23/11/2018

$\phi: \mathbb{N} \to \mathbb{Z}$

$\phi(n) = \# n(\mathbb{Z}_n) = \# \{ a : a$ ακέραιος, $1 \le a \le n$ και ΜΚΔ$(a,n) = 1 \}$

Δείξαμε $\phi(p^k) = p^k - p^{k-1}$ όταν p πρώτος, και $k \ge 1$.

Παραδειγμα: $\phi(3^{12}) = 3^{12} - 3^{11}$

Παρατηρηση: $\phi(2) = 1 \quad \phi(4) = 2$

$1, 2, 3, 4$

Συμπερασμα: Δεν ισχυει γενικα για την ϕ: $\phi(x\,n) = \phi(x)\,\phi(n)$ (πχ δεν ισχυει για $x = n = 2$)

Προταση: Εστω $x, y \in \mathbb{N}$ με ΜΚΔ$(x,y) = 1$. Τοτε $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$

Ορισμος: Μια συναρτηση $f: \mathbb{N} \to \mathbb{Z}$ λεγεται:

(i) πολλαπλασιαστικη αν $f(x \cdot y) = f(x) \cdot f(y)$ όταν ΜΚΔ$(x,y) = 1$

(ii) πληρως πολλαπλασιαστικη, αν $f(x \cdot y) = f(x) \cdot f(y)$ όταν $x, y \in \mathbb{N}$

Παραδειγμα: Ειδαμε ότι η συναρτηση ϕ ειναι πολλαπλασιαστικη αλλα δεν ειναι πληρως πολλαπλασιαστικη

Παραδειγμα: Η $f: \mathbb{N} \to \mathbb{Z}$ με $f(x) = x^3$ ειναι πληρως πολλαπλασιαστικη γιατι $f(xy) = (xy)^3 = x^3 y^3 = f(x) \cdot f(y)$

Παραδειγμα: Η συναρτηση $Z: \mathbb{N} \to \mathbb{Z}$ με $Z(x) =$ ο αριθμος των θετικων διαιρετων του x. Εχουμε δει ότι αν $x = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ πρωτογ. αναλυση τοτε $Z(x) = (a_1+1)(a_2+1) \dots (a_r+1)$ και ο τυπος ισχυει και αν καποια απο τα a_i ειναι μηδεν.

Έχουμε $Z(2)=2$, $Z(4)=3$, συνεπώς δεν ισχύει γενικά $Z(xy)=Z(x)\cdot Z(y)$. Συνεπώς η Z δεν είναι πλήρως πολλαπλασιαστική.

Πρόταση: Η $Z: \mathbb{N} \to \mathbb{Z}$ είναι πολλαπλασιαστική.

Απόδειξη: Έστω $x, y \in \mathbb{N}$ και $p_1, p_2, \dots, p_r$ πρώτοι, διαφορετικοί ανά δύο ώστε κάθε πρώτος διαιρέτης του x και κάθε πρώτος διαιρέτης του y είναι ένας από τα p_i. Τότε υπάρχουν $a_i, b_i \geq 0$ ώστε $x = p_1^{a_1} \cdots p_r^{a_r}$, $y = p_1^{b_1} \cdots p_r^{b_r}$.
Συνεπώς, $Z(x) = (a_1+1)\cdots(a_r+1)$, $Z(y) = (b_1+1)\cdots(b_r+1)$.
Έχουμε $x \cdot y = p_1^{a_1+b_1} p_2^{a_2+b_2} \cdots p_r^{a_r+b_r}$. Αφού $\text{ΜΚΔ}(x,y)=1$ ισχύει αν $a_i \neq 0$, τότε $b_i = 0$ και αν $b_i \neq 0$ τότε $a_i = 0$.
Άρα για κάθε i $(a_i+b_i+1) = (a_i+1)(b_i+1)$ $(*)$
(γιατί για κάθε i τουλάχιστον 1 από τα a_i ή b_i είναι 0)
Συνεπώς, $Z(xy) = \prod_{i=1}^{r}(a_i+b_i+1) \overset{(*)}{=} \prod_{i=1}^{r}\big((a_i+1)(b_i+1)\big) =$
$\left(\prod_{i=1}^{r}(a_i+1)\right)\left(\prod_{i=1}^{r}(b_i+1)\right) = Z(x)\cdot Z(y)$

Πρόταση: Έστω $n \in \mathbb{Z}$ με $n \geq 2$ και πρωταρχική ανάλυση $n = p_1^{a_1} \cdots p_r^{a_r}$ (όπου p_i πρώτοι, $p_i \neq p_j$ για $i \neq j$ και $a_i > 0$ ακέραιοι). Τότε $\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right) =$
$= \left(p_1^{a_1} - p_1^{a_1-1}\right)\left(p_2^{a_2} - p_2^{a_2-1}\right)\cdots\left(p_r^{a_r} - p_r^{a_r-1}\right)$

ΑΠΟΔΕΙΞΗ: Αφού από πρόταση ϕ πολλαπλ. έχουμε με επαγωγή $\phi(x_1 x_2 \ldots x_r) = \phi(x_1)\phi(x_2)\ldots\phi(x_r)$ όταν $ΜΚΔ(x_i, x_j) = 1$ για $i \neq j$. Συνεπώς $\phi(n) = \phi(p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}) = \phi(p_1^{a_1})\phi(p_2^{a_2}) \ldots \phi(p_r^{a_r}) \overset{\text{ΠΡΟΤΑΣΗ}}{=} (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}) \ldots (p_r^{a_r} - p_r^{a_r-1})$

ΙΣΧΥΡΙΣΜΟΣ: $n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_r}\right) = (p_1^{a_1} - p_1^{a_1-1}) \ldots (p_r^{a_r} - p_r^{a_r-1})$

ΑΠΟΔΕΙΞΗ (ΙΣΧΥΡΙΣΜΟΥ): $n\left(1 - \frac{1}{p_1}\right)\ldots\left(1 - \frac{1}{p_r}\right) = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r} \left(1 - \frac{1}{p_1}\right)\ldots\left(1 - \frac{1}{p_r}\right) = p_1^{a_1}\left(1 - \frac{1}{p_1}\right) \cdot p_2^{a_2}\left(1 - \frac{1}{p_2}\right) \ldots p_r^{a_r}\left(1 - \frac{1}{p_r}\right) =$

$= (p_1^{a_1} - p_1^{a_1-1}) \ldots (p_r^{a_r} - p_r^{a_r-1})$

ΠΑΡΑΔΕΙΓΜΑ: Υπολογίστε $\phi(56)$

ΛΥΣΗ: $56 = 2 \cdot 28 = 2^2 \cdot 14 = 2^3 \cdot 7$

Από πρόταση $\phi(56) = (2^3 - 2^2)(7^1 - 7^0) = 4 \cdot 6 = 24$

Δηλαδή: Υπάρχουν 24 ακέραιοι μεταξύ 1 και 56 που είναι σχετικά πρώτοι με το 56 (δηλ. έχουν ΜΚΔ με το 56 ίσο με 1)

ΟΡΙΣΜΟΣ: Έστω $n \geq 1$ ακέραιος. Οι n το πλήθος ακέραιοι $a_1, a_2, \ldots a_n$ λέγονται **πλήρες σύστημα υπολοίπων** $\mod n$ αν $\mathbb{Z}_n = \{[a_1]_n, [a_2]_n, \ldots [a_n]_n\}$

ΠΑΡΑΔΕΙΓΜΑ: Αν $a_1 = 0, a_2 = 1, a_3 = 2, \ldots a_n = n-1$ τότε οι $a_1, \ldots a_n$ είναι πλήρες σύστημα υπολοίπων $\mod n$ από πρόταση

ΠΑΡΑΔΕΙΓΜΑ: Έστω $n=2$ και $a_1 = 1$, $a_2 = 201$. Είναι τα a_1, a_2 ΠΣΥ mod n;

ΛΥΣΗ: Επειδή $[a_1]_n = [1]_n$, $[a_2]_n = [201]_n = [1]_n$

Άρα a_1, a_2 όχι ΠΣΥ mod n γιατί $[a_2]_2 = [a_1]_2$

ΕΡΩΤΗΜΑ: Έστω $a_1, a_2 \in \mathbb{Z}$. Πότε ισχύει a_1, a_2 ΠΣΥ mod 2;

ΛΥΣΗ: Αφού $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$ τότε a_1, a_2 Π.Σ.Υ. mod 2, αν ακριβώς ένα από τα a_1, a_2 είναι άρτιο, και το άλλο είναι περιττό.

ΠΡΟΤΑΣΗ: Έστω $n \geq 1$ ακέραιος και $a_1 \dots a_n$ ακέραιοι. Τα ακόλουθα είναι ισοδύναμα.

(1) $a_1 \dots a_n$ να είναι ΠΣΥ mod n

(2) Για κάθε $i \neq j$ $[a_i]_n \neq [a_j]_n$

(3) Έστω r_i το υπόλοιπο της Ευκλ. Διαίρεσης του a_i με το n. Τότε πρέπει $\{r_1, r_2, \dots, r_n\} = \{0, 1, 2, \dots, n-1\}$

(Ισοδύναμα πρέπει $r_i \neq r_j$ για $i \neq j$)

ΑΠΟΔΕΙΞΗ: Αφού από πρόταση $\mathbb{Z}_n = \{[0]_n, \dots, [n-1]_n\}$ και $[r_i]_n = [a_i]_n$ το αποτέλεσμα έπεται.

ΠΑΡΑΔΕΙΓΜΑ: Έστω $a_1, a_2, a_3 \in \mathbb{Z}$. Πότε είναι Π.Σ.Υ. mod 3;

ΛΥΣΗ: Από πρόταση πρέπει να αρκεί

(1) Κάποιο από τα a_i πολλαπλάσιο του 3 και

(2) Κάποιο από τα a_i είναι της μορφής $3q+1$ (δηλ. το υπόλοιπο της Ευκλ. Διαίρ. του a_i με το 3 είναι 1)

(3) Κάποιο από τα a_i είναι της μορφής $3q+2$
Έστω $a_1 = 11$, $a_2 = 15$, $a_3 = 20$. Είναι τα a_1, a_2, a_3 ΠΣΥ mod3
Αφού $a_1 = 9+2 = 3\cdot3+2$ το a_1 είναι της μορφής $3q+2$.
Το a_2 είναι της μορφής $3q$. Τέλος το a_3 είναι επίσης της μορφής $3q+2$. Συνεπώς, a_1, a_2, a_3 όχι ΠΣΥ mod3 γιατί δεν υπάρχει a_i της μορφής $3q+1$.

Παράδειγμα: Τα $a_1 = 11$, $a_2 = 15$, $a_3 = -5$ είναι ΠΣΥ mod3, γιατί a_1 μορφής $3q+2$
a_2 μορφής $3q$
a_3 μορφής $3q+1$

Παράδειγμα: $n = 10$. Έστω $a_1 \dots a_{10}$ ΔΕΚΑ ΘΕΤΙΚΟΙ ΑΚΕΡΑΙΟΙ
Έστω r_i το υπόλοιπο της Ευκλ. Διαιρ. του a_i με το 10. Φανερά r_i το τελευταίο δεκαδικό ψηφίο του a_i. Από την πρόταση, τα $a_1, \dots, a_{10}$ είναι ΠΣΥ mod10 αν-ν για κάθε $j \in \{0,1,2,\dots,9\}$ υπάρχει r_i με $r_i = j$.

Συμπέρασμα: Τα $a_1 \dots a_{10}$ είναι ΠΣΥ mod10, αν-ν $b_i \neq b_j$ για $i \neq j$, όπου $b_i \in \{0,\dots,9\}$ το τελευταίο δεκαδικό ψηφίο του a_i.

Παράδειγμα: Έστω $a_1 \dots a_{10} = 2013, 2022, 55, 177, 9, 44, 36, 78, 1000, 11$. Τα τελευταία δεκαδικά ψηφία τους είναι
3, 2, 5, 7, 9, 4, 6, 8, 0, 1
Αφού δεν έχουμε επαναλήψεις τα $a_1, \dots, a_{10}$ είναι ΠΣΥ mod10. Αν αλλάξουμε το a_{10} σε 33 τότε τα $a_1 \dots a_{10}$ δεν είναι ΠΣΥ mod10 γιατί $[a_1]_{10} = [3]_{10} = [a_{10}]_{10}$.

Πρόταση: Έστω $n \geq 2$, $k \in \mathbb{Z}$. Θέτουμε $a_1 = k$, $a_2 = k+1$, $a_3 = k+2$, ... $a_n = k+n-1$. Τότε $a_1, a_2 \ldots a_n$ ΠΣΥ mod n

Απόδειξη: Από την πρόταση, αρκεί να δείξουμε ότι αν $1 \leq i < j \leq n$ τότε $[a_i]_n \neq [a_j]_n \in \mathbb{Z}_n$. Έστω ότι δεν ισχύει για κάποια i, j άρα $[a_i]_n = [a_j]_n$. Δηλ. συνεπάγεται $n \mid a_j - a_i$. Αλλά

$$a_j - a_i = k+(j-1) - (k-(i-1)) = j-i$$

Αλλά $0 < j-i < n$, άρα $n \nmid j-i$ αντίφαση.