Η εξίσωση του Fermat για τον εκθέτη n=3.
Μία στοιχειώδης προσέγγιση

Αλέξανδρος Γ. Συγκελάκης *

6 Απριλίου 2006

Περίληψη

Θέμα της εργασίας αυτής, είναι η απόδειξη οτι η εξίσωση $x^3 + y^3 = z^3$ όπου $xyz \neq 0$, δεν έχει ακέραιες λύσεις. Είναι η μερική περίπτωση του Τελευταίου Θεωρήματος του Fermat για $n = 3$. Ο Euler, έδωσε δύο αποδείξεις για το θέμα αυτό. Η μία, ήταν πολύ καινοτόμος χρησιμοποιώντας άρρητους αριθμούς. Δυστυχώς ο Euler, έκανε ένα λάθος στους ισχυρισμούς του στην απόδειξη αυτή. Παρα ταύτα η μέθοδος αυτή, αποκάλυψε μία πολλά υποσχόμενη προσεγγιση για το τελευταίο Θεώρημα του Fermat με το οποίο ασχολήθηκαν αργότερα οι Gauss, Dirichlet και Kummer αλλά και πολλοί άλλοι σύγχρονοι μαθηματικοί μέχρι και τον A. Wiles, ο οποίος και έδωσε την ολοκληρωμένη απόδειξη του Θεωρήματος (1994).

Η δεύτερη απόδειξη (αυτή που παρουσιάζεται και στην εργασία αυτή), είναι πολυ ευρηματική, χρησιμοποιώντας όμως μεθόδους, μόνο στοιχειώδους Θεωρίας Αριθμών.

1 Γενικές Προτάσεις και Λήμματα

Λήμμα 1.1 *Μπορούμε να φέρουμε την εξίσωση $x^n + y^n = z^n$ σε μία μορφή, τέτοια ώστε τα x, y, z, να είναι πρώτοι μεταξύ τους ανα δύο.*

Απόδειξη

Έστω $(x, y) = d$. Τότε $x = dx', y = dy'$, με $(x', y') = 1$, και $x'^n + y'^n = \left(\frac{z}{d}\right)^n$. Άρα $\left(\frac{z}{d}\right)^n \in \mathbb{Z}$, οπότε από γνωστή άσκηση, $\frac{z}{d} \in \mathbb{Z}$. Θέτουμε τότε $\frac{z}{d} = z'$, οπότε καταλήγουμε στην $x'^n + y'^n = z'^n$.

Είναι εύκολο τώρα να δούμε οτι $(x', z') = 1$ και $(y', z') = 1$, διότι εαν π.χ. ο πρώτος p διαιρεί τους x', z', τότε p / y'^n δηλαδή p / y' που αντιβαίνει στην $(x', y') = 1$. $\square$

Παρατήρηση: Βάσει του Λήμματος (1.1) μπορούμε στο εξής να υποθέτουμε οτι στην εξίσωση $x^3 + y^3 = z^3$, που μελετούμε, οι x, y, z είναι ανα δύο πρώτοι μεταξύ τους. Επίσης $x \neq y \neq z \neq x$.

*Τμήμα Μαθηματικών, Πανεπιστήμιο Κρήτης

Έπεται οτι ένας ακριβώς είναι άρτιος. Μπορούμε χωρίς βλάβη της γενικότητος, να υποθέσουμε τον z άρτιο και τους x, y περιττούς. (Εαν π.χ. ο x είναι άρτιος, τότε $(-z)^3 + y^3 = (-x)^3$ και θέτουμε όπου $-z$ το x και όπου $-x$ το z).

Μπορούμε να υποθέσουμε τον z θετικό (διαφορετικά θα γράφαμε $(-x)^3 + (-y)^3 = (-z)^3$ και θα αντικαθιστούσαμε τους $-x, -y, -z$ από τους x, y, z αντιστοίχως). Αλλά τότε λόγω της $z^3 = (x+y)(x^2 - xy + y^2) = (x+y)\big[(x - \frac{y}{2})^2 + \frac{3y^2}{4}\big]$, ο $x+y$ είναι θετικός. Λόγω συμμετρίας του ρόλου των x, y και της $x \neq y$ μπορούμε να υποθέσουμε $x > y$. Συνοψίζοντας:

Από εδώ και στο εξής, **εξίσωση του Fermat**, εννοούμε την $x^3 + y^3 = z^3$ όπου $x \cdot y \cdot z \neq 0$,οι x, y, z είναι ανα δύο πρώτοι μεταξύ τους,z άρτιος, $x > y$ και $x + y > 0$, άρα $z > 0$.

Θεώρημα 1.1 *Εαν η εξίσωση του Fermat $x^3 + y^3 = z^3$ έχει λύση, υπάρχουν ακέραιοι p, q θετικοί πρώτοι μεταξύ τους και διαφορετικής αρτιότητος[1], τέτοιοι ώστε $x = p + q, y = p - q$ και $z^3 = 2p(p^2 + 3q^2)$.*

Απόδειξη: Αφού ο z είναι άρτιος, οι x, y είναι περιττοί άρα μπορούμε να θέσουμε $x + y = 2p$, $x - y = 2q$ όπου οι ακέραιοι p, q είναι > 0 (βλέπε παρατήρηση πιο πάνω). Από την άσκηση 1 του Β′ Φυλλαδίου έχουμε ότι $(p, q) = (\frac{x+y}{2}, \frac{x-y}{2}) = 1$ και ένας ακριβώς από τους q, p είναι άρτιος. Τέλος $x = p+q$, $y = p - q$ οπότε η εξίσωσή μας γράφεται: $(p+q)^3 + (p-q)^3 = z^3$ δηλαδή $2p(p^2 + 3q^2) = z^3$.

□

Λήμμα 1.2 *Εαν οι πρώτοι μεταξύ τους ακέραιοι p, q, έχουν διαφορετική αρτιότητα τότε $(2p, p^2 + 3q^2) = 1$ ή 3 ανάλογα με το αν $3 \nmid p$ ή $3 | p$ αντίστοιχα.*

Απόδειξη:

Έστω $(2p, p^2 + 3q^2) = t$. Ο $p^2 + 3q^2$ είναι περιττός, άρα ο t είναι περιττός. Συνεπώς $p \equiv 0 \pmod t$ και $p^2 + 3q^2 \equiv 0 \pmod t$. Ο συνδιασμός των δύο σχέσεων δίνει $3q^2 \equiv 0 \pmod t$. Αν είναι $t > 1$, τότε $(q, t) = 1$ (διότι $t | p$), άρα και $(q^2, t) = 1$. Έπεται οτι $3 \equiv 0 \pmod t$, δηλαδή $t | 3$. Άρα $t = 1$ ή $t = 3$.

□

Λήμμα 1.3 *Ισχύει η ταυτότητα $(a^2 + kb^2)(c^2 + kd^2) = (ac - kbd)^2 + k(ad + bc)^2$ της οποίας εμείς θα κάνουμε χρήση για $k = 3$.* □

[1] Λέγοντας οτι δύο αριθμοί έχουν ίδια **αρτιότητα**, εννοούμε οτι και οι δύο είναι άρτιοι ή και οι δύο περιττοί και κατ'επέκτασιν, δύο αριθμοί έχουν διαφορετική αρτιότητα όταν ένας εκ των δύο είναι άρτιος και ο άλλος περιττός (Πρόκειται για μετάφραση της αγγλικής λέξεως parity).

Λήμμα 1.4 *Εαν το 2 διαιρεί ένα ακέραιο της μορφής $\square + 3 \cdot \square$, τότε και το 4 διαιρεί τον αριθμό αυτό και το πηλίκο της διαίρεσης αυτής δια 4, είναι ένας ακέραιος της ίδιας μορφής.*

Απόδειξη:

Έστω $2|a^2 = 3b^2$. Τότε παρατηρούμε ότι τα a, b έχουν την ίδια αρτιότητα.

Εαν και οι δύο είναι άρτιοι, τότε $a = 2c$, $b = 2d$ και $a^2+3b^2 = (2c)^2+3(2d)^2 = 4(c^2 + 3d^2)$.

Εαν είναι και οι δύο είναι περιττοί, τότε το 4 διαιρεί έναν ακριβώς εκ των $a + b, a - b$ (Άσκηση 1, Φυλλάδιο Β'). Θα δείξουμε οτι εαν $4|(a + b)$ το Λήμμα ισχύει (η περίπτωση $4|(a - b)$ είναι εντελώς ανάλογη). Καταρχήν, $4(a^2 + 3b^2) = (1^2 + 3 \cdot 1^2)(a^2 + 3b^2) = (a - 3b)^2 + 3(a + b)^2$ (πρβλ. Λήμμα 1.3) και αφού $a - 3b = (a + b) - 4b$, άρα $4|a - 3b$. Συνεπώς $4|a^2 + 3b^2$. Αφού όμως $4|a - 3b$ και $4|a + b$, γνωρίζουμε οτι υπάρχουν ακέραιοι u, v τέτοιοι ώστε $a - 3b = 4u$ και $a + b = 4v$. Λυνοντας ως προς a, b, έχουμε $a = u + 3v, b = v - u$ και με απλές πράξεις διαπιστώνουμε οτι $\dfrac{a^2 + 3b^2}{4} = u^2 + 3v^2$.

$\square$

Λήμμα 1.5 *Εαν ένας πρώτος της μορφής $\square + 3 \cdot \square$ διαιρεί το $a^2 + 3b^2$, τότε υπάρχουν ακέραιοι c, d τέτοιοι ώστε: $a^2 + 3b^2 = (p^2 + 3q^2)(c^2 + 3d^2)$.*

Απόδειξη:

Έστω $p^2 + 3q^2$ πρώτος και ας υποθέσουμε ότι $(p^2 + 3q^2)|(a^2 + 3b^2)$. Τότε υπάρχει ακέραιος k, τέτοιος ώστε $a^2 + 3b^2 = k(p^2 + 3q^2)$ και τότε, με απλές πράξεις, έχουμε

$$(pb - aq)(pb + aq) = (p^2 + 3q^2)(b^2 - q^2k)$$

Άρα ο πρώτος $p^2 + 3q^2$ διαιρεί ένα τουλάχιστον από τους παράγοντες του αριστερού μέλους. Άρα για $\varepsilon = 1$ ή -1, $(pb + \varepsilon aq) = (p^2 + 3q^2)d$, όπου ο d είναι κάποιος ακέραιος. Όμως,

$$(p^2+3q^2)(a^2+3b^2) = (pa-\varepsilon 3qb)^2+3(pb+\varepsilon aq)^2 \text{ (Λήμμα 1.3), άρα } p^2+3q^2|pa-\varepsilon 3qb \tag{1.1}$$

και θέτουμε $pa - 3\varepsilon qb = c(p^2 + 3q^2)$ για κάποιο $c \in \mathbb{Z}$. Άρα λόγω και της (1.1),

$$\begin{aligned}(p^2 + 3q^2)(a^2 + 3b^2) = (pa - 3\varepsilon qb)^2 + 3(pb + \varepsilon aq)^2 &= [c(p^2 + 3q^2)]^2 + 3[d(p^2 + 3q^2)]^2 \\ &= (p^2 + 3q^2)^2(c^2 + 3d^2)\end{aligned}$$

Άρα τελικά, $(a^2 + 3b^2) = (p^2 + 3q^2)(c^2 + 3d^2)$.

$\square$

Λήμμα 1.6 *Εαν ο ακέραιος $a^2 + 3b^2$ έχει ένα περιττό παράγοντα > 1, που δεν είναι της ίδιας μορφής, τότε και το πηλίκο έχει ενα παράγοντα, που δεν είναι της ίδιας μορφής.*

Απόδειξη:
Έστω a^2+3b^2 ο ελάχιστος ακέραιος με την ιδιότητα της εκφώνησης. Τότε $a^2+3b^2=kg$ και ο $k>1$ είναι περιττός $\neq \Box+3\cdot\Box$. Άρα $g>1$.

- Εαν ο g έχει περιττό διαιρέτη >1, τότε ισχυριζόμαστε ότι κάθε περιττός πρώτος διαιρέτης του g δεν είναι της μορφής $\Box+3\cdot\Box$. Πράγματι, εαν ο p^2+3q^2 είναι περιττός πρώτος διαιρέτης του g, τότε $g=(p^2+3q^2)g_1$ και από το Λήμμα (1.5), $\dfrac{a^2+3b^2}{p^2+3q^2}=c^2+3d^2$, άρα $c^2+3d^2=kg_1$ και αυτό αντιβαίνει στον τρόπο που επιλέξαμε τον a^2+3b^2.

- Εαν ο g δεν έχει περιττό διαιρέτη >1, τότε $g=2^n,\ n\geq 1$. Επειδή $2|a^2+3b^2$, το Λήμμα (1.4) μας λέει οτι $4|a^2+3b^2$ (άρα $n\geq 2$) και ακόμη, $\frac{a^2+3b^2}{4}=c^2+3d^2$. Άρα $c^2+3d^2=k2^{n-2}$ και ερχόμαστε ξανά σε αντίφαση με την επιλογή του a^2+3b^2.

$\Box$

Θεώρημα 1.2 *Εαν p,q θετικοί αριθμοί, πρώτοι μεταξύ τους, διαφορετικής αρτιότητας και έτσι ώστε ο ακέραιος p^2+3q^2 να είναι τέλειος κύβος, τότε, υπάρχουν αριθμοί A,B, τέτοιοι ώστε:*

- $p=A^3-9AB^2$
- $q=3A^2B-3B^3$
- $(A,B)=1$

Απόδειξη:
Θα δουλέψουμε στο σώμα $\mathbb{Q}(\omega)$ με $\omega^2+\omega+1=0$. Είναι γνωστό οτι οι μονάδες του δακτυλίου $\mathbb{Z}(\omega)$ είναι οι $\{1,\omega,\omega^2\}$.

Αφού ο p^2+3q^2 είναι τέλειος κύβος, άρα υπάρχει περιττός ακέραιος u (οι p,q έχουν διαφορετική αρτιότητα) τέτοιος ώστε $p^2+3q^2=u^3$ δηλαδή $(p+i\sqrt{3}q)(p-i\sqrt{3}q)=u^3$. Όμως $i\sqrt{3}=2\omega+1$ και η παραπάνω σχέση γράφεται $[(p+q)+2q\omega]\cdot[(p-q)-2q\omega]=u^3$. Όμως εαν Μ.Κ.Δ$((p+q)+2q\omega,(p-q)-2q\omega)\neq$ μονάδα, τότε πρέπει να υπάρχει πρώτος αριθμός $\pi\in\mathbb{Q}(\omega)$, με $\pi|(p+q)+2q\omega$ και $\pi|(p-q)-2q\omega$, απ'οπου $\pi|2p$ και $\pi|2q(2\omega+1)$.

Έστω $\pi|2p$. Τότε $\pi|2$ ή $\pi|p$

(i) Έστω $\pi|2$. Τότε αφού $N(\pi)|4$ και $N(\pi)\neq 1$ (π πρώτος άρα όχι μονάδα) ο $N(\pi)$ είναι άρτιος. Από την άλλη αφού $\pi|2$ και $\pi|(p+q)+2q\omega$, έχουμε $\pi|p+q$ δηλαδή $N(\pi)|(p+q)^2$ και επειδή $N(\pi)$ άρτιος καταλήγουμε σε άτοπο αφού $(p+q)^2$ =περιττός λόγω του οτι τα p,q έχουν διαφορετική αρτιότητα.

(ii) Έστω $\pi|p$. Τότε καθώς $\pi|2q(2\omega+1)$ έχουμε $\pi|q$ ή $\pi|(2\omega+1)$ και εαν $\pi|q$ καταλήγουμε σε άτοπο λόγω της $(p,q)=1$. Απ'την άλλη, εαν $\pi|(2\omega+1)$

τότε καθώς ο $2\omega+1$ είναι πρώτος, έχουμε $\pi = \varepsilon(2\omega+1)$, με ε=μονάδα. Άρα $N(\pi) = N(2\omega+1) = 3$ και καθώς $\pi|p$ έχω $3|N(p)$ δηλαδή $3|p$. Άρα $p = 3p_1$ για κάποιο ακέραιο p_1. Τότε $9p_1^2 + 3q^2 = u^3$ απ'όπου $3|u$ δηλαδή $u = 3u_1$ για κάποιο ακέραιο u_1. Αντικαθιστώντας παίρνουμε $3p_1^2 + q^2 = 9u_1^3$, απ'όπου $3|q$, άτοπο καθώς $(p,q) = 1$.

Συνεπώς $((p+q)+2q\omega, (p-q)-2q\omega) =$ μονάδα. Άρα κάθε ένας από αυτούς τους παράγοντες είναι της μορφής « (τέλειος κύβος)·(μονάδα) ». Άρα $(p+q)+2q\omega = (a+b\omega)^3$ ή $\omega(a+b\omega)^3$ ή $\omega^2(a+b\omega)^3$.

Εαν ήταν $(p+q)+2q\omega = \omega(a+b\omega)^3$, τότε αναπτύσοντας την ταυτότητα θα έπαιρνα $2q = a^3 - 3a^2b + b^3$ και $p+q = -3a^2b + 3ab^2$. Συνδιάζοντας οτι p,q διαφορετικής αρτιότητας, και παίρνοντας περιπτώσεις για τα a,b καταλήγουμε πολύ εύκολα σε άτοπο. Με όμοιο σκεπτικό απορρίπτεται και η περίπτωση να έχουμε $(p+q)+2q\omega = \omega^2(a+b\omega)^3$.

Τέλος εαν $(p+q)+2q\omega = (a+b\omega)^3$ τότε παίρνω $p+q = a^3 - 3ab^2 + b^3, 2q = 3a^2b - 3ab^2$. Με απλές δοκιμές βρίσκω οτι a,b είναι περιττοί. Υπάρχουν λοιπόν ακέραιοι A,B τέτοιοι ώστε $a = -A+B, b = -A-B$ με $(A,B) = 1$, και αντικαθιστώντας παραπάνω τις τιμές των a,b, παίρνουμε $q = 3A^2B - 3B^3, p = A^3 - 9AB^2$, όπως ακριβώς χρειαζόμασταν. □

Θεώρημα 1.3 *Δεν υπάρχει λύση (x,y,z) της εξίσωσης του Fermat, τέτοια ώστε να ικανοποιεί τις συνθήκες του Θεωρήματος 1.1 και να ισχύει* $(2p, p^2+3q^2) = 1$.

Απόδειξη:

Έστω οτι υπάρχει ελάχιστη λύση (x,y,z) υπό την έννοια οτι το γινόμενο $|xyz|$ είναι ελάχιστο και θα βρω μία λύση της οποίας η απόλυτη τιμή του γινομένου θα είναι μικρότερη, συνεπώς με την μέθοδο της άπειρης καθόδου καταλήγουμε σε άτοπο:

Σύμφωνα με την Άσκηση 3 του Φυλλαδίου Β′, οι $2p$ και p^2+3q^2 είναι τέλειοι κύβοι. Όμως σύμφωνα με το Θεώρημα 1.2, υπάρχουν ακέραιοι a,b τέτοιοι ώστε $p = a^3 - 9ab^2, q = 3a^2b - 3b^3, (a,b) = 1$ και οι a,b έχουν διαφορετική αρτιότητα. Επίσης $3 \nmid a$ διότι διαφορετικά οι p,q θα ήταν συγχρόνως διαιρετοί δια 3. Όμως $2p = 2a^3 - 18ab^2 = (2a)(a-3b)(a+3b)$, και είναι απλή άσκηση να δείξει κανείς ότι οι $2a, a-3b, a+3b$ είναι ανα δύο πρώτοι μεταξύ τους, βασισμένοι στο ότι οι $a \pm 3b$ είναι περιττοί, οι a,b πρώτοι μεταξύ τους και $3 \nmid a$.

Συνεπώς καθένας απ'τους $2a, a-3b, a+3b$ είναι τέλειος κύβος, άρα υπάρχουν ακέραιοι A,B,C τέτοιοι ώστε: $2a = A^3,\ \ a-3b = B^3,\ \ a+3b = C^3$. Αυτό όμως δίνει μια καινούρια λύση στην εξίσωση του Fermat καθώς $A^3 = 2a = (a-3b)+(a+3b) = B^3 + C^3$, και είναι αναγκαστικά μικρότερη απ'την x,y,z, αφού $|A^3B^3C^3| = |2a(a-3b)(a+3b)| = 2|p|$ ενώ $z^3 = 2p(p^2+3q^2)$ (πρβλ. Θεώρημα 1.1). Συνεπώς $|A^3B^3C^3| < |x^3y^3z^3|$ άρα $|ABC| < |xyz|$, άτοπο διότι είχαμε επιλέξει τη λύση (x,y,z) της εξίσωσης του Fermat έτσι ώστε ο $|xyz|$ να είναι ελάχιστος.

□

Θεώρημα 1.4 *Δεν υπάρχει λύση (x, y, z) της εξίσωσης του Fermat, τέτοια ώστε να ικανοποιεί τις συνθήκες του Θεωρήματος 1.1 και να ισχύει $(2p, p^2 + 3q^2) = 3$.*

Απόδειξη: Έστω οτι υπάρχει ελάχιστη λύση (x, y, z) υπό την έννοια οτι το $|z|$ είναι ελάχιστο και θα καταλήξω σε μία άλλη μικρότερη λύση, συνεπώς με την μέθοδο της άπειρης καθόδου καταλήγουμε σε άτοπο:

Καταρχήν το 3 διαιρεί τον p, αλλά δεν διαιρεί τον q καθώς $3|2p$ και $(p, q) = 1$. Άρα υπάρχει s τέτοιο ώστε: $p = 3s$ και $2p(p^2 + 3q^2) = 2 \cdot 3s(3 \cdot 3s^2 + 3q^2) = 18s(q^2 + 3s^2)$. Αφήνεται στον αναγνώστη ν'αποδείξει οτι $(18s, q^2 + 3s^2) = 1$ καθώς πρόκειται για άσκηση ρουτίνας.

Από το Θεώρημα 1.1 έχουμε ότι ο $2p(p^2 + 3q^2)$ είναι τέλειος κύβος, δηλαδή ο $18s(q^2 + 3s^2)$ είναι τέλειος κύβος. Από την Άσκηση 3 του Φυλλαδίου Β΄ και το γεγονός οτι $(18s, q^2 + 3s^2) = 1$, συμπεραίνουμε οτι καθένας απ'τους $q^2 + 3s^2$ και $18s$, είναι τέλειος κύβος. Άρα, σύμφωνα με το Θεώρημα 1.2, αφού ο $q^2 + 3s^2$ είναι τέλειος κύβος, υπάρχουν a, b τέτοιοι ώστε: $q = a^3 - 9ab^2$, $s = 3a^2b - 3b^3$, $(a, b) = 1$. Όμως τέλειος κύβος είναι και ο $18s = 3^3 2b(a + b)(a - b)$, άρα ο $2b(a - b)(a + b)$ είναι τέλειος κύβος. Είναι και πάλι άσκηση ρουτίνας ν'αποδείξει κανείς οτι οι $2b, a - b, a + b$ είναι ανα δύο πρώτοι μεταξύ τους.

Άρα κάθε ένας από αυτούς είναι κύβος, οπότε υπάρχουν ακέραιοι A, B, C τέτοιοι ώστε: $2b = A^3$, $a - b = B^3$, $a + b = C^3$. Αυτό όμως δίνει μια καινούρια λύση στην εξίσωση του Fermat, καθώς $A^3 = 2b = (a + b) - (a - b) = C^3 - B^3$ δηλαδή $A^3 + B^3 = C^3$. Όμως $|C^3| = |a + b| < |s| = |3b(a - b)(a + b)| < |p|$. Όμως $z^3 = 2p(p^2 + 3q^2)$ (πρβλ. Θεώρημα 1.1 και αρχική παρατήρηση). Έτσι οδηγούμαστε σε μία άλλη λύση της εξισώσεως του Fermat, μικρότερη της προηγούμενης, αφού εαν $z^3 = 2p(p^2 + 3q^2)$, τότε καθώς $|C^3| < |p| < |2p(p^2 + 3q^2)| = |z^3|$, έχουμε $|C|^3 < |z|^3$ απ'όπου $|C| < |z|$ και έχουμε τελειώσει. Άρα λοιπόν δεν υπάρχει λύση της εξίσωσης του Fermat ούτε όταν $(2p, p^2 + 3q^2) = 3$.

$\square$

2 Η εξίσωση του Fermat για τον εκθέτη n=3 είναι αδύνατη

- Ας υποθέσουμε οτι έχουμε λύσεις της εξίσωσης του Fermat
- Τότε από το Θεώρημα 1.1, θα υπάρχουν p, q τέτοιοι ώστε:

  ✓ $(p, q) = 1$

  ✓ Οι p, q είναι θετικοί

  ✓ Έχουν διαφορετική αρτιότητα

  ✓ Ο ακέραιος $2p(p^2 + 3q^2)$ είναι τέλειος κύβος
- Επίσης ξέρουμε οτι $(2p, p^2 + 3q^2) = 1$ ή 3 (Λήμμα 1.2)
- Εαν $(2p, p^2 + 3q^2) = 1$ τότε δεν υπάρχει λύση της εξίσωσης του Fermat (Θεώρημα 1.3).

- Εαν $(2p, p^2 + 3q^2) = 3$ τότε τότε δεν υπάρχει και πάλι λύση της εξίσωσης του Fermat (Θεώρημα 1.4).

- Και στις δύο περιπτώσεις λοιπόν, καταλήγουμε σε άτοπο, πράγμα που δηλώνει οτι **η εξίσωση του Fermat δεν έχει ακέραιες λύσεις για τον εκθέτη** $n = 3$**.**

Αναφορές

[1] H. M. Edwards, Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory p. 39–57.

[2] P. Ribenboim, Fermat's Last Theorem for Amateurs p. 24–40.

[3] Larry Freeman, http://fermatslasttheorem.blogspot.com/2005/05/fermats-last-theorem-proof-for-n3.html