Το Κινέζικο Θεώρημα

Π. Καραζέρης

27 Απριλίου 2016

Αποδεικνύουμε εδώ το λεγόμενο Κινέζικο Θεώρημα (περί Υπολοίπων), στην εντελώς γενική εκδοχή του ως αποτέλεσμα της Θεωρίας Δακτυλίων. Εν συνεχεία εξηγούμε πώς εξειδικεύεται στο κλασικώτερο αριθμοθεωρητικό αποτέλεσμα περί ύπαρξης ταυτόχρονης λύσης για ένα σύστημα ισοτιμιών, δηλαδή της εύρεσης ενός αριθμού που να αφήνει δεδομένα υπόλοιπα όταν διαιρεθεί με δεδομένους φυσικούς αριθμούς $n_1, \ldots n_k$, οι οποίοι είναι ανά δύο σχετικώς πρώτοι μεταξύ τους. Σε αυτήν τη μορφή το αποτέλεσμα ήταν γνωστό στον Κινέζο μαθηματικό Sun Tzu κατά τον 3^o με 5^o αιώνα μ.Χ και εξ αιτίας αυτού παίρνει το ιδιαίτερο όνομά του.

1 Θεώρημα. *Δίνονται ομομορφισμοί αντιμεταθετικών δακτυλίων $f_i \colon A \to B_i$, $i = 1, ..., n$, οι οποίοι είναι όλοι τους επί ως συναρτήσεις και για τους πυρήνες των οποίων ισχύει ότι $\mathrm{Ker} f_i + \mathrm{Ker} f_j = A$, όταν $i \neq j$. Τότε ο επαγόμενος ομομορφισμός προς το γινόμενο των B_i, $f \colon A \to \prod_{i=1}^{n} B_i$, με $f(a) = (f_1(a), ..., f_n(a))$, είναι επί.*

Απόδειξη: Θέλουμε, για ένα δεδομένο στοιχείο $(b_1, ..., b_n) \in \prod_{i=1}^{n} B_i$, να βρούμε ένα $a \in A$, τέτοιο ώστε

$$f(a) = (f_1(a), ..., f_n(a)) = (b_1, ..., b_n),$$

δηλαδή τέτοιο ώστε, για κάθε $i = 1, ..., n$, να είναι $f_i(a) = b_i$.

Θεωρούμε ένα δεδομένο i_0. Τότε για κάθε $j \neq i_0$, επειδή είναι $\mathrm{Ker} f_{i_0} + \mathrm{Ker} f_j = A$, θα υπάρχουν $a_{i_0} \in \mathrm{Ker} f_{i_0}$ και $a_j \in \mathrm{Ker} f_j$ τέτοια ώστε $a_{i_0} + a_j = 1$. Ετσι λοιπόν, για κάθε τέτοιο a_j έχουμε ότι

$$f_{i_0}(a_j) = 0 + f_{i_0}(a_j) = f_{i_0}(a_{i_0}) + f_{i_0}(a_j) = f_{i_0}(a_{i_0} + a_j) = f_{i_0}(1) = 1$$

Σχηματίζουμε τώρα το γινόμενο

$$u_{i_0} = \prod_{j \neq i_0} a_j = a_1 \cdot \ldots \cdot a_{i_0 - 1} \cdot a_{i_0 + 1} \cdot \ldots \cdot a_n$$

Από το επιχείρημα που δώσαμε αμέσως παραπάνω προκύπτει ότι

$$f_{i_0}(u_{i_0}) = f_{i_0}(\prod_{j \neq i_0} a_j) = f_{i_0}(a_1) \cdot \ldots \cdot f_{i_0}(a_{i_0 - 1}) \cdot f_{i_0}(a_{i_0 + 1}) \cdot \ldots \cdot f_{i_0}(a_n) = 1$$

Επίσης για οποιοδήποτε $j \neq i_0$ έχουμε $f_j(u_{i_0}) = 0$, δεδομένου ότι ο παράγοντας a_j του γινομένου που ορίζει το u_{i_0} ανήκει στον πυρήνα του f_j επομένως το γινόμενο των εικόνων του f_j μηδενίζεται.

Επιπλέον, από το γεγονός ότι ο κάθε f_i είναι επί, υπάρχει $\alpha_i \in A$, τέτοιο ώστε $f_i(\alpha_i) = b_i$. Ισχυριζόμαστε ότι το ζητούμενο $a \in A$ είναι το άθροισμα

$$a = \sum_{j=1}^{n} u_j \alpha_j,$$

όπου τα u_j ορίστηκαν παραπάνω. Πράγματι λοιπόν, για κάθε $i = 1, ..., n$ έχουμε

$$\begin{aligned} f_i(a) &= f_i(\sum_{j=1}^{n} u_j \alpha_j) \\ &= f_i(u_i \alpha_i) + f_i(\sum_{j \neq i} u_j \alpha_j) \\ &= f_i(u_i \alpha_i) + \sum_{j \neq i} f_i(u_j \alpha_j) \\ &= f_i(u_i) f_i(\alpha_i) + \sum_{j \neq i} f_i(u_j) f_i(\alpha_j) \\ &= 1 \cdot b_i + 0 \\ &= b_i, \end{aligned}$$

όπως επιθυμούσαμε να δείξουμε. ∎

2 Πόρισμα. *Αν A είναι ένας αντιμεταθετικός δακτύλιος και $\{I_i \mid i = 1, ..., n\}$ είναι ένα πεπερασμένο σύνολο ιδεωδών του, τα οποία είναι τέτοια ώστε για $i \neq j$ να ισχύει ότι $I_i + I_j = A$, τότε ο ομομορφισμός*

$$\varepsilon \colon A \to \frac{A}{I_1} \times ... \times \frac{A}{I_n}$$

με

$$\varepsilon(a) = ([a]_{I_1}, ..., [a]_{I_n})$$

είναι επί.

Απόδειξη Ο ε επάγεται όπως στο παραπάνω Θεώρημα από τους κανονικούς ομομορφισμούς $\varepsilon_i \colon A \to A/I_i$, οι οποίοι είναι προφανώς επί και έχουν ως πυρήνες τα ιδεώδη I_i. ∎

3 Πόρισμα. *Αν* $n_1, \ ..., \ n_k$ *είναι φυσικοί αριθμοί για τους οποίους ισχύει ότι μκδ*$(n_i, n_j) = 1$, *όταν* $i \neq j$ *και* $a_1, \ ..., \ a_k$ *είναι φυσικοί αριθμοί τέτοιοι ώστε* $0 \leq a_i < n_i$, *τότε υπάρχει φυσικός αριθμός* x *ώστε να αληθεύουν ταυτόχρονα οι σχέσεις*

$$x \equiv a_1 \mathrm{mod} n_1$$

$$...$$

$$x \equiv a_k \mathrm{mod} n_k$$

Απόδειξη Θεωρούμε τους κανονικούς ομομορφισμούς $\varepsilon_k \colon \mathbb{Z} \to \mathbb{Z}_{n_k}$ οι οποίοι είναι επί και έχουν ως πυρήνες τα ιδεώδη $n_k\mathbb{Z}$ (τα σύνολα των ακέραιων πολλαπλασίων των n_k). Αφού μκδ$(n_i, n_j) = 1$, όταν $i \neq j$, έχουμε πως το $1 \in \mathbb{Z}$ γράφεται ως $1 = n_i d_i + n_j d_j$, για κάποιους ακεραίους d_i, d_j, δηλαδή ότι $\mathbb{Z} = n_i\mathbb{Z} + n_j\mathbb{Z}$. Επομένως εφαρμόζεται το Θεώρημα, το οποίο μας δίνει πως υπάρχει κάποιο $x \in \mathbb{Z}$ έτσι ώστε το

$$\varepsilon(x) = (\varepsilon_1(x), ..., \varepsilon_k(x) = ([x]_{n_1}, ..., [x]_{n_k})$$

να ισούται με το δοσμένο $([a_1]_{n_1}, ..., [a_k]_{n_k}) \in \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k}$, με άλλα λόγια τέτοιο ώστε να συναληθεύουν οι δοσμένες ισοτιμίες. ∎