08/11/2018

Δείξαμε: Αν a περιττός, τότε ο a^2 είναι της μορφής $8q+1$, δηλ. το υπόλοιπο της διαίρεσης του a με το 8 είναι 1.

Εφαρμογή:

Ο αριθμός $8\cdot 525+3$ δεν είναι τετράγωνο ακεραίου. Το ίδιο ισχύει αν αντικαταστήσαμε το 525 με οποιοδήποτε ακέραιο. και το 3 με 5 ή 7.

Εφαρμογή: Αν $a, b \in \mathbb{Z}$ περιττοί, τότε $8 \mid a^2-b^2$.

Απόδειξη: Αφού a περιττός, έχουμε ότι υπάρχει $k_1 \in \mathbb{Z}$ με $a^2 = 8k_1+1$. Ομοίως, υπάρχει $k_2 \in \mathbb{Z}$ με $b^2 = 8k_2+1$. Συνεπώς $a^2-b^2 = (8k_1+1) - (8k_2+1) = 8(k_1-k_2)$. Άρα $8 \mid a^2-b^2$.

(Παράδειγμα. αν $a=5$, $b=3$, $a^2-b^2 = 25-9 = 16 = 2\cdot 8$).

Πρόταση: Έστω $n \in \mathbb{Z}$. Τότε $4 \nmid n^2+2$

δεν διαιρεί.

Απόδειξη: Υποθέτουμε $n \in \mathbb{Z}$ και $4 \mid n^2+2$ και θα βρούμε αντίφαση

- Περίπτωση-1: n περιττός, τότε n^2 περιττός και άρα n^2+2 περιττός, άρα $2 \nmid n^2+2$ άρα $4 \nmid n^2+2$ αντίφαση
- Περίπτωση-2: n άρτιος, τότε υπάρχει $k \in \mathbb{Z}$ με $n=2k$

Συνεπώς, $n^2 = 4k^2 \Rightarrow n^2+2 = 4k^2+2$

Άρα το υπόλοιπο της ευκλ. διαίρεσης του n^2+2 με το 4 είναι 2 και όχι 0. Αλλά υποθέσαμε $4 \mid n^2+2$ άρα αντίφαση.

→ ΚΡΙΤΗΡΙΑ ΔΙΑΙΡΕΤΟΤΗΤΑΣ (με 2, 5, 10, 3, ...)

ΠΡΟΤΑΣΗ: Για κάθε $n \geq 1$, έχουμε $3 \mid 10^n - 1$

ΑΠΟΔΕΙΞΗ: Επαγωγή στο n.

ΒΗΜΑ - 1ο: Για $n = 1$ ισχύει, γιατί $3 \mid 10 - 1 = 9$

ΒΗΜΑ - 2ο: Υποθέτουμε $n \geq 1$ και ότι $3 \mid 10^n - 1$

ΝΔΟ $3 \mid 10^{n+1} - 1$.

Πράγματι, $10^{n+1} - 1 = 10 \cdot 10^n - 1 = (9+1) \cdot 10^n - 1 =$

$= 9 \cdot 10^n + (10^n - 1)$

Φανερά $3 \mid 9 \cdot 10^n$ (γιατί $3 \mid 9$) και από υπόθεση επαγωγής

$3 \mid 10^n - 1$. Άρα $3 \mid 9 \cdot 10^n + (10^n - 1) = 10^{n+1} - 1$.

↳ Διαιρεί.

ΥΠΕΝΘΥΜΙΣΗ: Έστω $a_0, \ldots a_r \in \{0, 1, \ldots, 9\}$ Τότε

ορίζουμε $(a_r, a_{r-1}, \ldots a_0)_{10} = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \ldots + a_1 \cdot 10 + a_0$

ΠΑΡΑΔΕΙΓΜΑ: $(\underset{a_3}{0}, \underset{a_2}{5}, \underset{a_1}{0}, \underset{a_0}{7})_{10} = 0 \cdot 10^3 + 5 \cdot 10^2 + 0 \cdot 10 + 7 = 507$

ΠΡΟΤΑΣΗ: Έστω $k \in \mathbb{N}$ με $k = (a_r, a_{r-1}, a_{r-2}, \ldots a_1, a_0)_{10}$

όπου $0 \leq a_i \leq 9$ $\forall i$.

Τότε (1) $2 \mid k$ αν και μόνο αν $a_0 \in \{0, 2, 4, 6, 8\}$

(2) $5 \mid k$ " " " " $a_0 \in \{0, 5\}$

(3) $10 \mid k$ " " " " $a_0 = 0$

(4) $3 \mid k$ " " " " $3 \mid (a_0 + a_1 + \ldots + a_r)$

ΑΠΟΔΕΙΞΗ: (4)

$k = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots + a_r \cdot 10^r$

Θα κάνουμε χρήση του $3 \mid 10^n - 1^{(*)}$ $\forall n \geq 1$. Γράφουμε $k = a_0 + a_1 \cdot 10 - a_1 + a_1 + a_2 \cdot 10^2 - a_2 + a_2 + \dots + a_r \cdot 10^r - a_r + a_r =$
$= (a_0 + a_1 + \dots a_r) + (10^1 - 1)a_1 + (10^2 - 1)a_2 + \dots (10^r - 1)a_r$

Από (*) έχουμε ότι υπάρχει $m \in \mathbb{Z}$ ώστε

$(10^1 - 1)a_1 + \dots + (10^r - 1)a_r = 3 \cdot m$

Άρα $k = 3m + (a_0 + \dots + a_r)$ και άρα το υπόλοιπο της διαίρεσης του k με το 3 είναι το ίδιο με το υπόλοιπο της διαίρεσης του $(a_0 + \dots + a_r)$ με το 3. Το αποτέλεσμα έπεται.

ΠΑΡΑΔΕΙΓΜΑ. Διαιρεί το 3 το 2018;

ΑΠΑΝΤΗΣΗ: $2018 = (\underset{a_3}{2}\underset{a_2}{0}\underset{a_1}{1}\underset{a_0}{8})_{10}$ και $a_0 + a_1 + a_2 + a_3 = 11$

Αφού $3 \nmid 11$, από την πρόταση $3 \nmid 2018$.

ΑΣΚΗΣΗ.

(a) Δείξτε ότι αν $n \geq 1$ περιττός τότε $11 \mid 10^n + 1$

(b) Δείξτε ότι αν $n \geq 1$ άρτιος $11 \mid 10^n - 1$

(c) Έστω $k \in \mathbb{Z}$ με $k = (a_r, a_{r-1}, \dots, a_1, a_0)_k$.
Τότε $11 \mid k$ αν και μόνο αν $11 \mid (a_r - a_{r-1} + a_{r-2} - a_{r-3} + \dots)$

ΠΑΡΑΔΕΙΓΜΑ-1: Διαιρεί το 11 το 2018;

ΛΥΣΗ: $2018 = (\underset{a_3}{2}\ \underset{a_2}{0}\ \underset{a_1}{1}\underset{a_0}{8})_{10}$

Έχουμε $a_3 - a_2 + a_1 - a_0 = 2 - 0 + 1 - 8 = -5$

Αφού 11 δεν διαιρεί το -5, έχουμε από την άσκηση
$11 \nmid 2018$

(b) Διαιρεί το 11 το 7018;
Ναι, γιατί $7018 = (7\ 0\ 1\ 8)_{10}$ και $7 - 0 + 1 - 8 = 0$
και $11 \mid 0$.

ΟΡΙΣΜΟΣ: Έστω $a \in \mathbb{Z}$. Ο a λέγεται ΣΥΝΘΕΤΟΣ αν $a \geq 2$ και a όχι πρώτος.

ΠΑΡΑΔΕΙΓΜΑ: Οι αριθμοί 4, 6, 8, 9, 10 είναι σύνθετοι.

ΠΡΟΤΑΣΗ: Έστω $a \in \mathbb{Z}$ με $a \geq 2$. Τότε ο a είναι σύνθετος αν και μόνο αν υπάρχουν ακέραιοι k_1, k_2 με $2 \leq k_1$, $2 \leq k_2$, ώστε $a = k_1 k_2$.

ΑΠΟΔΕΙΞΗ: Άμεσον από τους ορισμούς.

ΟΡΙΣΜΟΣ: Έστω $a \in \mathbb{Z}$. Οι πρώτοι διαιρέτες του a είναι οι πρώτοι p με $p \mid a$.

ΠΑΡΑΔΕΙΓΜΑ: Οι πρώτοι διαιρέτες του 25 είναι μόνο το 5.
Οι πρώτοι διαιρέτες του 12 είναι τα 2, 3.

ΠΡΟΤΑΣΗ: Έστω $a \geq 2$ και S το σύνολο των ακεραίων $d \geq 2$ που διαιρούν το a. Τότε:
(1) $S \neq \emptyset$
(2) Το ελάχιστο στοιχείο του S είναι πρώτος.

ΑΠΟΔΕΙΞΗ:

(1) Αφού $\alpha \in S$, $S \neq \emptyset$.

(2) Από θεώρημα, το S έχει ελάχιστο στοιχείο, έστω $d_0 \in S$.

Ισχυρισμός: d_0 πρώτος.

ΑΠΟΔΕΙΞΗ: Έστω ότι δεν είναι πρώτος. Τότε είναι σύνθετος.
Άρα υπάρχουν k_1, k_2 με $2 \leq k_1$, $2 \leq k_2$ ώστε $d_0 = k_1 k_2$ $(*)$
Αφού $2 \leq k_1$, $2 \leq k_2$, και $d_0 = k_1 k_2 \Rightarrow k_1 \leq d_0 - 1$
Επομένως, $(*) \Rightarrow k_1 \in S$, και $k_1 < d_0$, αντίφαση.

ΠΟΡΙΣΜΑ: Έστω $\alpha \in \mathbb{Z}$ με $\alpha \geq 2$. Τότε ο α έχει έναν πρώτο διαιρέτη.

ΘΕΩΡΗΜΑ: (Ευκλείδης) Το πλήθος των πρώτων είναι άπειρο.

ΑΠΟΔΕΙΞΗ: Υποθέτουμε ότι το σύνολο των πρώτων είναι πεπερασμένο, και θα καταλήξουμε σε αντίφαση. Έστω $p_1, p_2, \ldots p_s$ όλοι οι πρώτοι.
Θέτουμε $\alpha = p_1 p_2 \ldots p_s + 1 \in \mathbb{Z}$ με $\alpha \geq 2$.

Από το πόρισμα, ο α έχει πρώτο διαιρέτη. Άρα αφού κάθε πρώτος είναι ένας από τους $p_1, \ldots, p_s$ υπάρχει i με $1 \leq i \leq s$ ώστε $p_i \mid \alpha$. Αλλά, από τον ορισμό του α, το υπόλοιπο της Ευκλ. διαίρεσης του α με το p_i είναι 1. Άρα $p_i \nmid \alpha$, αντίφαση.

ΠΑΡΑΤΗΡΗΣΗ: Το θεώρημα μας λέει ότι αν $k \in \mathbb{Z}$ με $k \geq 1$, υπάρχει πρώτος p με $k < p$.

ΕΡΩΤΗΜΑ: Υπάρχουν μεγάλα διαστήματα ακεραίων χωρίς πρώτους;

ΑΠΑΝΤΗΣΗ: Ναι, λόγω της πρότασης.

→ ΠΡΟΤΑΣΗ: Έστω $n \geq 2$. Τότε οι n διαδοχικοί ακέραιοι $(n+1)!+2$, $(n+1)!+3$, ..., $(n+1)!+(n+1)$ είναι σύνθετοι.

ΥΠΕΝΘΥΜΙΣΗ: Έστω $k \geq 1$. Τότε $k! = 1 \cdot 2 \cdot 3 \cdots n$.

ΠΑΡΑΔΕΙΓΜΑ: $1! = 1$, $2! = 1 \cdot 2 = 2$, $3! = 1 \cdot 2 \cdot 3 = 6$, $4! = 24$, $5! = 120$.

ΑΠΟΔΕΙΞΗ ΠΡΟΤΑΣΗΣ: Φανερά για $2 \leq a \leq n+1$ ισχύει ότι $a \mid (n+1)!$. Άρα $a \mid (n+1)! + a$.
Αφού $n \geq 2 \Rightarrow a < (n+1)! + a$. Συνεπώς, ο $(n+1)! + a$ έχει διαιρέτη το a, και $2 \leq a < (n+1)! + a$.
Άρα, ο $(n+1)! + a$ είναι σύνθετος.

ΟΡΙΣΜΟΣ: Έστω $x \in \mathbb{R}$. Ορίζουμε $\pi(x)$ = ο αριθμός των πρώτων p με $p \leq x$.

ΠΑΡΑΔΕΙΓΜΑΤΑ:
Αν $x \leq 1$, $\pi(x) = 0$
Αν $x = 8$, $\pi(x) = 4$ γιατί οι πρώτοι μικρότεροι ή ίσοι του 8 είναι οι $2, 3, 5, 7$.

ΘΕΩΡΗΜΑ: [Πρώτων Αριθμών, Hadamard - de la Vallée Poussin, 1896]

$$\lim_{x \to +\infty} \frac{\pi(x)}{\left(\frac{x}{\ln x}\right)} = 1$$

Δηλαδή, για x αρκετά μεγάλο, ο αριθμός $\pi(x)$ που μετράει τον αριθμό των πρώτων $\leq x$ είναι περίπου $\frac{x}{\ln x}$