Τμήμα Μαθηματικών,
Πανεπιστήμιο Κρήτης

Αλγεβρικές καμπύλες, εικασία του Riemann και κωδικοποίηση

Μάριος Μαγιολαδίτης

Διπλωματική Εργασία

Ηράκλειο, 2001

Η διπλωματική αυτή εργασία κατατέθηκε στο Τμήμα Μαθηματικών του Πανεπιστημίου Κρήτης το Νοέμβρη του 2001. Επιβλέπων ήταν ο καθηγητής Γιάννης Α. Αντωνιάδης.

Την επιτροπή αξιολόγησης αποτέλεσαν οι: Γιάννης Αντωνιάδης, Αλέξης Κουβιδάκης, Αριστείδης Κοντογιώργης

Περιεχόμενα

Εισαγωγή

Η εργασία έχει σαν σκοπό να δείξει την χρησιμότητα της μελέτης των αλγεβρικών καμπυλών πάνω σε πεπερασμένα σώματα, τόσο σε προβλήματα Θεωρίας Αριθμών όσο και στην Κωδικοποίηση.

Στο πρώτο κεφάλαιο μελετώνται βασικές ιδιότητες της θεωρίας, όπως για παράδειγμα τα σημεία τομής αλγεβρικών καμπυλών και η πολλαπλότητά τους. Στη συνέχεια ορίζονται οι ελλειπτικές καμπύλες στο σώμα **Q** των ρητών αριθμών και διατυπώνονται σημαντικά θεωρήματα που αφορούν στην ομάδα των ρητών σημείων αυτών.

Στο δεύτερο κεφάλαιο μελετώνται ελλειπτικές καμπύλες πάνω σε πεπερασμένα σώματα της μορφής $\mathbf{F}_q$ και ορίζεται η ομάδα $E(\mathbf{F}_q)$ των ρητών τους σημείων. Στη συνέχεια δείχνεται πως αν έχουμε μια ελλειπτική καμπύλη Ε ορισμένη στο **Q**, με ακέραιους συντελεστές και την ανάγουμε mod p για κατάλληλους πρώτους p τότε η ομάδα Φ των ρητών σημείων πεπερασμένης τάξης της Ε εμφυτεύεται ισόμορφα σε υποομάδα της $E(\mathbf{F}_p)$. Η μελέτη της $E(\mathbf{F}_p)$ μας δίνει χρήσιμες πληροφορίες και για την Φ. Για να δώσουμε ένα άνω φράγμα για το πλήθος των ρητών σημείων μιας αλγεβρικής καμπύλης ορισμένης πάνω στο $\mathbf{F}_q$ διατυπώνουμε την εικασία του Riemann για καμπύλες γένους g πάνω από το $\mathbf{F}_q$ ενώ παρουσιάζεται αναλυτικά η απόδειξη του Manin στο θεώρημα του Hasse το οποίο αποτελεί ειδική περίπτωση της εικασίας του Riemann. Επίσης, εξηγείται η σχέση της με την περίφημη εικασία του Riemann και την ζ-ήτα συνάρτηση. Το κεφάλαιο κλείνει με μια επιστολή του κύριου Roquette στον κύριο Lemmermeyer η οποία αποδεικνύει ότι η απόδειξη του Manin και η απόδειξη του Hasse είναι, κατ' ουσία, οι ίδιες.

Στο τρίτο κεφάλαιο διατυπώνονται βασικές έννοιες της θεωρίας κωδικοποίησης και δίνονται κάποια φράγματα για το πόσο καλούς κώδικες μπορούμε να κατασκευάσουμε. Στη συνέχεια δίνονται κάποια επιπλέον στοιχεία της θεωρίας αλγεβρικών καμπυλών, όπως π.χ. η έννοια του διαιρέτη μιας καμπύλης, και ορίζονται οι γεωμετρικοί Reed-Solomon κώδικες. Τέλος, δείχνεται ότι αν θεωρήσουμε αλγεβρικές καμπύλες με μεγάλο πλήθος ρητών σημείων μπορούμε να κατασκευάσουμε καλούς κώδικες. Η εργασία κλείνει με την αναλυτική παρουσίαση δύο αλγεβρογεωμετρικών κωδίκων.

Θα ήθελα να ευχαριστήσω θερμά τον καθηγητή Γιάννη Α. Αντωνιάδη για την πολύτιμη βοήθειά του. Με βοήθησε να γνωρίσω έναν πολύ όμορφο κλάδο των Μαθηματικών και χάρη στην επιμονή του ολοκληρώθηκε αυτή η εργασία.

Θερμές ευχαριστίες επίσης χρωστώ στον καθηγητή κ. Peter Roquette (Heidelberg) που επέτρεψε να συμπεριλάβω την επιστολή του στην εργασία μου καθώς και τον καθηγητή κ. Ruud Pellikaan (Eindhoven) για τη βοήθειά του σε κάποια προβλήματα κωδικοποίησης.

Κεφάλαιο I

Στοιχεία Θεωρίας Αλγεβρικών Καμπυλών

Σε αυτό το κεφάλαιο θα αναφέρουμε περιληπτικά κάποια στοιχεία της θεωρίας αλγεβρικών καμπυλών. Για περισσότερες πληροφορίες παραπέμπουμε τον ενδιαφερόμενο αναγνώστη στα [A1] και [S1].

1. Προβολικό επίπεδο

Επεκτείνουμε το αφινικό (x, y)-επίπεδο με την **επ' άπειρο ευθεία** και σχηματίζουμε το προβολικό επίπεδο. Κάθε ευθεία του αφινικού επιπέδου συμπληρώνεται σε μία ευθεία του προβολικού επιπέδου με την πρόσθεση ενός επ' άπειρον σημείου, του σημείου τομής της δοσμένης ευθείας με την επ' άπειρον ευθεία. Κάθε σημείο της επ' άπειρο ευθείας αντιστοιχεί σε μία οικογένεια παραλλήλων ευθειών και είναι ακριβώς τα ζευγάρια εκείνα των ευθειών τα οποία είναι παράλληλα στον αφινικό μας χώρο, τα οποία τέμνονται επί της επ' άπειρο ευθείας.

Μία βασική γεωμετρική σχέση ανάμεσα στα σημεία και τις ευθείες του προβολικού επιπέδου αποτελεί η παρακάτω ιδιότητα.

(P) Δύο διακεκριμένα σημεία ορίζουν μοναδική ευθεία και δύο διακεκριμένες ευθείες τέμνονται σε ακριβώς ένα σημείο.

Ας ρίξουμε μια ματιά στην αναλυτική περιγραφή του προβολικού επιπέδου.

Θεωρούμε τον τρισδιάστατο χώρο με συντεταγμένες (w, x, y). Μία ευθεία γραμμή που περνάει από την αρχή των αξόνων (0, 0, 0) ορίζεται μονοσήμαντα από οποιοδήποτε σημείο (w, x, y) διάφορο του (0, 0, 0). Επιπλέον δύο σημεία (w, x, y) και (w', x', y') ορίζουν την ίδια ευθεία που περνάει από την αρχή (0, 0, 0) τότε και μόνο τότε όταν υπάρχει μια σταθερά α, $\alpha \neq 0$, τέτοια ώστε

$$w' = \alpha w,\ x' = \alpha x \text{ και } y' = \alpha y \qquad (1.1.1)$$

Έστω P_2 το σύνολο όλων των ευθειών που περνούν από την αρχή (0, 0, 0). Τα σημεία του P_2 μπορούν να παραμετρικοποιηθούν από τις κλάσεις ισοδυναμίας των τριάδων (w, x, y) μέσω της σχέσης ισοδυναμίας (1.1.1) (λέγονται ομογενείς συντεταγμένες). Την κλάση ισοδυναμίας του σημείου (w, x, y) την συμβολίζουμε με [w, x, y].

Το ερώτημα που προκύπτει είναι:
Από ποιο σύνολο (σώμα) παίρνουμε τις συντεταγμένες w, x, y;

(α') Στην κλασική αναλυτική γεωμετρία είναι το σώμα **R** των πραγματικών αριθμών.

(β') Σε προβλήματα ρητών σημείων είναι το σώμα **Q** των ρητών αριθμών.

(γ') Στην κλασική αλγεβρική γεωμετρία είναι το **C** των μιγαδικών αριθμών.

Τα w, x, y θα είναι στοιχεία ενός σώματος k και το προβολικό επίπεδο

$$P_2(k):=\{[w, x, y] \mid w, x, y \in k \text{ όχι όλα μηδέν}\}.$$

Εμφυτεύουμε το αφινικό (x, y)-επίπεδο k^2 στο προβολικό $P_2(k)$ ως εξής:

$$(x, y) \rightarrow [1, x, y].$$

Κάθε σημείο $[w, x, y] \in P_2(k)$ με $w \neq 0$ παριστά το σημείο $\left(\frac{x}{w}, \frac{y}{w}\right)$ του k^2 διότι

$$[w, x, y] = [1, \frac{x}{w}, \frac{y}{w}] \text{ στο } P_2(k).$$

Ορίζουμε **ευθεία** στο $P_2(k)$

$$E = \{[w, x, y] \mid aw + bx + cy = 0, \text{ όπου } (a, b, c) \neq (0, 0, 0)\}.$$

Για a = 1, b = 0, c = 0 έχουμε w = 0 την **επ' άπειρο** ευθεία, η οποία αποτελείται από όλα τα σημεία της μορφής [0, x, y].

Για w = 1 παίρνουμε a + bx +cy = 0 που είναι μία συνηθισμένη αφινική ευθεία όταν $bc \neq 0$.

Δύο σύνολα συντελεστών a, b, c και a′, b′, c′ ορίζουν την <u>ίδια</u> ευθεία τότε και μόνο τότε όταν υπάρχει κάποιο στοιχείο $u \in k$, $u \neq 0$ τέτοιο ώστε $a' = ua$, $b' = ub$, $c' = uc$.

2. Επίπεδες αλγεβρικές καμπύλες

Μέχρι στιγμής μελετήσαμε τις ευθείες στον προβολικό χώρο και είδαμε ότι έχουν εξίσωση l(w, x, y) = 0 όπου l(w, x, y) ομογενές πολυώνυμο πρώτου βαθμού.

Μια **επίπεδη αλγεβρική καμπύλη** C_f **βαθμού** d είναι το σύνολο όλων των σημείων $[w, x, y] \in P_2(k)$ τέτοιων ώστε f(w, x, y) = 0 όπου το f είναι ομογενές πολυώνυμο βαθμού d με συντελεστές από το σώμα k.

Αφού για κάθε ομογενές πολυώνυμο βαθμού d ισχύει $f(\lambda w, \lambda x, \lambda y) = \lambda^d (w, x, y)$, αν για κάποιο αντιπρόσωπο (w, x, y) της κλάσης [w, x, y] ισχύει f(w, x, y) = 0, το ίδιο θα ισχύει και για κάθε στοιχείο άλλο της κλάσης. (Δες [S1], παράρτημα A, κεφάλαιο 2, σελίδα 225)

Την αντίστοιχη **αφινική καμπύλη** την παίρνουμε για w = 1. Έστω g(x, y) = f(1, x, y). Προφανώς deg g(x, y) ≤ d.

Ορίζουμε $C_g^{aff} = \{(x, y) \in k^2 \mid g(x, y) = 0\}$.

Προφανώς $C_g^{aff} = C_f \cap k^2$.

Αντίστροφα αν g(x, y) πολυώνυμο βαθμού μικρότερου ή ίσου με d τότε το πολυώνυμο $f(w, x, y) = w^d g\left(\frac{x}{w}, \frac{y}{w}\right)$ είναι ομογενές βαθμού d και f(1, x, y) = g(x, y).

Αφού $f(w, x, y) = 0 \Leftrightarrow f(w, x, y)^2 = 0$ το σύνολο των σημείων της C_f **δεν** ορίζει μονοσήμαντα την εξίσωση f (w, x, y) = 0. Αν το f έχει την ανάλυση $f = f_1 f_2 \ldots f_r$ τότε προφανώς ισχύει:

$$C_f = C_{f_1} \cup C_{f_2} \cup \ldots \cup C_{f_r}.$$

Αν πάλι $f \mid f'$ τότε $C_f \subset C_{f'}$.

Δεδομένου ότι η απάντηση στο ερώτημα πότε το πολυώνυμο f αναλύεται σε γινόμενο παραγόντων και πότε όχι εξαρτάται από το σώμα k, θα μιλάμε για την επίπεδη αλγεβρική καμπύλη πάνω από το σώμα k. Τέλος, για να είμαστε σίγουροι ότι υπάρχουν αρκετά σημεία πάνω στην καμπύλη, θα παίρνουμε τις συντεταγμένες των σημείων κάθε φορά από συγκεκριμένη επέκταση K του k.

Ορισμός 1.2.1 Μία **ανάγωγη επίπεδη αλγεβρική καμπύλη** C_f **βαθμού** d **ορισμένη υπέρ το σώμα k** ορίζεται από ένα ανάγωγο ομογενές πολυώνυμο $f(w, x, y) \in k[w, x, y]$ βαθμού d και είναι μία συνάρτηση η οποία, για κάθε επέκταση K του k μας δίνει το σύνολο

$$C_f(K) = \{[w, x, y] \in P_2(K) \mid f(w, x, y) = 0\}.$$

Αν η $f = f_1^{a(1)} f_2^{a(2)} \ldots f_r^{a(r)}$ είναι η ανάλυση του ομογενούς πολυωνύμου f βαθμού d του k[w, x, y] σε γινόμενο πρώτων παραγόντων τότε ισχύει :

$$C_f(K) = C_{f_1}(K) \cup C_{f_2}(K) \cup ... \cup C_{f_r}(K).$$

Η καμπύλη C_{fi} λέγεται (ανάγωγη) **συνιστώσα** της C_f και ο φυσικός αριθμός a(i) **πολλαπλότητα** της C_{fi}.

- Καμπύλες πρώτου βαθμού είναι οι **ευθείες**.
- Καμπύλες δευτέρου βαθμού λέγονται **κωνικές τομές**.
- Καμπύλες τρίτου βαθμού λέγονται **κυβικές καμπύλες**.
- Καμπύλες τέταρτου βαθμού λέγονται **τετραδικές καμπύλες**, και ούτω καθ' εξής.

Αν $K \subset K'$ επεκτάσεις του k τότε ισχύει $P_2(K) \subset P_2(K')$ και $C_f(K) \subset C_f(K')$.

Τέλος, αναφέρουμε την παρακάτω πρόταση:

Πρόταση 1.2.2 Έστω $f(X_1, X_2, \ldots, X_n) \in k[X_1, X_2, \ldots, X_n]$ όπου k σώμα.
Υποθέτουμε ότι $f(a_1, a_2, \ldots, a_n) = 0$ για όλα τα στοιχεία $a_1, a_2, \ldots, a_n$ ενός άπειρου υποσυνόλου T του k. Τότε $f(X_1, X_2, \ldots, X_n) \equiv 0$.

Απόδειξη Θα κάνουμε επαγωγή ως προς το πλήθος των μεταβλητών n του πολυωνύμου.

Για n = 1. Έστω $f(X) \in k[X]$ με degF(X) = m. Αν το f(X) δεν είναι το μηδενικό πολυώνυμο τότε έχει το πολύ m ρίζες μέσα στο k το οποίο δεν ισχύει. Άρα, η πρόταση ισχύει για n =1.

Έστω ότι η πρόταση ισχύει για όλα τα πολυώνυμα με n – 1 μεταβλητές. Γράφουμε:

$$f(X_1, X_2, \ldots, X_n) = f_0 + f_1 X_n + \ldots f_m X_n^m$$

όπου $m \geq 0$ και $f_1, f_2, \ldots, f_m \in k[X_1, X_2, \ldots, X_{n-1}]$. Αν f καποιο μη-μηδενικό πολυώνυμο μπορούμε να υποθέσουμε ότι $f_m \neq 0$. Από την υπόθεση της μαθηματικής επαγωγής έπεται ότι υπάρχουν στοιχεία $a_1, a_2, \ldots, a_n$ του συνόλου T τέτοια ώστε $f_m(a_1, a_2, \ldots, a_{n-1}) \neq 0$. Τότε όμως, αν $\deg_{X_n} f = m$, θα έχουμε το πολύ m δυνατότητες για το a_n έτσι ώστε $f(a_1, a_2, \ldots, a_n) = 0$, άτοπο διότι T άπειρο. Άρα το $f(X_1, X_2, \ldots, X_n)$ είναι το μηδενικό πολυώνυμο.

3. Σημεία τομής αλγεβρικών καμπυλών και ο βαθμός πολλαπλότητάς τους

Στην παράγραφο αυτή υποθέτουμε ότι το σώμα k έχει χαρακτηριστική **μηδέν**. Επομένως το k έχει άπειρο πλήθος στοιχείων. Αν στην καμπύλη C_f που ορίζεται από το $f(W, X, Y) \in k[W, X, Y]$ υποθέσουμε ότι $W \nmid f(W, X, Y)$ (δηλαδή ότι η C_f δεν περιέχει σαν συνιστώσα την επ' άπειρο ευθεία) τότε μπορούμε να θεωρήσουμε το $g(X, Y) = f(1, X, Y)$ και να παρατηρήσουμε αμέσως ότι οι λύσεις της $g(X, Y) = 0$ σε κάποια επέκταση K του k είναι το σύνολο των "πεπερασμένων" σημείων της καμπύλης $C_f(K)$.

Η ελευθερία επιλογής της επ' άπειρο ευθείας θα είναι χρήσιμη στα επόμενα. Αφού το K είναι απειροσύνολο, υπάρχουν άπειρες ευθείες στον προβολικό χώρο $P_2(K)$, άρα υπάρχει τουλάχιστο μία που δεν είναι συνιστώσα του $C_f(K)$. Αυτήν διαλέγουμε ως επ' άπειρον ευθεία.

Έστω $P_1 = [w_1, x_1, y_1]$ και $P_2 = [w_2, x_2, y_2]$ σημεία του $P_2(K)$. Η ευθεία που ορίζουν είναι η $L : \lambda P_1 + \mu P_2$ όπου $\lambda, \mu \in K$ όχι συγχρόνως μηδέν. Οι συντεταγμένες κάθε σημείου τομής των L και $C_f(K)$ θα επαληθεύουν την εξίσωση

$$f(\lambda w_1 + \mu w_2, \lambda x_1 + \mu x_2, \lambda y_1 + \mu y_2) = 0.$$

Ξεχωρίζουμε δύο περιπτώσεις:

(i) Έστω ότι $f(\lambda w_1 + \mu w_2, \lambda x_1 + \mu x_2, \lambda y_1 + \mu y_2) = 0$ για **όλα** τα $\lambda, \mu \in K$. Διαλέγουμε κατάλληλο σύστημα συντεταγμένων, έτσι ώστε η ευθεία L να είναι επ' άπειρο ευθεία $W = 0$. Τότε έχουμε:

$$f(0, x, y) = 0, \text{ για κάθε } x, y \in K.$$

Η πρόταση 1.2.2 δίνει ότι $f(0, X, \Psi) = 0$. Συνεπώς, ο W είναι κοινός παράγοντας των όρων του $f(W, X, Y)$ δηλαδή η ευθεία L ($W = 0$) είναι συνιστώσα της $C_f(K)$.

(ii) Έστω τώρα ότι το $f(\lambda P_1 + \mu P_2)$ **δεν** είναι το εκ ταυτότητας μηδενικό πολυώνυμο ως προς λ και μ. Τότε το $f(\lambda P_1 + \mu P_2)$ είναι ομογενές πολυώνυμο βαθμού d ως προς λ και μ. Αν K είναι **αλγεβρικά κλειστό** τότε από την

Πρόταση Αν K αλγεβρικά κλειστό σώμα και $f(X_0, X_1) \in K[X_0, X_1]$ ομογενές πολυώνυμο βαθμού d τότε υπάρχουν d ζευγάρια σταθερών $a_i, b_i \in K$ τέτοια ώστε $f(X_0, X_1) = \alpha \prod (a_i X_1 - b_i X_0)$ $\alpha \neq 0$.. (Δες [A1], πρόταση 11 σελίδα 22).

συνεπάγεται ότι η εξίσωση $f(\lambda P_1 + \mu P_2) = 0$ επαληθεύεται από ακριβώς d λόγους λ/μ όπου μία ρίζα πολλαπλότητας r μετριέται r-φορές. Κάθε λόγος ορίζει **ακριβώς** ένα σημείο της τομής $L \cap C_f(K)$. Ώστε:

Αναφέρουμε χωρίς απόδειξη τις παρακάτω προτάσεις:

Πρόταση 1.3.1 Αν K αλγεβρικά κλειστό σώμα τότε μία ευθεία L του $P_2(K)$ ή είναι συνιστώσα της $C_f(K)$ ή έχει ακριβώς d σημεία τομής (deg f = d). (Δες [A1], πρόταση 23, σελίδα 33).

Πρόταση 1.3.2 Αν η καμπύλη C_f υπέρ το αλγεβρικά κλειστό σώμα K περιέχει μόνο **απλές** συνιστώσες τότε από οποιοδήποτε σημείο $P \in P_2(K)$, $P \notin C_f(K)$, περνάει μία ευθεία που τέμνει την $C_f(K)$ σε d διακεκριμένα σημεία. (Δες [A1], πρόταση 24, σελίδα 33).

Ορισμός 1.3.3 Έστω C_f αλγεβρική καμπύλη υπέρ το σώμα k η οποία περιέχει μόνο απλές συνιστώσες. Θα καλούμε **τάξη της C_f** (ως προς το σώμα k) το μέγιστο αριθμό τομών της C_f με μία οποιαδήποτε ευθεία L.

Εξετάζουμε τώρα το πρόβλημα των σημείων τομής ευθείας και αλγεβρικής καμπύλης $C_f(K)$ όταν οι ευθείες περνούν από δοσμένο **σημείο της καμπύλης** $P \in C_f(K)$.

Διαλέγουμε κατάλληλο σύστημα συντεταγμένων έτσι ώστε οι αφινικές συντεταγμένες του P να είναι (a, b) οπότε αμέσως προκύπτει ότι για το συνεταιρικό του f αφινικό πολυώνυμο g(X, Y) ισχύει g(a, b) = 0.

Οι παραμετρικές εξισώσεις των ευθειών L που περνούν από το σημείο P = (a, b) γράφονται

$$\left\{ \begin{array}{l} x = a + \lambda t \\ y = b + \mu t \end{array} \right\}$$

και ορίζονται πλήρως από τον λόγο $\frac{\lambda}{\mu}$.

Τα σημεία τομής δίνονται από την σχέση

$$g(a + \lambda t, b + \mu t) = 0.$$

Αναπτύσσουμε το αριστερό μέλος σε σειρά Taylor ως προς t. Έχουμε

$$\left(\frac{\partial g}{\partial x}\Big|_{(a,b)} \lambda + \frac{\partial g}{\partial y}\Big|_{(a,b)} \mu \right) t + \frac{1}{2}\left(\frac{\partial^2 g}{\partial x^2}\Big|_{(a,b)} \lambda + 2\frac{\partial^2 g}{\partial x \partial y}\Big|_{(a,b)} \lambda\mu + \frac{\partial^2 g}{\partial y^2}\Big|_{(a,b)} \mu^2 \right) t^2 + \ldots = 0$$

Πρώτη περίπτωση: Υποθέτουμε ότι οι $\frac{\partial g}{\partial x}\Big|_{(a,b)}$ και $\frac{\partial g}{\partial y}\Big|_{(a,b)}$ δεν είναι συγχρόνως μηδέν. Αυτό σημαίνει ότι η λύση t = 0 είναι απλή. Συνεπώς κάθε ευθεία που περνάει από το P έχει **απλή** τομή με την C_f στο P. Μοναδική εξαίρεση αποτελεί η ευθεία που έχει τιμές στα λ και μ έτσι ώστε $\frac{\partial g}{\partial x}\Big|_{(a,b)} \lambda + \frac{\partial g}{\partial y}\Big|_{(a,b)} \mu = 0$.

Ορισμός 1.3.4 Η ευθεία αυτή θα λέγεται **εφαπτόμενη** της C_f στο P.

Δεύτερη περίπτωση: Υποθέτουμε ότι στο σημείο P οι $\frac{\partial g}{\partial x}, \frac{\partial g}{\partial y}$ είναι μηδέν αλλά δεν είναι όλες οι $\frac{\partial^2 g}{\partial x^2}, \frac{\partial^2 g}{\partial x \partial y}, \frac{\partial^2 g}{\partial y^2}$ συγχρόνως μηδέν.

Τότε κάθε ευθεία που περνάει από το P έχει σημείο τομής το P με βαθμό πολλαπλότητας τουλάχιστον 2 και **το πολύ 2** ευθείες που αντιστοιχούν στις ρίζες τις $\frac{\partial^2 g}{\partial x^2}\Big|_{(a,b)} \lambda + 2\frac{\partial^2 g}{\partial x \partial y}\Big|_{(a,b)} \lambda\mu + \frac{\partial^2 g}{\partial y^2}\Big|_{(a,b)} \mu^2 = 0$ έχουν βαθμό πολλαπλότητας μεγαλύτερο του 2. Οι δύο αυτές εξαιρέσεις λέγονται εφαπτόμενες της C_f στο P (αν η παραπάνω εξίσωση έχει διπλή ρίζα τότε λέμε ότι οι εφαπτόμενες συμπίπτουν).

r-οστή περίπτωση: Υποθέτουμε ότι όλες οι παράγωγοι της g, μέχρι και (r–1)-τάξεως συμπεριλαμβανομένης, μηδενίζονται στο P, αλλά τουλάχιστον μια παράγωγος r-τάξεως **δεν** μηδενίζεται στο P. Τότε κάθε ευθεία που περνάει από το P έχει σημείο τομής με την καμπύλη P με βαθμό πολλαπλότητας τουλάχιστον r και υπάρχουν **ακριβώς** r ευθείες που έχουν πιο πολλά από r σημεία τομής. Οι εξαιρέσιμες αυτές ευθείες λέγονται εφαπτόμενες της C_f στο P και αντιστοιχούν στις ρίζες του πολυωνύμου

$$\frac{\partial^r g}{\partial x^r}\Big|_{(a,b)} \lambda^r + \binom{r}{1}\frac{\partial^r g}{\partial x^{r-1}\partial y}\Big|_{(a,b)} \lambda^{r-1}\mu + \ldots + \binom{r}{r}\frac{\partial^r g}{\partial y^r}\Big|_{(a,b)} \mu^r = 0$$

και μετριούνται με πολλαπλότητα ίση προς της πολλαπλότητα της αντίστοιχης ρίζας της παραπάνω εξίσωσης.

Ορισμός 1.3.5 Στην περίπτωση r θα λέμε ότι το P είναι ένα σημείο της καμπύλης C_f βαθμού πολλαπλότητας r.

Σημείωση 1.3.6 Αφού το g(X, Y) δεν είναι εκ ταυτότητας μηδέν έπεται ότι η περίπτωση r θα συμβαίνει για κάποιο r με $1 \le r \le d$.

- Ένα σημείο βαθμού πολλαπλότητας 1, θα λέγεται **απλό**.
- Ένα σημείο βαθμού πολλαπλότητας 2, θα λέγεται **διπλό**.
- κ.ο.κ.

Ορισμός 1.3.7 Κάθε σημείο της καμπύλης C_f βαθμού πολλαπλότητας μεγαλύτερου του 1 θα λέγεται **ιδιάζον** (singular).

Προφανώς, ένα σημείο P = (a, b) θα είναι ιδιάζον, ακριβώς τότε όταν ισχύει

$$g(a, b) = \frac{\partial g}{\partial x}(a, b) = \frac{\partial g}{\partial y}(a, b) = 0.$$

Ορισμός 1.3.8 Η καμπύλη C_f θα λέγεται **μη-ιδιάζουσα** (non-singular) όταν **κάθε** σημείο της είναι μη-ιδιάζον. Αν η C_f έχει ένα τουλάχιστον ιδιάζον σημείο θα λέγεται **ιδιάζουσα**.

Ορισμός 1.3.9 Έστω C_f μια μη-ιδιάζουσα καμπύλη βαθμού m τότε **γένος της καμπύλης** ονομάζουμε το $\frac{1}{2}$ (m – 1)(m – 2).

Πρόταση 1.3.10 Έστω ότι το g(X, Y) δεν έχει όρους βαθμού μικρότερου του r και έχει μερικούς όρους βαθμούς r. Τότε η αρχή των συντεταγμένων είναι ένα σημείο βαθμού πολλαπλότητας r της καμπύλης g(X, Y) = 0 και η καμπύλη που ορίζεται από την εξίσωση g_r (X, Y) = 0, (όπου g_r (X, Y) οι όροι της g βαθμού r), έχει σαν συνιστώσες τις εφαπτόμενες της g στην αρχή των συντεταγμένων.

Σε προβολικές συντεταγμένες ισχύει η

Πρόταση 1.3.11 Ένα σημείο P είναι βαθμού πολλαπλότητας r της f(W, X, Y) = 0 ακριβώς τότε όταν όλες οι παράγωγοι τάξης (r –1) του f μηδενίζονται στο P αλλά αυτό δεν συμβαίνει για όλες τις παραγώγους τάξης r. (Δες [A1], πρόταση 32, σελίδα 36).

Παρατήρηση 1.3.12 Προφανώς το σημείο P=[1, a, b] είναι ιδιάζον σημείο της καμπύλης

$$f(w, x, y) = 0$$

αν και μόνο αν

$$\frac{\partial f}{\partial w}(P) = \frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.$$

Πρόταση 1.3.13 Έστω C_f και $C_{f'}$ δύο επίπεδες αλγεβρικές καμπύλες βαθμού m και n αντίστοιχα, ορισμένες υπέρ το σώμα k. Αν για κάποια επέκταση K του k το σύνολο $C_f(K) \cap C_{f'}(K)$ έχει **πιό πολλά** από mn σημεία τότε οι C_f και $C_{f'}$ έχουν κοινή συνιστώσα. (Δες [A1], πρόταση 34, σελίδα 37).

Πρόταση 1.3.14 Αν δύο αλγεβρικές καμπύλες C_f και $C_{f'}$ ορισμένες στο σώμα k βαθμού m και n αντίστοιχα **δεν έχουν κοινή συνιστώσα** στην επέκταση K του k και τα σημεία τομής τους, έστω P_i (i= 1, 2, …), έχουν βαθμό πολλαπλότητας r_i και s_i ως προς τις δύο καμπύλες αντίστοιχα, τότε

$$\sum_i r_i s_i \leq mn$$

(δες [A1], πρόταση 36, σελίδα 40).

Παρατήρηση 1.3.15 Η τελευταία πρόταση είναι χρήσιμη στη διαπίστωση ότι μερικές καμπύλες με «αρκετά» στο πλήθος ιδιάζοντα σημεία, δεν μπορούν να είναι ανάγωγες π.χ. μια κυβική καμπύλη με δύο διπλά σημεία θα πρέπει να έχει σαν συνιστώσα την ευθεία που τα συνδέει, διότι αλλιώς τα σημεία τομής της κυβικής καμπύλης και της

ευθείας θα έδιναν $\sum_i r_i s_i = 4 > 3 \cdot 1$. Ώστε **μια ανάγωγη κυβική καμπύλη περιέχει το πολύ ένα ιδιάζον σημείο. Μια ανάγωγη κωνική τομή δεν περιέχει κανένα.**

Πρόταση 1.3.16 Έστω C_f και $C_{f'}$ δύο αλγεβρικές καμπύλες υπέρ του σώματος k και οι δύο βαθμού n. Υποθέτουμε ότι για κάποια επέκταση $K \supset k$ ισχύει

$$\#\left(C_f(K) \cap C_{f'}(K)\right) = n^2$$

και ότι **ακριβώς** mn σημεία τομής ανήκουν σε μία ανάγωγη καμπύλη βαθμού m. Τότε τα υπόλοιπα n(n–m) σημεία τομής βρίσκονται πάνω σε μία καμπύλη βαθμού n–m. (Δες [A1], πρόταση 38, σελίδα 41).

Πρόταση 1.3.17 Έστω C_0 και C_1 είναι δύο κωνικές τομές με ακριβώς 4 διακεκριμένα σημεία μεταξύ τους, (έστω P_1, P_2, P_3, P_4), ορισμένες πάνω από ένα άπειρο σώμα K. Κάθε άλλη κωνική τομή που περνάει από τα P_1, P_2, P_3, P_4 είναι της μορφής

$$b_0C_0 + b_1C_1 \qquad \text{όπου } b_0, b_1 \in K.$$

(Δες [A1], πρόταση 39, σελίδα 42).

Το επόμενο θεώρημα είναι βασικό για την αποδειξη της προσεταιριστικότητας στη δομή ομάδας της πρόσθεσης των ρητών σημείων ελλειπτικής καμπύλης:

Θεώρημα 1.3.18 Έστω Γ_0 και Γ_1 δύο κυβικές καμπύλες, οι οποίες τέμνονται σε ακριβώς 9 σημεία τομής του $P_2(K)$, όπου K άπειρο σώμα. Αν μία επίπεδη κυβική καμπύλη Γ περνάει από οκτώ από τα σημεία τομής των δύο καμπυλών Γ_0 και Γ_1, τότε περνάει και από το ένατο και έχει τη μορφή

$$\Gamma = b_0 \Gamma_0 + b_1 \Gamma_1 \qquad \text{όπου } b_0, b_1 \in K.$$

(Δες [A1], θεώρημα 40, σελίδα 42).

Θα κλείσουμε την παράγραφο αναφέροντας, χωρίς απόδειξη, το ακόλουθο

Θεώρημα 1.3.19 (Θεώρημα του Bezout) Αν C_f και $C_{f'}$ δύο προβολικές επίπεδες καμπύλες, υπέρ του αλγεβρικά κλειστού σώματος $\tilde{k}$, βαθμού m και n αντίστοιχα, οι οποίες δεν έχουν κοινή συνιστώσα, τότε έχουν, στο $\tilde{k}$, **ακριβώς** mn σημεία τομής. (Δες [W])

4. Σημεία καμπής (inflections ή flexes)

Ορισμός 1.4.1 Ένα σημείο P = [w, x, y] μιας αλγεβρικής καμπύλης C_f θα λέγεται **σημείο καμπής** της C_f τότε και μόνο τότε αν

(i) το P είναι μη-ιδιάζον και

(ii) ο βαθμός πολλαπλότητας της εφαπτόμενης στο P είναι μεγαλύτερος ή ίσος του 3.

Σημείωση 1.4.2 Από τον ορισμό έπεται ότι αν μια καμπύλη έχει σαν συνιστώσα κάποια ευθεία τότε κάθε μη-ιδιάζον σημείο της που ανήκει στην ευθεία είναι σημείο καμπής.

Αυτή η περίπτωση δεν μας ενδιαφέρει, έτσι θα θεωρούμε μόνο καμπύλες που δεν έχουν ευθεία σαν συνιστώσα (δες πρόταση 1.3.10)

Λόγω της πρότασης 1.3.10 για να είναι η αρχή των συντεταγμένων [1, 0, 0] ένα σημείο καμπής με εφαπτόμενη την ευθεία

$$bX - aY = 0$$

θα πρέπει το πολυώνυμο f(1, X, Y) να έχει την εξής μορφή:

$$f(1, X, Y) = (bX - aY) + h_2(X, Y) + \ldots + h_d(X, Y),$$

όπου το $h_i(X, Y)$ είναι ομογενές πολυώνυμο βαθμού i για i = 2, 3, …, d και

$$h_2(at, bt) = t^2 h_2(a, b) = 0.$$

Έστω τώρα μία κωνική τομή C υπέρ το σώμα k.

Υποθέτουμε ότι η C έχει ένα ιδιάζον σημείο. Μια ευθεία L που περνάει από το σημείο αυτό τέμνει (μέσα στην αλγεβρική θήκη του k, $\widetilde{k}$) την κωνική τομή και σε ένα άλλο σημείο. Αφού $1 \cdot 2 + 1 \cdot 1 = 3 > 2$ η πρόταση 1.3.14 δίνει ότι L και C έχουν κοινή συνιστώσα δηλαδή η ευθεία L είναι συνιστώσα της κωνικής τομής C, και επομένως η C δεν είναι ανάγωγη. Από την άλλη μεριά αν η C δεν είναι ανάγωγη τοτέ είτε αποτελείται από ένα ζευγάρι διακεκριμένων ευθειών, οπότε το σημείο τομής είναι ιδιάζον είτε από το γινόμενο μιας ευθείας με τον εαυτό της, οπότε όλα τα σημεία είναι ιδιάζοντα.

Συμπέρασμα: Η κωνική τομή C είναι **ανάγωγη** αν και μόνο αν δεν έχει κανένα ιδιάζον σημείο.

Οι κυβικές καμπύλες (συναρτήσεις της μορφής $Y^2 = f(X)$, όπου f(X) πολυώνυμο τρίτου βαθμού) όπως αναφέραμε και στην προηγούμενη παράγραφο (δες πρόταση 1.3.15) περιέχουν το πολύ ένα ιδιάζον σημείο. Υπάρχουν δύο είδη ιδιάζουσων κυβικών καμπυλών. Σε ποιο από τα δύο είδη ανήκει μια δεδομένη κυβική καμπύλη εξαρτάται από το αν το πολυώνυμο f έχει κάποια διπλή ή τριπλή ρίζα. (Δες [S1], παράγραφος I.3, σελίδα 26).

1. Η κυβική καμπύλη $Y^2 = X^2 (X + 1)$ είναι ιδιάζουσα. Το ρητό σημείο $O = (0, 0)$ ανήκει στην καμπύλη και είναι ιδιάζον σημείο της. Σε αυτή την περίπτωση η f έχει διπλή ρίζα και η καμπύλη έχει δύο διακεκριμένες εφαπτόμενες στο O με τύπους $Y = \pm\sqrt{X}$.

2. Η κυβική καμπύλη $Y^2 = X^3$ είναι επίσης ιδιάζουσα. Όπως και πριν, το ρητό σημείο $O = (0, 0)$ ανήκει στην καμπύλη και είναι ιδιάζον σημείο της. Σε αυτή την περίπτωση η f έχει τριπλή ρίζα και η καμπύλη έχει κορυφή στο O.

Πρόταση 1.4.3 Η κωνική τομή C_f όπου $f(X_0, X_1, X_2) = \sum_{i,j=0}^{2} a_{ij} X_i X_j$ (με $a_{ij} = a_{ji}$) **δεν είναι ανάγωγη** τότε και μόνο τότε όταν η ορίζουσα $\det(a_{ij})$ είναι ίση με μηδέν. (Δες [A1], πρόταση 43, σελίδα 45).

Απόδειξη Η κωνική τομή C_f δεν είναι ανάγωγη αν και μόνο αν έχει ένα ιδιάζον σημείο, έστω $P[x_0, x_1, x_2]$. Οπότε, λόγω της πρότασης 1.3.12, αν και μόνο αν

$$\frac{\partial f}{\partial x_0}(P) = \frac{\partial f}{\partial x_1}(P) = \frac{\partial f}{\partial x_2}(P) = 0.$$

Δηλαδή αν και μόνο αν το παραπάνω σύστημα έχει μια μη τετριμμένη λύση. Επειδή,

$$\frac{\partial f}{\partial x_i}(P) = 2\sum_{i,j=0}^{2} a_{ij} x_j, \text{ για κάθε } i = 0, 1, 2$$

το σύστημα έχει μη-τετριμμένη λύση αν και μόνο αν $\det(a_{ij}) = 0$.

Χωρίς απόδειξη αναφέρουμε την παρακάτω

Πρόταση 1.4.4 Έστω τώρα C_f μία αλγεβρική καμπύλη, $f(X_0, X_1, X_2) \in k[X_0, X_1, X_2]$. Τα σημεία καμπής είναι ακριβώς τα μη ιδιάζοντα σημεία της καμπύλης τα οποία είναι σημεία τομής με την εσσιανή

$$H(X_0, X_1, X_2) := \det\begin{pmatrix} \frac{\partial^2 f}{\partial X_0^2} & \frac{\partial^2 f}{\partial X_1 \partial X_0} & \frac{\partial^2 f}{\partial X_2 \partial X_0} \\ \frac{\partial^2 f}{\partial X_0 \partial X_1} & \frac{\partial^2 f}{\partial X_1^2} & \frac{\partial^2 f}{\partial X_2 \partial X_1} \\ \frac{\partial^2 f}{\partial X_0 \partial X_2} & \frac{\partial^2 f}{\partial X_1 \partial X_2} & \frac{\partial^2 f}{\partial X_2^2} \end{pmatrix}$$

(Δες [A1], πρόταση 44, σελίδα 46).

Παρατήρηση Αφού το f είναι ομογενές πολυώνυμο βαθμού d έπεται ότι η H είναι ομογενές πολυώνυμο βαθμού $3(d - 2)$.

Πόρισμα 1.4.5 Κάθε μη-ιδιάζουσα καμπύλη τάξης μεγαλύτερης ή ίσης του 3 έχει τουλάχιστον ένα σημείο καμπής. Μια κωνική τομή δεν έχει κανένα σημείο καμπής.

Έστω, τώρα, ότι μία μη-ιδιάζουσα κυβική καμπύλη έχει το σημείο καμπής [1, 0, 0] με εφαπτόμενη ευθεία την Y =0, δηλαδή τον άξονα των X. Η καμπύλη μας θα έχει τη μορφή

$$f(1, X, Y) = Y + h_2(X, Y) + h_3(X, Y) = Y + bXY + aY^2 + h_3(X, Y)$$

διότι, για Y = 0, θα πρέπει $h_2(X, 0) = 0$. Άρα

$$f(W, X, Y) = W^2Y + aY^2W + bWXY + h_3(X, Y).$$

Αν κάνουμε τώρα το ίδιο και πάρουμε το επ' άπειρο σημείο [0, 0, 1] σαν σημείο καμπής, με εφαπτόμενη την επ' άπειρο ευθεία W = 0, τότε καταλήγουμε στην εξίσωση του παρακάτω ορισμού.

Ορισμός 1.4.6 Η εξίσωση μίας μη-ιδιάζουσας κυβικής καμπύλης C στην **κανονική** της **μορφή** είναι

$$WY^2 + a_1WXY + a_3W^2Y = X^3 + a_2X^2W + a_4XW^2 + a_6W^3.$$

(Μερικές φορές λέγεται και **γενικευμένη μορφή του Weierstrass**).

Επομένως, για να πάρουμε την κανονική μορφή πρέπει να μεταφέρουμε ένα σημείο καμπής στο άπειρο έτσι ώστε η εφαπτόμενη να είναι η επ' άπειρο ευθεία.

Αν η χαρακτηριστική του σώματος k είναι διαφορετική του 2, τότε μπορούμε να γράψουμε την κανονική μορφή ως εξής:

$$W\left[Y^2 + 2\left(\frac{a_1X + a_3W}{2}\right)Y + \left(\frac{a_1X + a_3W}{2}\right)^2\right] = X^3 + \frac{b_2}{4}X^2W + \frac{b_4}{4}XW^2 + \frac{b_6}{4}W^3$$

όπου

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

Θέτουμε

$$b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2$$

και βρίσκουμε

$$4b_8 = b_2b_6 - b_4.$$

Για $\eta = Y + \frac{a_1 + a_3W}{2}$ η κανονική μορφή γίνεται

$$W\eta^2 = X^3 + \frac{b_2}{4}X^2W + \frac{b_4}{4}XW^2 + \frac{b_6}{4}W^3$$

Αν η χαρακτηριστική του σώματος k είναι διάφορη των 2 και 3 τότε για

$$c_4 = b_2^2 - 24b_4 \text{ και } c_6 = -b_2^3 + 36b_2b_4 - 216b_6$$

Για $\xi = X + \frac{b_2}{12}$ η κανονική μορφή γίνεται

$$W\eta^2 = \xi^3 + \frac{c_4}{48}\xi W^2 - \frac{c_6}{864}W^3.$$

Παρατηρούμε ότι τα b_2, b_4, b_6, b_8 και c_4, c_6 είναι ακέραιοι αν τα a_1, a_2, a_3, a_4, a_6 είναι ακέραιοι.

Προκύπτει λοιπόν ο παρακάτω ορισμός:

Ορισμός 1.4.7 Θα λέμε ότι μια μη-ιδιάζουσα κυβική καμπύλη C έχει εξίσωση στη **μορφή** του **Weierstrass** όταν έχει τη μορφή

$$WY^2 = X^3 + bW^2X + cW^3$$

Σε αφινικές συντεταγμένες η εξίσωση γράφεται

$$Y^2 = f(X),$$

όπου $f(X) \in K[X]$, κυβικό, μονικό πολυώνυμο του οποίου το άθροισμα των ριζών είναι ίσο με μηδέν.

Το πολυώνυμο $f(X) = X^3 + bX + c$ έχει διπλή ρίζα σε κάποια επέκταση του K ακριβώς τότε όταν για την διακρίνουσα D(f) του f ισχύει $D(f) = -4b^3 - 27c^2 = 0$.

Πρόταση 1.4.8 Ένα σημείο [1, a, 0] της C με εξίσωση $WY^2 = X^3 + bW^2X + cW^3$ είναι **μη-ιδιάζον** ακριβώς τότε όταν το a είναι **απλή** ρίζα του $X^3 + bX + c$. (Δες [A1], πρόταση 48, σελίδα 49).

Παρατήρηση 1.4.9 Επομένως, από την πρόταση 1.4.8 φαίνεται ότι η κυβική καμπύλη $Y^2 = X^3 + bX + c$ είναι μη ιδιάζουσα αν και μόνο αν $D(f) \neq 0$ όπου $D(f) = -4b^3 - 27c^2$.

5. Ελλειπτικές καμπύλες

Έστω, τώρα, Ε μια μη-ιδιάζουσα κυβική καμπύλη ορισμένη στο σώμα **Q** των ρητών αριθμών. Επομένως, (δες ορισμό 1.4.7) η καμπύλη έχει μια εξίσωση της μορφής:

$$E : WY^2 = f(X)$$

όπου $f(X) = X^3 + bW^2X + cW^3$ και $b, c \in \mathbf{Q}$.
Επίσης, (δες παρατήρηση 1.4.8) $D(f) = -4b^3 - 27c^2 \neq 0$.

Ορισμός 1.5.1 Κάθε σημείο του αφινικού επιπέδου με ρητές συντεταγμένες το οποίο επαληθεύει την εξίσωση της καμπύλης θα λέγεται **ρητό σημείο της καμπύλης**.

Ορισμός 1.5.2 Μια ευθεία θα λέγεται **ρητή ευθεία** αν μπορεί να γραφεί στη μορφή

$$a X + b Y + c = 0 \text{ όπου } a, b, c \in \mathbf{Q}.$$

Παρατήρηση 1.5.3 Αν πάρουμε δύο ρητά σημεία $P = (x_1, y_1)$, $Q = (x_2, y_2)$ μιας μη-ιδιάζουσας ρητής κυβικής καμπύλης Ε τότε η ευθεία που ορίζουν είναι η ρητή ευθεία

$$L : (y_1 - y_2) X + (x_2 - x_1) Y + (x_1y_2 - y_1x_2) = 0.$$

Η ευθεία L τέμνει την καμπύλη Ε σε ένα ακόμα σημείο PQ που είναι επίσης ρητό. Επίσης, αν από κάποιο ρητό σημείο P τη καμπύλης Ε φέρουμε την εφαπτόμενη στο σημείο αυτό τότε η εφαπτόμενη τέμνει την Ε σε ένα άλλο ρητό σημείο PP.

Στο εξής θα συμβολίζουμε με PQ το τρίτο σημείο τομής της ευθείας που περνάει από τα P και Q με την κυβική καμπύλη.

Αν, επομένως ξέρουμε κάποια ρητά σημεία πάνω σε μια μη-ιδιάζουσα ρητή κυβική καμπύλη μπορούμε να παράγουμε κι άλλα.

Ας δώσουμε τώρα τον παρακάτω ορισμό:

Ορισμός 1.5.4 Έστω C μια μη-ιδιάζουσα (non-singular) ρητή κυβική καμπύλη και O ένα ρητό σημείο αυτής. Αν P και Q σημεία της C τότε **άθροισμα** P+Q ορίζεται να είναι το τρίτο σημείο τομής της ευθείας που περνάει από τα O και PQ με την C.

Η πρόσθεση που μόλις ορίσαμε είναι αντιμεταθετική και το O είναι ουδέτερο στοιχείο της.

Για κάθε ρητό σημείο της καμπύλης μπορούμε να βρούμε ένα ρητό αντίθετό του. Είναι το τρίτο σημείο τομής της ευθείας που περνάει από τα P και OO με την κυβική καμπύλη.

Αποδεικνύεται επίσης, με χρήση του θεωρήματος 1.3.18, ότι η πράξη είναι και προσεταιριστική και επομένως το σύνολο των ρητών σημείων μιας μη-ιδιάζουσας ρητής κυβικής καμπύλης εφοδιασμένο με αυτή την πράξη είναι **αβελιανή ομάδα**.

Ορισμός 1.5.5 Μια **ελλειπτική καμπύλη** είναι μια μη-ιδιάζουσα (non-singular) ρητή κυβική καμπύλη με συντελεστές ακεραίους αριθμούς η οποία έχει ένα ρητό σημείο (θα το συμβολίζουμε με Ο) και είναι εφοδιασμένη με την παραπάνω πράξη ομάδας.

Συμβολισμός 1.5.6 Την ομάδα των ρητών σημείων μιας ελλειπτικής καμπύλης Ε ορισμένης πάνω στο σώμα **Q** θα την συμβολίζουμε με Ε(**Q**).

Θεώρημα 1.5.7 (Θεώρημα του Mordell) Η ομάδα Ε(**Q**) των ρητών σημείων μιας ελλειπτικής καμπύλης Ε ορισμένης στο **Q** είναι πεπερασμένα παραγόμενη αβελιανή ομάδα. (Για απόδειξη δες [A1], κεφάλαιο 5).

Ορισμός 1.5.8 **Τάξη** ενός ρητού σημειού Ρ μιας ελλειπτικής καμπύλης Ε ονομάζουμε την τάξη της κυκλικής υποομάδας <P> της Ε που παράγεται από το Ρ. Αν η υποομάδα είναι πεπερασμένη τότε λέμε ότι το σημείο είναι **πεπερασμένης τάξης**.

Θεώρημα 1.5.9 (Θεώρημα των Lutz-Nagell) Έστω Ε ελλειπτική καμπύλη. Όλα τα σημεία πεπερασμένης τάξης P = (x, y) της Ε(**Q**) έχουν **ακέραιες συντεταγμένες** x και y και μάλιστα είτε y = 0 οπότε είναι σημεία τάξης 2 είτε y | D(f). (Για απόδειξη δες [A1], θεώρημα 1, σελίδα 64)

Ισχύει η ισχυρότερη μορφή του Θεωρήματος των Lutz-Nagell:

Πρόταση 1.5.10 Αν ισχύει ότι y | D(f) τότε ισχύει και y^2 | D(f). (Δες [S2], πρόταση 7.2, σελίδα 221)

Παρατήρηση 1.5.11 Έστω P, Q, R τρία διακεκριμένα σημεία μιας ελλειπτικής καμπύλης Ε. Τα P, Q, R είναι συνευθειακά αν και μόνο αν P + Q + R = O.

Πράγματι, P + Q + R = O $\Leftrightarrow$ P + Q = –R $\Leftrightarrow$ R = PQ $\Leftrightarrow$ P, Q, R συνευθειακά.

Έστω, στη συνέχεια, Ε: $Y^2 = X^3 + bX + c$ μια ελλειπτική καμπύλη και P, Q ρητά σημεία της. Θα δώσουμε κάποιους τύπους που θα μας επιτρέπουν να υπολογίζουμε το P+Q εύκολα.

Παίρνουμε σαν ουδέτερο στοιχείο της ελλειπτικής καμπύλης Ε, το επ' άπειρον. Δηλαδή O = [0, 0, 1]. Παρατηρούμε ότι αν P = (x, y) σημείο της Ε τότε –P = (x, –y).

Έστω, $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $PQ = (x_3, y_3)$. Τότε $P+Q = –PQ = (x_3, –y_3)$. Υποθέτουμε ότι γνωρίζουμε τις συντεταγμένες των σημείων P, Q και θέλουμε να υπολογίσουμε τις συντεταγμένες του σημείου P+Q.

Η ευθεία που ορίζουν τα P και Q είναι, όπως γράψαμε και προηγουμένως, η ρητή ευθεία $L : (y_1 – y_2) X + (x_2 – x_1) Y + (x_1y_2 – y_1x_2) = 0$.

Διακρίνουμε δύο περιπτώσεις:

Πρώτη περίπτωση: Αν $x_1 \neq x_2$. Η L μπορεί να γραφτεί στη μορφή $Y = \lambda X + \nu$ όπου τα λ και ν δίνονται από τους τύπους $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ και $\nu = y_1 – \lambda x_1 = y_2 – \lambda x_2$. Από την κατασκευής της η ευθεία L τέμνει την καμπύλη Ε στα σημεία P, Q. Για να

υπολογίσουμε το τρίτο σημείο τομής PQ αντικαθιστούμε το Y από την προηγούμενη σχέση στον τύπο της Ε.

$$(\lambda X + \nu)^2 = X^3 + bX + c$$

ή αλλιώς

$$X^3 - \lambda^2 X^2 + (b - 2\lambda\nu)X + (c - \nu^2) = 0$$

Η τελευταία σχέση είναι μια εξίσωση τρίτου βαθμού ως προς x και έχει σαν ρίζες τα x_1, x_2, x_3 οπότε ισχύει:

$$X^3 - \lambda^2 X^2 + (b - 2\lambda\nu)X + (c - \nu^2) = (X - x_1)(X - x_2)(X - x_3) \qquad (1.5.12)$$

Επομένως, ισχύει: $x_1 + x_2 + x_3 = -(-\lambda^2)$ ή αλλιώς

$$x_3 = \lambda^2 - x_1 - x_2 \text{ και } y_3 = \lambda x_3 + \nu \qquad (1.5.13)$$

οπότε, αντικαθιστώντας και τα λ και ν έχουμε

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \text{ και } y_3 = \frac{y_2 - y_1}{x_2 - x_1}(x_3 - x_1) + y_1 \qquad (1.5.14)$$

Δεύτερη περίπτωση: Αν $x_1 = x_2$. Τότε αν φέρουμε την ευθεία $x = x_1$, επ' αυτής βρίσκονται το P, το –P και, από την πρόταση 1.5.11, το επ' άπειρον σημείο O. Επομένως, είτε Q = P είτε Q = –P.

- Αν Q = –P τότε P+Q = P + (–P) = O.

- Αν Q = P τότε και $y_2 = y_1$. Οπότε έχουμε ότι P + Q = P + P = 2P. Για να βρούμε το σημείο 2P φέρνουμε την εφαπτομένη στο P η οποία τέμνει την καμπύλη στο σημείο PP = (x_3, y_3), και στη συνέχεια την κάθετη στον άξονα των x που περνάει από το σημείο PP.

Σε αυτή την περίπτωση:

Από την σχέση $Y^2 = X^3 + bX + c$ έχουμε ότι $\lambda = \left.\frac{dY}{dX}\right|_P = \frac{3x_1^2 + b}{2y_1}$. Αντικαθιστάμε το λ στους τύπους (1.5.12) και το Y^2 με $X^3 + bX + c$ και βρίσκουμε:

$$x_3 = -2x_1 + \frac{(3x_1^2 + b)^2}{4(x_1^3 + bx_1 + c)} = \frac{x_1^4 - 2bx_1^2 - 8cx_1 + b^2}{4(x_1^3 + bx_1 + c)} \qquad (1.5.15)$$

(δες [S1], παράγραφος I.4, σελίδα 31)

Κεφάλαιο ΙΙ

Κυβικές Καμπύλες πάνω σε Πεπερασμένα Σώματα

1. Ρητά σημεία πάνω σε κυβικές καμπύλες

Σκοπός μας είναι να μελετήσουμε κυβικές καμπύλες πάνω από ένα πεπερασμένο σώμα, το σώμα των αριθμών modulo p. Αυτό σημαίνει ότι η εξίσωση της καμπύλης δεν θα έχει πλέον συντελεστές ρητούς αριθμούς αλλά ότι οι συντελεστές θα ανήκουν στο πεπερασμένο σώμα με p στοιχεία. Το σώμα αυτό θα το συμβολίσουμε με $\mathbf{F}_p$. Αυτό που θα κάνουμε θα είναι να μελετήσουμε τις κυβικές εξισώσεις C : F(x, y) = 0 με συντελεστές από το σώμα $\mathbf{F}_p$ και να αναζητήσουμε λύσεις (x, y) με x, y $\in \mathbf{F}_p$. Γενικότερα, θα αναζητήσουμε λύσεις με x, y $\in \mathbf{F}_q$ όπου $\mathbf{F}_q$ είναι μια επέκταση του $\mathbf{F}_p$ με $q = p^e$ στοιχεία. Τη λύση αυτή θα την ονομάζουμε σημείο της καμπύλης C. Αν οι συντεταγμένες x, y βρίσκονται στο $\mathbf{F}_p$ θα την ονομάζουμε ρητό σημείο της καμπύλης C.

Παρατήρηση 2.1.1 Έστω μια μη-ιδιάζουσα (non-singular) κυβική καμπύλη ορισμένη σε κάποιο σώμα K. Τότε το άθροισμα δύο ρητών σημείων της, εδώ εννοούμε σημεία με συντεταγμένες από το σώμα K, ορίζεται όπως και στο 1.5.4. Με αυτή την πράξη κατασκευάζουμε την αβελιανή ομάδα των ρητών σημείων της καμπύλης.

Παρατήρηση 2.1.2 Προφανώς η παρατήρηση 1.5.11 προκύπτει άμεσα από τον ορισμό της πρόσθεσης σημείων και επομένως ισχύει για κάθε σώμα K.

Παρατήρηση 2.1.3 Οι τύποι 1.5.13, 1.5.14 και 1.5.15 του αθροίσματος δύο ρητών σημείων μιας ελλειπτικής καμπύλης ισχύουν σε κάθε σώμα K.

Έστω η κυβική καμπύλη

$$C : \quad y^2 = x^3 + ax^2 + bx + c$$

για κάποια a, b, c $\in \mathbf{F}_p$. Στα επόμενα υποθέτουμε ότι $p \neq 2$. Η καμπύλη είναι non-singular αν και μόνο αν η διακρίνουσα $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$ της καμπύλης είναι διάφορη του μηδενός σαν στοιχείο του $\mathbf{F}_p$. (Δες παρατήρηση 1.4.9)

Εργαζόμενοι ανάλογα όπως και στην περίπτωση που το πολυώνυμο f(x) δεν έχει δευτεροβάθμιο όρο, υπολογίζουμε τις συντεταγμένες του αθροίσματος P+Q δύο ρητών σημείων P, Q της C με $P = (x_1, y_1)$ και $Q = (x_2, y_2)$ ως εξής:

$$x_3 = \lambda^2 - a - x_1 - x_2 \text{ και } y_3 = -(\lambda x_3 + \nu). \qquad (2.1.4)$$

Όπου

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{αν} \quad x_1 \neq x_2 \\ \dfrac{3x_1^2 + 2ax_1 + b}{2y_1}, & \text{αν} \quad P_1 = P_2 \end{cases}$$

και $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$.

Συμβολισμός 2.1.5 Όταν η καμπύλη C είναι ορισμένη πάνω από σώμα K θα γράφουμε πολλές φορές $C|_K$.

Ορισμός 2.1.6 Έστω $C|_K$. Συμβολίζουμε την αβελιανή ομάδα των K-ρητών σημείων της με C(K).

Προτού εξετάσουμε τη θεωρία γενικά, ας δούμε ένα παράδειγμα. Έστω η ελλειπτική καμπύλη E με τύπο:

$$E: \quad y^2 = x^3 + x + 1$$

ορισμένη πάνω από το σώμα $\mathbf{F}_5$. **Πως θα βρούμε τα ρητά της σημεία;**

Επειδή τα x, y πρέπει να είναι στο $\mathbf{F}_5$ αρκεί να πάρουμε κάθε μια από τις πέντε τιμές για το x να τις εφαρμόσουμε στο πολυώνυμο $x^3 + x + 1$ και να ελέγξουμε αν το αποτέλεσμα είναι τετραγωνικό υπόλοιπο στο $\mathbf{F}_5$.

Έχουμε:

x	$x^3 + x + 1 = y^2$	τετραγωνικό υπόλοιπο	y
0	1	ΝΑΙ	1,-1
1	1 +1 +1 = 3	ΟΧΙ	-
2	2^3 +2 +1 = 1	ΝΑΙ	1,-1
3	3^3 +3 +1 = 1	ΝΑΙ	1,-1
4	4^3 +4 +1 = 4	ΝΑΙ	2,-2

Επομένως, συμπεριλαμβανομένου και του «έπ' άπειρον» σημείου O, έχουμε εννιά σημεία:

$$E(\mathbf{F}_5) = \{O, (0, \pm 1), (2, \pm 1), (3, \pm 1), (4, \pm 2)\}.$$

Επειδή η $E(\mathbf{F}_5)$ είναι αβελιανή ομάδα τάξης εννιά θα είναι ισόμορφη είτε με την κυκλική ομάδα $\mathbf{Z}_9$ είτε με την $\mathbf{Z}_3 \times \mathbf{Z}_3$. Μπορούμε να το εξακριβώσουμε κάνοντας τον πίνακα της ομάδας. Έστω P = (0,1) τότε υπολογίζουμε με χρήση του τύπου 2.1.4 το $2P = (x_3, y_3)$. (Δεν ξεχνάμε ότι δουλεύουμε στο $\mathbf{F}_5$).

Έχουμε:

$a = 0, b = 1, x_1 = 0, y_1 = 0, \lambda = \left(3\cdot 0^2 + 2\cdot 0\cdot 0 + 1\right)\cdot\left(2\cdot 1\right)^{-1} = 2^{-1} = 3$

$\nu = y_1 - \lambda x_1 = 1 - 3\cdot 0 = 1$. Άρα, $x_3 = 3^2 - 0 - 0 - 0 = 4$ και $y_3 = -3\cdot 4 - 1 = 2$.

Δηλαδή 2P = (4,2).

Ανάλογα βρίσκουμε ότι 3P = (2,1) και 4P = (3, –1). Άρα ord(P)>3.

Επομένως, η $E(\mathbf{F}_5)$ είναι **κυκλική ομάδα** τάξης εννιά. Το $P_1 = 3P = (2,1)$ έχει τάξη 3. Τάξη 3 έχει επίσης το $P_2 = -P_1 = (2, -1)$. Όλα τα υπόλοιπα μη-μηδενικά στοιχεία έχουν τάξη 9.

Όπως φαίνεται και από το παράδειγμα επειδή υπάρχουν πεπερασμένες τιμές για τα x, y, τα σημεία (x, y) είναι πεπερασμένα και **η $C(\mathbf{F}_p)$ είναι μια πεπερασμένη ομάδα**. Είναι μάλιστα προφανές ότι η τάξη της $C(\mathbf{F}_p)$ είναι το πολύ $2p+1$. Ένα φυσικό ερώτημα που γεννιέται είναι πόσο μεγάλη είναι; Πως μπορούμε να προσδιορίσουμε το πλήθος των σημείων στην $C(\mathbf{F}_p)$;

2. Σημεία πεπερασμένης τάξης

Στη συνέχεια θα προσπαθήσουμε να μελετήσουμε μια μέθοδο μέσω της οποίας μπορούμε να υπολογίσουμε τα ρητά σημεία πεπερασμένης τάξης μια ρητής ελλειπτικής καμπύλης E με ακέραιους συντελεστές. Η ιδέα είναι να θεωρήσουμε τη καμπύλη τοπικά, δηλαδή να ανάγουμε την καμπύλη για κάθε πρώτο αριθμό p. Αν λοιπόν θεωρήσουμε την καμπύλη E mod p, δηλαδή με αναγωγή των συντελεστών mod p, τότε έχουμε μια καμπύλη ορισμένη στο σώμα $\mathbf{F}_p$. Φυσικά η καμπύλη ενδέχεται να έχει ιδιάζοντα σημεία (singularities). Θα είναι ελλειπτική καμπύλη τότε και μόνο τότε όταν η διακρίνουσα D δεν διαιρείται από το p.

Έστω C μια κυβική καμπύλη με εξίσωση:

$$C: \quad y^2 = x^3 + ax^2 + bx + c$$

με ακέραιους συντελεστές a, b, c.

Όπως ξέρουμε η ομάδα C(**Q**) των ρητών σημείων της καμπύλης C είναι πεπερασμένα παραγόμενη (Θεώρημα του Mordell) και τα σημεία πεπερασμένης τάξης έχουν ακέραιες συντεταγμένες (Θεώρημα των Lutz – Nagell).

Θα συμβολίζουμε με $z \to \tilde{z}$ την συνάρτηση αναγωγής modulo p,

$$Z \to \frac{Z}{pZ} = \mathbf{F}_p, \; z \mapsto \tilde{z}$$

Μπορούμε να πάρουμε την εξίσωση της καμπύλης C, η οποία έχει ακέραιους συντελεστές, και να ανάγουμε τους συντελεστές της modulo p ώστε να πάρουμε μια νέα καμπύλη με συντελεστές στο σώμα $\mathbf{F}_p$:

$$\tilde{C}: \quad y^2 = x^3 + \tilde{a}x^2 + \tilde{b}x + \tilde{c}$$

Πότε θα είναι η $\tilde{C}$ μη-ιδιάζουσα (non-singular);

Όταν $p \geq 3$ και η διακρίνουσα

$$\tilde{D} = -4\tilde{a}^3\tilde{c} + \tilde{a}^2\tilde{b}^2 + 18\tilde{a}\tilde{b}\tilde{c} - 4\tilde{b}^3 - 27\tilde{c}^2$$

είναι διάφορη του μηδενός. Αλλά επειδή η αναγωγή modulo p είναι ομομορφισμός η διακρίνουσα $\tilde{D}$ είναι η αναγωγή modulo p της διακρίνουσας D της κυβικής καμπύλης C. Δηλαδή η $\tilde{C}$ είναι non-singular αν για τον πρώτο p ισχύει $p \geq 3$ και $p \nmid D$.

Έχοντας ανάγει την καμπύλη C είναι φυσιολογικό να πάρουμε σημεία πάνω στην C και να προσπαθήσουμε να τα ανάγουμε modulo p ώστε να πάρουμε σημεία πάνω στην $\tilde{C}$. Αυτό μπορούμε να το κάνουμε με την προϋπόθεση ότι οι συντεταγμένες του σημείου δεν έχουν p στον παρανομαστή τους. Ειδικότερα, αν τα σημείο έχει ακέραιες συντεταγμένες τότε μπορούμε να το ανάγουμε modulo p για κάθε πρώτο p.

Αν P = (x, y) ρητό σημείο της καμπύλης C με ακέραιες συντεταγμένες τότε τα x και y ικανοποιούν την εξίσωση:

$$y^2 = x^3 + ax^2 + bx + c$$

Αυτή η εξίσωση είναι σχέση ακεραίων άρα μπορούμε να την ανάγουμε modulo p και να πάρουμε την εξίσωση:

$$\tilde{y}^2 = \tilde{x}^3 + \tilde{a}\tilde{x}^2 + \tilde{b}\tilde{x} + \tilde{c}$$

Η παραπάνω εξίσωση μας λέει ότι το $\tilde{P} = (\tilde{x}, \tilde{y})$ είναι σημείο της ομάδας $\tilde{C}(\mathbf{F}_p)$. Άρα παίρνουμε μια απεικόνιση από τα στοιχεία της C(**Q**) με <u>ακέραιες συντεταγμένες</u> στην $\tilde{C}(\mathbf{F}_p)$.

Από το θεώρημα των Lutz - Nagell (θεώρημα 1.5.9) γνωρίζουμε ότι όλα τα σημεία πεπερασμένης τάξης της C(**Q**) έχουν ακέραιες συντεταγμένες (και μάλιστα y = 0 ή y διαιρεί την D(f) την διακρίνουσα του f(x)).

Τώρα θα μελετήσουμε το σύνολο των σημείων πεπερασμένης τάξης το οποίο θα συμβολίσουμε

$$\Phi := \{P = (x, y) \in C(\mathbf{Q}) : \mathrm{ord}(P) < +\infty\}$$

Προφανώς, το Φ είναι **υποομάδα** της C(**Q**) επειδή αν P_1, P_2 σημεία πεπερασμένης τάξης, έστω $m_1P_1 = O$ και έστω $m_2P_2 = O$ τότε ισχύει ότι $m_1m_2(P_1 - P_2) = m_1m_2P_1 - m_1m_2P_2 = O - O = O$. Άρα $P_1 - P_2 \in \Phi$.

Επειδή η Φ αποτελείται από σημεία με ακέραιες συντεταγμένες και το O, μπορούμε να ορίσουμε μια απεικόνιση αναγωγής modulo p.

$$\begin{cases} \Phi \to \tilde{C}(F_p) \\ P \mapsto \tilde{P} = \begin{cases} (\tilde{x},\tilde{y}) & \text{αν } P = (x,y) \\ \tilde{O} & \text{αν } P = O \end{cases} \end{cases}$$

Η Φ είναι ομάδα, υποομάδα της C(**Q**). Αν διαλέξουμε $p \nmid 2D$ τότε ξέρουμε ότι και η $\tilde{C}(\mathbf{F}_p)$ είναι επίσης ομάδα. Άρα έχουμε μια απεικόνιση από την ομάδα Φ στην ομάδα $\tilde{C}(\mathbf{F}_p)$. Θα αποδείξουμε τώρα ότι η παραπάνω απεικόνιση είναι ομομορφισμός ομάδων.

Πρώτα, παρατηρούμε ότι:

$$-P = (x, -y) = (\tilde{x}, -\tilde{y}) = -\tilde{P}$$

Αρκεί τώρα να δείξουμε ότι $P_1 + P_2 + P_3 = O \Rightarrow \tilde{P}_1 + \tilde{P}_2 + \tilde{P}_3 = O$. Θα πρέπει να διακρίνουμε περιπτώσεις.

Αν κάποιος από τους P_1, P_2, P_3 είναι O, π.χ. ο P_3, έχουμε: $P_1 + P_2 = O$ ή $P_1 = -P_2$. Τότε $\tilde{P}_1 = -P_2$ ή $\tilde{P}_1 = -\tilde{P}_2$ ή $\tilde{P}_1 + \tilde{P}_2 = \tilde{O}$ που είναι και το ζητούμενο.

Ας υποθέσουμε τώρα ότι P_1, P_2, P_3 είναι διάφοροι του O. Γράφουμε τις συντεταγμένες τους ως εξής:

$$P_1 = (x_1, y_1), \qquad P_2 = (x_2, y_2), \qquad P_3 = (x_3, y_3)$$

Από παρατήρηση 2.1.2 η συνθήκη $P_1 + P_2 + P_3 = O$ είναι ισοδύναμη με το να πούμε ότι τα P_1, P_2, P_3 είναι συνευθειακά. Όπως αποδείξαμε και στο προηγούμενο κεφάλαιο οι συντεταγμένες του P_3 προκύπτουν από την σχέση 1.5.12

$$x^3 + ax^2 + bx + c - (\lambda x + \nu)^2 = (x - x_1)(x - x_2)(x - x_3).$$

Αυτή είναι και η σχέση που μας εξασφαλίζει ότι $P_1 + P_2 + P_3 = O$ ανεξάρτητα με το γεγονός αν τα σημεία είναι διακεκριμένα ή όχι.

Ανάγοντας την τελευταία εξίσωση modulo p παίρνουμε:

$$x^3 + \tilde{a}x^2 + \tilde{b}x + \tilde{c} - (\tilde{\lambda}x + \tilde{\nu})^2 = (x - \tilde{x}_1)(x - \tilde{x}_2)(x - \tilde{x}_3)$$

Φυσικά, μπορούμε να ανάγουμε και τις εξισώσεις $y_i = \lambda x_i + \nu \ \left(i \in \{1,2,3\}\right)$ modulo p και να πάρουμε $\tilde{y}_i = \tilde{\lambda}\tilde{x}_i + \tilde{\nu} \ \left(i \in \{1,2,3\}\right)$. Αυτό σημαίνει ότι η ευθεία $y = \tilde{\lambda}x + \tilde{\nu}$ τέμνει την καμπύλη $\tilde{C}$ στα τρία σημεία $\tilde{P}_1, \tilde{P}_2, \tilde{P}_3$. Επιπλέον, αν δύο από τα σημεία $\tilde{P}_1, \tilde{P}_2, \tilde{P}_3$ ταυτίζονται π.χ. $\tilde{P}_1 = \tilde{P}_2$ τότε η ευθεία είναι η εφαπτόμενη της $\tilde{C}$ στο $\tilde{P}_1$, και αν $\tilde{P}_1 = \tilde{P}_2 = \tilde{P}_3$ τότε η ευθεία με την καμπύλη έχουν τριπλό σημείο επαφής. Συνεπώς, σε κάθε περίπτωση:

$$\tilde{P}_1 + \tilde{P}_2 + \tilde{P}_3 = O$$

το οποίο και αποδείχνει ότι η αναγωγή modulo p είναι ομομορφισμός από την Φ στην $\tilde{C}(\mathbf{F}_p)$.

Επιπλέον, είναι μονομορφισμός (ομομορφισμός ένας-προς-ένα) αφού ένα μη-μηδενικό σημείο (x, y) της Φ απεικονίζεται στο $(\tilde{x},\tilde{y}) \in \tilde{C}(\mathbf{F}_p)$ το οποίο είναι διάφορο του $\tilde{O}$. Επομένως, ο πυρήνας της απεικόνισης αναγωγής modulo p αποτελείται μόνο από το O. Αυτό ισοδυναμεί στο γεγονός ότι η απεικόνιση είναι ένα-προς-ένα.

Επομένως, η Φ θα είναι ισόμορφη με μια υποομάδα της $\tilde{C}(\mathbf{F}_p)$ για κάθε πρώτο p ($p \nmid 2D$). Αυτό θα μας φανεί χρήσιμο σε πολλές περιπτώσεις στο να βρούμε την Φ με πολύ λίγη δουλειά.

Πριν δώσουμε κάποια παραδείγματα ας διατυπώσουμε, ξανά, το θεώρημα που μόλις αποδείξαμε:

Θεώρημα 2.2.1 (**Θεώρημα Αναγωγής Modulo p**) Έστω C μια μη-ιδιάζουσα κυβική καμπύλη

$$C: \quad y^2 = x^3 + ax^2 + bx + c$$

με ακέραιες συντεταγμένες a, b, c και έστω D η διακρίνουσα

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

Έστω $\Phi \subseteq C(\mathbf{Q})$ η υποομάδα των σημείων πεπερασμένης τάξης της C. Για κάθε πρώτο p, έστω $P \to \widetilde{P}$ η απεικόνιση αναγωγής modulo p, με τύπο:

$$\begin{cases} \Phi \to \widetilde{C}(F_p) \\ P \mapsto \widetilde{P} = \begin{cases} (\widetilde{x}, \widetilde{y}) & \text{αν } P = (x, y) \\ \widetilde{O} & \text{αν } P = O \end{cases} \end{cases}$$

Αν $p \nmid 2D$ τότε η απεικόνιση είναι **ισομορφισμός** της Φ σε μια υποομάδα της $\widetilde{C}(\mathbf{F}_p)$.

Ας δώσουμε λοιπόν τρία παραδείγματα χρήσης του παραπάνω θεωρήματος για τον υπολογισμό των σημείων πεπερασμένης τάξης.

Παράδειγμα 2.2.2 $C: \ y^2 = x^3 + 3$

Η διακρίνουσα για αυτήν την καμπύλη είναι $D = -27 \cdot 3^2 = -243 = -3^5$, άρα υπάρχει ένας μονομορφισμός $\Phi \to \widetilde{C}(\mathbf{F}_p)$ για κάθε πρώτο $p \geq 5$.

Θα υπολογίσουμε τις ομάδες $\widetilde{C}(\mathbf{F}_5)$ και $\widetilde{C}(\mathbf{F}_7)$.

Στο σώμα $\mathbf{F}_5$ έχουμε:

x	$x^3 + 3 = y^2$	τετραγωνικό υπόλοιπο	y
0	3	ΟΧΙ	-
1	1+3 = 4	ΝΑΙ	2, 3
2	2^3+3 = 1	ΝΑΙ	1, 4
3	3^3+3 = 0	ΝΑΙ	0
4	4^3+3 = 2	ΟΧΙ	-

Άρα αν συνυπολογίσουμε και το Ο έχουμε ότι $\#\widetilde{C}(\mathbf{F}_5) = 6$.

Στο σώμα $\mathbf{F}_7$ έχουμε:

x	$x^3 + 3 = y^2$	τετραγωνικό υπόλοιπο	y
0	3	ΟΧΙ	-
1	4	ΝΑΙ	2, 5
2	4	ΝΑΙ	2, 5
3	2	ΝΑΙ	3, 4
4	4	ΝΑΙ	2, 5
5	2	ΝΑΙ	3, 4
6	2	ΝΑΙ	3, 4

Άρα αν συνυπολογίσουμε και το Ο έχουμε ότι $\#\widetilde{C}(\mathbf{F}_7) = 13$.

Επειδή $\Phi \le \widetilde{C}(\mathbf{F}_5)$ και $\Phi \le \widetilde{C}(\mathbf{F}_7)$ πρέπει $\#\Phi \mid \#\widetilde{C}(\mathbf{F}_5)$ και $\#\Phi \mid \#\widetilde{C}(\mathbf{F}_7)$.
Δηλαδή $\#\Phi \mid 6$ και $\#\Phi \mid 13$. Αλλά $(6,13) = 1$. Άρα $\#\Phi = 1$. Με άλλα λόγια η C δεν έχει άλλα σημεία πεπερασμένης τάξης πλην του Ο.

Παρατηρούμε ότι το $(1, 2) \in C(\mathbf{Q})$ και σύμφωνα με τα παραπάνω έχει άπειρη τάξη. Άρα η καμπύλη C έχει άπειρα ρητά σημεία.

Έχει αξία να συγκρίνουμε την μέθοδο που χρησιμοποιήσαμε με την μέθοδο που προκύπτει από το θεώρημα των Lutz – Nagell (θεώρημα 1.5.9) και την πρόταση 1.5.10. Χρησιμοποιώντας την πρόταση 1.5.10 πρέπει να αποδείξουμε ότι <u>δεν</u> υπάρχουν σημεία της C τέτοια ώστε το τετράγωνο της y-συντεταγμένης να διαιρεί το –243 δηλαδή σημεία τέτοια ώστε $y \in \{\pm1, \pm3, \pm9, \pm27, \pm81\}$. Εύκολα φαίνεται ότι για $y = \pm1$ έχουμε $1 = x^3 + 3$ ή $x^3 = -2$ η οποία δεν μας δίνει ρητά σημεία. Έστω τώρα ότι $3 \mid y$ τότε από την εξίσωση $y^2 = x^3 + 3$ φαίνεται ότι πρέπει και $3 \mid x$ τότε όμως γράφουμε $3 = y^2 - x^3$. Έχουμε ότι $9 \mid y^2 - x^3$ άρα πρέπει $9 \mid 3$ το οποίο είναι <u>άτοπο</u>. Συνεπώς και με το θεώρημα των Lutz – Nagell αποδείξαμε ότι $\#\Phi = 1$.

<u>Παράδειγμα 2.2.3</u> $\quad C: \; y^2 = x^3 + x$

Η διακρίνουσα για αυτήν την καμπύλη είναι $D = -4 \cdot 1^3 = -4$. Επειδή η διακρίνουσα είναι σχετικά μικρή φαίνεται να πλεονεκτεί το θεώρημα των Lutz – Nagell, εμείς όμως θα χρησιμοποιήσουμε το θεώρημα αναγωγής. Έχουμε μια ένα-προς-ένα απεικόνιση $\Phi \to \widetilde{C}(\mathbf{F}_p)$ για κάθε πρώτο $p \ge 3$.

Κάνουμε κάποιους πρώτους υπολογισμούς:

Στο σώμα $\mathbf{F}_3$ έχουμε:

x	$x^3 + x = y^2$	y
0	0	0
1	2	-
2	1	1, 2

Άρα αν συνυπολογίσουμε και το Ο έχουμε ότι $\#\widetilde{C}(\mathbf{F}_3) = 4$.

Στο σώμα $\mathbf{F}_5$ έχουμε:

x	$x^3 + x = y^2$	y
0	0	0
1	2	-
2	0	0
3	0	0
4	3	-

Άρα αν συνυπολογίσουμε και το Ο έχουμε ότι $\#\widetilde{C}(\mathbf{F}_5) = 4$.

Στο σώμα $\mathbf{F}_7$ έχουμε:

x	$x^3 + x = y^2$	y
0	0	0
1	2	3, 4
2	3	-
3	2	3, 4
4	5	-
5	4	2, 5
6	5	-

Άρα αν συνυπολογίσουμε και το Ο έχουμε ότι $\#\widetilde{C}(\mathbf{F}_7) = 8$.

Θα αποδείξουμε τώρα ότι $4 \mid \#\widetilde{C}(\mathbf{F}_p)$ για κάθε πρώτο $p \geq 3$.

Δύο προφανή σημεία της καμπύλης

$$\widetilde{C}: \quad y^2 = x(x^2 + 1) \qquad (1)$$

είναι το Ο και το (0, 0).

Διακρίνουμε δύο περιπτώσεις:

- Αν $p \equiv 1 \pmod 4$ τότε $\left(\frac{-1}{p}\right) = 1$ άρα υπάρχει $x_0 \in \mathbf{F}_p$ τέτοιο ώστε $x_0^2 \equiv -1 \pmod p$.
Επομένως, τα σημεία $(x_0, 0)$ και $(-x_0, 0)$ είναι κι αυτά σημεία της (1). Μέχρι εδώ έχουμε βρει τέσσερα σημεία.

Επιπλέον, αν για κάποιο x_1 ισχύει $x_1(x_1^2 + 1) = c$ όπου c είναι τετραγωνικό υπόλοιπο mod p διάφορο του μηδενός τότε η $y^2 = c$ έχει δύο λύσεις, έστω y_1 και y_2. Δηλαδή, τα σημεία (x_1, y_1) και (x_1, y_2) ανήκουν στην (1). Ακόμα ισχύει ότι $-x_1((-x_1)^2+1) = -c$ και $\left(\frac{-c}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{c}{p}\right) = \left(\frac{c}{p}\right)$. Επομένως, η $y^2 = -c$ έχει δύο λύσεις, έστω y_3 και y_4, και τα σημεία $(-x_1, y_3)$ και $(-x_1, y_4)$ ανήκουν στην (1). Δηλαδή παίρνουμε τετράδες λύσεων.

Οπότε, $4 \mid \#\widetilde{C}(\mathbf{F}_p)$.

- Αν $p \equiv 3 \pmod 4$ τότε $\left(\frac{-1}{p}\right) = -1$ και επομένως ισχύει $\left(\frac{-c}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{c}{p}\right) = -\left(\frac{c}{p}\right)$.

Αν για κάποιο x_1 ισχύει $x_1(x_1^2 + 1) = c$ όπου c είναι τετραγωνικό υπόλοιπο mod p διάφορο του μηδενός τότε η $y^2 = c$ έχει δύο λύσεις. Αν το c δεν είναι τετραγωνικό υπόλοιπο mod p τότε για το $-x_1$ ισχύει $-x_1((-x_1)^2+1) = -c$ όπου το –c είναι τετραγωνικό υπόλοιπο mod p. Άρα, μαζί με τις δύο προφανείς λύσεις, θα έχουμε συνολικά $\frac{p-1}{2} \cdot 2 + 2 = p + 1$ σημεία πάνω στην $\widetilde{C}$. Ισχύει $p + 1 \equiv 3+1 \equiv 0 \pmod 4$.
Οπότε, και πάλι, $4 \mid \#\widetilde{C}(\mathbf{F}_p)$.

Ας κοιτάξουμε τις ομάδες $\widetilde{C}(\mathbf{F}_3)$ και $\widetilde{C}(\mathbf{F}_5)$:

$$\widetilde{C}(\mathbf{F}_3) = \{O, (0, 0), (2, 1), (2, 2)\}$$
$$\widetilde{C}(\mathbf{F}_5) = \{O, (0, 0), (2, 0), (3, 0)\}$$

Επειδή για ένα σημείο P = (x, y) ισχύει –P = (x, –y) έχουμε ότι το σημείο P έχει τάξη δύο αν και μόνο αν y = 0. Άρα η $\widetilde{C}(\mathbf{F}_3)$ έχει μόνο ένα σημείο τάξης δύο ενώ η $\widetilde{C}(\mathbf{F}_5)$ έχει τρία. Άρα

$$\widetilde{C}(\mathbf{F}_3) \cong \mathbf{Z}_4, \qquad \widetilde{C}(\mathbf{F}_5) \cong \mathbf{Z}_2 \times \mathbf{Z}_2$$

Επειδή $\Phi \le \widetilde{C}(\mathbf{F}_3)$ και $\Phi \le \widetilde{C}(\mathbf{F}_5)$ οι μόνες περιπτώσεις είναι είτε η Φ να είναι τετριμμένη είτε κυκλική τάξης 2. Παρατηρούμε ότι $(0, 0) \in C(\mathbf{Q})$ και είναι τάξης δύο, άρα συμπεραίνουμε ότι $\Phi = \{O, (0, 0)\}$.

Παράδειγμα 2.2.4 $\qquad C : y^2 = x^3 - 43x + 166$

Η διακρίνουσα για αυτήν την καμπύλη είναι $D = -4\cdot(-43)^3 - 27\cdot 166^2 = -425984 = -2^{15}\cdot 13$.

Θα προσπαθήσουμε να βρούμε ένα σημείο της καμπύλης με ακέραιες συντεταγμένες χρησιμοποιώντας το ισχυρότερο του θεωρήματος των Lutz – Nagell (πρόταση 1.5.10). Έστω $P = (x, y) \in C$ σημείο με ακέραιες συντεταγμένες. Πρέπει $y^2 \mid D$.

Δοκιμάζουμε για $y = \pm 1$:
Έχουμε $1 = x^3 - 43x + 166$ ή $x(x^2 - 43) = -165$ ή $x(x^2 - 43) = -3 \cdot 5 \cdot 11$. Επειδή η εξίσωση $x^2 \equiv 43 \pmod p$ είναι αδύνατη για p = 3, 5, 11 θα πρέπει $x^2 - 43 = \pm 1$. Δηλαδή $x^2 = 42$ είτε $x^2 = 44$. Άτοπο για x ακέραιο.

Δοκιμάζουμε για $y = \pm 2$:

Έχουμε $4 = x^3 - 43x + 166$ ή $x(x^2 - 43) = -162$ ή $x(x^2 - 43) = -2 \cdot 3^4$. Επειδή η εξίσωση $x^2 \equiv 43 \pmod 3$ είναι αδύνατη θα πρέπει $x^2 - 43 = \pm 1, \pm 2$. Δηλαδή $x^2 = 41, 42, 44, 45$. Άτοπο για x ακέραιο.

Δοκιμάζουμε για $y = \pm 4$:
Έχουμε $16 = x^3 - 43x + 166$ ή $x(x^2 - 43) = -150$ ή $x(x^2 - 43) = -2 \cdot 3 \cdot 5^2$. Επειδή η εξίσωση $x^2 \equiv 43 \pmod p$ είναι αδύνατη για $p = 3, 5$ θα πρέπει $x^2 - 43 = \pm 1, \pm 2$. Δηλαδή $x^2 = 41, 42, 44, 45$. Άτοπο για x ακέραιο.

Δοκιμάζουμε για $y = \pm 8$:
Έχουμε $64 = x^3 - 43x + 166$ ή $x(x^2 - 43) = -102$. Η εξίσωση αυτή έχει λύση $x = 3$.

Άρα το σημείο $P = (3, 8)$ μπορεί να έχει πεπερασμένη τάξη.

Για να προσδιορίσουμε τη τάξη του στοιχείου P ας πάρουμε την αναγωγή της καμπύλης C modulo 5 και ας υπολογίσουμε τη ομάδα $\widetilde{C}(\mathbf{F}_5)$:

$$\widetilde{C} : \quad y^2 = x^3 + 2x + 1$$

x	$x^3 + 2x + 1 = y^2$	y
0	1	1, 4
1	4	2, 3
2	3	-
3	4	2, 3
4	3	-

Άρα αν συνυπολογίσουμε και το O έχουμε ότι $\#\widetilde{C}(\mathbf{F}_5) = 7$.

Επομένως, αν $\mathrm{ord}(P) > 7$ τότε $\mathrm{ord}(P) = +\infty$. Υπολογίζουμε το 2P:

$a = 0, b = -43, x_1 = 3, y_1 = 8, \lambda = \dfrac{3 \cdot 3^2 - 43}{2 \cdot 8} = -1, \nu = y_1 - \lambda x_1 = 8 + 3 = 11.$

Άρα, $2P = (x_3, y_3)$ όπου $x_3 = (-1)^2 - 6 = -5$ και $y_3 = -5 - 11 = -16$. Δηλαδή έχουμε ότι $2P = (-5, -16)$. Ανάλογα βρίσκουμε ότι $3P = (11, -32)$, $4P = (11, 32)$, $5P = (-5, 16)$ και $6P = (3, -8) = -P$. Άρα $7P = O$ και $\mathrm{ord}(P) = 7$. Επειδή $\Phi \leq \widetilde{C}(\mathbf{F}_5)$ και $P \in \Phi$ ισχύει ότι $\Phi \cong \mathbf{Z}_7$ και μάλιστα

$$\Phi = \langle P \rangle = \{O, (3, \pm 8), (-5, \pm 16), (11, \pm 32)\}.$$

Ένα δύσκολο πρόβλημα είναι να καθοριστούν ποιες τιμές είναι πιθανές για την τάξη των σημείων πεπερασμένης τάξης μιας ελλειπτικής καμπύλης. Αναφέρουμε χωρίς απόδειξη το πολύ όμορφο αλλά και πολύ δύσκολο

Θεώρημα 2.2.5 (Mazur, 1976) Έστω E μια μη-ιδιάζουσα κυβική καμπύλη ορισμένη στο σώμα **Q** των ρητών αριθμών. Έστω ότι η E(**Q**) περιέχει ένα σημείο

πεπερασμένης τάξης m. Τότε $1 \leq m \leq 10$ είτε $m = 12$. Πιο συγκεκριμένα, η ομάδα των σημείων πεπερασμένης τάξης της E είναι ισόμορφη με μια από εξής ομάδες:

(i) $\mathbf{Z}_N$ με $1 \leq N \leq 10$ είτε $N = 12$
(ii) $\mathbf{Z}_2 \times \mathbf{Z}_{2N}$ με $1 \leq N \leq 4$.

(Δες [S1], σελίδα 58)

3. Η εικασία του Riemann

(για αλγεβρικά σώματα συναρτήσεων μια μεταβλητής με συντελεστές από το πεπερασμένο σώμα $\mathbf{F}_q$)

Έχουμε δει ότι για κάθε πρώτο p υπάρχει ένα σώμα $\mathbf{F}_p$ με p στοιχεία. Μάλιστα, δοθέντος πρώτου p και ακεραίου $r \geq 1$ υπάρχει ακριβώς ένα σώμα $\mathbf{F}_q$ με $q = p^r$ στοιχεία. Το σώμα $\mathbf{F}_q$ περιέχει το $\mathbf{F}_p$ και για κάθε α στο $\mathbf{F}_q$ ισχύει $p\alpha = 0$. Αντιστρόφως, κάθε πεπερασμένο σώμα είναι ισόμορφο προς κάποιο $\mathbf{F}_q$ για κάποιο $q = p^r$. Το σώμα $\mathbf{F}_q$ χαρακτηρίζεται από την ιδιότητα όλα τα στοιχεία του να είναι ακριβώς οι ρίζες του πολυωνύμου

$$f(X) = X^q - X$$

δηλαδή

$$f(X) = \prod_{\alpha \in F_q} (X - \alpha)$$

Πρόταση 2.3.1 Έστω K σώμα το οποίο περιέχει το $\mathbf{F}_q$. Η απεικόνιση $Fr: K \to K$ με τύπο $Fr(x) = x^q$ είναι ένας **$\mathbf{F}_q$-ενδομορφισμός** του δακτυλίου K. (Ενδομορφισμός για τον οποίο ισχύει $Fr(\alpha) = \alpha$ για κάθε $\alpha \in \mathbf{F}_q$).

Απόδειξη Έστω $x, y \in K$. Τότε

1. $(x + y)^q = x^q + y^q$
2. $(xy)^q = x^q y^q$ και $\alpha^q = \alpha$ αν $\alpha \in \mathbf{F}_q$.

Ο δεύτερος ισχυρισμός δεν χρειάζεται απόδειξη.
Ο πρώτος έπεται από το γεγονός ότι για τους διωνυμικούς συντελεστές στη σχέση

$$(x + y)^q = \sum_{j=0}^{q} \binom{q}{j} x^j y^{q-j}$$

για $j = 1, \ldots, q - 1$, ισχύει $\binom{q}{j} = \frac{q!}{j!(q-j)!} = \frac{(q-j+1)(q-j+2)\cdot\ldots\cdot q}{1\cdot 2\cdot\ldots\cdot k}$. Μπορούμε να γράψουμε τη σχέση σαν $(q-j-+1)(q-j+2)\cdot\ldots\cdot q = \binom{q}{j}\cdot 1\cdot 2\cdot\ldots\cdot k$. Ο $q = p^r$ διαιρεί το αριστερό μέρος της σχέσης και δεν διαιρεί του 1, 2,…, k άρα διαιρεί το $\binom{q}{j}$, και επειδή η χαρακτηριστική του σώματος είναι p, μόνο ο πρώτος και ο τελευταίος όρος του αθροίσματος «επιζούν», αφού $\binom{q}{0} = \binom{q}{q} = 1$ ενώ όλοι υπόλοιποι όροι είναι μηδέν.

Έτσι, η απεικόνιση Fr: $K \to K$ είναι ένας $\mathbf{F}_q$-ενδομορφισμός του δακτυλίου K, ο οποίος μάλιστα ονομάζεται **ενδομορφισμός του Frobenius**. Ο ενδομορφισμός του Frobenius επεκτείνεται φυσιολογικά, κατά συνιστώσες, στον αφινικό και προβολικό χώρο.

Ενδιαφερόμαστε να υπολογίσουμε το πλήθος N_q των λύσεων στο $\mathbf{F}_q \times \mathbf{F}_q$ της εξίσωσης

$$Y^2 = f(X)$$

όπου $f(X) = AX^3 + BX^2 + CX + D \in \mathbf{F}_q[X]$, πολυώνυμο τρίτου βαθμού ($A \neq 0$) χωρίς πολλαπλές ρίζες (έχει μόνο απλές). Υποθέτουμε ότι $p \neq 2, 3$ άρα, όπως δείξαμε στο κεφάλαιο 1, η εξίσωση μπορεί να γραφεί στη μορφή του Weierstrass (βλέπε ορισμό 1.4.7):

$$Y^2 = X^3 + bX + c$$

για κάποια $b, c \in \mathbf{F}_q$. Μαζί με το επ' άπειρον σημείο **O**, οι λύσεις αυτές σχηματίζουν μια αβελιανή ομάδα τάξης $N'_q = N_q + 1$. Αυτή είναι η ομάδα των $\mathbf{F}_q$ ρητών σημείων της ελλειπτικής καμπύλης E που καθορίζεται από την παραπάνω εξίσωση. Έστω $q = p$. Το 1924, ο Artin υπέθεσε την παρακάτω προσέγγιση για το N_p : $|N_p - p| \leq 2\sqrt{p}$. Στην πραγματικότητα, ένας ισοδύναμος τύπος αυτής της ανισότητας είναι το ανάλογο για το σώμα των ρητών συναρτήσεων που αντιστοιχεί πάνω στην καμπύλη E με αυτό που υπέθεσε ο Riemann πολύ νωρίτερα για το σώμα των ρητών αριθμών, και είναι ευρέως γνωστό ως η εικασία του Riemann. Ο Gauss ήταν ο πρώτος που μελέτησε τη συμπεριφορά του N_p για τις διάφορες τιμές του p για την καμπύλη

$$Y^2 = X^3 - 432$$

Στην πραγματικότητα έδωσε έναν ακριβή τύπο για το N_p.

Θεώρημα 2.3.2 (Gauss, 1801) Έστω N_p το πλήθος των λύσεων στο $\mathbf{F}_p \times \mathbf{F}_p$ της εξίσωσης $Y^2 = X^3 - 432$, $p \neq 2, 3$. Τότε

1. $N_p = p$ για $p \equiv 2 \pmod 3$
2. Αν $p \equiv 1 \pmod 3$, υπάρχουν ακέραιοι A, B μοναδικοί κατά προσέγγιση προσήμου, τέτοιοι ώστε $4p = A^2 + 27B^2$. Αν το πρόσημο του A επιλεχθεί έτσι ώστε να ισχύει $A \equiv 1 \pmod 3$, τότε $N_p = p + A - 2$. Συγκεκριμένα, $|N_p - p| \leq 2\sqrt{p}$.

Η εικασία του Artin αποδείχθηκε από τον Hasse το 1936. Αργότερα, το 1948 ο Weil τη γενίκευσε στο περίφημο θεώρημά του (η εικασία του Riemann για καμπύλες πάνω από πεπερασμένα σώματα) και έκανε κάποιες εικασίες, γνωστές και σαν εικασίες του Weil.

Θεώρημα 2.3.3 **Η εικασία του Riemann για καμπύλες πάνω από πεπερασμένα σώματα** (Weil). Το πλήθος N_q των σημείων με συντεταγμένες στο $\mathbf{F}_q$ πάνω σε μια

ανάγωγη, μη – ιδιάζουσα καμπύλη ορισμένη πάνω από το $\mathbf{F}_q$ και γένους g ικανοποιεί την ανισότητα

$$|N_q - q| \leq 2g\sqrt{q} \quad (1)$$

Ο Manin έδωσε μια πλήρη στοιχειώδη απόδειξη του θεωρήματος του Hasse και μια απόδειξη με χρήση θεωρίας εκτιμήσεων οφείλεται στον Zimmer. Η απόδειξη του Weil της εικασίας του Riemann εξαρτάται σε μεγάλο βαθμό από την αλγεβρική γεωμετρία. Μια κάπως απλούστερη απόδειξη δόθηκε από τον Roquette. Αργότερα μια στοιχειώδης απόδειξη ξεκίνησε από τον Stepanov και ολοκληρώθηκε από τον W. Schmidt. Μια πολύ κομψή, μα λιγότερο στοιχειώδης απόδειξη βασισμένη στη μέθοδο του Stepanov δόθηκε από τον Bombieri. Για περισσότερα ιστορικά στοιχεία παραπέμπουμε τον ενδιαφερόμενο αναγνώστη στα [Ch1] και [Ch2]. Εμείς εδώ θα περιοριστούμε στην απόδειξη του θεωρήματος του Hasse ακολουθώντας την απόδειξη του Manin.

Θεώρημα 2.3.4 (Hasse, 1936) Έστω $p \neq 2, 3$. Το πλήθος N_p των λύσεων στο $\mathbf{F}_p \times \mathbf{F}_p$ της ελλειπτικής καμπύλης

$$Y^2 = X^3 + bX + c$$

όπου $a, b \in \mathbf{F}_p$ με $\Delta = -4b^3 - 27c^2$ στο $\mathbf{F}_p^*$ τότε το N_p ικανοποιεί την ανισότητα

$$|N_p - p| \leq 2\sqrt{p}$$

Παρατήρηση 2.3.5 Αν η καμπύλη είναι προβολική, υπάρχει ένα επιπλέον σημείο (το επ' άπειρον σημείο). Τότε ο συνολικός αριθμός των σημείων είναι $N'_q = N_q + 1$ και ο τύπος του θεωρήματος 2.3.3 γίνεται

$$|N'_q - (q + 1)| \leq 2g\sqrt{q}$$

Στη συνέχεια θα εξηγήσουμε γιατί το θεώρημα του Hasse λέγεται και εικασία του Riemann για την ελλειπτική καμπύλη. Κατ' αρχήν υπενθυμίζουμε ότι η ζ-ήτα συνάρτηση του Riemann ορίζεται ως εξής $\zeta(s) = \sum_{n \in N} n^{-s}$, για $s \in \mathbf{C}$ με $\mathrm{Re}(s) > 1$. Αποδεικνύεται ότι η συνάρτηση επεκτείνεται αναλυτικά σ' όλο το μιγαδικό επίπεδο εκτός από τον μοναδικό, απλό, πόλο για $s = 1$. Επιπλέον επαληθεύει μια συναρτησιακή εξίσωση η οποία συνδέει την $\zeta(s)$ με την $\zeta(1 - s)$. Ακριβέστερα, αν $\xi(s) = \pi^{-\frac{s}{2}} \Gamma(\frac{s}{2}) \zeta(s)$ τότε ισχύει $\xi(s) = \xi(1 - s)$, όπου $\Gamma(s)$ είναι η γνωστή Γ-συνάρτηση.

Η εικασία του Riemann αναφέρεται στην υπόθεση ότι όλες οι ρίζες της συνάρτησης $\zeta(s)$ για $0 \leq \mathrm{Re}(s) \leq 1$ βρίσκονται πάνω στον άξονα με $\mathrm{Re}(s) = \frac{1}{2}$. Για ελλειπτικές καμπύλες τώρα Ε ορισμένες πάνω από ένα πεπερασμένο σώμα $\mathbf{F}_p$ η ζήτα συνάρτηση ορίζεται ως

$$Z(E|_{F_p}, T) = \frac{1 - \alpha_p T + pT^2}{(1-T)(1-pT)},$$

όπου $\alpha_p = \alpha_p(E) = p - N_p$. Παραλείπουμε εδώ να αναφέρουμε τις ιδιότητες της συνάρτησης αυτής, ανάλογες της ζ-ήτα συνάρτησης του Riemann. Λόγω του θεωρήματος του Hasse, έπεται ότι το τριώνυμο $pT^2 - \alpha_p T + 1$ έχει διακρίνουσα

$$\Delta(E) = \alpha_p^2 - 4p < 0.$$

Οι δύο ρίζες του τριωνύμου θα είναι επομένως συζυγείς μιγαδικές, έστω a και $\bar{a}$. Επομένως, θα έχουμε:

$$1 - \alpha_p T + pT^2 = (1 - aT)(1 - \bar{a}T)$$

όπου $a + \bar{a} = \alpha_p$ και $|a| = |\bar{a}| = \sqrt{p}$.

Αν τώρα αλλάξουμε τη μεταβλητή $T = p^{-s}$ όπου $s = \sigma + it \in \mathbf{C}$ και ορίσουμε

$$\zeta(E|_{F_p}, s) := Z(E|_{F_p}, p^{-s}) = \frac{1 - \alpha_p p^{-s} + p^{1-2s}}{(1-p^{-s})(1-p^{1-s})}$$

Έχουμε:

$\zeta(E|_{F_p}, s) = 0$ τότε και μόνο τότε όταν $1 - ap^{-s} = 0$ ή $1 - \bar{a}p^{-s} = 0$. Δηλαδή ότι $p^s = a$ ή $p^s = \bar{a}$. Τώρα, επειδή $|p^s| = p^{Re(s)} = p^\sigma$ έχουμε ότι η σχέση $|p^s| = \sqrt{p}$ είναι ισοδύναμη με $\sigma = \frac{1}{2}$, δηλαδή την αλήθεια της εικασίας του Riemann για την $\zeta(E|_{F_p}, s)$. Παρατηρούμε λοιπόν ότι η εικασία του Riemann για την συνάρτηση $\zeta(E|_{F_p}, s)$ είναι ισοδύναμη με το ότι $|a| = |\bar{a}| = \sqrt{p}$. Για το πολυώνυμο $P(T)= 1 - \alpha_p T + pT^2$ ισχύει ότι $|\alpha_p| = |a + \bar{a}| \le |a| + |\bar{a}| = 2\sqrt{p}$. Δηλαδή $|N_p - p| \le 2\sqrt{p}$. Αποδείξαμε ότι η εικασία του Riemann για την συνάρτηση $\zeta(E|_{F_p}, s)$ συνεπάγεται το θεώρημα του Hasse και αντιστρόφως.

4. Η κατά Manin απόδειξη του θεωρήματος του Hasse

Πρώτα πρώτα, ας επισημάνουμε ότι το θεώρημα του Hasse:

Αν p πρώτος διάφορος του 2 και του 3 και N_p το πλήθος των λύσεων στο $F_p \times F_p$ της εξίσωσης

$$\mathbf{Y^2 = X^3 + bX + c}$$

όπου $b, c \in F_q$ με $\Delta = -4b^3 - 27c^2$ στο F_p^* τότε το N_p ικανοποιεί την ανισότητα

$$\mathbf{|N_p - p| \le 2\sqrt{p}},$$

ισχύει και στην περίπτωση που θα αντικαταστήσουμε το p με $q = p^r$.

Ορισμός 2.4.1 Έστω E_1, E_2 δύο ελλειπτικές καμπύλες πάνω από ένα σώμα K. Τότε η E_1 είναι ένα **twist** της E_2 αν οι E_1 και E_2 γίνονται ισόμορφες πάνω από μια πεπερασμένη επέκταση L του K.

Παράδειγμα 2.4.2 Έστω E_1, E_2 δύο ελλειπτικές καμπύλες πάνω από το σώμα **Q** των ρητών αριθμών, που δίνονται από τις εξισώσεις

$$E_1 : Y^2 = X^3 + bX + c$$

$$E_2 : d\,Y^2 = X^3 + bX + c$$

όπου $a, b, d \in \mathbf{Z}$ και d ελεύθερος τετραγώνου (square-free).

Οι E_1 και E_2 δεν είναι ισόμορφες στο **Q**, αν όμως πάρουμε την πεπερασμένη επέκταση $L = \mathbf{Q}(\sqrt{d})$, τότε η E_2 γράφεται στο L:

$$E_2 : (\sqrt{d}\,Y)^2 = X^3 + bX + c$$

Τότε **υπάρχει** ισομορφισμός $\Phi : E_1 \to E_2$ που ορίζεται από $(X, Y) \mapsto (X, \sqrt{d}\,Y)$. Επομένως η $E_1|_{\mathbf{Q}}$ είναι twist της $E_2|_{\mathbf{Q}}$.

Πρόταση 2.4.3 Έστω $K = \mathbf{F}_p(x)$ το σώμα των ρητών συναρτήσεων μιας μεταβλητής πάνω από το $\mathbf{F}_p$ και ας υποθέσουμε ότι το E είναι η ελλειπτική καμπύλη με εξίσωση:

$$E : Y^2 = X^3 + bX + c \quad (b, c \in \mathbf{F}_p) \qquad (1)$$

Η E ορίζεται πάνω από το $\mathbf{F}_p$ άρα και πάνω από το $K = \mathbf{F}_p(x)$

Αν E_λ είναι η ελλειπτική καμπύλη που δίνεται από την εξίσωση

$$E_\lambda : \lambda\, Y^2 = X^3 + bX + c \qquad (2)$$

όπου $\lambda = \lambda(x) = x^3 + bx + c \in K = \mathbf{F}_p(x)$

τότε οι Ε και E_λ ορίζονται και οι δύο πάνω από το Κ και η E_λ είναι μια twist της Ε πάνω από το Κ.

Απόδειξη Όπως και στο παράδειγμα, παίρνουμε την πεπερασμένη επέκταση L = $K(\sqrt{\lambda})$, τότε οι Ε και E_λ ορίζονται πάνω από το L και η E_λ γράφεται:

$$E_\lambda : (\sqrt{\lambda}\, Y)^2 = X^3 + bX + c$$

Τότε **υπάρχει** ισομορφισμός $\Phi_\lambda : E \to E_\lambda$ με τύπο $(X, Y) \mapsto (X, \sqrt{\lambda}\, Y)$. Επομένως η $E|_K$ είναι twist της $E_\lambda|_K$.

Για να αποδείξουμε το θεώρημα του Hasse, πρέπει να θεωρήσουμε την ομάδα $E_\lambda(K)$ των Κ-ρητών σημείων πάνω στην E_λ.

Έστω $P = (X_1, Y_1)$, $Q = (X_2, Y_2)$, $P+Q = (X_3, Y_3) = (X_1, Y_1) + (X_2, Y_2) \in E_\lambda(K)$. Θα δώσουμε κάποιους τύπους αντίστοιχους με τους 1.5.14 και 1.5.15 που θα μας επιτρέπουν να υπολογίζουμε το P+Q εύκολα.

Αν $X_1 \neq X_2$, όπως και στο κεφάλαιο 1, γράφουμε την ευθεία L που ορίζουν τα P και Q στη μορφή $Y = \kappa X + \nu$ όπου τα κ και ν δίνονται από τους τύπους $\kappa = \dfrac{Y_2 - Y_1}{X_2 - X_1}$ και $\nu = Y_1 - \kappa X_1 = Y_2 - \kappa X_2$. Από την κατασκευής της η ευθεία L τέμνει την καμπύλη Ε στα σημεία P, Q. Για να υπολογίσουμε το τρίτο σημείο τομής PQ αντικαθιστούμε το Y από την προηγούμενη σχέση στον τύπο της Ε.

$$\lambda(\kappa X + \nu)^2 = X^3 + bX + c$$

ή αλλιώς

$$X^3 - \lambda\kappa^2 X^2 + (b - 2\lambda\kappa\nu)X + (c - \nu^2) = 0$$

Η τελευταία σχέση είναι μια εξίσωση τρίτου βαθμού ως προς Χ και έχει σαν ρίζες τα X_1, X_2, X_3 οπότε ισχύει:

$$X^3 - \lambda\kappa^2 X^2 + (b - 2\lambda\kappa\nu)X + (c - \nu^2) = (X - X_1)(X - X_2)(X - X_3) \qquad (2.4.4)$$

Επομένως, ισχύει: $X_1 + X_2 + X_3 = -(-\lambda\kappa^2)$ ή αλλιώς

$$X_3 = \lambda\kappa^2 - X_1 - X_2 \text{ και } Y_3 = \kappa X_3 + \nu \qquad (2.4.5)$$

οπότε, αντικαθιστώντας και τα κ και ν, έχουμε

$$X_3 = \lambda\left(\frac{Y_2 - Y_1}{X_2 - X_1}\right)^2 - (X_1 + X_2) \text{ και } Y_3 = \frac{Y_2 - Y_1}{X_2 - X_1}(X_3 - X_1) + Y_1 \qquad (2.4.6)$$

Ανάλογα αν $(X, Y) = 2(X_1, Y_1)$ τότε

Από την σχέση $\lambda Y^2 = X^3 + bX + c$ έχουμε ότι $\kappa = \left.\frac{dY}{dX}\right|_{(X_1,Y_1)} = \frac{3X_1^2 + b}{2\lambda Y_1}$.

Αντικαθιστούμε το κ στους τύπους 1.5.12 και το λY^2 με $X^3 + aX + b$ και βρίσκουμε:

$$X_3 = \frac{(3X_1^2 + b)^2}{4(X_1^3 + bX_1 + c)} - 2X_1 = \frac{X_1^4 - 2bX_1^2 - 8cX_1 + b^2}{4(X_1^3 + bX_1 + c)} \qquad (2.4.7)$$

Αν στην εξίσωση (2) θέσουμε $X = x \in K = F_p(x)$, τότε έχουμε:

$$\lambda Y^2 = x^3 + bx + c \text{ ή } \lambda Y^2 = \lambda \text{ ή } Y^2 = 1 \text{ ή } Y = \pm 1.$$

Άρα δύο λύσεις της (2) είναι

$$(x, 1) \text{ και } (x, -1) = -(x, 1)$$

Μία λιγότερο προφανής λύση είναι:

$$X_0 = x^p, \qquad Y_0 = (x^3 + bx + c)^{\frac{p-1}{2}}$$

Πράγματι, αν (X_0, Y_0) σημείο της E_λ με $X_0 = x^p$ τότε $\lambda Y_0^2 = (x^p)^3 + bx^p + c$ ή λόγω της πρότασης 2.3.1:

$$\lambda Y_0^2 = (x^3 + bx + c)^p$$

Ισχύει: $(x^3 + bx + c)^p = (x^3 + bx + c)(x^3 + bx + c)^{p-1} = \lambda \left((x^3 + bx + c)^{\frac{p-1}{2}} \right)^2$.

Επομένως, $\lambda Y_0^2 = \lambda \left((x^3 + bx + c)^{\frac{p-1}{2}} \right)^2$ ή $Y_0^2 = \left((x^3 + bx + c)^{\frac{p-1}{2}} \right)^2$.

Από την τελευταία σχέση προκύπτει και η ορθότητα του ισχυρισμού αφού

$$(x^3 + bx + c)^{\frac{p-1}{2}} = \lambda^{\frac{p-1}{2}} \in K.$$

Έστω $(X_n, Y_n) = (X_0, Y_0) + n(x, 1) \quad n \in \mathbf{Z}$ (2.4.8)

Αν $(X_n, Y_n) \neq 0$ αποδεικνύεται ότι $X_n \neq 0$. (Δες παρακάτω λήμμα 2.5.1)

Γράφουμε το X_n σαν ανάγωγο κλάσμα στη μορφή $X_n = \frac{P_n}{Q_n}$ όπου $Q_n, P_n \in \mathbf{F}_p[x]$ και P_n μονικό και ορίζουμε την συνάρτηση:

$$d: \mathbf{Z} \to \{0, 1, 2, 3, ...\}$$

όπου

$$d(n) = d_n = \begin{cases} 0, & \text{αν } (X_n, Y_n) = 0 \\ \deg(P_n), & \text{αλλιώς} \end{cases}$$

Σύμφωνα με τον ορισμό του P_n η συνάρτηση d είναι καλά ορισμένη.

Η απόδειξη του Manin βασίζεται στην ακόλουθη **βασική ταυτότητα**:

ΒΑΣΙΚΗ ΤΑΥΤΟΤΗΤΑ: $d_{n-1} + d_{n+1} = 2d_n + 2$.

(Η απόδειξη της βασικής ταυτότητας βρίσκεται στην παράγραφο 2.5)

Η σύνδεση μεταξύ του θεωρήματος του Hasse και της συνάρτησης d(n) είναι η ακόλουθη ταυτότητα:

$$d_{-1} - d_0 - 1 = N_p - p \qquad (2.4.9)$$

Για να αποδείξουμε την (2.4.9) θα χρειαστεί να απλοποιήσουμε τη ρητή συνάρτηση X_{-1} μέχρις ανάγωγου κλάσματος.

Ο τύπος (2.4.8) μας δίνει ότι $(X_{-1}, Y_{-1}) = (X_0, Y_0) + (x, -1)$. Από τον νόμο πρόσθεσης (2.4.6) έχουμε:

$$X_{-1} = \lambda \frac{\left[\left(x^3 + bx + c\right)^{\frac{p-1}{2}} + 1\right]^2}{\left(x^p - x\right)^2} - (x^p + x) =$$

$$= \frac{\left(x^3 + bx + c\right)\left[\left(x^3 + bx + c\right)^{\frac{p-1}{2}} + 1\right]^2}{\left(x^p - x\right)^2} - (x^p + x) =$$

$$= \frac{\lambda\left(\lambda^{\frac{p-1}{2}} + 1\right)^2 - (x^p + x)\left(x^p - x\right)^2}{\left(x^p - x\right)^2} =$$

$$= \frac{\lambda\left(\lambda^{p-1} + 2\lambda^{\frac{p-1}{2}} + 1\right) - (x^p + x)\left(x^p - x\right)^2}{\left(x^p - x\right)^2} =$$

$$= \frac{\left(\lambda^p + 2\lambda^{\frac{p+1}{2}} + \lambda\right) - (x^p + x)\left(x^p - x\right)^2}{\left(x^p - x\right)^2} =$$

$$= \frac{\left((x^3 + bx + c)^p + 2\lambda^{\frac{p+1}{2}} + \lambda\right) - (x^{3p} - x^{2p+1} - x^{p+2} + x^3)}{\left(x^p - x\right)^2}.$$

Οπότε με χρήση της πρότασης 2.3.1

$$X_{-1} = \frac{\left((x^{3p} + bx^p + c) + 2\lambda^{\frac{p+1}{2}} + \lambda\right) - (x^{3p} - x^{2p+1} - x^{p+2} + x^3)}{(x^p - x)^2} =$$

$$= \frac{x^{3p} + bx^p + c + 2\lambda^{\frac{p+1}{2}} + \lambda - x^{3p} + x^{2p+1} + x^{p+2} - x^3)}{(x^p - x)^2} =$$

$$= \frac{x^{2p+1} + x^{p+2} + bx^p + 2\lambda^{\frac{p+1}{2}} + \lambda - x^3 + c}{(x^p - x)^2}.$$

Το λ είναι πολυώνυμο τρίτου βαθμού ως προς x ενώ το $\lambda^{\frac{p+1}{2}}$ είναι βαθμού $3\frac{p+1}{2}$, βαθμού δηλαδή μικρότερου του 2p. Επομένως,

$$X_{-1} = \frac{x^{2p+1} + R(x)}{(x^p - x)^2}$$

όπου R(x) είναι πολυώνυμο βαθμού το πολύ 2p.

Για να γράψουμε το X_{-1} σαν **ανάγωγο** κλάσμα $\frac{P_{-1}}{Q_{-1}}$ παρατηρούμε πρώτα απ' όλα ότι

$$(x^p - x) = x(x - 1) \ldots (x - p + 1)$$

Άρα για τον παρονομαστή ισχύει:

$$(x^p - x)^2 = x^2 (x - 1)^2 \ldots (x - p + 1)^2$$

Όπως φαίνεται από την αρχική σχέση που δώσαμε για το X_{-1} (δες σελίδα 44) για να απλοποιηθεί κάποιος παράγοντας από τον παρονομαστή πρέπει να διαιρεί από τον αριθμητή είτε το $\left((x^3 + bx + c)^{\frac{p-1}{2}}\right)^2 + 1$ είτε το $\lambda = x^3 + bx + c$. Επομένως, οι μόνοι παράγοντες που απλοποιούνται από τον παρονομαστή είναι:

– είτε $(x - r)^2$ όταν $(r^3 + rx + c)^{\frac{p-1}{2}} = -1$ δηλαδή όταν για το σύμβολο του Legendre ισχύει $\left(\frac{r^3 + br + c}{p}\right) = -1$

– είτε $x - r$ όταν $r^3 + br + c = 0$ $(0 \le r < p)$.

Αν m το πλήθος των κοινών παραγόντων του πρώτου είδους και n του δεύτερου τότε

$$d_{-1} = \deg P_{-1} = 2p + 1 - 2m - n$$

Αλλά,

$$d_0 = \deg(P_0) = \deg(x^p) = p \qquad (2.4.10)$$

Οπότε,

$$d_{-1} - d_0 = p + 1 - 2m - n \qquad (2.4.11)$$

Παρατηρούμε επίσης ότι κάθε r στο $\mathbf{F}_p$ με $r^3 + ar + b \neq 0$ και $\left(\frac{r^3 + br + c}{p}\right) = 1$ θα δώσει δύο λύσεις ενώ θα πάρουμε μόνο μία λύση από την $r^3 + br + c = 0$. Έχουμε ότι $\left(\frac{r^3 + br + c}{p}\right) = 1$ ισχύει για $p - m - n$ τιμές του r ενώ $r^3 + br + c = 0$ ισχύει n τιμές.

Οπότε, $N_p = 2(p - m - n) + n$ ή $N_p = 2(p - m) - n$ και η σχέση (2.4.9) προκύπτει από την (2.4.11).

Λήμμα 2.4.12 Η συνάρτηση d(n) είναι ένα τετραγωνικό πολυώνυμο δευτέρου βαθμού του n. Ακριβέστερα ισχύει:

$$d_n = n^2 - (d_{-1} - d_0 - 1)\, n + d_0$$

Απόδειξη
Πρώτα, θα αποδείξουμε ότι το λήμμα αληθεύει για $n = -1$ και $n = 0$.
Για $n = -1$ η ισότητα γράφεται

$$d_{-1} = (-1)^2 - (d_{-1} - d_0 - 1)(-1) + d_0 \text{ ή } d_{-1} = 1 + d_{-1} - d_0 - 1 + d_0$$

Άρα το λήμμα αληθεύει για $n = -1$.

Για $n = 0$ η ισότητα γράφεται

$$d_0 = 0^2 - (d_{-1} - d_0 - 1)\, 0 + d_0 \text{ ή } d_0 = d_0.$$

Άρα το λήμμα αληθεύει και για $n = 0$.

Στη συνέχεια θα εργασθούμε επαγωγικά ως προς n.
Ας υποθέσουμε ότι αληθεύει για $n - 1$ και n $(n \geq 0)$.

Από τη βασική ταυτότητα ισχύει

$$\begin{aligned} d_{n+1} &= 2d_n - d_{n-1} + 2 \\ &= 2[n^2 - (d_{-1} - d_0 - 1)n + d_0] - [(n-1)^2 - (d_{-1} - d_0 - 1)(n-1) + d_0] + 2 \\ &= (n+1)^2 - (d_{-1} - d_0 - 1)(n+1) + d_0. \end{aligned}$$

Άρα αποδείξαμε το λήμμα για $n + 1$. Με επαγωγή το λήμμα ισχύει για όλα τα $n \geq -1$. Με ανάλογο τρόπο, αποδεικνύεται ότι ισχύει και για όλα τα $n \leq 0$.

Απόδειξη του θεωρήματος του Hasse

Ορίζουμε το δευτεροβάθμιο πολυώνυμο

$$d(x) = x^2 - (d_{-1} - d_0 - 1)x + d_0 = x^2 - (N_p - p)x + d_0$$

Δείξαμε ότι $d_0 = p$ (δες 2.4.10). Επομένως, η διακρίνουσά του πολυωνύμου d(x) είναι

$$D = (N_p - p)^2 - 4p.$$

Αν δείξουμε ότι $D \leq 0$ για κάθε p θα έχουμε αποδείξει και το θεώρημα του Hasse. Η διακρίνουσα D δεν μπορεί να είναι θετική, για οποιοδήποτε p, αλλιώς το πολυώνυμο d(x) θα είχε δυο διακεκριμένες μεταξύ τους πραγματικές ρίζες. Έστω α, β ($\alpha < \beta$) αυτές οι ρίζες. Ανάμεσα τους το πολυώνυμο δίνει μόνο αρνητικές τιμές. Επειδή, για κάθε $n \in \mathbf{Z}$ ισχύει $d(n) \geq 0$, έπεται ότι οι δύο ρίζες του πολυωνύμου θα βρίσκονται μεταξύ δύο διαδοχικών ακεραίων δηλαδή υπάρχει $n_0 \in \mathbf{Z}$ τέτοιο ώστε:

$$n_0 \leq \alpha < \beta \leq n_0 + 1$$

Επιπλέον, οι δύο ισότητες δεν μπορούν να ισχύουν ταυτόχρονα γιατί, λόγω του ορισμού της η d(n), δεν μπορεί να είναι μηδέν για δύο συνεχόμενους ακέραιους αφού αν έχουμε $d_{n_0} = 0$ τότε έπεται ότι $(X_{n_0}, Y_{n_0}) = 0$ τότε όμως ισχύει ότι $(X_{n_0+1}, Y_{n_0+1}) = (X_{n_0}, Y_{n_0}) + (x, 1) = (x, 1)$ και επομένως $d(n_0 + 1) = 1 \neq 0$.

Άρα από τους αριθμούς α, β το πολύ ένας μπορεί να είναι ακέραιος. Οπότε, λόγω της ανισότητας, ισχύει ότι $(\alpha - \beta) \notin \mathbf{Z}$. Από αυτή την σχέση καταλήγουμε σε **άτοπο** γιατί αφού τα α, β είναι ρίζες της d(x) αυτό σημαίνει ότι $D = (\alpha + \beta)^2 - 4\alpha\beta = (\alpha - \beta)^2$. Επομένως, θα έπρεπε $D \in \mathbf{Z}$ και ταυτόχρονα $(\alpha - \beta)^2 \notin \mathbf{Z}$

Άρα $(N_p - p)^2 - 4p \leq 0$ το οποίο αποδεικνύει το θεώρημα.

Η απόδειξη του Manin περιλαμβάνεται μεταξύ άλλων, και στο βιβλίο του Franz Lemmermeyer, Elliptishe Kurven I, (Μπορείτε να το βρείτε στο διαδίκτυο στην διεύθυνση: http://www.rzuser.uni-heidelberg.de/~hb3/ellc.html). Ο κύριος Lemmermeyer ενημέρωσε το δάσκαλό του καθηγητή κύριο Peter Roquette σχετικά με την ύπαρξη της απόδειξης αυτής. Ακολουθεί αντίγραφο της επιστολής του κυρίου Roquette προς τον κύριο Lemmermeyer στα Γερμανικά όπου αποδεικνύεται ότι η απόδειξη του Manin είναι κατ' ουσία η ίδια με την απόδειξη του Hasse.

29.4.1998

Lieber Herr Lemmermeyer,

besten Dank für die Zusendung Ihres Maninshen Beweises. Bei der Lektüre Ihres Aufschriebs habe ich mich daran erinnern können, daß ich den Maninshen Beweis seinerzeit studiert habe; es ist schon lange her. Und ich kann mich auch an den Eindruck erinnern, den ich damals nach der Lektüre der Arbeit hatte, nämlich daß dies in der Tat im wesentlichen derselbe Beweis wie bei Hasse ist, nur eben unter Benutzung der expliziten Formel für das Additionstheorem der elliptischen Funktionen, was Hasse wegen Charakteristik 2 und 3 vollständig vermeiden wollte (und vermieden hat), und unter Weglassung der strukturellen Deutung der eingeführten Begriffe (was ebenfalls nicht im Sinne von Hasse war).

Allerdings hat natürlich der Maninsche Beweis einen gewissen Wert zum Vortrag in einer Vorlesung für Hörer mit wenigen Vorkenntnissen: das sei ihm gerne zugestanden. (Aufgabe: führe diesen Beweis für Charakteristik 3 und 2 durch!)

Lassen Sie mich vielleicht erklärren, wie ich die Sache sehe. Die $\mathbf{F}_q$-rationalen Punkte von E sind definitionsgemäß gekennzeitchnet als die Fixpunkte der Frobenius-Isogenie π von E. Das ist der Grund dafür, daß der Hassende Beweis der Begriff „Isogenie“ benutzt (er sagt: „Meromorhismus“).

Sie X = (x, y) ein allgemeiner Punkt von E (über einem Definitionskörper K, den wir der Einfachheit halber als algebraisch abgeschlossen voraussetezen wollen, was aber nicht notwendig ist). Es ist also $y^2 = x^3 - ax - b$. Es ist K(X) = K(x, y) der Funktionenkörper von E. Jede Isogenie μ wird dann gegeben durch der Punkt $\mu X = (x_\mu, y_\mu)$, der rational ist in K(X). Die „Norm” von μ wird definiert durch den Körpergrad:

$$N(\mu) = [K(X) : K(\mu X)] \tag{1}$$

In der Regel ist $N(\mu)$ gleich der Anzahl der Punkte im Kern von μ, nämlich dann wenn μ separabel ist (d.h. wenn K(X) separabel ist über $K(\mu X)$). Hierbei muß man aber den unendlich fernen Punkt mitzählen, die Kurve E also projectiv auffassen. Insbesondere folgt

$$N(\pi - 1) = N_q + 1 \tag{2}$$

denn die $\mathbf{F}_q$-rationalen Punkte bilden den Kern von $\pi - 1$. (Die 1 auf der linken Seite bezeichnet die identische Isogenie; die 1 auf der rechten Seite von (2) ist natürliche Zahl; sie zählt den unendlich fernen Punkt: wie bei Ihnen schreibe ich hier also N_q für die Anzahl der $\mathbf{F}_q$-rationalen Punkte im endlichen.

Die obige Formel (2) ist die Formel ($\#E(\mathbf{F}_q) = N_q + 1 = d_{-1}$) bei Ihnen. […]

Der Hassesche Beweis besteht nun darin, die *Normenadditionsformel* zu beweisen:

$$N(\mu + \nu) + N(\mu - \nu) = 2N(\mu) + 2N(\nu) \tag{3}$$

welche zeigt, daß die Norm eine quadratische, *positiv definite* Form definiert auf der additiven Gruppe der Isogenien (wozu auch die uneigentliche Isogenie 0 gezählt wird).

Natürlich genügt es im Hinblick auf (2), diejenige Untergruppe zu betrachten, die aufgespannt wird von der Eins-Isogenie 1 und der Frobenius-Isogenie $\pi = \pi_q$ zu $\mathbf{F}_q$. Und weiter genügt es, für die Folge $\mu_n = 1 - n\pi$ die Regel

$$N(\mu_{n+1}) + N(\mu_{n-1}) = 2\,N(\mu_n) + 2 \qquad (4)$$

zu zeigen (was ein Spezialfall von (4) ist). Man sieht den Zusammenhang mit der von Ihnen so genannten „Grundrelation": $d_{n-1} + d_{n+1} = 2d_n + 2$.

Den einzigen neuen Gedanken von Manin sehe ich darin, die Isogenenien μ von E darzustellen als K(x)-rationale Punkte der getwisteten Kurve

$$E_\lambda : \lambda z^2 = u^3 + au + b \qquad \text{wobei} \qquad \lambda = x^3 + ax + b. \qquad (5)$$

Zu jeder Isogenie μ von E gehört ein K(x)-rationaler Punkt (u, z) von E_λ, nämlich $u = x_\mu$, $z = y_\mu / y$, und zwar ist dabei $\upsilon_\infty(u) < 0$, wobei υ_∞ die Bewertung der unendlichen Stelle von K(x) ist, also der negative Grad einer rationalen Funktion. Und umgekehrt: jedem K(x)-rationalen Punkt (u, z) von E_λ entspricht auf diese Weise eine isogenie μ, derart daß $x_\mu = u$ und $y_\mu = yz$. (Der unendlich ferne Punkt von E_λ gehört zur uneigentlichen Isogenie $\mu = 0$.)

Dabei entspricht der Addition von Isogenien die Addition von Punkten der getwisteten Kurve. Und die Norm einer Isogenie ist

$$N(\mu) = [K(X) : K(\mu X)] = [K(x) : K(x_\mu)] = [K(x) : K(u)] \qquad (6)$$

Schriebt man $u = f / g$ mit teilerfremden Polynomen f, g, so ist $\upsilon_\infty(u) = -\,\mathrm{Grad}(f) + \mathrm{Grad}(g) < 0$ und daher

$$[K(x) : K(u)] = \mathrm{Grad}(f) \qquad (7)$$

Somit sehen wir, daß die auf Seite 3 Ihres Manuskripts eingenführte Zahl d_n nichts anderes ist als die Norm der zugenhörigen Isogenie.

Dieser Zusammenhang erlaubt es Manin, dem Leser den Begriff der Isogenie vorzuenthalten und mit rationalen Punkten der getwisteten Kurve zu rechnen. In Wahrheit ist es aber, wie gesagt, der Hassesche Beweis.

5. Απόδειξη της Βασικής Ταυτότητας

Για την απόδειξη θα χρειαστούμε το ακόλουθο λήμμα:

Λήμμα 2.5.1 Αν $(X_n, Y_n) \neq 0$ τότε $\deg P_n > \deg Q_n$, ειδικότερα $X_n \neq 0$.

Απόδειξη Για να αποδείξουμε ότι ο βαθμός του αριθμητή μιας ανάγωγης ρητής συνάρτησης R(x) στο $\mathbf{F}_p(x)$ είναι μεγαλύτερος από το βαθμό του παρονομαστή, συνήθως υπολογίζουμε το R(x) όταν $x \to \infty$ και δείχνουμε ότι $\lim_{x\to\infty} R(x) = \infty$.

Το λήμμα προφανώς ισχύει για n = 0 αφού $X_0 = x^P$ και $\deg P_0 = \deg x^P > \deg 1 = \deg Q_0$.

Το λήμμα ισχύει επίσης και για όλα τα $n > 0$ για τα οποία $(X_{n-1}, Y_{n-1}) = 0$ γιατί τότε $(X_n, Y_n) = (x, 1)$ και $\deg P_n = \deg x > \deg 1 = \deg Q_n$.

Υποθέτουμε ότι το λήμμα ισχύει για κάποιο $n \geq 0$ για το οποίο $(X_{n-1}, Y_{n-1}) \neq 0$. Συνεχίζουμε επαγωγικά.

Αρκεί να αποδείξουμε ότι το λήμμα ισχύει για n + 1 και θα το έχουμε δείξει για όλα τα $n \geq 0$. Δηλαδή αρκεί να δείξουμε ότι αν $(X_{n+1}, Y_{n+1}) \neq 0$ τότε έπεται ότι $\deg P_{n+1} > \deg Q_{n+1}$.

Ισχύει:

$$\lambda Y^2_{n+1} = X^3_{n+1} + bX_{n+1} + c \quad \text{ή} \quad Y^2_{n+1} = \frac{X^3_{n+1} + bX_{n+1} + c}{x^3 + bx + c}.$$

Ακόμα, επειδή $X_{n+1}(x) = \dfrac{P_{n+1}(x)}{Q_{n+1}(x)}$ ισχύει ότι

$$\lim_{x\to\infty} X_{n+1}(x) < \infty \Leftrightarrow \deg P_{n+1}(x) \leq \deg Q_{n+1}(x)$$

Επομένως, ο αριθμητής στην παραπάνω έκφραση του Y^2_{n+1} όταν $x \to \infty$ είναι μικρότερος του ∞ όταν ισχύει $\deg P_{n+1}(x) \leq \deg Q_{n+1}(x)$. Τότε όμως ο παρονομαστής τείνει στο ∞.

Οπότε:

$$\lim_{x\to\infty} Y_{n+1}(x) = 0 \Leftrightarrow \deg P_{n+1}(x) \leq \deg Q_{n+1}(x)$$

Συνεπώς, $$\lim_{x\to\infty} Y_{n+1}(x) \neq 0 \Leftrightarrow \deg P_{n+1}(x) > \deg Q_{n+1}(x)$$

Θα χρησιμοποιήσουμε τη μέθοδο της εις άτοπον απαγωγής.

Υποθέτουμε ότι $\deg P_{n+1}(x) \leq \deg Q_{n+1}(x)$. Δηλαδή $\lim_{x\to\infty} Y_{n+1}(x) = 0$.

Ισχύει $$(X_{n+1}, Y_{n+1}) = (X_n, Y_n) + (x, 1)$$

ή αλλιώς

$$(X_{n+1}, -Y_{n+1}) + (X_n, Y_n) + (x, 1) = 0 \qquad (2.5.2)$$

Άρα τα σημεία $(X_{n+1}, -Y_{n+1})$, (X_n, Y_n), $(x, 1)$ βρίσκονται πάνω σε ευθεία.

Η εξίσωση της ευθείας L που περνάει από τα (X_n, Y_n) και $(x, 1)$ είναι

$$L : Y - 1 = \frac{1 - Y_n}{x - X_n} (X - x)$$

Το $(X_{n+1}, -Y_{n+1})$ είναι σημείο της L άρα έχουμε

$$-Y_{n+1} - 1 = \frac{1 - Y_n}{x - X_n} (X_{n+1} - x)$$

$$\text{ή} \quad Y_{n+1} + 1 = \frac{1 - Y_n}{x - X_n} (x - X_{n+1})$$

$$\text{ή} \quad Y_{n+1} = \frac{1 - Y_n}{x - X_n} (x - X_{n+1}) - 1$$

Οπότε, επειδή $\lim_{x\to\infty} Y_{n+1}(x) = 0$ έπεται ότι $\lim_{x\to\infty}\left[\frac{1 - Y_n}{x - X_n}(x - X_{n+1}) - 1\right] = 0$ ή αλλιώς ότι

$$\lim_{x\to\infty}\left[\frac{1 - Y_n}{1 - \frac{X_n}{x}}\left(1 - \frac{X_{n+1}}{x}\right) - 1\right] = 0$$

αλλά, αφού deg $P_{n+1}(x) \le$ deg $Q_{n+1}(x)$ ισχύει deg $P_{n+1}(x) <$ deg $Q_{n+1}(x) + 1$ δηλαδή deg$P_{n+1}(x) <$ deg $[xQ_{n+1}(x)]$ και επομένως,

$$\lim_{x\to\infty} \frac{X_{n+1}}{x} = \lim_{x\to\infty} \frac{P_{n+1}}{xQ_{n+1}} = 0 \qquad (2.5.3)$$

Δηλαδή, ισχύει ότι

$$\lim_{x\to\infty} \frac{1 - Y_n}{1 - \frac{X_n}{x}} = 1 \qquad (2.5.4)$$

Ο νόμος της πρόσθεσης (addition formula) (2.4.6) δίνει:

$$X_{n+1} = \left(\frac{1 - Y_n}{x - X_n}\right)^2 (x^3 + bx + c) - (x + X_n)$$

Οπότε παίρνουμε

$$\frac{X_{n+1}}{x} = \left(\frac{1-Y_n}{1-\frac{X_n}{x}}\right)^2 \left(1+\frac{b}{x^2}+\frac{c}{x^3}\right)-1-\frac{X_n}{x} \qquad (2.5.5)$$

Από τις σχέσεις (2.5.3) και (2.5.5) συμπεραίνουμε ότι:

$$\lim_{x\to 0}\left[\left(\frac{1-Y_n}{1-\frac{X_n}{x}}\right)^2 \left(1+\frac{b}{x^2}+\frac{c}{x^3}\right)-1-\frac{X_n}{x}\right] \to 0$$

Λόγω όμως της σχέσης (2.5.4) έπεται ότι

$$\lim_{x\to 0}\left[\left(\frac{1-Y_n}{1-\frac{X_n}{x}}\right)^2 \left(1+\frac{b}{x^2}+\frac{c}{x^3}\right)-1-\frac{X_n}{x}\right] =$$

$$= \lim_{x\to 0}\left[\left(\frac{1-Y_n}{1-\frac{X_n}{x}}\right)^2 \left(1+\frac{b}{x^2}+\frac{c}{x^3}\right)\right] -1 - \lim_{x\to 0}\frac{X_n}{x} =$$

$$= 1 -1 - \lim_{x\to 0}\frac{X_n}{x} =$$

$$= - \lim_{x\to 0}\frac{X_n}{x}$$

Δηλαδή $\lim_{x\to 0}\frac{X_n}{x} \to 0$.

Αυτό όμως, σημαίνει ότι deg $P_n(x)$ < deg $[xQ_n(x)]$. Οπότε deg $P_n(x) \le$ deg $Q_n(x)$, το οποίο είναι <u>άτοπο</u> λόγω της υπόθεσης της μαθηματικής επαγωγής ότι deg $P_n(x) >$ deg $Q_n(x)$.

Αυτή η αντίφαση αποδεικνύει και το λήμμα για κάθε $n \ge 0$. Η απόδειξη για $n \le 0$ γίνεται ανάλογα.

Τώρα θα αποδείξουμε τη βασική ταυτότητα: $\mathbf{d_{n-1} + d_{n+1} = 2d_n + 2}$

1. Αν ένα από τα (X_{n-1}, Y_{n-1}), (X_n, Y_n), (X_{n+1}, Y_{n+1}) είναι μηδέν τότε η βασική ταυτότητα είναι τετριμμένη.

Πράγματι, χρησιμοποιούμε τη σχέση (2.5.2) και έχουμε:

i. Αν $(X_n,Y_n) = 0$ έπεται ότι $(X_0,Y_0) + n(x, 1) = 0$.
Τότε, $(X_{n+1}, Y_{n+1}) = (X_0,Y_0) + (n+1)(x, 1) = (X_0,Y_0) + n(x, 1) + (x, 1) = 0 + (x, 1) = (x, 1)$.
Δηλαδή $X_{n+1} = x$, $Y_{n+1} = 1$
Ακόμα $(X_{n-1}, Y_{n-1}) = (X_n, Y_n) - (x, 1) = -(x, 1) = (x, -1)$

Οπότε $X_{n-1} = x$, $Y_{n-1} = -1$
Και τελικά $d_n = 0$ και $d_{n-1} = d_{n+1} = 1$

ii. Αν $(X_{n-1}, Y_{n-1}) = 0$ έπεται ότι $(X_n, Y_n) = (X_0, Y_0) + n(x, 1)$
ή αλλιώς $(X_n, Y_n) = (X_0, Y_0) + (n-1)(x-1) + (x, 1) = (X_{n-1}, Y_{n-1}) + (x, 1) = (x,1)$

Άρα $d_{n-1} = 0$, $d_n = 1$.

Από το νόμο της πρόσθεσης (2.4.7) έχουμε: $(X_{n+1}, Y_{n+1}) = (X_n, Y_n) + (x, 1) = 2(x, 1)$.

$$X_{n+1} = \frac{\left(3x^2+b\right)^2}{4\left(x^3+bx+c\right)} - 2x = \frac{9x^4+6bx^2+b^2-8x^4-8bx^2-8cx}{4\left(x^3+bx+c\right)} =$$

$$= \frac{x^4-2bx^2-8cx+b^2}{4\left(x^3+bx+c\right)}.$$

Υπολογίζουμε τον μέγιστο κοινό διαιρέτη αριθμητή και παρονομαστή:

- Αν $b \neq 0$ τότε

$$x^4 - 2bx - 8cx + b^2 = x(x^3 + bx + c) + (-3bx^2 - 9cx + b^2)$$

$$x^3 + bx + c = \left(-\frac{1}{3b}x + \frac{c}{b^2}\right)(-3bx^2 - 9cx + b^2) + \left(\frac{4b}{3} + \frac{9c^2}{b^2}\right)x$$

$$-3bx^2 - 9cx + b^2 = (-3bx - 9c)\left(\frac{4b}{3} + \frac{9c^2}{b^2}\right)^{-1}\left(\frac{4b}{3} + \frac{9c^2}{b^2}\right)x + b^2$$

Το b^2 είναι μονάδα (αντιστρέψιμο στοιχείο) του δακτυλίου $\mathbf{F}_p(x)$ οπότε τα πολυώνυμα $x^4 - 2bx - 8cx + b^2$ και $x^3 + bx + c$ είναι πρώτα μεταξύ τους.

- Αν $b = 0$ τότε αναγκαστικά $c \neq 0$ και

$x^4 - 2bx - 8cx + b^2 = x^4 - 8cx$,
$x^3 + bx + c = x^3 + c$

Οπότε:

$$x^4 - 8cx = x(x^3 + c) - 9cx$$

$$x^3 + c = -\frac{1}{9c}x^2(-9cx) + c$$

Το c είναι μονάδα (αντιστρέψιμο στοιχείο) του δακτυλίου $\mathbf{F}_p(x)$ οπότε τα πολυώνυμα $x^4 - 8cx$ και $x^3 + c$ είναι πρώτα μεταξύ τους.

Σε κάθε περίπτωση $d_{n+1} = 4$.

Επομένως $d_{n-1} + d_{n+1} = 0 + 4 = 2 + 2 = d_n + 2$. Δηλαδή, και σ' αυτή την περίπτωση, ισχύει η βασική ταυτότητα.

iii. Αν $(X_{n+1}, Y_{n+1}) = 0$ τότε $(X_n, Y_n) = -(x, 1) = (x, -1)$

Άρα $d_{n+1} = 0$, $d_n = 1$.
Ανάλογα όπως και πριν, από τον τύπο (2.4.7) έχουμε:

$$(X_{n-1}, Y_{n-1}) = -2(x, 1) = 2(x, -1) \text{ και } X_{n-1} = \frac{\left(3x^2 + b\right)^2}{4\left(x^3 + bx + c\right)} - 2x =$$

$$\frac{x^4 - 2bx^2 - 8cx + b^2}{4\left(x^3 + bx + c\right)}.$$

Οπότε $d_{n-1} = 4$ και έχουμε $4 + 0 = 2 \cdot 1 + 2$ που ισχύει.

2. Έστω τώρα ότι $(X_{n-1}, Y_{n-1}) \neq 0$, $(X_n, Y_n) \neq 0$, $(X_{n+1}, Y_{n+1}) \neq 0$.

Από τη σχέση (2.5.2) έχουμε:

$(X_n, Y_n) = (X_{n-1}, Y_{n-1}) + (x, 1)$ ή

$(X_{n-1}, Y_{n-1}) = (X_n, Y_n) - (x, 1)$ ή

$(X_{n-1}, Y_{n-1}) = (X_n, Y_n) + (x, -1)$

Από το νόμο της πρόσθεσης (2.4.6) και με χρήση της σχέσης $X_n = \frac{P_n}{Q_n}$ έχουμε:

$$X_{n-1} = \lambda\frac{\left(Y_n + 1\right)^2}{\left(X_n - x\right)^2} - (x + X_n) =$$

$$= \frac{\lambda\left(Y_n + 1\right)^2 - \left(x + X_n\right)\left(X_n - x\right)^2}{\left(X_n - x\right)^2} =$$

$$= \frac{\lambda\left(Y_n + 1\right)^2 - \left(x + \frac{P_n}{Q_n}\right)\left(\frac{P_n}{Q_n} - x\right)^2}{\left(\frac{P_n}{Q_n} - x\right)^2} =$$

$$= \frac{Q_n^3\lambda(Y_n+1)^2-(xQ_n+P_n)(P_n-xQ_n)^2}{Q_n(xQ_n-P_n)^2} =$$

$$= \frac{\lambda Q_n^2(Y_n+1)^2-(x+X_n)(P_n-xQ_n)^2}{(xQ_n-P_n)^2} = \qquad (2.5.6)$$

$$= \frac{\lambda Q_n^2(Y_n^2+2Y_n+1)-(x+X_n)(P_n^2-xP_nQ_n+x^2Q_n^2)}{(xQ_n-P_n)^2} =$$

$$= \frac{Q_n^2(\lambda Y_n^2+2\lambda Y_n+\lambda)-x(P_n^2-xP_nQ_n+x^2Q_n^2)-X_n(P_n^2-xP_nQ_n+x^2Q_n^2)}{(xQ_n-P_n)^2} =$$

$$= \frac{Q_n^2(X_n^3+bX_n+c+2\lambda Y_n+\lambda)-xP_n^2+x^2P_nQ_n-x^3Q_n^2-X_nP_n^2+xP_n^2-x^2P_nQ_n}{(xQ_n-P_n)^2} =$$

$$= \frac{Q_n^2X_n^3+Q_n^2(bX_n+c+2\lambda Y_n+\lambda)-xP_n^2-x^3Q_n^2-X_nP_n^2+xP_n^2}{(xQ_n-P_n)^2} =$$

$$= \frac{bP_nQ_n+cQ_n^2+2\lambda Y_nQ_n^2+\lambda Q_n^2-xP_n^2-x^3Q_n^2+xP_n^2}{(xQ_n-P_n)^2} =$$

$$= \frac{(xQ_n+P_n)(xP_n+bQ_n)+(\lambda-x^3-bx+c-bx)Q_n^2+2\lambda Y_nQ_n^2}{(xQ_n-P_n)^2} =$$

$$= \frac{(xQ_n+P_n)(xP_n+bQ_n)+2cQ_n^2+2\lambda Y_nQ_n^2}{(xQ_n-P_n)^2}.$$

Δηλαδή, $$X_{n-1} = \frac{P_{n-1}}{Q_{n-1}} = \frac{R}{(xQ_n-P_n)^2} \qquad (2.5.7)$$

όπου $R = (xQ_n + P_n)(xP_n + bQ_n) + 2cQ_n^2 + 2\lambda Y_nQ_n^2$.

Και ανάλογα

$(X_{n+1}, Y_{n+1}) = (X_n, Y_n) + (x, 1)$

Οπότε,

$$X_{n+1} = \lambda\frac{(Y_n-1)^2}{(X_n-x)^2} - (x+X_n) = \frac{\lambda Q_n^2(Y_n-1)^2-(x+X_n)(P_n-xQ_n)^2}{(xQ_n-P_n)^2} \qquad (2.5.8)$$

$$= \frac{(xQ_n+P_n)(xP_n+bQ_n)+2cQ_n^2-2\lambda Y_nQ_n^2}{(xQ_n-P_n)^2}.$$

Δηλαδή, $$X_{n+1} = \frac{P_{n+1}}{Q_{n+1}} = \frac{S}{(xQ_n-P_n)^2} \qquad (2.5.9)$$

όπου $S = (xQ_n + P_n)(xP_n + bQ_n) + 2c\,Q_n^2 - 2\lambda Y_n Q_n^2$.

Πολλαπλασιάζοντας τις παραπάνω εκφράσεις για τα X_{n-1} και X_{n+1} έχουμε:

$$X_{n-1}\cdot X_{n+1} = \frac{P_{n-1}\cdot P_{n+1}}{Q_{n-1}\cdot Q_{n+1}} = \frac{R\cdot S}{(xQ_n - P_n)^4} =$$

$$= \frac{\left[(xQ_n + P_n)(xP_n + bQ_n) + 2cQ_n^2\right]^2 - 4\lambda^2\cdot Y_n^2\cdot Q_n^4}{(xQ_n - P_n)^4} =$$

$$= \frac{\left[(xQ_n + P_n)(xP_n + bQ_n) + 2cQ_n^2\right]^2 - 4\lambda(X_n^3 + bX_n + c)\cdot Q_n^4}{(xQ_n - P_n)^4} =$$

$$= \frac{\left[(xQ_n + P_n)(xP_n + bQ_n) + 2cQ_n^2\right]^2 - 4(x^3 + bx + c)(P_n^3Q_n + bP_n^4Q_n^3 + cQ_n^4)}{(xQ_n - P_n)^4} =$$

$$= \frac{x^4Q_n^2P_n^2 + 2x^3Q_n^3Pb + x^2Q_n^4b^2 - 2x^3Q_nP_n^3 + 4x^2Q_n^2P_n^2b + 2xQ_n^3P_nb^2 + P_n^4x^2}{(xQ_n - P_n)^4} +$$

$$+ \frac{-2P_n^3xbQ_n + P_n^2b^2Q_n^2 + 4cQ_n^3x^2P_n + 4cQ_n^3b + 4cQ_n^2xP_n^2}{(xQ_n - P_n)^4} +$$

$$+ \frac{-4x^3bP_n^4Q_n^3 - 4x^3cQ_n^4 - 4b^2xP_n^4Q_n^3 - 4cP_n^3Q_n - 4cbP_n^4Q_n^3}{(xQ_n - P_n)^4} =$$

$$= \frac{(xQ_n - P_n)^2\left[(xP_n - bQ_n)^2 - 4cQ_n(xQ_n + P_n)\right]}{(xQ_n - P_n)^4} =$$

$$= \frac{(xP_n - bQ_n)^2 - 4cQ_n(xQ_n + P_n)}{(xQ_n - P_n)^2}. \qquad (2.5.10)$$

Αν δείξουμε ότι $Q_{n-1}\cdot Q_{n+1} = k\cdot(xQ_n - P_n)^2$, όπου $k \in \mathbf{F}_p$ τότε

$$P_{n-1}\cdot P_{n+1} = k\cdot[(xP_n - bQ_n)^2 - 4cQ_n(xQ_n + P_n)]$$

και τότε:

$$d_{n-1} + d_{n+1} = \deg(P_{n-1}\cdot P_{n+1}) = \deg(x^2\cdot P_n^2\cdot k) = \deg(x^2) + \deg(P_n^2) = 2d_n + 2$$

και θα έχουμε αποδείξει την βασική ταυτότητα.

Από τις ενδιάμεσες ισότητες της (2.5.10) προκύπτει ότι:

$$(xQ_n - P_n)^2\,R\cdot S = (xQ_n - P_n)^4\cdot[(xP_n - bQ_n)^2 - 4cQ_n(xQ_n + P_n)] \text{ ή}$$

$$R\cdot S = (xQ_n - P_n)^2\cdot[(xP_n - bQ_n)^2 - 4cQ_n(xQ_n + P_n)]$$

Δηλαδή, $(xQ_n - P_n)^2 \mid R \cdot S$

Επομένως υπάρχουν πολυώνυμα $R_1, S_1 \in \mathbf{F}_p[x]$ τέτοια ώστε $(xQ_n - P_n)^2 = R_1 \cdot S_1$ όπου $R_1 \mid R$ και $S_1 \mid S$.

Έχουμε ότι $X_{n-1} = \frac{P_{n-1}}{Q_{n-1}} \overset{(2.5.7)}{=} \frac{R}{(xQ_n - P_n)^2} = \frac{R}{R_1 \cdot S_1} = \frac{\frac{R}{R_1}}{S_1}$ επειδή $\frac{P_{n-1}}{Q_{n-1}}$ ανάγωγο, δηλαδή $\text{ΜΚΔ}(Q_{n-1}, P_{n-1}) = 1$, έπεται ότι $Q_{n-1} \mid S_1$.

Ομοίως, $X_{n+1} = \frac{P_{n+1}}{Q_{n+1}} \overset{(2.5.9)}{=} \frac{S}{(xQ_n - P_n)^2} = \frac{S}{R_1 \cdot S_1} = \frac{\frac{S}{S_1}}{R_1}$ και $\text{ΜΚΔ}(Q_{n+1}, P_{n+1}) = 1$. Οπότε $Q_{n+1} \mid R_1$.

Επομένως, το $Q_{n-1} \cdot Q_{n+1}$ διαιρεί το $S_1 \cdot R_1 = (xQ_n - P_n)^2$.

Δηλαδή:

Για να δείξουμε ότι $Q_{n-1} \cdot Q_{n+1} = k \cdot (xQ_n - P_n)^2$ αρκεί να δείξουμε ότι το πολυώνυμο $(xQ_n - P_n)^2$ διαιρεί το $Q_{n-1} \cdot Q_{n+1}$ (1)

Ορισμός 2.5.11 Αν στον Ευκλείδειο δακτύλιο $\mathbf{F}_p[x]$ πάρουμε ένα τυχαίο πολυώνυμο $A \neq 0$ και ένα ανάγωγο f τότε $v_f(A)$ θα συμβολίζει τον εκθέτη του f στην ανάλυση του A σε γινόμενο πρώτων (αναγώγων) παραγόντων. Αν $A = 0$ ορίζουμε $v_f(A) = \infty$. Είναι σαφές ότι αφού A πολυώνυμο για την $v_f(A)$ θα ισχύει: $v_f(A) \in \{0, 1, 2, \ldots\} \cup \{\infty\}$.
Η συνάρτηση v_f επεκτείνεται και στο σώμα των ρητών συναρτήσεων $\mathbf{F}_p(x)$ ως εξής:
Αν $T \in \mathbf{F}_p(x)$ και $T = \frac{A}{B}$ με $A, B \in \mathbf{F}_p[x]$ τότε η συνάρτηση $v_f(T)$ ορίζεται να είναι $v_f(T) = v_f(A) - v_f(B)$. Οπότε $v_f(T) \in \mathbf{Z} \cup \{\infty\}$.

Αν τώρα $A, B \in \mathbf{F}_p(x)$ και $A \mid B$ τότε προφανώς $v_f(A) \leq v_f(B)$ για κάθε $f \in \mathbf{F}_p[x]$, f ανάγωγο.

Επομένως, $A \nmid B$ σημαίνει ότι υπάρχει ανάγωγο $f \in \mathbf{F}_p[x]$ τέτοιο ώστε

$$v_f(A) > v_f(B)$$

Παρατήρηση 2.5.12 Για κάθε $A \in \mathbf{F}_p(x)$ ισχύει $v_f(A^2) = 2\, v_f(A)$

Έστω λοιπόν ότι $(xQ_n - P_n)^2 \nmid Q_{n-1} \cdot Q_{n+1}$ τότε υπάρχει ανάγωγο πολυώνυμο $f \in \mathbf{F}_p[x]$ τέτοιο ώστε:

$$v_f((xQ_n - P_n)^2) > v_f(Q_{n-1} \cdot Q_{n+1}) \quad \text{ή}$$

$$2\, v_f(xQ_n - P_n) > v_f(Q_{n-1} \cdot Q_{n+1}) \qquad (2.5.13)$$

Για ευκολία στους επόμενους υπολογισμούς ορίζουμε

$$T: = (xP_n - bQ_n)^2 - 4cQ_n\,(xQ_n + P_n) \qquad (2.5.14)$$

Οπότε, από την σχέση (2.5.10), έχουμε:

$$\frac{P_{n-1}\cdot P_{n+1}}{Q_{n-1}\cdot Q_{n+1}} = \frac{T}{\left(xQ_n - P_n\right)^2},$$

δηλαδή

$$T = \frac{P_{n-1}\cdot P_{n+1}\cdot\left(xQ_n - P_n\right)^2}{Q_{n-1}\cdot Q_{n+1}} \qquad (2.5.15)$$

Από την τελευταία σχέση και την (2.5.13) προκύπτει ότι το f διαιρεί το T.

Επειδή το f διαιρεί το $(xQ_n - P_n)^2$ αν αποδείξουμε ότι το f διαιρεί το R και το S τότε, από τις (2.5.6) και (2.5.8), θα έχουμε ότι

$$f \mid \lambda Q_n^2\ (Y_n + 1)^2 \text{ και } f \mid \lambda Q_n^2\ (Y_n - 1)^2$$

Έστω ότι το f διαιρεί το Q_n, τότε επειδή διαιρεί το $xQ_n - P_n$ θα διαιρεί και το P_n που είναι <u>άτοπο</u> αφού $ΜΚΔ(P_n, Q_n) = 1$. Άρα, το f δεν διαιρεί το Q_n και έχουμε

$$f \mid \lambda\,(Y_n + 1) \text{ και } f \mid \lambda\,(Y_n - 1)$$

Έστω ότι το f <u>δεν</u> διαιρεί το λ. Τότε $f \mid (Y_n + 1)$ και $f \mid (Y_n - 1)$ και επομένως f διαιρεί το $(Y_n + 1) - (Y_n - 1) = 2$, που είναι <u>άτοπο</u> αφού έχουμε υποθέσει ότι το f είναι ανάγωγο και επομένως <u>δεν</u> είναι μονάδα του $\mathbf{F}_p[x]$.

Επομένως το f διαιρεί το $\lambda = x^3 + bx + c$.

Γράφουμε το T σαν πολυώνυμο του P_n:

$T = (xP_n - bQ_n)^2 - 4cQ_n\,(xQ_n + P_n) = x^2P_n^2 - 2bxP_nQ_n + b^2Q_n^2 - 4cxQ_n^2 - 4cQ_nP_n =$ $x^2P_n^2 + (-2bx - 4c)Q_nP_n + (b^2 - 4cxQ_n^2)$ και στη συνέχεια διαιρούμε το T με $xQ_n - P_n$ και βρίσκουμε:

$$T = -(xQ_n - P_n)\,[x^2P_n + (x^3 - 2bx - 4c)Q_n] + (x^4 - 2bx - 8cx + b^2)Q_n^2.$$

Επειδή το f διαιρεί το T και το πολυώνυμο $xQ_n - P_n$ θα πρέπει να διαιρεί και το πολυώνυμο $(x^4 - 2bx - 8cx + b^2)Q_n^2$ και επειδή το f δεν διαιρεί το Q_n έπεται ότι το f διαιρεί το $x^4 - 2bx - 8cx + b^2$. Τότε όμως, θα πρέπει το f να διαιρεί και το

$$(3x^3 - 5bx - 27c)(x^3 + bx + c) - (3x^2 + b)\,(x^4 - 2bx - 8cx + b^2) = -4b^3 - 27c^2 = \Delta,$$

δηλαδή τη διακρίνουσα της ελλειπτικής καμπύλης, που είναι <u>άτοπο</u> για τον ίδιο λόγο όπως προηγουμένως.

Συνεπώς, αν αποδείξουμε το f διαιρεί το R και το S η απόδειξη θα έχει τελειώσει.

Έχουμε ότι, το f διαιρεί το T και επίσης το T διαιρεί το RS (δες ενδιάμεσες ισότητες της (2.5.10)). Επομένως, $f \mid RS$. Δηλαδή $f \mid R$ είτε $f \mid S$.

Χωρίς περιορισμό της γενικότητας ας υποθέσουμε ότι $f \mid R$ και $f \nmid S$. (Η απόδειξη στην περίπτωση $f \mid S$ και $f \nmid R$ είναι εντελώς όμοια).

Επειδή $f \nmid S$ και $f \mid (xQ_n - P_n)^2$, δες (2.5.13), έχουμε ότι $v_f(Q_{n+1}) = v_f(Q_{n+1}S) \overset{(2.5.9)}{=} v_f((xQ_n - P_n)^2 P_{n+1}) = v_f((xQ_n - P_n)^2) + v_f(P_{n+1}) > 0$. Συνεπώς, $f \mid Q_{n+1}$. Τότε όμως επειδή $\text{ΜΚΔ}(P_{n+1}, Q_{n+1}) = 1$ έπεται ότι $f \nmid P_{n+1}$ ή αλλιώς

$$v_f(P_{n+1}) = 0 \tag{2.5.16}$$

και επίσης

$$v_f(Q_{n+1}) = 2\, v_f(xQ_n - P_n) \tag{2.5.17}$$

Στη συνέχεια υπολογίζουμε το $v_f(T)$.

Κατ' αρχήν επειδή το f διαιρεί το R θα διαιρεί και το $T = R \cdot S \cdot (xQ_n - P_n)^2$, δηλαδή $v_f(T) > 0$. Επίσης λόγω της σχέσης (2.5.15) έχουμε

$$0 < v_f(T) = v_f\left(\frac{P_{n-1} \cdot P_{n+1} \cdot (xQ_n - P_n)^2}{Q_{n-1} \cdot Q_{n+1}}\right) = v_f\left(P_{n-1} \cdot P_{n+1} \cdot (xQ_n - P_n)^2\right) - v_f\,(Q_{n-1}Q_{n+1}) =$$

$v_f(P_{n-1}) + v_f(P_{n+1}) + 2\, v_f(xQ_n - P_n) - v_f\,(Q_{n-1}) - v_f\,(Q_{n+1})$.

Λόγω των σχέσεων (2.5.16) και (2.5.17) έχουμε ότι

$$0 < v_f(T) = v_f(P_{n-1}) - v_f\,(Q_{n-1})$$

Δηλαδή,

$$v_f(P_{n-1}) > v_f\,(Q_{n-1})$$

Πράγμα που σημαίνει ότι $v_f(P_{n-1}) > 0$. Συνεπώς, το f διαιρεί το P_{n-1} και επειδή $\text{ΜΚΔ}(P_{n-1}, Q_{n-1}) = 1$, έπεται ότι το f δεν διαιρεί το Q_{n-1}, δηλαδή ότι

$$v_f\,(Q_{n-1}) = 0. \tag{2.5.18}$$

Άρα, λόγω των (2.5.17) και (2.5.18), έχουμε:

$$v_f\,(Q_{n-1}Q_{n+1}) = v_f\,(Q_{n-1}) + v_f\,(Q_{n+1}) = 0 + 2v_f(xQ_n - P_n) = 2v_f(xQ_n - P_n)$$

<u>άτοπο</u>, διότι εμείς υποθέσαμε, δες (2.5.13), ότι $2\, v_f\,(xQ_n - P_n) > v_f\,(Q_{n-1} \cdot Q_{n+1})$.

Επομένως, δείξαμε ότι $(xQ_n - P_n)^2 \mid (Q_{n-1} \cdot Q_{n+1})$. Δηλαδή, αποδείξαμε την βασική ταυτότητα.

Κεφάλαιο ΙΙΙ

Αλγεβρικές Καμπύλες και Θεωρία Κωδικοποίησης

1. Στοιχεία θεωρίας κωδικοποίησης

Ορισμός 3.1.1

(i) **Αλφάβητο** ονομάζεται το πεπερασμένο σύνολο των συμβόλων (πολλές φορές θα τα ονομάζουμε **γράμματα**) που χρησιμοποιούμε για να καταγράψουμε-διατυπώσουμε ένα μήνυμα. Το αλφάβητό μας, σε αυτό το κεφάλαιο, θα είναι το πεπερασμένο σώμα $\mathbf{F}_q$.
(ii) Ένα **k-μήνυμα** αποτελείται από μια ακολουθία γραμμάτων των αλφαβήτου μας μήκους k. Είναι δηλαδή της μορφής: $a_1, a_2 \ldots, a_k$ με $a_i \in \mathbf{F}_q$.
(iii) Η αντίστοιχη **κωδική λέξη** x ενός k-μηνύματος είναι μια ακολουθία μήκους n. Είναι δηλαδή της μορφής $x = x_1, x_2 \ldots, x_n$ με $x_i \in \mathbf{F}_q$ και $n \geq k$. Όπου (σχεδόν) πάντα θα ισχύει ότι $x_1 = a_1, x_2 = a_2, \ldots, x_k = a_k$ ενώ τα υπόλοιπα n – k σύμβολα $(x_{k+1}, x_{k+2}, \ldots, x_n)$ θα τα λέμε **σύμβολα ελέγχου** (**check symbols** ή **control symbols**).

Συμβολισμός 3.1.2 Οι κωδικές λέξεις θα γράφονται x ή $x_1, x_2, \ldots, x_n$ ή $(x_1, x_2, \ldots, x_n)$ ή $x_1x_2\ldots x_n$.

Ορισμός 3.1.3 Θα ονομάζουμε **διάνυσμα λήψης** (ή **μήνυμα λήψης**) το διάνυσμα $y = y_1, y_2, \ldots, y_n$ που λαμβάνουμε. Το y εν γένει είναι διαφορετικό από το μήνυμα x που μας στέλνουνε. Το $e := y - x = e_1e_2\ldots e_n$ θα λέγεται **διάνυσμα λάθους** (ή απλά **λάθος**).

Ορισμός 3.1.4 Ένας **n-κώδικας** C είναι ένα υποσύνολο του $\mathbf{F}_q^n$. Ακριβέστερα ο κώδικας θα λέγεται **(n, k)-κώδικας**, όπου k το μήκος του μηνύματος που κωδικοποιούμε. Αν ο κώδικας C είναι $\mathbf{F}_q$-διανυσματικός υπόχωρος του $\mathbf{F}_q^n$ τότε θα λέγεται **(n, k)-γραμμικός κώδικας**. Τα στοιχεία του C θα είναι οι κωδικές λέξεις.

Παραδείγματα 3.1.5

(i) Έστω C = {000, 001, 010, 011} υποσύνολο του $\mathbf{F}_2^3$. Ο C αποτελείται από ακριβώς αυτές τις κωδικές λέξεις που έχουν σαν πρώτο στοιχείο το 0 και εύκολα φαίνεται ότι ο C είναι ένας γραμμικός 3-κώδικας.
(ii) Επίσης, το C = {00, 11, 22} αποτελεί ένα γραμμικό 2-κώδικα του $\mathbf{F}_3^2$.

Όταν πάρουμε το y θα πρέπει να αποφασίσουμε ποια κωδική λέξη μας έχουν στείλει. Θα διαλέγουμε από το σύνολο C μια κωδική λέξη που διαφέρει λιγότερο από το y. Αυτό το αξίωμα ονομάζεται **μέγιστης πιθανότητας αποκωδικοποίηση**.

Ορισμός 3.1.6 **Απόσταση Hamming** d(x, y) δύο διανυσμάτων x, y στο $\mathbf{F}_q^n$, με

$$x = x_1, x_2 \ldots, x_n \text{ και } y = y_1, y_2 \ldots, y_n,$$

είναι το πλήθος των συντεταγμένων στις οποίες τα x και y διαφέρουν. Δηλαδή

$$d(x, y) = \#\{i \in \mathbf{N},\ 1 \le i \le n \mid x_i \ne y_i\}$$

Ορισμός 3.1.7 **Βάρος (weight) Hamming** w(x) ενός διανύσματος $x = x_1, x_2 \ldots, x_n$ στο $\mathbf{F}_q^n$ είναι το πλήθος των μη-μηδενικών συντεταγμένων του x. Δηλαδή,

$$w(x) = \#\{i \in \mathbf{N},\ 1 \le i \le n \mid x_i \ne 0\}$$

Προφανώς, w(x) = d(x, 0).

Παράδειγμα 3.1.8 Έστω $C \subseteq \mathbf{F}_3^4$.
Το βάρος Hamming του 1201 είναι w(1201) = 3.
Η απόσταση Hamming των 1201 και 2211 είναι d(1201, 2211) = 2.

Παρατήρηση 3.1.9 Η απόσταση Hamming d(C) είναι μια μετρική στον $\mathbf{F}_q^n$ και το βάρος Hamming w είναι μια νόρμα στον $\mathbf{F}_2^n$.

Ορισμός 3.1.10 Αν $C \subseteq \mathbf{F}_q^n$ ένας (n, k)-κώδικας, **η ελάχιστη απόσταση $d_{min}(C)$ του κώδικα** είναι

$$d_{min}(C) = \min_{\substack{u,v \in C \\ u \ne v}} d(u, v)$$

Άρα, όταν παίρνουμε το y πρέπει να ελέγχουμε τις q^k κωδικές λέξεις για να βρούμε ποια έχει την μικρότερη απόσταση Hamming από το y. Προφανώς, αυτή η διαδικασία είναι αδύνατη για μεγάλα k και ένας από τους στόχους της θεωρίας κωδίκων είναι να βρει κώδικες με γρηγορότερους αλγόριθμους αποκωδικοποίησης.

Το επόμενο αποτέλεσμα μας δείχνει ότι για κάθε γραμμικό κώδικα, η ελάχιστη απόσταση μπορεί να υπολογισθεί από το βάρος Hamming των κωδικών λέξεων.

Μια από τις πιο σημαντικές ιδιότητες των γραμμικών κωδίκων είναι η παρακάτω

Πρόταση 3.1.11 Έστω C ένας γραμμικός (n, k)-κώδικας. Η ελάχιστη απόσταση του C είναι ίση με το ελάχιστο δυνατό βάρος που έχει κωδική λέξη διάφορη του μηδενικού στοιχείου.

Απόδειξη Έστω w το ελάχιστο δυνατό βάρος Hamming κωδικής λέξης διάφορης του μηδενικού στοιχείου 0. Έστω $x \in C$ μια κωδική λέξη βάρους Hamming w. Τότε ισχύει ότι d(x, 0) = w(x) = w. Επομένως, ισχύει ότι $w \ge d_{min}(C)$. Τώρα έστω u και v ένα ζευγάρι κωδικών λέξεων του C με απόσταση τέτοια ώστε $d(u, v) = d_{min}(C)$. Αφού C γραμμικός κώδικας έπεται ότι και η u – v είναι επίσης κωδική λέξη. Η u – v έχει βάρος $d_{min}(C)$. Επομένως, $d_{min}(C) \ge w$. Δηλαδή, $d_{min}(C) = w$.

Ορισμός 3.1.12 Το σύνολο $S_r(x) := \{y \in \mathbf{F}_q^n \mid d(x, y) \le r\}$ θα λέγεται η **σφαίρα ακτίνας r ως προς το x** $\in \mathbf{F}_q^n$.

Παράδειγμα 3.1.13 Έστω $C = \mathbf{F}_2^3$ τότε ο κύκλος με ακτίνα 1 ως προς το 100 είναι

$$S_1(100) = \{100,000,110,101\}.$$

Στόχος Παίρνοντας σφαίρες κατάλληλης ακτίνας r κέντρου κωδικής λέξης θα πρέπει κατά το δυνατό να καλύπτει η ένωσή τους όλο το χώρο $\mathbf{F}_q^n$ ώστε να μπορούμε να αποκωδικοποιούμε όλα τα κωδικοποιημένα μηνύματα που λαμβάνουμε ενώ συγχρόνως η ακτίνα r θα πρέπει να είναι αρκετά μικρή ώστε οι σφαίρες να μην τέμνονται (ή εφάπτονται) και να μπορούμε να αποκωδικοποιούμε μονοσήμαντα.

Πρέπει πάντως να ισχύει ότι $r < \frac{1}{2} d_{min}(C)$.

Η σημασία της ιδέας της ελάχιστης απόστασης δίνεται από την

Πρόταση 3.1.14 Υποθέτουμε ότι ο C είναι γραμμικός κώδικας με ελάχιστη απόσταση $d_{min}(C) = d$. Ο C **ανιχνεύει** την ύπαρξη d–1 ή λιγότερων λαθών και **διορθώνει** e λάθη για κάθε e τέτοιο ώστε $2e + 1 \le d$.

Απόδειξη Έστω ότι λάβαμε το μήνυμα y με απόσταση f από την κωδική λέξη x, όπου $f \le d–1$. Φανταζόμαστε ότι η x είναι η μεταδιδόμενη (αρχική) λέξη και y η λέξη που πήραμε τελικά. Δηλαδή έχουμε f λάθη κατά την μεταφορά. Επειδή d είναι η ελάχιστη απόσταση του C η λέξη y καταλαβαίνουμε αμέσως ότι δεν μπορεί να είναι κωδική λέξη. Δηλαδή, ο κώδικας C ανακαλύπτει $d – 1$ ή λιγότερα λάθη.

Αν τώρα το μήνυμα y έχει απόσταση e από την κωδική λέξη x και $2e + 1 \le d$ τότε δεν υπάρχει άλλη κωδική λέξη πιο κοντά στη y, διότι αν $d(y, x_1) \le e$ για κάποια x_1 τότε θα ίσχυε

$$d(x, x_1) \le d(x, y) + d(y, x_1) \le e + e < d$$

άτοπο, διότι η ελάχιστη απόσταση του κώδικα C είναι d. Επομένως, υπάρχει μοναδική κοντινότερη λέξη του y και συνεπώς ο C διορθώνει e λάθη σ' αυτήν την περίπτωση.

Ένα από τα βασικά προβλήματα στη θεωρία κωδίκων είναι να ελαχιστοποιηθούν τα λάθη αλλά χωρίς να μειωθεί υποχρεωτικά **η αναλογία της πληροφορίας** $\frac{k}{n}$.

Κεντρικό πρόβλημα της Θεωρίας Κωδίκων είναι το εξής:

Δίνονται d, n *φυσικοί αριθμοί. Να υπολογιστεί ο μέγιστος αριθμός διανυσμάτων, έστω* $A_q(n, d)$*, του διανυσματικού χώρου* $\mathbf{F}_q^n$ *τα οποία ανά δυο να έχουν απόσταση μεγαλύτερη ή ίση με* d. *Φυσικά, αν είναι δυνατόν να βρεθούν τα διανύσματα.*

Για q = 2 θα συμβολίζουμε A(n, d) = A_2(n, d).

Ο επόμενος πίνακας μας δίνει κάποιες τιμές του A(n, d) για d = 3

N	3	4	5	6	7	8	9	10
A(n, 3)	2	2	4	8	16	20	40	άγνωστος, μεταξύ 72 και 79

Αυτό το πρόβλημα χαρακτηρίζεται και σαν "discrete sphere packing problem" (Conway and Sloan, 1988)

Ορισμός 3.1.15 Ένας κώδικας C ο οποίος **διορθώνει** την ύπαρξη t λαθών θα λέγεται **t-κώδικας διόρθωσης λαθών** (**t-error-correcting code**), ενώ ένας κώδικας C που **ανιχνεύει** e λάθη θα λέγεται **e-κώδικας ανίχνευσης λαθών** (**e-error-detecting code**).

Έστω τώρα C κώδικας ως προς το $\mathbf{F}_q$ μήκους n με πλήθος κωδικών λέξεων M. Υποθέτουμε ότι ο κώδικας είναι ένας t-κώδικας διόρθωσης λαθών. Υπάρχουν $(q-1)^m\binom{n}{m}$ διανύσματα του $\mathbf{F}_q^n$ τα οποία έχουν βάρος m στο $\mathbf{F}_q$. Αν $c \in C$ τότε μέσα στην σφαίρα $S_t(c)$ υπάρχουν $1 + (q-1)\binom{n}{1} + \ldots + (q-1)^t\binom{n}{t}$ διανύσματα του $\mathbf{F}_q^n$.

Θεώρημα 3.1.16 (Φράγμα του Hamming) Οι παράμετροι q, n, t, M ενός t-κώδικα διόρθωσης λαθών C ορισμένου στο σώμα $\mathbf{F}_q$ μήκους n με M κωδικές λέξεις ικανοποιούν την ανισότητα

$$M\left(1 + (q-1)\binom{n}{1} + \ldots + (q-1)^t\binom{n}{t}\right) \le q^n.$$

Αν όλα τα διανύσματα του $\mathbf{F}_q^n$ είναι μέσα σε σφαίρες ακτίνας t κέντρου κωδικών λέξεων ενός (n, k)-γραμμικού κώδικα τότε παίρνουμε μια ειδική κατηγορία κωδίκων:

Ορισμός 3.1.17 Ένας t-κώδικας διόρθωσης λαθών ορισμένος στο σώμα $\mathbf{F}_q$ θα ονομάζεται **τέλειος** αν στο θεώρημα 3.1.16 ισχύει η ισότητα.

Αν ο C είναι κώδικας όπως αυτός του θεωρήματος 3.1.16 με $d_{min}(C) = d = 2t + 1$, τότε αν διαγράψουμε τα τελευταία d – 1 σύμβολα πάλι έχουμε έναν κώδικα με όλες τις κωδικές λέξεις διαφορετικές. Ο κώδικας που προκύπτει έχει μήκος n – d + 1, και παίρνουμε το

Θεώρημα 3.1.18 (Φράγμα του Singleton) Αν ένας κώδικας $C \subseteq \mathbf{F}_q^n$ έχει ελάχιστη απόσταση d, τότε $|C| \le q^{n-d+1}$ ή αλλιώς $k \le n - d + 1$.

Ορισμός 3.1.19 Ένας κώδικας C θα λέγεται **διαχωρίσιμος μέγιστης απόστασης** (**maximum distance separable**) ή πιο απλά **κώδικας MDS** αν στο θεώρημα 3.1.18 ισχύει η ισότητα.

Παράδειγμα 3.1.20 Έστω ο κώδικας

$$C = \{000000, 001011, 010101, 011110, 100110, 101101, 110011, 111000\} \subseteq \mathbf{F}_2^6$$

όπου $d_{min}(C) = 3$. Έχουμε επομένως, M = 8, q = 2, n = 6, d = 3, t = 1. Το φράγμα του Hamming δίνει την ανισότητα $8\left(1+\binom{6}{1}\right) \le 2^6$, δηλαδή 56 < 64. Αυτό σημαίνει ότι μόνο 64 – 56 = 8 λέξεις μήκους 6 στο $\mathbf{F}_2^6$ βρίσκονται έξω από κάποια σφαίρα και δεν μπορούν να διορθωθούν σωστά (αυτό είναι προφανές και από το γεγονός ότι έχουμε 8 μη τεμνόμενες σφαίρες με 7 στοιχεία η κάθε μια). Ένα παράδειγμα μιας από τις 8 λέξεις που δεν μπορούν να διορθωθούν σωστά είναι η 100100 η οποία έχει απόσταση μεγαλύτερη ή ίση του 2 από όλες τις κωδικές λέξεις. Το φράγμα του Singleton μας δίνει $8 \le 2^4 = 16$, άρα ο C δεν είναι MDS.

Ας υποθέσουμε τώρα ότι τα σύμβολα ελέγχου μπορούν να προκύψουν από το k-μήνυμα με τέτοιο τρόπο ώστε οι κωδικές λέξεις x να ικανοποιούν το σύστημα με γραμμικές εξισώσεις

$$Hx^T = 0,$$

όπου H είναι ένας δοσμένος (n – k) × n πίνακας με στοιχεία από το σώμα $\mathbf{F}_q$. Η **κανονική μορφή** για τον πίνακα H είναι $[A \mid I_{n-k}]$ όπου A ένας (n – k) × k πίνακας και I_{n-k} ο (n – k) × (n – k) μοναδιαίος πίνακας.

Προκύπτει ο παρακάτω

Ορισμός 3.1.21 Έστω H ένας (n – k) × n πίνακας με βαθμό n – k και στοιχεία από το σώμα $\mathbf{F}_q$. Το σύνολο όλων των n-διάστατων διανυσμάτων x που ικανοποιούν την εξίσωση $Hx^T = 0$ ονομάζονται **γραμμικός κώδικας** C πάνω από το $\mathbf{F}_q$ με **μήκος** n. Ο πίνακας H είναι ο **πίνακας ελέγχου ισοτιμίας (parity-check matrix)** του κώδικα.C ο οποίος ονομάζεται και γραμμικός (n, k)-κώδικας. Αν ο H είναι στην μορφή $[A \mid I_{n-k}]$ τότε τα πρώτα k σύμβολα από την κωδική λέξη x είναι το αρχικό k-μήνυμα, ενώ τα υπόλοιπα n – k σύμβολα του x είναι τα σύμβολα ελέγχου. Ο C ονομάζεται επίσης **συστηματικός γραμμικός (n, k)-κώδικας** και τότε θεωρούμε ότι ο H είναι στην **κανονική μορφή**. Αν q = 2 τότε ο C ονομάζεται **δυαδικός κώδικας** (**binary code**).

Παρατήρηση 3.1.22 Το σύνολο C των λύσεων x της $Hx^T = 0$ (ή αλλιώς ο **μηδενόχωρος** του H) είναι ένας υπόχωρος του διανυσματικού χώρου $\mathbf{F}_q^n$ με διάσταση k. Επειδή οι κωδικές λέξεις είναι προσθετική ομάδα, ο C ονομάζεται επίσης **κώδικας-ομάδα**.

Παράδειγμα 3.1.23 (**Κώδικας Επανάληψης**) Αν κάθε κωδική λέξη ενός κώδικα C αποτελείται από ένα μόνο σύμβολο $a_1 \in \mathbf{F}_q$ και τα υπόλοιπα n–1 σύμβολα ελέγχου $x_2 = \ldots = x_n$ είναι όλα ίσα με a_1 (Το a_1 επαναλαμβάνεται άλλες n–1 φορές) τότε λαμβάνουμε έναν διαδικό (n, 1)-κώδικα με πίνακα ελέγχου ισοτιμίας

$$H = \begin{bmatrix} 1 & 1 & 0 & \dots & 0 \\ 1 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \dots & 1 \end{bmatrix}$$

Υπάρχουν μόνο δύο κωδικές λέξεις σε αυτόν τον κώδικα. Οι λέξεις 00…0 και 11…1.

Στους κώδικες επανάληψης μπορούμε, φυσικά, να χρησιμοποιήσουμε κωδικές λέξεις με περισσότερα από ένα σύμβολα για το αρχικό μήνυμα. Αν για παράδειγμα μεταδώσουμε ένα μήνυμα μήκους k τρεις φορές και συγκρίνουμε τις αντίστοιχες «συντεταγμένες» x_i, x_{k+i}, x_{2k+i} της κωδικής λέξης

$$x_1 \dots x_i \dots x_k x_{k+1} \dots x_{k+i} \dots x_{2k} x_{2k+1} \dots x_{2k+i} \dots x_{3k},$$

τότε ποιο ήταν το k-μήνυμα που στάλθηκε το αποφασίζουμε με το «πλειοψηφικό σύστημα», δηλαδή αν $x_i = x_{k+i} \neq x_{2k+i}$, τότε μάλλον έχει σταλεί το x_i και όχι το x_{2k+i}. Είναι συχνά πάντως μη πρακτικό, δύσκολο ή πολύ δαπανηρό να στέλνουμε το αρχικό μήνυμα πάνω από μία φορά.

Είδαμε, ότι σε ένα συστηματικό κώδικα, ένα μήνυμα $a = a_1, \dots, a_k$ κωδικοποιείται σε ένα κωδικό μήνυμα $x = x_1, \dots, x_n$ με $x_1 = a_1, x_2 = a_2, \dots, x_k = a_k$. Οι εξισώσεις ελέγχου $[A \mid I_{n-k}]x^T = 0$ δίνονται από το σύστημα

$$\begin{pmatrix} x_{k+1} \\ \vdots \\ x_n \end{pmatrix} = -A \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = -A \begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix}$$

από όπου παίρνουμε

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{bmatrix} I_k \\ -A \end{bmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix}$$

το οποίο γράφεται και στη μορφή

$$(x_1, \dots, x_n) = (a_1, \dots, a_k)\,[I_k \mid -A^T].$$

Ορισμός 3.1.24 Ο πίνακας $G = [I_k \mid -A^T]$ ονομάζεται (**κανονικός**) **γεννήτορας πίνακας** (ή **κανονικός βασικός πίνακας** ή **πίνακας κωδικοποίησης**) του γραμμικού (n, k)-κώδικα με πίνακα ελέγχου ισοτιμίας $H = [A \mid I_{n-k}]$ στην κανονική μορφή.

Ισχύει: $GH^T = 0$.

Παραδείγματα 3.1.25

(1) Έστω $G = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$.

Ο γραμμικός (2,3)-κώδικας $C \subseteq \mathbf{F}_2^3$ αποτελείται από όλους τους συνδυασμούς των δυο γραμμών:

$$000,\ 101,\ 011,\ 110$$

Οι κωδικές λέξεις μπορούν να περιγραφούν σαν διανύσματα της μορφής uG, όπου u = 00, 01, 10, 11. Κάθε κωδική λέξη, διάφορη της μηδενικής, έχει βάρος ίσο με 2. Αυτό σημαίνει ότι ο κώδικας ανιχνεύει μέχρι 1 λάθος, αλλά δεν διορθώνει λάθη.

(2) Αν $G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$.

Από τις τρεις γραμμές του πίνακα παίρνουμε τον (3, 6)-κώδικα $C \subseteq \mathbf{F}_2^6$ ο οποίος αποτελείται από 8 κωδικές λέξεις:

$$000000,\ 100110,\ 010101,\ 001011,\ 110011,\ 011110,\ 101101,\ 111000$$

Όπως και πριν κάθε κωδική λέξη x μπορεί να περιγραφεί σαν διανύσματα της μορφής $x = uG$, όπου $u = u_1u_2u_3$ με $u_i \in \mathbf{F}_2$.

Υπάρχουν τέσσερις κωδικές λέξεις βάρους 3, τρεις κωδικές λέξεις βάρους 4 και μια κωδική λέξη βάρους 0. Η ελάχιστη απόσταση του κώδικα είναι 3, επομένως ανακαλύπτει δύο λάθη και διορθώνει ένα λάθος.

(3) Αν $G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 2 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 2 & 2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$.

τότε ο κώδικας $C \subseteq \mathbf{F}_3^{12}$ αποτελείται από κωδικές λέξεις x όπου η κάθε μια μπορεί να περιγραφεί σαν διάνυσμα της μορφής $x = uG$, όπου $u = u_1u_2u_3u_4u_5u_6$ με $u_i \in \mathbf{F}_3$.
Η ελάχιστη απόσταση του κώδικα είναι το πολύ 5, αφού υπάρχει ήδη γραμμή του πίνακα G βάρους 5. Μπορεί να αποδειχθεί ότι ο κώδικας έχει ελάχιστη απόσταση ακριβώς 5. Ο κώδικας αυτός ονομάζεται **κώδικας Golay**.

Για περισσότερες πληροφορίες για τους κώδικες Golay παραπέμπουμε τον ενδιαφερόμενο αναγνώστη στο [MS], κεφάλαιο 20.

Θεώρημα 3.1.26 Έστω G ο γεννήτορας πίνακας ενός γραμμικού κώδικα C. Τότε οι γραμμές του G σχηματίζουν μια βάση του C.

Απόδειξη Οι k γραμμές του πίνακα G είναι γραμμικώς ανεξάρτητες από τον ορισμό του γεννήτορα πίνακα ενός γραμμικού κώδικα. Αν r είναι ένα διάνυσμα-γραμμή του G τότε $rH^T = 0$ άρα και $Hr^T = 0$ για κάθε $r \in C$. τώρα, dimC είναι η διάσταση του μηδενόχωρου του H, η οποία είναι n – rank(H) = k. Επομένως, οι k γραμμές του G σχηματίζουν μια βάση του C.

Ένας κώδικας μπορεί να έχει πολλούς πίνακες ελέγχου ισοτιμίας και γεννήτορες πίνακες. Κάθε $k \times n$ πίνακας του οποίου ο χώρος γραμμών είναι ίσος με τον C μπορεί να είναι επίσης ένας γεννήτορας πίνακας του C.

Αν ο «γεννήτορας πίνακας» H δεν είναι στην κανονική μορφή μπορούμε να τον μετατρέψουμε σε ένα πίνακα της μορφής $[I_k \mid -A^T]$ χωρίς να αλλάξουμε τον μηδενόχωρο του H, δηλαδή τον κώδικα C. Μετά μετατρέπουμε τις συντεταγμένες για να σχηματίσουμε τον πίνακα H' ο οποίος να είναι σε κανονική μορφή. Οι συντεταγμένες του κώδικα C' που αντιστοιχεί στον H' είναι «ισοδύναμος» με τον C με την ακόλουθη έννοια:

Ορισμός 3.1.27 Δύο κώδικες C και C' ίδιου μήκους n θα λέγονται **ισοδύναμοι** αν υπάρχει μια μετάθεση π του συνόλου {1, 2, …, n} τέτοια ώστε

$$(x_1, \ldots, x_n) \in C \Leftrightarrow \left(x_{\pi(1)}, \ldots, x_{\pi(n)}\right) \in C'$$

Έτσι, σχηματίζουμε τον γεννήτορα πίνακα G' του πίνακα C' και ύστερα εφαρμόζουμε την αντίστροφη μετάθεση π^{-1} στις συντεταγμένες.

Ας αναφέρουμε έναν ορισμό που θα μας χρειαστεί σε επόμενη παράγραφο:

Ορισμός 3.1.28 Ένα γραμμικός κώδικας C μήκους n, διάστασης k και ελάχιστης απόστασης d θα ονομάζεται **(n, k, d)-κώδικας**.

Έστω τώρα, $u = u_1, \ldots, u_n$ και $v = v_1, \ldots, v_n$ δύο διανύσματα του διανυσματικού χώρου $\mathbf{F}_q^n$ και έστω $u \cdot v = u_1v_1 + \ldots + u_nv_n$ να συμβολίζει το γινόμενο των u και v πάνω από τον $\mathbf{F}_q^n$. Αν $u \cdot v = 0$ τότε τα u και v θα λέγονται **ορθογώνια**.

Ορισμός 3.1.29 Έστω C ένας γραμμικός (n, k)-κώδικας ορισμένος στο σώμα $\mathbf{F}_q$. Ο **δυϊκός** (ή **ορθογώνιος) κώδικας** $C^\perp$ του κώδικα C ορίζεται να είναι ο

$$C^\perp = \{u \mid uv = 0 \text{ για κάθε } v \in C\}$$

Επειδή ο C είναι ένας k-διάστατος υπόχωρος του n-διάστατου διανυσματικού χώρου $\mathbf{F}_q^n$ το ορθογώνιο συμπλήρωμα του C είναι διάστασης n – k και είναι ένας (n, n – k) κώδικας. Μπορεί να αποδειχτεί ότι αν ο κώδικας C έχει γεννήτορα τον πίνακα G και πίνακα ελέγχου ισοτιμίας H τότε ο $C^\perp$ έχει γεννήτορα πίνακα τον H και πίνακα ελέγχου ισοτιμίας του G. Η ορθογωνιότητα των δύο κωδίκων μπορεί να εκφραστεί

από τη σχέση $GH^T = HG^T = 0$. Τώρα θα συνοψίσουμε κάποιες απλές ιδιότητες των γραμμικών κωδίκων.

Παρατήρηση 3.1.30 Έστω mld(H) ο ελάχιστος αριθμός γραμμικά εξαρτημένων στηλών του H. Επειδή οποιεσδήποτε rank(H) + 1 το πλήθος στήλες του H είναι γραμμικά εξαρτημένες προφανώς ισχύει, $mld(H) \leq rank(H) + 1$ για κάθε πίνακα H.

Θεώρημα 3.1.31 Έστω H ένας πίνακας ελέγχου ισοτιμίας ενός (n, k, d)-κώδικα C με $n > k$. Τότε ισχύουν:

(i) $dimC = k = n - rank(H)$
(ii) $d = mld(H)$
(iii) $d \leq n - k + 1$.

Απόδειξη Το (i) είναι προφανές ενώ το (iii) προκύπτει από το (ii) και την προηγούμενη παρατήρηση. Για να αποδείξουμε το (ii) ας υποθέσουμε ότι ο H έχει στήλες $s_1, \ldots, s_n$. Παίρνουμε μια κωδική λέξη $c = (c_1, \ldots, c_n) \in C$ με βάρος w. Τότε επειδή

$$Hc^T = c_1s_1 + \ldots c_ns_n$$

ισχύει ότι $c_1s_1 + \ldots c_ns_n = 0$. Έχουμε επίσης ότι η c έχει μη-μηδενική συντεταγμένη σε w θέσεις επομένως κάποιες w, και μάλιστα όχι λιγότερες, στο πλήθος στήλες του H είναι γραμμικά εξαρτημένες. Δηλαδή, $mld(H) = w$. Εφαρμόζοντας την πρόταση 3.1.11 έχουμε ότι η ελάχιστη απόσταση d του κώδικα είναι ίση με το βάρος της c και συνεπώς το ζητούμενο.

Προκειμένου να επιβεβαιώσουμε την ύπαρξη γραμμικών (n, k)-κωδίκων με ελάχιστη απόσταση d πάνω από το $\mathbf{F}_q$ αρκεί να δείξουμε ότι υπάρχει $(n - k) \times n$ πίνακας H με $mld(H) = d$.

Θεώρημα 3.1.32 (Φράγμα των Gilbert – Varshamov)

Αν

$$q^{n-k} > \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i$$

τότε μπορούμε να κατασκευάσουμε έναν γραμμικό (n, k)-κώδικα ορισμένο στο σώμα $\mathbf{F}_q$ με ελάχιστη απόσταση μεγαλύτερη ή ίση από d. (Δες [LP], κεφάλαιο 4, θεώρημα 17.14, σελίδα 196).

Απόδειξη Θα κατασκευάσουμε έναν $(n - k) \times n$ πίνακα ελέγχου ισοτιμίας H ενός τέτοιου κώδικα. Έστω ότι η πρώτη στήλη του H είναι ένα οποιοδήποτε διάνυσμα μήκους $n - k$ με στοιχεία από το $\mathbf{F}_q$. Η δεύτερη στήλη είναι ένα οποιοδήποτε διάνυσμα μήκους $n - k$ με στοιχεία από το $\mathbf{F}_q$ το οποίο δεν είναι (βαθμωτό) πολλαπλάσιο της πρώτης στήλης. Έστω ότι έτσι έχουμε επιλέξει $j - 1$ στήλες από τις οποίες οποιεσδήποτε $d - 1$ από αυτές είναι γραμμικά ανεξάρτητες. Υπάρχουν το πολύ

$\sum_{i=0}^{d-2}\binom{j-1}{i}(q-1)^i$ διανύσματα τα οποία λαμβάνουμε αν πάρουμε γραμμικούς συνδυασμούς από το πολύ $d-2$ από αυτές τις $j-1$ στήλες. Αν ισχύει η ανισότητα του θεωρήματος μπορούμε να βρούμε μια επιπλέον στήλη η οποία να είναι γραμμικά ανεξάρτητη με οποιεσδήποτε $d-2$ από τις πρώτες $j-1$ στήλες. Με αυτόν τον τρόπο κατασκευάζουμε τελικά ένα πίνακα τάξης $n-k$. Λόγω του ότι δεν υπάρχουν $d-1$ στήλες του Η οι οποίες να είναι γραμμικά εξαρτημένες ο κώδικας που προκύπτει έχει ελάχιστη απόσταση μεγαλύτερη ή ίση από d.

Χωρίς απόδειξη αναφέρουμε το

Θεώρημα 3.1.33 (Φράγμα του Plotkin) Αν υπάρχει ένας γραμμικός κώδικας μήκους n με M κωδικές λέξεις και ελάχιστη απόσταση d πάνω από το $\mathbf{F}_q$ τότε

$$d \le n\,\frac{M(q-1)}{(M-1)q}$$

(Δες [LP], κεφάλαιο 4, θεώρημα 17.15, σελίδα 197).

Για να πετύχουμε καλύτερα αποτελέσματα μπορούμε να δημιουργήσουμε **πλεγμένους κώδικες** (**concatenated codes**) συνδέοντας αλυσιδωτά δύο κώδικες με τον παρακάτω τρόπο:

Έστω C_1 ένας (n_1, k_1, d_1)-κώδικας και C_2 ένας (n_2, k_2, d_2)-κώδικας. Έστω ότι το μήνυμα που θέλουμε να στείλουμε είναι το $\alpha = \alpha_1, \ldots, \alpha_{k_1}$ όπου $\alpha_i = \beta_{i_1}, \beta_{i_2}, \ldots, \beta_{i_{k_2}}$ με $\alpha_i \in GF(2^{k_2})$. Μέσω του κώδικα C_1 κωδικοποιούμε το α στο $c = c_1, \ldots, c_{n_1}$ όπου $c_i \in GF(2^{k_2})$ και είναι της μορφής $c_i = \gamma_{i_1}, \gamma_{i_2}, \ldots, \gamma_{i_{k_2}}$. Στη συνέχεια παίρνουμε κάθε c_i και το κωδικοποιούμε με την βοήθεια του κώδικα C_2 στο $y_i = y_{i_1}, y_{i_2}, \ldots, y_{i_{n_2}}$. Επομένως, συνολικά το μήνυμα α που θέλουμε να στείλουμε κωδικοποιείται μέσω του κώδικα C, ο οποίος προκύπτει από την αλυσιδωτή σύνδεση των κωδίκων C_1 και C_2, στην κωδική λέξη $c = (y_{1_1}, y_{1_2}, \ldots, y_{1_{n_2}})(y_{2_1}, y_{2_2}, \ldots, y_{2_{n_2}})\ldots(y_{n_{11}}, y_{n_{12}}, \ldots, y_{n_{1n_2}})$

Ισχύει η ακόλουθη

Πρόταση 3.1.34 Η ελάχιστη απόσταση του κώδικα C, που περιγράψαμε παραπάνω, είναι τουλάχιστον $d_1 \cdot d_2$.

2. Κώδικες που ορίζονται μέσω αλγεβρικών καμπυλών

Έστω **F** η αλγεβρική θήκη του σώματος $\mathbf{F}_q$. Αν $\boldsymbol{X}$ αφινική καμπύλη ορισμένη πάνω στο σώμα $\mathbf{F}_q$, τότε $\mathbf{F}_q[\boldsymbol{X}]$ είναι ο δακτύλιος συντεταγμένων της $\boldsymbol{X}$ και $\mathbf{F}_q(\boldsymbol{X})$ το σώμα συναρτήσεών της, το οποίο είναι το σώμα πηλίκων του $\mathbf{F}_q[\boldsymbol{X}]$. Θα υποθέτουμε πάντα ότι η καμπύλη είναι απολύτως ανάγωγη, δηλαδή ότι παραμένει ανάγωγη ακόμη και όταν θεωρηθεί σαν καμπύλη πάνω από το σώμα **F**. Ανάλογες παραδοχές ισχύουν και για προβολικές καμπύλες. Ας σημειωθεί ότι για κάθε πολυώνυμο $F \in \mathbf{F}_q[X, Y]$ ισχύει $F(x_1, y_1)^q = F(x_1^q, y_1^q)$. Αυτό σημαίνει ότι, αν (x_1, y_1) είναι ρίζα του F, ορισμένη στο σώμα $\mathbf{F}_q$, τότε το (x_1^q, y_1^q) είναι επίσης ρίζα του F.

Αν τώρα η καμπύλη $\boldsymbol{X}$ ορίζεται στο σώμα $\mathbf{F}_q$ και P είναι ένα σημείο της καμπύλης τότε σύμφωνα με την παραπάνω παρατήρηση το Fr(P) είναι επίσης σημείο της καμπύλης $\boldsymbol{X}$ (δες πρόταση 2.3.1).

Ορισμός 3.2.1 Ένας **διαιρέτης** D της καμπύλης $\boldsymbol{X}$ είναι ένα τυπικό άθροισμα της μορφής $D = \sum_{P \in X} n_P P$ όπου $n_P \in \mathbf{Z}$ και $n_P = 0$ για σχεδόν όλα τα σημεία P της $\boldsymbol{X}$.

Ορίζουμε την πρόσθεση διαιρετών εντελώς φυσιολογικά, κατά συνιστώσες.

Ορισμός 3.2.2 Ο **φορέας** (**support**) ενός διαιρέτη είναι το σύνολο των σημείων P για τα οποία ο συντελεστής n_P είναι διάφορος του μηδενός. Ο διαιρέτης θα λέγεται **effective** όταν όλοι οι συντελεστές n_P είναι μη αρνητικοί.

Ορισμός 3.2.3 **Βαθμός** deg(D) ενός διαιρέτη $D = \sum_{P \in X} n_P P$ θα λέγεται το, πεπερασμένο, άθροισμα $\deg(D) = \sum_{P \in X} n_P$.

Ορισμός 3.2.4 Ο διαιρέτης D μιας καμπύλης $\boldsymbol{X}$ θα λέγεται **ρητός** όταν οι συντελεστές P και Fr(P) είναι ίδιοι για κάθε σημείο P της $\boldsymbol{X}$.

Ορισμός 3.2.5 Για κάθε διαιρέτη D της καμπύλης $\boldsymbol{X}$ ορίζεται ο πεπερασμένης διάστασης **F**-διανυσματικός χώρος

$$L(D) := \{ f \in \mathbf{F}(\boldsymbol{X})^* \mid < f > + D \geq 0 \} \cup \{0\}.$$

Με $< f >$ θα συμβολίζουμε τον **κύριο διαιρέτη** της ρητής συνάρτησης f, ο οποίος ορίζεται σαν $< f > = \sum_{P \in X} n_P P$ και ο συντελεστής n_P είναι διάφορος του μηδενός για τα σημεία P στα οποία η f έχει **ρίζα** πολλαπλότητας n_P, $n_P > 0$ και στα σημεία που η f έχει πόλο τάξης $-n_P$, $n_P < 0$ ενώ σε όλα τα άλλα σημεία ο συντελεστής n_P είναι μηδέν.

Αναφέρουμε χωρίς απόδειξη το

Θεώρημα 3.2.6 Ο βαθμός του κύριου διαιρέτη $< f >$ μιας ρητής συνάρτησης f είναι πάντοτε 0. (Για απόδειξη δες [Ho], θεώρημα 2.32, σελίδα 885)

Μπορούμε να τροποποιήσουμε τον ορισμό 3.2.5 για να ορίσουμε τον **F**-διανυσματικό χώρο $L(D)_{rat.}$ των ρητών διαιρετών της καμπύλης $\boldsymbol{X}$ ως εξής:

Ορισμός 3.2.7 Για κάθε **ρητό** διαιρέτη D της καμπύλης $\boldsymbol{X}$ ορίζεται ο πεπερασμένης διάστασης **F**-διανυσματικός χώρος

$$L(D)_{rat.} := \{ f \in \mathbf{F}_q(\boldsymbol{X})^* \mid < f > + D \geq 0 \} \cup \{0\}.$$

Η τροποποίηση αυτή δεν δημιουργεί προβλήματα, διότι όλες οι προτάσεις που χρειαζόμαστε που ισχύουν για τον αρχικό ορισμό του L(D) στο σώμα **F** ισχύουν και για τον $L(D)_{rat.}$ στο σώμα $\mathbf{F}_q$.

Στο εξής όταν γράφουμε L(D) θα αναφερόμαστε στον $L(D)_{rat.}$

Παρατήρηση 3.2.8 Αν D διαιρέτης με $D = \sum n_i Q_i$ όπου $n_i \in \mathbf{Z}$ και f μια ρητή συνάρτηση στο χώρο L(D) τότε όταν είναι $n_i < 0$ η f έχει **ρίζα** στο Q_i πολλαπλότητας τουλάχιστον $|n_i|$, ενώ όταν $n_i > 0$ τότε η f έχει το Q_i σαν **πόλο** τάξης το πολύ n_i.

Έστω λοιπόν $\boldsymbol{X}$ απόλυτα ανάγωγη μη-ιδιάζουσα προβολική καμπύλη ορισμένη στο σώμα $\mathbf{F}_q$.

Αν $P_1, P_2, \ldots, P_n$ ρητά σημεία της $\boldsymbol{X}$ και D ο διαιρέτης $D := P_1 + P_2 + \ldots + P_n$. Έστω ακόμα G κάποιος άλλος διαιρέτης της $\boldsymbol{X}$ τέτοιος ώστε ο φορέας του G να είναι **ξένος** προς τον φορέα της D και επιπλέον να ισχύει:

$$2g - 2 < \deg(G) < n.$$

Ορισμός 3.2.9 Ο γραμμικός κώδικας C(D, G) μήκους n στο σώμα $\mathbf{F}_q$ είναι η εικόνα της γραμμικής συνάρτησης

$$\alpha : L(G) \rightarrow \mathbf{F}_q^n$$

όπου $\alpha(f) = \left(f(P_1), f(P_2), \ldots, f(P_n)\right)$. Κώδικες αυτού του τύπου, λέγονται **γεωμετρικοί Reed-Solomon κώδικες**.

Ισχύει το ακόλουθο

Θεώρημα 3.2.10 Ο κώδικας C(D, G) έχει διάσταση $\kappa = \deg(G) - g + 1$, όπου g είναι το γένος της καμπύλης $\boldsymbol{X}$ και ελάχιστη απόσταση

$$d \geq n - \deg(G)$$

Απόδειξη Έστω $f \in L(G)$, δηλαδή $< f > + G \geq 0$.
Έστω ότι η f ανήκει στον πυρήνα του α, δηλαδή

$$\alpha(f) = (f(P_1), f(P_2), \ldots, f(P_n)) = (0, 0, \ldots, 0)$$

πράγμα που σημαίνει ότι η f έχει ρίζες στα σημεία $P_1, P_2, \ldots, P_n$ τάξης τουλάχιστον ένα. Επειδή $D = P_1 + P_2 + \ldots + P_n$ έχουμε ότι $-D = -P_1 - P_2 - \ldots - P_n$. Ο –D έχει πόλους στα σημεία $P_1, P_2, \ldots, P_n$ τάξης <u>ακριβώς</u> ένα. Επομένως, $< f > + G - D \geq 0$. Πράγμα που σημαίνει ότι $f \in L(G - D)$.

Ο βαθμός του –D είναι $\deg(-D) = -n$ και επομένως βαθμός του διαιρέτη G – D είναι $\deg(G - D) = \deg G + \deg(-D) < n - n = 0$. Σύμφωνα με γνωστό θεώρημα της θεωρίας αλγεβρικών καμπυλών όταν ο βαθμός ενός διαιρέτη Δ είναι μικρότερος του μηδενός, τότε ο χώρος $L(\Delta)$ έχει διάσταση $l(\Delta) = 0$. (Δες [Ho], θεώρημα 2.37, σελίδα 886). Επομένως, $L(G - D) = \{0\}$, δηλαδή

$$f \in \ker\alpha \Leftrightarrow f = 0$$

οπότε καταλήγουμε στο συμπέρασμα ότι η απεικόνιση α είναι ένα προς ένα.

Εξ' υποθέσεως ισχύει, $2g - 2 < \deg(G) < n$. Άμεση συνέπεια του θεωρήματος των Riemann – Roch (δες [Ho], θεώρημα 2.55, σελίδα 890) είναι ότι αν ο βαθμός, ενός διαιρέτη Δ, είναι $\deg(\Delta) > 2g - 2$ τότε έχει διάσταση $l(\Delta) = \deg(\Delta) - g + 1$ (δες [Ho], συνέπεια 2.58, σελίδα 890). Επομένως, $\kappa = l(G) = \deg(G) - g + 1$.

Θα αποδείξουμε τώρα ότι η ελάχιστη απόσταση του κώδικα είναι μεγαλύτερη ή ίση από $n - \deg(G)$.

Αν η εικόνα α(f), $f \in L(G)$, έχει βάρος d τότε αυτό σημαίνει ότι <u>δεν</u> μηδενίζεται σε ακριβώς d σημεία εκ των $P_1, P_2, \ldots, P_n$. Συνεπώς μηδενίζεται σε ακριβώς n – d σημεία εκ των $P_1, P_2, \ldots, P_n$. Άρα $f(P_{i_1}) = f(P_{i_2}) = \ldots = f(P_{i_{n-d}}) = 0$. Ονομάζουμε E τον διαιρέτη $E = P_{i_1} + P_{i_2} + \ldots + P_{i_{n-d}}$. Επομένως $< f > + G - E \geq 0$. Πράγμα που σημαίνει ότι $f \in L(G - E)$. Από τους βαθμούς των αντίστοιχων διαιρετών έχουμε ότι $\deg G + \deg< f > - \deg E \geq 0$. Από το θεώρημα 3.2.6 έχουμε ότι $\deg< f > = 0$ άρα ισχύει $\deg G - \deg E \geq 0$ ή $\deg G - (n - d) \geq 0$. Και τελικά $d \geq n - \deg G$ και η απόδειξη έχει τελειώσει.

Είναι προφανές ότι έχουμε κατασκευάσει μερικούς **καλούς** κώδικες. Αν εφαρμόσουμε το θεώρημα 3.2.10 για καμπύλη γένους 0, τότε βλέπουμε ότι αυτός είναι ένας MDS κώδικας. Πράγματι το θεώρημα μας δίνει ότι

$$d \geq n - \kappa + 1$$

το οποίο συνδυαζόμενο με το φράγμα του Singleton $\kappa \leq n - d + 1$ δίνει $\kappa = n - d + 1$ δηλαδή έναν MDS κώδικα.

Γενικά, για καμπύλες μικρού γένους έχουμε κώδικες οι οποίοι πλησιάζουν αρκετά στο φράγμα του Singleton.

3. Παραδείγματα αλγεβρογεωμετρικών κωδίκων

Γνωρίζουμε ήδη ότι για να κατασκευάσουμε καλούς κώδικες θα πρέπει να κατασκευάσουμε κώδικες μεγάλου μήκους. Για να χρησιμοποιήσουμε μεθόδους της αλγεβρικής γεωμετρίας είναι αναγκαίο να θεωρήσουμε αλγεβρικές καμπύλες με μεγάλο πλήθος ρητών σημείων. Ο αριθμός αυτός των ρητών σημείων αποτελεί ένα φράγμα για το μήκος του κώδικα. Κεντρικό πρόβλημα της αλγεβρικής γεωμετρίας είναι να βρεθούν (άνω) φράγματα για το πλήθος των ρητών σημείων μια αλγεβρικής καμπύλης ή γενικότερα μιας πολλαπλότητας. Επομένως, είναι πάρα πολύ χρήσιμο το θεώρημα των Hasse – Weil (θεώρημα 2.3.3). Μάλιστα στα επόμενα παραδείγματα θα χρησιμοποιήσουμε το ακόλουθο φράγμα του Serre, το οποίο αποτελεί βελτίωση του φράγματος των Hasse – Weil.

Θεώρημα 3.3.1 (Φράγμα του Serre) Έστω $\boldsymbol{X}$ καμπύλη γένους g ορισμένη στο σώμα $\mathbf{F}_q$. Αν με $N_q(\boldsymbol{X})$ συμβολίζουμε το πλήθος των ρητών της σημείων τότε

$$\left| N_q(\boldsymbol{X}) - (q + 1) \right| \leq \left\lfloor 2\sqrt{q} \right\rfloor g.$$

(Για απόδειξη δες [St], κεφάλαιο 3, θεώρημα 3.1, σελίδα 180)

Ας αναφέρουμε δύο παραδείγματα αλγεβρογεωμετρικών κωδίκων.

Παράδειγμα 3.3.2 Έστω K_3 η τετραδική καμπύλη του Klein ορισμένη στο σώμα $\mathbf{F}_8$

$$K_3: X^3Y + Y^3Z + Z^3X = 0$$

Η καμπύλη είναι μη-ιδιάζουσα και έχει γένος 3 (βλέπε ορισμό 1.3.9). Από το φράγμα του Serre (θεώρημα 3.3.1) έχουμε ότι η καμπύλη μπορεί να έχει το πολύ $\left\lfloor 2\sqrt{8} \cdot 3 \right\rfloor + (8 + 1) = 15 + 9 = 24$ ρητά σημεία.

Θα αποδείξουμε ότι έχει ακριβώς 24. Ως γνωστό το σώμα $\mathbf{F}_8$ είναι μια απλή επέκταση βαθμού 3 του $\mathbf{F}_2$ και είναι της μορφής $\mathbf{F}_2(\xi)$ όπου $\xi^3 = \xi + 1$. Θα μελετήσουμε τα ρητά σημεία της καμπύλης $\boldsymbol{X}$ διαδοχικά ως προς τα σώματα $\mathbf{F}_2$ και $\mathbf{F}_8$. Κατ' αρχήν τα ρητά σημεία της καμπύλης ως προς το σώμα $\mathbf{F}_2$ είναι τα [1, 0, 0], [0, 1, 0], [0, 0, 1]. Ως προς το σώμα $\mathbf{F}_8$ αν ένα ρητό σημείο [x, y, z] έχει μια συντεταγμένη ίση με μηδέν, τότε αυτό το σημείο είναι κατ' ανάγκη ένα από τα παραπάνω ρητά σημεία ως προς το σώμα $\mathbf{F}_2$. Αν τώρα $xyz \neq 0$ μπορούμε να θεωρήσουμε $z = 1$. Η πολλαπλασιαστική ομάδα $\mathbf{F}_8^*$ είναι κυκλική τάξης 7 παραγόμενη από το στοιχείο ξ. Επειδή λοιπόν ισχύει $y \neq 0$ παίρνουμε $y = \xi^i$ $(0 \leq i \leq 6)$. Γράφουμε $x = \xi^{3i} \eta$. Αντικαθιστώντας στην εξίσωση της K_3 παίρνουμε

$$\xi^{9i} \eta^3 \xi^i + \xi^{3i} + \xi^{3i} \eta = 0$$

ή

$$\xi^{7i} \eta^3 + 1 + \eta = 0$$

ή

$$\eta^3 + \eta + 1 = 0$$

Επομένως, το η είναι λύση της εξίσωσης $X^3 + X + 1 = 0$ οπότε το η θα είναι και κάποιο από τα ξ, ξ^2, ξ^4.

Δηλαδή η K_3 έχει συνολικά $3 + 7 \cdot 3 = 24$ ρητά σημεία.

Έστω Q = (0, 0, 1) και έστω D το άθροισμα των υπόλοιπων 23 σημείων. G = 10Q. Από το θεώρημα 3.2.10 βρίσκουμε ότι ο κώδικας C(D, G) που δημιουργήσαμε έχει διάσταση ίση με $\kappa = \deg(G) - g + 1 = 10 - 3 + 1 = 8$ και ελάχιστη απόσταση $d \geq 23 - 10 = 13$. Είναι δηλαδή ένας (23, 8, 13)-κώδικας. Συνδέουμε αλυσιδωτά αυτόν τον κώδικα με τον (4, 3, 2)-απλού ελέγχου ισοτιμίας κώδικα ως εξής: Τα σύμβολα στις κωδικές λέξεις του C(D, G) είναι στοιχεία του $\mathbf{F}_8$ τα οποία τα βλέπουμε σαν διανύσματα-στήλη μήκους 3 πάνω από το $\mathbf{F}_2$ και μετά βάζουμε δίπλα τον πίνακα ελέγχου ισοτιμίας. Ο κώδικας C που προκύπτει είναι ένας δυαδικός (92, 24, d)-κώδικας με $d \geq 13 \cdot 2 = 26$ (Δες παρατήρηση 3.1.34). Ο συμπιεσμένος κώδικας του C, ένας (91, 24, d – 1)-κώδικας. Για d = 26 ο συμπιεσμένος (91, 24, d – 1)-κώδικας αποτελεί μέχρι σήμερα παγκόσμιο ρεκόρ για κώδικες με n = 91 και d = 25. (Δες [Ho], κεφάλαιο 10, παράγραφος 2.8, παράδειγμα 2.75).

Παράδειγμα 3.3.3 Έστω το σώμα $\mathbf{F}_4 = \{0, 1, a, \bar{a}\}$ όπου $a^2 = a + 1 = \bar{a}$ και $a^3 = 1$. Η χαρακτηριστική του σώματος είναι $ch\mathbf{F}_4 = 2$. Θεωρούμε την καμπύλη $\boldsymbol{X}$ ορισμένη στο $\mathbf{F}_4$ που δίνεται από την εξίσωση:

$$\boldsymbol{X}: X^2Y + aY^2Z + \bar{a}\,Z^2X = 0$$

Η $\boldsymbol{X}$ είναι μια μη-ιδιάζουσα καμπύλη αφού αν P = [x, y, z] ένα ιδιάζον σημείο της θα πρέπει: $\frac{\partial}{\partial X}\boldsymbol{X}\Big|_{P=(x,y,z)} = \frac{\partial}{\partial Y}\boldsymbol{X}\Big|_{P=(x,y,z)} = \frac{\partial}{\partial Z}\boldsymbol{X}\Big|_{P=(x,y,z)} = 0$ ή $2xy + \bar{a}\,z^2 = 2ayz + x^2 = 2\bar{a}\,z + ay^2 = 0$ ή $\bar{a}\,z^2 = x^2 = ay^2 = 0$ ή x = y = z = 0, το οποίο είναι άτοπο.

Επομένως, η $\boldsymbol{X}$ έχει γένος 1 και το φράγμα του Serre μας δίνει ότι $N_q(\boldsymbol{X}) \leq (4 + 1) + 1\,[2\sqrt{4}\,] = 9$. Δηλαδή ότι η καμπύλη έχει το πολύ 9 ρητά σημεία.

Όπως φαίνεται στον παρακάτω πίνακα η καμπύλη έχει ακριβώς 9 ρητά σημεία:

	P_1	P_2	P_3	P_4	P_5	P_6	Q_1	Q_2	Q_3
x	1	0	0	1	1	1	a	1	1
y	0	1	0	a	$\bar{a}$	1	1	a	1
z	0	0	1	$\bar{a}$	a	1	1	1	a

Έστω $D = P_1 + P_2 + \ldots + P_6$ και $G = 2Q_1 + Q_2$.

Ο βαθμός του διαιρέτη G είναι $\deg(G) = 2 + 1 > 2g - 2 = 2 \cdot 1 - 2 = 0$. Επομένως, είναι άμεση συνέπεια του θεωρήματος Riemann – Roch (δες [Ho], θεώρημα 2.55, σελίδα 890) ότι

$$l(G) := \dim L(G) = \deg(G) - g + 1 = 3 - 1 + 1 = 3$$

Ισχυριζόμαστε ότι οι ρητές συναρτήσεις

$$f_1(X,Y,Z) := \frac{X}{X + Y + \bar{a}Z},$$
$$f_2(X,Y,Z) := \frac{Y}{X + Y + \bar{a}Z},$$
$$f_3(X,Y,Z) := \frac{\bar{a}Z}{X + Y + \bar{a}Z}$$

είναι μια βάση του χώρου L(G).

Σύμφωνα με την παρατήρηση 3.2.8, για να αποδείξουμε ότι οι $f_1(X,Y,Z), f_2(X,Y,Z), f_3(X,Y,Z) \in L(G)$ αρκεί να αποδείξουμε ότι στα σημεία Q_1 και Q_2 έχουν πόλους τάξης το πολύ 2 και 1 αντίστοιχα. Πράγματι, εύκολα διαπιστώνουμε ότι τα σημεία Q_1 και Q_2 είναι πόλοι των f_1, f_2, f_3. Αυτό διότι στα σημεία αυτά δεν μηδενίζεται ο αριθμητής ενώ μηδενίζεται ο παρονομαστής της κάθε μιας από τις f_1, f_2, f_3:

$$\left(X + Y + \bar{a}Z\right)\Big|_{Q_1=(a,1,1)} = a + 1 + \bar{a} = a^2 + a + 1 = 0$$
$$\left(X + Y + \bar{a}Z\right)\Big|_{Q_2=(1,a,1)} = 1 + + a + \bar{a} = a^2 + a + 1 = 0$$

Τα σημεία λοιπόν Q_1 και Q_2 είναι σημεία τομής της ευθείας $\varepsilon : X + Y + \bar{a}Z = 0$ με την κυβική καμπύλη $\boldsymbol{X}$. Πράγματι, η ε τέμνει την $\boldsymbol{X}$ στο Q_2 και η εφαπτόμενη της καμπύλης $\boldsymbol{X}$ είναι

$$\frac{\partial}{\partial X}\boldsymbol{X}\Big|_{Q_1=(a,1,1)} X + \frac{\partial}{\partial Y}\boldsymbol{X}\Big|_{Q_1=(a,1,1)} Y + \frac{\partial}{\partial Z}\boldsymbol{X}\Big|_{Q_1=(a,1,1)} Z = 0.$$

Οπότε, $a^2 X + a^2 Y + a Z = 0$ ή $a^3 X + a^3 Y + a^2 Z = 0$ ή $X + Y + \bar{a} Z = 0$

Λόγω του θεωρήματος του Bezout (θεώρημα 1.3.19) τα σημεία τομής της ευθείας ε και της καμπύλης $\boldsymbol{X}$ είναι 3 άρα η πολλαπλότητα τομής τους είναι ακριβώς 2 στο Q_1 και 1 στο Q_2.

Με βάση τα παραπάνω προκύπτει το συμπέρασμα ότι $f_1(X,Y,Z), f_2(X,Y,Z), f_3(X,Y,Z) \in L(G)$. Επειδή είναι και γραμμικά ανεξάρτητες αποτελούν μια βάση του χώρου L(G).

Συνεπώς από το θεώρημα 3.2.10 έχουμε ότι ο κώδικας C(D, G) μήκους 6 έχει ελάχιστη απόσταση $d \geq 6 - 3 = 3$. Η σχέση $\kappa \leq n - d + 1$ από το φράγμα του Singleton (θεώρημα 3.1.18) μας δίνει $3 \leq 6 - d + 1$ ή $d \leq 4$. Ο κώδικας είναι ισοδύναμος με τον λεγόμενο Hexacode, έχουν και οι δυο τον ίδιο γεννήτορα πίνακα. Κάνοντας χρήση μεθόδων της πεπερασμένης γεωμετρίας έχει αποδειχθεί ότι ο Hexacode έχει ελάχιστη απόσταση d = 4. Επομένως, και ο C(D, G) έχει ελάχιστη απόσταση d = 4 δηλαδή

ισχύει $\kappa = n - d + 4$, πράγμα που σημαίνει ότι ο $C(D, G)$ είναι ένας MDS κώδικας. (Για τον Hexacode δες [Pe]).

Βιβλιογραφία

[A1] Γ. Α. Αντωνιάδη, Αριθμητική Ελλειπτικών Καμπυλών, Έκδοση ΕΠΕΑΕΚ «Προμηθέας», Ηράκλειο 1999

[A2] Γ. Α. Αντωνιάδη, Εφαρμοσμένη Άλγεβρα, Έκδοση ΕΠΕΑΕΚ «Προμηθέας», Ηράκλειο 2000

[Ch1] J. S. Chahal, Manin's Proof of the Hasse Inequality Revisited, Nieuw Archief voor Wiskunde, pp. 219 – 232, Vierde serie Deel 13 No 2, juli 1995

[Ch2] J. S. Chahal, Topics in Number Theory, Plenum Press, New York 1988

[La] Κ. Λάκκη, Άλγεβρα, Θεσσαλονίκη 1993

[MS] F. J. MacWilliams, N. J. A. Sloane, The Theory of Error-Correcting Code, North-Holland Mathematical Library, Sixth printing: 1988

[Ho] Tom Hoholdt, J. H. van Lint, Ruud Pellikaan (authors), V. S. Pless, W. C. Huffman and R. A. Brualdi (editors), Handbook of Coding Theory, pp. 871-961, Elsevier Science, Amsterdam, 1998

[Le] Franz Lemmermeyer, Elliptishe Kurven I, διαθέσιμη στο διαδίκτυο στην διεύθυνση: http://www.rzuser.uni-heidelberg.de/~hb3/ellc.html

[LP] Rudolf Lidl - Gunter Pilz, Applied Abstract Algebra, Springer-Verlag 1998

[Pe] Mario De Boer, Rund Pellikaan, Gröbner bases for error-correcting codes and their decoding, Some tapas of computer algebra, Springer, Berlin 1999

[S1] Joseph H. Silverman, John Tate, Rational Points on Elliptic Curves, Springer-Verlag 1992

[S2] Joseph H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag 1986

[St] Henning Stichtenoth, Algebraic Function Field and Codes, Springer-Verlag 1993

[W] R. J. Walker, Algebraic Curves, Dover, New York 1962

Ευρετήριο