Στοιχεία προσθετικής αριθμοθεωρίας (Η συνάρτηση διαμέρισης και η εικασία *Waring*)

Χριστίνα Δασκαλάκη

Επιβλέπων καθηγητής
Ιωάννης Αντωνιάδης

Μεταπτυχιακή Εργασία

Τμήμα Μαθηματικών και Εφαρμοσμένων Μαθηματικών
Πανεπιστήμιο Κρήτης
Ηράκλειο
Μάιος 2016

Η παρούσα μεταπτυχιακή εργασία κατατέθηκε στο τμήμα Μαθηματικών και Εφαρμοσμένων Μαθηματικών του Πανεπιστημίου Κρήτης τον Μάιο του 2016 στα πλαίσια του μεταπτυχιακού προγράμματος «Μαθηματικά και Εφαρμογές τους» στην κατεύθυνση «Μαθηματικά για την Εκπαίδευση».
Την επιτροπή αξιολόγησης αποτέλεσαν οι:

Ιωάννης Αντωνιάδης, (επιβλέπων),
Μαρία Λουκάκη,
Χρήστος Κουρουνιώτης,

τους οποίους ευχαριστώ για την συμμετοχή τους στην επιτροπή αυτή.
Ιδιαίτερα ευχαριστώ τον κ. Αντωνιάδη γιατί χωρίς την συμβολή του δεν θα ήταν δυνατή η άρτια ολοκλήρωση αυτής της εργασίας. Επίσης, τον ευχαριστώ για το χρόνο που μου διέθεσε όλο αυτό το διάστημα, την καθοδήγησή του αλλά και για τις πολύτιμες συμβουλές του στην διάρκεια των μεταπτυχιακών μου σπουδών.
Τέλος, θα ήθελα να ευχαριστήσω τον κύριο Μιχάλη Παπαδημητράκη, την κυρία Μαρία Λουκάκη καθώς και τον κύριο Χρήστο Κουρουνιώτη για όλη τους την βοήθεια κατά την διάρκεια των σπουδών μου.

Στους γονείς μου, Βίκτωρα και Ελένη
και στο σύντροφο μου Γιάννη

Περιεχόμενα

1 Διαμερίσεις **5**

1.1 Εισαγωγή 5

1.2 Απειρογινόμενα 5

1.3 Μερικές στοιχειώδεις ιδιότητες της συνάρτησης διαμέρισης 8

1.4 Γραφική παράσταση 13

1.5 Η ταυτότητα του *Jacobi* 20

1.6 Εκτιμήσεις για το $p(n)$ 32

2 Θεώρημα *Lagrange* **37**

2.1 Στοιχειώδης απόδειξη 37

2.2 Απόδειξη με χρήση του θεωρήματος του *Minkowski* 42

3 Απόδειξη του *Hilbert* **της εικασίας** *Waring* **47**

3.1 Εισαγωγή 47

3.2 Βοηθητικές προτάσεις 48

3.3 Απόδειξη της εικασίας *Waring* 54

59

Εισαγωγή

Στην παρούσα μεταπτυχιακή εργασία διαπραγματευόμαστε δυο βασικά θέματα της προσθετικής Αριθμοθεωρίας. Το πρώτο είναι η μελέτη της συνάρτησης $p(n)$, όλων των δυνατών διαμερίσεων φυσικών αριθμών και το δεύτερο η εικασία $Waring$ και η απόδειξη της. Επειδή η "φύση" των φυσικών αριθμών είναι πολλαπλασιαστική, η αντιμετώπιση προβλημάτων της προσθετικής Αριθμοθεωρίας είναι ιδιαίτερα δύσκολη και επιτυγχάνεται κυρίως με χρήση αναλυτικών μεθόδων.
Η εργασία χωρίζεται σε τρία Κεφάλαια. Στο πρώτο κεφάλαιο μελετάται το πρόβλημα των διαμερίσεων. Πρώτα απ΄ όλα μελετώνται ως προς τη σύγκλιση τα απειρογινόμενα και αποδεικνύονται το Θεώρημα του $Euler$ καθώς και θεωρήματα στα οποία υπολογίζεται η διαφορά των παραστάσεων ενός φυσικού αριθμού όταν οι προσθεταίοι είναι μόνο περιττού ή μόνο άρτιου πλήθους αντίστοιχα. Ακολουθεί το θεώρημα του $Euler$ για πενταγωνικούς αριθμούς και το θεώρημα των $Rogers - Ramanujan$, χωρίς απόδειξη. Το σημαντικότερο θεώρημα του Κεφαλαίου είναι το θεώρημα της ταυτότητας του $Jacobi$ για το τριπλό γινόμενο.
Το Κεφάλαιο αυτό κλείνει με την απόδειξη της ισοτιμίας

$$p(5n+4) \equiv 0 \pmod 5$$

και την καταγραφή μερικών, πιο πρόσφατων αποτελεσμάτων.

Στο δεύτερο Κεφάλαιο αποδεικνύεται το θεώρημα του $Lagrange$, ότι κάθε φυσικός αριθμός μπορεί να παρασταθεί ως άθροισμα το πολύ τεσσάρων τετραγώνων μη-αρνητικών ακεραίων αριθμών. Δίνονται δυο αποδείξεις. Η πρώτη χρησιμοποιεί στοιχειώδη θεωρία αριθμών και η δεύτερη το θεώρημα του $Minkowski$.
Την ίδια εποχή που ο $Lagrange$ απέδειξε το θεώρημα του δευτέρου Κεφαλαίου, δηλαδή στα 1770, ο $Waring$ διατύπωσε την ομώνυμη, πολύ πιο γενική εικασία ότι για κάθε k φυσικό αριθμό, κάθε μη-αρνητικός ακέραιος μπορεί να γραφεί ως πεπερασμένο άθροισμα k δυνάμεων. Αν με $g(k)$ συμβολίσουμε τον ελάχιστο φυσικό αριθμό τέτοιον ώστε κάθε μη-αρνητικός ακέραιος να είναι άθροισμα $k-$δυνάμεων από ακριβώς s το πλήθος προσθεταίων, τότε η εικασία $Waring$ είναι ότι $g(k)$ είναι πεπερασμένος. Σύμφωνα με το θεώρημα του $Lagrange$ $g(2) = 4$. Είναι προφανές ότι $g(3) \geq 9$, αφού ο αριθμός 23 χρειάζεται 9 προσθεταίους, το ίδιο και ο 239 ενώ $g(4) \geq 19$, αφού για το

79 χρειαζόμαστε 19 προσθεταίους.
Η εικασία *Waring* αποδείχθηκε από τον *Hilbert* το 1909 [17].

Στα 1913 ο *Erhard Schmidt* [23] απέδειξε τη λεγόμενη ταυτότητα του *Hilbert* με χρήση της θεωρίας των κυρτών συνόλων. Στην παρούσα εργασία αποδεικνύουμε το δεύτερο μέρος της εικασίας, σύμφωνα με το βιβλίο του *Pollack* [17]

Ηράκλειο, Μάιος 2016

Κεφάλαιο 1

Διαμερίσεις

1.1 Εισαγωγή

Στο κεφάλαιο αυτό θα ασχοληθούμε με το πρόβλημα των διαμερίσεων ενός φυσικού αριθμού.

Ορισμός 1.1.1. *Μια διαμέριση του n είναι μια έκφραση του n ως άθροισμα $n = a_1 + a_2 + ... + a_r$ όπου τα a_i είναι θετικοί ακέραιοι.*

Συχνά το σύνολο $\{a_1, a_2, ..., a_r\}$ λέγεται διαμέριση του n. Τα a_i λέγονται μέρη της διαμέρισης. Η σειρά των προσθεταίων δεν ≪παίζει≫ ιδιαίτερο ρόλο, αν και συνηθίζεται η διαμέριση να γράφεται σε φθίνουσα τάξη, $a_1 \geq a_2 \geq ... \geq a_r$. Αυτό που βασικά μας ενδιαφέρει είναι η συνάρτηση $p(n)$ η οποία, για κάθε n παριστά το πλήθος των διαμερίσεων του n.
Για παράδειγμα, αν $n = 3$, τότε οι δυνατές διαμερίσεις είναι
3, 2+1, 1+1+1, δηλαδή $p(3) = 3$.
Αν $n = 5$, τότε οι διαμερίσεις είναι
5, 4+1, 3+2, 3+1+1, 2+2+1, 2+1+1+1, 1+1+1+1+1, δηλαδή $p(5) = 7$.
Αν $n = 6$, τότε οι διαμερίσεις είναι
6, 5+1, 4+2, 4+1+1, 3+3, 3+2+1, 3+1+1+1, 2+2+2, 2+2+1+1, 2+1+1+1+1, 1+1+1+1+1+1, δηλαδή $p(6) = 11$.

1.2 Απειρογινόμενα

Προκειμένου να μελετήσουμε τη συνάρτηση $p(n)$, θα χρειαστούμε μερικές βασικές ιδιότητες των απειρογινομένων.

Ορισμός 1.2.1. *Ενα απειρογινόμενο πραγματικών αριθμών* $a_1 a_2 ... a_n ... = \prod_{n=1}^{\infty} a_n$ *είναι η ακολουθία των μερικών γινομένων* $a_1, a_1a_2, ..., a_1a_2...a_n, ...$. *Αν ονομάσουμε* P_n *το μερικό γινόμενο* $P_n := a_1a_2...a_n$, *τότε λέμε ότι το απειρογινόμενο συγκλίνει στην τιμή* $P := \lim_{n\to\infty} P_n$, *όταν το όριο υπάρχει και είναι διάφορο του μηδενός.*

Παρατήρηση: Υπάρχουν σοβαροί λόγοι που εξαιρούμε την τιμή μηδέν.
Έτσι, αν επιτρέπαμε την τιμή $P = 0$, τότε κάθε απειρογινόμενο με ένα παράγοντα ίσο με μηδέν, θα συνέκλινε και μάλιστα η σύγκλιση θα ήταν ανεξάρτητη από όλους τους όρους της ακολουθίας των μερικών γινομένων.
Όμως θα επιθυμούσαμε να μπορούμε να εκφράσουμε μια συνάρτηση σε απειρογινόμενο ακόμη και στην περίπτωση που η συνάρτηση παίρνει την τιμή μηδέν.
Έτσι τροποποιούμε κάπως τον παραπάνω ορισμό, ως εξης:

Ορισμός 1.2.2. *Το απειρογινόμενο* $\prod_{n=1}^{\infty} a_n$ *συγκλίνει όταν έχει το πολύ πεπερασμένο πλήθος παραγόντων ίσων με μηδέν και τα μερικά γινόμενα των μη-μηδενικών παραγόντων απαρτίζουν μια ακολουθία μερικών γινομένων η οποία έχει όριο πεπερασμένο και διάφορο του μηδενός.*

Είναι προφανές ότι, αν το απειρογινόμενο $\prod_{n=1}^{\infty} a_n$ συγκλίνει και παραλείψουμε τους μηδενικούς όρους της ακολουθίας των μερικών παραγόντων, τότε το a_n γράφεται ως $a_n = \frac{P_n}{P_{n-1}}$ και συνεπώς $\lim_{n\to\infty} a_n = 1$.

Επομένως, είναι προτιμότερο να γραφεί το απειρογινόμενο στη μορφή $\prod_{n=1}^{\infty}(1+a_n)$ οπότε μια αναγκαία συνθήκη για τη σύγκλιση αυτού είναι ότι $\lim_{n\to\infty} a_n = 0$.

Θεώρημα 1.2.1. *Αν* $a_n \geq 0$ *για κάθε* $n \geq 1$, *τότε το απειρογινόμενο* $\prod_{n=1}^{\infty}(1 + a_n)$ *συγκλίνει, ακριβώς τότε όταν η σειρά* $\sum_{n=1}^{\infty} a_n$ *συγκλίνει.*

Απόδειξη. Έστω $S_n := \sum_{k=1}^{n} a_k$.
Ισχυει $1 \leq 1 + S_n \leq \prod_{k=1}^{n}(1 + a_k) \leq \prod_{k=1}^{n} e^{a_k} = e^{S_n}$.

Επομένως, το απειρογινόμενο συγκλίνει ακριβώς τότε όταν η σειρά $\sum_{k=1}^{\infty} a_k$ συγκλίνει.

□

Ανάλογη πρόταση ισχύει για το απειρογινόμενο $\prod_{n=1}^{\infty}(1-a_n)$.
Συγκεκριμένα ισχύει το:

Θεώρημα 1.2.2. *Αν $a_n \geq 0$ για κάθε $n \geq 1$, τότε το απειρογινόμενο $\prod_{n=1}^{\infty}(1-a_n)$ συγκλίνει, ακριβώς τότε όταν η σειρά $\sum_{n=1}^{\infty} a_n$ συγκλίνει.*

Απόδειξη. Αν η ακολουθία a_n δεν τείνει στο μηδέν, τότε το απειρογινόμενο και η σειρά αποκλίνουν.
Αν τώρα $\lim_{n\to\infty} a_n = 0$, τότε αυτό σημαίνει ότι υπάρχει ένας φυσικός αριθμός n_0 τέτοιος ώστε για κάθε $n > n_0$ να ισχύει $a_n < \frac{1}{2}$, δηλαδή $\frac{1}{2} < 1 - a_n < 1$.
Μελετούμε το απειρογινόμενο και τη σειρά, κατ' αρχήν, για $n \geq n_0$.
Αν το απειρογινόμενο συγκλίνει, τότε τα γινόμενα $P_n := (1-a_{n_0+1})...(1-a_n)$ αποτελούν μια μονότονα φθίνουσα ακολουθία η οποία συγκλίνει σε κάποιο θετικό αριθμό. Έστω $r_{n_0} > 0$.
Επειδή $a_n < 1$, έπεται ότι $1 + a_n \leq \dfrac{1}{1-a_n}$.
Επομένως, $(1+a_{n_0+1})(1+a_{n_0+2})...(1+a_n) \leqslant \frac{1}{r_{n_0}}$.
Από τα παραπάνω προκύπτει ότι, αφού το απειρογινόμενο $\prod_{n=1}^{\infty}(1-a_n)$ συγκλίνει, έπεται ότι συγκλίνει και το απειρογινόμενο $\prod_{n=1}^{\infty}(1+a_n)$. Από το θεώρημα 1.2.1, συνεπάγεται ότι και η σειρά $\sum_{n=1}^{\infty} a_n$ συγκλίνει.
Αντίστροφα, αν η σειρά $\sum_{n=1}^{\infty} a_n$ συγκλίνει τότε συγκλίνει και η σειρά $\sum_{n=1}^{\infty} 2a_n$.
Συνεπώς, σύμφωνα με το θεώρημα 1.2.1, συγκλίνει και το απειρογινόμενο $\prod_{n=1}^{\infty}(1+2a_n)$.
Επομένως, υπάρχει σταθερά $c > 0$ τέτοια ώστε
$(1+2a_{n_0+1})(1+2a_{n_0+2})...(1+2a_n) < c$.
Από τη σχέση $0 < a_n \leqslant \frac{1}{2}$, έπεται ότι $1 - a_n \geqslant \dfrac{1}{1+2a_n}$.
Αυτό σημαίνει ότι $(1-a_{n_0+1})(1-a_{n_0+2})...(1-a_n) > \frac{1}{c} > 0$.

Το γινόμενο του αριστερού μέλους αποτελεί μια μονότονα φθίνουσα ακολουθία. Άρα το όριο αυτού είναι κάποιος θετικός αριθμός, δηλαδή το απειρογινόμενο $\prod_{n=1}^{\infty}(1-a_n)$ συγκλίνει. □

Ορισμός 1.2.3. *Το απειρογινόμενο* $\prod_{n=1}^{\infty}(1+a_n)$ *συγκλίνει απόλυτα όταν το απειρογινόμενο* $\prod_{n=1}^{\infty}(1+\mid a_n \mid)$ *συγκλίνει.*

Ισχύει:

Θεώρημα 1.2.3. *Το απειρογινόμενο* $\prod_{n=1}^{\infty}(1+a_n)$ *συγκλίνει απόλυτα ακριβώς τότε όταν η σειρά* $\sum_{n=1}^{\infty} a_n$ *συγκλίνει απόλυτα.*

Απόδειξη. Αν $b_n :=\mid a_n \mid$ τότε $b_n \geq 0$ για κάθε n, οπότε από το θεώρημα 1.2.1 προκύπτει ότι το απειρογινόμενο $\prod_{n=1}^{\infty}(1+b_n)$ συγκλίνει ακριβώς τότε όταν η σειρά $\sum_{n=1}^{\infty} b_n$ συγκλίνει, δηλαδή συγκλίνει η σειρά $\sum_{n=1}^{\infty} \mid a_n \mid$, πράγμα που σημαίνει ότι η $\sum_{n=1}^{\infty} a_n$ συγκλίνει απόλυτα. □

1.3 Μερικές στοιχειώδεις ιδιότητες της συνάρτησης διαμέρισης

Θα αρχίσουμε με μερικούς συμβολισμούς. Έστω $\mathbb{N}$ το σύνολο των θετικών ακεραίων. Αν $\mathbf{H} \subseteq \mathbb{N}$, θεωρούμε $\widehat{\mathbf{H}}$ να είναι το σύνολο όλων των διαμερίσεων με όρους στο $\mathbf{H}$ και έστω $\widehat{\mathbf{H}}_d$ το σύνολο αυτών των διαμερίσεων στο $\widehat{\mathbf{H}}$ στις οποίες κανένας όρος δεν χρησιμοποιείται περισσότερες από d φορές. Επομένως, το $\widehat{\mathbb{N}}$ συμβολίζει το σύνολο όλων των διαμερίσεων και το $\widehat{\mathbb{N}}_1$ συμβολίζει το σύνολο όλων των διαμερίσεων με μη επαναλαμβανόμενους όρους. Επιπλέον, έστω $p(\widehat{\mathbf{H}}, n)$ να είναι το πλήθος των διαμερίσεων ενός θετικού ακεραίου n που περιέχονται στο $\widehat{\mathbf{H}}$. Γράφουμε $p(n)$ αντί για το $p(\widehat{\mathbb{N}}, n)$. Τέλος θεωρούμε ότι $p(0)=1$ και $p(m)=0$ αν $m<0$.

Τα βασικά εργαλεία στη θεωρία των διαμερίσεων είναι οι γεννήτριες συναρτήσεις. Αυτές ορίζονται ως εξής:

Ορισμός 1.3.1. *Έστω* $\{a_0, a_1, ...\}$ *να είναι μια άπειρη ακολουθία ακεραίων. Η δυναμοσειρά* $f(x) = \sum_{n=0}^{\infty} a_n x^n$ *ονομάζεται γεννήτρια συνάρτηση αυτής της ακολουθίας.*

Στην προσθετική αριθμοθεωρία είναι βολικό να χρησιμοποιούμε δυναμοσειρές ως γεννήτριες συναρτήσεις. Στην πολλαπλασιαστική αριθμοθεωρία αντίστοιχο ρόλο έχουν οι σειρές $Dirichlet$.
Σημειώνουμε ότι η ακολουθία $\{a_0, a_1, ...\}$ καθορίζεται πλήρως από τη δυναμοσειρά $f(x)$.

Θεώρημα 1.3.1. *(Θεώρημα του Euler). Αν* $|x| < 1$ *τότε ισχύει*

$$\prod_{m=1}^{\infty} \frac{1}{1-x^m} = \sum_{n=0}^{\infty} p(n) x^n$$

όπου $p(0) = 1$.

Απόδειξη. Αρχικά θα δώσουμε μια τυπική απόδειξη αγνοώντας τη σύγκλιση και στη συνέχεια θα δώσουμε μια αυστηρή απόδειξη αυτής της ιδιότητας.
Αν κάθε παράγοντας του γινομένου επεκτείνεται σε μια δυναμοσειρά παίρνουμε

$$\prod_{m=1}^{\infty} \frac{1}{1-x^m} = (1 + x + x^2 + ...) \cdot (1 + x^2 + x^4 + ...) \cdot ...$$

Τώρα θα πολλαπλασιάσουμε τη σειρά από τα δεξιά σαν να είχαμε πολυώνυμα και θα μαζέψουμε μαζί τις δυνάμεις του x, έτσι θα δημιουργηθεί μια δυναμοσειρά της μορφής

$$1 + \sum_{k=1}^{\infty} a(k) x^k$$

Θα δείξουμε ότι $a(k) = p(k)$.
Ας υποθέσουμε ότι παίρνουμε τον όρο x^{k_1} από την πρώτη γεωμετρική σειρά, τον όρο x^{2k_2} από τη δεύτερη,..., τον όρο x^{mk_m} από τη m-οστή, όπου κάθε $k_i \geq 0$ με $i = 1, ..., m$.
Έτσι το γινόμενο γίνεται
$x^{k_1} \cdot x^{2k_2} \cdot ... x^{mk_m} = x^k$ όπου $k := k_1 + 2k_2 + ... + mk_m$
Αυτό μπορεί να γραφεί ως εξής:

$$k = (1 + 1 + ... + 1) + (2 + 2 + .. + 2) + ... + (m + m + ... + m)$$

όπου η πρώτη παρένθεση περιέχει το 1, k_1 φορές, η δεύτερη το 2, k_2 φορές, ..., η m-οστή το m, k_m φορές.
Αυτή είναι μια διαμέριση του k σε θετικούς προσθετέους. Επιπλέον κάθε διαμέριση του k θα παράγει ένα τέτοιο όρο x^k και αντιστρόφως κάθε όρος x^k προέρχεται από μια αντίστοιχη διαμέριση του k. Συνεπώς, ο συντελεστής $a(k)$ του x^k είναι ίσος με $p(k)$, τον αριθμό των διαμερίσεων του k.

Ο προηγούμενος ισχυρισμός δεν αποτελεί μια αυστηρή απόδειξη επειδή έχουμε αγνοήσει τη σύγκλιση και επειδή έχουμε πολλαπλασιάσει μαζί άπειρο πλήθος γεωμετρικών σειρών, θεωρώντας τις σαν να ήταν πολυώνυμο. Στη συνέχεια θα δώσουμε μια αυστηρή απόδειξη.

Η δυναμοσειρά $\displaystyle\sum_{n=1}^{\infty} x^n$ συγκλίνει απόλυτα για $0 \leq x < 1$.

Επομένως, απο το θεώρημα 1.2.3, και το απειρογινόμενο $\displaystyle\prod_{n=1}^{\infty}(1-x^n)$ συγκλίνει απόλυτα για $0 \leq x < 1$. Άμεση συνέπεια της παραπάνω παρατήρησης είναι ότι και το $\displaystyle\prod_{n=1}^{\infty}\frac{1}{1-x^n}$ συγκλίνει απόλυτα για $0 \leq x < 1$

Για το λόγο αυτό περιορίζουμε το x να βρίσκεται στο διάστημα $0 \leq x < 1$ και εισάγουμε δυο συναρτήσεις

$$F_m(x) := \prod_{k=1}^{m}\frac{1}{1-x^k} \text{ και } F(x) := \prod_{k=1}^{\infty}\frac{1}{1-x^k} = \lim_{m\to\infty} F_m(x)$$

Το οριζόμενο γινόμενο $F(x)$ συγκλίνει απόλυτα αν $0 \leq x < 1$. Παρατηρούμε ότι για κάθε σταθερό x, η ακολουθία $F_m(x)$ είναι αύξουσα. Πράγματι,

$$F_{m+1}(x) = \prod_{n=1}^{m+1}\frac{1}{1-x^n} = \frac{1}{1-x^{m+1}}\prod_{n=1}^{m}\frac{1}{1-x^n} = \frac{1}{1-x^{m+1}}F_m(x) \geq F_m(x)$$

Το $F_m(x)$ είναι το γινόμενο πεπερασμένου πλήθους απολύτως συγκλινόντων δυναμοσειρών. Επομένως και το γινόμενο είναι μια απολύτως συγκλίνουσα δυναμοσειρά.

Επειδή $F_m(x)$ είναι αύξουσα, $F_m(x) \leq F(x)$ για κάθε σταθέρο x όπου $0 \leq x < 1$ και κάθε m. Τώρα $F_m(x)$ είναι το γινόμενο πεπερασμένου πλήθους απόλυτα συγκλινουσών σειρών, έτσι, μπορούμε να το γράψουμε ως εξής

$$F_m(x) = 1 + \sum_{k=1}^{\infty} p_m(k)x^k$$

Εδώ $p_m(k)$ είναι το πλήθος των λύσεων της εξίσωσης $k = k_1 + 2k_2 + ... + mk_m$.
Με άλλα λόγια, $p_m(k)$ είναι ο αριθμός των διαμερίσεων του k σε μέρη που δεν υπερβαίνουν το m.

Αν $m \geq k$ τότε $p_m(k) = p(k)$.
Επιπλέον, γενικά ισχύει ότι πάντα έχουμε $p_m(k) \leq p(k)$. Αυτό σημαίνει ότι

$$\lim_{m\to\infty} p_m(k) = p(k)$$

Τώρα θα διασπάσουμε τη σειρά $F_m(x)$ σε δυο μέρη,

$$F_m(x) = \sum_{k=0}^{m} p_m(k)x^k + \sum_{k=m+1}^{\infty} p_m(k)x^k = \sum_{k=0}^{m} p(k)x^k + \sum_{k=m+1}^{\infty} p_m(k)x^k$$

Επειδή $x \geq 0$, έχουμε $\displaystyle\sum_{k=0}^{m} p(k)x^k \leq F_m(x) \leq F(x)$.

Αυτό δείχνει ότι η σειρά $\displaystyle\sum_{k=0}^{\infty} p(k)x^k$ συγκλίνει.

Επιπλέον επειδή $p_m(k) \leq p(k)$ έχουμε

$$\sum_{k=0}^{\infty} p_m(k)x^k \leq \sum_{k=0}^{\infty} p(k)x^k \leq F(x).$$

Έτσι για κάθε σταθερό x, η σειρά $\displaystyle\sum_{k=0}^{\infty} p_m(k)x^k$ συγκλίνει ομοιόμορφα ως προς m.
Αφήνοντας το $m \to \infty$ παίρνουμε

$$F(x) = \lim_{m\to\infty} F_m(x) = \lim_{m\to\infty} \sum_{k=0}^{\infty} p_m(k)x^k = \sum_{k=0}^{\infty} \lim_{m\to\infty} p_m(k)x^k = \sum_{k=0}^{\infty} p(k)x^k$$

όπου αποδεικνύει την ιδιότητα του *Euler* για $0 \leq x < 1$.
Αυτό μπορούμε να το επεκτείνουμε από την αναλυτική συνέχεια στον μοναδιαίο δίσκο $\mid x \mid < 1$. □

Θεώρημα 1.3.2. *Έστω $H \subset \mathbb{N}$, d ένας θετικός ακέραιος και f,f_d να δίνονται από τους τύπους*

$$f(x) = \sum_{n=0}^{\infty} p(\widehat{H}, n)x^n \text{ και } f_d(x) = \sum_{n=0}^{\infty} p(\widehat{H}_d, n)x^n$$

τότε $f(x) = \prod_{n \in H} \frac{1}{1-x^n}$ *και* $f_d(x) = \prod_{n \in H} \frac{1-x^{(d+1)n}}{1-x^n}$

Απόδειξη. Αν αγνοήσουμε τη σύγκλιση, έχουμε
$\prod_{n \in H} \frac{1}{1-x^n} = \prod_{n \in H}(1 + x^n + ... + x^{kn} + ...) = \sum^{*} x^{x_1 h_1 + ... + x_k h_k}$
όπου $h_1, h_2, ...$ είναι απαρίθμηση κατά αύξουσα σειρά των στοιχείων του H και το άθροισμα $\sum^{*}$ λαμβάνεται πάνω απ΄ όλες τις πεπερασμένες ακολουθίες μη-αρνητικών ακεραίων $x_1, ..., x_k$ για $k = 1, 2, ...$.
Τώρα, για κάθε n, x_n που εμφανίζονται σε αυτό το άθροισμα κάθε φορά, η εξίσωση

$$n = x_1 h_1 + ... + x_k h_k$$

έχει λύση $x_1, ..., x_k$ και τότε n είναι μια διαμέριση στο $\widehat{H}$.
Αντιστρόφως, κάθε διαμέριση που αποτελείται από θετικούς ακεραίους και χρησιμοποιεί στοιχεία του H, θα εμφανίζεται σαν εκθέτης στο άθροισμα $\sum^{*}$.

Ανάλογα, αποδεικνύεται και ότι

$$f_d(x) = \sum_{n=0}^{\infty} p(\widehat{H}_d, n) x^n$$

Στη συνέχεια, γνωρίζουμε ότι

$$\prod_{n \in H} \frac{1}{1-x^n} = \sum_{n=0}^{\infty} p(\widehat{H}, n) x^n$$

τα αθροίσματα και τα γινόμενα παραπάνω συγκλίνουν όταν
$0 < x < 1$. Δίνουμε τώρα μια αυστηρή απόδειξη της σχέσης

$$f(x) = \sum_{n=0}^{\infty} p(\widehat{H}, n) x^n$$

Πρώτα απ΄ όλα,

$$\prod_{i=1}^{n}(1 + x^{h_i} + ... + x^{kh_i} + ...)$$

είναι πεπερασμένο γινόμενο από απόλυτα συγκλίνουσες σειρές και έτσι συγκλίνει και το ίδιο απόλυτα. Επίσης,

$$S_m = \sum_{n=0}^{h_m} p(\widehat{H}, n)x^n \leq \prod_{i=1}^{m} \frac{1}{1-x^{h_i}} < \prod_{i=1}^{\infty} \frac{1}{1-x^{h_i}} < \infty$$

Η τελευταία ανισότητα προκύπτει από τη σύγκλίση της $\sum_{i=1}^{\infty} x^{h_i}$.

Ως εκ τούτου, το S_m είναι μια αύξουσα φραγμένη σειρά και έτσι τείνει σε κάποιον αριθμό. Έπειτα,

$$\sum_{n=0}^{\infty} p(\widehat{H}, n)x^n \geq \prod_{i=1}^{m} \frac{1}{1-x^{h_i}} \to \prod_{i=1}^{\infty} \frac{1}{1-x^{h_i}} \text{ καθώς } m \to \infty$$

□

Θεώρημα 1.3.3. *Αν O συμβολίζει το σύνολο των περιττών θετικών ακεραίων τότε ισχύει $p(\widehat{O}, n) = p(\widehat{N_1}, n)$*

Απόδειξη. Εφαρμόζουμε το θεώρημα 1.3.2 για $f(x) = \sum_{n=0}^{\infty} p(\widehat{O}, n)x^n$ και στη δεύτερη σχέση θεωρούμε $d = 1$ και $H = \mathbb{N}$ τότε ισχύει

$$\sum_{n=0}^{\infty} p(\widehat{O}, n)x^n = \prod_{n=1}^{\infty} \frac{1}{1-x^{2n-1}} \text{ και } \sum_{n=0}^{\infty} p(\widehat{N_1}, n)x^n = \prod_{n=1}^{\infty} \frac{1-x^{2n}}{1-x^n}.$$

Αλλά $\prod_{n=1}^{\infty} \frac{1-x^{2n}}{1-x^n} = \frac{1-x^2}{1-x} \cdot \frac{1-x^4}{1-x^2} \cdot \frac{1-x^6}{1-x^3} \cdots = \prod_{n=1}^{\infty} \frac{1}{1-x^{2n-1}}$

από την ακύρωση των εναλλασσόμενων όρων του παρονομαστή.

Άρα $\sum_{n=0}^{\infty} p(\widehat{O}, n)x^n = \sum_{n=0}^{\infty} p(\widehat{N_1}, n)x^n$

Το αποτέλεσμα έπεται επειδή ταυτόσημες συναρτήσεις έχουν ταυτόσημες δυναμοσειρές.

□

1.4 Γραφική παράσταση

Ας θεωρήσουμε για παράδειγμα $n = 13$ με τη διαμέριση 13=5+3+3+2 . Μπορούμε να την αναπαραστήσουμε με το παρακάτω διάγραμμα με τελείες:

. . . . .
. . .
. . .
. .

Έτσι οι τέσσερις προσθετέοι αναπαρίστανται από οριζόντιες γραμμές με τελείες.

Το διάγραμμα μπορεί να διαβαστεί και κάθετα, έτσι το 13 έχει επίσης τη διαμέριση 4+4+3+1+1. Αυτές οι δυο διαμερίσεις ονομάζονται συζυγείς.Αξίζει επίσης να σημειωθεί ότι αυτή η απλή αναπαράσταση έχει μερικές χρήσιμες συνέπειες.

Ορισμός 1.4.1. *Έστω n φυσικός αριθμός και οι διαμερίσεις του* $\mathbf{a}$ *και* $\mathbf{b}$*, τότε* $n = a_1 + a_2 + ... + a_k = b_1 + b_2 + ... + b_m$ *όπου* $a_{i+1} \leq a_i$ *και* $b_{i+1} \leq b_i$ *για κάθε* i *. Αναπαριστούμε τη διαμέριση* $\mathbf{a}$ *με το σύνολο των σημείων στο επίπεδο στη μορφή*

$$\begin{gathered}(0,0),(1,0),...,(a_1-1,0)\\(0,-1),(1,-1),...,(a_2-1,-1)\\.\\.\\.\\(0,-k+1),(1,-k+1),...,(a_k-1,-k+1)\end{gathered}$$

Παρόμοια παράσταση σχηματίζουμε και για το $\mathbf{b}$*. Έτσι, οι διαμερίσεις* $\mathbf{a}$ *και* $\mathbf{b}$ *ονομάζονται συζυγείς αν η παράσταση με τις τελείες για την διαμέριση* $\mathbf{a}$ *είναι συμμετρική ως προς την παράσταση της διαμέρισης* $\mathbf{b}$ *ως προς τον άξονα* $y = -x$*.*

Θεώρημα 1.4.1. *Ο αριθμός των διαμερίσεων του n με το πολύ m προσθετέους ισούται με τον αριθμό των διαμερίσεων του n στις οποίες κανένας προσθετέος δεν υπερβαίνει το m.*

Απόδειξη. Προκύπτει άμεσα από τον προηγούμενο ορισμό αφού η συζυγία ορίζει μια 1-1 αντιστοιχία ανάμεσα στις δύο κλάσεις των διαμερίσεων. □

Παράδειγμα: *Αν $n = 5$ και $m = 2$, οι διαμερίσεις του 5 με το πολύ 2-προσθεταίους είναι 5, 4+1, 3+2 και οι διαμερίσεις όπου κανένας προσθεταίος δεν είναι μεγαλύτερος του 2 είναι*

2+2+1, 2+1+1+1, 1+1+1+1+1

δηλαδή 3=3.

Ερχόμαστε τώρα στο θεώρημα του Euler για τους πενταγωνικούς αριθμούς όπου παρέχεται ένας λειτουργικός αλγόριθμος για τον υπολογισμό του $p(n)$. Σημειώνουμε ότι πενταγωνικός είναι κάθε αριθμός της μορφής

$$\frac{m(3m+1)}{2} \text{ ή } \frac{m(3m-1)}{2} \text{ με } m = 1, 2, ...$$

Θεώρημα 1.4.2. *Έστω $p_1(\widehat{H}, n)$ και $p_2(\widehat{H}, n)$ να συμβολίζουν τον αριθμό των διαμερίσεων του n στο H όπου οι προσθετέοι είναι μόνο περιττού ή μόνο άρτιου πλήθους αντίστοιχα.Έχουμε:*

$$p_2(\widehat{N_1}, n) - p_1(\widehat{N_1}, n) = \begin{cases} \text{(-1)}^r, \text{ αν } n = \dfrac{r(3r \pm 1)}{2}, r \in \mathbb{N} \\ \text{0,αλλιώς} \end{cases}$$

Θα δώσουμε μια στοιχειώδη απόδειξη μέσω της θεωρίας γραφημάτων,σύμφωνα με τον Franklin.

Απόδειξη. Έστω $\mathbf{a}$ μια διαμέριση του n σε r διακριτούς προσθετέους.
Έτσι $n = a_1 + a_2 + ... + a_r$ και $a_i > a_{i+1}$ για όλα τα i. Έστω $s(\mathbf{a}) = a_r$ ο μικρότερος προσθεταίος της διαμέρισης και $t(\mathbf{a})$ ο μεγαλύτερος ακέραιος c τέτοιος ώστε

$$\begin{gathered} a_1 = a_2 + 1 \\ \alpha_2 = a_3 + 1 \\ . \\ . \\ . \\ \alpha_{c-1} = a_c + 1 \end{gathered}$$

και έστω $t(\mathbf{a}) = 1$ αν $a_1 \neq a_2 + 1$.
Σημειώνουμε ότι $t(\mathbf{a}) \leq r$. Ορίζουμε μια αντιστοιχία ανάμεσα στις διαμερίσεις του n που απαριθμούνται από τα $p_1(\widehat{N_1}, n)$ και $p_2(\widehat{N_1}, n)$.
Περίπτωση 1: $s(\mathbf{a}) \leq t(\mathbf{a})$
Θεωρούμε τη διαμέριση $\mathbf{a}$ του n, προσθέτουμε ένα στους πρώτους $s(\mathbf{a})$ όρους και διαγράφουμε τον τελευταίο όρο. Έτσι η καινούργια διαμέριση είναι

$$n = (a_1 + 1) + ... + (a_{s(\mathbf{a})} + 1) + a_{s(\mathbf{a})+1} + ... + a_{r-1}$$

Περίπτωση 2: $s(\mathbf{a}) > t(\mathbf{a})$
Θεωρούμε τη διαμέριση $\mathbf{a}$ του n, αφαιρούμε ένα από κάθε ένα από τους πρώτους $t(\mathbf{a})$ όρους και προσθέτουμε στο τέλος τον όρο $t(\mathbf{a})$. Έτσι η καινούργια διαμέριση είναι

$$(a_1 - 1) + ... + (a_{t(\mathbf{a})} - 1) + a_{t(\mathbf{a})+1} + ... + a_r + t(\mathbf{a})$$

Αφού $a_{t(\mathbf{a})} - 1 > a_{t(\mathbf{a})+1}$ και $a_r > t(\mathbf{a})$ η παραπάνω είναι μια διαμέριση σε διακριτούς προσθετέους.

Αυτές οι δυο περιπτώσεις μας δίνουν μια ένα προς ένα αντιστοιχία ανάμεσα στις διαμερίσεις που απαριθμούνται από τα $p_1(\widehat{N_1}, n)$ και $p_2(\widehat{N_1}, n)$ εκτός από τις επόμενες ειδικές περιπτώσεις.

Αρχικά θεωρούμε το παράδειγμα $n = 12$ με τη διαμέριση c :12=5+4+3
Έτσι, $s(c) = 3 =$ ο τελευταίος προσθεταίος και $t(c) = 3$ αφού

$$a_1 = 5, a_2 = a_1 - 1 = 4 \text{ και } a_3 = a_2 - 1 = 3$$

Συνεπώς αποτυγχάνουν οι παραπάνω περιπτώσεις.
Οι ειδικές περιπτώσεις είναι οι ακόλουθες:
$(i) s(\mathbf{a}) = t(\mathbf{a}) = r$ όταν $n = (2r-1) + (2r-2) + ... + r = \dfrac{r(3r-1)}{2}$ και
(ii) $s(\mathbf{a}) = t(\mathbf{a}) = r + 1$ όταν $n = 2r + (2r-1) + ... + (r+1) = \dfrac{r(3r+1)}{2}$ Ο όρος $(-1)^r$ στο θεώρημα υπολογίζει αυτές τις ειδικές περιπτώσεις και έτσι προκύπτει το αποτέλεσμα. □

Θεώρημα 1.4.3. *(Θεώρημα του Euler για πενταγωνικούς αριθμούς)*
Για $0 < x < 1$

$$\prod_{n=1}^{\infty}(1-x^n) = 1 + \sum_{m=1}^{\infty}(-1)^m x^{\frac{m(3m-1)}{2}}(1+x^m) = \sum_{m=-\infty}^{\infty}(-1)^m x^{\frac{m(3m-1)}{2}}$$

Απόδειξη. Χρησιμοποιώντας τη σχέση $(-m)(-3m-1) = m(3m+1)$ στη δεύτερη σειρά έχουμε

$$\sum_{m=-\infty}^{\infty}(-1)^m x^{\frac{m(3m-1)}{2}} = 1 + \sum_{m=1}^{\infty}(-1)^m x^{\frac{m(3m-1)}{2}} + \sum_{m=-1}^{-\infty}(-1)^m x^{\frac{m(3m-1)}{2}} \quad (1.1)$$

Θέτουμε στο άθροισμα $\displaystyle\sum_{m=-1}^{-\infty}(-1)^m x^{\frac{m(3m-1)}{2}}$ όπου m το $-l$ τότε προκύπτει

$$\sum_{-l=-1}^{-\infty}(-1)^{-l} x^{\frac{-l(-3l-1)}{2}} = \sum_{l=1}^{\infty}(-1)^l x^{\frac{l(3l+1)}{2}} = \sum_{m=1}^{\infty}(-1)^m x^{\frac{m(3m+1)}{2}} \quad (1.2)$$

άρα η σχεση 1.1 γίνεται διαδοχικά

$$\sum_{m=-\infty}^{\infty}(-1)^m x^{\frac{m(3m-1)}{2}} = 1 + \sum_{m=1}^{\infty}(-1)^m x^{\frac{m(3m-1)}{2}} + \sum_{m=1}^{\infty}(-1)^m x^{\frac{m(3m+1)}{2}}$$

Έτσι από το προηγούμενο θεώρημα αν $n = \frac{m(3m-1)}{2}$ τότε

$$\sum_{m=1}^{\infty}(-1)^m x^{\frac{m(3m-1)}{2}} = \sum_{n=1}^{\infty}(p_2(\widehat{N_1}, n) - p_1(\widehat{N_1}, n))x^n$$

και

$$\sum_{m=1}^{\infty}(-1)^m x^{\frac{m(3m+1)}{2}} = 0$$

ενώ αν $n = \frac{m(3m+1)}{2}$ τότε

$$\sum_{m=1}^{\infty}(-1)^m x^{\frac{m(3m-1)}{2}} = 0$$

και

$$\sum_{m=1}^{\infty}(-1)^m x^{\frac{m(3m+1)}{2}} = \sum_{n=1}^{\infty}(p_2(\widehat{N_1}, n) - p_1(\widehat{N_1}, n))x^n$$

και για $n = 0$ *έχουμε*

$$p_2(\widehat{N_1}, n) - p_1(\widehat{N_1}, n) = 1$$

Συνεπώς,

$$\sum_{m=1}^{\infty}(-1)^m x^{\frac{m(3m+1)}{2}} = \sum_{n=0}^{\infty}(p_2(\widehat{N_1}, n) - p_1(\widehat{N_1}, n))x^n$$

Επιπλέον,

$$\prod_{n=1}^{\infty}(1 - x^n) = \sum^{*}(-1)^{a_1+a_2+\ldots}x^{a_1+2a_2+3a_3+\ldots}$$

όπου το $\sum^{*}$ *συμβολίζει το άθροισμα ως προς όλες τις πεπερασμένες ακολουθίες, από μηδέν και ένα.*

Για παράδειγμα στην ακολουθία $(a_1, a_2, ..., a_l, ...) = (1, 0, ..., 0, ...)$ *αντιστοιχεί ο όρος* $(-1)^{a_1}x^{a_1} = (-1)^1x^1 = -x$
στην ακολουθία $(0, 1, 0, ..., 0, ...)$ *αντιστοιχεί ο όρος* $(-1)^{a_2}x^{2a_2} = -x^2$
Σημειώνουμε ότι το x^n *εμφανίζεται στο άθροισμα όταν*

$$n = n_1 + n_2 + ... + n_r$$

όπου τα n_i *είναι διακεκριμένοι μεταξύ τους και* $0 < n_i \leq n$. *Σε αυτή την περίπτωση το πρόσημο είναι* $(-1)^r$. *(Για παράδειγμα, για* $n = 3 = 1 + 2$ *το* x^3 *εμφανίζεται στο άθροισμα και μάλιστα με συντελεστή* $(-1)^1 = -1$ *όταν* $r = 1$ *αλλά και με συντελεστή* $(-1)^2 = 1$ *όταν* $r = 2$, *έτσι το* x^3 *αναιρείται από το άθροισμα).Τότε το* x^n *το γράφουμε* $x^{a_1+2a_2+3a_3+\cdots}$ *όπου* $a_i = 1$ *όταν* $i = n_j$, $j = 1, ..., r$ *και* $a_i = 0$ *αλλιώς. (Για παράδειγμα,* *3=1+2 άρα* $n_1 = 1$ *και* $n_2 = 2$ *αλλά* $3 = a_1 + 2a_2 + 3a_3 + ...$ *όπου για* $i = 1 = n_1$ *παίρνουμε* $a_1 = 1$ *και για* $i = 2 = n_2$ *παίρνουμε* $a_2 = 1$. *Έτσι,* $3 = 1 + 2 \cdot 1$*).*

Τώρα, $a_1 + 2a_2 + 3a_3 + ...$ *είναι μια διαμέριση σε διακεκριμένους προσθετέους και έχει έναν περιττό (άρτιο) αριθμό από προσθετέους αν και μόνο αν* $(-1)^{a_1+a_2+\cdots} = -1$ *ή* 1 *αντίστοιχα.*
Ως εκ τούτου,

$$\prod_{n=1}^{\infty}(1-x^n) = \sum_{n=0}^{\infty}(p_2(\widehat{N_1}, n) - p_1(\widehat{N_1}, n))x^n$$

Άρα,

$$\prod_{n=1}^{\infty}(1-x^n) = \sum_{m=-\infty}^{\infty}(-1)^m x^{\frac{m(3m-1)}{2}}$$

και

$$\sum_{m=-\infty}^{\infty}(-1)^m x^{\frac{m(3m-1)}{2}} = 1 + \sum_{m=1}^{\infty}(-1)^m[x^{\frac{m(3m-1)}{2}} + x^{\frac{m(3m+1)}{2}}] =$$

$$= 1 + \sum_{m=1}^{\infty}(-1)^m x^{\frac{m(3m-1)}{2}}[1 + x^{(\frac{m(3m+1)}{2} - \frac{m(3m-1)}{2})}] =$$

$$= 1 + \sum_{m=1}^{\infty}(-1)^m x^{\frac{m(3m-1)}{2}}[1 + x^{\frac{3m^2+m-3m^2+m}{2}}] =$$

$$= 1 + \sum_{m=1}^{\infty}(-1)^m x^{\frac{m(3m-1)}{2}}(1 + x^m).$$

Συνεπώς,

$$\prod_{n=1}^{\infty}(1-x^n) = 1 + \sum_{m=1}^{\infty}(-1)^m x^{\frac{m(3m-1)}{2}}(1 + x^m)$$

□

Θεώρημα 1.4.4. *Αν* $n > 0$ *τότε*

$$p(n) - p(n-1) - p(n-2) + ... + (-1)^m p(n - \frac{m(3m-1)}{2}) + (-1)^m p(n - \frac{m(3m+1)}{2}) + ... = 0$$

Σημειώνουμε ότι $p(0) = 1$ *και* $p(n) = 0$ *αν* $n < 0$.

Απόδειξη. Αρκεί αν δείξουμε ότι

$$p(n) - p(n-1) - p(n-2) + p(n-5) + p(n-7) + ... = 0$$

Αν $P(n)$ συμβολίζει το άθροισμα στην αριστερή πλευρά της ισότητας, τότε

$$\sum_{n=0}^{\infty} P(n)x^n = \sum_{n=0}^{\infty} p(n)x^n - \sum_{n=0}^{\infty} p(n-1)x^n - \sum_{n=0}^{\infty} p(n-2)x^n +$$

$$+\sum_{n=0}^{\infty} p(n-5)x^n + \sum_{n=0}^{\infty} p(n-7)x^n + ... =$$

$$= \sum_{n=0}^{\infty} p(n)x^n - x\sum_{n=0}^{\infty} p(n-1)x^{n-1} - x^2\sum_{n=0}^{\infty} p(n-2)x^{n-2} +$$

$$+x^5\sum_{n=0}^{\infty} p(n-5)x^{n-5} + x^7\sum_{n=0}^{\infty} p(n-7)x^{n-7} + ...$$

αλλά $p(n) = 0$ όταν $n < 0$.
Συνεπώς

$$\sum_{n=0}^{\infty} P(n)x^n = \sum_{n=0}^{\infty} p(n)x^n - x\sum_{n=0}^{\infty} p(n)x^n - x^2\sum_{n=0}^{\infty} p(n)x^n + ... =$$

$$= \sum_{n=0}^{\infty} p(n)x^n(1 - x - x^2 + x^5 + x^7 + ...)$$

Αλλά από το θεώρημα 1.4.3 προκύπτει ότι

$$\sum_{n=0}^{\infty} p(n)x^n(1 - x - x^2 + x^5 + x^7 + ...) = 1 + \sum_{m=1}^{\infty}(-1)^m x^{\frac{m(3m-1)}{2}}(1 + x^m) = \prod_{n=1}^{\infty}(1 - x^n)$$

και από το θεώρημα 1.3.3 έχουμε

$$\frac{1}{\prod_{m=1}^{\infty}(1 - x^m)} = \sum_{n=0}^{\infty} p(n)x^n$$

Συνεπώς,

$$\textstyle\sum_{n=0}^{\infty} P(n)x^n = 1$$

Ως εκ τούτου,$P(n) = 0$ αν $n > 0$ $\square$

Παρατήρηση: Το θεώρημα παρέχει μια αναδρομική διαδικασία για τον υπολογισμό του $p(n)$. Αυτό είναι πολύ χρήσιμο για μεγάλα n.Εδώ θα δόσουμε μερικά απλά παραδείγματα.

$$p(5) - p(4) - p(3) + p(0) = 0$$

άρα

$$p(5) = p(4) + p(3) - p(0) = p(4) + p(3) - 1$$

εφαρμόζω το παραπάνω θεώρημα για $n = 4$ τότε $p(4) - p(3) - p(2) = 0$
άρα $p(4) = p(3) + p(2)$, συνεπώς,

$$p(5) = p(3) + p(2) + p(3) - 1 = 2p(3) + p(2) - 1$$

$$\text{και } p(3) = p(2) + p(1)$$

$$\text{άρα } p(5) = 3p(2) + 2p(1) - 1 = 3 \cdot 2 + 2 - 1 = 7$$

Χωρίς απόδειξη αναφέρουμε το

Θεώρημα 1.4.5. *(Rogers – Ramanujan) Ο αριθμός των διαμερίσεων του n σε μέρη που διαφέρουν τουλάχιστον κατα δύο είναι ίσος με τον αριθμό των διαμερίσεων του n σε μέρη που είναι ισότιμα με ένα ή τέσσερα modulo 5. [10]*

1.5 Η ταυτότητα του *Jacobi*

Σε αυτή την ενότητα περιγράφεται η διάσημη ταυτότητα του *Jacobi*. Το θεώρημα του *Euler* για πενταγωνικούς αριθμούς και πολλές άλλες ταυτότητες διαμέρισης βρίσκονται ως ειδικές περιπτώσεις του τύπου του *Jacobi*.

Θεώρημα 1.5.1. *(ταυτότητα του Jacobi για το τριπλό γινόμενο)*
Για μιγαδικούς x και z με $\mid x \mid < 1$ και $z \neq 0$ ισχύει

$$\prod_{n=1}^{\infty} (1 - x^{2n})(1 + x^{2n-1}z^2)(1 + \frac{x^{2n-1}}{z^2}) = \sum_{m=-\infty}^{\infty} x^{m^2} z^{2m} \tag{1.3}$$

Απόδειξη. Το z είναι ένας σταθερός μιγαδικός αριθμός και έστω $k = \mid z \mid$.
Επειδή $\mid x \mid < 1$ θα υπάρχει κάποιο $n_0 \in \mathbf{N}$ τέτοιο ώστε $\forall n \geq n_0$ να ισχύει

$$\mid x \mid^n \mid z \mid^2 < 1$$

(αφού $\mid x \mid^n \to 0$). Έτσι, αν θέσουμε

$$a_n = x^n z^2$$

η σειρά $\sum_{n=1}^{\infty} | a_n |$ συγκλίνει. Άρα από το θεώρημα 1.2.3, το απειρογινόμενο

$$\prod_{n=1}^{\infty}(1+ | a_n |) = \prod_{n=1}^{\infty}(1 + x^n z^2)$$

συγκλίνει απόλυτα.
Συνεπώς και το $\prod_{n=1}^{\infty}(1 + x^{2n-1}z^2)$ συγκλίνει απόλυτα.
Τώρα, αφού $| x |< 1$ θα υπάρχει $n_0 \in \mathbb{N}$ τέτοιο ώστε $\forall n \geq n_0$ να ισχύει $| x |^{2n}< 1$ άρα αν θέσουμε $a_n = x^{2n}$
τότε η σειρά $\sum_{n=0}^{\infty} | x |^{2n}$ συγκλίνει άρα και το απειρογινόμενο $\prod_{n=1}^{\infty}(1 - x^{2n})$.
Ομοίως προκύπτει ότι και το απειρογινόμενο $\prod_{n=1}^{\infty} | 1 + \frac{x^{2n-1}}{z^2} |$ συγκλίνει.
Επιπλέον, για κάθε σταθερό x με $| x |< 1$ οι σειρές και τα γινόμενα συγκλίνουν ομοιόμορφα στα συμπαγή υποσύνολα του $z-$επιπέδου που δεν περιέχουν το $z = 0$. Έτσι κάθε μέλος της 1.3 είναι μια αναλυτική συνάρτηση του z για $z \neq 0$. Για σταθερό $z \neq 0$, η σειρά και τα γινόμενα συγκλίνουν ομοιόμορφα για $| x |\leq r < 1$, συνεπώς αναπαριστούν αναλυτικές συναρτήσεις του x στο δίσκο $| x |< 1$.
Για να το αποδείξουμε κρατάμε σταθερό το x και ορίζουμε $F(z)$ για $z \neq 0$ από την εξίσωση

$$F(z) = \prod_{n=1}^{\infty}(1 + x^{2n-1}z^2)(1 + x^{2n-1}z^{-2}) \tag{1.4}$$

Πρώτα δείχνουμε ότι η F ικανοποιεί τη συναρτησιακή εξίσωση

$$xz^2 F(xz) = F(z)$$

Από τη σχέση 1.4 βρίσκουμε

$$F(xz) = \prod_{n=1}^{\infty}(1 + x^{2n-1}(xz)^2)(1 + \frac{x^{2n-1}}{(xz)^2}) =$$

$$= \prod_{n=1}^{\infty}(1 + x^{2n+1}z^2)(1 + x^{2n-3}z^{-2}) =$$

$$= \prod_{m=2}^{\infty}(1 + x^{2m-1}z^2) \prod_{r=0}^{\infty}(1 + x^{2r-1}z^{-2})$$

το οποίο προκύπτει αν θέσουμε $m = n + 1$, $r = n - 1$
Έπειτα,

$$xz^2 = xz^2 \frac{1 + xz^2}{1 + xz^2} = \frac{1 + xz^2}{1 + \frac{1}{xz^2}}$$

Συνεπώς,

$$xz^2 f(xz) = \frac{1 + xz^2}{1 + \frac{1}{xz^2}} \prod_{m=2}^{\infty} (1 + x^{2m-1} z^2) \prod_{r=0}^{\infty} (1 + \frac{x^{2r-1}}{z^2}) =$$

$$= (1 + xz^2) \prod_{m=2}^{\infty} (1 + x^{2m-1} z^2) \frac{1}{1 + \frac{1}{xz^2}} \prod_{r=0}^{\infty} (1 + \frac{x^{2r-1}}{z^2}) =$$

$$= \prod_{m=1}^{\infty} (1 + x^{2m-1} z^2) \prod_{r=1}^{\infty} (1 + \frac{x^{2r-1}}{z^2}) =$$

$$= \prod_{n=1}^{\infty} (1 + x^{2n-1} z^2)(1 + \frac{x^{2n-1}}{z^2}) = F(z)$$

Έστω τώρα

$$G(z) = \prod_{n=1}^{\infty} (1 - x^{2n})(1 + x^{2n-1} z^2)(1 + \frac{x^{2n-1}}{z^2})$$

τότε

$$G(z) = F(z) \prod_{n=1}^{\infty} (1 - x^{2n})$$

και

$$G(z) = xz^2 G(xz)$$

αφού

$$xz^2 G(xz) = xz^2 F(xz) \prod_{n=1}^{\infty} (1 - x^{2n}) = F(z) \prod_{n=1}^{\infty} (1 - x^{2n}) = G(z)$$

Επιπλέον, $G(z)$ είναι μια άρτια συνάρτηση αφού έχει συμμετρικό πεδίο ορισμού (το οποίο είναι το $\mathbb{C} - \{0\}$) και

$$G(-z) = F(-z) \prod_{n=1}^{\infty} (1 - x^{2n}) = \prod_{n=1}^{\infty} (1 + x^{2n-1} z^2)(1 + \frac{x^{2n-1}}{z^2}) \prod_{n=1}^{\infty} (1 - x^{2n})$$

$$= F(z) \prod_{n=1}^{\infty} (1 - x^{2n}) = G(z)$$

Είναι επίσης αναλυτική για όλα τα $z \neq 0$, έτσι έχει ένα ανάπτυγμα *Laurent* της μορφής

$$G(z) = \sum_{n=-\infty}^{\infty} a_m z^{2m} \tag{1.5}$$

και $G(-z) = \displaystyle\sum_{n=-\infty}^{\infty} a_{-m} z^{-2m} = \sum_{n=-\infty}^{\infty} a_m z^{2m} = G(z)$, άρα $a_{-m} = a_m$ (οι συντελεστές του a_m εξαρτώνται απο το x).
Τώρα θα δείξουμε ότι

$$a_m = x^{2m-1} a_{m-1}$$

Έχουμε

$$xz^2 G(xz) = xz^2 \sum_{m=-\infty}^{\infty} a_m (xz)^{2m} = \sum_{m=-\infty}^{\infty} a_m x^{2m+1} z^{2m+2}$$

Θέτουμε $l = m + 1$ τότε $m = l - 1$ οπότε

$$xz^2 G(xz) = \sum_{l=-\infty}^{\infty} a_{l-1} x^{2l-1} z^{2l}$$

άρα

$$G(z) = \sum_{m=-\infty}^{\infty} a_{m-1} x^{2m-1} z^{2m}$$

οπότε και

$$\sum_{m=-\infty}^{\infty} a_m z^{2m} = \sum_{m=-\infty}^{\infty} a_{m-1} x^{2m-1} z^{2m}$$

και συνεπώς

$$a_m = a_{m-1} x^{2m-1}.$$

Οι συντελεστές αυτοί επαναλαμβάνονται συνεχώς έτσι

$$a_m = x^{2m-1} a_{m-1}$$

$$a_{m-1} = x^{2(m-1)-1} a_{m-2} = x^{2m-3} a_{m-2}.$$

Επομένως,

$$a_m = x^{2m-1} x^{2m-3} a_{m-2} = \tfrac{x^{2m}}{x} \tfrac{x^{2m}}{x^3} a_{m-2} =$$

$$= \frac{x^{2m} x^{2m} \cdots x^{2m}}{x x^3 \cdots x^{2m-1}} a_0 =$$

$$= \frac{(x^{2m})^m}{x^{m\frac{(2m-1)+1}{2}}} a_0 = \frac{x^{2m^2}}{x^{m^2}} a_0 =$$

$$= x^{m^2} a_0 \text{ για όλα τα } m \geq 0$$

Αυτή η σχέση ισχύει επίσης και για $m < 0$ αφού $a_{-m} = a_m$.
Τελικά για κάθε $m \in \mathbb{Z}$ ισχύει $a_m = a_0 x^m$.
Για το λόγο αυτό, η 1.5 γίνεται

$$G_x(z) = \sum_{m=-\infty}^{\infty} a_0(x) x^{m^2} z^{2m} = a_0(x) \sum_{m=-\infty}^{\infty} x^{m^2} z^{2m} \tag{1.6}$$

όπου γράψαμε το $G_x(z)$ αντί για το $G(z)$ και το $a_0(x)$ αντί για το a_0, για να δηλώσουμε την εξάρτηση από το x.
Όταν $x \longrightarrow 0$ έχουμε

$$x^k \longrightarrow 0 \text{ για κάθε } k \neq 0,$$

έτσι για κάθε $m \neq 0$ σταθερό ισχύει $x^{m^2} z^{2m} \longrightarrow 0$.
Άν $m = 0$ τότε

$$\lim_{x \to 0} G(z) = \lim_{x \to 0} a_0(x) \cdot 1$$

άρα

$$\lim_{x \to 0} F(z) \prod_{m=1}^{\infty} (1 - x^{2n}) = \lim_{x \to 0} a_0(x)$$

και επομένως,

$$\lim_{x \to 0} a_0(x) = 1 \cdot 1 \cdot 1$$

συνεπώς $a_0(x) \to 1$ όταν $x \to 0$.
Για να ολοκληρώσουμε την απόδειξη, πρέπει να δείξουμε ότι $a_0(x) = 1$ για όλα τα x.
Παίρνουμε $z = e^{\frac{\pi i}{4}}$ τότε

$$z^2 = e^{\frac{2\pi i}{4}} = e^{\frac{\pi i}{2}} = \cos\tfrac{\pi}{2} + i \sin\tfrac{\pi}{2} = i$$

άρα αντικαθιστώντας στην 1.6 βρίσκουμε

$$G_x(e^{\frac{\pi i}{4}}) = a_0(x) \sum_{m=-\infty}^{\infty} x^{m^2} (e^{\frac{\pi i}{4}})^{2m} = a_0(x) \sum_{m=-\infty}^{\infty} x^{m^2} i^m \tag{1.7}$$

και

$$i^{2m} = 1 \Longleftrightarrow i^m = -\tfrac{1}{i^m} \Longleftrightarrow i^m = -i^{-m}$$

έτσι στην 1.7 οι περιττοί όροι αναιρούνται

$$(\ x^{m^2}i^m \text{ με το } x^{(-m)^2}i^{-m} = -x^{m^2}i^m \ )$$

και μένουν μόνο οι άρτιοι, συνεπώς

$$G_x(e^{\frac{\pi i}{4}}) = a_0(x) \sum_{n=-\infty}^{\infty} x^{(2n)^2} i^{2n} = a_0(x) \sum_{n=-\infty}^{\infty} (-1)^n x^{(2n)^2}$$

άρα

$$\frac{G_x(e^{\frac{\pi i}{4}})}{a_0(x)} = \sum_{n=-\infty}^{\infty} (-1)^n x^{(2n)^2} \tag{1.8}$$

και

$$\alpha_0(x^4) = \frac{a_0(x^4) \displaystyle\sum_{m=-\infty}^{\infty} (x^4)^{m^2} i^{2m}}{a_0(x^4)} = \sum_{m=-\infty}^{\infty} x^{4m^2}(-1)^m = \sum_{m=-\infty}^{\infty} x^{(2m)^2}(-1)^m$$

$$\sum_{n=-\infty}^{\infty} x^{(2n)^2}(-1)^n = \frac{G_x(e^{\frac{\pi i}{4}})}{a_0(x)} \tag{1.9}$$

όπου $G_{x^4}(i) = G_x(e^{\frac{\pi i}{4}})$
αφού

$$G_x(e^{\frac{\pi i}{4}}) = \prod_{n=1}^{\infty} (1 + x^{2n-1} e^{\frac{2\pi i}{4}})(1 + \frac{x^{2n-1}}{e^{\frac{2\pi i}{4}}}) \prod_{n=1}^{\infty} (1 - x^{2n}) =$$

$$= \prod_{n=1}^{\infty} (1 + x^{2n-1} i)(1 + \frac{x^{2n-1}}{i})(1 - x^{2n}) =$$

$$= \prod_{n=1}^{\infty} (1 + x^{2n-1} i)(1 - i x^{2n-1})(1 - x^{2n}) = \prod_{n=1}^{\infty} (1 - i^2 x^{(2n-1)2})(1 - x^{2n}) =$$

$$= \prod_{n=1}^{\infty} (1 + x^{4n-2})(1 - x^{2n})$$

και, επειδή κάθε άρτιος αριθμός είναι της μορφής $4n$ ή $4n-2$, έχουμε

$$\prod_{n=1}^{\infty} (1 - x^{2n}) = \prod_{n=1}^{\infty} (1 - x^{4n})(1 - x^{4n-2})$$

έτσι,

$$G_x(e^{\frac{\pi i}{4}}) = \prod_{n=1}^{\infty}(1-x^{4n})(1-x^{4n-2})(1+x^{4n-2}) =$$

$$= \prod_{n=1}^{\infty}(1-x^{4n})(1-x^{8n-4}) =$$

$$= \prod_{n=1}^{\infty}(1-x^{4(2n)})(1-x^{4(2n-2)})(1-x^{8n-4}) =$$

$$= \prod_{n=1}^{\infty}(1-x^{8n})(1-x^{8n-4})(1-x^{8n-4}) =$$

$$= \prod_{n=1}^{\infty}(1+x^{4(2n-1)}i^2)(1+x^{4(2n-1)})(1-x^{4\cdot 2n}) = G_{x^4}(i)$$

έτσι, η 1.11 συνεπάγεται $a_0(x) = a_0(x^4)$.
Αντικαθιστώντας το x με x^4, x^{4^2} ,...., βρίσκουμε

$$a_o(x) = a_o(x^{4^k}) \text{ για } k = 1, 2, ...$$

$$\text{αλλά } x^{4^k} \to 0 \text{ καθώς } k \to \infty \text{ και } a_0(x) \to 1 \text{ καθώς } x \to 0,$$

επομένως

$$a_o(x) = 1 \text{ για όλα τα } x$$

Αυτό ολοκληρώνει την απόδειξη.

□

Αν αντικαταστήσουμε το x με $-x^{\frac{3}{2}}$ και το z με το $x^{\frac{1}{4}}$ θα έχουμε

$$\prod_{n=1}^{\infty}(1-(-(x^{\frac{3}{2}}))^{2n})(1+(-x^{\frac{3}{2}})^{2n-1}x^{\frac{1}{4}2})\ (1+\frac{(-x^{\frac{3}{2}})^{2n-1}}{x^{\frac{1}{4}2}}) =$$

$$= \sum_{n=-\infty}^{\infty}(-x^{\frac{3}{2}})^{n^2}x^{\frac{1}{4}2n}$$

$$\Leftrightarrow \prod_{n=1}^{\infty}(1-x^{3n})(1+(-1)^{2n-1}x^{3n-\frac{3}{2}+\frac{1}{2}})\ (1+(-1)^{2n-1}x^{3n-\frac{3}{2}-\frac{1}{2}}) =$$

$$= \sum_{n=-\infty}^{\infty}(-x^{\frac{3}{2}})^{n^2}x^{\frac{n}{2}}$$

$$\Leftrightarrow \prod_{n=1}^{\infty}(1-x^{3n})(1-x^{3n-1})(1-x^{3n-2}) = \sum_{n=-\infty}^{\infty}(-1)^{n^2}(x^{\frac{3}{2}})^{n^2}x^{\frac{n}{2}}$$

$$\Leftrightarrow \prod_{n=1}^{\infty}(1-x^{n}) = \sum_{n=-\infty}^{\infty}(-1)^{n}x^{\frac{3}{2}n^2+\frac{n}{2}}$$

$$\Leftrightarrow \prod_{n=1}^{\infty}(1-x^{n}) = \sum_{n=-\infty}^{\infty}(-1)^{n}x^{\frac{n(3n+1)}{2}}$$

Θεώρημα 1.5.2. *i)* $\sum_{n=-\infty}^{\infty}x^{n^2} = \prod_{n=1}^{\infty}(1-x^{2n})(1+x^{2n-1})^2$

ii) $\sum_{n=0}^{\infty}(-1)^n(2n+1)x^{\frac{n(n+1)}{2}} = \prod_{n=1}^{\infty}(1-x^n)^3$

iii) $\sum_{n=0}^{\infty}x^{\frac{n(n+1)}{2}} = \prod_{n=1}^{\infty}(1-x^{2n})(1+x^n) = \dfrac{(1-x^2)(1-x^4)....}{(1-x)(1-x^3)....}$

Το *i)* συχνά ονομάζεται επίσης ταυτότητα του *Jacobi*.

Απόδειξη. *i)* Αν στην ταυτότητα του *Jacobi* θέσουμε $z=1$ προκύπτει:

$$\prod_{n=1}^{\infty}(1-x^{2n})(1+x^{2n-1}1^2)(1+\frac{x^{2n-1}}{1^2}) = \sum_{m=-\infty}^{\infty}x^{m^2}1^{2m},$$

$$\prod_{n=1}^{\infty}(1-x^{2n})(1+x^{2n-1})(1+x^{2n-1}) = \sum_{m=-\infty}^{\infty}x^{m^2},$$

$$\prod_{n=1}^{\infty}(1-x^{2n})(1+x^{2n-1})^2 = \sum_{n=-\infty}^{\infty}x^{n^2},$$

ii) Αν στην ταυτότητα του *Jacobi* αντικαταστήσουμε το x με $x^{\frac{1}{2}}$ και το z^2 με $x^{\frac{1}{2}}y$ και πολλαπλασιάσουμε με $\dfrac{y}{y+1}$ προκύπτει:

$$\frac{y}{y+1}\prod_{n=1}^{\infty}(1-x^n)(1+x^{\frac{1}{2}(2n-1)}x^{\frac{1}{2}}y)(1+\frac{x^{\frac{1}{2}(2n-1)}}{x^{\frac{1}{2}}y}) = \frac{y}{y+1}\sum_{n=-\infty}^{\infty}x^{\frac{n^2}{2}}x^{\frac{n}{2}}y^n$$

$$\frac{y}{y+1}\prod_{n=1}^{\infty}(1-x^n)(1+x^ny)(1+\frac{x^{n-1}}{y}) = \frac{y}{y+1}\sum_{n=-\infty}^{\infty}x^{\frac{n(n+1)}{2}}y^n \qquad (1.10)$$

όπου

$$\frac{y}{y+1}\prod_{n=1}^{\infty}(1+\frac{x^{n-1}}{y}) = \frac{y}{y+1}(1+\frac{x^0}{y})(1+\frac{x^1}{y})(1+\frac{x^2}{y})... =$$

$$= \frac{y}{y+1}(1+\tfrac{1}{y})(1+\tfrac{x}{y})(1+\tfrac{x^2}{y})... =$$

$$= \frac{y}{y+1}\frac{y+1}{y}(1+\frac{x}{y})(1+\frac{x^2}{y})... = (1+\tfrac{x}{y})(1+\tfrac{x^2}{y})...$$

Άρα η 1.11 γίνεται

$$\prod_{n=1}^{\infty}(1-x^n)(1+x^n y)(1+\frac{x^n}{y}) = \frac{y}{y+1}\sum_{n=-\infty}^{\infty}x^{\frac{n(n+1)}{2}}y^n$$

Αν

$$T(y) := \frac{y}{y+1}\sum_{n=-\infty}^{\infty}x^{\frac{n(n+1)}{2}}y^n$$

τότε

$$\lim_{y\to -1}T(y) = \lim_{y\to -1}\prod_{n=1}^{\infty}(1-x^n)(1+x^n y)(1+\frac{x^n}{y}) =$$

$$= \prod_{n=1}^{\infty}(1-x^n)(1-x^n)(1-x^n) = \prod_{n=1}^{\infty}(1-x^n)^3$$

Επιπλέον,

$$\sum_{n=-\infty}^{\infty}x^{\frac{n(n+1)}{2}}(-1)^n = [\sum_{n=0}^{\infty}+\sum_{n=-1}^{-\infty}](-1)^n x^{\frac{n(n+1)}{2}}$$

$$= 1 - x + x^3 - ... - 1 + x - x^3 + ... = 0$$

Έτσι,

$$T(y) = \frac{y}{y+1}\sum_{n=-\infty}^{\infty}x^{\frac{n(n+1)}{2}}y^n$$

$$= \frac{y}{y+1}\sum_{n=-\infty}^{\infty}x^{\frac{n(n+1)}{2}}y^n - \frac{y}{y+1}\sum_{n=-\infty}^{\infty}x^{\frac{n(n+1)}{2}}(-1)^n =$$

$$= \frac{y}{y+1}\sum_{n=-\infty}^{\infty}x^{\frac{n(n+1)}{2}}[y^n-(-1)^n] =$$

$$= \sum_{n=-\infty}^{\infty} x^{\frac{n(n+1)}{2}} \frac{y(y^n - (-1)^n)}{y+1}$$

και

$$\frac{y(y^n - (-1)^n)}{y+1} = y\frac{y^n - (-1)^n}{y-(-1)} = y[y^{n-1} + y^{n-2}(-1) + ... + y(-1)^{n-2} + (-1)^{n-1}]$$

Όταν $y \to -1$ έχουμε

$$(-1)[(-1)^{n-1} + (-1)^{n-1} + ... + (-1)^{n-1}] = (-1)(-1)^{n-1}n = (-1)^n n$$

Ως εκ τούτου, απο την ομοιόμορφη σύγκλιση, έχουμε

$$T(-1) = \lim_{y\to -1} \sum_{n=-\infty}^{\infty} x^{\frac{n(n+1)}{2}} y\frac{y^n - (-1)^n}{y+1}$$

$$= \sum_{n=-\infty}^{\infty} x^{\frac{n(n+1)}{2}} [\lim_{y\to -1} \frac{y(y^n - (-1)^n)}{y+1}]$$

$$= \sum_{n=-\infty}^{\infty} x^{\frac{n(n+1)}{2}} [(-1)^n n]$$

Όμως,

$$\lim_{y\to -1} T(y) = \prod_{n=1}^{\infty} (1 - x^n)^3$$

και ο $n-$οστός όρος στο άθροισμα είναι

$$(-1)^n n x^{\frac{n(n+1)}{2}}$$

Ενώ ο $(-n-1)$ όρος είναι

$$(-1)^{(-n-1)}(-n-1)x^{\frac{(-n-1)(-n)}{2}} = (-1)^{-(n+1)}(-(n+1))x^{\frac{(-(n+1)(-n)}{2}} =$$
$$(-1)^{n+1}(-1)(n+1)x^{\frac{(n)(n+1)}{2}}$$

Έτσι,

$$T(-1) = \sum_{n=-\infty}^{\infty} (-1)^n n x^{\frac{n(n+1)}{2}} = [\sum_{n=-1}^{-\infty} + \sum_{n=0}^{\infty}](-1)^n n x^{\frac{n(n+1)}{2}} =$$

$$= \sum_{n=0}^{\infty} (-1)^{-n-1}(-n-1)x^{\frac{(-n)(-n-1+1)}{2}} + \sum_{n=0}^{\infty} (-1)^n n x^{\frac{n(n+1)}{2}} =$$

$$= \sum_{n=0}^{\infty}(-1)^{n+2}(n+1)x^{\frac{n(n+1)}{2}} + \sum_{n=0}^{\infty}(-1)^{n}nx^{\frac{n(n+1)}{2}} =$$

$$= \sum_{n=0}^{\infty}(-1)^{n}(n+1)x^{\frac{n(n+1)}{2}} + \sum_{n=0}^{\infty}(-1)^{n}nx^{\frac{n(n+1)}{2}} = \sum_{n=0}^{\infty}(-1)^{n}(2n+1)x^{\frac{n(n+1)}{2}}$$

οπότε

$$\sum_{n=0}^{\infty}(-1)^{n}(2n+1)x^{\frac{n(n+1)}{2}} = \prod_{n=1}^{\infty}(1-x^n)^3$$

iii) Αν στην ταυτότητα του *Jacobi* αντικαταστήσουμε το x με $x^{\frac{1}{2}}$ και το z με $x^{\frac{1}{2}}$ προκύπτει:

$$\prod_{n=1}^{\infty}(1-x^{\frac{1}{2}2n})(1+x^{\frac{1}{2}(2n-1)}x^{\frac{1}{4}2})(1+\frac{x^{\frac{1}{2}(2n-1)}}{x^{\frac{1}{4}2}}) = \sum_{n=-\infty}^{\infty}x^{\frac{1}{2}n^2}x^{\frac{1}{4}2n}$$

$$\prod_{n=1}^{\infty}(1-x^{n})(1+x^{n-\frac{1}{2}+\frac{1}{2}})(1+x^{n-\frac{1}{2}-\frac{1}{2}}) = \sum_{n=-\infty}^{\infty}x^{\frac{n^2+n}{2}}$$

$$\prod_{n=1}^{\infty}(1-x^{n})(1+x^{n})(1+x^{n-1}) = \sum_{n=-\infty}^{\infty}x^{\frac{n(n+1)}{2}}$$

$$\prod_{n=1}^{\infty}(1-x^{2n})(1+x^{n-1}) = \sum_{n=-\infty}^{\infty}x^{\frac{n(n+1)}{2}}$$

Έπειτα ισχύει ο τύπος

$$\prod_{n=1}^{\infty}(1+x^n) = \frac{1}{2}\prod_{n=1}^{\infty}(1+x^{n-1})$$

αφού

$\prod_{n=1}^{\infty}(1+x^n) = (1+x^1)(1+x^2)(1+x^3)...$ και

$\frac{1}{2}\prod_{n=1}^{\infty}(1+x^{n-1}) = \frac{1}{2}(1+x^0)(1+x^1)(1+x^2)...$

$$= \tfrac{1}{2}2(1+x^1)(1+x^2)... = (1+x^1)(1+x^2)... = \prod_{n=1}^{\infty}(1+x^n)$$

Άρα

$$2\prod_{n=1}^{\infty}(1-x^{2n})(1+x^n) = \sum_{n=-\infty}^{\infty} x^{\frac{n(n+1)}{2}}$$

$$\prod_{n=1}^{\infty}(1-x^{2n})(1+x^n) = \frac{1}{2}\sum_{n=-\infty}^{\infty} x^{\frac{n(n+1)}{2}} = \frac{1}{2}2\sum_{n=0}^{\infty} x^{\frac{n(n+1)}{2}} = \sum_{n=0}^{\infty} x^{\frac{n(n+1)}{2}}$$

Παραπάνω χρησιμοποιήσαμε τη σχέση

$$\sum_{n=-\infty}^{\infty} x^{\frac{n(n+1)}{2}} = 2\sum_{n=0}^{\infty} x^{\frac{n(n+1)}{2}}$$

αφού

$$\sum_{n=-\infty}^{\infty} x^{\frac{n(n+1)}{2}} = \sum_{n=-1}^{-\infty} x^{\frac{n(n+1)}{2}} + \sum_{n=0}^{\infty} x^{\frac{n(n+1)}{2}} = \sum_{n=0}^{\infty} x^{\frac{-(n+1)(-n)}{2}} + \sum_{n=0}^{\infty} x^{\frac{n(n+1)}{2}}$$

$$= 2\sum_{n=0}^{\infty} x^{\frac{n(n+1)}{2}}$$

και

$$\prod_{n=1}^{\infty}(1-x^{2n})(1+x^n) = (1-x^2)(1+x)(1-x^4)(1+x^2)(1-x^6)(1+x^3)(1-x^8)(1+x^4)...$$

$$= (1-x^2)(1-x^4)(1-x^6)(1-x^8)...(1+x)(1+x^2)(1+x^3)(1+x^4)...$$

$$= (1-x^2)(1-x^4)(1-x^6)(1-x^8)...\frac{1-x^2}{1-x}\frac{1-x^4}{1-x^2}\frac{1-x^6}{1-x^3}\frac{1-x^8}{1-x^4}$$

$$= \frac{(1-x^2)(1-x^4)(1-x^6)(1-x^8)...}{(1-x)(1-x^3)}.$$

□

1.6 Εκτιμήσεις για το $p(n)$

Αρκετοί τύποι τόσο ασυμπτωτικοί όσο και ακριβείς έχουν αναπτυχθεί για τη συνάρτηση διαμέρισης p. Αυτοί είναι αρκετά περίπλοκοι και απαιτούν μεθόδους πέρα από το πεδίο αυτής της εργασίας για την παραγωγή τους. Μια εκδοχή του ασυμπτωτικού τύπου είναι η ακόλουθη $p(n) \sim \dfrac{1}{4n\sqrt{3}} e^{\pi\sqrt{\frac{2n}{3}}}$ καθώς $n \to \infty$.Δείτε στο βιβλίο του $Andrews(1976)$ για τον ακριβή τύπο και στο βιβλίο του $Knopp(1970)$ για το ασυμπτωτικό ανάπτυγμα.
Χρησιμοποιώντας στοιχειώδεις μεθόδους, ένα εύλογο κάτω φράγμα και ένα καλό πάνω φράγμα μπορούν να βρεθούν για το $p(n)$. Θα αποδείξουμε το παρακάτω θεώρημα.

Θεώρημα 1.6.1. *Για κάθε $n > 1$ έχουμε* $2^{[\sqrt{n}]} < p(n) < e^{\pi\sqrt{\frac{2n}{3}}}$

Απόδειξη. Το κάτω φράγμα: Έστω $a_1, a_2, ..., a_r$ να είναι διαφορετικοί ακέραιοι τέτοιοι ώστε $1 \leq a_i \leq [\sqrt{n}]$ και τέτοιοι ώστε $r \leq [\sqrt{n}]$.
Επειδή

$$a_1 + a_2 + ... + a_r \leq 1 + 2 + ... + [\sqrt{n}] < [\sqrt{n}]^2 \leq n$$

έχουμε διαμέριση του n με $r + 1$ όρους
$n = a_1 + a_2 + ... + a_r + (n - a_1 - a_2 - .... - a_r)$.
Για σταθεροποιημένο r, ο αριθμός των διαμερίσεων αυτού του τύπου δίνεται από το διωνυμικό όρο $\binom{[\sqrt{n}]}{r}$
Ως εκ τούτου ο συνολικός αριθμός των διαμερίσεων αυτού του τύπου είναι

$$1 + \binom{[\sqrt{n}]}{1} + ... + \binom{[\sqrt{n}]}{r} + ... + \binom{[\sqrt{n}]}{[\sqrt{n}]} = (1+1)^{[\sqrt{n}]} = 2^{[\sqrt{n}]}$$

Άρα υπάρχει τουλάχιστον μια ακόμα διαμέριση, η οποία ίσως έχει επαναλαμβανόμενους όρους. Συνεπώς $2^{[\sqrt{n}]} < p(n)$.
Για το άνω φράγμα: Χρειαζόμαστε δύο λήμματα.

Λήμμα 1.6.1. *: Άν $0 < x < 1$ και $j > 1$ τότε* $\frac{1}{j}(\dfrac{x^j}{1-x^j}) < \dfrac{x}{j^2(1-x)}$

Για να το αποδείξουμε θα εφαρμόσουμε το θεώρημα μέσης τιμής για τη συνάρτηση y^j όταν $x \leq y \leq 1$ Έτσι, $\dfrac{1-x^j}{1-x} = jz^{j-1}$ για κάποιο z με $x < z < 1$. Αλλά $jz^{j-1} > jx^{j-1}$ και έτσι έχουμε

$$1 - x^j > jx^{j-1}(1-x)$$

αυτό ολοκληρώνει την απόδειξη του λήμματος.

Λήμμα 1.6.2. *: Άν* $0 < x < 1$ *τότε* $-\log(x) < \dfrac{1-x}{x}$

Για να το αποδείξουμε θα χρησιμοποιήσουμε ξανά το θεώρημα μεσης τιμής, αυτή τη φορά για τη συνάρτηση $\log(y)$ όταν

$$1 \leq y \leq \tfrac{1}{x}.$$

Έτσι για κάποιο t που ικανοποιεί την ανίσωση $1 < t < \frac{1}{x}$ έχουμε $-\log(x) = \log(\frac{1}{x}) - \log(1) = \frac{1}{t}(\frac{1}{x} - 1) < \dfrac{1-x}{x}$.

Επιστρέφουμε τώρα στη δημιουργία του άνω φράγματος του θεωρήματος.
Αν $0 < x < 1$ έχουμε

$$\log(\prod_{n=1}^{\infty} \frac{1}{1-x^n}) = -\sum_{n=1}^{\infty} \log(1-x^n) = \sum_{n=1}^{\infty}\sum_{j=1}^{\infty} \frac{x^{nj}}{j} =$$

$$= \sum_{j=1}^{\infty} \frac{1}{j} \sum_{n=1}^{\infty} x^{nj} = \sum_{j=1}^{\infty} \frac{x^j}{j(1-x^j)} < \frac{x}{1-x} \sum_{j=1}^{\infty} \frac{1}{j^2} = \frac{\pi^2 x}{6(1-x)}$$

από το πρώτο λήμμα. Χρησιμοποιώντας το θεώρημα του *Euler* έχουμε

$$p(n)x^n < \prod_{n=1}^{\infty} \frac{1}{1-x^n} \text{ άρα } p(n) < \frac{\prod_{n=1}^{\infty} \frac{1}{1-x^n}}{x^n} \text{ και έτσι}$$

$$\log(p(n)) \leq \log([\prod_{n=1}^{\infty} \frac{1}{1-x^n}) - n\log(x) < \frac{\pi^2 x}{6(1-x)} + \frac{n(1-x)}{x}$$

Αυτό ισχύει για όλα τα x που ικανοποιούν την ανίσωση $0 < x < 1$, έτσι μπορούμε να επιλέξουμε

$$x = \frac{\sqrt{6n}}{\pi + \sqrt{6n}}$$

και τότε οι δυο όροι στη δεξιά πλευρά της ανισότητας είναι ίσοι. Αυτό έχει ως συνέπεια $\dfrac{1-x}{x} = \dfrac{\pi}{\sqrt{6n}}$ και $\log(p(n)) < \pi\sqrt{\dfrac{2n}{3}}$
και έτσι προκύπτει το αποτέλεσμα. □

Θεώρημα 1.6.2. $p(5n+4) \equiv 0(\mathrm{mod} 5)$

Απόδειξη. Θα αρχίσουμε με κάποια σχόλια.
Υποθέτουμε ότι $f(x)$ και $g(x)$ είναι δυναμοσειρές του x, τότε $f(x) \equiv g(x)(\bmod m)$ αν και μόνο αν ο συντελεστής σε κάθε δύναμη του x στην f είναι ίσος με τον αντίστοιχο της $g(\bmod m)$.
Έπειτα, αν $\mid x \mid < 1$, ισχύουν

$$\sum_{n=0}^{\infty}(x^5)^n = \frac{1}{1-x^5} \text{ και } \sum_{n=0}^{\infty} x^n = \frac{1}{1-x}.$$

Παραγωγίζουμε διαδοχικά την τελευταία δυναμοσειρά οπότε προκύπτει:

$$\sum_{n=0}^{\infty}(n+1)x^n = \frac{1}{(1-x)^2}, \sum_{n=0}^{\infty}(n+1)(n+2)x^n = \frac{2}{(1-x)^3}$$

$$\sum_{n=0}^{\infty}(n+1)(n+2)(n+3)x^n = \frac{6}{(1-x)^4} \text{ και}$$

$$\sum_{n=0}^{\infty}(n+1)(n+2)(n+3)(n+4)x^n = \frac{24}{(1-x)^5}$$

Επομένως,

$$\sum_{n=0}^{\infty}\frac{(n+1)(n+2)(n+3)(n+4)}{24}x^n = \frac{1}{(1-x)^5}$$

Οι συντελεστές της δυναμοσειράς είναι

$$\frac{(n+1)(n+2)(n+3)(n+4)}{24} = \frac{(n+4)!}{n!4!} = \tbinom{n+4}{n} \in \mathbb{Z}.$$

Οι συντελεστές αυτοί διαιρούνται με 5, όταν ο αριθμητής διαιρείται με 5. Αν το 5 δεν διαιρεί το n, τότε $n \equiv 1, 2, 3, 4(\bmod 5)$, οπότε κάποιος από τους $n+1, n+2, n+3, n+4$ θα διαιρείται με 5, δηλαδή αν το 5 δεν διαιρεί το n τότε $\tbinom{n+4}{n} \equiv 0(\bmod 5)$. Όταν το 5 διαιρεί το n δηλαδή $n \equiv 0(\bmod 5)$ τότε

$$\frac{(n+1)(n+2)(n+3)(n+4)}{24} \equiv 1(\bmod 5)$$

Επομένως, $(\bmod 5)$ όλοι οι συντελεστές του x^n μηδενίζονται εκτός από τους συντελεστές των όρων x^{5m}.
Συνεπώς,

$$\sum_{n=0}^{\infty}\frac{(n+1)(n+2)(n+3)(n+4)}{24}x^n \equiv \sum_{m=0}^{\infty} 1 \cdot x^{5m} \equiv \frac{1}{1-x^5}(\bmod 5)$$

δηλαδή αποδείξαμε ότι $\frac{1}{(1-x)^5} \equiv \frac{1}{1-x^5}(\mathrm{mod}5)$
Από τα παραπάνω προκύπτει ότι, αν δείξουμε ότι οι συντελεστές του $x^{5m}, (m=1,2,...)$ στο απειρογινόμενο $x\prod_{n=1}^{\infty}(1-x^n)^4$ διαιρούνται με 5 θα έχουμε τελειώσει αφού

$$x+\sum_{n=2}^{\infty}p(n-1)x^n=\sum_{n=1}^{\infty}p(n-1)x^n=\sum_{n=0}^{\infty}p(n-1)x^n=$$

$$=x\sum_{n=0}^{\infty}p(n-1)x^{n-1}=x\prod_{n=1}^{\infty}\frac{1}{1-x^n}=$$

$$=x\frac{\prod_{n=1}^{\infty}(1-x^n)^4}{\prod_{n=1}^{\infty}(1-x^n)^5}=x\frac{\prod_{n=1}^{\infty}(1-x^n)^4}{\prod_{n=1}^{\infty}(1-x^{5n})}(\mathrm{mod}5)$$

Σημειώνουμε ότι εμφανίζονται μόνο οι όροι της μορφής x^{5n} όταν αναπτύξουμε τον παρονομαστή. Από το θεώρημα 1.4.3 και 1.5.2 (ii) έχουμε

$$\prod_{n=1}^{\infty}(1-x^n)=\sum_{m=-\infty}^{\infty}(-1)^m x^{\frac{m(3m-1)}{2}}$$

$$\prod_{n=1}^{\infty}(1-x^n)^3=\sum_{n=0}^{\infty}(-1)^n(2n+1)x^{\frac{n(n+1)}{2}}$$

Έτσι,

$$x\prod_{n=1}^{\infty}(1-x^n)^4=[x\prod_{n=1}^{\infty}(1-x^n)][\prod_{n=1}^{\infty}(1-x^n)^3]$$

$$=x[\sum_{m=-\infty}^{\infty}(-1)^m x^{\frac{m(3m-1)}{2}}][\sum_{n=0}^{\infty}(-1)^n(2n+1)x^{\frac{n(n+1)}{2}}]$$

$$=\sum_{m=-\infty}^{\infty}\sum_{n=0}^{\infty}[(-1)^{m+n}(2n+1)x^t]$$

όπου $t=1+\frac{m(3m-1)}{2}+\frac{n(n+1)}{2}$. Από τη σχέση, $8t=8+4m(3m-1)+4n(n+1)$ συνεπάγεται

$$12m^2 - 4m + 4n^2 + 4n + 8 = 8t,$$
$$\Rightarrow 2(m-1)^2 + (2n+1)^2 = 8t - 10m^2 - 5,$$
$$\Rightarrow 2(m-1)^2 + (2n+1)^2 \equiv 8t(\bmod 5),$$

Έτσι το $2(m-1)^2 \equiv 0, 2, 3(\bmod 5)$

Ομοίως, $(2n+1)^2 \equiv 0, \pm 1(\bmod 5) \equiv 0, 1, 4, (\bmod 5)$ Αν το 5 διαιρεί το t τότε

$$2(m-1)^2 + (2n+1)^2 \equiv 0(\bmod 5)$$

από το οποίο συνεπάγεται ότι $5 \mid (m-1)$ και $5 \mid (2n+1)$. Αυτό σημαίνει ότι ο συντελεστής του $x^{5k}, (t = 5k)$ διαιρείται με 5 αφού το $5 \mid (2n+1)$.
Επομένως, αποδείξαμε ότι οι συντελεστές των δυνάμεων x^{5m} του απειρογινομένου $x \prod_{n=1}^{\infty} (1 - x^n)^4$ διαιρούνται με 5, οπότε και $p(5n+4) \equiv 0(\bmod 5)$

□

Σημείωση: Η ισοτιμία

$$p(5n+4) \equiv 0(\bmod 5) \tag{1.11}$$

ανακαλύφθηκε από τον *Ramanujan*. Ο ίδιος ανακάλυψε και τις ισοτιμίες

$$p(7n+5) \equiv 0(\bmod 7) \tag{1.12}$$

και

$$p(11n+6) \equiv 0(\bmod 11) \tag{1.13}$$

και μάλιστα τις απέδειξε. Μάλιστα ο *Ramanujan* έκανε την ακόλουθη γενικότερη εικασία. Συγκεκριμένα, αν $\delta = 5^a 7^b 11^c$ και $24^n \equiv 1(\bmod \delta)$ τότε $p(n) \equiv 0(\bmod \delta)$.
Χωρίς απόδειξη διατύπωσε επίσης την ισχύ των ισοτιμιών

$$\sum_{m=0}^{\infty} p(5m+4)x^m = 5\frac{\varphi(x^5)^5}{\varphi(x)^6} \tag{1.14}$$

και

$$\sum_{m=0}^{\infty} p(7m+5)x^m = 7\frac{\varphi(x^7)^3}{\varphi(x)^4} + 49x\frac{\varphi(x^7)^7}{\varphi(x)^8} \tag{1.15}$$

όπου $\varphi(x) = \displaystyle\prod_{n=1}^{\infty} (1 - x^n)$. Επειδή οι συναρτήσεις των δεξιών μελών των παραπάνω σχέσεων είναι δυναμοσειρές με ακέραιους συντελεστές, οι αρχικές είναι άμεση συνέπεια των (1.14), (1.15). Οι αποδείξεις των (1.11), (1.12), (1.13) είναι δυνατές με τη χρήση της θεωρίας των *modular* συναρτήσεων, αλλά αυτό είναι εκτός των στόχων της παρούσας εργασίας. Ο ενδιαφερόμενος αναγνώστης παραπέμπεται στο άρθρο επισκόπησης [2]

Κεφάλαιο 2

Θεώρημα *Lagrange*

2.1 Στοιχειώδης απόδειξη

Το 3 γράφεται ως άθροισμα τριών τετραγώνων ($3 = 1^2 + 1^2 + 1^2$). Για το 7 χρειαζόμαστε τέσσερα τετράγωνα ($7 = 2^2 + 1^2 + 1^2 + 1^2$). Το ακόλουθο θεώρημα του *Lagrange* μας εξασφαλίζει ότι για κάθε φυσικό αριθμό αρκούν τέσσερα τέλεια τετράγωνα. Ο *Bachet* πίστευε ότι ο *Fermat* είχε μια απόδειξη την οποία όμως ποτέ δεν δημοσιοποίησε. Ο *Euler* δεν κατάφερε να το αποδείξει αλλά ο *Lagrange* το επέτυχε, γι΄ αυτό και λέγεται θεώρημα του *Lagrange*.

Θεώρημα 2.1.1. *Κάθε φυσικός γράφεται ως άθροισμα από το πολύ τέσσερα τετράγωνα ακεραίων αριθμών.*

Απόδειξη. Κατ΄ αρχήν παρατηρούμε ότι αν δύο φυσικοί αριθμοί γράφονται ως άθροισμα τεσσάρων τετραγώνων, τότε το ίδιο ισχύει και για το γινόμενο τους. Αυτό προκύπτει από τον ακόλουθο πολλαπλασιασμό πινάκων.

$$\begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} \begin{pmatrix} c & -\overline{d} \\ d & \overline{c} \end{pmatrix} = \begin{pmatrix} p & -\overline{s} \\ s & \overline{p} \end{pmatrix}$$

(όπου $p = ac - \overline{b}d$ και $s = bc + \overline{a}d$)
Παίρνουμε την ορίζουσα και των δυο μελών και έχουμε

$(\alpha\overline{a} + b\overline{b})(c\overline{c} + d\overline{d}) = p\overline{p} + s\overline{s}$ (2.1)

$$\Rightarrow (N(a) + N(b))(N(c) + N(d)) = N(p) + N(s)$$

Επομένως, αρκεί να παρατηρήσουμε ότι η *norm* κάθε μιγαδικού αριθμού $z = k + li$, γράφεται ως άθροισμα δυο τετραγώνων, $N(z) = k^2 + l^2$
Συνεπώς, από την (1) προκύπτει ότι το γινόμενο δυο φυσικών αριθμών οι οποίοι γράφονται ως άθροισμα τεσσάρων τετραγώνων μη-αρνητικών ακεραίων, γράφεται ως άθροισμα τεσσάρων τετραγώνων μη-αρνητικών ακεραίων.
Σύμφωνα με το θεμελιώδες θεώρημα της αριθμητικής, αρκεί να αποδείξουμε ότι κάθε πρώτος αριθμός γράφεται ως άθροισμα τεσσάρων τετραγώνων μη-αρνητικών ακεραίων.
Προφανώς, αυτό ισχύει για το 2, αφού

$$2 = 1^2 + 1^2 + 0^2 + 0^2$$

Έστω τώρα $p \in \mathbb{P}$, $p \neq 2$.
Άρα $p \equiv 1 \pmod 4$ ή $p \equiv 3 \pmod 4$.
Θα εξετάσουμε τις δυο περιπτώσεις ξεχωριστά.
Υποθέτουμε ότι $p \equiv 3 \pmod 4$. Έστω c ο ελάχιστος φυσικός ο οποίος είναι μη τετραγωνικό υπόλοιπο *modulo p*. Προφανώς υπάρχουν πάντοτε μη τετραγωνικά υπόλοιπα $\pmod p$ [1]. Επομένως όλοι οι προηγούμενοι είναι τετραγωνικά υπόλοιπα $\pmod p$.
Για το c ισχύει $2 \leq c \leq p - 1$ (αφού το 1 είναι πάντα τετραγωνικό υπόλοιπο).
Ισχύουν $(\frac{c-1}{p}) = 1$ και $(\frac{c}{p}) = -1$.
Υπολογίζουμε το

$$(\frac{-c}{p}) = (\frac{-1}{p})(\frac{c}{p}) = (-1)^{\frac{p-1}{2}}(\frac{c}{p}) = (-1)^{\frac{p-1}{2}}(-1) = 1$$

Άρα οι ισοδυναμίες

$$X^2 \equiv c - 1 \pmod p \text{ και } Y^2 \equiv -c \pmod p$$

έχουν λύση έστω $x, y \in \mathbb{Z}$ αντίστοιχα.
Επομένως, $x^2 + 1 - c \equiv 0 \pmod p$ και συνεπώς

$$x^2 + 1 + y^2 \equiv 0 \pmod p.$$

Μπορούμε να επιλέξουμε τα x, y έτσι ώστε

$$0 \leq x, y \leq \tfrac{p-1}{2}$$

Αυτό σημαίνει ότι υπάρχει φυσικός αριθμός h, $h < p$ τέτοιος ώστε η διοφαντική εξίσωση

$${x_1}^2 + {x_2}^2 + {x_3}^2 + {x_4}^2 = hp$$

να έχει μια τουλάχιστον λύση, την $x_1 = x, x_2 = 1, x_3 = y, x_4 = 0$. Έστω h ο ελάχιστος φυσικός τέτοιος ώστε η εξίσωση αυτή να έχει ακέραια λύση. Θα δείξουμε ότι $h = 1$.
Αν h άρτιος τότε το πλήθος των περιττών x_i είναι κατ' ανάγκη άρτιο. Χωρίς βλάβη της γενικότητας, αλλάζοντας αν χρειαστεί αρίθμηση, μπορούμε να υποθέσουμε ότι

$$x_1 \pm x_2 \text{ και } x_3 \pm x_4$$

είναι άρτιοι. Οπότε,

$$(\frac{x_1+x_2}{2})^2 + (\frac{x_1-x_2}{2})^2 + (\frac{x_3+x_4}{2})^2 + (\frac{x_3-x_4}{2})^2 = 2\frac{hp}{4} = \frac{h}{2}p$$

Άτοπο, λογω του ότι ο h είναι ο ελάχιστος με την ιδιότητα ότι η διοφαντική εξίσωση

$$x_1{}^2 + x_2{}^2 + x_3{}^2 + x_4{}^2 \equiv 0 \pmod p$$

έχει λύση. Επομένως, ο h είναι περιττός.
Έστω $h \geq 3$ και $y_i \in \mathbb{Z}$ τέτοιοι ώστε

$$y_i \equiv x_i \pmod h \text{ με } | y_i | \leq \frac{h-1}{2} \text{ για κάθε } i = 1,2,3,4$$

Προφανώς, $(y_1, y_2, y_3, y_4) \neq (0,0,0,0)$ διότι αλλιώς θα είχαμε $x_i \equiv 0 \pmod p$ για κάθε $i = 1,2,3,4$ οπότε και

$$x_1{}^2 + x_2{}^2 + x_3{}^2 + x_4{}^2 \equiv 0 \pmod{p^2}$$

δηλαδή $p^2 \mid hp$. Αυτό σημαίνει ότι $p \mid h$, δηλαδή ότι $h \geq p$ άτοπο αφού $h < p$. Ισχύει

$$(y_1, y_2, y_3, y_4) \neq (0,0,0,0)$$

και

$$y_i < \frac{h-1}{2}$$

Επομένως,

$$0 < y_1{}^2 + y_2{}^2 + y_3{}^2 + y_4{}^2 \leq 4(\frac{h-1}{2})^2 = (h-1)^2 < h^2 \tag{2.2}$$

Επειδή, $y_i \equiv x_i \pmod h$, έπεται ότι

$$y_1{}^2 + y_2{}^2 + y_3{}^2 + y_4{}^2 \equiv x_1{}^2 + x_2{}^2 + x_3{}^2 + x_4{}^2 = hp \equiv 0 \pmod h \tag{2.3}$$

Από τις σχέσεις 2.2 και 2.3 έπεται ότι

$$y_1{}^2 + y_2{}^2 + y_3{}^2 + y_4{}^2 = h'h < h^2$$

δηλαδή ότι $h' < h$.
Χρησιμοποιούμε τώρα την αρχική ταυτότητα, για

$$a = x_1 + x_2 i, b = x_3 + x_4 i, c = y_1 - y_2 i, d = -y_3 - y_4 i$$

$$r = (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4) + (-x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3)i$$

$$s = (-x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2) + (-x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1)i$$

Το πραγματικό και το φανταστικό μέρος των r και s διαιρούνται με h. Πράγματι, $x_iy_i \equiv {y_i}^2 (mod h)$ για κάθε $i = 1, 2, 3, 4$.
Επομένως,

$$r \equiv ({y_1}^2 + {y_2}^2 + {y_3}^2 + {y_4}^2) + (-y_1y_2 + y_2y_1 + y_3y_4 - y_4y_3)i$$

δηλαδή $Rer \equiv 0 \pmod h$ και $Imr \equiv 0 \pmod h$. Αυτό ισχύει και για το πραγματικό και το μιγαδικό μέρος του s. Αυτό σημαίνει ότι $h^2 \mid N(r)$ και $h^2 \mid N(s)$ δηλαδή ότι

$$h^2 \mid N(r) + N(s)$$

Οπότε

$$hp \cdot hh' = ({x_1}^2 + {x_2}^2 + {x_3}^2 + {x_4}^2)({y_1}^2 + {y_2}^2 + {y_3}^2 + {y_4}^2) = h^2({u_1}^2 + {u_2}^2 + {u_3}^2 + {u_4}^2)$$

Απλοποιούμε το h^2 και προκύπτει

$$h'p = {u_1}^2 + {u_2}^2 + {u_3}^2 + {u_4}^2$$

όπου $u_1, u_2, u_3, u_4 \in \mathbf{Z}$ και $h' < h$
Άτοπο αφού το h είναι το ελάχιστο ώστε το hp να γράφεται ως άθροισμα τεσσάρρων τετραγώνων, άρα $h = 1$. □

Στη συνέχεια θα εξετάσουμε την περίπτωση κατά την οποία ο πρώτος $p \equiv 1 \pmod 4$. Εδώ θα αποδείξουμε κάτι ισχυρότερο. Συγκεκριμένα θα αποδείξουμε

Πρόταση 2.1.1. *Κάθε πρώτος p, $p \equiv 1 \pmod 4$ γράφεται ως άθροισμα δυο τετραγώνων.*

Απόδειξη. Αν p $p \equiv 1 \pmod 4$ τότε

$$(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = 1$$

άρα η ισοδυναμία $X^2 \equiv -1 \pmod p$ έχει λύση.
Έστω $x_0 \pmod p$ μια λύση δηλαδή ${x_0}^2 \equiv -1 \pmod p$ (το $x_0 \neq 0 \pmod p$ αφού $0 \neq -1 \pmod p$ και το p δεν διαιρεί το x_0 οπότε $(p, x_0) = 1$). Άρα η ισοδυναμία $x_0 X = y \pmod p$ έχει πάντα μοναδική λύση για κάθε $y \in \mathbb{N}$.
Αν x_1 μια λύση της $x_0 X = y \pmod p$, τότε $x_0 \cdot x_1 \equiv y \pmod p$, επομένως από τη μια μεριά ισχύει

$$(x_0 x_1)^2 = {x_0}^2 {x_1}^2 = -{x_1}^2 \pmod p$$

και από την άλλη

$$(x_0 x_1)^2 \equiv {y_1}^2 \pmod p$$

άρα ${x_1}^2 + {y_1}^2 \equiv 0 \pmod p$

□

Θα αποδείξουμε ότι μπορούμε να κατασκευάσουμε τα

$$x_1, y_1 \in \mathbb{Z} \text{ ώστε } 0 < {x_1}^2 + {y_1}^2 < 2p.$$

Θεωρούμε όλους τους όρους της μορφής $x_0 x - y$ όπου $0 \leq x, y \leq [\sqrt{p}]$ το πλήθος τους είναι $([\sqrt{p}] + 1)^2$. Όμως, $([\sqrt{p}] + 1)^2 > p$ άρα υπάρχουν τουλάχιστον δυο αριθμοί της μορφής $x_0 x - y$ οι οποίοι είναι ισοδύναμοι $\pmod p$, δηλαδή

$$\exists x_1, y_1 \in \mathbf{Z} \text{ και } x_2, y_2 \in \mathbf{Z} \text{ με } (x_1, y_1) \neq (x_2, y_2)$$

τέτοια ώστε $x_0 x_1 - y_1 \equiv x_0 x_2 - y_2 \pmod p$.
Αν ονομάσουμε $x_3 := x_1 - x_2$ και $y_3 = y_1 - y_2$ τότε

$$x_0(x_1 - x_2) \equiv y_1 - y_2 (modp) \Rightarrow x_0 x_3 \equiv y_3 \pmod p$$

Θα αποδείξουμε ότι

$${x_3}^2 + {y_3}^2 \equiv 0 \pmod p \ (2.4)$$

Αφού $x_0 x_3 \equiv y_3 \pmod p$ και ${x_0}^2 \equiv -1 \pmod p$ και $0 <\mid x_3 \mid< \sqrt{p}$,$0 <\mid y_3 \mid< \sqrt{p}$ προκύπτει

$0 < {x_3}^2 < p$ και $0 < {y_3}^2 < p$, δηλαδή

$$0 < {x_3}^2 + {y_3}^2 < 2p \tag{2.5}$$

Συνεπώς απο τις 2.4 και 2.5 προκύπτει

$${x_3}^2 + {y_3}^2 = p \text{ και } p = {x_3}^2 + {y_3}^2 + 0^2 + 0^2$$

Παρατήρηση: Από την τελευταία πρόταση προκύπτει ότι κάθε πρώτος $p, p \equiv 1 \pmod 4$ γράφεται ως άθροισμα τεσσάρων τετραγώνων και συνεπώς ολοκληρώθηκε η απόδειξη του θεωρήματος του *Lagrange*.

2.2 Απόδειξη με χρήση του θεωρήματος του *Minkowski*

Θα δώσουμε μια διαφορετική απόδειξη του θεωρήματος του *Lagrange*, κάνοντας χρήση του θεωρήματος του *Minkowski*.

Το θεώρημα του *Minkowski* βεβαιώνει την ύπαρξη μέσα σε ένα κατάλληλο σύνολο X ενός μη μηδενικού σημείου ενός πλέγματος L, με την προϋπόθεση ότι ο όγκος του X είναι αρκετά μεγαλύτερος σε σχέση με εκείνον της θεμελιώδους περιοχής του L. Ο *Minkowski* ανακάλυψε ότι αυτή η παρατήρηση έχει πολλές μη τετριμμένες και σημαντικές συνέπειες και χρησιμοποιήθηκε ως βάση για την εκτεταμένη θεωρία της γεωμετρίας των αριθμών. Ως άμεση περίπτωση εφαρμογής θα αποδείξουμε τα θεωρήματα των δύο και των τεσσάρων τετραγώνων της κλασικής θεωρίας αριθμών.

Ορισμός 2.2.1. *Ένα υποσύνολο $X \subseteq \mathbb{R}^n$ λέγεται κυρτό όταν για οποιαδήποτε $x, y \in X$ όλα τα σημεία του ευθυγράμμου τμήματος που ενώνει το x με το y επίσης ανήκουν στο X.*

Με αλγεβρικούς όρους το X είναι κυρτό αν για $x, y \in X$ το σημείο $lx + (1-l)y \in X$ για όλα τα πραγματικά l με $0 \leq l \leq 1$
Για παράδειγμα ο κύκλος, η έλλειψη, το τετράγωνο και το τρίγωνο είναι κυρτά στο $\mathbb{R}^2$ ενώ ένα στεφάνι ή μια ημισέληνος δεν είναι.

Ορισμός 2.2.2. *Ένα υποσύνολο $X \subseteq \mathbb{R}^n$ λέγεται (κεντρικά) συμμετρικό όταν το $x \in X$ συνεπάγεται και το $-x \in X$.*

Ο κύκλος, το τετράγωνο, η έλλειψη και το στεφάνι είναι κεντρικά συμμετρικά ενώ το τρίγωνο και η ημισέλινος δεν είναι.
Θα αποδείξουμε τώρα το θεώρημα του *Minkowski*.

Θεώρημα 2.2.1. *Το θεώρημα του Minkowski Έστω L ένα $n-$διάστατο πλέγμα στον $\mathbb{R}^n$ με θεμελιώδη περιοχή T και έστω X ένα φραγμένο, κεντρικά συμμετρικό, κυρτό υποσύνολο του $\mathbb{R}^n$.*
Συμβολίζουμε $u(X)$ τον όγκο του X. Αν $u(X) > 2^n u(T)$ τότε το X περιέχει ένα μη μηδενικό σημείο του L.

Πρόταση 2.2.1. *Αν p είναι πρώτος και έχει τη μορφή $4k+1$ τότε ο p είναι το άθροισμα δύο ακεραίων τετραγώνων.*

Απόδειξη. Η πολλαπλασιαστική ομάδα G του σώματος $\mathbf{Z_p}$ είναι κυκλική και έχει τάξη $p-1=4k$. Επειδή το 4 διαιρεί την τάξη της ομάδας $G = \mathbf{Z_p}^*$, και Z_p είναι κυκλική. Έπεται ότι υπάρχει μοναδική υποομάδα τάξης 4, η οποία επίσης είναι κυκλική. Άρα

η $\mathbf{Z_p}$ περιέχει ένα στοιχείο u τάξης 4. Επομένως, το u^2 έχει τάξη δύο και $u^2 \equiv -1 \pmod p$ αφού το -1 είναι το μόνο στοιχείο τάξης 2 στην G.
Έστω τώρα,$L \subseteq \mathbb{R}^2$ το πλέγμα του $\mathbb{R}^2$ που περιέχει όλα τα ζευγάρια (a, b) με $a, b \in \mathbb{Z}$ τέτοια ώστε $b \equiv ua \pmod p$ δηλαδή

$$L = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid b \equiv ua(modp)\}$$

$$\text{όπου } u \in X \text{ με } u^2 \equiv -1 \pmod p$$

Θα δείξουμε ότι αυτή είναι υποομάδα του $\mathbb{Z}^2$ και έχει δείκτη p.
Έστω φ:$\mathbb{Z} \times \mathbb{Z} \to \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ η απεικόνιση

$$(a, b) \to (b - ua)modp$$

Η φ είναι προσθετικός ομομορφισμός ομάδων. Πράγματι,

φ$[(a_1, b_1) + (a_2, b_2)\ ]=$ φ$[(a_1 + a_2, b_1 + b_2)\ ]=$
$= [(b_1 + b_2) - u(a_1 + a_2)] \pmod p = [(b_1 - ua_1) + (b_2 - ua_2)] \pmod p$=
$= (b_1 - ua_1) \pmod p + (b_2 - ua_2) \pmod p =$ φ$[(a_1, b_1)]$ + φ$[(a_2, b_2)\ ]$.

Είναι επιμορφισμός ομάδων: Έστω $x \in \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ και b τυχαίο, $b \in \mathbf{Z}$ θεωρούμε την ισοτιμία $uy \equiv (x + b) \pmod p$ Το p δεν διαιρεί το u γιατί αν το p διαιρούσε το u τότε $u^2 \equiv 0 \pmod p$ ενώ

$$u^2 \equiv -1 \pmod p,$$

άτοπο. Συνεπώς, ο Μ.Κ.Δ.(p, u)=1, οπότε, η ισοτιμία έχει μοναδική λύση, δηλαδή $\exists a \in \mathbf{Z}$ τέτοιο ώστε

$$au \equiv x + b \pmod p \Rightarrow au - b \equiv x \pmod p$$

άρα

$$\exists (a, b) \in \mathbf{Z} \times \mathbf{Z} \text{ τέτοιο ώστε } x \equiv -b + au \pmod p$$

Ο πυρήνας της φ είναι:

$$ker\ \varphi = \{(a, b) \in Z \times Z \mid b - au \equiv 0 \pmod p\} = L$$

Συνεπώς από το πρώτο θεώρημα ισομορφισμών ομάδων προκύπτει ότι

$$\frac{\mathbb{Z} \times \mathbb{Z}}{L} \cong \frac{\mathbb{Z}}{p\mathbb{Z}}$$

άρα

$$[\mathbb{Z} \times \mathbb{Z} : L] = [\mathbb{Z} : p\mathbb{Z}] = p.$$

Έτσι ο όγκος μιας θεμελιώδους περιοχής της L είναι p, δηλαδή $u(T) = p$. Χρησιμοποιώντας το θεώρημα του *Minkowski*, για το παραπάνω L, αν για X πάρουμε ένα κατάλληλο κύκλο ώστε να ισχύει

$$u(X) > 2^n u(T)$$

δηλαδή $\pi r^2 > 4p$. Θεωρούμε ένα κύκλο κέντρου $(0,0)$, ακτίνας r και διαλέγουμε

$$r^2 = \tfrac{3p}{2}.$$

Τότε υπάρχει ένα μη μηδενικό σημείο $(a,b) \in L$ τέτοιο ώστε

$$0 \neq a^2 + b^2 \leq r^2 = \tfrac{3p}{2} < 2p$$

αλλά έχουμε

$$a^2 + b^2 \equiv a^2 + u^2 a^2 \equiv 0 \pmod p$$

Συνεπώς, $a^2 + b^2$ είναι πολλαπλάσιο του p, αυστηρά ανάμεσα στο μηδέν και στο $2p$, άρα αναγκαστικά είναι ίσο με p. □

Αναγόμενοι στο παραπάνω επιχείρημα οδηγούμαστε σέ ένα άλλο διάσημο θεώρημα, το θεώρημα του *Lagrange* για το άθροισμα των τεσσάρων τετραγώνων.

Θεώρημα 2.2.2. *(Το θεώρημα των τεσσάρων τετραγώνων) Κάθε θετικός ακέραιος γράφεται ως άθροισμα τεσσάρων μη αρνητικών ακεραίων τετραγώνων.*

Απόδειξη. Θα αποδείξουμε το θεώρημα για πρώτους p και θα το επεκτείνουμε σε όλους τους ακεραίους.
Το 2 γράφεται ως εξής :

$$2 = 1^2 + 1^2 + 0^2 + 0^2$$

Έστω τώρα p περιττός πρώτος.

Ισχυριζόμαστε ότι η ταυτότητα

$$u^2 + v^2 + 1 = 0 \pmod p$$

έχει μια λύση με $u, v \in \mathbf{Z}$.

Γι αυτή την επιλογή των u, v θεωρούμε το πλέγμα $L \subseteq \mathbf{Z}^4$ που αποτελείται από όλα τα (a,b,c,d) τέτοια ώστε

$$y \equiv ua + vb \pmod p \text{ και } d \equiv ub - va \pmod p.$$

Το L έχει δείκτη p^2 στο $\mathbf{Z}^4$. Έτσι ο όγκος της θεμελιώδους περιοχής είναι p^2. Τώρα μια τετραδιάστατη σφαίρα κέντρου την αρχή των αξόνων και ακτίνας r έχει όγκο $\frac{\pi^2 r^4}{2}$. Επιλέγουμε r ώστε να τον κάνουμε μεγαλύτερο από $16p^2$, έστω $r^2 = 1,9p$. Τότε υπάρχει μια τετράδα σημείων $0 \neq (a,b,c,d)$ σε αυτό το τεσσάρων διαστάσεων σχήμα ώστε

$$0 < a^2 + b^2 + c^2 + d^2 \leq r^2 = 1,9p < 2p$$

Πράγματι, και

$$a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod p$$

$$a^2 + b^2 + c^2 + d^2 \equiv a^2 + b^2 + (ua + vb)^2 + (ub - va)^2 \equiv$$
$$a^2 + b^2 + u^2a^2 + v^2b^2 + 2uvab + u^2b^2 + v^2a^2 - 2uvab$$
$$\equiv a^2(1 + u^2 + v^2) + b^2(1 + u^2 + v^2) \equiv 0 \pmod p$$

.
Ως εκ τούτου, όπως και στην προηγούμενη απόδειξη πρέπει να είναι ίσο με p.
Για να γράψουμε τώρα έναν αυθαίρετο ακέραιο ως άθροισμα τεσσάρων τετραγώνων, αρκεί να τον παραγοντοποιήσουμε σε πρώτους και να εφαρμόσουμε την ταυτότητα:

$$(a^2+b^2+c^2+d^2)(A^2+B^2+C^2+D^2) = (aA-bB-cC-dD)^2+(aB+bA+cD-dC)^2+$$

$$+(aC - bD + cA + dB)^2 + (aD + bC - cB + dA)^2$$

□

Κεφάλαιο 3

Απόδειξη του *Hilbert* της εικασίας *Waring*

3.1 Εισαγωγή

Έχουμε δει στο δεύτερο κεφάλαιο ότι κάθε φυσικός αριθμός παρίσταται ως άθροισμα τεσσάρων τετραγώνων. Την ίδια περίπου εποχή και συγκεκριμένα το 1770, ο $Waring$ διατύπωσε την εικασία ότι: Κάθε $n \in \mathbb{N}$ γράφεται ως άθροισμα το πολύ 9 κύβων ή 19 τέταρτων δυνάμεων και γενικότερα:
Εικασία του $Waring$: Για κάθε φυσικό αριθμό k υπάρχει ένας φυσικός $g(k)$ τέτοιος ώστε κάθε φυσικός αριθμός n γράφεται με το πολύ $g(k)$ προσθεταίους $k-$δυνάμεων.
Παράδειγμα: Από το θεώρημα του $Lagrange$ συνάγουμε ότι για $k = 2$ το $g(2) = 4$. Επομένως κάθε $n \in \mathbb{N}$ γράφεται ως άθροισμα 4 τετραγώνων. Η εικασία του $Waring$ για $k = 3$ ήταν $g(3) = 9$ και για $k = 4, g(4) = 19$.
Το βασικό θέμα του παρόντος κεφαλαίου είναι η εύρεση ενός άνω φράγματος της συνάρτησης $g(k)$. Σε πρώτο βήμα όμως θα δώσουμε ένα κάτω φράγμα της συνάρτησης αυτής.

Πρόταση 3.1.1. *Για* $k \geqslant 2$ *ισχύει*

$$g(k) \geq 2^k + [(\frac{3}{2})^k] - 2$$

Για παράδειγμα όταν $k = 2$, $g(2) \geq 2^2 + [(\frac{3}{2})^2] - 2 = 4$

Απόδειξη. Θέλουμε να δείξουμε ότι ο φυσικός αριθμός

$$n = 2^k[(\frac{3}{2})^k] - 1$$

γράφεται ως άθροισμα $k-$δυνάμεων.(Χρειαζόμαστε τουλάχιστον $2^k + [(\frac{3}{2})^k] - 2$ προσθεταίους)
Επειδή $n < 3^k$ εμφανίζονται μόνο τα 1^k και 2^k. Έστω ότι χρειαζόμαστε a προσθεταίους της μορφής 2^k και b προσθεταίους της μορφής 1^k όπου $b < 2^k$ τότε

$$n = a \cdot 2^k + b \cdot 1^k$$

Συνεπώς,

$$g(k) \geq a + b = a + (n - a \cdot 2^k) = n - a(2^k - 1)$$
$$\text{Το } a < [(\tfrac{3}{2})^k] \text{ άρα } a \leq [(\tfrac{3}{2})^k] - 1$$

$$g(k) \geq n - ([(\tfrac{3}{2})^k] - 1)(2^k - 1) = n - [(\tfrac{3}{2})^k] \cdot 2^k + 2^k + [(\tfrac{3}{2})^k] - 1 =$$
$$2^k + n - [(\tfrac{3}{2})^k] \cdot 2^k + [(\tfrac{3}{2})^k] - 1$$

$$= [(\tfrac{3}{2})^k] - 1 + 2^k - 1 = 2^k + [(\tfrac{3}{2})^k] - 2$$

□

Θεώρημα 3.1.1. *$g(k) < \infty$ για κάθε σταθερό φυσικό αριθμό κ.*

Η απόδειξη του θεωρήματος αυτού οφείλεται στον *Hilbert* [11]. Η απόδειξη του ήταν πολύ πολύπλοκη στα αναλυτικά του επιχειρήματα. Λίγο αργότερα, μέρος της απόδειξης δόθηκε από τον *E.Schmidt* [23] .Ο *Schmidt* χρησιμοποίησε τη θεωρία των κυρτών συνόλων. Το θεώρημα του *Schmidt* δεν θα αποδειχθεί στην παρούσα εργασία. Για το δεύτερο μέρος του θεωρήματος θα χρησιμοποιήσουμε το βιβλίο του *Pollack* [18]. Η απόδειξη στηρίζεται σε μια τροποποίηση του *Dress* [5], [6] της απόδειξης του *Hilbert*. Σύμφωνα με το θεώρημα του *Lagrange* κάθε φυσικός αριθμός παρίσταται ως άθροισμα τεσσάρων τετραγώνων. Επειδή οι αριθμοί της μορφής $4^m(8k+7)$, $m \geq 0$ και $k \geq 0$ δεν είναι δυνατόν να παρασταθούν ως άθροισμα τριών τετραγώνων μη αρνητικών αριθμών, έπεται ότι $g(2) = 4$.
Είναι φανερό ότι ο αριθμός 23 χρειάζεται 9 κύβους για να γραφεί ως άθροισμα κύβων. Έπεται ότι $g(3) \geq 9$. Επίσης, επειδή ο αριθμός 79 χρειάζεται 19 δυνάμεις στην τετάρτη έπεται ότι $g(4) \geq 19$. Η εικασία του *Waring* ήταν ότι $g(3) = 9$ καθώς και ότι $g(4) = 19$. Σχετικά με διάφορα επιπλέον ιστορικά στοιχεία και πρόσφατα σχετικά αποτελέσματα θα αναφερθούμε στο τέλος του κεφαλαίου.

3.2 Βοηθητικές προτάσεις

Κατ΄ αρχήν θα χρησιμοποιήσουμε το ακόλουθο

Θεώρημα 3.2.1. *(Ταυτότητα του Hilbert) Έστω $k \in \mathbf{N}$ και $N := \binom{2k+4}{4}$. Υπάρχει μια τυπική ταυτότητα με ανεξάρτητες μεταβλητές $X_1, X_2, ..., X_5$ της μορφής*

$$M \cdot ({X_1}^2 + ... + {X_5}^2)^k = \sum_{i=0}^{N} m_i(a_{i1}X_1 + ... + a_{i5}X_5)^{2k} + m_{N+1}{X_5}^{2k} \tag{3.1}$$

όπου M και m_{N+1} είναι θετικοί ακέραιοι, τα $m_i, (0 \leq i \leq N)$ είναι μη αρνητικοί ακέραιοι και τα $a_{ij}, 0 \leq i \leq N, 0 \leq j \leq 5$, είναι ακέραιοι.

Το θεώρημα αυτό αποδείχθηκε, όπως είπαμε και παραπάνω από τον $E.Schmidt$[23] ο οποίος χρησιμοποίησε τη θεωρία της κυρτότητας. Το θεώρημα αυτό δεν αποδεικνύεται στην παρούσα εργασία. Το παραπάνω θεώρημα έχει την ακόλουθη σημαντική συνέπεια.

Θεώρημα 3.2.2. *Σταθεροποιούμε ένα φυσικό αριθμό k όπως στην ταυτότητα του Hilbert, τότε με M όπως στην 3.1 μπορούμε να βρούμε ένα φυσικό αριθμό Q με την ακόλουθη ιδιότητα:*

Για κάθε μη αρνητικό ακέραιο l και κάθε ακέραιο x με $\mid x \mid \leq \sqrt{l}$ να ισχύει

$$Ml^k = x^{2k} + \sum_{h=1}^{Q} {u_h}^{2k}$$

για κάποιους κατάλληλα επιλεγμένους ακέραιους $u_1, u_2, ..., u_Q$

Απόδειξη. Αν $\mid x \mid \leq \sqrt{l}$ τότε

$$x^2 \leq l \Rightarrow l - x^2 \geq 0$$

Οπότε απο το θεώρημα του $Lagrange$ για το άθροισμα τεσσάρων τετραγώνων έπεται ότι υπάρχουν

$$x_1, x_2, x_3, x_4 \in \mathbf{Z},$$

έτσι ώστε να ισχύει

$$l - x^2 = {x_1}^2 + {x_2}^2 + {x_3}^2 + {x_4}^2$$

Θέτουμε $x := x_5$ οπότε $l = {x_1}^2 + {x_2}^2 + {x_3}^2 + {x_4}^2 + {x_5}^2$
Οπότε η 3.1 για $X_i = x_i$, $1 \leq i \leq 5$ γράφεται

$$M \cdot ({x_1}^2 + ... + {x_5}^2)^k = \sum_{i=0}^{N} m_i(a_{i1}x_1 + ... + a_{i5}x_5)^{2k} + m_{N+1}{x_5}^{2k}$$

Η σχέση αυτή γράφεται

$$M{\cdot}l^k = \sum_{i=0}^{N}[(a_{i1}x_1 + ... + a_{i5}x_5)^{2k}+...+(a_{i1}x_1 + ... + a_{i5}x_5)^{2k}]+{x_5}^{2k}+({x_5}^{2k}+...+{x_5}^{2k})$$

Το πλήθος των προσθεταίων της μορφής $(a_{i1}x_1 + ... + a_{i5}x_5)^{2k}$ είναι το m_i ενώ το πλήθος των προσθεταίων της μορφής ${x_5}^{2k}$ είναι $(m_{N+1} - 1)$.
Συνεπώς το Ml^k γράφεται στη μορφή $Ml^k = {x_5}^{2k} + \sum_{h=1}^{Q} {u_h}^{2k}$,
όπου $Q := m_{N+1} - 1 + \sum_{i=0}^{N} m_i$ □

Το επόμενο λήμμα εγγυάται την ύπαρξη μιας άλλης οικογένειας πολυωνυμικών ταυτοτήτων . Οι ταυτότητες αυτές ήταν γνωστές από καιρό αλλά πρώτη φορά χρησιμοποιήθηκαν από τον *Dress* στην απόδειξη του θεωρήματος 3.1.1.

Λήμμα 3.2.1. *Για κάθε φυσικό αριθμό k υπάρχει μια ταυτότητα μιας μεταβλητής, έστω T, της μορφής*

$$\sum_{i=1}^{R}(T+a_i)^{2k} - \sum_{j=1}^{R}(T+{a_j}')^{2k} = AT + B$$

όπου R και A είναι φυσικοί αριθμοί και $B, a_1, ..., a_R, {a_1}', ..., {a_R}'$ είναι ακέραιοι. Μάλιστα μπορούμε να επιλέξουμε $R = 2^{2k-2}$ και $A = (2k)!$.

Απόδειξη. Θεωρούμε τον διαφορικό τελεστή $\Delta : \mathbb{Z}[T] \to \mathbb{Z}[T]$ που ορίζεται από τη σχέση $(\Delta F)(T) = F(T+1) - F(T)$
Πρώτα απ όλα, αν $a_n T^n$ είναι ο όρος μεγαλύτερης δύναμης του Τ στο πολυώνυμο $F(T)$ όπου $n > 0$, τότε ο όρος της μεγαλύτερης δύναμης του $(\Delta F)(T)$ είναι na_nT^{n-1} διότι
$F(T) = a_nT^n + a_{n-1}T^{n-1}+$ όροι βαθμού μικρότερου του $(n-1)$
$F(T+1) = a_n(T+1)^n + a_{n-1}(T+1)^{n-1}+$ όροι βαθμού μικρότερου του $(n-1) =$
$= a_nT^n + na_nT^{n-1} + a_{n-1}(T^{n-1}+$ όροι βαθμού μικρότερου του $(n-1) =$
$= a_nT^n + na_nT^{n-1} + a_{n-1}T^{n-1}+$ όροι βαθμού μικρότερου του $(n-1)$
Επομένως, $F(T+1) - F(T) = na_nT^{n-1}+$ όροι με βαθμό μικρότερο από $(n-1)$.
Με Δ^r συμβολίζουμε τη σύνθεση $\Delta \circ \Delta \circ ... \circ$ (r φορές)
Έτσι, για κάθε φυσικό αριθμό r και $F(T) \in \mathbb{Z}[T]$ ισχύει

$$(\Delta^r F)(T) = \sum_{j=0}^{r}\binom{r}{j}(-1)^{r-j}F(T+j) \tag{3.2}$$

Πράγματι, για $r = 1$ ισχύει

$$(\Delta F)(T) = \sum_{j=0}^{1} \binom{r}{j} (-1)^{r-j} F(T+j) =$$

$$= \tbinom{1}{0}(-1)^{1-0}F(T+0) + \tbinom{1}{1}(-1)^{1-1}F(T+1) = F(T+1) - F(T).$$

Υποθέτουμε ότι ισχύει για r και θα αποδείξουμε ότι ισχύει και για $(r+1)$.

$$\begin{aligned}(\Delta^{r+1}F)(T) &= \Delta[(\Delta^r F)(T)] = (\Delta^r F)(T+1) - (\Delta^r F)(T) = \\ =&\sum_{j=0}^{r} \binom{r}{j}(-1)^{r-j}F(T+1+j) - \sum_{j=0}^{r}\binom{r}{j}(-1)^{r-j}F(T+j) = \\ &= \sum_{j=0}^{r}\binom{r}{j}(-1)^{r-j}F(T+(j+1)) - \sum_{j=0}^{r}\binom{r}{j}(-1)^{r-j}F(T+j)\end{aligned}$$

αλλά το άθροισμα

$$\sum_{k=0}^{r}\binom{r}{k}(-1)^{r-k}F(T+(k+1)) = \sum_{j=1}^{r+1}\binom{r}{j-1}(-1)^{r-(j-1)}F(T+j) \text{ για } j := k+1$$

Επομένως,

$$(\Delta^{r+1}F)(T) = \sum_{j=1}^{r+1}\binom{r}{j-1}(-1)^{r-(j-1)}F(T+j) - \sum_{j=0}^{r}\binom{r}{j}(-1)^{r-j}F(T+j) =$$

$$= \tbinom{r}{r}(-1)^{r-r}F(T+r+1) + \sum_{j=1}^{r}\binom{r}{j-1}(-1)^{r-(j-1)}F(T+j) -$$
$$\sum_{j=1}^{r}\binom{r}{j}(-1)^{r-j}F(T+j) - \binom{r}{0}(-1)^{r-0}F(T+0)$$

$$= \tbinom{r+1}{r+1}(-1)^{r-r}F(T+(r+1)) + \sum_{j=1}^{r}[\binom{r}{j-1} + \binom{r}{j}](-1)^{r-(j-1)}F(T+j) -$$
$$\binom{r}{0}(-1)^{r-0}F(T+0)$$

(Ως γνωστό $\binom{r}{j-1} + \binom{r}{j} = \binom{r+1}{j}$)

$$= \tbinom{r+1}{r+1}(-1)^{(r+1)-(r+1)}F(T+(r+1)) + \sum_{j=1}^{r}\binom{r+1}{j}(-1)^{r+1-j}F(T+j) +$$
$$\binom{r+1}{0}(-1)^{(r+1)-0}F(T+0) =$$

$$= \sum_{j=0}^{r+1} \binom{r+1}{j} (-1)^{r+1-j} F(T+j),$$

δηλαδή ισχύει και για $r+1$. Συνεπώς ισχύει για κάθε r.
Τώρα παίρνουμε $F(T) = T^{2k}$ έτσι

$$\Delta F(T) = F(T+1) - F(T) = (T+1)^{2k} - T^{2k} = 2k \cdot 1 \cdot T^{2k-1} + \text{ όροι βαθμού μικρότερου του } (2k-1)$$

$$\Delta^2(F(T)) = \Delta(\Delta(F(T))) = (T+2)^{2k} - (T+1)^{2k} - (T+1)^{2k} + T^{2k} = (2k-1)2kT^{2k-2} + \text{ όροι βαθμού μικρότερου του } (2k-1)$$

$$\Delta^3(F(T)) = (2k-2)(2k-1)2kT^{2k-3} + ...$$

και συνεχίζοντας επαγωγικά
$\Delta^{(2k-1)}(F(T)) = 2 \cdot 3 \cdot ... \cdot (2k-2)(2k-1)2kT^{2k-(2k-1)} + ... = (2k)!T + B$, για κάποιο ακέραιο B.

Εφαρμόζουμε τώρα την ιδιότητα 3.2 με $r = 2k-1$ και έχουμε

$$(2k!)T + B = (\Delta^{2k-1})(F(T)) = \sum_{j=0}^{2k-1} \binom{2k-1}{j} (-1)^{2k-1-j} F(T+j) =$$

$$= \sum_{j=0,2\nmid j}^{2k-1} \binom{2k-1}{j} (+1) F(T+j) + \sum_{j=0,2|j}^{2k-1} \binom{2k-1}{j} (-1) F(T+j) =$$

$$= \sum_{j=0,2\nmid j}^{2k-1} \binom{2k-1}{j} (T+j)^{2k} - \sum_{j=0,2|j}^{2k-1} \binom{2k-1}{j} (T+j)^{2k} \tag{3.3}$$

Στη συνέχεια χρησιμοποιούμε τη γνωστή ταυτότητα

$$\sum_{j=0,2|j}^{m} \binom{m}{j} = \sum_{j=0,2\nmid j}^{m} \binom{m}{j}$$

Απόδειξη της ταυτότητας:

$$(1-1)^m = \sum_{j=0}^{m} \binom{m}{j} 1^j (-1)^{m-j}$$

Αν m άρτιος:

$$0 = \sum_{j=0,2|j}^{m} \binom{m}{j} \cdot 1 + \sum_{j=0,2\nmid j}^{m} \binom{m}{j} (-1)$$

$$\Rightarrow \sum_{j=0,2\nmid j}^{m} \binom{m}{j} = \sum_{j=0,2\mid j}^{m} \binom{m}{j}$$

Ομοίως αποδεικνύεται όταν ο m είναι περιττός.
Συνεπώς,

$$\sum_{j=0,2\nmid j}^{2k-1} \binom{2k-1}{j} = \sum_{j=0,2\mid j}^{2k-1} \binom{2k-1}{j} = \frac{1}{2}\sum_{j=0}^{2k-1} \binom{2k-1}{j} = 2^{2k-2} \tag{3.4}$$

αφού

$$\sum_{j=0}^{2k-1} \binom{2k-1}{j} = (1+1)^{2k-1} = 2^{2k-1}$$

Οπότε $A = (2k)!$.
Έχουμε ήδη αποδείξει ότι το $A = (2k!)$. Στη συνέχεια θα αποδείξουμε ότι $R = 2^{2k-2}$.
Από την 3.4 έχουμε

$$\sum_{0\le j\le 2k-1, 2\nmid j} \binom{2k-1}{j} = 2^{2k-2}$$

Εμείς έχουμε,

$$\sum_{0\le j\le 2k-1, 2\nmid j} \binom{2k-1}{j} (T+j)^{2k}$$

$= \binom{2k-1}{1}(T+1)^{2k} + \binom{2k-1}{3}(T+3)^{2k} + ... + \binom{2k-1}{2k-1}(T+2k-1)^{2k} =$

$= (T+1)^{2k} + ... + (T+1)^{2k} \quad , \binom{2k-1}{1}$- φορές
$+(T+3)^{2k} + ... + (T+3)^{2k} \quad , \binom{2k-1}{3}$- φορές

.
.
.
$+(T+2k-1)^{2k} \quad \binom{2k-1}{2k-1}$- φορές

$= \sum_{j=1}^{2^{2k-2}} (T+a_i)^{2k}$, δηλαδή $R = 2^{2k-2}$
Ομοίως για j άρτιο. □

Το επόμενο λήμμα αναφέρεται στο πόσο καλά μπορεί να προσεγγιστεί ένας μη-αρνητικός πραγματικός αριθμός από ένα άθροισμα κ-οστών δυνάμεων μη αρνητικών ακεραίων.
Ο συμβολισμός $A \ll B$ σημαίνει $\mid A \mid \le c \mid B \mid$ για κάποια σταθερά $c \in \mathbb{R}$

Λήμμα 3.2.2. : *Έστω κ ένας φυσικός αριθμός και* $v = \dfrac{k-1}{k}$, *τότε για κάθε* $x \geqslant 0$ *ισχύει*

$$0 \leqslant x - [x^{\frac{1}{k}}]^k \leqslant kx^v$$

Συνεπώς, για κάθε $x \geqslant 0$ *και* $t \in \mathbb{N}$, *υπάρχουν μη αρνητικοί ακέραιοι* $z_1, ..., z_t$ *ώστε*

$$x - {z_1}^k - {z_2}^k - ... - {z_t}^k \ll_{k,t} x^{v^t}$$

Απόδειξη. Εφαρμόζοντας το θεώρημα μέσης τιμής στο διάστημα $[[x^{\frac{1}{k}}], x^{\frac{1}{k}}]$ για τη συνάρτηση $f(x) = x^k$ βρίσκουμε ότι

$$\exists x_0 \in ([x^{\frac{1}{k}}], x^{\frac{1}{k}})$$

ώστε

$$\frac{(x^{\frac{1}{k}})^k - [x^{\frac{1}{k}}]^k}{x^{\frac{1}{k}} - [x^{\frac{1}{k}}]} = \frac{d}{dx}(x^k) \mid_{x=x_0}$$

Έτσι,

$$0 < x - [x^{\frac{1}{k}}] \leq \frac{x - [x^{\frac{1}{k}}]^k}{x^{\frac{1}{k}} - [x^{\frac{1}{k}}]} = k(x_0)^{k-1} \leqslant k(x^{\frac{1}{k}})^{k-1} = kx^v$$

Έστω

$$z_1 = [x^{\frac{1}{k}}] \in \mathbb{Z} \Rightarrow x_1 := x - {z_1}^k \geqslant 0$$

Εφαρμόζουμε τον πρώτο τύπο για το x_1 και συνεχίζουμε επαγωγικά

$$r \ll x_1 - [x_1^{\frac{1}{k}}]^k \leq k{x_1}^v = k(x - {z_1}^k)^v \leq k(kx^v)^v \leq k^2 x^{v^2} \ll_{k,t} x^{v_t}$$

□

3.3 Απόδειξη της εικασίας *Waring*

Απόδειξη. Σταθεροποιούμε ένα $k \in \mathbb{N}$. Υπενθυμίζουμε ότι $g(k, m)$ είναι ο ελάχιστος φυσικός αριθμός μη αρνητικών $k-$δυνάμεων που χρειάζεται για να παρασταθεί ο m. Θέλουμε να δείξουμε ότι ο $g(k, m)$ είναι φραγμένος και ανεξάρτητος από το m. Είναι αρκετό να το αποδείξουμε για όλα τα μεγάλα m.
Σταθεροποιούμε ένα R όπως στο λήμμα 3.2.1 και ένα M όπως στα θεωρήματα 3.2.1 και 3.2.2. Υπενθυμίζουμε ότι τα M και R εξαρτώνται αποκλειστικά από το k.
Έστω m ένας (αρκετά) μεγάλος φυσικός αριθμός, τον οποίο πρόκειται να γράψουμε αργότερα ως άθροισμα μη-αρνητικών $k-$δυνάμεων και l^k η πιο μεγάλη $k-$οστή δύναμη

τέτοια ώστε $l^k \leq \dfrac{m}{RM}$. Άρα l είναι ο πιο μεγάλος ακέραιος τέτοιος ώστε $l \leq (\dfrac{m}{RM})^{\frac{1}{k}}$
άρα $l = [(\frac{m}{RM})^{\frac{1}{k}}]$.
Για αρκετά μεγάλο m ισχύει

$$\frac{1}{2}(\frac{m}{RM})^{\frac{1}{k}} \leq l \leq (\frac{m}{RM})^{\frac{1}{k}} \tag{3.5}$$

Θεωρούμε $m > 2^k RM$ τότε ισχύει η ανισότητα $\frac{1}{2}(\frac{m}{RM})^{\frac{1}{k}} \leq (\frac{m}{RM})^{\frac{1}{k}} - 1$

Επειδή τώρα $m > RM$ προκύπτει ότι

$$\tfrac{1}{2}(\tfrac{m}{RM})^{\frac{1}{k}} \leq l \leq (\tfrac{m}{RM})^{\frac{1}{k}}$$

Επιπλέον, απο το λήμμα 3.2.2 αν θέσουμε $x := \frac{m}{RM}$, έχουμε

$$x = \frac{m}{RM} = l^k + \tfrac{r_1}{RM} \Rightarrow m = RMl^k + r_1$$

και

$$0 \leq \tfrac{m}{RM} - [\tfrac{m}{RM}^{\frac{1}{k}}]^k \leq k(\tfrac{m}{RM})^{\frac{k-1}{k}}$$

Θέτουμε

$$r := (\tfrac{m}{RM}) - [\tfrac{m}{RM}^{\frac{1}{k}}]^k = (\tfrac{m}{RM}) - l^k \Rightarrow m - RMl^k = rRM = r_1$$

Οπότε

$$0 \leq r \leq k(\tfrac{m}{RM})^{\frac{k-1}{k}} \Rightarrow 0 \leq rRM \leq kRM(\tfrac{m}{RM})^{\frac{k-1}{k}} \Rightarrow 0 \leq r_1 \leq kRM(\tfrac{m}{RM})^{\frac{k-1}{k}}$$

Έστω $v = \frac{k-1}{k}$ και t ο ελάχιστος φυσικός αριθμός τέτοιο ώστε $v^t < \dfrac{1}{2k}$ τότε

$$\lim_{k \to +\infty} \frac{1}{2k} = 0$$

άρα

$$v^t \to 0$$

οπότε η ακολουθία u^t φθίνει. Από το λήμμα 3.2.2 με $x = r_1$ έχουμε

$$r_1 - {z_1}^k - {z_2}^k - ... - {z_t}^k = r_t,$$

δηλαδή με z_i μη αρνητικούς ακεραίους

$$r_1 = {z_1}^k + {z_2}^k + ... + {z_{t-1}}^k + r_t$$

όπου

$$r_t \ll_{k,t} {r_1}^{v^{t-1}} \tag{3.6}$$

Από τη σχέση $r_1 \leq kRM\dfrac{m^v}{(RM)^v} = c_1 m^v$ όπου $c_1 = c(k,t)$. Έπεται ότι $r_1 \ll m^v$ οπότε έχουμε $r_t \ll_{k,t} {r_1}^{v^{t-1}} \ll_{k,t} m^{v^t}$.
Υποθέτουμε ότι τα $x_1, x_2, ..., x_R$ παριστάνουν ακεραίους με

$$\mid x_i \mid < \sqrt{l},\ \forall i = 1, 2, ..., R$$

Ποιοί είναι αυτοί οι ακέραιοι θα απαντηθεί στη συνέχεια.
Εφαρμόζουμε το θεώρημα 3.2.2 για κάθε x_i έχουμε

$$Ml^k = {x_1}^{2k} + \sum_{h=1}^{Q} {u_h}^{2k}$$

$$Ml^k = {x_2}^{2k} + \sum_{h=Q+1}^{2Q} {u_h}^{2k}$$

$$.$$
$$.$$
$$.$$

$$Ml^k = {x_R}^{2k} + \sum_{h=(R-1)Q+1}^{RQ} {u_h}^{2k}$$

για κάποιους ακέραιους $u_1, u_2, ..., u_{RQ}$
Έτσι, προσθέτουμε τις RMl^k καιr_1 και έχουμε

$$m = RMl^k + r_1 = \textstyle\sum_{j=1}^{R} {x_j}^{2k} + \displaystyle\sum_{h=1}^{QR} {u_h}^{2k} + {z_1}^k + {z_2}^k + ... + {z_{t-1}}^k + r_t$$

Άρα το m γράφεται ως άθροισμα $k-$δυνάμεων απο $R + QR + t - 1$ το πλήθος και έχουμε υπόλοιπο r_t.
Πήραμε R αριθμούς, $x_1, ..., x_R$ με $\mid x_i \mid \leq \sqrt{l}$. Για να δείξουμε ότι το r_t είναι ένα άθροισμα πεπερασμένου πλήθους $k-$δυνάμεων, θα εξιδεικεύσουμε τα x_i, θα εφαρμόσουμε το λήμμα 3.2.1 αλλά για τα

$$x_j = n + {a'}_j, j = 1, ..., R \text{ και } T = n$$

Σύμφωνα με το λήμμα 3.2.1 ισχύει

$$\sum_{j=1}^{R}(T+a'_j)^{2k}=\sum_{i=1}^{R}(T+a_i)^{2k}-(AT+B)$$

Άρα για $y=T+a_i, x_j=n+a'_j$ έχουμε

$$\sum_{j=1}^{R}{x_j}^{k}=\sum_{i=1}^{2R}{y_i}^{2k}-(An+B)$$

Επομένως,

$$m=\sum_{i=1}^{R}{y_i}^{2k}+\sum_{h=1}^{QR}{u_h}^{2k}+{z_1}^{k}+{z_2}^{k}+...+{z_{t-1}}^{k}+r_t-(An+B)$$

Θα επιλέξουμε το n ώστε $0\leq r_t-(An+B)<A$
Αρκεί να θέσουμε $n:=[\frac{r_t-B}{A}]$
Έχουμε

$$\frac{r_t-B}{A}-1\leq[\tfrac{r_t-B}{A}]\Rightarrow -[\tfrac{r_t-B}{A}]\leq 1-\frac{r_t-B}{A}$$

Άρα

$$\begin{gathered}r_t-(A[\tfrac{r_t-B}{A}]+B)\leq r_t+A(1-\tfrac{r_t-B}{A})-B\\ 0>-A\end{gathered}$$

Ισχύει αφού $A=(2k)!>0$ άρα $r_t-(An+B)\geqslant 0$.
Τώρα, για να δούμε ότι επιτρέπεται να επιλέξουμε έτσι το n πρέπει να αποδείξουμε ότι τα $x_j=n+a'_j$ πληρούν τον περιορισμό

$$\mid x_j\mid\leq\sqrt{l}\text{ το } x_j=n+a'_j=[\tfrac{r_t-B}{A}]+a'_j$$

Από την 3.6 $x_j\ll r_t+1$ όπου

$$r_t\ll {r_1}^{v^t-1}\leq m^{v^t}$$

άρα $x_j\ll m^{v^t}$, ενώ από την 3.5

$$l\geq[\tfrac{1}{2}(RM)^{\frac{1}{k}}]m^{\frac{1}{k}}$$

άρα

$$l\gg m^{\frac{1}{k}}\text{ άρα }\sqrt{l}\gg m^{\frac{1}{2k}}$$

$$x_j\ll m^{v^t}\leqslant m^{\frac{1}{2k}}\ll\sqrt{l}$$

διότι επιλέξαμε t τέτοιο ώστε $v^t < \frac{1}{2k}$.
Τέλος $0 < r_t - (An + B) < A$ άρα το $r_t - (An + B) < A$.
Άρα το $r_t - (An + B)$ γράφεται ως άθροισμα $k-$δυνάμεων και μάλιστα το
$1^k + ... + 1^k = r_t - (An + B) < A$
δηλάδη το άθροισμα φράσεται από το A. Άρα $g(k, m) < R + QR + t - 1 + A$ που φράσεται από σταθερά εξαρτημένη μόνο από το k. □

Σημείωση: Οι *A. Wieferich* [26] και A. *Kempner* [12] απέδειξαν ότι $g(3) = 9$. Αμέσως μετά την απόδειξη αυτή ο *Landau* [14] παρατήρησε ότι υπάρχουν πεπερασμένου πλήθους ακέραιοι οι οποίοι χρειάζονται 9 κύβους, δηλαδή ότι για αρκετά μεγάλους προσθεταίους 8 κύβοι είναι αρκετοί. Μάλιστα, ο *Dickson* [8] απέδειξε ότι μόνο οι 23 και 239 είναι αυτοί που χρειάζονται 9 κύβους, θετικών ακεραίων.

Ορισμός 3.3.1. *Ένα σύνολο ακεραίων θα λέγεται ασυμπτωτική βάση τάξης h όταν κάθε αρκετά μεγάλος ακέραιος μπορεί να γραφεί ως άθροισμα h στοιχείων του συνόλου.*

Επομένως, σύμφωνα με το θεώρημα του *Landau* οι κύβοι είναι μια ασυμπτωτική βάση τάξης οχτώ. Αργότερα ο *Linnik* [15] απέδειξε ότι μόνο πεπερασμένου πλήθους ακεραίων απαιτεί 8 κύβους και συνεπώς κάθε αρκετά μεγάλος ακέραιος γράφεται ως άθροισμα επτά κύβων.
Από την άλλη μεριά, μελέτη ισοδύναμιών *modulo* 9 δείχνει ότι υπάρχει άπειρο πλήθος θετικών ακεραίων οι οποίοι δεν γράφονται ως άθροισμα τριών κύβων. Αν επομένως $G(3)$ συμβολίζει τον ελάχιστο ακέραιο h τέτοιο ώστε οι κύβοι να είναι μια ασυμπτωτική βάση τάξης h, τότε $4 \leq G(3) \leq 7$. Ο ακριβώς προσδιορισμός του $G(3)$ είναι ένα σημαντικό άλυτο πρόβλημα της προσθετικής αριθμοθεωρίας. Η εικασία του *Waring* ότι για $g(4) = 19$ αποδείχθηκε το 1992 από τους *Balasubramanjan* [4] και *Deshouillers and Dress* [6].
Άνω φράγματα του αριθμού $g(k)$ έχουν δοθεί από τον *Rieger* [19] [21]

$$g(k) < (2k + 1)^{260(k+3)^{3k+8}}$$

τα οποία καλυτέρεψε ο *Rieger* το 1956 [20] σε

$$g(k) < (2k + 1)^{260(k+1)^8}$$

και ο *Pollack* [17] σε

$$g(k) < (2k + 1)^{2000k^5}.$$

Τέλος, αναφέρουμε την εργασία του *Trevor D. Wooley*, *arXiv*: 1602.03221*v*1 [*mathNT*], 9 *Feb*. 2016 σύμφωνα με την οποία $G(7) \leq 31$, $G(8) \leq 39$, κλπ.
Ας σημειωθεί ακόμη ότι το αμέσως προηγούμενο σχετικό αποτέλεσμα, ήταν του *Wooley* [27] όπου $G(7) \leq 33$ και $G(8) \leq 42$.

Βιβλιογραφία

[1] Γιάννης Αντωνιάδης, Αριστείδης Κοντογεωργής, Θεωρία Αριθμών και εφαρμογές, *http://eclass.uoa.gr/modules/document/file.php/MATH443/NumberTheoryNov.pdf*.

[2] *H.L.Alder*, *Partition identities- fron Euler to present*, *Amer. Math. Monthly* 76 (1969), 733 – 749.

[3] *Tom M. Apostol*, *Introduction to Analytic Number Theory*, *Springer-Verlag*, *New York* 1976.

[4] *R. Balasubramanian*, *Hardy – Ramanujan Journal*, 8, (1985), 1 – 40.

[5] *F. Dress*, *Methodes elementaries dans le probleme de Waring pour les*, *entiers*, *Universite de Provence*, *Marseille*, 1971, *Journees Arithmetiques Francaises*, *Mai* 1971.

[6] *F. Dress*, *Theorie additive des mombres*, *probleme de Waring et theoreme de Hilbert*, *Enseignement Math* (2) 18 (1972), 175 – 190; *errata*, *ibid* (2) 18 (1972), 301 – 302 (1973).

[7] *J. – M. Deshouillers and F. Dress*, *Annali Scuola Normale Super. Pisa*, 19 (1992) 113 – 153.

[8] *L. E. Dickson*, *History of the Theory of Numbers*, *Chelsea* 1971.

[9] *W.J. Ellison*, *Waring's Problem*, *AM. Math. Monthly*, 78, (1971), 10 – 36.

[10] *G.H. Hardy and E.M. Wright*, *An Introduction to the Theory of Numbers*, *Fifth edition*, *Clarendon Press Oxford* 1979.

[11] *D.Hilbert*, *Beweis fur die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n – ter Potenzen* (*Waringsches Problem*). *Dem Andenken an Hermann Minkowski gewidmet*, *Math. Ann.* 67 (1909), 281 – 300.

[12] *A. Kemper*, *Math. Annalen*, 72 (1912), 387 – 399.

[13] *Knopp, M. I.* (1970). *Modular functions in analytic number theory. Markham, Chicago, I*11.

[14] *E. Landau, Math. Annalen*, 66 (1909), 102 – 106.

[15] *Yu V. Linnik, Mat. Sbornik N S*, 12, (1943), 218 – 224.

[16] *Meltyn B.Nathanson, Additive Number Theory, The Classical Bases, Springer, New York* 1996.

[17] *Paul Pollack, A note on Hilbert's solution of Waring's Problem, Cent. Eur. J. Math.* 9 (2011), 294 – 301.

[18] *Paul Pollack, Not Always Buried Deep, A Second Course in Elementary Number Theory, AMS, United States* 2009.

[19] *G. J. Rieger, Archiv der Mathematik*, 4 (1953), 275 – 281.

[20] *G. J. Rieger, J. Reine Angew. Mathematik* 195 (1956), 108 – 120.

[21] *G. J. Rieger, Mitt. Math. Sem. Giessen* 44 (1953) 35 *pp*

[22] *H.E. Rose A Course in Number Theory, Second Edition, Oxford Science Publications, Oxford* 1996.

[23] *E.Schmidt, Zum Hilbertschen Beweise des Waringchen Theorems, Math. Ann* 74 (1913), 271 – 274.

[24] *Ian Stewart, Algebraic Number Theory and Fermat's Last Theorem*, (*Third Edition*) *A K Peters, Massachusetts* 2002.

[25] *Trevor D.Wooley, On Waring's Problem for Intermediate Powers, arXiv* : 1602.03221*v*1 [*math.NT*] 9 *Feb* 2016.

[26] *A. Wieferich, Math. Annalen*, 66 (1909), 95 – 101.

[27] *R. C. Vaughanand and T. D. Wooley, Philos.Trans.Roy.Soc.London, Ser A* 345 (1993), 385 – 396.