ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΚΑΙ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ
ΤΗΣ
ΈΦΗΣ ΣΥΡΡΑΚΟΥ

Η ΑΠΟΔΕΙΞΗ ΤΗΣ ΕΙΚΑΣΙΑΣ ΤΟΥ CATALAN

ΗΡΑΚΛΕΙΟ
ΙΑΝΟΥΑΡΙΟΣ 2007

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ
ΓΙΑΝΝΗΣ Α. ΑΝΤΩΝΙΑΔΗΣ

Η μεταπτυχιακή αυτή εργασία κατατέθηκε στο Τμήμα Μαθηματικών της Σχολής Θετικών και Τεχνολογικών Επιστημών του Πανεπιστημίου Κρήτης τον Ιανουάριο του 2007.

Την επιτροπή αξιολόγησης αποτέλεσαν οι:

Γιάννης Αντωνιάδης

Αριστείδης Κοντογεώργης

Νίκος Τζανάκης

UNIVERSITY OF CRETE

DEPARTMENT OF MATHEMATICS

EFI SYRRAKOY

THE PROOF OF CATALAN'S CONJECTURE

HERAKLION
JANUARY 2007

Abstract

Catalan conjectured that 8 and 9 are the only consecutive integers which are perfect powers. In other words, the diophantine equation

$$X^m - Y^n = 1 \qquad (m > 1, n > 1, x > 0, y > 0)$$

has no solutions other than $x^m = 3^2,\ y^n = 2^3$.
The conjecture which dates back to 1844 was recently proven by the mathematician Preda Mihăilescu.
In this master thesis we present the proof of Catalan's conjecture.

Στη γιαγιά και στον παππού μου,
Θεονύμφη και Ανδρέα.

Περιεχόμενα

Εισαγωγή **7**

1 Αποτελέσματα με χρήση στοιχειώδους Θεωρίας Αριθμών **13**
1.1 Η εξίσωση του Catalan για $p = q$ 13
1.2 Η εξίσωση του Catalan για $p = 2$ και $q = 3$ 13
1.3 Η εξίσωση του Catalan για $p = 3$ και $q = 2$ 17
1.4 Η εξίσωση του Catalan για $p = 2$ και $q > 3$ 18
1.5 Η εξίσωση του Catalan για $q = 2$ και $p > 3$ 21
1.6 Οι σχέσεις του Cassels 23

2 Οι ισοδυναμίες του Inkeri **33**
2.1 Κυκλοτομικά σώματα αριθμών 33
2.2 Το θεώρημα του Inkeri 36

3 Το πρώτο θεώρημα του Mihăilescu **41**
3.1 Το ιδεώδες του Stickelberger 41
3.2 Το θεώρημα του Mihăilescu 42

4 Γραμμικές μορφές λογαρίθμων **47**

5 Η απόδειξη του Mihăilescu **51**
5.1 Δακτύλιοι και Modules 51
5.2 Δακτύλιοι ομάδας 55
5.3 Ο δακτύλιος $R = \mathbb{F}_q[G]$ και κάποια $R-$modules 55
5.4 Τα τρία βασικά θεωρήματα και η απόδειξη της εικασίας του Catalan 59
5.5 Η απόδειξη του θεωρήματος 5.4.1 60
5.6 Η απόδειξη του θεωρήματος 5.4.2 62
5.7 Η απόδειξη του θεωρήματος 5.4.3 68

Α΄ Αλγεβρική Θεωρία Αριθμών **69**
Α΄.1 Αλγεβρικοί και ακέραιοι αλγεβρικοί αριθμοί - Αλγεβρικά σώματα αριθμών 69
Α΄.2 Συζυγείς αριθμοί-Ίχνος-Norm 71
Α΄.3 Μονάδες 72
Α΄.4 Ιδεώδη 72
Α΄.5 Πρώτα ιδεώδη και ανάλυση ιδεωδών σε γινόμενο πρώτων ιδεωδών 75

Α′.6 Αριθμός κλάσεων ιδεωδών 77
Α′.7 Διακλάδωση-Νόμος ανάλυσης 77
Α′.8 Τετραγωνικά σώματα αριθμών 78

Βιβλιογραφία **81**

Εισαγωγή

Ένας από τους κύριους σκοπούς της Θεωρίας Αριθμών είναι η εύρεση μεθόδων λύσεων διοφαντικών εξισώσεων, δηλαδή πολυωνυμικών εξισώσεων με ακέραιους συντελεστές των οποίων ζητείται η εύρεση όλων των ακεραίων ή ρητών λύσεων.
Κλασικό παράδειγμα αποτελεί η εικασία του Fermat, ότι η εξίσωση

$$X^n + Y^n = Z^n,$$

για κάθε $n \in \mathbb{N}, n \geq 3$ δεν έχει μη-τετριμμένη ακέραια λύση (x, y, z) με $xyz \neq 0$. Είναι σε όλους γνωστό ότι η εικασία τελικά υπέκυψε στις προσπάθειες των Μαθηματικών, αλλά πολύ αργότερα, 350 περίπου χρόνια μετά τη διατύπωσή της.

Στην παρούσα εργασία θα ασχοληθούμε με μία άλλη φημισμένη εικασία, αυτή του Βέλγου μαθηματικού Eugène Catalan (1814 – 1894).
Στα 1844 δημοσιεύθηκε στο Crelle's Journal, τόμος 27, σελίδα 192, το ακόλουθο απόσπασμα επιστολής του Catalan, η οποία είχε ως αποδέκτη τον εκδότη του περιοδικού.
«Κύριε, παρακαλώ να δημοσιεύσετε στο περιοδικό σας το ακόλουθο θεώρημα. Πιστεύω ότι είναι αληθές παρά το ότι δεν τα κατάφερα να το αποδείξω μέχρι στιγμής· ίσως άλλοι να είναι πιο τυχεροί.»
«Δεν υπάρχουν διαδοχικοί ακέραιοι, εκτός των 8 και 9, οι οποίοι να είναι δυνάμεις ακεραίων. Με άλλα λόγια η (διοφαντική) εξίσωση

$$X^m - Y^n = 1$$

έχει σαν μοναδική, μη-τετριμμένη ($m > 1, n > 1, xy \neq 0$), λύση στους μη-αρνητικούς ακεραίους την $(x = 3, m = 2, y = 2, n = 3)$.»
Προτού αναφερθούμε στην Ιστορία επίλυσης της εικασίας του Catalan, θα γυρίσουμε για λίγο πίσω και θα αναφερθούμε στην προϊστορία της.
Ο Philippe de Vitry έθεσε το πρόβλημα «αν μπορεί ο $3^m \pm 1$ να είναι δύναμη του 2.»
Το πρόβλημα αυτό απαντήθηκε από τον Levi ben Gerson, τον επονομαζόμενο και Leo Hebraius (1288 – 1344). Ο Gerson [16] απέδειξε ότι αν

$$3^m \pm 1 = 2^n, \text{ τότε } m = 2 \text{ και } n = 3.$$

Στα 1657 ο Fermat, σε επιστολή του προς τον Frénicle de Bessy [7], πρότεινε να αποδειχθεί ότι, αν p περιττός πρώτος και n φυσικός ≥ 2, τότε το $p^n + 1$ δεν είναι ποτέ τέλειο

τετράγωνο και ότι το ίδιο ισχύει και για το $2^n + 1$, όταν $n \geq 4$. Ο Frénicle απέδειξε τις προτάσεις του Fermat, αλλά η απόδειξή του έγινε γνωστή μόλις το 1944 ([17]).
Στα 1738 ο Euler [14], χρησιμοποιώντας τη μέθοδο της άπειρης καθόδου (Fermat), απέδειξε ότι, αν η διαφορά μεταξύ ενός τετραγώνου και ενός κύβου είναι ± 1, τότε οι αριθμοί αυτοί είναι 9 και 8. Απέδειξε δηλαδή την εικασία του Catalan για $m = 2$ και $n = 3$.

Είναι εύκολο να αποδειχθεί ότι δε χρειάζεται να μελετήσουμε την εξίσωση του Catalan με οποιουσδήποτε εκθέτες. Αρκεί να θεωρήσουμε την περίπτωση που

$$m = p,\ n = q,\ p \neq q \text{ και } p, q \text{ πρώτοι αριθμοί.}$$

Με βάση κυρίως τη μεθοδολογία, η απόδειξη χωρίζεται σε τρεις, θα λέγαμε, περιόδους.
Η πρώτη περίοδος αναφέρεται κυρίως σε αποτελέσματα με χρήση στοιχειωδών μεθόδων.
Το επόμενο βήμα, μετά την απόδειξη του Euler για $p = 2$ και $q = 3$, ήταν η μελέτη των εξισώσεων της μορφής

$$X^2 - Y^q = \pm 1 \qquad (q \geq 5).$$

Η εξίσωση αυτή χωρίζεται σε δύο εξισώσεις, ανάλογα με το πρόσημο. Η πρώτη, της μορφής $X^p - Y^2 = 1$ είναι απλή, δεν έχει μη-τετριμμένες λύσεις και αποδείχθηκε από τον V. A. Lebesgue [20] στα 1850, μερικά χρόνια αργότερα από τη διατύπωση της εικασίας. (Ας σημειωθεί εδώ ότι ο Lebesgue δεν είναι το ίδιο πρόσωπο με τον γνωστό Lebesque της Θεωρίας Μέτρου, ο οποίος γεννήθηκε το 1875.) Είναι αξιοσημείωτο ότι η δεύτερη μορφή, $X^2 - Y^q = 1$, χρειάστηκε 120 χρόνια για να αποδειχθεί. Προτού όμως αποδειχθεί είχαμε ενδιαφέροντα ενδιάμεσα αποτελέσματα.
Στα 1921 ο Nagell [30] απέδειξε ότι η εξίσωση $X^3 \pm 1 = Y^m$ (m όχι δύναμη του 2) έχει μόνο τετριμμένες λύσεις. (Εδώ χρειάστηκαν και κάποια αποτελέσματα του Ljunggren [21] (1942/1943) για την πλήρη απόδειξη ενός ενδιαμέσου βήματος.)
Στα 1934 ο Nagell [32] απέδειξε ότι, αν η εξίσωση $X^2 - Y^q = 1$, όπου q είναι πρώτος > 3, έχει μη-τετριμμένη λύση, τότε $q \equiv 1 \pmod 8$.
Στη συνέχεια, στα 1940/1941 ο Obláth [33] απέδειξε ότι, αν η εξίσωση $X^2 - Y^q = 1$ έχει μη-τετριμμένη λύση, τότε θα πρέπει $2^{q-1} \equiv 1 \pmod{q^2}$ και $3^{q-1} \equiv 1 \pmod{q^2}$.
Η σύνδεση αυτή με ισοδυναμίες τέτοιου τύπου είναι επηρεασμένη από τα θεωρήματα των Wieferich και Mirimanof σχετικά με την εξίσωση του Fermat

$$X^p + Y^p = Z^p, p \in \mathbb{P}.$$

Αν η εξίσωση του Fermat $X^p + Y^p = Z^p$ έχει μη-τετριμμένη λύση (x, y, z) και $p \nmid xyz$, τότε $2^{p-1} \equiv 1 \pmod{p^2}$ (Wieferich [41], 1909). Ας σημειωθεί εδώ ότι μέχρι σήμερα δύο μόνο Wieferich πρώτοι είναι γνωστοί, οι 1093 και 3511, και αυτό μετά από έλεγχο όλων των πρώτων $p < 4 \cdot 10^{12}$. Βλέπουμε δηλαδή ότι πρώτοι αριθμοί που ικανοποιούν τις παραπάνω ισοδυναμίες είναι εξαιρετικά σπάνιοι.
Στα 1961 οι Inkeri και Hyyrö [19] απέδειξαν ότι, αν υπάρχει μη-τετριμμένη λύση (x, y) της εξίσωσης, τότε θα πρέπει

$$\begin{aligned} x &> 2^{q(q-2)} > 10^{3 \cdot 10^9} \\ y &> 4^{q-2} > 10^{6 \cdot 10^5}. \end{aligned}$$

Τελικά στα 1960 ο Chao Ko [12] απέδειξε (δημοσιεύτηκε σε μετάφραση από τα κινέζικα στα 1964) ότι η εξίσωση $X^2 - Y^q = 1$ έχει μόνο τετριμμένες λύσεις.
Η απόδειξη αυτή απλοποιήθηκε αρκετά στα 1976 από τον Chein [13].
Στα 1924 ο Nagell [31] απέδειξε ότι, αν η εξίσωση $X^2 - Y^q = 1$ (q πρώτος, $q > 3$) έχει μη-τετριμμένη λύση (x, y), τότε $2 \mid y$ και $q \mid x$.
Το αποτέλεσμα αυτό γενικεύτηκε στα 1960 από τον Cassels [11], ο οποίος απέδειξε με στοιχειώδη αλλά ιδιοφυή τρόπο ότι, αν για περιττούς πρώτους p, q με $p \neq q$ η εξίσωση $X^p - Y^q = 1$ έχει μη-τετριμμένη λύση (x, y), τότε $p \mid y$ και $q \mid x$.
Στόχος μας είναι να βρούμε ότι τα x, y, p, q έχουν τόσο καλές ιδιότητες ώστε τελικά να αποδειχθεί ότι δεν υπάρχουν.
Θα πρέπει να σημειώσουμε εδώ ότι μέχρι τις αρχές της δεκετίας του εβδομήντα δεν ήταν γνωστό όχι μόνο αν η εικασία του Catalan ισχύει, αλλά ούτε καν αν έχει πεπερασμένο ή άπειρο πλήθος λύσεων. Ο λόγος είναι ότι η εξίσωση έχει τέσσερις αγνώστους.
Αν οι περιττοί πρώτοι p και q με $p \neq q$ είναι σταθεροί, τότε γνωρίζουμε ότι το πλήθος των λύσεων της διοφαντικής εξίσωσης $X^p - Y^q = 1$ είναι πεπερασμένο (Siegel [36], 1929).

Η δεύτερη περίοδος αναφέρεται σε αποτελέσματα με χρήση υπερβατικών μεθόδων.
Στα μέσα της δεκαετίας του εξήντα ο Alan Baker [6] απέδειξε μία σειρά από θεωρήματα στα οποία βρίσκει κάτω φράγματα γραμμικών μορφών λογαρίθμων.
Ο Tijdeman [38] στα 1976 εφάρμοσε τη θεωρία του Baker κατά ιδιοφυή τρόπο σε δύο γραμμικές μορφές λογαρίθμων και κατάφερε να αποδείξει ότι υπάρχει μία σταθερά $C > 0$, η οποία είναι υπολογίσιμη, τέτοια ώστε αν (x, y, p, q) είναι μη-τετριμμένη λύση της εξίσωσης του Catalan, τότε $\max\{x, y, p, q\} < C$.
Θα μπορούσε να πει κανείς ότι ουσιαστικά με το αποτέλεσμα του Tijdeman το πρόβλημα λύθηκε. Άμεση συνέπεια του θεωρήματος του Tijdeman είναι ότι η εξίσωση έχει πεπερασμένο πλήθος λύσεων. Επομένως, αυτό που απομένει είναι να ελέγξουμε όλες τις τετράδες (x, y, p, q) φυσικών αριθμών μικρότερων του C. Δυστυχώς αυτό είναι αδύνατο να επιτευχθεί. Το φράγμα είναι τόσο μεγάλο ($e^{e^{e^{e^{730}}}}$!) που οι περιπτώσεις που απομένουν να εξετασθούν είναι τόσο πολλές ώστε αυτό να είναι αδύνατο να επιτευχθεί ακόμη και με τους ταχύτερους υπολογιστές. Ακολουθεί μία σειρά εργασιών στις οποίες βελτιώνεται αρκετά το φράγμα του Tijdeman.
Το καλύτερο μέχρι σήμερα γνωστό αποτέλεσμα είναι ότι αν (x, y, p, q) είναι μη-τετριμμένη λύση της εξίσωσης του Catalan, τότε

$$\max\{p, q\} < 7,8 \cdot 10^{16}$$

και οφείλεται στον M. Mignotte [24].
Δυσυχώς το αποτέλεσμα είναι και πάλι αρκετά μεγάλο και είναι αδύνατο να καταστεί δυνατός ο έλεγχος όλων των ενδιαμέσων περιπτώσεων.

Η τρίτη περίοδος σηματοδοτεί την επιστροφή στην Αλγεβρική Θεωρία Αριθμών και την (προχωρημένη) Θεωρία των Κυκλοτομικών Σωμάτων.
Στα 1990 ο Inkeri [18] απέδειξε ότι αν (x, y, p, q) είναι μη-τετριμμένη λύση της εξίσωσης του Catalan, τότε

(i) Αν q δε διαιρεί τον αριθμό κλάσεων ιδεωδών h_p του κυκλοτομικού σώματος αριθμών $K = \mathbb{Q}(\zeta_p)$, όπου $\zeta_p := e^{\frac{2\pi i}{p}}$, τότε

$$q^2 \mid x \text{ και } p^{q-1} \equiv 1 \pmod{q^2}.$$

(ii) Αν p δε διαιρεί τον αριθμό κλάσεων ιδεωδών h_p του κυκλοτομικού σώματος αριθμών $K = \mathbb{Q}(\zeta_q)$, όπου $\zeta_q := e^{\frac{2\pi i}{q}}$, τότε

$$p^2 \mid y \text{ και } q^{p-1} \equiv 1 \pmod{p^2}.$$

Η απόδειξη είναι κλασική και ανάλογη αντίστοιχου αποτελέσματος για την εξίσωση του Fermat. Στηρίζεται φυσικά κατά μεγάλο μέρος και στα αποτελέσματα του Cassels. Εδώ περνούμε από αριθμούς σε ιδεώδη και στη συνέχεια «προσγειωνόμαστε» στους ακεραίους με «αυτόματο πιλότο» τον περιορισμό $q \nmid h_p$.
Το πρόβλημα συνέχιζε να παραμένει στην περίπτωση που δεν ίσχυαν οι υποθέσεις της μη διαιρετότητας του αριθμού κλάσεων ιδεωδών στο θεώρημα του Inkeri.
Το τελικό βήμα έγινε από τον Mihăilescu, ο οποίος σε μία σειρά εργασιών από το 1999 μέχρι το 2003-2004 ([26], [27], [28], [29]) κατάφερε να αποδείξει πλήρως την εικασία.
Στην πρώτη του εργασία [26] (1999) απέδειξε τις ισοδυναμίες του Inkeri χωρίς κανένα περιορισμό, για να αποδειχθεί, όπως γίνεται συχνά, ότι οι περιορισμοί του Inkeri ήταν τεχνητοί και οφείλονταν στην αποδεικτική μέθοδο που εφαρμόστηκε. Η πρώτη ιδιοφυής ιδέα του Mihăilescu ήταν να δράσει πάνω στην (υποτιθέμενη) λύση της εξίσωσης με στοιχεία του ιδεώδους του Stickelberger, τα οποία, ως γνωστό, έχουν ιδιότητα μηδενιστή όταν δράσουν σε ιδεώδη του κυκλοτομικού σώματος αριθμών.
Οι υπολογισμοί μέσω του θεωρήματος του Mihăilescu έχουν ελαττωθεί σημαντικά. Αρκεί να σημειώσουμε ότι οι δύο πιο μικροί πρώτοι που πληρούν τις ισοδυναμίες του Mihăilescu είναι $(p, q) = (83, 4871)$ και $(p, q) = (911, 318017)$, και οι οποίοι μπορούν να εξαιρεθούν μέσω άλλων υπολογισμών.
Συνδυάζοντας τα αποτελέσματα των Tijdeman και Mihăilescu, οι Mignotte και Roy [25] υπολόγισαν ένα κάτω φράγμα για τα p, q, ότι δηλαδή $\min\{p, q\} \geq 10^7$.
Στη συνέχεια η απόδειξη γίνεται σε δύο βήματα.

Στο πρώτο βήμα αποδεικνύεται ότι αν οι p, q είναι περιττοί πρώτοι με $p \neq q$ και $p \equiv 1 \pmod{q}$, τότε η εξίσωση του Catalan δεν έχει μη-τετριμμένη λύση.
Η απόδειξη στηρίζεται στα γνωστά σχετικά αποτελέσματα της υπερβατικής αριθμοθεωρίας. Αν $p \equiv 1 \pmod{q}$, τότε $p \equiv 1 \pmod{q^2}$, δηλαδή $p = \ell q^2 + 1$, για κάποιο ακέραιο ℓ. Εύκολα αποδεικνύεται ότι $p > 4q^2$. Από το θεώρημα του Tijdeman προκύπτει ότι

$$p \leq 24,34 \cdot q\Big(\max\{\log \frac{p+1}{\log q} + 0,14,\ 21\}\Big)^2 \log q.$$

Άμεση συνέπεια αυτής της σχέσης είναι ότι για $q \geq 28000$ έχουμε $p \leq 4q^2$. Είναι πλέον εύκολο (με χρήση ηλεκτρονικού υπολογιστή) να ελέγξουμε ότι δεν υπάρχουν πρώτοι p, q τέτοιοι ώστε $q \leq 28000$, $1 + 4q^2 \leq p \leq 24,34 \cdot q\Big(\max\{\log \frac{p+1}{\log q} + 0,14,\ 21\}\Big)^2 \log q$,

$$p \equiv 1 \pmod{q^2} \text{ και } q^{p-1} \equiv 1 \pmod{p^2}$$

Στο δεύτερο βήμα υποθέτουμε ότι $p \not\equiv 1 \pmod{q}$.
Θεωρούμε το κυκλοτομικό σώμα αριθμών $K = \mathbb{Q}(\zeta)$, $\zeta := e^{\frac{2\pi i}{p}}$.
Αν $G := Gal(K/\mathbb{Q})$, τότε ο δακτύλιος ομάδας $\mathbb{F}_q[G]$ είναι ευθύ γινόμενο σωμάτων αφού το q δε διαιρεί την τάξη της ομάδας G ($|G| = p-1$).
Ο δακτύλιος αυτός δρα τόσο στην ομάδα E των μονάδων του K όσο και στην ομάδα H των κλάσεων ιδεωδών αυτού.
Αποδεικνύεται ότι E/E^q είναι ένα κυκλικό $\mathbb{F}_q[G]-$module του οποίου ο μηδενιστής (annihilator) παράγεται από το norm στοιχείο $N := \sum_{\sigma \in G} \sigma$ του $\mathbb{F}_q[G]$ και το $1-\iota$, όπου ι είναι η μιγαδική συζυγία.
Στη συνέχεια θεωρούμε την υποομάδα C των κυκλοτομικών μονάδων του K.
Ως γνωστό ο δείκτης $[E : C]$ συνδέεται στενά με τον αριθμό κλάσεων ιδεωδών του K (παραπέμπουμε στο [2]).
Μία σημαντική υποομάδα της ομάδας C είναι η ομάδα C_q των $q-$primary κυκλοτομικών μονάδων.
Το στοιχείο $a \in \mathbb{Z}[\zeta]$ θα λέγεται $q-$primary αν υπάρχει $\beta \in \mathbb{Z}[\zeta]$ τέτοιο ώστε

$$a \equiv \beta^q \pmod{q^2}.$$

Πιο γενικά, το στοιχείο $a \in K^*$ θα λέγεται $q-$primary αν

$$a = a_1 a_2^{-1} \gamma^q,$$

όπου τα $a_1, a_2 \in \mathbb{Z}[\zeta]$ είναι $q-$primary και $\gamma \in K^*$.
Η μελέτη του $\mathbb{F}_q[G]-$module E/E^q γίνεται σε τρία ενδιάμεσα βήματα.
Θεωρούμε τα $\mathbb{F}_q[G]-$modules

$$E/CE^q, \;\; C/C_q \;\; \text{και} \;\; C_q/(C_q \cap E^q)$$

και αποδεικνύουμε ότι οι μηδενιστές τους, έστω I_1, I_2, I_3, είναι ανά δύο πρώτοι μεταξύ τους και ότι ισχύει

$$I_1 I_2 I_3 = (N, 1-\iota).$$

Στη συνέχεια αποδεικνύεται, ανεξάρτητα από την εξίσωση του Catalan, ότι για $p > q$ ισχύει $I_2 \neq < 1 > = R = \mathbb{F}_q[G]$. Ενώ, αν υποθέσουμε ότι υπάρχει λύση (x, y, p, q) της εξίσωσης του Catalan, τότε $I_1 I_3 \subseteq (N, 1-\iota)$ και από την τελευταία σχέση προκύπτει εύκολα ότι $I_2 = < 1 >$, άτοπο!

Για να πετύχουμε το σκοπό μας θεωρούμε τη δράση στοιχείων του δακτυλίου ομάδας $\mathbb{F}_q[G]$ ειδικής μορφής $\Theta = \sum_{\sigma \in G} n_\sigma \sigma$ με $\sum_{\sigma \in G} n_\sigma = 0$ στα στοιχεία $(x-\zeta)$ του δακτυλίου $\mathbb{Z}[\zeta]$.
Αποδεικνύουμε ότι για τέτοια στοιχεία Θ ισχύει

$$(x-\zeta)^\Theta \in (K^*)^q$$

και συγχρόνως ότι για όλα τα διάφορα του μηδενικού στοιχεία αυτής της ειδικής μορφής ισχύει

$$(x-\zeta)^\Theta \notin (K^*)^q.$$

Για την απόδειξη της πρώτης σχέσης χρησιμοποιούμε ένα βαθύ θεώρημα του Thaine σύμφωνα με το οποίο ένα άρτιο στοιχείο Θ του $\mathbb{Z}[G]$ το οποίο μηδενίζει το $q-$part της E/C μηδενίζει και το $q-$part του $(+)-$part της ομάδας κλάσεων ιδεωδών H του K. Ας σημειωθεί εδώ ότι η ομάδα κλάσεων ιδεωδών H^+ είναι η ομάδα κλάδεων ιδεωδών του μέγιστου πραγματικού υποσώματος του K ([2]).
Η απόδειξη της δεύτερης σχέσης περιέχει την πιο όμορφη ιδέα του Mihăilescu. Συνδυάζει τη Θεωρία Συναρτήσεων με την Αλγεβρική Θεωρία Αριθμών και τη Γεωμετρία των Αριθμών.
Είναι γνωστό ότι για κάθε περιττό φυσικό αριθμό n η απεικόνιση $\varphi : \mathbb{R} \to \mathbb{R}$ που ανιστοιχεί κάθε $a \in \mathbb{R}$ στο $a^n \in \mathbb{R}$ είναι ένας ομοιομορφισμός του $\mathbb{R}$. Η αντίστροφη συνάρτηση δίνεται, μέσα στο μοναδιαίο κύκλο, από τη διωνυμική σειρά $\sum_{k=0}^{\infty} \binom{\frac{1}{n}}{k} T^k$.
Από τη μελέτη της σειράς προκύπτει ότι όταν θεωρήσουμε κάποιο $\Theta \in \mathbb{Z}[G]$ με μηαρνητικούς συντελεστές n_σ των οποίων το άθροισμα είναι mq, τότε ο ακέραιος αλγεβρικός

$$q^{m+\mathrm{ord}_q(m!)} x^m (1 - \frac{\zeta}{x})^{\frac{\Theta}{q}}$$

είναι ίσος προς το $P(T)(x)$, όπου $P(T)$ είναι ένα πολυώνυμο το οποίο modulo $q\mathbb{Z}[\zeta][T]$ είναι ίσο με $q^{m+\mathrm{ord}_q(m!)} a_m(\Theta)$. Οι συντελεστές $a_m(\Theta)$ είναι οι $m-$οστοί συντελεστές της

$$\Big(\sum_{k=0}^{\infty} \binom{\frac{1}{q}}{k} (\zeta T)^k\Big)^{\Theta}.$$

Τελικά αποδεικνύεται ότι κατ' ανάγκη όλοι οι συντελεστές του Θ διαιρούνται με q, δηλαδή ότι το Θ είναι ίσο με μηδέν modulo q και συνεπώς έχουμε αποδείξει πλήρως την εικασία του Catalan.
Θα πρέπει ακόμη να σημειώσουμε ότι ο Mihăilescu κατάφερε εν τω μεταξύ να αποδείξει πλήρως την εικασία χωρίς να κάνει χρήση υπερβατικών μεθόδων και ηλεκτρονικού υπολογιστή. Η ιδέα της απόδειξης είναι η εξής: Αν (x, y, p, q) είναι λύση της εξίσωσης του Catalan, τότε, μέσω αυτής, δίνονται δύο ιδεώδη A, B του $\mathbb{Z}[G]$ τέτοια ώστε αφενός $A \subseteq B$ και αφετέρου το A έχει περισσότερα στοιχεία (κάποιου είδους) απ' ότι το B, άτοπο.
Το μέρος αυτό δεν περιέχεται στην μεταπτυχιακή μας εργασία.
Ο τρόπος γραφής του Mihăilescu είναι αρκετά περίπλοκος. Το καθήκον της απλοποίησης αρκετών από τις τεχνικές του εξετέλεσε με επιτυχία ο Yuri Bilu ([8], [9]).
Επίσης, λόγω του ενδιαφέροντος του θέματος, έχουμε μία σειρά από περιγραφικά άρθρα ([15], [23], [35]).
Τέλος να σημειώσουμε ότι η εικασία του Fermat, η εικασία του Catalan και το πρόβλημα του Waring αποτελούν ειδικές περιπτώσεις (φημισμένες εικασίες) μίας κάπως πιο γενικής θεώρησης αυτής των powered numbers. ([22]).

Θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στον καθηγητή μου κ. Γιάννη Α. Αντωνιάδη του οποίου η συμβολή ήταν πολύτιμη στην εκπόνηση αυτής της εργασίας.
Επίσης θα ήθελα να ευχαριστήσω τόσο τον κ. Paulo Ribenboim ο οποίος μας προμήθευσε ένα αντίγραφο του εξαντλημένου και δυσεύρετου σήμερα βιβλίου του [34], όσο και τον κ. Yuri Bilu ο οποίος, περί τα τέλη Σεπτεμβρίου, έθεσε στη διάθεσή μας αντίγραφο μέρους του υπό συγγραφή βιβλίου των Bilu, Bugeaud, Mignotte [10].

Κεφάλαιο 1

Αποτελέσματα με χρήση στοιχειώδους Θεωρίας Αριθμών

1.1 Η εξίσωση του Catalan για p = q

Πρόταση 1.1.1

Έστω p ένας πρώτος. Η εξίσωση $X^p = Y^p + 1$ δεν έχει ακέραια λύση (x, y) με $xy \neq 0$.

Απόδειξη:

Υποθέτουμε ότι (x, y) είναι μία ακέραια λύση της εξίσωσης με $xy \neq 0$.
Αν $p = 2$, τότε $x^2 - y^2 = 1$, δηλαδή $x - y = x + y = \pm 1$. Αφαιρώντας τις εξισώσεις αυτές κατά μέλη έχουμε $y = 0$, το οποίο είναι άτοπο.
Αν $p \geq 3$, τότε από την εξίσωση $x^p = y^p + 1$ έπεται ότι

$$(x - y)(x^{p-1} + x^{p-2}y + \ldots + xy^{p-2} + y^{p-1}) = 1,$$

δηλαδή $x = y \pm 1$. Αν $x = y + 1$, τότε $x^p = (y + 1)^p > y^p + 1$, το οποίο είναι άτοπο. Αν $x = y - 1$, τότε $x^p = (y - 1)^p < y^p - 1$, το οποίο είναι επίσης άτοπο. Επομένως, η εξίσωση $X^p = Y^p + 1$ δεν έχει ακέραια λύση (x, y) με $xy \neq 0$.

1.2 Η εξίσωση του Catalan για p = 2 και q = 3

Λήμμα 1.2.1

Αν a είναι στοιχείο του $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ και η norm $N(a)$ είναι τετράγωνο ακεραίου, τότε $a = xb^2$, όπου x είναι ακέραιος και b στοιχείο του $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$.

Απόδειξη:

Στο δακτύλιο $R = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ των ακεραίων αλγεβρικών αριθμών του τετραγωνικού σώματος αριθμών $K = \mathbb{Q}(\sqrt{-3})$ ισχύει η μονοσήμαντη ανάλυση, δηλαδή αν a είναι στοιχείο του $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, τότε το a αναλύεται στον R σε γινόμενο αναγώγων στοιχείων.
Αν p είναι ένας πρώτος αριθμός, τότε:

(i) Για $p \neq 2$ έχουμε:
Αν $p \not| -3$ και $(\frac{-3}{p}) = 1$, τότε $p = \pi_1\pi_2$, όπου π_1, π_2 είναι ανάγωγα στοιχεία του R και $N(\pi_1) = N(\pi_2) = p$.
Αν $p \not| -3$ και $(\frac{-3}{p}) = -1$, τότε p είναι ανάγωγο στοιχείο του R και $N(p) = p^2$.
Αν $p \mid -3$, τότε $p = r^2$, όπου r είναι ανάγωγο στοιχείο του R και $N(r) = p$.
(ii) Για $p = 2$ έχουμε 2 ανάγωγο στοιχείο του R και $N(2) = 2^2$, αφού $-3 \equiv 5 \pmod 8$.
Άρα $a = \pi_1^{\beta_1}\pi_2^{\beta_2}\ldots\pi_\kappa^{\beta_\kappa}p_1^{\gamma_1}p_2^{\gamma_2}\ldots p_\lambda^{\gamma_\lambda}r_1^{2\delta_1}r_2^{2\delta_2}\ldots r_\mu^{2\delta_\mu}2^\epsilon$, δηλαδή

$$N(a) = q_1^{\beta_1}\ldots q_\kappa^{\beta_\kappa}p_1^{2\gamma_1}p_2^{2\gamma_2}\ldots p_\lambda^{2\gamma_\lambda}s_1^{2\delta_1}s_2^{2\delta_2}\ldots s_\mu^{2\delta_\mu}2^{2\epsilon}.$$

Για να είναι η norm $N(a)$ τετράγωνο ακεραίου θα πρέπει

$$\beta_1 \equiv \beta_2 \equiv \ldots \equiv \beta_\kappa \equiv 0 \pmod 2,$$

δηλαδή $\beta_i = 2\zeta_i$, για κάθε $i = 1, \ldots, \kappa$.
Επομένως

$$\begin{aligned} a &= \pi_1^{2\zeta_1}\pi_2^{2\zeta_2}\ldots\pi_r^{2\zeta_\kappa}p_1^{\gamma_1}p_2^{\gamma_2}\ldots p_\lambda^{\gamma_\lambda}r_1^{2\delta_1}r_2^{2\delta_2}\ldots r_\mu^{2\delta_\mu}2^\epsilon \\ &= (\pi_1^{\zeta_1}\pi_2^{\zeta_2}\ldots\pi_r^{\zeta_\kappa}r_1^{\delta_1}r_2^{\delta_2}\ldots r_\mu^{\delta_\mu})^2 p_1^{\gamma_1}p_2^{\gamma_2}\ldots p_\lambda^{\gamma_\lambda}2^\epsilon \\ &= xb^2, \end{aligned}$$

όπου $x = p_1^{\gamma_1}p_2^{\gamma_2}\ldots p_\lambda^{\gamma_\lambda}2^\delta$ είναι ακέραιος και $b = \pi_1^{\zeta_1}\pi_2^{\zeta_2}\ldots\pi_r^{\zeta_\kappa}r_1^{\delta_1}r_2^{\delta_2}\ldots r_\mu^{\delta_\mu}$ στοιχείο του $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$.

□

Πρόταση 1.2.1

Δεν υπάρχουν ακέραιοι b, c με $bc \neq 0$, $\gcd(b, c) = 1$ και $b \not\equiv 0 \pmod 3$ για τους οποίους $bc(b^2 - 3bc + 3c^2)$ να είναι τετράγωνο > 1.

Απόδειξη:

Θα εφαρμόσουμε τη μέθοδο καθόδου του Fermat.
Υποθέτουμε ότι υπάρχουν ακέραιοι b, c με $bc \neq 0$, $\gcd(b, c) = 1$ και $b \not\equiv 0 \pmod 3$ για τους οποίους $bc(b^2-3bc+3c^2)$ είναι τετράγωνο > 1. Στη συνέχεια υποθέτουμε ότι η λύση αυτή είναι η λύση η οποία δίνει την ελάχιστη τιμή $bc(b^2-3bc+3c^2)$. Θα κατασκευάσουμε ένα ζευγάρι ακεραίων (s, t) με $st \neq 0$, $\gcd(s, t) = 1$ και $s \not\equiv 0 \pmod 3$ για το οποίο $st(s^2 - 3st + 3t^2)$ είναι τετράγωνο > 1, αλλά $st(s^2 - 3st + 3t^2) < bc(b^2 - 3bc + 3c^2)$ και έτσι καταλήγουμε σε άτοπο. Επομένως, δε μπορούν να υπάρχουν άκέραιοι b, c που ικανοποιούν τις υποθέσεις της Πρότασης για τους οποίους $bc(b^2 - 3bc + 3c^2)$ να είναι τετράγωνο > 1.
Επειδή $bc(b^2 - 3bc + 3c^2) > 0$ έχουμε είτε $b, c > 0$, είτε $b, c < 0$. Υποθέτουμε ότι $b, c > 0$. Επίσης οι τρεις παράγοντες στο γινόμενο $bc(b^2 - 3bc + 3c^2)$ είναι ανά δύο πρώτοι μεταξύ τους, αφού $\gcd(b, c) = 1$ και $b \not\equiv 0 \pmod 3$.
Επομένως

$$b = x^2 \tag{1.1}$$

$$c = y^2 \tag{1.2}$$

$$b^2 - 3bc + 3c^2 = z^2, \tag{1.3}$$

όπου x, y, z είναι ακέραιοι. Επιλέγουμε $x, y, z > 0$.
Όμως $b^2 - 3bc + 3c^2 = N(b + c\frac{-3+\sqrt{-3}}{2})$. Άρα $N(b + c\frac{-3+\sqrt{-3}}{2}) = z^2$. Από το Λήμμα 1.2.1 έπεται ότι

$$b + c\frac{-3+\sqrt{-3}}{2} = (\ell + n\frac{-3+\sqrt{-3}}{2})^2 k, \tag{1.4}$$

όπου ℓ, n, k είναι ακέραιοι.
Επιλέγουμε $\ell > 0$. Από τη σχέση (1.4) βρίσκουμε ότι

$$b = k(\ell^2 - 3n^2) \tag{1.5}$$
$$c = k(2\ell n - 3n^2). \tag{1.6}$$

Επειδή $\gcd(b, c) = 1$ έχουμε $k = \pm 1$. Θα δείξουμε ότι $\gcd(\ell, n) = 1$. Πράγματι, αν $d := \gcd(\ell, n) > 1$ και p' είναι ένας πρώτος που διαιρεί το d, τότε $p' \mid \ell^2 - 3n^2$ και $p' \mid 2\ell n - 3n^2$, δηλαδή $p' \mid b$ και $p' \mid c$, το οποίο είναι άτοπο διότι $\gcd(b, c) = 1$. Άρα $\gcd(\ell, n) = 1$.
Θα δείξουμε ότι $k = 1$, δηλαδή θα απορρίψουμε την περίπτωση $k = -1$. Πράγματι, αν $k = -1$, τότε από τις σχέσεις (1.1) και (1.5) έχουμε $3n^2 = \ell^2 + x^2$.
Όμως $\ell^2 + x^2 \equiv 0$ ή 1 ή $2 \pmod 4$ και $3n^2 \equiv 0$ ή $3 \pmod 4$. Οπότε από τη σχέση $3n^2 = \ell^2 + x^2$ έπεται ότι $\ell^2 \equiv 0 \pmod 4$, $x^2 \equiv 0 \pmod 4$ και $n^2 \equiv 0 \pmod 4$, το οποίο είναι άτοπο διότι $\gcd(\ell, n) = 1$. Άρα $k = 1$ και από τη σχέση (1.6) έχουμε $n > 0$, αφού $\ell > 0$ και $c = y^2$.
Επομένως

$$b = \ell^2 - 3n^2 \tag{1.7}$$
$$c = 2\ell n - 3n^2, \tag{1.8}$$

όπου ℓ, n είναι θετικοί ακέραιοι.
Από τις σχέσεις (1.7) και (1.1) έχουμε $x^2 + 3n^2 = \ell^2$, δηλαδή $N(x + \sqrt{-3}n) = \ell^2$. Από το Λήμμα 1.2.1 έπεται ότι

$$x + \sqrt{-3}n = m(\frac{s + t\sqrt{-3}}{2})^2, \tag{1.9}$$

όπου s, t, m είναι ακέραιοι και $t \equiv s \pmod 2$. Πράγματι, αν $\frac{s+t\sqrt{-3}}{2} = s' + t'\frac{1+i\sqrt{3}}{2}$, όπου s', t' είναι ακέραιοι, τότε $s = 2s' + t$, δηλαδή $t \equiv s \pmod 2$. Επιλέγουμε $s > 0$. Από τη σχέση (1.9) βρίσκουμε ότι

$$x = \frac{s^2 - 3t^2}{4} m \tag{1.10}$$
$$n = \frac{st}{2} m. \tag{1.11}$$

Επειδή $n, s > 0$ από τη σχέση (1.11) έπεται ότι οι t, m έχουν το ίδιο πρόσημο.
Θα δείξουμε ότι $\gcd(x, n) = 1$. Πράγματι, αν $d := \gcd(x, n) > 1$ και p' είναι ένας πρώτος

που διαιρεί το d, τότε $p' \mid x$ και $p' \mid n$, δηλαδή $p' \mid x^2$ και $p' \mid 3n^2$. Οπότε $p' \mid x^2+3n^2 = \ell^2$, το οποίο είναι άτοπο διότι $\gcd(\ell, n) = 1$. Άρα $\gcd(x, n) = 1$.
Επίσης $m \mid 2$. Πράγματι, από τις σχέσεις (1.10) και (1.11) έχουμε $m \mid 4x$ και $m \mid 4n$. Όμως $\gcd(4x, 4n) = 4\gcd(x, n) = 4$. Άρα $m \mid 4$. Αν $m = \pm 4$, τότε από τις σχέσεις (1.10) και (1.11) και επειδή $t \equiv s \pmod 2$, έχουμε $n \equiv 0 \pmod 2$ και $x \equiv 0 \pmod 2$. Αυτό όμως είναι άτοπο διότι $\gcd(x, n) = 1$. Άρα $m \mid 2$.
Από τη σχέση $x^2 + 3n^2 = \ell^2$, λόγω των σχέσεων (1.10) και (1.11), έχουμε

$$\ell = \frac{s^2 + 3t^2}{4}|m|, \tag{1.12}$$

αφού $\ell > 0$.
Από τη σχέση (1.8), λόγω των σχέσεων (1.11) και (1.12), έχουμε

$$(\frac{2y}{m})^2 = \frac{4c}{m^2} = s|t|(s^2 - 3s|t| + 3|t|^2), \tag{1.13}$$

δηλαδή $s|t|(s^2 - 3s|t| + 3|t|^2)$ είναι τετράγωνο ακεραίου.
Έχουμε κατασκευάσει ένα καινούριο ζευγάρι ακεραίων $(s, |t|)$. Θα αποδείξουμε ότι οι ακέραιοι $s, |t|$ ικανοποιούν τις υποθέσεις της Πρότασης και ότι $s|t|(s^2 - 3s|t| + 3|t|^2)$ είναι τετράγωνο > 1.
Πράγματι, αν $s = 0$ ή $t = 0$, τότε από τις σχέσεις (1.11) και (1.8) έχουμε $c = 0$, το οποίο είναι άτοπο. Άρα $st \neq 0$.
Αν $3 \mid s$, τότε $3 \mid s^2 - 3t^2$. Από τη σχέση (1.10) έπεται ότι $3 \mid 4x$, δηλαδή $3 \mid x$. Συνεπώς $3 \mid x^2 = b$, το οποίο είναι άτοπο διότι $b \not\equiv 0 \pmod 3$. Άρα $c \not\equiv 0 \pmod 3$.
Αν $d := \gcd(s, |t|)$, τότε από τις σχέσεις (1.10) και (1.11) και επειδή $\gcd(x, n) = 1$ έχουμε $d \mid 4$. Αν $d = \pm 4$, τότε υπάρχουν ακέραιοι κ,λ τέτοιοι ώστε $s = \pm 4\kappa$ και $|t| = \pm 4\lambda$. Από τις σχέσεις (1.10) και (1.11) προκύπτει ότι $x = 4(\kappa^2 - 3\lambda^2)m$ και $n = 8\kappa\lambda m$, το οποίο είναι άτοπο διότι $\gcd(x, n) = 1$. Αν $d = \pm 2$, τότε υπάρχουν ακέραιοι s', t' τέτοιοι ώστε $s = \pm 2s'$ και $|t| = \pm 2t'$. Η σχέση (1.9) γράφεται: $x + \sqrt{-3}n = 4m(\frac{s' + t'\sqrt{-3}}{2})^2 = m'(\frac{s' + t'\sqrt{-3}}{2})^2$, όπου $m' = 4m$ και $s' \equiv t' \pmod 2$. Άρα $x = \frac{s'^2 - 3t'^2}{4}m' = (s'^2 - 3t'^2)m$ και $n = \frac{s't'}{2}m' = 2s't'm$. Επίσης $m' \mid 2$ και $\gcd(s', t') = 1$. Επομένως, μπορούμε να επιλέξουμε τους $s, |t|$ έτσι ώστε $\gcd(s, |t|) = 1$.
Θα δείξουμε ότι $s|t|(s^2 - 3s|t| + 3|t|^2)$ είναι τετράγωνο > 1. Από τη σχέση (1.13) ο αριθμός $s|t|(s^2 - 3s|t| + 3|t|^2)$ είναι τετράγωνο. Επίσης $s|t|(s^2 - 3s|t| + 3|t|^2) \neq 0$. Πράγματι, $s^2 - 3s|t| + 3|t|^2 > 0$. Έτσι, αν $s|t|(s^2 - 3s|t| + 3|t|^2) = 0$, τότε $s = 0$ ή $t = 0$, το οποίο είναι άτοπο. Αν $s|t|(s^2 - 3s|t| + 3|t|^2) = 1$, τότε $s = |t| = 1$ και από τη σχέση (1.10) έχουμε $x = -\frac{1}{2}m$. Επειδή ο x είναι θετικός ακέραιος και $m \mid 2$ έπεται ότι $m = -2$. Οι m, t έχουν το ίδιο πρόσημο και συνεπώς $t = -1$. Οπότε από τις σχέσεις (1.11) και (1.12) έχουμε $n = 1$ και $\ell = 2$, Άρα, από τις σχέσεις (1.7) και (1.8) προκύπτει ότι $b = c = 1$, δηλαδή $bc(b^2 - 3bc + 3c^2) = 1$, το οποίο είναι άτοπο. Επομένως $s|t|(s^2 - 3s|t| + 3|t|^2)$ είναι τετράγωνο > 1.
Για την ολοκλήρωση της απόδειξης της Πρότασης μένει να δείξουμε ότι

$$s|t|(s^2 - 3s|t| + 3|t|^2) < bc(b^2 - 3bc + 3c^2).$$

Από τη σχέση (1.13) αρκεί να δείξουμε ότι $b(b^2-3bc+3c^2) > 4$, αφού $b, c > 0$ και $|m| \geq 1$. Αν υποθέσουμε ότι $b(b^2 - 3bc + 3c^2) \leq 4$, τότε έχουμε $b = 1$ ή $b = 4$, αφού $b = x^2$. Αν $b = 1$, τότε $3c^2 - 3c + 1 \leq 4$. Επειδή $c > 0$ έπεται ότι $c = 0$ ή $c = 1$, το οποίο είναι άτοπο διότι $bc(b^2 - 3bc + 3c^2) > 1$. Αν $b = 4$, τότε $3c^2 - 12c + 16 \leq 1$. Όμως η ανισότητα αυτή δεν έχει λύση στους πραγματικούς αριθμούς και συνεπώς καταλήγουμε σε άτοπο. Άρα $s|t|(s^2 - 3s|t| + 3|t|^2) < bc(b^2 - 3bc + 3c^2)$.

□

Θεώρημα 1.2.1

Οι ρητές λύσεις της εξίσωσης $X^2 - Y^3 = 1$ *είναι οι* $(x, y) = (0, -1), (\pm 1, 0)$ *και* $(\pm 3, 2)$. *Ειδικότερα, οι ακέραιες λύσεις της εξίσωσης* $X^2 - Y^3 = 1$ *με* $xy \neq 0$ *είναι οι* $(x, y) = (\pm 3, 2)$.

Απόδειξη:

Υποθέτουμε ότι (x, y) είναι μία ρητή λύση της εξίσωσης.
Αν θέσουμε $u = y + 1$, τότε η εξίσωση γράφεται:

$$x^2 = u^3 - 3u^2 + 3u. \tag{1.14}$$

Αν $u = \frac{b}{c}$, όπου οι b, c είναι ακέραιοι με $c \neq 0$ και $\gcd(b, c) = 1$, τότε από τη σχέση (1.14) έχουμε $(c^2x)^2 = bc(b^2 - 3bc + 3c^2)$, δηλαδή ο $s := bc(b^2 - 3bc + 3c^2)$ είναι τετράγωνο ακεραίου.
Αν $s = 0$, τότε $b = 0$ αφού $b^2 - 3bc + 3c^2 > 0$ και $c \neq 0$. Οπότε $u = 0$, δηλαδή $(x, y) = (0, -1)$.
Αν $s = 1$, τότε $b = c = \pm 1$, δηλαδή $u = 1$. Επομένως $(x, y) = (\pm 1, 0)$.
Αν $s \geq 2$, τότε από την Πρόταση 1.2.1 έπεται ότι $3 \mid b$. Αν $\beta := \frac{b}{3}$, τότε $\gcd(\beta, c) = 1$ και ο αριθμός $\frac{s}{9} = \beta c(3\beta^2 - 3\beta c + c^2)$ είναι τετράγωνο ακεραίου. Επειδή $s \geq 2$ έχουμε $s \neq 0$. Αν $s = 9$, τότε $\beta = c = \pm 1$, δηλαδή $u = 3$. Επομένως $(x, y) = (\pm 3, 2)$. Αν $s \geq 18$, τότε από την Πρόταση 1.2.1 έπεται ότι $3 \mid c$, το οποίο είναι άτοπο διότι $3 \mid b$ και $\gcd(b, c) = 1$.

□

1.3 Η εξίσωση του Catalan για p = 3 και q = 2

Θεώρημα 1.3.1

Η εξίσωση $X^3 = Y^2 + 1$ *δεν έχει ακέραια λύση* (x, y) *με* $xy \neq 0$.

Απόδειξη:

Υποθέτουμε ότι (x, y) είναι μία ακέραια λύση της εξίσωσης με $xy \neq 0$.
Η δοθείσα εξίσωση γράφεται: $x^3 = (y + i)(y - i)$, όπου $y + i, y - i$ είναι στοιχεία του δακτυλίου $\mathbb{Z}[i]$. Ο $\mathbb{Z}[i]$ είναι δακτύλιος μονοσήμαντης ανάλυσης με ομάδα των μονάδων $E(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$. Παρατηρούμε ότι $2 = (-i)(1 + i)^2$, όπου το $1 + i$ είναι ανάγωγο στοιχείο του $\mathbb{Z}[i]$. Πράγματι, αν $1 + i = (a + bi)(c + di)$, όπου $a + bi, c + di$ είναι στοιχεία του $\mathbb{Z}[i]$, τότε $2 = N(1+i) = N(a+bi)N(c+di)$, δηλαδή $N(a+bi) = \pm 1$ ή $N(c+di) = \pm 1$. Συνεπώς, είτε το $a + bi$ είναι μονάδα του δακτυλίου, είτε το $c + di$ είναι μονάδα αυτού.

Άρα, το $1+i$ είναι ανάγωγο στοιχείο του $\mathbb{Z}[i]$.
Αν $d := \gcd(y+i, y-i)$, τότε $d \mid 2$. Ισχυριζόμαστε ότι $d \cong 1$ (κατά προσέγγιση μονάδας). Πράγματι, αν $d \ncong 1$, τότε $1+i \mid d \mid y+i$, δηλαδή $N(1+i) \mid N(y+i)$. Από την τελευταία σχέση έπεται ότι $2 \mid y^2+1 = x^3$, δηλαδή $2 \mid x$ και άρα $2^3 \mid x^3 = y^2+1$. Έτσι, $y^2 \equiv -1 \pmod 8$, το οποίο είναι αδύνατο. Άρα $d \cong 1$.
Οπότε υπάρχει z στον $\mathbb{Z}[i]$ τ.ω. $y+i = \varepsilon z^3$, όπου ε είναι μία μονάδα του $\mathbb{Z}[i]$. Επειδή το 3 και η τάξη της ομάδας των μονάδων του $\mathbb{Z}[i]$ είναι πρώτοι μεταξύ τους έπεται ότι κάθε μονάδα ε του $\mathbb{Z}[i]$ γράφεται ως τρίτη δύναμη μιας μονάδας ε′ του $\mathbb{Z}[i]$, δηλαδή $y+i = h^3$, όπου $h = a+bi$ είναι στοιχείο του $\mathbb{Z}[i]$. Άρα $y+i = (a^3-3ab^2) + i(3a^2b-b^3)$, δηλαδή $(3a^2-b^2)b = 1$ και συνεπώς $b = \pm 1$. Επομένως $3a^2-1 = \pm 1$, δηλαδή $a = 0$. Οπότε $y = 0$, το οποίο είναι άτοπο.

□

1.4 Η εξίσωση του Catalan για p = 2 και q > 3

Λήμμα 1.4.1

Αν q είναι ένας περιττός πρώτος και $\gcd(x,y) = 1$, τότε $\gcd\Big(x+y, \frac{x^q+y^q}{x+y}\Big) = 1$ ή q.

Απόδειξη:
Έχουμε

$$\begin{aligned}
x^{q-1} &= (x+y)x^{q-2} - x^{q-2}y \\
-x^{q-2}y &= (x+y)(-x^{q-3}y) + x^{q-3}y^2 \\
x^{q-3}y^2 &= (x+y)(x^{q-4}y^2) - x^{q-4}y^3 \\
&\vdots \\
-xy^{q-2} &= (x+y)(-y^{q-2}) + y^{q-1}.
\end{aligned}$$

Επομένως

$$\begin{aligned}
-xy^{q-2} &\equiv y^{q-1} \Big(\mathrm{mod}\ (x+y)\Big) \\
&\vdots \\
x^{q-3}y^2 &\equiv y^{q-1} \Big(\mathrm{mod}\ (x+y)\Big) \\
-x^{q-2}y &\equiv y^{q-1} \Big(\mathrm{mod}\ (x+y)\Big) \\
x^{q-1} &\equiv y^{q-1} \Big(\mathrm{mod}\ (x+y)\Big).
\end{aligned}$$

Οπότε

$$\frac{x^q+y^q}{x+y} = x^{q-1} - x^{q-2}y + x^{q-3}y^2 - \ldots - xy^{q-2} + y^{q-1} \equiv qy^{q-1} \Big(\mathrm{mod}\ (x+y)\Big).$$

Από την τελευταία ισοδυναμία έπεται ότι $d := \gcd\Big(x+y, \frac{x^q+y^q}{x+y}\Big) \mid qy^{q-1}$.
Όμως $\gcd(d, y^{q-1}) = 1$, αφού $\gcd(x,y) = 1$. Άρα $d \mid q$. Συνεπώς

$$d := \gcd\Big(x+y, \frac{x^q+y^q}{x+y}\Big) = 1 \text{ ή } q.$$

□

Λήμμα 1.4.2
Αν $x^2 = y^q + 1$, όπου q είναι ένας πρώτος και $x > 1$, τότε $2 \mid y$ και $q \mid x$.

Απόδειξη:
Καταρχήν η δοθείσα εξίσωση γράφεται: $y^q = (x-1)(x+1)$. Υποθέτουμε ότι $2 \nmid y$.
Αν $d := \gcd(x-1, x+1)$, τότε $d \mid 2$. Όμως $d \neq 2$ διότι $2 \nmid y$. Άρα $\gcd(x-1, x+1) = 1$.
Συνεπώς, υπάρχουν ακέραιοι a, b τ.ω $x-1 = a^q$ και $x+1 = b^q$, δηλαδή $b^q - a^q = 2$, το οποίο είναι αδύνατο, εκτός εάν $b = 1$ και $a = -1$. Τότε όμως, αφού $ab = y$, θα είχαμε $y = -1$, δηλαδή $x = 0$, το οποίο είναι άτοπο. Άρα $2 \mid y$.
Επομένως, υπάρχουν ακέραιοι a, b τ.ω. $x \mp 1 = 2a^q$ και $x \pm 1 = 2^{q-1}b^q$. Αν αφαιρέσουμε αυτές τις σχέσεις κατά μέλη παίρνουμε

$$2^{q-2}b^q - a^q = \pm 1. \tag{1.15}$$

Υποθέτουμε ότι $q \nmid x$. Η εξίσωση γράφεται: $(y+1)(\frac{y^q+1}{y+1}) = x^2$. Επειδή $q \nmid x$ από το Λήμμα 1.4.1 έχουμε $\gcd\Big(y+1, \frac{y^q+1}{y+1}\Big) = 1$.
Οπότε υπάρχουν ακέραιοι c, d τ.ω.

$$\frac{y^q+1}{y+1} = c^2 \tag{1.16}$$

$$y+1 = d^2. \tag{1.17}$$

Η εξίσωση (1.16) είναι αδύνατη (δες [30]) για $|y| > 2^{q-3}$.
Επειδή $2 \nmid a$ και $\gcd\Big(\frac{a^q \pm 1}{a \pm 1}, a \pm 1\Big) = 1$ ή q ο αριθμός $\frac{a^q \pm 1}{a \pm 1}$ είναι περιττός. Επομένως, ο $\frac{2^{q-2}b^q}{a\pm 1} = \frac{a^q \pm 1}{a \pm 1}$ είναι περιττός και συνεπώς $a \pm 1 \geq 2^{q-2}$, δηλαδή $a \geq 2^{q-2} \mp 1 \geq 2^{q-2} - 1$.
Άρα $y = 2ab \geq 2(2^{q-2} - 1) = 2^{q-1} - 2 > 2^{q-3}$ και καταλήγουμε σε άτοπο. Συνεπώς $q \mid x$.
□

Λήμμα 1.4.3 (Πυθαγόρειες τριάδες)
Οι θετικές ακέραιες λύσεις της εξίσωσης $X^2 + Y^2 = Z^2$, όπου ο Y είναι άρτιος, $\gcd(X,Y) = 1$ και $XYZ \neq 0$, είναι

$$x = a^2 - b^2,\ y = 2ab,\ z = a^2 + b^2\ (a > b).$$

Απόδειξη:
Έστω (x, y, z) μία λύση της εξίσωσης $X^2 + Y^2 = Z^2$. Επειδή $\gcd(x,y) = 1$ έχουμε $\gcd(x,z) = 1$ και $\gcd(z,y) = 1$. Επομένως, οι x, z είναι περιττοί.

Η δοθείσα εξίσωση γράφεται: $x^2 = (z-y)(z+y)$. Αν $d := \gcd(z-y, z+y)$, τότε $d \mid 2$. Όμως οι $z+y,\ z-y$ είναι περιττοί. Συνεπώς $d = 1$.
Άρα, $z+y = A^2,\ z-y = B^2$ και $x = AB$, όπου οι A, B είναι περιττοί και $\gcd(A,B) = 1$. Συνεπώς, $z = \frac{A^2+B^2}{2}$ και $y = \frac{A^2-B^2}{2}$.
Αν θέσουμε $A = a+b$ και $B = a-b$, τότε ο ένας εκ των a, b είναι άρτιος και ο άλλος περιττός και $\gcd(a,b) = 1$. Επομένως

$$x = a^2 - b^2,\ y = 2ab,\ z = a^2 + b^2\ (a > b).$$

□

Θεώρημα 1.4.1

Έστω q ένας πρώτος > 3. Η εξίσωση $X^2 = Y^q + 1$ δεν έχει λύση στους φυσικούς αριθμούς.

Απόδειξη:

Ας υποθέσουμε ότι υπάρχουν φυσικοί αριθμοί x, y και πρώτος $q > 3$ τέτοιοι ώστε $x^2 = y^q + 1$.
Από το Λήμμα 1.4.2 έχουμε $2 \mid y$ και $q \mid x$.
Παρατηρούμε ότι $2 \nmid x$ διότι αν $2 \mid x$, τότε ο y θα ήταν περιττός, το οποίο είναι άτοπο. Άρα $\gcd(x+1, x-1) = 2$. Συνεπώς, ξεχωρίζουμε δύο περιπτώσεις:

$$1)\ x+1 = 2^{q-1}y_1^q,\ x-1 = 2y_2^q,$$

$$2)\ x+1 = 2y_2^q,\ x-1 = 2^{q-1}y_1^q,$$

όπου $y = 2y_1y_2, \gcd(y_1, y_2) = 1$ και $2 \nmid y_2$.
Περίπτωση 1: Υποθέτουμε ότι $x+1 = 2^{q-1}y_1^q$ και $x-1 = 2y_2^q$. Αφαιρώντας τις δύο αυτές σχέσεις κατά μέλη έχουμε $y_2^q = 2^{q-2}y_1^q - 1$, από την οποία προκύπτει ότι

$$(y_2^2)^q + (2y_1)^q = (y_2^q + 2)^q = (\frac{x+3}{2})^2. \tag{1.18}$$

Επειδή $q \mid x$ και $q > 3$ έχουμε $q \nmid \frac{x+3}{2}$. Από τη σχέση (1.18) έχουμε

$$(\frac{x+3}{2})^2 = (y_2^2 + 2y_1)\Big[\frac{(y_2^2)^q + (2y_1)^q}{y_2^2 + 2y_1}\Big]. \tag{1.19}$$

Επίσης $d := \gcd(y_2^2, 2y_1) = 1$. Πράγματι, αν είναι $d > 1$, τότε υπάρχει πρώτος p' που διαιρεί το d και συνεπώς $p' \mid y_2^2$, δηλαδή $p' \mid y_2$ (προφανώς $p' \neq 2$, αφού $2 \nmid y_2$). Ακόμα $p' \mid 2y_1$, δηλαδή $p' \mid y_1$. Αυτό όμως είναι άτοπο διότι $\gcd(y_1, y_2) = 1$.
Επομένως, από το Λήμμα 1.4.1 έχουμε $d' := \gcd\Big(y_2^2 + 2y_1, \frac{(y_2^2)^q + (2y_1)^q}{y_2^2 + 2y_1}\Big) = 1$ ή q.
Επειδή $d' \mid (y_2^2 + 2y_1) \mid (\frac{x+3}{2})^2$ και $q \nmid \frac{x+3}{2}$ έπεται ότι $d' = 1$.
Άρα, από τη σχέση (1.19) έχουμε $y_2^2 + 2y_1 = h^2$, όπου $h \mid \frac{x+3}{2}$. Πολλαπλασιάζοντας τη σχέση αυτή με y_2^2 προκύπτει η σχέση

$$(hy_2)^2 + y_1^2 = (y_2^2 + y_1)^2. \tag{1.20}$$

Επειδή $\gcd(y_1, y_2) = 1$ έχουμε $\gcd(hy_2, y_1) = 1$. Επίσης ο h είναι περιττός, αφού ο y_2 είναι περιττός. Πράγματι, αν h άρτιος, τότε h^2 άρτιος και y_2^2 περιττός, δηλαδή $2y_1$ περιττός, το οποίο είναι αδύνατο. Άρα, αν h =2κ+1 και y_2 =2λ+1, όπου κ,λ είναι ακέραιοι, τότε $4 \mid (h^2 - y_2^2)$, δηλαδή $2 \mid y_1$.
Οπότε από το Λήμμα 1.4.3 οι λύσεις της (1.20) είναι

$$hy_2 = a^2 - b^2,\ y_1 = 2ab,\ y_2^2 + y_1 = a^2 + b^2\ (a > b).$$

Επομένως, $(a-b)^2 = (y_2^2 + y_1) - y_1 = y_2^2$, το οποίο δίνει $y_2 = a - b$.
Άρα $y_1 - y_2 = 2ab - (a-b) = a(2b-1) + b > 0$, δηλαδή $y_1 > y_2$. Όμως $y_2^q = 2^{q-2}y_1^q - 1 > y_1^q$, δηλαδή $y_2 > y_1$ και συνεπώς καταλήγουμε σε άτοπο. Έτσι ολοκληρώνεται η περίπτωση 1.
Περίπτωση 2: Υποθέτουμε ότι $x + 1 = 2y_2^q,\ x - 1 = 2^{q-1}y_1^q$. Όπως και στην περίπτωση 1, έχουμε $(y_2^2)^q - (2y_1)^q = (y_2^q - 2)^q = (\frac{x-3}{2})^2$ και συνεπώς $y_2^2 - 2y_1 = h^2$, όπου $h \mid \frac{x-3}{2}$. Επομένως $(hy_2)^2 + y_1^2 = (y_2^2 - y_1)^2$. Από το Λήμμα 1.4.3 έπεται ότι

$$hy_2 = a^2 - b^2,\ y_1 = 2ab,\ y_2^2 - y_1 = a^2 + b^2\ (a > b).$$

Έτσι $y_1 - y_2 = 2ab - (a+b) = (a-1)(b-1) + (ab-1) > 0$, δηλαδή $y_1 > y_2$. Όμως $y_2^q = 2^{q-2}y_1^q + 1 > y_1^q$, δηλαδή $y_2 > y_1$ και συνεπώς καταλήγουμε σε άτοπο. Έτσι ολοκληρώνεται και η περίπτωση 2.

□

1.5 Η εξίσωση του Catalan για q = 2 και p > 3

Θεώρημα 1.5.1

Έστω p ένας πρώτος > 3. Η εξίσωση $X^p = Y^2 + 1$ δεν έχει ακέραια λύση (x, y) με $xy \neq 0$.

Απόδειξη:

Υποθέτουμε ότι (x, y) είναι μία ακέραια λύση της εξίσωσης με $xy \neq 0$.
Αν ο x ήταν άρτιος, τότε $x^p \equiv 0 \pmod 8$, δηλαδή $y^2 = x^p - 1 \equiv 7 \pmod 8$, το οποίο δεν ισχύει. Άρα, ο x είναι περιττός και συνεπώς ο y θα είναι άρτιος.
Η δοθείσα εξίσωση γράφεται: $x^p = (1 + yi)(1 - yi)$ στο δακτύλιο των ακεραίων $\mathbb{Z}[i]$. Ο $\mathbb{Z}[i]$ είναι δακτύλιος μονοσήμαντης ανάλυσης με ομάδα των μονάδων $E(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$. Αν $d := \gcd(1 + yi, 1 - yi)$, τότε $d \mid 2$. Όμως $2 = (-i)(1+i)^2$, όπου $1 + i$ είναι ανάγωγο στοιχείο του $\mathbb{Z}[i]$. Άρα, αν $d \ncong 1$, τότε $1 + i \mid d \mid 1 + yi$, δηλαδή $2 \mid 1 + y^2 = x^p$. Αυτό όμως είναι άτοπο. Επομένως $d = \gcd(1 + yi, 1 - yi) \cong 1$. Επειδή το p και η τάξη της ομάδας των μονάδων του $\mathbb{Z}[i]$ είναι πρώτοι μεταξύ τους έχουμε

$$\begin{aligned} 1 + yi &= a^p \\ 1 - yi &= \overline{a}^p, \end{aligned}$$

για κάποιο a στον $\mathbb{Z}[i]$. Προσθέτοντας τις δύο αυτές σχέσεις έχουμε

$$2 = a^p + \overline{a}^p = (a + \overline{a})(a^{p-1} - a^{p-2}\overline{a} + \ldots + \overline{a}^{p-1}).$$

Επειδή $x = a\overline{a}$ και x περιττός έπεται ότι οι $a, \overline{a}$ είναι περιττοί στον $\mathbb{Z}[i]$. Άρα, ο δεύτερος παράγοντας στο γινόμενο είναι ένα αλγεβρικό άθροισμα p περιττών όρων, δηλαδή θα είναι και ο ίδιος περιττός στον $\mathbb{Z}[i]$. Επομένως $a + \overline{a} = \pm 2$. Αν $a = b + ui$ και $\overline{a} = b - ui$, όπου b, u είναι ακέραιοι, τότε $a = \pm(1 \pm ui)$. Επίσης ο u είναι άρτιος διότι ο $x = u^2 + 1$ είναι περιττός. Παίρνουμε

$$(1 + ui)^p + (1 - ui)^p = \pm 2.$$

Κοιτάζοντας την παραπάνω εξίσωση (mod 8) και επειδή ο u είναι άρτιος έχουμε

$$(1 + ui)^p + (1 - ui)^p = 2 + 2\binom{p}{2}(ui)^2 + 2\binom{p}{4}(ui)^4 + \ldots + 2\binom{p}{p-1}(ui)^{p-1} = 2.$$

Αν $u \neq 0$, διαιρούμε με $2u^2$ και έχουμε

$$\binom{p}{2} + \binom{p}{4}(ui)^2 + \ldots + \binom{p}{p-1}(ui)^{p-3} = 0. \tag{1.21}$$

Όμως

$$\mathrm{ord}_2\Big(\binom{p}{k}(ui)^{k-2}\Big) > \mathrm{ord}_2\binom{p}{2}, \tag{1.22}$$

για όλα τα άρτια $k \geq 4$.
Πράγματι,

$$\binom{p}{k}\binom{p}{2}^{-1}(ui)^{k-2} = \binom{p-2}{k-2}\frac{2}{k(k-1)}(ui)^{k-2}.$$

Άρα, αρκεί να δείξουμε ότι $\mathrm{ord}_2\Big(\binom{p-2}{k-2}\frac{2}{k(k-1)}(ui)^{k-2}\Big) > 0$.
Έχουμε $\mathrm{ord}_2\Big(2(ui)^{k-2}\Big) \geq k - 1 > \frac{\log k}{\log 2} \geq \mathrm{ord}_2(k) = \mathrm{ord}_2\Big(k(k-1)\Big)$, για όλα τα άρτια $k \geq 4$.
Επομένως

$$\mathrm{ord}_2\Big(\binom{p-2}{k-2}\frac{2}{k(k-1)}(ui)^{k-2}\Big) = \mathrm{ord}_2\Big(\binom{p-2}{k-2}\Big) - \mathrm{ord}_2\Big(k(k-1)\Big) + \mathrm{ord}_2\Big(2(ui)^{k-2}\Big) > 0,$$

δηλαδή αποδείξαμε την αλήθεια της (1.22).
Η σχέση (1.21) δε μπορεί να ισχύει. Πράγματι, αν η σχέση (1.21) ισχύει και

$$t = \mathrm{ord}_2\Big(\binom{p}{2}\Big),\ t_4 = \mathrm{ord}_2\Big(\binom{p}{4}(ui)^2\Big), \ldots,\ t_{p-1} = \mathrm{ord}_2\Big(\binom{p}{p-1}(ui)^{p-3}\Big),$$

δηλαδή $\binom{p}{2} = 2^t s$, $\binom{p}{4}(ui)^2 = 2^{t_4}s_4, \ldots, \binom{p}{p-1}(ui)^{p-3} = 2^{t_{p-1}}s_{p-1}$, τότε

$$2^t s + 2^{t_4}s_4 + \ldots + 2^{t_{p-1}}s_{p-1} = 0. \tag{1.23}$$

Όμως από τη σχέση (1.22) έχουμε $t < t_4, \ldots, t < t_{p-1}$. Επομένως, από τη σχέση (1.23) έπεται ότι $2 \mid s$, το οποίο είναι άτοπο διότι ο s είναι περιττός.
Άρα, $u = 0$, δηλαδή $y = 0$ και καταλήγουμε σε άτοπο.

□

1.6 Οι σχέσεις του Cassels

Στη συνέχεια θα αποδείξουμε το ακόλουθο Θεώρημα:

Θεώρημα 1.6.1
Έστω p, q πρώτοι αριθμοί με $p > q > 2$. Αν $x^p - y^q = \pm 1$, όπου οι x, y είναι ακέραιοι με $x > 1$ και $y > 1$, τότε $q \mid x$ και $p \mid y$.

Λήμμα 1.6.1
Αν p είναι ένας πρώτος > 2 και $a \neq \mp 1$ είναι ένας ακέραιος, τότε

$$\gcd\Big(\frac{a^p \pm 1}{a \pm 1}, a \pm 1\Big) = 1 \text{ ή } p. \tag{1.24}$$

Αν ο gcd *είναι p, τότε*

$$\frac{a^p \pm 1}{a \pm 1} \equiv p \pmod{p^2}. \tag{1.25}$$

Απόδειξη:
Από το γνωστό διωνυμικό τύπο, για κάθε $k = 1, 2, \ldots, p-1$, έχουμε

$$a^{p-k} = \Big[(a \pm 1) \mp 1\Big]^{p-k} = \sum_{i=0}^{p-k} \binom{p-k}{i} (a \pm 1)^i (\mp 1)^{p-k-i}.$$

Επομένως

$$a^{p-k} \equiv \binom{p-k}{0} (\mp 1)^{p-k} \Big(\mod (a \pm 1)\Big),$$

για κάθε $k = 1, 2, \ldots, p-1$.
Οπότε

$$\begin{aligned} \frac{a^p \pm 1}{a \pm 1} &= a^{p-1} \mp a^{p-2} + a^{p-3} \mp \ldots \mp a + 1 \\ &\equiv 1 + 1 + 1 + \ldots + 1 \Big(\mod (a \pm 1)\Big) \\ &\equiv p \Big(\mod (a \pm 1)\Big). \end{aligned} \tag{1.26}$$

Από την τελευταία ισοδυναμία έπεται ότι $\gcd\Big(\frac{a^p \pm 1}{a \pm 1}, a \pm 1\Big) = 1$ ή p.
Αν υποθέσουμε ότι $p \mid (a \pm 1)$, δηλαδή

$$a \pm 1 = p^j d \qquad (j \geq 1), \tag{1.27}$$

τότε

$$\begin{aligned} a^p \pm 1 &= (\mp 1 + p^j d)^p \pm 1 \\ &= p^{j+1} d \mp \frac{1}{2} p(p-1)(p^j d)^2 + \frac{1}{6} p(p-1)(p-2)(p^j d)^3 \mp \ldots + (p^j d)^p \end{aligned} \tag{1.28}$$

Επομένως, από τις σχέσεις (1.27) και (1.28) έπεται ότι $\frac{a^p \pm 1}{a \pm 1} \equiv p \pmod{p^2}$.

□

Πόρισμα 1.6.1

Αν υποθέσουμε ότι $a \pm 1 \neq 0$ *και* $p^j | (a \pm 1)$, *τότε*

$$\frac{a^p \pm 1}{a \pm 1} \equiv p \pmod{p^{j+1}}, \tag{1.29}$$

ενώ

$$\frac{a^p \pm 1}{a \pm 1} \neq p. \tag{1.30}$$

Απόδειξη:

Η σχέση (1.29) είναι προφανής λόγω των σχέσεων (1.27) και (1.28).
Από τις σχέσεις (1.27) και (1.28) έχουμε

$$\frac{a^p \pm 1}{a \pm 1} = p \mp \binom{p}{2} p^j d + \binom{p}{3} p^{2j} d^2 \mp ... + p^{(p-1)j} d^{p-1},$$

δηλαδή το $\frac{a^p \pm 1}{a \pm 1} - p$ είναι αλγεβρικό άθροισμα $p-1$ όρων, όπου

$$\pm \binom{p}{2} p^j d < \binom{p}{3} p^{2j} d^2, ..., \pm \binom{p}{p-1} p^{(p-2)j} d^{p-2} < p^{(p-1)j} d^{p-1}.$$

Επομένως $\frac{a^p \pm 1}{a \pm 1} \neq p$.

□

Λήμμα 1.6.2

Έστω p, q *δύο πρώτοι με* $p > q > 2$. *Αν* $x^p - y^q = \pm 1$, *όπου οι* x, y *είναι ακέραιοι με* $x > 1$ *και* $y > 1$, *τότε* $q \mid (y \pm 1)$.

Απόδειξη:

Αν $q \not| (y \pm 1)$, τότε από το Λήμμα 1.6.1 για $a = y$ και q αντί p έχουμε

$$x^p = y^q \pm 1 = (y \pm 1)(\frac{y^q \pm 1}{y \pm 1}),$$

όπου

$$\gcd\Big(y \pm 1, \frac{y^q \pm 1}{y \pm 1}\Big) = 1.$$

Άρα

$$y \pm 1 = u^p,$$

για κάποιο ακέραιο $u > 1$ (Αν $u = 1$, τότε $y = 0$ ή $y = 2$. Όμως $y > 1$, άρα δε μπορεί να ισχύει $y = 0$. Επίσης ούτε η τιμή $y = 2$ είναι δεκτή αφού $x^p \geq 2^p > 2^q - 1$ και συνεπώς δεν ισχύει $x^p = 2^q - 1$).
Στη συνέχεια θα μελετήσουμε ξεχωριστά τις εξισώσεις $x^p - y^q = 1$ και $x^p - y^q = -1$.
1) Αν $x^p - y^q = 1$, τότε

$$x^p = y^q + 1 = (u^p - 1)^q + 1 < u^{pq}$$

και έτσι

$$x \leq u^q - 1.$$

Άρα έχουμε $x^p \leq (u^q - 1)^p$. Επαγωγικά ως προς n αποδεικνύεται ότι, αν $n > m$, τότε $(u^m - 1)^n < (u^n - 1)^m$, όπου $u > 1$. Συνεπώς $(u^q - 1)^p < (u^p - 1)^q$, αφού $p > q$. Οπότε

$$x^p \leq (u^q - 1)^p < (u^p - 1)^q = y^q, \tag{1.31}$$

το οποίο είναι άτοπο διότι $x^p = y^q + 1$.
2) Αν $x^p = y^q - 1$, τότε

$$x^p = y^q - 1 = (u^p + 1)^q - 1 > u^{pq}$$

και έτσι

$$x \geq u^q + 1.$$

Άρα έχουμε $x^p \geq (u^q + 1)^p$. Επαγωγικά ως προς n αποδεικνύεται ότι, αν $n > m$, τότε $(u^m + 1)^n > (u^n + 1)^m$, όπου $u > 1$. Συνεπώς $(u^q + 1)^p > (u^p + 1)^q$, αφού $p > q$. Οπότε

$$x^p \geq (u^q + 1)^p > (u^p + 1)^q = y^q, \tag{1.32}$$

το οποίο είναι άτοπο.
Επομένως $q \mid (y \pm 1)$.

□

Πρόταση 1.6.1

Αν υποθέσουμε ότι τα x, y, p, q ικανοποιούν τις υποθέσεις του Θεωρήματος 1.6.1, τότε υπάρχουν ακέραιοι u, v τ.ω

$$y \pm 1 = q^{p-1}u^p, \tag{1.33}$$

$$\frac{y^q \pm 1}{y \pm 1} = qv^p, \tag{1.34}$$

όπου

$$v \equiv 1 \pmod{q^{p-1}}, \tag{1.35}$$

$$v \neq 1. \tag{1.36}$$

Απόδειξη:

Από τα Λήμματα 1.6.1 και 1.6.2 έχουμε $x^p = (y \pm 1)(\frac{y^q \pm 1}{y \pm 1})$, όπου $\gcd\Big(y \pm 1, \frac{y^q \pm 1}{y \pm 1}\Big) = q$. Επομένως, υπάρχουν ακέραιοι u, v τ.ω.

$$y \pm 1 = q^k u^p$$

και

$$\frac{y^q \pm 1}{y \pm 1} = q^\ell v^p,$$

όπου $k = 1$ και $\ell = p - 1$ ή $k = p - 1$ και $\ell = 1$.
Από το Πόρισμα 1.6.1 (για $j = 1$) έχουμε $\frac{y^q \pm 1}{y \pm 1} \equiv q \pmod{q^2}$ και $\frac{y^q \pm 1}{y \pm 1} \neq q$. Επομένως $\frac{y^q \pm 1}{y \pm 1} = qv^p$ και $v \neq 1$. Οπότε $y \pm 1 = q^{p-1}u^p$.
Επειδή $q^{p-1} \mid (y \pm 1)$ έπεται ότι $\frac{y^q \pm 1}{y \pm 1} \equiv q \pmod{q^p}$.
Άρα

$$v^p \equiv 1 \pmod{q^{p-1}}. \tag{1.37}$$

Συνεπώς $\mathrm{ord}(v \mod q^{p-1}) \mid p$, δηλαδή $\mathrm{ord}(v \mod q^{p-1}) = 1$ ή p.
Όμως $\gcd(v, q^{p-1}) = 1$, δηλαδή $v^{q^{p-2}(q-1)} \equiv 1 \pmod{q^{p-1}}$. Αν $\mathrm{ord}(v \mod q^{p-1}) = p$, τότε θα πρέπει $p \mid (q-1)$, το οποίο είναι άτοπο διότι $p > q > q - 1$. Επομένως έχουμε $\mathrm{ord}(v \mod q^{p-1}) = 1$, δηλαδή $v \equiv 1 \pmod{q^{p-1}}$.

□

Πόρισμα 1.6.2
Έχουμε

$$x \equiv qu \pmod{q^{p-1}}, \tag{1.38}$$
$$x \neq qu. \tag{1.39}$$

Απόδειξη:
Από την Πρόταση 1.6.1 και επειδή $x^p = (y \pm 1)(\frac{y^q \pm 1}{y \pm 1})$ έχουμε $x = quv$. Από τις σχέσεις (1.35) και (1.36) έπεται ότι $x \equiv qu \pmod{q^{p-1}}$ και $x \neq qu$.

□

Λήμμα 1.6.3
Έστω $\nu = \frac{\alpha}{b}$ ένας ρητός αριθμός με $\gcd(\alpha, b) = 1$. Για κάθε μη-αρνητικό ακέραιο k υπάρχει θετικός ακέραιος N τέτοιος ώστε $b^N \binom{\nu}{k} \in \mathbb{Z}$.

Απόδειξη:
Ισχύει το εξής:
Αν $a, a - \omega, \ldots, a - (m-1)\omega$ είναι $m-$διαδοχικοί όροι μίας αριθμητικής προόδου και c τέτοιος ώστε $\gcd(c, \omega) = 1$, τότε

$$\mathrm{ord}_c\Big(a(a-\omega)\ldots(a-(m-1)\omega)\Big) \geq \Big[\frac{m}{c}\Big]. \tag{1.40}$$

Πράγματι, ας μετρήσουμε αρχικά πόσους παράγοντες διαιρεί ο c. Ο c διαιρεί παράγοντες της μορφής $a - \ell\omega$ $(\ell = 0, 1, \ldots, m-1)$ αν και μόνο αν $\omega\ell \equiv a \pmod{c}$. Επειδή $\gcd(c, \omega) = 1$ η παραπάνω ισοδυναμία έχει μοναδική λύση $(\mathrm{mod}\ c)$. Άρα, από $0, \ldots, c-1$ έχουμε ακριβώς μία λύση, από $c, \ldots, 2c-1$ έχουμε ακριβώς μία λύση,.... Μέχρι το $m-1$ θα έχουμε ακριβώς $\left[\frac{m}{c}\right]$ λύσεις.

Υπάρχουν παράγοντες που δε διαιρούνται με c. Όμως οι παράγοντες αυτοί μπορεί να διαιρούνται με κάποιον διαιρέτη του c και συνεπώς στο γινόμενο να έχουμε

$$\mathrm{ord}_c\Big(a(a-\omega)\dots(a-(m-1)\omega)\Big) \geq \Big[\frac{m}{c}\Big].$$

Έχουμε

$$\binom{\nu}{k} = \frac{\alpha(\alpha-b)\dots(\alpha-(k-1)b))}{b^k k!}.$$

Έστω p' ένας πρώτος που δε διαιρεί το b. Εφαρμόζοντας τη σχέση (1.40) για $m=k$, $\omega=b, a=\alpha$ και $c=p', p'^2, \dots$ προκύπτει ότι

$$\mathrm{ord}_{p'}\Big(\alpha(\alpha-b)\dots(\alpha-(k-1)b)\Big) \geq \Big[\frac{k}{p'}\Big] + \Big[\frac{k}{p'^2}\Big] + \dots = \mathrm{ord}_{p'}(k!).$$

Έτσι οι μόνοι πρώτοι πράγοντες του $b^k k!$ είναι οι πρώτοι διαιρέτες του b και έπεται το ζητούμενο.

□

Απόδειξη του Θεωρήματος 1.6.1:

Η δοθείσα εξίσωση γράφεται: $x^p = (y\pm 1)(\frac{y^q\pm 1}{y\pm 1})$. Από το Λήμμα 1.6.2 $q \mid (y\pm 1)$. Επομένως $q \mid x^p$, δηλαδή $q \mid x$.
Υποθέτουμε ότι $p \not| (x\mp 1)$ και θα καταλήξουμε σε άτοπο.
Έχουμε $y^q = (x\mp 1)(\frac{x^p\mp 1}{x\mp 1})$, όπου $\gcd\Big(x\mp 1, \frac{x^p\mp 1}{x\mp 1}\Big) = 1$. Άρα, υπάρχει ακέραιος z τ.ω. $x\mp 1 = z^q$. Όμως $z \neq 1$. Πράγματι, αν $z=1$, τότε $x=0$ ή $x=2$. Επειδή $x>1$ δε μπορεί να ισχύει $x=0$. Επίσης ούτε η τιμή $x=2$ είναι δεκτή, αφού $q>2$ και συνεπώς δεν ισχύει ότι $q \mid 2$. Άρα

$$x\mp 1 = z^q, \tag{1.41}$$

για κάποιο ακέραιο $z>1$.
Θα δείξουμε ότι

$$z > u. \tag{1.42}$$

Πράγματι, επειδή $z^q = x\mp 1 \geq \frac{1}{2}x$ και $y^q \pm 1 > \frac{1}{2}y^q$ έχουμε $z^{pq} \geq (\frac{1}{2}x)^p > (\frac{1}{2})^{p+1}y^q$. Όμως, από την Πρόταση 1.6.1, $y\pm 1 = q^{p-1}u^p$, δηλαδή $y > \frac{1}{2}q^{p-1}u^p$.
Επομένως $z^{pq} > (\frac{1}{2})^{p+1}(\frac{1}{2}q^{p-1}u^p)^q > u^{pq}$ (επειδή $p>q>2$), δηλαδή $z>u$.
Επίσης

$$z^q \geq \frac{1}{2}q^{p-1}. \tag{1.43}$$

Πράγματι, από το Πόρισμα 1.6.2 και τη σχέση (1.41) έχουμε

$$\Big|z^q \pm 1 - qu\Big| \geq q^{p-1}. \tag{1.44}$$

Αν υποθέσουμε ότι η σχέση (1.43) δεν ισχύει, τότε

$$\left|qu \mp 1\right| > \frac{1}{2}q^{p-1}. \tag{1.45}$$

Από τη σχέση (1.45) έπεται ότι $u > 1$. Αν $\varphi(u) := u^q - qu - 1$, όπου $u \geq 2$ και $q \geq 3$, τότε $\varphi'(u) = q(u^{q-1} - 1) > 0$, για κάθε $u \geq 2$. Άρα, η $\varphi(u)$ είναι αύξουσα για κάθε $u \geq 2$. Επαγωγικά ως προς m αποδεικνύεται ότι, αν $m \geq 3$, τότε ισχύει $2^m - 2m - 1 > 0$. Επομένως $2^q - 2q - 1 > 0$, για κάθε $q \geq 3$. Συνεπώς $u^q > qu + 1$. Άρα $z^q > u^q > qu + 1$, δηλαδή $z^q > \frac{1}{2}q^{p-1}$ και καταλήγουμε σε άτοπο.
Αν $x^p = y^q - 1$, τότε $x^p = (z^q - 1)^p$. Ενώ αν $x^p = y^q + 1$, τότε

$$y^q = x^p - 1 = (z^q + 1)^p - 1 \geq (z^q - 1)^p.$$

Συνεπώς $\min(x^p, y^q) \geq (z^q - 1)^p$. Από τη σχέση (1.43) έπεται ότι

$$(z^q - 1)^p \geq z^{pq}(1 - 2q^{-p+1})^p.$$

Επειδή $q \geq 3,\ p \geq 5$ και $q < p$ έχουμε $1 - 2q^{-p+1} > q^{-\frac{1}{p}}$. Επομένως

$$\min(x^p, y^q) \geq (z^q - 1)^p \geq z^{pq}(1 - 2q^{-p+1})^p > q^{-1}z^{pq}. \tag{1.46}$$

Επειδή $\left|(x^{\frac{p}{q}})^q - y^q\right| = 1$ έχουμε

$$\left|x^{\frac{p}{q}} - y\right| = \frac{1}{\left|x^{\frac{p(q-1)}{q}} + x^{\frac{p(q-2)}{q}}y + \ldots + y^{q-1}\right|} \leq \frac{1}{q\min\left\{x^{\frac{p(q-1)}{q}},\ y^{q-1}\right\}}. \tag{1.47}$$

Εργαζόμενοι ανάλογα, όπως για να αποδείξουμε τη σχέση (1.46), έχουμε

$$\min\left\{x^{\frac{p(q-1)}{q}},\ y^{q-1}\right\} \geq (z^q - 1)^{\frac{p(q-1)}{q}} \geq z^{p(q-1)}(1 - 2q^{-p+1})^{\frac{p(q-1)}{q}} > z^{p(q-1)}q^{-1}. \tag{1.48}$$

Επομένως, από τις σχέσεις (1.47) και (1.48) έπεται ότι

$$\left|x^{\frac{p}{q}} - y\right| < z^{-p(q-1)}. \tag{1.49}$$

Στη συνέχεια, από τις σχέσεις (1.41),(1.43) και τον τύπο της διωνυμικής δυναμοσειράς έχουμε

$$x^{\frac{p}{q}} = (z^q \pm 1)^{\frac{p}{q}} = \sum_{r=0}^{\infty} t_r, \tag{1.50}$$

όπου

$$t_r = (\pm 1)^r \frac{\frac{p}{q}(\frac{p}{q} - 1)\ldots(\frac{p}{q} - r + 1)}{r!}z^{p-rq}. \tag{1.51}$$

Θέτουμε

$$R := \Big[\frac{p}{q}\Big] + 1 \tag{1.52}$$

και

$$P := \Big[\frac{R}{q-1}\Big]. \tag{1.53}$$

Από το Λήμμα 1.6.3 ο αριθμός $z^{Rq-p}q^{R+P}t_r$ είναι ακέραιος για κάθε $r \leq R$. Ο αριθμός $z^{Rq-p}y$ είναι επίσης ακέραιος διότι $Rq > p$.
Επομένως ο

$$I := z^{Rq-p}q^{R+P}\Big\{(y - x^{\frac{p}{q}}) + \sum_{r>R}^{\infty} t_r\Big\} \tag{1.54}$$

είναι ακέραιος.
Θα δείξουμε ότι $I \neq 0$ και $|I| < 1$. Τέτοιος ακέραιος δε μπορεί να υπάρχει και έτσι θα καταλήξουμε σε άτοπο.
Επειδή $\left|\frac{t_{r+1}}{t_r}\right| = \frac{(\frac{p}{q}-r)r!}{(r+1)!}z^{-q} = \frac{\frac{p}{q}-r}{r+1}z^{-q}$ και $\frac{p}{q} < R$ έχουμε

$$\left|\frac{t_{r+1}}{t_r}\right| < z^{-q} \leq 2q^{-p+1}, \tag{1.55}$$

για όλα τα $r > R$.
Επίσης

$$\Big|\frac{p}{q}(\frac{p}{q}-1)\dots(\frac{p}{q}-R)\Big| < R(R-1)\dots 2\Big|\frac{p}{q}-R+1\Big| \cdot \Big|\frac{p}{q}-R\Big| \leq \frac{1}{4}R! \tag{1.56}$$

και

$$\Big|\frac{p}{q}(\frac{p}{q}-1)\dots(\frac{p}{q}-R)\Big| > (R-1)(R-2)\dots 1\Big|\frac{p}{q}-R+1\Big| \cdot \Big|\frac{p}{q}-R\Big| > \frac{(R-1)!}{q^2}. \tag{1.57}$$

Από τις σχέσεις (1.56) και (1.57) έπεται ότι

$$\frac{1}{q^2(R+1)^2} < \left|z^{(R+1)q-p}t_{R+1}\right| < \frac{1}{4}. \tag{1.58}$$

Από τη σχέση (1.54) έχουμε

$$I = I_1 + I_2 + I_3, \tag{1.59}$$

όπου

$$I_1 = z^{Rq-p}q^{R+P}(y - x^{\frac{p}{q}}), \tag{1.60}$$

$$I_2 = z^{Rq-p}q^{R+P}t_{R+1}, \tag{1.61}$$

$$I_3 = z^{Rq-p}q^{R+P}\sum_{r>R+1} t_r. \tag{1.62}$$

Οπότε $\left|\frac{I_3}{I_2}\right| = \left|\frac{\sum_{r>R+1} t_r}{t_{R+1}}\right| = \left|\frac{t_{R+2}}{t_{R+1}} + \frac{t_{R+3}}{t_{R+1}} + \ldots\right|$.
Όμως, από τη σχέση (1.55), έχουμε

$$\left|\frac{t_{R+2}}{t_{R+1}} + \frac{t_{R+3}}{t_{R+1}} + \ldots\right| < \sum_{s=1}^{\infty} (2q^{-p+1})^s = \frac{2q^{-p+1}}{1-2q^{-p+1}}.$$

Επειδή $q \geq 3$ και $p \geq 5$ ισχύει $\frac{2q^{-p+1}}{1-2q^{-p+1}} \leq \frac{2\cdot 3^{-5+1}}{1-2\cdot 3^{-5+1}} < \frac{1}{10}$.
Άρα

$$\left|\frac{I_3}{I_2}\right| < \frac{1}{10}. \tag{1.63}$$

Επίσης από τις σχέσεις (1.49) και (1.58) έχουμε

$$\left|\frac{I_1}{I_2}\right| = \left|\frac{y - x^{\frac{p}{q}}}{t_{R+1}}\right| < \frac{z^{-p(q-1)}}{t_{R+1}} < q^2(R+1)^2 z^{(R+1-p)q}.$$

Όμως, επειδή $q \geq 3$ και $p \geq 5$, έχουμε

$$R + 1 - p = \left[\frac{p}{q}\right] + 2 - p \leq \left[\frac{5}{q}\right] + 2 - 5 \leq \left[\frac{5}{3}\right] + 2 - 5 = -2. \tag{1.64}$$

Έτσι, και λόγω της σχέσης (1.43), έχουμε $q^2(R+1)^2 z^{(R+1-p)q} \leq q^2(p-2)^2(\frac{1}{2}q^{p-1})^{-2}$.
Άρα

$$\left|\frac{I_1}{I_2}\right| \leq \Big(2(p-2)q^{2-p}\Big)^2 \leq \Big(2\cdot(5-2)\cdot 3^{2-5}\Big)^2 < \frac{1}{10}. \tag{1.65}$$

Από τις σχέσεις (1.59), (1.63) και (1.65) έπεται ότι $I \neq 0$ και συνεπώς

$$|I| \geq 1, \tag{1.66}$$

αφού είναι ακέραιος.
Επίσης από τις σχέσεις (1.43) και (1.58) έχουμε

$$|I_2| = \left|z^{Rq-p} q^{R+P} t_{R+1}\right| \leq \frac{1}{4} z^{-q} q^{R+P} \leq \frac{1}{2} q^{R+P-p+1}. \tag{1.67}$$

Οπότε, από τις σχέσεις (1.63), (1.65), (1.66) και (1.67), προκύπτει ότι

$$1 \leq |I| \leq \Big(1 + \frac{1}{10} + \frac{1}{10}\Big)\frac{1}{2} q^{R+P-p+1} < q^{R+P-p+1}. \tag{1.68}$$

Επομένως

$$R + P - p + 1 > 0. \tag{1.69}$$

Από τις σχέσεις (1.64) και (1.69) έχουμε

$$P = \Big[\frac{R}{q-1}\Big] \geq 3,$$

δηλαδή

$$R \geq 3(q-1)$$

και έτσι

$$p > q\Big[\frac{p}{q}\Big] \geq q(3q-4). \tag{1.70}$$

Τέλος

$$R + P \leq R\Big(1 + \frac{1}{q-1}\Big) \leq (\frac{p}{q} + 2)(\frac{q}{q-1}) = \frac{p}{q-1} + \frac{2q}{q-1}. \tag{1.71}$$

Όμως

$$\frac{p}{q-1} + \frac{2q}{q-1} = \frac{p+2q}{q-1} < p - 1. \tag{1.72}$$

Πράγματι, από τη σχέση (1.70) και επειδή $q \geq 3$ έχουμε $p > 15$. Οπότε προκύπτει ότι $p(q-2) > 15(q-2) > 3q-1$, δηλαδή η σχέση (1.72) ισχύει. Άρα

$$R + P < p - 1. \tag{1.73}$$

Λόγω των σχέσεων (1.69) και (1.73) καταλήγουμε σε άτοπο και συνεπώς $p \mid (x \mp 1)$. Επειδή $y^q = (x \mp 1)(\frac{x^p \mp 1}{x \mp 1})$ έπεται ότι $p \mid y^q$, δηλαδή $p \mid y$.

□

Επειδή η εξίσωση $x^p - y^q = 1$ γράφεται $(-y)^q - (-x)^p = 1$ μπορούμε τα x, y, p, q να τα αντικαταστήσουμε με $-y, -x, q, p$. Επομένως, έχουμε το παρακάτω Θεώρημα:

Θεώρημα 1.6.2 (Cassels)
Αν υποθέσουμε ότι η εξίσωση $X^p - Y^q = 1$, όπου οι p, q είναι περιττοί πρώτοι με $p \neq q$, έχει ακέραια λύση (x, y) με $xy \neq 0$, τότε $q \mid x$ και $p \mid y$.
Επίσης υπάρχουν μη-μηδενικοί ακέραιοι b, v τέτοιοι ώστε

$$y + 1 = q^{p-1}b^p, \tag{1.74}$$

$$\frac{y^q + 1}{y + 1} = qv^p, \tag{1.75}$$

$$x = qbv, \tag{1.76}$$

όπου $q \nmid v$.
Συμμετρικά, υπάρχουν μη-μηδενικοί ακέραιοι a, u τέτοιοι ώστε

$$x - 1 = p^{q-1}a^q, \tag{1.77}$$

$$\frac{x^p - 1}{x - 1} = pu^q, \tag{1.78}$$

$$y = pau, \tag{1.79}$$

όπου $p \nmid u$.

Οι σχέσεις του Cassels δίνουν διάφορα κάτω φράγματα για τα x, y.
Για παράδειγμα, από τις σχέσεις (1.74) και (1.77) έπεται ότι

$$|y| \geq q^{p-1} - 1 \tag{1.80}$$
$$|x| \geq p^{q-1} - 1. \tag{1.81}$$

Πρόταση 1.6.2
Αν $p \not| (q-1)$, *τότε* $q^{p-2} \mid (v-1)$.

Απόδειξη:
Επειδή η σχέση (1.75) γράφεται

$$\Big((-y)^{q-1} - 1\Big) + \Big((-y)^{q-2} - 1\Big) + \ldots + (-y-1) = q(v^p - 1)$$

έχουμε $(y+1) \mid q(v^p - 1)$. Από τη σχέση (1.74) έπεται ότι $v^p \equiv 1 \pmod{q^{p-2}}$, δηλαδή η τάξη του $v \pmod{q^{p-2}}$ είναι 1 ή p. Επειδή $p \not| (q-1)$ έχουμε $p \not| q^{p-3}(q-1)$ και άρα $v \equiv 1 \pmod{q^{p-2}}$.

□

Πόρισμα 1.6.3
Έχουμε $|x| \geq q^{p-1}$.

Απόδειξη:
Αν $p \mid (q-1)$, τότε $p < q$ και από τη σχέση (1.81) έπεται το ζητούμενο.
Αν $p \not| (q-1)$, τότε από την Πρόταση 1.6.2 έχουμε $q^{p-2} \mid (v-1)$. Επειδή $|y| \geq 2$ και $(y,q) \neq (2,3)$ ισχύει $\frac{y^q+1}{y+1} > q$, δηλαδή $v > 1$. Άρα $v \geq q^{p-2}+1$. Επειδή $x = qbv$ προκύπτει ότι $|x| \geq qv \geq q^{p-1} + q > q^{p-1}$.

□

Κεφάλαιο 2

Οι ισοδυναμίες του Inkeri

2.1 Κυκλοτομικά σώματα αριθμών

Στην παράγραφο αυτή θα μελετήσουμε τα σώματα που προκύπτουν από το σώμα $\mathbb{Q}$ των ρητών αριθμών με την επισύναψη των $n-$ριζών της μονάδας. Τα σώματα αυτά λέγονται κυκλοτομικά σώματα. Για μία πλήρη ανάπτυξη της θεωρίας των κυκλοτομικών σωμάτων παραπέμπουμε στα ([4], [39]).
Θα μελετήσουμε την περίπτωση όπου ο n είναι ένας περιττός πρώτος αριθμός p.
Οι $p-$ρίζες της μονάδας, δηλαδή οι ρίζες του πολυωνύμου $x^p - 1$, είναι οι αριθμοί

$$1,\ \zeta = e^{\frac{2\pi i}{p}},\ \zeta^2,\ \ldots,\ \zeta^{p-1}.$$

Άρα ισχύει

$$x^p - 1 = (x-1)(x-\zeta)\ldots(x-\zeta^{p-1}),$$

δηλαδή

$$f(x) = \frac{x^p - 1}{x-1} = x^{p-1} + x^{p-2} + \ldots + x + 1 = (x-\zeta)\ldots(x-\zeta^{p-1}).$$

Το κυκλοτομικό πολυώνυμο $f(x)$ είναι ανάγωγο στο $\mathbb{Q}$ διότι το πολυώνυμο

$$f(x+1) = \frac{(x+1)^p - 1}{x+1-1} = x^{p-1} + \binom{p}{1} x^{p-2} + \ldots + \binom{p}{p-1}$$

ικανοποιεί τις συνθήκες του κριτηρίου του Eisenstein. Συνεπώς ισχύει

$$f(x) = \mathrm{Irr}(\zeta^m, \mathbb{Q}) \qquad (m = 1, \ldots, p-1).$$

Για το κυκλοτομικό σώμα K_p των $p-$ριζών της μονάδας έχουμε

$$K_p = \mathbb{Q}(\zeta, \zeta^2, \ldots, \zeta^{p-1}) = \mathbb{Q}(\zeta)$$

και $[K_p : \mathbb{Q}] = \text{degIrr}(\zeta, \mathbb{Q}) = p - 1$.
Αν ζ είναι μία πρωταρχική $p-$ρίζα της μονάδας, τότε οι δυνάμεις αυτής

$$\zeta^0 = 1,\ \zeta,\ \zeta^2,\ \ldots,\ \zeta^{p-1}$$

είναι διάφορες μεταξύ τους και αποτελούν το σύνολο των $p-$ριζών της μονάδας. Άρα, οι συζυγείς αριθμοί του ζ στο σώμα $K_p = \mathbb{Q}(\zeta)$, που είναι οι ρίζες του πολυωνύμου $f(x) = \text{Irr}(\zeta, \mathbb{Q})$, είναι οι δυνάμεις

$$\zeta,\ \zeta^2,\ \ldots,\ \zeta^{p-1}.$$

Η επέκταση $K_p/\mathbb{Q}$ είναι επέκταση του Galois. Έστω $G :=\text{Gal}(K_p/\mathbb{Q})$. Για κάθε ακέραιο a πρώτο ως προς τον p υπάρχει μοναδικό $\sigma_a \in G$ τέτοιο ώστε $\sigma_a(\zeta) = \zeta^a$. Προφανώς $\sigma_{ab} = \sigma_a \circ \sigma_b$. Επίσης $\sigma_a = \sigma_{a'}$, όπου $a' \in (\mathbb{Z}/p\mathbb{Z})^*$, αν και μόνο αν $a \equiv a' \pmod p$. Άρα

$$G = \{\sigma_1,\ \sigma_2,\ \ldots\ ,\ \sigma_{p-1}\}.$$

Ακόμη σ_{p-1} είναι η μιγαδική συζυγία και $\sigma_{p-1} \circ \sigma_a = \sigma_{p-a}$.
Η απεικόνιση

$$\begin{array}{rcl} (\mathbb{Z}/p\mathbb{Z})^* & \to & G \\ a \pmod p & \mapsto & \sigma_a \end{array}$$

είναι ισομορφισμός και άρα $G :=\text{Gal}(K_p/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*$, δηλαδή η ομάδα Galois της επέκτασης $K_p/\mathbb{Q}$ είναι κυκλική τάξης $p - 1$.
Ο δακτύλιος των ακεραίων αλγεβρικών αριθμών του κυκλοτομικού σώματος $K_p = \mathbb{Q}(\zeta)$ είναι ο $D_p = \mathbb{Z}[\zeta]$. Ο δακτύλιος $\mathbb{Z}[\zeta]$ είναι δακτύλιος του Dedekind, δηλαδή κάθε ιδεώδες του K_p αναλύεται μονοσήμαντα σε γινόμενο πρώτων ιδεωδών του K_p.
Από τη σχέση $x^{p-1} + x^{p-2} + \ldots + x + 1 = (x - \zeta) \ldots (x - \zeta^{p-1})$ για $x = 1$ παίρνουμε

$$p = \prod_{i=1}^{p-1} (1 - \zeta^i).$$

Αν $\lambda := 1 - \zeta$, τότε

$$p = \lambda^{p-1}\ \varepsilon_2\ \varepsilon_3\ \ \ldots\ \varepsilon_{p-1},$$

όπου τα

$$\varepsilon_i = \frac{1 - \zeta^i}{1 - \zeta},\ \text{για } i = 2, 3, \ldots, p - 1$$

είναι μονάδες του D_p. Πράγματι, για κάθε $i = 2, 3, \ldots, p - 1$ έχουμε

$$\varepsilon_i = \frac{1 - \zeta^i}{1 - \zeta} = 1 + \zeta + \zeta^2 + \ldots + \zeta^{i-1} \in \mathbb{Z}[\zeta].$$

Θα αποδείξουμε ότι $\varepsilon_i^{-1} = \frac{1-\zeta}{1-\zeta^i} \in \mathbb{Z}[\zeta]$, για κάθε $i = 2, 3, \ldots, p-1$.
Υπάρχει φυσικός αριθμός j τέτοιος ώστε $ij \equiv 1 \pmod{p}$, αφού $\gcd(i,p) = 1$. Οπότε, για κάθε $i = 2, 3, \ldots, p-1$,

$$\varepsilon_i^{-1} = \frac{1-\zeta}{1-\zeta^i} = \frac{1-\zeta^{ij}}{1-\zeta^i} = 1 + \zeta^i + \zeta^{2i} + \ldots + \zeta^{(j-1)i} \in \mathbb{Z}[\zeta].$$

Άρα, οι αριθμοί $\varepsilon_2,\ \varepsilon_3,\ \ldots,\ \varepsilon_{p-1}$ είναι μονάδες του δακτυλίου D_p και συνεπώς

$$p = \varepsilon\ \lambda^{p-1},$$

όπου ε μονάδα του D_p.

Λήμμα 2.1.1
Υποθέτουμε ότι $a = a_0 + a_1\zeta + \ldots + a_{p-1}\zeta^{p-1}$ με $a_i \in \mathbb{Z}$ και ένα τουλάχιστον $a_i = 0$. Αν n είναι ένας ακέραιος που διαιρεί τον a, τότε ο n διαιρεί κάθε a_j.

Τα παρακάτω θεωρήματα δίνουν το νόμο αναλύσεως του κυκλοτομικού σώματος $K_p = \mathbb{Q}(\zeta)$.

Θεώρημα 2.1.1
Αν ζ είναι μία πρωταρχική $p-$ρίζα της μονάδας, όπου p περιττός πρώτος αριθμός, και $\lambda = 1 - \zeta$, τότε το ιδεώδες $< \lambda > = < 1 - \zeta >$ του κυκλοτομικού σώματος K_p είναι πρώτο και η ανάλυση του ιδεώδους $< p >$ σε γινόμενο πρώτων ιδεωδών του K_p είναι

$$< p > = < \lambda >^{p-1} = (< 1 - \zeta >)^{p-1}.$$

Θεώρημα 2.1.2
Έστω ζ μία πρωταρχική $p-$ρίζα της μονάδας, όπου p περιττός πρώτος αριθμός. Αν q είναι ένας πρώτος αριθμός διάφορος του p και f ο ελάχιστος μη-μηδενικός φυσικός αριθμός για τον οποίο ισχύει

$$q^f \equiv 1 \pmod{p},$$

τότε η ανάλυση του ιδεώδους $< q >$ σε γινόμενο πρώτων ιδεωδών του κυκλοτομικού σώματος $K_p = \mathbb{Q}(\zeta)$ έχει τη μορφή

$$< q > = P_1 P_2 \ldots P_s,$$

όπου τα πρώτα ιδεώδη $P_1, P_2, \ldots, P_s$ έχουν τον ίδιο βαθμό f και το πλήθος αυτών s ορίζεται από τη σχέση $p - 1 = fs$.

Στη συνέχεια θα μελετήσουμε την ομάδα των μονάδων και την ομάδα των ριζών της μονάδας του κυκλοτομικού σώματος $K_p = \mathbb{Q}(\zeta)$.

Από το Θεώρημα του Dirichlet η ομάδα E των μονάδων είναι το ευθύ γινόμενο

$$E = < \zeta > \otimes < \varepsilon_1 > \otimes \ldots \otimes < \varepsilon_r >$$

μίας κυκλικής ομάδας $< \zeta >$ πεπερασμένης τάξης και r κυκλικών ομάδων (άπειρης τάξης) $< \varepsilon_1 >, \ldots, < \varepsilon_r >$, όπου $\varepsilon_1, \ldots, \varepsilon_r$ είναι μονάδες του D_p και $r := \frac{p-3}{2}$.

Λήμμα 2.1.2

Αν a είναι ένας ακέραιος αλγεβρικός αριθμός του αλγεβρικού σώματος αριθμών K_p του οποίου όλοι οι συζυγείς αριθμοί έχουν μέτρο 1, τότε ο a είναι ρίζα της μονάδας.

Λήμμα 2.1.3

Οι μόνες ρίζες της μονάδας που ανήκουν στο κυκλοτομικό σώμα K_p είναι οι $\pm\zeta^s$, όπου s ακέραιος αριθμός.

Πόρισμα 2.1.1

Αν q είναι ένας περιττός πρώτος διάφορος του p, τότε κάθε ρίζα της μονάδας του κυκλοτομικού σώματος K_p είναι $q-$δύναμη μίας άλλης ρίζας της μονάδας.

Θεώρημα 2.1.3 (Kummer)

Κάθε μονάδα ε του κυκλοτομικού σώματος $K_p = \mathbb{Q}(\zeta)$ έχει τη μορφή $\varepsilon = \eta\zeta^s$, όπου η είναι μία πραγματική μονάδα και s ένας ακέραιος αριθμός.

Τέλος υπάρχει μία υποομάδα C της ομάδας E όλων των μονάδων, η οποία έχει βαθμό $r = \frac{p-3}{2}$ και λέγεται ομάδα των κυκλοτομικών μονάδων του σώματος K_p. Είναι πολλαπλασιαστική ομάδα και παράγεται από το $-\zeta$ και τις μονάδες της μορφής $\frac{1-\zeta^k}{1-\zeta}$, για $k = 2, 3, \ldots p-1$.

2.2 Το θεώρημα του Inkeri

Στην παράγραφο αυτή οι p, q με $p \neq q$ συμβολίζουν δύο περιττούς πρώτους.

Θεώρημα 2.2.1

Υποθέτουμε ότι η εξίσωση $X^p - Y^q = 1$ έχει ακέραια λύση (x, y) με $xy \neq 0$. Αν ο αριθμός κλάσεων h_p του κυκλοτομικού σώματος αριθμών $K_p = \mathbb{Q}(\zeta)$ δε διαιρείται από το q, τότε υπάρχουν συζυγείς μιγαδικοί ακέραιοι $a, \overline{a}$ και $b, \overline{b}$, όχι μονάδες, τ.ω

$$a^q + \overline{a}^q = \varepsilon^p \tag{2.1}$$

$$b^q + \overline{b}^q = \eta x, \tag{2.2}$$

όπου ε, η είναι πραγματικές μονάδες του δακτυλίου $D_p = \mathbb{Z}[\zeta]$ των ακεραίων αλγεβρικών αριθμών του K_p.

Απόδειξη:

Έστω (x, y) ακέραια λύση της εξίσωσης με $xy \neq 0$.
Σύμφωνα με το Θεώρημα 1.6.2 έχουμε

$$\frac{x^p - 1}{x - 1} = (x - \zeta)(x - \zeta^2)\ldots(x - \zeta^{p-1}) = pu^q \tag{2.3}$$

και

$$x = qbv, \tag{2.4}$$

όπου οι u, b, v είναι μη-μηδενικοί ακέραιοι και $p \nmid u$, $q \nmid v$.
Ο u είναι ακέραιος > 1. Πράγματι, επειδή $|x| \geq q \geq 3$ ισχύει

$$\frac{x^p - 1}{x - 1} \geq |x|^{p-1} - |x|^{p-2} + \ldots - |x| + 1 \tag{2.5}$$

$$\geq |x|^{p-2}(|x| - 1) + 1 \geq 3^{p-2} + 1 > p. \tag{2.6}$$

Από τις σχέσεις (2.3) και (2.6) έχουμε $u > 1$.
Επίσης $p = (1-\zeta)(1-\zeta^2)\ldots(1-\zeta^{p-1})$ και συνεπώς η εξίσωση (2.3) γράφεται

$$\prod_{i=1}^{p-1} \delta_i = u^q, \qquad \text{με} \qquad \delta_i = \frac{x - \zeta^i}{1 - \zeta^i}. \tag{2.7}$$

Οι παράγοντες δ_i ανήκουν στο δακτύλιο D_p. Πράγματι, $\delta_i = \frac{x-\zeta^i}{1-\zeta^i} = \frac{x-1}{1-\zeta^i} + 1$. Όμως, λόγω του Θεωρήματος 1.6.2, $p = \prod_{i=1}^{p-1}(1-\zeta^i) \mid x - 1$. Άρα $1 - \zeta^i \mid p \mid x - 1$ στο δακτύλιο D_p και έτσι οι δ_i ανήκουν στον D_p.
Από τη σχέση (2.7), αν περάσουμε στα ιδεώδη, έχουμε $\prod_{i=1}^{p-1} < \delta_i > = < u >^q$.
Θα δείξουμε ότι τα ιδεώδη $< \delta_i >$ είναι ανά δύο πρώτα μεταξύ τους. Πράγματι, αν υποθέσουμε ότι τα ιδεώδη $< \delta_i >$ και $< \delta_j >$ $(i \neq j)$ έχουν κοινό παράγοντα ένα πρώτο ιδεώδες P, δηλαδή $P \mid < \delta_i >$ και $P \mid < \delta_j >$, τότε από τη σχέση

$$(1 - \zeta^i)\frac{x - \zeta^i}{1 - \zeta^i} - (1 - \zeta^j)\frac{x - \zeta^j}{1 - \zeta^j} = \zeta^j - \zeta^i$$

προκύπτει ότι $P \mid < \zeta^j - \zeta^i >$. Όμως $< \zeta^j - \zeta^i > = < 1 - \zeta^i > = < 1 - \zeta^j > = < 1 - \zeta >$.
Άρα $P = < 1 - \zeta >$. Επειδή $< p > = (< 1 - \zeta >)^{p-1} = P^{p-1}$ και $p \mid x - 1$ έχουμε $P \mid \frac{x-1}{1-\zeta^i}$, δηλαδή $\beta_i = \frac{x-1}{1-\zeta^i} + 1 \equiv 1 \pmod{P}$, το οποίο είναι άτοπο αφού $\beta_i \equiv 0 \pmod{P}$.
Επομένως

$$< \delta_i > = A_i^q \qquad (i = 1, 2, \ldots, p-1), \tag{2.8}$$

όπου A_i είναι ιδεώδη του D_p, ανά δύο πρώτα μεταξύ τους.
Επειδή $q \nmid h_p$ και ο q είναι πρώτος έχουμε $\gcd(q, h_p) = 1$. Άρα, το ιδεώδες A_i είναι κύριο ιδεώδες, δηλαδή υπάρχει a_i στο δακτύλιο D_p τ.ω $A_i = < a_i >$. Οπότε από τη σχέση (2.8) έπεται ότι $< \delta_i > = < a_i^q >$. Για $i = 1$ έχουμε

$$x - \zeta = \varepsilon_1(1 - \zeta)a_1^q, \tag{2.9}$$

όπου ε_1 είναι μονάδα του δακτυλίου D_p και a_1 στοιχείο αυτού. Από τη θεωρία των κυκλοτομικών σωμάτων έχουμε $\varepsilon_1 = \zeta^k \eta_1$, όπου η_1 είναι πραγματική μονάδα του δακτυλίου D_p και k ακέραιος. Αν στην εξίσωση (2.9) το ζ αντικατασταθεί από το ζ^2, τότε

$$x - \zeta^2 = \zeta^{2k+1}\eta(\zeta^{-1} - \zeta)a_2^q, \tag{2.10}$$

όπου η είναι πραγματική μονάδα του D_p και a_2 στοιχείο αυτού.
Επειδή οι p, q είναι πρώτοι και $p \neq q$ υπάρχουν ακέραιοι c, d τ.ω $1 = cp - dq$. Συνεπώς $\zeta^{2k+1} = \zeta^{(2k+1)(cp-dq)} = \zeta^{(2k+1)(-dq)} = \left(\zeta^{-(2k+1)d}\right)^q$. Άρα, η εξίσωση (2.10) γράφεται

$$x - \zeta^2 = \eta(\zeta^{-1} - \zeta)\gamma^q, \tag{2.11}$$

όπου γ ανήκει στον D_p (όχι μονάδα).
Η μιγαδική συζυγία στέλνει το ζ στο ζ^{-1}. Από την εξίσωση (2.11) έχουμε

$$x - \zeta^{-2} = \eta(\zeta - \zeta^{-1})\overline{\gamma}^q. \tag{2.12}$$

Αφαιρώντας τις εξισώσεις (2.11) και (2.12) κατά μέλη προκύπτει ότι

$$\zeta + \zeta^{-1} = \eta(\gamma^q + \overline{\gamma}^q). \tag{2.13}$$

0 αριθμός $\varepsilon_2 = \frac{\zeta+\zeta^{-1}}{\eta}$ είναι πραγματική μονάδα του D_p. Για $\varepsilon = \varepsilon_2^c$ και $a = \varepsilon_2^d\gamma$, χρησιμοποιώντας την εξίσωση (2.13), προκύπτει ότι $a^q + \overline{a}^q = \varepsilon^p$.
Πολλαπλασιάζοντας την εξίσωση (2.11) με ζ^{-2} έχουμε $\zeta^{-2}x - 1 = \eta(\zeta^{-1} - \zeta)\zeta^{-2}\gamma^q$. Όμως $\zeta = \zeta^{-dq}$, δηλαδή $\zeta^{-2} = \zeta^{2dq}$. Άρα

$$\zeta^{-2}x - 1 = \eta(\zeta^{-1} - \zeta)b^q, \tag{2.14}$$

όπου $b = \zeta^{2d}\gamma$. Από την εξίσωση (2.14) εφαρμόζοντας τη μιγαδική συζυγία παίρνουμε

$$\zeta^2 x - 1 = \eta(\zeta - \zeta^{-1})\overline{b}^q. \tag{2.15}$$

Αφαιρώντας τις εξισώσεις (2.14) και (2.15) κατά μέλη και διαιρώντας με $\eta(\zeta^{-1} - \zeta)$ έχουμε

$$b^q + \overline{b}^q = \eta' x, \tag{2.16}$$

όπου $\eta' := \frac{\zeta^{-2}-\zeta^2}{\eta(\zeta^{-1}-\zeta)} = \frac{\zeta+\zeta^{-1}}{\eta}$ είναι πραγματική μονάδα του D_p.

□

Θεώρημα 2.2.2

Έστω h_p και h_q οι αριθμοί κλάσεων των κυκλοτομικών σωμάτων αριθμών $K_p = \mathbb{Q}(\zeta_p)$ και $K_q = \mathbb{Q}(\zeta_q)$. Αν υποθέσουμε ότι η εξίσωση $X^p - Y^q = 1$ έχει ακέραια λύση (x, y) με $xy \neq 0$, τότε

$$(i)\ x \equiv 0 \pmod{q^2} \text{ και } p^q \equiv p \pmod{q^2},\ \text{αν } q \nmid h_p, \tag{2.17}$$

$$(ii)\ y \equiv 0 \pmod{p^2} \text{ και } q^p \equiv q \pmod{p^2},\ \text{αν } p \nmid h_q. \tag{2.18}$$

Απόδειξη:

Υποθέτουμε ότι η εξίσωση $x^p - y^q = 1$ έχει ακέραια λύση (x, y) με $xy \neq 0$.
Αν $q \nmid h_p$, τότε από το Θεώρημα 2.2.1 έπεται ότι

$$\eta x = b^q + \overline{b}^q = (b + \overline{b})^q + q(b\overline{b})(b + \overline{b})d, \tag{2.19}$$

όπου οι $d, \eta, b, \overline{b}$ ανήκουν στο δακτύλιο D_p.
Από το Θεώρημα 1.6.2 έχουμε $q \mid x$. Επομένως, από τη σχέση (2.19) προκύπτει ότι

$$(b + \overline{b})^q \equiv 0 \pmod{q} \tag{2.20}$$

στο δακτύλιο D_p.
Από τη θεωρία των κυκλοτομικών σωμάτων η ανάλυση του ιδεώδους $< q >$ σε γινόμενο πρώτων ιδεωδών του κυκλοτομικού σώματος K_p έχει τη μορφή

$$< q >= P_1 P_2 \dots P_s, \tag{2.21}$$

όπου τα πρώτα ιδεώδη $P_1, P_2 \dots, P_s$ έχουν τον ίδιο βαθμό f και το πλήθος αυτών s ορίζεται από τη σχέση $p-1 = fs$.
Έστω P ένα από τα πρώτα ιδεώδη $P_1, P_2 \dots, P_s$. Από τη σχέση (2.20) και επειδή το ιδεώδες P είναι πρώτο έπεται οτι $P \mid (b+\bar{b})$, δηλαδή $P^2 \mid (b+\bar{b})^2$. Επίσης $P^2 \mid q(b+\bar{b})$. Οπότε από τη σχέση (2.19) συμπεραίνουμε ότι $P^2 \mid \eta x$. Όμως η είναι μονάδα του δακτυλίου D_p και συνεπώς $P^2 \mid x$. Επειδή $x = qx_1$, όπου ο x_1 είναι ακέραιος, και $P^2 \nmid q$ έχουμε $P \mid x_1$. Επομένως $q \mid x_1$, αφού $P \bigcap \mathbb{Z} = q\mathbb{Z}$. Άρα $q^2 \mid x$.
Επειδή

$$\frac{x^p - 1}{x-1} = x^{p-1} + x^{p-2} + \dots + x + 1 = pu^q \text{ και } q^2 \mid x \tag{2.22}$$

προκύπτει ότι $pu^q \equiv 1 \pmod{q^2}$ και συνεπώς

$$p^{q-1} u^{\varphi(q^2)} \equiv 1 \pmod{q^2}. \tag{2.23}$$

Επειδή $\gcd(u, q^2) = 1$ έχουμε $u^{\varphi(q^2)} \equiv 1 \pmod{q^2}$. Άρα, από τη σχέση (1.23) έπεται ότι $p^{q-1} \equiv 1 \pmod{q^2}$, δηλαδή $p^q \equiv p \pmod{q^2}$.
Επειδή η εξίσωση $x^p - y^q = 1$ γράφεται $(-y)^q - (-x)^p = 1$ μπορούμε στις σχέσεις της περίπτωσης (i) τα x, y, p, q να τα αντικαταστήσουμε με $-y, -x, q, p$ και έτσι αποδεικνύεται και η περίπτωση (ii).

□

Κεφάλαιο 3

Το πρώτο θεώρημα του Mihăilescu

Οι ισοδυναμίες του Inkeri ισχύουν στην περίπτωση όπου $q \nmid h_p$ και $p \nmid h_q$.
Η πρώτη σημαντική ιδέα του Mihăilescu ήταν η εύρεση μίας μεθόδου μέσω της οποίας θα έχουμε αποδείξει τις ισοδυναμίες του Inkeri χωρίς τους παραπάνω περιορισμούς.
Η βασική ιδέα του Mihăilescu ήταν να χρησιμοποιήσει το ιδεώδες του Stickelberger.

3.1 Το ιδεώδες του Stickelberger

Έστω K ένας αντιμεταθετικός δακτύλιος και H μία πεπερασμένη ομάδα.
Ορίζουμε το σύνολο

$$K[H] := \{\sum_{\sigma \in G} \lambda_\sigma \cdot \sigma : \lambda_\sigma \in K\}.$$

Στο σύνολο $K[H]$ ορίζουμε πρόσθεση και πολλαπλασιασμό ως εξής:

$$\sum_{\sigma \in G} \lambda_\sigma \cdot \sigma \oplus \sum_{\tau \in G} \mu_\tau \cdot \tau = \sum_{t \in G} (\lambda_t + \mu_t) \cdot t$$

και

$$\sum_{\sigma \in G} \lambda_\sigma \cdot \sigma \odot \sum_{\tau \in G} \mu_\tau \cdot \tau = \sum_{t \in G} \nu_t \cdot t,$$

όπου

$$\nu_t = \sum_{\substack{\sigma, \tau \in G \\ \sigma\tau = t}} \lambda_\sigma \mu_\tau.$$

Το $(K[H], \oplus, \odot)$ αποτελεί δακτύλιο και λέγεται δακτύλιος της ομάδας H υπεράνω του δακτυλίου K.

Έστω το κυκλοτομικό σώμα αριθμών $K_p = \mathbb{Q}(\zeta)$. Αν $G :=\mathrm{Gal}(K_p/\mathbb{Q})$, τότε

$$G = \{\sigma_1,\ \sigma_2,\ \ldots\ ,\ \sigma_{p-1}\},$$

όπου $\sigma_a(\zeta) = \zeta^a$, για κάθε $a \in (\mathbb{Z}/p\mathbb{Z})^*$.
Έστω $\{x\}$ το κλασματικό μέρος του ρητού αριθμού x, δηλαδή $x - \{x\} = [x] \in \mathbb{Z}$ και $0 \leq \{x\} < 1$. Το στοιχείο

$$\theta = \sum_{a=1}^{p-1} \Big\{\frac{a}{p}\Big\}\sigma_a^{-1} \in \mathbb{Q}[G]$$

λέγεται στοιχείο του Stickelberger.
Το ιδεώδες του Stickelberger $I(p)$ ορίζεται να είναι $\mathbb{Z}[G] \bigcap \theta\mathbb{Z}[G]$, δηλαδή αποτελείται από τα $\mathbb{Z}[G]-$πολλαπλάσια του θ που έχουν ακέραιους συντελεστές.

Θεώρημα 3.1.1

Έστω $I'(p)$ ένα ιδεώδες του $\mathbb{Z}[G]$ που παράγεται από στοιχεία της μορφής $c - \sigma_c$, με $\gcd(c, p) = 1$. Αν $\beta \in \mathbb{Z}[G]$, τότε

$$\beta\theta \in \mathbb{Z}[G] \Leftrightarrow \beta \in I'(p).$$

Άρα $I(p) = \theta I'(p)$.

Θεώρημα 3.1.2 (Stickelberger)

Έστω A ένα κλασματικό ιδεώδες του K_p και $\beta \in \mathbb{Z}[G]$. Αν $\beta\theta \in \mathbb{Z}[G]$, τότε το ιδεώδες $A^{\beta\theta}$ είναι κύριο. Επομένως, το ιδεώδες του Stickelberger μηδενίζει (annihilates) την ομάδα κλάσεων ιδεωδών του K_p.
([39], Παράγραφος 6.2)

Έχουμε

$$\Theta_c = (c - \sigma_c)\theta = \sum_{a=1}^{p-1}\Big(c\Big\{\frac{a}{p}\Big\} - \Big\{\frac{ac}{p}\Big\}\Big)\sigma_a^{-1} = \sum_{a=1}^{p-1}\Big(\Big[\frac{ac}{p}\Big] - c\Big[\frac{a}{p}\Big]\Big)\sigma_a^{-1}.$$

Ειδικότερα,

$$\Theta_2 = \sum_{a=\frac{p+1}{2}}^{p-1} \sigma_a^{-1}.$$

Ορίζουμε $\lambda := (1-\zeta)^\Theta$ για κάποιο $\Theta \in I(p)$. Ο $\lambda/\overline{\lambda}$ είναι μία ρίζα της μονάδας. Επίσης αν ε είναι μία μονάδα του D_p, τότε $\varepsilon/\overline{\varepsilon}$ είναι μία ρίζα της μονάδας ([39], Κεφάλαιο 1 και χρήση Λήμματος 1.6). Τέλος επειδή κάθε ρίζα της μονάδας στο K_p είναι μία $2p-$ρίζα της μονάδας και $\gcd(q, 2p) = 1$ έπεται ότι κάθε ρίζα της μονάδας είναι $q-$δύναμη μίας $2p-$ρίζας της μονάδας.

3.2 Το θεώρημα του Mihăilescu

Λήμμα 3.2.1

Έστω P ένα ακέραιο πρώτο ιδεώδες του δακτυλίου A των ακεραίων αλγεβρικών αριθμών ενός αλγεβρικού σώματος αριθμών K με norm δύναμη πρώτου αριθμού q.
Αν $a, b \in A$ με $a^q \equiv b^q \pmod{P}$, τότε $a^q \equiv b^q \pmod{P^2}$.

Απόδειξη:

Αν $N_K(P) = q^r$, τότε $|A/P| = N_K(P) = q^r$. Επειδή το πρώτο ιδεώδες P είναι μέγιστο ο δακτύλιος A/P είναι σώμα. Άρα $t^{q^r} \equiv t \pmod{P}$, για κάθε $t \in A$. Οπότε υψώνοντας και τα δύο μέλη της ισοδυναμίας $a^q \equiv b^q \pmod{P}$ στην $q^{r-1}-$δύναμη προκύπτει ότι $a \equiv a^{q^r} \equiv b^{q^r} \equiv b \pmod{P}$. Αν $c := a - b$, τότε $c \equiv 0 \pmod{P}$.
Επομένως

$$a^q - b^q = (b+c)^q - b^q = \sum_{j=1}^{q} \binom{q}{j} c^j b^{q-j} \equiv 0 \ \Big(\mathrm{mod}\ (qc, c^q)\Big).$$

Όμως $P^2 \mid qc$ και $P^2 \mid c^q$. Συνεπώς $a^q \equiv b^q \pmod{P^2}$.

□

Θεώρημα 3.2.1

Αν υποθέσουμε ότι η εξίσωση $X^p - Y^q = 1$ έχει ακέραια λύση (x, y), όπου p, q είναι περιττοί πρώτοι και $xy \neq 0$, τότε $q^2 \mid x$, $p^2 \mid y$ και

$$p^{q-1} \equiv 1 \pmod{q^2}, \tag{3.1}$$
$$q^{p-1} \equiv 1 \pmod{p^2}. \tag{3.2}$$

Απόδειξη:

Υποθέτουμε ότι η εξίσωση $X^p - Y^q = 1$ έχει ακέραια λύση (x, y) με $xy \neq 0$.
Σύμφωνα με τα Θεωρήματα 1.6.2 και 2.2.1 έχουμε

$$\frac{x^p - 1}{x - 1} = (x - \zeta)(x - \zeta^2) \dots (x - \zeta^{p-1}) = pu^q \tag{3.3}$$

και

$$x \equiv 1 \pmod{p}, \tag{3.4}$$

όπου u είναι ακέραιος > 1 και $p \nmid u$.
Επίσης $p = (1 - \zeta)(1 - \zeta^2) \dots (1 - \zeta^{p-1})$ και συνεπώς η εξίσωση (3.3) γράφεται

$$\prod_{i=1}^{p-1} \beta_i = u^q, \qquad \text{με} \qquad \beta_i = \frac{x - \zeta^i}{1 - \zeta^i}. \tag{3.5}$$

Οι παράγοντες β_i ανήκουν στο δακτύλιο $D_p = \mathbb{Z}[\zeta_p]$ των ακεραίων αλγεβρικών αριθμών του $K_p = \mathbb{Q}(\zeta_p)$. Πράγματι, λόγω της σχέσης (3.4) έχουμε

$$x - \zeta^i \equiv 1 - \zeta^i \equiv 0 \ \Big(\mathrm{mod}\ (1 - \zeta^i)\Big)$$

και έτσι οι β_i είναι αλγεβρικοί ακέραιοι.
Από τη σχέση (3.5), αν περάσουμε στα ιδεώδη, έχουμε $\prod_{i=1}^{p-1} < \beta_i > = < u >^q$.
Θα δείξουμε ότι τα ιδεώδη $< \beta_i >$ είναι ανά δύο πρώτα μεταξύ τους. Πράγματι, αν

υποθέσουμε ότι τα ιδεώδη $<\beta_i>$ και $<\beta_j>$ $(i \neq j)$ έχουν κοινό παράγοντα ένα πρώτο ιδεώδες P, δηλαδή $P \mid <\beta_i>$ και $P \mid <\beta_j>$, τότε από τη σχέση

$$(1-\zeta^i)\frac{x-\zeta^i}{1-\zeta^i} - (1-\zeta^j)\frac{x-\zeta^j}{1-\zeta^j} = \zeta^j - \zeta^i$$

προκύπτει ότι $P \mid <\zeta^j - \zeta^i>$. Όμως $<\zeta^j - \zeta^i> = <1-\zeta^i> = <1-\zeta^j> = <1-\zeta>$. Άρα $P = <1-\zeta>$. Από το Θεώρημα 1.6.2 έχουμε $p \mid x-1$. Επειδή $<p> = P^{p-1}$ έπεται ότι $P \mid \frac{x-1}{1-\zeta^i}$, δηλαδή $\beta_i = \frac{x-1}{1-\zeta^i} + 1 \equiv 1 \pmod{P}$, το οποίο είναι άτοπο αφού $\beta_i \equiv 0 \pmod{P}$.
Επομένως

$$<\beta_i> = A_i^q \qquad (i = 1, 2, \ldots, p-1), \tag{3.6}$$

όπου A_i είναι ιδεώδη του δακτυλίου D_p των ακεραίων αλγεβρικών αριθμών του σώματος $K_p = \mathbb{Q}(\zeta_p)$, ανά δύο πρώτα μεταξύ τους.
Για οποιοδήποτε στοιχείο Θ του ιδεώδους του Stickelberger έχουμε $<\beta>^\Theta = <A^\Theta>^q$, όπου $\beta = \beta_1$ και $A = A_1$. Όμως το Θ δρα στο A και δίνει κύριο ιδεώδες. Συνεπώς, υπάρχει $a \in A$ τέτοιο ώστε $A^\Theta = <a>$. Οπότε $<\beta>^\Theta = <a>^q$. Άρα

$$\Big(\frac{1-\zeta^{-1}x}{1-\zeta^{-1}}\Big)^\Theta = \Big(\frac{x-\zeta}{1-\zeta}\Big)^\Theta = \varepsilon a^q, \tag{3.7}$$

όπου ε είναι μονάδα του D_p.
Αν θέσουμε $\lambda := (1-\zeta^{-1})^\Theta$, τότε $\overline{\lambda} = \lambda\delta^q$, όπου δ είναι μία $2p-$ρίζα της μονάδας. Συνεπώς $\overline{\lambda}\varepsilon = \lambda\varepsilon\delta^q$.
Επίσης

$$\Big(\frac{1-\zeta x}{1-\zeta}\Big)^\Theta = \Big(\frac{x-\zeta^{-1}}{1-\zeta^{-1}}\Big)^\Theta = \varepsilon\overline{a}^q. \tag{3.8}$$

Αφαιρώντας την εξίσωση (3.8) από την εξίσωση (3.7) προκύπτει ότι

$$(1-x\zeta^{-1})^\Theta - (1-x\zeta)^\Theta = \lambda\varepsilon\Big(a^q - (\delta\overline{a})^q\Big). \tag{3.9}$$

Από το Θεώρημα 1.6.2 έχουμε $q \mid x$. Άρα, το αριστερό μέλος της εξίσωσης (3.9) είναι $1-1 \equiv 0 \pmod{q}$. Έστω Q ένα οποιοδήποτε πρώτο ιδεώδες του $K_p = \mathbb{Q}(\zeta)$ που διαιρεί το q. Από τη σχέση (3.9) έπεται ότι $Q \mid \lambda\varepsilon\Big(a^q - (\delta\overline{a})^q\Big)$. Επειδή ε είναι μονάδα και $Q \nmid \lambda$ έχουμε $Q \mid a^q - (\delta\overline{a})^q$ και έτσι, από το Λήμμα 3.2.1, $Q^2 \mid a^q - (\delta\overline{a})^q$.
Αν $\Theta = \sum_{i=1}^{p-1} a_i\sigma_i$, όπου $a_i \in \mathbb{Z}$ και $\sigma_i \in G$, τότε

$$(1-x\zeta)^\Theta = (1-x\zeta)^{\sum_{i=1}^{p-1} a_i\sigma_i} = \prod_{i=1}^{p-1}(1-x\zeta)^{a_i\sigma_i} = \prod_{i=1}^{p-1}(1-x\zeta^i)^{a_i}.$$

Όμως

$$\prod_{i=1}^{p-1}(1-x\zeta^i)^{a_i} \equiv \prod_{i=1}^{p-1}(1-a_ix\zeta^i) \pmod{x^2} \equiv 1 - x\sum_{i=1}^{p-1} a_i\zeta^i \pmod{x^2}.$$

Άρα

$$(1-x\zeta)^{\Theta} \equiv 1 - x\sum_{i=1}^{p-1} a_i\zeta^i \pmod{x^2}. \tag{3.10}$$

Αν στην εξίσωση (3.10) εφαρμόσουμε τη μιγαδική συζυγία προκύπτει η ισοδυναμία

$$(1-x\zeta^{-1})^{\Theta} \equiv 1 - x\sum_{i=1}^{p-1} a_i\zeta^{-i} \pmod{x^2}. \tag{3.11}$$

Από τις σχέσεις (3.10) και (3.11) έπεται ότι

$$(1-x\zeta^{-1})^{\Theta} - (1-x\zeta)^{\Theta} \equiv x\sum_{i=1}^{p-1}(a_i - a_{p-i})\zeta^i \pmod{x^2}. \tag{3.12}$$

Από τη σχέση (3.9) και επειδή $Q^2 \mid a^q - (\delta\overline{a})^q$ έχουμε $Q^2 \mid (1-x\zeta^{-1})^{\Theta} - (1-x\zeta)^{\Theta}$. Όμως $Q^2 \mid x^2$ και συνεπώς από τη σχέση (3.12) προκύπτει ότι

$$x\sum_{i=1}^{p-1}(a_i - a_{p-i})\zeta^i \equiv 0 \pmod{Q^2}. \tag{3.13}$$

Επομένως, από τη σχέση (3.13) και επειδή $Q \mid x$ έχουμε $Q^2 \mid x$ ή

$$\sum_{i=1}^{p-1}(a_i - a_{p-i})\zeta^i \equiv 0 \pmod{Q}. \tag{3.14}$$

Θα δείξουμε ότι η ισοδυναμία (3.14) δε μπορεί να ισχύει. Πράγματι, αν η ισοδυναμία (3.14) ισχύει για κάθε πρώτο ιδεώδες Q του q, τότε $q \mid \sum_{i=1}^{p-1}(a_i - a_{p-i})\zeta^i$. Επομένως, από το Λήμμα 2.1.1 ισχύει $q \mid a_i - a_{p-i}$, για κάθε $i = 1, \ldots, p-1$.
Για $\Theta = \Theta_2$, δηλαδή $\sum_{i=1}^{p-1} a_i\sigma_i = \sum_{i=\frac{p+1}{2}}^{p-1} \sigma_i^{-1}$ προκύπτει ότι

$$\begin{aligned} a_i &= 1, \qquad i = 1, \ldots, \frac{p-1}{2} \\ a_i &= 0, \qquad i = \frac{p+1}{2}, \ldots, p-1. \end{aligned}$$

Οπότε $q \mid a_{\frac{p-1}{2}} - a_{\frac{p+1}{2}} = 1 - 0 = 1$, το οποίο είναι άτοπο. Άρα $Q^2 \mid x$. Επειδή το ιδεώδες Q ήταν ένα οποιοδήποτε πρώτο ιδεώδες του q έπεται ότι $Q_i^2 \mid x$ για όλα τα πρώτα ιδεώδη $Q_1, Q_2, \ldots, Q_s$ του q. Όμως τα Q_i^2 και Q_j^2 $(i \neq j)$ είναι πρώτα μεταξύ τους και συνεπώς και το γινόμενό τους, το οποίο είναι q^2, διαιρεί το x.
Από το Θεώρημα 1.6.2 και επειδή $q^2 \mid x$ έχουμε $p^{q-1}a^q \equiv -1 \pmod{q^2}$. Επίσης επειδή $\gcd(p,q) = 1$ ισχύει $p^{q-1} \equiv 1 \pmod{q}$. Οπότε προκύπτει ότι $a^q \equiv -1 \pmod{q}$, δηλαδή $a^q \equiv (-1)^q \pmod{q}$. Από την τελευταία ισοδυναμία έπεται ότι $a^q \equiv -1 \pmod{q^2}$. Άρα $p^{q-1} \equiv -p^{q-1}a^q \equiv 1 \pmod{q^2}$.
Επειδή η εξίσωση $x^p - y^q = 1$ γράφεται $(-y)^q - (-x)^p = 1$ μπορούμε τα x, y, p, q να τα αντικαταστήσουμε με τα $-y, -x, q, p$. Επομένως $p^2 \mid y$ και $q^{p-1} \equiv 1 \pmod{p^2}$.

□

Ορισμός 3.2.1

Ζευγάρια (p, q) πρώτων αριθμών που ικανοποιούν τις ισοδυναμίες του Θεωρήματος 3.2.1 λέγονται ζευγάρια Wieferich.

Μέχρι σήμερα μόνο 6 ζευγάρια Wieferich είναι γνωστά και είναι τα εξής:

$$(2, 1093),\ (3, 1006003),\ (5, 1645333507),\ (83, 4871),$$

$$(911, 318917),\ (2903, 18787).$$

Κεφάλαιο 4

Γραμμικές μορφές λογαρίθμων

Η ιδέα του Tijdeman [38] ήταν να εφαρμόσει τη θεωρία γραμμικών μορφών λογαρίθμων αλγεβρικών (ρητών) αριθμών και, πιο συγκεκριμένα, το ακόλουθο

Θεώρημα 4.0.2 (Baker,[6])
Υποθέτουμε ότι $b_j \in \mathbb{Z},\ r_j \in \mathbb{Q},\ r_j > 0$ *για κάθε* $j = 1, 2, \ldots, n$ *και*

$$\Lambda := b_1 \log r_1 + b_2 \log r_2 + \ldots + b_n \log r_n.$$

Για κάθε ρητό αριθμό $r = \frac{s}{t}$ *με* $\gcd(s,t) = 1$ *ορίζουμε το ύψος του* r

$$H(r) := \log \max(|s|, |t|).$$

Αν $B := \max\Big(|b_1|, |b_2|, \ldots, |b_n|\Big)$ *και* $\Lambda \neq 0$, *τότε*

$$|\Lambda| \geq \log(-C \log B),$$

όπου C *είναι μία υπολογίσιμη θετική σταθερά, η οποία εξαρτάται μόνο από το* n *και από τα ύψη των* $r_1, r_2, \ldots, r_n$. *Μάλιστα* $C = c(n)H(r_1)H(r_2)\ldots H(r_n)$.

Όταν κάποιος θέλει να είναι συγκεκριμένος η αριθμητική τιμή της σταθεράς $c(n)$ είναι πολύ σημαντική.
Ο E. Matveev απέδειξε ότι μπορεί κανείς να πάρει την $c(n) = c^n$, όπου c είναι μία υπολογίσιμη απόλυτη σταθερά.

Αν τώρα (x, y, p, q) είναι μία, μη-τετριμμένη, λύση της εξίσωσης του Catalan και a, b οι ακέραιοι του Θεωρήματος 1.6.2, ορίζουμε

$$\Lambda_1 := q \log q - p \log p + pq \log \frac{pa}{qb}.$$

Έχουμε

$$\Lambda_1 = \log \frac{(p^{q-1}a^q)^p}{(q^{p-1}b^p)^q} = \log \frac{(x-1)^p}{(y+1)^q} = p \log(x-1) - q \log(y+1).$$

Επίσης ορίζουμε τη γραμμική μορφή

$$\Lambda_2 := q \log q + p \log \frac{p^{q-1}a^q + 1}{q^q b^q}.$$

Έχουμε

$$\Lambda_2 = \log \frac{y^q + 1}{(y+1)^q} = \log \frac{x^p}{(y+1)^q} = p \log x - q \log(y+1).$$

Επειδή

$$(x-1)^p < x^p = y^q + 1 < (y+1)^q$$

έπεται ότι

$$\Lambda_1 \neq 0 \text{ και } \Lambda_2 \neq 0.$$

Άρα, μπορούμε να εφαρμόσουμε το Θεώρημα του Baker και να βρούμε κάτω φράγματα των $|\Lambda_1|$ και $|\Lambda_2|$. Από τις δύο αυτές σχέσεις προκύπτουν δύο ανισότητες ανάμεσα στα p και q. Υποθέτουμε ότι $q < p$ και απαλοίφουμε το q, οπότε τελικά προκύπτει μία ανισότητα της μορφής

$$p < c_1 (\log p)^{c_2},$$

όπου c_1 και c_2 απόλυτες σταθερές. Έχουμε δηλαδή ένα άνω φράγμα για το p και συνεπώς και για το q. (Αν $p < q$ εργαζόμαστε όμοια και βρίσκουμε ένα άνω φράγμα για το q.)
Το σημαντικότατο συμπέρασμα του αποτελέσματος του Tijdeman ήταν ότι η εξίσωση του Catalan έχει το πολύ πεπερασμένο πλήθος λύσεων.
Ο M. Langevin επεξεργάστηκε την απόδειξη του Tijdeman και έδωσε συγκεκριμένα φράγματα $p, q \leq 10^{110}$. Ακολούθησαν μία σειρά από καλύτερα φράγματα μέχρι το 2000 που ο M. Mignotte [24] απέδειξε ότι

$$p \leq 7,8 \cdot 10^{16} \text{ και } q \leq 7,2 \cdot 10^{11}.$$

Από το θεώρημα του Tijdeman προκύπτει η ανισότητα

$$p \leq 24,34 \cdot q \Big(\max\{\log \frac{p+1}{\log q} + 0,14,\ 21\} \Big)^2 \log q. \tag{4.1}$$

Συνδυάζοντας τα αποτελέσματα των Tijdeman και Mihăilescu, οι Mignotte και Roy [25] απέδειξαν ότι

$$\min\{p, q\} \geq 10^7. \tag{4.2}$$

Με βάση την ανισότητα (4.1) του Tijdeman θα αποδείξουμε την ακόλουθη

Πρόταση 4.0.1
Αν $q \geq 28000$, τότε $p \leq 4q^2$.

Απόδειξη:

Υποθέτουμε ότι

$$\log\frac{p+1}{\log q}+0,14\leq 21.$$

Αν $p\geq 4q^2$, τότε από τη σχέση (4.1) θα είχαμε $4q^2\leq 24,34\cdot q21^2\log q$, δηλαδή $q\leq 2683,5\log q$, το οποίο δεν ισχύει για $q\geq 28000$.
Αν τώρα

$$\log\frac{p+1}{\log q}+0,14\geq 21,$$

τότε η ανισότητα (4.1) γράφεται

$$p\leq 24,34\cdot q\Big(\log\frac{p+1}{\log q}+0,14\Big)^2\log q.$$

Επειδή $q\geq 28000$ έχουμε $0,14-\log\log q\leq 0,14-\log\log 28000\leq -2,18$.
Συνεπώς

$$\frac{p}{\Big(\log(p+1)-2,18\Big)^2}\leq 24,34\cdot q\log q. \tag{4.3}$$

Αν

$$f(p):=\frac{p}{\Big(\log(p+1)-2,18\Big)^2},$$

τότε $f'(p)>0$, για κάθε $p\geq 67$.
Επομένως, αν υποθέσουμε ότι $p\geq 4q^2$, αντικαθιστούμε στη σχέση (4.3) το p με $4q^2$ και έχουμε

$$q\leq 6,085\Big(\log(4q^2+1)-2,18\Big)^2\log q.$$

Επειδή $\log(4q^2+1)-2,18\leq\log q^2$ προκύπτει ότι $q\leq 24,34\log^3 q$, το οποίο είναι αδύνατο για $q\geq 28000$.

□

Θεώρημα 4.0.3

Αν (x,y,p,q) είναι λύση της εξίσωσης του Catalan, τότε $p\not\equiv 1\pmod q$ και, για λόγους συμμετρίας, $q\not\equiv 1\pmod p$.

Απόδειξη:

Αν υποθέσουμε ότι $p\equiv 1\pmod q$, τότε $p^q\equiv 1\pmod{q^2}$. Όμως οι p,q είναι αριθμοί του Wieferich, δηλαδή ικανοποιούν την ισοδυναμία $p^{q-1}\equiv 1\pmod{q^2}$.
Άρα

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

Επειδή ο p είναι περιττός πρώτος έχουμε $p\neq q^2+1$ και $p\neq 3q^2+1$. Επίσης ισχύει $p\neq 2q^2+1$. Πράγματι, αν $p=2q^2+1$ και επειδή από τη σχέση (4.2) έχουμε $q\neq 3$, τότε

$p = 2q^2 + 1 \equiv 0 \pmod 3$. Όμως $p > q$ και έτσι καταλήγουμε σε άτοπο.
Επομένως $p \geq 4q^2 + 1 > 4q^2$. Όμως αν $q \geq 28000$ αυτό δεν ισχύει σύμφωνα με την Πρόταση 4.0.1. Από την άλλη μεριά, ο Mihăilescu απέδειξε, με χρήση του υπολογιστή και χρόνο μικρότερο του ενός λεπτού, ότι δεν υπάρχει ζευγάρι (p, q) τέτοιο ώστε $q \leq 28000$,

$$1 + 4q^2 \leq p \leq 24,34 \cdot q\Big(\max\{\log \frac{p+1}{\log q} + 0,14,\ 21\}\Big)^2 \log q,$$

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

□

Παρατηρήση:

Θα ήταν πολύ ενδιαφέρον να έχουμε μία πλήρη αλγεβρική απόδειξη ότι $p \not\equiv 1 \pmod q$ ή τουλάχιστον μία απόδειξη ανεξάρτητη των ηλεκτρονικών υπολογιστών. Αυτό επιτεύχθηκε και πάλι από τον Mihăilescu.

Κεφάλαιο 5

Η απόδειξη του Mihăilescu

5.1 Δακτύλιοι και Modules

Στην παράγραφο αυτή όλοι οι δακτύλιοι είναι αντιμεταθετικοί με μοναδιαίο.

Το ιδεώδες A ενός δακτυλίου R λέγεται ριζικό αν ο δακτύλιος πηλίκο R/A δεν έχει μη-μηδενικά μηδενοδύναμα στοιχεία. Δηλαδή το A είναι ριζικό ιδεώδες του R αν για κάθε $a \in R$ και κάθε θετικό ακέραιο m ισχύει:

$$a^m \in A \Rightarrow a \in A.$$

Έστω R ένας δακτύλιος. Το M λέγεται $R-$module όταν:
(1) Το M είναι προσθετική αβελιανή ομάδα.
(2) Υπάρχει μία εξωτερική πράξη

$$\begin{aligned} R \times M &\rightarrow M \\ (r, m) &\mapsto r \cdot m \end{aligned}$$

τέτοια ώστε για όλα τα $r, r_1, r_2 \in R$ και $m, m_1, m_2 \in M$ να ισχύουν:
(i) $(r_1 + r_2)m = r_1 m + r_2 m$
(ii) $r(m_1 + m_2) = rm_1 + rm_2$
(iii) $r_1(r_2 m) = (r_1 r_2)m$.
Αν επιπλέον ισχύει η
(iv) $1 \cdot m = m$, τότε το M λέγεται μοναδιαίο (unitary) $R-$module.

Αν $N \subseteq M$, τότε το N λέγεται υποmodule του M όταν το N είναι επίσης $R-$module ως προς τις πράξεις του M. Επίσης η προσθετική ομάδα πηλίκο M/N γίνεται $R-$module αν ορίσουμε $r(m + N) = rm + N,\ r \in R,\ m \in M$.

Έστω R ένας δακτύλιος και M ένα $R-$module. Αν $S \subseteq M$, τότε ο $R-$μηδενιστής ($R-$annihilator) του S είναι όλα εκείνα τα $a \in R$ για τα οποία $aS = 0$ και είναι ιδεώδες του R (για περισσότερες πληροφορίες στα modules παραπέμπουμε στο [5]).

Στη συνέχεια θα αναφέρουμε κάποιες προτάσεις όσον αφορά στα $R-$modules και θα μελετήσουμε δακτύλιους R οι οποίοι είναι ευθύ γινόμενο σωμάτων.

Έστω R ένας δακτύλιος και M ένα $R-$module. Το M λέγεται κυκλικό αν παράγεται από ένα στοιχείο, δηλαδή αν υπάρχει $m \in M$ τέτοιο ώστε $M = Rm$.

Αν $M = Rm$ είναι ένα κυκλικό $R-$module, τότε ann(M)=ann(m) και το M είναι ισόμορφο, ως $R-$module, με το δακτύλιο πηλίκο $R/\text{ann(M)}$.

Επειδή τα υπomodules του $R/\text{ann(M)}$ είναι τα ιδεώδη του δακτυλίου $R/\text{ann(M)}$ έχουμε μία ένα προς ένα αντιστοιχία ανάμεσα στα υπomodules του M και τα ιδεώδη του $R/\text{ann(M)}$. Η αντιστοιχία αυτή περιγράφεται ως εξής: Αν A είναι ένα ιδεώδες του $R/\text{ann(M)}$, τότε το αντίστοιχο υπomodule του M είναι Am. Αντίστροφα, αν N είναι ένα υπomodule του M, τότε το αντίστοιχο ιδεώδες A αποτελείται απ' όλα τα $a \in R$ για τα οποία $am \in N$.

Αν N είναι ένα υπomodule του κυκλικού $R-$module $M = Rm$, τότε το πηλίκο M/N είναι ένα κυκλικό $R-$module που παράγεται από την εικόνα του m. Επίσης αν ο R είναι δακτύλιος κυρίων ιδεωδών, τότε και ο $R/\text{ann(M)}$ είναι δακτύλιος κυρίων ιδεωδών. Επομένως, ισχύει η παρακάτω πρόταση:

Πρόταση 5.1.1

Αν R είναι ένας δακτύλιος και M ένα κυκλικό $R-$module, τότε κάθε πηλίκο του M είναι κυκλικό. Αν R είναι δακτύλιος κυρίων ιδεωδών, τότε κάθε υπomodule ενός κυκλικού $R-$module είναι επίσης κυκλικό.

Έστω R ένας δακτύλιος και M ένα $R-$module. Το M λέγεται πεπερασμένα παραγόμενο αν παράγεται από πεπερασμένου πλήθους στοιχεία, δηλαδή αν υπάρχουν $m_1, m_2, \ldots, m_n \in M$ τέτοια ώστε $M = Rm_1 + Rm_2 + \ldots + Rm_n$.

Πρόταση 5.1.2

Έστω R ένας δακτύλιος και M ένα πεπερασμένα παραγόμενο $R-$module. Αν A είναι ένα ιδεώδες του R τέτοιο ώστε το ιδεώδες $A+ann_R(M)$ του R να είναι ριζικό, τότε ο $ann_{R/A}(M/AM)$ είναι η εικόνα του $ann_R(M)$ στον R/A.

Απόδειξη:

Θέτουμε $\overline{R} := R/A$ και $\overline{M} := M/AM$.
Αν $a \in \text{ann}_R(M)$, δηλαδή $a \in R$ τέτοιο ώστε $aM = 0$, τότε η εικόνα του a στον $\overline{R}$ είναι $\overline{a} = a + A$. Θα δείξουμε ότι το $\overline{a}$ μηδενίζει (annihilates) το $\overline{M}$. Πράγματι, αν $\overline{m} \in \overline{M}$, δηλαδή $\overline{m} = m + AM$, όπου $m \in M$, τότε

$$\overline{a} \cdot \overline{m} = (a + A)(m + AM) = am + AM = 0 + AM = AM,$$

δηλαδή το $\overline{a}$ μηδενίζει (annihilates) το $\overline{M}$.
Αντίστροφα, αν $\overline{a} \in \text{ann}_{\overline{R}}(\overline{M})$, δηλαδή $\overline{a} \in \overline{R}$ τέτοιο ώστε $\overline{a}\ \overline{m} = AM,\ \forall \overline{m} \in \overline{M}$, τότε $am \in AM,\ \forall m \in M$. Έστω φ ένας ενδομορφισμός του M τέτοιος ώστε $\varphi(M) \subseteq AM$. Σύμφωνα με το ([1], Πρόταση 2.4) υπάρχει θετικός ακέραιος n τέτοιος ώστε

$$\varphi^n + \beta_1\varphi^{n-1} + \ldots + \beta_n = 0,$$

όπου $\beta_1, \ldots, \beta_n \in A$. Επειδή $aM \subseteq AM$ θεωρούμε ως φ τον παρακάτω ενδομορφισμό: $a(m) := am \in AM$.

Άρα $a^n+\beta_1 a^{n-1}+\ldots+\beta_n = 0$, δηλαδή $(a^n+\beta_1 a^{n-1}+\ldots+\beta_n)(m) = 0(m) = 0,\ \forall m \in M$ και επομένως $\gamma := a^n + \beta_1 a^{n-1} + \ldots + \beta_n \in \mathrm{ann}_R(M)$.
Οπότε $a^n = \gamma - (\beta_1 a^{n-1} - \ldots - \beta_n) \in A+\mathrm{ann}_R(M)$. Όμως το ιδεώδες $A+\mathrm{ann}_R(M)$ είναι ριζικό ιδεώδες του R και συνεπώς $a \in A+\mathrm{ann}_R(M)$, δηλαδή $a = \alpha + \beta$, όπου $\alpha \in A$ και $\beta \in \mathrm{ann}_R(M)$. Από την τελευταία σχέση έπεται ότι η εικόνα $\overline{\beta}$ του β στον $\overline{R}$ είναι $\overline{\beta} = \beta + A = a + A = \overline{a}$.

□

Πρόταση 5.1.3

Αν R είναι ευθύ γινόμενο από πεπερασμένα το πλήθος σωμάτα, δηλαδή

$$R = K_1 \times K_2 \times \ldots \times K_s$$

και θέσουμε $A = \{1, 2, \ldots, s\}$, τότε

(1) Αν $B \subseteq A$, τότε το σύνολο $I(B) := \{(x_1, x_2, \ldots, x_s) \in R : x_\beta = 0,\ \forall \beta \in B\}$ είναι ιδεώδες του R και όλα τα ιδεώδη είναι αυτής της μορφής για κάποιο υποσύνολο B του A. Ειδικότερα, κάθε πηλίκο του R είναι ευθύ γινόμενο σωμάτων.

(2) Αν $B, \Gamma \subseteq A$, τότε

$$I(B)I(\Gamma) = I(B \cup \Gamma) \qquad \text{και} \qquad I(B) + I(\Gamma) = I(B \cap \Gamma).$$

Οπότε αν I, I' είναι δύο ιδεώδη του R, τότε

$$II' = I \cap I'.$$

Επίσης για κάθε $b \in II'$ υπάρχουν $a \in I$ και $a' \in I'$ τέτοια ώστε $b = aa'$. Ειδικότερα, $I^2 = I$ και για κάθε $a \in I$ υπάρχουν $a_1, a_2 \in I$ τέτοια ώστε $a = a_1 a_2$.

(3) Για κάθε ιδεώδες I του R υπάρχει μοναδικό ιδεώδες $I^\perp$ του R τέτοιο ώστε

$$I + I^\perp = R \qquad \text{και} \qquad II^\perp =< 0 > .$$

Το ιδεώδες $I^\perp$ είναι το συμπληρωματικό του ιδεώδους I. Αν $I = I(B)$, για κάποιο $B \subseteq A$, τότε $I^\perp := I(A/B) = \{(x_1, x_2, \ldots, x_s) : x_\beta = 0,\ \forall \beta \notin B\}$.

(4) Αν I, I' είναι δύο ιδεώδη του R, τότε

$$(II')^\perp = I^\perp + I'^\perp \qquad \text{και} \qquad (I + I')^\perp = I^\perp I'^\perp.$$

Επίσης $II' =< 0 > \Leftrightarrow I' \subseteq I^\perp$.

(5) Αν M είναι ένα $R-$module, τότε υπάρχει $m \in M$ τέτοιο ώστε $ann_R(m) = ann_R(M)$, δηλαδή το M έχει υπομοδούλι ισόμορφο με $R/ann_R(M)$. Ειδικότερα, αν ο R είναι πεπερασμένος, τότε $|M| \geq |R/ann_R(M)|$, με την ισότητα να ισχύει αν και μόνο αν το M είναι κυκλικό.

(6) Αν M είναι ένα κυκλικό $R-$module και M' ένα υπομοδούλι του M, τότε

$$ann_R(M') + ann_R(M/M') = R$$

και

$$ann_R(M')ann_R(M/M') = ann_R(M).$$

Απόδειξη:

(1) Το σύνολο $I(B)$ είναι ιδεώδες του R, αφού αν $x, y \in I(B)$ και $r \in R$, τότε $x - y \in I(B)$ και $rx \in I(B)$.
Έστω I ένα ιδεώδες του R. Θα δείξουμε ότι $I = I(B)$, για κάποιο $B \subseteq A$. Πράγματι, αρκεί να θεωρήσουμε $B = \{a \in A : x_a = 0,\ \forall (x_a)_{a\in A} \in I\}$.

(2) Αν $I(B) = \{(x_1, \ldots, x_s) \in R : x_\beta = 0,\ \forall \beta \in B\}$ και $I(\Gamma) = \{(y_1, \ldots, y_s) \in R : y_\gamma = 0,\ \forall \gamma \in \Gamma\}$, όπου $B, \Gamma \subseteq A$, τότε

$$I(B)I(\Gamma) = \{(w_1, \ldots, w_s) = (x_1y_1, \ldots, x_sy_s) \in R : w_i = 0,\ \forall i \in B \cup \Gamma\} = I(B \cup \Gamma).$$

και

$$I(B)+I(\Gamma) = \{(z_1, \ldots, z_s) = (x_1+y_1, \ldots, x_s+y_s) \in R : z_j = 0,\ \forall j \in B\cap\Gamma\} = I(B\cap\Gamma).$$

Για οποιαδήποτε δύο ιδεώδη I, I' του R έχουμε $II' \subseteq I \cap I'$. Αν $I = I(B)$, για κάποιο $B \subseteq A$ και $I' = I(\Gamma)$, για κάποιο $\Gamma \subseteq A$, τότε $I\cap I' = I(B)\cap I(\Gamma) \subseteq I(B\cup\Gamma) = I(B)I(\Gamma)$. Επομένως $II' = I \cap I'$.

(3) Αν $I = I(B)$, για κάποιο $B \subseteq A$, τότε $I^\perp = I(A/B)$ και από το (2) έχουμε

$$I + I^\perp = I(B) + I(A/B) = I(B \cap (A/B)) = R$$

και

$$II^\perp = I(B)I(A/B) = I(B \cup (A/B)) = I(A) =< 0 > .$$

(4) Αν $I = I(B)$, για κάποιο $B \subseteq A$, και $I' = I(\Gamma)$, για κάποιο $\Gamma \subseteq A$, τότε από τις σχέσεις των (2) και (3) έπεται ότι

$$(II')^\perp = (I(B \cup \Gamma))^\perp = I(A/(B \cup \Gamma)) = I((A/B) \cap (A/\Gamma)) = I^\perp + I'^\perp$$

και

$$(I + I')^\perp = (I(B \cap \Gamma))^\perp = I(A/(B \cap \Gamma)) = I((A/B) \cup (A/\Gamma)) = I^\perp I'^\perp.$$

Επίσης αν $II' = I(B)I(\Gamma) =< 0 >$, τότε $B \cup \Gamma = A$ και συνεπώς $I' \subseteq I^\perp$. Αντίστροφα, αν $I' \subseteq I^\perp$ και $x \in II'$, τότε $x \in I$ και $x \in I' \subseteq I^\perp$, δηλαδή $x = 0$.

(5) Για $\beta \in A$ ορίζουμε το στοιχείο

$$1_\beta := \{(x_1, \ldots, x_s) : x_\beta = 1 \text{ και } x_a = 0 \text{ για } a \neq \beta\}.$$

Έστω $B \subseteq A$ τέτοιο ώστε $\mathrm{ann}_R(M) = I(B)$. Ισχυριζόμαστε ότι $\forall \beta \in B$ υπάρχει $b_\beta \in M$ τέτοιο ώστε $\mathrm{ann}_R(b_\beta) \subseteq I(\{\beta\})$. Πράγματι, ας υποθέσουμε ότι υπάρχει $\beta \in B$ τέτοιο ώστε $\forall b \in M$ να ισχύει $\mathrm{ann}_R(b) \not\subseteq I(\{\beta\})$, δηλαδή $\forall b \in M$ υπάρχει $x \in R/I(\{\beta\})$ τέτοιο ώστε $xb = 0$. Επειδή για κάθε $x \in R/I(\{\beta\})$ υπάρχει $y \in R$ τέτοιο ώστε $yx = 1_\beta$ έπεται ότι $1_\beta b = 0,\ \forall b \in M$, το οποίο είναι άτοπο διότι $1_\beta \notin \mathrm{ann}_R(M)$.
Θέτουμε $m := \sum_{\beta\in B} 1_\beta b_\beta \in M$. Αν $x = (x_a)_{a\in A} \in \mathrm{ann}_R(m)$, τότε $\forall \beta \in B$ έχουμε $xb_\beta = 1_\beta xm = 0$, δηλαδή $x \in I(\{\beta\})$, αφού $\mathrm{ann}_R(b_\beta) \subseteq I(\{\beta\})$.
Επομένως $x \in \cap_{\beta\in B} I(\{\beta\}) = I(B)$, δηλαδή $\mathrm{ann}_R(m) \subseteq \mathrm{ann}_R(M)$. Προφανώς ισχύει $\mathrm{ann}_R(M) \subseteq \mathrm{ann}_R(m)$ και συνεπώς $\mathrm{ann}_R(m) =\mathrm{ann}_R(M)$.

(6) Αν $B \subseteq A$ τέτοιο ώστε $\mathrm{ann}_R(M) = I(B)$, τότε $\mathrm{ann}_R(M') = I(B')$, όπου $B' \subseteq B$. Επειδή το M είναι κυκλικό $R-$module από το (5) έχουμε $M \cong R/I(B) \cong I(A/B)$. Επίσης $M' \cong I(A/B')$. Οπότε $a \in \mathrm{ann}_R(M/M')$ $=\mathrm{ann}_R(I(A/B)/I(A/B'))$, δηλαδή $a(x_1, \ldots, x_s) \in I(A/B')$, $\forall (x_1, \ldots, x_s) \in I(A/B)$, αν και μόνο αν $a \in I(B/B')$ και συνεπώς $\mathrm{ann}_R(M/M') = I(B/B')$. Από τις σχέσεις του (2) και επειδή $B' \cap (B/B') = \emptyset$ και $B' \cup (B/B') = B$ έπεται το ζητούμενο.

□

5.2 Δακτύλιοι ομάδας

Έστω A ένας αντιμεταθετικός δακτύλιος και G μία πεπερασμένη αβελιανή ομάδα. Θεωρούμε το δακτύλιο ομάδας $A[G]$. Ορίζουμε τη συνάρτηση βάρους $w : A[G] \to A$ ως εξής:

$$w(\sum_{\sigma \in G} n_\sigma \sigma) = \sum_{\sigma \in G} n_\sigma.$$

Η συνάρτηση βάρους είναι προσθετική και πολλαπλασιαστική και συνεπώς είναι ομομορφισμός δακτυλίων. Ο πυρήνας αυτού του ομομορφισμού που αποτελείται από τα στοιχεία βάρους 0 λέγεται το augmentation ιδεώδες του $A[G]$. Παράγεται από στοιχεία της μορφής $\sigma - \tau$, όπου $\sigma, \tau \in G$.
Το στοιχείο $N = \sum_{\sigma \in G} \sigma \in A[G]$ λέγεται norm στοιχείο του $A[G]$. Προφανώς ισχύει $xN = N$, $\forall x \in G$. Επομένως, $\forall x \in A[G]$ έχουμε $xN = w(x)N$. Ειδικότερα ισχύει $A[G]N = AN$. Το ιδεώδες $< N >= A[G]N$ λέγεται norm ιδεώδες του $A[G]$.

Πρόταση 5.2.1
Έστω G μία πεπερασμένη κυκλική ομάδα τάξης n. Αν K είναι ένα σώμα με χαρακτηριστική που δε διαιρεί το n, τότε ο δακτύλιος ομάδας $K[G]$ είναι ευθύ γινόμενο από πεπερασμένα το πλήθος σώματα.

Απόδειξη:
Αν $G =< a >$, τότε θεωρούμε την απεικόνιση $\varphi : K[x] \to K[G]$, η οποία αντιστοιχεί κάθε $f(x) \in K[x]$ στο $f(a) \in K[G]$. Η φ είναι επιμορφισμός δακτυλίων με πυρήνα $\mathrm{Ker}(\varphi) =< x^n - 1 >$. Επομένως $K[G] \cong K[x]/ < x^n - 1 >$. Επειδή η χαρακτηριστική του σώματος K δε διαιρεί το n το πολυώνυμο $x^n - 1$ είναι διαχωρίσιμο υπέρ του K, δηλαδή το $K[x]/ < x^n - 1 >$ είναι ευθύ γινόμενο πεπερασμένων επεκτάσεων του K.

□

5.3 Ο δακτύλιος $\mathbf{R = \mathbb{F}_q[G]}$ και κάποια $\mathbf{R-}$modules

Στην παράγραφο αυτή οι p, q είναι περιττοί πρώτοι με $p \neq q$ και

$$p \not\equiv 1 \pmod{q}. \tag{5.1}$$

Επίσης $\zeta := \zeta_p$ είναι μία πρωταρχική $p-$ρίζα της μονάδας, $K = \mathbb{Q}(\zeta)$, $G =\mathrm{Gal}(K/\mathbb{Q})$ και $\iota \in G$ είναι η μιγαδική συζυγία.

Τέλος E είναι η ομάδα των μονάδων του σώματος K και W είναι η ομάδα των ριζών της μονάδας του σώματος K. Θυμίζουμε ότι από το Θεώρημα του Dirichlet η ομάδα E έχει βαθμό $\frac{p-3}{2}$.

Θεωρούμε το δακτύλιο ομάδας $R = \mathbb{F}_q[G]$. Από τη σχέση (5.1) και την Πρόταση 5.2.1 έπεται ότι ο R είναι ευθύ γινόμενο σωμάτων.

Από την Πρόταση 5.1.3:3 για κάθε ιδεώδες $I \trianglelefteq R$ υπάρχει μοναδικό ιδεώδες $I^{\perp} \trianglelefteq R$ τέτοιο ώστε $I + I^{\perp} = R$ και $II^{\perp} =< 0 >$. Για παράδειγμα, $< 1+\iota >^{\perp} =< 1-\iota >$ και $< N >^{\perp}$ είναι το augmentation ιδεώδες, όπου

$$N = \sum_{\sigma \in G} \sigma \in R$$

είναι το norm στοιχείο του R.

Ο κύριος στόχος αυτής της παραγράφου είναι να μελετήσουμε την ομάδα E/E^q και να υπολογίσουμε το μηδενιστή (annihilator) αυτής. Για το σκοπό αυτό αρχικά θα μελετήσουμε την ομάδα $\overline{E} = E/W$, η οποία είναι ελεύθερη αβελιανή ομάδα βαθμού $\frac{p-3}{2}$.

Μία προσθετική αβελιανή ομάδα $A = \{a, b, c, \ldots\}$ είναι $G-$module (δες [40]) αν είναι μοναδιαίο (unitary) $\mathbb{Z}[G]-$module.

Αν η A είναι $G-$module, τότε

$$\begin{aligned} \sigma(a+b) &= \sigma a + \sigma b \\ \sigma(\tau a) &= (\sigma\tau)a \\ 1(a) &= a, \end{aligned}$$

για οποιαδήποτε στοιχεία $\sigma, \tau \in G$ και $a, b \in A$.
Αντίστροφα, αν η G δρα στην προσθετική ομάδα A σύμφωνα με τις παραπάνω σχέσεις, τότε η A γίνεται $\mathbb{Z}[G]-$module όταν $(\sum_{\sigma\in G} n_\sigma \sigma)(a) = \sum_{\sigma\in G}[n_\sigma(\sigma a)]$.

Αν η ομάδα A είναι πολλαπλασιαστική, τότε η δράση της G συμβολίζεται με a^σ και τότε $(a^\sigma)^\tau = a^{\sigma\tau}$ και $a^{\sum_{\sigma\in G} n_\sigma \sigma} = \prod_{\sigma\in G}(a^{n_\sigma\sigma})$.

Η $\overline{E}$ είναι $G-$module, αφού οι E, W είναι $G-$modules. Θέλουμε να υπολογίσουμε το μηδενιστή του $G-$module $\overline{E}$, δηλαδή όλα εκείνα τα $\Theta \in \mathbb{Z}[G]$ για τα οποία $\eta^\Theta \in W$, για κάθε $\eta \in E$.

Είναι φανερό ότι το norm στοιχείο $N = \sum_{\sigma\in G}\sigma$ ανήκει στο μηδενιστή του $\overline{E}$. Επίσης το $1-\iota$ ανήκει στο μηδενιστή του $\overline{E}$, αφού για κάθε μονάδα η το πηλίκο $\eta/\overline{\eta}$ είναι ρίζα της μονάδας. Επομένως, ο μηδενιστής του $\overline{E}$ περιέχει το ιδεώδες $(N, 1-\iota)$. Όμως περιέχει κάτι περισσότερο.

Θεώρημα 5.3.1

Ο μηδενιστής (annihilator) του $\overline{E}$ είναι το ιδεώδες I του $\mathbb{Z}[G]$ που αποτελείται από όλα τα Θ για τα οποία $2\Theta \in (N, 1-\iota)$.

Για την απόδειξη του Θεωρήματος 5.3.1 χρειαζόμαστε το παρακάτω

Λήμμα 5.3.1

Αν $a_1, \ldots, a_r \in \mathbb{Z}$ τέτοια ώστε το $\Theta = a_1\sigma_1 + \ldots + a_r\sigma_r$ να μηδενίζει το $\overline{E}$, όπου $r = \frac{p-3}{2}$ είναι ο βαθμός της E, τότε $a_1 = \ldots = a_r = 0$.

Απόδειξη:

Θεωρούμε την απεικόνιση $\lambda : E \to \mathbb{R}^r$, η οποία αντιστοιχεί κάθε $\eta \in E$ στο διάνυσμα $(\log|\eta^{\sigma_1}|, \ldots, \log|\eta^{\sigma_r}|)$. Ο πυρήνας της λ είναι το W και η εικόνα $\lambda(E)$ είναι lattice στον $\mathbb{R}^r$. Αν το Θ μηδενίζει το $\overline{E}$, τότε

$$a_1 \log|\eta^{\sigma_1}| + \ldots + a_r \log|\eta^{\sigma_r}| = 0,$$

για κάθε $\eta \in E$. Πράγματι, $a_1 \log|\eta^{\sigma_1}| + \ldots + a_r \log|\eta^{\sigma_r}| = \log|\eta^{\Theta}| = 0$, αφού $\eta^{\Theta} \in W$. Αν τα $a_1 = \ldots = a_r$ δεν ήταν όλα μηδέν, τότε η εικόνα $\lambda(E)$ θα ανήκε σ'ενα γνήσιο υποσύνολο του $\mathbb{R}^r$. Αυτό όμως είναι αδύνατο διότι η εικόνα $\lambda(E)$ είναι lattice.

□

Απόδειξη του Θεωρήματος 5.3.1:
Αν $m\Theta \in \mathrm{ann}_{\mathbb{Z}[G]}(\overline{E})$, όπου m μη-μηδενικός ακέραιος, τότε $\Theta \in \mathrm{ann}_{\mathbb{Z}[G]}(\overline{E})$, αφού αν $\eta^{m\Theta}$ είναι ρίζα της μονάδας για κάθε $\eta \in E$, τότε η^{Θ} είναι επίσης ρίζα της μονάδας.
Άρα, αν $\Theta \in I$, δηλαδή $2\Theta \in (N, 1-\iota) \subseteq \mathrm{ann}_{\mathbb{Z}[G]}(\overline{E})$, τότε $\Theta \in \mathrm{ann}_{\mathbb{Z}[G]}(\overline{E})$ και συνεπώς $I \subseteq \mathrm{ann}_{\mathbb{Z}[G]}(\overline{E})$.
Μένει να δείξουμε ότι $\mathrm{ann}_{\mathbb{Z}[G]}(\overline{E}) \subseteq I$. Θέτουμε

$$N' = \sigma_1 + \ldots + \sigma_{\frac{P-1}{2}}.$$

Επειδή $\sigma_{p-k} = \iota\sigma_k$ έχουμε $\sigma_k - \sigma_{p-k} = \sigma_k(1-\iota)$. Επομένως

$$2N' = N - N'(1-\iota) \in (N, 1-\iota),$$

δηλαδή $N' \in I$.
Έστω Θ ένα στοιχείο του $\mathbb{Z}[G]$ που μηδενίζει το $\overline{E}$. Χρησιμοποιώντας τη σχέση $\sigma_{p-k} = \iota\sigma_k$ μπορούμε να γράψουμε $\Theta = \Theta' + \iota\Theta''$, όπου Θ' και Θ'' είναι γραμμικοί συνδυασμοί των $\sigma_1, \ldots, \sigma_m$ με $m = \frac{p-1}{2}$. Αν

$$\Theta' = a'_1\sigma_1 + \ldots + a'_m\sigma_m \text{ και } \Theta'' = a''_1\sigma_1 + \ldots + a''_m\sigma_m,$$

τότε το

$$\Theta + (1-\iota)\Theta'' - (a'_m + a''_m)N'$$

είναι γραμμικός συνδυασμός των $\sigma_1, \ldots, \sigma_{m-1}$ και μηδενίζει το $\overline{E}$.
Από το Λήμμα 5.3.1 θα πρέπει

$$\Theta = -(1-\iota)\Theta'' + (a'_m + a''_m)N'$$

και συνεπώς $\Theta \in I$.

□

Θεώρημα 5.3.2

Αν $p \not\equiv 1 \pmod{q}$, τότε E/E^q είναι κυκλικό $\mathbb{F}_q[G]-$module και

$$ann_{\mathbb{F}[G]}(E/E^q) =< N > \oplus < 1-\iota > . \tag{5.2}$$

Απόδειξη:

Ο πυρήνας του φυσικού $G-$επιμορφισμού

$$\varphi : E \to \overline{E} \to \overline{E}/\overline{E}^q$$

είναι WE^q. Πράγματι,

$$\begin{aligned} \ker(\varphi) &= \{\varepsilon \in E : \overline{\varepsilon}\overline{E}^q \subseteq \overline{E}^q\} \\ &= \{\varepsilon \in E : \overline{\varepsilon} \in \overline{E}^q\} \\ &= \{\varepsilon \in E : \varepsilon W \subseteq \overline{E}^q\} \\ &= \{\varepsilon \in E : \varepsilon \in WE^q\}. \end{aligned}$$

Επειδή όλα τα στοιχεία του W είναι $q-$δυνάμεις στοιχείων του W ο πυρήνας είναι E^q. Επομένως, τα E/E^q και $\overline{E}/\overline{E}^q$ είναι ισόμορφα ως $G-$modules. Άρα, είναι ισόμορφα και ως $\mathbb{F}_q[G]-$modules. Οπότε αρκεί να δείξουμε ότι το $\overline{E}/\overline{E}^q$ είναι κυκλικό $\mathbb{F}_q[G]-$module και να βρούμε το μηδενιστή (annihilator) αυτού.
Επειδή $q \not| p-1$ ο δακτύλιος ομάδας $\mathbb{F}_q[G]$ είναι ευθύ γινόμενο σωμάτων (πεπερασμένα το πλήθος) και έτσι δεν έχει μηδενοδύναμα στοιχεία. Όμως $\mathbb{Z}[G]/q\mathbb{Z}[G] = \mathbb{F}_q[G]$ και συνεπώς το ιδεώδες $q\mathbb{Z}[G]$ είναι ριζικό ιδεώδες του $\mathbb{Z}[G]$. Επίσης, επειδή κάθε πηλίκο του $\mathbb{F}_q[G]$ είναι ευθύ γινόμενο σωμάτων κάθε ιδεώδες του $\mathbb{Z}[G]$ που περιέχει το $q\mathbb{Z}[G]$ είναι επίσης ριζικό. Άρα, το ιδεώδες $q\mathbb{Z}[G]+\mathrm{ann}_{\mathbb{Z}[G]}(\overline{E})$ είναι ριζικό ιδεώδες του $\mathbb{Z}[G]$. Από την Πρόταση 5.1.2 έπεται ότι ο $\mathbb{F}_q[G]-$μηδενιστής του $\overline{E}/\overline{E}^q$ είναι η εικόνα του $\mathrm{ann}_{\mathbb{Z}[G]}(\overline{E})$ στο $\mathbb{F}_q[G]$. Επομένως, από το Θεώρημα 5.3.1 το ιδεώδες $\mathrm{ann}_{\mathbb{F}_q[G]}(\overline{E}/\overline{E}^q)$ αποτελείται από στοιχεία $\Theta \in \mathbb{F}_q[G]$ τέτοια ώστε $2\Theta \in (N, 1-\iota)$, όπου από τώρα και έπειτα N είναι το norm στοιχείο του $\mathbb{F}_q[G]$ και όχι του $\mathbb{Z}[G]$. Όμως το 2 είναι αντιστρέψιμο στοιχείο στο $\mathbb{F}_q[G]$ και έτσι έχουμε

$$\mathrm{ann}_{\mathbb{F}_q[G]}(\overline{E}/\overline{E}^q) = (N, 1-\iota).$$

Επειδή $< N >= \mathbb{F}_q N$ και $w(N) = p-1 \neq 0$ στο $\mathbb{F}_q[G]$ τα μη-μηδενικά στοιχεία του $< N >$ έχουν μη-μηδενικό βάρος. Άρα $< N > \cap < 1-\iota >=< 0 >$ και συνεπώς

$$\mathrm{ann}_{\mathbb{F}_q[G]}(\overline{E}/\overline{E}^q) =< N > \oplus < 1-\iota > .$$

Μένει να δείξουμε ότι το $\overline{E}/\overline{E}^q$ είναι κυκλικό $\mathbb{F}_q[G]-$module. Από την Πρόταση 5.1.3:5 αρκεί να δείξουμε ότι $\left|\overline{E}/\overline{E}^q\right| = \left|\mathbb{F}_q[G]/\mathrm{ann}_{\mathbb{F}_q[G]}(\overline{E}/\overline{E}^q)\right|$.
Η ομάδα $\overline{E}$ έχει βαθμό $\frac{p-3}{2}$ και έτσι $\left|\overline{E}/\overline{E}^q\right| = q^{\frac{p-3}{2}}$. Επειδή $< N >= \mathbb{F}_q N$ η $\mathbb{F}_q-$διάσταση του κύριου ιδεώδους $< N >$ είναι 1. Επίσης η $\mathbb{F}_q-$διάσταση του κύριου ιδεώδους $< 1-\iota >$ είναι $\frac{p-1}{2}$. Οπότε η $\mathbb{F}_q-$διάσταση του $\mathrm{ann}_{\mathbb{F}_q[G]}(\overline{E}/\overline{E}^q)$ είναι $\frac{p+1}{2}$. Επομένως

$$\left|\mathbb{F}_q[G]/\mathrm{ann}_{\mathbb{F}_q[G]}(\overline{E}/\overline{E}^q)\right| = q^{p-1-\frac{p+1}{2}} = q^{\frac{p-3}{2}} = \left|\overline{E}/\overline{E}^q\right|.$$

□

Ορισμός 5.3.1

Το στοιχείο $a \in \mathbb{Z}[\zeta]$ θα λέγεται q-primary αν υπάρχει $\beta \in \mathbb{Z}[\zeta]$ τέτοιο ώστε

$$a \equiv \beta^q \pmod{q^2}.$$

Ορισμός 5.3.2

Έστω a ένα μη-μηδενικό στοιχείο του K^*. Το a λέγεται q-primary αν $a = a_1 a_2^{-1}\gamma^q$, όπου τα $a_1, a_2 \in \mathbb{Z}[\zeta]$ είναι q-primary και $\gamma \in K^*$.

Συμβολίζουμε με C και C_q τις ομάδες των κυκλοτομικών μονάδων και των q-primary κυκλοτομικών μονάδων του σώματος K. Θυμίζουμε ότι η ομάδα των κυκλοτομικών μονάδων είναι πολλαπλασιαστική και παράγεται από το $-\zeta$ και τις μονάδες της μορφής $\frac{1-\zeta^k}{1-\zeta}$, $k = 2, 3, \ldots, p-1$. Είναι υποομάδα της ομάδας E των μονάδων και έχει βαθμό $r = \frac{p-3}{2}$.

Τα $R-$modules E/CE^q, C/C_q και $C_q/(C_q \cap E^q)$, καθώς και οι μηδενιστές αυτών, παίζουν σημαντικό ρόλο στην απόδειξη της εικασίας του Catalan.

Έχουμε

$$C_q E^q/E^q \cong C_q/(C_q \cap E^q)$$

και

$$CE^q/C_q E^q \cong CC_q E^q/C_q E^q \cong C/(C \cap C_q E^q) \cong C/C_q.$$

Από την Πρόταση 5.1.1 τα παραπάνω $R-$modules είναι κυκλικά. Επομένως, από την Πρόταση 5.1.3:6 και τη σχέση (5.2) έπεται η ακόλουθη

Πρόταση 5.3.1

Τα ιδεώδη

$$I_1 = ann_{\mathbb{F}_q[G]}(E/CE^q),\ \ I_2 = ann_{\mathbb{F}_q[G]}(C/C_q),\ \ I_3 = ann_{\mathbb{F}_q[G]}(C_q/(C_q \cap E^q)) \qquad (5.3)$$

είναι ανά δύο πρώτα μεταξύ τους και

$$I_1 I_2 I_3 = (N, 1-\iota). \qquad (5.4)$$

5.4 Τα τρία βασικά θεωρήματα και η απόδειξη της εικασίας του Catalan

Όπως και πριν, στην παράγραφο αυτή οι p, q είναι περιττοί πρώτοι με $p \neq q$, $\zeta := \zeta_p$ είναι μία πρωταρχική $p-$ρίζα της μονάδας, $K = \mathbb{Q}(\zeta)$, $G =$Gal$(K/\mathbb{Q})$ και $\iota \in G$ είναι η μιγαδική συζυγία. Επίσης C και C_q είναι οι ομάδες των κυκλοτομικών μονάδων και των q-primary κυκλοτομικών μονάδων του σώματος K.

Η απόδειξη της αλήθειας της εικασίας του Catalan αποτελείται από τρία βασικά Θεωρήματα.

Στα δύο πρώτα θεωρήματα (x, y, p, q) είναι μία λύση της εξίσωσης του Catalan. Ειδικότερα, από το Θεώρημα 4.0.3 ισχύει $p \not\equiv 1 \pmod{q}$.

Θεώρημα 5.4.1

Αν $\Theta \in < N >^{\perp} < 1 + \iota > I_1 I_3$, τότε $(x-\zeta)^{\Theta} \in (K^*)^q$.

Θεώρημα 5.4.2

Υποθέτουμε ότι $q \geq 7$. Αν $(x-\zeta)^{\Theta} \in (K^*)^q$, όπου $\Theta \in < N >^{\perp} < 1+\iota >$, τότε $\Theta = 0$.

Το τρίτο θεώρημα είναι ένα γενικό αποτέλεσμα, ανεξάρτητο της εξίσωσης του Catalan.

Θεώρημα 5.4.3
Αν p, q είναι περιττοί πρώτοι με $p > q$, τότε $C_q \neq C$.

Χρησιμοποιώντας τα Θεωρήματα 5.4.1-5.4.3 θα δείξουμε ότι η εικασία του Catalan είναι αληθινή.

Έστω (x, y, p, q) λύση της εξίσωσης του Catalan. Επειδή $(-y, -x, q, p)$ είναι επίσης λύση υποθέτουμε ότι $p > q$. Επίσης μπορούμε να υποθέσουμε ότι $q \geq 7$, λόγω της σχέσης (4.2). Άρα, οι υποθέσεις των Θεωρημάτων 5.4.1-5.4.3 ικανοποιούνται.
Από τα Θεωρήματα 5.4.1 και 5.4.2 έπεται ότι $< N >^{\perp} < 1 + \iota > I_1 I_3 =< 0 >$. Από την Πρόταση 5.1.3:4 και τη σχέση $I_1 I_2 I_3 = (N, 1 - \iota)$ έχουμε

$$I_1 I_3 \subseteq (< N >^{\perp} < 1 + \iota >)^{\perp} =< N > + < 1 + \iota >^{\perp} =< N > + < 1 - \iota >= I_1 I_2 I_3.$$

Όμως από την Πρόταση 5.3.1 τα I_2 και $I_1 I_3$ είναι πρώτα μεταξύ τους, δηλαδή $I_2 + I_1 I_3 = R$. Επομένως

$$1 \in I_2 + I_1 I_3 \subseteq I_2 + I_1 I_2 I_3 \subseteq I_2 + I_2 = I_2,$$

δηλαδή $I_2 =< 1 >$. Επειδή $I_2 = \mathrm{ann}(C/C_q)$ έχουμε $C = C_q$, το οποίο είναι άτοπο από το Θεώρημα 5.4.3.

□

5.5 Η απόδειξη του θεωρήματος 5.4.1

Όπως και στην παράγραφο 5.3, στην παράγραφο αυτή E, C και C_q είναι οι ομάδες των μονάδων, των κυκλοτομικών μονάδων και των q-primary κυκλοτομικών μονάδων του σώματος K, αντίστοιχα.

Έστω H η ομάδα κλάσεων ιδεωδών του σώματος $K = \mathbb{Q}(\zeta)$ και H^+ το ″plus-part″ της H, το οποίο αποτελείται από τις κλάσεις που παραμένουν σταθερές από τη δράση της μιγαδικής συζυγίας ([2]).

Ένα στοιχείο Θ του $\mathbb{F}_q[G]$ ή $\mathbb{Z}[G]$ θα λέγεται άρτιο αν διαιρείται με $1 + \iota$. Ισοδύναμα, το $\Theta = \sum_{\sigma \in G} n_\sigma \sigma$ θα λέγεται άρτιο αν για κάθε $\sigma \in G$ έχουμε $n_\sigma = n_{\overline{\sigma}}$, όπου $\overline{\sigma} = \iota\sigma$.

Με τον όρο q-part μίας ομάδας εννοούμε την q-Sylow υποομάδα αυτής.

Θεώρημα 5.5.1 (Thaine, [37])
Αν Θ είναι ένα άρτιο στοιχείο του $\mathbb{Z}[G]$ που μηδενίζει το q-part της ομάδας E/C, τότε το Θ μηδενίζει και το q-part της H^+.

Το αποτέλεσμα του Thaine είναι πιο γενικό. Έστω L ένα πραγματικό αβελιανό σώμα και E_L, C_L, H_L και G_L οι ομάδες των μονάδων, των κυκλοτομικών μονάδων, των κλάσεων ιδεωδών και του Galois του σώματος L, αντίστοιχα. Αν q είναι ένας περιττός πρώτος που δε διαιρεί το $[L : Q]$, τότε κάθε $\Theta \in \mathbb{Z}[G_L]$ που μηδενίζει το q-part της ομάδας E_L/C_L μηδενίζει και το q-part της H_L.
Στην περίπτωσή μας $L = \mathbb{Q}(\zeta + \overline{\zeta})$ και $q \not| [L : Q]$, αφού $p \not\equiv 1 \pmod{q}$.

Η παρακάτω Πρόταση αποτελεί συνέπεια του Θεωρήματος του Thaine.

Πρόταση 5.5.1
Κάθε $\Theta \in <1+\iota> I_1$ *έχει μία lifting* $\tilde{\Theta} \in \mathbb{Z}[G]$ *που μηδενίζει το q-part της* H.

Απόδειξη:
Έστω q^m η τάξη του q-part της E/C.
Από την Πρόταση 5.1.3:2 υπάρχουν $\Theta_1, \ldots, \Theta_m \in I_1$ τέτοια ώστε $\Theta = (1+\iota)^2\Theta_1 \ldots \Theta_m$. Θέτουμε $\tilde{\Theta}' = (1+\iota)\tilde{\Theta}_1 \ldots \Theta_m$ και $\tilde{\Theta} = (1+\iota)\tilde{\Theta}'$, όπου $\tilde{\Theta}_1, \ldots, \tilde{\Theta_m}$ είναι οι liftings των $\Theta_1, \ldots, \Theta_m$, αντίστοιχα. Επειδή $\Theta_i \in I_1 = \mathrm{ann}(E/CE^q)$ έχουμε $E^{\Theta_i} \subseteq CE^q$, δηλαδή $E^{\tilde{\Theta}_i} \subseteq CE^q$ και συνεπώς $E^{\tilde{\Theta}'} \subseteq CE^{q^m}$. Από τον ορισμό του m αυτό σημαίνει ότι το $\tilde{\Theta}'$ μηδενίζει το q-part της E/C. Από το Θεώρημα του Thaine θα μηδενίζει και το q-part της H^+. Επειδή $H^{1+\iota} \subseteq H^+$ έπεται ότι το q-part της H μηδενίζεται από το $\tilde{\Theta} = (1+\iota)\tilde{\Theta}'$.

□

Πρόταση 5.5.2
Για κάθε $\Theta \in <1+\iota><N>^{\perp} I_1$ *έχουμε* $(x-\zeta)^{\Theta} \in E(K^*)^q$.

Απόδειξη:
Θέτουμε $\lambda := \frac{x-\zeta}{1-\zeta}$. Από την απόδειξη του Θεωρήματος 3.2.1 υπάρχει ιδεώδες A του K τέτοιο ώστε $<\lambda> = A^q$, δηλαδή το ιδεώδες A στην $q-$δύναμη δίνει κύριο ιδεώδες. Οπότε η τάξη του ιδεώδους A στην ομάδα H είναι 1 ή q και συνεπώς το ιδεώδες A ανήκει στο q-part της H.
Από την Πρόταση 5.5.1 υπάρχει $\tilde{\Theta} \in \mathbb{Z}[G]$ που μηδενίζει το q-part της H. Επομένως, το ιδεώδες $A^{\tilde{\Theta}}$ είναι κύριο ιδεώδες, δηλαδή $A^{\tilde{\Theta}} = <\gamma>$, όπου $\gamma \in K^*$. Άρα $<\lambda^{\tilde{\Theta}}> = <\gamma>^q$, δηλαδή υπάρχει $\varepsilon \in E$ τέτοιο ώστε $\lambda^{\tilde{\Theta}} = \varepsilon\gamma^q$. Από την τελευταία σχέση έπεται ότι $\lambda^{\Theta} \in E(K^*)^q$.
Από την άλλη μεριά, επειδή το Θ ανήκει στο augmentation ιδεώδες $<N>^{\perp}$ έχουμε $(1-\zeta)^{\Theta} \in C(K^*)^q \subseteq E(K^*)^q$. Πράγματι, το augmentation ιδεώδες παράγεται από στοιχεία της μορφής $\sigma-\tau$, όπου $\sigma, \tau \in G$ και $(1-\zeta)^{\sigma-\tau}$ είναι κυκλοτομική μονάδα. Επομένως

$$(x-\zeta)^{\Theta} = \lambda^{\Theta}(1-\zeta)^{\Theta} \in E(K^*)^q.$$

□

Πρόταση 5.5.3
Για κάθε $\Theta \in <1+\iota><N>^{\perp} I_1$ *έχουμε* $(x-\zeta)^{\Theta} \in C_q(K^*)^q$.

Απόδειξη:
Από την Πρόταση 5.1.3:2 έχουμε $\Theta = \Theta_1\Theta_2$ με $\Theta_1 \in <1+\iota><N>^{\perp} I_1$ και $\Theta_2 \in I_1$. Από την Πρόταση 5.5.2 έπεται ότι $(x-\zeta)^{\Theta_1} \in E(K^*)^q$. Επειδή $\Theta_2 \in I_1 = \mathrm{ann}(E/CE^q)$ έχουμε

$$(x-\zeta)^{\Theta} = (x-\zeta)^{\Theta_1\Theta_2} \in E^{\Theta_2}(K^*)^q \subseteq C(K^*)^q,$$

δηλαδή $(x-\zeta)^{\Theta} = \eta a^q$, με $\eta \in C$ και $a \in K^*$. Από το Θεώρημα 3.2.1 έχουμε $q^2 \mid x$ και συνεπώς $\eta a^q \equiv (-\zeta)^{\Theta} \pmod{q^2}$. Όμως το $-\zeta$ είναι q-δύναμη και άρα το η είναι q-primary. Επομένως $(x-\zeta)^{\Theta} = \eta a^q \in C_q(K^*)^q$.

□

Απόδειξη του Θεωρήματος 5.4.1:
Έστω $\Theta \in < 1+\iota >< N >^{\perp} I_1 I_3$. Από την Πρόταση 5.1.3:2 έχουμε $\Theta = \Theta_1\Theta_2$, όπου $\Theta_1 \in < 1+\iota >< N >^{\perp} I_1$ και $\Theta_2 \in I_3$. Από την Πρόταση 5.5.3 και επειδή $\Theta_2 \in I_3 = \mathrm{ann}(C_q/(C_q \cap E^q))$ έπεται ότι

$$(x-\zeta)^{\Theta} = (x-\zeta)^{\Theta_1\Theta_2} \in C_q^{\Theta_2}(K^*)^q \subseteq (K^*)^q.$$

□

5.6 Η απόδειξη του θεωρήματος 5.4.2

Στην απόδειξη του Θεωρήματος 5.4.2 είναι πιο πρακτικό να δουλέψουμε στο δακτύλιο ομάδας $\mathbb{Z}[G]$, παρά στον $\mathbb{F}_q[G]$. Οπότε χρειάζεται να βρούμε μία κατάλληλη lifting του $\Theta \in \mathbb{F}_q[G]$ στο $\mathbb{Z}[G]$. Επειδή $(x-\zeta)^{\Theta}$ είναι q-δύναμη αν και μόνο αν $(x-\zeta)^{-\Theta}$ είναι q-δύναμη, αρκεί να βρούμε μία lifting του Θ ή του $(-\Theta)$.

Το $\Theta = \sum_{\sigma\in G} n_\sigma \sigma \in \mathbb{Z}[G]$ θα λέγεται μη-αρνητικό αν $n_\sigma \geq 0$, για κάθε $\sigma \in G$. Τέλος θα λέμε ότι το $\Theta \in \mathbb{Z}[G]$ είναι θετικό αν είναι μη-αρνητικό και διάφορο του μηδενός.

Πρόταση 5.6.1
Αν $\Theta \in \mathbb{F}_q[G]$, τότε το Θ ή το $(-\Theta)$ έχει μη-αρνητική lifting $\tilde{\Theta} \in \mathbb{Z}[G]$ τέτοια ώστε $w(\tilde{\Theta}) \leq \frac{q(p-1)}{2}$. Αν το Θ ανήκει στο augmentation ιδεώδες του $\mathbb{F}_q[G]$, τότε $q \mid w(\tilde{\Theta})$. Αν το Θ είναι άρτιο, τότε και το $\tilde{\Theta}$ είναι άρτιο.

Απόδειξη:
Έστω $\tilde{\Theta}_1$ η ελάχιστη μη-αρνητική lifting του Θ, δηλαδή $\tilde{\Theta}_1 = \sum_{\sigma\in G} \tilde{n}_\sigma \sigma$, όπου οι συντελεστές $\tilde{n}_\sigma \in \{0, 1, \ldots, q-1\}$. Αν θέσουμε $\tilde{\Theta}_2 = q\sum_{\sigma\in G}\sigma - \tilde{\Theta}_1$, τότε $\tilde{\Theta}_2$ είναι μη-αρνητική lifting του $(-\Theta)$.
Αν το $\Theta = \sum_{\sigma\in G} n_\sigma\sigma$ είναι άρτιο, επειδή $\tilde{n}_\sigma \equiv n_\sigma \pmod q$ έχουμε $\tilde{n}_{\overline{\sigma}} \equiv n_{\overline{\sigma}} \pmod q$ και $\tilde{n}_\sigma \equiv n_{\overline{\sigma}} \pmod q$, δηλαδή $\tilde{n}_\sigma \equiv \tilde{n}_{\overline{\sigma}} \pmod q$. Όμως $0 \leq \tilde{n}_\sigma, \tilde{n}_{\overline{\sigma}} \leq q-1$ και συνεπώς $\tilde{n}_\sigma = \tilde{n}_{\overline{\sigma}}$, δηλαδή το $\tilde{\Theta}_1$ είναι άρτιο. Επομένως, και το $\tilde{\Theta}_2$ είναι άρτιο.
Αν το Θ ανήκει στο augmentation ιδεώδες του $\mathbb{F}_q[G]$, δηλαδή $w(\Theta) = 0$, τότε προκύπτει ότι $w(\tilde{\Theta}_1) \equiv 0 \pmod q$ και $w(\tilde{\Theta}_2) \equiv 0 \pmod q$.
Επειδή $w(\tilde{\Theta}_1) + w(\tilde{\Theta}_2) = q(p-1)$ ένα από τα $w(\tilde{\Theta}_1)$, $w(\tilde{\Theta}_2)$ θα είναι μικρότερο ή ίσο του $\frac{q(p-1)}{2}$.

□

Λόγω της παραπάνω Πρότασης το Θεώρημα 5.4.2 είναι ισοδύναμο με το ακόλουθο

Θεώρημα 5.6.1
Υποθέτουμε ότι $q \geq 7$. Αν $(x-\zeta)^{\Theta} \in (K^*)^q$, όπου Θ είναι ένα άρτιο θετικό στοιχείο του $\mathbb{Z}[G]$ τέτοιο ώστε $q \mid w(\Theta)$ και $w(\Theta) \leq \frac{q(p-1)}{2}$, τότε $q \mid \Theta$.

Για την απόδειξη του Θεωρήματος 5.6.1 θα χρειαστούμε τα παρακάτω:

Η δυναμοσειρά $(1-\zeta T)^{\frac{\Theta}{q}}$

Θα μελετήσουμε τις ιδιότητες της δυναμοσειράς $(1-\zeta T)^{\frac{\Theta}{q}}$ του Mihăilescu. Τα μικρά γράμματα $t, z, \ldots$, σημαίνουν μιγαδικούς αριθμούς, ενώ το T θα συμβολίζει ανεξάρτητη μεταβλητή. Για παράδειγμα, $(1+T)^r$ είναι η διωνυμική σειρά $\sum_{k=0}^{\infty}\binom{r}{k}T^k$, ενώ, για $|t|<1$, η έκφραση $(1+t)^r$ είναι ο μιγαδικός αριθμός που είναι ίσος με το άθροισμα της διωνυμικής σειράς για $T=t$. Ειδικότερα, ο $(1+t)^r$ είναι θετικός πραγματικός αριθμός αν $r\in\mathbb{R}$ και $t\in(-1,1)$.

Έστω $\Theta=\sum_{\sigma\in G}n_\sigma\sigma\in\mathbb{Z}[G]$. Η σειρά για την οποία ενδιαφερόμαστε είναι

$$(1-\zeta T)^{\frac{\Theta}{q}}=\prod_{\sigma\in G}(1-\zeta^\sigma T)^{\frac{n_\sigma}{q}}. \tag{5.5}$$

Η ακτίνα σύγκλισής της είναι 1. Γράφουμε

$$(1-\zeta T)^{\frac{\Theta}{q}}=\sum_{k=0}^{\infty}a_k(\Theta)T^k \tag{5.6}$$

και συμβολίζουμε με $S_m(T):=\sum_{k=0}^{m}a_k(\Theta)T^k$ το m-οστό μερικό της άθροισμα.

Πρόταση 5.6.2

Έστω Θ μη-αρνητικό στοιχείο του $\mathbb{Z}[G]$. Για $|z|<1$ έχουμε

$$\left|(1-\zeta z)^{\frac{\Theta}{q}}-S_m(z)\right|\le\binom{\frac{\omega(\Theta)}{q}+m}{m+1}(1-|z|)^{\frac{-\omega(\Theta)}{q}-m-1}|z|^{m+1}. \tag{5.7}$$

Απόδειξη:

Η δυναμοσειρά $\sum_{k=0}^{\infty}a_kT^k$ με μιγαδικούς συντελεστές κυριαρχείται (is dominated) από τη σειρά $\sum_{k=0}^{\infty}b_kT^k$ με μη-αρνητικούς πραγματικούς συντελεστές αν $|a_k|\le b_k$, για κάθε $k=0,1,\ldots$. Η σχέση της κυριαρχίας διατηρείται στην πρόσθεση και τον πολλαπλασιασμό δυναμοσειρών. Επίσης αν η $A(T)=\sum_{k=0}^{\infty}a_kT^k$ κυριαρχείται από την $B(T)=\sum_{k=0}^{\infty}b_kT^k$ και t είναι ένας μιγαδικός αριθμός τέτοιος ώστε η $B(T)$ να συγκλίνει στο $T=|t|$, τότε η $A(T)$ συγκλίνει στο $T=t$ και $|A(t)|\le B(|t|)$. Τέλος για κάθε μη-αρνητικό ακέραιο m έχουμε $|A(t)-A_m(t)|\le|B(|t|)-B_m(|t|)|$, όπου $A_m(T)$ και $B_m(T)$ είναι τα m-οστά μερικά αθροίσματα των $A(T)$ και $B(T)$.

Έστω r ένας θετικός πραγματικός αριθμός και χ ένας μιγαδικός αριθμός με $|\chi|\le 1$. Η διωνυμική σειρά $(1+\chi T)^r=\sum_{k=0}^{\infty}\binom{r}{k}\chi^kT^k$ κυριαρχείται από τη διωνυμική σειρά $(1-T)^{-r}=\sum_{k=0}^{\infty}(-1)^k\binom{-r}{k}T^k$, αφού οι συντελεστές $(-1)^k\binom{-r}{k}$ είναι θετικοί και $\left|\binom{r}{k}\chi^k\right|\le(-1)^k\binom{-r}{k}$. Επομένως, η $(1-\zeta T)^{\frac{\Theta}{q}}$ κυριαρχείται από την $(1-T)^{-\nu}$, όπου $\nu=\frac{\omega(\Theta)}{q}$. Πράγματι, $(1-\zeta T)^{\frac{\Theta}{q}}=\prod_{\sigma\in G}(1-\zeta^\sigma T)^{\frac{n_\sigma}{q}}$ και κάθε ένας παράγοντας του γινομένου κυριαρχείται από την $(1-T)^{-\frac{n_\sigma}{q}}$. Συνεπώς, το γινόμενο κυριαρχείται από

$\prod_{\sigma\in G}(1-T)^{-\frac{n_\sigma}{q}} = (1-T)^{-\frac{\omega(\Theta)}{q}}$. Αν ορίσουμε $\overline{S}_m(T)$ να είναι το m-οστό μερικό άθροισμα της $(1-T)^{-\nu}$, τότε προκύπτει ότι

$$\begin{aligned}\left|(1-\zeta z)^{\frac{\Theta}{q}} - S_m(z)\right| &\leq \left|(1-|z|)^{-\nu} - \overline{S}_m(|z|)\right| \\ &\leq \sup_{0\leq\xi\leq|z|}\left|\left(\frac{d^{m+1}(1-T)^{-\nu}}{dT^{m+1}}\Big|_{T=\xi}\right)\right|\frac{|z|^{m+1}}{(m+1)!} \\ &\leq \binom{\nu+m}{m+1}(1-|z|)^{-\nu-m-1}|z|^{m+1}.\end{aligned}$$

□

Στη συνέχεια θα μελετήσουμε την αριθμητική των συντελεστών της σειράς $(1-\zeta T)^{\frac{\Theta}{q}}$ του Mihăilescu. Ο $a\in K$ θα λέγεται q-ακέραιος αν $q^N a\in\mathbb{Z}[\zeta]$, για κάποιο αρκετά μεγάλο θετικό ακέραιο N.

Πρόταση 5.6.3

Οι συντελεστές $a_0(\Theta), a_1(\Theta),\ldots$ της σειράς $(1-\zeta T)^{\frac{\Theta}{q}}$ του Mihăilescu είναι q-ακέραιοι. Αν

$$(1-\zeta T)^{\frac{\Theta}{q}} = \sum_{k=0}^{\infty}\frac{\alpha_k(\Theta)}{q^k k!}T^k, \tag{5.8}$$

έτσι ώστε $a_k(\Theta) = \frac{\alpha_k(\Theta)}{q^k k!}$, τότε για $k=0,1,\ldots$ έχουμε

$$\alpha_k(\Theta)\in\mathbb{Z}[\zeta] \qquad \text{και} \qquad \alpha_k(\Theta)\equiv(-\sum_{\sigma\in G}n_\sigma\sigma)^k \pmod q. \tag{5.9}$$

Για την απόδειξη της παραπάνω Πρότασης χρειαζόμαστε το ακόλουθο

Λήμμα 5.6.1

Έστω R μία ακεραία περιοχή, K το σώμα πηλίκων αυτής και $A(T),\ B(T)$ και $C(T)=A(T)B(T)$ δυναμοσειρές υπέρ του K.
Αν

$$A(T)=\sum_{k=0}^{\infty}\frac{a_k}{k!}T^k,\ B(T)=\sum_{k=0}^{\infty}\frac{b_k}{k!}T^k,\ C(T)=\sum_{k=0}^{\infty}\frac{c_k}{k!}T^k,$$

όπου $a_k, b_k\in R$ και

$$a_k\equiv a^k \pmod I,\ b_k\equiv b^k \pmod I \qquad (k=0,1,\ldots),$$

για κάποια $a,b\in R$ και κάποιο ιδεώδες I του R, τότε οι συντελεστές $c_k\in R$ και

$$c_k\equiv(a+b)^k \pmod I \qquad (k=0,1,\ldots).$$

Απόδειξη:

Έχουμε $c_k = \sum_{i=0}^{k} \binom{k}{i} a_i b_{k-i}$. Επομένως $c_k \in R$ και

$$c_k \equiv \sum_{i=0}^{k} \binom{k}{i} a^i b^{k-i} \equiv (a+b)^k \pmod{I}.$$

□

Απόδειξη της Πρότασης 5.6.3:
Από το Λήμμα 1.6.3, για κάθε $n \in \mathbb{Z}$ οι συντελεστές της σειράς

$$(1-\zeta T)^{\frac{n}{q}} = \sum_{k=0}^{\infty} \binom{\frac{n}{q}}{k} (-\zeta)^k T^k$$

είναι q-ακέραιοι. Συνεπώς, και οι συντελεστές της σειράς $(1-\zeta T)^{\frac{\Theta}{q}}$ θα είναι q-ακέραιοι. Επίσης

$$(1-\zeta q T)^{\frac{n}{q}} = \sum_{k=0}^{\infty} \binom{\frac{n}{q}}{k} (-\zeta q)^k T^k = \sum_{k=0}^{\infty} \frac{b_k}{k!} T^k,$$

όπου $b_k = k! \binom{\frac{n}{q}}{k} (-\zeta q)^k = n(n-q)\dots(n-(k-1)q)(-\zeta)^k \equiv (-n\zeta)^k \pmod{q}$.
Όμως

$$\sum_{k=0}^{\infty} \frac{\alpha_k(\Theta)}{k!} T^k = \prod_{\sigma \in G} (1-\zeta^\sigma q T)^{\frac{n_\sigma}{q}}.$$

Εφαρμόζοντας το Λήμμα 5.6.1 στην παραπάνω εξίσωση, προκύπτει ότι $\alpha_k(\Theta) \in \mathbb{Z}[\zeta]$ και $\alpha_k(\Theta) \equiv (-\sum_{\sigma \in G} n_\sigma \sigma)^k \pmod{q}$, για $k = 0, 1, \dots$.

□

Η δράση της G επεκτείνεται στο δακτύλιο των δυναμοσειρών $K[T]$, δηλαδή $(\sum_{k=0}^{\infty} a_k T^k)^\sigma = \sum_{k=0}^{\infty} a_k^\sigma T^k$ και έχουμε

$$\left((1-\zeta T)^{\frac{\Theta}{q}}\right)^\sigma = (1-\zeta T)^{\frac{\sigma\Theta}{q}}. \tag{5.10}$$

Χρειάζεται όμως προσοχή όταν αντικαθιστούμε τη μεταβλητή T με κάποια τιμή t. Για παράδειγμα, αν $t \in \mathbb{Q}$ με $|t| < 1$, τότε δεν είναι απαραίτητο να ισχύει $\left((1-\zeta t)^{\frac{\Theta}{q}}\right)^\sigma = (1-\zeta t)^{\frac{\sigma\Theta}{q}}$, αφού $(1-\zeta t)^{\frac{\Theta}{q}}$ δεν ανήκει απαραίτητα στο σώμα K.

Η παρακάτω Πρόταση μας δίνει τις προϋποθέσεις ώστε η σχέση (5.10) να επεκτείνεται στις τιμές της δυναμοσειράς.

Πρόταση 5.6.4

Υποθέτουμε ότι το Θ είναι άρτιο. Αν $t \in \mathbb{Q}$ με $|t| < 1$ και $(1-\zeta t)^{\frac{\Theta}{q}} \in K$, τότε

$$\left((1-\zeta t)^{\frac{\Theta}{q}}\right)^\sigma = (1-\zeta t)^{\frac{\sigma\Theta}{q}}, \ \forall\, \sigma \in G. \tag{5.11}$$

Απόδειξη:

Επειδή το Θ είναι άρτιο η σειρά $(1-\zeta T)^{\frac{\Theta}{q}}$ έχει πραγματικούς συντελεστές. Πράγματι, αν γράψουμε $\Theta = \Theta'(1+\iota)$, χρησιμοποιώντας τη σχέση (5.10), έχουμε

$$\begin{aligned}(1-\zeta T)^{\frac{\Theta}{q}} &= (1-\zeta T)^{\frac{\Theta'}{q}}(1-\zeta T)^{\frac{\Theta'\iota}{q}} \\ &= (1-\zeta T)^{\frac{\Theta'}{q}}\left((1-\zeta T)^{\frac{\Theta'}{q}}\right)^{\iota} \\ &= (1-\zeta T)^{\frac{\Theta'}{q}}\overline{(1-\zeta T)^{\frac{\Theta'}{q}}}\end{aligned}$$

και συνεπώς η σειρά $(1-\zeta T)^{\frac{\Theta}{q}}$ έχει πραγματικούς συντελεστές.
Άρα

$$a := (1-\zeta t)^{\frac{\Theta}{q}} \in \mathbb{R}.$$

Επομένως, το a ανήκει στο πραγματικό σώμα $\mathbb{Q}(\zeta+\zeta^{-1})$, δηλαδή $a^\sigma \in \mathbb{R}$, για κάθε $\sigma \in G$. Αν $\sigma \in G$, επειδή το Θ είναι άρτιο και το $\sigma\Theta$ θα είναι επίσης άρτιο και έτσι

$$b := (1-\zeta t)^{\frac{\sigma\Theta}{q}} \in \mathbb{R}.$$

Όμως $(a^\sigma)^q = (a^q)^\sigma = \left((1-\zeta t)^\Theta\right)^\sigma = (1-\zeta t)^{\sigma\Theta}$, δηλαδή το a^σ είναι ίσο με την πραγματική q-ρίζα του $(1-\zeta t)^{\sigma\Theta}$, που είναι το b.

□

Απόδειξη του Θεωρήματος 5.6.1:

• Ο αριθμός $(1-\frac{\zeta}{x})^{\frac{\Theta}{q}}$

Επειδή $(x-\zeta)^\Theta \in (K^*)^q$ το $(x-\zeta)^\Theta$ έχει q-ρίζα στο σώμα K. Η ρίζα αυτή είναι και μοναδική αφού το σώμα K δεν περιέχει q-ρίζες της μονάδας διαφορετικές του 1.
Ο αριθμός $(x-\zeta)^\Theta$ είναι θετικός πραγματικός διότι το Θ είναι άρτιο. Πράγματι, αν γράψουμε $\Theta = \Theta'(1+\iota)$, τότε $(x-\zeta)^\Theta = (x-\zeta)^{\Theta'}\overline{(x-\zeta)^{\Theta'}} > 0$. Επομένως, η πραγματική q-ρίζα του $(x-\zeta)^\Theta$ ανήκει στο K και είναι ίση με $x^{\frac{\omega(\Theta)}{q}}(1-\frac{\zeta}{x})^{\frac{\Theta}{q}}$, αφού $(x-\zeta)^\Theta = \prod_{\sigma\in G}(1-\frac{\zeta^\sigma}{x})^{n_\sigma}x^{n_\sigma} = x^{\omega(\Theta)}(1-\frac{\zeta}{x})^\Theta$, όπου $(1-\frac{\zeta}{x})^{\frac{\Theta}{q}}$ ορίζεται ως το άθροισμα της σειράς του Mihăilescu

$$(1-\zeta T)^{\frac{\Theta}{q}} = \sum_{k=0}^{\infty} a_k(\Theta)T^k \tag{5.12}$$

στο $T = \frac{1}{x}$.
Επειδή $q \mid w(\Theta)$ και το Θ είναι άρτιο έπεται ότι $w(\Theta) = mq$, όπου $m \in 2\mathbb{Z}$.
Άρα $x^m(1-\frac{\zeta}{x})^{\frac{\Theta}{q}} \in K$, δηλαδή $(1-\frac{\zeta}{x})^{\frac{\Theta}{q}} \in K$. Από την Πρόταση 5.6.4 έχουμε

$$\left((1-\frac{\zeta}{x})^{\frac{\Theta}{q}}\right)^\sigma = (1-\frac{\zeta}{x})^{\frac{\sigma\Theta}{q}},\ \forall\ \sigma \in G. \tag{5.13}$$

• Το πολυώνυμο $P(T)$

Για $k = 1, 2, \ldots$ θέτουμε $E(k) := k + \mathrm{ord}_q(k!)$.

Ισχύουν τα παρακάτω:

$$E(k+1) \geq E(k)+1, \tag{5.14}$$

$$E(k) \leq \frac{kq}{q-1}. \tag{5.15}$$

Πράγματι, $E(k+1) = (k+1) + \mathrm{ord}_q\Big((k+1)!\Big) = (k+1) + \mathrm{ord}_q\Big(k!(k+1)\Big) = k+1 + \mathrm{ord}_q(k!) + \mathrm{ord}_q(k+1) \geq E(k)+1$.
Αν $k = q^\ell t$, όπου $q \not| t$, τότε

$$\begin{aligned}
\mathrm{ord}_q(k!) &= \Big[\frac{k}{q}\Big] + \Big[\frac{k}{q^2}\Big] + \ldots + \Big[\frac{k}{q^\ell}\Big] \\
&= q^{\ell-1}t + q^{\ell-2}t + \ldots + t \\
&= t\frac{q^\ell - 1}{q-1} \\
&= \frac{k-t}{q-1} \leq \frac{k}{q-1}
\end{aligned}$$

και άρα $E(k) = k + \mathrm{ord}_q(k!) \leq k + \frac{k}{q-1} = \frac{kq}{q-1}$.
Επειδή το Θ είναι θετικό έχουμε $m > 0$. Θεωρούμε το πολυώνυμο

$$P(T) = q^{E(m)}\Big(a_0(\Theta)T^m + a_1(\Theta)T^{m-1} + \ldots + a_m(\Theta)\Big), \tag{5.16}$$

όπου $a_k(\Theta)$ είναι οι συντελεστές της σειράς (5.12) του Mihăilescu. Από την Πρόταση 5.6.3 οι συντελεστές $a_k(\Theta)$ είναι q-ακέραιοι, δηλαδή για κάθε k υπάρχει ακέραιος N τέτοιος ώστε $q^N a_k(\Theta) \in \mathbb{Z}[\zeta]$. Επίσης $q^k k! a_k(\Theta) \in \mathbb{Z}[\zeta]$. Συνεπώς $q^{E(k)}a_k(\Theta) = q^{k+\mathrm{ord}_q(k!)}a_k(\Theta) \in \mathbb{Z}[\zeta]$. Άρα $P(T) \in \mathbb{Z}[\zeta][T]$. Οπότε από τη σχέση (5.14) έχουμε

$$P(T) \in q^{E(m)}a_m(\Theta) + q\mathbb{Z}[\zeta][T]. \tag{5.17}$$

Επίσης από τη σχέση (5.10) έχουμε

$$P^\sigma(T) = q^{E(m)}\Big(a_0(\sigma\Theta)T^m + a_1(\sigma\Theta)T^{m-1} + \ldots + a_m(\sigma\Theta)\Big),\ \forall\ \sigma \in G. \tag{5.18}$$

• Ο αριθμός β και οι συζυγείς του
Επειδή το Θ είναι μη-αρνητικό ο αριθμός $(x-\zeta)^\Theta$ είναι αλγεβρικός ακέραιος. Επομένως, και η q-ρίζα $x^m(1-\frac{\zeta}{x})^{\frac{\Theta}{q}}$ του $(x-\zeta)^\Theta$ θα είναι επίσης αλγεβρικός ακέραιος. Άρα, ο αριθμός

$$\beta := q^{E(m)}x^m(1-\frac{\zeta}{x})^{\frac{\Theta}{q}} - P(x) \tag{5.19}$$

είναι αλγεβρικός ακέραιος.
Από τις σχέσεις (5.13) και (5.18) προκύπτει ότι

$$\beta^\sigma = q^{E(m)}x^m\Big((1-\frac{\zeta}{x})^{\frac{\sigma\Theta}{q}} - \sum_{k=0}^{m} a_k(\sigma\Theta)x^{-k}\Big),\ \forall\ \sigma \in G. \tag{5.20}$$

Από την Πρόταση 5.6.2 έπεται ότι

$$|\beta^\sigma| \le q^{E(m)}x^m \binom{2m}{m+1}(1-|x|^{-1})^{-2m-1}|x|^{-1} = A|x|^{-1}. \tag{5.21}$$

Από το Πόρισμα 1.6.3 $|x| \ge q^{p-1}$ και έτσι $|x| \ge 49$, αφού $q \ge 7$. Οπότε από τη σχέση (5.15) και επειδή $2^{2m} = (1+1)^{2m} = \sum_{j=0}^{2m}\binom{2m}{j} \ge \binom{2m}{m+1}$ έχουμε $A < q^{\frac{mq}{q-1}}2,05^{2m}$. Όμως $w(\Theta) \le \frac{q(p-1)}{2}$, δηλαδή $m \le \frac{p-1}{2}$. Συνεπώς $A < (2,05q^{\frac{7}{12}})^{p-1} < q^{p-1}$, αφού $q \ge 7$. Άρα $A < |x|$, δηλαδή $|\beta^\sigma| < 1,\ \forall\ \sigma \in G$. Επειδή ο β είναι αλγεβρικός ακέραιος θα πρέπει $\beta = 0$.
Επομένως $P(x) = q^{E(m)}x^m(1-\frac{\zeta}{x})^{\frac{\Theta}{q}}$. Επειδή ο $x^m(1-\frac{\zeta}{x})^{\frac{\Theta}{q}}$ είναι αλγεβρικός ακέραιος από τη σχέση (5.17) έπεται ότι

$$q^{E(m)}a_m(\Theta) \equiv 0 \pmod q. \tag{5.22}$$

Από τη σχέση (5.22), λόγω της Πρότασης 5.6.3, θα πρέπει $q \mid (\sum_{\sigma\in G} n_\sigma\zeta^\sigma)^m$.
Όμως το q δε διακλαδίζεται στο σώμα K και συνεπώς θα έχουμε $q \mid \sum_{\sigma\in G} n_\sigma\zeta^\sigma$. Από το Λήμμα 2.1.1 προκύπτει ότι $q \mid n_\sigma,\ \forall\ \sigma \in G$. Άρα $q \mid \Theta$.

□

5.7 Η απόδειξη του θεωρήματος 5.4.3

Θεωρούμε το πολυώνυμο

$$f(T) = \frac{(1+T)^q - 1 - T^q}{q} \in \mathbb{Z}[T]. \tag{5.23}$$

Το $f(T)$ είναι ένα μη-μηδενικό μονικό πολυώνυμο βαθμού $q-1$.
Υποθέτουμε ότι όλες οι κυκλοτομικές μονάδες του σώματος K είναι q-primary.
Ειδικότερα, η $1+\zeta^q = \frac{1-\zeta^{2q}}{1-\zeta^q}$ είναι q-primary, δηλαδή υπάρχει $\beta \in \mathbb{Z}[\zeta]$ τέτοιο ώστε $1+\zeta^q \equiv \beta^q \pmod{q^2}$. Άρα $(1+\zeta)^q \equiv 1+\zeta^q \equiv \beta^q \pmod q$. Από το Λήμμα 3.2.1 έχουμε $(1+\zeta)^q \equiv \beta^q \pmod{Q^2}$, για κάθε πρώτο ιδεώδες $Q \mid q$. Επειδή το q δε διακλαδίζεται στο K έπεται ότι $(1+\zeta)^q \equiv \beta^q \pmod{q^2}$, δηλαδή $(1+\zeta)^q \equiv 1+\zeta^q \pmod{q^2}$. Η τελευταία ισοδυναμία λόγω της σχέσης (5.23) γράφεται ως $f(\zeta) \equiv 0 \pmod q$.
Αν δράσουμε με τα στοιχεία της ομάδας του Galois, τότε $f(\zeta^\sigma) \equiv 0 \pmod q, \forall\sigma \in G$. Αν τώρα Q είναι ένα πρώτο ιδεώδες του K τέτοιο ώστε $Q \mid q$, τότε έχουμε $p-1$ ισοδυναμίες

$$f(\zeta^\sigma) \equiv 0 \pmod Q \qquad (\sigma \in G). \tag{5.24}$$

Επειδή $\zeta^\sigma \not\equiv \zeta^\tau \pmod Q$ για διαφορετικά μεταξύ τους $\sigma, \tau \in G$, από τη σχέση (5.24) προκύπτει ότι

$$p-1 \le \deg f = q-1,$$

το οποίο είναι άτοπο διότι $p > q$.

□

Παράρτημα Α΄

Αλγεβρική Θεωρία Αριθμών

Ό,τι περιλαμβάνει το παράρτημα αντλήθηκε από το [4].

Α΄.1 Αλγεβρικοί και ακέραιοι αλγεβρικοί αριθμοί Αλγεβρικά σώματα αριθμών

Ορισμός Α΄.1.1
Ένας μιγαδικός αριθμός a θα λέγεται αλγεβρικός αν είναι ρίζα ενός μη-μηδενικού πολυωνύμου με ρητούς συντελεστές.

Για τη συνέχεια θα θεωρήσουμε $\tilde{\mathbb{Q}}$ να είναι το σύνολο όλων των αλγεβρικών αριθμών.

Θεώρημα Α΄.1.1
Το σύνολο $\tilde{\mathbb{Q}}$ των αλγεβρικών αριθμών είναι ένα υπόσωμα του σώματος $\mathbb{C}$ των μιγαδικών αριθμών.

Ορισμός Α΄.1.2
Ο αλγεβρικός αριθμός a θα λέγεται ακέραιος αλγεβρικός αν το ανάγωγο πολυώνυμο αυτού, $\mathrm{Irr}(a, \mathbb{Q})$, έχει ακέραιους συντελεστές.

Θεώρημα Α΄.1.2
Αν ο αλγεβρικός αριθμός a είναι ρίζα ενός μονικού πολυωνύμου με ακέραιους συντελεστές, τότε ο αριθμός αυτός είναι ακέραιος αλγεβρικός.

Γενίκευση του Θεωρήματος Α΄.1.2 αποτελεί το ακόλουθο

Θεώρημα Α΄.1.3
Αν ο μιγαδικός αριθμός a είναι ρίζα ενός μονικού πολυωνύμου με ακέραιους αλγεβρικούς συντελεστές, τότε ο a είναι ακέραιος αλγεβρικός αριθμός.

Γράφουμε $\tilde{\mathbb{Z}}$ για το σύνολο όλων των ακεραίων αλγεβρικών αριθμών.

Θεώρημα Α΄.1.4
Το σύνολο $\tilde{\mathbb{Z}}$ των ακεραίων αλγεβρικών αριθμών αποτελεί ακεραία περιοχή.

Θεώρημα Α΄.1.5
Ισχύει

$$\tilde{\mathbb{Z}} \bigcap \mathbb{Q} = \mathbb{Z},$$

δηλαδή αν ένας ακέραιος αλγεβρικός αριθμός είναι ρητός, τότε αυτός θα είναι ακέραιος και αντίστροφα κάθε ακέραιος αριθμός είναι ακέραιος αλγεβρικός.

Το σύνολο $\tilde{\mathbb{Q}}$ των αλγεβρικών αριθμών είναι επέκταση του σώματος $\mathbb{Q}$ των ρητών αριθμών απείρου βαθμού και δεν παρουσιάζει ενδιαφέρον για τη Θεωρία Αριθμών. Ενδιαφέρον για τη Θεωρία Αριθμών παρουσιάζουν εκείνα τα υποσώματα K του σώματος των μιγαδικών αριθμών, τα οποία είναι πεπερασμένες επεκτάσεις του σώματος των ρητών αριθμών.

Καταρχήν ισχύει το ακόλουθο

Θεώρημα Α΄.1.6
Αν K είναι μία πεπερασμένη επέκταση του σώματος $\mathbb{Q}$ των ρητών αριθμών, η οποία περιέχεται στο σώμα $\mathbb{C}$ των μιγαδικών αριθμών, τότε ισχύει $K \subset \tilde{\mathbb{Q}}$, δηλαδή οι αριθμοί του K είναι αλγεβρικοί.

Ορισμός Α΄.1.3
Αλγεβρικό σώμα αριθμών θα λέγεται κάθε πεπερασμένη επέκταση του σώματος των ρητών αριθμών, η οποία περιέχεται στο σώμα των μιγαδικών αριθμών.

Έστω θ ένας αλγεβρικός αριθμός. Ορίζουμε $\mathbb{Q}(\theta)$ να είναι το ελάχιστο υπόσωμα του σώματος $\mathbb{C}$ των μιγαδικών αριθμών που περιέχει το θ και το σώμα $\mathbb{Q}$ των ρητών αριθμών.

Θεώρημα Α΄.1.7
Αν θ είναι ένας αλγεβρικός αριθμός, τότε το σώμα $\mathbb{Q}(\theta)$ είναι αλγεβρικό σώμα αριθμών βαθμού $[\mathbb{Q}(\theta) : \mathbb{Q}] = n$, όπου n είναι ο βαθμός του πολυωνύμου $p(x) = \mathrm{Irr}(\theta, \mathbb{Q})$.

Αν K είναι ένα αλγεβρικό σώμα αριθμών, τότε η επέκταση $K/\mathbb{Q}$ είναι πεπερασμένη. Επειδή $\mathrm{char}(\mathbb{Q}) = 0$ είναι και διαχωρίσιμη. Συνεπώς, η επέκταση $K/\mathbb{Q}$ είναι απλή και έχουμε το παρακάτω Θεώρημα:

Θεώρημα Α΄.1.8
Αν K είναι ένα αλγεβρικό σώμα αριθμών, τότε υπάρχει ένας αλγεβρικός αριθμός θ τέτοιος ώστε να ισχύει

$$K = \mathbb{Q}(\theta).$$

Για τη μελέτη ενός αλγεβρικού σώματος αριθμών σημαντικό ρόλο παίζουν οι ακέραιοι αλγεβρικοί αριθμοί αυτού.

Ορισμός Α΄.1.4

Για οποιοδήποτε σώμα αριθμών K γράφουμε

$$R = K \bigcap \tilde{\mathbb{Z}}$$

και ονομάζουμε το R δακτύλιο των ακεραίων αλγεβρικών αριθμών του K.

Θεώρημα Α΄.1.9

Το σύνολο R των ακεραίων αλγεβρικών αριθμών ενός αλγεβρικού σώματος αριθμών K αποτελεί ακεραία περιοχή.

Θεώρημα Α΄.1.10

Αν K είναι ένα αλγεβρικό σώμα αριθμών, τότε υπάρχει ένας ακέραιος αλγεβρικός αριθμός θ τέτοιος ώστε να ισχύει

$$K = \mathbb{Q}(\theta).$$

Α΄.2 Συζυγείς αριθμοί-Ίχνος-Norm

Έστω $K = \mathbb{Q}(\theta)$ ένα αλγεβρικό σώμα αριθμών με $[K : \mathbb{Q}] = n$. Θα μελετήσουμε τους $\mathbb{Q}-$ισομορφισμούς του σώματος $\mathbb{Q}(\theta)$ στο σώμα $\mathbb{C}$ των μιγαδικών αριθμών, δηλαδή εκείνους τους ισομορφισμούς $\sigma : \mathbb{Q}(\theta) \to \mathbb{C}$ που αφήνουν τους ρητούς αριθμούς σταθερούς.

Θεώρημα Α΄.2.1

Υπάρχουν ακριβώς n $\mathbb{Q}-$ισομορφισμοί του σώματος $\mathbb{Q}(\theta)$ στο σώμα των μιγαδικών αριθμών.

Ορισμός Α΄.2.1

Αν $\sigma_1, \sigma_2, \ldots, \sigma_n$ είναι οι $\mathbb{Q}-$ισομορφισμοί του σώματος $\mathbb{Q}(\theta)$ στο σώμα των μιγαδικών αριθμών και $a \in K$, τότε οι αριθμοί $a^{(i)} = \sigma_i(a),\ i = 1, 2, \ldots, n$ λέγονται συζυγείς αριθμοί του a.

Ορισμός Α΄.2.2

Αν a είναι στοιχείο του $\mathbb{Q}(\theta)$, τότε οι αριθμοί

$$S_K(a) = a^{(1)} + a^{(2)} + \ldots + a^{(n)},$$

$$N_K(a) = a^{(1)} a^{(2)} \ldots a^{(n)}$$

καλούνται αντίστοιχα ίχνος και norm του a.

Α΄.3 Μονάδες

Ορισμός Α΄.3.1

Ένας ακέραιος αλγεβρικός αριθμός ε θα λέγεται μονάδα αν ο αντίστροφος αυτού αριθμός ε^{-1} είναι επίσης ακέραιος αλγεβρικός αριθμός.

Θεωρούμε το σύνολο E όλων των μονάδων. Το σύνολο E αποτελεί αντιμεταθετική ομάδα ως προς τον πολλαπλασιασμό. Αν θεωρήσουμε το σύνολο E_K των μονάδων που ανήκουν στο αλγεβρικό σώμα αριθμών K, τότε το E_K αποτελεί μία υποομάδα της ομάδας E όλων των μονάδων.

Θεώρημα Α΄.3.1

Ο αριθμός ε του αλγεβρικού σώματος αριθμών K είναι μονάδα αν είναι ακέραιος αλγεβρικός αριθμός και ισχύει

$$N_K(\varepsilon) = \pm 1.$$

Τέλος αναφέρουμε το Θεώρημα του Dirichlet.

Θεώρημα Α΄.3.2

Έστω K ένα αλγεβρικό σώμα αριθμών. Υπάρχει αλγεβρικός αριθμός θ τέτοιος ώστε $K = \mathbb{Q}(\theta)$. Υποθέτουμε ότι το πολυώνυμο $f(x) = \mathrm{Irr}(\theta, \mathbb{Q})$ έχει r_1 πραγματικές ρίζες και $2r_2$ μιγαδικές ρίζες (το πλήθος των μιγαδικών ριζών είναι άρτιο διότι με κάθε μιγαδική ρίζα υπάρχει και η συζυγής μιγαδική αυτής). Αν θέσουμε $r_1 + r_2 - 1 = r$, τότε υπάρχουν r μονάδες $\varepsilon_1, \varepsilon_2, \ldots \varepsilon_r$ του K, οι οποίες θα λέγονται θεμελιώδεις μονάδες του K, και μία ρίζα της μονάδας ζ του K μέγιστης τάξης m έτσι ώστε κάθε μονάδα ε του K να έχει μία μονοσήμαντη παράσταση

$$\varepsilon = \zeta^s \varepsilon_1^{s_1} \varepsilon_2^{s_2} \ldots \varepsilon_r^{s_r},$$

όπου $0 \leq s < m$ και s_i ακέραιοι.

Από το Θεώρημα του Dirichlet προκύπτει ότι η ομάδα E_K των μονάδων ενός αλγεβρικού σώματος αριθμών K είναι το ευθύ γινόμενο

$$E_K = < \zeta > \otimes < \varepsilon_1 > \otimes \ldots \otimes < \varepsilon_r >$$

μίας κυκλικής ομάδας $< \zeta >$ τάξης m και r κυκλικών ομάδων $< \varepsilon_1 >, \ldots, < \varepsilon_r >$ άπειρης τάξης.

Α΄.4 Ιδεώδη

Αν R είναι ο δακτύλιος των ακεραίων αλγεβρικών αριθμών ενός αλγεβρικού σώματος αριθμών K, τότε στον R είναι δυνατή η ανάλυση σε γινόμενο πρώτων στοιχείων.

Αποδεικνύεται ότι υπάρχουν αλγεβρικά σώματα αριθμών στα οποία δεν ισχύει η μονοσήμαντη ανάλυση. Για το λόγο αυτό η ιδέα του Kummer ήταν η αντιστοίχιση των ακεραίων αλγεβρικών αριθμών ενός αλγεβρικού σώματος αριθμών σε μία αντιμεταθετική πολλαπλασιαστική ομάδα στην οποία ισχύει η μονοσήμαντη ανάλυση. Τα στοιχεία της ομάδας αυτής λέγονται ιδεώδη του αλγεβρικού σώματος αριθμών.

Ορισμός Α΄.4.1

Ένα υποσύνολο A του αλγεβρικού σώματος αριθμών K θα λέγεται ιδεώδες του K, αν πληρούνται οι παρακάτω ιδιότητες:
(i) Αν $a_1 \in A$, $a_2 \in A$, τότε $a_1 - a_2 \in A$, δηλαδή το A αποτελεί ομάδα ως προς την πρόσθεση του σώματος.
(ii) Αν $a \in A$, $r \in R$, τότε $ra \in A$, όπου R είναι ο δακτύλιος των ακεραίων αλγεβρικών αριθμών του K.
(iii) Υπάρχει $a \not\equiv 0$ στο A.
(iv) Υπάρχει $\delta \not\equiv 0$ στο K τέτοιο ώστε να ισχύει $\delta A \subset R$.

Στην ιδιότητα (iv) μπορούμε να υποθέσουμε ότι ο δ είναι ακέραιος αλγεβρικός αριθμός του K, διότι αν είναι $\delta = \frac{\delta_1}{m}$, όπου δ_1 ακέραιος αλγεβρικός αριθμός και m φυσικός αριθμός, τότε ισχύει $\delta_1 A = \delta m \subset \delta A \subset R$.

Αν το ιδεώδες A περιέχεται στο δακτύλιο R των ακεραίων αλγεβρικών αριθμών του K, τότε θα λέγεται ακέραιο ιδεώδες του K, διαφορετικά το A θα λέγεται κλασματικό ιδεώδες του K.
Τα ακέραια ιδεώδη του K είναι τα γνωστά από την Άλγεβρα ιδεώδη του δακτυλίου R.
Αν A είναι ένα κλασματικό ιδεώδες του K, τότε υπάρχει ένας ακέραιος αλγεβρικός αριθμός δ του K τέτοιος ώστε το σύνολο $\delta A = B \subset R$. Το B είναι ακέραιο ιδεώδες και ισχύει $A = \delta^{-1}B$. Αντίστροφα, αν B είναι ένα ακέραιο ιδεώδες του αλγεβρικού σώματος αριθμών K και $\delta \neq 0$ ένας ακέραιος αλγεβρικός αριθμός του K, τότε το σύνολο $A = \delta^{-1}B$ είναι ένα κλασματικό ιδεώδες του K.

Αν a είναι διάφορος του μηδενός αριθμός του K, τότε το σύνολο

$$< a >= Ra = \{ra : r \in R\}$$

θα λέγεται κύριο ιδεώδες του K που παράγεται από τον αριθμό a. Αν ο a είναι ακέραιος αλγεβρικός αριθμός, τότε το ιδεώδες $< a >$ είναι ακέραιο, ενώ αν ο a δεν είναι ακέραιος αλγεβρικός, τότε το ιδεώδες $< a >$ είναι κλασματικό.

Θεώρημα Α΄.4.1

Αν το ιδεώδες A του αλγεβρικού σώματος αριθμών K περιέχει μία μονάδα του K, τότε το A θα περιέχει το δακτύλιο R των ακεραίων αλγεβρικών αριθμών του K.

Πόρισμα Α΄.4.1

Αν το ακέραιο ιδεώδες A του αλγεβρικού σώματος αριθμών K περιέχει μία μονάδα, τότε ισχύει $A = R =< 1 >$.

Αν A, B είναι δύο ιδεώδη του αλγεβρικού σώματος αριθμών K, τότε ορίζουμε το άθροισμα $A + B$ και το γινόμενο AB αυτών ως εξής:

$$\begin{aligned} A + B &= \Big\{a + b : a \in A, b \in B\Big\}, \\ AB &= \Big\{\sum ab : a \in A, b \in B\Big\}. \end{aligned}$$

Τα σύνολα $A+B$ και AB είναι ιδεώδη του K και $A \subset A+B$, $B \subset A+B$.

Θα λέμε ότι το ιδεώδες A διαιρεί το ιδεώδες B, αν $B \subset A$. Επίσης θα λέμε ότι το ιδεώδες A διαιρεί τον αριθμό a του αλγεβρικού σώματος αριθμών K, αν $A \mid < a >$ ή ισοδύναμα $a \in A$.

Θεώρημα Α΄.4.2

Αν a, b είναι διάφοροι του μηδενός αριθμοί του αλγεβρικού σώματος αριθμών K, τότε

$(i) < a > \mid < b > \Leftrightarrow \exists\, r \in R : b = ra$,

$(ii) < a > = < b > \Leftrightarrow \exists$ *μονάδα* ε *του* $K : b = \varepsilon a$,

όπου R είναι ο δακτύλιος των ακεραίων αλγεβρικών αριθμών του K.

Αν για τα ακέραια ιδεώδη A, B του K ισχύει $A + B = R$, τότε τα ιδεώδη αυτά θα καλούνται πρώτα μεταξύ τους.

Θεώρημα Α΄.4.3

Τα ακέραια ιδεώδη A, B του αλγεβρικού σώματος αριθμών K είναι πρώτα μεταξύ τους αν και μόνο αν υπάρχει ένας αριθμός a του A και ένας αριθμός b του B τέτοιοι ώστε να ισχύει $a + b = 1$.

Θεώρημα Α΄.4.4

Αν A, B είναι ακέραια ιδεώδη του αλγεβρικού σώματος αριθμών K, τότε

$$AB \subset A \bigcap B.$$

Αν τα A, B είναι πρώτα μεταξύ τους, τότε

$$AB = A \bigcap B.$$

Έστω M ένα ακέραιο ιδεώδες του αλγεβρικού σώματος αριθμών K. Το M ορίζει στο δακτύλιο R των ακεραίων αλγεβρικών αριθμών του K μία σχέση ισοδυναμίας ως εξής:

$$a \equiv b \pmod{M} \Leftrightarrow a - b \in M.$$

Η σχέση αυτή χωρίζει το δακτύλιο R σε κλάσεις ισοδυναμίας, το σύνολο των οποίων συμβολίζουμε με R/M. Η κλάση ισοδυναμίας στην οποία ανήκει ο αριθμός a του R είναι το σύνολο $\{x \in R : x \equiv a \pmod{M}\} = a + M$. Ορίζουμε στο σύνολο R/M πρόσθεση και πολλαπλασιασμό ως εξής:

$$(a + M) + (b + M) = a + b + M,$$

$$(a + M)(b + M) = ab + M.$$

Το σύνολο R/M αποτελεί ως προς τις παραπάνω πράξεις αντιμεταθετικό δακτύλιο με μοναδιαίο στοιχείο και έχει πεπερασμένου πλήθους στοιχεία.

Ορισμός Α΄.4.2

Αν M είναι ένα ακέραιο ιδεώδες του αλγεβρικού σώματος αριθμών K, τότε το πλήθος των στοιχείων του δακτυλίου R/M λέγεται norm του M και συμβολίζεται με $N_K(M)$.

Για τη norm ακεραίων ιδεωδών ισχύουν τα παρακάτω Θεωρήματα:

Θεώρημα Α΄.4.5
Για κάθε ακέραιο ιδεώδες M του αλγεβρικού σώματος αριθμών K έχουμε $N_K(M) \in M$.

Θεώρημα Α΄.4.6
Αν τα ακέραια ιδεώδη A, B του αλγεβρικού σώματος αριθμών K είναι πρώτα μεταξύ τους, τότε

$$N_K(AB) = N_K(A)N_K(B).$$

Το Θεώρημα Α΄.4.6 γενικεύεται και για περισσότερα ακέραια ιδεώδη τα οποία είναι ανά δύο πρώτα μεταξύ τους.

Θεώρημα Α΄.4.7
Αν $A_1, A_2, \ldots, A_m$ είναι ανά δύο πρώτα μεταξύ τους ακέραια ιδεώδη του αλγεβρικού σώματος αριθμών K, τότε $R/A_1A_2 \ldots A_m \cong R/A_1 \oplus \ldots \oplus R/A_m$.

Α΄.5 Πρώτα ιδεώδη και ανάλυση ιδεωδών σε γινόμενο πρώτων ιδεωδών

Έστω K ένα αλγεβρικό σώμα αριθμών και R ο δακτύλιος των ακεραίων αλγεβρικών αριθμών του K.

Ορισμός Α΄.5.1
Ένα ιδεώδες P του αλγεβρικού σώματος αριθμών K θα λέγεται πρώτο αν είναι ακέραιο ιδεώδες διάφορο του R και ισχύει

$$P \mid ab,\ a \in R,\ b \in R \Rightarrow P \mid a \text{ ή } P \mid b.$$

Θεώρημα Α΄.5.1
Ένα ακέραιο ιδεώδες P του αλγεβρικού σώματος αριθμών K είναι πρώτο αν και μόνο αν ο δακτύλιος R/P είναι ακεραία περιοχή με περισσότερα του ενός στοιχεία.

Ορισμός Α΄.5.2
Ένα ακέραιο ιδεώδες M του αλγεβρικού σώματος αριθμών K θα λέγεται μέγιστο αν είναι διάφορο του R και για κάθε ακέραιο ιδεώδες A του K για το οποίο ισχύει $M \subset A$ έχουμε $A = M$ ή $A = R$.

Θεώρημα Α΄.5.2
Ένα ακέραιο ιδεώδες M του αλγεβρικού σώματος αριθμών K είναι μέγιστο αν και μόνο αν ο δακτύλιος R/M είναι σώμα.

Από τα παρακάτω Θεωρήματα προκύπτει ότι τα πρώτα ιδεώδη ενός αλγεβρικού σώματος αριθμών K αποτελούν γενίκευση των πρώτων αριθμών του σώματος των ρητών αριθμών.

Θεώρημα Α΄.5.3

Κάθε πρώτο ιδεώδες P του αλγεβρικού σώματος αριθμών K είναι μέγιστο.

Θεώρημα Α΄.5.4

Τα μόνα ακέραια ιδεώδη ενός αλγεβρικού σώματος αριθμών K τα οποία διαιρούν το πρώτο ιδεώδες P του K είναι τα ιδεώδη $<1>$ και P.

Θεώρημα Α΄.5.5

Αν το πρώτο ιδεώδες P του αλγεβρικού σώματος αριθμών K διαιρεί το γινόμενο δύο ακεραίων ιδεωδών A, B του K, τότε το P διαιρεί έναν τουλάχιστον από τους παράγοντες A, B.

Θεώρημα Α΄.5.6

Κάθε ακέραιο ιδεώδες $A \neq R$ έχει έναν τουλάχιστον πρώτο διαιρέτη.

Για τη norm ενός πρώτου ιδεώδους ισχύει το ακόλουθο

Θεώρημα Α΄.5.7

Κάθε πρώτο ιδεώδες P του αλγεβρικού σώματος αριθμών K περιέχει ακριβώς ένα πρώτο αριθμό p για τον οποίο ισχύει $N_K(P) = p^f$, όπου f φυσικός αριθμός διάφορος του μηδενός.

Ορισμός Α΄.5.3

Αν P είναι ένα πρώτο ιδεώδες του αλγεβρικού σώματος αριθμών K, τότε ο βαθμός $f = [R/P : \mathbb{Z}_p]$ της επέκτασης $R/P/\mathbb{Z}_p$ θα λέγεται βαθμός του πρώτου ιδεώδους P και $N_K(P) = p^f$, όπου p ο πρώτος αριθμός που ανήκει στο ιδεώδες P.

Για κάθε ιδεώδες του αλγεβρικού σώματος αριθμών K ισχύει το ακόλουθο

Θεώρημα Α΄.5.8

Κάθε ιδεώδες A του αλγεβρικού σώματος αριθμών K αναλύεται μονοσήμαντα σε γινόμενο πρώτων ιδεωδών του K.

Με τη βοήθεια της μονοσήμαντης ανάλυσης σε γινόμενο πρώτων ιδεωδών αποδεικνύονται τα παρακάτω Θεωρήματα:

Θεώρημα Α΄.5.9

Αν A και B είναι ακέραια ιδεώδη του αλγεβρικού σώματος αριθμών K, τότε ισχύει

$$N_K(AB) = N_K(A)N_K(B).$$

Θεώρημα Α΄.5.10

Αν A είναι ένα κλασματικό ιδεώδες του αλγεβρικού σώματος αριθμών K και $A = \prod_p P^{a_p}$, $a_p \in \mathbb{Z}$, η ανάλυση αυτού σε γινόμενο πρώτων ιδεωδών, τότε η norm του A ορίζεται από τη σχέση

$$N_K(A) = \prod_p N_K(P)^{a_p}.$$

Από τον ορισμό της norm προκύπτει και για κλασματικά ιδεώδη ότι

$$N_K(AB) = N_K(A)N_K(B).$$

Α΄.6 Αριθμός κλάσεων ιδεωδών

Έστω K ένα αλγεβρικό σώμα αριθμών και R ο δακτύλιος των ακεραίων αλγεβρικών αριθμών του K. Θεωρούμε την ομάδα G όλων των ιδεωδών του K και το υποσύνολο αυτής H όλων των κυρίων ιδεωδών $< a >= aR,\ a \neq 0$ του K. Το H αποτελεί υποομάδα της G.

Η ομάδα πηλίκο G/H λέγεται ομάδα των κλάσεων ιδεωδών του K και η τάξη της λέγεται αριθμός των κλάσεων ιδεωδών του K. Δύο ιδεώδη A και B του K ανήκουν στην ίδια κλάση, δηλαδή $A \sim B$, αν υπάρχει ένας αριθμός $\delta \neq 0$ του K τέτοιος ώστε να ισχύει $B = \delta A$.

Η μελέτη του αριθμού h των κλάσεων ιδεωδών ενός αλγεβρικού σώματος αριθμών είναι ένα από τα σημαντικότερα θέματα της θεωρίας των αλγεβρικών σωμάτων αριθμών διότι σχετίζεται με τη μονοσήμαντη ανάλυση στο σώμα.

Θεώρημα Α΄.6.1

Ο αριθμός h των κλάσεων ιδεωδών ενός αλγεβρικού σώματος αριθμών είναι πεπερασμένος.

Αν h είναι ο αριθμός των κλάσεων ιδεωδών του K, τότε για κάθε ιδεώδες A του K το ιδεώδες A^h είναι κύριο ιδεώδες. Πράγματι, αν H είναι η ομάδα των κυρίων ιδεωδών του K, τότε $(AH)^h = H$, δηλαδή $A^h H = H$ και συνεπώς $A^h \in H$.

Θεώρημα Α΄.6.2

Ο δακτύλιος R των ακεραίων αλγεβρικών αριθμών ενός αλγεβρικού σώματος αριθμών K είναι δακτύλιος με μονοσήμαντη ανάλυση αν και μόνο αν ο αριθμός των κλάσεων ιδεωδών του K είναι 1.

Α΄.7 Διακλάδωση-Νόμος ανάλυσης

Έστω K ένα αλγεβρικό σώμα αριθμών και R ο δακτύλιος των ακεραίων αλγεβρικών αριθμών του K. Αν p είναι ένας πρώτος αριθμός, τότε το κύριο ιδεώδες $< p >= pR$ του K έχει μία μονοσήμαντη ανάλυση

$$< p >= P_1^{e_1} P_2^{e_2} \dots P_s^{e_s}$$

σε γινόμενο πρώτων ιδεωδών του K. Τα ιδεώδη $P_1, P_2, \dots, P_s$ είναι τα μόνα πρώτα ιδεώδη του K που περιέχουν τον αριθμό p. Επίσης για κάθε $i = 1, 2, \dots, s$ ισχύει $< p > \subset P_i^{e_i}$ και $< p > \not\subset P_i^{e_{i+1}}$.

Ορισμός Α΄.7.1

Ο αριθμός s των πρώτων ιδεωδών του K τα οποία περιέχουν τον πρώτο αριθμό p λέγεται αριθμός ανάλυσης του p στο K.

Για κάθε $i = 1, 2, \dots, s$ ο αριθμός e_i λέγεται δείκτης του πρώτου ιδεώδους P_i στο K. Αν είναι $e_i = 1$, τότε το P_i λέγεται αδιακλάδωτο ιδεώδες. Αν $e_i > 1$, τότε λέμε ότι το

ιδεώδες P_i διακλαδίζεται στο K. Επίσης αν ισχύει $e_1 = e_2 = \ldots = e_s = 1$, τότε ο πρώτος αριθμός p λέγεται αδιακλάδωτος. Τέλος αν ένα τουλάχιστον από τα $e_1, e_2, \ldots, e_s$ είναι μεγαλύτερο του 1, τότε λέμε ότι ο πρώτος αριθμός p διακλαδίζεται στο K.

Η εύρεση της ανάλυσης τυχαίου πρώτου αριθμού σε γινόμενο πρώτων ιδεωδών του K λέγεται νόμος ανάλυσης για το K.

Θεώρημα Α′.7.1

Αν

$$< p >= P_1^{e_1} P_2^{e_2} \ldots P_s^{e_s}$$

είναι η ανάλυση του ιδεώδους $< p >= pR$ σε γινόμενο πρώτων ιδεωδών του K και $f_1, f_2, \ldots, f_s$ είναι οι βαθμοί των $P_1, P_2, \ldots, P_s$ αντίστοιχα, τότε

$$e_1 f_1 + e_2 f_2 + \ldots + e_s f_s = n,$$

όπου n είναι ο βαθμός της επέκτασης $K/\mathbb{Q}$.

Έστω p ένας πρώτος αριθμός. Αν υπάρχει ακριβώς ένα πρώτο ιδεώδες P του αλγεβρικού σώματος αριθμών K το οποίο περιέχει τον p και του οποίου ο δείκτης διακλαδώσεως είναι ίσος με το βαθμό της επέκτασης $K/\mathbb{Q}$, τότε θα λέμε ότι ο p διακλαδίζεται πλήρως στο K. Αν το κύριο ιδεώδες $< p >$ του K αναλύεται σε γινόμενο διαφόρων μεταξύ τους πρώτων ιδεωδών του K βαθμού 1, τότε θα λέμε ότι ο p αναλύεται πλήρως στο K. Στην περίπτωση αυτή το πλήθος των πρώτων ιδεωδών του K που περιέχουν τον p είναι $[K : \mathbb{Q}]$.

Α′.8 Τετραγωνικά σώματα αριθμών

Η παράγραφος αυτή αναφέρεται στα τετραγωνικά σώματα αριθμών, δηλαδή στα αλγεβρικά σώματα αριθμών K των οποίων ο βαθμός της επέκτασης $K/\mathbb{Q}$ είναι 2.

Έστω $K = \mathbb{Q}(\theta)$ ένα τετραγωνικό σώμα αριθμών, όπου θ είναι ένας ακέραιος αλγεβρικός αριθμός. Ισχύει το ακόλουθο

Θεώρημα Α′.8.1

Αν K είναι ένα τετραγωνικό σώμα αριθμών, τότε υπάρχει ένας ακέραιος αριθμός $m \neq 1$, ο οποίος δε διαιρείται με το τετράγωνο ενός πρώτου αριθμού, τέτοιος ώστε

$$K = \mathbb{Q}(\sqrt{m}).$$

Το σώμα K είναι σώμα ανάλυσης του διαχωρισίμου πολυωνύμου $x^2 - m$. Άρα η επέκταση $K/\mathbb{Q}$ είναι επέκταση του Galois. Αν $\alpha = a + b\sqrt{m} \in K = \mathbb{Q}(\sqrt{m})$, όπου $a, b \in \mathbb{Q}$, τότε $S_K(\alpha) = 2a$ και $N_K(\alpha) = a^2 - mb^2$.

Στη συνέχεια θα αναφερθούμε στους ακέραιους αλγεβρικούς αριθμούς του τετραγωνικού σώματος αριθμών $K = \mathbb{Q}(\sqrt{m})$.

Θεώρημα Α′.8.2

Ένας αριθμός a του τετραγωνικού σώματος αριθμών K είναι ακέραιος αλγεβρικός αν και μόνο αν το ίχνος $S_K(a)$ και η norm $N_K(a)$ του a είναι ακέραιοι αριθμοί.

Θεώρημα Α′.8.3

Ο αριθμός $\alpha = \frac{a+b\sqrt{m}}{2}$, όπου $a, b \in \mathbb{Q}$, του τετραγωνικού σώματος $K = \mathbb{Q}(\sqrt{m})$ είναι ακέραιος αλγεβρικός αν και μόνο αν οι a, b είναι ακέραιοι αριθμοί και ισχύει

$$a \equiv b \pmod 2 \text{ για } m \equiv 1 \pmod 4,$$

$$a \equiv b \equiv 0 \pmod 2 \text{ για } m \equiv 2 \text{ ή } 3 \pmod 4.$$

Θεώρημα Α′.8.4

Ο δακτύλιος R των ακεραίων αλγεβρικών αριθμών του τετραγωνικού σώματος αριθμών $K = \mathbb{Q}(\sqrt{m})$ είναι

(i) $\mathbb{Z}[\sqrt{m}]$, *αν* $m \not\equiv 1 \pmod 4$,

(ii) $\mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{m}]$, *αν* $m \equiv 1 \pmod 4$.

Τέλος θα μελετήσουμε το νόμο ανάλυσης και τις μονάδες ενός τετραγωνικού σώματος αριθμών $K = \mathbb{Q}(\sqrt{m})$.

Θεώρημα Α′.8.5

Έστω $K = \mathbb{Q}(\sqrt{m})$ ένα τετραγωνικό σώμα αριθμών και p ένας πρώτος αριθμός.

(i) Για $p \neq 2$:

Αν $p \not| m$ και $(\frac{m}{p}) = 1$, τότε $< p >= P_1 P_2$.

Αν $p \not| m$ και $(\frac{m}{p}) = -1$, τότε το ιδεώδες $< p >$ του K είναι πρώτο.

Αν $p \mid m$, τότε $< p >= P^2$.

(ii) Για $p = 2$:

Αν $m \equiv 1 \pmod 8$, τότε $< 2 >= P_1 P_2$.

Αν $m \equiv 5 \pmod 8$, τότε το ιδεώδες $< 2 >$ του K είναι πρώτο.

Αν $m \equiv 2$ ή $3 \pmod 4$, τότε $< 2 >= P^2$.

Τα P_1, P_2, P είναι πρώτα ιδεώδη με $P_1 \neq P_2$.

Θεώρημα Α′.8.6

Η ομάδα E των μονάδων ενός μιγαδικού τετραγωνικού σώματος αριθμών $K = \mathbb{Q}(\sqrt{m})$ αποτελείται από τις $t-$ρίζες της μονάδας, όπου

$$t = 4 \text{ για } m = -1,$$

$$t = 2 \text{ για } m = -2 \text{ και } m < -4,$$

$$t = 6 \text{ για } m = -3.$$

Η ομάδα E των μονάδων ενός πραγματικού σώματος αριθμών $K = \mathbb{Q}(\sqrt{m})$ είναι το ευθύ γινόμενο της κυκλικής ομάδας $< -1 >= \{1, -1\}$ τάξης 2 και μίας κυκλικής ομάδας $< \varepsilon_1 >$ άπειρης τάξης.

Σημείωση: Το Θεώρημα Α′.8.6 αποτελεί το Θεώρημα Α′.3.2 του Dirichlet για το τετραγωνικό σώμα αριθμών $K = \mathbb{Q}(\sqrt{m})$.

Βιβλιογραφία

[1] Αντωνιάδης Γ. Α., Θεωρία Παραστάσεων Πεπερασμένων Ομάδων, Έκδοση ΕΠΕΑΕΚ «Προμηθέας», Πανεπιστήμιο Κρήτης, Ηράκλειο (1998).

[2] Αντωνιάδης Γ. Α., Θεωρία Αριθμών ΙΙ, $L-$σειρές, Έκδοση ΕΠΕΑΕΚ «Προμηθέας», Πανεπιστήμιο Κρήτης, Ηράκλειο (1999).

[3] Λάκκης Κ., Άλγεβρα, Θεσσαλονίκη (1983).

[4] Λάκκης Κ., Θεωρία Αριθμών, Εκδόσεις Ζήτη, Θεσσαλονίκη (1988).

[5] Atiyah M.F., Macdonald I.G., Introduction to Commutative Algebra, Addison-Wesley (1969).

[6] Baker A., Linear forms in the logarithms of algebraic numbers I-IV, Mathematika **13** (1966), 204-216, **14** (1967), 102-107, 220-224, **15** (1968), 204-216.

[7] Frénicle de Bessy, Traité des Triangles Rectangles en Nombres, Vol. I, Mém. Acad. Royale Sci. de Paris 5 (1729).

[8] Bilu Yu. F., Catalan's conjecture (after Mihăilescu), Séminaire Bourbaki, Exposé 909, 55ème année (2002-2003).

[9] Bilu Yu. F., Catalan without logarithmic forms (after Bugeaud, Hanrot and Mihăilescu), J. Th. Nombres Bordeaux **17** (2005), 69-85.

[10] Bilu Y. F., Bugeaud Y., Mignotte M., The Problem of Catalan, Springer, Berlin (2006).

[11] Cassels J.W.S., On the equation $a^x - b^y = 1,\ II$, Proc. Camb. Philos. Soc. **56** (1960), 97-103.

[12] Chao Ko., On the diophantine equation $x^2 = y^n + 1$, Scientia Sinica (Notes) **14** (1965), 457-460.

[13] Chein E.Z., A note on the equation $x^2 = y^q + 1$, Proc. Am. Math. Soc. **56** (1976), 83-84.

[14] Euler L., Theorematum quorundam arithmeticorum demonstrationes, Opera Omnia, Ser. I, Vol. II, Commentationes Arithmeticae I, 38-58, B. G. Teubner, Basel (1915).

[15] Frey G., Der satz von Preda Mihăilescu, Die Vermutung von Catalan ist richtig, DMV-Mitteilungen **4** (2002), 8-13.

[16] Levi ben Gerson (1288-1344), στο βιβλίο Dickson L. E., History of the Theory of Numbers, Vol. II, σελ. 731, Chelsea Publ. Co., New York (1971).

[17] Hofmann J. E., Neues über Fermats zahlentheoretische Herausforderung von 1657, Abh. Preussischen Akad. d. Wiss., Berlin No 9 (1944), 1-52.

[18] Inkeri K., On Catalan's conjecture, J. Number Th. **34** (1990), 142-152.

[19] Inkeri K., Hyyrö S., On the congruence $3^{p-1} \equiv 1 \pmod{p^2}$ and the diophantine equation $x^2 - 1 = y^p$, Ann. Univ. Turku, Ser. AI, No 50 (1961), 1-2.

[20] Lebesgue V. A., Sur l' impossibilité en nombres entiers de l' équation $x^m = y^2 + 1$, Nouv. Ann. de Math. **9** (1850), 178-181.

[21] Ljunggren W., New propositions about the indeterminate equation $\frac{x^n-1}{x-1} = y^q$ (in Norwegian), Norske Mat. Tidsskrift **25** (1943), 17-20.

[22] Mazur B., Questions about Powers of Numbers, Notices of the AMS **47** (2), (2000), 195-202.

[23] Metsänkylä T., Catalan's conjecture: another old diophantine problem solved, Bull. Amer. Math. Soc. **41** (2004), 43-57.

[24] Mignotte M., Catalan's equation just before 2000, Number Theory (Turku, 1999), de Gruyter, Berlin (2001), 247-254.

[25] Mignotte M., Roy Y., Minorations pour l' equation de Catalan, C. R. Acad. Sci. Paris **324** (1997), 377-380.

[26] Mihăilescu P., A class number free criterion for Catalan's conjecture, J. Number Th. **99** (2003), 225-231.

[27] Mihăilescu P., Primary cyclotomic units and a proof of Catalan's conjecture, J. reine angew. Math. **572** (2004), 167-195.

[28] Mihăilescu P., On the class groups of cyclotomic extensions in the presence of a solution to Catalan's equation, J. Number Th. **118** (1), (2006), 225-231.

[29] Mihăilescu P., On the relative class groups of cyclotomic extensions in the presence of a solution to Catalan's equation, υποβλήθηκε στο J. Number Th.

[30] Nagell T., Sur l' équation indéterminée $\frac{x^n-1}{x-1} = y^2$, Norsk Mat. Forenings Skrifter, Ser. I, No 3 (1921), 1-17.

[31] Nagell T., Sur l' impossibilité de l' équation indéterminée $z^p + 1 = y^2$, Norsk Mat. Forenings Skrifter, Ser. I, No 4 (1921), 1-10.

[32] Nagell T., Sur une équation diophantienne à deux indéterminées, Det Kong, Norske Vidensk, Selskab Forhandliger, Trondhejm, No 38 (1934), 136-139.

[33] Obláth R., Sobre ecuaciones diofánticas imposibles de la forma $x^m + 1 = y^n$, Rev. Mat. Hisp. Amer., IV 1 (1941), 122-140.

[34] Ribenboim P., Catalan's conjecture (Are 8 and 9 the Only Consecutive Powers?), Academic Press, Boston (1994).

[35] Schoof R., Catalan's conjecture, (http://www.mat.uniroma2.it/∼schoof/), 2^a Università di Roma "Tor Vergata", Rome (2003).

[36] Siegel C. L., Über einige Anwendungen diophantischer Approximationen, Gesammelte Abhandlungen, Vol. I, Springer-Verlag, Berlin (1966), 209-266.

[37] Thaine F., On the ideal class groups of real abelian number fields, Ann. Math. **128** (1988), 1-18.

[38] Tijdeman R., On the equation of Catalan, Acta Arith. **29** (1976), 197-209.

[39] Washington L., Introduction to Cyclotomic Fields, Springer-Verlag, New York (1982).

[40] Weiss E., Cohomology of Groups, Academic Press, New York (1969).

[41] Wieferich A., Zum letzten Fermat'schen Theorem, J. f. d. reine u. angew. Math. 136 (1909), 293-302.