ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

ΤΜΗΜΑ **Β΄**

ΛΥΣΕΙΣ ΑΣΚΗΣΕΩΝ - ΦΥΛΛΑΔΙΟ **3**

ΔΙΔΑΣΚΩΝ: Α. Μπεληγιάννης

ΙΣΤΟΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ:
http://users.uoi.gr/abeligia/NumberTheory/NT2016/NT2016.html

Πέμπτη 3 Νοεμβρίου 2016

Άσκηση 1. *Αφού βρείτε την πρωτογενή ανάλυση των αριθμών* 130, 2275, 1998, 2004, *και* 2016, *να υπολογίσετε τους μέγιστους κοινούς διαιρέτες*

$$(130, 2275) \quad \textit{και} \quad (1998, 2004, 2016)$$

Λύση. Η πρωτογενής ανάλυση των αριθμών 130 και 2275 είναι

$$130 = 2 \cdot 5 \cdot 13 \quad \text{και} \quad 2275 = 5^2 \cdot 7 \cdot 13$$

Γράφουμε $130 = 2^1 \cdot 5^1 \cdot 7^0 \cdot 13^1$ και $2275 = 2^0 \cdot 5^2 \cdot 7^1 \cdot 13^1$. Τότε έχουμε

$$(130, 2275) = 2^{\min\{1,0\}} \cdot 5^{\min\{1,2\}} \cdot 7^{\min\{0,1\}} \cdot 13^{\min\{1,1\}} = 2^0 \cdot 5^1 \cdot 7^0 \cdot 13^1 = 5 \cdot 13 = 65$$

Συνεπώς ο μέγιστος κοινός διαιρέτης των αριθμών 130 και 2275 είναι $(130, 2275) = 65$.

Παρόμοια οι πρωτογενείς αναλύσεις των αριθμών 1998, 2004, και 2016, είναι:

$$1998 = 2 \cdot 3^3 \cdot 37, \qquad 2004 = 2^2 \cdot 3 \cdot 167, \qquad 2016 = 2^5 \cdot 3^2 \cdot 37$$

Γράφουμε $1998 = 2^1 \cdot 3^3 \cdot 37^1 \cdot 167^0$, $2004 = 2^2 \cdot 3^1 \cdot 37^0 \cdot 167$, και $2016 = 2^5 \cdot 3^2 \cdot 37^1 \cdot 167^0$. Τότε θα έχουμε

$$(1998, 2004, 2016) = 2^{\min\{1,2,5\}} \cdot 3^{\min\{3,1,2\}} \cdot 37^{\min\{1,0,1\}} \cdot 167^{\min\{0,1,0\}} = 2^1 \cdot 3^1 \cdot 37^0 \cdot 167^0 = 2 \cdot 3 = 6$$

Άρα ο μέγιστος κοινός διαιρέτης των αριθμών 1998, 2004, και 2016 είναι $(1998, 2004, 2016) = 6$. ■

Άσκηση 2. *Δείξτε ότι για κάθε ακέραιο* k *ισχύει ότι:*

$$(7k + 5, 11k + 8) = 1 \quad \& \quad (8k + 3, 5k + 2) = 1$$

Λύση. • Έστω $(7k + 5, 11k + 8) = d$. Τότε

$$d \mid 7k{+}5 \ \& \ d \mid 11k{+}8 \implies d \mid 11(7k{+}5) \ \& \ d \mid 7(11k{+}8) \implies d \mid 77k{+}55 \ \& \ d \mid 77k{+}56 \implies d \mid 1$$

και επομένως $d = 1$.

ΔΙΑΦΟΡΕΤΙΚΑ: $-11(7k + 5) + 7(11k + 8) = -55 + 56 = 1$, και άρα $(7k + 5, 11k + 8) = 1$.

• Έστω $(8k + 3, 5k + 2) = d$. Τότε

$$d \mid 8k{+}3 \ \& \ d \mid 5k{+}2 \implies d \mid 5(8k{+}3) \ \& \ d \mid 8(5k{+}2) \implies d \mid 40k{+}15 \ \& \ d \mid 40k{+}16 \implies d \mid 1$$

και επομένως $d = 1$.

ΔΙΑΦΟΡΕΤΙΚΑ: $(-5)(8k + 3) + 8(5k + 2) = -15 + 16 = 1$, και άρα $(8k + 2, 5k + 2) = 1$. ■

Άσκηση 3. *Έστω οι ακέραιοι αριθμοί* $a_1, a_2, \cdots, a_n$, $n \geq 3$.

1. *Δείξτε ότι:*

$$\big(a_1, a_2, \cdots, a_n\big) = \big(|a_1|, |a_2|, \cdots, |a_n|\big)$$

2. *Δείξτε ότι αν* λ, *είναι ένας ακέραιος αριθμός, τότε:*

$$\big(\lambda a_1, \lambda a_2, \cdots, \lambda a_n\big) = |\lambda|\big(a_1, a_2, \cdots, a_n\big)$$

3. *Αν* $k \leq n-2$, *τότε:*

$$\big(a_1, a_2, \cdots, a_n\big) = \big(a_1, a_2, \cdots, a_k,\ (a_{k+1}, \cdots, a_n)\big)$$

4. *Αν* $b = x_1a_1 + x_2a_2 + \cdots + x_na_n$ *για κάποιους ακεραίους* $x_1, x_2, \cdots, x_n$, *τότε:*

$$\big(a_1, a_2, \cdots, a_n\big) = \big(a_1, a_2, \cdots, a_n, b\big)$$

5. *Αν* $a_k \neq 0$, $\forall k = 1, 2, \cdots, n$, *δείξτε ότι:*

$$\big(a_1, a_2, \cdots, a_n\big) = d \quad \Longleftrightarrow \quad d \mid a_1,\ d \mid a_2,\ \cdots,\ d \mid a_n \quad \textit{και} \quad \big(\frac{a_1}{d}, \frac{a_2}{d}, \cdots, \frac{a_n}{d}\big) = 1$$

Λύση. **1.** Επειδή $d \mid a \Longleftrightarrow d \mid |a|$, θέτοντας $d = (a_1, a_2, \cdots, a_n)$ και $\delta = (|a_1|, |a_2|, \cdots, |a_n|)$, θα έχουμε:

$$d \mid a_i,\ 1 \leq i \leq n, \quad \Longrightarrow \quad d \mid |a_i|,\ 1 \leq i \leq n, \quad \Longrightarrow \quad d \mid \delta$$

$$\delta \mid |a_i|,\ 1 \leq i \leq n, \quad \Longrightarrow \quad \delta \mid a_i,\ 1 \leq i \leq n, \quad \Longrightarrow \quad \delta \mid d$$

Επομένως επειδή $d, \delta \geq 1$, θα έχουμε $d = \delta$.

2. Έστω $d = (a_1, a_2, \cdots, a_n)$ και $\delta = (\lambda a_1, \lambda a_2, \cdots, \lambda a_n)$. Τότε θα δείξουμε ότι $|\lambda|d = \delta$. Υποθέτουμε πρώτα ότι $\lambda > 0$. Θα έχουμε:

$$d \mid a_k,\ 1 \leq k \leq n \quad \Longrightarrow \quad \lambda d \mid \lambda a_k,\ 1 \leq k \leq n$$

Από την άλλη πλευρά επειδή $d = (a_1, a_2, \cdots, a_n)$, έπεται ότι[1]: $d = x_1a_1 + x_2a_2 + \cdots + x_na_n$ για κάποιους ακεραίους $x_1, \cdots, x_n$. Τότε $\lambda d = x_1\lambda a_1 + x_2\lambda a_2 + \cdots + x_n\lambda a_n$. Επειδή $\lambda d \mid \lambda a_k,\ 1 \leq k \leq n$, θα έχουμε ότι: $\lambda d = (\lambda a_1, \lambda a_2, \cdots, \lambda a_n) = \delta$.

Παρόμοια δουλεύουμε αν $\lambda < 0$.

3. Έστω $d = (a_1, a_2, \cdots, a_n)$ και $\delta = (a_{k+1}, \cdots, a_n)$. Θέτοντας $d' = (a_1, a_2, \cdots, a_k)$, και $d'' = (d', \delta)$, θα δείξουμε ότι: $d = (d', \delta) = d''$. Επειδή $d = (a_1, a_2, \cdots, a_n)$, θα έχουμε:

$$d \mid a_i,\ 1 \leq i \leq n \implies d \mid a_i,\ 1 \leq i \leq k\ \&\ d \mid a_j,\ k{+}1 \leq j \leq n \implies d \mid d'\ \&\ d \mid \delta \implies d \mid (d', \delta) = d''$$

Αντίστροφα, επειδή $d' = (a_1, \cdots, a_k)$ και $\delta = (a_{k+1}, \cdots, a_n)$, θα έχουμε:

$$d'' \mid d'\ \&\ d'' \mid \delta \implies d'' \mid a_i,\ 1 \leq i \leq k\ \&\ d'' \mid a_j,\ k{+}1 \leq j \leq n \implies d'' \mid \delta \mid a_i,\ 1 \leq i \leq n \implies d'' \mid d$$

Επομένως θα έχουμε: $d = d''$.

4. Έστω $d = (a_1, a_2, \cdots, a_n)$ και $\delta = (a_1, a_2, \cdots, a_n, b)$. Θα δείξουμε ότι $d = \delta$. Επειδή

$$d \mid a_k,\ 1 \leq k \leq n \implies d \mid x_ka_k,\ 1 \leq k \leq n \implies d \mid (x_1a_1 + x_2a_2 + \cdots + x_na_n) \implies d \mid b \implies d \mid \delta$$

Αντίστροφα, προφανώς $\delta \mid a_k$, $1 \leq k \leq n$ και άρα $\delta \mid d$. Επομένως $d = \delta$.

---

[1] Υπενθυμίζουμε από τη Θεωρία ότι:

• «$(a_1, a_2, \cdots, a_n) = d$ *αν και μόνον αν* $d \mid a_k$, $\forall k = 1, 2, \cdots, n$ *και υπάρχουν ακέραιοι* $x_1, x_2, \cdots, x_n$ *έτσι ώστε:* $x_1a_1 + x_2a_2 + \cdots + x_na_n = d$. *Ιδιαίτερα:* $(a_1, a_2, \cdots, a_n) = 1$ *αν και μόνον αν υπάρχουν ακέραιοι* $x_1, x_2, \cdots, x_n$ *έτσι ώστε:* $x_1a_1 + x_2a_2 + \cdots + x_na_n = 1$.»

5. Θα έχουμε:

«$\Longrightarrow$» Έστω ότι $(a_1, a_2, \cdots, a_n) = d$. Τότε $d \mid a_k$, $\forall k = 1, 2, \cdots, n$ και υπάρχουν ακέραιοι $x_1, x_2, \cdots, x_n$ έτσι ώστε: $x_1a_1 + x_2a_2 + \cdots + x_na_n = d$. Επομένως θα έχουμε ότι

$$\frac{a_k}{d} \in \mathbb{Z}, \;\; 1 \leq k \leq n \quad \text{και} \quad x_1\frac{a_1}{d} + x_2\frac{a_2}{d} + \cdots + x_n\frac{a_n}{d} = 1$$

Άρα $(\frac{a_1}{d}, \frac{a_2}{d}, \cdots, \frac{a_n}{d}) = 1$.

«$\Longleftarrow$» Έστω ότι $d \mid a_k$, $\forall k = 1, 2, \cdots, n$ και $(\frac{a_1}{d}, \frac{a_2}{d}, \cdots, \frac{a_n}{d}) = 1$. Τότε υπάρχουν ακέραιοι $y_1, y_2, \cdots, y_n$ έτσι ώστε: $y_1\frac{a_1}{d} + y_2\frac{a_2}{d} + \cdots + y_n\frac{a_n}{d} = 1$. Τότε προφανώς θα έχουμε:

$$dy_1a_1 + dy_2a_2 + \cdots + dy_na_n = d \quad \Longrightarrow \quad (a_1, a_2, \cdots, a_n) = d$$

διότι $d \mid a_k$, $\forall k = 1, 2, \cdots, n$. ■

Άσκηση 4. **1.** *Αν a, b, c είναι ακέραιοι και $(a, b) = 1 = (a, c)$, δείξτε ότι:*

$$(a, bc) = 1$$

2. *Γενικότερα αν $a_1, a_2, \cdots, a_n$ και b είναι ακέραιοι και $(a_1, b) = (a_2, b) = \cdots = (a_n, b) = 1$, δείξτε ότι:*

$$(a_1a_2 \cdots a_n, b) = 1$$

Λύση. **1.** Έστω $d = (a, bc)$. Αν $d > 1$, τότε ο αριθμός d έχει έναν πρώτο διαιρέτη p. Έτσι $p \mid d$ και επομένως $p \mid a$ και $p \mid bc$. Επειδή ο p είναι πρώτος, έπεται ότι $p \mid b$ ή $p \mid c$. Αν $p \mid b$, τότε επειδή $p \mid a$ θα έχουμε $p \mid (a, b) = 1$ και άρα $p = 1$ το οποίο είναι άτοπο. Αν $p \mid c$, τότε επειδή $p \mid a$ θα έχουμε $p \mid (a, c) = 1$ και άρα $p = 1$ το οποίο είναι άτοπο. Άρα καταλήγουμε ότι $d = (a, bc) = 1$.

2. Η απόδειξη είναι παρόμοια: Έστω $d = (a_1a_2 \cdots a_n, b)$. Υποθέτουμε ότι $d > 1$ και επομένως ο αριθμός d έχει έναν πρώτο διαιρέτη p. Επειδή ο p είναι πρώτος και επειδή $p \mid a_1a_2 \cdots a_n$ (διότι $p \mid d$), έπεται ότι $p \mid a_k$ για κάποιο $k = 1, 2, \cdots, n$. Επειδή $p \mid b$, θα έχουμε ότι $p \mid (a_k, b) = 1$ και άρα $p = 1$ το οποίο είναι άτοπο. Άρα $d = (a_1a_2 \cdots a_n, b) = 1$. ■

Άσκηση 5. *Έστω a, b, c μη-μηδενικοί ακέραιοι αριθμοί.*

1. *Αν $(a, b) = 1$ και $c \mid (a + b)$, δείξτε ότι: $(c, a) = 1 = (c, b)$.*

2. *Αν $(b, c) = 1$, τότε: $(a, bc) = (a, b)(a, c)$.*

Λύση. **1.** Έστω $d = (a, c)$ και $\delta = (b, c)$.

• **1ος Τρόπος** Τότε $d \mid c$ και $d \mid a$. Εοειδή $c \mid a + b$, θα έχουμε $d \mid a + b$. Έτσι επειδή $d \mid a$ και $d \mid a + b$, θα έχουμε $d \mid a + b - a = a$, δηλαδή $d \mid b$. Επειδή $d \mid a$ και $d \mid b$, έπεται ότι $d \mid (a, b) = 1$, δηλαδή $d \mid 1$. Επομένως $d = (a, c) = 1$.

Ακριβώς παρόμοια δείχνουμε ότι $\delta = (b, c) = 1$.

• **2ος Τρόπος** Τότε $d \mid c$ και άρα $d \mid a+b$ διότι από την υπόθεση $c \mid a+b$. Επειδή $(a, b) = 1$, θα έχουμε $ax + by = 1$, για κάποιους ακεραίους x, y. Επειδή $d \mid a$ θα έχουμε $d \mid ax$ και $d \mid ay$ και επομένως $d \mid (1 - by)$. Τότε:

$$d \mid c \implies d \mid a+b \implies d \mid ay+by \;\&\; d \mid 1-by \implies d \mid ay+1 \;\&\; d \mid ay \implies d \mid 1 \implies d = 1$$

Άρα $(c, a) = 1$.

Παρόμοια θα έχουμε $\delta \mid c$ και άρα $\delta \mid a + b$ διότι από την υπόθεση $c \mid a + b$. Επειδή $\delta \mid b$ θα έχουμε $\delta \mid bx$ και $\delta \mid by$ και επομένως $\delta \mid (1 - ax)$. Τότε:

$$\delta \mid c \implies \delta \mid a+b \implies \delta \mid ax+bx \;\&\; \delta \mid 1-ax \implies \delta \mid bx+1 \;\&\; \delta \mid bx \implies \delta \mid 1 \implies \delta = 1$$

2. Θέτουμε: $d=(a,bc)$, $d_1=(a,b)$, $d_2=(a,c)$. Θα δείξουμε ότι $d=d_1d_2$.

Θα δείξουμε πρώτα ότι: $(d_1,d_2)=1$. Έστω $(d_1,d_2)=x$. Τότε:

$$x\mid d_1\ \&\ x\mid d_2\implies x\mid b\ \&\ x\mid c\implies x\mid (b,c)=1\implies x=1\implies (d_1,d_2)=1 \tag{1}$$

Από την άλλη πλευρά, επειδή $d_1=(a,b)$ και $d_2=(a,c)$, υπάρχουν ακέραιοι x_1,y_1,x_2,y_2, έτσι ώστε:

$$d_1=ax_1+by_1\quad\&\quad d_2=ax_2+cy_2\quad\Longrightarrow\quad d_1d_2=a(ax_1x_2+cx_1y_2+bx_2y_1)+bc(y_1y_2) \tag{2}$$

Λόγω της (2), για να δείξουμε ότι $d_1d_2=d$, αρκεί να δείξουμε ότι $d_1d_2\mid a$ και $d_1d_2\mid bc$. Θα έχουμε:

$$d_1\mid b\ \&\ d_2\mid c\implies d_1d_2\mid bc \tag{3}$$

$$d_1\mid a\ \&\ d_2\mid a\ \&\ (d_1,d_2)=1\quad\Longrightarrow\quad d_1d_2\mid a \tag{4}$$

Η απόδειξη της (3) είναι άμεση. Θα δείξουμε την σχέση (4). Αν $a=1$, τότε επειδή $d_1\mid a$ και $d_2\mid a$, θα έχουμε $d_1=d_2=1$ και άρα $d_1d_2=1\mid a$. Υποθέτουμε ότι $a>1$, και άρα μπορούμε να θεωρήσουμε την πρωτογενή ανάλυση $a=p_1^{a_1}\cdot p_2^{a_2}\cdots p_k^{a_k}$ του a. Επειδή $d_1\mid a$, έπεται ότι $d_1=p_1^{b_1}\cdot p_2^{b_2}\cdots p_k^{b_k}$, όπου $0\le b_i\le a_i$ και $1\le i\le k$. Επειδή $d_2\mid a$, έπεται ότι $d_2=p_1^{c_1}\cdot p_2^{c_2}\cdots p_k^{c_k}$, όπου $0\le c_i\le a_i$ και $1\le i\le k$. Επομένως

$$d_1d_2=p_1^{b_1+c_1}\cdot p_2^{b_2+c_2}\ \cdots\ p_k^{b_k+c_k}$$

Από την άλλη πλευρά, έχουμε:

$$1=(d_1,d_2)=p_1^{\min\{b_1,c_1\}}\cdot p_2^{\min\{b_2,c_2\}}\ \cdots\ p_k^{\min\{b_k,c_k\}}\quad\Longrightarrow\quad \min\{b_i,c_i\}=0,\ \ 1\le i\le k$$

Οι τελευταίες σχέσεις δίνουν ότι: $b_i+c_i\le a_i$, $1\le i\le k$. Πράγματι, αν $\min\{b_i,c_i\}=b_i$, τότε $b_i=0$, και άρα $b_i+c_i=c_i\le a_i$. Αν $\min\{b_i,c_i\}=c_i$, τότε $c_i=0$, και άρα $b_i+c_i=b_i\le a_i$. Επομένως σε κάθε περίπτωση: $b_i+c_i=c_i\le a_i$, $1\le i\le k$, και επομένως $d_1d_2\mid a$.

Από τις (2), (3) και (4) έπεται ότι $d_1d_2=(a,bc)=d$. ■

Άσκηση 6. *Έστω οι ακέραιοι αριθμοί a,b,c,d. Αν $b,d>0$ και $(a,b)=1=(c,d)$, και αν ο αριθμός $\frac{a}{b}+\frac{c}{d}$ είναι ακέραιος, δείξτε ότι: $b=d$.*

Λύση. Θα έχουμε:

$$\frac{a}{b}+\frac{c}{d}\in\mathbb{Z}\implies\frac{ad+bc}{bd}\in\mathbb{Z}\implies bd\mid ad+bc$$

Τότε θα έχουμε:

$$bd\mid d(ad+bc)\implies bd\mid ad^2+bdc\ \&\ bd\mid bdc\implies bd\mid ad^2\implies b\mid ad$$

Εποεμένως

$$(a,b)=1\qquad\&\qquad b\mid ad\implies b\mid d$$

Δουλεύοντας ακριβώς ανάλογα και χρησιμοποιώντας ότι $(c,d)=1$, θα έχουμε και $d\mid b$. Επομένως, επειδή $b,d>0$, θα έχουμε: $b=d$. ■

Άσκηση 7. *Αν x,y είναι θετικοί ακέραιοι και $x<y$, τότε:*

$$a^{2^x}+1\mid a^{2^y}-1\quad\textit{και άρα:}\quad\left(a^{2^y}-1,a^{2^x}+1\right)=a^{2^x}+1 \tag{†}$$

Λύση. Θα δείξουμε πρώτα με χρήση της Αρχής Μαθηματικής Επαγωγής ότι:

$$\forall k \in \mathbb{N}: \qquad a^{2^k} - 1 = (a-1) \cdot \prod_{i=0}^{k-1} (a^{2^i} + 1) = (a-1) \cdot (a^{2^0} + 1) \cdot (a^{2^1} + 1) \cdots (a^{2^{k-1}} + 1) \qquad (*)$$

- Για $k = 1$, προφανώς η (*) ισχύει διότι: $a^{2^1} - 1 = a^2 - 1 = (a-1) \cdot (a+1) = (a-1) \cdot (a^{2^0} + 1)$.
- Υποθέτουμε ότι η (*) ισχύει για $k = r$: $\quad a^{2^r} - 1 = (a-1) \cdot \prod_{i=0}^{r-1} (a^{2^i} + 1)$.
- Για $k = r+1$, χρησιμοποιώντας την Επαγωγική Υπόθεση, θα έχουμε:

$$a^{2^{r+1}} - 1 = a^{2^r \cdot 2} - 1 = (a^{2^r})^2 - 1 = (a^{2^r} - 1) \cdot (a^{2^r} + 1) = (a-1) \cdot \prod_{i=0}^{r-1} (a^{2^i} + 1)(a^{2^r} + 1) =$$

και άρα:

$$a^{2^{r+1}} - 1 = (a-1) \cdot \prod_{i=0}^{r} (a^{2^i} + 1)$$

Αν τώρα $y > x$, θα έχουμε $x \leq y - 1$ και άρα από τη σχέση $(*)$ έπεται ότι:

$$a^{2^y} - 1 = (a-1) \cdot \prod_{i=0}^{y-1} (a^{2^i} + 1) = (a-1) \cdot (a^{2^0} + 1) \cdot (a^{2^1} + 1) \cdots (a^{2^x} + 1) \cdots (a^{2^{y-1}} + 1)$$

Δηλαδή $(a^{2^x} + 1) \mid (a^{2^y} - 1)$. Τότε όμως θα έχουμε και: $\left(a^{2^y} - 1, a^{2^x} + 1\right) = a^{2^x} + 1$. ■

Άσκηση 8. *Αν a, n, m είναι θετικοί ακέραιοι και $n \neq m$, δείξτε ότι:*

$$\left(a^{2^m} + 1, a^{2^n} + 1\right) = \begin{cases} 1, & \text{αν } a\text{: άρτιος} \\ \\ 2, & \text{αν } a\text{: περιττός} \end{cases}$$

Λύση. Υποθέτουμε ότι $n < m$, και έστω $d = (a^{2^m} + 1, a^{2^n} + 1)$. Τότε από την Άσκηση 7, έπεται ότι $a^{2^n} + 1 \mid a^{2^m} - 1$, και επομένως υπάρχει ακέραιος δ έτσι ώστε:

$$a^{2^m} - 1 = \delta \cdot (a^{2^n} + 1)$$

Θα έχουμε $a^{2^m} + 1 = a^{2^m} - 1 + 2 = \delta \cdot (a^{2^n} + 1) + 2$ και άρα

$$d = (\delta \cdot (a^{2^n} + 1) + 2, a^{2^n} + 1)$$

Επειδή, όπως προκύπτει εύκολα, ισχύει[2] $(a + k \cdot b, b) = (a, b)$, $\forall a, b, k \in \mathbb{Z}$, θα έχουμε

$$d = (2, a^{2^n} + 1) \quad \Longrightarrow \quad d \mid 2 \;\; \& \;\; d \mid a^{2^n} + 1 \quad \Longrightarrow \quad d = 1 \;\; \text{ή} \;\; d = 2 \;\; \& \;\; d \mid a^{2^n} + 1$$

- Αν ο a είναι άρτιος, τότε προφανώς ο αριθμός $a^{2^n} + 1$ είναι περιττός και προφανώς τότε $d = 1$.
- Αν ο a είναι περιττός, τότε προφανώς a^{2^n} είναι περιττός και άρα ο αριθμός $a^{2^n} + 1$ είναι άρτιος. Προφανώς τότε $d = 2$. ■

---

[2] Πράγματι, έστω $d = (a, b)$ και $\delta = (a + kb, b)$. Τότε:

$$d \mid a \;\; \& \;\; d \mid b \;\; \Longrightarrow \;\; d \mid a \;\; \& \;\; d \mid kb \;\; \Longrightarrow \;\; d \mid a + kb \;\; \& \;\; d \mid b \;\; \Longrightarrow \;\; d \mid (a + kb, b) \;\; \Longrightarrow \;\; d \mid \delta$$

Παρόμοια

$$\delta \mid a + kb \;\; \& \;\; \delta \mid b \;\; \Longrightarrow \;\; \delta \mid a + kb \;\; \& \;\; \delta \mid kb \;\; \Longrightarrow \;\; \delta \mid a + kb - kb = a \;\; \& \;\; \delta \mid b \;\; \Longrightarrow \;\; \delta \mid (a, b) \;\; \Longrightarrow \;\; \delta \mid d$$

Επομένως $d = \delta$.

Άσκηση 9. *Αν a, n, m είναι φυσικοί αριθμοί, και ο n είναι περιττός, να δείξετε ότι:*

$$(a^n - 1, a^m + 1) = 1 \ \ \acute{\eta} \ \ 2$$

Ισχύει η παραπάνω ισότητα αν ο n είναι άρτιος;

Λύση. Έστω $d = (a^n - 1, a^m + 1)$. Τότε $a^n - 1 = dr$ και $a^m + 1 = ds$, για κάποιους θετικούς ακέραιους r, s, και επομένως:

$$a^n = dr + 1 \qquad \& \qquad a^m = ds - 1$$

Τότε χρησιμοποιώντας διαδοχικά το διώνυμο του Νεύτωνα[3]

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

θα έχουμε:

$$a^{nm} = (a^n)^m = (dr+1)^m = \sum_{k=0}^{m} \binom{m}{k} (dr)^k = 1 + \sum_{k=1}^{m} \binom{m}{k} (dr)^k = 1 + Ad \qquad (*)$$

όπου $A = \sum_{k=1}^{m} \binom{m}{k} r^k d^{k-1}$.

Παρόμοια, χρησιμοποιώντας ότι ο n είναι περιττός, θα έχουμε:

$$a^{nm} = (a^m)^n = (ds-1)^n = (-1)^n (1-ds)^n = -\sum_{k=0}^{n} \binom{n}{k} (-ds)^k = -1 + Bd \qquad (**)$$

όπου $B = -\sum_{k=1}^{n} \binom{n}{k} (-)^k d^{k-1} s^k$.

Από τις σχέσεις $(*)$ και $(**)$ θα έχουμε: $Ad + 1 = Bd - 1$ και προφανώς $A \neq B$. Τότε $(B - A)d = 2$ και επομένως $d \mid 2$. Δηλαδή $d = 1$ ή 2.

Διαλέγοντας στην Άσκηση 7: $a = 2$, $n = 2^x$, όπου $x \geq 1$, και $m = 2^y$ στη σχέση $(\dagger)$, έπεται ότι $(a^m - 1, a^n + 1) = a^{2^x} + 1 > 2$ και έτσι η αρχικός ισχυριμός δεν ισχύει για την περίπτωση κατά την οποία ο αριθμός n είναι άρτιος. ■

---

[3] Οι διωνυμικοί συντελεστές $\binom{n}{k}$, όπου $n, k \in \mathbb{N}_0$ και $k \leq n$, ορίζονται ως εξής:

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$$

είναι θετικοί ακέραιοι, και εκφράζουν το πλήθος των διαφορετικών τρόπων με τους οποίους μπορούμε να επιλέξουμε k αντικείμενα από n το πλήθος αντικείμενα. Έτσι για παράδειγμα:

$$\binom{4}{2} = \frac{4!}{2!\,(4-2)!} = \frac{1\cdot 2\cdot 3\cdot 4}{1\cdot 2\cdot 1\cdot 2} = 6, \qquad \binom{15}{8} = \frac{15!}{8!\,(15-8)!} = \frac{1\cdot 2\cdots 15}{1\cdot 2\cdots 8\cdot 1\cdot 2\cdots 7} = 6435$$

Ο τύπος του Νεύτωνα τότε μπορεί να γραφεί ως εξής:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = \binom{n}{0} a^{n-0} b^0 + \binom{n}{1} a^{n-1} b^1 + \binom{n}{2} a^{n-2} b^2 + \cdots + \binom{n}{n-1} a^{n-(n-1)} b^{n-1} + \binom{n}{n} a^{n-n} b^n$$

$$= a^n + n a^{n-1} b + \frac{n(n-1)}{2} a^{n-2} b^2 + \cdots + \frac{n!}{k!\,(n-k)!} a^{n-k} b^k + \cdots + n a b^{n-1} + b^n$$

Μια χρήσιμη σχέση μεταξύ των διωνυμικών συντελεστών (η οποία μπορεί να χρησιμοποιηθεί στην απόδειξη, με την Αρχή Μαθηματικής Επαγωγής, του τύπου του διωνύμου του Νεύτωνα) είναι η εξής:

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$$

Άσκηση 10. *Δείξτε οτι:*

1. $(a,b)=1 \iff (a^n,b^m)=1, \ \ \forall n,m\geq 1.$
2. $(a^n,b^n)=(a,b)^n.$

Λύση. **1.** «$\Longrightarrow$» Έστω $(a,b)=1$ και υποθέτουμε ότι $d=(a^n,b^m)$. Αν $d\neq 1$, τότε $d>1$ και άρα ο d έχει έναν πρώτο διαιρέτη p. Τότε $p\mid a^n$ και άρα επειδή ο p είναι πρώτος θα έχουμε $p\mid a$. Παρόμοια επειδή $p\mid b^m$ και ο p είναι πρώτος, θα έχουμε $p\mid b$. Από τις σχέσεις $d\mid a$ και $p\mid b$ έπεται ότι $p\mid (a,b)=1$ το οποίο είναι άτοπο διότι ο p είναι πρώτος. Άρα $(a^n,b^m)=1$.

«$\Longleftarrow$» Έστω $(a^n,b^m)=1$, και υποθέτουμε ότι $d=(a,b)$. Αν $d\neq 1$, τότε $d>1$ και άρα ο d έχει έναν πρώτο διαιρέτη p. Τότε $p\mid a$ και $p\mid b$ και επομένως θα έχουμε $p\mid a^n$ και $p\mid b^m$, $\forall n,m\geq 1$. Τότε $d\mid (a^n,b^m)=1$ το οποίο είναι άτοπο διότι ο p είναι πρώτος. Άρα $(a,b)=1$.

2. Αν $a=1$ ή $b=1$, τότε ο ισχυρσιμός είναι αληθής διότι: $(1^n,b^n)=(1,b^n)=1=1^n=(1,b)^n$ και παρόμοια $(a^n,1^n)=(a^n,1)=1=1^n=(a,1)^n$.

Υποθέτουμε ότι $a,b>1$ και επομένως μπορούμε να γράψουμε:

$$a=p_1^{a_1}\cdots p_k^{a_k} \quad \& \quad b=p_1^{b_1}\cdots p_k^{b_k}$$

όπου οι $p_1,\cdots,p_k$ είναι πρώτοι, $k\geq 1$, και $a_i,b_i\geq 0$, $1\leq i\leq k$. Θα έχουμε

$$a^n=p_1^{na_1}\cdots p_k^{na_k} \quad \& \quad b^n=p_1^{nb_1}\cdots p_k^{nb_k} \quad \text{και άρα:} \quad (a^n,b^n)=p_1^{\min\{na_1,nb_1\}}\cdots p_k^{\min\{na_k,nb_k\}}$$

Από την άλλη πλευρά θα έχουμε $(a,b)=p_1^{\min\{a_1,b_1\}}\cdots p_k^{\min\{a_k,b_k\}}$, και άρα:

$$(a,b)^n=(p_1^{\min\{a_1,b_1\}}\cdots p_k^{\min\{a_k,b_k\}})^n=p_1^{n\min\{a_1,b_1\}}\cdots p_k^{n\min\{a_k,b_k\}}$$

Επειδή

$$\forall n,x,y\geq 1: \qquad n\min\{x,y\}=\min\{nx,ny\}$$

τελικά θα έχουμε:

$$(a^n,b^n)=p_1^{\min\{na_1,nb_1\}}\cdots p_k^{\min\{na_k,nb_k\}}=p_1^{n\min\{a_1,b_1\}}\cdots p_k^{n\min\{a_k,b_k\}}=(a,b)^n \qquad \blacksquare$$

Άσκηση 11. *Αν a,b είναι ακέραιοι οι οποίοι είναι πρώτοι μεταξύ τους, δηλαδή $(a,b)=1$, να βρεδεί ο μέγιστος κοινός διαιρέτης:*

$$d=\left(a^{2015}+b^{2016},ab\right)$$

Λύση. Θα δείξουμε ότι $d=1$. Υποθέτουμε ότι $d>1$. Τότε γνωρίζουμε ότι ο d έχει έναν πρώτο διαιρέτη p. Θα έχουμε:

$$p\mid d \implies \begin{cases} p\mid a^{2015}+b^{2016} \\ \quad \& \\ p\mid ab \end{cases} \implies \begin{cases} p\mid a^{2015}+b^{2016} \\ \quad \& \\ p\mid a \quad \text{ή} \quad p\mid b \end{cases}$$

(1) Αν $p\mid a$, τότε προφανώς $p\mid a^{2015}$. Επειδή $p\mid a^{2015}+b^{2016}$, έπεται ότι $p\mid b^{2016}$. Επειδή ο p είναι πρώτος, έπεται ότι $p\mid b$. Τότε θα έχουμε $p\mid a$ και $p\mid b$ και επομένως $p\mid (a,b)=1$, το οποίο είναι άτοπο.

(2) Αν $p\mid b$, τότε προφανώς $p\mid b^{2016}$. Επειδή $p\mid a^{2015}+b^{2016}$, έπεται ότι $p\mid a^{2015}$. Επειδή ο p είναι πρώτος, έπεται ότι $p\mid a$. Τότε θα έχουμε $p\mid a$ και $p\mid b$ και επομένως $p\mid (a,b)=1$, το οποίο είναι άτοπο.

Στο άτοπο καταλήξαμε υποθέτοντας ότι $d>1$. Άρα $d=1$. $\blacksquare$

Άσκηση 12. *Αν $n, m \in \mathbb{N}$, όπου $n \neq m$, να δείξετε ότι*[4]*:*

$$\left(2^{2^n}+1, 2^{2^m}+1\right) = 1$$

Με τη βοήθεια της παραπάνω σχέσης να δείξετε ότι υπάρχουν άπειροι πρώτοι αριθμοί.

Λύση. • **Πρώτος Τρόπος**: Το ζητούμενο προκύπτει θέτοντας $a = 2$ στην Άσκηση 8.

• **Δεύτερος Τρόπος**: Έστω $d = \left(2^{2^n}+1, 2^{2^m}+1\right)$. Χωρίς βλάβη της γενικότητας υποθέτουμε ότι $n > m$ και έστω $n = m + s$. Τότε

$$2^{2^n} - 1 = 2^{2^{m+s}} - 1 = 2^{2^m \cdot 2^s} - 1 = (2^{2^m})^{2^s} - 1 = \alpha^{2^s} - 1$$

όπου $\alpha = 2^{2^m}$ και άρα[5]

$$\frac{2^{2^n}-1}{2^{2^m}+1} = \frac{\alpha^{2^s}-1}{\alpha+1} = \alpha^{2^s-1} - \alpha^{2^s-2} + \cdots - 1 \in \mathbb{N}$$

Συνεπώς έχουμε

$$2^{2^m}+1 \mid 2^{2^n}-1 \implies \begin{cases} 2^{2^m}+1 \mid 2^{2^n}+1-2 \\ \\ d \mid 2^{2^m}+1 \end{cases} \implies d \mid 2^{2^n}+1-2 \implies \begin{cases} d \mid 2^{2^n}+1-2 \\ \\ d \mid 2^{2^n}+1 \end{cases} \implies d \mid 2$$

Αν ο αριθμός d είναι άρτιος, τότε $2 \mid d$ και άρα $d = 2$. Όμως αφού $2 \mid 2^{2^n}+1$ και $2 \mid 2^{2^n}$ έπεται ότι $2 \mid 1$ που είναι άτοπο. Συνεπώς ο d είναι περιττός και αφού διαιρεί το 2 έχουμε αναγκαστικά ότι $d = 1$. Άρα πράγματι

$$\left(2^{2^n}+1, 2^{2^m}+1\right) = 1$$

Θεωρούμε το σύνολο

$$\mathcal{S} = \left\{2^{2^n}+1 \mid n \in \mathbb{N}\right\} = \left\{2^{2^1}+1, 2^{2^2}+1, 2^{2^3}+1, \cdots\right\}$$

Προφανώς το παραπάνω σύνολο είναι άπειρο. Για κάθε $n \in \mathbb{N}$ έστω p_n ένας πρώτος διαιρέτης του $2^{2^n}+1$. Τότε για $n \neq m$ έπεται ότι $p_n \neq p_m$, διότι διαφορετικά αν $p_n = p_m = p$ τότε

$$p \mid 2^{2^n}+1 \quad \text{και} \quad p \mid 2^{2^m}+1 \implies p \mid \left(2^{2^n}+1, 2^{2^m}+1\right) = 1 \implies p = 1$$

που είναι άτοπο. Άρα το σύνολο των πρώτων διαιρετών των αριθμών $2^{2^n}+1$ είναι άπειρο και επομένως υπάρχουν άπειροι πρώτοι αριθμοί. ■

Άσκηση 13. *Έστω a, b θετικοί ακέραιοι και p ένας πρώτος αριθμός. Είναι οι ακόλουθες προτάσεις αληθείς ή ψευδείς; Για κάθε μια να δοθεί απόδειξη (αν η πρόταση είναι αληθής) ή να δοθεί αντιπαράδειγμα (αν η πρόταση είναι ψευδής):*

1. *Αν $(a, p^2) = p$, τότε: $(a^2, p^2) = p^2$.*
2. *Αν $(a, p^2) = p$ και $(b, p^2) = p^2$, τότε: $(ab, p^4) = p^3$.*
3. *Αν $(a, p^2) = p$ και $(b, p^2) = p$, τότε: $(ab, p^4) = p^2$.*
4. *Αν $(a, p^2) = p$, τότε: $(a + p, p^2) = p$.*

Λύση. **1.** Έστω $(a, p^2) = p$. Τότε $p \mid a$ και άρα $a = pq$ με $(p, q) = 1$. Αν $(p, q) = d$ τότε $d \mid p$ και άρα $d = 1$ ή $d = p$. Στη περίπτωση που $d = p$ έχουμε $p \mid q$, δηλαδή $q = p \cdot b$ και τότε

$$a = p \cdot q = p^2 \cdot b \implies p^2 \mid a \implies (a, p^2) = p^2 \neq p$$

[4] Οι αριθμοί $f_n = 2^{2^n}+1, \forall n \geq 0$ καλούνται αριθμοί του Fermat.

[5] Στην σχέση που ακολουθεί χρησιμοποιούμε τη γνωστή ταυτότητα

$$a^n - b^n = (a+b)(a^{n-1} - a^{n-2}b + \cdots + ab^{n-2} - b^{n-1}), \qquad \text{αν } n: \text{ άρτιος}$$

που είναι άτοπο. Άρα $(p,q)=1$. Τότε

$$a^2 = p^2 \cdot q^2 \quad \text{και} \quad p \nmid q^2 \implies (a^2, p^2) = p^2$$

Συνεπώς η πρόταση (1) είναι αληθής.

2. Θέτουμε $a=p$ και $b=p^3$. Τότε $(p,p^2)=p$ και $(p^3,p^2)=p^2$ αλλά

$$(ab, p^4) = (p\cdot p^3, p4) = (p^4, p^4) = p^4 \neq p^3$$

Άρα η δεύτερη πρόταση είναι ψευδής.

3. Υποθέτουμε ότι $(a,p^2)=p$ και $(b,p^2)=p$. Τότε

$$\begin{cases} p \mid a \\ \\ p \mid b \end{cases} \implies \begin{cases} a = p\cdot q_1 \\ \\ b = p \cdot q_2 \end{cases}$$

και προφανώς όπως στο (1) έχουμε $(p,q_1)=(p,q_2)=1$. Τότε $ab = p^2 q_1 q_2$ και p^2 είναι η μεγαλύτερη δύναμη του p που διαιρεί το ab. Επομένως $(ab,p^4)=p^2$.

4. Για $a=p=2$ έχουμε ότι $(a,p^2)=(2,2^2)=2=p$ αλλά

$$(a+p, p^2) = (2+2, 2^2) = (4,4) = 4 \neq 2 = p$$

Άρα η πρόταση (4) είναι ψευδής. ■

Άσκηση 14. **1.** *Δείξτε ότι αν b,c είναι μη μηδενικοί ακέραιοι με $(b,c)=1$ τότε να δειχθεί ότι, $\forall n,m \in \mathbb{N}$:*

$$(b, c^m) = 1 = (b^n, c)$$

2. *Θεωρούμε το πολυώνυμο με ακέραιους συντελεστές*

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n, \qquad a_i \in \mathbb{Z},\ \ 0 \leq i \leq n,\ \ n>0, \quad \& \quad a_0,\ a_n \neq 0$$

Αν $\frac{b}{c}$ είναι ρητή ρίζα του $f(x)$, όπου b,c μη μηδενικοί ακέραιοι πρώτοι μεταξύ τους, να δειχθεί ότι:

$$b \mid a_0 \quad \& \quad c \mid a_n$$

Λύση. **1.** Υποθέτουμε αντίθετα ότι $(b,c^m)=d>1$. Τότε υπάρχει πρώτος αριθμός p με $p \mid d$. Άρα $p \mid b$ και $p \mid c^m$. Αφού ο p είναι πρώτος και $p \mid c^m$ έπεται ότι $p \mid c$. Τότε έχουμε

$$p \mid b \quad \text{και} \quad p \mid c \implies p \mid (b,c) \implies p \mid 1$$

που είναι άτοπο. Συνεπώς $(b,c^m)=1$.

2. Αφού b/c είναι ρητή ρίζα του $f(x)$ τότε έχουμε

$$\begin{aligned} f(\frac{b}{c}) = 0 &\implies a_0 + a_1 \frac{b}{c} + \cdots + a_n (\frac{b}{c})^n = 0 \\ &\implies a_0 c^n + a_1 b c^{n-1} + \cdots + a_n b^n = 0 \\ &\implies a_0 c^n = b(-a_1 c^{n-1} - \cdots - a_n b^{n-1}) \\ &\implies b \mid a_0 c^n \end{aligned}$$

Αφού $(b,c)=1$ έπεται από το πρώτο μέρος της άσκησης ότι $(b,c^n)=1$. Επομένως

$$b \mid a_0 c^n \implies b \mid a_0$$

Όμοια από τη σχέση $a_0 c^n + a_1 b c^{n-1} + \cdots + a_n b^n = 0$ έπεται ότι

$$\begin{aligned} a_n b^n &= -a_0 c^n - a_1 b c^{n-1} - \cdots - a_{n-1} b^{n-1} c \\ &= c(-a_0 c^{n-1} - a_1 b c^{n-2} - \cdots - a_{n-1} b^{n-1}) \\ &\implies c \mid a_n b^n \end{aligned}$$

Αφού $(b,c)=1$ έχουμε $(c,b^n)=1$ και άρα $c \mid a_n$. ■

Άσκηση 15. *Έστω k ένας ακέραιος. Να δείξετε ότι οι αριθμοί*

$$6k-1,\ \ 6k+1,\ \ 6k+2,\ \ 6k+3,\ \ 6k+5$$

είναι σχετικά πρώτοι μεταξύ τους.

Λύση. Έστω $(6k+a, 6k+b) = d$, όπου $a, b \in \{-1, 1, 2, 3, 5\}$. Θα δείξουμε ότι $d = 1$. Έχουμε

$$\begin{cases} d \mid 6k+a \\ \\ d \mid 6k+b \end{cases} \implies \begin{cases} d \mid a-b \\ \\ d \mid b-a \end{cases}$$

Αν $a < b$, τότε $b - a \in \{1, 2, 3, 4, 6\}$. Επειδή $d \mid b-a$ έχουμε ότι $d \in \{1, 2, 3, 4, 6\}$. Αρκεί να δείξουμε ότι

$$2 \nmid 6k+a \quad \text{και} \quad 3 \nmid 6k+b$$

Αν $p = 2$ ή 3 και $p \mid (6k+a, 6k+b) = d$ τότε

$$\begin{cases} p = 2 \ \text{ ή } \ 3 \\ \\ p \mid 6k+a \end{cases} \implies \begin{cases} p \mid 6k \\ \\ p \mid 6k+a \end{cases} \implies p \mid a$$

και

$$\begin{cases} p = 2 \ \text{ ή } \ 3 \\ \\ p \mid 6k+b \end{cases} \implies \begin{cases} p \mid 6k \\ \\ p \mid 6k+b \end{cases} \implies p \mid b$$

Όμως για $p = 2$ ή 3 δεν υπάρχει $a, b \in \{-1, 1, 2, 3, 5\}$ με $p \mid a$, $p \mid b$ και $a < b$. Όμοια δουλεύουμε στη περίπτωση που $b < a$. Άρα $d = 1$ και επομένως

$$(6k+a, 6k+b) = 1, \ \ \forall a, b \in \{-1, 1, 2, 3, 5\}$$

Συνεπώς οι αριθμοί $6k-1, 6k+1, 6k+2, 6k+3, 6k+5$ είναι σχετικά πρώτοι μεταξύ τους ανα δυο και άρα είναι σχετικά πρώτοι μεταξύ τους. ■

Άσκηση 16. *Έστω $a, b \in \mathbb{N}$, και υποθέτουμε ότι: $(a, b) = 1$. Να δείξετε ότι:*

1. $\big(a+b, a-b\big) = 1 \ \ \text{ή} \ \ 2.$
2. $\big(2a+b, a+2b\big) = 1 \ \ \text{ή} \ \ 3.$
3. $\big(a+b, a-b, ab\big) = 1 \ \ \text{ή} \ \ 2.$

Μπορείτε να προσδιορίσετε, στις παραπάνω περιπτώσεις (1), (2), (3), πότε ακριβώς ο μέγιστος διαιρέτης έχει την τιμή 1, 2, ή 3;

Λύση. **1.** Έστω $d = \big(a+b, a-b\big)$. Τότε

$$\begin{cases} d \mid a+b \\ \\ d \mid a-b \end{cases} \implies \begin{cases} d \mid 2a \\ \\ d \mid 2b \end{cases}$$

Διακρίνουμε δυο περιπτώσεις:
(α): Έστω $2 \nmid d$. Τότε έχουμε

$$\begin{cases} (d, 2) = 1 \\ \\ d \mid 2a \\ \\ d \mid 2b \end{cases} \implies \begin{cases} d \mid a \\ \\ d \mid b \end{cases} \implies d \mid (a, b) = 1 \implies d = 1$$

(β): Έστω $2 \mid d$. Άρα $d = 2 \cdot d'$ και τότε

$$\begin{cases} 2a = dx = 2d'x \\ \\ 2b = dy = 2d'y \end{cases} \implies \begin{cases} d' \mid a \\ \\ d' \mid b \end{cases} \implies d' \mid (a,b) = 1 \implies d' = 1 \implies d = 2d' = 2$$

Επομένως δείξαμε ότι $\big(a+b, a-b\big) = 1 \quad$ ή $\quad 2$.

- Για το δεύτερο ερώτημα έχουμε:

Παρατηρούμε ότι, επειδή $(a,b) = 1$, οι αριθμοί a, b δεν μπορεί να είναι και οι δύο άρτιοι.

Έστω ότι οι αριθμοί a, b είναι περιττοί, δηλαδή $a = 2k+1$ και $b = 2n+1$. Τότε $a+b = 2(k+n+1)$ και $a-b = 2(k-n)$. Συνεπώς σε αυτή τη περίπτωση έχουμε ότι $d = 2$.

Αν ένας από τους αριθμούς a ή b είναι περιττός τότε το άθροισμα $a+b$ είναι περιττός, δηλαδή $2 \nmid a+b$. Άρα $d = 1$.

Αντίστροφα αν $d = 2$ από τα παραπάνω έπεται ότι οι αριθμοί a, b είναι και οι δύο περιττοί, και αν $d = 1$, τότε ο ένας είναι περιττός και ο άλλος άρτιος.

2. Έστω $d = \big(2a+b, a+2b\big)$. Τότε

$$\begin{cases} d \mid 2a+b \\ \\ d \mid a+2b \end{cases} \implies d \mid 2a+b-(a+2b) \implies d \mid a-b$$

και άρα

$$\begin{cases} d \mid a-b \\ \\ d \mid 2a+b \\ \\ d \mid a+2b \end{cases} \implies \begin{cases} d \mid 3a \\ \\ d \mid 3b \end{cases} \implies d \mid (3a, 3b) = 3(a,b) \overset{(a,b)=1}{\implies} d \mid 3$$

Συνεπώς $d = 1$ ή $d = 3$ και έτσι έχουμε το ζητούμενο.

- Για το δεύτερο ερώτημα διακρίνουμε τις παρακάτω περιπτωσεις:

(α΄) Έστω $a = 3k$. Επειδή $(a,b) = 1$, έπεται ότι $b \neq 3n$. Αν $b = 3n+1$ ή $b = 3n+2$ τότε $3 \nmid 2a+b$ και άρα $d = 1$.

(β΄) Έστω $a = 3k+1$. Αν $b = 3n$ τότε $3 \nmid 2b+a$ και άρα $d = 1$. Αν $b = 3n+1$ τότε $3 \mid 2a+b$ και $3 \mid a+2b$, συνεπώς $d = 3$. Τέλος, αν $b = 3n+2$ τότε $3 \nmid 2a+b$ και άρα $d = 1$.

(γ΄) Έστω $a = 3k+2$. Αν $b = 3n$ τότε $3 \nmid 2b+a$ και άρα $d = 1$. Αν $b = 3n+1$ τότε $3 \nmid a+2b$ και άρα $d = 1$. Αν $b = 3n+2$ τότε

$$a+2b = 3(k+2n+2) \quad \text{και} \quad 2a+b = 3(2k+n+2)$$

Επομένως $3 \mid 2a+b$ και $3 \mid a+2b$, άρα $d = 3$.

3. Από το ερώτημα (1) έχουμε

$$\big(a+b, a-b, ab\big) = \big((a+b, a-b), ab\big) = \begin{cases} (1, ab) = 1 \\ \\ (2, ab) = 1 \quad \text{ή} \quad 2 \end{cases}$$

Άρα $\big(a+b, a-b, ab\big) = 1 \quad$ ή $\quad 2$.

- Για το δεύτερο ερώτημα έχουμε:

Όπως και παραπάνω, επειδή $(a,b) = 1$, οι αριθμοί a, b δεν μπορεί και οι δύο να είναι άρτιοι. Αν ένας από τους δυο είναι άρτιος και ο άλλος είναι περιττός τότε από το ερώτημα (1) έχουμε ότι $(a+b, a-b) = 1$ και άρα $d = 1$.

Αν οι αριθμοί a, b είναι περιττοί τότε το γινόμενο ab είναι περιττός αριθμός. Άρα $2 \nmid d$ και αφού $d = 1$ ή 2 τότε αναγκαστικά έχουμε $d = 1$. ■

Άσκηση 17. *Έστω a, b φυσικοί αριθμοί με μέγιστο κοινό διαιρέτη $(a, b) = 1$. Υποθέτουμε ότι υπάρχει θετικός ακέραιος $c \in \mathbb{N}$ έτις ώστε $ab = c^2$. Να δειχθεί ότι υπάρχουν $x, y \in \mathbb{N} \cup \{0\}$ έτσι ώστε $a = x^2$ και $b = y^2$.*

Λύση. Υποθέτοντας ότι δεν υπάρχει $x \in \mathbb{N}$ με $a = x^2$ θα καταλήξουμε σε άτοπο. Η απόδειξη στην περίπτωση του b είναι εντελώς όμοια.

Αφού λοιπόν $\nexists\, x \in \mathbb{N}$ με $a = x^2$, συμπεραίνουμε ότι υπάρχει κάποιος πρώτος αριθμός p με $p \mid a$ και με $p^2 \nmid a$. Ας πούμε $a = p\ell, \ell \in \mathbb{N}$, όπου όμως $p \nmid \ell$. Συνεπώς, $(p, \ell) = 1$, αφού ο p είναι πρώτος αριθμός.

Έχουμε $ab = p\ell b = c^2$ και επομένως

$$p \mid c^2 \implies p \mid c \implies p^2 \mid c^2 = ab = p\ell b \implies p \mid \ell b$$

Αφού όμως $(p, \ell) = 1$, πρέπει $p \mid b$ και γι' αυτό $(a, b) \neq 1$ που αντίκειται στην υπόθεση ότι $(a, b) = 1$. ■

Άσκηση 18. *Έστω a, b δύο φυσικοί αριθμοί > 1 για τους οποίους ισχύει ότι:*

$$a \mid b^2,\ \ b^2 \mid a^3,\ \ a^3 \mid b^4,\ \ b^4 \mid a^5,\ \ \ldots \quad . \tag{*}$$

Να δειχθεί ότι $a = b$.

Λύση. Θεωρούμε τις πρωτογενείς αναλύσεις των a, b:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s} \qquad \& \qquad b = q_1^{\beta_1} q_2^{\beta_2} \ldots q_t^{\beta_t}$$

όπου $s, t \in \mathbb{N}$ και οι p_i, $1 \leq i \leq s$ και q_j, $1 \leq j \leq t$ είναι ανά δύο διαφορετικοί πρώτοι αριθμοί.

Παρατηρούμε ότι για τυχόντες φυσικούς αριθμούς n, m η πρωτογενής ανάλυση τού a^n είναι η

$$a^n = p_1^{n\alpha_1} p_2^{n\alpha_2} \ldots p_i^{n\alpha_i} \ldots p_s^{n\alpha_s}$$

και η πρωτογενής ανάλυση τού b^m είναι η

$$b^m = q_1^{m\beta_1} q_2^{m\beta_2} \ldots q_j^{m\beta_j} \ldots q_t^{m\beta_t}.$$

Έχουμε $\{p_1, p_2, \ldots, p_s\} \subseteq \{q_1, q_2, \ldots, q_t\}$ διότι $a \mid b^2$, και $\{q_1, q_2, \ldots, q_t\} \subseteq \{p_1, p_2, \ldots, p_s\}$ διότι $b^2 \mid a^3$. Επομένως $\{p_1, p_2, \ldots, p_s\} = \{q_1, q_2, \ldots, q_t\}$. Συνεπώς $s = t$ και επιπλέον μπορούμε να υποθέσουμε, χωρίς περιορισμό τής γενικότητας, ότι $p_i = q_i, \forall i, 1 \leq i \leq s$.

Έστω p_i οποιοσδήποτε από τους πρώτους αριθμούς τού συνόλου $\{p_1, p_2, \ldots, p_s\}$. Λόγω τής (*) έπεται ότι

$$\forall i,\ 1 \leq i \leq s: \qquad 2\beta_i \geq \alpha_i, \quad 3\alpha_i \geq 2\beta_i, \quad 4\beta_i \geq 3\alpha_i, \quad 5\alpha_i \geq 4\beta_i, \quad \ldots$$

Συνεπώς, είναι

$$\forall i,\ 1 \leq i \leq s, \qquad 5\alpha_i \geq 4\beta_i \geq 3\alpha_i, \qquad 3\alpha_i \geq 2\beta_i \geq \alpha_i.$$

Επομένως,

$$\forall i, 1 \leq i \leq s: \quad (5\alpha_i - 3\alpha_i) \geq (4\beta_i - 2\beta_i) \geq (3\alpha_i - \alpha_i) \iff 2\alpha_i \geq 2\beta_i \geq 2\alpha_i \implies \alpha_i = \beta_i$$

Επειδή οι αντίστοιχοι εκθέτες α_i και β_i των πρώτων p_i που εμφανίζονται στις πρωτογενείς αναλύσεις των αριθμών a και b είναι ίσοι $\forall i, 1 \leq i \leq s$, έπεται ότι οι a και b είναι ίσοι. ■

Άσκηση 19.

1. *Να δείξετε ότι $\big(1147, 851\big) = 37$ και ακολούθως να βρεθούν ακέραιοι x και y έτσι ώστε:*

$$37 = 1147x + 851y$$

2. *Να υπολογίσετε τον Μέγιστο Κοινό Διαιρέτη d και το Ελάχιστο Κοινό Πολλαπλάσιο δ των αριθμών 1485 και 1745. Στη συνέχεια να βρεθούν ακέραιοι x και y έτσι ώστε:*

$$d = 1485x + 1745y$$

Λύση. **1.** Έχουμε:

$$\begin{aligned} 1147 &= 851 \cdot 1 + 296 \\ 851 &= 296 \cdot 2 + 259 \\ 296 &= 259 \cdot 1 + 37 \\ 259 &= 37 \cdot 7 \end{aligned}$$

και άρα πράγματι $\big(1147, 851\big) = 37$. Έχουμε

$$\begin{aligned} 37 &= 296 - 259 \cdot 1 \\ &= 296 - 1 \cdot (851 - 296 \cdot 2) \\ &= 3 \cdot 296 - 851 \\ &= 3 \cdot (1147 - 851) - 851 \\ &= 1147 \cdot 3 + 851 \cdot (-4) \end{aligned}$$

Επομένως $x = 3$ και $y = -4$.

2. Έχουμε:

$$\begin{aligned} 1745 &= 1 \cdot 1485 + 260 \\ 1485 &= 5 \cdot 260 + 185 \\ 260 &= 1 \cdot 185 + 75 \\ 185 &= 2 \cdot 75 + 35 \\ 75 &= 2 \cdot 35 + 5 \\ 35 &= 7 \cdot 5 \end{aligned}$$

και άρα $d = \big(1485, 1745\big) = 5$. Για το Ελάχιστο Κοινό Πολλαπλάσιο δ των αριθμών $a = 1485$ και $b = 1745$ από γνωστό Θεώρημα[6] έπεται ότι

$$d \cdot \delta = |a \cdot b| = a \cdot b \implies \delta = \frac{1485 \cdot 1745}{5} = 518265$$

Έχουμε

$$\begin{aligned} 5 &= 75 - 2 \cdot 35 \\ &= 75 - 2 \cdot (185 - 2 \cdot 75) \\ &= 5 \cdot 75 - 2 \cdot 185 \\ &= 5 \cdot (260 - 1 \cdot 185) - 2 \cdot 185 \\ &= 5 \cdot 260 - 7 \cdot 185 \\ &= 5 \cdot 260 - 7 \cdot (1485 - 5 \cdot 260) \\ &= 40 \cdot 260 - 7 \cdot 1485 \\ &= 40 \cdot (1745 - 1 \cdot 1485) - 7 \cdot 1485 \\ &= -47 \cdot 1485 + 40 \cdot 1745 \end{aligned}$$

Άρα $x = -47$ και $y = 40$.

■

[6] Υπενθυμίζουμε ότι αν a, b είναι θετικοί ακέραιοι, τότε:

$$(a, b)[a, b] = ab$$

Άσκηση 20. *Αν a, b είναι φυσικοί αριθμοί, να δείξετε ότι:*

$$(a,b) = \big(a+b, [a,b]\big)$$

Ως εφαρμογή, βρείτε δύο φυσικούς αριθμούς έτσι ώστε το άθροισμά τους να είναι 798 και το ελάχιστο κοινό τους πολλαπλάσιο να είναι 10.780.

Λύση. Έστω $d = (a,b)$. Τότε $a = da'$ και $b = db'$ με a', b' ακέραιους. Έχουμε

$$\begin{aligned} \big(a+b, [a,b]\big) &= \big(da' + db', [da', db']\big) \\ &= \big(d(a'+b'), d[a',b']\big) \\ &= d\big(a'+b', [a',b']\big) \end{aligned}$$

Επίσης

$$(a,b) = (da', db') = d(a', b')$$

και άρα αρκεί να δείξουμε ότι

$$\big(a'+b', [a',b']\big) = (a',b')$$

Γνωρίζουμε από τη Θεωρία ότι αν $d = (a,b)$ τότε $(\frac{a}{d}, \frac{b}{d}) = 1$. Επομένως έχουμε ότι $(a',b') = 1$ και άρα από τη παραπάνω σχέση αρκεί να δείξουμε ότι

$$\big(a'+b', [a',b']\big) = 1$$

Έχουμε

$$\big(a'+b', [a',b']\big) = \big(a'+b', \frac{a'b'}{(a',b')}\big) = \big(a'+b', a'b'\big)$$

Υποθέτουμε ότι $\big(a'+b', a'b'\big) \neq 1$ και θα καταλήξουμε σε αντίφαση. Τότε υπάρχει πρώτος αριθμός p έτσι ώστε $p \mid a'+b'$ και

$$p \mid a'b' \implies p \mid a' \quad \text{ή} \quad p \mid b'$$

Αν $p \mid a'$ τότε

$$\begin{cases} p \mid a' \\ \\ p \mid a'+b' \end{cases} \implies p \mid b' \implies p \mid (a',b') = 1$$

που είναι άτοπο. Όμοια καταλήγουμε σε άτοπο αν $p \mid b'$. Άρα $\big(a'+b', a'b'\big) = 1$ και επομένως έχουμε το ζητούμενο: $(a,b) = \big(a+b, [a,b]\big)$.

- Εφαρμογή: Ψαχνουμε δύο φυσικούς αριθμούς a, b έτσι ώστε $a+b = 798$ και $[a,b] = 10.780$. Μπορούμε να υποθέσουμε ότι $a \geq b$. Εύκολα βρίσκουμε ότι $\big(a+b, [a,b]\big) = (798, 10780) = 14$ και άρα $(a,b) = 14$. Επομένως

$$(a,b) \cdot [a,b] = a \cdot b \implies a \cdot b = 14 \cdot 10780 = 150920$$

Άρα ψάχνουμε a, b έτσι ώστε

$$\begin{cases} a+b = 798 \\ \\ a \cdot b = 150920 \end{cases}$$

Λύνοντας το παραπάνω σύστημα βρίσκουμε ότι $a = 490$ και $b = 308$. ■

Άσκηση 21. *Αν a, b, c είναι φυσικοί αριθμοί, να δείξετε ότι:*

$$(a,b,c)[ab, ac, bc] = abc \quad \& \quad [a,b,c](ab, ac, bc) = abc$$

Λύση. Αν $a=b=c=1$ τότε η πρόταση είναι φανερή. Υποθέτουμε ότι τουλαχιστον ένα από τα a,b,c είναι μεγαλύτερο του 1. Έστω $p_1,\dots,p_k$ οι πρώτοι που διαιρούν τουλάχιστον ένα από τα a,b,c. Τότε υπάρχουν $a_i,b_i,c_i\geq 0$ ώστε

$$a=p_1^{a_1}p_2^{a_2}\dots p_k^{a_k},\quad b=p_1^{b_1}p_2^{b_2}\dots p_k^{b_k},\quad c=p_1^{c_1}p_2^{c_2}\dots p_k^{c_k}$$

Έχουμε

$$ab=p_1^{a_1+b_1}p_2^{a_2+b_2}\dots p_k^{a_k+b_k},\quad ac=p_1^{a_1+c_1}p_2^{a_2+c_2}\dots p_k^{a_k+c_k},\quad bc=p_1^{b_1+c_1}p_2^{b_2+c_2}\dots p_k^{b_k+c_k}$$

και

$$\begin{cases}[a,b,c]=p_1^{\max\{a_1,b_1,c_1\}}\dots p_k^{\max\{a_k,b_k,c_k\}}\\ \\ (ab,ac,bc)=p_1^{\min\{a_1+b_1,a_1+c_1,b_1+c_1\}}\dots p_k^{\min\{a_k+b_k,a_k+c_k,b_k+c_k\}}\end{cases}$$

Τότε

$$\begin{aligned}[a,b,c](ab,ac,bc) &= p_1^{\max\{a_1,b_1,c_1\}}\dots p_k^{\max\{a_k,b_k,c_k\}}p_1^{\min\{a_1+b_1,a_1+c_1,b_1+c_1\}}\dots p_k^{\min\{a_k+b_k,a_k+c_k,b_k+c_k\}}\\ &= p_1^{a_1+b_1+c_1}\dots p_k^{a_k+b_k+c_k}\\ &= abc\end{aligned}$$

Για τη δεύτερη ισότητα παρατηρήστε ότι αν για παράδειγμα $\max\{a_1,b_1,c_1\}=a_1$ τότε $\min\{a_1+b_1,a_1+c_1,b_1+c_1\}=b_1+c_1$.

Για τη πρώτη σχέση δουλεύοντας όπως παραπάνω έχουμε

$$\begin{aligned}(a,b,c)[ab,ac,bc] &= p_1^{\min\{a_1,b_1,c_1\}}\dots p_k^{\min\{a_k,b_k,c_k\}}p_1^{\max\{a_1+b_1,a_1+c_1,b_1+c_1\}}\dots p_k^{\max\{a_k+b_k,a_k+c_k,b_k+c_k\}}\\ &= p_1^{a_1+b_1+c_1}\dots p_k^{a_k+b_k+c_k}\\ &= abc\end{aligned}$$

Άρα $(a,b,c)[ab,ac,bc]=abc$. ■

Άσκηση 22. *Έστω F_n και F_{n+1} δύο διαδοχικοί όροι της ακολουθίας Fibonacci, όπου $n\in\mathbb{N}$. Δείξτε ότι*

$$\big(F_n,F_{n+1}\big)=1,\quad \forall n\in\mathbb{N}$$

και επιπλέον δείξτε ότι στον Ευκλείδειο Αλγόριθμο για την εύρεση του μέγιστου κοινού διαιρέτη $(F_{n+1},F_{n+2})=1$, $n>1$, απαιτούνται ακριβώς n διαιρέσεις.

Λύση. Έστω $d=(F_n,F_{n+1})$. Τότε

$$d\mid F_n\quad\text{και}\quad d\mid F_{n+1}\tag{1}$$

Αν $n=1$ τότε $F_1=1$, $F_2=1$ και άρα $(F_1,F_2)=1$. Έστω $n\geq 2$. Τότε $F_{n+1}=F_n+F_{n-1}$ και από τη σχέση (1) έπεται ότι

$$d\mid F_{n-1}\tag{2}$$

Αφού $F_n=F_{n-1}+F_{n-2}$ τότε από τις σχέσεις (1) και (2) έχουμε ότι $d\mid F_{n-2}$. Συνεχίζοντας αυτή τη διαδικασία έχουμε

$$d\mid F_1=1\implies d=1=(F_n,F_{n+1})$$

Για την εύρεση του μέγιστου κοινού διαιρέτη (F_{n+1},F_{n+2}) από τον Ευκλείδειο Αλγόριθμο έχουμε

$$\begin{aligned}F_{n+2} &= F_{n+1}\cdot 1+F_n\\ F_{n+1} &= F_n\cdot 1+F_{n-1}\\ F_n &= F_{n-1}\cdot 1+F_{n-2}\\ &\vdots\\ F_4 &= F_3\cdot 1+F_2\\ F_3 &= F_2\cdot 2\end{aligned}$$

Συνεπώς έχουμε n το πλήθος διαιρέσεων και $(F_{n+2}, F_{n+1}) = F_2 = 1$. ■

Άσκηση 23. *Έστω $\{F_n\}_{n\geq 1}$ η ακολουθία Fibonacci. Να δείξετε ότι:*

(1)
$$F_{n+m} = F_m F_{n+1} + F_{m-1} F_n$$

(2)
$$n \mid m \implies F_n \mid F_m$$

(3)
$$(F_n, F_m) = F_{(n,m)}$$

Λύση. (1) Έστω $m \geq 1$ σταθερό. Θα εφαρμόσουμε την Αρχή της Μαθηματικής Επαγωγής ως προς $n \in \mathbb{N}$. Έχουμε:

• $n = 1$:
$$\begin{aligned} F_{m+1} &= F_m + F_{m-1} \\ &= F_m \cdot 1 + F_{m-1} \cdot 1 \\ &= F_m \cdot F_2 + F_{m-1} \cdot F_1 \\ &= F_m \cdot F_{1+1} + F_{m-1} \cdot F_1 \end{aligned}$$

Συνεπώς για $n = 1$ ισχύει.

• <u>*Επαγωγική Υπόθεση*</u>: Υποθέτουμε ότι
$$F_{m+r} = F_m \cdot F_{r+1} + F_{m-1} \cdot F_r$$
για κάθε $r = 1, 2, \cdots, k$.

• Για $r = k+1$ έχουμε
$$\begin{aligned} F_{m+k+1} &= F_{m+k} + F_{m+k-1} \\ &= F_m \cdot F_{k+1} + F_{m-1} \cdot F_k + F_m \cdot F_k + F_{m-1} \cdot F_{k-1} \\ &= F_m \cdot (F_{k+1} + F_k) + F_{m-1} \cdot (F_k + F_{k-1}) \\ &= F_m \cdot F_{k+2} + F_{m-1} \cdot F_{k+1} \end{aligned}$$

Επομένως για κάθε $n, m \geq 1$ ισχύει: $F_{n+m} = F_m F_{n+1} + F_{m-1} F_n$.

(2) Έστω $n \mid m$. Τότε υπάρχει $k \in \mathbb{N}$ έτσι ώστε $m = n \cdot k$.

• $k = 1$: Τότε $m = n$ και άρα $F_n \mid F_m$.

• $k = 2$: Άρα $m = 2n = n + n$ και τότε
$$F_m = F_{2n} = F_{n+n} = F_n \cdot F_{n+1} + F_{n-1} \cdot F_n = F_n \cdot (F_{n+1} + F_{n-1}) \implies F_n \mid F_m$$

• <u>*Επαγωγική Υπόθεση*</u>: Υποθέτουμε ότι $m = n \cdot k$ και $F_n \mid F_m$ για $k = 1, 2, \cdots, k-1$. Τότε έχουμε
$$F_m = F_{nk} = F_{(k-1)n+n} = F_n \cdot F_{(k-1)n+1} + F_{n-1} F_{(k-1)n}$$
Όμως από την υπόθεση της επαγωγής έχουμε ότι $F_n \mid F_{(k-1)n}$ και άρα $F_n \mid F_{n-1} F_{(k-1)n}$. Επομένως από τη παράπανω σχέση έπεται ότι $F_n \mid F_m$ και έτσι έχουμε το ζητούμενο.

(3) Μπορούμε να υποθέσουμε ότι $m \geq n$. Επομένως αρκεί να δείξουμε με ισχυρή επαγωγή ότι για κάθε $m \geq 1$ η πρόταση $P(m)$ ισχύει, όπου $P(m)$ είναι η πρόταση: Αν $0 < n \leq m$ τότε $(F_n, F_m) = F_{(n,m)}$.

Η $P(1)$ προφανώς ισχύει. Η $P(2)$ επίσης ισχύει, γιατί τότε αναγκαστικά $n = 1$ ή $n = 2$ και στις δύο περιπτώσεις
$$(F_n, F_m) = (1, 1) = 1 = F_{(n,m)}.$$

Έστω $m \geq 3$ και υποθέτουμε ότι οι $P(1), P(2), \ldots, P(m-1)$ ισχύουν. Θα δείξουμε ότι ισχύει η $P(m)$. Αν $m = n$ αυτό που θέλουμε να δείξουμε προφανώς ισχύει. Υποθέτουμε $m > n$. Θέτουμε $r_0 = m$, $r_1 = n$ και εφαρμόζουμε την Ευκλείδεια Διαίρεση:

$$\begin{aligned} r_0 &= r_1 q_1 + r_2 \quad 0 \leq r_2 < r_1 \\ r_1 &= r_2 q_2 + r_3 \quad 0 \leq r_3 < r_2 \\ &\vdots \\ r_{t-2} &= r_{t-1} q_{t-1} + r_t \quad 0 \leq r_t < r_{t-1} \\ r_{t-1} &= r_t q_t \end{aligned}$$

Άρα $(m, n) = (r_0, r_1) = r_t$. Από το μέρος (1) της άσκησης έχουμε

$$F_m = F_{r_1 q_1 + r_2} = F_{r_1 q_1} \cdot F_{r_2+1} + F_{r_1 q_1 - 1} \cdot F_{r_2}$$

Άρα

$$(F_m, F_n) = (F_{r_1 q_1 + r_2}, F_n) = (F_{r_1 q_1} \cdot F_{r_2+1} + F_{r_1 q_1 - 1} \cdot F_{r_2}, F_{r_1})$$

Από το μέρος (2) της άσκησης έπεται ότι $F_{r_1} \mid F_{r_1 q_1}$ αφού $r_1 \mid r_1 q_1$. Τότε έχουμε

$$(F_m, F_n) = (F_{r_1 q_1 - 1} \cdot F_{r_2}, F_{r_1}) \tag{1}$$

Έστω a ο μεγαλύτερος από τα $r_1 = n$ και $r_1 q_1 - 1$. Άφού $r_1 q_1 - 1 = r_0 - r_2 - 1 < r_0 = m$ και υποθέσαμε ότι $m > n$, έχουμε $a < m$. Επομένως από την υπόθεση της επαγωγής η $P(a)$ ισχύει. Χρησιμοποιώντας ότι

$$(r_1, r_1 q_1 - 1) = (r_1, -1) = (r_1, 1) = 1$$

έχουμε από υπόθεση επαγωγής ότι $(F_{r_1 q_1 - 1}, F_{r_1}) = F_1 = 1$. Επομένως, η ισότητα (1) συνεπάγεται ότι

$$(F_m, F_n) = (F_{r_0}, F_{r_1}) = (F_{r_1}, F_{r_2})$$

Παρόμοια για κάθε i έχουμε ότι

$$(F_{r_i - 1}, F_{r_i - 2}) = (F_{r_i}, F_{r_i - 1})$$

και άρα έπεται ότι

$$(F_m, F_n) = (F_{r_2}, F_{r_1}) = \cdots = (F_{r_t}, F_{r_t - 1}) = F_{r_t}$$

Η τελευταία ισότητα ισχύει από το μέρος (2) της άσκησης διότι $r_t \mid r_{t-1}$. Όμως $r_t = (m, n)$ και άρα $(F_m, F_n) = F_{(m,n)}$. ■