

ΕΠΑΝΑΛΗΨΗ

1) ΝΑ ΔΟ $9 \mid 10^n + 3 \cdot 4^{n+2} + 5, n \geq 1$

ΛΥΣΗ

ΘΑ ΔΟ $9 \mid 15 + 3 \cdot 4^n = 3 \cdot (5 + 4^n) \Rightarrow 3 \mid 5 + 4^n \Rightarrow 3 \mid 3 + 2 + 4^n \Rightarrow$

$\Rightarrow 3 \mid 2 + (3+1)^n \Rightarrow 3 \mid \underbrace{2+1^3}_{3} + 3 \cdot 1 + 3 \cdot 3^2 \cdot 1 + 3 \quad \text{ΛΟΧΥΕΙ!}$

Μ και μέσω μαθηματικής επαγωγής.

Για $n=1$ η πρόταση είναι αληθής

Έστω ότι για $n=k$ η πρόταση είναι αληθής και ΘΑ ΔΟ
για $n=k+1$ η πρόταση αληθής.

Λοχύνει δηλαδή ότι

$9 \mid 10^k + 3 \cdot 4^{k+2} + 5$ και ΘΑ ΔΟ $9 \mid 10^{k+1} + 3 \cdot 4^{k+3} + 5, \forall k \geq 1$

Έχουμε $9 \mid \alpha \Rightarrow 9 \mid \beta$

$9 \mid \alpha$ και $9 \mid \beta - \alpha \Rightarrow 9 \mid \beta - \alpha + \alpha$

$10^{k+1} + 3 \cdot 4^{k+3} + 5 - (10^k + 3 \cdot 4^{k+2} + 5) =$

$= 10^k(10-1) + 3 \cdot 4^{k+2}(4-1) = 9 \cdot 10^k + 3 \cdot 4^{k+2} \cdot 3 = \text{πολ} 9$

ΠΑΡΑΤΗΡΗΣΗ:

$$\alpha^n + \beta^n = \begin{cases} \rightarrow \text{Αν } n=2^k \text{ τότε δεν μπορεί να αναλυθεί άλλο} \\ \rightarrow \text{Αν } n=2^{k+1} \text{ τότε} \\ \alpha^{2^{k+1}} + \beta^{2^{k+1}} = (\alpha + \beta) \cdot (\alpha^{2^k} - \alpha^{2^{k-1}}\beta + \dots + \beta^{2^k}) \\ \rightarrow \text{Αν } n=2^m(2k+1) \text{ τότε} \\ \alpha^{2^m(2k+1)} + \beta^{2^m(2k+1)} = (\alpha^{2^m} + \beta^{2^m}) (\alpha^{2^m 2^k} - \alpha^{2^m 2^{k-1}}\beta^{2^m} + \dots + \beta^{2^m 2^k}) \end{cases}$$

- Αν 2^{k+1} πρώτος $\Rightarrow$ k είναι δύναμη του 2
- Αν $2^k - 1$ πρώτος $\Rightarrow$ k πρώτος

Αλγόριθμος του ΕΥΚΛΕΙΔΗ

$$(a, b) = \gamma \Leftrightarrow \exists x, y \in \mathbb{Z} : ax + by = \gamma$$

ΠΡΟΤΟΓΕΝΗΣ ΑΝΑΛΥΣΗ:

$\forall n \in \mathbb{N} \quad \exists!$ πρώτοι $p_1, p_2, \dots, p_r$ διακεκριμένοι φυσικοί
 $k_1, k_2, \dots, k_r$ $\mu \text{ t } n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_r^{k_r}$

$$2) \text{ Εαν } (a, b) = 1 \text{ τότε vds } (2a+b, a+2b) = 1 \text{ ή } 3$$

Λύση

$$\begin{aligned} (2a+b, a+2b) &= (2a+b - (a+2b), a+2b) = \\ &= (a-b, a+2b) = (a-b, 2(a-b) + (a+2b)) = \\ &= (a-b, 3a) \end{aligned}$$

$$\begin{aligned} \text{Εξετάζουμε εαν } 3 \nmid a-b &\Rightarrow (a-b, 3a) = (a-b, a) = \\ &= (a-b-a, a) = (b, a) = 1 \end{aligned}$$

$$\left(\begin{array}{l} \text{ή εξετάζουμε εαν } 3 \mid a-b \Rightarrow \left\{ \begin{array}{l} 3 \mid a-b \Rightarrow 3 \mid b \\ 3 \mid a \end{array} \right. \\ \text{αλλά } (a, b) = 1 \quad \text{Αδύνατον} \end{array} \right)$$

3) - NAO $x, y, z \in \mathbb{Z}$ ώστε

$$112x + 96y + 24z = 8 \quad (112, 96, 24) = (2^4 \cdot 7, 2^5 \cdot 3, 2^3 \cdot 3) = 2^3 = 8$$

Wett

Εφόσον $(112, 96, 24) = 8/8$ τότε έχει λύση

$$14x + 12y + 3z = 1$$

As παρούμε

$$14x + 3z = 1 \cdot w, \quad (14, 3) = 1 \quad \text{όπου} \quad 1 \cdot w + 12 \cdot y = 1$$

με προφανή λύση των $(w_0, y_0) = (13, -1)$

(η μέση του Ευκλείδειου αλγορίθμου)

$$\text{Αρα} \quad w = w_0 + 12t = 13 + 12t \quad | \quad t \in \mathbb{Z}$$

$$y = y_0 - 1 \cdot t = -1 - t$$

$$\text{Τότε,} \quad 14x + 3z = 1 \xrightarrow{\text{Ευκλείδης}} (x_0, z_0) = (-1, 5)$$

$$\text{Τότε} \quad \left. \begin{array}{l} x = -1 + 3 \cdot s \quad \text{και} \quad z = 5 - 14 \cdot s \\ \text{Αλλά} \quad 14x + 3z = w \\ w + 12y = 1 \end{array} \right\} \begin{array}{l} x = (-1 + 3 \cdot s)w = (-1 + 3 \cdot s)(13 + 12t) \\ \text{και} \\ z = (5 - 14 \cdot s)w = (5 - 14 \cdot s)(13 + 12t) \\ \text{και} \end{array}$$

$$14x + 3z = w$$

$$w + 12y = 1$$

$$y = -1 - t, \quad t, s \in \mathbb{Z}$$

α) Να χαρακτηρίσετε πως συνεπικέρονται τα σωστά

$\mathbb{Z}_p$: πρώτος και $\mathbb{Z}_{n \neq p}$: πρώτος

β) Να χαρακτηρίσετε τη σύμβαση του Euler $\varphi(n)$ πολλαπλασιαστική

$$[a]_1^{\varphi(n)} = [1]_n \Leftrightarrow a^{\varphi(n)} \equiv 1 \pmod{n} \quad (a, n) = 1 \quad \text{Euler}$$

γ) Να χαρακτηρίσετε τις πρωταρχικές ρίζες $\text{ord}_n(a) = k$ ώστε

ο k να είναι ο μικρότερος ώστε $a^k \equiv 1 \pmod{n}$

όταν $\text{ord}_p(a) = \varphi(p) = p-1 \leftarrow$ πρωταρχική ρίζα

$$\mathbb{Z}_p^* = \{ [a^0]_p, [a^1]_p, [a^2]_p, \dots, [a^{\varphi(n)-1}]_p \}$$

5) να συμπληρώσουμε να βρισκόμαστε την τάξη $\text{ord}_n(a)$ όπου $(a, n) = 1$. Θα εφαρμόζουμε το θεώρημα, $\text{ord}_n(a) \mid \varphi(n)$ και αφού βρούμε τους διαλύτες θα τους δοκιμάσουμε.

4) ΝΑΟ $2^{3^n} \equiv 1 \pmod{7}$

ΜΕΤ

$$2^{\varphi(7)} = 2^6 \equiv 1 \pmod{7}$$

Αρα, $\text{ord}_7(2) = 1, 2, 3, 2 \cdot 3$

Με δοκιμές, $2^3 \equiv 8 \pmod{7} \equiv 1 \pmod{7}$

Αρα, $\text{ord}_7(2) = 3$.

Ετσι, $2^{3^n} = (2^3)^n \equiv 1 \pmod{7}$

5) $(a, 2) = 1 \quad \forall \delta \quad a^{2^n} \equiv 1 \pmod{2^{n+2}}$

ΜΕΤ

$$\varphi(2^{n+2}) = 2^{n+1} (2-1) = 2^n \cdot 2$$

$$(a^{2^n})^2 = a^{2^{n+2}} \equiv 1 \pmod{2^{n+2}} \leadsto$$

$$\swarrow \quad a^{2^n} \equiv 1 \pmod{2^{n+2}}$$

$$\searrow \quad a^{2^n} \equiv -1 \pmod{2^{n+2}} \equiv (2^{n+2} - 1) \pmod{2^{n+2}}$$

Με επαγωγή στο n

$$a^2 \equiv 1 \pmod{2^3} \equiv 1 \pmod{8}$$

$$(a, 2) = 1 \Leftrightarrow a = 2k+1$$

$$a = (1) \dot{\vee} (3) \dot{\vee} (5) \dot{\vee} (7)$$

$$3^2 \equiv 1 \pmod{8}$$

$$7^2 \equiv 1 \pmod{8}$$

Υποθέτουμε ότι ισχύει για n και το δείχνουμε για $n+1$

6) Να βρείτε τα $n \in \mathbb{N}$ εάν $\varphi(n) = 12$

η ασκηση αυτή έχει γίνει στα φύλλα