Θέματα Άλγεβρας, Αριθμητική Γεωμετρία

Λύσεις ασκήσεων Φυλλαδίου 9

Γιάννης Α. Αντωνιάδης

Άσκηση 1:

Ένα σημείο P μιας ελλειπτικής καμπύλης $E/_{\mathbb{Q}}$ θα λέγεται σημείο καμπής

$\Leftrightarrow\ PP = P.$

Τρία σημεία P, Q, R αυτής κείνται πάνω στην ίδια ευθεία

$\Leftrightarrow\ R = PQ\ \Leftrightarrow\ -R = P \oplus Q$

Τώρα το $P \oplus Q = U(PQ)$ και $-R = (UU)R.$

Επομένως, τα P, Q, R κείνται πάνω στην ίδια ευθεία

$\Leftrightarrow\ U(PQ) = (UU)R$

(Επειδή $U(PQ) = UR$)

$\Leftrightarrow\ UR = (UU)R$

$\Leftrightarrow\ U = UU\ \Leftrightarrow\ U$ είναι σημείο καμπής.

Άσκηση 2:

Έστω η $E/_{\mathbb{Q}}\quad Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$ και $P = (x, y).$

Έχουμε $x(2P) = \lambda^2 + a_1\lambda - a_2 - 2x$

$2yy' + a_1xy' + a_1y + a_3y' = 3x^2 + 2a_2x + a_4$

$y' = \frac{3x^2+2a_2x+a_4-a_1y}{2y+a_1x+a_3}$ και $\lambda = y'|_{P=(x,y)}$ άρα

$x(2P) = (\frac{3x^2+2a_2x+a_4-a_1y}{2y+a_1x+a_3})^2 + a_1\frac{3x^2+2a_2x+a_4-a_1y}{2y+a_1x+a_3} - a_2 - 2x \quad (1)$

Έχουμε ότι $(2y + a_1x + a_3)^2 = 4y^2 + a_1^2x^2 + a_3^2 + 4a_1xy + 4ya_3 + 2a_1a_3x$

$= 4(x^3 + a_2X^2 + a_4x + a_6 - a_1xy - a_3y) + a_1^2x^2 + a_3^2 + 4a_1xy + 4a_3y + 2a_1a_3x$

$= 4x^3 + (a_1^2 + 4a_2)x^2 + 2(a_1a_3 + 2a_4)x + (a_3^2 + 4a_6)$

Έχουμε $b_2 = a_1^2 + 4a_2, \quad b_4 = a_1a_3 + 2a_4, \quad b_6 = a_3^2 + 4a_6$

Άρα $(2y + a_1x + a_3)^2 = 4x^3 + b_2x^2 + 2b_4x + \beta_6 \quad (2)$

$(3x^2 + 2a_2x + a_4 - a_1y)^2 + a_1(3x^2 + 2a_2x + a_4 - a_1y)(2y + a_1x + a_3) - (a_2 +$

$2x)(2y + a_1x + a_3)^2$

$= 9x^4 + (12a_2 + a_1^2)x^3 + (4a_2^2 + 6a_4 + a_1^2a_2 - a_1a_3)x^2 + (4a_2a_4 + a_1^2a_4 - 2a_3^2)x -$

$(4a_2 + a_1^2 + 8x)(y^2 + a_1xy + a_3y) + a_4^2 + a_1a_3a_4 - a_2a_3^2$

$= 9x^4 + (12a_2 + a_1^2)x^3 + (4a_2^2 + 6a_4 + a_1^2a_2 - a_1a_3)x^2 + (4a_2a_4 + a_1^2a_4 - 2a_3^2)x -$

$(4a_2 + a_1^2 + 8x)(x^3 + a_2x^2 + a_4x + a_6) + a_4^2 + a_1a_3a_4 - a_2a_3^2$

$= x^4 + (-2a_4 - a_1a_3)x^2 + (-8a_6 - 2a_3^2)x + (a_4^2 + a_1a_3a_4 - a_2a_3^2 - a_1^2a_6 - 4a_2a_6)$

Θέτουμε $b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2$, άρα έχουμε

$(3x^2 + 2a_2x + a_4 - a_1y)^2 + a_1(3x^2 + 2a_2x + a_4 - a_1y)(2y + a_1x + a_3) - (a_2 +$

$2x)(2y + a_1x + a_3)^2 = x^2 - b_4x^2 - 2b_6x - b_8 \quad (3)$

Από τις (1), (2), (3) έπεται $x(2P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}$

Άσκηση 3:

${}^{E}/_{\mathbb{Q}} \quad Y^2 + Y = X^3 - X \quad P = (0, 0)$

$2YY' + Y' = 3X^2 - 1 \quad \Rightarrow \quad Y' = \frac{3X^2 - 1}{2Y + 1}$

Υπολογίζουμε το $2P$

$\lambda = Y'|_P = \frac{-1}{1} = -1 \quad V = y - \lambda x = 0 - (-1) = 0$

$X_3 = \lambda^2 + a_1\lambda - a_2 - 2X = (-1)^2 + 0(-1) - 0 - 2 \cdot 0 = 1$

$Y_3 = -(-1) \cdot 1 - 0 - 0 \cdot 0 - 1 = 0 \quad$ Άρα $2P = (1, 0)$

Για το $3 \cdot P = 2P + P$

$\lambda = \frac{Y_2 - Y_1}{X_2 - X_1} = \frac{0-0}{1-0} = 0 \quad V = Y_1 - \lambda X_1 = 0 - 0 \cdot 0 = 0$

$X_3 = \lambda^2 + a_1\lambda - a_2 - X_1 - X_2 = -1$

$Y_3 = -\lambda X_3 - V - a_1X_3 - a_3 = -1 \quad$ Άρα $3P = (-1, -1)$

Για το $4P = 3P + P$

$\lambda = \frac{-1-0}{-1-0} = 1 \quad V = Y_1 - \lambda X_1 = 0$

$X_3 = \lambda^2 + a_1\lambda - a_2 - X_1 - X_2 = 1 - (-1) = 2$

$Y_3 = -\lambda X_3 - V - a_1X_3 - a_3 = -2 - 1 = -3 \quad$ Άρα $4P = (2, -3)$

Για το $5P = 4P + P$

$\lambda = \frac{-3-0}{2-0} = -\frac{3}{2} \quad V = Y_1 - \lambda X_1 = 0$

$X_3 = \lambda^2 + a_1\lambda - a_2 - X_1 - X_2 = (-\frac{3}{2})^2 - 2 = \frac{9}{4} - 2 = \frac{1}{4}$

$Y_3 = -\lambda X_3 - V - a_1 X_3 - a_3 = \frac{3}{2}\frac{1}{4} - 1 = -\frac{5}{8}$ Άρα $5P = (\frac{1}{4}, -\frac{5}{8})$

Για το $6P = 5P + P$

$\lambda = \frac{-\frac{5}{8}-0}{\frac{1}{4}-0} = -\frac{5}{2}$ $V = 0$

$X_3 = \lambda^2 + a_1\lambda - a_2 - X_1 - X_2 = \frac{25}{4} - \frac{1}{4} = 6$

$Y_3 = -\lambda X_3 - V - a_1 X_3 - a_3 = \frac{5}{2}6 - 1 = 14$ Άρα $6P = (6, 14)$

Άσκηση 5:

Διακρίνουμε περιπτώσεις:

Αν $x \equiv 0(modp)$ παίρνουμε το σημείο $(0, 0)$.

Αν $x \not\equiv 0(modp)$

Αν $x^3 + ax \equiv 0(modp)$ έχουμε το σημείο $(x, 0)$ και αυτόματα παίρνουμε για το $-x$ το $(-x, 0)$

Αν $x^3 + ax \not\equiv 0(modp)$ κοιτάζουμε το σύμβολο $Legendre$

$(\frac{(-x^3)+a(-x)}{p}) = (\frac{-1}{p})(\frac{x^3+ax}{p}) = (-1)^{\frac{p-1}{2}}(\frac{x^3+ax}{p}) = (-1)^{\frac{4k+3-1}{2}}(\frac{x^3+ax}{p}) = (-1)^{2k+1}(\frac{x^3+ax}{p}) = -(\frac{x^3+ax}{p})$

Άρα $(\frac{x^3+ax}{p}) = 1 \Leftrightarrow (\frac{(-x)^3+a(-x)}{p}) = -1$

Αν $(\frac{x^3+ax}{p}) = 1$ τότε η $y^2 \equiv x^3 + ax(\frac{x^3+ax}{p})$ έχει δύο λύσεις την $(x^3 + ax)^{\frac{p+1}{4}}$, $-(x^3 + ax)^{\frac{p+1}{4}}$ αφού $p \equiv 3(mod4)$ και $p \geq 7$, άρα μπορούμε να πούμε ότι στο x αντιστοιχίζουμε το σημείο $(x, (x^3 + ax)^{\frac{p+1}{4}})$ και στο $-x$ το $(x, -(x^3 + ax)^{\frac{p+1}{4}})$

Άρα δοκιμάσαμε όλες τις τιμές του x στο $\mathbb{F}_p$ και βρήκαμε ότι σε κάθε μια μπορούμε να αντιστοιχίσουμε ένα σημείο. Επίσης δεν έχουμε μετρήσει διπλά κάποια διότι $y \equiv -y(modp) \Rightarrow 2y \equiv 0(modp) \Rightarrow y \equiv 0(modp)$ άρα δεν μπορούμε να έχουμε $(x^3 + ax)^{\frac{p+1}{4}} \equiv -(x^3 + ax)^{\frac{p+1}{4}}(modp)$ για κάποιο x αφού έχουμε υποθέσει ότι $x^3 + ax \not\equiv 0(modp)$. Άρα έχουμε p στοιχεία και ένα το επ' άπειρο $p + 1$

Άσκηση 6:

Παραπομπή στις σημειώσεις του Ιωάννη Α. Αντωνιάδη, Αριθμητική Ελλειπτικών Καμπύλων, Το Θεώρημα του *Mordell*, Πανεπιστήμιο Κρήτης, Ηράκλειο 1999, σελίδες 98-99.