Ασκήσεις Ελλειπτικών Καμπύλων

2 Φυλλάδιο

Παράδοση Παρασκευή 26 Μαρτίου

1. Θεωρούμε ένα ομογενές πολυώνυμο $f(x,y,z) \in k[x,y,z]$, βαθμού n. Αποδείξτε ότι
$$\nabla f(x_0,y_0,z_0) = nf(x,y,z).$$
Δείξτε ότι στην περίπτωση ομογενών πολυωνύμων, το να ελέγξουμε αν ένα σημείο $(x_0 : y_0 : z_0) \in \mathbb{P}^1(k)$, είναι η όχι ιδιόμορφο αρκεί να κυτάξουμε μόνο τις μερικές παραγώγους του.

2. Θεωρήστε την ελλιπτική καμπύλη στην «μακρά» μορφή του Weierstrass,
$$E : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$
Διατυπώστε τον ορίσμο της χαρακτηριστικής ενός σώματος. Αποδείξτε ότι αν η χαρακτηριστική του σώματος K είναι διαφορετική του $2, 3$, τότε ο μετασχηματισμός
$$x = x' - b_2/12, y = y' - \frac{a_1}{2}\left(x' - b_2/12\right) - a_3/2,$$
όπου $b_2 = a_1^2 + 4a_2$, φέρνει την ελλειπτική καμπύλη στην μορφή
$$E : y^2 = x^3 + ax + b,$$
για κάποια κατάλληλα a, b.

3. Έστω P, Q διαφορετικά ρητά σημεία της E με συντεταγμένες (x_1, y_1) και (x_2, y_2) αντίστοιχα. Αποδείξτε ότι το σημείο $P+Q$ αν $P \neq \pm Q$ έχει συντεταγμένες (x_3, y_3) που δίνονται από τον τύπο:
$$x_3 = \lambda^2 - x_1 - x_2, y_3 = -\lambda x_3 - \nu,$$
όπου $\lambda = (y_1 - y_2)/(x_1 - x_2)$ και $\nu = y_1 - \lambda x_1$.

4. Να χρησιμοποιήσετε ένα πρόγραμμα όπως το Maple, Mathematica προκειμένου να σχεδιάσετε τις γραφικές παραστάσεις των καμπύλων:
$$y^2 = x^3 - 1, \quad , y^2 = x^3 + 1, \quad y^2 = x^3 - 3x + 3$$
$$y^2 = x^3 - 4x, \quad , y^2 = x^3 - x, \quad y^2 = x^3.$$

5. Θεωρήστε την ελλειπτική καμπύλη που ορίζεται από την

$$y^2z = x^3 + axz^2 + bz^3,$$

σαν υποσύνολο του $\mathbb{P}^1(\mathbb{F}_p)$, όπου p πρώτος αριθμός και $\mathbb{F}_p$ είναι το σώμα με p στοιχεία. Αποδείξτε ότι η ελλειπτική καμπύλη έχει πεπερασμένα το πλήθος στοιχεία. Θεωρήστε το σύμβολο του Legendre ($\frac{\cdot}{p}$, και απόδειξτε ότι το πλήθος των σημείων της ελλειπτικής καμπύλης δίνεται από τον τύπο

$$\#E(\mathbb{F}_p) = 1 + q + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p} \right).$$