ΠΑΡΑΤΗΡΗΣΗ: Συνεπώς έχουμε n διαδοχικούς ακεραίους που ξεκινάν από $a\in\mathbb{Z}$, αυτοί είναι $\{a, a+1, a+2, \dots, a+n-1\}$.

Ορισμός: Έστω $n\geq 1$. Τότε n ακέραιοι $a_1, a_2, \dots, a_n$ είναι ΠΛΗΡΕΣ ΣΥΣΤΗΜΑ υπολοίπων modulo n, αν $\mathbb{Z}/n = \{[a_1]_n, [a_2]_n, \dots, [a_n]_n\}$

Π.χ. Έστω $n\geq 1$. Τότε οι ακέραιοι $0, 1, 2, \dots, n-1$ είναι πλήρες σύστημα υπολοίπων modulo n. Το ίδιο κ' οι ακέραιοι $1, 2, 3, \dots, n-1, n$

Π.χ.: Έστω $n=3$. Είναι οι 3 ακέραιοι $2, 3, 5$ πλήρες σύστημα υπολοίπων modulo 3;

Λύση: Έχουμε $\{[2]_3, [3]_3, [5]_3\} = \{[2]_3, [0]_3, [2]_3\} = \{[0]_3, [2]_3\} \neq \mathbb{Z}/3$.
Άρα δεν είναι.

Υπενθύμιση: Έστω $n\geq 1$ κ' $a_1, \dots, a_n$ n ακέραιοι. Λέμε ότι είναι πλήρες σύστημα υπολοίπων (π.σ.υ) mod n αν $\mathbb{Z}/n = \{[a_1]_n, [a_2]_n, \dots, [a_n]_n\}$

Π.χ. Οι $1, 2, 3, \dots, n$ είναι π.σ.υ mod n. Το ίδιο κ' τα $0, 1, 2, \dots, n-1$

Πρόταση: Έστω $n\geq 1$ κ' $a_1, \dots, a_n\in\mathbb{Z}$. Τα ακόλουθα είναι ισοδύναμα
(i) $a_1, \dots, a_n$ π.σ.υ mod n
(ii) Για $i\neq j$ $[a_i]_n \neq [a_j]_n$
(iii) Έστω r_i το υπόλοιπο της Ευκλείδειας Διαίρεσης του a_i με το n. Τότε $r_i\neq r_j$ για $i\neq j$

Απόδειξη: (i) $\Rightarrow$ (ii) Αφού $\#\mathbb{Z}/n = n$, φανερά $\{[a_1]_n, \dots, [a_n]_n\} = \mathbb{Z}/n$ συνεπάγεται $[a_i]_n \neq [a_j]_n$ για $i\neq j$

(ii) $\Rightarrow$ (i) Αφού $\#\mathbb{Z}/n = n$ αν $[a_i]_n \neq [a_j]_n$ για $i\neq j$ έχουμε ότι το υποσύνολο $\{[a_1]_n, \dots, [a_n]_n\}$ του $\mathbb{Z}/n$ έχει n στοιχεία. Αλλά $\#\mathbb{Z}/n = n$. Άρα από Θ. Ισότητα $\mathbb{Z}/n = \{[a_1]_n, \dots, [a_n]_n\}$

(ii) $\Leftrightarrow$ (iii) Αφού $[a_i]_n = [r_i]_n$ $\forall i$ κ' $0\leq r_i\leq n-1$ $\forall i$, άρα $[r_i]_n = [r_j]_n$ αν $r_i = r_j$, το αποτέλεσμα έπεται

Π.χ. Έστω $n=10$ κ' $a_1,\dots,a_{10}$ 10 θετικοί ακέραιοι. Τότε οι $a_1,\dots,a_{10}$ είναι πσυ mod 10, αν για $i\neq j$ το τελευταίο δεκαδικό ψηφίο του a_i είναι διάφορο από το τελευταίο δεκαδικό ψηφίο του a_j. Ο λόγος είναι η πρόταση μαζί με το ότι το τελευταίο δεκαδικό ψηφίο του a_i είναι ακριβώς το υπόλοιπο της Ευκλείδειας Διαίρεσης του a_i με το 10 (Προσοχή για αυτό δεν ισχύει, π.χ. αν $a_i=-1$, το υπόλοιπο της Ευκλείδειας Διαίρεσης του a με το 10 είναι το 9, γιατί $-1=(-1)10+9$ κ' $0\leq 9\leq 10-1$)

$-11 \quad -10 \quad 9$

Π.χ. Είναι οι $14, 24, 9, -11, 34, 68, -21, 87$ πσυ mod 8;

Λύση:

Έχουμε $[14]_8=[6]_8$, $[24]_8=[0]_8$, $[9]_8=[1]_8$, $[-11]_8=[5]_8$, $[34]_8=[2]_8$, $[68]_8=[4]_8$, $[-21]_8=[3]_8$, $[87]_8=[7]_8$

Συνεπώς οι αριθμοί είναι πσυ mod 8

Πρόταση: Έστω $n\geq 2$, $b,c\in\mathbb{Z}$ με $b\neq 0$ κ' ΜΚΔ$(b,n)=1$

Υποθέτουμε ότι τα $a_1,a_2,\dots,a_n$ είναι πσυ mod n

Τότε κ' τα $ba_1+c, ba_2+c, ba_3+c, \dots, ba_n+c$ είναι πσυ mod(n)

Απόδειξη: Έστω ότι δεν ισχύει. Τότε από την Πρόταση $\exists i,j$ με $i\neq j$ ώστε $[ba_i+c]_n=[ba_j+c]_n$.

Άρα $n\mid(ba_i+c)-(ba_j+c) \Rightarrow n\mid b(a_i-a_j) \underset{\text{ΜΚΔ}(b,n)=1}{\Rightarrow} n\mid(a_i-a_j)$

Άρα $[a_i]_n=[a_j]_n$, αντίφαση

ΠΑΡΑΤΗΡΗΣΗ: Προσοχή, η πρόταση δεν ισχύει γενικά αν ΜΚΔ$(b,n)\neq 1$.

π.χ. τα $0,1$ είναι πσυ mod 2, ενώ τα $2\cdot 0, 2\cdot 1$ δεν είναι

Άρα κ' το 2^8

Π.χ. Αφού ΜΚΔ$(2^8,5)=1$, έχουμε ότι αν $c\in\mathbb{Z}$ κ' $a_1,\dots,a_5$ πσυ mod 5, τότε κ' οι $2^8a_1+c, 2^8a_2+c, \dots, 2^8a_5+c$ είναι πσυ mod 5

Πρόταση: Έστω $n\geq 2$ κ' $a_1,\dots,a_n$ πσυ mod n. Τότε $\#\{i : \text{ΜΚΔ}(a_i,n)=1\}=\phi(n)$

Απόδειξη: Έχουμε δ.ο. $[b]_n=[c]_n \Rightarrow$ ΜΚΔ$(b,n)=$ ΜΚΔ(c,n)
Επίσης έχουμε δ.ο. $\phi(n)=\#\{j : 0\le j\le n-1$ κ' ΜΚΔ$(j,n)=1\}$. Άρα αν $a_1,\dots,a_n$ πσυ mod n έχουμε $\{[a_1]_n,[a_2]_n,\dots,[a_n]_n\}=\mathbb{Z}/=\{[0]_n,[1]_n,\dots,[n-1]_n\}$. Το αποτέλεσμα έπεται.

Φυλ 6 άσκ 6. Έστω $a,n\in\mathbb{Z}$ με $n\ge 1$. ΝΔΟ το σύνολο $S=\{a,a+1,\dots,a+n-1\}$ είναι πσυ mod n. Επίσης ΝΔΟ $\exists$ ακριβώς $\phi(n)$ στοιχεία του S πρώτα ως προς το n.

Λύση: Το $0,1,2,\dots,n-1$ είναι πσυ mod n. Από πρόταση για $b=1$ κ' $c=a$ έχουμε ότι το S είναι πσυ mod n.
(Θυμάσαι: $b\cdot 0+c, b\cdot 1+c,\dots, b(n-1)+c$ είναι πσυ mod n).
Από την τελευταία πρόταση, έχουμε ότι $\exists$ ακριβώς $\phi(n)$ από το $a,a+1,\dots,a+(n-1)$ πρώτα ως προς το n

ΥΠΕΝΘΥΜΙΣΗ: Αν $a,b\in\mathbb{Z}$ με $a<b$, τότε $\#\{a,a+1,a+2,\dots,b-1,b\}=b-a+1$

Φυλ 6 άσκ 7. Πόσοι ακέραιοι μεταξύ του 1368 κ' του 2018 είναι πρώτοι με το 21;

Λύση: Από Φυλ 6 άσκ 6 κάθε διάστημα 21 διαδοχικών ακεραίων έχει $\phi(21)$ από αυτούς αυτούς πρώτους με το 21. Έχουμε $21=3^1 7^1$ (πρωτογενής ανάλυση)
Συνεπώς, $\phi(21)=21(1-\frac{1}{3})(1-\frac{1}{7})=21\,\frac{2}{3}\,\frac{6}{7}=12$

Έχουμε $2018-1368+1=651$ κ' $651=31\cdot 21+0$.

Συνεπώς, το διάστημα των ακεραίων από 1368 έως το 2018 είναι ξένη ένωση 31 υποδιαστημάτων που το κάθε υποδιάστημα έχει 21 διαδοχικούς ακεραίους, άρα από Φυλ6 άσκ6 κάθε υποδιάστημα έχει $\phi(21)=12$ ακέραιους πρώτους με το 21. Συνεπώς, η απάντηση στην Άσκηση είναι $31\phi(21)=31\cdot 12=372$

Πχ. Ίδιο ερώτημα για 2019 αντί για 2018
Λύση: $2+0+1+9=12$, άρα $3|2019$, συνεπώς το 2019 δεν είναι πρώτος με το $21=3\cdot 7$. Συνεπώς, $\exists$ 372 ακέραιοι από Φυλ 6 άσκ 7, γιατί το 2019 δεν είναι.

Π.χ. Ίδιο ερώτημα για 2020 αντί για 2018

ΙΣΧΥΡΙΣΜΟΣ. $ΜΚΔ(2020,21)=1$

Λύση: Έστω ότι $ΜΚΔ(2020,21) \neq 1$. Τότε $\exists$ πρώτος p με $p|2020$ κ' $p|21=3\cdot 7$. Άρα $p=3$ ή $p=7$. Αλλά $2+2=4$ κ' $3\nmid 4$, άρα $3\nmid 2020$. Έχουμε $2020=288\cdot 7+4$, άρα $7\nmid 2020$, αντίφαση.

Συνεπώς $\exists$ $372+1=373$ ακέραιοι μεταξύ του 1368 κ' του 2020 πρώτοι με το 21.

Ορισμός: Έστω $n\geq 1$ κ' $b_1, b_2, \dots, b_{\phi(n)}$ $\phi(n)$ στο πλήθος ακέραιοι. Λέμε ότι αποτελούν ΠΕΡΙΟΡΙΣΜΕΝΟ (ή αναγωγικό) ΣΥΣΤΗΜΑ ΥΠΟΛΟΙΠΩΝ mod n, αν

$$\{[b_1]_n, [b_2]_n, \dots, [b_{\phi(n)}]_n\} = U(\mathbb{Z}_n)$$

Π.χ. $n=6$ $U(\mathbb{Z}_6)=\{[1]_6, [5]_6\}$

$$\phi(6)=\phi(2\cdot 3)=6\cdot\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)=2$$

Άρα τα $b_1=7$, $b_2=17$ είναι περιορισμένο σύστημα υπολοίπων mod 6, γιατί $[b_1]_6=[1]_6$, $[b_2]_6=[17]_6=[5]_6$.

ενώ τα $b_1=7, b_2=37$ ΔΕΝ είναι, γιατί:

$$[7]_6=[1]_6,\ [37]_6=[1]_6$$

άρα $\{[7]_6, [37]_6\} = \{[1]_6\} \neq U(\mathbb{Z}_6)$

Πρόταση: Έστω $n\geq 2$ κ' $b_1, b_2, \dots, b_{\phi(n)}$ ακέραιοι. Τα ακόλουθα είναι ισοδύναμα:

(i) $b_1, \dots, b_{\phi(n)}$ ΠΣΥ mod n

(ii) $ΜΚΔ(b_i, n)=1$ $\forall i$ κ' $[b_i]_n \neq [b_j]_n$ για $i\neq j$

Απόδειξη: Παρόμοια με την αντίστοιχη για Πλήρες Σύστημα Υπολοίπων mod n

Πρόταση: Έστω $n \geq 2$, $b_1, \dots, b_{\phi(n)}$ ΠΣΥ mod n κ' $e \in \mathbb{Z}$ με $ΜΚΔ(e,n)=1$. Τότε τα $eb_1, eb_2, \dots, eb_{\phi(n)}$ είναι επίσης ΠΣΥ mod n

Απόδειξη: ΙΣΧΥΡΙΣΜΟΣ 1. $ΜΚΔ(eb_i, n)=1$ $\forall i$

Απόδειξη: Πιο γενικά, ισχύει αν $x, y, n \in \mathbb{Z}$, $n \geq 2$ κ' $ΜΚΔ(x,n) = ΜΚΔ(y,n) = 1$, τότε $ΜΚΔ(xy, n) = 1$.

Πράγματι, αν $ΜΚΔ(xy) \neq 1$, $\exists$ πρώτος p με $p \mid xy$ κ' $p \mid n$.

Αφού $p \mid xy$ κι $p \mid n$ έχουμε

ΠΕΡΙΠΤΩΣΗ 1: $p \mid x$ κ' $p \mid n$, άρα $ΜΚΔ(x,n) \neq 1$, αντίφαση ή

ΠΕΡΙΠΤΩΣΗ 2: $p \mid y$ κ' $p \mid n$, άρα $ΜΚΔ(y,n) \neq 1$, αντίφαση.

ΙΣΧΥΡΙΣΜΟΣ 2: Έστω $i \neq j$. Τότε $[eb_i]_n \neq [eb_j]_n$

Απόδειξη: Έστω $[eb_i]_n = [eb_j]_n$. Τότε $n \mid e(b_i - b_j) \xRightarrow[ΜΚΔ(n,e)=1]{}$

$n \mid (b_i - b_j) \Rightarrow [b_i]_n = [b_j]_n$, αντίφαση

Από τους Ισχυρισμούς 1 κ' 2 η πρόταση έπεται.

ΠΑΡΑΤΗΡΗΣΗ: Στην απόδειξη είδαμε ότι αν $n \geq 2$ κ' $a, b \in \mathbb{Z}$ με $ΜΚΔ(a,n) = ΜΚΔ(b,n) = 1$, τότε $ΜΚΔ(ab, n) = 1$.

Συνεπώς αν $[a]_n, [b]_n \in U(\mathbb{Z}/n)$, έχουμε ότι $[a]_n [b]_n \in U(\mathbb{Z}/n)$.

Άρα το $U(\mathbb{Z}/n)$ με τον περιορισμό του πολλαπλασιασμού του $\mathbb{Z}/n$ γίνεται "ΟΜΑΔΑ" (γιατί η πράξη είναι καλά ορισμένη, προσεταιριστική, έχει ουδέτερο (το $[1]_n$) κ' κάθε στοιχείο έχει αντίστροφο)

Π.χ. Τα $b_1 = 1$, $b_2 = 7$, $b_3 = 18$, $b_4 = 24$ είναι ΠΣΥ mod 5, γιατί $ΜΚΔ(b_i, 5) = 1$ $\forall i$ κ' $[7]_5 = [2]_5$, $[18]_5 = [3]_5$, $[24]_5 = [4]_5$, άρα $\{[b_1]_5, [b_2]_5, \dots, [b_{\phi(5)}]_5\} = U(\mathbb{Z}/5)$

• Έστω $e = 2019$. Έχουμε $ΜΚΔ(e,5) = 1$, γιατί 5 πρώτος κ' $5 \nmid 2019$. Συνεπώς, από πρόταση οι $2019 \cdot 1 = 2019$, $2019 \cdot 7$, $2019 \cdot 18$, $2019 \cdot 24$ είναι ΠΣΥ mod 5

ΣΤΟΧΟΣ: Ν.δ.ο. για $a \in \mathbb{Z}$ με $a \geq 2$ ισχύει a πρώτος ανν $(a-1)! \equiv -1 \mod a$

(ισοδύναμα ανν $a \mid (a-1)! + 1$)

Ορισμός: Έστω $n \geq 1$. Ορίζουμε επαγωγικά το $n!$ ως εξής:

$$1! = 1 \text{ κ' } n! = n(n-1)! \text{ για } n \geq 2$$

Με άλλα λόγια, $n! = 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n-1) \cdot n$

π.χ. $2! = 1 \cdot 2 = 2$, $3! = 3 \cdot 2! = 6$, $4! = 4 \cdot 3! = 24$