03/12/2018

Πρόταση: Έστω $n \geq 1$ και $a, b \in \mathbb{Z}$. Υποθέτουμε $a \equiv b \bmod n$ (*)
Τότε $\text{ΜΚΔ}(a, n) = 1$ αν-ν $\text{ΜΚΔ}(b, n) = 1$.

Απόδειξη: Υποθέτουμε $\text{ΜΚΔ}(a, n) = 1$. Από (*) $n \mid b - a$ άρα υπάρχει $k \in \mathbb{Z}$ ώστε $b - a = kn \Rightarrow b = kn + a$. Συνεπώς,
$$\text{ΜΚΔ}(b, n) = \text{ΜΚΔ}(a + kn, n) \overset{\text{ΠΡΟΤΑΣΗ}}{=\!=} \text{ΜΚΔ}(a + kn - kn, n) = \text{ΜΚΔ}(a, n) = 1.$$

Παράδειγμα: Έχουμε $\text{ΜΚΔ}(3, 7) = 1$ και $52 \equiv 3 \bmod 7$ (γιατί $7 \mid (52 - 3 = 49)$). Συνεπώς από πρόταση $\text{ΜΚΔ}(52, 7) = \text{ΜΚΔ}(3, 7) = 1$

Παρατήρηση: Η απόδειξη της πρότασης, δίνει πιο γενικά ότι αν $a \equiv b \bmod n$, τότε $\text{ΜΚΔ}(a, n) = \text{ΜΚΔ}(b, n)$

Ορισμός: Έστω $n \geq 1$, $a \in \mathbb{Z}$ και $[a]_n$ το αντίστοιχο στοιχείο του $\mathbb{Z}_n$. Ορίζουμε $\text{ΜΚΔ}([a]_n, n) = \text{ΜΚΔ}(a, n)$. Από τα παραπάνω, ο ορισμός δεν εξαρτάται από την επιλογή του a γιατί $[a]_n = [b]_n \Rightarrow a \equiv b \bmod n \Rightarrow \text{ΜΚΔ}(a, n) = \text{ΜΚΔ}(b, n)$

ΠΑΡΑΔΕΙΓΜΑ: $n=3$, Τότε ΜΚΔ$(\underset{\mathbb{Z}_3}{[15]_3},3)$ = ΜΚΔ$(15,3)=3$

ΥΠΕΝΘΥΜΙΣΗ: Αν $n=1$, $\varphi(1)=1$, αν $n=p_1^{a_1}\ldots p_r^{a_r}$ τότε $\varphi(n)=(p_1^{a_1}-p_1^{a_1-1})$
$(p_2^{a_2}-p_2^{a_2-1})\ldots(p_r^{a_r}-p_r^{a_r-1})$ $\varphi=\varphi$ του Euler.

ΟΡΙΣΜΟΣ: Έστω $n\geq 1$ και $a_1,a_2,\ldots,a_{\varphi(n)}$ .. $\varphi(n)$ το πλήθος ακέραιοι.
Οι $a_1,\ldots a_{\varphi(n)}$ λέγονται περιορισμένο σύστημα υπολοίπων mod$n$, αν
(i) ΜΚΔ$(a_i,n)=1$, $\forall i$
Π.Σ.Υ mod$n$) (ii) $(1.(\mathbb{Z}_n))=\{[a_1]_n,[a_2]_n,\ldots,[a_{\varphi(n)}]_n\}$

ΠΑΡΑΤΗΡΗΣΗ: Από τους ορισμούς προκύπτει ο εξής αλγόριθμος:
→ **ΑΛΓΟΡΙΘΜΟΣ:** Έστω $n\geq 1$, $a_1\ldots a_{\varphi(n)}$ ακέραιοι. Δέχομε r_i το υπόλοιπο της Ευκλ. διαιρέσεως του a_i με το n. Τότε $a_1,\ldots a_{\varphi(n)}$ περ. Σ.Υ. mod$n$ αν-ν ΜΚΔ$(r_i,n)=1$ για κάθε i και οι ακέραιοι $r_1,\ldots r_{\varphi(n)}$ είναι διαφορετικοί ανά δύο.

ΠΡΟΤΑΣΗ: Έστω $a_1,\ldots a_{\varphi(n)}$ οι ακέραιοι μεταξύ 1 και n που είναι πρώτοι με το n. Τότε το $a_1,\ldots a_{\varphi(n)}$ είναι περιορισμένο Σ.Υ. mod$n$

ΑΠΟΔΕΙΞΗ: Άμεσο από τους ορισμούς

ΠΑΡΑΔΕΙΓΜΑ: $n=15$. Οι ακέραιοι 1, 2, 4, 7, 8, 11, 13, 14 είναι από την πρόταση περιορισμένο Σ.Υ mod 15. Συνεπώς $\varphi(15)=8$.

Ερώτημα: Έστω $n = 8 = 2^3$. Τότε $\varphi(n) = \varphi(8) = 2^3 - 2^2 = 4$
Είναι οι ακέραιοι 11, 21, 31, 41 περιορισμένο ΣΥ mod 8;

Απάντηση: Κατ' αρχήν αφού $\varphi(8) = 4$ οι αριθμοί έχουν το σωστό πλήθος. Εφαρμόζουμε τον αλγόριθμο. Έστω r_1 το υπόλοιπο της Ευκλ. Διαιρ. του a_i με το $n=8$. Τότε $r_1 = 3$, $r_2 = 5$, $r_3 = 7$, $r_4 = 1$.
Αφού $ΜΚΔ(r_i, 8) = 1$, για κάθε i, και οι αριθμοί r_1, r_2, r_3, r_4 είναι διαφορετικοί ανά δύο έπεται ότι a_1, a_2, a_3, a_4 περιορ. ΣΥ mod 8.

→ Είναι οι ακέραιοι 3, 5, 21, 22 περιορ. ΣΥ mod 8;
Απάντηση: Όχι, γιατί $ΜΚΔ(22, 8) \neq 1$.

→ Είναι οι ακέραιοι $\underset{a_1}{11}$, $\underset{a_2}{21}$, $\underset{a_3}{31}$, $\underset{a_4}{51}$ περιορ. ΣΥ mod 8;
Απάντηση: Έστω r_1, r_4 τα υπόλοιπα της ευκλ. διαιρ. του a_i με το 8. Έχουμε $r_1 = 3$, $r_2 = 5$, $r_3 = 7$, $r_4 = 3$. Αφού $r_1 = r_4$ από τον αλγόριθμο έπεται ότι οι $a_1, \dots, a_4$ ΔΕΝ είναι περιορ. Σ.Υ mod 8

Φυλλάδιο 6

Άσκηση 6:
Έστω $n \geq 1$, $a \in \mathbb{Z}$
Τότε οι $a, a+1, a+2, \dots, a+n-1$ είναι ΠΛΗΡΕΣ ΣΥ mod n, επίσης ακριβώς $\varphi(n)$ από αυτούς είναι πρώτοι ως προς το n.
Απόδειξη: Έχουμε δείξει στη θεωρία ότι είναι ΠΛΗΡΕΣ ΣΥ.
Από πρόταση, αν r_1 το υπόλοιπο της Ευκλ. διαιρ. του a με το n
r_2 " " " " " " $a+1$ " " "
r_n " " " " " " $a+n-1$ με το n

Έχουμε ότι τα r_i είναι διαφορετικά ανά δύο, συνεπώς το σύνολο τους είναι ίσο με το σύνολο $\{0,1,2,\dots,n-1\}$. Αφού $a+j$ πρώτο ως προς τον n, τότε το r_j+1 πρώτο ως προς τον n (από πρόταση), έχουμε ότι ο αριθμός από τα $a, a+1, a+n-1$ που είναι πρώτοι με τον n, είναι ίσος με τον αριθμό των ακεραίων στο $\{0,1,2,\dots,n-1\}$ που είναι πρώτοι με το n, και αυτός ο αριθμός εξ' ορισμού είναι ίσος με $\varphi(n)$.

ΠΑΡΑΔΕΙΓΜΑ: Πόσοι ακέραιοι k με $2018 \le k \le 2029$ είναι πρώτοι ως προς το 12;

ΛΥΣΗ: Οι ακέραιοι 2018, 2019, ..., 2029 είναι 12 διαδοχικοί. Επομένως από την άσκηση που λύσαμε κάναμε $\varphi(12)=\varphi(2^2 3)=(2^2-2)(3-1)=4$. Από αυτούς είναι πρώτοι με το 12.

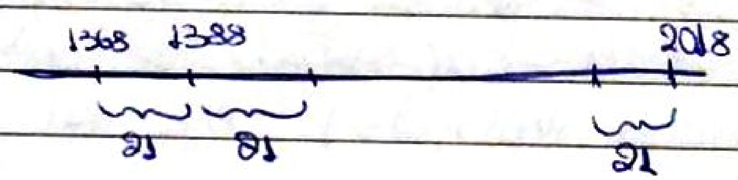
ΑΣΚΗΣΗ 7

Πόσοι ακέραιοι μεταξύ του 1368 και του 2018 είναι πρώτοι με το 21;

ΛΥΣΗ: Έχουμε 2018 - 1367 ακεραίους δηλ 651 ακεραίους

2018 | 21   651 | 21
1367   63 | 31
651   21

Έχουμε $651 = 31 \cdot 21$



Έχουμε 31 διαστήματα ξένα ανά δύο, ώστε κάθε διάστημα να περιέχει ακριβώς 21 διαδοχ. ακεραίους. Σε κάθε διάστημα από την προηγούμενη άσκηση υπάρχουν $\varphi(21)=\varphi(3\cdot 7)=(3-1)(7-1)=12$ ακέραιοι πρώτοι ως προς το 21. Συνεπώς υπάρχουν $31\cdot 12=372$ ακέραιοι μεταξύ του 1368 και του 2018 που είναι πρώτοι προς το 21.

Πρόταση: Έστω $n \geq 1$, $c \in \mathbb{Z}$ με $ΜΚΔ(c, n) = 1$ και $a_1, a_2, \dots, a_{\varphi(n)}$ περιορισμένο σ.υ. mod n. Δείξτε ότι οι ακέραιοι $(a_1, a_2, \dots, a_{\varphi(n)})$ είναι επίσης περιορ. σ.υ. mod n (Δηλαδή αν πολλαπλασιάσω ένα περιορ. σ.υ mod n με έναν ακέραιο πρώτο ως προς το n, επαίρνω ξανά περιορ. σ.υ. mod n)

Απόδειξη: Πρέπει να δείξουμε:

(i) $ΜΚΔ(a_i, n) = 1 \quad \forall i$

(ii) Αν $i \neq j$ $(a_i \not\equiv c a_j \bmod n$ (δηλαδή το n ΔΕΝ διαιρεί το $a_i - c a_j$)

Για το (i) → Έχουμε $ΜΚΔ(a_i, n) = 1 \Rightarrow$ υπάρχουν $x_1, y_1 \in \mathbb{Z}$ με

$$1 = x_1 a_1 + y_1 n \quad (1)$$

Επίσης $ΜΚΔ(c, n) = 1 \Rightarrow$ υπάρχουν $x_2, y_2 \in \mathbb{Z}$ με

$$1 = x_2 c + y_2 n \quad (2)$$

Πολλαπλασιάζοντας $(1) \cdot (2) \Rightarrow 1 = x_1 x_2 c a_1 + (x_1 a_1 y_2 + x_2 c y_1 + y_1 y_2 n) n \quad (3)$

$(3) \Rightarrow ΜΚΔ(a_i, n) = 1$

Για το (ii) → Έστω ότι για κάποια $i \neq j$ $c a_i \equiv c a_j \bmod n$

Τότε $n \mid c a_i - c a_j \Rightarrow n \mid c(a_i - a_j) \quad (4)$

Από υπόθεση $ΜΚΔ(n, c) = 1$. Άρα $(4) \Rightarrow n \mid a_i - a_j \Rightarrow$

$a_i \equiv a_j \bmod n$ αντίφαση.

Θεώρημα (Euler - Fermat): Έστω $n \geq 1$ και $a \in \mathbb{Z}$ με ΜΚΔ$(a,n)=1$. Τότε $a^{\varphi(n)} \equiv 1 \bmod n$.

Παράδειγμα: Έστω $n=5$. Τότε $\varphi(n)=4$. Συνεπώς για κάθε ακέραιο a με ΜΚΔ$(a,5)=1$, δηλ. για κάθε ακέραιο που δεν είναι πολλαπλάσιο του 5, $a^4 \equiv 1 \bmod 5$, δηλ. $5 \mid a^4 - 1$

Απόδειξη: Έστω $z_1, \dots, z_{\varphi(n)}$ περιορισμ. Σ.Υ. mod n. Από πρόταση $az_1, az_2, \dots, az_{\varphi(n)}$ επίσης περιορ. Σ.Υ. mod n. Συνεπώς υπάρχει $\sigma : \{1, \dots, \varphi(n)\} \to \{1, \dots, \varphi(n)\}$ 1-1 και επί ώστε $az_i \equiv z_{\sigma(i)} \bmod n$ για $i=1,2,\dots,\varphi(n)$

Πολλαπλ. $a^{\varphi(n)} z_1 z_2 \cdots z_{\varphi(n)} \equiv z_1 z_2 \cdots z_{\varphi(n)} \bmod n \Rightarrow$

$n \mid a^{\varphi(n)} z_1 \cdots z_{\varphi(n)} - z_1 \cdots z_{\varphi(n)} = (a^{\varphi(n)} - 1) z_1 z_2 \cdots z_{\varphi(n)}$

Αφού ΜΚΔ$(n,z_i)=1$ για κάθε i έπεται $n \mid a^{\varphi(n)} - 1$, άρα το θεώρημα.

Παράδειγμα: Δείξτε ότι $561 \mid 5^{320} - 1$

Απόδειξη: Έστω $n=561$. Ο n έχει πρωτογενή ανάλυση. Αφού $5+6+1=12$ πολλαπλάσιο του 3, $3 \mid n$ και $561 = 3 \cdot 187$. Αφού $1-8+7=0$ έχουμε $11 \mid 187$. Τελικά $561 = 3 \cdot 11 \cdot 17$. Συνεπώς $\varphi(561) = (3-3^0)(11-11^0)(17-17^0) = 2 \cdot 10 \cdot 16 = 320$. Αφού ΜΚΔ$(5,561)=1$ από Θ. Euler-Fermat $5^{\varphi(561)} \equiv 1 \bmod 561$, δηλ. $561 \mid 5^{320} - 1$.

Πόρισμα: Έστω $n \geq 2$ και $a \in \mathbb{Z}$ με ΜΚΔ$(a,n)=1$. Τότε στο $\mathbb{Z}_n$ $([a]_n)^{-1} = [a^{\varphi(n)-1}]_n$

Απόδειξη: Αφού $n \geq 3$, $\varphi(n) \geq 2$. Από Θ. Euler-Fermat

$$[a]_n [a^{\varphi(n)-1}]_n = [a^{\varphi(n)}]_n = [1]_n$$

ΠΑΡΑΤΗΡΗΣΗ: Στην πράξη συνήθως υπολογίζουμε το $([\alpha]n)^{-1}$ με Ευκλ. Αλγόριθμο, και όχι την παραπάνω πρόταση.

ΠΟΡΙΣΜΑ: Έστω p πρώτος και $\alpha \in \mathbb{Z}$ που δεν είναι πολλαπλάσιο του p. Τότε $\alpha^{p-1} \equiv 1 \bmod p$

ΑΠΟΔΕΙΞΗ: p πρώτος + α όχι πολλαπλάσιο του p $\Rightarrow$ ΜΚΔ$(\alpha, p) = 1$. Αφού p πρώτος, $\varphi(p) = p^1 - p^0 = p - 1$. Άρα το αποτέλεσμα έπεται από το Θ. Euler - Fermat.

ΠΡΟΤΑΣΗ: Έστω p πρώτος και $\alpha \in \mathbb{Z}$. Τότε $\alpha^p \equiv \alpha \bmod p$.

ΑΠΟΔΕΙΞΗ:

→ Περίπτωση - 1: ΜΚΔ$(\alpha, p) = 1$. Τότε από πόρισμα $\alpha^{p-1} \equiv 1 \bmod p$ $\Rightarrow p \mid \alpha^{p-1} - 1 \Rightarrow p \mid \alpha(\alpha^{p-1} - 1) \Rightarrow p \mid (\alpha^p - \alpha) \Rightarrow \alpha^p \equiv \alpha \bmod p$

→ Περίπτωση - 2: ΜΚΔ$(\alpha, p) = p$. Τότε $p \mid \alpha$ αφού p πρώτος. Συνεπώς, $\alpha^p \equiv 0 \bmod p$, $\alpha \equiv 0 \bmod p$, και η πρόταση ισχύει.

ΠΑΡΑΔΕΙΓΜΑ: Έστω $p = 2$ και $\alpha \in \mathbb{Z}$. Τότε $2 \mid \alpha^2 - \alpha$

$p = 3$ και $\alpha \in \mathbb{Z}$. Τότε $3 \mid \alpha^3 - \alpha$

$p = 5$ και $\alpha \in \mathbb{Z}$. Τότε $5 \mid \alpha^5 - \alpha$.

ΠΑΡΑΔΕΙΓΜΑ: Έστω $k \geq 1$ ακέραιος. Δείξτε ότι το υπόλοιπο της Ευκλ. Διαιρ. του 10^{6k+4} με το 7 είναι 4.