Author: Κ.Θ. Αναγνώστου

Title: Σχέση Ισοτιμίας Μόντουλο f στο C(x).

Abstract: Για την αντιμετώπιση προβλημάτων διαιρετότητας στο C(x), ορίζουμε κατά ανάλογο τρόπο όπως στο Z, την σχέση ισοτιμίας μόντουλο f, όπου f μη μηδενικό πολυώνυμο του C(x).

Creator: HDML

ΣΧΕΣΗ ΙΣΟΤΙΜΙΑΣ ΜΟΝΤΟΥΛΟ f ΣΤΟ C(x)

Κ.Θ. Αναγνώστου

Για την πιο εύκολη αντιμετώπιση προβλημάτων διαιρετότητας στο C(x) μπορούμε να ορίσουμε κατά ανάλογο τρόπο, όπως στο Z, την σχέση ισοτιμίας μόντουλο f, όπου f μη μηδενικό πολυώνυμο του C(x).

Θεωρώ το μη μηδενικό πολυώνυμο $f \in C(x)$, και τα $f_1, f_2 \in C(x)$.

ΟΡΙΣΜΟΣ

f_1 ισότιμο f_2 μόντουλο f ή $f_1 \equiv f_2$ (Modf) εάν $f/f_1 - f_2$

Η σχέση ισοτιμίας μόντουλο f έχει τις ακόλουθες ιδιότητες:

i) $f_1 \equiv f_1$ (Modf)
ii) $f_1 \equiv f_2$ (Modf) $\Rightarrow f_2 \equiv f_1$ (Modf)
iii) $f_1 \equiv f_2$ (Modf) και $f_2 \equiv f_3$ (Modf) $\Rightarrow f_1 \equiv f_3$ (Modf)

όπου f_1, f_2, f_3 οποιαδήποτε πολυώνυμα του C(x) και f μη μηδενικό πολυώνυμο του C(x).

ΑΠΟΔΕΙΞΗ

i) $f/f_1 - f_1 \Rightarrow f_1 \equiv f_1$ (Modf)
ii) $f/f_1 - f_2 \Rightarrow f/-(f_1 - f_2) \Rightarrow f/f_2 - f_1 \Rightarrow f_1 \equiv f_1$ (Modf)
iii) $f/f_1 - f_2 \Rightarrow f/f_1 - f_2 + f_2 - f_3 \Rightarrow f/f_1 - f_3 \Rightarrow f_1 \equiv f_3$ (Modf)
$f/\hat{} f_2 - f_3$

Οι ιδιότητες i), ii), iii) δείχνουν πώς η ισοτιμία μόντουλο f είναι μια σχέση ισοδυναμίας στο σύνολο C(x).

ΘΕΩΡΗΜΑ: Εάν $f_1, f_2, f_3, f_4 \in C(x)$, f μη μηδενικό πολυώνυμο του C(x) και $f_1 \equiv f_2$ (Modf), $f_3 \equiv f_4$ (Modf)
τότε: α) $f_1 + f_3 \equiv f_2 + f_4$ (Modf) β) $f_1 \cdot f_3 \equiv f_2 \cdot f_4$ (Modf)

ΑΠΟΔΕΙΞΗ

α) $f/f_1 - f_2$
και $\Rightarrow f/f_1 - f_2 + f_3 - f_4 \Rightarrow f/f_1 + f_3 - (f_2 + f_4)$
$f/f_3 - f_4$

άρα $f_1 + f_3 \equiv f_2 + f_4$ (Modf)

β) $f_1f_3 - f_2f_4 = f_1f_3 - f_2f_3 + f_2f_3 - f_2f_4 = f_3(f_1 - f_2) + f_2(f_3 - f_4)$ (1)

αλλά $\left.\begin{array}{l} f/f_1 - f_2 \Rightarrow f/f_3(f_1 - f_2) \\ f/f_3 - f_4 \Rightarrow f/f_2(f_3 - f_4) \end{array}\right\} \Rightarrow f/f_3(f_1 - f_2) + f_2(f_3 - f_4)$ (2)

(1), (2) $\Rightarrow f/f_1 \cdot f_3 - f_2f_4$ άρα $f_1f_3 \equiv f_2f_4$ (Modf)

ΠΟΡΙΣΜΑ 1ο Εάν $f_1 \equiv f_2$ (Modf) τότε $\alpha f_1 \equiv \alpha f_2$(Modf)

ΠΟΡΙΣΜΑ 2ο Εάν $f_1 \equiv f_2$ (Modf) τότε $f_1^{\nu} \equiv f_2^{\nu}$ (Modf), $\nu \in \mathbb{N}$

ΕΦΑΡΜΟΓΕΣ

1. Να δειχθεί ότι το πολυώνυμο $f(x) = x^{4\alpha} + x^{4\beta+1} + x^{4\gamma+2} + x^{4\delta+3}$ διαιρείται με το πολυώνυμο $g(x) = x^3 + x^2 + x + 1$ με $\alpha, \beta, \gamma, \delta \in \mathbb{N}$.

ΛΥΣΗ

$$x^4 \equiv 1(\text{Modg}) \Rightarrow \left\{\begin{array}{l} x^{4\alpha} \equiv 1(\text{Modg}) \\ x^{4b} \equiv 1(\text{Modg}) \\ x^{4\gamma} \equiv 1(\text{Modg}) \Rightarrow \\ x^{4\delta} \equiv 1(\text{Modg}) \end{array}\right. \left\{\begin{array}{l} x^{4\alpha} \equiv 1(\text{Modg}) \\ x^{4\beta+1} \equiv x(\text{Modg}) \\ x^{4\gamma+2} \equiv x^2(\text{Modg}) \Rightarrow \\ x^{4\delta+3} \equiv x^3(\text{Modg}) \end{array}\right.$$

$$\Rightarrow x^{4\alpha} + x^{4\beta+1} + x^{4\gamma+2} + x^{4\delta+3} \equiv 1 + x + x^2 + x^3 \text{ (Modg)} \Rightarrow$$

$$\left.\begin{array}{l} \Rightarrow f(x) \equiv g(x) \text{ (Mod)} \\ g(x) \equiv 0 \text{ (Modg)} \end{array}\right\} \Rightarrow f(x) \equiv 0 \text{ (Modg)} \quad \text{άρα} \quad g(x)/f(x)$$

2. Να δείξετε ότι το πολυώνυμο $f(x) = (x + 1)^{6\nu+1} + x^{6\nu+2}$ διαιρείται με το πολυώνυμο $g(x) = x^2 + x + 1$

ΛΥΣΗ

Ισχύει $$(x+1)^3 \equiv -1(\text{Modg}) \Rightarrow$$

$$\Rightarrow (x + 1)^{6\nu} \equiv 1(\text{Modg}) \Rightarrow (x + 1)^{6\nu+1} \equiv x + 1 \text{ (Modg)} \quad (1)$$

Επίσης $$x^3 \equiv 1(\text{Modg}) \Rightarrow x^{6\nu} \equiv 1(\text{Modg}) \Rightarrow x^{6\nu+2} \equiv x^2 \text{ (Modg)} \quad (2)$$

$$(1), (2) \Rightarrow (x + 1)^{6\nu+1} + x^{6\nu+2} \equiv x^2 + x + 1 \Rightarrow$$

$$\left.\begin{array}{l} f(x) \equiv g(x) \text{ (Mod)} \\ g(x) \equiv 0 \text{ (Modg)} \end{array}\right\} \Rightarrow f(x) \equiv 0 \text{ (Modg)} \quad \text{άρα} \quad g(x)/f(x)$$

3. Να δείξετε ότι το πολυώνυμο $g(x) = x^2 + x + 1$ διαιρεί το πολυώνυμο $f(x) = x^{6\nu-1} + x + 1$.

ΛΥΣΗ

Ισχύει $x^3 \equiv 1 \ (\text{Modg}) \Rightarrow x^{6v} \equiv 1 \ (\text{Modg})$ (1)

$x^2 + x \equiv x^2 + x \ (\text{Modg})$ (2)

(1), (2) $\Rightarrow x^{6v} + x^2 + x \equiv x^2 + x + 1 (\text{Modg}) \Rightarrow x \cdot (x^{6v-1} + x + 1) \equiv x^2 + x + 1 (\text{Modg})$

$$\left.\begin{array}{l} \Rightarrow x \cdot f(x) \equiv g(x) \ (\text{Modg}) \\ g(x) \equiv 0 \ (\text{Modg}) \end{array}\right\} \Rightarrow x \cdot f(x) \equiv 0 \ (\text{Modg}) \quad \text{άρα} \quad g(x)/x \cdot f(x) \tag{3}$$

όμως $(x, g(x)) = 1$ (4)

(3), (4) $\Rightarrow g(x)/f(x)$

4. Να δειχθεί ότι $x^v \equiv vx - (v - 1) \ (\text{Modg})$ όπου $g(x) = (x - 1)^2$

ΑΠΟΔΕΙΞΗ

Για $v = 1$ $x \equiv x (\text{Modg})$ ισχύει

έστω ότι ισχύει η πρόταση για $v = \kappa \geqslant 2 : x^\kappa \equiv \kappa x - (\kappa - 1) \ (\text{Modg})$ (1)

θα δείξω ότι για $v = \kappa + 1$ ισχύει η πρόταση:

$$x^{\kappa+1} \equiv (\kappa + 1)x - \kappa (\text{Modg})$$

έχω $x^\kappa \equiv \kappa x - (\kappa - 1) \ (\text{Mo} \ ) \Rightarrow x^{\kappa+1} \equiv \kappa x^2 - (\kappa - 1)x \ (\text{Modg})$ (2)

$$\kappa x^2 - (\kappa - 1)x \equiv (\kappa + 1)x - \kappa \ (\text{Modg}) \tag{3}$$

γιατί $\kappa x^2 - (\kappa - 1)x - (\kappa + 1)x + \kappa = \kappa(x^2 - 2x + 1) = \kappa(x - 1)^2 = k \cdot g(x)$

(2), (3) $\Rightarrow x^{\kappa+1} \equiv (\kappa + 1)x - \kappa (\text{Modg})$

άρα $\forall v \in \mathbb{N}^*$ ισχύει $x^v \equiv vx - (v - 1) \ (\text{Modg})$

5. Να υπολογισθούν τα κ, λ έτσι ώστε το πολυώνυμο $f(x) = \kappa x^4 + \lambda x^3 - 3$ να διαιρείται με το $g(x) = (x - 1)^2$.

ΛΥΣΗ

Από την εφαρμογή 4 έχω

$$x^4 \equiv 4x - 3 \ (\text{Modg}) \Rightarrow \kappa x^4 \equiv \kappa(4x - 3) \ (\text{Modg}) \tag{1}$$

όμοια $x^3 \equiv 3x - 2 (\text{Modg}) \Rightarrow \lambda x_3 \equiv \lambda(3x - 2) \ (\text{Modg})$ (2)

(1), (2) $\Rightarrow \kappa x^4 + \lambda x^3 \equiv \kappa(4x - 3) + \lambda(3x - 2) \ (\text{Modg}) \Rightarrow$

$\kappa x^4 + \lambda x^3 - 3 \equiv x(4\kappa + 3\lambda) + (-3\kappa - 2\lambda - 3) \ (\text{Modg}) \Rightarrow$

$f(x) = \pi(x) \cdot g(x) + x(4\kappa + 3\lambda) + (-3\kappa - 2\lambda - 3)$

για να διαιρεί το g(x) το f(x) πρέπει το πολυώνυμο

$$h(x) = x(4k + 3\lambda) + (-3\kappa - 2\lambda - 3)$$

να είναι το μηδενικό δηλαδή $\left.\begin{matrix} 4k + 3\lambda = 0 \\ 3\kappa + 2\lambda = 3 \end{matrix}\right\} \Rightarrow \begin{matrix} \kappa = 9 \\ \lambda = -12 \end{matrix}$

6. Να υπολογισθούν τα κ, λ έτσι ώστε το πολυώνυμο $f(x) = \kappa x^{\nu+1} + \lambda x^{\nu} + 1$ να έχει διπλή ρίζα τον αριθμό 1.

ΛΥΣΗ

Για να έχει το $f(x) = \kappa x^{\nu+1} + \lambda x^{\nu} + 1$ διπλή ρίζα τον αριθμό 1 πρέπει να διαιρείται με το $g(x) = (x - 1)^2$.

Από την εφαρμογή 4 έχω:

$$x^{\nu+1} \equiv (\nu + 1)x - \nu \ (\text{Modg}) \Rightarrow \kappa x^{n+1} \equiv \kappa(\nu + 1)x - \kappa\nu \ (\text{Modg}) \quad (1)$$

$$x^{\nu} \equiv \nu x - (\nu - 1) \ (\text{Modg}) \Rightarrow \lambda x^{\nu} \equiv \lambda\nu x - \lambda(\nu - 1) \ (\text{Modg}) \quad (2)$$

$$1 \equiv 1 \ (\text{Modg}) \quad (3)$$

$$(1), (2), (3) \Rightarrow f(x) \equiv x[\kappa(\nu + 1) + \lambda\nu] - \kappa\nu - \lambda(\nu - 1) + 1 \ (\text{Modg})$$

εργαζόμαστε με τον ίδιο τρόπο όπως στην εφαρμογή 5 και έχω τελικά $\kappa = \nu$, $\lambda = -(\nu + 1)$.

7. Για ποιες τιμές του $\nu \in \mathbb{N}$ το πολυώνυμο $f(x) = x^{2\nu} + x^{\nu} + 1$ διαιρείται με το $g(x) = x^2 + x + 1$.

ΛΥΣΗ

Θεωρώ το $\nu = 3\pi + \upsilon$ με $\pi \in \mathbb{N}$ και $\upsilon = 0, 1, 2$

τότε $$f(x) = x^{2(3\pi+\upsilon)} + x^{3\pi+\upsilon} + 1$$

$$x^3 \equiv 1 \ (\text{Modg}) \Rightarrow x^{6\pi} \equiv 1(\text{Modg}) \Rightarrow x^{6\pi+2\upsilon} \equiv x^{2\upsilon} \ (\text{Modg}) \quad (1)$$

$$x^3 \equiv 1 \ (\text{Mod g}) \Rightarrow x^{3\pi} \equiv 1 \ (\text{Modg}) \Rightarrow x^{3\pi+\upsilon} \equiv x^{\upsilon} \ (\text{Modg}) \quad (2)$$

$$1 \equiv 1 \ (\text{Modg}) \quad (3)$$

$$(1), \ (2), \ (3) \Rightarrow f(x) \equiv x^{2\upsilon} + x^{\upsilon} + 1(\text{Modg}) \quad \text{με} \quad \upsilon = 0, 1, 2$$

για $\upsilon = 0$ $\quad f(x) \equiv 3 \ (\text{Modg}) \Rightarrow g(x) \not| f(x)$

για $\upsilon = 1$ $\quad f(x) \equiv x^2 + x + 1 \ (\text{Modg}) \Rightarrow g(x)/f(x)$

για $\upsilon = 2$ $\quad f(x) \equiv x^4 + x^2 + 1 \ (\text{Modg})$

$x^4 + x^2 + 1 \equiv x^2 + x + 1 \ (\text{Modg}) \Big/ \Rightarrow g(x)/f(x)$

άρα όταν $\nu \neq 3\pi$, $\pi \in \mathbb{N}$ το $g(x)/f(x)$

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. ΑΡΙΘΜΟΘΕΩΡΙΑ J. HUNDTER Μετάφραση Ν. ΚΡΗΤΙΚΟΥ
2. ΠΟΛΥΩΝΥΜΑ Θ. ΚΑΖΑΝΤΖΗ