18/11/2016

Ασκηση 1 φυλ #2

Εστω p = πρώτος και $k \in \mathbb{N}^*$

Νδ οι διαιρέτες του p^k και το πλήθος τους

$p^\lambda / p^k \Leftrightarrow \lambda \leq k$, $\lambda \in \mathbb{N}$

Εστω $q \neq p$: q / p^k

από γνωστή πρόταση πρέπει

$q/p \Rightarrow q = p$ ή $q = 1$ άτοπο

$$\underbrace{1/p^k, p/p^k, \ldots, p^k/p^k}_{\text{πλήθος } k+1}$$

Άσκηση 2 #2 $\sigma(n) = \sigma(p_1^{k_1})(p_2^{k_2}) \cdot p_1^{k_1}$ $\sigma(12) \neq \sigma(2)\cdot\sigma(6)$

$\sigma(12) = \sigma(3)\cdot\sigma(4)$

α) $\sigma: \mathbb{N}^* \to \mathbb{N}^*$

$\sigma(2) = 1+2=3$

$\sigma(3) = 1+3=4$

$\sigma(6) = 1+2+3+6=12$

$\sigma(4) = 1+2+4=7$

$\sigma(12) = 1+2+3+4+6+12=28$

$(a,b)=1$

β) Νδο: $\sigma(p^k) = \frac{1-p^{k+1}}{1-p}$, p πρώτος $k\in\mathbb{N}^*$

1º Επαγ. βήμα:

για $k=1$: $\sigma(p) = \frac{1-p^2}{1-p} = \frac{(1-p)(1+p)}{1-p} = 1+p$ ισχύει

Γενικό Επαγ. βήμα: Υποθέτουμε ότι ισχύει $\sigma(p^k)$ αληθής και Θδο $\sigma(p^{k+1})$ αληθής

$$\sigma(p^{k+1}) = \frac{1-p^{k+2}}{1-p} = \frac{1-p^{k+1}+p^{k+1}-p^{k+2}}{1-p} = \frac{1-p^{k+1}}{1-p}$$

ή $\sigma(p^k) = (1+p+\dots+p^k)\frac{(1-p)}{1-p} = \frac{1^{k+1}-p^{k+1}}{1-p}$

π.χ. $\sigma(2^2) = \frac{1-2^3}{1-2} = \frac{2^3-1}{2-1} = 7$

Άσκηση 3 #2

$p_1=2$, $p_2=3$

Ευκλείδης: Υπο{θ}δ ότι είναι πεπερασμένοι $p_1 \dots p_k$

$p_1 \dots p_k + 1$ ~~πρώτος~~

$2\cdot3\cdot5 \dots 17+1 = 59\,509$ //

Υπάρχουν άπειροι πρώτοι της μορφής $4k+1$

Υποθέτουμε ότι είναι πεπερασμένοι

$4k_1+1, 4k_2+1, \dots, 4k_l+1$

Υπάρχουν άπειροι μορφής $4m+3$

$B = \underbrace{(4k_1+1)(4k_2+1) \dots (4k_l+1)}_{\text{φυσικός}} + 3 =$ $\boxed{\text{γινόμενο πρώτων}}$ από θ.μ. παρ.

$= (4k+1)\underbrace{q_1 \dots q_n}_{\text{άλλοι πρώτοι}} = A$

κάποιος.

$$\left.\begin{array}{l}(4k_i+1)/A \\ (4k_i+1)/B \\ 4(k_i+1)(4k_i+1)\ldots(4k\ell+1)\end{array}\right\} \Rightarrow \begin{array}{l} 4k_i+1/B-(4k_1+1)(4k_2+1)\ldots(4k_\ell+1) \\ 4k_i+1/3 \text{ αδύνατο}\end{array}$$

Άρα $B=q_1 \ldots q_n$ και $q_i=(4m_i+3)$

$(4k_1+1)\ldots(4k_\ell+1)=4(\Gamma)+1$

- $(4k_1+1)(4k_2+1)=4\cdot 4k_1k_2+4k_1+4k_2+1$

$(4m_1+3)(4m_2+3)\ldots(4m_n+3)=4\cdot\Delta+3^n$

$B=4\Gamma+1+3=A=4\Delta+3^n$

$\underbrace{4(\Gamma+1)}_{4}=\underbrace{4\Delta}_{4}+3^n \Rightarrow \underbrace{4}_{2^2}/3^n$ αδύνατο

Άσκηση 4 #2

a) Αν για (a,b,c) ισχύει $a^2+b^2=c^2$

Τότε ισχύει και για $(d a, d b, d c)$

Έστω $a'=d\cdot a$, $b'=d\cdot b$, $c'=d\cdot c$

Επομένως $a'^2+b'^2=c'^2 \Rightarrow (d\cdot a)^2+(db)^2=(dc)^2 \Rightarrow$

$\Rightarrow d^2a^2+d^2b^2=d^2c^2$

$\Rightarrow d^2(a^2+b^2)=d^2c^2$

$\Rightarrow a^2+b^2=c^2$ που ισχύει

b) Αν $a^2+b^2=c^2$ τότε a,b όχι περιττοί ή οι δυο

Έστω a,b περιττοί, άρα $a=2k+1$, $b=2\ell+1$

- $a^2=(2k+1)^2=4k^2+4k+1$
- $b^2=(2\ell+1)^2=4\ell^2+4\ell+1$

Έχουμε $4k^2+4k+1+4\ell^2+4\ell+1=c^2 \Rightarrow \underbrace{2(\overbrace{2k^2+2k+2\ell^2+2\ell+1}^{A})}_{\text{άρτιος}}=\underbrace{c^2}_{\text{άρτιος}}$

$$\left.\begin{array}{l} c=2m \\ c^2=\underbrace{4m^2}_{\text{άρτιος}}=2\cdot\underbrace{(A)}_{\text{περιττός}}\end{array}\right\} \Rightarrow \text{άρα άτοπο.}$$

γ) Αν $a^2+b^2=c^2$, $(a,b,c)=1$ και a άρτιος και b,c περιττοί

Τότε $(c-b)$, $(c+b)$ άρτιοι

$a=2k$

$b=2\ell+1$ $\quad c-b=2m+1-(2\ell+1)=2(m-\ell)$

$c=2m+1$ $\quad c+b=2m+1+2\ell+1=2(m+\ell+1)$ $\Big\}$ άρτιοι

$$\frac{c-b}{2}\cdot\frac{c+b}{2}=\frac{c^2-b^2}{4}=\frac{a^2}{4}=\left(\frac{a}{2}\right)^2$$

δ) $\left(\frac{c-b}{2},\frac{c+b}{2}\right)=1$ Ξέρουμε $(a,b,c)=1$

Υποθέτουμε ότι $\delta>1$

τότε $\delta/\frac{c-b}{2}$ και $\delta/\frac{c+b}{2}$

Άρα, $\delta/\left(\frac{c-b}{2}+\frac{c+b}{2}\right)=c \Rightarrow \delta/c$

$\delta/\left(\frac{c+b}{2}-\frac{c-b}{2}\right)=b \Rightarrow \delta/b$

$\left.\begin{matrix}\delta/c^2\\ \delta/b^2\end{matrix}\right\} \Longrightarrow$ άρα δ/a^2 $\exists$ πρώτος p/δ τ.ώ. p/a

$a^2+b^2=c^2$

δηλ. $p/(a,b,c)=1$ άτοπο

$$\left(\frac{a}{2}\right)^2=\frac{c-b}{2}\cdot\frac{c+b}{2}$$

$a=2k \Rightarrow \frac{a}{2}=k \Rightarrow \left(\frac{a}{2}\right)^2=k^2$ ~~άρα~~

άρα $\frac{a}{2}=p_1\cdot p_2\cdots p_k \Rightarrow \left(\frac{a}{2}\right)^2=p_1^2 p_2^2\cdots p_m^2=\frac{c-b}{2}\cdot\frac{c+b}{2}$

πρέπει $p_i^2/\frac{c-b}{2}$ ή $p_i^2/\frac{c+b}{2}$, $1\le i\le m$

δεν γίνεται $p_i/\frac{c-b}{2}$ και $p_i/\frac{c+b}{2}$

άρα $\frac{c-b}{2}$, $\frac{c+b}{2}$ θα είναι γινόμενο τετραγώνων πρώτων

ΙΔΙΟΤΗΤΕΣ ΣΤΑ modula

ΠΡΟΤΑΣΗ: Αν $m_1, \dots, m_k$ είναι φυσικοί >1 και $\boxed{[m_1, \dots, m_k] = m_1 \cdots m_k}$

Τότε $a \equiv b \bmod m_1 \cdots m_k \Leftrightarrow$

$\Leftrightarrow a \equiv b \bmod m_i$ για $i = 1, \dots, k$

Αποδ: $[m_1, \dots, m_k] = m_1 \cdot m_2 \cdots m_k$

$\Leftrightarrow \boxed{(m_i, m_j) = 1 \quad i \neq j}$

$a \equiv b \bmod (m_1 m_2 \cdots m_k) \Leftrightarrow a - b = \ell \, m_1 m_2 \cdots m_k \Rightarrow$

$\left.\begin{array}{l} m_i / m_1 m_2 \cdots m_k \\ m_i \not| \, m_j \quad i \neq j \end{array}\right\} \Rightarrow m_i / a-b \Leftrightarrow a \equiv b \bmod m_i$

πχ. $60 \equiv 12 \bmod 24 \Leftrightarrow$ $60 \equiv 12 \bmod 3$

$24 = 3 \cdot 8 = \underbrace{4 \cdot 6}_{\text{όχι πρώτοι μεταξύ τους}}$ $60 \equiv 12 \bmod 8 \equiv 4 \bmod 8$

$60 \equiv 12 \bmod 4$

$60 \equiv 12 \bmod 6$.

ΕΡΩΤΗΜΑ: $3x = 7 \Rightarrow 3^{-1} \cdot 3 = 3^{-1} \cdot 7$

στο $\mathbb{R}$, $\mathbb{Q}$ λύνεται στο $\mathbb{Z}$ όχι

πχ. $3x \equiv 2 \bmod 6$ ①

για $x =$ 0: όχι

1: όχι

2: όχι

3: όχι

4: όχι

5: όχι $\rightarrow$ άρα η ① δεν λύνεται

Γιατί δεν λύνεται;

Γιατί ΔΕΝ λύνεται;

Ζητάμε την αντίστροφη κλάση του 3
Δηλαδή θέλουμε $[a]_6\cdot[3]_6=[1]_6$
$[3a]=[1]_6 \Leftrightarrow 3a-1=6k$
$3|3a$ $\quad 3|a \Rightarrow 3|1$ αδύνατο

ΠΡΟΤΑΣΗ: Μια κλάση $[a]_m$ στο modulo m έχει αντίστροφη κλάση ή αντιστρέφεται αν $(a,m)=1$
Τότε υπάρχει $[b]_m$ με $[a]_m\cdot[b]_m=[1]_m$

Πότε ισχύει ο νόμος της Διαγραφής;
$a(x-y)=0$
$ax=ay$ με $a\neq 0 \Leftrightarrow x=y$
ισχύει $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R}$

Γνωρίζουμε ότι $\underset{2}{3x}=\underset{4}{3y} \mod 6$
όχι, γιατί ο 3 είναι μηδενοδιαιρέτης
$3\cdot 2\equiv 0 \mod 6$

ΘΕΩΡΗΜΑ: Έστω $m>1$ φυσικός και $a,b\in\mathbb{Z}$ με $(a,m)=1$
Αν $a\cdot b\equiv 0 \mod m \Rightarrow b\equiv \mod m$

Αποδ: $(a,m)=1 \Leftrightarrow \exists a^{-1} \mod m$
Έστω $a^{-1}=b \mod m \Leftrightarrow a\cdot b\equiv 1 \mod m$
$a\cdot b\equiv 0 \mod m \Rightarrow b\cdot a\cdot b\equiv b\cdot 0 \mod m \Rightarrow$
$\Rightarrow 1\cdot b\equiv 0 \mod m \Rightarrow b\equiv 0 \mod m$

ΠΡΟΤΑΣΗ: Έστω $m>1$, $a,b\in\mathbb{Z}^*$
Αν $a\cdot b\equiv 0 \mod m$, τότε $b\equiv 0 \mod\left(\frac{m}{(a,m)}\right)$

Αποδ. $ab = km \Rightarrow \frac{a}{(a,m)} \cdot b = k \cdot \frac{m}{(a,m)}$

Τώρα $\left(\frac{a}{(a,m)}, \frac{m}{(a,m)}\right) = 1$

Είναι πρώτοι $\Rightarrow$ άρα έχουν αντίστροφο

Έχουμε $\frac{a}{(a,m)} \cdot b = k \cdot \frac{m}{(a,m)} \Leftrightarrow \frac{a}{(a,m)} \cdot b \equiv 0 \bmod \frac{m}{(a,m)}$

$\left(\frac{a}{(a,m)}, \frac{m}{(a,m)}\right) = 1 \Leftrightarrow \exists \left[\frac{a}{(a,m)}\right]^{-1}_{\frac{m}{(a,m)}}$

Με το προηγούμενο $b \equiv 0 \bmod \left(\frac{m}{(a,m)}\right)$