15.11.2018

Θεώρημα Κάθε άρτιος τέλειος είναι της μορφής $2^{k-1}(2^k-1)$, όπου 2^k-1 είναι πρώτος (Euler).

Απόδειξη Έστω n τέλειος άρτιος

$\sigma(n) = 2n$

$n = 2^a \cdot m$

$\mu\kappa\delta(2, m) = 1$

$a = k-1 \Rightarrow k = a+1$ και άρα $n = 2^{k-1} \cdot m$, $k \geq 2$, $2^{k-1} > 1$

$n = 2^{k-1} \cdot m$

$\mu\kappa\delta(\underbrace{2^{2k-1}, m}_{\text{πρώτοι μεταξύ τους}}) = 1$

↳ αριθμητική πολλαπλασιαστική

$\sigma(2^{k-1} \cdot m) = 2 \cdot 2^{k-1} \cdot m \Rightarrow \sigma(2^{k-1})\sigma(m) = 2^k \cdot m \Rightarrow$

$\Rightarrow \frac{(2^k-1)}{2-1} \cdot \sigma(m) = 2^k \cdot m \Rightarrow (2^k-1)\sigma(m) = 2^k \cdot m \Rightarrow$

$\Rightarrow \sigma(m) = \frac{2^k \cdot m}{2^k-1} = \frac{2^k \cdot m - m + m}{2^k-1} \Rightarrow \sigma(m) = \frac{(2^k-1)m}{2^k-1} + \frac{m}{2^k-1} \Rightarrow$

$\sigma(m) = m + \underbrace{\frac{m}{2^k-1}}_{\delta}$ → αθροίσμα όλων των γνήσιων διαιρετών του m

$\Rightarrow \sigma(m) = m + \frac{m}{2^k-1} \Rightarrow \sigma(m) = m+\delta$ → το άθροισμα μόνο όλων διαφορετικών διαιρετών του m

Άρα το m έχει ακριβώς δύο διαιρέτες, τον m και τον δ. Άρα ο m είναι πρώτος, και οι διαιρέτες του είναι ο m και ο 1. Άρα $\delta = 1 \Rightarrow \frac{m}{2^k-1} = 1 \Rightarrow$

$\delta = \sigma(m) - n > 0$, δ γνήσιος διαιρέτης

$\delta = \frac{m}{2^k-1} \Rightarrow m = \delta(2^k-1)$, $\delta \mid m$

$1 \le \delta < m$

$\Rightarrow m = 2^k - 1$. Άρα $n = 2^{k-1}(2^k-1)$ όπου 2^k-1 είναι πρώτος αριθμός

Αριθμητικές Πολλαπλασιαστικές Συναρτήσεις

$F: \mathbb{N} \to \mathbb{C}$

i) $F(1) = 1$

ii) Αν $(m,n) = 1 \Rightarrow F(mn) = F(m)F(n)$

Πολλαπλασιαστικές: $I, \nu(n) = 1$, $\varepsilon(n) = \begin{cases} 1, & n = 1 \\ 0, & n > 1 \end{cases}$, τ, σ

Ενελικτικό Γινόμενο

$$f \cdot g(n) = \sum_{d \mid n} F(d) \cdot g\left(\frac{n}{d}\right)$$

$\varepsilon \cdot f = f = f \circ \varepsilon$

→ Φ συνάρτηση του Euler

$\varphi(n)$ μετράει το πλήθος των θετικών αριθμών μεταξύ του 1 και του n που είναι πρώτοι με το n

Η φ είναι αριθμητική πολλαπλασιαστική συνάρτηση.

Παραδείγματα

$\varphi(1)=1$

$\varphi(7)=6$ ① ② ③ ④ ⑤ ⑥ 7

$\varphi(5)=4$ ① ② ③ ④ 5

$\varphi(p)=p-1$, όπου p: πρώτος

$\varphi(6)=2$ ① 2 3 4 ⑤ 6

$\varphi(8)=4$ ① 2 ③ 4 ⑤ 6 ⑦ 8

$\varphi(10)=4$ ① 2 ③ 4 5 6 ⑦ 8 ⑨ 10

Αν $n>1 \Rightarrow n=p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$, τότε:

$$\varphi(n)=\varphi(p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s})=p_1^{a_1-1}(p_1-1)p_2^{a_2-1}(p_2-1)\cdots p_s^{a_s-1}(p_s-1)$$

Παράδειγμα Πόσοι αριθμοί μεταξύ του 1 και του 1000 είναι πρώτοι με το 1000?

$$\varphi(1000)=\varphi(2^3\cdot 5^3)=2^{3-1}(2-1)5^{3-1}(5-1)=4\cdot 1\cdot 5^2\cdot 4=$$
$$=16\cdot 25=400$$

Ισοτιμίες modulo n

Ορισμός Έστω n φυσικός αριθμός. Δύο ακέραιοι ονομάζονται ισότιμοι modulo n (με μέτρο το n) και γράφουμε

$a\equiv b \bmod n$ αν και μόνο αν $n \mid a-b$

$a\equiv b \bmod n \overset{ορ}{\Leftrightarrow} n \mid a-b$

a άρτιος $\Leftrightarrow a\equiv 0 \bmod 2 \Rightarrow 2 \mid a-0$

a περιττός $\Leftrightarrow a\equiv 1 \bmod 2 \Rightarrow 2 \mid a-1$

$a\equiv b \bmod n$
- → a ισότιμο b modulo n
- → a ισότιμο b modulo n
- → a ισότιμο b ως προς μέτρο το n

$a\not\equiv b \bmod n \Leftrightarrow n \nmid a-b$: a ανισότιμο b modulo n.

Θεώρημα Δύο ακέραιοι a, β είναι ισοϋπολοι modulo n αν και μόνο αν διαιρούμενοι με το n αφήνουν το ίδιο υπόλοιπο.

Απόδειξη ($\Leftarrow$) a, β αφήνουν το ίδιο υπόλοιπο αν διαιρεθούν με το n

$a = qn + r \quad , 0 \le r < n$

$\beta = \lambda n + r \quad , 0 \le r < n$

$a - \beta = qn + r - (\lambda n + r) = qn + r - \lambda n - r = (q - \lambda)n \Rightarrow$

$\Rightarrow n \mid a - \beta \Rightarrow a \equiv \beta \bmod n$

($\Rightarrow$) $a \equiv \beta \bmod n$

$a = qn + r_1 \quad , 0 \le r_1 < n$

$\beta = \lambda n + r_2 \quad , 0 \le r_2 < n$

Χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $r_1 \ge r_2$

$a - \beta = qn + r_1 - \lambda n - r_2$

$a \equiv \beta \bmod n \Rightarrow n \mid a - \beta \Rightarrow a - \beta = \gamma n$

$\gamma n = qn - \lambda n + (r_1 - r_2)$ → θέλω να το βγάλω 0

$0 \le r_1 - r_2 \le r_1 < n \Rightarrow 0 \le r_1 - r_2 < n$

$\gamma n = qn - \lambda n + r_1 - r_2 \Rightarrow r_1 - r_2 = (\gamma - q + \lambda)n = kn$

$r_1 - r_2 = kn$

$0 \le r_1 - r_2 < n \Rightarrow 0 \le kn < n \Rightarrow 0 \le k < 1 \Rightarrow k = 0$

Δηλαδή $r_1 - r_2 = 0 \Rightarrow r_1 = r_2$

Θεώρημα Η σχέση ισοτιμίας είναι σχέση ισοδυναμίας

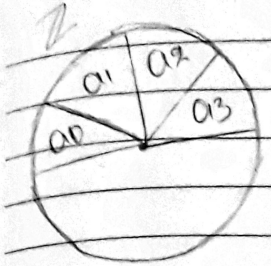
Απόδειξη (i) Έστω $a \in \mathbb{Z} : n \mid 0 \Rightarrow n \mid a - a \Rightarrow a \equiv a \bmod n$ (ανακλαστική)

(ii) Έστω $a \equiv \beta \bmod n \Rightarrow n \mid a - \beta \Rightarrow n \mid \beta - a \Rightarrow \beta \equiv a \bmod n$ (συμμετρική)

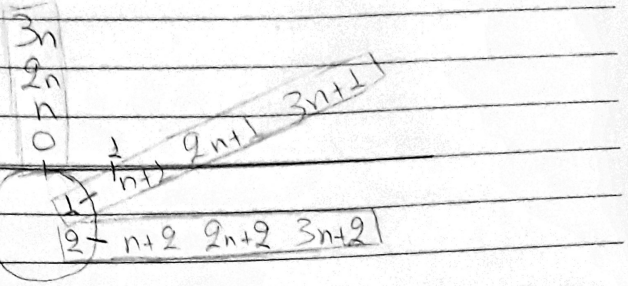
(iii) $\left.\begin{array}{l} a \equiv \beta \bmod n \Rightarrow n \mid a - \beta \\ \beta \equiv \gamma \bmod n \Rightarrow n \mid \beta - \gamma \end{array}\right\} \Rightarrow n \mid (a - \beta) + (\beta - \gamma) = a - \gamma$

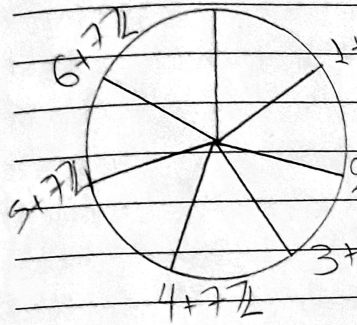
$\Rightarrow n \mid a - \gamma \Rightarrow a \equiv \gamma \bmod n$ (μεταβατική).

ℤ



κλάση του a: $[a]_n = \{\beta \in \mathbb{Z} / \beta \equiv a \bmod n\}$





$0+7\mathbb{Z} = \{7k+0 / k \in \mathbb{Z}\} = [0]_7 = [14]_7 = [777]_7$

$1+7\mathbb{Z} = \{7k+1 / k \in \mathbb{Z}\} = [1]_7 = [8]_7 = [71]_7$

(η διαφορά τους είναι πολλαπλάσιο του 7)

$[a]_n [\beta]_n = [a\beta]_n$

$[a]_n + [\beta n] = [a+\beta]_n$

Θεώρημα Έστω n φυσικός αριθμός και $\alpha, \beta, \gamma, \delta$ ακέραιοι.
Αν $\alpha \equiv \beta \bmod n$ και $\gamma \equiv \delta \bmod n$, τότε
$\alpha+\gamma = (\beta+\delta) \bmod n$ και $\alpha\gamma = \beta\delta \bmod n$

Απόδειξη $\left.\begin{array}{l} \alpha \equiv \beta \bmod n \Rightarrow n \mid \alpha-\beta \\ \gamma \equiv \delta \bmod n \Rightarrow n \mid \gamma-\delta \end{array}\right\} \Rightarrow n \mid (\alpha-\beta)+(\gamma-\delta)$

$\Rightarrow n \mid \alpha+\beta-\gamma-\delta \Rightarrow$

$\Rightarrow \alpha+\gamma = \beta+\delta \bmod n$

$\alpha \equiv \beta \bmod n \Rightarrow n \mid \alpha-\beta \Rightarrow \alpha-\beta = kn$

$\gamma \equiv \delta \bmod n \Rightarrow n \mid \gamma-\delta \Rightarrow \gamma-\delta = \lambda n$

$\alpha = \beta+kn$, $\gamma = \delta+\lambda n$

$\alpha\gamma = (\beta+kn)(\delta+\lambda n) = \beta\delta + \beta\lambda n + k\delta n + k\lambda n^2$

$\alpha\gamma - \beta\delta = \beta\lambda n + k\delta n + k\lambda n^2 = n(\beta\lambda + k\delta + k\lambda n) \Rightarrow$

$\Rightarrow n \mid \alpha\gamma - \beta\delta$