

Απαρίθμηση Σημείων Ελλειπτικών Καμπυλών Σε Πεπερασμένα Σώματα

Αθανάσιος Γ. Αγγελάκης

Δ.Π.Μ.Σ. «Εφαρμοσμένες Μαθηματικές Επιστήμες»
Σχολή Εφαρμοσμένων Μαθηματικών κ' Φυσικών Επιστημών
Εθνικό Μετσόβιο Πολυτεχνείο

Επιβλέπον Καθηγητής: Α. Παπαϊωάννου

Μέλη Τριμελούς Επιτροπής: Α. Κοντογεώργης, Π. Στεφανέας

Αθήνα, Ιούνιος 2010

Θα ήθελα να ευχαριστήσω θερμά τον καθηγητή μου κ. Α. Κοντογεώργη για τις αμέτρητες ώρες που κατανάλωσε μαζί μου στην βοήθειά του για την συγγραφή αυτής της εργασίας. Επίσης ευχαριστώ τους καθηγητές μου, κ. Α. Παπαϊωάννου ο οποίος κατάλαβε εξ'αρχής τι με ενδιέφερε στις μεταπτυχιακές σπουδές μου και μου έδειξε τον δρόμο, και τον κ. Π. Στεφανέα ο οποίος πίστεψε στις ικανότητές μου, καθώς επίσης κι όλους τους καθηγητές των μεταπτυχιακών σπουδών μου, μέσα από τα μαθήματα των οποίων ήρθα σε επαφή με όμορφους κόσμους των μαθηματικών.

Ιδιαίτερα θα ήθελα να ευχαριστήσω τους γονείς και την αδερφή μου για την συμπαράσταση, υποστήριξη και κατανόηση που δείχνουν σε έναν παράξενο άνθρωπο και τις θυσίες που έχουν κάνει γι'αυτόν.

Περιεχόμενα

1	Εισαγωγή	3
1.1	Περί Τίνος Πρόκειται	3
1.2	Αναλυτικότερα	4
2	Θεωρητικό Υπόβαθρο	6
2.1	Δακτύλιοι και Σώματα	6
2.2	$\mathbf{R}$ -submodule	9
2.3	Ο Δακτύλιος $\mathcal{O}$ των Αλγεβρικών Ακεραίων	10
2.4	Επεκτάσεις Σωμάτων	10
2.5	Ιδεώδη	11
2.5.1	Κύρια, Maximal και Πρώτα	11
2.5.2	Ρητά	12
2.6	Αλγόριθμοι	13
3	Ελλειπτικές Καμπύλες	15
3.1	Γενικά	15
3.2	Ο νόμος ομάδας	18
3.3	Ελλειπτικές Καμπύλες σε Πεπερασμένα Σώματα	21
3.3.1	Ενδομορφισμός του Frobenius	21
3.3.2	Σε Σώματα με χαρακτηριστική $p > 3$	22
3.3.3	Σε Σώματα με χαρακτηριστική $p=2$	23
3.3.4	Πολυώνυμα Διάρσεως	24
4	Τρεις Αλγόριθμοι	28
4.1	Ο Αλγόριθμος του Shanks	28
4.2	Ο Αλγόριθμος του J.F.Mestre	30
4.3	Ο Αλγόριθμος του Cornacchia	33
5	Ο Αλγόριθμος του Schoof	35
6	Η Υλοποίηση του Αλγορίθμου του Schoof στο Maple 13	39
6.1	Ο Κώδικας	39
6.2	Ανάλυση Κώδικα	48

Κεφάλαιο 1

Εισαγωγή

1.1 Περί Τίνος Πρόκειται

Αρχικά, στο κεφάλαιο 2, δίνουμε τους απαραίτητους ορισμούς ώστε όσο είναι δυνατόν, η εργασία να είναι αυτόνομη. Στο κεφάλαιο 3 ορίζουμε τις ελλειπτικές καμπύλες και βλέπουμε κάποιες ιδιότητες των σημείων τους. Αφού τις εξετάσουμε σε πεπερασμένα σώματα της μορφής $\mathbb{F}_q, q = p^n, n \in \mathbb{N}^*, p$ πρώτος, ορίζουμε στην συνέχεια τα πολυώνυμα διαίρεσης τα οποία έχουν καθοριστικό ρόλο στον αλγόριθμο του Schoof, για τον οποίο θα μιλήσουμε στο 5ο κεφάλαιο. Τέλος, αναφερόμαστε σε 3 αλγόριθμους που προηγήθηκαν του αλγορίθμου του Schoof, στο 4ο κεφάλαιο.

Ο πρώτος βασίζεται στην στρατηγική baby step - giant step του Shanks, ενώ ο δεύτερος είναι βελτίωση του πρώτου, ο οποίος είναι πολύ πρακτικός όταν το πεπερασμένο σώμα δεν είναι πολύ μεγάλο. Ο τρίτος αλγόριθμος είναι πολύ αποδοτικός όταν ο δακτύλιος των ενδομορφισμών της καμπύλης είναι γνωστός. Ο τέταρτος αλγόριθμος, εκείνος του Schoof, βασίζεται σε υπολογισμούς των torsion points μιας ελλειπτικής καμπύλης. Αυτός είναι ντετερμινιστικός πολυωνυμικού χρόνου αλγόριθμος.

1.2 Αναλυτικότερα

Έστω p ένας μεγάλος πρώτος κι έστω $\mathcal{E}$ μία ελλειπτική καμπύλη επί του $\mathbb{F}_p$ η οποία δίνεται από την εξίσωση του *Weierstrass*

$$Y^2 = X^3 + aX + b$$

για κάποια $a, b \in \mathbb{F}_p$. Επειδή έχουμε ότι $4a^3 + 27b^2 \neq 0 \pmod{p}$ η καμπύλη είναι non-singular. Περιγράφουμε διάφορες μεθόδους οι οποίες απαριθμούν τα ρητά σημεία της $\mathcal{E}$, δηλαδή μεθόδους οι οποίες προσδιορίζουν ακριβώς τον αριθμό των σημείων (x, y) της $\mathcal{E}$ με $x, y \in \mathbb{F}_p$.

Έστω $\mathcal{E}(\mathbb{F}_p)$ ότι δηλώνει το σύνολο των ρητών σημείων τη $\mathcal{E}$. Είναι εύκολο να δει κάποιος πως ο αριθμός των σημείων στο $\mathcal{E}(\mathbb{F}_p)$ με δωσμένη την τετμημένη X , με $x \in \mathbb{F}_p$, είναι 0, 1 ή 2. Πιο συγκεκριμένα υπάρχουν

$$1 + \left(\frac{x^3 + ax + b}{p} \right)$$

ρητά σημεία στην $\mathcal{E}$ όπου η τετμημένη X είναι ίση με το x . Εδώ το $\left(\frac{\cdot}{p} \right)$ δηλώνει το σύμβολο του τετραγωνικού υπολοίπου του Legendre¹. Συμπεριλαμβάνοντας και το σημείο στο άπειρο, το σύνολο των ρητών σημείων $\mathcal{E}(\mathbb{F}_p)$ της $\mathcal{E}$ έχει cardinality

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

Αυτό συνεπάγεται ότι το να υπολογίσουμε το άθροισμα

$$\sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p} \right)$$

είναι το ίδιο πρόβλημα με το να υπολογίσουμε το $\#\mathcal{E}(\mathbb{F}_p)$.

Για πολύ μικρούς πρώτους p ένας ευθύς υπολογισμός αυτού του αθροίσματος είναι ικανός να υπολογίσει το $\#\mathcal{E}(\mathbb{F}_p)$. Στην πράξη είναι προτιμότερο αρχικά να κάνουμε μία λίστα των τετραγώνων modulo p και στην συνέχεια να μετρήσουμε πόσο συχνά το $x^3 + ax + b$ είναι τετράγωνο για $x = 0, 1, \dots, p-1$. Ο χρόνος αυτού του αλγορίθμου είναι $O(p^{1+\epsilon})$, $\forall \epsilon > 0$.

Για μεγαλύτερους p υπάρχουν καλύτεροι αλγόριθμοι. Στην παράγραφο 4.1 θα μιλήσουμε για έναν αλγόριθμο ο οποίος βασίζεται στην στρατηγική baby step - giant step του Shanks. Ο χρόνος του είναι της τάξης $O(p^{\frac{1}{4}+\epsilon})$. Αυτός ο αλγόριθμος πρακτικά είναι εφαρμόσιμος για, κατά κάποιον τρόπο, μεγαλύτερους πρώτους, αλλά παρουσιάζει προβλήματα όταν ο p έχει περισσότερα από 20 δεκαδικά ψηφία.

Στην παράγραφο 4.2 εξηγούμε ένα όμορφο τέχνασμα, το οποίο οφείλεται στον

¹Το σύμβολο του Legendre ορίζεται για κάθε ακέραιο a και κάθε πρώτο $p \neq 2$ ως εξής,

$$\left(\frac{a}{p} \right) = \begin{cases} 0, & a \equiv 0 \pmod{p} \\ +1, & a \not\equiv 0 \pmod{p}, a \equiv x^2 \pmod{p}, x \in \mathbb{Z} \\ -1, & a \not\equiv 0 \pmod{p}, \nexists x \in \mathbb{Z} : a \equiv x^2 \pmod{p} \end{cases}$$

J.-F.Mestre, ο οποίος απλουστεύει ορισμένους θεωρητικούς υπολογισμούς, που αφορούν ομάδες, στον αλγόριθμο baby step - giant step.

Στην 4.3 θα δούμε έναν αλγόριθμο ο οποίος υπολογίζει τα σημεία μια ελλειπτικής καμπύλης E επί του $\mathbb{F}_p$ όταν ο δακτύλιος ενδομορφισμών της E είναι γνωστός. Θα μιλήσουμε για τον σχετικό αλγόριθμο του Cornacchia.

Στο πέμπτο κεφάλαιο θα μιλήσουμε για έναν ντετερμινιστικό πολυωνυμικού χρόνου αλγόριθμο ο οποίος απαριθμεί σημεία ελλειπτικής καμπύλης σε πεπερασμένο σώμα και οφείλεται στον R.Schoof. Βασίζεται σε υπολογισμούς με τα torsion points της ελλειπτικής καμπύλης. Ο χρόνος του είναι $O(\log^8 p)$.

Κεφάλαιο 2

Θεωρητικό Υπόβαθρο

2.1 Δακτύλιοι και Σώματα

Ορισμός 2.1.1 *Μια πράξη $\circ$ σε ένα σύνολο $\mathbf{K}$ καλείται προσεταιριστική αν*

$$x \circ (y \circ z) = (x \circ y) \circ z$$

για κάθε $x, y, z \in \mathbf{K}$.

Ορισμός 2.1.2 *Μια πράξη $\circ$ σε ένα σύνολο $\mathbf{K}$ καλείται μεταθετική αν*

$$x \circ y = y \circ x$$

για κάθε $x, y \in \mathbf{K}$.

Ορισμός 2.1.3 *Ένα στοιχείο e καλείται δεξιό ουδέτερο (αντίστ. αριστερό ουδέτερο) ως προς την πράξη $\circ$ αν*

$$a \circ e = a, (e \circ a = a)$$

για κάθε $a \in \mathbf{K}$.

Αν το στοιχείο e είναι ταυτόχρονα δεξιό και αριστερό ουδέτερο τότε καλείται ουδέτερο.

Πρόταση 2.1.1 *Αν υπάρχουν δεξιά και αριστερά ουδέτερα στοιχεία, τότε υπάρχει ένα μονοσήμαντα ορισμένο ουδέτερο στοιχείο.*

Απόδειξη. Βλέπε [1] σελ.3.

▲

Ορισμός 2.1.4 Ένα στοιχείο a' (αντίστοιχα a'') καλείται δεξιό συμμετρικό (αριστερό συμμετρικό) ενός στοιχείου $a \in \mathbf{K}$ ως προς την πράξη $\circ$ με ουδέτερο στοιχείο το e αν

$$a \circ a' = e, (a'' \circ a = e)$$

Αν το στοιχείο a' είναι ταυτόχρονα αριστερό και δεξιό συμμετρικό του a , δηλαδή αν ικανοποιεί την σχέση

$$a \circ a' = a' \circ a = e$$

τότε λέγεται συμμετρικό του a .

Πρόταση 2.1.2 Αν η πράξη $\circ$ είναι προσεταιριστική και υπάρχουν αριστερά και αριστερά συμμετρικά ενός στοιχείου a , τότε υπάρχει ένα μονοσήμαντα ορισμένο συμμετρικό στοιχείο του a .

Απόδειξη. Βλέπε [1] σελ.4.

▲

Ορισμός 2.1.5 Ένα ζεύγος $(\mathbf{K}, \circ)$ το οποίο αποτελείται από ένα σύνολο $\mathbf{K}$ και μία πράξη $\circ$ σ' αυτό καλείται ημιομάδα όταν η πράξη είναι προσεταιριστική. Αν επιπλέον υπάρχει ουδέτερο στοιχείο, τότε καλείται μονοειδές.

Ορισμός 2.1.6 Εάν $\mathbf{A}, \mathbf{B}$ είναι δύο σύνολα με πράξεις $\circ, *$ αντίστοιχα, τότε μία απεικόνιση $f : \mathbf{A} \rightarrow \mathbf{B}$ καλείται ομομορφισμός (ή απλώς μορφοισμός) αν $f(a_1 \circ a_2) = f(a_1) * f(a_2)$ για όλα τα $a_1, a_2 \in \mathbf{A}$. Αν η f είναι $1-1$, καλείται μονομορφισμός ενώ εάν είναι επί καλείται επιμορφισμός. Τέλος εάν είναι $1-1$ και επί καλείται ισομορφισμός.

Ορισμός 2.1.7 Ένα ζεύγος $(\mathbf{G}, \circ)$ καλείται ομάδα αν είναι μονοειδές κι επιπλέον κάθε στοιχείο του έχει συμμετρικό στοιχείο.

Εάν επιπλέον η πράξη είναι μεταθετική τότε η ομάδα λέγεται μεταθετική ή συνηθέστερα αβελιανή (προς τιμή του N. Abel).

Ορισμός 2.1.8 Έστω $\mathbf{G}$ πεπερασμένη ομάδα. Ο μικρότερος $\alpha \in \mathbb{N}^* : a^\alpha = e, \forall a \in \mathbf{G}$, όπου e το ουδέτερο στοιχείο της ομάδας, καλείται *exponent* της ομάδας $\mathbf{G}$ και συμβολίζεται με $\exp(\mathbf{G})$.

Ορισμός 2.1.9 Μια τριάδα $(\mathbf{R}, +, \cdot)$ η οποία αποτελείται από ένα μη κενό σύνολο $\mathbf{R}$ και δύο πράξεις $+, \cdot$ (πολλαπλασιασμό και πρόσθεση) καλείται δακτύλιος αν ισχύουν,

- Το ζεύγος $(\mathbf{R}, +)$ είναι αβελιανή ομάδα.
- Το ζεύγος $(\mathbf{R}, \cdot)$ είναι ημιομάδα.
- $(a + b)c = ac + bc, c(a + b) = ca + cb$ για όλα τα $a, b, c \in \mathbf{R}$.

Εάν επιπλέον ο πολλαπλασιασμός είναι μεταθετικός τότε ο δακτύλιος ονομάζεται μεταθετικός.

Επίσης αν υπάρχει ουδέτερο στοιχείο ως προς τον πολλαπλασιασμό (δηλαδή μοναδιαίο στοιχείο που συμβολίζεται με 1), τότε ο δακτύλιος λέγεται δακτύλιος με μοναδιαίο.

Ορισμός 2.1.10 *Ενδομορφισμός είναι ένας ομομορφισμός από ένα μαθηματικό αντικείμενο στον εαυτό του.*

Έστω $(\mathbf{A}, +)$ μία αβελιανή ομάδα. Τα στοιχεία του δακτυλίου των ενδομορφισμών της $\mathbf{A}$ είναι οι ενδομορφισμοί της $\mathbf{A}$, δηλαδή η ομάδα ομομορφισμών όπου $\mathbf{A} \rightarrow \mathbf{A}$. Έστω f, g δύο ενδομορφισμοί της $\mathbf{A}$. Τότε ισχύει

$$(f + g)(x) = f(x) + g(x), x \in \mathbf{A}$$

και το αποτέλεσμα $f + g$ είναι ένας ενδομορφισμός της $\mathbf{A}$. Επίσης ισχύει,

$$(f \cdot g)(x) = f(x) \cdot g(x), x \in \mathbf{A}$$

όπου και πάλι το γινόμενο fg είναι ένας ενδομορφισμός της $\mathbf{A}$.

Έχουμε λοιπόν πως το σύνολο όλων των ενδομορφισμών της $\mathbf{A}$ με πράξεις τις $(+, \cdot)$ ικανοποιεί τον ορισμό του δακτυλίου. Συνεπώς αυτός είναι ο δακτύλιος ενδομορφισμών της $\mathbf{A}$.

Ορισμός 2.1.11 Έστω $\mathbf{R}$ ένας μεταθετικός δακτύλιος και $a \in \mathbf{R}, a \neq 0$. Το a ονομάζεται διαιρέτης του μηδενός αν υπάρχει $b \in \mathbf{R} : ab = 0$.

Ορισμός 2.1.12 Αν υπάρχουν μη μηδενικοί ακέραιοι n τέτοιοι ώστε $na = 0$ για κάθε $a \in \mathbf{R}$, τότε ο ελάχιστος θετικός ακέραιος με αυτήν την ιδιότητα καλείται χαρακτηριστική του δακτυλίου $\mathbf{R}$.

Πρόταση 2.1.3 Ο δακτύλιος $\mathbf{R}$ έχει χαρακτηριστική $n, n > 0$ αν n είναι ο ελάχιστος θετικός ακέραιος για τον οποίο ισχύει $n1_{\mathbf{R}} = 0$.

Απόδειξη. Βλέπε [1] σελ.96.

▲

Ορισμός 2.1.13 Ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο όπου κάθε μη μηδενικό στοιχείο του έχει πολλαπλασιαστικό αντίστροφο ονομάζεται σώμα.

Ορισμός 2.1.14 Πεπερασμένο σώμα ονομάζεται το σώμα το οποίο έχει πεπερασμένο το πλήθος στοιχείων.

Τα σημαντικότερα παραδείγματα πεπερασμένων σωμάτων είναι εκείνα της μορφής $\mathbb{F}_q, q = p^n, p$ πρώτος, $n \in \mathbb{N}^*$.

Θεώρημα 2.1.1 Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα. Τότε το $\mathbb{F}$ έχει χαρακτηριστική $p > 0$ και το πλήθος των στοιχείων του είναι p^n , όπου n είναι ο βαθμός του $\mathbb{F}$ επί του πρώτου υποσώματός του.

Απόδειξη. Βλέπε [11] σελ.227.

▲

Θεώρημα 2.1.2 Ένα πεπερασμένο σώμα έχει $q = p^n$ στοιχεία, όπου ο p είναι πρώτος αριθμός και ο n θετικός ακέραιος. Για κάθε τέτοιο q υπάρχει ακριβώς ένα σώμα, ορισμένο ως προς ισομορφισμό, με q στοιχεία. Αυτό είναι το σώμα ριζών του $x^{p^n} - x$ επί του $\mathbb{F}$.

Απόδειξη. Βλέπε [11] σελ.228.

▲

2.2 R-submodule

Ορισμός 2.2.1 Έστω $\mathbf{R}$ δακτύλιος. Ένα $\mathbf{R}$ -module είναι μια αβελιανή ομάδα $\mathbf{M}$ μαζί με μία συνάρτηση,

$$\begin{aligned} \alpha: \mathbf{R} \times \mathbf{M} &\rightarrow \mathbf{M} \\ \alpha(r, m) &= rm, r \in \mathbf{R}, m \in \mathbf{M} \end{aligned}$$

για την οποία ισχύουν,

$$\begin{aligned} (r + s)m &= rm + sm \\ r(m + n) &= rm + rn \\ r(sm) &= (rs)m \\ 1m &= m \end{aligned}$$

για κάθε $r, s \in \mathbf{R}, m, n \in \mathbf{M}$.

Η συνάρτηση α καλείται $\mathbf{R}$ -δράση στην $\mathbf{M}$.

Εάν $\mathbf{R}$ είναι ένα σώμα $\mathbf{K}$, τότε ένα $\mathbf{R}$ -module είναι ένας διανυσματικός χώρος επί του $\mathbf{K}$.

Ορισμός 2.2.2 Ένα $\mathbf{R}$ -submodule της $\mathbf{M}$ είναι μία υποομάδα $\mathbf{N}$ της $\mathbf{M}$ (όσο αφορά την πρόσθεση), τέτοια ώστε,

$$n \in \mathbf{N}, r \in \mathbf{R} \Rightarrow rn \in \mathbf{N}$$

Ορισμός 2.2.3 Ορίζουμε το module πηλίκο $\mathbf{M}/\mathbf{N}$ να είναι η αντίστοιχη ομάδα πηλίκο με την $\mathbf{R}$ -δράση

$$r(\mathbf{N} + m) = \mathbf{N} + rm, r \in \mathbf{R}, m \in \mathbf{M}$$

Ένα $\mathbb{Z}$ -module είναι μία αβελιανή ομάδα $\mathbf{M}$, ενώ κάθε προσθετική αβελιανή ομάδα $\mathbf{M}$ μπορούμε να την μετατρέψουμε σε ένα $\mathbb{Z}$ -module ορίζοντας,

Ορισμός 2.2.4

$$\begin{aligned} 0m &= m \\ 1m &= m, m \in \mathbf{M} \end{aligned}$$

οπότε έχουμε,

$$\begin{aligned} (n + 1)m &= nm + m, n \in \mathcal{N}^* \\ (-n)m &= -nm, n \in \mathcal{N}^* \end{aligned}$$

2.3 Ο Δακτύλιος $\mathfrak{D}$ των Αλγεβρικών Ακεραίων

Ορισμός 2.3.1 Μονικό καλούμε το πολυώνυμο εκείνο του οποίου ο συντελεστής του μεγιστοβάθμιου όρου είναι 1.

Ορισμός 2.3.2 Ένας μιγαδικός αριθμός θ λέγεται αλγεβρικός ακέραιος όταν υπάρχει ένα μονικό πολυώνυμο $p(t)$ με ακέραιους συντελεστές τέτοιο ώστε $p(\theta) = 0$, δηλαδή,

$$\theta^n + a_{n-1}\theta^{n-1} + \dots + a_0 = 0$$

όπου $a_i \in \mathbb{Z}, \forall i = 0, \dots, n-1$.

Συμβολίζουμε με $\mathbf{B}$ το σύνολο των αλγεβρικών ακεραίων.

Ορισμός 2.3.3 Για κάθε σώμα αριθμών $\mathbf{K}$ γράφουμε,

$$\mathfrak{D} = \mathbf{K} \cap \mathbf{B}$$

και καλούμε τον $\mathfrak{D}$ δακτύλιο των αλγεβρικών ακεραίων του $\mathbf{K}$.

2.4 Επεκτάσεις Σωμάτων

Για την εύρεση ριζών πολυωνύμου p πάνω σε σώμα $\mathbf{K}$ είναι πολλές φορές αναγκαίο να περνούμε σε ένα μεγαλύτερο σώμα $\mathbf{L}$ το οποίο περιέχει το $\mathbf{K}$. Υπό αυτές τις συνθήκες το $\mathbf{L}$ καλείται σώμα επέκτασης του $\mathbf{K}$. Η επέκταση του $\mathbf{L}$ στο $\mathbf{K}$ συμβολίζεται,

$$\mathbf{L} : \mathbf{K}$$

Εάν το $\mathbf{K} : \mathbf{L}$ είναι μία επέκταση, τότε το $\mathbf{L}$ έχει δομή διανυσματικού χώρου επί του $\mathbf{K}$. Η διάσταση αυτού του διανυσματικού χώρου καλείται βαθμός της επέκτασης, ή ο βαθμός επέκτασης του $\mathbf{L}$ επί του $\mathbf{K}$ και γράφεται,

$$[\mathbf{L} : \mathbf{K}]$$

Ορισμός 2.4.1 Εάν έχουμε μία επέκταση $\mathbf{L} : \mathbf{K}$ κι ένα στοιχείο $\alpha \in \mathbf{L}$ τότε είτε υπάρχει είτε όχι πολυώνυμο $p \in \mathbf{K}[t]$ τέτοιο ώστε $p(\alpha) = 0$. Εάν δεν υπάρχει, τότε το α καλείται υπερβατικό επί του $\mathbf{K}$. Εάν υπάρχει, το α καλείται αλγεβρικό επί του $\mathbf{K}$.

Ορισμός 2.4.2 Εάν το α είναι αλγεβρικό επί του $\mathbf{K}$, τότε υπάρχει μοναδικό μονικό πολυώνυμο q ελαχίστου βαθμού με $q(\alpha) = 0$. Το q καλείται ελάχιστο πολυώνυμο του α επί του $\mathbf{K}$.

Το ελάχιστο πολυώνυμο του α είναι ανάγωγο επί του $\mathbf{K}$.

Εάν $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbf{L}$, τότε γράφουμε

$$\mathbf{K}(\alpha_1, \alpha_2, \dots, \alpha_n)$$

το οποίο είναι το ελάχιστο υπόσωμα του $\mathbf{L}$ το οποίο περιέχει το $\mathbf{K}$ και τα στοιχεία $\alpha_1, \alpha_2, \dots, \alpha_n$.

Με ανάλογο τρόπο, εάν το $\mathbf{S}$ είναι υποδακτύλιος του $\mathbf{R}$ και $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbf{R}$, τότε γράφουμε

$$\mathbf{R}[\alpha_1, \alpha_2, \dots, \alpha_n]$$

για τον ελάχιστο υποδακτύλιο του $\mathbf{R}$ που περιέχει τον $\mathbf{S}$ και τα στοιχεία $\alpha_1, \alpha_2, \dots, \alpha_n$. Ο $\mathbf{S}[\alpha_1, \alpha_2, \dots, \alpha_n]$ αποτελείται από όλα τα πολυώνυμα των $\alpha_1, \alpha_2, \dots, \alpha_n$ με συντελεστές από το $\mathbf{S}$.

2.5 Ιδεώδη

2.5.1 Κύρια, Maximal και Πρώτα

Ορισμός 2.5.1 Ιδεώδες $\mathfrak{I}$ είναι ένα μη μηδενικό υποσύνολο ενός δακτυλίου $\mathbf{R}$ τέτοιο ώστε,

$$\begin{aligned} r, s \in \mathfrak{I} &\Rightarrow r - s \in \mathfrak{I} \\ r \in \mathbf{R}, s \in \mathfrak{I} &\Rightarrow rs \in \mathfrak{I} \end{aligned}$$

Χρησιμοποιούμε την έννοια του δακτυλίου πηλίκου $\mathbf{R}/\mathfrak{I}$ τα στοιχεία του οποίου είναι της μορφής $\mathfrak{I} + r$, υποσύνολα της προσθετικής ομάδας του $\mathfrak{I}$ στον $\mathbf{R}$.

Ορισμός 2.5.2 Οι πράξεις του πολλαπλασιασμού και της πρόσθεσης, στον δακτύλιο πηλίκου, ορίζονται ως,

$$\begin{aligned} (\mathfrak{I} + r) + (\mathfrak{I} + s) &= \mathfrak{I} + (r + s) \\ (\mathfrak{I} + r)(\mathfrak{I} + s) &= \mathfrak{I} + rs \end{aligned}$$

για κάθε $r, s \in \mathbf{R}$.

Ορισμός 2.5.3 Έστω $\mathfrak{I}, \mathfrak{J} \subseteq \mathbf{R}$. Τότε τα $\mathfrak{I} + \mathfrak{J}, \mathfrak{I}\mathfrak{J}$ είναι ιδεώδη του $\mathbf{R}$ με,

$$\begin{aligned} \mathfrak{I} + \mathfrak{J} &= \{x + y \mid x \in \mathfrak{I}, y \in \mathfrak{J}\} \\ \mathfrak{I}\mathfrak{J} &= \{\sum x_i y_i \mid x \in \mathfrak{I}, y \in \mathfrak{J}\} \end{aligned}$$

Ορισμός 2.5.4 Κύριο ιδεώδες $\mathfrak{I}$ καλούμε το ιδεώδες το οποίο παράγεται από ένα μόνο στοιχείο του δακτυλίου $\mathbf{R}$, δηλαδή $\mathfrak{I} = \langle x \rangle, x \in \mathbf{R}$.

Έστω $\mathbf{R}$ δακτύλιος. Τότε,

Ορισμός 2.5.5 Το ιδεώδες $\mathfrak{a}$ του δακτυλίου $\mathbf{R}$ καλείται *maximal* εάν το $\mathfrak{a}$ είναι κανονικό ιδεώδες του $\mathbf{R}$ και δεν υπάρχουν άλλα ιδεώδη του $\mathbf{R}$ αυστηρά ανάμεσα στο $\mathfrak{a}$ και τον $\mathbf{R}$.

Ορισμός 2.5.6 Το ιδεώδες $\mathfrak{a} \neq \mathbf{R}$ του δακτυλίου $\mathbf{R}$ καλείται *πρώτο* εάν όταν τα $\mathfrak{b}, \mathfrak{c}$ είναι ιδεώδη του $\mathbf{R}$ με $\mathfrak{bc} \subseteq \mathfrak{a}$, τότε είτε $\mathfrak{b} \subseteq \mathfrak{a}$, είτε $\mathfrak{c} \subseteq \mathfrak{a}$.

Ορισμός 2.5.7 Ένα ιδεώδες $\mathfrak{a}$ του δακτυλίου $\mathbf{R}$ καλείται *πεπερασμένα παραγόμενο* εάν παράγεται από πεπερασμένο το πλήθος στοιχεία του $\mathbf{R}$, δηλαδή $\mathfrak{I} = \langle a_1, a_2, \dots, a_n \rangle, n \in \mathcal{N}$.

2.5.2 Ρητά

Ορισμός 2.5.8 Ένα $\mathfrak{D}$ -submodule $\mathfrak{a}$ του $\mathbf{K}$ καλείται ρητό ιδεώδες του $\mathfrak{D}$, εάν υπάρχει κάποιο μη μηδενικό $c \in \mathfrak{D}$ τέτοιο ώστε $c\mathfrak{a} \subseteq \mathfrak{D}$.

Δηλαδή το σύνολο $\mathfrak{b} = c\mathfrak{a}$ είναι ένα ιδεώδες του $\mathfrak{D}$ και $\mathfrak{a} = c^{-1}\mathfrak{b}$. Οπότε τα ρητά ιδεώδη του $\mathfrak{D}$ είναι υποσύνολα του $\mathbf{K}$ της μορφής $c^{-1}\mathfrak{b}$, όπου $\mathfrak{b}$ είναι ένα ιδεώδες του $\mathfrak{D}$ και c ένα μη μηδενικό στοιχείο του $\mathfrak{D}$.

Ορισμός 2.5.9 Για κάθε ιδεώδες $\mathfrak{a}$ του $\mathfrak{D}$ ορίζουμε,

$$\mathfrak{a}^{-1} = \{x \in \mathbf{K} \mid x\mathfrak{a} \subseteq \mathfrak{D}\}$$

Είναι φανερό ότι το $\mathfrak{a}^{-1}$ είναι ένα $\mathfrak{D}$ -submodule. Εάν $\mathfrak{a} \neq 0$ τότε για κάθε $c \in \mathfrak{a}$ έχουμε ότι $c\mathfrak{a}^{-1} \subseteq \mathfrak{D}$, οπότε το $\mathfrak{a}$ είναι ένα ρητό ιδεώδες.

Από τον ορισμό έχουμε ότι,

$$\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{a}^{-1}\mathfrak{a} \subseteq \mathfrak{D}$$

Αυτό σημαίνει ότι το ρητό ιδεώδες $\mathfrak{a}\mathfrak{a}^{-1}$ είναι ιδεώδες.

2.6 Αλγόριθμοι

Ορισμός, με την μαθηματική έννοια του όρου, του αλγορίθμου, δεν υπάρχει. Θα μπορούσαμε να πούμε διαισθητικά ότι,

Αλγόριθμος είναι μία διαδικασία η οποία αποτελείται από καθορισμένες καταστάσεις και δεδομένης μιας αρχικής κατάστασης πραγματοποιεί μια σειρά διαδοχικών λειτουργιών, ώστε να φτάσει σε μια δεδομένη τελική κατάσταση μετά από πεπερασμένο το πλήθος καταστάσεις.

Ο Al Khwarizmi Πέρσης μαθηματικός και αστρονόμος έγραψε μια διατριβή στην αραβική γλώσσα το 825 μ.Χ. με τίτλο: «Υπολογισμοί με το ινδοαραβικό σύστημα αρίθμησης». Μεταφράστηκε από τα αραβικά στα λατινικά τον 12ο αιώνα με τίτλο: «Algoritmi de numero Indorum», όπου με την λέξη Algoritmi ο μεταφραστής απέδωσε το όνομα του συγγραφέα Al Khwarizmi. Στην συνέχεια, κι επειδή η διατριβή είχε να κάνει με αριθμούς (από την ελληνική λέξη ‘αριθμός’), δεν άργησε να επικρατήσει η λέξη Αλγόριθμος.

Ένας από τους πρώτους αλγόριθμους ο οποίος έχει ηλικία 2300(!!!) χρόνια περίπου, είναι εκείνος του πατέρα της γεωμετρίας, του Έλληνα μαθηματικού Ευκλείδη (325π.Χ.-265π.Χ.), για την εύρεση του μέγιστου κοινού διαιρέτη δύο ακέραιων αριθμών.

Όποτε έχουμε έναν αλγόριθμο πάντα υπάρχουν τρία ερωτήματα στα οποία πρέπει να απαντούμε,

- είναι ορθός;
- πόσο χρόνο χρειάζεται συναρτήσει του αριθμού των υπολογιστικών βημάτων n ;
- μπορούμε να τον βελτιώσουμε;

Η ορθότητα έχει να κάνει με το κατά πόσο καλά ο αλγόριθμός μας περιγράφει το πρόβλημα που έχουμε. Το κατά πόσο κι εάν μπορούμε να τον βελτιώσουμε έχει να κάνει με τον χρόνο τον υπολογιστικών βημάτων n . Όμως εκφράζοντας τον χρόνο του αλγορίθμου με στοιχειώδη βήματα της μηχανής, αμέσως ο χρόνος του αλγορίθμου εξαρτάται από την μηχανή στην οποία τον τρέχουμε. Γι’αυτόν και για άλλους λόγους τελικά θα εκφράζουμε τον αλγοριθμικό χρόνο απαριθμώντας τα βασικά υπολογιστικά βήματα συναρτήσει του μεγέθους των στοιχείων της αρχικής κατάστασης.

Ακόμα και αυτή η σύμβαση όμως οδηγεί σε άλλες. Για παράδειγμα, αντί να πούμε ότι ένας αλγόριθμος χρειάζεται $5n^3 + 4n + 3$ υπολογιστικά βήματα δεδομένης μιας αρχικής κατάστασης μεγέθους n , λέμε απλά ότι χρειάζεται υπολογιστικά βήματα της τάξης του n^3 , δηλαδή λέμε ότι ο αλγόριθμος είναι $O(n^3)$. Παρατηρούμε ότι οι όροι μικρότερου βαθμού $4n + 3$ δεν μας απασχολούν, καθώς επίσης και ο συντελεστής του n^3 .

Σχεφτόμενοι τις $f(n), g(n)$ σαν τους υπολογιστικούς χρόνους δύο αλγορίθμων με δεδομένη αρχική κατάσταση μεγέθους n έχουμε,

Ορισμός 2.6.1 Έστω οι συναρτήσεις $f(n), g(n) : \mathbb{N} \rightarrow \mathbb{R}^+$. Θα λέμε ότι $f = O(g)$, δηλαδή ότι η f μεγαλώνει όχι γρηγορότερα από την g , εάν υπάρχει σταθερά $c > 0 : f(n) \leq g(n)$.

Υπάρχουν κάποιοι γενικοί κανόνες όπου με βάση αυτούς απλοποιούνται κάποιες συναρτήσεις παραλείποντας κάποιους όρους των,

- Οι πολλαπλασιαστικοί συντελεστές παραλείπονται, δηλαδή το $14n^2 \rightsquigarrow n^2$.
- Το n^a επικρατεί του n^b , εάν $a > b$. Για παράδειγμα, $n^a + n^b \rightsquigarrow n^a$.
- Κάθε εκθετικός όρος επικρατεί οποιουδήποτε πολυωνυμικού, δηλαδή

$$\begin{aligned} 3^n + n^5 &\rightsquigarrow 3^n \\ 3^n + 2^n &\rightsquigarrow 3^n \end{aligned} \cdot$$

- Παρόμοια, κάθε πολυωνυμικός όρος επικρατεί κάθε λογαριθμικού, δηλαδή

$$\begin{aligned} n + (\log n)^3 &\rightsquigarrow n \\ n^2 + n \log n &\rightsquigarrow n^2 \end{aligned} \cdot$$

Κεφάλαιο 3

Ελλειπτικές Καμπύλες

3.1 Γενικά

Ορισμός 3.1.1 Προβολικός n -διάστατος χώρος επί του $\mathbf{K}$, συμβολίζουμε με $\mathbb{P}^n(\overline{\mathbf{K}})$, είναι το σύνολο όλων των $(n+1)$ -άδων

$$(x_0, \dots, x_n) \in \mathbb{A}^{n+1}$$

ώστε τουλάχιστον ένα x_i να είναι μη μηδενικό, modulo την σχέση ισοδυναμίας η οποία δίνεται από την

$$(x_0, \dots, x_n) \sim (y_0, \dots, y_n)$$

εάν υπάρχει $\lambda \in \overline{\mathbf{K}}^*$ με $x_i = \lambda y_i, \forall i$. Μία σχέση ισοδυναμίας $\{(\lambda x_0, \dots, \lambda x_n)\}$ συμβολίζεται με $[(x_0, \dots, x_n)]$ και τα $x_0, \dots, x_n$ ονομάζονται ομογενείς συντεταγμένες για το αντίστοιχο σημείο στο $\mathbb{P}^n$. Το σύνολο των $\mathbf{K}$ -ρητών σημείων του $\mathbb{P}^n$ είναι το σύνολο

$$\mathbb{P}^n(\mathbf{K}) = \{[x_0, \dots, x_n] \in \mathbb{P}^n : x_i \in \mathbf{K} \forall i\}.$$

Ορισμός 3.1.2 Ένα πολυώνυμο $f \in \overline{\mathbf{K}}[X] = \overline{\mathbf{K}}[X_0, \dots, X_n]$ λέγεται ομογενές βαθμού n εάν

$$f(\lambda X_0, \dots, \lambda X_n) = \lambda^d f(X_0, \dots, X_n) \forall \lambda \in \overline{\mathbf{K}}.$$

Ορισμός 3.1.3 Έστω $\mathbf{K}, \overline{\mathbf{K}}, \mathbf{K}^*$ σώμα, η αλγεβρική κλειστότητα και η πολλαπλασιαστική του ομάδα αντίστοιχα. Μία ελλειπτική καμπύλη επί του $\mathbf{K}$ ορίζεται ως το σύνολο των λύσεων, στο προβολικό επίπεδο, $\mathbb{P}^2(\overline{\mathbf{K}})$ της ομογενούς εξίσωσης του Weierstrass της μορφής,

$$\mathcal{E} : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \quad (3.1)$$

όπου $a_1, a_2, a_3, a_4, a_6 \in \mathbf{K}$.

Μία καμπύλη της παραπάνω μορφής λέγεται non-singular με την έννοια ότι εάν η παραπάνω εξίσωση γραφεί στην μορφή $F(X, Y, Z) = 0$, τότε οι μερικές παράγωγοι $\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}, \frac{\partial F}{\partial Z}$ δεν πρέπει να μηδενίζονται ταυτόχρονα σε κάποιο σημείο της καμπύλης.

Ορισμός 3.1.4 Έστω το $\hat{\mathbf{K}}$ σώμα το οποίο ικανοποιεί τις $\mathbf{K} \subseteq \hat{\mathbf{K}} \subseteq \overline{\mathbf{K}}$. Ένα σημείο (X, Y, Z) της καμπύλης είναι $\hat{\mathbf{K}}$ -ρητό εάν $(X, Y, Z) = \alpha(\hat{X}, \hat{Y}, \hat{Z})$ για κάποιο $\alpha \in \overline{\mathbf{K}}, (\hat{X}, \hat{Y}, \hat{Z}) \in \hat{\mathbf{K}}^3 \setminus (0, 0, 0)$.

Το σύνολο των $\hat{\mathbf{K}}$ -ρητών σημείων της $\mathcal{E}$ συμβολίζεται με $\mathcal{E}(\hat{\mathbf{K}})$.

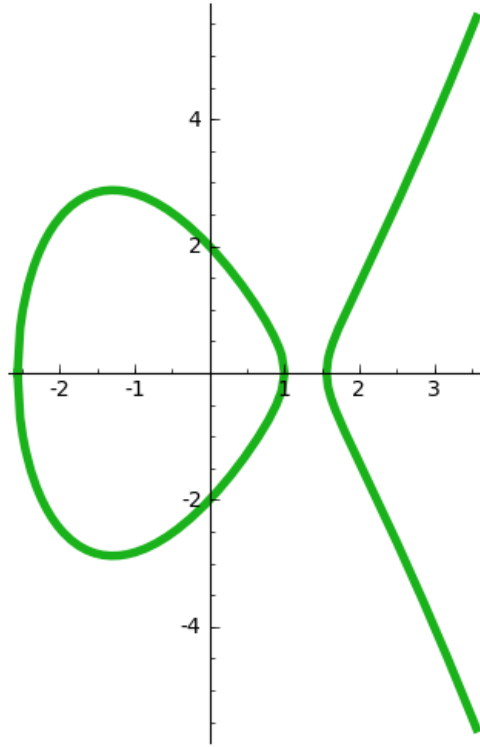
Ορισμός 3.1.5 Η καμπύλη έχει μόνο ένα ρητό σημείο με συντεταγμένη $Z = 0$, το σημείο $(0, 1, 0)$. Αυτό ονομάζεται σημείο στο άπειρο και συμβολίζεται με O .

Συνήθως θα χρησιμοποιούμε την affine μορφή της εξίσωσης του Weierstrass η οποία είναι,

$$\mathcal{E} : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \quad (3.2)$$

όπου $a_1, a_2, a_3, a_4, a_6 \in \mathbf{K}$.

Τα $\hat{\mathbf{K}}$ -ρητά σημεία της παραπάνω εξίσωσης είναι οι λύσεις της $\mathcal{E}$ στο $\hat{\mathbf{K}}^2$ και το σημείο του απείρου O . Για $Z \neq 0$ ένα προβολικό σημείο (X, Y, Z) το οποίο ικανοποιεί την (3.1) αντιστοιχεί σε ένα affine σημείο $(\frac{X}{Z}, \frac{Y}{Z})$ το οποίο ικανοποιεί την (3.2).



Η ελλειπτική καμπύλη $y^2 = x^3 - 5x + 4$ στο $\mathbb{R}$.

Με βάση την εξίσωση (3.2) ορίζουμε,

Ορισμός 3.1.6

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, b_4 = a_1a_3 + 2a_4, b_6 = a_3^2 + 4a_6, \\ b_8 &= a_2^6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24b_4, c_6 = -b_2^3 + 36b_2b_4 - 216b_6 \end{aligned}$$

Ορισμός 3.1.7 Διακρίνουσα της καμπύλης ορίζουμε να είναι,

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

Όταν $\text{char}(\mathbf{K}) \neq 2, 3$ τότε

$$\Delta = \frac{c_4^3 - c_6^2}{1728}$$

Μία καμπύλη τότε είναι non-singular εάν και μόνον εάν $\Delta \neq 0$.

Ορισμός 3.1.8 Όταν $\Delta \neq 0$ η j -invariant της καμπύλης ορίζεται να είναι,

$$j(\mathcal{E}) = \frac{c_4^3}{\Delta} \quad (3.3)$$

Λήμμα 3.1.1 Δύο ελλειπτικές καμπύλες $\mathcal{E}, \mathcal{E}'$ είναι ισόμορφες επί του $\mathbf{K}$ εάν και μόνον εάν υπάρχουν σταθερές $r, s, t \in \mathbf{K}, u \in \mathbf{K}^*$ τέτοιες ώστε οι μετασχηματισμοί

$$X = u^2X' + r, Y = u^3Y' + su^2X' + t$$

να μετατρέπουν την $\mathcal{E}$ στην $\mathcal{E}'$.

Απόδειξη. Βλέπε [3] σελ.31.

▲

Ένας τέτοιος μετασχηματισμός ορίζει ισομορφισμό ανάμεσα στα ρητά σημεία της $\mathcal{E}$ καμπύλης και στα ρητά σημεία της $\mathcal{E}'$ καμπύλης.

Λήμμα 3.1.2 Δύο ελλειπτικές καμπύλες οι οποίες είναι ισόμορφες επί του $\mathbf{K}$ έχουν την ίδια j -invariant. Αντίστροφα, δύο καμπύλες με την ίδια j -invariant είναι ισόμορφες επί του $\mathbf{K}$.

Απόδειξη. Βλέπε [3] σελ.31.

▲

Παρατηρούμε ότι ο ισομορφισμός ορίζεται σε σχέση με το σώμα $\mathbf{K}$. Καμπύλες οι οποίες δεν είναι ισόμορφες επί του $\mathbf{K}$, μπορούν να γίνουν ισόμορφες σε κάποιο $\bar{\mathbf{K}} \supseteq \mathbf{K}$.

3.2 Ο νόμος ομάδας

Υποθέτουμε ότι $\text{char}(\mathbf{K}) \neq 2, 3$ και θεωρούμε τις μεταβλητές

$$X = X' - \frac{b_2}{12}, Y = Y' - \frac{a_1}{2}(X' - \frac{b_2}{12}) - \frac{a_3}{2}$$

όπου το b_2 είναι ορισμένο στον Ορισμό 3.1.6. Αυτή η αλλαγή μεταβλητών μετατρέπει την εξίσωση (3.2) στην εξίσωση του Weierstrass

$$\mathcal{E} : Y^2 = X^3 + aX + b,$$

για κάποια $a, b \in \mathbf{K}$.

Έστω P, Q δύο διαφορετικά ρητά σημεία της ελλειπτικής καμπύλης $\mathcal{E}$. Η ευθεία η οποία ορίζεται από τα P, Q τέμνει την καμπύλη σε ένα τρίτο σημείο¹, έστω R , το οποίο θα είναι και αυτό ρητό αφού η ευθεία, η καμπύλη και τα σημεία P, Q ορίζονται επί του $\mathbf{K}$.

Ορισμός 3.2.1 Το συμμετρικό του R ως προς τον άξονα $x'x$ ορίζουμε να είναι το $P + Q$, το οποίο είναι και αυτό ρητό.

Για να προσθέσουμε το P στον εαυτό του βρίσκουμε την εφαπτομένη της καμπύλης στο σημείο αυτό. Αυτή πρέπει να τέμνει την $\mathcal{E}(\mathbf{K})$ σε ακριβώς ένα ακόμη σημείο, έστω το R καθώς η $\mathcal{E}$ ορίζεται από κυβική εξίσωση.

Ορισμός 3.2.2 Παίρνουμε το συμμετρικό του P ως προς τον άξονα $x'x$ και το σημείο που βρίσκουμε ορίζουμε να είναι το $[2]P = P + P$.

Ορισμός 3.2.3

Εάν η εφαπτομένη στο σημείο P είναι κάθετη, τότε ορίζουμε να τέμνει την καμπύλη στο O , οπότε $P + P = O$.

Η διαδικασία πρόσθεσης σημείων μιας ελλειπτικής καμπύλης, σύμφωνα με τους παραπάνω ορισμούς, ορίζει μία προσθετική αβελιανή ομάδα στο $\mathcal{E}(\hat{\mathbf{K}})$ για κάθε σώμα $\mathbf{K} \subseteq \hat{\mathbf{K}} \subseteq \bar{\mathbf{K}}$ με το σημείο στο άπειρο O να είναι ίσο με το ουδέτερο στοιχείο της πράξης.

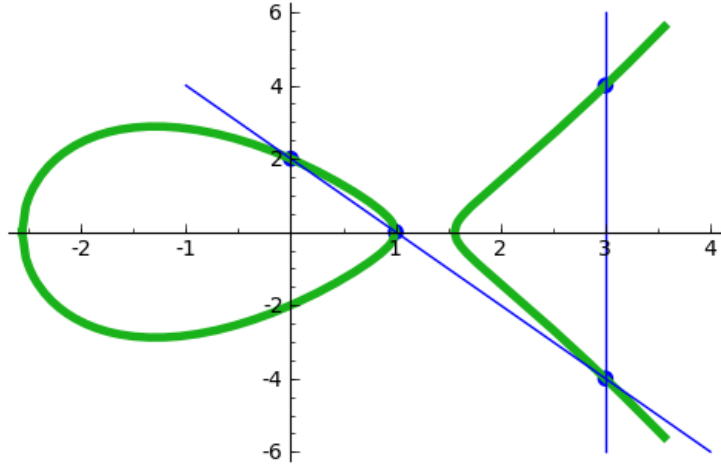
Χρησιμοποιώντας στο αριθμοθεωρητικό μαθηματικό πακέτο SAGE τις εντολές,

```
sage: E = EllipticCurve([-5,4])
sage: P = E.plot(thickness=4,rgbcolor=(0.1,0.7,0.1))
sage: ln0 = line([(3,-6),(3,6)])
sage: ln1 = line([(-1,4),(4,-6)])
sage: pt1 = point((1,0),pointsize=45)
sage: pt2 = point((0,2),pointsize=45)
sage: pt3 = point((3,4),pointsize=45)
sage: pt4 = point((3,-4),pointsize=45)
```

¹Σύμφωνα με το θεώρημα του Etienne Bezout 1730 – 1783, έστω A, B δύο καμπύλες στην επιφάνεια οι οποίες περιγράφονται από τις εξισώσεις $f(X, Y) = 0, g(X, Y) = 0$, όπου τα f, g είναι μη μηδενικά πολυώνυμα βαθμού m, n αντίστοιχα. Τότε οι A, B τέμνονται το πολύ σε $m * n$ σημεία.

```
sage: mygraph = (P + ln0 + ln1 + pt1 + pt2 + pt3 + pt4)
sage: mygraph.show()
```

έχουμε το παρακάτω σχήμα στο οποίο φαίνεται ο τρόπος πρόσθεσης σημείων ελλειπτικής καμπύλης.



Το άθροισμα των σημείων $(1, 0), (0, 2)$ στην ελλειπτική καμπύλη $y^2 = x^3 - 5x + 4$ στο $\mathbb{R}$, είναι το σημείο $(3, 4)$.

Λήμμα 3.2.1 *Τρία σημεία της καμπύλης $\mathcal{E}$ έχουν άθροισμα 0 εάν και μόνον εάν είναι συνευθειακά.*

Απόδειξη. Βλέπε [3] σελ.33.

Τα παρακάτω ισχύουν για κάθε χαρακτηριστική.

Λήμμα 3.2.2 *Έστω $\mathcal{E}$ η ελλειπτική καμπύλη με,*

$$\mathcal{E} : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

κι έστω $P_1(x_1, y_1), P_2(x_2, y_2)$ σημεία της καμπύλης αυτής. Τότε,

$$-P_1 = (x_1, -y_1 - a_1x_1 - a_3)$$

Έστω

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \mu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}, x_1 \neq x_2$$

και

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + ax_1 + a_3}, \mu = \frac{-x_1^2 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + ax_1 + a_3}, x_1 = x_2, P_2 \neq -P_1$$

Αν

$$P_3 = (x_3, y_3)$$

τότε τα x_3, y_3 δίνονται από τους τύπους

$$\begin{aligned} x_3 &= (\lambda)^2 + a_1\lambda - a_2 - x_1 - x_2 \\ y_3 &= -(\lambda + a_1)x_3 - \mu - a_3 \end{aligned}$$

Απόδειξη. Βλέπε [3] σελ.34.

▲

Ορισμός 3.2.4 Έστω ένας θετικός ακέραιος αριθμός m . Ορίζουμε την απεικόνιση

$$\begin{aligned} (x, y) &\rightarrow [m](x, y) \\ P &\rightarrow P + P + \dots + P \end{aligned}$$

m προσθετέοι. Έστω ακόμη ότι,

$$[0]P = O$$

και

$$[-m]P = -([m]P)$$

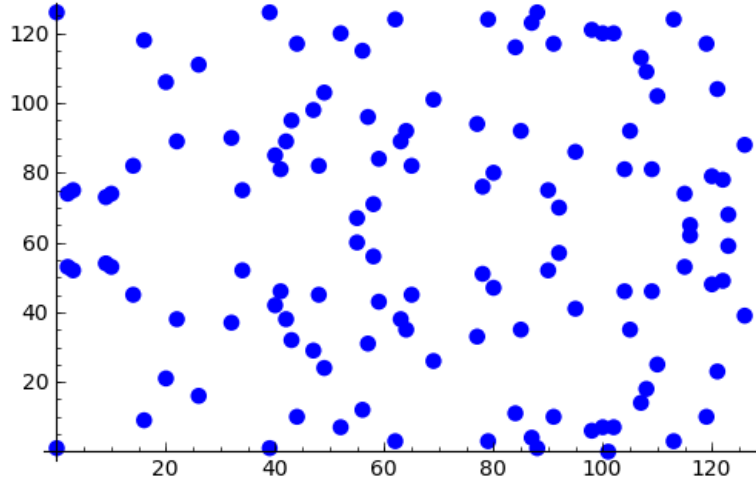
Ορισμός 3.2.5 Τάξη ενός σημείου P μιας ελλειπτικής καμπύλης $\mathcal{E}$ ονομάζεται ο θετικός ακέραιος m όταν

$$[m]P = O$$

3.3 Ελλειπτικές Καμπύλες σε Πεπερασμένα Σώματα

3.3.1 Ενδομορφισμός του Frobenius

Σε ένα πεπερασμένο σώμα $\mathbb{F}_q, q = p^n$, με p πρώτο αριθμό και n θετικό ακέραιο, ο αριθμός των ρητών σημείων μιας καμπύλης είναι πεπερασμένος και τον συμβολίζουμε με $\#\mathcal{E}(\mathbb{F}_q)$.



Η ελλειπτική καμπύλη $y^2 = x^3 - 5x + 4$ στο $\mathbb{F}_{127}$.

Ορισμός 3.3.1 Ορίζουμε την ποσότητα t ως,

$$\#\mathcal{E}(\mathbb{F}_q) = q + 1 - t$$

και ονομάζεται το ίχνος του Frobenius στο q .

Η απεικόνιση της q -οστής δύναμης του Frobenius πάνω σε μία ελλειπτική καμπύλη $\mathcal{E}$ ορισμένη επί του $\mathbb{F}_q$ ορίζεται ως,

Ορισμός 3.3.2

$$\phi : \begin{cases} \mathcal{E}(\overline{\mathbb{F}}_q) & \rightarrow \mathcal{E}(\overline{\mathbb{F}}_q) \\ (x, y) & \mapsto (x^q, y^q) \\ O & \mapsto O \end{cases}$$

Ισχύει ότι η συνάρτηση ϕ απεικονίζει σημεία της $\mathcal{E}$ σε σημεία της $\mathcal{E}$ και διατηρεί την δομή της προσθετικής ομάδας των σημείων της $\mathcal{E}$. Με άλλα λόγια η ϕ είναι ένας ενδομορφισμός ομάδας της $\mathcal{E}$ επί του $\mathbb{F}_q$ ο οποίος αναφέρεται ως ο ενδομορφισμός του Frobenius.

Το ίχνος του Frobenius t καθώς και ο ενδομορφισμός του Frobenius έχουν ουσιαστικό ρόλο στην μελέτη των ελλειπτικών καμπυλών. Συνδέονται με την σχέση,

$$\phi^2 - [t]\phi + [q] = 0$$

το οποίο σημαίνει ότι για ένα σημείο $P = (x, y)$ στην καμπύλη έχουμε,

$$(x^{q^2}, y^{q^2}) - [t](x^q, y^q) + [q](x, y) = O, t \in \mathbb{Z}$$

όπου η πρόσθεση και ο πολλαπλασιασμός δηλώνουν την πρόσθεση και τον πολλαπλασιασμό μεταξύ σημείων της καμπύλης.

Ορισμός 3.3.3 Η καμπύλη $\mathcal{E}(\mathbb{F}_q)$ λέγεται *anomalous* εάν το ίχνος του Frobenius της είναι 1. Οπότε έχουμε $\#\mathcal{E}(\mathbb{F}_q) = q$.

Ορισμός 3.3.4 Η καμπύλη $\mathcal{E}(\mathbb{F}_q)$ λέγεται *supersingular* εάν η χαρακτηριστική p διαιρεί το ίχνος t του Frobenius.

Ισοδύναμα,

Ορισμός 3.3.5 Μία καμπύλη επί του $\mathbb{F}_q$ το οποίο έχει χαρακτηριστική p είναι *supersingular* εάν και μόνον εάν

$$(p = 2 \text{ ή } p = 3 \text{ και } j(\mathcal{E}) = 0) \text{ ή } (p \geq 5 \text{ και } t = 0)$$

Επειδή πρακτικά αρκετά κρυπτοσυστήματα βασίζονται σε σώματα χαρακτηριστικής είτε 2 (π.χ. $\mathbb{F}_{2^n}$), είτε χαρακτηριστικής p , $\mathbb{F}_p$, για μεγάλο p πρώτο, στην συνέχεια θα διακρίνουμε κάποιες φορές αυτές τις περιπτώσεις.

3.3.2 Σε Σώματα με χαρακτηριστική $p > 3$

Υποθέτουμε ότι $\mathbf{K} = \mathbb{F}_q$, όπου $q = p^n$ για $p > 3$ πρώτο και ακέραιο $n \geq 1$. Η εξίσωση της ελλειπτικής καμπύλης, όπως έχει προλεχθεί, δίνεται από τον τύπο,

$$\mathcal{E}_{a,b} : Y^2 = X^3 + aX + b$$

Η διακρίνουσα της καμπύλης είναι $\Delta = -16(4a^3 + 27b^2)$ και η j -invariant της είναι $j(\mathcal{E}) = \frac{-1728(4a^3)}{\Delta}$. Η κλάση ισομορφισμών των καμπυλών επί του $\mathbf{K}$ σε αυτή την περίπτωση χαρακτηρίζεται από την σχέση,

$$\mathcal{E}_{a,b} \cong \mathcal{E}_{a',b'} \Leftrightarrow a' = u^4, b' = u^6b$$

για κάποιο $u \in \mathbf{K}^*$.

Από το Λήμμα 3.2.2 έχουμε τότε,

$$-P_1 = (x_1, -y_1)$$

Όταν $x_1 \neq x_2$ τότε,

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

ενώ όταν $x_1 = x_2, y_1 \neq 0$,

$$\lambda = \frac{3x_1^2 + a}{2y_1}$$

Εάν $P_3 = (x_3, y_3) = P_1 + P_2 \neq 0$ τότε τα x_3, y_3 δίνονται από τις σχέσεις,

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= (x_1 - x_3)\lambda - y_1 \end{aligned}$$

3.3.3 Σε Σώματα με χαρακτηριστική $p=2$

Υποθέτουμε ότι $\mathbf{K} = \mathbb{F}_q$, όπου $q = 2^n$ για $n \geq 1$ θετικό, ακέραιο. Σε αυτή την περίπτωση έχουμε για την j -invariant ότι $j(\mathcal{E}) = \frac{a_1^{12}}{\Delta}$. Υπό αυτές τις συνθήκες ένας αντιπρόσωπος για κάθε ισομορφισμό κλάσεων ελλειπτικών καμπυλών επί του $\mathbb{F}_q$ δίνεται από την,

$$\mathcal{E}_{a_2, a_6} : Y^2 + XY = X^3 + a_2X^2 + a_6$$

όπου $a_6 \in \mathbb{F}_q, a_2 \in \{0, \gamma\}$ με γ ένα συγκεκριμένο στοιχείο του $\mathbb{F}_q$. Από το Λήμμα 3.2.2 έχουμε τότε,

$$-P_1 = (x_1, y_1 + x_1)$$

Όταν $x_1 \neq x_2$ τότε,

$$\lambda = \frac{y_2 + y_1}{x_2 + x_1}, \mu = \frac{y_1x_2 + y_2x_1}{x_2 + x_1}$$

ενώ όταν $x_1 = x_2 \neq 0$,

$$\lambda = \frac{x_1^2 + y_1}{x_1}, \mu = x_1^2$$

Εάν $P_3 = (x_3, y_3) = P_1 + P_2 \neq 0$ τότε τα x_3, y_3 δίνονται από τις σχέσεις,

$$\begin{aligned} x_3 &= \lambda^2 + \lambda + a_2 + x_1 + x_2 \\ y_3 &= (x_1 - x_3)\lambda + x_3 + y_1 \end{aligned}$$

3.3.4 Πολυώνυμα Διαίρεσης

Τα πολυώνυμα διαίρεσης είναι θεμελιώδους σημασίας στο αλγόριθμο του Schoof για τον υπολογισμό του αριθμού των σημείων μιας ελλειπτικής καμπύλης σε πεπερασμένο σώμα, όπου είναι και ο κύριος σκοπός της εργασίας αυτής. Σε αυτή την παράγραφο θα ορίσουμε τα πολυώνυμα αυτά και θα σχολιάσουμε κάποιες ιδιότητές τους.

Με μια προσεκτική ματιά στις αλγεβρικές εκφράσεις που αφορούν τον νόμο ομάδας (πρβ.3.2), είναι φανερό ότι οι συντεταγμένες του αθροίσματος δύο σημείων $P_1 + P_2$ της καμπύλης είναι ρητές συναρτήσεις των συντεταγμένων των P_1, P_2 . Με επαναληπτική διαδικασία η απεικόνιση

$$(x, y) \mapsto [m](x, y)$$

μπορεί να εκφρασθεί με όρους ρητών συναρτήσεων των x, y . Πιο συγκεκριμένα έχουμε,

Λήμμα 3.3.1 Έστω $\mathcal{E}$ μια ελλειπτική καμπύλη ορισμένη στο σώμα $\mathbf{K}$ κι έστω m ένας θετικός ακέραιος. Τότε υπάρχουν πολυώνυμα $\psi_m, \theta_m, \omega_m$ τέτοια ώστε για $P = (x, y) \in \mathcal{E}(\mathbf{K})$ με $[m]P \neq 0$ έχουμε,

$$[m]P = \left(\frac{\theta_m(x, y)}{\psi_m^2(x, y)}, \frac{\omega_m(x, y)}{\psi_m^3(x, y)} \right) \quad (3.4)$$

Απόδειξη. Βλέπε [3] σελ.39. ▲

Το πολυώνυμο $\psi_m(x, y)$ ονομάζεται το m -οστό πολυώνυμο διαίρεσης της καμπύλης $\mathcal{E}$. Όπως θα φανεί παρακάτω, τα θ_m, ω_m εκφράζονται με παραστάσεις του ψ_m .

Παρουσιάζουμε τώρα αναδρομικούς ορισμούς των $\psi_m, \theta_m, \omega_m$.

Ορισμός 3.3.6 Έστω η εξίσωση (3.2) του Weierstrass της ελλειπτικής καμπύλης $\mathcal{E}$ επί του $\mathbf{K}$ και έστω ακόμη ότι έχουμε τις σταθερές που ορίσαμε στον ορισμό 3.1.6. Τότε το m -οστό πολυώνυμο διαίρεσης $\psi_m(x, y)$ ορίζεται με τον παρακάτω αναδρομικό τύπο,

$$\begin{aligned} \psi_0 &= 0 \\ \psi_1 &= 1 \\ \psi_2 &= 2y + a_1x + a_3 \\ \psi_3 &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8 \\ \psi_4 &= (2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + b_4b_8 - b_6^2)\psi_2 \\ \psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, m \geq 2 \\ \psi_{2m} &= \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{\psi_2}, m > 2 \end{aligned}$$

Οπότε για το θ_m έχουμε,

$$\theta_m = x\psi_m^2 - \psi_{m-1}\psi_{m+1}, m \geq 1$$

κι όταν $\text{char}(\mathbf{K}) \neq 2$ τα πολυώνυμα ω_m δίνονται από την σχέση,

$$2\psi_m\omega_m = \psi_{2m} - (a_1\theta_m + a_3\psi_m^2)\psi_m^2, m \geq 1.$$

Ορισμός 3.3.7 Όταν το $\mathbf{K}$ είναι πεπερασμένο σώμα $\mathbb{F}_q$, το $\mathcal{E}(\overline{\mathbf{K}})$ είναι *torsion* ομάδα. Δηλαδή κάθε σημείο P της καμπύλης $\mathcal{E}$ έχει πεπερασμένη τάξη.

Για κάποιον θετικό ακέραιο m το σύνολο των m -torsion σημείων της $\mathcal{E}$, το οποίο το συμβολίζουμε με $\mathcal{E}[m]$, ορίζεται ως,

Ορισμός 3.3.8

$$\mathcal{E}[m] = \{P \in \mathcal{E}(\overline{\mathbf{K}}) \mid [m]P = O\}$$

Γνωρίζουμε ότι $\mathcal{E}[m] \subseteq \mathcal{E}(\overline{\mathbf{K}})$. Ακόμη εξ ορισμού έχουμε ότι $O \in \mathcal{E}[m]$. Το m -οστό πολυώνυμο διαίρεσης ψ_m χαρακτηρίζει τα υπόλοιπα m -torsion σημεία της $\mathcal{E}$, σύμφωνα με το παρακάτω θεώρημα.

Θεώρημα 3.3.1 Έστω P σημείο στο $\mathcal{E}(\overline{\mathbf{K}}) \setminus O$ κι έστω $m \geq 1$. Τότε $P \in \mathcal{E}[m]$ εάν και μόνον εάν $\psi_m(P) = 0$.

Απόδειξη. Βλέπε [3] σελ.40.

▲

Παρατηρούμε ότι για τον υπολογισμό των m -torsion σημείων μπορούμε να χρησιμοποιήσουμε πολυώνυμο μιας μεταβλητής, αντί των πολυωνύμων ψ_m το οποία έχουν δύο μεταβλητές x, y .

Ορισμός 3.3.9

$$\bar{f}_m = \begin{cases} \psi_m, & m = 2k + 1, k \in \mathbb{N} \\ \frac{\psi_m}{\psi_2}, & m = 2k, k \in \mathbb{N} \end{cases}$$

Παρατηρώντας ότι το y χρησιμοποιείται στον αναδρομικό ορισμό του ψ_m μόνο μέσω του πολυωνύμου ψ_2 κι ότι το ψ_2^2 δεν εξαρτάται από το y , προκύπτει ότι το $\bar{f}_m$ είναι ένα πολυώνυμο το οποίο εξαρτάται μόνο από το x . Ο βαθμός του $\bar{f}_m$ είναι το πολύ $\frac{m^2-1}{2}$ εάν ο m είναι περιττός και το πολύ $\frac{m^2-4}{2}$ εάν ο m είναι άρτιος (οι βαθμοί είναι ακριβώς ίδιοι εάν $\text{char}(\mathbf{K})$ δεν διαιρεί τον m , για m περιττό, ή τον $\frac{m}{2}$, για m άρτιο). Το θεώρημα 3.3.1 μπορεί να αναδιατυπωθεί τώρα σύμφωνα με τον ορισμό του $\bar{f}_m$ ως εξής:

Λήμμα 3.3.2 Έστω $P = (x, y)$ σημείο στο $\mathcal{E}(\overline{\mathbf{K}}) \setminus O$ τέτοιο ώστε $[2]P \neq O$ κι έστω $m \geq 2$. Τότε $P \in \mathcal{E}[m]$ εάν και μόνον εάν $\bar{f}_m(x) = 0$.

Απόδειξη. Βλέπε [3] σελ.41.

▲

Το παραπάνω Λήμμα δεν συμπεριλαμβάνει τα 2 -torsion σημεία. Αυτά τα σημεία ικανοποιούν την $\psi_2(P) = 0$, το μέρος δηλαδή το οποίο διαιρείται με το ψ_m για να πάρουμε το $\bar{f}_m$, όταν το m είναι άρτιος.

Έστω $F(x) = 4x^3 + b_2x^2 + 2b_4x + b_6$. Τα πολυώνυμα $\bar{f}_m$ ικανοποιούν την παρακάτω αναδρομική σχέση,

$$\begin{aligned}\bar{f}_0 &= 0 \\ \bar{f}_1 &= 1 \\ \bar{f}_2 &= 1 \\ \bar{f}_3 &= \psi_3 \\ \bar{f}_4 &= \frac{\psi_4}{2} \\ \bar{f}_{2m+1} &= \begin{cases} \bar{f}_{m+2}\bar{f}_m^3 - F^2\bar{f}_{m-1}\bar{f}_{m+1}^3, & m \geq 3, m = 2k+1, k \in \mathbb{N} \\ F^2\bar{f}_{m+2}\bar{f}_m^3 - \bar{f}_{m-1}\bar{f}_{m+1}^3, & m \geq 2, m = 2k, k \in \mathbb{N} \end{cases} \\ \bar{f}_{2m} &= \bar{f}_{m+2}\bar{f}_{m-1}^2 - \bar{f}_{m-2}\bar{f}_{m+1}^2, m > 2\end{aligned}$$

Σε Σώματα με χαρακτηριστική $p > 3$

Η εξίσωση της ελλειπτικής καμπύλης υποθέτουμε ότι είναι της μορφής,

$$Y^2 = X^3 + aX + b, a, b \in \mathbb{F}_q$$

οπότε σύμφωνα με τον ορισμό 3.3.6 και λαμβάνοντας υπόψιν ότι

$$\begin{aligned}a_1 &= a_2 = a_3 = b_2 = 0 \\ a_4 &= a \\ a_6 &= b \\ b_4 &= 2a \\ b_6 &= 4b \\ b_8 &= -a^2\end{aligned}$$

έχουμε,

Ορισμός 3.3.10

$$\begin{aligned}\psi_0 &= 0 \\ \psi_1 &= 1 \\ \psi_2 &= 2y \\ \psi_3 &= 3x^4 + 6ax^2 + 12bx - a^2 \\ \psi_4 &= 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3) \\ \psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, m \geq 2 \\ \psi_{2m} &= \frac{(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)\psi_m}{2y}, m > 2\end{aligned}$$

Για έναν ακέραιο $m \geq 2$ κι ένα σημείο $P = (x, y) \in \mathcal{E}(\hat{K}) \setminus \mathcal{E}[m]$ το Λήμμα 3.3.1 γράφεται στην μορφή,

$$[m]P = \left(x - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2}, \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{4y\psi_m^3} \right)$$

όπου $\psi_m = \psi_m(x, y)$. Ο παραπάνω ορισμός (3.3.9) εύκολα μετατρέπεται σε αναδρομική σχέση για τα $\bar{f}_m$ σύμφωνα με τον,

Ορισμός 3.3.11

$$\bar{f}_m = \begin{cases} \psi_m, & m = 2k+1, k \in \mathbb{N} \\ \frac{\psi_m}{2y}, & m = 2k, k \in \mathbb{N} \end{cases}$$

Θέτουμε $F(x) = 4(x^3 + ax + b)$ (το οποίο είναι ίσο με $4y^4$ modulo την εξίσωση της καμπύλης), οπότε η αναδρομική σχέση είναι ίδια με εκείνη της γενικής περίπτωσης.

Σε Σώματα με χαρακτηριστική $p=2$

Ενδιαφερόμαστε μόνο για τις non-supersingular καμπύλες οι οποίες ορίζονται με την εξίσωση της μορφής,

$$Y^2 + XY = X^3 + a_2X^2 + a_6$$

οπότε σύμφωνα με τον ορισμό 3.3.6 και λαμβάνοντας υπόψιν ότι

$$\begin{aligned} a_3 &= a_4 = b_4 = b_6 = 0 \\ a_1 &= b_2 = 1 \\ b_8 &= a_6 \end{aligned}$$

έχουμε,

Ορισμός 3.3.12

$$\begin{aligned} \psi_0 &= 0 \\ \psi_1 &= 1 \\ \psi_2 &= x \\ \psi_3 &= x^4 + x^3 + a_6 \\ \psi_4 &= x^6 + a_2x^2 \\ \psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, m \geq 2 \\ \psi_{2m} &= \frac{(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)\psi_m}{x}, m > 3 \end{aligned}$$

Παρατηρούμε ότι σε αυτήν τη αναδρομική σχέση όλα τα ψ_m είναι πολυώνυμα μόνο του x . Θα σταθούμε στο γεγονός αυτό ορίζοντας σε αυτή την περίπτωση το,

Ορισμός 3.3.13

$$f_m(x) = \psi_m(x, y)$$

Οπότε, για έναν ακέραιο $m \geq 2$ κι ένα σημείο $P = (x, y \in \mathcal{E}(\hat{K})) \setminus \mathcal{E}[m]$ το Λήμμα 3.3.1 γράφεται στην μορφή,

$$[m]P = \left(x + \frac{f_{m-1}f_{m+1}}{f_m^2}, x + y + \frac{(x^2 + x + y)f_{m-1}f_{m+1} + f_{m-2}f_{m+1}^2}{xf_m^3} \right)$$

Ο ορισμός (3.3.9) εύκολα μετατρέπεται σε αναδρομική σχέση για τα f_m σύμφωνα με τον,

Ορισμός 3.3.14

$$f_m = \begin{cases} \bar{f}_m, & m = 2k + 1, k \in \mathbb{N} \\ xf_m, & m = 2k, k \in \mathbb{N} \end{cases}$$

Γενικά τα πολυώνυμα ψ_m καλούνται πολυώνυμα διαίρεσης. Σε αρκετές περιπτώσεις όμως πολυώνυμα διαίρεσης καλούνται και τα f_m .

Κεφάλαιο 4

Τρεις Αλγόριθμοι

4.1 Ο Αλγόριθμος του Shanks

Σε αυτή την ενότητα θα εξηγήσουμε τον αλγόριθμο baby step - giant step για να υπολογίσουμε σημεία της ελλειπτικής καμπύλης

$$\mathcal{E} : Y^2 = X^3 + aX + b$$

Σημαντικό ρόλο έχει ότι το σύνολο των σημείων του $\mathcal{E}(\mathbb{F}_p)$ αποτελεί μία προσθετική ομάδα (πρβ.3.2).

Το επόμενο αποτέλεσμα δίνει μια εκτίμηση της τάξης της ομάδας $\#\mathcal{E}(\mathbb{F}_p)$.

Θεώρημα 4.1.1 (H.Hasse,1933) Έστω p πρώτος και $\mathcal{E}$ μία ελλειπτική καμπύλη επί του $\mathbb{F}_p$. Τότε,

$$|p + 1 - \#\mathcal{E}(\mathbb{F}_p)| < 2\sqrt{p}$$

Απόδειξη. Βλέπε [8].

▲

Η ιδέα του αλγορίθμου είναι ότι ξεκινάει με ένα τυχαίο σημείο $P \in \mathcal{E}(\mathbb{F}_p)$ και υπολογίζει έναν ακέραιο m στο διάστημα $(p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$ τέτοιον ώστε $[m]P = 0$. Εάν ο m είναι ο μόνος ακέραιος με αυτή την ιδιότητα, τότε σύμφωνα με το Θεώρημα 4.1.1 προκύπτει ότι,

$$m \simeq \#\mathcal{E}(\mathbb{F}_p)$$

Για να βρει το σημείο εκκίνησης $P = (x, y) \in \mathcal{E}(\mathbb{F}_p)$, ο αλγόριθμος, διαλέγει τυχαίες τιμές του x ώσπου το $x^3 + ax + b$ να είναι τετράγωνο στο $\mathbb{F}_p$. Τότε υπολογίζει μία τετραγωνική ρίζα y του $x^3 + ax + b$.

Ο αριθμός m υπολογίζεται σύμφωνα με την στρατηγική baby step - giant step του D.Shanks. Η μέθοδός του έχει ως εξής.

Πρώτα κάνουμε τα baby steps: κάνουμε μια λίστα των πρώτων πολλαπλασίων $P, 2P, 3P, \dots, sP$ του P , όπου $s \simeq \sqrt{p}$. Παρατηρώντας ότι, επειδή το αντίστροφο ενός σημείου το λαμβάνουμε αλλάζοντας το πρόσημο της y συντεταγμένης του, γνωρίζουμε τις συντεταγμένες των $2s + 1$ σημείων $O, \pm P, \pm 2P, \dots, \pm sP$.

Στην συνέχεια υπολογίζουμε τα $Q = (2s + 1)P, R = (p + 1)P$ οπότε κάνουμε τα

giant steps: υπολογίζουμε τα $R, R \pm Q, R \pm 2Q, \dots, R \pm tQ$, όπου $t = \lceil \frac{2\sqrt{p}}{2s+1} \rceil$ το οποίο είναι περίπου ίσο με το $\sqrt[4]{p}$.

Σύμφωνα με το Θεώρημα 4.1.1 το σημείο $R + iQ$, για κάποιο ακέραιο $i = 0, \pm 1, \pm 2, \dots, \pm t$, είναι ίσο με κάποιο από τα σημεία που υπολογίσαμε στα baby steps. Οπότε για αυτό ακριβώς το i έχουμε ότι,

$$R + iQ = jP$$

για κάποιο $j \in \{0, \pm 1, \pm 2, \dots, \pm s\}$.

Συνεπώς για $m = p + 1 + (2s + 1)i - j$ έχουμε ότι $[m]P = 0$.

Αυτό σημαίνει ότι το $[m] \simeq \#\mathcal{E}(\mathbb{F}_p)$, δηλαδή βρίσκει ένα σημείο τάξης $[m]$ αλλά δεν γνωρίζουμε εάν αυτή η τάξη είναι και η τάξη της ομάδας των $\mathcal{E}(\mathbb{F}_p)$. Εξετάζοντας κι άλλα σημεία με τον ίδιο τρόπο, εάν έχουν τάξη μεγαλύτερη από την $[m]$, βρίσκουμε τελικά την τάξη των $\mathcal{E}(\mathbb{F}_p)$. Ο χρόνος του αλγόριθμου είναι $O(p^{\frac{1}{4}+\epsilon})$, $\forall \epsilon > 0$.

Ο αλγόριθμος αποτυγχάνει εάν υπάρχουν δύο διαφορετικοί ακέραιοι m, m' στο διάστημα $(p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$ με $[m]P = [m']P = O$. Αυτό όμως σπάνια συμβαίνει στην πραγματικότητα. Εάν συμβεί, τότε $[m - m']P = O$ οπότε αυτόματα γνωρίζουμε την τάξη d του P . Συνήθως αρκεί να επαναλάβουμε τον αλγόριθμο με ένα δεύτερο τυχαίο σημείο, διαφορετικό του πρώτου. Αυτήν τη φορά όμως το ότι γνωρίζουμε ότι το d διαιρεί το $\#\mathcal{E}(\mathbb{F}_p)$ συνήθως επισπεύδει την διαδικασία σημαντικά.

Πολύ πιο σπάνια ο αλγόριθμος αποτυγχάνει, όταν για κάθε P υπάρχουν περισσότερα από ένα m στο διάστημα $(p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$ τέτοια ώστε $[m]P = O$. Αυτό συμβαίνει όταν το $\exp(\mathcal{E}(\mathbb{F}_p))$ είναι πολύ μικρό. Αν και το να γράψει κανείς κάποιο πρόγραμμα που να περιλαμβάνει και αυτές τις σπάνιες περιπτώσεις, είναι γενικά επίπονο. Εντούτοις δεν αποτελούν σημαντικό πρόβλημα αφού για παράδειγμα κάποιος μπορεί να υπολογίσει ανεξάρτητους γεννήτορες της ομάδας.

Στην επόμενη ενότητα θα μιλήσουμε για το τέχνασμα του J.F.Mestre με το οποίο αποφεύγονται αυτά τα προβλήματα.

4.2 Ο Αλγόριθμος του J.F.Mestre

Θα εξηγήσουμε την ιδέα του J.F.Mestre ώστε να αποφύγουμε τα προβλήματα που αναφέρθηκαν στο τέλος της προηγούμενης παραγράφου. Χρησιμοποιεί την έννοια του quadratic twist της ελλειπτικής καμπύλης $\mathcal{E}$.

Εάν η ελλειπτική καμπύλη $\mathcal{E}$ δίνεται από τον τύπο

$$Y^2 = X^3 + aX + b$$

τότε η twisted καμπύλη $\mathcal{E}'$ δίνεται από τον τύπο

$$gY^2 = X^3 + aX + b$$

για κάποιο μη τετραγωνικό $g \in \mathbb{F}_p^*$. Η κλάση ισομορφισμού αυτής της καμπύλης δεν εξαρτάται από το την επιλογή του g . Η εξίσωση του Weierstrass για την καμπύλη $\mathcal{E}'$ είναι,

$$Y^2 = X^3 + ag^2X + bg^3$$

Γνωρίζουμε ότι,

$$\#\mathcal{E}'(\mathbb{F}_p) + \#\mathcal{E}(\mathbb{F}_p) = 2(p+1)$$

οπότε για τον υπολογισμό του $\#\mathcal{E}(\mathbb{F}_p)$ μπορούμε να υπολογίσουμε το $\#\mathcal{E}'(\mathbb{F}_p)$. Συνεπάγεται από τα Θεωρήματα 4.2.1 και 4.2.2, τα οποία ακολουθούν, ότι εάν το $\exp(\mathcal{E}(\mathbb{F}_p))$ είναι πολύ μικρό, τότε το $\exp(\mathcal{E}')$ της ομάδας των σημείων της quadratic twist δεν είναι. Μπορούμε να χρησιμοποιήσουμε αυτή την παρατήρηση ως εξής: εάν για την ελλειπτική καμπύλη $\mathcal{E}$ ο αλγόριθμος του Shanks απέτυχε για κάποιον αριθμό σημείων P , επειδή κάθε φορά περισσότερες από μία τιμές του m βρέθηκαν ώστε $[m]P = O$, τότε αντικαθιστούμε την $\mathcal{E}$ με την $\mathcal{E}'$ και προσπαθούμε ξανά.

Ορισμός 4.2.1 Η j -invariant της ελλειπτικής καμπύλης

$$\mathcal{E} : Y^2 = X^3 + aX + b$$

είναι,

$$j(\mathcal{E}) = 1728 \frac{4a^3}{4a^3 + 27b^2}$$

Εύκολα παρατηρούμε ότι η $\mathcal{E}$ και η quadratic twist $\mathcal{E}'$ αυτής, έχουν την ίδια j -invariant. Για τις περισσότερες j -invariant με $j \in \mathbb{F}_p$, υπάρχουν όσο αφορά τον ισομορφισμό, ακριβώς δύο ελλειπτικές καμπύλες επί του $\mathbb{F}_p$ με $j(\mathcal{E}) = j$. Η καμπύλη $\mathcal{E}$ και η quadratic twist αυτής. Υπάρχουν όμως δύο πολύ γνωστές εξαιρέσεις,

$$\begin{aligned} j &= 0, & p &= 1 \pmod{3} \\ j &= 1728, & p &= 1 \pmod{4} \end{aligned}$$

όπου στην πρώτη περίπτωση υπάρχουν 6 καμπύλες ενώ στη δεύτερη 4.

Οι μορφισμοί $f : \mathcal{E} \rightarrow \mathcal{E}'$, οι οποίοι διατηρούν το σημείο στο άπειρο, δημιουργούν έναν δακτύλιο $\text{End}(\mathcal{E})$ των $\mathbb{F}_p$ -ενδομορφισμών της $\mathcal{E}$. Είναι ισομορφικός με μία

μιγαδική τετραγωνική τάξη. Εάν το $d \in \mathbb{Z}_{<}$ δηλώνει την διακρίνουσα της τάξης έχουμε,

$$\text{End}(\mathcal{E}) \cong \mathbb{Z}[\delta] = \mathbb{Z} + \delta\mathbb{Z}$$

όπου,

$$\begin{aligned} \delta &= \frac{\sqrt{d}}{2}, & d &= 2k, k \in \mathbb{Z} \\ \delta &= \frac{1+\sqrt{d}}{2}, & d &= 2k+1, k \in \mathbb{Z} \end{aligned}$$

Μία ελλειπτική καμπύλη και η quadratic twist αυτής έχουν ισόμορφο ενδομορφισμό δακτυλίων.

Εάν $p = 1(\text{mod } 3)$, οι 6 καμπύλες με $j = 0$ όλες έχουν τον ενδομορφισμό δακτυλίου τους ισόμορφο με τον $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, ενώ αν $p = 1(\text{mod } 4)$, τότε οι 4 καμπύλες $\mathcal{E}$ με $j = 1728$ όλες έχουν $\text{End}(\mathcal{E})$ ισόμορφο με τον δακτύλιο των ακεραίων του Gauss $\mathbb{Z}[i]$.

Ο ενδομορφισμός του Frobenius, σύμφωνα με τον Ορισμό 3.3.2, δίνεται από την,

$$\phi : \begin{cases} \mathcal{E}(\overline{\mathbb{F}}_p) & \rightarrow \mathcal{E}(\overline{\mathbb{F}}_p) \\ (x, y) & \mapsto (x^p, y^p) \\ O & \mapsto O \end{cases}$$

ανήκει στον $\text{End}(\mathcal{E})$ και ικανοποιεί την εξίσωση,

$$\phi^2 - [t]\phi + [p] = O$$

στον δακτύλιο ενδομορφισμών της $\mathcal{E}$. Το t είναι το ίχνος του Frobenius το οποίο, σύμφωνα με τον Ορισμό 3.3.1, ικανοποιεί την,

$$\#\mathcal{E}(\mathbb{F}_p) = p + 1 - t.$$

Η ομάδα $\mathcal{E}(\mathbb{F}_p)$ είναι ακριβώς ο πυρήνας του ομομορφισμού $\phi - I_d$ δρώντας στην ομάδα των σημείων επί μιας αλγεβρικής κλειστότητας του $\mathbb{F}_p$. Συνεπώς, το $\exp(\mathcal{E}(\mathbb{F}_p))$ είναι,

$$\frac{p + 1 - t}{n}$$

όπου n είναι ο μέγιστος ακέραιος τέτοιος ώστε η $\mathcal{E}(\mathbb{F}_p)$ να περιέχει μια υποομάδα ισομορφική με το $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Ισοδύναμα, n είναι ο μέγιστος ακέραιος για τον οποίο $\phi = 1(\text{mod } n)$ στον $\text{End}(\mathcal{E})$.

Θεώρημα 4.2.1 (J.F.Mestre) Έστω $p > 457$ πρώτος κι έστω $\mathcal{E}$ μία ελλειπτική καμπύλη επί του $\mathbb{F}_p$. Τότε είτε η $\mathcal{E}$ είτε η quadratic twist $\mathcal{E}'$ αυτής, περιέχει ένα $\mathbb{F}_p$ -ρρητό σημείο τάξης το λιγότερο $4\sqrt{p}$.

Απόδειξη. Ο δακτύλιος ενδομορφισμών της $\mathcal{E}$ με τον δακτύλιο ενδομορφισμών της $\mathcal{E}'$ είναι ισόμορφοι με την ίδια τετραγωνική τάξη $\mathfrak{O}$ της διακρίνουσας d . Έστω $\phi \in \mathfrak{O}$ ο ενδομορφισμός του Frobenius της $\mathcal{E}$. Έστω ακόμη n ο μέγιστος ακέραιος τέτοιος ώστε $\phi = 1(\text{mod } n)$ στο $\text{End}(\mathcal{E})$ και $N = \frac{p+1-t}{n}$ να είναι το $\exp(\mathcal{E}(\mathbb{F}_p))$. Έχουμε τότε ότι,

$$\mathbb{Z}[\phi] \subset \mathbb{Z}\left[\frac{\phi - 1}{n}\right] \subset \mathfrak{O}$$

το οποίο σημαίνει ότι ο n διαιρεί τον δείκτη $[\mathfrak{O} : \mathbb{Z}[\phi]]$. Αφού $[\mathfrak{O} : \mathbb{Z}[\phi]]^2$ είναι ίσο με το πηλίκο των διακρινουσών των τάξεων $\mathfrak{O}$ και $\mathbb{Z}$ έχουμε ότι ο n^2 διαιρεί τον

$\frac{t^2-4p}{d}$, όπου $t^2 - 4p$ είναι η διακρίνουσα τάξης του $\mathbb{Z}[\phi]$
 Ομοίως, έστω m ο μέγιστος ακέραιος τέτοιος ώστε $-\phi = 1 \pmod{m}$ στον $\text{End}(\mathcal{E})$
 κι έστω $M = \frac{p+1-t}{m}$ το $\exp(\mathcal{E}')$. Τότε,

$$\mathbb{Z}[\phi] \subset \mathbb{Z}\left[\frac{\phi-1}{m}\right] \subset \mathfrak{O}$$

Οπότε ο m^2 επίσης διαιρεί τον $\frac{t^2-4p}{d}$.
 Αφού ο n διαιρεί τον $\phi-1$ και ο m διαιρεί τον $\phi+1$ παρατηρούμε ότι ο $\gcd(n, m)$
 διαιρεί τον $\gcd(\phi-1, \phi+1)$ ο οποίος διαιρεί το 2. Οπότε έχουμε,

$$n^2 m^2 \mid 4 \frac{t^2-4p}{d}$$

Επειδή $|d| \geq 3$ αυτό σημαίνει ότι $(nm)^2 \leq 4 \frac{4p-t^2}{d}$. Εάν $N, M < 4\sqrt{2}$ έχουμε ότι,

$$((p+1)^2 - t^2)^2 = (nNmM)^2 < (4\sqrt{p})^4 * 4 \frac{4p-t^2}{3}$$

οπότε,

$$p^4 + 4p^3 < (p+1)^4 \frac{4^6}{3} p^3 - t^4 - \left(\frac{4^5}{3} p^2 - 2(p+1)^2\right) t^2 \leq \frac{4^6}{3} p^3$$

το οποίο σημαίνει ότι $p < 1362$.

Εάν εξετάσουμε όλες τις περιπτώσεις για $p \leq 457$ θα δούμε πως το θεώρημα ισχύει.

▲

Για να είναι σίγουρος κανείς ότι ο αλγόριθμος του Shanks θα δουλέψει για μία ελλειπτική καμπύλη $\mathcal{E}$, δεν χρειάζεται να βρει ένα ρητό σημείο αυτής, τάξης το λιγότερο $4\sqrt{p}$. Αυτό που χρειάζεται είναι ένα σημείο P της καμπύλης με την ιδιότητα όπως περιγράφεται στο επόμενο θεώρημα.

Θεώρημα 4.2.2 (R. Schoof) Έστω $p > 229$ πρώτος κι έστω $\mathcal{E}$ μία ελλειπτική καμπύλη επί του $\mathbb{F}_p$. Τότε είτε η $\mathcal{E}$ είτε η quadratic twist αυτής $\mathcal{E}'$ περιέχει ένα $\mathbb{F}_p$ -ρητό σημείο P , με την ιδιότητα ότι ο μόνος ακέραιος $m \in (p+1-2\sqrt{p}, p+1+2\sqrt{p})$ για τον οποίο ισχύει $[m]P = O$, είναι η τάξη της ομάδας των σημείων της ελλειπτικής καμπύλης.

Απόδειξη. Από την απόδειξη του αποτελέσματος του J.F.Mestre το θεώρημα ισχύει για $p > 457$. Ένας υπολογισμός για κάθε περίπτωση ξεχωριστά μας δείχνει ότι ισχύει για κάθε $p > 229$.

▲

Πολλές ελλειπτικές καμπύλες $\mathcal{E}$ για τις οποίες το Θεώρημα 4.2.2 δεν ισχύει, έχουν j -invariant ίση με 0 ή με 1728 οπότε οι ενδομορφισμοί του δακτυλίου τους είναι ισόμορφοι με το $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ ή με το $\mathbb{Z}[i]$ αντίστοιχα. Όμως, εάν κάποιος γνωρίζει τον δακτύλιο ενδομορφισμών της $\mathcal{E}$, είναι πολύ εύκολο να υπολογίσει την $\#\mathcal{E}(\mathbb{F}_p)$ ακόμα κι όταν ο p είναι πολύ μεγάλος. Αυτό είναι μια συνέπεια του Θεωρήματος 4.3.1 της επόμενης παραγράφου. Όταν κάποιος εξαιρεί τις καμπύλες με j -invariant ίση με 0 ή 1728, τότε το Θεώρημα 4.2.1 ισχύει για $p > 193$, ενώ το Θεώρημα 4.2.2 ισχύει για $p > 53$.

4.3 Ο Αλγόριθμος του Cornacchia

Σε αυτή την παράγραφο θα εξηγήσουμε πώς υπολογίζουμε τον αριθμό σημείων μιας ελλειπτικής καμπύλης όταν ο δακτύλιος των ενδομορφισμών της είναι γνωστός. Σε αυτή την περίπτωση υπάρχει ένας εξαιρετικά ικανός αλγόριθμος.

Έστω p ένας μεγάλος πρώτος και $\mathcal{E}$ μία ελλειπτική καμπύλη επί του $\mathbb{F}_p$ της οποίας η εξίσωση είναι,

$$Y^2 = X^3 + aX + b$$

Έστω d να είναι η διακρίνουσα του δακτύλιου των ενδομορφισμών $\text{End}(\mathcal{E})$ της $\mathcal{E}$. Γνωρίζουμε ότι ο $\text{End}(\mathcal{E})$ είναι ισόμορφος με έναν υποδακτύλιο του $\mathbb{C}$,

$$\text{End}(\mathcal{E}) \cong \begin{cases} \frac{u+v\sqrt{d}}{2} & | \ u, v \in \mathbb{Z}, u \equiv v \pmod{2} \\ u + v\delta & | \ u, v \in \mathbb{Z} = \mathbb{Z} + \delta\mathbb{Z} \end{cases}$$

όπου,

$$\delta = \begin{cases} \frac{\sqrt{d}}{2}, & d = 2k, k \in \mathbb{Z} \\ \frac{1+\sqrt{d}}{2}, & d = 2k+1, k \in \mathbb{Z} \end{cases}$$

Ο ενδομορφισμός του Frobenius ϕ ικανοποιεί την,

$$\phi^2 - [t]\phi + [p] = 0$$

όπου ο t είναι ένας ακέραιος τέτοιος ώστε $t^2 < 4p$. Εάν ο p διαιρεί την d , τότε, σύμφωνα με την σχέση του Ορισμού 3.3.1 $\#\mathcal{E}(\mathbb{F}_p) = p+1-t$, προκύπτει ότι $t = 0$ και $\#\mathcal{E}(\mathbb{F}_p) = p+1$. Γι'αυτό τον λόγο από εδώ και στο εξής θα θεωρούμε ότι $p \nmid d$.

Για τον υπολογισμό του $\#\mathcal{E}(\mathbb{F}_p)$ αρκεί να υπολογίσουμε το ϕ . Θεωρούμε ότι,

$$p = \phi\bar{\phi}$$

Αυτό δείχνει ότι ο πρώτος p διαχωρίζεται μέσα στον $\text{End}(\mathcal{E})$ σε ένα γινόμενο δύο κύριων πρώτων ιδεωδών $\langle \phi \rangle$ και $\langle \bar{\phi} \rangle$ τάξης p .

Η ιδέα του αλγορίθμου είναι να υπολογίσει έναν γεννήτορα ενός πρώτου ιδεώδους $\mathfrak{p}$ το οποίο θα διαιρεί το p στο $\mathbb{Z}[\delta]$.

Εάν $d \neq -3$ ή $d \neq -4$, ένας γεννήτορας είναι μοναδικός, όσο αφορά το πρόσημο, οπότε βρίσκουμε το ϕ ή το συζυγές του, συνεπώς και το t . Αυτό αφήνει μόνο δύο ενδεχόμενα για το $\#\mathcal{E}(\mathbb{F}_p)$. Δεν είναι δύσκολο να αποφανθούμε για το ποιά από τις δύο τιμές είναι η σωστή. Είτε διαλέγουμε ένα τυχαίο σημείο $Q \in \mathcal{E}(\mathbb{F}_p)$ και ελέγχουμε αν $(p+1 \pm t)Q = O$, είτε την δράση του ϕ στα $3-torsion$ σημεία. Όταν $d = -3$ ή $d = -4$, τότε υπάρχουν αντίστοιχα 6 και 4 ενδεχόμενα για την τιμή του t . Όμως και αυτές οι περιπτώσεις μπορούν να εξεταστούν με τον ίδιο, αποτελεσματικό τρόπο.

Για τον υπολογισμό ενός γεννήτορα του πρώτου ιδεώδους $\mathfrak{p} \subset \mathbb{Z}[\delta]$, πρώτα υπολογίζουμε μία τετραγωνική ρίζα ϱ της $d \pmod{p}$. Αντικαθιστώντας το ϱ με το $p - \varrho$, εάν είναι απαραίτητο, μπορούμε να υποθέσουμε ότι $|\varrho| < p$ και $\varrho \equiv d \pmod{2}$. Τότε,

$$\mathfrak{p} = \left\langle \frac{\varrho + \sqrt{d}}{2}, p \right\rangle$$

είναι ένα πρώτο ιδεώδες τάξης p και διαιρεί το p . Επειδή το $\mathfrak{p}$ είναι κύριο, το ρητό ιδεώδες,

$$\mathbb{Z} + \frac{\varrho + \sqrt{d}}{2p} \mathbb{Z}$$

είναι ίσο με ένα ιδεώδες της μορφής $(\mathbb{Z} + \delta\mathbb{Z})\alpha$, για κάποιο $\alpha \in \mathbb{Z}[\delta]$.

Το επόμενο Θεώρημα δίνει έναν πιο απλό τρόπο υπολογισμού γεννήτορα του πρώτου ιδεώδους $\mathfrak{p}$.

Θεώρημα 4.3.1 (G.Cornacchia, 1908) Έστω $\mathfrak{D}$ να είναι μία μιγαδική τετραγωνική τάξη της διακρίνουσας d κι έστω p ένας πρώτος, διάφορος του 2, για τον οποίο η d να είναι ένα μη μηδενικό τετράγωνο modulo p . Έστω x ακέραιος με,

$$\begin{aligned} x^2 &= d \pmod{p} \\ x &= d \pmod{2} \\ 0 < x &< 2p \end{aligned}$$

Ορίζουμε την πεπερασμένη ακολουθία μη αρνητικών ακεραίων $x_0, x_1, \dots, x_t$ ως εξής,

$$\begin{aligned} x_0 &= 2p \\ x_1 &= x \\ x_{i+1} &= \text{rem}(x_{i-1}, x_i) \end{aligned}$$

όπου $\text{rem}(x_{i-1}, x_i)$ συμβολίζει το υπόλοιπο της διαίρεσης του x_{i-1} με τον x_i . Έστω ακόμη i να είναι ο ελάχιστος δείκτης για τον οποίο $x_i < 2\sqrt{p}$. Εάν η d διαιρεί το $x_i^2 - 4p$ και το πηλίκο είναι ένα τετράγωνο v^2 , τότε ο

$$\frac{x_i + v\sqrt{d}}{2}$$

είναι ένας γεννήτορας του πρώτου ιδεώδους $\mathfrak{p}$ της $\mathfrak{D}$ ο οποίος διαιρεί τον p . Εάν όχι, τότε τα πρώτα ιδεώδη $\mathfrak{p}$ της $\mathfrak{D}$ τα οποία διαιρούν τον p δεν είναι κύρια.

Απόδειξη. Βλέπε [4] σελ.33.

▲

Εάν η d είναι άρτια τότε οι αρχικές τιμές x_0, x_1 είναι επίσης άρτιοι, οπότε όλα τα x_i είναι άρτια, συνεπώς κάποιος θα μπορούσε να απλοποιήσει τον αλγόριθμο του Cornacchia διαιρώντας όλα τα x_i με το 2. Έστω δηλαδή ότι $x_0 = p, (x_1)^2 = \frac{d}{4} \pmod{p}$ και ο Ευκλείδειος αλγόριθμος να σταματάει όταν $x_i < \sqrt{p}$.

Χρησιμοποιώντας την μέθοδο που εξηγείται στο [7] και την γενική υπόθεση του Riemann¹, ο υπολογιστικός χρόνος είναι $O(\log p^4)$.

¹Πρωτάθηκε από τον B.Riemann το 1859 και είναι μια εικασία η οποία αφορά την κατανομή των ριζών της ζ συνάρτησης Riemann, $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$, $s \in \mathbb{C}, \text{Re}(s) > 1$, σύμφωνα με την οποία όλες οι μη τετρωμένες ρίζες της ζ έχουν πραγματικό μέρος ίσο με $\frac{1}{2}$.

Κεφάλαιο 5

Ο Αλγόριθμος του Schoof

Η γένεση ικανών αλγορίθμων απαρίθμησης σημείων καμπυλών προέρχεται από την εργασία του Schoof. Ο αλγόριθμός του, με χρόνο $O(\log^8 q)$, αποτελεί την βάση για οποιοδήποτε ικανό αλγόριθμο απαρίθμησης σημείων.

Σύμφωνα με το θεώρημα 4.1.1 του Hasse ισχύει,

$$\#\mathcal{E}(\mathbb{F}_q) = q + 1 - t, |t| \leq 2\sqrt{q}$$

Η κύρια ιδέα του αλγόριθμου είναι ο καθορισμός των t modulo πρώτων l , με $l \leq l_{max}$, όπου l_{max} είναι ο ελάχιστος πρώτος τέτοιος ώστε,

$$\prod_{2 \leq l \leq l_{max}} l > 4\sqrt{q}$$

Τότε εύκολα υπολογίζεται από το Κινέζικο Θεώρημα Υπολοίπων¹ η τιμή του t , οπότε καθορίζεται και η τάξη της ομάδας. Από το Θεώρημα Πρώτων Αριθμών² γνωρίζουμε ότι ο αριθμός των πρώτων που χρειαζόμαστε είναι $O(\frac{\log q}{\log \log q})$ και το μέγεθος του l_{max} είναι $O(\log q)$.

Μία σύντομη περιγραφή του αλγορίθμου θα ακολουθήσει, ενώ στην συνέχεια θα ασχοληθούμε λεπτομερέστερα με κάποιους υπολογισμούς.

Αρχικά παρατηρούμε ότι εύκολα βρίσκουμε την τιμή του t όταν $l = 2$ για κάθε μία περίπτωση σώματος επί του οποίου βρισκόμαστε.

Για την περίπτωση της περιττής χαρακτηριστικής έχουμε ότι $t = \#\mathcal{E}(\mathbb{F}_q) \bmod 2$, οπότε εύκολα προκύπτει ότι $\#\mathcal{E}(\mathbb{F}_q) = 1 \pmod{2} \Leftrightarrow$ το $X^3 + aX + b$ ανάγωγο επί

¹Το Κινέζικο Θεώρημα Υπολοίπων περιγράφεται σε ένα κινέζικο βιβλίο του τρίτου μ.Χ. αιώνα, σύμφωνα με το οποίο, έστω $n_1, n_2, \dots, n_k \in \mathbb{N}$ οι οποίοι είναι ανά δύο σχετικά πρώτοι. Τότε για $a_1, a_2, \dots, a_k \in \mathbb{N}$ υπάρχει $x \in \mathbb{Z}$ τέτοιος ώστε το σύστημα

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

έχει λύση.

²Έστω $\pi(x)$ να δηλώνει το πλήθος των πρώτων αριθμών οι οποίοι είναι μικρότεροι του x . Τότε σύμφωνα με το Θεώρημα Πρώτων Αριθμών έχουμε ότι $\pi(x) \sim \frac{x}{\ln x}$

του $\mathbb{F}_q$. Η τελευταία σχέση είναι ισοδύναμη με την $\gcd(X^3 + aX + b, X^q - X) = 1$. Για σώματα χαρακτηριστικής 2, επειδή η καμπύλη είναι non-supersingular, έχουμε ότι $t = 1 \pmod 2$.

Θα ασχοληθούμε τώρα με την περίπτωση όπου $l > 2$. Θυμόμαστε το ενδομορφισμό του Frobenius,

$$\phi : \begin{cases} \mathcal{E}(\overline{\mathbb{F}}_q) & \rightarrow \mathcal{E}(\overline{\mathbb{F}}_q) \\ (x, y) & \mapsto (x^q, y^q) \\ O & \mapsto O \end{cases}$$

όπου κάθε $P \in \mathcal{E}(\mathbb{F}_q)$ ικανοποιεί την εξίσωση,

$$\phi^2 - [t]\phi + [q] = 0 \quad (5.1)$$

Την παραπάνω εξίσωση θα την χρησιμοποιήσουμε για τα σημεία στο $\mathcal{E}[l]^* = \mathcal{E}[l] \setminus O$.

Έστω,

$$q_l = q(\text{mod } l)$$

και

$$t_l = t(\text{mod } l)$$

όπου οι ελάχιστοι μη αρνητικοί αντιπρόσωποι της κλάσης υπολοίπων είναι ο q_l και ο t_l . Εάν κάποια τιμή του $\tau \in \{0, 1, \dots, l-1\}$ βρεθεί έτσι ώστε για κάποιο σημείο $P = (x, y) \in \mathcal{E}[l]^*$ να έχουμε,

$$(x^{q^2}, y^{q^2}) + [q_l](x, y) = [\tau](x^q, y^q) \quad (5.2)$$

τότε προκύπτει ότι $\tau = t_l$, δηλαδή βρίσκουμε το $t \pmod l$. Η πρόσθεση στην παραπάνω εξίσωση είναι η πρόσθεση με τον τρόπο που ορίστηκε για την καμπύλη. Το τ το οποίο ικανοποιεί την εξίσωση (5.2) είναι μοναδικό αφού το l είναι πρώτος και $P \neq O$.

Για τον καθορισμό της τιμής του τ , ισχυριζόμαστε προς το παρόν ότι όλες οι τιμές του $\tau \in \{0, 1, \dots, l-1\}$ δοκιμάζονται. Πρώτα υπολογίζονται οι x -συντεταγμένες και στα δύο μέλη της εξίσωσης (5.2), όπου υπάρχουν στα $[q_l](x, y)$, $[\tau](x^q, y^q)$, για τον δοσμένο πρώτο l και την τιμή του τ το οποίο εξετάζουμε, τα οποία είναι ρητές συναρτήσεις των x, y , οι οποίες περιέχουν τα πολυώνυμα διαίρεσης, τα οποία έχουμε δει στην παράγραφο 3.3.4. Στην συνέχεια με την πράξη της πρόσθεσης, όπως ορίζεται για σημεία ελλειπτικών καμπυλών στην παράγραφο 3.2, υπολογίζουμε την x -συντεταγμένη του αθροίσματος,

$$(x^{q^2}, y^{q^2}) + [q_l](x, y)$$

Με απαλοιφή παρανομαστών κι εάν είναι απαραίτητο μειώνοντας όσες δυνάμεις του y είναι μεγαλύτερες της μονάδας modulo την εξίσωση της καμπύλης είτε $y^2 = x^3 + ax + b$ είτε $y^2 = xy + x^3 + a_6$, προκύπτει μία εξίσωση της μορφής,

$$a(x) - yb(x) = 0 \Rightarrow y = \frac{a(x)}{b(x)}$$

Η εξίσωση της καμπύλης με βάση κάποια από τις παραπάνω δύο εξισώσεις, έχει σαν μεταβλητή πλέον μόνο το x , οπότε γράφεται ως,

$$h_X(x) = 0$$

Μία σημαντική παρατήρηση στο καθορισμό της πολυπλοκότητας της διαδικασίας είναι ότι αφού το σημείο P , το οποίο ικανοποιεί την Εξίσωση (5.2), ανήκει στο $\mathcal{E}[l]^*$, όλοι οι πολυωνυμικοί υπολογισμοί γίνονται modulo το πολυώνυμο διαίρεσης f_l (πρβ.Ορισμό 3.3.9), το οποίο έχει βαθμό $O(l^2)$. Ιδιαίτερα, τα πολυώνυμα $x^{q^2}, y^{q^2}, x^q, y^q$ ανάγονται, χρησιμοποιώντας το f_l και την εξίσωση της ελλειπτικής καμπύλης, από βαθμό εκθετικό ως προς το $\log q$, σε βαθμό πολυωνυμικό. Συνεπώς ο βαθμός του $h_X(x)$ είναι $O(l^2)$.

Για να ελέγξουμε εάν η $h_X(x) = 0$ έχει λύση για την x -συντεταγμένη του σημείου που ανήκει στο $\mathcal{E}[l]^*$ (πρβ.Λήμμα 3.3.2), υπολογίζουμε τον μέγιστο κοινό διαιρέτη των h_X, f_l . Εάν,

$$\gcd(h_X, f_l) = 1$$

τότε δεν υπάρχει λύση στο $\mathcal{E}[l]^*$ η οποία να ικανοποιεί την Εξίσωση 5.2, οπότε δοκιμάζουμε την επόμενη τιμή του τ . Εάν,

$$\gcd(h_X, f_l) \neq 1$$

τότε υπάρχει σημείο στο $\mathcal{E}[l]^*$ τέτοιο ώστε,

$$(x^{q^2}, y^{q^2}) + [q_l](x, y) = \pm[\tau](x^q, y^q). \quad (5.3)$$

Το πρόσημο του σημείου του δεξιού μέλους της παραπάνω εξίσωσης δεν είναι προκαθορισμένο, διότι το πρόσημο της x -συντεταγμένης είναι το ίδιο για κάθε πρόσημο. Για να το καθορίσουμε, ισχυριζόμαστε αρχικά ότι στην Εξίσωση (5.3) είναι $+$. Υπολογίζουμε την y -συντεταγμένη και στα δύο μέλη της εξίσωσης, όπου όπως με την x -συντεταγμένη, μετά από την απαλοιφή παρανομαστών και την αντικατάσταση της y μεταβλητής, προκύπτει μια εξίσωση της μορφής,

$$h_Y(x) = 0$$

όπου το h_Y έχει αναχθεί στον βαθμό $O(l^2)$. Όμοια, εάν

$$\gcd(h_Y, f_l) \neq 1$$

τότε υπάρχει ένα σημείο που ικανοποιεί την Εξίσωση 5.3 και το πρόσημο είναι $+$. Εάν,

$$\gcd(h_Y, f_l) = 1$$

τότε το πρόσημο είναι $-$.

Παρατηρούμε ότι για δοσμένο τ η διαδικασία στην πραγματικότητα ελέγχει τα $\pm\tau$, οπότε είναι επαρκές το τ να ανήκει στο $0 \leq \tau \leq \frac{l-2}{2}$. Ακόμη, αν το $\tau = 0$ θα δούμε στην συνέχεια πώς αντιμετωπίζουμε αυτή την κατάσταση.

Γενικά τα σημεία του $\mathcal{E}[l]$ γνωρίζουμε ότι έχουν συντεταγμένες σε μία επέκταση σώματος του $\mathbb{F}_q$. Ο ακριβής υπολογισμός αυτών των σημείων, ο οποίος γενικά είναι πολύ δύσκολος, απλουστεύεται σημαντικά με τον υπολογισμό του $\gcd$.

Για τον υπολογισμό της πολυπλοκότητας έχουμε πρώτα να συμπεριλάβουμε τον υπολογισμό των δυνάμεων x^q, x^{p^2} κ.τ.λ. στον δακτύλιο,

$$\mathbb{F}_q[x, y]/(f_l, Y^2 - X^3 - aX - b)$$

και μετά l φορές την πρόσθεση του σημείου (x^q, y^q) , το οποίο ανάγεται σε μερικές προσθέσεις και πολλαπλασιασμούς στον ίδιο δακτύλιο. Επειδή τα στοιχεία του δακτυλίου έχουν μέγεθος $l^2 \log q$, η τάξη της δουλειάς που απαιτείται για τον υπολογισμό είναι $O(\log q (l^2 \log q)^2)$ και $O(l(l^2 \log q)^2)$ αντίστοιχα. Υποθέτουμε ότι ο συνήθης πολλαπλασιασμός μεταξύ δύο στοιχείων μήκους n λαμβάνει χρόνο $O(n^2)$. Σκεπτόμενοι ότι $l = O(\log q)$ κι ότι έχουμε να κάνουμε αυτόν τον υπολογισμό για κάθε l , συμπεραίνουμε ότι ο υπολογιστικός χρόνος είναι

$$O(\log^8 q)$$

Συνεπώς, αυτός είναι ένας ντετερμινιστικός πολυωνυμικού χρόνου αλγόριθμος, δηλαδή είναι ασυμπτωτικά πολύ γρήγορος. Στην πράξη όμως, δυστυχώς, συμπεριφέρεται πάρα πολύ αργά λόγω των πολύ μεγάλων βαθμών των πολυωνύμων διαίρεσης.

Κεφάλαιο 6

Η Υλοποίηση του Αλγορίθμου του Schoof στο Maple 13

6.1 Ο Κώδικας

```
1. mmP := proc(a,b,k,x,y,q)
2. ...local mm,m,p3,Y:
3. ...mm := k-1:
4. ...if mm = -1 then p3 := [0, 0] else
5. ....if mm = 0 then p3 := [x, y] else
6. ....Y[0] := 0:
7. ....Y[1] := 1:
8. ....Y[2] := mod(2*y, q):
9. ....if mod (Y[2] ,q)<>0 then
10. ....Y[3] := mod(3*x^{4}+6*a*x^{2} + 12*b*x-a^{2},
11. ....q):
12. ....Y[4] := mod(4*y*(x^6+5*a*x^4+20*b*x^3-5*a*x^2
13. ....-4*a
14. ....*b*x-8*b^2-a^3), q):
15. ....for m from 2 to mm do
16. ....Y[2*m+1] := mod(Y[m+2]*Y[m]^3-Y[m-1]*Y[m+1
17. ....]^3,}q):
```

```

18. ....Y[2*m] := mod(mod((mod ((Y[m+2]*Y[m-1]^2-Y
19. ....[m-2]*Y[m+1]^2)*Y[m], q))/(2*y), q), q):
20. ....end do:
21. ....if Y[m] <> 0 then
22. ....mP := mod((mod(x-Y[m-1]*Y[m+1], q))/(mod(Y
23. ....[m]^2, q)), q), mod((mod(Y[m+2]*Y[m-1]^2-Y
24. ....[m-2]*Y[m+1]^2, q))/(mod(4*y*Y[m]^3, q)),q
25. ....):
26. ....else
27. ....p3 := [0, 0]
28. ....fi:
29. ....else if mod(k, 2) = 1 then p3:=x,y]: else p3
30. ...., :=[0,0]: fi:
31. ....fi:
32. ....fi:
33. ...fi:
34. end proc:
35.
36. addElliptic:=proc(p1,p2,a,b,n)
37. ...local m,x3,y3,p3:
38. ...if irem(p1[2], n) = 0 then p1[2] = 0 end if:
39. ...if p1=[0 ,0] then p3:=p2:
40. ...else if p2=[0 ,0] then p3:=p1:
41. ....else if (p1[1]=p2[1] and (( p1[2]=0) or (p1[2]<>
42. ....p2[2]))) then p3:=p2:
43. ....else if p1=p2 then
44. ....m :=mod((3*p1[1]^2+a)/(2*p1[2]),n):
45. ....x3 := mod(m^2-p1[1]-p2[1], n):
46. ....y3 := mod(m*(p1[1]-x3)-p1[2], n):
47. ....p3 := [x3, y3]}

```

```

48. ....else }
49. ....m := mod((p2[2]-p1[2])/(mod(p2[1]-
50. ....p1[1],n)), n):
51. ....x3 := mod(m^2-p1[1]-p2[1], n):
52. ....y3 := mod(m*(p1[1]-x3)-p1[2], n):
53. ....p3 := [x3, y3]}
54. ....fi:
55. ....fi:
56. ....fi:
57. ...fi:
58. end proc:
59.
60. evalf(4*sqrt(127)) = 45.07771068
61. 2*3*5 = 30
62. l_max:= 7
63.
64. a := 3;
65. b := 1;
66. q := 127;
67. Sys[3] := {};
68. kk := 1;
69. while kk < 127 do
70. ...for x from 0 to 126 while Sys[3] = {} do
71. ....findYValue := proc (x, a, b, q)
72. ....numtheory[msqrt](x^3+a*x+b, 127):
73. ....end proc;
74. ....W := findYValue(x, a, b, q);
75. ....if W <> FAIL then
76. ....y := W;
77. ....x1 := x;

```

```

78. ....y1 := y;
79. ....a := 3;
80. ....b := 1;
81. ....q := 127;
82. ....l := 3;
83. ....q[1] := mod(q, 1);
84. ....t[1] := mod(t, 1);
85. ....if mmP(3, 1, l, x1, y1, 127) = [0, 0] then
86. ....for Taf from 0 to (l-1)/2 do
87. ....P1 := [mod(x1^(127^2), 127), mod(y1^(127^2),
88. .... 127)];
89. ....P2 := mmP(3, 1, q[1], x1, y1);
90. ....LLeg := addElliptic(P1, P2, 3, 1, 127);
91. ....RLeg := mmP(3, 1, Taf, mod(x1^127, 127), mod
92. ....(y1^127, 127), 127);
93. ....AllLeg := addElliptic(LLeg, RLeg, 3, 1, 127);
94. ....if AllLeg <> LLeg and AllLeg <> RLeg then
95. ....if LLeg = RLeg then
96. ....t[1] := Taf;
97. ....print(LLeg, RLeg, AllLeg);
98. ....Sys[3] := [t[1], 1];
99. ....print([x1, y1]);
100. ....print(Sys[3]);
101. ....break:
102. ....else
103. ....if AllLeg = [0, 0] then
104. ....t[1] := -Taf;
105. ....print(LLeg,
106. ....RLeg, AllLeg);
107. ....Sys[3] := [t[1], 1];

```

```

108. ....print([x1, y1]);
109. ....print(Sys[3]);
110. ....break:
111. ....fi:
112. ....fi:
113. ....fi:
114. ....end do:
115. ....fi:
116. ....fi:
117. ...end do;
118. ...kk := kk+1;
119. end do:
120.
121. a := 3;
122. b := 1;
123. q := 127;
124. Sys[5] := {};
125. kk := 1;
126. while kk < 127 do
127. ...for x from 0 to 126 while Sys[5] = {} do
128. ....findYValue := proc (x, a, b, q)
129. ....numtheory[msqrt](x^3+a*x+b, 127):
130. ....end proc;
131. ....W := findYValue(x, a, b, q);
132. ....if W <> FAIL then
133. ....y := W;
134. ....x1 := x;
135. ....y1 := y;
136. ....a := 3;
137. ....b := 1;

```

```

138. ....q := 127;
139. ....l := 5;
140. ....q[1] := mod(q, 1);
141. ....t[1] := mod(t, 1);
142. ....if mmP(3, 1, l, x1, y1, 127) = [0, 0] then
143. ....for Taf from 0 to (l-1)/2 do
144. ....P1 := [mod(x1^(127^2), 127), mod(y1^(127^2),
145. .... 127)];
146. ....P2 := mmP(3, 1, q[1], x1, y1);
147. ....LLeg := addElliptic(P1, P2, 3, 1, 127);
148. ....RLeg := mmP(3, 1, Taf, mod(x1^127, 127), mod
149. ....(y1^127, 127), 127);
150. ....AllLeg := addElliptic(LLeg, RLeg, 3, 1, 127);
151. ....if AllLeg <> LLeg and AllLeg <> RLeg then
152. ....if LLeg = RLeg then
153. ....t[1] := Taf;
154. ....print(LLeg, RLeg, AllLeg);
155. ....Sys[5] := [t[1], 1];
156. ....print([x1, y1]);
157. ....print(Sys[5]);
158. ....break:
159. ....else
160. ....if AllLeg = [0, 0] then
161. ....t[1] := -Taf;
162. ....print(LLeg,
163. ....RLeg, AllLeg);
164. ....Sys[5] := [t[1], 1];
165. ....print([x1, y1]);
166. ....print(Sys[5]);
167. ....break:

```

```
168. ....fi:
169. ....fi:
170. ....fi:
171. ....end do:
172. ....fi:
173. ....fi:
174. ...end do;
175. ...kk := kk+1;
176. end do:
177.
178. a := 3;
179. b := 1;
180. q := 127;
181. Sys[7] := {};
182. kk := 1;
183. while kk < 127 do
184. ...for x from 0 to 126 while Sys[7] = {} do
185. ....findYValue := proc (x, a, b, q)
186. ....numtheory[msqrt](x^3+a*x+b, 127):
187. ....end proc;
188. ....W := findYValue(x, a, b, q);
189. ....if W <> FAIL then
190. ....y := W;
191. ....x1 := x;
192. ....y1 := y;
193. ....a := 3;
194. ....b := 1;
195. ....q := 127;
196. ....l := 7;
197. ....q[l] := mod(q, 1);
```

```

198. ....t[1] := mod(t, 1);
199. ....if mmP(3, 1, 1, x1, y1, 127) = [0, 0] then
200. ....for Taf from 0 to (1-1)/2 do
201. ....P1 := [mod(x1^(127^2), 127), mod(y1^(127^2),
202. .... 127)];
203. ....P2 := mmP(3, 1, q[1], x1, y1);
204. ....LLeg := addElliptic(P1, P2, 3, 1, 127);
205. ....RLeg := mmP(3, 1, Taf, mod(x1^127, 127), mod
206. ....(y1^127, 127), 127);
207. ....AllLeg := addElliptic(LLeg, RLeg, 3, 1, 127);
208. ....if AllLeg <> LLeg and AllLeg <> RLeg then
209. ....if LLeg = RLeg then
210. ....t[1] := Taf;
211. ....print(LLeg, RLeg, AllLeg);
212. ....Sys[7] := [t[1], 1];
213. ....print([x1, y1]);
214. ....print(Sys[7]);
215. ....break:
216. ....else
217. ....if AllLeg = [0, 0] then
218. ....t[1] := -Taf;
219. ....print(LLeg,
220. ....RLeg, AllLeg);
221. ....Sys[7] := [t[1], 1];
222. ....print([x1, y1]);
223. ....print(Sys[7]);
224. ....break:
225. ....fi:
226. ....fi:
227. ....fi:

```

```

228. ....end do:
229. ....fi:
230. ....fi:
231. ...end do;
232. ...kk := kk+1:
233. end do:
234.
235. S := union(union({Sys[3]}, {Sys[5]}), {Sys[7]})
236. t := chrem([S[1][1], S[2][1]], [S[1][2], S[2][2]])
237. cardinalityOf := 127+1-t = 126

```

Με τις παρακάτω εντολές στο *SAGE* επαληθεύουμε ότι το cardinality της ελλειπτικής καμπύλης $y^2 = x^3 + 3 * x + 1$ στο $\mathbb{F}_p$ είναι 126.

```
sage: E = EllipticCurve(GF(127),[3,1])
```

```
sage: E
```

```
Elliptic Curve defined by y^2 = x^3 + 3*x + 1 over Finite Field
```

```
of size 127
```

```
sage: E.cardinality()
```

```
126
```

6.2 Ανάλυση Κώδικα

Γραμμή 1-34

Ορισμός της διαδικασίας mmP πολλαπλασιασμού ενός σημείου $P = (x, y)$ της ελλειπτικής καμπύλης $y^2 = x^3 + a * x + b$ στο πεπερασμένο σώμα $\mathbb{F}_q$, με έναν ακέραιο αριθμό k , σύμφωνα με την παράγραφο 3.2.2.

Γραμμή 2

Ορίζουμε τις τοπικές μεταβλητές.

Γραμμή 4

$0 * P = 0$

Γραμμή 5

$1 * P = P$

Γραμμή 6-20

Ορίζουμε τα πολυώνυμα διαίρεσης.

Γραμμή 9

Ελέγχουμε εάν η τάξη ενός σημείου δεν είναι 2.

Γραμμή 21-27

Σύμφωνα με τον Ορισμό 3.3.10 βρίσκουμε το ψ_m .

Γραμμή 29

Εξετάζουμε την περίπτωση η τάξη ενός σημείου να είναι 2.

Γραμμή 36-58

Ορισμός της διαδικασίας addElliptic πρόσθεσης δύο σημείων $p1, p2$ της ελλειπτικής καμπύλης $y^2 = x^3 + a * x + b$ στο πεπερασμένο σώμα $\mathbb{F}_n$ σύμφωνα με το Λήμμα 3.2.2.

Γραμμή 37

Ορίζουμε τις τοπικές μεταβλητές.

Γραμμή 60

Υπολογίζουμε το $4 * \sqrt{127}$ ώστε να βρούμε τον l_{max} .

Γραμμή 62

$l_{max} = 7$.

Γραμμή 64-119

Για $l = 3$ ελέγχουμε εάν υπάρχει τ ώστε $\tau = t(mod 3)$, οπότε $Sys_3 = \tau, 3$.

Γραμμή 121-176

Για $l = 5$ ελέγχουμε εάν υπάρχει τ ώστε $\tau = t(\text{mod}5)$, οπότε $Sys_5 = \tau, 5$.

Γραμμή 178-233

Για $l = 7$ ελέγχουμε εάν υπάρχει τ ώστε $\tau = t(\text{mod}7)$, οπότε $Sys_7 = \tau, 7$.

Γραμμή 235

$S = Sys_{357}$.

Γραμμή 236

Εφαρμόζουμε το Κινέζικο Θεώρημα Υπολοίπων στα στοιχεία του S και βρίσκουμε το ίχνος t του Frobenius.

Γραμμή 237

Από τον Ορισμό 3.3.1 βρίσκουμε το cardinality της ελλειπτικής καμπύλης $y^2 = x^3 + 3 * x + 1$ στο $\mathbb{GF}_{127}$.

Γραμμή 67

Ορίζουμε το $Sys_3 = \emptyset$.

Γραμμή 68

Μετρητής.

Γραμμή 69

Συνθήκη με την οποία ο αλγόριθμος σταματάει αφού έχει διατρέξει όλα τα σημεία της ελλειπτικής καμπύλης και το σύνολο Sys_3 παραμένει κενό. Δηλαδή δεν υπάρχουν 3-torsion σημεία της καμπύλης ώστε να ικανοποιούνται οι συνθήκες για την εύρεση του τ .

Γραμμή 70

Διατρέχει όλα τα πιθανά σημεία της ελλειπτικής καμπύλης εφόσον το $Sys_3 = \emptyset$. Δηλαδή, εάν $Sys_3 \neq \emptyset$, που σημαίνει ότι βρέθηκε τ ώστε $\tau = t(\text{mod}3)$, τότε σταματάει.

Γραμμή 71-73

Ορισμός της διαδικασίας findYValue η οποία επιστρέφει την τιμή της τεταγμένης ενός σημείου της ελλειπτικής καμπύλης, εάν για συγκεκριμένη τιμή της τεταγμένης αυτή υπάρχει. Διαφορετικά επιστρέφει ΦΑΙΛ.

Γραμμή 74

Το W παίρνει την τιμή της διαδικασίας findYValue.

Γραμμή 75

Εάν το σημείο (x, y) ανήκει στην ελλειπτική καμπύλη, τότε

Γραμμή 77-78

Αρχικοποιούμε τις τιμές των $x1, y1$.

Γραμμή 79-81

Ορίζουμε την ελλειπτική καμπύλη και το $\mathbb{F}_q$.

Γραμμή 82

Για την τιμή $l = 3$ έχουμε,

Γραμμή 83

$$q_3 = 127(\text{mod}3)$$

Γραμμή 84

$$t_3 = t(\text{mod}3)$$

Γραμμή 85

Αν το σημείο (x_1, y_1) ανήκει στην ελλειπτική καμπύλη τότε,

Γραμμή 86

Για $0 \leq \tau \leq \frac{l-1}{2}$ έχουμε,

Γραμμή 87-89

Ορίζουμε P_1, P_2 να είναι ο πρώτος και ο δεύτερος προσθεταίος του αριστερού μέλους της Εξίσωσης 5.2.

Γραμμή 90

LLeg είναι το αριστερό μέλος της Εξίσωσης 5.2.

Γραμμή 91-92

RLeg είναι το δεξί μέλος της Εξίσωσης 5.2.

Γραμμή 93

ΑλλΛεγ είναι το άθροισμα του αριστερού και του δεξιού μέλους της Εξίσωσης 5.2.

Γραμμή 94-113

Εξετάζουμε εάν LLeg=RLeg οπότε βρίσκουμε το $\tau = t(\text{mod}3)$, διαφορετικά εξετάζουμε εάν AllLeg=0 οπότε βρίσκουμε το $\tau = t(\text{mod}3)$. Συνεπώς $Sys_3 = \{\tau, 3\}$.

Γραμμή 118

Ο μετρητής αυξάνεται κατά 1.

Γραμμή 119

Τέλος ελέγχου για την τιμή $l = 3$.

Βιβλιογραφία

- [1] Σ.Ανδρεαδάκης - Εισαγωγή Στην Άλγεβρα, Συμμετρία 1993
- [2] Α.Παπαϊωάννου, Χ.Κουκουβίνος - Κρυπτογραφία, ΕΜΠ 2007
- [3] I.Blake, G.Seroyssi, N.Smart - Elliptic Curves In Cryptography, London Mathematical Society, Cambridge University Press 2004
- [4] G.Cornacchia - Su Di Un Metodo Per La Risoluzione In Numeri Interi Dell'Equazione $\sum_{h=0}^n C_h x^{n-h} y^h = P$, Giornale di Mat. di Battaglini 2006
- [5] S.Dasgupta, C.H.Papadimitriou, U.V.Vazirani - Algorithms, McGraw-Hill 2006
- [6] R.Schoof - Counting Points On Elliptic Curves Over Finite Fields, Journal de Theone des Nombres de Bordeaux 7 1995, p.219 – 254
- [7] D.Shanks - Five Number Theoretical Algorithms, Proc.2nd Manitoba Conference On Numerical Math.1972, p.51 – 70
- [8] J.Silverman - The Arithmetic Of Elliptic Curves, Springer-Verlag 1986
- [9] W.Stein - Elementary Number Theory, Springer 2009
- [10] I.N.Stewart, D.O.Tall - Algebraic Number Theory, Chapman and Hall 1979
- [11] I.N.Stewart - Galois Theory, Chapman and Hall 2004