Στοιχεία Θεωρίας αριθμών

Υπενθύμιση: αν $a, b \in \mathbb{R}$ με $a \neq b$ και $n \in \mathbb{N}$, τότε

$$\frac{a^n - b^n}{a - b} = \sum_{i=0}^{n-1} a^i b^{n-1-i}, \tag{1}$$

δηλαδή

$$\frac{a^n - b^n}{a - b} = b^{n-1} + ab^{n-2} + a^2 b^{n-3} + \ldots ba^{n-2} + a^{n-1}.$$

Αξίζει να παρατηρήσουμε ότι το πολυώνυμο στο δεξί μέλος της προηγούμενης σχέσης είναι **ομογενές βαθμού** $n-1$, δηλαδή οι δυνάμεις στα μονώνυμα που το αποτελούν αθροίζουν στο $n-1$.

Ορισμός 0.2.1. *Ένας φυσικός αριθμός $n > 1$ ο οποίος δεν είναι το γινόμενο δύο μικρότερων φυσικών αριθμών λέγεται* ***πρώτος****.*
Ένας φυσικός αριθμός $n > 1$ ο οποίος δεν είναι πρώτος λέγεται ***σύνθετος****.*

Δηλαδή, ενας σύνθετος αριθμός είναι ένας θετικός ακέραιος ο οποίος δε γράφεται ως το γινόμενο δύο μικρότερων θετικών ακέραιων, δηλαδή ισοδύναμα, είναι ένας θετικός ακέραιος ο οποίος έχει τουλάχιστον ένα διαιρέτη διαφορετικό από τη μονάδα αλλά και διαφορετικό από τον εαυτό του.

Έτσι, κάθε θετικός ακέραιος είναι είτε σύνθετος, είτε πρώτος είτε η μονάδα.

Υπάρχουν άπειροι στο πλήθος πρώτοι αριθμοί.

Θεώρημα 0.2.1 (Ευκλείδειος αλγόριθμος διαίρεσης)**.**
Για κάθε $a > 0$ και $b \in \mathbb{R}$, υπάρχουν μοναδικοί αριθμοί p, r έτσι ώστε

$$\boxed{b = qa + r, \quad 0 \leq r < a}\,.$$

Αν a, b, p, q, r όπως πιο πάνω, τότε, ο b καλείται ο **διαιρέτης**, a ο **διαιρετέος**, q το **πηλίκο** (της διαίρεσης) και r το **υπόλοιπο** (της διαίρεσης).

Θεώρημα 0.2.2 (Θεμελιώδες Θεώρημα της αριθμητικής)**.**
Κάθε $n \in \mathbb{Z},\ n > 1$ γράφεται κατά μοναδικό τρόπο ως γινόμενο δυνάμεων πρώτων αριθμών. Δηλαδή

$$n = \prod_{i=1}^{k} p_i^{n_i} = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_k^{n_k},$$

όπου p_i πρώτοι με $p_1 < p_2 < \ldots < p_k$ και $n \in \mathbb{Z}_+$.

Η πιο πάνω (μοναδική) αναπαράσταση του n λέγεται **η κανονική αναπαράσταση του n ως γινόμενο πρώτων.**

Πρόταση 0.2.1. *Μεταξύ τριών διαδοχικών ακεραίων αριθμών, μόνο ένας είναι πολλαπλάσιο του 3.*

Απόδειξη. Έστω $n-2, n-1, n$ τρείς (διαδοχικοί) ακέραιοι. Από τη διαίρεση του n με τον αριθμό 3 έχουμε:

$$n = 3q + r, \quad 0 \leq r < 3,$$

δηλαδή

$$n = 3q + r, \quad r = 0, 1, 2.$$

Αν $r = 0$, τότε $n = 3q$ και αρα ο 3 διαιρεί το n, αν $r = 1$, τότε $n = 3q + 1 \Rightarrow n - 1 = 3q$, δηλαδή ο ο 3 διαιρεί το $n-1$ και αν $r = 2$, τότε $n = 3q + 2 \Rightarrow n - 2 = 3q$, δηλαδή ο ο 3 διαιρεί το $n-2$. □

ΕΦΑΡΜΟΓΗ Να δειχθεί ότι για κάθε $n \in \mathbb{N},\ n \geq 3$ οι αριθμοί $2^n - 1$ και $2^n + 1$ δεν μπορεί να είναι ταυτόχρονα πρώτοι αριθμοί.

Απάντηση. Οι αριθμοί $2^n - 1,\ 2^n$ και $2^n + 1$ είναι διαδοχικοί ακέραιοι αριθμοί. Συνεπώς, από την προηγούμενη Πρόταση, μόνο ένας από αυτούς μπορεί να είναι πολλαπλάσιο του 3. Αλλά, ο 2^n δεν είναι πολλαπλάσιο του 3, διότι αυτή είναι και η κανονική του γραφή (η οποία είναι μοναδική). Άρα, είτε ο $2^n - 1$ είτε ο $2^n + 1$ είναι πολλαπλάσιο του 3 και το συμπέρασμα έπεται. □

2ος τρόπος: Υποθέτουμε ότι οι αριθμοί $2^n - 1$ και $2^n + 1$ είναι πρώτοι αριθμοί. Είναι

$$(2^n - 1)(2^n + 1) = 2^{2n} - 1 = 4^n - 1 = (4 - 1)\sum_{i=0}^{n-1} 4^i \cdot 1^{n-1-i} = 3\sum_{i=0}^{n-1} 4^i,$$

δηλαδή ο αριθμός $(2^n - 1)(2^n + 1)$ είναι πολλαπλάσιο του 3, άτοπο, αφού το γινόμενο $(2^n - 1)(2^n + 1)$ ως γινόμενο πρώτων αριθμών έχει μόνο 4 κανονικούς θετικούς διαιρέτες και αφού $n \geq 3$, ο 3 δεν είναι ένας από αυτούς. □

Ορισμός 0.2.2. *Οι αριθμοί $M_n = 2^n - 1,\ n \in \mathbb{N}$ καλούται* ***οι αριθμοί του Mersenne****.*

Έχουν πάρει το όνομά τους από το Γάλλο Marin Mersenne, ο οποίος τους μελέτησε κατά την αρχή του 17ου αιώνα.
Αν ο n είναι σύνθετος αριθμός, τότε και ο M_n είναι σύνθετος. Συνεπώς, οι πρώτοι αριθμοί του Mersenne M_p είναι οι πρώτοι αριθμοί οι οποίοι γράφονται ως $2^p - 1$, για κάποιο πρώτο αριθμό p.

Πρόταση 0.2.2. *Αν ο αριθμός M_n είναι πρώτος, τότε ο n είναι πρώτος.*

Απόδειξη. Έστω ότι ο M_n είναι πρώτος και υποθέτουμε ότι ο n δεν είναι πρώτος. Τότε $n = km$, για κάποιους $k, m \in \mathbb{N},\ 1 < k, m < n$. Είναι

$$M_n = 2^{km} - 1 = (2^k - 1)\sum_{i=0}^{m-1} 2^{ki}.$$

Αλλά, οι αριθμοί $2^k - 1$ και $\sum_{i=0}^{m-1} 2^{ki}$ είναι > 1, συνεπώς, από την πιο πάνω σχέση, έπεται ότι ο $M_n = 2^{km} - 1$ έχει κανονικούς (θετικούς) διαιρέτες, άτοπο, αφού M_n πρώτος. □

Το αντίστροφο της προηγούμενης Πρότασης δεν ισχύει. Οι M_{67} και M_{257} δεν είναι πρώτοι.

Γενικά, ο έλεγχος για να αποφανθούμε αν ένας αριθμός είναι πρώτος μπορεί να είναι ένα τρομερά δύσκολο έργο. Στην περίπτωση που οι αριθμοί είναι ειδικής μορφής, όπως π.χ. $2^n - 1,\ 2^n + 1$, είδαμε κριτήριο πότε είναι πρώτοι. Με κίνητρο τα πιο πάνω αποτελέσματα, μπορούμε να δείξουμε το ακόλουθο:

Θεώρημα 0.2.3. *Έστω $a > 1$ και $n \in \mathbb{N},\ n \geq 2$. Τότε*
(α) *Αν ο $a^n - 1$ είναι πρώτος, τότε ο $a = 2$ και n πρώτος αριθμός.*
(β) *Αν ο $a^n + 1$ είναι πρώτος, τότε ο a είναι άρτιος αριθμός και $n = 2^k$, για κάποιο $k \in \mathbb{N},\ k \geq 1$.*

Απόδειξη. Αποδεικνύουμε μόνο το **(α)**.
Έστω ότι $a > 2$. Τότε $a + 1 > 3$ και αφού $n > 1$, τότε

$$\sum_{i=0}^{n-1} a^i = a^{n-1} + a^{n-2} + \ldots + a + 1 > a + 1 > 3.$$

Επίσης, $a > 2 \Rightarrow a - 1 > 1$ και αρα από την (1), έχουμε ότι ο αριθμός $a^n - 1$ γράφεται ως γινόμενο δύο αριθμών > 1, άρα δεν είναι πρώτος, άτοπο. Άρα, $a = 2$. Ο δεύτερος ισχυρισμός έπεται από την

προηγούμενη Πρόταση.
Εναλλακτικά, έστω ότι ο $2^n - 1$ είναι πρώτος και υποθέτουμε ότι ο n δεν είναι πρώτος. Τότε $n = km$, για κάποιους $k, m \in \mathbb{N},\ 1 < k, m < n$. Είναι

$$2^n - 1 = 2^{km} - 1 = (2^m)^k - 1$$

και άρα, από πρίν πρέπει $2^m = 2 \Rightarrow m = 1$, άτοπο. □

▶ **Παράδειγμα 0.2.1.** *Να δειχθεί ότι αν ο n είναι σύνθετος αριθμός, τότε έχει (τουλάχιστον ένα) παράγοντα πρώτο αριθμό $p \leq \sqrt{n}$.*

Απάντηση. Έστω n σύνθετος αριθμός και υποθέτουμε ότι κάθε παράγοντας στην ανάλυσή του σε γινόμενο πρώτων αριθμών είναι $> \sqrt{n}$. Γράφουμε $n = mp$, για κάποιον πρώτο αριθμό p. Αφού n σύνθετος, τότε $m \neq 1$ και από την υπόθεση (αφού κάθε πρώτος παράγοντας του m είναι και πρώτος παράγοντας του n) κάθε πρώτος παράγοντας του m είναι $> \sqrt{n}$ και αρα $m > \sqrt{n}$. Τότε

$$n = pm > \sqrt{n} \cdot \sqrt{n} = n,$$

άτοπο.

Λήμμα 0.2.1.

(i) Αν $a|b$ και $b|c$, τότε $a|c$, δηλ. η σχέση διαιρετότητας είναι μεταβατική.

(ii) Αν $d|a$ και $d|b$, τότε $d|(sa + tb)$. Γενικότερα, αν ένας αριθμός διαιρεί κάποιους άλλους αριθμούς, τότε διαιρεί και κάθε γραμμικό συνδυασμό των αριθμών αυτών.

Απόδειξη.

(i) Έστω $a|b$ και $b|c$. Τότε $a \neq 0$ και $a|b \Rightarrow b = ka$ για κάποιο $k \in \mathbb{Z}$ και $b|c \Rightarrow c = \ell b$ για κάποιο $\ell \in \mathbb{Z}$. Τότε, $c = (k\ell)a \Rightarrow a|c$.

(ii) Έστω $d|a$ και $d|b$. Τότε $d \neq 0$ και $d|a \Rightarrow a = kd$ για κάποιο $k \in \mathbb{Z}$ και $d|b \Rightarrow b = \ell d$ για κάποιο $\ell \in \mathbb{Z}$. Άρα, $sa + tb = skd + t\ell d = (sk + t\ell)d \Rightarrow d|(sa + tb)$.

□

Λήμμα 0.2.2. *Αν $a, b \in \mathbb{Z}$ με $\mu\kappa\delta(a, b) = 1$ και $c \in \mathbb{Z}_*$, τότε $\mu\kappa\delta(a, bc) = \mu\kappa\delta(a, c)$.*

Απόδειξη. Έστω $d \in \mathbb{Z}$ με $\begin{cases} d|a \\ d|c \end{cases} \Rightarrow \begin{cases} d|a \\ d|(bc) \end{cases} \Rightarrow$ κάθε κοινός διαιρέτης των a και c είναι και κοινός διαιρέτης των a και bc. Έστω λοιπόν d κοινός διαιρέτης των a και bc. Τότε $d \in \mathbb{Z}$ με $\begin{cases} d|a \\ d|c \end{cases} \Rightarrow \begin{cases} d|(ac) \\ d|(bc) \end{cases} \Rightarrow d|\mu\kappa\delta(ac, bc)$. Αλλά, $\mu\kappa\delta(ac, bc) = |c|\underbrace{\mu\kappa\delta(a, b)}_{=1} = |c|$. □

Λήμμα 0.2.3. *Αν $a, b \in \mathbb{Z}$ με $a \neq 0$, τότε για κάθε $c \in \mathbb{Z}$, τότε*

$$\mu\kappa\delta(a, b) = \mu\kappa\delta(a, b + ca).$$

▶ **Παράδειγμα 0.2.2.** *Να βρεθεί ο* $\mu\kappa\delta(25, 60)$.

Λύση

$$\begin{aligned}\mu\kappa\delta(25,60) &= \mu\kappa\delta(25, 25\cdot 2+10)\\ &= \mu\kappa\delta(25,10) = \mu\kappa\delta(10,25)\\ &= \mu\kappa\delta(10, 2\cdot 10+5) = \mu\kappa\delta(10,5)\\ &= \mu\kappa\delta(5,10) = \mu\kappa\delta(5, 2\cdot 5)\\ &= \mu\kappa\delta(5,5) = 5\end{aligned}$$

(η προτελευταία ισότητα από το Λήμμα 0.2.2 ή από το ότι $\mu\kappa\delta(5, 2\cdot 5) = \mu\kappa\delta(5, 2\cdot 5+0) = \mu\kappa\delta(5,0)$).

Λήμμα 0.2.4. *Έστω* $a, b, c \in \mathbb{Z}$. *αν* $\mu\kappa\delta(a,b) = 1$ *και* $a|(bc)$, *τότε* $a|c$.

Απόδειξη. $a|(bc) \Rightarrow \mu\kappa\delta(a, bc) = |a|$. Επίσης, από το προηγούμενο Λήμμα έχουμε: $\mu\kappa\delta(a,b) = 1 \Rightarrow (a, bc) = (a, c)$. Από τα πιο πάνω, έχουμε ότι $\mu\kappa\delta(a,c) = |a|$ και αρα $a|c$. □

Λήμμα 0.2.5 (ταυτότητα του Bézout)**.** *Έστω* $a, b \in \mathbb{Z}_*$ *και* $d = \mu\kappa\delta(a,b)$. *Τότε, υπάρχουν* $x, y \in \mathbb{Z}$ *τέτοιοι ώστε* $ax + by = d$. *Επιπλέον, κάθε ακέραιος της μορφής* $ax + by$ *είναι πολλαπλάσιο του* d.

Απόδειξη. Έστω $a, b \in \mathbb{Z}_*$ και $d = \mu\kappa\delta(a,b)$. Θεωρούμε το σύνολο

$$S = \{ax + by \mid x, y \in \mathbb{Z} \text{ και } ax + by > 0\}.$$

Είναι $S \neq \emptyset$, αφού $a \in S : a = 1\cdot a + 0\cdot b$ (ή το $-a$). Τότε, αφού το S είναι ενα μη κενό υποσύνολο των φυσικών αριθμών, από τον Αρχή της καλής διάταξης, έπεται ότι έχει ελάχιστο στοιχείο, έστω το $d := ax + by$, για κάποιους $a, b \in \mathbb{Z}$.
Ο d είναι ο μκδ των a και b:
Από τον Αλγόριθμο της Ευκλείδειας Διαίρεσης του a με τον d, έχουμε ότι

$$a = dq + r, \quad 0 \leq r < d$$

Είναι

$$r = a - qd = a - q(as + bt) = a(1 - qA) - b(qB)$$

για κάποιους $A, B \in \mathbb{Z}$ και αρα $r \in S \cup \{0\}$. Αλλά, $0 \leq r < d$ και ο d είναι ο ελάχιστος θετικός ακέραιος στο $S \Rightarrow r \notin S \Rightarrow r = 0$. Συνεπώς, $d|a$.
Με τον ίδιο τρόπο, δείχνουμε ότι $d|b$.

Ο d είναι ο ελάχιστος εκ των μκδ των a και b:
Έστω c ενας μκδ των a και $b \Rightarrow \exists u, w$ τέτοιοι ώστε $a = cu$ και $b = cw$. Τότε,

$$d = aA + bB = cuA + cvB = c(uA + vB)$$

και αρα $c|d$. Συνεπώς, $c \leq d$. □

▶ **Παράδειγμα 0.2.3.** *Να βρεθεί ο* $\mu\kappa\delta(64, 24)$ *και να γραφεί στη μορφή* $64u + 24w$ *για κάποιους* $u, w \in \mathbb{Z}$.

Λύση

$$\begin{aligned}\text{μκδ}(64,24) &= \text{μκδ}(24,64) = \text{μκδ}(24, 24\cdot 2+16)\\ &= \text{μκδ}(24,16) = \text{μκδ}(16,24)\\ &= \text{μκδ}(16, 16\cdot 1+8) = \text{μκδ}(16,8)\\ &= \text{μκδ}(8,16) = \text{μκδ}(8, 2\cdot 8) = 8\end{aligned}$$

Τώρα,

$$\begin{aligned}\text{μκδ}(64,24) &= 8 = 24-16 \;=\; 24\cdot 1+(-1)\cdot 16\\ &= 24\cdot 1+(-1)\cdot(64-2\cdot 24) \;=\; 24+3\cdot 24-64\\ &= 3\cdot 24+(-1)\cdot 64.\end{aligned}$$

Λήμμα 0.2.6 (Λήμμα του Ευκλείδη)**.** *Αν p πρώτος αριθμός τέτοιος ώστε $p/(ab)$ όπου $a,b\in\mathbb{Z}$, τότε είτε $p|a$ είτε $p|b$.*
Ακολούθως, αποδείξτε ότι αν $a_i\in\mathbb{Z}$, $i=1,2,\ldots,n$ και p πρώτος αριθμός τέτοιος ώστε $p|a_1a_2\ldots a_n$, τότε $p|a_i$ για κάποιο $i=1,2,\ldots,n$

Απόδειξη. Αν $p|a$, τότε ισχύει. Υποθέτουμε λοιπόν ότι $p\nmid a$. Τότε $\text{μκδ}(p,a)=1$. Πράγματι, αν $\text{μκδ}(p,a)>1 \Longrightarrow \text{μκδ}(p,a)=p$ (αφού p πρώτος[1]) $\Longrightarrow p|a$, άτοπο. Έτσι,

$$\begin{cases} p|(ab) \\ \\ \text{μκδ}(p,a)=1 \end{cases} \Longrightarrow p|b$$

(από προηγούμενο Λήμμα). □

▶ **Παρατήρηση 0.2.1.** *Η υπόθεση ότι p πρώτος είναι απαραίτητη για την ισχύ του πιο πάνω. Για παράδειγμα, $4|2\cdot 2$ αλλά $4\nmid 2$.*
Η γενική περίπτωση αποδεικνύεται με επαγωγή (αφού την έχουμε δείξει για $n=2$.)

0.3 Ρητοί και άρρητοι αριθμοί

Άσκηση 0.3.1. *Να δειχθεί ότι ο αριθμός $\sqrt{2}$ είναι άρρητος.*

Λύση:
• Υποθέτουμε ότι ισχύει το αντίθετο, δηλ. ότι ο $\sqrt{2}$ είναι ρητός. Τότε $\exists p,q\in\mathbb{Z}$ με $q\neq 0$ και $\text{μκδ}(p,q)=1$ τέτοιοι ώστε $\sqrt{2}=p/q$.

• Προχωράμε στα λογικά συμπεράσματα τα οποία θα μας οδηγήσουν σε αντίφαση με την αρχική υπόθεση. Παρατηρούμε ότι οι αριθμοί p και q δεν μπορεί να είναι και οι δύο άρτιοι γιατί αν ήταν, το ανωτέρο κλάσμα θα απλοποιείτω περαιτέρω. **Άρα ένας μόνο από τους p και q είναι περιττός**. Αλλά

$$\sqrt{2}=p/q \Longrightarrow (\sqrt{2})^2=(p/q)^2 \Longrightarrow 2=p^2/q^2 \Longrightarrow 2q^2=p^2$$

και άρα ο p^2 είναι άρτιος. Τότε και ο p είναι άρτιος (αν p περιττός, τότε p^2, περιττός, άτοπο). **Συνεπώς, ο q είναι περιττός**.
Τώρα, αφού ο p είναι άρτιος, θα υπάρχει $\ell\in\mathbb{Z}$ τέτοιος ώστε $p=2\ell$. Έτσι,

$$\begin{cases} 2q^2=p^2 \\ p=2\ell \end{cases} \Longrightarrow 2q^2=(2\ell)^2 \Longrightarrow 2q^2=4\ell^2 \Longrightarrow q^2=2\ell^2$$

[1] οι μόνοι διαιρέτες ενός πρώτου αριθμού p είναι το 1 και ο p

και άρα ο q^2 είναι άρτιος, άρα και ο q είναι άρτιος.

• Αυτό όμως είναι άτοπο, γιατί ο q είναι περιττός. □

Άσκηση 0.3.2. *Να δειχθεί ότι ο αριθμός $\sqrt{3}$ είναι άρρητος.*

Λύση:
• Υποθέτουμε ότι ισχύει το αντίθετο, δηλ. ότι $\sqrt{3} \in \mathbb{Q} \Rightarrow \sqrt{3} = p/q$, όπου $p, q \in \mathbb{Z}$ με $q \neq 0$ και μκδ$(p, q) = 1$.

• Αλλά
$$\sqrt{3} = p/q \Longrightarrow (\sqrt{3})^2 = (p/q)^2 \Longrightarrow 3 = p^2/q^2 \Longrightarrow 3q^2 = p^2$$
και άρα ο 3 διαιρεί τον p^2. Τότε και ο 3 διαιρεί τον p. Πράγματι, αν
$$p = \prod_{i=1}^{k} p_i^{n_i} = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_k^{n_k},$$
τότε $3 = p_i^{n_i}$ για κάποιο i. Τότε, προφανώς, ο 3 είναι παράγοντας και του p^2. Άρα, υπάρχει $\ell \in \mathbb{Z}$ τέτοιος ώστε $p = 3\ell$. Έτσι,
$$\begin{cases} 3q^2 = p^2 \\ p = 3\ell \end{cases} \Longrightarrow 3q^2 = (3\ell)^2 \Longrightarrow 3q^2 = 9\ell^2 \Longrightarrow q^2 = 3\ell^2$$
και άρα ο 3 διαιρεί τον q^2, άρα και τον q.

• Δηλαδή ο 3 διαιρεί και τον p και τον q, άτοπο, γιατί μκδ$(p, q) = 1$. □

Το επόμενο αποτέλεσμα λέει ουσιαστικά ότι για κάθε $n \in \mathbb{N}$, ο $\sqrt{n}$ είναι είτε φυσικός είτε άρρητος.

Λήμμα 0.3.1. *Έστω $n \in \mathbb{N}$. $\sqrt{n} \in \mathbb{Q} \Longleftrightarrow$ ο n είναι τέλειο τετράγωνο (δηλ. αν γράφεται ως $n = m^2$, για κάποιο $m \in \mathbb{Z}$).*

Απόδειξη.
($\Longrightarrow$) Έστω ότι $\sqrt{n} \in \mathbb{Q} \Rightarrow n = p/q$, όπου $p, q \in \mathbb{Z}_+$ με $q \neq 0$ και μκδ$(p, q) = 1$ και έστω ότι ο n δεν είναι τέλειο τετράγωνο. Τότε στην κανονική αναπαράσταση του n, υπάρχει τουλάχιστον ενας παράγοντας p_i υψωμένος σε περιττή δύναμη.Τώρα,
$$\sqrt{n} = \frac{p}{q} \Rightarrow n = \frac{p^2}{q^2} \Rightarrow p^2 = nq^2.$$
Τότε, ο p_i εμφανίζεται σε περιττή δύναμη στο δεξί μέλος ενώ στο αριστερό μπορεί να εμφανιστεί μόνο σε άρτια δύναμη, άτοπο, από τη μοναδικότητα της κανονικής αναπαράστασης του nq^2.

($\Longleftarrow$) Προφανές. □

▶ **Παρατήρηση 0.3.1.** *Εναλλακτικά για το ευθύ ($\Longrightarrow$):*
Έστω ότι $\sqrt{n} \in \mathbb{Q} \Rightarrow n = p/q$, όπου $p, q \in \mathbb{Z}_+$ με $q \neq 0$ και μκδ$(p, q) = 1$ και έστω ότι ο n δεν είναι τέλειο τετράγωνο. Τότε $n = p^2/q^2$, άρα $p^2 = nq^2$. Τότε ο q διαιρεί τον p^2 και αφού μκδ$(p, q) = 1 \Rightarrow q$ διαιρεί τον p. Άρα $q = 1$, συνεπώς $n = p^2$, άτοπο.