Εθνικο και Καποδιστριακο Πανεπιστημιο Αθηνων
Τμημα Μαθηματικων

Εργασία για το μάθημα «*Θέματα Άλγεβρας & Γεωμετρίας*»

Διδάσκοντες: Ε. Ράπτης, Δ. Βάρσος

Ακαδημαϊκό έτος 2005-2006

Το Τελευταίο Θεώρημα του Fermat

Η μερική απόδειξη του Kummer

Άγγελος Μαντζαφλάρης
amantzaf@math.uoa.gr

Μάιος 2006

«είναι αδύνατο να ισχύει στους ακέραιους το $x^n + y^n = z^n$ για $n > 2$. Έχω ανακαλύψει μια πραγματικά θαυμάσια απόδειξη, όμως το περιθώριο της σελίδας είναι πολύ στενό για να την αναπτύξω»

Pierre De Fermat - 1637

«βλέπουμε λοιπόν ότι οι ιδεώδεις πρώτοι παράγοντες αποκαλύπτουν την ουσία των μιγαδικών αριθμών, τους κάνουν διαφανείς, όπως πρέπει να είναι, και φανερώνουν την εσωτερική κρυστάλλινη δομή τους»

Ernst Eduard Kummer - 1844

Περίληψη

Ένα πολύ όμορφο παράδειγμα εφαρμογής της σύγχρονης Αλγεβρικής Θεωρίας Αριθμών σε ένα κλασσικό μαθηματικό πρόβλημα είναι η ειδική περίπτωση του Kummer για το Τελευταίο Θεώρημα Fermat. Σε αυτήν την εργασία περιορίζουμε το Τελευταίο Θεώρημα του Fermat στο πρόβλημα εύρεσης ακέραιων λύσεων της εξίσωσης $x^p + y^p = z^p$ για p ειδικής κατηγορίας περιττό πρώτο. Δίνεται μια πλήρης, σύγχρονη εκδοχή της απόδειξης του Kummer για τους λεγόμενους «μη ιδιάζοντες πρώτους»(regular primes). Τέλος γίνεται αναδρομή στην ιστορία του Θεωρήματος, και παρουσιάζονται κάποιες εικασίες που συνδέονται με αυτό.

Περιεχόμενα

Εισαγωγή

Η ιστορία του Θεωρήματος του Fermat έχει κάποια συναρπαστικά στοιχεία που δύσκολα βρίσκονται σε μαθηματικά προβλήματα. Υπάρχει δαιμόνιο, πάθος, ζήλια και χρήμα(το 1908 ανακοινώθηκε ότι ο Paul Wolfskehl, ένας μάλλον άσημος αλλά αρκετά πλούσιος μαθηματικός, κληροδότησε το ποσό των 100.000 μάρκων για να προσφερθεί από το Πανεπιστήμιο του Göttingen σε όποιον αποδείξει το θεώρημα του Fermat), ακόμη και φυλετικές διακρίσεις (το 19^o αιώνα, η Sophie Germain αναγκάστηκε να υποκριθεί ανδρική ταυτότητα για να δουλέψει πάνω στο πρόβλημα και να αλληλογραφεί με άλλους μαθηματικούς).

Η διατύπωση είναι απατηλά απλή: «δεν υπάρχουν ακέραιοι x, y, z που ικανοποιούν $x^n + y^n = z^n$ για $n > 2$»(σε αντίθεση με την περίπτωση $n = 2$ που οι λύσεις είναι οι γνωστές *Πυθαγόρειες τριάδες*). Εμφανίστηκε για πρώτη φορά στις σημειώσεις του *Pierre Fermat* που εκδόθηκαν το 1670 και λύθηκε τελικά από τον *Andrew Wiles* το 1995*. Ο Fermat ισχυρίστηκε πως έχει μια «πραγματικά θαυμάσια απόδειξη αυτής της πρότασης, που όμως δε χωράει στο περιθώριο της σελίδας». Αν αυτό ισχύει, τότε αποκλείεται να ήταν παρόμοια με αυτήν του Wiles, που χρειάστηκε να ενοποιήσει κάθε λογής σύγχρονα μαθηματικά για να πετύχει το στόχο της. Αυτός είναι και ο λόγος που πολλοί(κυρίως ερασιτέχνες) προσπαθούν ακόμη να βρουν μια πιο απλή απόδειξη, με τα μαθηματικά της εποχής του Fermat. Ένα επιχείρημα υπέρ της ύπαρξης μιας τέτοιας απόδειξης είναι πως όλα τα άλλα θεωρήματα του Fermat αποδείχθηκαν αληθή ή μη λίγο μετά την δημοσιοποίησή τους(εξ΄ ου και και η ονομασία *«Τελευταίο»* Θεώρημα του Fermat).

Όσοι εργάζονται στο Μαθηματικό Τμήμα του Πανεπιστημίου του Göttingen σίγουρα χάρηκαν και ανακουφίστηκαν όταν έδωσαν τελικά το βραβείο Wolfskehl στον Wiles και ξεμπέρδεψαν με αυτήν την ιστορία. Για να πάρετε μια ιδέα του τι συνέβαινε, ο καθηγητής Edmund Landau που ήταν υπεύθυνος για τις συμμετοχές στο διαγωνισμό στις αρχές του προηγούμενου αιώνα, τύπωνε και ταχυδρομούσε πολλές κάρτες που έγραφαν:

> *Αγαπητέ ... ,*
> *Σας ευχαριστούμε για την εργασία σας για την απόδειξη του Τελευταίου Θεωρήματος του Fermat.*
> *Το πρώτο λάθος βρίσκεται: Σελίδα ... Γραμμή ... Αυτό καθιστά την απόδειξη άκυρη.*
> *Καθηγητής Edmund Landau*

και κατόπιν έδινε τις εργασίες στους μαθητές του ως ασκήσεις.

*Για την απόδειξη του Wiles παραπέμπουμε τον αναγνώστη στο [15].

Η αξία του προβλήματος έγκειται πιο πολύ στις ανακαλύψεις που έγιναν και τα καινούρια μαθηματικά που δημιουργήθηκαν από τις προσπάθειες να επιλυθεί, παρά στο ίδιο το πρόβλημα. Αυτό ήταν γνωστό αρκετά παλιά. Σε μια διάλεξή[†] του στο Διεθνές Συνέδριο Μαθηματικών στο Παρίσι το 1900, ο David Hilbert λέει:

> *Η απόπειρα λύσης ... είναι ένα εντυπωσιακό παράδειγμα της ώθησης που μπορεί να δώσει ένα τόσο ειδικό και ασήμαντο πρόβλημα στην επιστήμη. Ο Kummer, υποκινούμενος από το πρόβλημα του Fermat, οδηγήθηκε στην εισαγωγή της θεωρίας των ιδεωδών αριθμών και την ανακάλυψη του Νόμου της Μοναδικής Ανάλυσης των αριθμών ενός κυκλικού σώματος σε ιδεώδεις πρώτους παράγοντες - ένας νόμος ο οποίος μέχρι και σήμερα, με τη γενίκευσή του σε οποιοδήποτε αλγεβρικό σώμα από τον Dedekind και τον Kronecker, βρίσκεται στον πυρήνα της σύγχρονης Θεωρίας Αριθμών και η σημαντικότητά του ξεπερνά τα όρια της Θεωρίας Αριθμών και επεκτείνεται στην Άλγεβρα και τη Θεωρία Συναρτήσεων.*

Αυτήν την κληρονομιά που μας άφησε ο Kummer θα χρησιμοποιήσουμε και στην παρούσα εργασία για να αναπαράγουμε την (υπό συνθήκες) απόδειξη που έδωσε για το Τελευταίο Θεώρημα του Fermat:

Στην ενότητα (I.) παρουσιάζονται συνοπτικά βασικές έννοιες από την Αλγεβρική Θεωρία Αριθμών, ενώ στην ενότητα (II.) δίνεται το απαραίτητο υπόβαθρο και μερικά αποτελέσματα που χρειάζονται για την απόδειξη. Ακολουθεί η απόδειξη του Kummer στην (III.), χωρισμένη σε τρεις περιπτώσεις.

Στο Παράρτημα Α′. γίνεται μια ιστορική αναδρομή του Θεωρήματος του Fermat, έως την πρόσφατη τελική λύση του. Τελειώνουμε δίνοντας τροφή στον ανήσυχο αναγνώστη με την παρουσίαση τριών νέων προκλήσεων, οι οποίες συνδέονται με το Τελευταίο Θεώρημα του Fermat, στο Παράρτημα Β′.

Θέλω να ευχαριστήσω τους διδάσκοντες του μαθήματος *Θέματα Άλγεβρας & Γεωμετρίας I* και *II* κύριους Ευάγγελο Ράπτη και Δημήτριο Βάρσο, για την ευκαιρία που μου έδωσαν μέσα από αυτήν την εργασία να περιπλανηθώ στα συναρπαστικά μονοπάτια των μαθηματικών του Τελευταίου Θεωρήματος του Fermat και να νιώσω λίγο από το δέος που αυτό αναμφίβολα δημιουργεί σε κάθε μαθηματικό.

[†] Πρόκειται για τη διάσημη ομιλία «Μαθηματικά Προβλήματα»[23] του David Hilbert.

I. Στοιχεία Αλγεβρικής Θεωρίας Αριθμών

Θα δώσουμε τώρα το απαραίτητο υπόβαθρο και κάποια αποτελέσματα από την Αλγεβρική Θεωρία Αριθμών. Για αποδείξεις όσων παρουσιάζονται σε αυτήν την ενότητα παραπέμπουμε στο [1]. Θεωρούμε ότι ο αναγνώστης είναι εξοικειωμένος με τις βασικές έννοιες της σύγχρονης Άλγεβρας*.

i. Στοιχειώδεις έννοιες

Ορισμός 1.1. *Αλγεβρικός αριθμός λέγεται ο $\beta \in \mathbb{C}$ ανν υπάρχει μη μηδενικό πολυώνυμο $r(x) \in \mathbb{Q}[x]$ με ρίζα τον β.*

Λήμμα 1.1. *Οι αλγεβρικοί αριθμοί είναι υπόσωμα του $\mathbb{C}$.*

Ορισμός 1.2. *Αλγεβρικός ακέραιος ονομάζεται ο $\alpha \in \mathbb{C}$ ανν υπάρχει μη μηδενικό και μονικό πολυώνυμο $s(x) \in \mathbb{Z}[x]$ με ρίζα τον α.*

Λήμμα 1.2. *Οι αλγεβρικοί ακέραιοι ενός σώματος είναι υποδακτύλιος των αλγεβρικών αριθμών.*

Ορισμός 1.3. *Αριθμητικό σώμα ονομάζεται ένα πεπερασμένης διάστασης επί του $\mathbb{Q}$ υπόσωμα του $\mathbb{C}$.*

Ορισμός 1.4. *Τετραγωνικό σώμα είναι ένα αριθμητικό σώμα διάστασης 2 επί του $\mathbb{Q}$.*

Λήμμα 1.3. *Κάθε αριθμητικό σώμα είναι υπόσωμα των αλγεβρικών αριθμών.*

Λήμμα 1.4. *Τα αριθμητικά σώματα είναι της μορφής $\mathbb{Q}(\theta)$, όπου θ αλγεβρικός αριθμός.*

Λήμμα 1.5. *Αν k ακέραιος ελεύθερος τετραγώνου, οι αλγεβρικοί ακέραιοι του $\mathbb{Q}(\sqrt{k})$ είναι*

$$\mathfrak{D}_k = \begin{cases} \mathbb{Z}\left[\sqrt{k}\right] & , \ k \not\equiv 1 \pmod 4 \\ \mathbb{Z}\left[\frac{1}{2} + \frac{1}{2}\sqrt{k}\right] & , \ k \equiv 1 \pmod 4 \end{cases}$$

Λήμμα 1.6. *Αν K είναι ένα αριθμητικό σώμα διάστασης n, τότε*

(α′) *υπάρχουν ακριβώς n διακεκριμένοι μονομορφισμοί $\sigma_i : K \to \mathbb{C}, \ \ i = 1, \ldots, n$.*

(β′) *κάθε στοιχείο $\alpha \in K$ απεικονίζεται μέσω αυτών σε κάποια ρίζα του ελάχιστου πολυωνύμου(βαθμού m) του $f_a(x) \in \mathbb{Q}[x]$. Συγκεκριμένα, ακριβώς $\frac{n}{m}$ από τους σ_i απεικονίζουν το α στην ίδια ρίζα του $f_a(x)$.*

*Παραπέμπουμε στο [20], αρκούν τα κεφάλαια 1 έως 3 που συνήθως διδάσκονται στο προπτυχιακό μάθημα *Βασική Άλγεβρα* του Τμήματος Μαθηματικών του Ε.Κ.Π.Α

Ορισμός 1.5. *Ως νόρμα ενός στοιχείου $\alpha \in K$, όπου K αριθμητικό σώμα, ορίζουμε το γινόμενο:*

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

Λήμμα 1.7. *Αν $\alpha, \delta \in K$ είναι αλγεβρικοί ακέραιοι, τότε*

(α′) οι νόρμες $N(\alpha), N(\delta) \in \mathbb{Z}$.

(β′) ισχύει $N(\alpha\delta) = N(\alpha) \cdot N(\delta)$.

(γ′) Αν το α είναι αντιστρέψιμο, τότε $N(\alpha) = \pm 1$.

Λήμμα 1.8. *Αν ο $\theta \in K \cap \mathbb{Z}$, έπεται ότι $N(\theta) = \theta^n$, όπου n η διάσταση του K υπεράνω του $\mathbb{Q}$.*

Ορισμός 1.6. *Έστω $\mathfrak{D}$ ο δακτύλιος των αλγεβρικών ακεραίων ενός αριθμητικού σώματος K. Αν $\mathfrak{d} \lhd \mathfrak{D}$ ένα ιδεώδες του $\mathfrak{D}$,τότε ο δακτύλιος πηλίκο $\mathfrak{D}/\mathfrak{d}$ είναι πεπερασμένος. Ορίζουμε ως νόρμα του $\mathfrak{d}$ τη διάσταση αυτού: $N(\mathfrak{d}) = |\mathfrak{D}/\mathfrak{d}|$.*

Λήμμα 1.9. *Αν $\mathfrak{d}, \mathfrak{b} \lhd \mathfrak{D}$ τότε*

(α′) Αν το $\mathfrak{d} = \langle d \rangle$ είναι κύριο, τότε $N(\mathfrak{d}) = |N(d)|$.

(β′) $N(\mathfrak{d}\mathfrak{b}) = N(\mathfrak{d}) \cdot N(\mathfrak{b})$.

Ορισμός 1.7. *Ένα υποσύνολο $\mathfrak{a} \subseteq \mathfrak{D}$ καλείται κλασματικό ιδεώδες όταν υπάρχει μη μηδενικό $c \in K$ ώστε $c\mathfrak{a} \subseteq \mathfrak{D}$. Άρα τα κλασματικά ιδεώδη του $\mathfrak{D}$ είναι τα σύνολα της μορφής $c^{-1}\mathfrak{d}$, με $\mathfrak{d} \lhd \mathfrak{D}$.*

Ορισμός 1.8. *Ένα κλασματικό ιδεώδες $\mathfrak{a}$ του $\mathfrak{D}$ καλείται κύριο αννν $\mathfrak{a} = c^{-1}\mathfrak{d}$, και το $\mathfrak{d}$ είναι κύριο ιδεώδες του $\mathfrak{D}$.*

Λήμμα 1.10. *Τα κλασματικά ιδεώδη του $\mathfrak{D}$ με πράξη τον πολλαπλασιασμό έχουν τη δομή αβελιανής ομάδας, την οποία συμβολίζουμε με $\mathfrak{F}$.*

Ορισμός 1.9. *Για κάθε ιδεώδες $\mathfrak{a} \lhd \mathfrak{D}$ ορίζουμε το σύνολο $\mathfrak{a}^{-1} := \{c \in K \mid c\mathfrak{a} \subseteq \mathfrak{D}\}$, το οποίο είναι κλασματικό ιδεώδες και καλείται αντίστροφος του ιδεώδους $\mathfrak{a}$.*

Λήμμα 1.11. *Το σύνολο των κύριων κλασματικών ιδεωδών $\mathfrak{P}$ είναι υποομάδα της αβελιανής ομάδας $\mathfrak{F}$.*

Λήμμα 1.12. *Κάθε μη μηδενικό ιδεώδες $\mathfrak{d}$ του $\mathfrak{D}$ έχει αντίστροφο ιδεώδες, δηλαδή υπάρχει κλασματικό ιδεώδες $\mathfrak{d}^{-1}$ τέτοιο ώστε $\mathfrak{d}\mathfrak{d}^{-1} = \mathfrak{D} = \langle 1 \rangle$.*

ii. Παραγοντοποίηση σε δακτύλιο αλγεβρικών ακεραίων

Ακολουθούν τα βασικά θεωρήματα σχετικά με το δακτύλιο των αλγεβρικών ακεραίων ενός αριθμητικού σώματος και την παραγοντοποίηση των στοιχείων του. Η παραγοντοποίηση είναι ένα μεγάλο κεφάλαιο της Άλγεβρας, το οποίο έχει στενή σχέση με το Τελευταίο Θεώρημα του Fermat, καθώς αναπτύχθηκε με τις προσπάθειες μαθηματικών να αποδείξουν το Θεώρημα. Εδώ θα περιοριστούμε στα απολύτως απαραίτητα· για περαιτέρω μελέτη παραπέμπουμε στο [21].

Στα παρακάτω με $\mathfrak{D}$ συμβολίζουμε το δακτύλιο των αλγεβρικών ακεραίων ενός αριθμητικού σώματος K.

Ορισμός 1.10. *Έστω ακέραια περιοχή R. Τα στοιχεία $a, b \in R$ ονομάζονται συντροφικά, αν υπάρχει αντιστρέψιμο στοιχείο $u \in R$ ώστε $a = ub$. Παρατηρείστε ότι τότε $b = u^{-1}a$.*

Ορισμός 1.11. *Ένα ιδεώδες $\mathfrak{a}$ ενός δακτυλίου R ονομάζεται πρώτο αν για οποιαδήποτε ιδεώδη $\mathfrak{b}, \mathfrak{c}$ του R ισχύει η συνεπαγωγή:*

$$\mathfrak{bc} \subseteq \mathfrak{a} \Rightarrow \mathfrak{b} \subseteq \mathfrak{a} \quad \text{ή} \quad \mathfrak{c} \subseteq \mathfrak{a}$$

Λήμμα 1.13. *Αν ο αριθμός $N(\mathfrak{d})$ είναι πρώτος, τότε το $\mathfrak{d} \lhd \mathfrak{D}$ είναι πρώτο ιδεώδες.*

Λήμμα 1.14. *Για τα ιδεώδη του $\mathfrak{D}$ ισχύει $\mathfrak{a}/\mathfrak{b}$ ανν $\mathfrak{b} \subseteq \mathfrak{a}$.*

Ορισμός 1.12. *Η ομάδα πηλίκο της ομάδας των κλασματικών ιδεωδών $\mathfrak{F}$ προς την ομάδα των κύριων κλασματικών ιδεωδών $\mathfrak{P}$ λέγεται ομάδα κλάσεων του $\mathfrak{D}$ και συμβολίζεται $\mathfrak{H} := \mathfrak{F}/\mathfrak{P}$. Η τάξη της h καλείται κλάση του αριθμητικού σώματος K.*

Λήμμα 1.15. *Έστω h η κλάση του K και $\mathfrak{a}$ ένα ιδεώδες του $\mathfrak{D}$. Τότε*

(α′) Αν p ακέραιος σχετικά πρώτος με το h και το $\mathfrak{a}^p$ είναι κύριο, τότε το $\mathfrak{a}$ είναι κύριο ιδεώδες.

(β′) Το ιδεώδες $\mathfrak{a}^h$ είναι κύριο.

Ορισμός 1.13. *Μια ακέραια περιοχή ονομάζεται Περιοχή Κυρίων Ιδεωδών (Π.Κ.Ι.) ανν κάθε ιδεώδες της είναι κύριο ιδεώδες.*

Λήμμα 1.16. *(Θεώρημα Μοναδικής Παραγοντοποίησης) Η ανάλυση των στοιχείων του $\mathfrak{D}$ σε πρώτους παράγοντες είναι μοναδική ανν το $\mathfrak{D}$ είναι Π.Κ.Ι.*

Λήμμα 1.17. *Ο δακτύλιος $\mathfrak{D}$ είναι Π.Κ.Ι. ανν η κλάση του είναι $h = 1$.*

Λήμμα 1.18. *(Μοναδικότητα Παραγοντοποίησης Ιδεωδών) Κάθε ιδεώδες του $\mathfrak{D}$ αναλύεται κατά μοναδικό τρόπο σε γινόμενο πρώτων ιδεωδών.*

iii. Κυκλοτομικά σώματα

Ερχόμαστε τώρα στην κατηγορία των αριθμητικών σωμάτων στην οποία θα παραγοντοποιήσουμε την εξίσωση του Fermat.

Ορισμός 1.14. *Οι n μιγαδικές ρίζες της εξίσωσης $z^n = 1$, που δίνονται από τον τύπο*

$$\zeta_k = e^{2k\pi i/n} = \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right), \qquad k = 0, 1, \ldots, n-1$$

ονομάζονται $n-$οστές ρίζες της μονάδας.

Είναι εύκολο να δούμε ότι για κάθε ακέραιο d ισχύει $\zeta_k^d = \zeta_k^{d \pmod n}$.

Ορισμός 1.15. *Κάθε αριθμητικό σώμα $\mathbb{Q}(\zeta_m)$, όπου $\zeta_m = e^{2\pi i/m}$ για κάποιο $m \in \mathbb{Z}$ ονομάζεται κυκλοτομικό σώμα.*

Λήμμα 1.19. *Μια βάση του $\mathbb{Q}(\zeta_m)$, $\zeta_m = e^{2\pi i/m}$ είναι το σύνολο $\{1, \zeta, \ldots, \zeta^{m-1}\}$.*

Στα παρακάτω συμβολίζουμε $\zeta = e^{2\pi i/p}$ όπου p περιττός πρώτος, οπότε το $\mathbb{Q}[\zeta]$ είναι ένα κυκλοτομικό σώμα διάστασης $p-1$.

Λήμμα 1.20. *Το ελάχιστο πολυώνυμο $g(t) \in \mathbb{Q}[t]$ του ζ υπεράνω του $\mathbb{Q}$ είναι το*

$$g(t) = t^{p-1} + t^{p-2} + \cdots + t^2 + t + 1$$

Λήμμα 1.21. *Ο δακτύλιος των αλγεβρικών ακεραίων του $\mathbb{Q}(\zeta)$ είναι ο $\mathbb{Z}[\zeta]$.*

Λήμμα 1.22. *Αν $\sigma_i : \mathbb{Q}[\zeta] \to \mathbb{C}$, $i = 1, \ldots, p-1$ (οι μόνοι) διακεκριμένοι μονομορφισμοί, τότε $\sigma_i(\zeta) = \zeta^i$ για κάθε i.*

Λήμμα 1.23. *Ισχύουν τα εξής: $N(\zeta^s) = 1$, για κάθε $s \in \mathbb{Z}$ και $N(1-\zeta) = p$.*

Λήμμα 1.24. *Για το ιδεώδες $\langle 1-\zeta \rangle$ ισχύει $\langle 1-\zeta \rangle^{p-1} = \langle p \rangle$ και $N(\langle 1-\zeta \rangle) = p$.*

Έπεται ότι το $\ell := \langle 1-\zeta \rangle$ είναι πρώτο ιδεώδες. Το ιδεώδες αυτό βρίσκεται σε κομβικό σημείο στην απόδειξη του Θεωρήματος του Fermat.

Ορισμός 1.16. *Κυκλοτομικές μονάδες του $\mathbb{Q}(\zeta)$ ονομάζονται τα στοιχεία της μορφής $\dfrac{1-\zeta^r}{1-\zeta^s}$ με r, s σχετικά πρώτα με τον p. Το σύνολο των κυκλοτομικών μονάδων είναι υποομάδα της ομάδας των αντιστρέψιμων στοιχείων του $\mathbb{Z}[\zeta]$.*

Πράγματι, επειδή οι r, s είναι σχετικά πρώτοι με τον p, υπάρχει $t \in \mathbb{Z}$ ώστε $ts = r \pmod p$ άρα:

$$\frac{1-\zeta^r}{1-\zeta^s} = \frac{1-\zeta^{ts}}{1-\zeta^s} = \frac{(1-\zeta^s)(1+\zeta^s+\zeta^{2s}+\cdots+\zeta^{s(t-1)})}{1-\zeta^s} = 1+\zeta^s+\zeta^{2s}+\cdots+\zeta^{s(t-1)} \in \mathbb{Z}[\zeta]$$

II. Προαπαιτούμενα

Το πρώτο βήμα για να προσεγγίσουμε την εξίσωση του Fermat είναι να την παραγοντοποιήσουμε, με σκοπό να απλοποιηθεί κατά το δυνατό. Το πρώτο πράγμα που θα σκεφτόταν κανείς είναι η ταυτότητα:

$$z^p = x^p + y^p = (x+y)(x^{n-1} - x^{n-2}y + x^{n-3}y^2 + \cdots + y^{n-1})$$

Παρατηρήστε ότι ο βαθμός του δεύτερου παράγοντα στην παραπάνω σχέση παραμένει μεγάλος, οπότε η παραγοντοποίηση αυτή είναι αρκετά δύσχρηστη.

Αν θεωρήσουμε όμως το πολυώνυμο

$$x^p - y^p = 0$$

στο κυκλοτομικό σώμα $\mathbb{Q}[\zeta]$, με $\zeta = e^{2\pi i/p}$ και p περιττό πρώτο, τότε αυτό έχει ακριβώς p λύσεις σαν πολυώνυμο του x, και είναι οι $x = \zeta^k y$ για $k = 0, 1, \ldots, p-1$. Άρα η παραγοντοποίησή του είναι

$$x^p - y^p = (x-y)(x-\zeta y)(x-\zeta^2 y)\cdots(x-\zeta^{p-1}y)$$

και λαμβάνοντας υπόψιν ότι ο p είναι περιττός, αν αντικαταστήσουμε το y με $-y$ βρίσκουμε

$$x^p + y^p = (x+y)(x+\zeta y)(x+\zeta^2 y)\cdots(x+\zeta^{p-1}y)$$

Ο γάλλος μαθηματικός Lamé χρησιμοποίησε αυτές ακριβώς τις $p-$οστές ρίζες της μονάδας, για να παραγοντοποιήσει την εξίσωση του Fermat σε *γραμμικούς παράγοντες*, ως εξής:

$$z^p = x^p + y^p = (x+y)(x+\zeta y)(x+\zeta^2 y)\cdots(x+\zeta^{p-1}y) = \prod_{j=0}^{p-1}(x+\zeta^j y)$$

Μάλιστα βιάστηκε να συμπεράνει πως, αν οι παράγοντες στα δεξιά είναι μεταξύ τους σχετικά πρώτοι, καθένας από αυτούς είναι μια $p^{\text{οστή}}$ δύναμη κάποιου άλλου στοιχείου, για να μπορεί να ισχύει η σχέση. Ένας τέτοιος συλλογισμός θεωρεί δεδομένο το εξής:

> αν ένα γινόμενο σχετικά πρώτων αριθμών είναι μια $p^{\text{οστή}}$ δύναμη κάποιου άλλου αριθμού, τότε καθένας παράγοντας είναι επίσης μια $p^{\text{οστή}}$ δύναμη.

Όμως αν και το Θεμελιώδες Θεώρημα της Αριθμητικής* καθιστά το παραπάνω προφανές στους συνήθεις ακέραιους, κάτι τέτοιο **δεν** ισχύει στους ακέραιους του $\mathbb{Q}[\zeta]$, όπως φαίνεται από θεωρήματα σχετικά με την παραγοντοποίηση.

*Κάθε ακέραιος αναλύεται κατά μοναδικό τρόπο σε γινόμενο πρώτων αριθμών(εξαιρώντας οποιαδήποτε αναδιάταξη των όρων).

i. Πυθαγόρειες τριάδες

Οι λύσεις ακέραιες της της εξίσωσης του Fermat για $n = 2$ είναι άπειρες και δεν είναι άλλες από τις γνωστές† *Πυθαγόρειες τριάδες*. Ας δούμε ποιες είναι αυτές:

Θεώρημα 2.1. ***(Πυθαγόρειες τριάδες)*** *Οι λύσεις της εξίσωσης $x^2+y^2 = z^2$, με $x,\ y,\ z$ σχετικά πρώτους ανά δυο, δίνονται παραμετρικά από τους τύπους:*

$$x = r^2 - s^2 \quad , \quad \pm y = 2rs \quad , \quad \pm z = r^2 + s^2$$

(ή εναλλάσοντας τα $x,\ y$), όπου $r,\ s$ σχετικά πρώτοι και ακριβώς ένας εκ των δυο είναι περιττός.

Απόδειξη. Έστω ακέραιοι x, y, z σχετικά πρώτους ανά δυο με $x^2 + y^2 = z^2$. Παρατηρούμε πως κάποιος από αυτούς πρέπει να είναι άρτιος, διότι διαφορετικά θα ήταν άθροισμα περιττών ίσο με περιττό, το οποίο δε μπορεί να συμβεί. Επίσης, για να είναι σχετικά πρώτοι ανά δυο, πρέπει ακριβώς ένας από αυτούς να είναι άρτιος, αφού δυο άρτιοι δεν είναι σχετικά πρώτοι μεταξύ τους. Ο άρτιος αυτός δε μπορεί να είναι ο z, διότι αν $z = 2\kappa,\ y = 2\lambda + 1,\ x = 2\mu + 1$ θα είναι

$$(2\lambda + 1)^2 + (2\mu + 1)^2 = (2\kappa)^2 \Rightarrow 4\lambda^2 + 4\mu^2 + 4\lambda + 4\mu + 1 = 4\kappa^2 \Rightarrow 2 \equiv 0 \pmod 4$$

το οποίο είναι άτοπο.

Χωρίς βλάβη, θεωρούμε ότι ο y είναι άρτιος. Τότε

$$x^2 + y^2 = z^2 \Rightarrow y^2 = z^2 - x^2 \Rightarrow y^2 = (z + x)(z - x)$$

Οι δυο παράγοντες στα δεξιά είναι άρτιοι, ως άθροισμα και διαφορά περιττών και ομόσημοι, αφού είναι ίσοι με θετικό ακέραιο. Άρα $y = \pm 2a,\ z+x = \pm 2b,\ z-x = \pm 2c$, με $a, b, c \in \mathbb{N}$ και

$$(2a)^2 = 2b2c \Rightarrow a^2 = bc$$

Οι b, c είναι σχετικά πρώτοι, αφού αν είχαν κάποιον κοινό παράγοντα αυτός θα διαιρούσε τους $z - x$ και $z + x$, και τελικά (προσθέτοντας και αφαιρώντας) τους x, y. Οπότε για να είναι $a^2 = bc$, θα πρέπει καθένας από αυτούς να είναι τετράγωνο φυσικού:

$$\exists s, r \in \mathbb{N} \quad \text{ώστε} \quad b = s^2 \ , \ c = r^2$$

με s, r σχετικά πρώτους. Έτσι $z - x = \pm 2s^2,\ z + x = \pm 2r^2$ και:

$$\begin{aligned} z &= \frac{1}{2}(z + x + z - x) = \pm\frac{1}{2}(2s^2 + 2r^2) = \pm(s^2 + r^2) \\ x &= \frac{1}{2}(z + x - (z - x)) = \pm\frac{1}{2}(2s^2 - 2r^2) = \pm(r^2 - s^2) \end{aligned}$$

Κι επειδή οι x, y είναι περιττοί, ακριβώς ένας εκ των r, s είναι περιττός. Μένει να υπολογιστεί το y:

$$y = \pm 2a = \pm 2\sqrt{bc} = \pm 2sr$$ □

†ακόμη και στους αρχαίους Έλληνες και τους Βαβυλώνιους

ii. Μη ιδιάζοντες πρώτοι

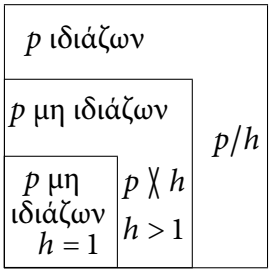
Ορισμός 2.1. *Ένας πρώτος p λέγεται* μη ιδιάζων *αν και μόνο αν δε διαιρεί την κλάση h του αριθμητικού σώματος $\mathbb{Q}(\zeta)$, όπου $\zeta = e^{2\pi i/p}$.*

Συνήθως στα μαθηματικά οι ορισμοί εφευρίσκονται αφού εμφανιστεί μια ανάλογη ανάγκη που τους επιβάλλει. Θα αναπτύξουμε το συλλογισμό που οδήγησε στον παραπάνω ορισμό.

Η μοναδική ανάλυση σε πρώτους παράγοντες ισχύει στο $\mathbb{Z}[\zeta]$ υπό συνθήκες. Συγκεκριμένα το (1.16) μας λέει πως ισχύει τότε και μόνο τότε όταν ο δακτύλιος των ακεραίων $\mathbb{Z}[\zeta]$ είναι Π.Κ.Ι ή ισοδύναμα έχει κλάση $h = 1$ σύμφωνα με το *Λήμμα (1.17)*. Εύλογο είναι να αναρωτηθούμε πότε συμβαίνει αυτό. Παραθέτουμε την απάντηση στο παρακάτω[26]:

Θεώρημα 2.2. *(Masley & Montgomery) Υπάρχουν ακριβώς 30 τιμές του $n \in \mathbb{N}$, με $n \not\equiv 2 \pmod 4$ για τις οποίες το $\mathbb{Z}[\zeta_n]$ είναι Π.Κ.Ι. Αυτές είναι: 1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84.*

το οποίο είναι τουλάχιστον απογοητευτικό για τους σκοπούς μας! Η παραγοντοποίηση που έκανε ο Lamé στην εξίσωση του Fermat είναι χρήσιμη μόνο για τα παραπάνω n. Γνωρίζουμε όμως κάτι ισχυρότερο για τα ιδεώδη του $\mathbb{Z}[\zeta]$. Εδώ δεν υπάρχει συνθήκη για να ισχύει η μοναδική ανάλυση. Προφανώς όμως η σχέση που έχουμε στη διάθεσή μας τώρα είναι ασθενέστερη από την αρχική. Θα πρέπει να εισάγουμε κατάλληλες συνθήκες για να πάνε όλα όπως πρέπει κατά την απόδειξη. Αυτές ακριβώς τις συνθήκες παρατήρησε ο Kummer και για να γίνουμε πιο συγκεκριμένοι, απαιτείται το συμπέρασμα του *Λήμματος (1.15α′)*. Είναι τώρα εύκολο να καταλάβει κανείς που αποβλέπει ο ορισμός των *μη ιδιαζόντων πρώτων*. Σχηματικά ο διαχωρισμός του συνόλου των πρώτων που γίνεται έχει ως εξής:



Το σύνολο $\{p \text{ πρώτος} : h = 1\}$ έχει όπως είδαμε 7 μόλις στοιχεία.

Το σύνολο $\{p \text{ πρώτος} : p \nmid h\}$ των μη ιδιαζόντων πρώτων δεν είναι γνωστό αν είναι πεπερασμένο ή άπειρο. Υπάρχει μια εικασία(Siegel) πως ασυμπτωτικά 60.65% του συνόλου των πρώτων είναι μη ιδιάζοντες, το οποίο επαληθεύεται υπολογιστικά (και συνεχίζει να κρατά καθώς η υπολογιστική ισχύς μεγαλώνει). Θα δούμε

ύστερα πως φτάνουμε σε αυτό το αποτέλεσμα με τη βοήθεια μιας πιθανοτικής υπόθεσης σχετικά με τους αριθμούς Bernoulli.

Αν και η επιβεβαίωση για το άπειρο πλήθος των μη ιδιαζόντων πρώτων δεν έχει επιτευχθεί, έχει αποδειχθεί (και μάλιστα αρκετά εύκολα) το παρακάτω[10]:

Θεώρημα 2.3. *(Jensen) Υπάρχουν άπειροι ιδιάζοντες πρώτοι αριθμοί.*

Μερικοί ιδιάζοντες πρώτοι είναι οι: 37, 59, 67, 101, 103, 131, 389, 401, 409, 541, 547, 557, 577, 587, 593, 607, 653, 659, 673, 677, 809, 811, 881, 887, 1061. Συνολικά υπάρχουν 65 ιδιάζοντες και 113 μη ιδιάζοντες πρώτοι έως το 1061 είναι.

Στον παρακάτω πίνακα φαίνεται η κλάση του δακτυλίου $\mathbb{Z}[\zeta]$ για διάφορα p.

p	3	5	7	11	13	17	19	23	29	31	**37**	41	43	47	53	**59**	61
h	1	1	1	1	1	1	1	3	8	9	37	121	211	695	4889	41241	76301

Οι πρώτοι 37, 59 είναι ιδιάζοντες(41241/59 = 699). Παρατηρήστε επίσης πως το για $p = 23$ το $\mathbb{Z}[\zeta]$ δεν είναι Περιοχή Μοναδικής Παραγοντοποίησης. Το σφάλμα μιας απόδειξης του θεωρήματος Fermat που υποθέτει κάτι τέτοιο γίνεται αρκετά νωρίς εμφανές.

iii. Αριθμοί Bernoulli

Θα θέλαμε τώρα ένα κριτήριο για τον εντοπισμό μη ιδιαζόντων πρώτων· ο ορισμός δεν καθιστά εύκολο των εντοπισμό τους, διότι ο υπολογισμός της κλάσης του $\mathbb{Z}[\zeta]$ είναι γενικά ένα δύσκολο πρόβλημα. Κατά ένα μαγευτικό τρόπο όμως, οι πρώτοι που μας ενδιαφέρουν σχετίζονται με τους λεγόμενους αριθμούς Bernoulli.

Ορισμός 2.2. *(αναδρομικός) Οι αριθμοί Bernoulli είναι οι όροι B_k της ακολουθίας:*

$$(k+1)B_k = -\sum_{m=0}^{k-1} \binom{k+1}{m} B_m, \quad B_0 = 1$$

Είναι φανερό ότι είναι μια ακολουθία ρητών. Οι ίδιοι αριθμοί καθορίζονται από τους συντελεστές της δυναμοσειράς:

$$\frac{t}{e^t - 1} = B_0 + \sum_{n=1}^{\infty} \frac{B_n}{n!} t^n, \quad B_0 = 1$$

απ΄ όπου με πράξεις βλέπουμε ότι

$$\sum_{k=0}^{n-1} \binom{n}{k} B_k = 0$$

Οι τιμές τους είναι πολύ ακανόνιστες: μεγαλώνουν αρκετά γρήγορα, και μάλιστα ισχύει $|B_{2m}| > 2(m/\pi e)^{2m}$. Για k περιττό μεγαλύτερο του 1 είναι μηδενικοί. Μερικοί B_k φαίνονται στον παρακάτω πίνακα.

κ	2	4	6	8	10	12	14	16
B_k	$\frac{1}{6}$	$-\frac{1}{30}$	$\frac{1}{42}$	$-\frac{1}{30}$	$\frac{5}{66}$	$-\frac{691}{2730}$	$\frac{7}{6}$	$-\frac{3617}{510}$

Τέλος ας δούμε πως συνδέονται οι αριθμοί αυτοί με τους πρώτους του Kummer. Αποδεικνύεται ότι η κλάση h του $\mathbb{Q}[\zeta]$ διαιρείται με τον p αν και μόνο αν υπάρχει αριθμός μεταξύ των

$$S_k = \sum_{n=1}^{p-1} n^k$$

ο οποίος διαιρείται με p^2. Συσχετίζοντας τους S_k με τους B_k αποδεικνύεται το

Θεώρημα 2.4. *Ένας πρώτος p είναι* μη ιδιάζων *αν και μόνο αν δε διαιρεί κανέναν απ΄ τους αριθμητές των αριθμών Bernoulli $B_2,\ B_4,\ \ldots,$ έως B_{p-3}.*

Έτσι έχουμε έναν αλγόριθμο προσδιορισμού ιδιαζόντων πρώτων. Παραδείγματος χάριν βλέπουμε ότι ο 37 είναι ιδιάζων, αφού

$$B_{32} = \frac{7709321041217}{510} = \frac{208360028141 \cdot 37}{510}$$

Σήμερα έχουν υπολογιστεί πάνω από 12.000.000 ιδιάζοντες πρώτοι[25].

Τέλος, ας δούμε πως φτάνουμε στην εικασία για το πλήθος των μη ιδιαζόντων πρώτων[‡]. Υποθέτουμε ότι η πιθανότητα ένας τυχόν πρώτος p να διαιρεί έναν άρτιου δείκτη αριθμό Bernoulli B_{2m} είναι $\frac{1}{p}$. Έστω η τυχαία μεταβλητή:

$$X:\ \text{ο } p \text{ διαιρεί ακριβώς } x \text{ από τους } B_2,\ B_4,\ \ldots, B_{p-3}$$

Τότε, η X ακολουθεί τη διωνυμική κατανομή με παραμέτρους $\nu := \frac{p-3}{2}$ και $\frac{1}{p}$. Αφήνοντας το ν να τείνει στο άπειρο, βλέπουμε ότι

$$\lim_{\nu\to\infty} \nu\frac{1}{p} = \lim_{p\to\infty}\left(\frac{p-3}{2}\cdot\frac{1}{p}\right) = \lim_{p\to\infty}\left(\frac{1}{2} - \frac{3}{2p}\right) = \frac{1}{2}$$

άρα ασυμπτωτικά, η πιθανότητα ο p να διαιρεί x αριθμούς Bernoulli ακολουθεί την κατανομή Poisson με παράμετρο $\frac{1}{2}$. Η συνάρτηση πιθανότητας είναι

$$f(x) = e^{-1/2}\frac{(1/2)^x}{x!} \quad , \quad x = 0, 1, 2, \ldots$$

Τελικά η πιθανότητα ο p να είναι μη ιδιάζων, είναι η πιθανότητα $x = 0$:

$$f(0) = e^{-1/2}\frac{(1/2)^0}{0!} = e^{-1/2} = \frac{1}{\sqrt{e}} \cong 0.6065$$

Όπως αναφέρθηκε, οι υπολογισμοί συμφωνούν στενά με αυτήν την πρόβλεψη.

[‡] Θα χρειαστούμε κάποιες γνώσεις πιθανοτήτων [22]

iv. Οι προτάσεις του Kummer

Ο Kummer έκανε μια εκτενής μελέτη του δακτυλίου των ακεραίων των κυκλοτομικών σωμάτων, της ομάδας των αντιστρέψιμων στοιχείων και της ομάδας κλάσης $\mathfrak{H}$. Αναφέρουμε μερικά από τα αποτελέσματα αυτά, τα οποία θα χρειαστούμε στην απόδειξη του Θεωρήματος του Fermat.

Λήμμα 2.1. *Οι μόνες ρίζες της μονάδας στο $\mathbb{Q}(\zeta)$ είναι στοιχεία της μορφής $\pm\zeta^s$ για κάποιο $s \in \mathbb{Z}$.*

Λήμμα 2.2. *Για κάθε $\delta \in \mathbb{Z}[\zeta]$ υπάρχει $\delta' \in \mathbb{Z}$ ώστε $\delta^p \equiv \delta' \pmod{\langle 1-\zeta\rangle^p}$.*

Λήμμα 2.3. *Αν $g(t) \in \mathbb{Z}[\zeta]$ ένα μονικό πολυώνυμο, που όλες οι μιγαδικές του ρίζες έχουν απόλυτη τιμή 1, τότε κάθε ρίζα του είναι και μια* ρίζα της μονάδας.

Λήμμα 2.4. *Κάθε αντιστρέψιμο στοιχείο στο $\mathbb{Z}[\zeta]$ είναι της μορφής $r\zeta^k$, για $r \in \mathbb{R}$ και $k \in \mathbb{Z}$.*

Για αποδείξεις των παραπάνω παραπέμπουμε στο [1]. Μεγάλης σημασίας για την απόδειξη της Δεύτερης Περίπτωσης είναι και το παρακάτω αποτέλεσμα, το οποίο αναφέρεται ως *Λήμμα του Kummer*. Πρόκειται για ένα βαθύ θεώρημα που αφορά στα αντιστρέψιμα στοιχεία του $\mathbb{Z}(\zeta)$. Η απόδειξή του απαιτεί μια ολόκληρη μαθηματική θεωρία(Class Field Theory), και μπορεί να βρεθεί στο [2]:

Λήμμα 2.5. *(**Λήμμα του Kummer**) Έστω p μη ιδιάζων πρώτος και $e \in \mathbb{Z}(\zeta)$ αντιστρέψιμο. Αν υπάρχει $r \in \mathbb{Z}[\zeta]$ ώστε $e \equiv r^p \pmod{\ell^p}$, τότε το e είναι η $p^{οστή}$ δύναμη ενός άλλου αντιστρέψιμου στοιχείου του $\mathbb{Z}(\zeta)$.*

πιο συνηθισμένη είναι η διατύπωση: *αν υπάρχει $r \in \mathbb{Z}$ ώστε $e \equiv r \pmod{p}$, τότε το e είναι η $p^{οστή}$ δύναμη ενός άλλου αντιστρέψιμου στοιχείου του $\mathbb{Z}(\zeta)$.* Σε αυτήν φτάνουμε με χρήση του Λήμματος 2.2.

III. Η απόδειξη του Kummer

Έγινε προσπάθεια ώστε η ανάγνωση της απόδειξης να μην αφήνει παρά μόνο ελάχιστες απορίες στον αναγνώστη, σε σημείο που μπορεί να χαρακτηριστεί κουραστικά αναλυτική(αν μπορεί κάποιος ποτέ να θεωρήσει κουραστική τη λύση σε ένα αίνιγμα ηλικίας τρεισήμισι αιώνων!). Οι συλλογισμοί εξηγούνται αναλυτικά και αναφέρονται οι προτάσεις - λήμματα που εμπλέκονται σε κάθε συμπέρασμα.

Κατ΄ αρχήν κάποιες παρατηρήσεις.

Παρατήρηση 3.1. Η εξίσωση $x^n + y^n = z^n$ έχει λύση αν και μόνο αν η $x^n + y^n + z^n = 0,\ n \geq 3$ έχει λύση.

Έστω (x_1, y_1, z_1) λύση της πρώτης εξίσωσης. Η τριάδα $(x_1, y_1, -z_1)$ ικανοποιεί τη δεύτερη εξίσωση. Ο μετασχηματισμός που έγινε είναι αμφιμονοσήμαντος.
Συμπέρασμα: Μπορούμε ισοδύναμα να θεωρήσουμε λύσεις της

$$x^n + y^n + z^n = 0$$

για την απόδειξη του θεωρήματος.

Παρατήρηση 3.2. Έστω ακέραιοι $x_1,\ y_1,\ z_1$ που ικανοποιούν $x_1^n + y_1^n + z_1^n = 0$. Τότε υπάρχουν ακέραιοι $x_2,\ y_2,\ z_2$ ανά δυο πρώτοι, ώστε να ικανοποιούν $x_2^n + y_2^n + z_2^n = 0$.

Πράγματι αν υπάρχει ένας κοινός παράγοντας q των $x_1,\ y_1$, τότε έχουμε $(qx_2)^n + (qy_2)^n + (z_1)^n$ και έπεται ότι $q^n(x_2^n + y_2^n) = (z_1)^n$, δηλαδή ο q είναι παράγοντας και του z_1, δηλαδή $z_1 = qz_2$ άρα

$$q^n(x_2^n + y_2^n) + q^n z_2^n = 0 \Rightarrow x_2^n + y_2^n + z_2^n = 0$$

Συμπέρασμα: Αρκεί να δειχθεί το θεώρημα για την περίπτωση που οι $x,\ y,\ z$ είναι ανά ζεύγη σχετικά πρώτοι.

Παρατήρηση 3.3. Αν η εξίσωση του Fermat είναι αδύνατη για έναν εκθέτη n, τότε είναι αδύνατη για κάθε πολλαπλάσιο του n.

Πράγματι αν η εξίσωση είναι αδύνατη για τον n, τότε η $(x^m)^n + (y^m)^n + (z^m)^n = 0$ είναι αδύνατη, για οποιονδήποτε ακέραιο m, άρα η $x^{mn} + y^{mn} + z^{mn} = 0$ δεν έχει λύσεις.
Συμπέρασμα: Αρκεί να δειχθεί το θεώρημα για την περίπτωση περιττού πρώτου εκθέτη και στην περίπτωση εκθέτη πολλαπλάσιου του 2.

Παρατήρηση 3.4. Κάθε ακέραιος $k \geq 3$ διαιρείται είτε με το 4 είτε με έναν περιττό πρώτο.

Αυτό φαίνεται αναλύοντας τον k σε πρώτους παράγοντες. Έστω ότι ο k γράφεται

$$k = 2^{q_1} \cdot p_2^{q_2} \cdots p_n^{q_n}$$

με $p_2,\ p_3, \ldots,\ p_n$ διακεκριμένους πρώτους και $q_1,\ q_2, \ldots,\ q_n \geq 0$. Διακρίνουμε τώρα τα παρακάτω ενδεχόμενα για τον εκθέτη q_1:

- Αν είναι $q_1 = 0$, τότε η ανάλυση του k σε πρώτους δεν περιέχει το 2. Άρα αφού $k \geq 3$ θα περιέχει έναν περιττό πρώτο(δηλαδή υπάρχει $q_i > 0, i > 1$).

- Αν είναι $q_1 = 1$, τότε $k = 2 \cdot p_2^{q_2} \cdots p_n^{q_n}$, άρα $2 \cdot p_2^{q_2} \cdots p_n^{q_n} \geq 3$, οπότε υπάρχει κάποιο $q_i > 0,\ i \in \{2, 3, \ldots, n\}$. Τελικά p_i / k, και ο p_i είναι περιττός πρώτος.

- Η περίπτωση $q_1 \geq 2$ σημαίνει ότι $q_1 = 2 + \rho$, με $\rho \geq 0$.
  Τότε όμως $k = 2^{2+\rho} \cdot p_2^{q_2} \cdots p_n^{q_n}$, άρα $k = 4 \cdot 2^{\rho} \cdot p_2^{q_2} \cdots p_n^{q_n}$ από όπου έπεται ότι $4/k$.

Συμπέρασμα: Αρκεί να δειχθεί το θεώρημα για τις περιπτώσεις εκθετών: 4 και περιττού πρώτου.

Με τα παραπάνω είμαστε σε θέση να διατυπώσουμε το (ισοδύναμο με το θεώρημα Fermat) πρόβλημα:

Αν p περιττός πρώτος αριθμός ή p = 4 , τότε η εξίσωση

$$\mathbf{x^p + y^p + z^p = 0} \quad , \quad \mathbf{xyz \neq 0} \tag{1}$$

δεν έχει ακέραιες λύσεις (x, y, z), με x, y, z ανά ζεύγη σχετικά πρώτους.

Το οποίο δεν έχει αποδειχθεί με τη συγκεκριμένη θεωρία, παρά μόνο για την κατηγορία των «μη ιδιαζόντων πρώτων».

Με αυτήν την *παραδοχή*, ότι δηλαδή **ο p είναι μη ιδιάζων πρώτος** χωρίζουμε το πρόβλημα στις εξής τρεις περιπτώσεις:

(i) Ο εκθέτης να είναι 4.

(ii) Κάθε ακέραιος της λύσης να είναι σχετικά πρώτος με τον p.

(iii) Ένας ακριβώς από τους ακεραίους της λύσης να διαιρείται με τον p.

τις οποίες θα αποδείξουμε αναλυτικά στις παραγράφους που ακολουθούν.

Ιστορικά, η (ii) αναφέρεται ως Πρώτη Περίπτωση του θεωρήματος, ενώ η (iii) ως Δεύτερη Περίπτωση.

i. Η περίπτωση $n = 4$

Ένα επιχείρημα ελάχιστου στοιχείου θα μας δώσει την αντίφαση που θέλουμε για να αποδείξουμε* ότι

Θεώρημα 3.1. *Η εξίσωση $x^4 + y^4 = z^4$ δεν έχει ακέραιες λύσεις.*

Απόδειξη. Παρατηρούμε πως αρκεί να δείξουμε πως η εξίσωση

$$x^4 + y^4 = z^2 \tag{2}$$

δεν έχει ακέραιες λύσεις, αφού κάθε λύση (x_1, y_1, z_1) της αρχικής μετασχηματίζεται στην (x_1, y_1, z_1^2) που είναι λύση της (2).

Χωρίς βλάβη τώρα κάνουμε τις εξής βοηθητικές υποθέσεις:

(i) Θεωρούμε μια λύση (x, y, z) της (2) με $x,\ y,\ z > 0$.

(ii) Υποθέτουμε ότι οι ακέραιοι $x,\ y,\ z$ είναι ανά δυο σχετικά πρώτοι.

Το *Λήμμα (2.1)* μας δίνει τις σχέσεις

$$x^2 = \alpha^2 - \beta^2, \quad y^2 = 2\alpha\beta, \quad z = \alpha^2 + \beta^2$$

όπου μόνο ο z είναι περιττός. Έτσι παίρνουμε $x^2 + \beta^2 = \alpha^2$, οπότε έχουμε μια καινούρια πυθαγόρεια τριάδα και θα είναι

$$x = \varepsilon^2 - \delta^2, \quad \beta = 2\varepsilon\delta, \quad \alpha = \varepsilon^2 + \delta^2$$

Συνδυάζοντας τα παραπάνω έχουμε

$$y^2 = 2\alpha\beta = 2 \cdot (\varepsilon^2 + \delta^2) \cdot 2\varepsilon\delta = 2^2\varepsilon\delta(\varepsilon^2 + \delta^2)$$

άρα ο y είναι άρτιος, δηλαδή $y = 2r,\ \ r \in \mathbb{N}$, και $(2r)^2 = 2^2\varepsilon\delta(\varepsilon^2 + \delta^2)$ ή

$$r^2 = \varepsilon\delta(\varepsilon^2 + \delta^2)$$

Παρατηρούμε τώρα πως οι παράγοντες $\varepsilon,\ \delta,\ \varepsilon^2 + \delta^2$ είναι σχετικά πρώτοι ανά δυο, άρα, εφόσον ισούνται με τετράγωνο αριθμού, καθένας απ′ αυτούς θα είναι τετράγωνο ενός φυσικού†. Είναι δηλαδή:

$$\alpha = \kappa^2, \quad \beta = \lambda^2, \quad \varepsilon^2 + \delta^2 = \mu^2$$

Συνδυάζοντας αυτές τις τρεις έχουμε: $\kappa^4 + \lambda^4 = \mu^2$ άρα η τριάδα (κ, λ, μ) είναι λύση της (2). Δείτε τώρα ότι:

$$\mu \leq \mu^2 = \varepsilon^2 + \delta^2 = \alpha < \alpha^2 + \beta^2 = z$$

Όμως ο z επελέγη ως ο μικρότερος ακέραιος που ικανοποιεί την (2), άρα $\mu < z$ αποτελεί αντίφαση. □

*Η απόδειξη αυτής της περίπτωσης έγινε από τον ίδιο τον Fermat, με τη μέθοδο της «άπειρης καθόδου»

†Προσέξτε αυτό το επιχείρημα! Στην απόδειξη των επόμενων περιπτώσεων του θεωρήματος ένα ανάλογο επιχείρημα θα χρειαστεί περισσότερη δουλειά για να διατυπωθεί, γιατί προϋποθέτει τη λεπτή ιδιότητα της μοναδικής ανάλυσης σε πρώτους παράγοντες.

ii. Πρώτη Περίπτωση για μη ιδιάζοντες πρώτους εκθέτες

Θεώρημα 3.2. *Έστω p περιττός και μη ιδιάζων πρώτος. Η (1) δεν έχει ακέραιες λύσεις, με την επιπλέον υπόθεση οι x, y, z να είναι σχετικά πρώτοι με τον p.*

Απόδειξη. Αρχικά θεωρούμε το κυκλοτομικό σώμα $\mathbb{Q}(\zeta)$, όπου $\zeta = e^{2\pi i/p}$ και παραγοντοποιούμε την εξίσωση (1) σε αυτό:

$$-z^p = x^p + y^p = (x+y)(x+\zeta y)(x+\zeta^2 y)\cdots(x+\zeta^{p-1}y) = \prod_{j=0}^{p-1}(x+\zeta^j y)$$

Και τη γράφουμε ισοδύναμα με τη χρήση ιδεωδών:

$$\prod_{j=0}^{p-1}\langle x+\zeta^j y\rangle = \langle z\rangle^p \tag{3}$$

Ισχυρισμός 1. *Οι παράγοντες $\langle x+y\rangle$, $\langle x+\zeta^1 y\rangle, \ldots, \langle x+\zeta^{p-1}y\rangle$ της σχέσης (3) είναι ανά δυο σχετικά πρώτοι.*

Απόδειξη Ισχυρισμού. Έστω πως υπάρχουν δυο ιδεώδη $\langle x+\zeta^i y\rangle$, $\langle x+\zeta^j y\rangle$ με $0 \le i < j \le p-1$, που δεν είναι σχετικά πρώτα. Τότε θα υπάρχει ένα πρώτο ιδεώδες $\mathfrak{p}$ που τα περιέχει. Άρα το $\mathfrak{p}$ θα περιέχει τη διαφορά

$$(x+\zeta^i y) - (x+\zeta^j y) \in \mathfrak{p}$$

δηλαδή

$$y\zeta^i(1-\zeta^{j-i}) \in \mathfrak{p}$$

Το ζ^i είναι αντιστρέψιμο στο $\mathbb{Z}[\zeta]$, οπότε $y(1-\zeta^{j-i}) \in \mathfrak{p}$ και τα $1-\zeta^{j-i}$, $1-\zeta$ είναι συντροφικά στοιχεία, άρα $y(1-\zeta) \in \mathfrak{p}$. Επειδή τώρα το $\mathfrak{p}$ είναι πρώτο ιδεώδες, δυο τινά μπορεί να συμβαίνουν (1.11):

(i) $\mathfrak{p} \supseteq \langle y\rangle$ ή

(ii) $\mathfrak{p} \supseteq \ell$

όπου συμβολίζουμε $\ell = \langle 1-\zeta\rangle$. Θα αποκλείσουμε αυτές τις δυο περιπτώσεις:

(i) Έστω $\mathfrak{p} \supseteq \langle y\rangle$, δηλαδή $y \in \mathfrak{p} \Rightarrow \zeta^i y \in \mathfrak{p}$, όμως από υπόθεση $(x+\zeta^i y) \in \mathfrak{p}$, άρα η διαφορά $(x+\zeta^i y) - \zeta^i y = x \in \mathfrak{p}$. Επειδή οι x, y είναι σχετικά πρώτοι, υπάρχουν ακέραιοι m, n ώστε $mx + ny = 1$. Το αριστερό μέλος ανήκει στο $\mathfrak{p}$ άρα $1 \in \mathfrak{p}$. Αυτό όμως είναι αδύνατο διότι το $\mathfrak{p}$ είναι πρώτο.

(ii) Έστω τώρα $\mathfrak{p} \supseteq \ell$, ή αλλιώς $(1-\zeta) \in \mathfrak{p}$. Έχουμε $N(1-\zeta) = p$, άρα από *Λήμμα (1.13)* το ℓ είναι πρώτο, επειδή η νόρμα του είναι πρώτος. Επίσης $\mathfrak{p}/\ell$ (*Λήμμα (1.14)*) και αυτά τα δυο είναι πρώτα ιδεώδη, δηλαδή θα είναι $\mathfrak{p} = \ell$. Εξ΄ ορισμού του το $\mathfrak{p}$ διαιρεί το αριστερό μέλος της (3), άρα $\ell/\langle z\rangle$. Παίρνοντας νόρμες:

$$\begin{aligned} &\Longrightarrow && N(\ell)/N(\langle z\rangle) \\ &\overset{(1.24),\ (1.8)}{\Longrightarrow} && p/z^{p-1} \\ &\overset{p\ \text{πρώτος}}{\Longrightarrow} && p/z \end{aligned}$$

Αυτό όμως είναι άτοπο εξ΄ υποθέσεως. ∎

Το αποτέλεσμα του *Ισχυρισμού 1* θα μας βοηθήσει να φτάσουμε στον βασικό:

Ισχυρισμός 2. *Υπάρχει ακέραιος $k \in \mathbb{Z}$ ώστε*

$$x\zeta^{-k} + y\zeta^{1-k} - x\zeta^{k} - y\zeta^{k-1} \equiv 0 \pmod{\langle p\rangle} \tag{4}$$

Απόδειξη Ισχυρισμού. Από το τη Μοναδικότητα Παραγοντοποίησης Ιδεωδών σε πρώτους παράγοντες (1.18) έπεται πως το $\langle z\rangle$ αναλύεται με μοναδικό τρόπο σε πρώτα ιδεώδη. Ο *Ισχυρισμός 1* όμως μας λέει πως οι παράγοντες του αριστερού μέλους της (3) είναι ανά δύο σχετικά πρώτοι. Άρα, καθένας απ΄ αυτούς είναι μια $p^{\text{οστή}}$ δύναμη κάποιου ιδεώδους, διότι διαφορετικά το $\langle z\rangle^p$ θα είχε δυο διαφορετικές παραγοντοποιήσεις σε πρώτους παράγοντες. Συγκεκριμένα, για τον δεύτερο παράγοντα του γινομένου θα υπάρχει ιδεώδες $\mathfrak{a}$ ώστε:

$$\langle x + \zeta y\rangle = \mathfrak{a}^p$$

Δηλαδή το $\mathfrak{a}^p$ είναι κύριο. Από την υπόθεση ότι ο p δεν είναι ιδιάζων, ο ορισμός (2.1) επιβάλλει ότι ο p δε διαιρεί την κλάση του $\mathbb{Q}(\zeta)$, άρα είναι σχετικά πρώτος με αυτήν. Έπεται από το Λήμμα (1.15) ότι το $\mathfrak{a}$ είναι κύριο. Έτσι υπάρχει $\delta \in \mathbb{Z}[\zeta]$ ώστε $\mathfrak{a} = \langle\delta\rangle$. Άρα υπάρχει ένα αντιστρέψιμο στοιχείο u του $\mathbb{Z}[\zeta]$ ώστε

$$x + \zeta y = u\delta^p \tag{5}$$

Θυμηθείτε από το Λήμμα (2.4) ότι

$$u = r\zeta^k \quad r \in \mathbb{R},\ \ k \in \mathbb{Z} \tag{6}$$

Επίσης από το Λήμμα (2.2) $\delta^p \equiv \delta' \pmod{\ell^p}$, $\delta' \in \mathbb{Z}$. Το Λήμμα (1.24) μας δίνει $\ell^{p-1} = \langle p\rangle \Rightarrow \langle p\rangle/\ell^p$ και η προηγούμενη σχέση γίνεται:

$$\delta^p \equiv \delta' \pmod{\langle p\rangle} \tag{7}$$

Μπορούμε τώρα να ξαναγράψουμε την (5) ως εξής:

$$\begin{aligned} & x+\zeta y = u\delta^p \\ \Longrightarrow \quad & x+\zeta y \equiv u\delta^p \pmod{\langle p\rangle} \\ \overset{(6)}{\Longrightarrow} \quad & x+\zeta y \equiv r\zeta^k\delta^p \pmod{\langle p\rangle} \\ \overset{(7)}{\Longrightarrow} \quad & x+\zeta y \equiv r\delta'\zeta^k \pmod{\langle p\rangle} \end{aligned}$$

Επειδή το ζ^k είναι αντιστρέψιμο, μπορούμε να διαιρέσουμε με αυτό και να λάβουμε:

$$\zeta^{-k}(x+\zeta y) \equiv r\delta' \pmod{\langle p\rangle}$$

Εφόσον $r\delta' \in \mathbb{R}$, παίρνοντας τους συζυγείς μιγαδικούς θα είναι:

$$\zeta^{k}(x+\zeta^{-1} y) \equiv r\delta' \pmod{\langle p\rangle}$$

Άρα

$$\zeta^{-k}(x+\zeta y) - \zeta^{k}(x+\zeta^{-1} y) \equiv r\delta' - r\delta' \equiv 0 \pmod{\langle p\rangle}$$

και μετά από πράξεις

$$x\zeta^{-k} + y\zeta^{1-k} - x\zeta^{k} - y\zeta^{k-1} \equiv 0 \pmod{\langle p\rangle}$$

άρα η σχέση αποδείχθηκε. ∎

Απομένει να απλοποιήσουμε το αριστερό μέλος της εξίσωσης (4). Αυτό θα γίνει βρίσκοντας κάποια σχέση μεταξύ του k και του p. Πράγματι:

Ισχυρισμός 3. *Για τον ακέραιο k της (4) ισχύει ότι:* $2k \equiv 1 \pmod{p}$.

Απόδειξη Ισχυρισμού. Αρχικά δείχνουμε διαδοχικά τα εξής δυο αποτελέσματα:

(i) Το στοιχείο $1+\zeta$ είναι αντιστρέψιμο.

(ii) Για τον ακέραιο k είναι $k \not\equiv 0 \pmod{p}$ και $k \not\equiv 1 \pmod{p}$.

Κατόπιν το (ii) θα μας φτάσει πολύ κοντά στην απόδειξη. Για το πρώτο:

(i) Θεωρούμε το ελάχιστο πολυώνυμο $g(t) \in \mathbb{Z}[t]$ του ζ. Από το Λήμμα (1.20) αυτό είναι το $g(t) = t^{p-1} + t^{p-2} + \cdots + t^2 + t + 1$. Παρατηρούμε ότι ο $p-1$ είναι άρτιος αριθμός, και το $g(t)$ έχει περιττό αριθμό όρων, δηλαδή είναι:

$$\begin{aligned} g(-1) &= (-1)^{p-1} + (-1)^{p-2} + \cdots + (-1)^2 + (-1) + 1 \\ &= 1 - 1 + 1 - 1 + \cdots + 1 - 1 + 1 \\ &= 1 \end{aligned}$$

Το $g(t)$ προφανώς έχει ρίζα το ζ, άρα για κάποιο πολυώνυμο $q(t) \in \mathbb{Z}[t]$ θα είναι:

$$\begin{aligned} & (t-\zeta)q(t) = g(t) \\ \Longrightarrow \quad & (-1-\zeta)q(-1) = g(-1) \\ \Longrightarrow \quad & -q(-1)(1+\zeta) = 1 \end{aligned}$$

Άρα το $-q(-1) \in \mathbb{Z}(\zeta)$ είναι ο αντίστροφος του $1+\zeta$ και το ζητούμενο ισχύει.

(ii) Έστω $k \equiv 0 \pmod{p}$.
Τότε $\zeta^k = \zeta^{-k} = 1,\ \zeta^{1-k} = \zeta,\ \zeta^{k-1} = \zeta^{-1}$ και η (4) γίνεται

$$\begin{aligned} & x + y\zeta^{1-k} - x - y\zeta^{k-1} \equiv 0 \pmod{\langle p \rangle} \\ \Longrightarrow \quad & y(\zeta - \zeta^{-1}) \equiv 0 \pmod{\langle p \rangle} \\ \Longrightarrow \quad & y\zeta^{-1}(\zeta^2 - 1) \equiv 0 \pmod{\langle p \rangle} \\ \Longrightarrow \quad & y\zeta^{-1}(\zeta+1)(\zeta-1) \equiv 0 \pmod{\langle p \rangle} \\ \Longrightarrow \quad & y(\zeta - 1) \equiv 0 \pmod{\langle p \rangle} \\ \Longrightarrow \quad & y(1-\zeta) \equiv 0 \pmod{\langle p \rangle} \end{aligned}$$

όπου λάβαμε υπόψιν ότι τα $\zeta^{-1},\ 1+\zeta$ είναι αντιστρέψιμα στοιχεία.

Όπως είδαμε και πριν(Λήμμα (1.24)) $\ell^{p-1} = \langle p \rangle$ και αφού $p - 1 \geq 2$ θα είναι:

$$(1-\zeta)/y \Rightarrow N(1-\zeta)/N(y) \overset{(1.23),\ (1.8)}{\Longrightarrow} p/y^{p-1} \overset{p \text{ πρώτος}}{\Longrightarrow} p/y$$

το οποίο είναι άτοπο από υπόθεση.

Όμοια, έστω $k \equiv 1 \pmod{p}$ ή αλλιώς $k - 1 \equiv 0 \pmod{p}$.
Τότε $\zeta^{k-1} = \zeta^{1-k} = 1,\ \zeta^k = \zeta,\ \zeta^{-k} = \zeta^{-1}$ και η (4) γίνεται

$$\begin{aligned} & x\zeta^{-1} + y - x\zeta - y \equiv 0 \pmod{\langle p \rangle} \\ \Longrightarrow \quad & x(\zeta^{-1} - \zeta) \equiv 0 \pmod{\langle p \rangle} \\ \Longrightarrow \quad & x\zeta^{-1}(1-\zeta^2) \equiv 0 \pmod{\langle p \rangle} \\ \Longrightarrow \quad & x\zeta^{-1}(1+\zeta)(1-\zeta) \equiv 0 \pmod{\langle p \rangle} \\ \Longrightarrow \quad & x(1-\zeta) \equiv 0 \pmod{\langle p \rangle} \end{aligned}$$

και εντελώς όμοια καταλήγουμε στην αντίφαση ότι p/x.

Έχουμε αποδείξει τα (i),(ii) και προχωρούμε θυμίζοντας ότι το σύνολο $\{1, \zeta, \ldots, \zeta^{p-1}\}$ είναι μια βάση του $\mathbb{Z}[\zeta]$ υπεράνω του $\mathbb{Z}$ (1.19). Επίσης η (4) μας εξασφαλίζει πως υπάρχει $a \in \mathbb{Z}[\zeta]$ ώστε

$$ap = x\zeta^{-k} + y\zeta^{1-k} - x\zeta^k - y\zeta^{k-1} \tag{8}$$

και διαιρώντας με p

$$a = \frac{x}{p}\zeta^{-k} + \frac{y}{p}\zeta^{1-k} - \frac{x}{p}\zeta^{k} - \frac{y}{p}\zeta^{k-1}$$

Το $a \neq 0$, γιατί διαφορετικά η λύση μας θα ήταν η μηδενική. Επίσης, είναι αδύνατο τα στοιχεία

$$\zeta^{-k},\ \zeta^{1-k},\ \zeta^{k},\ \zeta^{k-1}$$

να είναι **όλα** ανά δυο διαφορετικά μεταξύ τους, καθώς το a έχει μοναδική γραφή σαν γραμμικός συνδυασμός των στοιχείων της βάσης $\{1, \zeta, \ldots, \zeta^{p-1}\}$(το σύνολο είναι γραμμικά ανεξάρτητο και υπεράνω του $\mathbb{Q}$), άρα τότε οι συντελεστές $\frac{x}{p},\ \frac{y}{p} \in \mathbb{Z}$ το οποίο είναι άτοπο από υπόθεση(x, p και y, p σχετικά πρώτοι).

Συμπεραίνουμε πως υπάρχουν κάποια στοιχεία μεταξύ των $\zeta^{-k},\ \zeta^{1-k},\ \zeta^{k},\ \zeta^{k-1}$ που είναι ίσα. Ισοδύναμα, κάποιοι από τους $-k,\ 1-k,\ k,\ k-1$ θα είναι ισοϋπόλοιποι modulo p. Το (ii) αποκλείει τις περιπτώσεις[‡] να είναι

$$k \equiv -k \quad \text{ή} \quad k \equiv k-1 \quad \text{ή} \quad -k \equiv 1-k \quad \text{ή} \quad k-1 \equiv -k \quad \text{ή} \quad k-1 \equiv 1-k \pmod{p}$$

Τελικά η μόνη περίπτωση που υπάρχει είναι $k \equiv 1-k \pmod{p}$ άρα αποδείχθηκε ότι $2k \equiv 1 \pmod{p}$. ∎

Έχουμε αρκετές πληροφορίες για να προχωρήσουμε στο τελικό βήμα της απόδειξης.
Μπορούμε να πολλαπλασιάσουμε την (8) με ζ^k και να έχουμε:

$$ap\zeta^{k} = x + y\zeta - x\zeta^{2k} - y\zeta^{2k-1}$$

Και ο *Ισχυρισμός 3* μας λέει $\zeta^{2k} = \zeta$ και $\zeta^{2k-1} = 1$. Άρα

$$\begin{aligned} ap\zeta^{k} &= x + y\zeta - x\zeta - y \\ &= x(1-\zeta) + y(\zeta - 1) \\ &= x(1-\zeta) - y(1-\zeta) \\ &= (x-y)(1-\zeta) \end{aligned}$$

[‡]Οι δυνατές περιπτώσεις είναι οι έξι συνδυασμοί $\binom{4}{2}$

Λαμβάνοντας νόρμες έχουμε:

$$\begin{aligned}
& ap\zeta^k = (x-y)(1-\zeta) \\
\Longrightarrow \quad & N(ap\zeta^k) = N((x-y)(1-\zeta)) \\
\overset{(1.7\beta')}{\Longrightarrow} \quad & N(a)N(p)N(\zeta^k) = N(x-y)N(1-\zeta)) \\
\overset{(1.8),\ (1.23)}{\Longrightarrow} \quad & N(a)\cdot p^{p-1}\cdot 1 = (x-y)^{p-1}\cdot p \\
\Longrightarrow \quad & N(a)p^{p-2} = (x-y)^{p-1} \\
\overset{p\ \text{πρώτος},\ (1.7\alpha')}{\Longrightarrow} \quad & p/(x-y)^{p-1} \\
\Longrightarrow \quad & p/(x-y)
\end{aligned}$$

Δηλαδή $x-y \equiv 0 \pmod{p}$, και επειδή η αρχική μας εξίσωση (1) είναι συμμετρική ως προς $x,\ y,\ z$ μπορούμε να γράψουμε και $x-z \equiv 0 \pmod{p}$, άρα:

$$x \equiv y \equiv z \pmod{p} \tag{9}$$

Ξαναγράφουμε τώρα την (1) λαμβάνοντας modulo p:

$$\begin{aligned}
& x^p + y^p + z^p \equiv 0 \pmod{p} \\
\overset{(9)}{\Longrightarrow} \quad & 3x^p \equiv 0 \pmod{p} \\
\Longrightarrow \quad & p/x^p \quad \text{ή} \quad p/3 \\
\overset{p\ \text{πρώτος}}{\Longrightarrow} \quad & p/x \quad \text{ή} \quad p/3
\end{aligned}$$

Το πρώτο αποκλείεται εξ΄ υποθέσεως. Το δεύτερο σημαίνει $p = 3$. Άρα έχουμε πετύχει το στόχο μας για $p \neq 3$. Η απόδειξη ολοκληρώνεται με τον παρακάτω:

Ισχυρισμός 4. *Για $p = 3$ η εξίσωση (1) δεν έχει ακέραιες λύσεις.*

Απόδειξη Ισχυρισμού. Έστω $x,\ y,\ z$ που ικανοποιούν $x^3 + y^3 + z^3 = 0$. Θα δείξουμε ότι

$$x,\ y,\ z \equiv \pm 1 \pmod{9}$$

Έστω ότι για έναν απ΄ αυτούς, χωρίς βλάβη τον x, είναι $x \not\equiv \pm 1 \pmod{9}$. Τότε προφανώς $x \not\equiv \pm 1 \pmod{3}$. Δηλαδή είναι $x \equiv 0 \pmod{3}$, όμως αυτό είναι αδύνατο, επειδή υποθέσαμε ότι ο p δε διαιρείται με το 3. Άρα $x,\ y,\ z \equiv \pm 1 \pmod{9}$. Τελικά είναι:

$$0 \equiv x^3 + y^3 + z^3 \equiv \pm 1 \pm 1 \pm 1 \equiv \begin{cases} \pm 1 \\ \pm 3 \end{cases} \not\equiv 0 \pmod{9}$$

Άρα καταλήξαμε σε άτοπο. ∎

□

iii. Δεύτερη Περίπτωση για μη ιδιάζοντες πρώτους εκθέτες

Το βάρος της απόδειξης πέφτει σε ένα γενικότερο αποτέλεσμα, το *Θεώρημα 3.3.* Μια διαφορά με την Πρώτη Περίπτωση είναι πως δεν ισχύει ακριβώς ότι δήλωνει ο *Ισχυρισμός 1* της Πρώτης Περίπτωσης, αλλά κάτι παραπλήσιο, το οποίο χρειάζεται λίγη περισσότερη δουλειά. Η απόδειξη κρίνεται δυσκολότερη από την Πρώτη Περίπτωση, ιδιαίτερα επειδή γίνεται χρήση του περίφημου *Λήμματος του Kummer* (2.5).

Στην αρχή της απόδειξης του παρακάτω θεωρήματος, ο Kummer* ισχυρίστηκε πως μπορούμε να θεωρήσουμε τους $\alpha, \beta, \gamma \in \mathbb{Z}[\zeta]$ σχετικά πρώτους ανά δυο, όπως κάναμε στην *Παρατήρηση 3.2* για τους συνήθεις ακέραιους. Αυτό δεν είναι σωστό, καθώς η *Παρατήρηση 3.2* ισχύει στο $\mathbb{Z}$, όμως όχι στο $\mathbb{Z}[\zeta]$, επειδή αυτό δεν είναι Περιοχή Μοναδικής Παραγοντοποίησης(δεν αποκλείεται η ύπαρξη ενός κοινού διαιρέτη του οποίου το αντίστοιχο ιδεώδες δεν είναι κύριο) - άρα στο παρακάτω θεώρημα δεν μπορούμε να υποθέσουμε κάτι τέτοιο, τουλάχιστον χωρίς βλάβη της γενικότητας†. Εδώ θα δώσουμε μια απόδειξη του θεωρήματος απαλλαγμένη από αυτό το σφάλμα:

Θεώρημα 3.3. *Αν p περιττός, μη ιδιάζων πρώτος, η εξίσωση*

$$\alpha^p + \beta^p + w(1-\zeta)^{pn}\gamma^p = 0 \quad , \quad n \geq 1 \tag{10}$$

όπου $(1-\zeta) \nmid \alpha\beta\gamma$ και $w \in \mathbb{Z}[\zeta]$ αντιστρέψιμο, δεν έχει μη μηδενικές λύσεις $\alpha, \beta, \gamma \in \mathbb{Z}[\zeta]$.

Απόδειξη. Ξεκινάμε όπως πάντα παραγοντοποιώντας τη δοθείσα σχέση ως

$$\prod_{j=0}^{p-1}(\alpha + \zeta^j\beta) = -w(1-\zeta)^{pn}\gamma^p \tag{11}$$

ή περνώντας σε ιδεώδη(φυσικά $\langle -w\rangle = \langle 1\rangle$):

$$\prod_{j=0}^{p-1}\langle \alpha + \zeta^j\beta\rangle = \ell^{pn}\langle\gamma\rangle^p \tag{12}$$

όπου με ℓ συμβολίζουμε το ιδεώδες $\langle 1-\zeta\rangle$.

Σε αυτήν τη σχέση ιδεωδών, τα $\langle \alpha + \zeta^j\beta\rangle$ είναι όλα διαιρετά με το ℓ και είναι όλα διακεκριμένα modulo ℓ^2. Αυτές οι διαπιστώσεις αποδεικνύονται στους δυο ισχυρισμούς που ακολουθούν.

*Ο Kummer αποδεικνύει το Θεώρημα του Fermat για μη ιδιάζοντες πρώτους εκθέτες στο $\mathbb{Z}[\zeta]$, όχι απλώς στο $\mathbb{Z}$.

†Ο Hilbert διόρθωσε αργότερα την απόδειξη του Kummer, ώστε η υπόθεση αυτή να μην είναι απαραίτητη.

Ισχυρισμός 1. *Όλοι οι παράγοντες στο αριστερό μέλος της (12) διαιρούνται με το ℓ.*

Απόδειξη Ισχυρισμού. Ας παρατηρήσουμε πως υπάρχουν ακριβώς p κλάσεις υπολοίπων modulo ℓ. Πράγματι, $N(\ell) = p$ σημαίνει εξ ορισμού*(1.6)* ότι ο βαθμός του $\mathbb{Z}[\zeta]/_{\ell}$ είναι p, όσες και οι κλάσεις υπολοίπων modulo ℓ.

Επειδή τώρα το ℓ είναι πρώτο ιδεώδες, υπάρχει (τουλάχιστον) ένας παράγοντας στα αριστερά της (12) που διαιρείται με αυτό, λόγω της Μοναδικής Παραγοντοποίησης των ιδεωδών.

Θα δείξουμε πως στην πραγματικότητα όλοι οι παράγοντες διαιρούνται με αυτό: Είναι φανερό ότι το $\zeta^j - 1$ διαιρείται με $1-\zeta$. Έτσι, για $j = 1$ έως $p-1$ έχουμε:

$$\begin{aligned} & \zeta^j - 1 \equiv 0 \pmod{1-\zeta} \\ \Longrightarrow\ & \zeta^j \equiv 1 \pmod{1-\zeta} \\ \Longrightarrow\ & \beta\zeta^j \equiv \beta \pmod{1-\zeta} \\ \Longrightarrow\ & \alpha + \beta\zeta^j \equiv \alpha + \beta \pmod{1-\zeta} \end{aligned}$$

Άρα όλοι οι παράγοντες στα αριστερά της (12) είναι ισοϋπόλοιποι modulo $1-\zeta$, κι αφού ξέρουμε ότι μεταξύ αυτών υπάρχει ένας ισοϋπόλοιπος με 0, θα είναι

$$\alpha + \beta\zeta^j \equiv 0 \pmod{1-\zeta} \quad , \quad j = 0, \ldots, p-1$$ ∎

Ισχυρισμός 2. *Κάθε παράγοντας στο αριστερό μέλος της (12) ανήκει σε διαφορετική κλάση modulo ℓ^2.*

Απόδειξη Ισχυρισμού. Ας υποθέσουμε(εις άτοπο) ότι υπάρχουν $\kappa \neq \lambda$, με

$$\alpha + \zeta^\lambda\beta \equiv \alpha + \zeta^\kappa\beta \pmod{\ell^2} \quad , \quad \kappa > \lambda$$

Τότε

$$\begin{aligned} & \zeta^\lambda\beta \equiv \zeta^\kappa\beta \pmod{\ell^2} \\ \Longrightarrow\ & \beta\zeta^\lambda - \beta\zeta^\kappa \equiv 0 \pmod{\ell^2} \\ \Longrightarrow\ & \beta - \beta\zeta^{\kappa-\lambda} \equiv 0 \pmod{\ell^2} \\ \Longrightarrow\ & \beta(1-\zeta^{\kappa-\lambda}) \equiv 0 \pmod{\ell^2} \end{aligned}$$

Επειδή τα $1-\zeta^{\kappa-\lambda}, 1-\zeta$ είναι συντροφικά, το $1-\zeta^{\kappa-\lambda}$ διαιρείται με το $1-\zeta$ ακριβώς μια φορά, κι έτσι πρέπει να είναι $\beta \equiv 0 \pmod{\ell}$, πράγμα που αντιτίθεται στην υπόθεση του θεωρήματος. ∎

Θα αποδείξουμε τώρα επαγωγικά[‡] πως η (10) δεν έχει λύσεις.

• **Βάση της Επαγωγής:** Για $n = 1$ η (10) δεν έχει λύση (α, β, γ) με $\alpha\beta\gamma \neq 0$.

Έστω η εξίσωση (12) για $n = 1$:

$$\prod_{j=0}^{p-1} \langle \alpha + \zeta^j \beta \rangle = \ell^p \langle \gamma \rangle^p$$

Από *Ισχυρισμό 1* είναι $\alpha + \zeta^j \beta \equiv 0 \pmod{\ell}$, και το ℓ εμφανίζεται στην $p^{\text{οστή}}$ δύναμη στο δεξί μέλος, δηλαδή κάθε παράγοντας διαιρεί το ℓ ακριβώς μια φορά:

$$\alpha + \zeta^j \beta \not\equiv 0 \pmod{\ell^2} \qquad j = 0, \ldots, p-1$$

Παρατηρήστε ότι βρήκαμε p διαφορετικά μεταξύ τους(*Ισχυρισμός 2*) μη μηδενικά πολλαπλάσια του $1-\zeta$ modulo ℓ^2, το οποίο είναι αντιφατικό: Πράγματι, υπάρχουν ακριβώς p κλάσεις υπολοίπων modulo ℓ, άρα υπάρχουν ακριβώς p πολλαπλάσια του $1-\zeta$ modulo ℓ^2. Σε αυτά περιέχεται και το μηδενικό· άρα υπάρχουν **μόνο** $p-1$ μη μηδενικά πολλαπλάσια του $1-\zeta$ modulo ℓ^2.

• **Επαγωγικό Βήμα:** Αν δεν υπάρχει λύση της (10) για $n = k-1$ τότε δεν υπάρχει λύση για $n = k$.

Έστω (εις άτοπο) ότι υπάρχει λύση για $n = k,\ k > 1$. Θεωρούμε λοιπόν μια μη μηδενική τριάδα $\alpha, \beta, \gamma \in \mathbb{Z}[\zeta]$ που ικανοποιεί την (10). Θα δουλέψουμε με την αντίστοιχη εξίσωση ιδεωδών:

$$\prod_{j=0}^{p-1} \langle \alpha + \zeta^j \beta \rangle = \ell^{pk} \langle \gamma \rangle^p \tag{13}$$

Ισχυρισμός 3. *Υπάρχουν ιδεώδη* $\mathfrak{a}_0, \mathfrak{a}_1, \ldots, \mathfrak{a}_{p-1}$ *σχετικά πρώτα με το* ℓ *ώστε*

$$\langle \alpha + \zeta^j \beta \rangle \ell^{p(k-1)} = \langle \alpha + \beta \rangle (\mathfrak{a}_j \mathfrak{a}_0^{-1})^p \quad , \quad 1 \leq j \leq p-1 \tag{14}$$

Απόδειξη Ισχυρισμού. Θεωρούμε τον ιδεώδη μέγιστο κοινό διαιρέτη $\mathfrak{m}$ των $\langle \alpha \rangle,\ \langle \beta \rangle$. Από υπόθεση αυτός δε διαιρείται με το $1-\zeta$, αφού τα $\langle \alpha \rangle,\ \langle \beta \rangle$ έχουν αυτήν την ιδιότητα. Επίσης κάθε παράγοντας $\langle \alpha + \zeta^j \beta \rangle$ διαιρείται με τον $\mathfrak{m}$, αφού οι γεννήτορες

[‡] Ο ίδιος ο Fermat ήταν πολύ περήφανος για τη μέθοδο της «άπειρης καθόδου» την οποία επινόησε και χρησιμοποιούσε. Πρόκειται για την επαγωγή προς τα κάτω, και είναι η μέθοδος που χρησιμοποιείται εδώ.

είναι γραμμικοί συνδυασμοί των $\alpha,\ \beta$. Αυτοί οι παράγοντες όμως είναι διαιρετοί και με το ℓ, όπως δείξαμε στον *Ισχυρισμό 1.* Άρα έχουν τη μορφή:

$$\begin{aligned}\langle \alpha+\zeta^j\beta\rangle &= \ell\mathfrak{m}\mathfrak{p}_j \quad ,1\le j\le p-1\\ \langle \alpha+\beta\rangle &= \ell^{p(k-1)+1}\mathfrak{m}\mathfrak{p}_0\end{aligned}$$

για κάποια ιδεώδη $\mathfrak{p}_0,\mathfrak{p}_1,\dots,\mathfrak{p}_{p-1}$, σχετικά πρώτα με το ℓ.

Μια λεπτομέρεια είναι εδώ ο λόγος που ξεχωρίσαμε το $\langle\alpha+\beta\rangle$: Θυμηθείτε πως τα δυνατά υπόλοιπα των $\langle\alpha+\zeta^j\beta\rangle$ modulo ℓ^2 είναι p. Επειδή όμως τα $\langle\alpha+\zeta^j\beta\rangle$ είναι(*Ισχυρισμός 2*) διακεκριμένα modulo ℓ^2 και έχουν πλήθος p, ένα (και μόνο ένα) από αυτά θα είναι ισοϋπόλοιπο με το 0 modulo ℓ^2. Θεωρήσαμε λοιπόν, ότι αυτός ο παράγοντας είναι ο $\langle\alpha+\beta\rangle$. Αυτό δεν βλάπτει τη γενικότητα, διότι αν δεν ήταν αυτός, και ήταν ένας παράγοντας $\langle\alpha+\zeta^{j_0}\beta\rangle$ με $j_0\ge 1$, μπορούμε να αντικαταστήσουμε το β με το $\beta'=\zeta^{j_0}\beta$, και τότε όλοι οι παράγοντες θα ολισθούσαν modulo ℓ^2 και θα ήταν $\alpha+\beta'\equiv 0\pmod{\ell^2}$.

Συνεχίζουμε δείχνοντας πως ο μέγιστος διαιρέτης των $\langle\alpha+\zeta^j\beta\rangle$ είναι ακριβώς ο $\ell\mathfrak{m}$ ή ισοδύναμα, τα $\mathfrak{p}_0,\mathfrak{p}_1,\dots,\mathfrak{p}_{p-1}$ είναι ανά δύο σχετικά πρώτα: Έστω(εις άτοπο) πως υπάρχει ένας(γνήσιος) κοινός διαιρέτης $\mathfrak{p}$ των $\mathfrak{p}_\kappa$ και $\mathfrak{p}_\lambda$ για κάποιους δείκτες $\kappa<\lambda$. Τότε ο $\mathfrak{p}$ θα ήταν διαιρέτης των $\langle\alpha+\zeta^\kappa\beta\rangle$, $\langle\alpha+\zeta^\lambda\beta\rangle$, δηλαδή θα είχαν κοινό διαιρέτη το γινόμενο $\ell\mathfrak{m}\mathfrak{p}$. Από ιδιότητα του ιδεώδους η διαφορά

$$(\alpha+\zeta^\kappa\beta)-(\alpha+\zeta^\lambda\beta)=\beta\zeta^{\lambda-\kappa}\in\ell\mathfrak{m}\mathfrak{p}$$

κι επειδή το $\zeta^{\lambda-\kappa}$ είναι αντιστρέψιμο $\beta\in\ell\mathfrak{m}\mathfrak{p}$ το οποίο αντιτίθεται στην υπόθεση $\beta,\ 1-\zeta$ σχετικά πρώτα.

Η (13) γίνεται:

$$\begin{aligned}&\mathfrak{p}_0\mathfrak{p}_1\cdots\mathfrak{p}_{p-1}\mathfrak{m}^p\ell^{pk}=\ell^{pk}\langle\gamma\rangle^p\\ \Longrightarrow\quad &\mathfrak{p}_0\mathfrak{p}_1\cdots\mathfrak{p}_{p-1}\mathfrak{m}^p=\langle\gamma\rangle^p\end{aligned}$$

Αφού τα $\mathfrak{p}_j$ είναι μεταξύ τους πρώτα, συμπεραίνουμε(όπως στην Πρώτη Περίπτωση - λόγω Μοναδικής Παραγοντοποίησης των ιδεωδών) ότι καθένα από αυτά είναι η $p^{\text{οστή}}$ δύναμη κάποιου άλλου ιδεώδους:

$$\mathfrak{p}_j=\mathfrak{a}_j^p\quad,\quad 0\le j\le p-1$$

και φυσικά τα $\mathfrak{a}_j$ είναι κι αυτά μη διαιρετά με το ℓ. Αντικαθιστώντας:

$$\begin{aligned}\langle\alpha+\zeta^j\beta\rangle &= \ell\mathfrak{m}\mathfrak{a}_j^p\quad,\quad 1\le j\le p-1\\ \langle\alpha+\beta\rangle &= \ell^{p(k-1)+1}\mathfrak{m}\mathfrak{a}_0^p\end{aligned}$$

λύνουμε τη δεύτερη εξίσωση ως προς $\mathfrak{m}=\ell^{p(1-k)-1}\langle\alpha+\beta\rangle\mathfrak{a}_0^{-p}$ και αντικαθιστούμε στην πρώτη:

$$\langle\alpha+\zeta^j\beta\rangle = \ell^{p(1-k)}\langle\alpha+\beta\rangle\mathfrak{a}_0^{-p}\mathfrak{a}_j^p\quad,\quad 1\le j\le p-1$$

πράγμα που επαληθεύει τον ισχυρισμό. ∎

Τα ιδεώδη $(\mathfrak{a}_j\mathfrak{a}_0^{-1})^p$ είναι κύρια, αφού το δεξί μέλος σχέσης (14) είναι κύριο ιδεώδες(σαν γινόμενο τέτοιων). Επειδή ο p είναι μη ιδιάζων, το *Λήμμα (1.15)* μας λέει πως οι βάσεις τους $\mathfrak{a}_j\mathfrak{a}_0^{-1}$ είναι επίσης κύρια ιδεώδη, άρα

$$\mathfrak{a}_j\mathfrak{a}_0^{-1} = \langle \frac{\varepsilon_j}{\delta_j} \rangle \quad , \quad \varepsilon_j, \delta_j \in \mathbb{Z}[\zeta] \quad , \quad j = 1, \ldots, p-1$$

κι επειδή τα $\mathfrak{a}_j$ είναι σχετικά πρώτα με το ℓ, άρα μπορούμε να επιλέξουμε τα ε_j, δ_j μη διαιρετά με το $1-\zeta$. Τελικά περνώντας σε στοιχεία, η (14) γίνεται:

$$(\alpha + \zeta^j\beta)(1-\zeta)^{p(k-1)} \quad = \quad (\alpha+\beta)\left(\frac{\varepsilon_j}{\delta_j}\right)^p u_j \quad , \quad 1 \le j \le p-1 \tag{15}$$

όπου τα u_j είναι αντιστρέψιμα στοιχεία στο $\mathbb{Z}[\zeta]$. Από εδώ μπορούμε να φτάσουμε σε μια σχέση που μοιάζει αρκετά με την (10)(αλλά υπάρχει ακόμη μια ουσιώδης διαφορά - το στοιχείο e):

Ισχυρισμός 4. *Υπάρχουν στοιχεία $a, b, c, e, u \in \mathbb{Z}[\zeta]$, με e, u αντιστρέψιμα και a, b, c σχετικά πρώτα με το $1-\zeta$, που ικανοποιούν τη σχέση:*

$$a^p + eb^p + u\ell^{p(k-1)}c^p = 0 \tag{16}$$

Απόδειξη Ισχυρισμού. Η παρακάτω σχέση είναι προφανές ότι αποτελεί ταυτότητα:

$$(\alpha+\zeta\beta)(1+\zeta) - (\alpha+\zeta^2\beta) - \zeta(\alpha+\beta) = 0$$

Επίσης η (15) δίνει για $j = 1, 2$ τις εξής σχέσεις:

$$(\alpha+\zeta\beta)(1-\zeta)^{p(k-1)} \quad = \quad (\alpha+\beta)\left(\frac{\varepsilon_1}{\delta_1}\right)^p u_1$$
$$(\alpha+\zeta^2\beta)(1-\zeta)^{p(k-1)} \quad = \quad (\alpha+\beta)\left(\frac{\varepsilon_2}{\delta_2}\right)^p u_2$$

τις οποίες αντικαθιστούμε στην προηγούμενη ταυτότητα:

$$\begin{aligned}
& (\alpha+\zeta\beta)(1+\zeta) - (\alpha+\zeta^2\beta) - \zeta(\alpha+\beta) = 0 \\
\Rightarrow\ & \underbrace{(\alpha+\zeta\beta)(1-\zeta)^{p(k-1)}}(1+\zeta) - \underbrace{(\alpha+\zeta^2\beta)(1-\zeta)^{p(k-1)}} - \zeta(\alpha+\beta)(1-\zeta)^{p(k-1)} = 0 \\
\Rightarrow\ & (\alpha+\beta)\left(\frac{\varepsilon_1}{\delta_1}\right)^p u_1(1+\zeta) - (\alpha+\beta)\left(\frac{\varepsilon_2}{\delta_2}\right)^p u_2 - \zeta(\alpha+\beta)(1-\zeta)^{p(k-1)} = 0 \\
\Rightarrow\ & \left(\frac{\varepsilon_1}{\delta_1}\right)^p u_1(1+\zeta) - \left(\frac{\varepsilon_2}{\delta_2}\right)^p u_2 - \zeta(1-\zeta)^{p(k-1)} = 0 \\
\Rightarrow\ & \varepsilon_1^p\delta_2^p u_1(1+\zeta) - \varepsilon_2^p\delta_2^p u_2 - \zeta(1-\zeta)^{p(k-1)}\delta_1^p\delta_2^p = 0 \\
\Rightarrow\ & (\varepsilon_1\delta_2)^p - \frac{u_2}{u_1(1+\zeta)}(\varepsilon_2\delta_2)^p - \frac{\zeta}{u_1(1+\zeta)}(1-\zeta)^{p(k-1)}(\delta_1\delta_2)^p = 0
\end{aligned}$$

Στο σημείο που διαιρέσαμε με $\alpha + \beta$ πρέπει να διευκρινιστεί πως αυτό είναι διαφορετικό από το 0, αφού διαφορετικά η (11) δίνει $\gamma = 0$.

Αν θέσουμε $a = \varepsilon_1\delta_2,\ b = \varepsilon_2\delta_2,\ c = \delta_1\delta_2$ και $e = -\dfrac{u_2}{u_1(1+\zeta)},\ u = -\dfrac{\zeta}{u_1(1+\zeta)}$ διαπιστώνουμε πως τα $a,\ b,\ c \in \mathbb{Z}[\zeta]$ είναι σχετικά πρώτα με το ℓ, αφού έτσι έχουν επιλεγεί τα $\varepsilon_i,\ \delta_i$. Επίσης είναι

$$e = u_2u_1^{-1}(1-\zeta)^{-1} \quad , \quad u = -\zeta u_1^{-1}(1-\zeta)^{-1}$$

άρα είναι αντιστρέψιμα στοιχεία του $\mathbb{Z}[\zeta]$, ως γινόμενο τέτοιων, και το ζητούμενο αποδείχθηκε. ∎

Θα δείξουμε τώρα ότι το στοιχείο e είναι $p^{\text{οστή}}$ δύναμη ενός άλλου στοιχείου του $\mathbb{Z}[\zeta]$, με άλλα λόγια $\eta = \sqrt[p]{e} \in \mathbb{Z}[\zeta]$. Για να εφαρμόσουμε το *Λήμμα του Kummer* πρέπει να ερευνήσουμε το e modulo ℓ^p, για να δούμε αν είναι ισοϋπόλοιπο με κάποιον αλγεβρικό ακέραιο.

Ξέρουμε ότι τα $b,\ (1-\zeta)^p$ είναι σχετικά πρώτα, άρα υπάρχουν $r, \nu \in \mathbb{Z}[\zeta]$ τέτοια ώστε:

$$\begin{aligned} & br + (1-\zeta)^p\nu = 1 \\ \overset{(1-\zeta)^p\nu\equiv 0}{\Longrightarrow} \quad & br \equiv 1 \pmod{\ell^p} \end{aligned} \tag{17}$$

Γράφουμε τη σχέση (16) και λαμβάνουμε modulo ℓ^p:

$$\begin{aligned} & a^p + eb^p + u\ell^{p(k-1)}c^p = 0 \\ \overset{k-1>0}{\Longrightarrow} \quad & a^p + eb^p \equiv 0 \pmod{\ell^p} \\ \Longrightarrow \quad & a^pr^p + eb^pr^p \equiv 0 \pmod{\ell^p} \\ \overset{(17)}{\Longrightarrow} \quad & a^pr^p + e \equiv 0 \pmod{\ell^p} \\ \Longrightarrow \quad & e \equiv (-ar)^p \pmod{\ell^p} \end{aligned} \tag{18}$$

Έτσι για το e ισχύουν οι προϋποθέσεις του το *Λήμματος του Kummer* (2.5), άρα υπάρχει αντιστρέψιμο στοιχείο $\eta \in \mathbb{Z}[\zeta]$ με $e = \eta^p$. Το αντικαθιστούμε στη (16):

$$a^p + (\eta b)^p + u\ell^{p(k-1)}c^p = 0$$

Η τριάδα $(a, \eta b, c)$ είναι λύση της εξίσωσης (10) για $n = k$, πράγμα που αντιτίθεται στην επαγωγική μας υπόθεση, οπότε φθάσαμε σε άτοπο. □

Μόλις αποδείξαμε κάτι πολύ γενικότερο από εκείνο που θέλουμε, όπως θα γίνει φανερό στη σύντομη απόδειξη που ακολουθεί. Το κόλπο είναι να θεωρήσουμε τους συνήθεις ακέραιους της εξίσωσης του Fermat σαν στοιχεία στο $\mathbb{Z}[\zeta]$ και να παραγοντοποιήσουμε κατάλληλα τον πρώτο p που εμφανίζεται σε αυτούς.

Θεώρημα 3.4. *Έστω p περιττός και μη ιδιάζων πρώτος. Η (1) δεν έχει ακέραιες λύσεις, τέτοιες ώστε ακριβώς ένας απ΄τους x, y, z να διαιρείται με τον p.*

Απόδειξη. Έστω(εις άτοπο) πως μια τέτοια λύση υπάρχει. Αφού η εξίσωση

$$x^p + y^p + z^p = 0$$

είναι συμμετρική ως προς x, y, z, θεωρούμε χωρίς βλάβη ότι $p|z$. Άρα $z = p^k z_0$ όπου $k \geq 1$ και z_0 σχετικά πρώτος με τον p.

Σημειώνουμε ότι x, y, z_0 σχετικά πρώτα με τον p σημαίνει πως θα είναι σχετικά πρώτα με το $1-\zeta$, αν τα θεωρήσουμε σαν στοιχεία του $\mathbb{Z}[\zeta]$.

Επίσης, είναι $\langle p \rangle = \langle 1-\zeta \rangle^{p-1}$ (*Λήμμα (1.24)*) άρα υπάρχει αντιστρέψιμο στοιχείο $u \in \mathbb{Q}[\zeta]$ ώστε

$$p = u(1-\zeta)^{p-1}$$

Αντικαθιστώντας

$$z = p^k z_0 = u^k (1-\zeta)^{k(p-1)} z_0$$

και έχουμε

$$x^p + y^p + u^{pk}(1-\zeta)^{pk(p-1)} z_0^p = 0$$

το οποίο είναι άτοπο καθώς πρόκειται για την εξίσωση (10) για $(\alpha, \beta, \gamma) = (x, y, z_0)$, $w = u^{pk}$ και $n = k(p-1) \geq 1$, η οποία αποδείξαμε πως δεν έχει λύσεις στο $\mathbb{Z}[\zeta]$. □

Αυτές οι τρεις περιπτώσεις μας δίνουν την εικόνα για όλους τους μη ιδιάζοντες πρώτους· η εξίσωση έχει θετικές ακέραιες λύσεις αν και μόνο αν $p = 2$. Η περίπτωση ιδιαζόντων πρώτων δεν έχει αντιμετωπιστεί με αυτόν τον τρόπο μέχρι σήμερα.

Α′. Παράρτημα: Η ιστορία του Τ. Θ. του Fermat

Το τελευταίο θεώρημα του Fermat έχει μακρά ιστορία. Για περισσότερο από 3 αιώνες ήταν το πιο διάσημο άλυτο πρόβλημα στα μαθηματικά. Πολλοί κορυφαίοι μαθηματικοί προσπαθούσαν μέσα στο χρόνο να το αποδείξουν αλλά δεν τα κατάφερναν. Το Τελευταίο Θεώρημα του Fermat είχε καταλήξει να συμβολίζει το ανέφικτο. Οι προσπάθειες όμως αυτές αν και αποτυχημένες είχαν ένα πολύ θετικό και ουσιαστικό αποτέλεσμα, την ανάπτυξη καινούριων κλάδων των μαθηματικών.

Είναι σημαντικό να αναφέρουμε ότι η ιστορία του θεωρήματος του Fermat είναι πολύ παλαιότερη και από τον ίδιο τον Fermat. Η προέλευση αυτού του θεωρήματος είναι τόσο παλαιά όσο ο ανθρώπινος πολιτισμός. Έχει τις ρίζες του στο πολιτισμό που αναπτύχθηκε στην Εποχή του Χαλκού στην εύφορη πεδιάδα μεταξύ Τίγρη και Ευφράτη, στην αρχαία Βαβυλωνία. Στην καθημερινή ζωή των Βαβυλωνίων τα τετράγωνα αριθμών εμφανίζονται φυσιολογικά. Οι Βαβυλώνιοι ήθελαν να γνωρίζουν πότε το τετράγωνο ενός ακεραίου ήταν δυνατόν να χωριστεί σε τετράγωνα δυο άλλων ακεραίων. Παραδείγματος χάριν, ένας αγρότης ο οποίος είχε στη κατοχή του ένα αγρόκτημα 25 τ.μ. είναι δυνατόν να το ανταλλάξει με δυο τετράγωνα αγροκτήματα το ένα ίσο με 16 τ.μ. και το άλλο ίσο με 9 τ.μ. Σήμερα γράφουμε $5^2 = 3^2 + 4^2$. Οι τριάδες ακεραίων όπως το 3, 4 και 5 ονομάζονται πυθαγόρειες τριάδες και ήταν γνωστές στους Βαβυλώνιους περισσότερο από χίλια χρόνια πριν από την εποχή του διάσημου Έλληνα μαθηματικού Πυθαγόρα. Όλα αυτά τα στοιχεία είναι γνωστά από μια σπάνια πήλινη πλάκα η οποία χρονολογείται από το 1900 π.Χ.

Pierre De Fermat

Ας παρακολουθήσουμε λίγο την ιστορία αυτού του θεωρήματος που απασχόλησε τόσα χρόνια τη μαθηματική κοινότητα. Ο Pierre De Fermat ήταν Γάλλος νομικός του 17ου αιώνα και συγχρόνως ερασιτέχνης μαθηματικός. Γεννήθηκε τον Αύγουστο του 1601 στην Αυγούστα. Απέκτησε τρεις γιους και δυο κόρες από το γάμο του με την Louse Long. Από τους τρεις γιους του ο Clement Samuel κληρονόμησε το επιστημονικό έργο του πατέρα του και το εξέδωσε μετά το θάνατο του. Χάρη σ' αυτόν γνωρίζουμε σήμερα το διάσημο Τελευταίο Θεώρημα του Fermat καθώς υπήρχε γραμμένο μέσα σε ένα από τα βιβλία του που εξέδωσε ο γιος του και που διασώζεται μέχρι τις μέρες μας. Ο Bell[18] υποστηρίζει ότι ο Fermat, αν και νομικός στο επάγγελμα, ήταν ο πιο παραγωγικός μαθηματικός του 17ου αιώνα, ενός αιώνα που υπήρξε μάρτυρας της εργασίας ορισμένων από τα μεγαλύτερα πνεύματα μαθηματικών όλων των εποχών. Από τα εκπληκτικότερα επιτεύγματα του Fermat ήταν η ανάπτυξη των κύριων ιδεών του απειροστικού λογισμού, δεκατρία χρόνια πριν από τη γέννηση του Isaak Newton. Επίσης, μας παρέδωσε τη θεωρία των αριθμών, όπου πολύ σημαντική είναι η έννοια του πρώτου αριθμού.

Ο Fermat είχε γοητευτεί από τις μαθηματικές εργασίες των αρχαίων Ελλήνων. Οι αντιλήψεις του για τις ιδέες του διαφορικού λογισμού είχαν ενδεχομένως διαμορφωθεί στο πλαίσιο του έργου των κλασσικών αρχαίων Ελλήνων μαθηματικών,

Αρχιμήδη και Ευδόξου, οι οποίοι έζησαν αντίστοιχα τον 3ο και 4ο αιώνα π.Χ. Κάθε στιγμή του ελεύθερου χρόνου του ο Fermat μελετούσε το έργο των αρχαίων Ελλήνων. Το χόμπι του -το πάθος του- ήταν να προσπαθεί να γενικεύει τις εργασίες των αρχαίων και να αποκαλύπτει νέα ομορφιά στις ανακαλύψεις τους που είχαν μείνει θαμμένες για πάρα πολλά χρόνια. *«Έχω ανακαλύψει πλήθος υπερβολικά κομψών θεωρημάτων»* είχε πει κάποτε. Αυτά τα θεωρήματα τα σημείωνε στο περιθώριο των μεταφράσεων των αρχαίων βιβλίων τα οποία κατείχε.

Μια γρήγορη σημείωση

Τον Fermat τον μάγευαν οι αριθμοί. Σ' αυτούς έβρισκε ομορφιά και νόημα και παρουσίασε πλήθος θεωρημάτων στη θεωρία αριθμών. Μεταξύ των αγαπημένων αρχαίων κειμένων, μεταφρασμένων στα λατινικά, που αγαπούσε ο Fermat, ήταν τα *Αριθμητικά*, γραμμένα από τον Έλληνα μαθηματικό Διόφαντο που έζησε το 3ο αιώνα π.Χ. στην Αλεξάνδρεια. Περίπου το 1637, ο Fermat στο περιθώριο αυτού του βιβλίου του, δίπλα από ένα πρόβλημα ανάλυσης του τετραγώνου ενός ακεραίου σε τετράγωνα δυο ακεραίων έγραψε στα λατινικά:

> *«Από την άλλη πλευρά είναι αδύνατο να αναλύσουμε έναν κύβο σε δυο κύβους, μια τέταρτη δύναμη σε δυο τέταρτες δυνάμεις ή γενικά κάθε δύναμη, εκτός από το τετράγωνο, σε δυο δυνάμεις με τον ίδιο εκθέτη. Έχω ανακαλύψει όντως θαυμάσια απόδειξη αυτής της πρότασης, αλλά το περιθώριο δεν είναι αρκετά μεγάλο για να τη χωρέσει.»*

Αυτή η μυστηριώδης διατύπωση είχε ως αποτέλεσμα γενιές μαθηματικών να ασχοληθούν για να ανακαλύψουν *«την όντως θαυμάσια απόδειξη»* την οποία ο Fermat είχε ισχυριστεί ότι διέθετε.

Το «τελευταίο» Θεώρημα

Μέχρι τις αρχές του 18ου αιώνα κάθε άλλο θεώρημα του Fermat είχε αποδειχτεί σωστό ή λανθασμένο. Ωστόσο, τούτη η φαινομενικά απλή πρόταση παρέμεινε αναπόδεικτη. Ακόμα και στο δικό μας αιώνα οι υπολογιστές εγκατέλειψαν την προσπάθεια να αποδείξουν την ισχύ του θεωρήματος. Αν και οι υπολογιστές επαληθεύουν το θεώρημα για μεγάλο πλήθος αριθμών, είναι αδύνατο να το επαληθεύσουν για κάθε αριθμό. Αν και το θεώρημα είναι δυνατό να ελεγχθεί για δισεκατομμύρια αριθμούς απομένουν ωστόσο άπειροι αριθμοί και άπειροι εκθέτες. Το θεώρημα έπρεπε να αποδειχτεί μαθηματικά. Μάλιστα, τη δεκαετία του 1800 η Γαλλική και η Γερμανική Ακαδημία Επιστημών πρόσφεραν βραβείο σε οποιονδήποτε θα αποδείκνυε το θεώρημα. Κάθε χρόνο λοιπόν χιλιάδες μαθηματικοί και μανιώδεις ερασιτέχνες έστελναν αποδείξεις σε περιοδικά μαθηματικών και σε επιτροπές κρίσης. Όμως τελικά έμεναν με άδεια χέρια.

Ο ίδιος ο Fermat είχε κατορθώσει να αποδείξει το Τελευταίο Θεώρημα του για $n = 4$. Αντιλήφθηκε, επίσης, ότι αν για ορισμένη δύναμη του n υπάρχει λύση, τότε υπάρχει λύση και για κάθε πολλαπλάσιο του n. Αρκεί λοιπόν να θεωρήσουμε ως εκθέτη μόνο πρώτους αριθμούς (εκτός από τον 2). Ο Leonard Euler(1707-1783) απέδειξε ανεξάρτητα από το Fermat τις περιπτώσεις $n = 3$ και $n = 4$. Το 1828 ο Peter G. L. Dirichlet (1805- 1859) κατόρθωσε να αποδείξει τη περίπτωση $n = 5$.

Το 1830 ο Adrien -Marie Legendre(1752-1833) απέδειξε την ίδια περίπτωση. Ο Gabriel Lame(1795-1870) και ο Henri Lebesque(1875-1941) που τον διόρθωσε το 1840, μπόρεσαν να αποδείξουν την περίπτωση $n = 7$. Διακόσια χρόνια μετά τη διάσημη σημείωση του Fermat στο περιθώριο είχε αποδειχθεί απλώς για τους εκθέτες 3, 4, 5, 6 και 7. Έως το άπειρο ο δρόμος ήταν μακρύς. Όλοι οι μαθηματικοί αναζητούσαν την άπιαστη γενική απόδειξη, κατέληγαν ωστόσο σε αποδείξεις μόνο για ειδικές τιμές του εκθέτη.

Euler - Gauss

Η συνεισφορά των Euler, Gauss(1777-1855) στη μετέπειτα απόδειξη του Τελευταίου Θεωρήματος του Fermat ήταν πολύ σημαντική. Η πρωτοπόρα εργασία του Euler στη Μιγαδική Ανάλυση, κυρίως όμως στο πεδίο της Τοπολογίας αποδείχτηκε απαραίτητη στην κατανόηση και στην προσπάθεια επίλυσης του μυστηρίου του Fermat. Τα αποτελέσματα του Gauss στη Θεωρία Αριθμών είχαν μεγάλη σημασία σε κάθε προσπάθεια των μαθηματικών να αποδείξουν το τελευταίο θεώρημα του Fermat. Ωστόσο, ο ίδιος δεν προσπάθησε να το αποδείξει, παρόλο που η ακαδημία του Παρισιού προσέφερε μεγάλο βραβείο, όπως τον πληροφόρησε ο φίλος του H. W. M. Olbers. Ίσως, ήταν ο μόνος μαθηματικός της Ευρώπης που αντιλήφθηκε πόσο δύσκολη ήταν η απόδειξη. Ο ίδιος έγραψε στον Olbers την άποψη του για το Τελευταίο Θεώρημα του Fermat:

> *«Σου είμαι πολύ υποχρεωμένος για την είδηση που αφορά το βραβείο του Παρισιού. Ομολογώ ωστόσο, ότι επειδή το θεώρημα του Fermat είναι μια απομονωμένη πρόταση με ενδιαφέρει ελάχιστα: μπορώ εύκολα να παραθέσω πλήθος παρόμοιων προτάσεων τις οποίες δεν μπορούμε να τις αποδείξουμε, ούτε να τις ξεφορτωθούμε.»*

Sophie Germain

Η Sophie Germain(1776-1831), ήταν από τους σημαντικότερους μαθηματικούς που προσπάθησαν να αποδείξουν το τελευταίο θεώρημα του Fermat και συνέλαβε σημαντικά στη πρόοδο επίλυσης του. Διατύπωσε τη πρόταση ότι αν υπάρχει λύση της εξίσωσης του Fermat για $n = 5$ τότε καθένας από τους τρεις αριθμούς πρέπει να διαιρείται με το 5. Με βάση αυτό στο Τελευταίο Θεώρημα του Fermat διακρίνουμε δυο κατηγορίες αριθμών: τους μη διαιρετούς με το 5, τους υπόλοιπους αριθμούς. Το θεώρημα γενικεύτηκε ώστε να περιλάβει και άλλες δυνάμεις. Η Sophie Germain διατύπωσε ένα γενικό θεώρημα που επέτρεπε να αποδείξουμε το Τελευταίο Θεώρημα του Fermat για κάθε πρώτο αριθμό n μικρότερο από 100.

Fourier

Ένας άλλος μεγάλος μαθηματικός που με τις μελέτες του συνέβαλε κι αυτός στην απόδειξη του Τελευταίου Θεωρήματος του Fermat είναι ο Fourier (1768-1830). Ο Fourier ανέπτυξε μια πολύ σημαντική θεωρία στις περιοδικές συναρτήσεις. Είναι δυνατόν να προσδιορίσουμε τις περισσότερες συναρτήσεις σε οσοδήποτε βαθμό ακρίβειας επιθυμούμε ως άθροισμα πολλών (θεωρητικά άπειρων όταν επιθυμούμε απόλυτη ακρίβεια) ημιτονοειδών και συνημιτονοειδών συναρτήσεων. Η εφαρμογή των σειρών Fourier σε φυσικά φαινόμενα και σε μεθόδους που χρησιμοποιούν οι υπολογιστές είναι πολύ μεγάλη. Επιπλέον όμως οι συγκεκριμένες

σειρές εφαρμόζονται σε αμιγώς μαθηματικά θέματα, ένα πεδίο που δεν κέντριζε το ενδιαφέρον του Fourier. Τον 20ο αιώνα οι σειρές Fourier έπαιξαν ρόλο στη Θεωρία Αριθμών σαν εργαλείο για το μετασχηματισμό μαθηματικών στοιχείων από μια περιοχή σε άλλη στο πλαίσιο της εργασίας του Goro Shimura. Τώρα γνωρίζουμε ότι η απόδειξη της εικασίας του Shimura βρίσκεται σε κομβικό σημείο στο πλαίσιο της απόδειξης του Τελευταίου Θεωρήματος του Fermat. Η επέκταση των περιοδικών συναρτήσεων του Fourier στο μιγαδικό επίπεδο οδήγησε στην ανακάλυψη των αυτόμορφων συναρτήσεων και των μορφών modular. Το επίτευγμα αυτό είχε σημαντική επίδραση στο τελευταίο θεώρημα του Fermat μέσω της εργασίας ενός άλλου Γάλλου μαθηματικού του Henri Poincare.

Gabriel Lamé

Απόπειρα να αποδείξει το Τελευταίο Θεώρημα του Fermat έκανε και ο Gabriel Lamé. Η απόδειξη του στηριζόταν σε μια μέθοδο που είχε προτείνει ο Liouville και αφορούσε την παραγοντοποίηση του Fermat με γραμμικούς παράγοντες χρησιμοποιώντας μιγαδικούς αριθμούς. Ο ίδιος ο Liouville ωστόσο, υπέδειξε το λάθος στην απόδειξη του Lamé λέγοντας πως η παραγοντοποίηση που είχε προτείνει δεν ήταν μοναδική.

Ernst Eduard Kummer

Ο Ernst Eduard Kummer(1810-1893) είναι ο άνθρωπος που περισσότερο από κάθε σύγχρονό του έφθασε πλησιέστερα σε μια γενική λύση του προβλήματος του Fermat. Ο Kummer επινόησε όντως μια πλήρη μαθηματική θεωρία, τη θεωρία των *ιδεωδών αριθμών* προσπαθώντας να αποδείξει το Τελευταίο Θεώρημα Του Fermat. Η εργασία του Kummer με τους ιδεώδεις αριθμούς του επέτρεψε όπως είδαμε να αποδείξει το Τελευταίο Θεώρημα του Fermat για ένα μεγάλο αριθμό πρώτων εκθετών - κατά πάσα πιθανότητα άπειρο - καθώς και για τα άπειρα πολλαπλάσια των πρώτων αυτής της κατηγορίας. Το γεγονός ότι αυτή η σημαντική θεωρία είναι αποτέλεσμα έμπνευσης στο πλαίσιο της προσπάθειας επίλυσης του Τελευταίου Θεωρήματος του Fermat δείχνει πως είναι δυνατόν να αναπτύξουμε νέες θεωρίες προσπαθώντας να λύσουμε ειδικά προβλήματα.

Galois

Ακολουθεί η συνεισφορά του μεγάλου και ιδιοφυή μαθηματικού Galois(1811-1832) -αν και ήταν μόλις 20 χρόνων- στην προσπάθεια επίλυσης του Τελευταίου Θεωρήματος του Fermat καθώς η θεωρία του αποτελεί το κρίσιμο βήμα στη μέθοδο που ακολουθήθηκε μετά από ενάμιση αιώνα.

Abel

Ένας ακόμη μαθηματικός που συνέλαβε με το έργο του στη προσέγγιση του Τελευταίου Θεωρήματος του Fermat είναι ο Abel(1802-1829). Η έννοια τη αβελιανής ομάδας αποτελεί κρίσιμο στοιχείο στη σύγχρονη διαπραγμάτευση του προβλήματος αυτού.

Dedekind

Έπεται η εξίσου σημαντική συνεισφορά του Dedekind (1831-1916) στη σύγχρονη προσέγγιση του Τελευταίου Θεωρήματος του Fermat. Αυτή είναι η ανάπτυξη της *θεωρίας των ιδεωδών*, οι οποίοι ήταν γενίκευση των ιδεωδών αριθμών του Kummer. Έναν αιώνα μετά την ανάπτυξη του Dedekind οι ιδεώδεις θα ενέπνεαν τον Barry Mazur. Κατόπιν ο Andrew Wiles θα εκμεταλλευόταν την εργασία του Mazur.

Henri Poincare

Ένας άλλος μαθηματικός με εξαιρετικές ικανότητες είναι ο Henri Poincare(1854-1912). Η συμβολή του στην Τοπολογία, κλάδος που αναπτύχθηκε από τον Euler, ήταν πολύ σημαντική. Η μελέτη των μορφών, των επιφανειών και των συνεχών συναρτήσεων, όπως και οι μορφές Modular, τομέας στον οποίο ο Poincare υπήρξε πρωτοπόρος, έπαιξαν πολύ σημαντικό ρόλο στη σύγχρονη προσέγγιση του Τελευταίου Θεωρήματος του Fermat.

Mordell

Ο Mordell (1888-1972) στη συνέχεια ανακάλυψε μια σχέση μεταξύ των λύσεων αλγεβρικών εξισώσεων και της Τοπολογίας, που του φάνηκε πολύ παράξενη. Είναι μια σχέση μεταξύ του αριθμού των οπών σε μια επιφάνεια (δηλαδή του γένους της επιφάνειας) στο χώρο λύσεων μιας εξίσωσης και του ερωτήματος αν η εξίσωση έχει πεπερασμένο ή άπειρο πλήθος λύσεων. Έτσι, αν η επιφάνεια των λύσεων έχει γένος ανώτερο από δυο τότε η εξίσωση έχει πεπερασμένο πλήθος ακέραιων λύσεων. Ο ίδιος τελικά δεν κατάφερε να την αποδείξει, γι' αυτό έμεινε γνωστή ως εικασία του Mordell.

Gerd Faltings

Ο Gerd Faltings κατόρθωσε το 1983 να αποδείξει την εικασία του Mordell. Προέκυπτε επομένως το συμπέρασμα ότι επειδή το γένος της εξίσωσης του Fermat για n μεγαλύτερο από 3 είναι 2 ή περισσότερο, οι ακέραιες λύσεις της εξίσωσης, αν υπάρχουν, είναι πεπερασμένες.

Granville & Heath Brown

Οι Granville και Heath Brown χρησιμοποιώντας το αποτέλεσμα του Faltings απέδειξαν ότι το πλήθος των λύσεων της εξίσωσης του Fermat, αν υπάρχουν, ελαττώνεται εκθετικά με την αύξηση του n. Αποδείχτηκε ότι καθώς το n αυξάνεται το ποσοστό των εκθετών για τους οποίους το Τελευταίο Θεώρημα του Fermat μπορεί να αληθεύει προσεγγίζει το 1%.

Άρα, το 1983 η κατάσταση με το Τελευταίο Θεώρημα του Fermat έχει ως εξής: Έχει αποδειχθεί για κάθε n έως το 1.000.000 και επιπλέον, για μεγαλύτερα n αν υπάρχουν λύσεις τότε είναι ελάχιστες και ελαττώνονται με την αύξηση του n.

Η εικασία Shimura-Taniyama

Οι Yuataka Taniyama(1927-1958) και Goro Shimura, Ιάπωνες μαθηματικοί και φίλοι οργάνωσαν το Σεπτέμβριο του 1955 ένα συνέδριο στο Τόκιο. Ένας από τους προσκληθέντες ήταν ο Andre Weil. Μια εικασία διατυπώνεται δειλά από τον Taniyama, αλλά συνδέεται με το όνομα του Weil: «Μήπως οι αυτόμορφες συναρτήσεις συνδέονται με τις ελλειπτικές καμπύλες και όχι μόνο οι συναρτήσεις modular;» Ο Shimura μια δεκαετία αργότερα και αφού ο Taniyama έχει πεθάνει, αντιλαμβάνεται το λάθος του φίλου του και οδηγείται στη διατύπωση μιας πιο θαρραλέας εικασίας: «*κάθε ελλειπτική καμπύλη στους ρητούς ομογενοποιείται από μορφή modular*». Στις αρχές της δεκαετίας του '60 ο Shimura συναντά τον Serre ο οποίος τον αμφισβητεί και ισχυρίζεται ότι υπάρχουν ελλειπτικές καμπύλες στις οποίες αυτό δεν ισχύει. Τότε ο Shimura απαντά διατυπώνοντας με ακρίβεια την εικασία του: *Μια τέτοια καμπύλη πάντα ομογενοποιείται από μια καμπύλη modular*.

Η εικασία του Fray

Είμαστε στο 1984. Ένας άλλος μαθηματικός, ο Gerhard Frey βοηθά με το έργο του στο να φθάσουμε σιγά, σιγά στη λύση του περίφημου προβλήματος. Έχει μελετήσει τις εργασίες των Hasse, Weil, Mazur και έχει επηρεαστεί από αυτές. Προέ-

βαλε έναν ισχυρισμό ο οποίος φαινόταν προκλητικός:

> *«Αν η εικασία Shimura- Taniyama είναι όντως σωστή, το τελευταίο θεώρημα του Fermat αληθεύει.»*

Η πορεία της σκέψης του Frey ήταν ιδιοφυής. Αν υποθέσουμε ότι το Τελευταίο Θεώρημα του Fermat δεν ισχύει τότε για κάποια δύναμη n μεγαλύτερη του 2 υπάρχει λύση στην εξίσωση του Fermat: $x^n + y^n = z^n$ η όπου x, y, και z ακέραιοι. Από τις συγκεκριμένες εξισώσεις προκύπτει μια ιδιαίτερη ελλειπτική καμπύλη, της οποίας ο Frey προσδιόρισε την εξίσωση, η οποία ονομάζεται καμπύλη Frey και η οποία είναι μη modular. Όμως αν η εικασία των Shimura- Taniyama αληθεύει τότε κάθε ελλειπτική καμπύλη είναι modular. Άρα, μια τέτοια καμπύλη δεν μπορεί να υπάρχει.

Ο Ken Ribet ήταν αυτός που τελικά κατάφερε να αποδείξει την εικασία του Frey, μια εικασία που στην αρχή θεωρούσε ως «αστεία». Ο δρόμος για τη λύση του προβλήματος του Fermat με τις σύγχρονες μεθόδους της Αριθμητικής Αλγεβρικής Γεωμετρίας ήταν πλέον ανοιχτός. Απέμενε μόνο να βρεθεί αυτός που θα αποδείκνυε την εικασία Shimura- Taniyama. Τότε το Τελευταίο Θεώρημα του Fermat θα ίσχυε αυτομάτως.

Andrew Wiles

Ο Andrew Wiles είχε ως παιδικό όνειρο να αποδείξει το Τελευταίο Θεώρημα του Fermat. Ήταν μόλις 10 ετών όταν διάβασε για το πρόβλημα αυτό. Ωστόσο, για πολλά χρόνια το παραμέλησε μιας και το πρόβλημα αυτό δεν ήταν πλέον στη μόδα. Η αφορμή να ασχοληθεί ξανά με το Τελευταίο Θεώρημα του Fermat δόθηκε όταν πληροφορήθηκε από ένα φίλο του ότι ο Ken Ribet απέδειξε την εικασία του Frey. Ο Wiles ηλεκτρίστηκε. Εκείνη τη στιγμή αντιλήφθηκε ότι η ζωή του άλλαξε. Κλειδώθηκε στη σοφίτα του και άρχισε να εργάζεται.

Το μεγαλείο του Wiles έλεγε αργότερα ο Frey ήταν ότι πίστευε σε ότι έκανε, όταν ουδείς μαθηματικός στην υφήλιο πίστευε όντως ότι μέχρι το τέλος του 20ου αιώνα θα αποδεικνυόταν η εικασία Shimura- Taniyama. Εργάστηκε μυστικά και σκληρά για 7 χρόνια απομονωμένος από το κόσμο. Στη διάρκεια της επίπονης αυτής προσπάθειας του, ζήτησε τη βοήθεια μόνο δυο πολύ έμπιστων και εχέμυθων φίλων του, των Katz και Peter Sarnak, ώστε να επιβεβαιώνουν τα αποτελέσματα του βήμα προς βήμα.

Τρεις διαλέξεις

Στο τέλος του Ιουνίου του 1993 ο Andrew Wiles ταξίδευσε αεροπορικώς για την Αγγλία. Επέστρεφε στο πανεπιστήμιο του Cambridge όπου είκοσι χρόνια πριν υπήρξε φοιτητής. Ο καθηγητής John Coates, ο οποίος είχε επιβλέψει την εκπόνηση της διδακτορικής του διατριβής, οργάνωνε ένα συνέδριο με αντικείμενο τη Θεωρία Iwasawa, θέμα πάνω στο οποίο είχε εκπονήσει τη διατριβή του και διέθετε αρκετές γνώσεις. Του ζήτησε λοιπόν, να δώσει μια σύντομη ωριαία ομιλία σε θέμα της αρεσκείας του. Ο Andrew Wiles προς έκπληξη των άλλων που συμμετείχαν στο συνέδριο, λόγω της κλειστότητας του χαρακτήρα του, δέχτηκε. Ζήτησε όμως η

ομιλία του να είναι τρίωρη. Είχε έρθει η ώρα να πραγματοποιήσει το παιδικό του όνειρο.

Κανείς δεν γνώριζε το περιεχόμενο της ομιλίας του, ούτε και το σκοπό αυτής. Την πρώτη μέρα της ομιλίας του ο Andrew Wiles αντάμειψε τους περίπου είκοσι μαθηματικούς που είχαν έρθει στη διάλεξη του με ένα ισχυρό και απροσδόκητο αποτέλεσμα. Η αγωνία αυξανόταν. Υπήρχαν ακόμα άλλες δυο διαλέξεις. Τη δεύτερη μέρα η ένταση της παρουσίασης αυξήθηκε. Ο Andrew Wiles παρουσίασε πρωτότυπες ιδέες με τη μορφή νέων θεωρημάτων μαζί με τις αποδείξεις τους.

Την επόμενη μέρα, Τετάρτη 23 Ιουνίου 1993 ήταν η τελευταία διάλεξή του. Η αίθουσα είχε ξεχειλίσει. Ο Andrew Wiles άρχισε και πάλι να γράφει φαινομενικά ατέλειωτους τύπους και θεωρήματα πάνω στο πίνακα. *«Υπήρχε μόνο μια ενδεχόμενη αποκορύφωση, μόνο μια ενδεχόμενη κατάληξη της παρουσίασης του Wiles»* είπε αργότερα ο καθηγητής Ken Ribet. Ο Andrew Wiles τέλειωνε τις τελευταίες γραμμές της απόδειξης μιας αινιγματικής και πολύπλοκης μαθηματικής εικασίας, της εικασίας των Shimura-Taniyama. Τότε, ξαφνικά πρόσθεσε μια τελευταία γραμμή, επαναδιατυπώνοντας μια εξίσωση ηλικίας αιώνων. Πριν από επτά χρόνια ο Ken Ribet είχε αποδείξει ότι τούτη η εξίσωση αντιφάσκει με την εικασία των Shimura-Taniyama.

«Κι αυτό αποδεικνύει το Τελευταίο Θεώρημα του Fermat.»

είπε σχεδόν αδιάφορα.

«Νομίζω λοιπόν ότι σε τούτο το σημείο πρέπει να σταματήσω.»

Σε λίγα λεπτά σε όλο τον κόσμο το ηλεκτρονικό ταχυδρομείο άρχισε να αστράφτει και μηνύματα να ξετυλίγονται μέσα από μηχανές fax. Φαινόταν ότι το μυστήριο ηλικίας 350 ετών, το πιο διάσημο μαθηματικό πρόβλημα όλων των εποχών, είχε λυθεί. Οι εφημερίδες περιέγραφαν τον άνθρωπο που κατά τα φαινόμενα είχε λύσει το μαθηματικό πρόβλημα που είχε αντισταθεί περισσότερο από κάθε άλλο και η λύση του παρέμενε πρόκληση για περισσότερο από 350 χρόνια. Σε μια νύχτα το *Andrew Wiles*, το όνομα ενός ήσυχου και απομονωμένου ανθρώπου, μπήκε σε κάθε σπίτι.

Η απόδειξη του Andrew Wiles περιείχε έννοιες και θεωρίες οι οποίες την εποχή του Fermat ήταν άγνωστες, ακόμα και μέχρι τον $20^ο$ αιώνα. Ήταν επομένως απαραίτητο να επικυρωθούν από ειδικούς ανεξάρτητα του Andrew Wiles. Η απόδειξη στάλθηκε σε κορυφαίους μαθηματικούς. Η αισιοδοξία ωστόσο διάρκεσε λίγο· στη λογική της απόδειξης ανακαλύφτηκε ένα κενό. Ο Andrew Wiles προσπάθησε να το μπαλώσει αλλά μάταια· αυτό παρέμενε. Ο Wiles αποσύρθηκε στη σοφίτα του.

Η τελική λύση

Ωστόσο, το πρωινό της Δευτέρας της 19ης Σεπτεμβρίου του 1994 ήρθε η ώρα για να δοθεί επιτέλους η λύση του περίφημου αυτού προβλήματος. Τη λύση την έδωσε ο ίδιος ο Andrew Wiles. Η νέα απόδειξη ήταν διόρθωση αυτής που είχε παρουσιάσει τον Ιούνιο του 1993 στο πανεπιστήμιο του Cambridge, και που προς μεγάλη απογοήτευση του ίδιου ήταν λανθασμένη. Ευτυχώς, ένα χρόνο μετά την κατάρρευση της πρώτης του απόδειξης, και σε μια τελευταία απόπειρα πριν εγκαταλείψει κάθε προσπάθεια βρήκε το λάθος. Είχε βρει την σωστή απόδειξη.

> *«Ήταν η σημαντικότερη στιγμή σε ολόκληρη την επαγγελματική ζωή μου. Ξαφνικά, απολύτως αναπάντεχα ήρθε η απίστευτη ανακάλυψη... Ήταν τόσο απερίγραπτα όμορφη, ήταν τόσο απλή και συνάμα μεγαλόπρεπη. Την πρώτη νύχτα πήγα σπίτι και κοιμήθηκα με τις σκέψεις αυτής της ανακάλυψης. Και το επόμενο πρωί την ξαναέλεγα και την βρήκα εντάξει. Ήταν κάτι που ήθελα να το ανακοινώσω στη γυναίκα μου με μεγάλη ικανοποίηση. Το βρήκα! Βρήκα τη διόρθωση στην απόδειξή μου!»*

Ήταν αλήθεια και όχι όνειρο. Η εικασία του Fermat είχε επιτέλους μετατραπεί σε Θεώρημα! Ο ίδιος ο Andrew Wiles χαρακτήρισε την απόδειξη του ως απόδειξη του 20ου αιώνα καθώς χρησιμοποίησε την εργασία πολλών μαθηματικών του 20ου αιώνα. Σύμφωνα λοιπόν με τον ίδιο ήταν αδύνατο να έχει υπόψη του τούτη την απόδειξη ο Fermat όταν έγραφε στο περιθώριο της σελίδας τη διάσημη σημείωση του. Μήπως ο Fermat διέθετε άλλη απόδειξη; Η απάντηση είναι πιθανόν όχι. Δεν είμαστε όμως απόλυτα βέβαιοι και ίσως δεν το μάθουμε ποτέ.

Η βαθύτερη αξία του θεωρήματος δεν είναι απλώς ότι το θεώρημα σχετίζεται με όλη την πορεία του ανθρώπινου πολιτισμού, αλλά το ότι η τελική λύση του προβλήματος προέκυψε ανακαλύπτοντας πολύ χρήσιμα μαθηματικά και ενοποιώντας όλο το εύρος αυτών των μαθηματικών. Πρέπει να τονίσουμε ότι η επιχείρηση απόδειξης του θεωρήματος ήταν έργο πολλών ανθρώπων· ενδεικτικά θυμίζουμε τους *Ernst Kummer, Barry Mazur, Frey, Ribet, Shimura* και Taniyama. Κλείνουμε την αναφορά στην ιστορία του Τελευταίου Θεωρήματος του Fermat με κάποια λόγια του Andrew Wiles που περιγράφουν την επτάχρονη αναζήτηση του Ιερού Δισκοπότηρου των μαθηματικών:

> *«Ίσως, ο καλύτερος τρόπος για να περιγράψω την εμπειρία μου στα μαθηματικά είναι να την παρομοιάσω με την εμπειρία του να εισέρχεσαι σε ένα σκοτεινό μέγαρο. Εισέρχεσαι στο πρώτο σκοτεινό, απολύτως σκοτεινό δωμάτιο. Σκοντάφτεις δεξιά-αριστερά και πέφτεις επάνω στα έπιπλα. Σιγά, σιγά μαθαίνεις που βρίσκεται κάθε έπιπλο. Και τελικά μετά από περίπου έξι μήνες βρίσκεις το διακόπτη και ανάβεις το φως. Ξαφνικά λοιπόν, τα πάντα φωτίζονται και βλέπεις που βρισκόσουν. Κατόπιν εισέρχεσαι στο επόμενο σκοτεινό δωμάτιο...»*

Β′. Παράρτημα: Πέρα από το Τελευταίο Θεώρημα

Όσον αφορά τα Μέσα Μαζικής Ενημέρωσης και το ευρύ μη-μαθηματικό κοινό, η απόδειξη του A. Wiles είναι το τέλος της ιστορίας του Θεωρήματος του Fermat. Όμως αυτό είναι λανθασμένο για πολλούς λόγους.

Πρώτα απ΄ όλα αυτό που απέδειξε ο Wiles δεν είναι απλώς το Θεώρημα του Fermat. Είναι ένα πολύ ισχυρότερο αποτέλεσμα, από το οποίο έπεται το Θεώρημα του Fermat σαν Πόρισμα. Τα αποτελέσματα του Wiles είναι πολύ πιο χρήσιμα στα μαθηματικά απ΄ όσο είναι το ίδιο το Θεώρημα του Fermat(η ιστορία επαναλαμβάνεται!). Παραδείγματος χάριν, σηματοδοτεί την αρχή για τη λύση του Προγράμματος Langlands[28], ενός από τα κεντρικά ζητήματα στην σύγχρονη Θεωρία Αριθμών το οποίο μελετάει τη σχέση μεταξύ των συμμετριών στη Θεωρία Αριθμών και στη Γεωμετρία. Αν αυτό πετύχει, θα μας οδηγήσει σε μια ενοποιημένη θεωρία των Συναρτήσεων Ζήτα[29], οι οποίες είναι μαθηματικά αντικείμενα που εμφανίζονται σε πολλούς τομείς των Μαθηματικών και της Φυσικής. Επίσης, το Θεώρημα των Wiles-Taylor μπορεί να δώσει τεράστια ώθηση στη Διοφαντική Ανάλυση, οδηγώντας σε μια γενική θεωρία των Διοφαντικών Εξισώσεων με τρεις μεταβλητές*.

Η απόδειξη του Wiles γέννησε νέα προβλήματα κι έδωσε κατευθύνσεις για την αντιμετώπιση άλλων γρίφων, αρκετά γενικότερων από το Τελευταίο Θεώρημα του Fermat. Παρακάτω παρουσιάζονται σε απλή γλώσσα τρία ανοικτά προβλήματα, τα οποία επιζητούν λύση. Η απόδειξη οποιασδήποτε από τις παρακάτω εικασίες, ισοδυναμεί με μια απόδειξη του Τελευταίου Θεωρήματος του Fermat, το οποίο έπεται σαν πόρισμα!

i. Η εικασία του Beal

Ας επιτρέψουμε στους εκθέτες της εξίσωσης του Fermat να διαφέρουν:

$$x^n + y^m = z^k \quad , \quad xyz \neq 0$$

κι ας αναζητήσουμε ακέραιες λύσεις αυτής(εκτός των πυθαγόρειων τριάδων). Μια τέτοια είναι η $17^4 + 34^4 = 17^5$. Αν απαιτήσουμε οι βάσεις να είναι σχετικά πρώτοι αριθμοί, οι λύσεις είναι πιο σπάνιες. Θα δούμε μάλιστα, πως μόνο 10 λύσεις είναι γνωστές, και σε όλες εμφανίζεται ο εκθέτης 2. Υπάρχουν άραγε λύσεις χωρίς αυτόν τον εκθέτη;

Εικασία 1. *(***Beal***) Η εξίσωση* $x^n + y^m = z^k$, $xyz \neq 0$ *δεν έχει θετικές ακέραιες λύσεις, με* x, y, z *σχετικά πρώτους ανά δυο και* $n, m, k > 2$.

*Μια γενική και πλήρης θεωρία επίλυσης Διοφαντικών Εξισώσεων δεν υπάρχει, καθώς η απάντηση στο 10^o πρόβλημα του Hilbert[23], το οποίο θέτει αυτήν ακριβώς την ερώτηση, είναι αρνητική(Yu. V. Matiyasevich,1970)! Έτσι μια τέτοια θεωρία για τρεις μεταβλητές θα ήταν σπουδαίο επιτευγμα.

Παραδείγματος χάριν, η $3^3 + 6^3 = 3^5$ έχει βάσεις με κοινό παράγοντα το 3, ενώ η $7^6 + 7^7 = 98^3$ έχει βάσεις με κοινό παράγοντα το 7. Η εικασία δεν έχει αποδειχθεί σωστή ή λάθος. Ο εμπνευστής της (τραπεζικός)Beal, προσφέρει δεκάδες χιλιάδες δολάρια για την απόδειξη ή την διάψευση της.

Οι Darmon και Granville απέδειξαν το εξής [30]:

> Αν $n, m, k > 0$ και $\frac{1}{n} + \frac{1}{m} + \frac{1}{k} < 1$ τότε η εξίσωση του Beal έχει πεπερασμένο πλήθος λύσεων με βάσεις σχετικά πρώτους αριθμούς.

Η εικασία του Beal επιβάλλει $n, m, k > 2$, άρα η σχέση $\frac{1}{n} + \frac{1}{m} + \frac{1}{k} \geq 1$ ικανοποιείται μόνο για $n = m = k = 3$, για τους οποίους εκθέτες όμως δείξαμε στον *Ισχυρισμό 4* της **(III.ii)** πως δεν υπάρχουν ακέραιες λύσεις. Άρα τελικά η διοφαντική εξίσωση $x^n + y^m = z^k$, $n, m, k > 2$ έχει πάντα πεπερασμένο πλήθος λύσεων.

Στο [30] αναλύονται επίσης οι περιπτώσεις

- $n, m, k \geq 2$ και τουλάχιστον ένας εκθέτης να είναι μεγαλύτερος του 2, με x, y, z σχετικά πρώτους και $\frac{1}{n} + \frac{1}{m} + \frac{1}{k} > 1$.
- x, y, z σχετικά πρώτοι και $\frac{1}{n} + \frac{1}{m} + \frac{1}{k} < 1$

Ειδικότερα έχει διατυπωθεί η

Εικασία 2. *(***Fermat-Catalan***) Υπάρχουν πεπερασμένες το πλήθος τριάδες σχετικά πρώτων ανά δυο ακέραιων x, y, z, ώστε να ισχύει $x^n + y^m = z^k$, $xyz \neq 0$, με $n, m, k \in \mathbb{N}$ και $\frac{1}{n} + \frac{1}{m} + \frac{1}{k} < 1$.*

Συγκεκριμένα μόνο 10 τέτοιες λύσεις είναι γνωστές:

$$\begin{aligned}
1 + 2^3 &= 3^2 \\
2^5 + 7^2 &= 3^4 \\
7^3 + 13^2 &= 2^9 \\
2^7 + 17^3 &= 71^2 \\
3^5 + 11^4 &= 122^2 \\
17^7 + 76271^3 &= 21063928^2 \\
1414^3 + 2213459^2 &= 65^7 \\
9262^3 + 15312283^2 &= 113^7 \\
43^8 + 96222^3 &= 30042907^2 \\
33^8 + 1549034^2 &= 15613^3
\end{aligned}$$

Στις 5 πρώτες από αυτές συναντάμε λύσεις με διψήφιους ή τριψήφιους αριθμούς, ενώ στις υπόλοιπες οι λύσεις είναι ακέραιοι πολύ μεγαλύτερης τάξης[†]. Επίσης παρατηρήστε πως σε όλες εμφανίζεται ο εκθέτης 2. Τέλος ας αναφέρουμε πως οι Darmon και Merel έδειξαν [31] πρόσφατα πως δεν υπάρχουν σχετικά πρώτες λύσεις με εκθέτες $(n, n, 3)$, $n \geq 3$.

ii. Η εικασία ΑΒΓ

Η εικασία ΑΒΓ διατυπώθηκε για πρώτη φορά από τους David Masser και Joseph Osterlé το 1985[32]. Είναι αξιοσημείωτο ότι αν και αυτή η εικασία είναι εξαιρετικά απλή στη διατύπωση και θα μπορούσε να έχει διατυπωθεί πολύ νωρίτερα, η ανακάλυψή της είναι βασισμένη σε πρόσφατες έρευνες σχετικά με σώματα συναρτήσεων και ελλειπτικές καμπύλες. Πρόκειται για μια πρόταση που συνδέεται με την αναλυσιμότητα στην Αριθμητική Αλγεβρική Γεωμετρία. Επίσης φαίνεται συνδεδεμένη με πολλά προβλήματα της Θεωρίας Αριθμών και βρίσκεται κυριολεκτικά στα όρια του τι είναι γνωστό και τι άγνωστο!

Χρειαζόμαστε έναν ορισμό:

Ορισμός 1. *Κομμάτι ελεύθερο τετραγώνου $KET(k)$ενός ακέραιου $k \in \mathbb{Z}$ λέγεται το γινόμενο των πρώτων που διαιρούν τον k ακριβώς μία φορά. Ισοδύναμα, είναι το γινόμενο των πρώτων που εμφανίζονται στην πρώτη δύναμη στην ανάλυση του $|k|$ σε πρώτους παράγοντες:*

$$KET(k) := \prod_{p|k} p \quad , \quad p \text{ πρώτος}$$

Άρα, αν ο $n \in \mathbb{N}$ ελεύθερος τετραγώνου, θα είναι $\mathrm{KET}(n) = n$. Ομοίως και αν ο n είναι πρώτος.

Έστω A, B φυσικοί, και $\Gamma = A + B$. Συνήθως ισχύει $\mathrm{KET}(AB\Gamma) > \Gamma$. Όχι όμως πάντα(θεωρήστε για παράδειγμα $A = 1, B = 8, \Gamma = 9$). Ο David Masser απέδειξε πως το πηλίκο $\mathrm{KET}(AB\Gamma)/\Gamma$ μπορεί να γίνει οσοδήποτε μικρό, δηλαδή

$$\forall \varepsilon > 0 \;\; \exists A, B \in \mathbb{Z} \quad \text{ώστε} \quad \frac{\mathrm{KET}(AB\Gamma)}{\Gamma} < \varepsilon$$

Η εικασία μας λέει πως αυτό παύει να ισχύει αν αυξήσουμε ελάχιστα τον εκθέτη:

Εικασία 3. ***(ΑΒΓ)*** *Έστω A, B σχετικά πρώτοι ακέραιοι, $\Gamma = A + B$. Για κάθε $\varepsilon > 0$ υπάρχει σταθερά $\mu > 1$ ώστε*

$$\max(|A|, |B|, |\Gamma|) \leq \mu KET(AB\Gamma)^{1+\varepsilon}$$

[†]Οι 5 τελευταίες βρέθηκαν αρκετά πρόσφατα από τους Beukers και Zagier

Η εικασία αυτή μας επιτρέπει να αναδιατυπώσουμε πλήθος Διοφαντικών εξισώσεων και να τις λύσουμε! Επίσης είναι ικανή να μας οδηγήσει σε μια απόδειξη του Τελευταίου Θεωρήματος του Fermat. Για το σκοπό αυτό διατυπώνουμε διατυπώνουμε την εικασία πιο απλά, υποθέτοντας τους A, B θετικούς:

Εικασία 4. *Έστω A, B σχετικά πρώτοι θετικοί ακέραιοι, $\Gamma = A + B$.Για κάθε $n > 1$, το κλάσμα*

$$\frac{KET(AB\Gamma)^n}{\Gamma}$$

είναι κάτω φραγμένο(προφανώς από το $1/\mu$).

Έστω θετικοί ακέραιοι x, y, z σχετικά πρώτοι ανά δυο, με $x^k + y^k = z^k$. Θέτουμε $A = x^k,\ B = y^k,\ \Gamma = A+B$ και η εξίσωση του Fermat γίνεται $A+B = \Gamma$. Η παραπάνω εικασία λέει ότι για κάθε $n > 1$, θα υπάρχει $M > 0$ ώστε

$$\frac{\mathrm{KET}(x^k y^k z^k)^n}{\Gamma} \geq M$$

Χάριν απλότητας θεωρούμε $n = 2$ και $M = 1$. Προφανώς $\mathrm{KET}(x^k y^k z^k) \leq xyz$ καθώς και $x, y < z$. Άρα

$$\mathrm{KET}(x^k y^k z^k) \leq xyz < z^3 \overset{\Gamma>1}{\Longrightarrow} \frac{\mathrm{KET}(x^k y^k z^k)^2}{\Gamma} < \frac{(z^3)^2}{\Gamma} = \frac{z^6}{z^k} = z^{6-k}$$

Από την εικασία $AB\Gamma$ έπεται τώρα ότι $z^{6-k} > 1$, το οποίο είναι αντιφατικό για κάθε $k \geq 6$. Με παρόμοια επιχειρήματα μπορούμε να αποκλείσουμε τις περιπτώσεις $k = 3, 4, 5$.

Αυτή η σύντομη(!) απόδειξη δείχνει πως η εικασία αυτή είναι κατά πολύ βαθύτερη απ΄ όσο δείχνει με την πρώτη ματιά.

iii. Η εικασία των Birch και Swinnerton-Dyer

Ένα από τα 7 «Προβλήματα της Χιλιετίας» τα οποία έχει επικηρύξει το Clay Mathematics Institute[‡] με ένα εκατομμύριο δολάρια το καθένα, είναι η εν λόγω εικασία.

Σε γενικές γραμμές, μια ελλειπτική καμπύλη είναι το σύνολο των σημείων του του επιπέδου που ικανοποιούν μια εξίσωση της μορφής

$$y^2 = \alpha x^3 + \beta x^2 + \gamma x + \delta$$

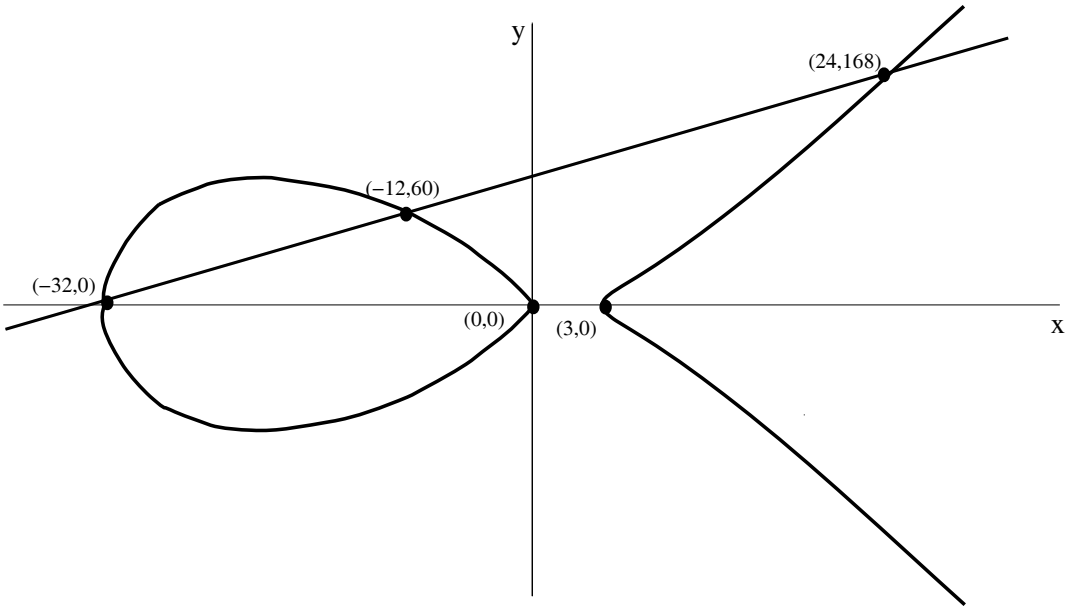
(παραλείπουμε μερικές τεχνικές λεπτομέρειες). Η θεωρία τους επεκτείνεται όμως και για $x, y \in \mathbb{C}$ ή γενικά σε οποιοδήποτε σώμα.

[‡]http://www.claymath.org/millennium/

Μια βασική πρόκληση των ελλειπτικών καμπύλων είναι η εύρεση όλων των ρητών σημείων πάνω σε μια τέτοια καμπύλη. Για παράδειγμα ο Fermat απέδειξε ότι οι μόνες ρητές λύσεις της ελλειπτικής εξίσωσης

$$y^2 = x^3 - x$$

είναι οι $(0,0)$, $(0,1)$, $(0,-1)$. Όμως η ελλειπτική καμπύλη $y^2 = x(x-3)(x+32)$ έχει πολλά ρητά σημεία. Το παρακάτω γράφημα δείχνει μερικά από αυτά:



Μάλιστα αποδεικνύεται πως κάθε ευθεία που τέμνει μια ελλειπτική καμπύλη σε δυο ρητά σημεία, διέρχεται και από τρίτο ρητό σημείο της. Έτσι έχοντας 2 ρητά σημεία, εύκολα βρίσκουμε κι ένα τρίτο. Τα ρητά σημεία μιας ελλειπτικής καμπύλης έχουν τη δομή ομάδας.

Κάνοντας υπολογισμούς σε πάρα πολλά παραδείγματα, οι Birch και Swinnerton-Dyer ανακάλυψαν μια ενδιαφέρουσα σχέση μεταξύ του πλήθους των ρητών σημείων μιας ελλειπτικής καμπύλης και της συμπεριφοράς μιας αναλυτικής συνάρτησης που σχετίζεται με την καμπύλη και καλείται L-συνάρτηση.

Εικασία 5. *(***Birch & Swinnerton-Dyer***) Έστω $\mathcal{C}$ μια ελλειπτική καμπύλη. Η σειρά Taylor της συνάρτησης $L(\mathcal{C},s)$ στο σημείο $s=1$ έχει τη μορφή*

$$L(\mathcal{C},s) = c(s-1)^r + \text{ όροι ψηλότερης τάξης}$$

όπου $c \neq 0$ και r η τάξη της ομάδας των ρητών σημείων της καμπύλης. Ειδικότερα, $L(\mathcal{C},1) = 0$ αν και μόνο αν η ομάδα των ρητών σημείων είναι άπειρη.

Με την παραπάνω γνώση, θα μπορούμε να αποφαινόμαστε για το πλήθος των ρητών σημείων μιας ελλειπτικής καμπύλης εκτιμώντας την $L(\mathcal{C}, s)$ στο σημείο 1.

Η εικασία συνδέεται και με ένα άλλο σημαντικό πρόβλημα της Αλγεβρικής Θεωρίας Αριθμών, το οποίο είναι γνωστό ως η εικασία του Serre, από το Γάλλο μαθηματικό Jean-Pierre Serre, ο οποίος τη διατύπωσε στις αρχές της δεκαετίας του ΄70. Αυτή έχει να κάνει με τις αναπαραστάσεις Galois και τις μορφές modular, και μια απόδειξή της θα δώσει σαν πόρισμα το Τελευταίο Θεώρημα του Fermat. Για περισσότερες πληροφορίες δείτε το [43]. Πολύ πρόσφατα ο Ινδός μαθηματικός Chandrashekhar Khare δημοσίευσε μια εργασία στην οποία δίνει μια μερική απόδειξη αυτής.

Αν η εικασία *Birch & Swinnerton-Dyer* αποδειχθεί, τότε θα λυθεί κι ένα πρόβλημα που ίσως απασχόλησε και τον ίδιο τον Πυθαγόρα: Δοθέντος ενός φυσικού αριθμού, υπάρχει ορθογώνιο τρίγωνο με ρητού μήκους πλευρές, με εμβαδόν ίσο με αυτόν τον αριθμό; Παραδείγματος χάριν, το ορθογώνιο τρίγωνο με πλευρές 3,4,5 έχει εμβαδόν 6. Επίσης το εμβαδόν του ορθογώνιου τριγώνου με πλευρές $\frac{3}{2}, \frac{20}{3}, \frac{41}{6}$ είναι 4. Όμως κανένα ορθογώνιο τρίγωνο με ρητές πλευρές δεν έχει εμβαδόν ίσο με 1,2,3 ή 4. Κι αυτό το πρόβλημα έχει τις ρίζες του στις ελλειπτικές καμπύλες, διότι ένα ορθογώνιο τρίγωνο με εμβαδόν E αντιστοιχεί σε μια ρητή λύση μιας ελλειπτικής καμπύλης με εξίσωση $y^2 = x^3 - E^2x$.

Η μια κατεύθυνση της εικασίας έχει αποδειχθεί για μια συγκεκριμένη κλάση ελλειπτικών καμπύλων: Οι A. Wiles και J. Coates έδειξαν πως γι αυτήν την κλάση, άπειρος αριθμός ρητών σημείων οδηγεί στη σχέση $L(\mathcal{C}, 1) = 0$. Γίνονται προσπάθειες να αποδειχθεί το συμπέρασμα αυτό για την κλάση των modular καμπύλων, και τότε θα ισχύει σε πλήρη γενικότητα, αφού όπως έδειξαν οι Shimura- Taniyama (και αποτέλεσε τον πυρήνα της απόδειξης του Wiles) κάθε ελλειπτική καμπύλη είναι modular. Αυτό φυσικά θα ήταν η απόδειξη μόνο της μιας κατεύθυνσης της εικασίας. Όπως λέει ο ίδιος ο A. Wiles, «*Η άλλη κατεύθυνση είναι αρκετά πιο δύσκολη. Έχω ισχυρό προαίσθημα πως οι καμπύλες modular θα είναι πολύ σημαντικές στην ολοκλήρωση της απόδειξης.*»

Βιβλιογραφία

Αλγεβρική Θεωρία αριθμών

[1] I.N. Stewart and D.O. Tall, *Algebraic Number Theory*, Chapman and Hall Mathematics Series, 1979

[2] Z.I. Borevič and I.R. Šafarevič, *Number Theory*, Academic Press, 1979

[3] H. Koch, *Algebraic Number Theory*, Springer, 1997

[4] S. Lang, *Algebraic Number Theory*, Addison-Weslay, 1970

[5] P. Ribenboim, *Algebraic Numbers, Springer-Verlag*, Wiley-Interscience, New York, 1972

[6] P. Ribenboim, *Classical theory of algebraic numbers*, Universitext, Springer, 2001

[7] L. C. Washington, I*ntroduction to Cyclotomic Fields*, Springer-Verlag, New York, 1996

Το Τελευταίο Θεώρημα του Fermat

[8] H.M. Edwards, *Fermat's Last Theorem*, Springer, 1977

[9] H M Edwards, *The background of Kummer's proof of Fermat's last theorem for regular primes*, Arch. History Exact Sci. 14, 1975

[10] P. Ribenboim, *13 lectures on Fermat's last theorem*, New York, 1979

[11] P. Ribenboim, *Kummer's ideas on Fermat's last theorem*, Enseign. Math., 1983

[12] D.A. Cox, *Introduction to Fermat's last theorem*, Amer. Math. Monthly 101,1994

[13] A. van der Poorten, *Notes on Fermat's last theorem*, New York, 1996

[14] A. van der Poorten, *Remarks on Fermat's last theorem*, Austral. Math. Soc. Gaz., 1994

[15] Andrew Wiles, *Modular elliptic curves and Fermat's Last Theorem, Ring-theoretic properties of certain Hecke algebras*, Annals of Mathematics 141(443-551, 553-572), 1995

Ιστορικά

[16] Simon Singh *Το τελευταίο Θεώρημα του Φερμά*, Τραυλός, 1998

[17] A. Aczel, *Πώς ο A. Wiles έλυσε το τελευταίο θεώρημα του Φερμά*, Τροχαλία, 1998

[18] E.T. Bell, *Οι Μαθηματικοί*, Τόμος Ι, Πανεπιστημιακές Εκδόσεις Κρήτης, 1998

[19] P. Ribenboim, *The history of Fermat's last theorem*, Bol. Soc. Paran. Mat., 1984

Άλλες Αναφορές

[20] Δ. Βάρσος,Δ. Δεριζιώτης, Μ. Μαλιάκας, Σ. Παπασταυρίδης, Ε. Ράπτης, Ο. Ταλέλλη, *Μια εισαγωγή στην Άλγεβρα*, Σοφία, 2003

[21] Μ. Μαλιάκας, *Μεταθετική Άλγεβρα & Εφαρμογές*, Συμμετρία, 1999

[22] Χ. Χαραλαμπίδης, *Θεωρία Πιθανοτήτων και Εφαρμογές*, Συμμετρία, 2000

[23] Hilbert, D. *Mathematical Problems*, Bull. American Mathematics Society, 1901-1902

[24] P. Ribenboim, *The new Book of Prime Number Records*, Springer, 1996

[25] J. Buhler, R. Crandall, R. Ernvall, T. Metsankyla and M. Shokrollahi, *Irregular primes and cyclotomic invariants to 12 million*

[26] Masley, *On the Class Number of Cyclotomic fields*,1972

[27] D. Goldfeld, *Beyond the Last Theorem*, Math Horizons, September 1996

[28] Gelbart, S.S., *An elementary introduction to the Langlands program*, Bulletin Amer. Math. Soc. 10, 1984

[29] S.J. Patterson, *An Introduction to the Theory of the Riemann Zeta-Function*, Cambridge University Press, 1988

[30] H. Darmon and A. Granville, *On the equations* $z^m = F(x; y)$ *and* $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. 27, 1995

[31] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat"s Last Theorem*(preprint)

[32] J. Osterlé, Nouvelles approches du Théoréme de Fermat, Sem. Bourbaki, n^o 694, 1987-88

[33] S. Lang, *Old and new conjectured diophantine inequalities*, Bull. Amer. Math. Soc. 23, 1990

Πηγές από τον Παγκόσμιο Ιστό

[34] Number Fields
http://rooster.stanford.edu/~ben/maths/numberfield/

[35] Number Theory -Fermat's Last Theorem:
http://www.math.nmsu.edu/~history/book/numbertheory.pdf

[36] Fermat's Last Theorem:
http://www.geocities.com/fermatnow/flt/index.htm

[37] Bluff your way in Fermat's Last Theorem:
http://math.stanford.edu/~lekheng/flt/

[38] AMS Notice - The proof of FLT:
http://www.ams.org/notices/199507/faltings.pdf

[39] Fermat's Last Theorem Blog:
http://fermatslasttheorem.blogspot.com/

[40] The Mathematics of Fermat's Last Theorem:
http://cgd.best.vwh.net/home/flt/flt01.htm

[41] Introduction on Bernoulli's numbers:
http://numbers.computation.free.fr/Constants/Miscellaneous/bernoulli.html

[42] The Bernoulli Number Page:
http://www.bernoulli.org/

[43] Bas Edixhoven, Serre's conjecture:
http://www.math.leidenuniv.nl/~edix/public_html_rennes/publications/boston.html