

07/05/15.

Hinweis zum Euler

$$\varphi: \mathbb{N} \rightarrow \mathbb{C}, \quad \varphi(n) = \left| \left\{ k \in \mathbb{N} \mid \begin{array}{l} 1 \leq k \leq n \\ (k, n) = 1 \end{array} \right\} \right|$$

$$\varphi(1) = 1$$

$$\varphi(6) = 2$$

$$\varphi(2) = 1$$

$$\varphi(7) = 6$$

$$\varphi(3) = 2$$

$$\varphi(8) = 4$$

$$\varphi(4) = 2$$

$$\varphi(9) = 6$$

$$\varphi(5) = 4$$

$$\varphi(10) = 4$$

ΘΕΩΡΗΜΑ GAUSS : $\forall n \in \mathbb{N}$: $n = \sum_{d|n} \varphi(d)$

Απόδειξη : Θεωρούμε το σύνολο $N_n = \{1, 2, \dots, n\}$.

Για κάθε $d|n$:

$$S_d = \{t \in \mathbb{N} \mid (t, n) = d\}.$$

Θ.δ.ο. η συλλογή των υποσυνόλων $\{S_d\}_{d|n}$ είναι μια διαμέριση του N_n .

• $\forall d|n : d \in S_d \Rightarrow S_d \neq \emptyset$.

• Έστω $S_{d_1} \cap S_{d_2} \neq \emptyset$ όπου $d_1|n$ & $d_2|n$.

Τότε $\exists t \in S_{d_1} \cap S_{d_2} \Rightarrow \begin{cases} t \in S_{d_1} \Rightarrow (t, n) = d_1 \\ t \in S_{d_2} \Rightarrow (t, n) = d_2 \end{cases} \Rightarrow \boxed{d_1 = d_2}$

Επομένως : $d_1 \neq d_2 \Rightarrow S_{d_1} \cap S_{d_2} = \emptyset$.

• Θ.δ.ο. $N_n = \bigcup_{d|n} S_d$. Διότι αν $t \in N_n = \{1, 2, \dots, n\}$ & αν $(t, n) = d \stackrel{d|n}{\Rightarrow}$ $d|n$ & οραφάτως $t \in S_d$.

Άρα $\{S_d\}_{d|n}$ είναι διαμέριση του N_n .

Τότε $|N_n| = n = \sum_{d|n} |S_d|$ & άρα αρκεί να β
$$n = \sum_{d|n} \varphi(d)$$

Θεωρούμε το σύνολο $A_d = \left\{ b \in \mathbb{N} : \begin{matrix} 1 \leq b \leq \frac{n}{d} \\ (b, \frac{n}{d}) = 1 \end{matrix} \right\} \forall d|n$.

Οό $|S_d| = |A_d|$

Προφανώς $|A_d| = \varphi\left(\frac{n}{d}\right)$ (κατά ορισμό).

Θεωρούμε την αντιστοίχηση : $f : S_d \rightarrow A_d$, $f(t) = \frac{t}{d}$

Διότι $t \in S_d \Rightarrow (t, n) = d \Rightarrow \left(\frac{t}{d}, \frac{n}{d}\right) = 1 \Rightarrow \frac{t}{d} \in A_d$.

Η f είναι 1-1 διότι για $t_1, t_2 \in S_d$ $f(t_1) = f(t_2) \Rightarrow \frac{t_1}{d} = \frac{t_2}{d} \Rightarrow \boxed{t_1 = t_2}$

If f είναι επί στον $\mathbb{N}$ αν $b \in A_d \Rightarrow 1 \leq b \leq \frac{n}{d}$ & $f(b, \frac{n}{d}) = 1$.

Τότε για $t = b \cdot d \Rightarrow f(b \cdot d) = \frac{bd}{d} = b$

Άρα $|A_d| = |S_d|$

Άρα $n = \sum_{d|n} |S_d| = \sum_{d|n} |A_d| = \sum_{d|n} \varphi(\frac{n}{d}) = \sum_{d|n} \varphi(d)$.

↔

$n = \sum_{d|n} \varphi(d) \Rightarrow i(n) = \sum_{d|n} \varphi(d) \stackrel{\text{Möbius}}{=} \varphi(n) = \sum_{d|n} \mu(d) i(\frac{n}{d}) \Rightarrow$

$\Rightarrow \varphi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d} \Rightarrow \forall n \in \mathbb{N}: \varphi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d} =$

$= \sum_{d|n} \mu(\frac{n}{d}) \cdot d = \varphi(n) \Rightarrow \boxed{\varphi = \mu * i} \Rightarrow \begin{matrix} \text{ } \\ \text{ } \end{matrix} \xrightarrow[k \in \mathbb{N}]{l \in \mathbb{N}}$

$\Rightarrow \boxed{\varphi \in M} \Rightarrow \forall n \in \mathbb{N} \exists n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ (συνθετός αριθμός)
 $\varphi(n) = \varphi(p_1^{\alpha_1} \dots p_k^{\alpha_k}) =$
 $= \varphi(p_1^{\alpha_1}) \dots \varphi(p_k^{\alpha_k})$.

Άρα αρκεί να γνωρίζουμε την τιμή $\varphi(p^\alpha)$, p : πρώτος.

$\varphi(p^\alpha) = \sum_{d|p^\alpha} \mu(d) \cdot \frac{p^\alpha}{d} = \mu(1) \cdot \frac{p^\alpha}{1} + \mu(p) \cdot \frac{p^\alpha}{p} + \mu(p^2) \cdot \frac{p^\alpha}{p^2} + \dots +$
 $+ \mu(p^\alpha) \cdot \frac{p^\alpha}{p^\alpha} =$

~~$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$~~ $\Rightarrow$

$\Rightarrow \boxed{\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}}$

Άρα: $\varphi(1) = 1$ & αν $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ πρώτ. αριθμοί του $n > 1$
 τότε $\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1-1}) \dots (p_k^{\alpha_k} - p_k^{\alpha_k-1}) =$
 $= p_1^{\alpha_1} \dots p_k^{\alpha_k} (1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_k}) \Rightarrow$

$\Rightarrow \boxed{\varphi(n) = n \cdot (1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_k})}$

Π.χ. $n = 1.000.000 = 2^6 \cdot 5^6$: πρώτοι αριθμοί του
 $\varphi(10^6) = 2^6 \cdot 5^6 \cdot (1 - \frac{1}{2}) (1 - \frac{1}{5}) = 2^5 \cdot 5^5$.

Πρόταση: $\forall n \geq 3: \varphi(n) \equiv \text{άρτιος}$.

Απόδειξη: ①: Έστω ότι $n = 2^k$, $k \geq 2$ (αφού $n \geq 3$)

Τότε: $\varphi(2^k) = 2^k - 2^{k-1} = 2^{k-1}$: άρτιος

② Έστω ότι $n \neq 2^k$. Τότε ο n έχει

πρώτο πρῶτο διαιρέτη. Τότε: $n = p^k \cdot m$, όπου $k \geq 1$ και

$(p^k, m) = 1$. Τότε $\varphi(n) = \varphi(p^k \cdot m) \stackrel{\varphi \in \text{ML}}{=} \varphi(p^k) \cdot \varphi(m) =$

$= (p^k - p^{k-1}) \varphi(m) = p^{k-1} (p-1) \varphi(m) \Rightarrow$

$\Rightarrow (p-1) \mid \varphi(n)$

p : ~~πρῶτος~~ $\Rightarrow p-1$ άρτιος. $\Rightarrow 2 \mid \varphi(n) \Rightarrow \varphi(n)$: άρτιος

Φυλλάδιο #6

Ασκ ①, (i) $\forall n \in \mathbb{N}: \varphi(n) = n \Leftrightarrow n = 1$

(ii) n : άρτιος $\Rightarrow \varphi(n) < n-1$.

(iii) n : πρῶτος $\Rightarrow \varphi(n) = n-1$.

Λύση (i) ($\Leftarrow$) Αν $n = 1 \Rightarrow \varphi(n) = \varphi(1) = 1 = n$

($\Rightarrow$) Αν $\varphi(n) = n$ κ' $n > 1$ τότε $(n, n) = n > 1 \Rightarrow$
 $\Rightarrow \varphi(n) < n$ άτοπο $\Rightarrow \varphi(n) = n$, αν $n = 1$.

(ii) (i): Έστω n : άρτιος $\mu n > 1$. Τότε $n = d \cdot d'$
όπου $1 < d, d' < n$. Τότε $(n, n) = n > 1$ κ' $(d, n) = d > 1$
άρα $\varphi(n) \leq n-2$.

(iii) ($\Rightarrow$) Αν n : πρῶτος τότε $\varphi(n) = n' - n^0 = n-1$

($\Leftarrow$) Έστω ότι $\varphi(n) = n-1$. τότε προφανώς από

(i) $\Rightarrow n > 1$. κ' από (ii) $\Rightarrow n$ δεν είναι άρτιος
κ' άρα n : πρῶτος.

Ασκ. ⑤ ① Αν $n \geq 1$ τότε ποια έχει υπάρχει μεταξύ των
 $\varphi(2n)$ κ' $2\varphi(n)$.

② Αν $n \geq 1$ να υπολογιστεί η τιμή $\varphi(3n)$ συναρτήσει
της $\varphi(n)$.

Λύση: ① Αν $n = 1 \Rightarrow \varphi(2n) = \varphi(2) = 1$

$2\varphi(n) = 2\varphi(1) = 2 \cdot 1 = 2 > \varphi(2n)$ κ' ~~από~~

$2\varphi(n) = 2\varphi(2n)$

$$\text{Έστω ότι } 2 \nmid n \Rightarrow (2, n) = 1 \stackrel{\varphi \in M}{\Rightarrow} \varphi(2n) = \varphi(2) \cdot \varphi(n) = 1 \cdot \varphi(n) = \varphi(n) \Rightarrow \boxed{2\varphi(n) = 2\varphi(2n)}$$

$$\begin{aligned} \text{Έστω ότι } 2 \mid n \Rightarrow n &= 2^k \cdot m, \text{ όπου } (2^k, m) = 1 \\ \text{Τότε } \varphi(2n) &= \varphi(2 \cdot 2^k \cdot m) = \varphi(2^{k+1} \cdot m) \stackrel{\varphi \in M}{=} \varphi(2^{k+1}) \cdot \varphi(m) = \\ &= (2^{k+1} - 2^k) \varphi(m) = 2^k \varphi(m) = 2 \cdot 2^{k-1} \cdot \varphi(m) = \\ &= 2 \cdot \varphi(2^k) \cdot \varphi(m) \stackrel{\varphi \in M}{=} 2 \varphi(2^k \cdot m) = 2 \varphi(n) \Rightarrow \\ &\Rightarrow \boxed{\varphi(2n) = 2 \varphi(n)} \end{aligned}$$

② Έστω ότι $3 \nmid n$, τότε $(3, n) = 1$ και άρα

$$\varphi(3n) \stackrel{\varphi \in M}{=} \varphi(3) \cdot \varphi(n) = 2 \cdot \varphi(n)$$

$$3 \mid n \Rightarrow n = 3^k \cdot m, \text{ κ' } (3^k, m) = 1$$

$$\varphi(3n) = \varphi(3 \cdot 3^k \cdot m) = \varphi(3^{k+1}) \stackrel{\varphi \in M}{\underset{(3^k, m)=1}{=}} \varphi(3^{k+1}) \cdot \varphi(m) =$$

$$= (3^{k+1} - 3^k) \varphi(m) = 2 \varphi(m)$$

$$3\varphi(n) = \varphi(3^k \cdot m) \stackrel{\varphi \in M}{\underset{(3^k, m)=1}{=}} 3 \cdot \varphi(3^k) \cdot \varphi(m) = 3(3^k - 3^{k-1}) \varphi(m) =$$

$$= 3 \cdot 3^{k-1} \cdot 2 \cdot \varphi(m) = 3^k \cdot 2 \cdot \varphi(m)$$

$$\Rightarrow \boxed{\varphi(3n) = 3\varphi(n)}$$

$$\text{Άρα: } \begin{cases} 3 \nmid n \Rightarrow \varphi(3n) = 2\varphi(n) \\ 3 \mid n \Rightarrow \varphi(3n) = 3\varphi(n) \end{cases}$$

Άσκ. ③ n άρτος $\Leftrightarrow \sum_{d \mid n} \mu(d) \cdot \varphi(d) = 0$

$$\begin{aligned} \text{Λύση: } \sum_{n=p_1^{\alpha_1} \dots p_k^{\alpha_k}} \mu(d) \varphi(d) &= (1 - \varphi(p_1)) \dots (1 - \varphi(p_k)) = \\ &= (1 - (p_1 - 1)) \dots (1 - (p_k - 1)) = \\ &= (2 - p_1) \dots (2 - p_k) = 0 \Leftrightarrow \end{aligned}$$

$$\Leftrightarrow \exists i = 1, \dots, k : 2 - p_i = 0 \Leftrightarrow \exists i = 1, \dots, k : p_i = 2 \Leftrightarrow$$

$$\Leftrightarrow n \text{ άρτος}$$

$$f \text{ not 1 k' } \Rightarrow$$

$$\Rightarrow \sum_{d \mid n} \mu(d) f(d) = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{otherwise} \end{cases}$$

Α6κ (14): $\sum_{d|m} \frac{\mu^2(d)}{\varphi(d)} = \frac{n}{\varphi(n)}$, με $\mu^2(n) = [\mu(n)]^2$
 $\mu: \mathbb{N} \rightarrow \mathbb{C}$.

Λύση: Έστω η συνάρτηση $f: \mathbb{N} \rightarrow \mathbb{C}$, $f(n) = \frac{\mu^2(n)}{\varphi(n)}$, $\forall n \in \mathbb{N}$.

Τότε ενόψει μ, φ είναι πολλαπλασιαστικές $\boxed{f \in M}$

Τότε και η $F: \mathbb{N} \rightarrow \mathbb{C}$, $F(n) = \sum_{d|m} f(d) = \sum_{d|m} \frac{\mu^2(d)}{\varphi(d)}$ είναι πολλαπλασιαστική.

• Αν $n=1$. Τότε $\sum_{d|1} \frac{\mu^2(d)}{\varphi(d)} = 1 = \frac{1}{\varphi(1)}$

Άρα το πρόβλημα ισχύει για $n=1$.

Αν $n > 1$ τότε έστω $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ η πρωτεύουσα ανάλυσή.

$F(n) = F(p_1^{\alpha_1}) \dots F(p_k^{\alpha_k})$. Άρα αρκεί να υπολογίσουμε $F(p^\alpha)$ p -πρωτεύουσα, $\alpha \in \mathbb{N}$

Έχουμε: $F(p^\alpha) = \sum_{d|p^\alpha} \frac{\mu^2(d)}{\varphi(d)} = \frac{\mu^2(1)}{\varphi(1)} + \frac{\mu^2(p)}{\varphi(p)} + \dots + \frac{\mu^2(p^\alpha)}{\varphi(p^\alpha)} =$
 $= \frac{1}{1} + \frac{(-1)^2}{p-1} \Rightarrow \boxed{F(p^\alpha) = \frac{p}{p-1}}$

Άρα $F(n) = \frac{p_1}{p_1-1} \cdot \frac{p_2}{p_2-1} \dots \frac{p_k}{p_k-1} = \frac{p_1^{\alpha_1} \dots p_k^{\alpha_k}}{p_1^{\alpha_1-1} \dots p_k^{\alpha_k-1} (p_1-1) \dots (p_k-1)} =$
 $= \frac{n}{\varphi(n)}$

~~✓~~

Α6κ (10): (1) ΝΟ. $\exists n \in \mathbb{N}: \varphi(n) = 2, 4, 6, 8, 10, 12$.
 (2) $\nexists n \in \mathbb{N}: \varphi(n) = 14$.

Λύση (1) $\varphi(3)=2$, $\varphi(5)=4$, $\varphi(7)=6$, $\varphi(11)=10$, $\varphi(13)=12$.
 $\varphi(15) = \varphi(3 \cdot 5) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8$.

(2) Έστω ότι $n \in \mathbb{N}: \varphi(n) = 14$.

Προφανώς $n \geq 2 \Rightarrow$ πρωτεύουσα ανάλυση: $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$

Τότε $\varphi(n) = p_1^{\alpha_1-1} \dots p_k^{\alpha_k-1} (p_1-1) \dots (p_k-1) = 14 = 2 \cdot 7 \Rightarrow$

$$\Rightarrow 7 \mid p_1^{x_1-1} \dots p_k^{x_k-1} (p_1-1) \dots (p_k-1) \Rightarrow \begin{cases} 7 \mid p_i^{x_i-1}, \text{ για } i=1, \dots, k \\ \text{ή} \\ 7 \mid p_i-1 \end{cases} \quad (A) \quad (B)$$

(A) Αν $7 \mid p_i^{x_i-1} \Rightarrow p_i = 7$ (αφού $p_i \neq 7$: πρώτος).

Οπότε $p_i-1 = 6 \mid \varphi(m) = 14$ ΑΤΟΝΟ (δίδει $6 \nmid 14$).

(B) $7 \mid p_i-1 \Rightarrow p_i-1 = 7k \Rightarrow p_i = 7k+1$, για $k \geq 1$.

Για $k=1 \Rightarrow p_i=8$ ΑΤΟΝΟ (δίδει p_i : πρώτος)

$k=2 \Rightarrow p_i=15$ // - //

Άρα $k \geq 3$

Οπότε $p_i = 7k+1 \geq 7 \cdot 3 + 1 = 22 \Rightarrow p_i-1 \geq 21$

όμως $(p_i-1) \mid \varphi(m) = 14$ ΑΤΟΝΟ (δίδει $21 > 14$)

Άρα από (A), (B): $\nexists n \in \mathbb{N} : \varphi(m) = 14$

ΤΕΛΕΙΟΙ ΑΡΙΘΜΟΙ

Ο αριθμός n καλείται τέλειος $\Leftrightarrow 6(n) - n = n \Leftrightarrow 6(n) = 2n$

Παράδειγμα: Οι αριθμοί 6, 28, 496, 8.128 είναι τέλειοι.

(Αρχαίοι Έλληνες). Ο επόμενος τέλειος αριθμός είναι αρκετά μεγάλος (33.550.336)

Είναι γνωστοί μόνο 48 τέλειοι αριθμοί.

Ανοικτά προβλήματα: - Είναι το πλήθος των τέλειων αριθμών άπειρο;

- ~~Εάν υπάρχει~~ Υπάρχει πεπεσμένος τέλειος αριθμός;

Θεώρημα: ① Αν ο αριθμός 2^k-1 είναι πρώτος, $k \geq 2$, τότε ο αριθμός $n = 2^{k-1}(2^k-1)$ είναι τέλειος άρτιος.

② Αν ο αριθμός n είναι τέλειος άρτιος αριθμός τότε $n = 2^{k-1}(2^k-1)$, 2^k-1 : πρώτος, $k \geq 2$.

Ένας αριθμός της μορφής 2^k-1 καλείται πρώτος του Mersenne $\Leftrightarrow 2^k-1$: πρώτος $k' \geq 2$.

Αν $\varphi(2^k-1) = 2^{k-1}$: Η αντεκτίσση: $\left\{ \begin{array}{l} \text{πρώτοι του Mersenne} \\ 2^k-1 \end{array} \right\} \rightarrow \left\{ \begin{array}{l} \text{τέλειοι} \\ \text{αριθμοί} \\ \text{αριθμοί} \end{array} \right\}$

είναι 1-1 k' επί.