

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

ΘΕΩΡΗΜΑ [GAUSS]: $n = \sum_{d|n} \varphi(d)$

Απόδειξη. Θεωρούμε το σύνολο $S = \{1, 2, \dots, n\}$
και για κάθε $d|n$ θεωρούμε το σύνολο $S_d = \{t \in S \mid (t,n)=d\}$

Έχουμε $\tau(d)$ τέτοια υποσύνολα $S_d = S_{d_1}, S_{d_2}, \dots, S_{d_{\tau(d)}}$

ΠΡΟΤΙΜΗ Η συλλογή υποσυνόλων S_d , $d|n$ αποτελεί μια διαμέριση του S , δηλαδή:

① $\forall d|n: S_d \neq \emptyset$, διότι $d \in S_d$

② Αν d_1, d_2 είναι γειτονικά διαιρέτες του n και $d_1 \neq d_2$, τότε $S_{d_1} \cap S_{d_2} = \emptyset$, διότι:
αν $t \in S_{d_1} \cap S_{d_2}$ τότε $(t,n)=d_1$
 $(t,n)=d_2 \Rightarrow d_1 = d_2$ ΑΤΟΝΟ

③ $S = \bigcup_{d|n} S_d$, διότι αν $t \in S = \{1, 2, \dots, n\}$ και
θέσουμε $d = (t,n)$ τότε προφανώς $t \in S_d \Rightarrow t \in \bigcup_{d|n} S_d$

Αρα S_{d_1}, S_{d_2} είναι μερικά τας.

$$\begin{aligned} S &= \bigcup_{i=1}^n S_i \\ &\Downarrow \\ |S| &\neq \sum_{i=1}^n |S_i| \end{aligned}$$

Επειδή τα σύνολα $\{S_d \mid d|n\}$: διαμέριση του S , θα έχουμε

$$|S| = \left| \bigcup_{d|n} S_d \right| = \sum_{d|n} |S_d| \Rightarrow n = \sum_{d|n} |S_d|. \text{ Έστω } t \in S_d \Rightarrow \begin{matrix} 1 \leq t \leq n \\ (t,n)=d \end{matrix} \Rightarrow$$

$$\Rightarrow \left(\frac{t}{d}, \frac{n}{d} \right) = 1 \text{ και } 1 \leq \frac{t}{d} \leq \frac{n}{d} \text{ θεωρούμε το σύνολο } A_d = \left\{ 1 \leq b \leq \frac{n}{d} \mid \left(b, \frac{n}{d} \right) = 1 \right\}$$

$$\text{ή } A_d = \left\{ b \in \mathbb{N} \mid \begin{matrix} 1 \leq b \leq \frac{n}{d} \\ \text{και } \left(b, \frac{n}{d} \right) = 1 \end{matrix} \right\} \text{ (άλλη γραφή)}$$

Τότε $|A_d| = g(\frac{n}{d})$. Ορίσαμε απεικόνιση $f: S_d \rightarrow A_d, f(\tau) = \frac{\tau}{d} \in A_d$.

Η f είναι 1-1, διότι: αν $f(\tau_1) = f(\tau_2) \Rightarrow \frac{\tau_1}{d} = \frac{\tau_2}{d} \Rightarrow \tau_1 = \tau_2$. Η f είναι, διότι
 έστω $b \in A_d$

Τότε $f(bd) = \frac{bd}{d} = b$. Άρα f είναι 1-1 κ' είναι $\Rightarrow |S_d| = |A_d| = g(\frac{n}{d}), \forall d|n$

$$\text{Άρα } n = \sum_{d|n} |S_d| = \sum_{d|n} g(\frac{n}{d}) = \sum_{d|n} g(d) \quad \blacksquare$$

Αν S είναι τότε μια συλλογή υποσυνόλων $S_1, \dots, S_n$ αν S καλείται
 διαμέριση του S (α)

$$(a) \quad (1) \quad \forall i=1, \dots, n : S_i \neq \emptyset$$

$$(2) \quad i \neq j \Rightarrow S_i \cap S_j = \emptyset$$

$$(3) \quad S = \bigcup_{i=1}^n S_i$$

$$|S| = \sum_{i=1}^n |S_i|$$

Θεώρημα Gauss: $\forall n \geq 1 : n = \sum_{d|n} g(d) \quad n = \sum_{d|n} g(d) \nu(\frac{n}{d}) = (g * \nu)(n)$

$$\text{Αν } \tilde{g}: \mathbb{N} \rightarrow \mathbb{C} : \tilde{g}(n) = n \Rightarrow$$

$$\int \Rightarrow \tilde{g}(n) = (g * \nu)(n) \quad \forall n \geq 1 \Rightarrow$$

$$\tilde{g} = g * \nu \xrightarrow[\nu \in \text{muf}]{\text{mof/ke}} \tilde{g} * \nu = (g * \nu) * \nu = g * (\nu * \nu) =$$

$$= g * \varepsilon = g \Rightarrow$$

$$\Rightarrow \boxed{g = i * \nu = \nu * i} \Rightarrow g(n) = \sum_{d|n} i(d) \nu(\frac{n}{d}) = \sum_{d|n} d \cdot 1(\frac{n}{d})$$

$$\text{p (1) } i \neq 0, \text{ διότι } i(1) = 1 \neq 0 \quad i(m \cdot n) = m \cdot n = i(m) i(n) \quad \Rightarrow \sum_{d|n} i(d) \cdot 1(\frac{n}{d}) = \sum_{d|n} i(d) \cdot \frac{n}{d}$$

$$(2) \quad i \in m \text{ Άρα } i \in m \Rightarrow g * i \in m$$

$\varphi(1)=1$, αν $n > 1$, τότε έστω $n = p_1^{a_1} \dots p_k^{a_k}$ η πρωτογενής διάσπαση του $n \Rightarrow$
 $\varphi(n) = \varphi(p_1^{a_1} \dots p_k^{a_k}) = \varphi(p_1^{a_1}) \dots \varphi(p_k^{a_k})$ ΠΡΟΒΛΗΜΑ: $\varphi(p^a) = ?$ αν p πρώτος
 $a \geq 1$

ΛΗΜΜΑ: $\forall p$ πρώτος, $\forall a \geq 1$: $\varphi(p^a) = p^a - p^{a-1}$

Απόδειξη: Έστω $S = \{1, p, p^2, \dots, p^a\}$. Διαίρετες του $p^a = 1, p, p^2, \dots, p^a$
 $\left\{ k \in \mathbb{N} \mid 1 \leq k \leq p^a \atop (k, p^a) = 1 \right\}$ Όμως: p πρώτος $\Rightarrow (k, p^a) = 1 \Leftrightarrow (k, p) = 1$
 Οι αριθμοί $k \in \mathbb{N} : 1 \leq k \leq p^a$ οι οποίοι διαιρούνται
 από τον p είναι $p, 2p, 3p, \dots, p^a = p^{a-1} p$ οι

οποίοι είναι σε πλήθος p^{a-1}
~~Οι υπόλοιποι θα είναι σε πλήθος $p^a - p^{a-1}$ και θα είναι όλοι οι αριθμοί~~
 $k : 1 \leq k \leq p^a$ οι οποίοι είναι πρώτοι προς τον p , και άρα πρώτοι και προς
 τον p^a . Άρα $\left| \left\{ k \in \mathbb{N} \mid 1 \leq k \leq p^a \atop (k, p^a) = 1 \right\} \right| = \varphi(p^a) = p^a - p^{a-1}$

Άρα αν $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ είναι η πρωτογενής διάσπαση του $n > 1$, τότε:

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{a_1}) \varphi(p_2^{a_2}) \dots \varphi(p_k^{a_k}) = (p_1^{a_1} - p_1^{a_1-1}) (p_2^{a_2} - p_2^{a_2-1}) \dots (p_k^{a_k} - p_k^{a_k-1}) = \\ &= p_1^{a_1} \dots p_k^{a_k} \left(\frac{p_1-1}{p_1} \right) \dots \left(\frac{p_k-1}{p_k} \right) = p_1^{a_1} \dots p_k^{a_k} \left(1 - \frac{1}{p_1} \right) \dots \left(1 - \frac{1}{p_k} \right) = n \left(1 - \frac{1}{p_1} \right) \dots \left(1 - \frac{1}{p_k} \right) \end{aligned}$$

Παράδειγμα: $\varphi(2015) = \varphi(5 \cdot 13 \cdot 31) = \varphi(5) \varphi(13) \varphi(31) = (5-1)(13-1)(31-1) =$
 $2015 = 5 \cdot 13 \cdot 31$
 $= 4 \cdot 12 \cdot 30 = 1440$

p πρώτος $\Rightarrow \varphi(p) = p-1$

ΠΡΟΤΑΣΗ: $\varphi(1) = \varphi(2) = 1$ και $\forall n \geq 3$: $\varphi(n)$: άρτιος

Απόδειξη: Έστω $n \geq 3$ (a) Υποθέτουμε ότι: $n = 2^k$, για κάποιο $k \geq 2$

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

(b) Υποθέτουμε ότι: $n = p^k \cdot m$, όπου p : πρώτος, $k \geq 1$ και $(p, m) = 1 = (p^k, m)$

Τότε $\varphi(n) = \varphi(p^k \cdot m) = \varphi(p^k) \varphi(m) = \varphi(p^k) \varphi(m) = (p^k - p^{k-1}) \varphi(m) = p^{k-1}(p-1) \varphi(m)$; άρτιος, διότι $p-1$ άρτιος

ΠΡΟΒΛΗΜΑ:

Αν m : άρτιος, υπάρχει $x \in \mathbb{N}$: $\varphi(x) = m$;
Α Αντίστροφα είναι όχι.

ΑΝΟΙΧΤΟ ΠΡΟΒΛΗΜΑ: $\exists m \in \mathbb{N}$: η εξίσωση $\varphi(x) = m$ έχει ακριβώς μία λύση;

ΠΡΟΒΛΗΜΑ: Γενικά p : πρώτος $\varphi(p) = p-1 \mid p-1$
Υπάρχει συνάρτηση φ τέτοια η: $\varphi(n) \mid n-1$;

Αν υπάρχει τέτοια συνάρτηση φ , τότε $n \leq 10^{2.000.000}$

ΑΣΚΗΣΗ: ① $V * V, f * f, V * i, \varphi * T$

$$(V * V)(n) = \sum_{d|n} V(d) \cdot V\left(\frac{n}{d}\right) = \sum_{d|n} 1 \cdot 1 = \sum_{d|n} 1 = \tau(n), \forall n \geq 1 \Rightarrow \boxed{V * V = T} \Rightarrow$$

$$(V * V) * f = T * f \Rightarrow V * (V * f) = T * f \Rightarrow \boxed{V * f = T * f} \Rightarrow \boxed{V = T * f} \Rightarrow$$

$$V * f = (T * f) * f \Rightarrow \boxed{f * (T * f) = T} \Rightarrow \boxed{T^{-1} = f * f}$$

$$(V * i)(n) = \sum_{d|n} V(d) i\left(\frac{n}{d}\right) = \sum_{d|n} 1 \cdot \frac{n}{d} = \sum_{d|n} \frac{n}{d} = \sum_{d|n} d = \sigma(n), \forall n \geq 1 \Rightarrow$$

$$\Rightarrow V * i = \sigma$$

④ $\Rightarrow f * (V * i) = f * \sigma \Rightarrow (f * V) * i = f * \sigma \Rightarrow \boxed{f * i = f * \sigma} \Rightarrow i = f * \sigma$

$$\textcircled{2} \sum_{d|n} \tau(d) f\left(\frac{n}{d}\right) = \sum_{d|n} \sigma(d) f\left(\frac{n}{d}\right) = (\sigma * f)(n) = i(n) = n$$

a' trópas: $\tau * \tau = V \Rightarrow V(n) = 1 = (\tau * \tau)(n) = \sum_{d|n} \tau(d) f\left(\frac{n}{d}\right) \quad \text{--- ~~scribbled out~~ ---}$

b' trópas: $\sum_{d|n} 1 = \tau(n) \Rightarrow \tau(n) = \sum_{d|n} V(d) \xrightarrow[\text{Möbius}]{\text{αντίστροφο}} V(n) = \sum_{d|n} \tau(d) f\left(\frac{n}{d}\right)$

$\parallel$
 $\downarrow$

Αντίστροφον Ζήβατο 3 ύπερ 12-3.
 Ατγ. 3.