m - z_m) = 0$.
  Αν οι φυσικοί αριθμοί $\langle y_1, \ldots, y_m, z_1, \ldots, z_m \rangle$ αποτελούν λύση αυτής τότε και οι ακέραιοι αριθμοί $x_1 = y_1 - z_1, \ldots, x_m = y_m - z_m$ αποτελούν λύση της $D(x_1, \ldots, x_m) = 0$.

  Αντίστροφα, αν οι ακέραιοι $\langle x_1, \ldots, x_m \rangle$ είναι μια λύση της $D(x_1, \ldots, x_m) = 0$ τότε υπάρχουν φυσικοί αριθμοί $y_1, \ldots, y_m, z_1, \ldots, z_m$ ώστε $x_1 = y_1 - z_1, \ldots, x_m = y_m - z_m$.
  Άρα οι φυσικοί αριθμοί $y_1, \ldots, y_m, z_1, \ldots, z_m$ αποτελούν λύση της $D(y_1 - z_1, \ldots, y_m - z_m) = 0$.

- Το πρόβλημα B ανάγεται στο πρόβλημα A: Έστω $D(x_1,\ldots,x_m)=0$ διοφαντική εξίσωση και $\langle x_1,\ldots,x_m\rangle$ μη αρνητική λύση αυτής. Με βάση το θεώρημα Lagrange υπάρχουν ακέραιοι $w_i, y_i, z_i, u_i,\ i=1,\ldots,m$ ώστε $x_i = w_i^2+y_i^2+z_i^2+u_i^2,\ i=1,\ldots,m$.
  Άρα η εξίσωση $D(w_1^2+y_1^2+z_1^2+u_1^2,\ldots,w_m^2+y_m^2+z_m^2+u_m^2)=0$ έχει λύση στους ακεραίους την $\langle w_1,\ldots,w_m,y_1,\ldots,y_m,z_1,\ldots,z_m,u_1,\ldots,u_m\rangle$.
  Επίσης αν η εξίσωση $D(w_1^2+y_1^2+z_1^2+u_1^2,\ldots,w_m^2+y_m^2+z_m^2+u_m^2)=0$ έχει λύση στους ακεραίους την $\langle w_1,\ldots,w_m,y_1,\ldots,y_m,z_1,\ldots,z_m,u_1,\ldots,u_m\rangle$ Θέτουμε $x_i = w_i^2+y_i^2+z_i^2+u_i^2,\ i=1,\ldots,m$. Άρα οι αριθμοί $\langle x_1,\ldots,x_m\rangle$ αποτελούν μη αρνητική λύση της $D(x_1,\ldots,x_m)=0$.

Άρα τα δύο προβλήματα ως προβλήματα απόφασης είναι ισοδύναμα. Ωστόσο είναι πιο εύκολο να ασχοληθούμε με το ερώτημα για την ύπαρξη λύσεων στους φυσικούς.

2.3 Διοφαντικά σύνολα

Ορισμός 2.2 *Ένα σύνολο $n-$άδων $\mathfrak{M}$ καλείται '**διοφαντικό**' αν ισχύει η ισοδυναμία:*

$$\langle a_1,\ldots,a_n\rangle \in \mathfrak{M} \Leftrightarrow \exists x_1,\ldots,x_m[D(a_1,\ldots,a_n,x_1,\ldots,x_m)=0]$$

όπου $D(a_1,\ldots,a_n,x_1,\ldots,x_m)=0$ είναι διοφαντική εξίσωση με n παραμέτρους και m αγνώστους.

- *Ο αριθμός n καλείται '**διάσταση**' του συνόλου $\mathfrak{M}$.*
- *Η παραπάνω ισοδυναμία, καθώς και η διοφαντική εξίσωση $D(a_1,\ldots,a_n,x_1,\ldots,x_m)=0$ καλείται '**διοφαντική αναπαράσταση**' του διοφαντικού συνόλου $\mathfrak{M}$.*

Ιδιότητες:

- Η ένωση δύο διοφαντικών συνόλων της ίδιας διάστασης είναι διοφαντικό σύνολο.
  Αν $D_1(a_1,\ldots,a_n,x_1,\ldots,x_m)=0$ και $D_2(a_1,\ldots,a_n,x_1,\ldots,x_m)=0$ είναι οι διοφαντικές αναπαραστάσεις των δύο συνόλων τότε η διοφαντική εξίσωση $D_1(a_1,\ldots,a_n,x_1,\ldots,x_m)\cdot D_2(a_1,\ldots,a_n,x_1,\ldots,x_m)=0$ είναι η διοφαντική αναπαράσταση της ένωσής τους.

- Η τομή δύο διοφαντικών συνόλων της ίδιας διάστασης είναι διοφαντικό σύνολο.
  Αν $D_1(a_1,\ldots,a_n,x_1,\ldots,x_m)=0$ και $D_2(a_1,\ldots,a_n,x_1,\ldots,x_m)=0$ είναι οι διοφαντικές αναπαραστάσεις των δύο συνόλων τότε η διοφαντική εξίσωση $D_1^2(a_1,\ldots,a_n,x_1,\ldots,x_m)+D_2^2(a_1,\ldots,a_n,x_1,\ldots,x_m)=0$ είναι η διοφαντική αναπαράσταση της τομής τους.

Το επόμενο λήμμα οφείλεται στον Hilary Putnam [9]

Λήμμα 2.1 *Ένα σύνολο φυσικών αριθμών $\mathcal{S}$ είναι διοφαντικό αν και μόνο αν είναι το σύνολο των θετικών ακεραίων στο πεδίο τιμών κάποιου πολυωνύμου με ακέραιους συντελεστές και τιμές στις μεταβλητές του φυσικούς αριθμούς.*

Απόδειξη: Έστω $\mathcal{S}$ σύνολο φυσικών αριθμών.Θα δειχθεί οτι:

$$\mathcal{S} \text{ είναι διοφαντικό} \Longleftrightarrow [a\in\mathcal{S}\Leftrightarrow \exists x_0,\ldots,x_m[a=P(x_0,\ldots,x_m)]]$$

όπου $P(x_0,\ldots,x_m)$ πολυώνυμο με ακέραιους συντελεστές.
$(\Longrightarrow)$: Έστω ότι το $\mathcal{S}$ είναι διοφαντικό σύνολο.Τότε ισχύει:
$a\in\mathcal{S}\Leftrightarrow\exists x_1,\ldots,x_m[D(a,x_1,\ldots,x_m)=0]$ όπου $D(x_0,\ldots,x_m)$ πολυώνυμο με ακέραιους συντελεστές. Αν η εξίσωση $D(a,x_1,\ldots,x_m)=0$ έχει λύση στους $x_1,\ldots,x_m$ τότε και η εξίσωση $(x_0+1)(1-D^2(x_0,\ldots,x_m))-1=a$ έχει λύση στους $x_0,\ldots,x_m$ (για $x_0=a$).
Επίσης αν η εξίσωση $(x_0+1)(1-D^2(x_0,\ldots,x_m))-1=a$ έχει λύση στους $x_0,\ldots,x_m$ τότε θα πρέπει $1-D^2(x_0,\ldots,x_m)>0$ το οποίο ισχύει μόνο όταν $D(x_0,\ldots,x_m)=0$. Αλλά τότε θα ισχύει ότι $x_0=a$. Άρα η εξίσωση $D(a,x_1,\ldots,x_m)=0$ έχει λύση στους $x_1,\ldots,x_m$.
Δηλαδή $a\in\mathcal{S}\Leftrightarrow\exists x_0,\ldots,x_m[(x_0+1)(1-D^2(x_0,\ldots,x_m))-1=a]$. Θέτοντας $P(x_0,\ldots,x_m)=(x_0+1)(1-D^2(x_0,\ldots,x_m))-1$ έχουμε ότι
$a\in\mathcal{S}\Leftrightarrow\exists x_0,\ldots,x_m[a=P(x_0,\ldots,x_m)]$
$(\Longleftarrow)$: Έστω ότι $a\in\mathcal{S}\Leftrightarrow\exists x_0,\ldots,x_m[a=P(x_0,\ldots,x_m)]$. Θέτουμε $D(x,x_0,\ldots,x_m)=x-P(x_0,\ldots,x_m)$.
Τότε $a\in\mathcal{S}\Leftrightarrow\exists x_0,\ldots,x_m[D(a,x_0,\ldots,x_m)=0]$. Άρα το $\mathcal{S}$ είναι διοφαντικό σύνολο. □

2.4 Διοφαντικές σχέσεις και συναρτήσεις

Ορισμός 2.3 *Μια συνάρτηση f n ορισμάτων καλείται '**διοφαντική**' αν το γράφημα της είναι διοφαντικό σύνολο, δηλαδη αν ισχύει η ισοδυναμία:*

$$a=f(a_1,\ldots,a_n)\Leftrightarrow\exists x_1,\ldots,x_m[D(a,a_1,\ldots,a_n,x_1,\ldots,x_m)=0]$$

όπου $D(a, a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$ *είναι διοφαντική εξίσωση.*

- *Η παραπάνω ισοδυναμία καθώς επίσης και η διοφαντική εξίσωση* $D(a, a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$ *καλείται '**διοφαντική αναπαράσταση**' της συνάρτησης* f.

Η κλάση των διοφαντικών σχέσεων είναι κλειστή ως προς:

υπαρξιακό ποσοδείκτη: Αν $\mathcal{R}_1(x, a_1, \ldots, a_n)$ είναι διοφαντική σχέση τότε και η σχέση

$$\mathcal{R}(a_1, \ldots, a_n) \Leftrightarrow \exists x \mathcal{R}_1(x, a_1, \ldots, a_n)$$

είναι διοφαντική και η αναπαράσταση αυτής είναι η $D(x, a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$ όπου $D(x, a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$ είναι η διοφαντική αναπαράσταση της $\mathcal{R}_1$.

διοφαντικές αντικαταστάσεις: Αν $\mathcal{R}(t_1, \ldots, t_n)$ διοφαντική σχέση και $\underline{t_1}, \ldots, \underline{t_n}$ διοφαντικοί όροι (εκφράσεις που κατασκευάζονται από φυσικούς αριθμούς, μεταβλητές, τα σύμβολα $+, -, \cdot$ και σύμβολα για διοφαντικές συναρτήσεις) τότε και η σχέση $\mathcal{R}(\underline{t_1}, \ldots, \underline{t_n})$ είναι διοφαντική.

Πράγματι: μια εξίσωση της μορφής $P(\underline{t_1}, \ldots, \underline{t_n}) = 0$, όπου P πολυώνυμο με ακέραιους συντελεστές είναι διοφαντική σχέση. Η εξίσωση $P(\underline{t_1}, \ldots, \underline{t_n}) = 0$ μπορεί να μετασχηματιστεί σε ένα ισοδύναμο σύστημα εξισώσεων που αποτελείται από εξισώσεις της μορφής $\alpha = \beta + \gamma$, $\alpha = \beta \cdot \gamma$, $\alpha = f(\beta_1, \cdots, \beta_n)$ όπου $\alpha, \beta, \gamma, \beta_1, \cdots, \beta_n$ μεταβλητές ή φυσικοί αριθμοί και f διοφαντική συνάρτηση. Αντικαθιστώντας τις εξισώσεις της μορφής $\alpha = f(\beta_1, \cdots, \beta_n)$ με τη διοφαντική αναπαράσταση της f και συμπτύσσσοντας τις εξισώσεις του συστήματος σε μια, προκύπτει διοφαντική εξίσωση ισοδύναμη με την $P(\underline{t_1}, \ldots, \underline{t_n}) = 0$. Τότε

$$\mathcal{R}(\underline{t_1}, \ldots, \underline{t_n}) \Leftrightarrow \exists t_1, \ldots, t_n [\mathcal{R}(t_1, \ldots, t_n) \wedge t_1 = \underline{t_1} \wedge \cdots t_n = \underline{t_n}]$$

όπου οι εξισώσεις $t_i = \underline{t_i}$, $i = 1 \ldots n$ μπορούν να αντιμετωπιστούν όπως η παραπάνω $P(\underline{t_1}, \ldots, \underline{t_n}) = 0$.

2.5 Παραδείγματα διοφαντικών σχέσεων και συναρτήσεων.

- **Η σχέση "$\neq$" είναι διοφαντική**
  $a_1 \neq a_2 \Leftrightarrow \exists x[(a_1 - a_2)^2 = x + 1]$

- **Η σχέση " $\leq$ " είναι διοφαντική**
  $a \leq b \Leftrightarrow \exists x[a + x = b]$

- **Η σχέση " $<$ " είναι διοφαντική**
  $a < b \Leftrightarrow \exists x[a + x + 1 = b]$

- **Η σχέση " $|$ " είναι διοφαντική**
  $a \mid b \Leftrightarrow \exists x[ax = b]$

- **Η ιδιότητα ' ο a είναι άρτιος ' είναι διοφαντική**
  $Even(a) \Leftrightarrow \exists x[a = 2x]$

- **Η ιδιότητα ' ο a είναι περιττός ' είναι διοφαντική**
  $Odd(a) \Leftrightarrow Even(a + 1)$

- **Η συνάρτηση "$rem(b, c)$" (το υπόλοιπο της διαίρεσης του b με το c) είναι διοφαντική**
  $a = rem(b, c) \Leftrightarrow a < c \wedge c \mid b - a$

- **Η συνάρτηση "$arem(b, c)$" είναι διοφαντική**
  όπου $arem(b, c)$ είναι η συνάρτηση που ορίζεται ως εξής:
  $arem(b, c) \equiv \pm b \pmod{c} \& 0 \leq arem(b, c) \leq \frac{c}{2}$

- **Η σχέση " $\nmid$ " είναι διοφαντική**

- **Η συνάρτηση "$b \; div \; c$" (το πηλίκο της ακέραιας διαίρεσης του b με το c) είναι διοφαντική**

- **Η συνάρτηση "$b \pmod{c}$" είναι διοφαντική**

- **Η συνάρτηση "$\gcd(b, c)$" (ο μέγιστος κοινός διαιρέτης των θετικών ακεραίων b και c) είναι διοφαντική**

3 Κάποια αριθμοθεωρητικά θεωρήματα

Στην παράγραφο αυτή θα διατυπωθούν και θα αποδειχθούν δύο θεωρήματα από τη θεωρία αριθμών τα οποία χρησιμοποιήθηκαν στην απόδειξη που δόθηκε για την αρνητική απάντηση στο 10^o πρόβλημα του Hilbert .

Θεώρημα 3.1 ***(θεώρημα υπολοίπων κινέζου)*** *Έστω ότι $q_1, \ldots, q_n$ είναι πρώτοι ανά δύο φυσικοί αριθμοί και $a_1, \ldots, a_n$ είναι επίσης φυσικοί αριθμοί τέτοιοι ώστε*

$$a_i < q_i, \; i = 1, \ldots, n.$$

Τότε υπάρχει ένας μοναδικός αριθμός a ώστε:

$$0 \leq a < q_1 \cdots q_n$$

και

$$a_i = rem(a, q_i), \; i = 1, \ldots, n.$$

Απόδειξη
Θέτουμε $m = q_1 \cdots q_n$, και θεωρούμε τις m $n-$άδες αριθμών:

$$\begin{array}{c} \langle rem(0, q_1), \ldots, rem(0, q_n) \rangle \\ \langle rem(1, q_1), \ldots, rem(1, q_n) \rangle \\ \vdots \\ \langle rem(m-1, q_1), \ldots, rem(m-1, q_n) \rangle \end{array} \tag{3.1}$$

Ισχυρισμός 1**:** $rem(a, q_i) \neq rem(b, q_i)$ για $0 \leq b \leq a < m$ και $i = 1, \ldots, n$.
Αν ίσχυε ότι $rem(a, q_i) = rem(b, q_i)$ θα είχαμε ότι $q_i \mid a - b, \; i = 1, \ldots, n$. Όμως επειδή οι $q_1, \ldots, q_n$ είναι ανά δύο πρώτοι θα ίσχυε ότι $q_1 \cdots q_n \mid a - b$, δηλαδή ότι $m \mid a - b$ το οποίο είναι άτοπο αφού $a, b < m$.

Άρα οι $n-$άδες (3.1) είναι όλες διαφορετικές μεταξύ τους.

Ισχυρισμός 2**:** Κάθε $n-$άδα φυσικών αριθμών $\langle a_1, \ldots, a_n \rangle$ με $a_i < q_i, \; i = 1, \ldots, n$ είναι ακριβώς μία από τις m $n-$άδες (3.1).
Πράγματι, υπάρχουν $q_1 \cdots q_n$ $n-$άδες φυσικών αριθμών, $\langle a_1, \ldots, a_n \rangle$ με $a_i < q_i, \; i = 1, \ldots, n$. Επίσης για κάθε $n-$άδα $\langle rem(a, q_1), \ldots, rem(a, q_n) \rangle$ από τις (3.1), ισχύει ότι $rem(a, q_i) < q_i, \; i = 1, \ldots, n$.

Άρα δεδομένης της $n-$άδας $\langle a_1, \ldots, a_n \rangle$ για την οποία ισχύει ότι $a_i < q_i, \; i = 1, \ldots, n$, υπάρχει ένας μοναδικός αριθμός a για τον οποίο έχουμε ότι $0 \leq a < m$ και ότι $a_i = rem(a, q_i), \; i = 1, \ldots, n$. $\square$

Θεώρημα 3.2 ***(Kummer)*** *Αν p είναι πρώτος αριθμός, τότε*

$$\tau_p(m,n) = deg_p\left(\binom{m+n}{m}\right).$$

Με $\tau_p(m,n)$ συμβολίζουμε τον αριθμό των κρατουμένων κατά την πρόσθεση των αριθμών m, n, όταν αυτοί γραφούν ως αναπτύγματα με βάση το p, ενώ με $deg_p(k)$ τον εκθέτη του p στο κανονικό ανάπτυγμα του k σε πρώτους παράγοντες.

Απόδειξη
Εφόσον ισχύει ότι

$$\binom{m+n}{m} = \frac{(m+n)!}{m!n!}$$

έπεται ότι

$$deg_p\left(\binom{m+n}{m}\right) = deg_p((m+n)!) - deg_p(m!) - deg_p(n!). \tag{3.2}$$

Όμως επειδή μεταξύ των αριθμών $1, 2, \ldots, k$ υπάρχουν $k\, div\, p$ αριθμοί που διαιρούνται με το p, $k\, div\, p^2$ αριθμοί που διαιρούνται με το p^2 κ.ο.κ, θα ισχύει ότι:

$$deg_p(k!) = k\, div\, p + k\, div\, p^2 + \ldots.$$

Έστω ένας αριθμός $k > 0$, και έστω ότι διαιρούμε τους αριθμούς $m, n, m+n$ με το p^k. Τότε θα έχουμε:

$$m = (m\, div\, p^k)p^k + m',\ \text{όπου}\ m' < p^k$$

$$n = (n\, div\, p^k)p^k + n',\ \text{όπου}\ n' < p^k$$

Τότε θα έχουμε ότι $m' + n' < 2p^k$. Άρα το $(m' + n')\, div\, p^k$ θα είναι είτε 0 είτε 1 ανάλογα αν υπάρχει κρατούμενο κατά την πρόσθεση των $k-1$ ψηφίων των m και n. Άρα θα ισχύει ότι:

$$\tau_p(m,n) = \sum_{k\geq 1}(m' + n')\, div\, p^k \tag{3.3}$$

Όμως ισχύει ότι:

$$m + n = (m\, div\, p^k + n\, div\, p^k)p^k + (m' + n')$$

και διαιρώντας με το p^k, προκύπτει ότι:

$$(m+n)\,div\,p^k = m\,div\,p^k + n\,div\,p^k + (m'+n')\,div\,p^k.$$

Άρα

$$(m'+n')\,div\,p^k = (m+n)\,div\,p^k - m\,div\,p^k - n\,div\,p^k.$$

Τότε από τις σχέσεις (3.2) και (3.3) έπεται ότι

$$\tau_p(m,n) = deg_p\left(\binom{m+n}{m}\right). \square$$

Το θεώρημα αυτό γράφτηκε το 1852 από τον E.E.Kummer και δημοσιεύτηκε σε ένα Γερμανικό μαθηματικό περιοδικό. Μια απόδειξη για το θεώρημα αυτό μπορεί να βρεθεί επίσης στο [11].

4 Η εκθετικότητα είναι διοφαντική

4.1 Η εκθετική συνάρτηση είναι διοφαντική

Στην παράγραφο αυτή θα αποδειχθεί οτι η εκθετική συνάρτηση $f(b,c) = b^c$ είναι διοφαντική. Αρκεί να αποδειχθεί οτι το σύνολο $\mathfrak{M} = \{< a, b, c >|\ a = b^c\}$ είναι διοφαντικό.

Ορισμός 4.1 *Ορίζουμε την αναδρομική ακολουθία φυσικών αριθμών $a_b(n)$ ως εξής:*

$$\begin{aligned} a_b(0) &= 0 \\ a_b(1) &= 1 \\ a_b(n+2) &= b a_b(n+1) - a_b(n) \end{aligned}$$

Παρατήρηση 4.1 *Για την ακολουθία $a_b(n)$ ισχύουν τα εξής:*

1. *Η ακολουθία $a_b(n)$ είναι γνησίως αύξουσα.*
   Δηλαδή ισχύει: $0 = a_b(0) < a_b(1) < \cdots < a_b(n) < a_b(n+1) < \cdots$

   Πράγματι: Έστω ότι ισχύει η σχέση $a_b(k) < a_b(k+1)$ για κάθε $k < n$. Ισχύει $a_b(n+1) = ba_b(n) - a_b(n-1)$. Τότε από την επαγωγική υπόθεση έχουμε ότι:

   $$a_b(n+1) > ba_b(n) - a_b(n) = (b-1)a_b(n) \geq a_b(n) \quad \textit{παίρνοντας} \quad b \geq 2$$

   Άρα για $b \geq 2$ και για κάθε n ισχύει: $a_b(n) < a_b(n+1)$.

2. *$a_2(n) = n$ το οποίο αποδεικνύεται επίσης με επαγωγή.*

3. *Αν ισχύει ότι $b_1 \equiv b_2 \pmod q$ τότε ισχύει ότι $a_{b_1}(n) \equiv a_{b_2}(n) \pmod q$*

   Πράγματι: Έστω ότι ισχύει για κάθε $k < n$ το εξής:
   $b_1 \equiv b_2 \pmod q \to a_{b_1}(k) \equiv a_{b_2}(k) \pmod q$. Τότε έπεται ότι:

   $$\begin{aligned} a_{b_1}(n) &= b_1 a_{b_1}(n-1) - a_{b_1}(n-2) \\ &\equiv b_2 a_{b_2}(n-1) - a_{b_2}(n-2) \pmod q \\ &\equiv a_{b_2}(n) \pmod q \end{aligned}$$

   Άρα για κάθε n ισχύει: $b_1 \equiv b_2 \pmod q \to a_{b_1}(n) \equiv a_{b_2}(n) \pmod q$.

4. $a_b(n) \equiv n \pmod{b-2}$ *το οποίο έπεται από τις παρατηρήσεις 4.1(2) και 4.1(3).*

Ορισμός 4.2 *Ορίζουμε την ακολουθία πινάκων $A_b(n)$ ως εξής:*

$$A_b(n) = \begin{pmatrix} a_b(n+1) & -a_b(n) \\ a_b(n) & -a_b(n-1) \end{pmatrix}, \text{ παίρνοντας } a_b(-1) = -1$$

Παρατήρηση 4.2

1. *Οι πίνακες $A_b(n)$, $n = 0, 1, 2, \ldots$ ορίζονται αναδρομικά ως εξής:*
   $A_b(0) = I_2$
   $A_b(n+1) = A_b(n)L_b$
   όπου $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ *και* $L_b = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}$.

2. $A_b(n) = L_b^n$

3. $\det(A_b(n)) = 1$

Λήμμα 4.1 $x^2 - bxy + y^2 = 1$, *όπου* $x, y \in \mathbb{N}$ *και* $y < x$, *αν και μόνο αν υπάρχει* m *τέτοιο που* $x = a_b(m+1)$ *και* $y = a_b(m)$.

Απόδειξη

$(\Longleftarrow)$: Έστω οτι υπάρχει m τέτοιο που $x = a_b(m+1)$ και $y = a_b(m)$.Τότε λόγω της παρατήρησης 4.1(1) έπεται ότι $y < x$. Επίσης $\det(A_b(m+1)) = 1$ και επειδή $\det(A_b(m+1)) = a_b^2(m+1) - a_b(m+2)a_b(m)$ έπεται ότι $x^2 - bxy + y^2 = 1$.

$(\Longrightarrow)$: Έστω ότι ισχύουν $x^2 - bxy + y^2 = 1$ και $y < x$. Με επαγωγή στο y θα αποδείχθεί ότι υπάρχει m τέτοιο που $x = a_b(m+1)$ και $y = a_b(m)$.
$\mathbf{y = 0}$: τότε αφού ισχύει $x^2 - bxy + y^2 = 1$ έπεται ότι $x = 1$. Δηλαδή $y = a_b(0)$ και $x = a_b(1)$ που σημαίνει ότι $m = 0$.
$\mathbf{y > 0}$: $x^2 - bxy + y^2 = 1 \Rightarrow x^2 = bxy + 1 - y^2 \Rightarrow$

$$\Rightarrow \begin{cases} x = by + \frac{1-y^2}{x} \leq by \\ x = by + \frac{1}{x} - \frac{y^2}{x} > by + \frac{1}{x} - y > by - y \end{cases}$$

Θέτοντας $x_1 = y$ και $y_1 = by - x$ έπεται ότι $y_1 < y$ και $y_1 < x_1$

$$\begin{aligned} \text{Επίσης} \quad x_1^2 - bx_1y_1 + y_1^2 &= y^2 - by(by-x) + (by-x)^2 \\ &= y^2 - b^2y^2 + bxy + b^2y^2 - 2bxy + x^2 \\ &= x^2 - bxy + y^2 \\ &= 1 \end{aligned}$$

Αρα από επαγωγική υπόθεση υπάρχει m_1 τέτοιο που $x_1 = a_b(m_1+1)$ και $y_1 = a_b(m_1)$. Θέτοντας $m = m_1 + 1$ έπεται ότι $y = x_1 = a_b(m)$ και $x = by - y_1 = ba_b(m) - a_b(m-1) = a_b(m+1)$.

Δηλαδή υπάρχει m: $x = a_b(m+1)$ και $y = a_b(m)$. □

Λήμμα 4.2 *Αν $m = kl$ τότε $a_b(m) \equiv (-1)^{l-1} l a_b(k) a_b^l(k-1) \pmod{a_b^2(k)}$.*

Απόδειξη

$$\begin{aligned} A_b(m) &= L_b^m \\ &= (L_b^k)^l \\ &= A_b^l(k) \\ &= [a_b(k)L_b - a_b(k-1)I_2]^l \\ &= \sum_{i=0}^{l} a_b^i(k) L_b^i (-1)^{l-i} a_b^{l-i}(k-1) I_2^{l-i} \end{aligned}$$

Τότε θα έχουμε ότι:

$$A_b(m) \equiv (-1)^l a_b^l(k-1) I_2 + (-1)^{l-1} l a_b(k) a_b^{l-1}(k-1) L^b \pmod{a_b^2(k)}$$

και επειδή $A_b(m) = \begin{pmatrix} a_b(m+1) & -a_b(m) \\ a_b(m) & -a_b(m-1) \end{pmatrix}$ θα ισχύει ότι:
$a_b(m) \equiv (-1)^{l-1} l a_b(k) a_b^l(k-1) \pmod{a_b^2(k)}$. □

Λήμμα 4.3 *Άν $a_b^2(k) \mid a_b(m)$ τότε $a_b(k) \mid m$.*

Απόδειξη

Από τον αλγόριθμο της ευκλείδειας διαίρεσης ισχύει $m = kl + n,\ 0 \le n < k$. Τότε

$$A_b(m) = L_b^m = L_b^{kl+n} = (L_b^k)^l L_b^n = A_b^l(k) A_b(n)$$

Άρα

$$\begin{aligned} &\begin{pmatrix} a_b(m+1) & -a_b(m) \\ a_b(m) & -a_b(m-1) \end{pmatrix} \\ \equiv &\begin{pmatrix} a_b(n+1) & -a_b(n) \\ a_b(n) & -a_b(n-1) \end{pmatrix} \begin{pmatrix} a_b(k+1) & 0 \\ 0 & -a_b(k-1) \end{pmatrix}^l \pmod{a_b(k)} \end{aligned}$$

που σημαίνει ότι $a_b(m) \equiv a_b(n)a_b^l(k+1) \pmod{a_b(k)}$
Από την παρατήρηση 4.2.3 έπεται ότι $a_b^2(k) - a_b(k+1)a_b(k-1) = 1$ που σημαίνει ότι:
Οι $a_b(k), a_b(k+1)$ είναι σχετικά πρώτοι και
οι $a_b(k), a_b(k-1)$ είναι σχετικά πρώτοι επίσης.
Ισχύει $a_b^2(k) \mid a_b(m)$ και άρα $a_b(k) \mid a_b(m)$.
Αυτό σημαίνει ότι $a_b(k) \mid a_b(n)a_b^l(k+1)$ και επειδή $a_b(k), a_b(k+1)$ είναι σχετικά πρώτοι έπεται ότι $a_b(k) \mid a_b(n)$.
Όμως $n < k \Rightarrow a_b(n) < a_b(k)$ (λόγω της παρατήρησης 4.1(1) και άρα $a_b(n) = 0$ που σημαίνει ότι $n = 0$.
Άρα $m = kl$. Τότε από το Λημμα 4.2 έπεται ότι:

$$a_b(m) \equiv (-1)^{l-1} l a_b(k) a_b^l(k-1) \pmod{a_b^2(k)}.$$

Από υπόθεση έχουμε ότι $a_b^2(k) \mid a_b(m)$.
Άρα $a_b^2(k) \mid (-1)^{l-1} l a_b(k) a_b^l(k-1)$.
Δηλαδή $a_b(k) \mid l a_b^l(k-1)$ και επειδή $a_b(k), a_b(k-1)$ είναι σχετικά πρώτοι έπεται ότι $a_b(k) \mid l$. Άρα $a_b(k) \mid kl$.
Δηλαδή $a_b(k) \mid m$. $\square$

Θεώρημα 4.1 *Το σύνολο* $\mathfrak{N} = \{< a, b, c >\mid\ b \geq 4\ \&\ a = a_b(c)\}$ *είναι διοφαντικό.*

Απόδειξη
Αυτό που θα δειχθεί είναι ότι το σύστημα:

$$b \geq 4 \tag{4.1}$$

$$u^2 - but + t^2 = 1 \tag{4.2}$$

$$s^2 - bsr + r^2 = 1 \tag{4.3}$$

$$r < s \tag{4.4}$$

$$u^2 \mid s \tag{4.5}$$

$$v = bs - 2r \tag{4.6}$$

$$v \mid w - b \tag{4.7}$$

$$u \mid w - 2 \tag{4.8}$$

$$w > 2 \tag{4.9}$$

$$x^2 - wxy + y^2 = 1 \tag{4.10}$$

$$2a < u \tag{4.11}$$

$$a = arem(x, v) \tag{4.12}$$

$$c = arem(x, u) \tag{4.13}$$

έχει λύση ως προς u, t, s, r, v, w, x, y αν και μόνο αν $b \geq 4$ & $a = a_b(c)$
Τότε το σύνολο $\mathfrak{N}$ προφανώς θα είναι διοφαντικό.

($\Longrightarrow$) : Έστω ότι το παραπάνω σύστημα έχει λύση. Από τις σχέσεις (4.1), (4.2) και λόγω του Λήμματος 4.1 έπεται ότι υπάρχει k ώστε $u = a_b(k)$.
Επίσης από τις σχέσεις (4.1), (4.2), (4.3) και λόγω του Λήμματος 4.1 έπεται ότι υπάρχει m ώστε $s = a_b(m), r = a_b(m-1)$.
Από τη σχέση (4.5) και λόγω του Λήμματος 4.3 έπεται ότι $a_b(k) \mid a_b(m)$ δηλαδή ότι $u \mid a_b(m)$.
Από τη σχέση (4.6) έχουμε ότι $v = a_b(m+1) - a_b(m-1)$. Λόγω των σχέσεων(4.9), (4.10) και του Λήμματος 4.1 προκύπτει ότι ύπάρχει n τέτοιο που $x = a_w(n)$.
Από τη σχέση (4.7) έχουμε ότι $w \equiv b \pmod v$ και με βάση την Παρατήρηση 4.1(3) έπεται ότι $a_w(n) \equiv a_b(n) \pmod v$, δηλαδή
$x \equiv a_b(n) \pmod v$.
Επίσης από την (4.8) έχουμε ότι $w \equiv 2 \pmod u$ και λόγω της Παρατήρησης 4.1(3) έπεται ότι $a_w(n) \equiv n \pmod u$, δηλαδή $x \equiv n \pmod u$.
Από τον αλγόριθμο της ευκλείδιας διαίρεσης έχουμε:
$n = 2ml \pm j$ όπου $j \leq m$.
Τότε $A_b(n) = L_b^n = L_b^{2ml \pm j} = [(L_b^m)^2]^l (L_b)^{\pm j} = [A_b^2(m)]^l [A_b(j)]^{\pm 1}$.
Όμως ισχύει

$$\begin{aligned} A_b(m) &= \begin{pmatrix} a_b(m+1) & -a_b(m) \\ a_b(m) & -a_b(m-1) \end{pmatrix} \\ &\equiv -\begin{pmatrix} -a_b(m-1) & a_b(m) \\ -a_b(m) & a_b(m+1) \end{pmatrix} \pmod v \\ &\equiv -[A_b(m)]^{-1} \pmod v. \end{aligned}$$

Άρα

$$A_b^2(m) \equiv -I_2 \pmod v.$$

Συνεπώς

$$A_b(n) \equiv \pm [A_b(j)]^{\pm 1} \pmod v.$$

Επίσης
$$A_b(j) \equiv -[A_b(j)]^{-1} \pmod v.$$
Άρα
$$a_b(n) \equiv \pm a_b(j) \pmod v.$$
Άρα
$$x \equiv \pm a_b(j) \pmod v, \ j \leq m.$$
Επίσης έχουμε ότι
$$\begin{aligned} 2a_b(j) &< 2a_b(m) \\ &\leq (b-2)a_b(m) \\ &= ba_b(m) - 2a_b(m) \\ &\leq ba_b(m) - 2a_b(m-1) \\ &= v. \end{aligned}$$

Άρα $\ arem(x,v) = a_b(j), \ j \leq m.$
Δηλαδή $\ a = a_b(j), \ j \leq m \ $ λόγω της (4.12).
Επίσης $\ 2j \leq 2a_b(j) = 2a < u \ $ (λόγω της (4.11)).
Άρα $\ arem(x,u) = arem(n,u)$
και επειδή ισχύουν: $\quad n = 2ml \pm j$
$u \mid m$
$2j < u$
έπεται ότι $\ arem(x,u) = j.$
Άρα λόγω της (4.13) έπεται ότι $c = j$ που σημαίνει ότι $a = a_b(c)$.

$(\Longleftarrow)$: Έστω α,b, c για τα οποία ισχύει ότι: $b \geq 4$ & $a = a_b(c)$.
Θα δειχθεί ότι $\exists s, r, t, u, v, w$ που ικανοποιούν τις σχέσεις (4.1) – (4.13).
Διαλέγω ένα k ώστε $u = a_b(k)$: περιττός και $2a < u$.
Θέτοντας $t = a_b(k+1)$, λόγω του Λήμματος 4.1, προκύπτει ότι
$u^2 - but + t^2 = 1$.
Διαλέγω $m = uk$ (δηλαδή διαλέγω ένα πολλαπλάσιο του k).
Θέτοντας $s = a_b(m)$ και $r = a_b(m-1)$ από το Λήμμα 4.1 προκύπτει ότι
$s^2 - bsr + r^2 = 1$ και $r < s$.
Τότε από το Λήμμα 4.2 έπεται ότι $s \equiv (-1)^{u-1} u a_b(k) a_b^{u-1}(k-1) \pmod{u^2}$
που σημαίνει ότι $u^2 \mid s$.
Θέτουμε $v = bs - 2r$.
Ισχύει: $bs - 2r \geq 4a_b(m) - 2a_b(m-1) > 2a_b(m)$

Δηλαδή $v > 2a_b(m)$.
Επίσης u, v είναι σχετικά πρώτοι, διότι:

Έστω $d \mid u$ και $d \mid v$. Τότε $d \mid u^2$ και $u^2 \mid s$.
Άρα $d \mid s$ και $d \mid bs - 2r$. Άρα $d \mid r$ και επομένως
$d \mid s^2 - bsr + r^2$. Αυτό σημαίνει ότι $d \mid 1$. Άρα $d = 1$.

Από το κινέζικο θεώρημα υπολοίπων έπεται ότι υπάρχει w τέτοιο που:

$$w \equiv b \pmod v$$

$$w \equiv 2 \pmod u$$

$$w > 2$$

Θέτοντας $x = a_w(c)$ και $y = a_w(c+1)$ λόγω του Λήμματος 4.2 προκύπτει ότι $x^2 - wxy + y^2 = 1$
Λόγω της Παρατήρησης 4.1(3) έχουμε ότι:
$x = a_w(c) \equiv a_b(c) \pmod v = a \pmod v$ και επειδή $v > 2a_b(m) > 2a$ έπεται ότι $arem(x, v) = a$.
Επειδή $w \equiv 2 \pmod u$ και λόγω της Παρατήρησης 4.1(3) έχουμε ότι $x = a_w(c) \equiv c \pmod u$. Επίσης ισχύει: $2c \leq 2a_b(c) = 2a < u$. Άρα $arem(x, u) = c$.
Άρα όλες οι εξισώσεις (4.1) – (4.13) ικανοποιούνται. □

Θεώρημα 4.2 *Η εκθετική συνάρτηση είναι διοφαντική.*

Απόδειξη
Κατ' αρχήν ορίζουμε ότι: $0^0 = 1$
Με επαγωγή αποδεικνύεται ότι ισχύει: $(b-1)^n \leq a_b(n+1) \leq b^n$.

Πράγματι: Η παραπάνω σχέση ισχύει για $n = 0$.
Έστω ότι ισχύει $(b-1)^n \leq a_b(n+1) \leq b^n$.
Τότε $a_b(n+2) = ba_b(n+1) - a_b(n) \leq ba_b(n+1) \leq bb^n = b^{n+1}$ (λόγω της επαγωγικής υπόθεσης).
Επίσης

$$\begin{aligned} a_b(n+2) &= ba_b(n+1) - a_b(n) \\ &\geq ba_b(n+1) - a_b(n+1) \\ &= (b-1)a_b(n+1) \\ &\geq (b-1)(b-1)^n \\ &= (b-1)^{n+1}. \end{aligned}$$

Άρα ισχύει $(b-1)^{n+1} \leq a_b(n+2) \leq b^{n+1}$.

Θα δειχθεί ότι για σταθερό b και αρκετά μεγάλες τιμές του x ισχύει:

$$b^c = a_{bx+4}(c+1)\, div\, a_x(c+1)$$

Πράγματι:

$$\frac{a_{bx+4}(c+1)}{a_x(c+1)} \geq \frac{(bx+3)^c}{x^c} = \left(b + \frac{3}{x}\right)^c \geq b^c$$

- $b = 0$
  - $c = 0$
    Είναι $b^c = 1$.
    Επίσης $\quad \dfrac{a_{bx+4}(c+1)}{a_x(c+1)} = \dfrac{a_4(1)}{a_x(1)} = 1.$
    Άρα $\quad a_{bx+4}(c+1)\, div\, a_x(c+1) = 1.$
  - $c \neq 0, \quad x > 4$
    Είναι $b^c = 0$.
    Επίσης $\quad \dfrac{a_{bx+4}(c+1)}{a_x(c+1)} = \dfrac{a_4(c+1)}{a_x(c+1)} < 1$ λόγω της Παρατήρησης 4.1(1).
    Άρα $\quad a_{bx+4}(c+1)\, div\, a_x(c+1) = 0.$
- $b > 0,\ c > 0,\ x > 16c$

$$\begin{aligned}
\frac{a_{bx+4}(c+1)}{a_x(c+1)} &\leq \frac{(bx+4)^c}{(x-1)^c} \\
&\leq \frac{\left(1+\frac{4}{x}\right)^c}{\left(1-\frac{1}{x}\right)^c} b^c \\
&\leq \frac{b^c}{\left(1-\frac{1}{x}\right)^c\left(1-\frac{4}{x}\right)^c} \\
&\leq \frac{b^c}{\left(1-\frac{4}{x}\right)^{2c}} \\
&\leq \frac{b^c}{1-\frac{8c}{x}} \\
&\leq b^c\left(1+\frac{16c}{x}\right).
\end{aligned}$$

Άρα, εφόσον ισχύει $\quad b^c \leq \dfrac{a_{bx+4}(c+1)}{a_x(c+1)}$ για όλα τα x για να ισχύει $b^c = a_{bx+4}(c+1)\, div\, a_x(c+1)$ θα πρέπει $b^c\, \dfrac{16c}{x} < 1$, δηλαδή αρκεί $x > 16\, c\, b^c$.

Άρα για $x > 16\, c\, b^c$ ισχύει ότι $b^c = a_{bx+4}(c+1)\, div\, a_x(c+1)$.

Παίρνοντας $x = 16(c+1)a_{b+4}(c+1)$ έχουμε ότι $b^c = a_{bx+4}(c+1)\, div\, a_x(c+1)$. Η συνάρτηση $g(b,c) = a_b(c)$ είναι διοφαντική (θεώρημα 4.1)καθώς επίσης και η συνάρτηση "div" (κεφάλαιο 1), και επειδή όπως αποδείχτηκε στο κεφάλαιο 1 η κλάση των διοφαντικών συναρήσεων είναι κλειστή κάτω από διοφαντικές αντικαταστάσεις, έπεται ότι η εκθετική συνάρτηση $f(b,c) = b^c$ είναι επίσης διοφαντική.

4.2 Εκθετικές διοφαντικές εξισώσεις

Ορισμός 4.3 *'Εκθετική διοφαντική εξίσωση' είναι μια εξίσωση της μορφής $E_L(x_1,\ldots,x_m) = E_R(x_1,\ldots,x_m)$ όπου E_L, E_R είναι εκφράσεις που κατασκευάζονται από μεταβλητές και φυσικούς αριθμούς χρησιμοποιώντας πρόσθεση, πολλαπλασιασμό και εκθετικότητα.*

Θεώρημα 4.3 *Η κλάση των σχέσεων (συνόλων, συναρτήσεων, ιδιοτήτων) που η αναπαράστασή τους είναι μια εκθετική διοφαντική εξίσωση ταυτίζεται με την κλάση των διοφαντικών σχέσεων (συνόλων, συναρτήσεων, ιδιοτήτων).*

Απόδειξη
Στο Θεώρημα 4.2 έχει δειχθεί ότι η εκθετική συνάρτηση είναι διοφαντική. Άρα σύμφωνα με την παράγραφο 2.4 κάθε εκθετική διοφαντική εξίσωση $P(\underline{t_1},\ldots,\underline{t_n}) = 0$ μετασχηματίζεται σε μια απλή διοφαντική εξίσωση.

Το τελευταίο Θεώρημα του Fermat :
Η εξίσωση $(p+1)^{s+3} + (q+1)^{s+3} = (r+1)^{s+3}$ δεν έχει λύση στους αγνώστους p, q, r, s.

Η σχέση $R(p,q,r,s) \Leftrightarrow (p+1)^{s+3}+(q+1)^{s+3} = (r+1)^{s+3}$ είναι διοφαντική (διότι οι διοφαντικές σχέσεις είναι κλειστές κάτω από διοφαντικές αντικαταστάσεις και η εκθετική συνάρτηση είναι διοφαντική). Άρα μπορούμε να κατασκευάσουμε πολυώνυμο F με ακέραιους συντελεστές ώστε:
$(p+1)^{s+3}+(q+1)^{s+3} = (r+1)^{s+3} \Leftrightarrow \exists x_1,\ldots,x_m[F(p,q,r,s,x_1,\ldots,x_m) = 0]$.

Άρα το τελευταίο Θεώρημα του Fermat είναι ισοδύναμο με το εξής: η εξίσωση $F(p, q, r, s, x_1, \ldots, x_m) = 0$ δεν έχει λύση στους αγνώστους $p, q, r, s, x_1, \ldots, x_m$.

5 Κωδικοποίηση πεπερασμένων ακολουθιών φυσικών αριθμών

5.1 Κωδικοποίηση κατά Cantor

Ορισμός 5.1 *'Ο κωδικός Cantor ' ενός ζεύγους φυσικών αριθμών* $\langle a,b\rangle$ *είναι:*
$Cantor(a,b) = \dfrac{(a+b)^2+3a+b}{2}$.

Ορισμός 5.2 *Ο κωδικός Cantor μιας* $n-$*άδας φυσικών αριθμών*
$\langle a_1,\ldots,a_n\rangle$ *ορίζεται αναδρομικά ως εξής:*
$Cantor_1(a_1) = a_1$
$Cantor_{n+1}(a_1,\ldots,a_n,a_{n+1}) = Cantor_n(a_1,\ldots,a_n,Cantor(a_{n-1},a_n))$

Παρατήρηση 5.1

- *Συμβολίζουμε με* $El_{n,m}(c)$ *τη συνάρτηση η οποία δίνει το* $m-$*οστό στοιχείο μιας* $n-$*άδας φυσικών αριθμών της οποίας ο κωδικός κατά Cantor είναι* c. *Τότε ισχύει:*

$$El_{n,m}(c) = a \Leftrightarrow \exists x_1,\ldots,x_{m-1},x_{m+1},\ldots,x_n$$
$$[2^{2^n}Cantor_n(x_1,\ldots,x_{m-1},a,x_{m+1},\ldots,x_n) = 2^{2^n}c]$$

  Άρα η συνάρτηση $El_{n,m}(c)$ *ως συνάρτηση του* c *είναι διοφαντική.*

- *Κάθε πεπερασμένη ακολουθία φυσικών αριθμών έχει ένα μόνο κωδικό κατά Cantor .*

5.2 Κωδικοποίηση κατά θέση (Positional coding)

Ορισμός 5.3 *Η τριάδα* $\langle a,b,c\rangle$ *λέγεται* '**κωδικός κατά θέση**' *μιας* $n-$*άδας φυσικών αριθμών* $\langle a_1,\ldots,a_n\rangle$ *αν:*
$c = n$
$b > a_i,\ i = 1,\ldots,n$
$a = a_n b^{n-1} + \cdots + a_1 b^0$

- a*: κωδικός της* $\langle a_1,\ldots,a_n\rangle$, b*: βάση και* c*: μήκος.*
- *Η τριάδα* $\langle 0,b,0\rangle$ *είναι ο κωδικός κατά θέση της κενής πλειάδας.*

Παρατήρηση 5.2

- *Με την κωδικοποίηση κατά θέση μπορούμε να κωδικοποιούμε ακολουθίες φυσικών αριθμών απροσδιόριστου μήκους.*

- *Κάθε πλειάδα έχει άπειρα πολλούς κωδικούς κατά θέση. Ένα για κάθε βάση.*

- *Μια τριάδα $\langle a,b,c\rangle$ δεν είναι πάντα κωδικός κατά θέση μιας πλειάδας φυσικών αριθμών. Θεωρούμε τη σχέση:*
  $Code(a,b,c)$: η τριάδα $\langle a,b,c\rangle$ είναι κωδικός κατά θέση μιας πλειάδας αριθμών.
  Ισχύει $Code(a,b,c) \Leftrightarrow b \geq 2 \quad \& \quad a < b^c$ που σημαίνει ότι η σχέση $Code(a,b,c)$ είναι διοφαντική.

- *Συμβολίζουμε με $El(a,b,i)$ τη συνάρτηση που δίνει το $i-$οστό στοιχείο της πλειάδας με κωδικό a ως προς τη βάση b. Τότε ισχύει:*

  $$a_i = El(a,b,i) \Leftrightarrow \exists\, x,y,z[i = z{+}1 \wedge a = xb^i{+}a_ib^z{+}y \wedge a_i < b \wedge y < b^z]$$

  Άρα η συνάρτηση $El(a,b,i)$ είναι διοφαντική.

5.3 Μερικές διοφαντικές σχέσεις

Θεώρημα 5.1 *Η συνάρτηση $f(n,m) = \binom{n}{m}$ είναι διοφαντική.*

Απόδειξη

Ισχύει $\quad (b+1)^n = \binom{n}{0}b^0 + \binom{n}{1}b^1 + \cdots + \binom{n}{n}b^n.$

Άρα η τριάδα $\quad \langle (b+1)^n, b, n+1\rangle \quad$ είναι κωδικός κατά θέση της $n+1-$άδας $\langle \binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}\rangle$ ως προς τη βάση b (για αρκετά μεγάλο b).

Παίρνοντας $b = 2^n + 1$ $\left(2^n = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}\right)$ προκύπτει ότι $c = \binom{n}{m} \Leftrightarrow c = El((2^n+1)^n, 2^n, m+1)$ και επειδή η συνάρτηση El είναι διοφαντική έπεται ότι και η συνάρτηση $f(n,m) = \binom{n}{m}$ είναι διοφαντική.

□

Θεώρημα 5.2 *Η συνάρτηση $g(m) = m!$ είναι διοφαντική.*

Απόδειξη
Ισχύει ότι $\displaystyle\binom{n}{m} = \frac{n!}{m!\,(n-m)!}$.
Άρα

$$\begin{aligned} m! &= \frac{n!}{\binom{n}{m}\,(n-m)!} \\ &= \frac{[n-(m-1)]\dots(n-1)n}{\binom{n}{m}} \\ &= \frac{n^m}{\binom{n}{m}}\left(1-\frac{m-1}{n}\right)\cdots 1 \\ &\le \frac{n^m}{\binom{n}{m}} \end{aligned}$$

Επίσης

$$\begin{aligned} \frac{n^m}{\binom{n}{m}} &= \frac{n^m m!(n-m)!}{n!} \\ &= \frac{m!n^m}{[n-(m-1)]\dots(n-1)n} \\ &= \frac{m!}{\left(1-\frac{m-1}{n}\right)\left(1-\frac{1}{n}\right)} \\ &\le \frac{m!}{\left(1-\frac{m}{n}\right)^m} \\ &\le m!\left(1+\frac{2m^2}{n}\right) \end{aligned}$$

Άρα για αρκετά μεγάλο n, όπως για παράδειγμα για $n = 2m^{m+2}+1$, έχουμε ότι: $m! = (2m^{m+2}+1)^m \, div \displaystyle\binom{2m^{m+2}+1}{m}$. Επειδή οι διωνυμικοί συντελεστές και η συνάρτηση "div" είναι διοφαντικές έπεται ότι και η συνάρτηση παραγοντικό είναι διοφαντική. □

Θεώρημα 5.3 *Η ιδιότητα $Prime(a)$: 'ο a είναι πρώτος αριθμός' είναι διοφαντική.*

Απόδειξη
$Prime(a) \Leftrightarrow a > 1 \ \& \ \gcd(a,(a-1)!) = 1$

Η συνάρτηση gcd καθώς επίσης και το παραγοντικό είναι διοφαντικές και άρα η ιδιότητα "$Prime(a)$" είναι διοφαντική. $\square$

5.4 Σχέσεις μεταξύ πλειάδων φυσικών αριθμών

Μεταξύ δύο πλειάδων φυσικών αριθμών ορίζονται οι σχέσεις "$Equal$", "$NotGreater$", "$Small$" ως εξής:

- $Equal(a_1, b_1, c_1, a_2, b_2, c_2) \Leftrightarrow < a_1, b_1, c_1 >$ και $< a_2, b_2, c_2 >$ είναι κωδικοί της ιδιας πλειάδας αριθμών

- $$NotGreater(a_1, b_1, a_2, b_2) \Leftrightarrow \exists c\big[Code(a_1, b_1, c) \,\&\, Code(a_2, b_2, c) \\ \&\, \forall k \leq c\,[El(a_1, b_1, k) \leq El(a_2, b_2, k)]\big]$$

- $Small(a, b, c, e) \Leftrightarrow Code(a, b, c) \;\&\; \forall k \leq c\,[El(a, b, k) \leq e]$

Θα αποδείξουμε ότι οι παραπάνω σχέσεις είναι διοφαντικές. Για να το δείξουμε αυτό θα χρησιμοποιήσουμε τις σχέσεις "$PNotGreater$", "$PSmall$", "Eq" και τη συνάρτηση "$Repeat$" οι οποίες ορίζονται ως εξής:

- $PNotGreater(a_1, a_2, b) \Leftrightarrow Prime(b) \quad \& \quad NotGreater(a_1, b, a_2, b)$

  Από το θεώρημα του Kummer (3.2) ισχύει ότι:
  $PNotGreater(a_1, a_2, b) \Leftrightarrow Prime(b) \wedge b \nmid \binom{a_2}{a_1}$
  Επειδή η ιδιότητα "$Prime$" και η σχέση "$\nmid$" είναι διοφαντικές έπεται ότι και η σχέση "$PNotGreater$" είναι διοφαντική.

- Η συνάρτηση $Repeat(p, q, r)$ δίνει τον κωδικό της πλειάδας $\langle p, \ldots, p\rangle$ μήκους r ως προς τη βάση q όπου ισχύει $p < q$.
  Ισχύει ότι $Repeat(p, q, r) = \dfrac{p\,(q^r - 1)}{q - 1}$.
  Επειδή η εκθετική συνάρτηση είναι διοφαντική, έπεται ότι και η συνάρτηση $Repeat(p, q, r)$ είναι διοφαντική.

- $PSmall(a, b, c, e) \Leftrightarrow Prime(b) \quad \& \quad Small(a, b, c, e)$

$$\begin{aligned} PSmall(a, b, c, e) &\Leftrightarrow Prime(b) \;\&\; Code(a, b, c) \;\&\; \forall k \leq c\,[El(a, b, k) \leq e] \\ &\Leftrightarrow Prime(b) \;\&\; \begin{cases} b \leq e \\ \text{ή} \\ PNotGreater(a, Repeat(e, b, c), b) \end{cases} \end{aligned}$$

Άρα $PSmall(a,b,c,e) \Leftrightarrow Prime(b)$ &
$$[b \leq e \vee PNotGreater(a, Repeat(e,b,c), b)]$$
Άρα η σχέση $PSmall(a,b,c,e)$ είναι διοφαντική.

- $Eq(a_1,b_1,c_1,a_2,b_2,c_2) \Leftrightarrow Code(a_1,b_1,c_1)$ & $c_1 = c_2$ &
$$PSmall(a_2,b_2,c_2,b_1-1) \ \&$$
$$b_1^{c_1} + b_1 < b_2 \ \&\ a_1 \equiv a_2 \pmod{b_2 - b_1}$$
Παρατηρούμε ότι η σχέση $Eq(a_1,b_1,c_1,a_2,b_2,c_2)$ είναι διοφαντική.

Λήμμα 5.1 *Αν $\langle a_2, b_2, c\rangle$ είναι ο κωδικός κατά θέση κάποιας πλειάδας φυσικών αριθμών, της οποίας κάθε στοιχείο είναι μικρότερο από το b_1 και a_1 είναι ο κωδικός της ίδιας πλειάδας ως προς τη βάση b_1. Τότε:*

$$\begin{gathered} a_1 \equiv a_2 \pmod{b_2 - b_1} \\ a_1 < b_1^c \end{gathered} \tag{5.1}$$

Απόδειξη
Είναι $a_2 = e_c b_2^{c-1} + \cdots + e_1 b_2^0$ και $a_1 = e_c b_1^{c-1} + \cdots + e_1 b_1^0$. Προφανώς ισχύει $a_1 < b_1^c$. Τότε $a_2 - a_1 = e_c(b_2^{c-1} - b_1^{c-1}) + \cdots + e_2(b_2 - b_1)$. Άρα $b_2 - b_1 \mid a_2 - a_1$ που σημαίνει ότι $a_1 \equiv a_2 \pmod{b_2 - b_1}$. □

Παρατήρηση 5.3 *Αν $b_1^c < b_2 - b_1$, που σημαίνει ότι το b_2 είναι αρκετά μεγάλο, τότε το a_1 ορίζεται μοναδικά από τις σχέσεις 5.1*

Σύμφωνα με το Λήμμα 5.1 η σχέση $Eq(a_1,b_1,c_1,a_2,b_2,c_2)$ εκφράζει το εξής:
Η τριάδα $\langle a_1,b_1,c_1\rangle$ είναι κωδικός κατά θέση πλειάδας, της οποίας και η τριάδα $\langle a_2,b_2,c_2\rangle$, όπου b_2 πρώτος, είναι επίσης κωδικός κατά θέση.
Προφανώς ισχύει: $Eq(a_1,b_1,c_1,a_2,b_2,c_2) \Rightarrow Equal(a_1,b_1,c_1,a_2,b_2,c_2)$.

Έχοντας δείξει ότι οι παραπάνω σχέσεις είναι διοφαντικές εύκολα αποδεικνύεται ότι και οι σχέσεις "$Equal$", "$NotGreater$", "$Small$" είναι επίσης διοφαντικές.
Πράγματι:

$$Equal(a_1,b_1,c_1,a_2,b_2,c_2) \Leftrightarrow$$
$$\exists x,y,z[Eq(a_1,b_1,c_1,x,y,z) \ \wedge\ Eq(x,y,z,a_2,b_2,c_2)]$$

$$NotGreater(a_1, b_1, a_2, b_2) \Leftrightarrow$$
$$\exists x_1, x_2, y, z[Equal(a_1, b_1, z, x_1, y, z) \ \wedge \ Equal(a_2, b_2, z, x_2, y, z) \wedge PNotGreater(x_1, x_2, y)]$$

$$Small(a, b, c, e) \ \Leftrightarrow \ \exists x, y, z[Equal(a, b, c, x, y, z) \quad \wedge \quad PSmall(x, y, z, e)]$$

6 Κωδικοποίηση διοφαντικών σχέσεων και συναρτήσεων

6.1 Καθολική διοφαντική εξίσωση

Ορισμός 6.1 *'Καθολική διοφαντική εξίσωση' είναι μια διοφαντική εξίσωση της μορφής* $U(a_1,\ldots,a_n,k_1,\ldots,k_l,y_1,\ldots,y_w)=0$*, όπου* $a_1,\ldots,a_n,k_1,\ldots,k_l$ *είναι παράμετροι και* $y_1,\ldots,y_w$ *είναι άγνωστοι, τέτοια που για κάθε διοφαντική εξίσωση* $D(a_1,\ldots,a_n,x_1,\ldots,x_m)=0$ *με* n *παραμέτρους και αυθαίρετο αριθμό αγνώστων, υπάρχουν αριθμοί* $k_1^D,\ldots,k_l^D$ *ώστε η εξίσωση*
$D(a_1,\ldots,a_n,x_1,\ldots,x_m)=0$ *έχει λύση στους αγνώστους* $x_1,\ldots,x_m$ *για εκείνα τα* $a_1,\ldots,a_n$ *για τα οποία η εξίσωση* $U(a_1,\ldots,a_n,k_1,\ldots,k_l,y_1,\ldots,y_w)=0$ *έχει λύση στους αγνώστους* $y_1,\ldots,y_w$.
Οι παράμετροι $a_1,\ldots,a_n$ *λέγονται '***παράμετροι στοιχείων***'.*
Οι παράμετροι $k_1,\ldots,k_l$ *λέγονται '***παράμετροι κωδικών***'.*

Παρατήρηση 6.1 *Έστω* $\mathfrak{M}$ *διοφαντικό σύνολο διάστασης* n *και*
$D(a_1,\ldots,a_n,x_1,\ldots,x_m)=0$ *η διοφαντική εξίσωση που το ορίζει.*
Αν $U(a_1,\ldots,a_n,k_1,\ldots,k_l,y_1,\ldots,y_w)=0$ *είναι καθολική διοφαντική εξίσωση με* n *παραμέτρους στοιχείων από τον ορισμό 6.4 έχουμε ότι υπάρχουν αριθμοί* $k_1^D,\ldots,k_l^D$ *ώστε:*

$$\begin{aligned}\langle a_1,\ldots,a_n\rangle\in\mathfrak{M} &\Leftrightarrow \exists x_1,\ldots,x_m[D(a_1,\ldots,a_n,x_1,\ldots,x_m)=0]\\ &\Leftrightarrow \exists y_1,\ldots,y_w[U(a_1,\ldots,a_n,k_1^D,\ldots,k_l^D,y_1,\ldots,y_w)=0]\end{aligned}$$

Δηλαδή το $\mathfrak{M}$ *αναπαρίσταται από την καθολική διοφαντική εξίσωση*

$$U(a_1,\ldots,a_n,k_1,\ldots,k_l,y_1,\ldots,y_w)=0,$$

και η πλειάδα $\langle k_1^D,\ldots,k_l^D\rangle$ *είναι κωδικός του διοφαντικού συνόλου* $\mathfrak{M}$.

Λήμμα 6.1 *Αν* $U(a_1,\ldots,a_n,k_1,\ldots,k_l,y_1,\ldots,y_w)=0$ *είναι καθολική διοφαντική εξίσωση με* n *παραμέτρους στοιχείων,* l *παραμέτρους κωδικών και* w *αγνώστους, τότε και η εξίσωση* $V(a_1,\ldots,a_n,k,k_1,\ldots,k_l,y_1,\ldots,y_w)=0$ *όπου*

$$\begin{aligned}&V(a_1,\ldots,a_n,k,k_1,\ldots,k_l,y_1,\ldots,y_w)=\\ &\qquad U^2(a_1,\ldots,a_n,k_1,\ldots,k_l,y_1,\ldots,y_w)+[k-2^{2^l}Cantor_l(k_1,\ldots,k_l)]^2\end{aligned}$$

είναι καθολική διοφαντική εξίσωση με n *παραμέτρους στοιχείων, 1 παράμετρο κωδικού και* $l+w$ *αγνώστους.*

Απόδειξη
Έστω $D(a_1,\ldots,a_n,x_1,\ldots,x_m)=0$ διοφαντική εξίσωση με n παραμέτρους. Εφόσον $U(a_1,\ldots,a_n,k_1,\ldots,k_l,y_1,\ldots,y_w)=0$ είναι καθολική διοφαντική εξίσωση με n παραμέτρους στοιχείων, υπάρχουν αριθμοί $k_1^D,\ldots,k_l^D$ ώστε:

$$\exists x_1,\ldots,x_m[D(a_1,\ldots,a_n,x_1,\ldots,x_m)=0] \Leftrightarrow \\ \exists y_1,\ldots,y_w[U(a_1,\ldots,a_n,k_1^D,\ldots,k_l^D,y_1,\ldots,y_w)=0]$$

Ισχυρισμός: Υπάρχει ο αριθμός $k^D=2^{2^l}Cantor_l(k_1^D,\ldots,k_l^D)$ ώστε:

$$\exists y_1,\ldots,y_w[U(a_1,\ldots,a_n,k_1^D,\ldots,k_l^D,y_1,\ldots,y_w)=0] \Leftrightarrow \\ \exists k_1,\ldots,k_l,y_1,\ldots,y_w[V(a_1,\ldots,a_n,k^D,k_1,\ldots,k_l,y_1,\ldots,y_w)=0]$$

Πράγματι:

- Αν $\exists y_1,\ldots,y_w[U(a_1,\ldots,a_n,k_1^D,\ldots,k_l^D,y_1,\ldots,y_w)=0]$ τότε $\exists k_1,\ldots,k_l,y_1,\ldots,y_w[V(a_1,\ldots,a_n,k^D,k_1,\ldots,k_l,y_1,\ldots,y_w)=0]$

- Αν $\exists k_1,\ldots,k_l,y_1,\ldots,y_w[V(a_1,\ldots,a_n,k^D,k_1,\ldots,k_l,y_1,\ldots,y_w)=0]$ τότε $\exists k_1,\ldots,k_l,y_1,\ldots,y_w[U(a_1,\ldots,a_n,k_1,\ldots,k_l,y_1,\ldots,y_w)=0]$ και $k^D=2^{2^l}Cantor_l(k_1,\ldots,k_l)$. Όμως $k^D=2^{2^l}Cantor_l(k_1^D,\ldots,k_l^D)$ και άρα $k_1=k_1^D,\ldots,k_l=k_l^D$.
  Άρα $\exists y_1,\ldots,y_w[U(a_1,\ldots,a_n,k_1^D,\ldots,k_l^D,y_1,\ldots,y_w)=0]$.

Άρα υπάρχει αριθμός k^D ώστε:

$$\exists x_1,\ldots,x_m[D(a_1,\ldots,a_n,x_1,\ldots,x_m)=0] \Leftrightarrow \\ \exists k_1,\ldots,k_l,y_1,\ldots,y_w[V(a_1,\ldots,a_n,k^D,k_1,\ldots,k_l,y_1,\ldots,y_w)=0]$$

Δηλαδή η διοφαντική εξίσωση $V(a_1,\ldots,a_n,k,k_1,\ldots,k_l,y_1,\ldots,y_w)=0$ είναι καθολική.

Παρατήρηση 6.2 *Αν $\mathfrak{M}$ διοφαντικό σύνολο διάστασης n και $\langle k_1^D,\ldots,k_l^D\rangle$ ο κωδικός αυτού, τότε το $\mathfrak{M}$ μπορεί να αναπαρασταθεί από μια καθολική διοφαντική εξίσωση με n παραμέτρους στοιχείων και 1 παράμετρο κωδικού και ο κωδικός του ως προς αυτή την αναπαράσταση είναι $k^D=2^{2^l}Cantor_l(k_1^D,\ldots,k_l^D)$.*
$\square$

6.2 Κωδικοποίηση μιας διοφαντικής εξίσωσης

Έστω $D(x_0, \ldots, x_m) = 0$ μια διοφαντική εξίσωση. Ισχύει:

$$D(x_0, \ldots, x_m) = C_L(x_0, \ldots, x_m) - C_R(x_0, \ldots, x_m)$$

όπου C_L, C_R είναι πολυώνυμα με συντελεστές φυσικούς αριθμούς.

$\langle b, c, d, e, f \rangle$ είναι κωδικός ενός πολυωνύμου $C(x_0, \ldots, x_m)$ με συντελεστές φυσικούς αριθμούς αν:

- e είναι ο αριθμός των αγνώστων στο πολυώνυμο C.
- d είναι ένας αριθμός μεγαλύτερος από τον ολικό βαθμό του C.
- $f = 2^{d^1} + \cdots + 2^{d^e}$.
- c ειναι ο κωδικός του πολυωνύμου C ως προς τη βάση b.
  Δηλαδή αν $c_{i_0 \ldots i_m}$ είναι ο συντελεστής του όρου $x_0^{i_0} \cdots x_m^{i_m}$ στο πολυώνυμο C τότε:

  $$c = \sum_{i_0 + \cdots + i_m < d} i_0! \cdots i_m!(d-1-i_0-\cdots-i_m)! c_{i_0 \ldots i_m} b^{d^{m+1} - i_0 d^0 - \cdots - i_m d^m}.$$
- $b > d! \max\{c_{i_0 \ldots i_m}\}$.

$\langle b, c_L, c_R, d, e, f \rangle$ είναι κωδικός της διοφαντικής εξίσωσης $D(x_0, \ldots, x_m) = 0$ αν:

- $\langle b, c_L, d, e, f \rangle$ είναι κωδικός του πολυωνύμου C_L.
- $\langle b, c_R, d, e, f \rangle$ είναι κωδικός του πολυωνύμου C_R.

Παρατήρηση 6.3

- *Η τριάδα $\langle d, e, f \rangle$ καλείται 'μορφή' της διοφαντικής εξίσωσης $D(x_0, \ldots, x_m) = 0$.*
- *Ορίζουμε τη σχέση:* $Format(d, e, f) \Leftrightarrow f = 2^{d^1} + \cdots + 2^{d^e}$

- *Ορίζουμε τη σχέση:*

$$ECode(b, c_L, c_R, d, e, f) \Leftrightarrow$$
$$\langle b, c_L, c_R, d, e, f\rangle \textit{είναι κωδικός μιας διοφαντικής εξίσωσης}$$

Οι σχέσεις "Format" και "ECode" είναι διοφαντικές.

6.3 Κωδικοποίηση των πιθανών λύσεων μιας διοφαντικής εξίσωσης

$\langle d, e, f, g, h\rangle$ είναι κωδικός μιας πιθανής λύσης $\langle x_1, \ldots, x_m\rangle$ μιας διοφαντικής εξίσωσης $D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$ αν:

- $\langle d, e, f\rangle$ είναι 'μορφή' της διοφαντικής εξίσωσης $D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$.
- g είναι αριθμός μεγαλύτερος από τους $1, x_1, \ldots, x_m$.
- $h = x_1 g^{d^1} + \cdots + x_m g^{d^m}$

Ορίζουμε τις σχέσεις:

$$SCode(d, e, f, g, h) \Leftrightarrow \langle d, e, f, g, h\rangle$$
$$\text{είναι κωδικός μιας πιθανής λύσης μιας διοφαντικής εξίσωσης}$$

$$SC(d, e, f, g, h) \Leftrightarrow$$
$$\exists t[Equal(f, 2, d^e + 1, t, g, d^e + 1) \wedge NotGreater(h, (g-1)t, g)]$$

Προφανώς η σχέση "SC" είναι διοφαντική.

Λήμμα 6.2

$$Format(d, e, f) \Longrightarrow [SC(d, e, f, g, h) \Leftrightarrow SCode(d, e, f, g, h)]$$

Απόδειξη
Αν ισχύει η σχέση $Format(d, e, f)$ τότε $f = 2^{d^1} + \cdots + 2^{d^e}$.

($\Longrightarrow$): Αν ισχύει $SC(d,e,f,g,h)$ τότε υπάρχει t τέτοιο ώστε $t = g^{d^1} + \cdots + g^{d^e}$ και επειδή ισχύει η σχέση $NotGreater(h,(g-1)t,g)$ έπεται ότι $h = x_1 g^{d^1} + \cdots + x_e g^{d^e}$ όπου $x_i < g,\ i = 1,\ldots,e$. Άρα $\langle d,e,f,g,h\rangle$ είναι κωδικός της πιθανής λύσης $x_1,\ldots,x_e$ της διοφαντικής εξίσωσης $D(a_1,\ldots,a_n,x_1,\ldots,x_e) = 0$. Άρα ισχύει η σχέση $SCode(d,e,f,g,h)$.

($\Longleftarrow$): Έστω ότι ισχύει η σχέση $SCode(d,e,f,g,h)$.
Τότε $h = x_1 g^{d^1} + \cdots + x_e g^{d^e}$ και $g > 1, x_1,\ldots,x_e$. Επίσης υπάρχει t ώστε να ισχύει η σχέση $Equal(f,2,d^e+1,t,g,d^e+1)$ και αυτό είναι το $t = g^{d^1} + \cdots + g^{d^e}$. Άρα ισχύει και ότι $NotGreater(h,(g-1)t,g)$, που σημαίνει ότι ισχύει η σχέση $SC(d,e,f,g,h)$. $\Box$

Λήμμα 6.3 *Αν $\langle b,c,d,e,f\rangle$ είναι κωδικός του πολυωνύμου $C(a,x_1,\ldots,x_m)$ και $\langle d,e,f,g,h\rangle$ ο κωδικός μιας πιθανής λύσης του $\langle y_1,\ldots,y_m\rangle$, τότε υπάρχει $w > (1+a+h)^{d-1}c$ και $s,\ t$ ώστε:*

$$C(a,y_1,\ldots,y_m) = \frac{El\left((1+aw+t)^{d-1}s, w, d^e+1\right)}{(d-1)!}$$

Απόδειξη
$\langle b,c,d,e,f\rangle$: κωδικός του πολυωνύμου $C(a,x_1,\ldots,x_m)$
$\langle d,e,f,g,h\rangle$: κωδικός μιας πιθανής λύσης $\langle y_1,\ldots,y_m\rangle$
Έστω w ένας αρκετά μεγάλος αριθμός. Χρησιμοποιώντας ως βάση το w παίρνουμε:

$$s = \sum_{i_0+\cdots+i_m<d} i_0!\cdots i_m!(d-1-i_0-\cdots-i_m)!\, c_{i_0\ldots i_m}\, w^{d^{m+1}-i_0 d^0-\cdots-i_m d^m}$$

$$t = y_1 w^{d^1} + \cdots + y_m w^{d^m}$$

Τότε ισχύουν οι σχέσεις:

$$Equal\,(c,b,d^{e+1}+1,s,w,d^{e+1}+1) \quad \text{και} \quad Equal\,(h,g,d^e+1,t,g,d^e+1).$$

Επίσης $\langle w,s,d,e,f\rangle$ είναι κωδικός του πολυωνύμου $C(a,x_1,\ldots,x_m)$ και $\langle d,e,f,w,t\rangle$ είναι κωδικός της πιθανής λύσης $\langle y_1,\ldots,y_m\rangle$.

$$\text{Ισχύει:}\quad (1+aw+t)^{d-1} = (1+aw^{d^0}+y_1 w^{d^1}+\cdots+y_m w^{d^m})^{d-1}$$
$$= \sum_{i_0+\cdots+i_m<d} \binom{d-1}{i_0\cdots i_m} a^{i_0} y_1^{i_1}\cdots y_m^{i_m}\, w^{i_0 d^0+\cdots+i_m d^m}$$

$$\text{Τότε:}\quad (1+aw+t)^{d-1}s = \sum_{k=0}^{2d^{m+1}-1} C_k\, w^k,$$

όπου C_k είναι εκφράσεις που περιέχουν τα $a, y_1, \ldots, y_m, c_{i_0\ldots i_m}$. Τότε:

$$\begin{aligned} C_{d^{e+1}} &= \sum_{i_0+\cdots+i_m<d} i_0!\cdots i_m! \binom{d-1}{i_0\cdots i_m} c_{i_0\ldots i_m}\, a^{i_0} y_1^{i_1}\cdots y_m^{i_m} \\ &= (d-1)!\, C(a, y_1, \ldots, y_m) \end{aligned}$$

Αν $w > C_0, C_1, \ldots, C_{2d^{m+1}-1}$ τότε:

$$C(a, y_1, \ldots, y_m) = \frac{El\left((1+aw+t)^{d-1}s, w, d^e+1\right)}{(d-1)!}$$

Άρα, αν $w > (1+a+h)^{d-1}c$ τότε:

$$C(a, y_1, \ldots, y_m) = \frac{El\left((1+aw+t)^{d-1}s, w, d^e+1\right)}{(d-1)!} \quad \square$$

Ορισμός 6.2 *Ορίζουμε τη σχέση:*

$$\begin{aligned} Solution(a, b, c_L, c_R, d, e, f, g, h) \Leftrightarrow SC(d, e, f, g, h)\ \wedge \exists s_L, s_R, t, w \\ [w > (1+a+h)^{d-1}(c_L+c_R) \\ \wedge\ Equal\,(c_L, b, d^{e+1}+1, s_L, w, d^{e+1}+1) \\ \wedge\ Equal\,(c_R, b, d^{e+1}+1, s_R, w, d^{e+1}+1) \\ \wedge\ Equal\,(h, g, d^e+1, t, w, d^e+1) \\ \wedge\ El\left((1+aw+t)^{d-1}s_L, w, d^e+1\right) = El\left((1+aw+t)^{d-1}s_R, w, d^e+1\right)] \end{aligned}$$

Η σχέση "Solution" είναι διοφαντική.

Λήμμα 6.4

$$\begin{aligned} &ECode(b, c_L, c_R, d, e, f) \Longrightarrow \\ &\quad \Big[\exists g, h[SCode(d, e, f, g, h)\ \wedge\ Solution(a, b, c_L, c_R, d, e, f, g, h)] \Leftrightarrow \\ &\qquad\qquad \exists x_1, \ldots, x_m[D_{b,c_L,c_R,d,e,f}(a, x_1, \ldots, x_m) = 0]\Big] \end{aligned}$$

όπου $D_{b,c_L,c_R,d,e,f}(a, x_1, \ldots, x_m) = 0$ *είναι η διοφαντική εξίσωση με κωδικό* $\langle b, c_L, c_R, d, e, f\rangle$.

Απόδειξη
Ισχύει η σχέση $ECode(b, c_L, c_R, d, e, f)$, άρα και η $Format(d, e, f)$. Έστω η διοφαντική εξίσωση $D_{b,c_L,c_R,d,e,f}(a, x_1, \ldots, x_m) = 0$ με κωδικό $\langle b, c_L, c_R, d, e, f\rangle$.

($\Longrightarrow$): Έστω ότι υπάρχουν g, h ώστε να ισχύουν οι σχέσεις $SCode(d, e, f, g, h)$ και $Solution(a, b, c_L, c_R, d, e, f, g, h)$. Τότε $\langle d, e, f, g, h\rangle$ κωδικός μιας πιθανής λύσης της εξίσωσης $D_{b,c_L,c_R,d,e,f}(a, x_1, \ldots, x_m) = 0$ και λόγω του ορισμού 6.2 και του λήμματος 6.3, έπεται ότι υπάρχουν $x_1, \ldots, x_m$ ώστε $D_{b,c_L,c_R,d,e,f}(a, x_1, \ldots, x_m) = 0$.

($\Longleftarrow$): Έστω ότι η εξίσωση $D_{b,c_L,c_R,d,e,f}(a, x_1, \ldots, x_m) = 0$ έχει λύση στους $x_1, \ldots, x_m$. Τότε υπάρχουν g, h ώστε $\langle d, e, f, g, h\rangle$ να είναι κωδικός της λύσης αυτής και άρα ισχύει η σχέση $SCode(d, e, f, g, h)$ και επειδή ισχύει επίσης η $Format(d, e, f)$ έπεται ότι ισχύει και η $SC(d, e, f, g, h)$. Επίσης από το λήμμα 6.3 έπεται ότι υπάρχουν s_L, s_R, t, w ώστε:

$$w > (1 + a + h)^{d-1}(c_L + c_R)$$

$$Equal\,(c_L, b, d^{e+1} + 1, s_L, w, d^{e+1} + 1)$$

$$Equal\,(c_R, b, d^{e+1} + 1, s_R, w, d^{e+1} + 1)$$

$$Equal\,(h, g, d^e + 1, t, w, d^e + 1)$$

και επειδή $C_L(a, x_1, \ldots, x_m) = C_R(a, x_1, \ldots, x_m)$ έπεται ότι:

$$El\,((1 + aw + t)^{d-1}s_L, w, d^e + 1) = El\,((1 + aw + t)^{d-1}s_R, w, d^e + 1)$$

Άρα ισχύει και η σχέση $Solution(a, b, c_L, c_R, d, e, f, g, h)$. $\square$

6.4 Κωδικοποίηση διοφαντικών συνόλων

Λήμμα 6.5 *Υπάρχει μια καθολική διοφαντική εξίσωση* $U_1(a, k, y_1, \ldots, y_m) = 0$ *με 1 παράμετρο στοιχείων, 1 παράμετρο κωδικών και* m *αγνώστους (*m*:σταθερό).*

Απόδειξη

Βήμα 1. Κατασκευή μιας καθολική διοφαντικής εξίσωσης με 1 παράμετρο στοιχείων, 6 παραμέτρους κωδικών και $m - 6$ αγνώστους.

Η σχέση $Solution(a, b, c_L, c_R, d, e, f, g, h)$ είναι διοφαντική, και έστω $U(a, b, c_L, c_R, d, e, f, g, h, y_9, \ldots, y_m) = 0$ η διοφαντική εξίσωση που την ορίζει. Τότε:

$$Solution(a, b, c_L, c_R, d, e, f, g, h) \Leftrightarrow$$
$$\exists y_9, \ldots, y_m[U(a, b, c_L, c_R, d, e, f, g, h, y_9, \ldots, y_m) = 0]$$

Έστω $D(a, x_1, \ldots, x_w) = 0$ διοφαντική εξίσωση με 1 παράμετρο, και $\langle b^D, c_L^D, c_R^D, d^D, e^D, f^D \rangle$ ο κωδικός αυτής.
Τότε ισχύει η σχέση $ECode(b^D, c_L^D, c_R^D, d^D, e^D, f^D)$. Από το λήμμα 6.4 έπεται ότι:

$$\begin{aligned} &\exists g, h \big[SCode(d^D, e^D, f^D, g, h) \\ &\qquad \wedge \; Solution(a, b^D, c_L^D, c_R^D, d^D, e^D, f^D, g, h) \big] \Leftrightarrow \\ &\qquad\qquad \exists x_1, \ldots, x_w \, [D(a, x_1, \ldots, x_w) = 0] \end{aligned}$$

Δηλαδή,

$$\begin{aligned} &\exists g, h \big[SCode(d^D, e^D, f^D, g, h) \\ &\quad \wedge \; \exists y_9, \ldots, y_m [U(a, b^D, c_L^D, c_R^D, d^D, e^D, f^D, g, h, y_9, \ldots, y_m) = 0] \big] \Leftrightarrow \\ &\qquad\qquad \exists x_1, \ldots, x_w \, [D(a, x_1, \ldots, x_w) = 0] \end{aligned}$$

Άρα:

$$\begin{aligned} \forall a \Big[&\exists y_7, \ldots, y_m [U(a, b^D, c_L^D, c_R^D, d^D, e^D, f^D, y_7, \ldots, y_m) = 0] \Leftrightarrow \\ &\qquad\qquad \exists x_1, \ldots, x_w \, [D(a, x_1, \ldots, x_w) = 0] \Big] \end{aligned}$$

Συνεπώς η διοφαντική εξίσωση $U(a, b, c_L, c_R, d, e, f, y_7, \ldots, y_m) = 0$ είναι καθολική, με 1 παράμετρο στοιχείων, 6 παραμέτρους κωδικών και $m-7$ αγνώστους.

Βήμα 2. Κατασκευή μιας καθολική διοφαντικής εξίσωσης με 1 παράμετρο στοιχείων, 1 παράμετρο κωδικών και m αγνώστους.

Θέτουμε

$$\begin{aligned} &U_1(a, k, y_1, \ldots, y_m) = \\ &U^2(a, b, c_L, c_R, d, e, f, y_7, \ldots, y_m) + \big[k - 2^{2^6} Cantor_6(b, c_L, c_R, d, e, f) \big] \end{aligned}$$

Τότε από το λήμμα 6.1 έπεται ότι η $U_1(a, y_1, \ldots, y_m)$ είναι καθολική διοφαντική εξίσωση με 1 παράμετρο στοιχείων, 1 παραμέτρο κωδικών και m αγνώστους. $\square$

Πόρισμα 6.1 *Κάθε διοφαντικό σύνολο διάστασης* 1 *μπορεί να αναπαρασταθεί από την καθολική διοφαντική εξίσωση* $U_1(a,k,y_1,\ldots,y_m)=0$ *και ο κωδικός του είναι ο* $k^D = 2^{2^6} Cantor_6(b,c_L,c_R,d,e,f)$ *όπου* $\langle b,c_L,c_R,d,e,f\rangle$ *ο κωδικός της εξίσωσης που το ορίζει.*

Θεώρημα 6.1 *Υπάρχει* m *(σταθερό) ώστε για κάθε* n *υπάρχει καθολική διοφαντική εξίσωση* $U_n(a_1,\ldots,a_n,k,y_1,\ldots,y_m)=0$ *με* n *παραμέτρους στοιχείων,* 1 *παράμετρο κωδικών και* m *αγνώστους.*

Απόδειξη

Για $n=1$ το θεώρημα ισχύει εφόσον έχει δειχθεί στο λήμμα 6.5 ότι υπάρχει η καθολική διοφαντική εξίσωση $U_1(a,k,y_1,\ldots,y_m)=0$ με 1 παράμετρο στοιχείων, 1 παραμέτρο κωδικών και m αγνώστους, η οποία κωδικοποιεί τα διοφαντικά σύνολα διάστασης 1.

Έστω ότι $n>1$.

Θέτουμε

$$U_n(a_1,\ldots,a_n,k,y_1,\ldots,y_m) = U_1(2^{2^n} Cantor_n(a_1,\ldots,a_n),k,y_1,\ldots,y_m)$$

Η εξίσωση $U_n(a_1,\ldots,a_n,k,y_1,\ldots,y_m)=0$ είναι καθολική.

Πράγματι: Έστω $D(a_1,\ldots,a_n,x_1,\ldots,x_w)=0$ μια διοφαντική εξίσωση με n παραμέτρους. Θεωρούμε τη διοφαντική εξίσωση:

$$\begin{aligned} &D_1(a,z_1,\ldots,z_n,x_1,\ldots,x_w) = \\ &\qquad D^2(z_1,\ldots,z_n,x_1,\ldots,x_w) + \big[a - 2^{2^n} Cantor_n(z_1,\ldots,z_n)\big]. \end{aligned}$$

Εφόσον η $U_1(a,k,y_1,\ldots,y_m)=0$ είναι καθολική έπεται ότι υπάρχει k^{D_1} ώστε η εξίσωση $D_1(a,z_1,\ldots,z_n,x_1,\ldots,x_w)=0$ έχει λύση για εκείνα τα a για τα οποία η εξίσωση $U_1(a,k^{D_1},y_1,\ldots,y_m)=0$ έχει λύση στους $y_1,\ldots,y_m$. Όμως ισχύει ότι:

$$\begin{aligned} &\exists x_1,\ldots,x_w\big[D_1(2^{2^n} Cantor_n(a_1,\ldots,a_n),a_1,\ldots,a_n,x_1,\ldots,x_w)=0\big] \Leftrightarrow \\ &\qquad \exists x_1,\ldots,x_w\big[D(a_1,\ldots,a_n,x_1,\ldots,x_w)=0\big]. \end{aligned}$$

Άρα ισχύει:

$$\begin{aligned} &\exists x_1,\ldots,x_w\big[D(a_1,\ldots,a_n,x_1,\ldots,x_w)=0\big] \\ &\quad \Leftrightarrow \exists y_1,\ldots,y_m\big[U_1(2^{2^n} Cantor_n(a_1,\ldots,a_n),k^{D_1},y_1,\ldots,y_m)=0\big] \\ &\qquad \Leftrightarrow \exists y_1,\ldots,y_m\big[U_n(a_1,\ldots,a_n,k^{D_1},y_1,\ldots,y_m)=0\big]. \end{aligned}$$

Άρα η διοφαντική εξίσωση $U_n(a_1,\ldots,a_n,k,y_1,\ldots,y_m)=0$ είναι καθολική.

Για $n=0$, θέτουμε: $U_0(k,y_1,\ldots,y_m)=U_1(0,k,y_1,\ldots,y_m)$.
Έστω η διοφαντική εξίσωση $D(a,x_1,\ldots,x_w)=0$.
Εφόσον η $U_1(a,k,y_1,\ldots,y_m)=0$ είναι καθολική έπεται ότι υπάρχει k^D ώστε:

$$\begin{aligned}\exists x_1,\ldots,x_w[D(0,x_1,\ldots,x_w)=0] &\Leftrightarrow \exists y_1,\ldots,y_m[U_1(0,k^D,y_1,\ldots,y_m)=0]\\ &\Leftrightarrow \exists y_1,\ldots,y_m[U_0(k^D,y_1,\ldots,y_m)=0]\end{aligned}$$

Άρα η $U_0(k,y_1,\ldots,y_m)=0$ είναι καθολική. □

Πόρισμα 6.2 *Κάθε διοφαντικό σύνολο $\mathfrak{M}_i$ διάστασης n κωδικοποιείται με έναν αριθμό k_i τέτοιον που:*

$$\langle a_1,\ldots,a_n\rangle\in\mathfrak{M}_i\Leftrightarrow\exists y_1,\ldots,y_m[U_n(a_1,\ldots,a_n,k_i,y_1,\ldots,y_m)=0]$$

Θεώρημα 6.2 *Η κλάση των διοφαντικών σχέσεων κ.ο.κ. δεν είναι κλειστή ως προς την άρνηση $\neg$.*

Απόδειξη
Θεωρούμε το σύνολο $\mathfrak{M}=\{a\mid\exists y_1,\ldots,y_m[U_1(a,a,y_1,\ldots,y_m)=0]\}$ το οποίο είναι διοφαντικό. Συμβολίζουμε με $\overline{\mathfrak{M}}$ το συμπλήρωμα του $\mathfrak{M}$.
Έστω ότι το $\overline{\mathfrak{M}}$ είναι διοφαντικό σύνολο και έστω $k^{\overline{\mathfrak{M}}}$ ο κωδικός του. Τότε:

$$\beta\in\overline{\mathfrak{M}}\Leftrightarrow\exists y_1,\ldots,y_m[U_1(\beta,k^{\overline{\mathfrak{M}}},y_1,\ldots,y_m)=0] \tag{6.1}$$

- Έστω ότι υπάρχουν $y_1,\ldots,y_m$ ώστε να ισχύει
  $U_1(k^{\overline{\mathfrak{M}}},k^{\overline{\mathfrak{M}}},y_1,\ldots,y_m)=0$.
  Τότε από τον ορισμό του συνόλου $\mathfrak{M}$ έπεται ότι $k^{\overline{\mathfrak{M}}}\in\mathfrak{M}$. Επίσης από τη σχέση (6.1) έπεται ότι $k^{\overline{\mathfrak{M}}}\in\overline{\mathfrak{M}}$ το οποίο έρχεται σε αντίφαση με το προηγούμενο.

- Έστω ότι δεν υπάρχουν $y_1,\ldots,y_m$ ώστε να ισχύει $U_1(k^{\overline{\mathfrak{M}}},k^{\overline{\mathfrak{M}}},y_1,\ldots,y_m)=0$.
  Τότε από τον ορισμό του συνόλου $\mathfrak{M}$ έπεται ότι $k^{\overline{\mathfrak{M}}}\notin\mathfrak{M}$. Δηλαδή $k^{\overline{\mathfrak{M}}}\in\overline{\mathfrak{M}}$. Επίσης από τη σχέση (6.1) έπεται ότι $k^{\overline{\mathfrak{M}}}\notin\overline{\mathfrak{M}}$ το οποίο είναι άτοπο.

Άρα το συμπλήρωμα του $\mathfrak{M}$ δεν είναι διοφαντικό σύνολο. □

Παρατήρηση 6.4 *Συμβολίζουμε με $\mathfrak{M}_i^n$ το διοφαντικό σύνολο διάστασης n με κωδικό τον αριθμό i.*

7 Η λύση στο 10^o πρόβλημα του Hilbert

7.1 Η κλάση των διοφαντικών σχέσεων είναι κλειστή ως προς τους φραγμένους ποσοδείκτες

Θεώρημα 7.1 *Αν $R(a_1, \ldots, a_n)$ είναι διοφαντική σχέση, τότε:*

1. *Η σχέση $R_1(a_1, \ldots, a_n) \Leftrightarrow \exists y < a_n\, R(a_1, \ldots, a_{n-1}, y)$ είναι διοφαντική.*

2. *Η σχέση $R_2(a_1, \ldots, a_n) \Leftrightarrow \forall y < a_n\, R(a_1, \ldots, a_{n-1}, y)$ είναι διοφαντική.*

Απόδειξη
Το θεώρημα θα αποδειχθεί για την περίπτωση όπου $n = 2$.
Δηλαδή θα αποδειχθεί ότι αν $R(a, b)$ είναι διοφαντική σχέση τότε:

1. Η σχέση $R_1(a, b) \Leftrightarrow \exists y < b\, R(a, y)$ είναι διοφαντική.

2. Η σχέση $R_2(a, b) \Leftrightarrow \forall y < b\, R(a, y)$ είναι διοφαντική.

Εφόσον $R(a, b)$ είναι διοφαντική σχέση, έπεται ότι:

$$R(a, b) \Leftrightarrow \exists x_1, \ldots, x_m [D(a, b, x_1, \ldots, x_m) = 0] \tag{7.1}$$

όπου $D(a, b, x_1, \ldots, x_m) = 0$ είναι η διοφαντική εξίσωση που ορίζει τη σχέση $R(a, b)$.

1. Από τη σχέση (7.1) έπεται ότι:

   $$R_1(a, b) \Leftrightarrow \exists y < b\, \exists x_1, \ldots, x_m [D(a, y, x_1, \ldots, x_m) = 0]$$

   Δηλαδή

   $$R_1(a, b) \Leftrightarrow \exists y, x_1, \ldots, x_m [y < b \,\wedge\, D(a, y, x_1, \ldots, x_m) = 0]$$

   που σημαίνει ότι η σχέση $R_1(a, b)$ είναι διοφαντική.

2. Λόγω της σχέσης (7.1) ισχύει ότι:

   $$R_2(a, b) \Leftrightarrow \forall y < b\, \exists x_1, \ldots, x_m [D(a, y, x_1, \ldots, x_m) = 0].$$

Στη συνέχεια θα αποδειχθεί ότι:

$$\forall y < b\, \exists x_1, \ldots, x_m [D(a, y, x_1, \ldots, x_m) = 0] \Leftrightarrow$$
$$\exists q, w, z_0, \ldots, z_m \Bigg[b!(b + w + B(a, b, w))! \mid q + 1 \\ \wedge\ z_0 = q \\ \wedge\ \binom{q}{b} \Big| \binom{z_i}{w},\ i = 0, \ldots, m \\ \wedge\ D(a, z_0, \ldots, z_m) \equiv 0 \pmod{\binom{q}{b}} \Bigg]$$

όπου $B(a, b, w)$ είναι το πολυώνυμο που προκύπτει από το πολυώνυμο $D(a, b, x_1, \ldots, x_m)$ με αντικατάσταση όλων των αγνώστων x_i από το w.

($\Longrightarrow$): Έστω ότι $\forall y < b\, \exists x_1, \ldots, x_m [D(a, y, x_1, \ldots, x_m) = 0]$.
Δηλαδή $\exists x_{1y}, \ldots, x_{my} [D(a, y, x_{1y}, \ldots, x_{my}) = 0]$ για κάθε $y < b$.
Αυτό σημαίνει ότι υπάρχουν b τον αριθμό λύσεις $\langle x_{1y}, \ldots, x_{my} \rangle$ για $y = 0, \ldots, b - 1$ της εξίσωσης $D(a, y, x_1, \ldots, x_m) = 0$.
Επιλέγουμε έναν αριθμό w τέτοιον ώστε $x_{iy} < w$ για κάθε $i = 1, \ldots, m$ και για κάθε $y = 0, \ldots, b - 1$.
Επίσης διαλέγουμε έναν αριθμό q ώστε: $b!(b+w+B(a, b, w))! \mid q+1$.
Θέτουμε: $q_y = \dfrac{q + 1}{y + 1} - 1,\ y = 0, \ldots, b - 1$.
Τότε ισχύει ότι: $q_0 \cdots q_{b-1} = \prod_{y=0}^{b-1} \dfrac{q - y}{y + 1} = \dbinom{q}{b}$.

Ισχυρισμός 1: Οι $q_0, \ldots, q_{b-1}$ είναι σχετικά πρώτοι.
Πράγματι: Έστω $0 \le l \le k < b$ και έστω ότι $d | q_k$ και $d | q_l$.
Τότε $d \Big| \dfrac{q + 1}{k + 1} - 1$ και $d \Big| \dfrac{q + 1}{l + 1} - 1$ που σημαίνει ότι
$d \Big| q + 1 \left(\dfrac{1}{k + 1} - \dfrac{1}{l + 1} \right)$. Δηλαδή $d \Big| \dfrac{q + 1}{(k + 1)(l + 1)} (l - k)$.
Εφόσον $d \Big| \dfrac{q + 1}{k + 1} - 1$ έπεται ότι $\gcd(d, \dfrac{q + 1}{k + 1}) = 1$, που σημαίνει ότι $d \nmid \dfrac{q + 1}{k + 1}$. Όμοια $d \nmid \dfrac{q + 1}{l + 1}$ και $q + 1 = \lambda b!(b + w + B(a, b, w))!$.
Άρα $d \nmid \dfrac{q + 1}{(k + 1)(l + 1)}$ που σημαίνει ότι $d | \, l - k$.

Δηλαδή $d < l - k < b$ και επειδή $d \nmid \dfrac{q+1}{k+1}$ έπεται ότι $d \nmid 2, \ldots, d \nmid b-1$. Άρα $d = 1$.

Ισχυρισμός 2: $q_y, w!$ είναι σχετικά πρώτοι για $y = 0, \ldots, b-1$.
Πράγματι: Έστω $d|q_y$ και $d|w!$. Τότε έπεται ότι $d \nmid \dfrac{q+1}{y+1}$ και επειδή $q+1 = \lambda b!(b+w+B(a,b,w))!$ αν $d|w!$ τότε $d\Big| \dfrac{q+1}{y+1}$, το οποίο είναι άτοπο.

Εφόσον οι $q_0, \ldots, q_{b-1}$ είναι σχετικά πρώτοι, από το θεώρημα υπολοίπων του κινέζου, έπεται ότι υπάρχουν $z_1, \ldots, z_m$ τέτοια ώστε:

$$x_{iy} = rem(z_i, q_y),\ i = 1, \ldots, m,\ y = 0, \ldots, b-1.$$

Για τον ίδιο λόγο υπάρχει z_0 ώστε:

$$y = rem(z_0, q_y),\ y = 0, \ldots, b-1.$$

Τότε έπεται ότι:

$$D(a, y, x_{1y}, \ldots, x_{my}) \equiv D(a, y, z_0, \ldots, z_m) \pmod{q_y}$$

και επειδή $D(a, y, x_{1y}, \ldots, x_{my}) = 0$ για $y = 0, \ldots, b-1$ έπεται ότι:

$$\forall y < b[D(a, y, x_{1y}, \ldots, x_{my}) = 0] \Leftrightarrow$$

$$\forall y < b[D(a, y, z_0, \ldots, z_m) \equiv 0 \pmod{q_y}] \Leftrightarrow$$
$$D(a, y, z_0, \ldots, z_m) \equiv 0 \pmod{q_0 \cdots q_{b-1}} \Leftrightarrow$$
$$D(a, y, z_0, \ldots, z_m) \equiv 0 \pmod{\binom{q}{b}}.$$

Ισχύει ότι $y = rem(q, q_y)$ και άρα θέτοντας $z_0 = q$ έπεται ότι $y = rem(z_0, q_y)$.
Για $i = 1, \ldots, m$ και $y = 0, \ldots, b-1$ ισχύει ότι $x_{iy} = rem(z_i, q_y)$.
Τότε έπεται ότι $q_y | z_i - x_{iy}$ και επειδή $x_{iy} < w$ έπεται ότι $q_y \Big| \prod_{k=0}^{w-1}(z_i - k)$ που σημαίνει ότι $q_y \Big| \binom{z_i}{w} w!$ και επειδή $q_y, w!$ είναι σχετικά πρώτοι έπεται ότι $q_y \Big| \binom{z_i}{w}$. Δηλαδή για $i = 1, \ldots, m$ και

$y=0,\dots,b-1$ ισχύει ότι $q_y \Big| \binom{z_i}{w}$.

Άρα $q_0\cdots q_{b-1}\Big|\binom{z_i}{w},\ i=1,\dots,m$.

Δηλαδή $\binom{q}{b}\Big|\binom{z_i}{w},\ i=1,\dots,m$.

Άρα έπεται ότι υπάρχουν $q,w,z_0,\dots,z_m$ τέτοια ώστε:

$$b!(b+w+B(a,b,w))! \mid q+1 \ \wedge\ z_0=q\ \wedge\ \binom{q}{b}\Big|\binom{z_i}{w},\ i=0,\dots,m$$
$$\wedge\ D(a,z_0,\dots,z_m)\equiv 0 \pmod{\binom{q}{b}}.$$

($\Longleftarrow$): Για $y=0,\dots,b-1$ θέτουμε $q_y=\dfrac{q+1}{y+1}-1$.

Τότε $q_0\cdots q_{b-1}=\binom{q}{b}$. Αφού $\binom{q}{b}\Big|\binom{z_i}{w},\ i=0,\dots,m$ έπεται ότι $q_0\cdots q_{b-1}\Big|\binom{z_i}{w},\ i=0,\dots,m$ που σημαίνει ότι $q_y\Big|\binom{z_i}{w},\ i=1,\dots,m,\ y=0,\dots,b-1$.

Άρα $q_y\Big|\dfrac{(z_i)!}{w!(z_i-w)!}$, δηλαδή $q_y\Big|\dfrac{(z_i-w+1)\cdots z_i}{w!}$, που σημαίνει ότι $q_y\Big|\prod_{k=0}^{w-1}(z_i-k)$ για $i=1,\dots,m$ και $y=0,\dots,b-1$.

Έστω p_y πρώτος αριθμός τέτοιος ώστε $p_y|q_y$ για $y=0,\dots,b-1$.

$$\text{Τότε:}\quad p_y\Big|\prod_{k=0}^{w-1}(z_i-k)\quad \text{για } i=1,\dots,m,\ y=0,\dots,b-1.$$

Επειδή ο p_y είναι πρώτος αριθμός, έπεται ότι υπάρχει x_{iy} ώστε:

$$x_{iy}<w\quad \text{και}\quad p_y\Big|\, z_i-x_{iy}\quad \text{για } i=1,\dots,m,\ y=0,\dots,b-1.$$

Άρα ισχύει $\quad x_{iy}=rem(z_i,p_y)\quad$ για $i=1,\dots,m,\ y=0,\dots,b-1$.

Επίσης ισχύει ότι $z_0=q$. Επειδή $q_y=\dfrac{q+1}{y+1}-1$ έπεται ότι $q_y|\,z_0-y$ και άρα $p_y|\,z_0-y$, που σημαίνει ότι $y=rem(z_0,p_y)$.

Άρα υπάρχουν $x_{iy},\ i=1,\dots,m,\ y=0,\dots,b-1$ ώστε να ισχύουν:

$$\begin{aligned}&x_{iy}=rem(z_i,p_y),\ i=1,\dots,m,\ y=0,\dots,b-1\\&y=rem(z_0,p_y),\ y=0,\dots,b-1.\end{aligned}$$

Τότε έπεται ότι για $y=0,\dots,b-1$ ισχύει:

$$D(a,y,x_{1y},\dots,x_{my})\equiv D(a,z_0,\dots,z_m)\pmod{p_y}.$$

Επίσης ισχύει ότι $|D(a,y,x_{1y},\dots,x_{my})|\leq B(a,b,w)$.
Ισχυρισμός 3: $p_y>B(a,b,w)$.
Πράγματι: Είναι $p_y|q_y$. Άρα $\gcd(p_y,\dfrac{q+1}{y+1})=1$.
Επίσης $b!(b+w+B(a,b,w))!\mid q+1$ και άρα
$q+1=\lambda b!(b+w+B(a,b,w))!$. Επειδή p_y είναι πρώτος αριθμός έπεται ότι $p_y>b+w+B(a,b,w)$. Άρα $p_y>B(a,b,w)$.

Λόγω του ισχυρισμού 3, ισχύει ότι $|D(a,y,x_{1y},\dots,x_{my})|\leq p_y$.
Από υπόθεση έχουμε ότι $D(a,z_0,\dots,z_m)\equiv 0 \pmod{\binom{q}{b}}$. Αυτό σημαίνει ότι $D(a,z_0,\dots,z_m)\equiv 0\pmod{q_0\cdots q_{b-1}}$ και επειδή οι αριθμοί $q_0\cdots q_{b-1}$ είναι σχετικά πρώτοι, έπεται ότι
$D(a,z_0,\dots,z_m)\equiv 0\pmod{q_y},\ y=0,\dots,b-1$.
Άρα $D(a,z_0,\dots,z_m)\equiv 0\pmod{p_y},\ y=0,\dots,b-1$.
Τότε έπεται ότι $D(a,y,x_{1y},\dots,x_{my})=0$ για $y=0,\dots,b-1$.
Άρα ισχύει ότι:

$$\forall y<b\exists x_{1y},\dots,x_{my}[D(a,y,x_{1y},\dots,x_{my})=0].$$

Άρα ισχύει ότι:

$$\begin{aligned}R_2(a,b)\Leftrightarrow \exists q,w,z_0,\dots,z_m\Bigg[&b!(b+w+B(a,b,w))!\mid q+1\\&\wedge\ z_0=q\\&\wedge\ \binom{q}{b}\Big|\binom{z_i}{w},\ i=0,\dots,m\\&\wedge\ D(a,z_0,\dots,z_m)\equiv 0\pmod{\binom{q}{b}}\Bigg],\end{aligned}$$

που σημαίνει ότι η σχέση $R_2(a,b)$ είναι διοφαντική. $\square$

7.2 Αναδρομικές συναρτήσεις

Ορισμός 7.1 *Η κλάση των* '**αναδρομικών συναρτήσεων**' *είναι η μικρότερη κλάση συναρτήσεων στους φυσικούς αριθμούς, η οποία:*

- *περιέχει τις συναρτήσεις:*

$$S(x) = x + 1$$

$$Pd(x) = x - 1$$

$$C_q^n(x_1, \ldots, x_n) = q$$

$$P_i^n(x_1, \ldots, x_n) = x_i$$

- *είναι κλειστή κάτω από τους εξής κανόνες:*

  1. *Σύνθεση*

  $$f(x_1, \ldots, x_n) = g(h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n))$$

  2. *Πρωτογενή αναδρομή*

  $$\begin{aligned} &f(0, x_1, \ldots, x_n) = g(x_1, \ldots, x_n) \\ &f(n+1, x_1, \ldots, x_n) = h(f(n, x_1, \ldots, x_n), n, x_1, \ldots, x_n) \end{aligned}$$

  3. *Ελαχιστοποίηση*

  $$f(x_1, \ldots, x_n) = \mu y[g(y, x_1, \ldots, x_n) = 0],$$

  όπου η g είναι συνάρτηση για την οποία ισχύει ότι $\forall x_1, \ldots, x_n \exists y[g(y, x_1, \ldots, x_n) = 0]$.

Ορισμός 7.2

- *Μια σχέση καλείται* '**αναδρομική**' *αν η χαρακτηριστική της συνάρτηση είναι αναδρομική.*

- *Ενα σύνολο καλείται* '**αναδρομικό**' *αν η χαρακτηριστική του συνάρτηση είναι αναδρομική.*

Ορισμός 7.3

- *Μια σχέση $R(x_1, \ldots, x_n)$ καλείται 'Σ_1' αν υπάρχει μια αναδρομική σχέση $Q(x_1, \ldots, x_n, y)$ τέτοια ώστε να ισχύει:*

$$R(x_1, \ldots, x_n) \Leftrightarrow \exists y\, Q(x_1, \ldots, x_n, y)$$

- *Ένα σύνολο A καλείται '**αναδρομικά απαριθμητό**' αν η σχέση $x \in A$ είναι Σ_1 σχέση.*

Θέση Church-Turing
Οι κλάσεις των υπολογίσιμων συναρτήσεων και των αναδρομικών ταυτίζονται.

Η θέση Church-Turing ταυτίζει τη διαισθητική έννοια της υπολογισιμότητας με την αυστηρή (μαθηματική) έννοια της αναδρομικότητας. Ο Turing ταύτισε τις έννοιες υπολογισιμότητας και μηχανικής υπολογισιμότητας, ορίζοντας αυστηρά μια κλάση μηχανών, τις μηχανές Turing και δίνοντας επιχειρήματα ότι οι υπολογισμοί οποιασδήποτε κατασκευάσιμης μηχανής προσομοιώνονται από κάποια μηχανή Turing .

7.3 Η κλάση των διοφαντικών σχέσεων ταυτίζεται με την κλάση των Σ_1 σχέσεων

Θεώρημα 7.2 *Μια συνάρτηση είναι διοφαντική αν και μόνο αν είναι αναδρομική.*

Απόδειξη

($\Longrightarrow$): Αν f είναι διοφαντική συνάρτηση, τότε ισχύει

$$f(a_1, \ldots, a_n) = a \Leftrightarrow \exists x_1, \ldots, x_m\, [D(a, a_1, \ldots, a_n, x_1, \ldots, x_m) = 0.$$

Επειδή τα πολυώνυμα είναι αναδρομικές συναρτήσεις, έχουμε ότι το γράφημα της f είναι Σ_1 σχέση. Αυτό σημαίνει ότι η f είναι αναδρομική συνάρτηση.

($\Longleftarrow$): Αν η συνάρτηση f είναι αναδρομική, με επαγωγή αποδεικνύεται ότι είναι και διοφαντική. Πράγματι, αν η f είναι κάποια από τις συναρτήσεις S, Pd, C_q^n, P_i^n τότε:

- $f(x) = S(x)$
  $a = S(x) \Leftrightarrow a = x + 1$
- $f(x) = Pd(x)$
  $a = Pd(x) \Leftrightarrow a = x - 1$
- $f(x_1, \ldots, x_n) = C_q^n(x_1, \ldots, x_n)$
  $a = C_q^n(x_1, \ldots, x_n) \Leftrightarrow a = q$
- $f(x_1, \ldots, x_n) = P_i^n(x_1, \ldots, x_n)$
  $a = P_i^n(x_1, \ldots, x_n) \Leftrightarrow a = x_i$

Αν η f ορίζεται με σύνθεση, πρωτογενή αναδρομή ή ελαχιστοποίση, τότε:

Σύνθεση: Αν $f(x_1, \ldots, x_n) = h(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n))$, τότε:

$$\begin{aligned} a = f(x_1, \ldots, x_n) \Leftrightarrow \exists t_1, \ldots, t_m [t_1 = g_1(x_1, \ldots, x_n) \wedge \\ \ldots \wedge t_m = g_m(x_1, \ldots, x_n) \wedge a = h(t_1, \ldots, t_m)] \end{aligned}$$

Όμως από επαγωγική υπόθεση οι συναρτήσεις $h, g_1, \ldots, g_m$ είναι διοφαντικές. Άρα και η f είναι διοφαντική συνάρτηση.

Πρωτογενής αναδρομή:

$$\begin{aligned} &f(0, x_1, \ldots, x_n) = g(x_1, \ldots, x_n) \\ &f(n+1, x_1, \ldots, x_n) = h(f(n, x_1, \ldots, x_n), n, x_1, \ldots, x_n) \end{aligned}$$

Έστω $El(t, b, i)$ είναι η διοφαντική συνάρτηση που δίνει το $i-$οστό στοιχείο μιας πλειάδας με cipher t και βάση b, την οποία ορίσαμε στην παράγραφο 5.2. Τότε ισχύει:

$$\begin{aligned} a = f(n, x_1, \ldots, x_n) \Leftrightarrow \exists\, b, t \Big[El(t, b, 1) = g(x_1, \ldots, x_n) \\ \wedge\, \forall i < n \, [El(t, b, i+1) = h(El(t, b, i), i, x_1, \ldots, x_n)] \\ \wedge\, El(t, b, n) = a \Big] \end{aligned}$$

Από επαγωγική υπόθεση έχουμε ότι οι συναρτήσεις g, h είναι διοφαντικές και επειδή οι διοφαντικές σχέσεις είναι κλειστές κάτω από φραγμένους ποσοδείκτες έπεται ότι η συνάρτηση f είναι διοφαντική.

Ελαχιστοποίηση: Αν $f(x_1,\ldots,x_n) = \mu i\,[g(i,x_1,\ldots,x_n) = 0]$ με την προϋπόθεση ότι $\forall x_1,\ldots,x_n \exists i\,[g(i,x_1,\ldots,x_n) = 0]$ τότε:

$$a = f(x_1,\ldots,x_n) \Leftrightarrow g(a,x_1,\ldots,x_n) = 0 \wedge \forall\, t < a\,[g(t,x_1,\ldots,x_n) \neq 0]$$

Εφόσον η συνάρτηση g είναι διοφαντική λόγω της επαγωγικής υπόθεσης, έπεται ότι και η f θα είναι διοφαντική. $\square$

Πόρισμα 7.1 *Η κλάση των διοφαντικών σχέσεων ταυτίζεται με την κλάση των Σ_1 σχέσεων.*

Απόδειξη

($\Longleftarrow$): Εστω $R(x_1,\ldots,x_n)$ είναι μια Σ_1 σχέση. Τότε υπάρχει αναδρομική σχέση $Q(x_1,\ldots,x_n,y)$ τέτοια ώστε να ισχύει:

$$\begin{aligned} R(x_1,\ldots,x_n) &\Leftrightarrow \exists y Q(x_1,\ldots,x_n,y) \\ &\Leftrightarrow \exists y\,[g(x_1,\ldots,x_n,y) = 0] \end{aligned}$$

όπου η συνάρτηση $g(x_1,\ldots,x_n,y)$ είναι αναδρομική και άρα σύμφωνα με το θεώρημα 7.2 διοφαντική. Άρα έπεται ότι η σχέση $R(x_1,\ldots,x_n)$ είναι διοφαντική.

($\Longrightarrow$): Άν η σχέση $R(x_1,\ldots,x_n)$ είναι διοφαντική, τότε:

$$R(x_1,\ldots,x_n) \Leftrightarrow \exists y_1,\ldots,y_m[D(x_1,\ldots,x_n,y_1,\ldots,y_m) = 0]$$

όπου $D(x_1,\ldots,x_n,y_1,\ldots,y_m) = 0$ είναι διοφαντική εξίσωση. Αυτό σημαίνει ότι το $D(x_1,\ldots,x_n,y_1,\ldots,y_m)$ είναι πολυώνυμο με ακέραιους συντελεστές, και άρα η σχέση $D(x_1,\ldots,x_n,y_1,\ldots,y_m) = 0$ είναι αναδρομική. Συνεπώς η σχέση $R(x_1,\ldots,x_n)$ είναι Σ_1. $\square$

7.4 Το 10^o πρόβλημα του Hilbert έχει αρνητική απάντηση

Στο θεώρημα 6.2 είχαμε ορίσει το διοφαντικό σύνολο

$$\mathfrak{N} = \left\{a \mid a \in \mathfrak{M}_a^1\right\}$$

του οποίου όμως το συμπλήρωμα δεν είναι διοφαντικό.

Λήμμα 7.1 *Η συνάρτηση* $g(n,x) = \begin{cases} 2 & \text{αν } x \in \mathfrak{M}_n^1 \\ 1 & \text{αν } x \notin \mathfrak{M}_n^1 \end{cases}$ *δεν είναι αναδρομική.*

Απόδειξη
Ας θεωρήσουμε ότι η συνάρτηση $g(n,x)$ είναι αναδρομική. Τότε σύμφωνα με το θεώρημα 7.2 είναι και διοφαντική. Δηλαδή ισχύει:

$$a = g(n,x) \Leftrightarrow \exists y_1,\ldots,y_m[D(n,x,a,y_1,\ldots,y_m) = 0,$$

όπου $D(n,x,a,y_1,\ldots,y_m) = 0$ είναι διοφαντική εξίσωση. Τότε ισχύει:

$$1 = g(n,n) \Leftrightarrow \exists y_1,\ldots,y_m[D(n,n,1,y_1,\ldots,y_m) = 0.$$

Αλλά, ισχύει επίσης ότι:

$$1 = g(n,n) \Leftrightarrow n \notin \mathfrak{M}_n^1.$$

Αυτό σημαίνει ότι:

$$n \notin \mathfrak{M}_n^1 \Leftrightarrow \exists y_1,\ldots,y_m[D(n,n,1,y_1,\ldots,y_m) = 0.$$

Δηλαδή,

$$n \in \overline{\mathfrak{N}} \Leftrightarrow \exists y_1,\ldots,y_m[D(n,n,1,y_1,\ldots,y_m) = 0$$

που σημαίνει ότι το σύνολο $\overline{\mathfrak{N}}$ είναι διοφαντικό. Αυτό όμως δεν ισχύει λόγω του θεωρήματος 6.2. Άρα η υπόθεση ότι η συνάρτηση $g(n,x)$ είναι αναδρομική ήταν λανθασμένη. □

Ας υποθέσουμε ότι υπάρχει αλγόριθμος που αποφασίζει αν μια συγκεκριμένη διοφαντική εξίσωση έχει λύση ή όχι στους φυσικούς.
Συμβολίζουμε με $\mathfrak{M}_n^1$ το διοφαντικό σύνολο διάστασης 1 του οποίου ο κωδικός είναι ο αριθμός n. Τότε έχουμε ότι:

$$a \in \mathfrak{M}_n^1 \Leftrightarrow \exists y_1,\ldots,y_m[U_1(a,n,y_1,\ldots,y_m) = 0]$$

Υπάρχει δηλαδή αλγόριθμος που για δεδομένα $\langle n,a\rangle$ αποφασίζει αν η καθολική διοφαντική εξίσωση $U_1(a,n,y_1,\ldots,y_m) = 0$ έχει λύση ή όχι στους φυσικούς. Ο αλγόριθμος αυτός για δεδομένα $\langle n,a\rangle$ θα αποφασίζει αν $a \in \mathfrak{M}_n^1$. Τότε ο αλγόριθμος αυτός μπορεί να χρησιμοποιηθεί για τον υπολογισμό της συνάρτησης g που ορίστηκε στο λήμμα 7.1. Από τη θέση Church-Turing , αυτό σημαίνει ότι η συνάρτηση g είναι αναδρομική το οποίο όμως λόγω του λήμματος 7.1 δεν ισχύει.

Το συμπέρασμα είναι ότι δεν υπάρχει αλγόριθμος που να αποφασίζει αν μια διοφαντική εξίσωση έχει λύση ή όχι στους φυσικούς αριθμούς. Το αποτέλεσμα αυτό επεκτείνεται και στο αντίστοιχο ερώτημα για την ύπαρξη λύσεων μιας διοφαντικής εξίσωσης στους ακεραίους, αφού όπως είδαμε και στην παράγραφο 2.2 τα δύο προβλήματα είναι ανάλογα.

8 Πολυπλοκότητα των καθολικών διοφαντικών εξισώσεων

8.1 Συμβολισμοί–Αρχικά λήμματα

Στην παράγραφο 6.4 αποδείχθηκε η ύπαρξη μιας καθολικής διοφαντικής εξίσωσης $U_1(a, k, x_1, \ldots, x_m)$ με 1 παράμετρο στοιχείων, 1 παράμετρο κωδικών και m αγνώστους, όπου m είναι κάποιος σταθερός αριθμός, τέτοια ώστε, αν $\mathfrak{M}$ είναι διοφαντικό σύνολο διάστασης 1, υπάρχει $k^{\mathfrak{M}}$ ώστε να ισχύει η ισοδυναμία:

$$a \in \mathfrak{M} \Leftrightarrow \exists x_1, \ldots, x_m[U_1(a, k^{\mathfrak{M}}, x_1, \ldots, x_m) = 0]$$

Κατά καιρούς έχει μελετηθεί η πολυπλοκότητα των καθολικών διοφαντικών εξισώσεων. Ένα μέτρο για την πολυπλοκότητα των καθολικών διοφαντικών εξισώσεων, είναι το ζεύγος (m, d) του αριθμού των αγνώστων και του ολικού βαθμού της εξίσωσης. Το 1970 ο Y.Matiyasevich ανακοίνωσε ότι ο αριθμός των αγνώστων μιας καθολικής διοφαντικής εξίσωσης είναι μικρότερος από 200, ενώ μετά από λίγο χρονικό διάστημα η J.Robinson μείωσε των αριθμό των αγνώστων σε 35. Στη συνέχεια δουλεύοντας με τον Y.Matiyasevich μείωσε τον αριθμό των αγνώστων σε 24. Το 1973 ο Y.Matiyasevich και η J.Robinson κατασκεύασαν καθολική διοφαντική εξίσωση με 13 αγνώστους. Το αποτέλεσμα αυτό δημοσιεύτηκε το 1975[8]. Στο άρθρο αυτό ο Y.Matiyasevich διατύπωσε την πιθανότητα επιπλέον μείωσης του αριθμού των αγνώστων σε 9. Η κατασκευή μιας καθολικής διοφαντικής εξίσωσης με 9 αγνώστους παρουσιάστηκε αναλυτικά το 1982 από τον J.Jones [5].

Για την κατασκευή αυτής της διοφαντικής εξίσωσης θα χρειαστούν κάποια αρχικά λήμματα.

- Με $A = \square$ εννοούμε ότι το A είναι τετράγωνο κάποιου αριθμού.
- Με $N\, pow\, 2$ εννοούμε ότι το N είναι μια δύναμη του 2.
- Αν $x^2 - (A^2 - 1)y^2 = 1$ όπου $A > 1$ είναι εξίσωση του Pell [2], συμβολίζουμε τις λύσεις αυτής ως $x = \chi_A(n),\ y = \psi_A(n)$.

Λήμμα 8.1 *Αν $N\, pow\, 2$, τότε $\tau_2(aN, bN) = \tau_2(a, b)$.*
Με $\tau_p(m, n)$ υπενθυμίζουμε ότι συμβολίζουμε τον αριθμό των κρατουμένων κατά την πρόσθεση των αριθμών m, n, όταν αυτοί γραφούν ως αναπτύγματα με βάση το p.

Λήμμα 8.2 *Αν* $N \, pow \, 2$, $0 \le S_1 < N$, $0 \le T_1 < N$ *τότε*

$$\begin{matrix} \tau_2(S_1,T_1)=0 \\ \tau_2(S_2,T_2)=0 \end{matrix} \Leftrightarrow \tau_2(S_1+S_2N, T_1+T_2N)=0.$$

Λήμμα 8.3 *Αν* $N_i \, pow \, 2$, $0 \le S_i < N$, $0 \le T_i < N$ *για* $i = 1,\dots,n$ *και* $S = \sum_{i=1}^n S_i N_1 \cdots N_{i-1}$, $T = \sum_{i=1}^n T_i N_1 \cdots N_{i-1}$ *και* $N = \prod_{i=1}^n N_i$, *τότε*

1. $\bigwedge_{i=1}^n \tau_2(S_i,T_i)=0 \Leftrightarrow \tau_2(S,T)=0$.
2. $S < N$ *και* $T < N$.

Λήμμα 8.4 *Αν* $N \, pow \, 2$, $0 \le S < N$, $0 \le T < N$ *και* $R = S(N^2-N)+(T+1)(N^2-1)$ *τότε*

$$\tau_2(S,T)=0 \Leftrightarrow N^2 \left| \binom{2R}{R} \right. .$$

Λήμμα 8.5 *Αν* $R \ge 8$, $N \ge 8$, $R \ge b$ *και* $N \ge b > 0$, *τότε ισχύει ότι* $N^2 \left| \binom{2R}{R} \right.$ *και* $b \, pow \, 2$ *αν και μόνο αν υπάρχουν θετικοί ακέραιοι αριθμοί* h, s, w, φ *και ακέραιοι* A, B', C, K, M, P, U, V, W, Y *που ικανοποιούν τις σχέσεις:*

$$\begin{gathered} P = 2M^2U \\ (P^2-1)K^2+1 = \square \\ (\frac{C}{K}-Y)^2 < \frac{1}{4} \\ K = R+1+h(P-1) \\ M = RY \\ A = M(U+1) \\ B' = 2R+1 \\ C = B'+\varphi \\ U = N^2w \\ Y = N^2s \\ W = bw \\ V = 2 \\ (V^2-1)WC \equiv V(W^2-1) \pmod{2AV-V^2-1} \\ C = \psi_A(B'). \end{gathered}$$

Λήμμα 8.6 *Έστω ότι $A > 1$, $1 < B \leq C$, και είτε $2B \leq C$ είτε B είναι περιττός. Τότε ισχύει ότι $C = \psi_A(B)$ αν και μόνο αν υπάρχουν θετικοί ακέραιοι i, j και ακέραιοι D, E, F, H, G, I, τέτοιοι ώστε:*

$$DEF = \square$$

$$F \mid H - C$$
$$D = (A^2 - 1)C^2 + 1$$
$$E = iJDC^2$$
$$F = (A^2 - 1)E^2 + 1$$
$$G = A + F(CD + 1 - A)$$
$$H = B + jC$$
$$I = (G^2 - 1)H^2 + 1$$

8.2 Κατασκευή καθολικής διοφαντικής εξίσωσης με 9 αγνώστους

Αν $\mathfrak{M}$ είναι διοφαντικό σύνολο, τότε ισχύει η ισοδυναμία:

$$a \in \mathfrak{M} \Leftrightarrow \exists x_1, \ldots, x_m[U(a, x_1, \ldots, x_m) = 0]$$

όπου η $U(a, x_1, \ldots, x_m) = 0$ είναι καθολική διοφαντική εξίσωση με m αγνώστους.
Στη συνέχεια θα κατασκευαστεί μια άλλη καθολική διοφαντική εξίσωση με 9 αγνώστους.

Έστω d ο ολικός βαθμός του πολυωνύμου $U(x_0, x_1, \ldots, x_m)$.
Υποθέτουμε ότι $U(a, 0, \ldots, 0) \neq 0$ για κάθε $a \geq 0$.
Ισχύει ότι:

$$(1 + x_0 + \cdots + x_m)^d = \sum_{i_0 + i_1 + \cdots + i_m \leq d} c_{i_0,\ldots,i_m} x_0^{i_0} x_1^{i_1} \cdots x_m^{i_m},$$

όπου $c_{i_0,\ldots,i_m} = \dfrac{d!}{i_0! \cdots i_m!(d - i_0 - \ldots - i_m)!}$ είναι διαιρέτες του $d!$. Άρα υπάρχουν θετικοί ακέραιοι $Q_{i_0,\ldots,i_m}$ ώστε: $c_{i_0,\ldots,i_m} Q_{i_0,\ldots,i_m} = d!$.

Αν $d_{i_0,\ldots,i_m}$ είναι οι συντελεστές του πολυωνύμου $U(x_0, x_1, \ldots, x_m)$ τότε υπάρχουν οι ακέραιοι $P_{i_0,\ldots,i_m} = Q_{i_0,\ldots,i_m} d_{i_0,\ldots,i_m}$ ώστε:

$$d!U(x_0, x_1, \ldots, x_m) = \sum_{i_0+i_1+\cdots+i_m \le d} c_{i_0,\ldots,i_m} P_{i_0,\ldots,i_m} x_0^{i_0} x_1^{i_1} \cdots x_m^{i_m}.$$

Εφόσον υποθέσαμε ότι $U(0, 0, \ldots, 0) > 0$ έπεται ότι ο σταθερός όρος του πολυωνύμου $U(x_0, x_1, \ldots, x_m)$ είναι θετικός και συνεπώς το ίδιο συμβαίνει και για τον ακέραιο $P_{0,\ldots,0}$. Θέτουμε $m^* = \max |P_{i_0,\ldots,i_m}|$.
Επιλέγουμε θετικό ακέραιο β ώστε:

$$\beta \; pow \; 2$$
$$2(2+m)^d m^* < \beta$$

Θεωρούμε μια μεταβλητή b που συμβολίζει ένα ανώτατο όριο για το μέγεθος μιας λύσης του πολυωνύμου $U(x_0, x_1, \ldots, x_m)$. Με την έκφραση 'μέγεθος μιας λύσης πολυωνύμου' εννοούμε τη μεγαλύτερη τιμή που μπορούν να πάρουν τα στοιχεία μιας λύσης.
Υποθέτουμε ότι:

$$b \; pow \; 2 \; ,$$

και ορίζουμε

$$B = \beta b^d.$$

Ορισμός 8.1 *Ο αριθμός c είναι* '**κωδικός**' *μιας πιθανής λύσης $\langle z_0, \ldots, z_m \rangle$ με όριο b, του πολυωνύμου $U(x_0, x_1, \ldots, x_m)$, αν:*

$$c = 1 + \sum_{i=0}^{m} z_i B^{(d+1)^i} \quad \textit{όπου} \quad 0 \le z_i < b, \; i = 1, \ldots, m.$$

Η κωδικοποίηση των πιθανών λύσεων ενός πολυωνύμου είναι σχεδόν ιδια με την κωδικοποίηση των πιθανών λύσεων μιας διφαντικής εξίσωσης που εισάγαμε στην παράγραφο 6.3.

Ισχυρισμός 1: Ο αριθμός c είναι κωδικός της πιθανής λύσης $\langle a, z_1, \ldots, z_m \rangle$ με όριο b, του πολυωνύμου $U(x_0, x_1, \ldots, x_m)$ αν και μόνο αν υπάρχει θετικός ακέραιος g ώστε να ισχύουν τα εξής:

$$\begin{aligned} &c = 1 + aB + g \\ &a < b \\ &g < 2bB^{(d+1)^m} \\ &\tau_2(g, M_1) = 0 \end{aligned}$$

όπου $M_1 = \sum_{j=0}^{(d+1)^m} m_j B^j$ και
$m_j = \begin{cases} B-b, & \text{αν } j=(d+1)^i \text{ για κάποιο } i \geq 1 \\ B-1, & \text{διαφορετικά} \end{cases}$

Απόδειξη ισχυρισμού:
Είναι $M_1 = (B-1)+(B-1)B+\cdots+(B-b)B^{d+1}+\cdots+(B-b)B^{(d+1)^m}$. Αν το g γραφεί ως ανάπτυγμα με βάση το B, εφόσον ισχύει ότι $\tau_2(g, M_1) = 0$ έπεται ότι ο συντελεστής του B θα είναι 0. Επίσης οι συντελεστές των B^j, όπου $j \neq (d+1)^i$ για κάθε $i \geq 1$, θα είναι επίσης 0, ενώ οι συντελεστές των $B^{(d+1)^i}$ θα είναι αριθμοί μικρότεροι από το b. Άρα ο αριθμός c είναι κωδικός με όριο b της πιθανής λύσης $\langle a, z_1, \ldots, z_m \rangle$. Το αντίστροφο είναι τετριμένο. $\square$

Ισχυρισμός 2: Αν c είναι κωδικός της πιθανής λύσης $\langle z_0, z_1, \ldots, z_m \rangle$, με όριο b του πολυωνύμου $U(x_0, x_1, \ldots, x_m)$,
$D_0 = \sum_{i_0+i_1+\cdots+i_m \leq d} P_{i_0,\ldots,i_m} B^{(d+1)^{m+1}-i_0-i_1(d+1)-\cdots-i_m(d+1)^m}$,
και $E_0 = c^d D_0 + \sum_{i=0}^{(2d+1)(d+1)^m} \dfrac{B}{2} B^i$, τότε η $m-$άδα $\langle z_0, z_1, \ldots, z_m \rangle$ είναι λύση του πολυωνύμου $U(x_0, x_1, \ldots, x_m)$ αν και μόνο αν ισχύει ότι
$\tau_2(E_0, (\dfrac{B}{2}-1)B^{(d+1)^{m+1}}) = 0$.

Απόδειξη ισχυρισμού: Εφόσον c είναι κωδικός με όριο b της πιθανής λύσης $\langle z_0, z_1, \ldots, z_m \rangle$ έπεται ότι $c = 1 + \sum_{i=0}^{m} z_i B^{(d+1)^i}$.
Τότε $c^d = \sum_{i_0+i_1+\cdots+i_m \leq d} c_{i_0,\ldots,i_m} z_0^{i_0} \cdots z_m^{i_m} B^{i_0+i_1(d+1)+\cdots+i_m(d+1)^m}$, και άρα το $c^d D_0$ είναι ένα πολυώνυμο του B με βαθμό το πολύ $(2d+1)(d+1)^m$ και ο συντελεστής του $B^{(d+1)^{m+1}}$ είναι το $d!U(z_0, z_1, \ldots, z_m)$. Εφόσον $B = \beta b^d$ και $2(2+m)^d m^* < \beta$ ισχύουν τα εξής:

$$\frac{B}{2} = \frac{\beta b^d}{2} > (2+m)^d m^* b^d > c_{i_0,\ldots,i_m} P_{i'_0,\ldots,i'_m} z_0^{i_0} \cdots z_m^{i_m}$$

Άρα όλοι οι συντελεστές του πολυωνύμου $c^d D_0$ είναι μικρότεροι από το $\dfrac{B}{2}$. Αυτό σημαίνει ότι οι συντελεστές του πολυωνύμου E_0 είναι μικρότεροι του B. Ο συντελεστής του $B^{(d+1)^{m+1}}$ στο πολυώνυμο E_0 είναι ο $d!U(z_0, z_1, \ldots, z_m) + \dfrac{B}{2}$.
Εφόσον ισχύει ότι $\tau_2(E_0, (\dfrac{B}{2}-1)B^{(d+1)^{m+1}}) = 0$, έπεται ότι
$U(z_0, z_1, \ldots, z_m) = 0$. Δηλαδή η $m-$άδα $\langle z_0, z_1, \ldots, z_m \rangle$ είναι λύση του πολυωνύμου $U(x_0, x_1, \ldots, x_m)$. $\square$

Από το λήμμα 8.1 έπεται ότι:

$$\tau_2(E_0, (\frac{B}{2} - 1)B^{(d+1)^{m+1}}) = \tau_2(2E_0, (B-2)B^{(d+1)^{m+1}})$$

Πόρισμα 8.1

$$\exists x_1, \ldots, x_m[U(a, x_1, \ldots, x_m) = 0] \Leftrightarrow \begin{cases} c = 1 + aB + g \\ a < b \\ g < 2bB^{(d+1)^m} \\ \tau_2(g, M_1) = 0 \\ \tau_2(2E_0, (B-2)B^{(d+1)^{m+1}}), \end{cases}$$

όπου τα M_1, E_0 ορίστηκαν παραπάνω. $\square$

Θέτουμε:

$$S_1 = 2E_0$$
$$T_1 = (B-2)B^{(d+1)^{m+1}}$$
$$N_1 = 2B^{(2d+1)(d+1)^{m+1}}$$
$$S_2 = g$$
$$T_2 = M_1$$
$$N_2 = B^{(d+1)^{m+1}}$$
$$S = S_1 + S_2 N_1$$
$$T = T_1 + T_2 N_1$$
$$N = N_1 N_2.$$

Εφόσον ισχύουν ότι $a < b$, $g < 2bB^{(d+1)^m}$ και $D_0 > 0$ έπεται ότι $0 \leq S_i < N_i$, $0 \leq T_i < N_i$ για $i = 1, 2$. Τότε από το λήμμα 8.2 ισχύει ότι:

$$\begin{bmatrix} c = 1 + aB + g \\ a < b \\ g < 2bB^{(d+1)^m} \\ \tau_2(g, M_1) = 0 \\ \tau_2(2E_0, (B-2)B^{(d+1)^{m+1}}) \end{bmatrix} \Leftrightarrow \begin{bmatrix} c = 1 + aB + g \\ a < b \\ g < 2bB^{(d+1)^m} \\ \tau_2(S, T) = 0 \end{bmatrix}$$

και επίσης από το λήμμα 8.3 έπεται ότι $0 \leq S < N$ και $0 \leq T < N$.
Θέτοντας $R = S(N^2 - N) + (T+1)(N^2-1)$, από το λήμμα 8.4 έπεται ότι:

$$\tau_2(S,T) = 0 \Leftrightarrow N^2 \bigg| \binom{2R}{R}.$$

Καθώς υποθέσαμε ότι $b \; pow \; 2$, από το λήμμα 8.5 ισχύει ότι $N^2 \bigg| \binom{2R}{R}$ αν και μόνο αν υπάρχουν $h, s, w, \varphi, A, B', C, K, M, P, U, V, W, Y$, τέτοια ώστε:

$$P = 2M^2U \tag{8.1}$$

$$(P^2-1)K^2+1 = \square \tag{8.2}$$

$$(\frac{C}{K} - Y)^2 < \frac{1}{4} \tag{8.3}$$

$$K = R + 1 + h(P-1) \tag{8.4}$$

$$M = RY \tag{8.5}$$

$$A = M(U+1) \tag{8.6}$$

$$B' = 2R + 1 \tag{8.7}$$

$$C = B' + \varphi \tag{8.8}$$

$$U = N^2 w \tag{8.9}$$

$$Y = N^2 s \tag{8.10}$$

$$W = bw \tag{8.11}$$

$$V = 2 \tag{8.12}$$

$$(V^2-1)WC \equiv V(W^2-1) \pmod{2AV - V^2 - 1} \tag{8.13}$$

$$C = \psi_A(B') \tag{8.14}$$

Από τη σχέση (8.7) έχουμε ότι ο B' είναι περιττός. Άρα από το λήμμα 8.6 έπεται ότι η σχέση (8.14) ισχύει αν και μόνο αν υπάρχουν θετικοί ακέραιοι i, j

τέτοιοι ώστε:

$$DEF = \square \tag{8.15α'}$$
$$F \mid H - C \tag{8.15β'}$$
$$D = (A^2 - 1)C^2 + 1 \tag{8.15γ'}$$
$$E = iJDC^2 \tag{8.15δ'}$$
$$F = (A^2 - 1)E^2 + 1 \tag{8.15ε'}$$
$$G = A + F(CD + 1 - A) \tag{8.15ϛ'}$$
$$H = B' + jC \tag{8.15ζ'}$$
$$I = (G^2 - 1)H^2 + 1 \tag{8.15η'}$$

όπου J είναι ένας αυθαίρετος θετικός ακέραιος αριθμός.
Αποδυκνύοντας το λήμμα 8.5, φαίνεται ότι η σχέση που ισχύει στην πραγματικότητα είναι ότι $(\frac{C}{K} - Y)^2 < \frac{1}{16}$. Επομένως ισχύει η ισοδυναμία:

$$\begin{array}{l} g < 2bB^{(d+1)^m} \\ (\frac{C}{K} - Y)^2 < \frac{1}{4} \end{array} \Leftrightarrow 4(\frac{C}{K} - Y)^2 + \frac{g}{2bB^{(d+1)^m}} < 1 \tag{8.3'}$$

Τετριμένα ισχύει και η ακόλουθη ισοδυναμία:

$$a < b \Leftrightarrow \exists \varepsilon \, [a + \varepsilon = b]$$

Συνοψίζοντας λοιπόν έχουμε ότι:

$$\begin{array}{l} c = 1 + aB + g \\ a < b \\ g < 2bB^{(d+1)^m} \\ \tau_2(S,T) = 0 \end{array} \Leftrightarrow \begin{array}{c} \exists\, h, s, w, \varphi, A, B', C, K, M, P, U, V, W, Y, i, j, \varepsilon \\ c = 1 + aB + g \\ a + \varepsilon = b \\ (8.1), (8.2), (8.3'), (8.4) - (8.13) \\ (8.15α') - (8.15η') \end{array}$$

Αν πάρουμε ως $J = 2AV - V^2 - 1$ τότε έχουμε τα εξής:
Από τις σχέσεις (8.15ε') και (8.15δ') έχουμε ότι $F = (A^2 - 1)i^2J^2D^2C^4 + 1$ που σημαίνει ότι οι αριθμοί F, J είναι σχετικά πρώτοι.
Παίρνοντας ως C όχι τον αριθμό που ορίζεται από την σχέση (8.8) αλλά έναν αριθμό μεγαλύτερο από τον αριθμό W, τον

$$C = B' + W + \varphi \tag{8.8'}$$

προκύπτει ότι $(V^2-1)WC - V(W^2-1) > 0$. Επίσης από τη σχέση (8.15ζ′) έχουμε ότι $H - C > 0$. Τότε ισχύει η ισοδυναμία:

$$(8.13) \wedge (8.15\beta') \Leftrightarrow FJ \mid [(V^2-1)WC - V(W^2-1)]F + (H-C)J \quad (8.13')$$

Άρα το τελευταίο σύστημα σχέσεων είναι ισοδύναμο με το εξής σύστημα:

$$\begin{gathered} \exists\, h, s, w, \varphi, A, B', C, K, M, P, U, V, W, Y, i, j, \varepsilon \\ c = 1 + aB + g \\ a + \varepsilon = b \\ (8.1), (8.2), (8.3'), (8.4) - (8.7) \\ (8.8'), (8.9) - (8.12) \\ (8.13') \\ (8.15\alpha'),\ (8.15\gamma') - (8.15\eta') \end{gathered}$$

Απαλείφοντας με αντικατάσταση τις μεταβλητές, προκύπτει η ισοδυναμία:

$$a \in \mathfrak{M} \Leftrightarrow \begin{gathered} \exists g, h, i, j, s, w, \varepsilon, \varphi \\ a + \varepsilon = b \\ DEF = \square \\ 4(\frac{C}{K} - Y)^2 + \frac{g}{2bB^{(d+1)^m}} < 1 \\ FJ \mid [(V^2-1)WC - V(W^2-1)]F + (H-C)J \end{gathered}$$

όπου η σχέση $DEF = \square$ είναι ισοδύναμη με το ότι $\exists n\,[DEF = n^2]$. Συμπτύσσοντας τις παραπάνω τέσσερις σχέσεις έπεται ότι υπάρχει πολυώνυμο $P(a, g, h, i, j, s, w, \varepsilon, \varphi, n)$ τέτοιο ώστε:

$$a \in \mathfrak{M} \Leftrightarrow \exists g, h, i, j, s, w, \varepsilon, \varphi, n\,[P(a, g, h, i, j, s, w, \varepsilon, \varphi, n) = 0].$$

Το αποτέλεσμα είναι ότι η διοφαντική εξίσωση $P(a, g, h, i, j, s, w, \varepsilon, \varphi, n) = 0$ είναι καθολική διοφαντική εξίσωση με 9 αγνώστους.
Αποδεικνύεται ότι ο βαθμός της καθολικής διοφαντικής εξίσωσης $P(a, g, h, i, j, s, w, \varepsilon, \varphi, n) = 0$ με 9 αγνώστους είναι περίπου $d = 1,638 \times 10^{45}$.
Στη συνέχεια δίνεται ένας πίνακας με τα γνωστά ζεύγη, αριθμός αγνώστων–βαθμός,

μιας καθολικής διοφαντικής εξίσωσης.

$$
\begin{array}{llll}
m = 58, & d = 4 & m = 21, & d = 96 \\
m = 38, & d = 8 & m = 19, & d = 2668 \\
m = 32, & d = 12 & m = 14, & d = 2,0 \times 10^5 \\
m = 29, & d = 16 & m = 13, & d = 6,6 \times 10^{43} \\
m = 28, & d = 20 & m = 12, & d = 1,3 \times 10^{44} \\
m = 26, & d = 24 & m = 11, & d = 4,6 \times 10^{44} \\
m = 25, & d = 28 & m = 10, & d = 8,6 \times 10^{44} \\
m = 24, & d = 36 & m = 9, & d = 1,6 \times 10^{45}
\end{array}
$$

Αυτό που είναι άξιο παρατήρησης είναι ότι κατά τη μείωση του αριθμού των αγνώστων από 14 σε 13, ο βαθμός της καθολικής διοφαντικής εξίσωσης αυξάνεται σημαντικά.

Αναφορές

[1] Davis Martin, *Arithmetical problems and recursively enumerable predicates*, J.Symbolic Logic, 18(1), pp 33-41, 1953.

[2] Davis Martin, *Hilbert's tenth problem is unsolvable*, Amer.Math.Monthly, 80(3), pp 233-269, 1973.

[3] Davis Martin, Putnam Hilary and Robinson Julia, *The decision problem for exponential Diophantine equations*, Ann.Math., 74, pp 425-436, 1961.

[4] Hilbert David, *Mathematische Probleme*, Bull.Amer.Math.Soc., 8, pp 437-479, 1901-1902.

[5] Jones James, *Universal diophantine equation*, J.Symbolic Logic, 47(3), pp 549-571, 1982

[6] Matiyasevich Yuri, *Hilbert's Tenth Problem*, MIT Press, 1993.

[7] Matiyasevich Yuri, *Enumerable sets are Diophantine (Russian)*, Dokl.Akad.Nauk SSSR, 191, pp 279-282, 1970.

[8] Matiyasevich Yuri and Robinson Julia, *Reduction of an arbitrary Diophantine equation to one in 13 unknowns*, Acta Arith., 27, pp 521-553, 1975.

[9] Putnam Hilary, *An unsolvable problem in number theory*, J.Symbolic Logic, 25(3), pp 220-232, 1960.

[10] Robinson Julia, *Existential definability in Arithmetic*, Trans.Amer.Math.Soc., 72, pp 437-449, 1952.

[11] Singmaster David, *Notes on binomial coefficients I,II,III*, J.London Math.Soc.(2), 8(3), pp 545-548, 549-554, 555-560, 1974.