29-11-16

Η συνάρτηση φ του Euler

$\forall n \in \mathbb{N}: \varphi(n) = |\{k \in \mathbb{N} \mid {}^{1 \le k \le n}_{(k,n)=1}\}|$

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

Απόδειξη: Έστω $S = \{1, 2, \ldots, n\}$, για κάθε $d|n$, θεωρούμε το σύνολο $S_d = \{t \in \mathbb{N} \mid (t,n) = d\} \subseteq S$

Η συλλογή υποσυνόλων S_d, $\forall d|n$ είναι μια διαμέριση του S, διότι:

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

↳ Έστω $d_1|n$, $d_2|n$ και $d_1 \neq d_2$. Τότε, αν

$$t \in S_{d_1} \cap S_{d_2} \Rightarrow \begin{cases} (t,n) = d_1 \\ (t,n) = d_2 \end{cases} \longrightarrow d_1 = d_2 = \text{Άτοπο}$$

διότι $d_1 \neq d_2$

Άρα: $S_{d_1} \cap S_{d_2} = \emptyset$

↳ Προφανώς $\bigcup_{d|n} S_d \subseteq S$. Έστω $t \in S$. Αν $(t,n) = d$

τότε ισχύει $t \in S_d$

Επομένως $S \subseteq \bigcup_{d|S} S_d$. Άρα, η συλλογή υποσυνόλων

$\{S_d \mid d|n\}$: διαμέριση του S

Αν $\{S_1, \ldots, S_n\}$: διαμέριση ενός συνόλου S, τότε: $S_1, S_2 \subseteq S$

$S_1 \cup S_2 = S$

→ Θεώρημα Gauss: $\forall n \in \mathbb{N}: n = \sum_{d|n} \varphi(d)$

Απόδειξη: Άρα: $|S| = \sum_{d|n} |S_d| \Rightarrow n = \sum_{d|n} |S_d|$

Θα δείξω ότι: $|S_d| = \varphi\left(\frac{n}{d}\right)$ ⊛

Αν ισχύει η ⊛, τότε θα έχουμε:

$$n = \sum_{d|n} |S_d| = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi(d)$$

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

Θεωρούμε το σύνολο $A_d = \left\{k \in \mathbb{N} \;\middle|\; \begin{matrix} 1 \le k \le \frac{n}{d} \\ (k, \frac{n}{d}) = 1 \end{matrix}\right\}$

Τότε: $|A_d| = \varphi\left(\frac{n}{d}\right)$

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

Θεωρούμε απεικόνιση: $F: S_d \to A_d$, $F(t) = \frac{t}{d}$

Η F: 1-1, διότι αν $F(t_1) = F(t_2) \Rightarrow \frac{t_1}{d} = \frac{t_2}{d} \Rightarrow t_1 = t_2$

Η F: επί διότι $\forall s \in A_d \Rightarrow$

$$\Rightarrow \begin{cases} 1 \le s \le \frac{n}{d} \\ \left(s, \frac{n}{d}\right) = 1 \Rightarrow d\left(s, \frac{n}{d}\right) = d \Rightarrow (ds, n) = d \Rightarrow \\ \Rightarrow ds \in S_d \end{cases}$$

$F(d\cdot s) = \frac{d\cdot s}{d} = s$. Άρα f: 1-1 και επί

$|S_d| = |A_d| = \varphi\left(\frac{n}{d}\right)$

$\forall n \in \mathbb{N}: n = \sum_{d|n} \varphi(d) \Rightarrow i(n) = \sum_{d|n} \varphi(d)\cdot 1 =$

$= \sum_{d|n} \varphi(d)\, v\left(\frac{n}{d}\right) \Rightarrow i(n) = (\varphi * v)(n)$. Άρα: $i = \varphi * v \Rightarrow$

$\Rightarrow i * \mu = (\varphi * v) * \mu \Rightarrow i * \mu = \varphi * (v * \mu) = \varphi * \varepsilon = \varphi \Rightarrow$

$\Rightarrow \boxed{\varphi = i * \mu}$

Επειδή $i, \mu \in M \Rightarrow \varphi = i * \mu \in M$. Άρα: $\varphi \in M$

$\forall n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$: πρωτογενής ανάλυση του $n > 1$

$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k})$ ① $p \nmid k \Rightarrow (p,k) = 1$

Λήμμα: $\forall p$: πρώτο, $\forall \alpha \in \mathbb{N}: \varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$

Απόδειξη: Έστω $k \in \mathbb{N}: 1 \le k \le p^\alpha$ και $(k, p^\alpha) = 1 \Leftrightarrow$

$\Leftrightarrow (k,p) = 1 \Leftrightarrow p \nmid k$. Άρα $\varphi(p^\alpha) = p^\alpha$: πλήθος των k

$k: 1 \le k \le p$, $p \mid k$

Οι αριθμοί $k: 1 \le k \le p^\alpha$ που διαιρούνται απ' το p είναι:
$p, 2p, 3p, \ldots, p^{\alpha-1}\cdot p$, οι οποίοι είναι σε πλήθος $p^{\alpha-1}$.

② Έστω ότι $n \neq 2^k, \forall k \geq 2$. Τότε ο n θα έχει έναν περιττό πρώτο διαιρέτη p και επομένως $n = p^k \cdot m$ όπου $(p, m) = 1 \Rightarrow (p^k, m) = 1$

Τότε: $\varphi(n) = \varphi(p^k \cdot m) = \varphi(p^k)\varphi(m) = (p^k - p^{k-1}) \cdot \varphi(m) =$

$= p^{k-1}(p-1)\varphi(m)$: άρτιος, διότι p: περιττός

$(p^k, m) = 1$. Άρα $\varphi(n)$: άρτιος

1| Αν p: πρώτος $\Rightarrow \varphi(p) = p-1 \mid p-1$

↳ Εικασία του Lehmer: Δεν υπάρχει σύνθετος αριθμός n: $\varphi(n) \mid n-1$

↳ Εικασία του Carmichael: $\exists\, m \in \mathbb{N}$ έτσι ώστε η εξίσωση $\varphi(x) = m$ να έχει ακριβώς μία λύση.

Άσκηση {SOS}: $\forall n \in \mathbb{N}$: n άρτιος $\iff \sum_{d \mid n} \mu(d)\varphi(d) = 0$

$$\left\{ F \in M \Rightarrow \sum_{d \mid n} \mu(d) F(d) = \begin{cases} 1, & n = 1 \\ (1 - F(p_1)) \cdots (1 - F(p_k)), & n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} > 1 \end{cases} \right\}$$

Λύση: $\forall\, n > 1$: $\sum_{d \mid n} \mu(d)\varphi(d) = (1 - \varphi(p_1)) \cdots (1 - \varphi(p_k)) =$

$= (1 - (p_1 - 1)) \cdots (1 - (p_k - 1)) = (2 - p_1) \cdots (2 - p_k)$, $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

Προφανώς $\sum_{d \mid n} \mu(d)\varphi(d) = 0 \iff (2 - p_1) \cdots (2 - p_k) = 0 \iff$

$\iff 2 - p_1 = 0 \iff p_1 = 2 \iff 2 \mid n \iff n$: άρτιος

Άσκηση $\sum_{d|n} \mu(d)\varphi(d) = \begin{cases} 1, & n=1 \\ (2-p_1)\cdots(2-p_k), & n>1 \end{cases}$

↳ Άσκηση: $\sum_{d|n} \frac{\mu^2(d)}{\varphi(d)} = ?$

$$\sum_{d|n} \frac{\mu^2(d)}{\varphi(d)} = \sum_{d|n} \mu(d)\cdot\frac{\mu(d)}{\varphi(d)}$$

Θεωρούμε $F: \mathbb{N} \to \mathbb{C}$, όπου: $F(n) = \frac{\mu(n)}{\varphi(n)}$ $(\varphi(n)\neq 0 \ \forall n\in\mathbb{N})$

$F(1) = \frac{\mu(1)}{\varphi(1)} = \frac{1}{1} = 1$, αν $n,m\in\mathbb{N}: (n,m)=1$ τότε: $\Rightarrow$

$$F(n\cdot m) = \frac{\mu(n\cdot m)}{\varphi(n\cdot m)} = \frac{\mu(n)\cdot\mu(m)}{\varphi(n)\cdot\varphi(m)} = F(n)\cdot F(m)$$

$\Rightarrow F\in M$

$$\sum_{d|n} \frac{\mu^2(d)}{\varphi(d)} = \sum_{d|n} \mu(d)F(d) = \begin{cases} 1, & n=1 \\ (1-f(p_1))\cdots(1-f(p_k)), & n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}>1 \end{cases}$$

Όμως, $\forall p$: πρώτο $F(p) = \frac{\mu(p)}{\varphi(p)} = -\frac{1}{p-1}$ ∴ Άτοπο

$$\sum_{\substack{d|n \\ n>1}} \frac{\mu^2(d)}{\varphi(d)} = \left(1+\frac{1}{p_1-1}\right)\cdot\left(1+\frac{1}{p_k-1}\right)$$

↳ Άσκηση: Για τις συναρτήσεις $\sigma, \tau, 1, \varphi, i, \nu$ ισχύουν τα εξής:

$\tau = \nu * \nu$ $\quad (\nu*\nu)(n) = \sum_{d|n} \nu(d)\,\nu\left(\frac{n}{d}\right) = \sum_{d|n} 1\cdot 1 = \sum_{d|n} 1 =$

$= \tau(n) \Rightarrow \boxed{\tau = \nu*\nu}$

$\sigma = \nu * i$ $\quad (\nu * i)(n) = \sum_{d|n} i(d)\,\nu\left(\frac{n}{d}\right) = \sum_{d|n} d\cdot 1 = \sum_{d|n} d = \sigma(n)$

$\Rightarrow \boxed{\sigma = \nu * i}$

$\varphi * \nu = i$ Θεώρημα Gauss

$\sigma = \varphi * \tau$, $\sigma = \nu * i = \nu * (\varphi * \nu) = \nu * (\nu * \varphi) = (\nu * \nu) * \varphi =$

$= \tau * \varphi \Rightarrow \boxed{\sigma = \tau * \varphi}$