Θέματα Άλγεβρας, Αριθμητική Γεωμετρία

Λύσεις ασκήσεων Φυλλαδίου 1

Γιάννης Α. Αντωνιάδης

Άσκηση 1:

Έστω ότι η εξίσωση $x^2+py^3+p^2z^3=0$ είχε μία ακέραια λύση (x_0,y_0,z_0).
Τότε χ.β.τ.γ. $\text{ΜΚΔ}(x_0,y_0,z_0)=1$ διότι αν $\text{ΜΚΔ}(x_0,y_0,z_0)=f$ τότε
$x_0=fx_0',\ y_0=fy_0',\ z_0=fz_0'$ και
$f^3x_0'^3+pf^3y_0'^3+p^2f^3z_0'^3=0 \ \Rightarrow\ x_0'^3+py_0'^3+p^2z_0'^3=0$ η (x_0',y_0',z_0') θα ήταν μια λύση με $\text{ΜΚΔ}(x_0',y_0',z_0')=1$.
$x_0^3=-py_0^3-p^2z_0^3$ οπότε (αφού $p|-py_0^3-p^2z_0^3$) τότε $p|x_0^3$ και αφού p πρώτος τότε $p|x_0$.
Έστω $x_0=px_1$ τότε $(px_1)^3+py_0^3+p^2z_0^3=0 \ \Rightarrow\ p^2x_1^3+y_0^3+pz_0^3=0$
$\Rightarrow\ y_0^3+pz_0^3+p^2x_1^3=0$ άρα η (y_0,z_0,x_1) είναι επίσης λύση της αρχικής.
Όμως με παρόμοιο επιχείρημα $p|y_0$ και έστω $y_0=py_1$.
$(py_1)^3+pz_0^3+p^2x_1^3=0 \ \Rightarrow\ p^2y_1^2+z_0^3+px_1^3=0 \ \Rightarrow\ z_0^3+px_1^3+p^2y_1^3=0$
άρα η (z_0,x_1,y_1) λύση της αρχικής.
Πάλι θα έχω $p|z_0$.
Όμως τώρα κατέληξα ότι $p|x_0$ και $p|y_0$ και $p|z_0$ άρα $p|\text{ΜΚΔ}(x_0,y_0,z_0)=1$
άτοπο άρα η εξίσωση δεν έχει ακέραιες λύσεις.

Άσκηση 2:

Η εξίσωση έχει προφανείς λύσεις, για $xyz=0$. Έστω τώρα (x,y,z) μία μη τετριμμένη λύση της $x^2+y^2=z^2$. Μπορούμε να υποθέσουμε ότι
$\text{ΜΚΔ}(x,y,z)=1$ διότι αν $\text{ΜΚΔ}(x,y,z)=d>1$ τότε
$x=dx_1,\ y=dy_1,\ z=dz_1$ και $d^2x_1^2+d^2y_1^2=d^2z_1^2 \ \Rightarrow\ x_1^2+y_1^2=z_1^2$ άρα
(x_1,y_1,z_1) λύση με $\text{ΜΚΔ}(x_1,y_1,z_1)=1$.
Στη συγκεκριμένη περίπτωση, η υπόθεση ότι
$\text{ΜΚΔ}(x,y,z)=1 \ \Rightarrow\ \text{ΜΚΔ}(x,y)=\text{ΜΚΔ}(y,z)=\text{ΜΚΔ}(z,x)=1.$
Όντως αν υποθέταμε ότι $\text{ΜΚΔ}(x,y)=d>1$ και p πρώτος που διαιρεί το d τότε $p|x^2$ και $p|y^2$ και $p|z^2$ οπότε και $p|z$, άρα θα έχουμε $p|\text{ΜΚΔ}(x,y,z)=1$ άτοπο.
Επίσης αν υποθέσουμε ότι $\text{ΜΚΔ}(x,z)=d>1$ και p πρώτος που διαιρεί το d τότε $p|x^2$ και $p|y^2$ και $p|z^2 \ \Rightarrow\ p|z$, και τελικά $p|\text{ΜΚΔ}(x,y,z)=1$ άτοπο.

Ένας από τα x, y θα είναι περιττός και ο άλλος άρτιος, διότι αν ήταν και οι δύο περιττοί τότε $x^2+y^2 \equiv 2(mod4) \;\Rightarrow\; z^2 \equiv 2(mod4)$ άτοπο.

Επίσης αν ήταν και οι δύο άρτιοι, δηλαδή $2|x,\ 2|y$ τότε και

$2|z \;\Rightarrow\; 2|\text{ΜΚΔ}(x,y,z)=1$ άτοπο.

Αφού λοιπόν ένας είναι άρτιος και ο άλλος περιττός τότε και ο z περιττός.

Χωρίς βλάβη της γενικότητας υποθέτουμε ότι $x \equiv 1(mod2)$ και $y \equiv 0(mod2)$.

Τότε $x^2+y^2=z^2 \;\Rightarrow\; y^2=z^2-x^2 \;\Rightarrow\; y^2=(z-x)(z+x) \;\Rightarrow\; \frac{z+x}{y}=\frac{y}{z-x}$.

Έστω ότι $\frac{z+x}{y}=\frac{m}{n}$ με $(m,n)=1$, τότε $\left.\begin{array}{l}\frac{z}{y}+\frac{x}{y}=\frac{m}{n}\\ \frac{z}{y}-\frac{x}{y}=\frac{n}{m}\end{array}\right\} \Rightarrow \left\{\begin{array}{l}\frac{z}{y}=\frac{n^2+m^2}{2nm}\\ \frac{z}{y}=\frac{n^2-m^2}{2nm}\end{array}\right.$

με $(z,y)=1$ και $(x,y)=1$

Προφανώς $\text{ΜΚΔ}(n^2+m^2,2nm)=\text{ΜΚΔ}((m+n)^2,2mn)$.

Έστω ότι $\text{ΜΚΔ}(m^2+2mn+n^2,2mn)>1$.

Τότε θα υπήρχε πρώτος p που θα διαιρούσε το $(m+n)^2$ και είτε το 2 είτε το n είτε το m.

Έστω ότι $p|m$ και $p|m^2+2mn+n^2$ τότε $p|n^2 \;\Rightarrow\; p|n$ άρα $p|\text{ΜΚΔ}(m,n)=1$ άτοπο.

Όμοια αν $p|n$ καταλήγουμε σε άτοπο άρα αρκεί να δείξουμε ότι

$2 \nmid m^2+n^2 \;\Rightarrow\; 2 \nmid (m+n)^2$.

Αν $2|m^2+n^2$ τότε $m \equiv n(mod2)$.

Αν $2|m$ και $2|n \;\Rightarrow\; 2|\text{ΜΚΔ}(m,n)=1$ άτοπο.

Αν $m \equiv 1(mod2),\ n \equiv 1(mod2)$ τότε $2|m^2+n^2$ και $m^2+n^2 \equiv 2(mod4)$ άρα το $\frac{m^2+n^2}{2}$ είναι περιττός όπως και το $\frac{2mn}{2}$ όμως $\frac{z}{y}=\frac{\frac{m^2+n^2}{2}}{mn}$ με $z \equiv 1(mod2)$ και $y \equiv 0(mod2)$ αλλά $\frac{m^2+n^2}{2}$ περιττός και mn περιττός, άτοπο.

Άρα τελικά $\text{ΜΚΔ}(n^2+m^2,2nm)=1$ και αφού $\frac{z}{y}=\frac{m^2+n^2}{2mn}$ και $(z,y)=1$ τότε $z=m^2+n^2$ και $y=2mn$.

Τέλος από την $\frac{n^2-m^2}{2mn} \xrightarrow{y=2mn} x=n^2-m^2$.

Επομένως το σύνολο των, μη τετριμμένων λύσεων της εξίσωσης δίνεται από τις σχέσεις $\left\{\begin{array}{l}x=d(m^2-n^2)\\ y=d(2mn)\\ z=d(m^2+n^2)\end{array}\right\}$ όπου $d \in \mathbb{Z}\setminus\{0\},\ m,n \in \mathbb{Z}, m>n,\ (m,n)=1$ και ο ένας άρτιος και ο άλλος περιττός.

Άσκηση 3:

Θέλουμε x_1 τ.ω. $x_1^2 \equiv 2(mod7^2)$ και $x_1 \equiv 4(mod7)$.

Έχουμε $x_1 = 4 + 7a_1$ άρα

$x_1^2 - 2 \equiv (4 + 7a_1)^2 - 2 = 14 + 8 \cdot 7a_1 + 49a_1^2 \;\Rightarrow\; x_1^2 - 2 \equiv 7(2 + 8a_1)(mod 7^2)$

$x_1 - 2 \equiv 0(mod 7^2) \;\Leftrightarrow\; 2 + 8a_1 \equiv 0(mod 7)$

$2 + 8a_1 \equiv 0(mod 7) \;\Rightarrow\; a_1 = 5(mod 7)$

Άρα $x_1 \equiv 4 + 7 \cdot 5 = 39(mod 7^2)$

Για $n = 3:$ Θέλουμε $x_2^2 \equiv 2(mod 7^3)$ και $x_2 = 39(mod 7^2)$

$x_2 = 39 + 7^2 a_2$ άρα $x_2^2 - 2 = (39 + 7^2 a_2)^2 - 2 = 31 \cdot 7^2 + 78 \cdot 7^2 a_2 + 7^4 a_2^2$

$x_2^2 - 2 \equiv 7^2(31 + 78a_2)(mod 7^3)$

$x_2^2 - 2 \equiv 0(mod 7^3) \;\Leftrightarrow\; 31 + 78a_2 \equiv 0(mod 7)$

$31 + 78a_2 \equiv 0(mod 7) \;\Rightarrow\; 3 + a_2 \equiv 0(mod 7) \;\Rightarrow\; a_2 = 4(mod 7)$

Οπότε $x_2 \equiv 39 + 7^2 \cdot 4 \equiv 235(mod 7^3)$.

Για $n = 4:$ Θέλουμε $q_3^2 \equiv 2(mod 7^4)$ και $x_3 \equiv x_2(mod 7^3)$

$x_3 = 235 + 7^3 a_3$ άρα $x_3^2 - 2 = (235 + 7^3 a_3)^2 - 2 = 161 \cdot 7^3 + 470 \cdot 7^3 a_3 + 7^6 a_3^2$

$x_3^2 - 2 \equiv 7^3(161 + 470a_3)(mod 7^4)$

$x_3^2 \equiv 0(mod 7^4) \;\Leftrightarrow\; 161 + 470a_3 \equiv (mod 7)$

$161 + 470a_3 \equiv 0(mod 7) \;\Rightarrow\; a_3 \equiv 0(mod 7)$, οπότε $x_3 \equiv 235(mod 7^4)$. Τελικά

$(\bar{4},\ \bar{39},\ 2\bar{35},\ 2\bar{35}, \cdots)$.

Άσκηση 4:

(α) Για να έχει λύση η $x^2 = 7$ στον $\mathbb{Z}_3$ πρέπει η ισοτιμία $x^2 \equiv 7(mod 3)$ να έχει λύση.

$(\frac{7}{3}) = \frac{1}{3} = 1$. Επομένως η $x^2 = 7$ έχει λύση στον $\mathbb{Z}_3$. Όπως παραπάνω υπολογίζουμε ότι οι λύσεις είναι

$$\begin{array}{lcl} x_0 \equiv 1(mod 3) & & x_0 \equiv 2(mod 3) \\ x_1 \equiv 4(mod 3^2) & \text{και} & x_1 \equiv 5(mod 3^2) \\ x_2 \equiv 13(mod 3^3) & & x_2 \equiv 14(mod 3^3) \end{array} .$$

(β) Υπολογίζουμε το $(\frac{17}{5003})$ μέσω του νόμου της τετραγωνικής αντιστροφής

$(\frac{17}{5003}) = (-1)^{\frac{16 \cdot 5002}{4}}(\frac{5003}{17}) = (-1)^{4 \cdot 5002}(\frac{5}{17}) = (\frac{5}{17})$

$(\frac{5}{17}) \equiv 5^8 \equiv -1(mod 17)$ άρα $(\frac{17}{5003}) = -1$.

Επομένως, η εξίσωση x^2, δεν έχει λύση στον $\mathbb{Z}_{5003}$.

(γ) $x^2 \equiv -1(mod 2)$ έχει λύση το 1 προφανώς άρα $x_0 \equiv 1(mod 2)$

Ψάχνουμε x_1 τ.ω. $x_1^2 \equiv 1(mod 2^2)$ και $x_1 \equiv x_0 \equiv 1(mod 2)$.

Έχουμε $x_1 = 2a_1 + 1$ άρα

$x_1^2 - 1 = (2a_1 + 1)^2 - 1 = 1^2 + 2 \cdot 2a_1 + 4a_1^2 - 1 \equiv 0(mod4)$, δηλαδή,

$x_1^2 - 1 \equiv 0(mod2^2)$ είτε $a_1 \equiv 0(mod2)$ είτε $a_1 \equiv 1(mod2)$.

Επιλέγουμε $a_1 \equiv 1(mod2)$ άρα $x_1 = 3$

Ψάχνουμε x_2 τ.ω. $x_2^2 \equiv 1(mod2^3)$ και $x_2 \equiv x_1(mod2^2)$.

$x_2 = 3 + 2^2a_2$ οπότε $x_2^2 - 1 = (3 + 2^2a_2)^2 - 1 = 8 + 2^3a_2 + 2^4a_2^2$

$x_2^2 - 1 \equiv 0(mod2^3)$ είτε $a_2 \equiv 0(mod2)$ είτε $a_2 \equiv 1(mod2)$.

Επιλέγουμε $a_2 \equiv 1(mod2)$ άρα $x_2 \equiv 7(mod8)$

$(\bar{1},\ \bar{3},\ \bar{7}, ...)$.

Σημείωση: Αν $a_1 \equiv 0(mod2)$, έχουμε $x_1 \equiv 1(mod4)$ και $x_2 \equiv 1(mod8)$.

Άσκηση 5:

$\sum_{i=0}^{n}(p-1)p^i = \sum_{i=0}^{n}(p^{i+1}-p^i) = p^{n+1}-1$

$|(p^{n+1}-1)-(-1)|_p = |p^{n+1}-1+1|_p = |p^{n+1}|_p = \frac{1}{p^{n+1}}$

$\lim_{n\to+\infty}\frac{1}{p^{n+1}} = 0$, άρα $\lim_{n\to+\infty}|(p^{n+1}-1)-(-1)|_p = 0$

$\lim_{n\to+\infty}\sum_{i=0}^{n}(p-1)p^i = -1 \;\Rightarrow\; \sum_{i=0}^{\infty}(p-i)p^i = -1.$