Η Περίπτωση ΙΙ της Εξίσωσης του Fermat για Εκθέτη 5

Νικόλαος Δ. Κατσίπης *

23 Μαρτίου 2006

Το άρθρο αυτό αποτελεί το περιεχόμενο εργασίας, που παρουσιάστηκε στα πλαίσια του μεταπτυχιακού μαθήματος : *Η Θεωρία Αριθμών στην Εκπαίδευση* .

1 Η Απόδειξη

Η απόδειξη του τελευταίου θεωρήματος του Fermat για την πέμπτη δύναμη δημοσιεύτηκε το 1825 από δύο πολύ μεγάλους μαθηματικούς, τον Dirichlet και τον Legendre, οι οποίοι έδρασαν με διαφορά μιας γενιάς. Ο Legendre ήταν ένας άνδρας εβδομήντα ετών που είχε ζήσει από κοντά την πολιτική αναταραχή της Γαλλικής Επανάστασης. Η αποτυχία του στην υποστήριξη της υποψήφιας κυβέρνησης στο Εθνικό Ινστιτούτο είχε ως αποτέλεσμα την διακοπή της σύνταξης του, και μέχρι που συνείσφερε στο Τελευταίο Θεώρημα του Fermat ήταν άπορος. Από την άλλη, ο Dirichlet ήταν ένας νεαρός αριθμοθεωρητικός, που μόλις είχε κλείσει τα είκοσι. Και οι δύο, ανεξάρτητα ο ένας από τον άλλο, κατάφεραν να αποδείξουν ότι η περίπτωση $n = 5$ δεν είχε καθόλου λύσεις. Και οι δύο βασίσθηκαν στο θεώρημα της Sophie Germain (βλ. Λήμμα 2, παρακάτω).

Σκοπός τις εργασίας αυτής είναι η απόδειξη του :

Θεώρημα 1: *Οι ακέραιες λύσεις της διοφαντικής εξίσωσης* $x^5+y^5=z^5$ *είναι μόνο τα* (x,y,z) *όπου* $xyz=0$.

Το τελευταίο θεώρημα του Fermat χωρίζεται σε δύο περιπτώσεις :
Περίπτωση Ι: Κανένας από τους αριθμούς x,y,z δεν διαιρείται με n .
Περίπτωση ΙΙ: Ένας ακριβώς από τους x,y,z διαιρείται με n .

*Τμήμα Μαθηματικών, Πανεπιστήμιο Κρήτης

Σε αυτή την εργασία θα ασχοληθούμε με την περίπτωση II και όχι με την περίπτωση I. Η αλήθεια του θεωρήματος 1 στην περίπτωση I αποδεικνύεται χρησιμοποιώντας το παρακάτω θεώρημα :

Λήμμα 2 *(Sophie Germain)*: *Αν* $x^n+y^n=z^n$ *και* n *είναι πρώτος* ≥ 3 *και* $2n+1$ *είναι πρώτος, τότε ο* n *πρέπει να διαιρεί έναν από τους* x,y,z.

Πριν την απόδειξη του θεωρήματος 1 θα αναφέρουμε κάποια λήμματα, τα οποία θα μας χρειαστούν στην απόδειξη .

Λήμμα 3: *Αν* (x,y,z) *είναι μια ακέραια λύση της διοφαντικής εξίσωσης* $x^5+y^5=z^5$, *με* $xyz\neq 0$, *τότε* $\mu\kappa\delta(x,y)=\mu\kappa\delta(x,z)=\mu\kappa\delta(y,z)=1$.

Απόδειξη: Γενικά αν υπάρχει λύση της εξίσωσης θεωρώ την ελάχιστη, δηλαδή αυτή που έχει το $|x|$ ελάχιστο. Τότε μκδ(x,y,z)=1. Αν ήταν μκδ$(x,y)>1$ τότε θα υπήρχε πρώτος p τέτοιος ώστε: $p|x$ και $p|y$.Τότε όμως $x=px_1$ και $x=py_1$,όπου x_1,y_1 ακέραιοι .Από αυτό συνεπάγεται ότι $p^5|z^5$,δηλαδή $(p/z)^5\in\mathbb{Z}$ Οπότε συμπεραίνουμε ότι $(p/z)\in\mathbb{Z}$. Αντικαθιστούμε στην εξίσωση και έχουμε ότι: $p^5x_1^5+p^5y_1^5=p^5z_1^5$, δηλαδή $x_1^5+y_1^5=z_1^5$ και η (x_1,y_1,z_1) είναι μικρότερη λύση. Άτοπο ,άρα μκδ(x,y)=1. Με παρόμοιο τρόπο καταλήγουμε και ότι μκδ(x,z)=1, μκδ(z,y)=1.

Λήμμα 4: *Μπορούμε να υποθέσουμε ότι οι* x,y *είναι περιττοί και ο* z *είναι άρτιος.*

Απόδειξη: Από το λήμμα 3 είναι γνωστό ότι μκδ(x,y,z)=1. Οπότε τουλάχιστον δύο από τα x,y,z θα είναι περιττοί και ένα το πολύ θα είναι άρτιο. Αν δύο είναι περιττοί τότε το άλλο θα είναι άρτιο, αφού : (περιττός)+(περιττός)= (άρτιος) και επίσης (περιττός)-(περιττός)= (άρτιος). Αν ο z είναι άρτιος τότε δεν έχουμε να αποδείξουμε τίποτα. Υποθέτουμε ότι ο x είναι άρτιος. Υπάρχουν z', x' τέτοια ώστε :$z'=-z$ και $x'=-x$. Οπότε ο x' είναι άρτιος και : $(-1)^5(x')^5+y^5=(-1)^5(z')^5$. Άρα, $y^5+(z')^5=(x')^5$, το οποίο είναι της μορφής $x^5+y^5=z^5$, με z άρτιο. Ανάλογα μπορούμε να εργαστούμε αν υποθέσουμε ότι ο y είναι άρτιος.

Λήμμα 5: *Αν* $a,b\in\mathbb{Z}$, *μη μηδενικοί, και ικανοποιούν τα εξής :* $\mu\kappa\delta(a,b)$=1,*οι* a,b *είναι διαφορετικής αρτιότητας ,* $5|b$ *και* $5\not|a$ *και το* a^2-5b^2 *είναι πέμπτη δύναμη ακεραίου, τότε υπάρχουν* $c,d\in\mathbb{Z}$ *τέτοια ώστε :*
$a=c(c^4+50c^2d^2+125d^4)$ *και* $b=5d(c^4+10c^2d^2+5d^4)$, *όπου* c,d *μη μηδενικοί ακέραιοι με* $\mu\kappa\delta(c,d)$=1, *διφορετικής αρτιότητας και το 5 δεν διαιρεί το* c.

Απόδειξη: Θα παραγοντοποιήσουμε το a^2-5b^2. Ισχύει λοιπόν ότι :

$a^2 - 5b^2 = (a + b\sqrt{5})(a - b\sqrt{5})$. Θα εργαστούμε στον δακτύλιο $\mathbb{Z}[\omega]$, όπου $\omega = \frac{-1+\sqrt{5}}{2}$, $\omega^2 + \omega - 1 = 0$ [1].
Θα δείξουμε πρώτα ότι μκδ$(a + b\sqrt{5}, a - b\sqrt{5}) = 1$. Υποθέτουμε ότι μκδ$(a + b\sqrt{5}, a - b\sqrt{5}) = d \in \mathbb{Z}[(1 + \sqrt{5})/2]$ με $N(d) > 1$. Τότε θα υπάρχει *πρώτος* $\pi \in \mathbb{Z}[\omega]$, τέτοιος ώστε : $\pi|d$. Οπότε $\pi|2a$ και $\pi|2b\sqrt{5}$.
Το $\pi \not| 2$ και $\pi \not| \sqrt{5}$ [2]. Οπότε $\pi|a$ και $\pi|b$, το οποίο είναι άτοπο, διότι a, b πρώτοι μεταξύ τους.
Άρα μκδ$(a + b\sqrt{5}, a - b\sqrt{5})$=1.
Οπότε απο μονοσήμαντη ανάλυση του $Z[\omega]$ συμπεραίνουμε ότι τα $a+b\sqrt{5}, a-b\sqrt{5}$ είναι το καθένα πέμπτη δύναμη *ακεραίου* επί κατάλληλη μονάδα του δακτυλίου $Z[\omega]$. Οπότε υπάρχουν $u, v, k \in \mathbb{Z}$ τέτοια ώστε : $a + b\sqrt{5} = (u + v\omega)^5\omega^k$. Όμως κάθε ακέραιος μπορεί να γραφτεί στην μορφή $5q + r$ όπου $r = 0, 1, 2, 3$ ή 4. Άρα $(u+v\omega)^5\omega^k = ((u+v\omega)^5\omega^q)^5\omega^r$. Ο $((u+v\omega)^5\omega^q)^5$ είναι της μορφής $(u+v\omega)^5$, (με κατάλληλη αλλαγή της σημασίας των u, v). Οπότε, $a+b\sqrt{5} = (u+v\omega)^5\omega^r = C + D\omega$, (αν κάνουμε τις πράξεις)′ για κάποιους ακέραιους C, D. Άρα αρκεί να δειχτεί ότι, αν $b \equiv 0 \pmod 5$, τότε το r δεν μπορεί να είναι 1,2,3 ή 4.
Επειδή $a + b\sqrt{5} = (a + b) + 2b\omega$, έχουμε ότι $C = a + b \equiv 0 \pmod 5$ και $D = 2b \equiv 0 \pmod 5$. Έχουμε λοιπόν,
$r = 1$: Αναπτύσοντας το $(u + v\omega)^5\omega = C + D\omega$ παίρνουμε ότι $C \equiv 0 \pmod 5$, άτοπο.
$r = 2$: Αναπτύσοντας το $(u+v\omega)^5\omega^2 = C+D\omega$ έχουμε ότι $C \equiv u^5+2v^5 \equiv u+2v \pmod 5$ [3], $D \equiv 4u^5 + 3v^5 \equiv 4u + 3v \pmod 5$ [4]. Όμως $D \equiv 0 \pmod 5$, άρα $u \equiv 3v \pmod 5$. Αλλά τότε $C \equiv 0 \pmod 5$, το οποίο είναι άτοπο.
$r = 3, 4$: Αποκλείονται όπως η περίπτωση $r = 2$.
Μένει η περίπτωση $r = 0$: Είναι $C \equiv u + v, D \equiv v \pmod 2$. Αλλά $D = 2b$, άρα ο v είναι άρτιος, $v = 2d$. Άρα $u + v\omega = u + 2d\omega = (u - d) + d(2\omega + 1) = c + d\sqrt{5}$ [5],όπου $c = u - d$.
Άρα $a+b\sqrt{5} = (c+d\sqrt{5})^5 = c^5+5c^4d\sqrt{5}+50c^3d^2+50c^2d^3\sqrt{5}+125cd^4+25d^5\sqrt{5}$.
Άρα : $a = c^5 + 50c^3d^2 + 125cd^4 = c(c^4 + 50c^2d^2 + 125d^4)$ και
$b = 5c^4d + 50c^2d^3 + 25d^5 = 5d(c^4 + 10c^2d^2 + 5d^4)$. Τα c, d έχουν τις παρακάτω ιδιότητες :

---

[1] Στον $\mathbb{Z}[\omega]$ ισχύει η μονοσήμαντη ανάλυση. Μονάδες είναι τα $\pm\omega^n$, $n \in \mathbb{Z}$. $N(a + b\omega) = a^2 - ab - b^2$. Οι 2, $\sqrt{5} = 2\omega + 1$ είναι *πρώτοι*

[2] Επειδή το 2 είναι *πρώτος*, $\pi = 2u'$, όπου u' μονάδα του $\mathbb{Z}[\omega]$. Παίρνοντας νόρμες έχουμε ότι $4|(a + b\sqrt{5})(a - b\sqrt{5}) = a^2 - 5b^2$, άτοπο διότι οι a, b είναι διαφορετικής αρτιότητας. Αν $\pi|\sqrt{5}$ τότε π συνεταιρικός του 5, άρα $5|a$, άτοπο

[3] Μικρο Θεώρημα του Fermat : $x^p \equiv x \pmod p, p$ πρώτος

[4] Μικρο Θεώρημα του Fermat

[5] $2\omega + 1 = \sqrt{5}$

1. Μκδ(c,d)=1. Αυτό έπεται από το γεγονός ότι μκδ(a,b)=1

2. Οι c,d είναι ο ένας άρτιος και ο άλλος περιττός. Δεν γίνεται να είναι και οι δύο άρτιοι, διότι μκδ(c,d)=1. Επίσης δεν γίνεται να είναι και οι δύο περιττοί, διότι τότε οι a,b θα ήταν και οι δύο άρτιοι, το οποίο είναι αδύνατο.

3. Το 5 δεν διαιρεί το c. Αν το $5|c$ τότε $C \equiv 0 \pmod 5$, το οποίο είναι άτοπο.

Λήμμα 6: *Αν $a,b \in \mathbb{Z}$ και ικανοποιούν τα εξής : μκδ(a,b)=1, a,b περιττοί και οι δύο, $5|b$ και $5 \not| a$ και το $(a^2-5b^2)/4$ είναι πέμπτη δύναμη ακεραίου, τότε υπάρχουν μη μηδενικά $c,d \in \mathbb{Z}$ τέτοια ώστε :*
$a = c(c^4+50c^2d^2+125d^4)/16$ *και* $b = 5d(c^4+10c^2d^2+5d^4)/16$ *με μκδ$((c,d)$=1, c,d περιττοί και οι δύο και το 5 δεν διαιρεί το c.*

Απόδειξη: Η απόδειξη είναι όμοια με αυτή του λήμματος 5, αρκεί να εργαστούμε πάλι στο $\mathbb{Z}[(1+\sqrt{5})/2]$ και να εξετάσουμε το μκδ$(a+b\sqrt{5})/2, (a-b\sqrt{5})/2)$.

Λήμμα 7: *Δεν υπάρχουν $x,y,z \in \mathbb{Z}$ με $xyz \neq 0$ τέτοια ώστε $x^5+y^5=z^5$, μκδ(x,y)=μκδ(x,z)=μκδ(y,z)=1, x,y περιττοί, z άρτιος και $5|z$.*

Απόδειξη: Έστω ότι υπάρχουν τέτοια x,y,z. Για το z θα ισχύει : $z = 2^m5^nz'$ με $m \geq 1$, $n \geq 1$, μκδ$(z',2)$=1, μκδ$(z',5)$=1 και $2^{5m}5^{5n}(z')^5 = x^5+y^5$. Επειδή οι x,y είναι και οι δύο περιττοί έχουμε ότι οι $x+y, x-y$ είναι άρτιοι. Άρα υπάρχουν μη μηδενικά $p,q \in \mathbb{Z}$ [6] τέτοια ώστε : $x+y=2p$, $x-y=2q$ με p,q διαφορετικής αρτιότητας και μκδ(p,q)=1 [7]. Οπότε $x=p+q$ και $y=p-q$ και αντικαθιστώντας στην εξίσωση έχουμε :

$$z^5 = 2^{5m}5^{5n}(z')^5 = x^5+y^5 = (p+q)^5+(p-q)^5 = 2p(p^4+10p^2q^2+5q^4). \quad (1)$$

Από αυτό φαίνεται ότι $5|2p(p^4+10p^2q^2+5q^4)$. Άρα, είτε $5|2p$, είτε $5|(p^4+10p^2q^2+5q^4)$. Και στις δύο περιπτώσεις συμπεραίνουμε ότι $5|p$. Άρα υπάρχει μη μηδενικό $r \in \mathbb{Z}$ τέτοιο ώστε $p=5r$. Ο μκδ(p,r)=1, αφού μκδ(p,q)=1. Επίσης οι r, q είναι διαφορετικής αρτιότητας, αφού το ίδιο ισχύει και για τους p, q. Αντικαθιστώντας στην 1 έχουμε :

$$z^5 = 2^{5m}5^{5n}(z')^5 = 2 \cdot 5^2r(q^4+50q^2r^2+125r^4). \quad (2)$$

Από αυτό έχουμε ότι $5^{5n}|2 \cdot 5^2r(q^4+50q^2r^2+125r^4)$, δηλαδή $5^{5n-2}|2r(q^4+50q^2r^2+125r^4)$. Επειδή 5 δεν διαιρεί το q, [8] το 5 δεν διαιρεί το $(q^4+50q^2r^2+$

[6] Θα ειναι μη μηδενικά διότι διαφορετικά μκδ$(x,y) \neq 1$

[7] Είναι γνωστό ότι όταν οι x,y είναι περιττοί, πρώτοι μεταξύ τους, τότε μκδ$(x+y,x-y)$=2

[8] $5|p$ και μκδ(p,q)=1

$125r^4$). Οπότε $5|2r$, άρα $5|r$. Θέτουμε

$$q^4 + 50q^2r^2 + 125r^4 = t, \;\; q^2 + 25r^2 = a, \;\; 10r^2 = b$$

. Έτσι έχουμε ότι $t = a^2 - 5b^2$ και λόγω της 2

$$z^5 = 2 \cdot 5^2 rt. \tag{3}$$

Για τα r, t ισχύουν τα εξής :

(i) μκδ$(a, b) = 1$ (βλ. σχόλια 1.1).

(ii) Ο $5|a$ και $5 \not| b$.
Αφού $b = 10r^2$ έχουμε αμέσως ότι $5|b$. Το 5 όμως δεν διαιρεί το a διότι από (i) έχουμε ότι μκδ(a,b)=1.

(iii) Ο b είναι άρτιος και ο a είναι περιττός.
Αυτό διότι $2|b = 10r^2$ ενώ το 2 δεν διαιρεί το a αφού μκδ(a,b)=1.

(iv) μκδ$(2 \cdot 5r^2,t)$=1 (βλ. σχόλια 1.2).

Λόγω της (3) και της (iv) μπορούμε να συμπεράνουμε ότι τα t ,$2 \cdot 5^2 r$ είναι πέμπτες δυνάμεις ακεραίων. Όμως $t = a^2 - 5b^2$, άρα λόγω των $(i) - (iii)$ και του λήμματος 5, συμπεραίνουμε ότι ότι οδηγηθήκαμε στην εξής κατάσταση :

$$(*) \begin{cases} a = c(c^4 + 50c^2d^2 + 125d^4) \text{ και } b = 5d(c^4 + 10c^2d^2 + 5d^4) \\ c, d \text{ μη μηδενικοί, πρώτοι μεταξύ τους, διαφορετικής αρτιότητας και } 5 \not| c \\ a^2 - 5b^2 = \text{πέμπτη δύναμη.} \end{cases}$$

Έστω $a' = c^2 + 5d^2$, $b' = 2d^2$. Οι a', b' έχουν τις ακόλουθες ιδιότητες :

(a) μκδ(a',b')=1 (βλ. σχόλια 1.3).

(b) Ο $5|b'$, $5 \not| a'$.
Έχουμε δείξει ότι $5|r$. Επειδή $b = 10r^2$ [9], έπεται ότι $5^3|b$. Άρα $5^2|d$, οπότε $5|u' = 2d^2$. Το 5 δεν γίνεται να διαιρεί το a' διότι απο (a) μκδ(a',b')=1.

[9] Από το (iv)

(c) Τα a', b'είναι διαφορετικής αρτιότητας.
Το a' είναι άρτιος εξ ορισμού. Οπότε το b' θα είναι περιττός, αφού απο (a) μκδ(a',b')=1.

(d) Το $a'^2-5b'^2 = c^4+10c^2d^2+5d^4$ είναι πέμπτη δύναμη ακεραίου (βλ. σχόλια 1.4).

Από τις ιδιότητες $(a)-(d)$ και χρησιμοποιώντας το λήμμα 5 για το $a'^2-5b'^2$ έχουμε ότι :
$c^2+5d^2 = a' = c'(c'^4+50c'^2d'^2+125d'^4)$ και $2d^2 = b' = 5d'(c'^4+10c'^2d'^2+5d'^4)$ για κατάλληλους μη μηδενικούς ακεραίους c', d', διαφορετικής αρτιότητας, όπου μκδ(c',d')=1 και το 5 δεν διαιρεί το c. Επίσης $5|d'$, διότι $5^2|2d^2$ [10].
Έχουμε ότι $(2\cdot 5^8)(2d^2) = 2^2 5^8 d^2 = (2\cdot 5^4 d)^2$. Ξέρουμε ότι το $(2\cdot 5^4 d)$ είναι πέμπτη δύναμη ακεραίου. Οπότε και το $(2\cdot 5^4 d)^2$ θα είναι πέμπτη δύναμη ακεραίου.
Επίσης το $2\cdot 5^9 d'(c'^4+10c'^2d'^2+5d'^4)$ είναι πέμπτη δύναμη ακεραίου διότι :
$2\cdot 5^9 d'(c'^4+10c'^2d'^2+5d'^4) = (2\cdot 5^8)(5d'(c'^4+10c'^2d'^2+5d'^4) = (2\cdot 5^8)(2d^2)$, το οποίο είναι πέμπτη δύναμη ακεραίου.
Ισχύει ότι ο μκδ$(2\cdot 5^9 d', (c'^4+10c'^2d'^2+5d'^4))$=1.
Άρα επανερχόμαστε στην κατάσταση **(*)** τώρα όμως με τα a', b', c', d' στην θέση των a, b, c, d.
Επιπλέον $0 < d' < d$. Πράγματι,
$25d'^5 \leq 5d'(c'^4+10c'^3d'^2+5d'^4) = 2d^2$ [11]. Οπότε, $25d'^5 \leq 2d^2$, δηλαδή $d' \leq \sqrt[5]{2d^2/25}$. Όμως $\sqrt[5]{2d^2/25} < d$, άρα $d' < d$.
Συνεχίζοντας όσες φορές θέλουμε αυτή την διαδικασία θα επιστρέφουμε στην κατάσταση (*) και τη θέση του αρχικού d θα παίρνουν νέα $d', d'', \cdots$, όπου $1 \leq \cdots < d'' < d' < d$. Αλλά έτσι έχουμε άπειρη κάθοδο στους φυσικούς αριθμούς, άτοπο.

Λήμμα 8: *Δεν υπάρχουν $x,y,z\in\mathbb{Z}$ με $xyz\neq 0$ τέτοια ώστε $x^5+y^5=z^5$, μκδ(x,y)=μκδ(x,z)=μκδ(y,z)=1, x, y περιττοί, z άρτιος και $5|x$ ή $5|y$.*

Απόδειξη: Έστω ότι υπάρχουν τέτοια x,y,z .Υποθέτουμε χωρίς βλάβη της γενικότητας ότι $5|x$. Επειδή το $5|x$ ξέρουμε ότι υπάρχουν $n\in\mathbb{N}$ και $x'\in\mathbb{Z}$, τέτοια ώστε $x = 5^n x'$ με $n\geq 1$, μκδ$(x',5)$=1. Άρα $5^{5n}x'^5 = y^5+z^5$. Πολλαπλασιάζω με 2^5 και στα δύο μέλη και έχω : $(2^5)(5)^{5n})x'^5 = 2^5(y^5+z^5)$. Έστω $p = y+z$, $q = y-z$. Ισχύουν οι παρακάτω ιδιότητες :

(a) Οι p, q είναι και οι δύο περιττοί.

[10] Από το (b)
[11] $c', d' \neq 0$, οπότε $c', d' \geq 1$

Αυτό διότι ο y είναι περιττός και ο z είναι άρτιος.

(b) Μκδ(p,q)=1.
Διαφορετικά θα υπήρχε πρώτος f τέτοιος ωστε $f|p$ και $f|q$. Καταλήγω όμως σε άτοπο διότι μκδ(y,z)=1.

(c) $p,q \neq 0$ [12].

(d) $(2^5)(5)^{5n})x'^5 = 2^5(y^5+z^5) = (2y)^5+(2z)^5 = (p+q)^5+(p-q)^5 = 2p(p^4+10p^2q^2+5q^4)$

(e) $5|p$.
Από το (d) συνεπάγεται ότι $5|2p(p^4+10p^2q^2+5q^4)$. Άρα είτε $5|2p$ είτε $5|(p^4+10p^2q^2+5q^4)$. Άν $5|2p$ τότε $5|p$.Αν $5|(p^4+10p^2q^2+5q^4)$ τότε πάλι έπεται ότι $5|p$.
Άρα υπάρχει $r \in \mathbb{Z}$ τέτοιο ώστε $p=5r$.

(f) Μκδ(r,q)=1.
Αυτό διότι από το (b) μκδ(p,q)=1.

(g) Τα q,r είναι και τα δύο περιττοί [13].
Αντικαθιστώντας το $p=5r$ έχουμε :
$(2^5)(5)^{5n})x'^5 = 2p(p^4+10p^2q^2+5q^4) = 2\cdot 5^2 r(q^4+50q^2r^2+125r^4)$. Από αυτό έχουμε ότι :

(h) $5|r$ (βλ. σχόλια 2.1).
Αυτό διότι $5^{5n}|2\cdot 5^2 r(q^4+50q^2r^2+125r^4$. Δηλαδή $5^{5n-2}|2r(q^4+50q^2r^2+125r^4)$. Επειδή $n \geq 1$ $5n \geq 5$, το $5n > 2$. Το 5 δεν διαιρεί το $q^4+50q^2r^2+125r^4$ [14]. Άρα, σύμφωνα με τα προηγούμενα, $5|\|2r$,οπότε $5|r$.

Έστω

$$q^4+50q^2r^2+125r^4 = t', q^2+25r^2 = a', 10r^2 = b'.$$

Σημειώνουμε ότι $t' = a'^2-5b'^2$. Τα a', b' είναι άρτιοι. Άρα υπάρχουν $a,b \in \mathbb{Z}$ τέτοια ώστε : $a=(1/2)a'$ και $b=(1/2)b'$. Έστω : $t=(1/4)t' = (1/4)(a'^2-5b'^2) = [(1/2)a']^2-5[(1/2)b']^2 = a^2-5b^2$. Τα a,b έχουν τις ακόλουθες ιδιότητες :

[12] Αν $y+z=0$ ή $y-z=0$ τότε $y=z$ ή $y=-z$ το οποίο είναι αδύνατο
[13] Περιττός διαιρούμενος με το 5 =περιττός
[14] Το $5|p$ και μκδ(p,q)=1

(i) μκδ(a,b)=1.

(ii) $5|b$ και $5\not|a$.
Από τον ορισμό του b έπεται ότι $5|b$. Το 5 δεν διαιρεί το a διότι από το (i) μκδ(a,b)=1.

(iii) Τα a,b είναι και τα δύο περιττοί.
Το b είναι περιττός διότι από το (g) το r είναι περιττός. Το a είναι περιττός επειδή από το (g) τα q,r είναι και τα δύο περιττοί [15].

(iv) $(5^2r)(t/4)$ =πέμπτη δύναμη ακεραίου.
Από πριν : $(2^5)(5)^{5n})x'^5 = 2\cdot 5^2r(q^4+50q^2r^2+125r^4)$. Άρα $(2^5)(5)^{5n})x'^5 = 2\cdot 5^2rt' = 2^3\cdot 5^2rt$. Διαιρώντας και τα δύο μέλη με 2^5 : $5^{5n}x'^5 = (5^2rt)/4$.

(v) Μκδ$(5^2r,t/4)$=1.
Υποθέτουμε το αντίθετο και καταλήγουμε σε άτοπο χρησιμοποιώντας το ότι μκδ(r,q)=1.

(vi) $t/4 = (1/4)(a^2-5b^2)$ =πέμπτη δύναμη ακεραίου.
Αυτό έπεται απο τα (iv), (v).

Σύμφωνα με τα παραπάνω και εφαρμόζοντας το λήμμα 6 συμπεραίνουμε ότι : $a = c(c^4+50c^2d^2+125d^4)/16$ και $b = 5d(c^4+10c^2d^2+5d^4)/16$, όπου c,d μη μηδενικοί ακέραιοι, με μκδ(c,d)=1, c,d και οι δύο περιττοί και $5\not|c$. Επίσης $5/d$, διότι $5^3/b$ [16] και 5 δεν διαιρεί το $c^4+10c^2d^2+5d^4$.

Επίσης : $5^3b = (1/4)(5^4d)[([c^2+5d^2]/2)^2-5d^4]$ και 5^3b είναι πεμπτη δύναμη [17].
Λόγω του ότι τα c,d είναι και τα δύο περιττοί, έπεται ότι :
$[(c^2+5d^2)/2]^2-5d^4 \equiv 0 \pmod 4$.
Εύκολα αποδεικνύεται ότι μκδ$(5^4d,(1/4)[[(c^2+5d^2)/2]^2-5d^4])$ =1.
Οπότε, τα 5^4d και $(1/4)[[(c^2+5d^2)/2]^2-5d^4]$ είναι το καθένα πέμπτη δύναμη ακεραίου.
Εφαρμόζοντας λοιπόν το λήμμα 6, έπεται ότι: :
$(c^2+5d^2)/2 = c'(c'^4+50c'^2d'^2+125d'^4)/16$ και $d^2 = 5d'(c'^4+10c'^2d'^2+5d'^4)/16$
, όπου c',d' μη μηδενικοί ακέραιοι, περιττοί και οι δύο και $5\not|c'$.
Επίσης προκύπτει ότι $5|d'$, διότι $5^2|d^2$ και 5 δεν διαιρεί το $c'^4+10c'^2d'^2+5d'^4$.
Κάνοντας πράξεις παρατηρούμε ότι :

[15] $(\text{περιττός})^2 \equiv 1 \pmod 4$

[16] Από (h), $b=(1/2)b', b'=10r^2$ και $5/r$

[17] $b=(1/2)b'=5r^2$. Απο (iv) και (v) έχουμε ότι 5^2r =πεμπτη δύναμη. Οπότε $(5^2r)^2 = 5^4r^2 = 5^3b$ =πέμπτη δύναμη

$(5^8)(d^2) = (1/4)(5^9 d')[([c'^2 + 5d'^2]/2)^2 - 5(d'^2)^2]$.
Εύκολα πάλι αποδεικνύεται ότι μκδ$(5^9 d', (1/4)([c'^2 + 5d'^2]/2)^2 - 5(d'^2)^2)$=1.
Επίσης γνωρίζουμε ότι $5^8 d^2$ είναι πέμπτη δύναμη ακεραίου, αφού το $5^4 d$ είναι πέμπτη δύναμη ακεραίου.
Οπότε πάλι συμπεραίνουμε ότι τα $5^9 d'$ και $(1/4)([c'^2 + 5d'^2]/2)^2 - 5(d'^2)^2)$ είναι το καθένα πέμπτη δύναμη ακεραίου.
Έπεται ότι $1 \leq d' \leq d$, διότι : $25d'^5 < 16d^2$, από τον ορισμό των c', d'. Έπεται ότι $d' < d$,διότι διαφορετικα, αφού και οι δύο είναι μη μηδενικοί ακέραιοι, θα ήταν $25d'^5 \leq 16d^2$, άτοπο. Μπορούμε να επαναλάβουμε την ίδια διαδικασία όσες φορές θέλουμε. Συνεχίζοντας όσες φορές θέλουμε αυτή την διαδικασία τη θέση του αρχικού d θα παίρνουν νέα $d', d'', \cdots$, όπου $1 \leq \cdots < d'' < d' < d$. Αλλά έτσι έχουμε άπειρη κάθοδο στους φυσικούς αριθμούς, άτοπο.

Επανερχόμαστε τώρα στην απόδειξη του θεωρήματος 1.
Η περιπτωση I αποδείχτηκε, όπως είπαμε, στην αρχή της εργασίας αυτής. Η περιπτωση II χωρίζεται σε δύο υποπεριπτώσεις :

1. Το 5 διαιρεί το z .
2. Το 5 δεν διαιρεί το z .

   Η αλήθεια του θεωρήματος 1, στην υποπερίπτωση 1, αποδεικνύεται από το λήμμα 7 και στην υποπερίπτωση 2 απο το λήμμα 8.

2 Σχόλια

1. **Σχόλια που αναφέρονται στην απόδειξη του λήμματος 7.**

   1.1 μκδ$(a, b) = 1$.
   Αν ηταν μκδ(a,b)>1 τότε θα υπήρχε πρώτος f τέτοιος ώστε $f|a$ και $f|b$. Αφού $f|b$ έχουμε ότι $f|10r^2$.Άρα για τον πρώτο f έχουμε τις ακόλουθες τρεις πιθανές περιπτώσεις :
   Περίπτωση 1: $f = 2$.
   Περίπτωση 2: $f = 5$.
   Περίπτωση 3: f/r.
   Η περίπτωση 1 απορρίπτεται αφού ο a είναι περιττός. Ο a είναι περιττός διότι οι p, r όπως αναφέραμε είναι ο ένας άρτιος και ο άλλος περιττός. Η περίπτωση 2 απορρίπτεται αφού ο f δεν μπορεί να είναι 5 διότι $5|p$ και μκδ(p,q)=1. Αυτό σημαίνει ότι ο 5 δεν διαιρεί το q και άρα ο 5

δεν διαιρεί το $a = q^2 + 25r^2$.
Η περίπτωση 3 απορρίπτεται αφού, αν ο f διαιρεί το r και ο f διαιρεί το a τότε ο f θα διαιρεί το q, [18] αλλά αυτό είναι άτοπο, διότι μκδ(r,q)=1.
Άρα τετοιος πρώτος δεν γίνεται να υπάρχει.

1.2 μκδ($2 \cdot 5r^2$,t)=1.
Η απόδειξη αυτού είναι η εξής :
Έστω ότι υπάρχει πρώτος f που διαιρεί και τους δύο. Το $f \neq 2$ διότι ο t είναι περιττός [19]. Το $f \neq 5$ διότι το t δεν διαιρείται με 5, αφού στην απόδειξη της περίπτωσης 2 της ιδιότητας (i) για τα a, b, είχαμε δείξει ότι ο 5 δεν διαιρεί το q. Τέλος ο f δεν διαιρεί το r διότι μκδ(r,t)=1.
Άρα τέτοιος πρώτος δεν γίνεται να υπάρχει.

1.3 μκδ(a',b')=1.
Έστω ότι δεν ισχύει. Άρα υπάρχει πρώτος f τέτοιος ώστε : $f|c+5d^2$ και $f|2d^2$. Οπότε θα έχουμε τρεις πιθανές περιπτώσεις :
Περίπτωση 1: $f = 2$.
Περίπτωση 2: $f = 5$.
Περίπτωση 3: $f|b$ και $f|c$.
Η περίπτωση 1 απορρίπτεται αφού $a' = c^2 + 5d^2$ είναι περιττός[20].
Η περίπτωση 2 απορρίπτεται αφού ο 5 δεν διαιρεί το c, λόγω των υποθέσεων για τα c, d.
Η περίπτωση 3 απορρίπτεται αφού μκδ(c,d)=1.

1.4 Το $a'^2 - 5b'^2 = c^4 + 10c^2d^2 + 5d^4$ είναι πέμπτη δύναμη ακεραίου (βλ. σχόλια 1.4).
Η απόδειξη αυτού είναι η εξής :
Έχουμε ότι $2 \cdot 5^2r$ είναι πέμπτη δύναμη ακεραίου, άρα και ο $(2 \cdot 5^2r)^2$ είναι πέμπτη δύναμη ακεραίου. Όμως :
$(2 \cdot 5^2r)^2 = 2 \cdot 5^3 \cdot 10r^2 = (2 \cdot 5^3)b = (2 \cdot 5^3)[5d(c^4 + 10c^2d^2 + 5d^4)] = (2 \cdot 5^4d)(c^4 + 10c^2d^2 + 5d^4)$. Θα δείξουμε τώρα ότι μκδ($2 \cdot 5^4d$,$c^4 + 10c^2d^2 + 5d^4$)=1.
Αν αυτό δεν ισχυεί, τότε θα υπάρχει ένας πρωτος f τέτοιος ώστε : f¸$2 \cdot 5^4d$ και f¸$c^4 + 10c^2d^2 + 5d^4$. Υπάρχουν τρεις πιθανές περιπτώσεις :
Περίπτωση 1: $f = 2$.
Περίπτωση 2: $f = 5$.
Περίπτωση 3: f/c και f/d .
Με ακριβώς τον ίδιο τρόπο, όπως και πριν, αποκλείονται και οι τρεις

[18] Αφού $a = q^2 + 25r^2$
[19] $t = (q^2 + 25r^2)^2 - 5(10r^2)^2$ και q, r ο ένας άρτιος και ο άλλος περιττός
[20] Τα c, d είναι ο ένας άρτιος και ο άλλος περιττός

περιπτώσεις. Οπότε, συμπεραίνουμε ότι :
$2 \cdot 5^4 d$ και $c^4 + 10c^2d^2 + 5d^4$ είναι ο καθένας πέμπτη δύναμη ακεραίου.

2. **Σχόλια που αναφέρονται στην απόδειξη του λήμματος 8.**

2.1 $5|r$.
Αυτό διότι $5^{5n}|2 \cdot 5^2 r(q^4 + 50q^2r^2 + 125r^4$. Δηλαδή $5^{5n-2}|2r(q^4 + 50q^2r^2 + 125r^4)$. Επειδή $n \geq 1$ $5n \geq 5$, το $5n > 2$. Το 5 δεν διαιρεί το $q^4 + 50q^2r^2 + 125r^4$ [21]. Άρα, σύμφωνα με τα προηγούμενα, $5|||2r$,οπότε $5|r$.

Αναφορές

[1] Harold M. Edwards, Springer-Verlag, Fermat's Last Theorem

[2] Simon Singh, Π. Τραυλός, Το Τελευταίο Θεώρημα του Fermat

[21] Το $5|p$ και μκδ(p, q)=1