Εφαρμογές του Θεωρήματος Lagrange στη Θεωρία Αριθμών

Ⓐ **Θεώρημα Euler**: Έστω $n \in \mathbb{N}$ και $\alpha \in \mathbb{Z}$ με $(\alpha, n) = 1$. Τότε $\alpha^{\varphi(n)} \equiv 1 \pmod{n}$.

Απόδειξη: Επειδή $(\alpha, n) = 1$ έπεται ότι $[\alpha]_n \in U(\mathbb{Z}_n)$. Εφ' όσον, $|U(\mathbb{Z}_n)| = \varphi(n)$, έχουμε: $([\alpha]_n)^{\varphi(n)} = [1]_n \Rightarrow \underbrace{[\alpha]_n \cdots [\alpha]_n}_{\varphi(n)\text{-φορές}} = [1]_n$

$$\Rightarrow [\underbrace{\alpha \cdots \alpha}_{\varphi(n)\text{-φορές}}]_n = [1]_n \Rightarrow [\alpha^{\varphi(n)}]_n = [1]_n$$

$$\Rightarrow \alpha^{\varphi(n)} \equiv 1 \pmod{n}$$

∎

Ⓑ **Μικρό Θεώρημα Fermat**: Έστω p ένας πρώτος αριθμός και έστω $\alpha \in \mathbb{Z}$ με $p \nmid \alpha$.

Τότε $\alpha^{p-1} \equiv 1 \pmod{p}$

<u>Απόδειξη</u>: Επειδή p: πρώτος και $p \nmid a$, ισχύει $(a,p)=1$. Επιπλέον, $\varphi(p)=p-1$ και από το Θεώρημα Euler, $a^{\varphi(p)} \equiv 1 \pmod{p} \Rightarrow$

$$\Rightarrow a^{p-1} \equiv 1 \pmod{p}.$$

∎

(Γ) <u>Θεώρημα Wilson</u>: Για ένα θετικό ακέραιο $p \geq 2$, τα ακόλουθα είναι ισοδύναμα:

(i) ο p είναι πρώτος αριθμός

(ii) $(p-1)! \equiv -1 \pmod{p}$

<u>Απόδειξη</u>: Αν $p=2$ τότε p: πρώτος και ισχύει: $(2-1)! = 1! = 1 \equiv -1 \pmod{2}$

. Υποθέτουμε λοιπόν ότι $p \geq 3$.

(i) $\Rightarrow$ (ii) Έστω p: πρώτος. Αφού $p \geq 3$, ο p θα είναι περιττός. Στην ομάδα $(U(\mathbb{Z}_p), \cdot)$ έχουμε $[1]_p \neq [-1]_p$ και

$U(\mathbb{Z}_p) = \{[1]_p, [2]_p, \ldots, [p-1]_p\}$ με

$|U(\mathbb{Z}_p)| = \varphi(p) = p-1$. Έστω $[x]_p \in U(\mathbb{Z}_p)$ με $[x]_p = [x]_p^{-1}$. Τότε $[x]_p [x]_p = [x]_p^{-1} [x]_p$

$\Rightarrow [x^2]_p = [1]_p \Rightarrow p \mid x^2 - 1 = (x-1)(x+1)$

$\xrightarrow[\text{πρώτος}]{p:} p \mid x-1$ ή $p \mid x+1$

$\Rightarrow [x]_p = [1]_p$ ή $[x]_p = [-1]_p = [p-1]_p$

Άρα, το μόνο στοιχείο της $U(\mathbb{Z}_p)$ το οποίο συμπίπτει με τον αντίστροφο του, εκτός του $[1]_p$, είναι το $[p-1]_p$, δηλαδή στο γινόμενο όλων των στοιχείων της ομάδας $U(\mathbb{Z}_p)$, $[1]_p \cdot [2]_p \cdots [p-1]_p = [1 \cdot 2 \cdots (p-1)]_p = [(p-1)!]_p$, τα στοιχεία $[2]_p, \ldots, [p-2]_p$ εμφανίζονται ως ζεύγη $\{[x]_p, [x]_p^{-1}\}$ με $[x]_p \neq [x]_p^{-1}$ και άρα δεν συνεισφέρουν στο παραπάνω γινόμενο παρά μόνο το ουδέτερο στοιχείο. Επομένως,

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

$$\Rightarrow (p-1)! \equiv -1 \pmod{p}.$$

(ii) $\Rightarrow$ (i) Υποθέτουμε $(p-1)! \equiv -1 \pmod{p}$, δηλαδή $p \mid (p-1)!+1$. Έστω, προς άτοπο, p: όχι πρώτος. Τότε $p = ab$ όπου $1 < a, b < p$.

Αφού $a \leq p-1$ θα έχουμε $a \mid (p-1)!$ (1)

Επιπλέον, $\left.\begin{matrix} a \mid p \\ p \mid (p-1)!+1 \end{matrix}\right\} \Rightarrow a \mid (p-1)!+1$ (2)

Από (1), (2): $a \mid (p-1)!+1-(p-1)! \Rightarrow a \mid 1$

$\Rightarrow a = 1$, άτοπο. Ώστε, p πρώτος.

Ισχύει το αντίστροφο του θεωρήματος Lagrange;; Δηλαδή, αν d είναι ένας θετικός διαιρέτης της τάξης μιας πεπερασμένης ομάδας G, υπάρχει $H \leq G$ ώστε $|H| = d$;

! Αποδεικνύεται ότι η εναλλάσσουσα υποομάδα $(A_4, \circ)$ τάξης $|A_4| = 12$ δεν έχει υποομάδα τάξης $6 | 12$.