Φυλλάδιο 2

Βρείτε όλα τα $n \in \mathbb{N}$ για τα οποία $\phi(n)$ περιττός.

Λύση:

$\phi(1) = 1$, $\phi(2) = 2\left(1 - \frac{1}{2}\right) = 1$.

$\phi(3) = 3\left(1 - \frac{1}{3}\right) = 2$, $\phi(4) = \phi(2^2) = 2^2\left(1 - \frac{1}{2}\right) = 2$

$\phi(5) = 5\left(1 - \frac{1}{5}\right) = 4$.

Ισχυρισμός: Έστω $n \geq 3$. Τότε $\phi(n)$ άρτιος

Απόδειξη: Περίπτωση 1: $\exists$ περιττός πρώτος p_1 με $p_1 | n$

Άρα $n = 2^a p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$, όπου $a \geq 0$, $b_i \geq 1$ $\forall i$,

p_i περιττοί πρώτοι με $p_i \neq p_j$ για $i \neq j$

Άρα: Αν $a = 0$, $\phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) = (p_1 - 1) \cdots (p_r - 1) p_1^{b_1 - 1} \cdots p_r^{b_r - 1}$

που είναι άρτιος, γιατί $p_1 - 1$ άρτιος.

Αν $a > 0$ $\phi(n) = n\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) = 2^{a-1}(p_1 - 1) \cdots (p_r - 1) \cdot p_1^{b_1 - 1} \cdots p_r^{b_r - 1}$

που είναι άρτιος, γιατί $p_1 - 1$ άρτιος

Περίπτωση 2: $\exists a \geq 2$ με $n = 2^a$,

τότε $\phi(n) = 2^a\left(1 - \frac{1}{2}\right) = 2^{a-1}$ άρτιος, γιατί $a \geq 2$

ΠΑΡΑΤΗΡΗΣΗ: Χρησιμοποιήσαμε ότι αν $n \geq 3$ ακέραιος, τότε

ή n διαιρείται από περιττό πρώτο

ή n δύναμη του 2

Φυλ 7 ασκ 3. Να βρεθούν $n \in \mathbb{N}$ με $\phi(n) = 2, 4, 6, 8, 10, 12$.

Λύση:

$\phi(3) = 3\left(1 - \frac{1}{3}\right) = 2$, $\phi(5) = 4$, $\phi(7) = 6$.

$\phi(16) = \phi(2^4) = 2^4\left(1 - \frac{1}{2}\right) = 2^3 = 8$, $\phi(11) = 10$, $\phi(13) = 12$

Φυλ 7 ασκ 4.

Ν.Ο. $\nexists n \in \mathbb{N}$ με $\phi(n) = 14$

Λύση:

Έστω ότι $\exists n \in \mathbb{N}$ με $\phi(n) = 14$. Αφού $\phi(n) = \#U(2n)$ έχουμε $n \geq 15$.

Ισχυρισμός 1: $\nexists$ περιττοί πρώτοι $p_1 \neq p_2$ με $p_1 | n$ και $p_2 | n$.

Απόδειξη ↓: Έστω ότι $n = 2^a p_1^{b_1} p_2^{b_2} p_3^{b_3} \cdots p_r^{b_r}$ με $a \geq 0$, $b_i \geq 1$ $\forall i$ $r \geq 2$ και p_i περιττοί πρώτοι με $p_i \neq p_j$ για $i \neq j$

Τότε: (i) Αν $a = 0$ $\phi(n) = (p_1 - 1)(p_2 - 1) \cdots (p_r - 1) p_1^{b_1 - 1} p_2^{b_2 - 1} \cdots p_r^{b_r - 1}$

Αφού $2 | (p_1 - 1)$ και $2 | (p_2 - 1) \Rightarrow 4 | \phi(n) = 14$, αντίφαση

(ii) Αν $a \geq 1$ $\phi(n) = 2^{a-1}(p_1 - 1) \cdots (p_r - 1) p_1^{b_1 - 1} p_2^{b_2 - 1} \cdots p_r^{b_r - 1}$

και $2 | p_1 - 1$ και $2 | p_2 - 1 \Rightarrow 4 | (p_1 - 1)(p_2 - 1) \Rightarrow 4 | \phi(n) = 14$, αντίφαση

Συνεπώς, $n = 2^a p_1^b$ με p_1 περιττό πρώτο, $a \geq 0$, $b \geq 0$

Υποπερίπτωση 1: $a = 0$. Τότε $n = p_1^b$ με $b \geq 1$

(Αφού $n \geq 15$), άρα $\phi(n) = (p_1 - 1) p_1^{b-1} = 14 = 2 \cdot 7$

Αν $b = 1 \Rightarrow p_1 = 2 \cdot 7 + 1 = 15$, αντίφαση

Αν $b \geq 2$, $p_1 | p_1^{b-1} \Rightarrow p_1 | 2 \cdot 7 \Rightarrow p_1 = 7$ (p_1 περιττός)

και άρα $2 = p_1 - 1 = 7 - 1 = 6$, αντίφαση

Υποπερίπτωση 2: $a = 1$. Τότε $\phi(n) = \phi(2 \cdot p_1^b) = 2 p_1^b \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{p_1}\right) =$

$= \phi(p_1^b)$

Αντίφαση, όπως ↓

Υποπερίπτωση 3: $a \geq 2$

Τότε αν $b=0$. $\phi(n)=\phi(2^a)=2^a\left(1-\frac{1}{2}\right)=2^{a-1}=14$

αυτίφαση, γιατί 14 όχι δύναμη του 2.

Εστω αν $b \geq 1$

$$\phi(n)=\phi(2^a p_1)=2^a p_1\left(1-\frac{1}{2}\right)\left(1-\frac{1}{p_1}\right)=$$
$$=2^{a-1}p_1(p_1-1)$$

Άρα $\left.\begin{array}{l} 2 \mid 2^{a-1} \\ \text{κ'} \\ 2 \mid p_1-1 \end{array}\right\} \Rightarrow 4 \mid \phi(n)=14$, αυτίφαση

Φυλ 7 σελ 5. Έστω $n \in \mathbb{N}$. Θέτουμε $S=\{x \in \mathbb{N} : \phi(n)=n\}$. Δ.Ο. S πεπερασμένο σύνολο.

(παρατήρηση: αυτό σύνθεση, το κενό σύνολο είναι πεπερασμένο)

Λύση: Έστω $x=p_1^{b_1}p_2^{b_2}\cdots p_r^{b_r}$ πρωτογενής ανάλυση με p_i πρώτους, $p_i \neq p_j$ για $i \neq j$ κ' $b_i>0$. Τότε

$$\phi(x)=x\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right)=(p_1-1)(p_2-1)\cdots(p_r-1)p_1^{b_1-1}\cdots p_r^{b_r-1}$$

Υποθέτουμε $\phi(x)=n$

Τότε από (*) $\phi(x) \geq p_i-1 \ \forall i \Rightarrow n \geq p_i-1 \Rightarrow p_i \leq n+1$

Συνεπώς, οι πρώτοι διαιρέτες του x (με $\phi(x)=n$) είναι $\leq n+1$, άρα πεπερασμένο σύνολο.

Έστω $T=\{p_i : p \text{ πρώτος κ' } p \leq n+1\}=\{q_1,\dots,q_w\}$

Άρα $x=q_1^{c_1}\cdots q_r^{c_r}$ με $c_i \geq 0$. Αν κάποιο $c_i \geq 2$,

τότε από (*) $q_i^{c_i-1} \mid \phi(x)=n$, αυτίφαση, γιατί $q_i \geq 2$

άρα $q_i^{c_i-1} > n$

Άρα $\forall i$, το σύνολο των θετικών εκθετών c_i είναι πεπερασμένο. Το αποτέλεσμα έπεται

ΥΠΕΝΘΥΜΙΣΗ: Θ.Wilson (άλλη διατύπωση) p πρώτος $\Rightarrow (p-1)! \equiv -1 \bmod p$

Φυλ 7 αθκ 11

Έστω $p>2$ πρώτος. Τότε $(p-2)! \equiv 1 \bmod p$

Απόδειξη: Έχουμε από Θ. Wilson $[(p-1)!]_p = [-1]_p$

$\Leftrightarrow [(p-2)!(p-1)]_p = [-1]_p$ $[p-1]_p [(p-2)!] = [-1]_p \Rightarrow$

$[-1]_p [(p-2)!]_p = [-1]_p \Rightarrow [-1]_p [-1]_p [(p-2)!]_p = [-1]_p [-1]_p$

$\rightarrow [(p-2)!]_p = [1]_p$. Άρα $(p-2)! \equiv 1 \bmod p$

Φυλ 7 αθκ 7. Ο.Ο. $11 | 10!+1$ κ' $13 | 12!+1$

Λύση: 11 πρώτος, άρα από Θ.Wilson $10! \equiv -1 \bmod 11$, δηλαδή $11 | 10!+1$

13 πρώτος, άρα από Θ. wilson $12! \equiv -1 \bmod 13$, δηλ δηλαδή $13 | 12!+1$.

(Υπενθύμιση: $a \equiv b \bmod m$ σημ $m | (a-b)$

ΥΠΕΝΘΥΜΙΣΗ: (1) Αν $m \geq 2$ κ' $ΜΚΔ(a,m) = 1$, τότε $a^{\varphi(m)} \equiv 1 \bmod m$

(2) Αν p πρώτος κ' $p \nmid a$, τότε $a^{p-1} \equiv 1 \bmod p$

(3) Αν p πρώτος κ' $a \in \mathbb{Z}$, τότε $a^p \equiv a \bmod p$

(4) Αν $a, b \geq 1$ κ' $c \in \mathbb{N}$, με $ΜΚΔ(a,b) = 1$,

τότε $ab | c$ σημ $a | c$ κ' $b | c$

π.χ $15 | n$ σημ $(3 | n)$ κ' $(5 | n)$

σημ (το τελευταίο δεκαδικό ψηφίο του n είναι 0 ή 5 κ' το 3 διαιρεί το

άθροισμα των δεκαδικών ψηφίων του n)

Θεωρούμε τη συνάρτηση με $D.O. = \mathbb{R}$

$$\alpha(x) = \frac{1}{5}x^5 + \frac{1}{3}x^3 + \frac{7}{15}x$$

Λύση: $\alpha = \frac{3x^5 + 5x^3 + 7x}{15}$. Συνεπώς αρκεί να $\forall x \in \mathbb{R}, 15 \mid (3x^5 + 5x^3 + 7x)$.

Αφού $15 = 3 \cdot 5$ και $\mu\kappa\delta(3,5) = 1$

αρκεί να $\forall n \in \mathbb{Z}$, $3 \mid 3n^5+5n^3+7n$
$5 \mid 3n^5+5n^3+7n$ γι' αυτό

Για το 3: $[3n^6]_3 = [3]_3[n^5]_3 = [0]_3[n^5]_3 = [0]_3$
Αφού 3 πρώτος $[n^3]_3 = [n]_3 \Rightarrow [5n^3]_3 = [5]_3[n^3]_3 = [2]_3[n]_3 = [2n]_3$
κ' $[7n]_3 = [7]_3[n]_3 = [1]_3[n]_3 = [n]_3$
$[3n^5+5n^3+7n]_3 = [0]_3 + [2n]_3 + [n]_3 = [3n]_3 = [3]_3[n]_3 = [0]_3[n]_3 = [0]_3$
Συνεπώς, $3 \mid 3n^5+5n^3+7n$

Για το 5: Αφού 5 πρώτος $[n^5]_n = [n]_5 \Rightarrow [3n^5]_5 = [3]_5[n^5]_5 = [3]_5[n]_5 = [3n]_5$
$[5n^3]_5 = [5]_5[n^3]_5 = [0]_5[n^3]_5 = [0]_5$
$[7n]_5 = [70]_5[n]_5 = [2]_5[n]_5 = [2n]_5$
Συνεπώς, $[3n^5+5n^3+7n]_5 = [3n^5]_5 + [5n^3]_5 + [7n]_5$
$= [3n]_5 + [0]_5 + [2n]_5 = [5n]_5 = [5]_5[n]_5 = [0]_5[n]_5 = [0]_5$

Άρα $5 \mid 3n^5+5n^3+7n$

Φυλ 7 σελ 10.
Δ.Ο. $\forall n \in \mathbb{Z}$, $42 \mid n^7-n$
Λύση:
$42 \mid 2 \cdot 3 \cdot 7$
Άρα αρκεί να $\forall n$, $2 \mid n^7-n$, $3 \mid n^7-n$ κ' $7 \mid n^7-n$
(γιατί αν $a,b,c,d \in \mathbb{Z}$ με $a \geq 1, b \geq 1, c \geq 1$ κ' $\text{ΜΚΔ}(a,b)=1$, $\text{ΜΚΔ}(a,c)=1$, $\text{ΜΚΔ}(b,c)=1$ έχουμε $abc \mid d$ αν $a \mid d$ κ' $b \mid d$ κ' $c \mid d$)

Για το 2: Από θεώρημα, αφού 2 πρώτος $n^2 \equiv n \bmod 2$. Άρα $[n^2]_2 = [n]_2$
$\Rightarrow ([n^2]_2)^2 = ([n]_2)^2 \Rightarrow [n^4]_2 = [n^2]_2 = [n]_2 \Rightarrow$
$[n^5]_2 = [n^4]_2[n]_2 = [n]_2[n]_2 = [n^2]_2 = [n]_2 \Rightarrow$

$[n^7]_2 = [n^5]_2 [n^2]_2 = [n]_2 [n]_2 = [n^2]_2 = [n]_2$, άρα $2 | n^7 - n$

Για το 3 από θεώρημα. $n^3 \equiv n \bmod 3$. Άρα $[n^3]_3 = [n]_3 \Rightarrow$

$[n^3]_3 [n^3]_3 = [n]_3 [n]_3$

$\Rightarrow [n^7]_3 = [n]_3 [n]_3 [n]_3 \Rightarrow [n^3]_3 = [n]_3$

Συνεπώς, $3 | n^7 - n$

Τέλος, για το 7, από το θεώρημα $n^7 \equiv n \bmod 7$, γιατί 7 πρώτος

άρα $7 | n^7 - n$

ΥΠΕΝΘΥΜΙΣΗ: Έαν $n \geq 2$ κ' $a, r \in \mathbb{Z}$. Αν $[a]_n = [r]_n$ κ' $0 \leq r \leq n-1$, τότε r είναι το υπόλοιπο της Ευκλείδειας Διαίρεσης του a με το n

Φυλ 7 αβκ 8: Βρείτε το υπόλοιπο της Ευκλείδειας Διαίρεσης του

$a = 7 \cdot 8 \cdot 9 \cdot 15 \cdot 16 \cdot 17 \cdot 23 \cdot 24 \cdot 25 \cdot 43$ με το 11

Λύση: Έχουμε $[15]_{11} = [4]_{11}$, $[16]_{11} = [5]_{11}$, $[17]_{11} = [6]_{11}$, $[23]_{11} = [1]_{11}$

$[24]_{11} = [9]_{11}$, $[25]_{11} = [3]_{11}$ κ' $[43]_{11} = [10]_{11}$.

Άρα $[a]_{11} = [7]_{11} [8]_{11} [9]_{11} [4]_{11} [5]_{11} [6]_{11} [1]_{11} [9]_{11} [3]_{11} [10]_{11}$

$= [10!]_{11} \equiv [-1]_{11} = [10]_{11}$

Θ. Wilson, για 11 πρώτος

Συνεπώς, το υπόλοιπο είναι 10

• Το ίδιο του 5^{100} με το 7

Λύση: Έχουμε 7 πρώτος, άρα $\phi(7) = 7 - 1 = 6$ κ' $\mu\kappa\delta(5, 7) = 1$.

Συνεπώς, από Θ. Euler-Fermat $5^{\phi(7)} \equiv 1 \bmod 7 \Rightarrow 5^6 \equiv 1 \bmod 7$

Έχουμε $100 = 16 \cdot 6 + 4 = 16\phi(7) + 4$

$100 \mid 6$
$40 \quad 16$
4

Συνεπώς, $[5^{100}]_7 = [5^{16\phi(7)+4}]_7 = ([5^{\phi(7)}]_7)^{16} [5^4]_7 = [1]_7 [5^4]_7 =$

Θ. Euler-Fermat

$= [5^4]_7 = ([5^2]_7)^2 = ([4]_7)^2 = [16]_7 = [2]_7$

Συνεπώς, το υπόλοιπο είναι 2