Το πρόβλημα του διακριτού λογάριθμου και ελλειπτικές καμπύλες

Εμμανουήλ Δουλγεράκης

Επιβλέπων Καθηγητής

Ιωάννης Α. Αντωνιάδης

Πτυχιακή εργασία

Τμήμα Μαθηματικών και Εφαρμοσμένων Μαθηματικών
Πανεπιστήμιο Κρήτης

Η παρούσα πτυχιακή εργασία παρουσιάστηκε στο Τμήμα Μαθηματικών και Εφαρμοσμένων Μαθηματικών την 30η Ιουνίου 2015. Την επιτροπή αξιολόγησης αποτέλεσαν οι Ιωάννης Α. Αντωνιάδης, Θεόδουλος Γαρεφαλάκης, Νικόλαος Γ. Τζανάκης.

Θα επιθυμούσα να ευχαριστήσω τους καθηγητές μου κ. Ι. Αντωνιάδη, Θ. Γαρεφαλάκη, Ν. Τζανάκη που συμμετείχαν στην εξεταστική επιτροπή. Ιδιαιτέρως ευχαριστώ τον κ. Αντωνιάδη υπό την επίβλεψη και την καθοδήγηση του οποίου εκπονήθηκε αυτή η εργασία.

Στους γονείς μου !

Περιεχόμενα

Εισαγωγή

Ο στόχος της παρούσης πτυχιακής εργασίας είναι αρχικά, η ανάπτυξη μιας θεωρίας πάνω στις ελλειπτικές καμπύλες, την οποία στη συνέχεια θα προσπαθήσουμε να χρησιμοποιήσουμε για να επιτεθούμε στο πρόβλημα του διακριτού λογάριθμου. Το πρόβλημα του διακριτού λογάριθμου παίζει σημαντικό ρόλο στη σύχρονη κρυπτογραφία. Ευρείας χρήσεως κρυπτοσυστήματα όπως το El Gamal, αλλά και πρωτόκολλα όπως για παράδειγμα το πρωτόκολλο ανταλλαγής κλειδιών Diffie-Hellman στηρίζουν την ασφάλεια τους στην δυσκολία του προβλήματος του διακριτού λογάριθμου. Όπως θα δούμε παρακάτω το πρόβλημα του διακριτού λογάριθμου μπορεί να αναφέρεται σε διάφορες ομάδες.

Το πρώτο κεφάλαιο ασχολείται με το πρόβλημα του διακριτού λογάριθμου στην πολλαπλασιαστική ομάδα ενός πεπερασμένου σώματος. Γίνεται μια μικρή εισαγωγή στις ιδέες που κρύβονται πίσω από τον index calculus, έναν αλγόριθμο ο οποίος αντιμετωπίζει το πρόβλημα σε αυτή τη κατηγορία ομάδων. Μια άλλη κλάση ομάδων στην οποία μπορεί να αναφέρεται το πρόβλημα του διακριτού λογάριθμου είναι η ομάδα των ρητών σημείων μιας ελλειπτικής καμπύλης.

Συνεπώς στο δεύτερο κεφάλαιο αναπτύσεται μια βασική θεώρια ελλειπτικών καμπυλών που θα χρειαστούμε για να εξετάσουμε το πρόβλημα. Αρχικά ορίζουμε βασικές έννοιες ελλειπτικών καμπυλών και στην συνέχεια ξεκινάμε να χτίζουμε τη θεωρία μας. Το πρώτο θέμα με το οποίο θα ασχοληθούμε είναι οι ενδομορφισμοί ελλειπτικών καμπυλών, με απώτερο σκοπό να κατανοήσουμε καλύτερα τον ενδομορφισμό που δίνεται από τον πολλαπλασιασμό με $n \in \mathbb{Z}$ κάθε σημείου της ελλειπτικής μας καμπύλης. Ακολουθεί μια αναφορά στις ιδιάζουσες καμπύλες και ύστερα μελετάμε δυο πολύ σημαντικές έννοιες, τα ρητά σημεία πεπερασμένης τάξης (torsion points) και τα πολυώνυμα διαίρεσης (division polynomials).

Εφοδιασμένοι με αυτά τα εργαλεία στη συνέχεια εισάγουμε τις διγραμμικές συζεύξεις (pairing) Weil και Tate-Lichtenbaum. Αυτές είναι δύο απεικονίσεις που θα χρησιμοποιήσουμε αρκετά στο κεφάλαιο 3. Συγκεκριμένα αυτές οι δύο απεικονίσεις αντιστοιχούν σημεία ελλειπτικών καμπυλών σε $n-$ρίζες της μονάδας. Αυτό το γεγονός θα εκμεταλλευτούμε για να δείξουμε πως μπορούμε να ανάγουμε το πρόβλημα του διακριτού λογάριθμου από την ομάδα των ρητών σημείων μιας ελλειπτικής καμπύλης, σε αυτό μιας πολλαπλασιαστικής ομάδας ενός πεπερασμένου σώματος. Στο κεφάλαιο 3 λοιπόν θα περιγράψουμε δύο διαφορετικούς αλγόριθμους που μπορούν να το κάνουν αυτό, την επίθεση MOV και την επίθεση Frey-Ruck. Βασικό βοηθητικό σύγγραμμα για την μελέτη όλων των θεμάτων σχετικά με τις ελλειπτικές καμπύλες ήταν το [2].

Τέλος στο τέταρτο κεφάλαιο της εργασίας θα ασχοληθούμε με τον αλγόριθμο παραγοντοποίησης p-1 του Pollard. Κατά την επεξεργασία του θέματος χρησιμοποιήθηκε κυρίως το [1]. Εκεί θα παρουσιάσουμε έναν τρόπο τον οποίο βρήκαμε ώστε να μπορούμε να αντιμετωπίσουμε κάποιες περιπτώσεις στις οποίες ο κλασικός αλγόριθμος αποτυγχάνει.

Κεφάλαιο 1

Ο Διακριτός Λογάριθμος

Έστω p πρώτος και a, b ακέραιοι που δεν διαιρούνται με το p. Ας υποθέσουμε ότι ξέρουμε ότι υπάρχει ένας ακέραιος k τ.ω. $a^k \equiv b \pmod{p}$. Το κλασικό πρόβλημα του διακριτού λογάριθμου είναι να βρούμε το k. Από τη στιγμή που και το $k + (p-1)$ είναι επίσης λύση, το k μπορούμε να θεωρήσουμε ότι ορίζεται $(mod\ (p-1))$ ή mod ένα διαιρέτη d του $p-1$ αν $a^d \equiv 1 \pmod{p}$. Πιο γενικά, έστω G μια ομάδα και έστω $a, b \in G$. Υποθέτουμε οτι ξέρουμε οτι υπάρχει $k \in \mathbb{Z}$ τέτοιο ώστε $a^k = b$. Και σ' αυτή τη περίπτωση το πρόβλημα του διακριτού λογάριθμου είναι να βρούμε το k. Για παράδειγμα, G θα μπορούσε να είναι η πολλαπλασιαστική ομάδα ${\mathbb{F}_q}^*$ ενός πεπερασμένου σώματος. Επίσης η G θα μπορούσε να είναι και η $E(\mathbb{F}_q)$ για κάποια ελλειπτική καμπύλη. Σ' αυτή τη περίπτωση τα a και b είναι σημεία πάνω στην E και προσπαθούμε να βρούμε έναν ακέραιο k τ.ω. $ka = b$. Η ασφάλεια πολλών κρυπτοσυστημάτων βασίζεται στη δυσκολία του προβλήματος του διακριτού λογάριθμου.

Μια μέθοδος για να επιτεθούμε στο πρόβλημα είναι με "ωμή βία". Δοκιμάζουμε όλες τις δυνατές τιμές του k μέχρι κάποια να δουλέψει. Αυτό όμως δεν είναι πρακτικό όταν το k είναι ένας πολύ μεγάλος ακέραιος, για παράδειγμα με μερικές εκατοντάδες ψηφία. Άρα χρειαζόμαστε καλύτερες τεχνικές για να επιτεθούμε στο πρόβλημα. Μια τέτοια τεχνική είναι αυτή του index calculus η οποία μπορεί να χρησιμοποιηθεί στο ${\mathbb{F}_p}^*$ και πιο γενικά στην πολλαπλασιαστική ομάδα ενός πεπερασμένου σώματος. Ωστόσο δεν εφαρμόζεται σε τυχαίες ομάδες. Υπάρχουν κι άλλες μέθοδοι, πιο γενικές, όπως η Pohlig-Hellman, Baby step-Giant step, Pollard ρ και λ. Αυτές μπορούν να εφαρμοστούν και για την ομάδα των ρητών σημείων μιας ελλειπτικής καμπύλης. Τελικά θα δείξουμε οτι για κάποιες ειδικές κλάσεις ελλειπτικών καμπυλών, μπορούμε να ανάγουμε το πρόβλημα του διακριτού λογάριθμου από την ομάδα $E(\mathbb{F}_q)$ σε αυτό

της $\mathbb{F}_q{}^*$.

1.1 Index Caclulus

Έστω p πρώτος και g μια πρωταρχική ρίζα $(mod\ p)$ το οποίο σημαίνει οτι το g είναι γεννήτορας της κυκλικής ομάδας $\mathbb{F}_p{}^*$. Οπότε κάθε $h \not\equiv 0 \pmod p$ μπορεί να γραφεί ως $h \equiv g^k \pmod p$ για κάποιο ακέραιο k ο οποίος είναι μοναδικά καθορισμένος $(mod\ (p-1))$. Έστω $k = L(h)$ ο διακριτός λογάριθμος του h ως προς $g\,(mod\ p)$ άρα $g^{L(h)} \equiv h \pmod p$. Έστω $h_1,\ h_2 \in \mathbb{F}_p{}^*$ τότε $g^{L(h_1h_2)} \equiv h_1h_2 \equiv g^{L(h_1)+L(h_2)} \pmod p$. Επομένως $L(h_1h_2) \equiv L(h_1) + L(h_2) \pmod{(p-1)}$

Ο index calculus είναι μια μέθοδος υπολογισμού τιμών της λογαριθμικής συνάρτησης L. Η ιδέα είναι να υπολογίσουμε το $L(l)$ για αρκετούς μικρούς πρώτους l και μετά να χρησιμοποιήσουμε αυτές τις πληροφορίες για να υπολογίσουμε το $L(h)$ για τυχαίο h. Το σύνολο των "μικρών" πρώτων που θα επιλέξουμε καλείται βάση παραγοντοποίησης.

Αρχικά θα υπολογίζουμε δυνάμεις του $g\,(mod\ p)$ και αν το αποτέλεσμα παραγοντοποιείται από τους πρώτους της βάσης μας θα κρατάμε την σχέση. Όταν θα έχουμε αρκετές σχέσεις θα είμαστε σε θέση να λύσουμε ένα σύστημα το οποίο θα μας επιτρέψει να υπολογίσουμε την τιμή της συνάρτησης L για όλους τους πρώτους της βάσης παραγοντοποίησης που έχουμε επιλέξει. Στη συνέχεια αν θέλουμε να λύσουμε το πρόβλημα $a^k \equiv b \pmod p$ τότε θα υπολογίζουμε την τιμή $bg^i\,(mod\ p)$ για αρκετές τιμές του i μέχρις ότου το αποτέλεσμα να παραγοντοποιείται από την βάση που έχουμε επιλέξει. Τότε χρησιμοποιώντας τα αποτελέσματα που έχουμε καταγράψει από το προηγούμενο βήμα θα βρούμε το k. Με ένα παράδειγμα θα γίνει πιο κατανοητή η μέθοδος.

Παράδειγμα : Έστω $p = 1223$ και $g = 5$ και θέλουμε να λύσουμε το πρόβλημα $5^k \equiv 329 \pmod p$.

Επιλέγουμε την βάση παραγοντοποίησης μας να είναι $B = \{2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17\}$.

Μετά από μερικές δοκιμές καταλήγουμε στις παρακάτω σχέσεις:

$$5^9 \equiv -2 \cdot 3 \pmod{1223} \tag{1.1}$$
$$5^{13} \equiv -3^4 \pmod{1223} \tag{1.2}$$
$$5^{28} \equiv 11 \cdot 13 \pmod{1223} \tag{1.3}$$
$$5^{54} \equiv 2 \cdot 7 \cdot 13 \pmod{1223} \tag{1.4}$$
$$5^{58} \equiv 11 \pmod{1223} \tag{1.5}$$
$$5^{66} \equiv 2^2 \cdot 7 \cdot 17 \pmod{1223} \tag{1.6}$$

Αυτές οι εξισώσεις μπορούν να μετατραπούν σε εξισώσεις για διακριτούς λογάριθμους. Αυτό θα μας οδηγήσει σε ένα γραμμικό σύστημα με άγνωστους τις τιμές της συνάρτησης L για τους πρώτους της βάσης παραγοντοποίησης που έχουμε επιλέξει. Οπότε γνωρίζοντας οτι $5^{611} \equiv -1 \pmod{1223}$ μπορούμε να καταλήξουμε στο παρακάτω σύστημα.

$$\begin{aligned}
611 + L(2) + L(3) &\equiv 9 \pmod{1222} \\
611 + 4L(3) &\equiv 13 \pmod{1222} \\
L(11) + L(13) &\equiv 28 \pmod{1222} \\
L(2) + L(7) + L(13) &\equiv 54 \pmod{1222} \\
L(11) &\equiv 58 \pmod{1222} \\
2L(2) + L(7) + L(17) &\equiv 66 \pmod{1222}
\end{aligned}$$

Από την πέμπτη εξίσωση έχουμε κατευθείαν ότι $L(11) = 58$. Αντικαθιστώντας στην τρίτη εξίσωση τώρα πάιρνουμε ότι $L(13) = 1192$. Η δεύτερη εξίσωση μας δείνει οτι $L(3) = 156$ ή $L(3) = 767$ όμως,

$$5^{767} \equiv 1220 \pmod{1223} \quad \text{και} \quad 5^{156} \equiv 3 \pmod{1223}$$

οπότε $L(3) = 156$. Από την πρώτη εξίσωση συμπεραίνουμε ότι $L(2) = 464$ και από την τέταρτη οτι $L(7) = 842$ αντίστοιχα. Τέλος από την έκτη εξίσωση συμπεραίνουμε οτι $L(17) = 740$ και προφανώς έχουμε ότι $L(5) = 1$. Οπότε εφόσον έχουμε την τιμή της συνάρτησης L για όλους τους πρώτους της βάσης παραγοντοποίησης μπορούμε να προχωρήσουμε στο επόμενο βήμα. Τώρα δοκιμάζουμε τιμές για το i μέχρις ότου το $329 \cdot 5^i \pmod{1223}$ να παραγοντοποιείται από τους πρώτους της βάσης παραγοντοποίησης που έχουμε επιλέξει. Μετά από μερικές δοκιμές βρίσκουμε ότι

$$329 \cdot 5^{37} \equiv 3 \cdot 7 \cdot 11 \pmod{1223}$$

Αυτό μας οδηγεί στην παρακάτω σχέση,

$$L(329) + 37 \equiv L(3) + L(7) + L(11) \pmod{1222}$$

Άρα $L(329) \equiv 156 + 842 + 58 - 37 \pmod{1222} \Rightarrow L(329) = 1019$.

Η μέθοδος του index calculus όπως είδαμε μπορεί να εφαρμοστεί στην ${\mathbb{F}_p}^*$ αλλά μπορούμε να την γενικεύσουμε και για την πολλαπλασιαστική ομάδα ${\mathbb{F}_q}^*$ οποιουδήποτε πεπερασμένου σώματος.

Κεφάλαιο 2

Ελλειπτικές Καμπύλες

2.1 Βασικές ΄Εννοιες

΄Εστω ένα σώμα K, ορίζουμε την εξής σχέση για τα στοιχεία $(x_1,\, y_1,\, z_1)$, $(x_2,\, y_2,\, z_2)$ του K^3 εξαιρώντας το $(0,\, 0,\, 0)$. $(x_1,\, y_1,\, z_1) \sim (x_2,\, y_2,\, z_2)$ αν υπάρχει $a \in K^*$ τ.ω. $x_2 = ax_1,\ y_2 = ay_1,\ z_2 = az_1,$. Αποδεικνύεται ότι αυτή είναι μια σχέση ισοδυναμίας. Την κλάση ισοδυναμίας ενός σημείου $(x,\, y,\, z)$ την συμβολίζουμε με $[x,\, y,\, z]$.

Ορισμός. *Το προβολικό επίπεδο $\mathbb{P}^2(K)$ ορίζεται να είναι το συνόλο των κλάσεων ισοδυναμίας που έπεται από την παραπάνω σχέση.*

Τα πεπερασμένα σημεία του $\mathbb{P}^2(K)$ είναι αυτά για τα οποία $z \neq 0$ και αντιστοιχούν αμφιμονοσήμαντα στα σημεία του αφινικού επιπέδου $\mathbb{A}^2(K)$ δηλαδή $[x,\, y,\, z] \leftrightarrow (x,\, y)$. Τα επ' άπειρο σημεία του προβολικού επιπέδου $\mathbb{P}^2(K)$ αντιστοιχούν στην τιμή $z = 0$.

Ορισμός. *΄Εστω C ανάγωγη (δεν αναλύεται σε γινόμενο πολυωνύμων μικρότερου βαθμού) κυβική καμπύλη. ΄Ενα σημείο P θα λέγεται ιδιάζον όταν κάθε ευθεία που διέρχεται από το P τέμνει την C σε ακριβώς ένα ακόμη σημείο. Αν η καμπύλη μας δεν έχει κανένα τέτοιο σημείο τότε λέγεται μη-ιδιάζουσα.*

Θεωρούμε μια μη-ιδιάζουσα προβολική κυβική καμπύλη $C|_K$. Το επ' άπειρο σημείο της καμπύλης θεωρείται, πάντοτε, K-ρητό σημείο της καμπύλης. Η καμπύλη μπορεί να παρασταθεί από την γενικευμένη εξίσωση Weierstrass $Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$ όπου $a_1,\, a_2,\, a_3,\, a_4,\, a_6 \in K$. Η καμπύλη έχει ένα επ' άπειρο σημείο, αφού για $z = 0$ έπεται $x^3 = 0$ δηλαδή $x = 0$ και συνεπώς το σημείο αυτό είναι το $[0,\, 1,\, 0]$.

Παρατήρηση : Αν η $chK \neq 2$, τότε η καμπύλη μπορεί να παρασταθεί από μια εξίσωση της μορφής $Y^2Z = X^3 + b_2X^2Z + b_3XZ^2 + b_4Z^3$ με $b_2,\, b_3,\, b_4 \in K$.
Αν τώρα $chK \neq 2, 3$ τότε η καμπύλη μπορεί να παρασταθεί από μια εξίσωση της μορφής $Y^2Z = X^3 + aXZ^2 + bZ^3$ με $a,\, b \in K$ η οποία λέγεται εξίσωση του Weierstrass.

Από εδώ και πέρα θα γράφουμε την εξίσωση της καμπύλης μας αφινικά δηλαδή στην τελευταία περίπτωση θα έχουμε μια εξίσωση της μορφής $Y^2 = X^3 + aX + b$. Εδώ τώρα το γεγονός ότι η καμπύλη είναι μηιδιάζουσα είναι ισοδύναμο με το να είναι η διακρίνουσα του X^3+aX+b διάφορη του μηδενός, δηλαδή $\Delta = 4a^3 + 27b^2 \neq 0$.

Για κάθε επέκταση L/K ορίζεται το σύνολο

$$E(L) = \{(x, y) \in L \times L : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}$$

,
όπου $\mathcal{O}$ το επ' άπειρο σημείο. Αυτό το σύνολο μπορούμε να το εφοδιάσουμε με μια πράξη πρόσθεσης με ουδέτερο στοιχείο το επ' άπειρο στοιχείο $\mathcal{O} = [0,\, 1,\, 0]$.

Έστω $P_1,\, P_2 \in E(K)$ με $P_1 = (x_1, y_1)$ και $P_2 = (x_2, y_2)$ τότε ορίζεται το σημείο $R = P_1 + P_2 \in E(K)$. Διακρίνουμε περιπτώσεις:

Αν $P_1 = \mathcal{O}$ τότε $R = P_2$ ή αν $P_2 = \mathcal{O}$ τότε $R = P_1$.
Αλλιώς αν $x_1 = x_2$ και $y_1 = -y_2$ τότε $R = \mathcal{O}$.
Διαφορετικά θέτουμε

$$\lambda = \begin{cases} \frac{3{x_1}^2 + a}{2y_1} & \text{αν } P_1 = P_2 \\ \frac{y_1 - y_2}{x_1 - x_2} & \text{αλλιώς} \end{cases}$$

Τότε $R = (\lambda^2 - x_1 - x_2, -\lambda x_3 - \nu)$ όπου $\nu = y_1 - \lambda x_1$ και $x_3 = \lambda^2 - x_1 - x_2$.

Πρόταση 2.1.1. *Η παραπάνω πράξη εφοδιάζει το σύνολο $E(K)$ με δομή αβελιανής ομάδας με ουδέτερο το στοιχείο $\mathcal{O}$.*

Γεωμετρική ερμηνεία: Η πράξη η οποία ορίσαμε πάνω στο σύνολο $E(K)$ μπορεί να ερμηνευθεί και γεωμετρικά. Έστω λοιπόν $P_1 = (x_1, y_1)$

και $P_2 = (x_2, y_2)$ δυο διαφορετικά σημεία της ελλειπτικής καμπύλης η οποία ορίζεται από την εξίσωση $y^2 = x^3 + ax + b$ και θεωρούμε ότι $x_1 \neq x_2$. Έστω L η ευθεία που διέρχεται από τα P_1 και P_2. Τότε η L τέμνει την E σε ακριβώς ένα ακόμα σημείο, το $R = (x_3, y_3)$, τότε το $Q = (x_3, -y_3)$ είναι το άθροισμα των δύο σημείων P_1 και P_2. Συμβολίκα γράφουμε $Q = P_1 \oplus P_2$. Αν $P_1 = P_2$ τότε θεωρούμε την εφαπτομένη που περνάει από αυτο το σημείο και κοιτάμε πάλι ποιό είναι το τρίτο σημείο τομής με την E.

Θεώρημα Mordell. *Έστω E μια ελλειπτική καμπύλη ορισμένη υπέρ το $\mathbb{Q}$. Τότε η $E(\mathbb{Q})$ είναι μια πεπερασμένα παραγόμενη αβελιανή ομάδα.*

Μια απόδειξη του θεωρήματος δίνεται στο [3].

Ορισμός. *Το σύνολο των σημείων της E(K) που έχουν πεπερασμένη τάξη το συμβολίζουμε $E(K)_{tor}$.*

Παρατήρηση : Για το $E(K)_{tor}$ ισχύει ότι είναι υποομάδα της E(K).

2.2 Ενδομορφισμοί Ελλειπτικών Καμπυλών

Θεωρούμε μια ελλειπτική καμπύλη $E\mid_K$ και $\overline{K}$ μια αλγεβρική θήκη του K τότε $E(\overline{K}) := \{P = (x,\, y) \in \overline{K} \times \overline{K} \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$

Ορισμός. *Ενδομορφισμός της E είναι μια απεικόνιση $a : E(\overline{K}) \to E(\overline{K})$ η οποία είναι ομομορφισμός ομάδων και δίνεται μέσω ρητών συναρτήσεων.*

Δηλαδή έχουμε $a(P_1 \oplus P_2) = a(P_1) \oplus a(P_2)$ και αν $P = (x,\, y)$ τότε $a(x, y) = (R_1(x,\, y),\, R_2(x,\, y))$ όπου $R_i(x,\, y) = \dfrac{F_i(x,\, y)}{G_i(x,\, y)}$ για $i = 1,\, 2$ με τα $F_i(x,\, y)$ και $G_i(x,\, y)$ να ανήκουν στο $\overline{K}[X,\, Y]$. Προφανώς αφού a ομομορφισμός $a(\mathcal{O}) = \mathcal{O}$. Υποθέτουμε ότι a όχι τετριμμένος, δηλαδή $\exists\, P = (x,\, y) \in E(\overline{K})$ τ.ω. $a(P) = a(x,\, y) \neq \mathcal{O}$.

Παράδειγμα : Έστω E η ελλειπτική καμπύλη που ορίζεται από την εξίσωση $y^2 = x^3 + Ax + B$ και έστω επίσης μια απεικόνιση
$a : E(\overline{K}) \to E(\overline{K})$ τ.ω. $a(P) = 2P$. Έχουμε $a(x, y) = (R_1(x,\, y),\, R_2(x,\, y))$

όπου

$$\begin{aligned} R_1(x,\, y) &= \left(\frac{3x^2+A}{2y}\right)^2 - 2x \\ R_2(x,\, y) &= -\left(\frac{3x^2+A}{2y}\right) R_1(x,\, y) - y + \left(\frac{3x^2+A}{2y}\right) x \\ &= \left(\frac{3x^2+A}{2y}\right)\left(3x - \left(\frac{3x^2+A}{2y}\right)^2\right) - y \end{aligned}$$

Επίσης,
$a(P) = 2P$
$a(Q) = 2Q$, οπότε και
$a(P \oplus Q) = 2(P \oplus Q) = 2P \oplus 2Q = a(P) \oplus a(Q)$

'Εστω $y^2 = x^3 + Ax + B$,$\Delta \neq 0$. $\forall\, (x,\, y) \in E(\overline{K})$ μπορούμε να αντικαταστήσουμε κάθε άρτια δύναμη του y από το x^3+Ax+B και κάθε περιττή δύναμη του y γίνεται y(πολυώνυμο του x). Συνεπώς,

$$\begin{aligned} R(x,\, y) &= \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y} \\ &= \frac{[p_1(x) + p_2(x)y][p_3(x) - p_4(x)y]}{[p_3(x) + p_4(x)y][p_3(x) - p_4(x)y]} \\ &= \frac{q_1(x) + q_2(x)y}{q_3(x)} \end{aligned}$$

Θεωρούμε ένα ενδομορφισμό με $a(x, y) = (R_1(x,\, y),\, R_2(x,\, y))$ και

$$R_1(x,\, y) = \frac{q_1(x) + q_2(x)y}{q_3(x)}\ ,\ R_2(x,\, y) = \frac{q_4(x) + q_5(x)y}{q_6(x)}$$

Ο a είναι ομομορφισμός ομάδων άρα $a(x, -y) = a(-(x, y)) = -a(x, y)$. Επομένως

$$\begin{aligned} a(x, -y) &= (R_1(x,\, -y),\, R_2(x,\, -y)) \\ -a(x, y) &= -(R_1(x,\, y),\, R_2(x,\, y)) \\ &= (R_1(x,\, y),\, -R_2(x,\, y)) \end{aligned}$$

Οπότε παίρνουμε

$$\begin{aligned} R_1(x,\, -y) &= R_1(x,\, y) \\ R_2(x,\, -y) &= -R_2(x,\, y) \end{aligned}$$

Όμως $R_1(x,\,-y) = \dfrac{q_1(x) - q_2(x)y}{q_3(x)}$, $R_1(x,\,y) = \dfrac{q_1(x) + q_2(x)y}{q_3(x)} \Rightarrow$
$q_2(x)y = -q_2(x)y \quad \Rightarrow\ q_2(x) = 0$

Όμοια $R_2(x,\,-y) = -R_2(x,\,y) \Rightarrow \dfrac{q_4(x) + q_5(x)(-y)}{q_6(x)} = \dfrac{-q_4(x) - q_5(x)y}{q_6(x)} \Rightarrow$
$q_4(x) = 0$. Άρα καταλήγουμε στο συμπέρασμα ότι $a(x,\,y) = (r_1(x),\,r_2(x)y)$ όπου $r_1(x)$, $r_2(x)$ ρητές συναρτήσεις της μεταβλητής x με συντελεστές από το σώμα K.
Ερώτημα: Αν $r_1(x) = \dfrac{p(x)}{q(x)}$ με $(p(x)\,,\,q(x)) = 1$ τι γίνετε αν $q(x) = 0$?
Αν $q(x) = 0$ τότε ορίζουμε ότι $a(x,\,y) = \mathcal{O}$

Ορισμός. *Ο βαθμός* $\deg(a)$ *του ενδομορφισμού* a *με* $a(x,\,y) = (r_1(x),\,r_2(x)y)$ *ορίζεται να είναι* $\deg(a) = \max\{\deg p(x),\,\deg q(x)\}$ *όπου* $r_1(x) = \dfrac{p(x)}{q(x)}$ *αν ο* a *δεν είναι ο τετριμμένος. Αν* $a = 0$, *τότε* $\deg(0) = 0$.

Ορισμός. *Ο ενδομορφισμός* a, $a \neq 0$ *θα λέγεται διαχωρίσιμος (seperable) ενδομορφισμός* $\Leftrightarrow\ r_1'(x) \not\equiv 0$.

Παράδειγμα : Θεωρούμε τον ενδομορφισμό $a(P) = 2P$ μιας ελλειπτικής καμπύλης ορισμένης πάνω από ένα σώμα χαρακτηριστικής 0 και έχουμε,

$$\begin{aligned} R_1(x,\,y) &= \left(\frac{3x^2 + A}{2y}\right)^2 - 2x \\ R_1(x,\,y) &= \frac{9x^4 + 6Ax^2 + A^2 - 8x(x^3 + Ax + B)}{4(x^3 + Ax + B)} \\ &= \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)} \\ &= r_1(x) \end{aligned}$$

Άρα $\deg(a) = \max\{4,\,3\} = 4$. Άρα ο a είναι ένας ενδομορφισμός βαθμού 4. Για να είναι και διαχωρίσιμος πρέπει $r_1'(x) \not\equiv 0 \Leftrightarrow p'(x) \not\equiv 0$ ή $q'(x) \not\equiv 0$. Όμως $q'(x) = 4(x^3 + A)$ το οποίο δεν είναι το μηδενικό πολυώνυμο σε χαρακτηριστική 0 οπότε ο ενδομορφισμός είναι διαχωρίσιμος.

Θεωρούμε τον προηγούμενο ενδομορφισμό αλλά αυτή τη φορά για μια ελλειπτική καμπύλη σε χαρακτηριστική 2. Από τη θεωρία [2] γνωρίζουμε ότι αν δουλεύουμε σε σώμα χαρακτηριστικής 2 μπορούμε να

μετασχηματίσουμε την εξίσωση της καμπύλης μας σε μια από τις παρακάτω.

$$y^2 + xy = x^3 + a_2x^2 + a_6 \quad \text{ή}$$
$$y^2 + a_3y = x^3 + a_4x + a_6$$

Αρχικά θα θεωρήσουμε ότι η εξίσωση της καμπύλης έχει την μορφή $y^2 + xy = x^3 + a_2x^2 + a_6$. Έχουμε ότι $a(x,\, y) = (r_1(x),\, R_2(x,\, y))$ με $r_1(x) = \dfrac{x^4 + a_6}{x^2}$ οπότε $\deg(a) = \max\{4,\, 2\} = 4$.

$$p(x) = x^4 + a_6 \quad \Rightarrow\ p'(x) = 4x^3 = 0$$

$q'(x) = 2x = 0$ άρα $r_1'(x) = 0$ οπότε δεν είναι διαχωρίσιμος.

Παρατηρήσεις : Γενικά αν $chK = p$ τότε ο ενδομορφισμός
$a : E(\overline{K}) \to E(\overline{K})$ με $a(P) = pP$ είναι ενδομορφισμός βαθμού p^2 αλλά όχι διαχωρίσιμος.

Σημαντικό παράδειγμα είναι ο ενδομορφισμός του Frobenius. Υποθέτουμε $E\ |_{\mathbb{F}_q}$ και ορίζουμε ο ενδομορφισμός του Frobenius να είναι $\phi_q(x,\, y) = (x^q,\, y^q)$.

Λήμμα 2.2.1. *Έστω $E\ |_{\mathbb{F}_q}$ τότε ο ϕ_q είναι ενδομορφισμός της E με $\deg(\phi_q) = q$ αλλά ϕ_q δεν είναι διαχωρίσιμος.*

Απόδειξη. Προφανώς η $\phi_q(x,\, y)$ δίνεται μέσω ρητών συναρτήσεων (και μάλιστα πολυωνύμων) και $\deg(\phi_q) = q$. Θέλουμε να δείξουμε ότι η ϕ_q είναι ομομορφισμός ομάδων.
$\phi_q : E(\overline{\mathbb{F}_q}) \to E(\overline{\mathbb{F}_q})$. Έστω $P_1 = (x_1,\, y_1) \in E(\overline{\mathbb{F}_q})\ ,\ P_2 = (x_2,\, y_2) \in E(\overline{\mathbb{F}_q})$ Υποθέτουμε $P_1 \neq P_2$ και $x_1 \neq x_2$.
$P_3 = P_1 \oplus P_2 = (x_3,\, y_3)$ με $x_3 = \lambda^2 - x_1 - x_2\ ,\ y_3 = \lambda(x_1 - x_3) - y_1$ όπου $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$. Υψώνουμε στη q δύναμη άρα ${x_3}^q = (\lambda^2 - x_1 - x_2)^q = \lambda^{2q} - {x_1}^q - {x_2}^q = (\lambda^q)^2 - {x_1}^q - {x_2}^q = {m'}^2 - {x_1}^q - {x_2}^q$

$$\text{όπου } m' = \lambda^q = \Big(\frac{y_2 - y_1}{x_2 - x_1}\Big)^q = \frac{{y_2}^q - {y_1}^q}{{x_2}^q - {x_1}^q}$$

${y_3}^q = [\lambda(x_1 - x_3) - y_1]^q = \lambda^q({x_1}^q - {x_3}^q) - {y_1}^q = m'({x_1}^q - {x_3}^q) - {y_1}^q$

Επίσης

$$\phi_q(x_3,\, y_3) = ({x_3}^q\, {y_3}^q)$$
$$\phi_q(x_1,\, y_1) = ({x_1}^q,\, {y_1}^q)$$
$$\phi_q(x_2,\, y_2) = ({x_2}^q,\, {y_2}^q)$$

m' είναι η κλίση της ευθείας που περνάει από τα $({x_1}^q, {y_1}^q)$ και $({x_2}^q, {y_2}^q)$ οπότε $\phi_q(x_1, y_1) + \phi_q(x_2, y_2) = \phi_q(x_3, y_3)$
Αν $P_1 = P_2 = (x_1, y_1)$ τότε $P_3 = 2P_1 = (x_3, y_3)$ με $x_3 = \lambda^2 - 2x_1$, $y_3 = \lambda(x_1 - x_3) - y_1$ όπου $\lambda = \dfrac{3{x_1}^2 + A}{2y_1}$
Υψώνουμε στη q δύναμη:
${x_3}^q = \lambda^{2q} - 2^q {x_1}^q = (m')^2 - 2{x_1}^q$
${y_3}^q = [\lambda(x_1 - x_3) - y_1]^q = \lambda^q({x_1}^q - {x_3}^q) - {y_1}^q = m'({x_1}^q - {x_3}^q) - {y_1}^q$
όπου $m' = \dfrac{3^q {x_1}^{2q} + A^q}{2^q {y_1}^q} = \dfrac{3({x_1}^q)^2 + A}{2{y_1}^q}$
Άρα $\phi_q(2(x_1, y_1)) = \phi_q(x_1, y_1) + \phi_q(x_1, y_1)$
Τέλος $r_1'(x) = qx^{q-1} = 0$, άρα όχι διαχωρίσιμος. □

Πρόταση 2.2.1. *Έστω $\alpha \neq 0$ διαχωρίσιμος ενδομορφισμός της E. Τότε* $\deg(\alpha) = \#Ker(\alpha)$ *όπου $Ker(\alpha)$ ο πυρήνας του ομομορφισμού $\alpha : E(\overline{K}) \to E(\overline{K})$. Αν ο $\alpha \neq 0$ δεν είναι διαχωρίσιμος, τότε* $\deg(\alpha) > \#Ker(\alpha)$.

Απόδειξη. Έχουμε ότι $\alpha(x, y) = (r_1(x), r_2(x)y)$ όπου $r_1(x) = \dfrac{p(x)}{q(x)}$ και α διαχωρίσιμος $\Rightarrow r_1'(x) \not\equiv 0 \Rightarrow p'(x)q(x) - p(x)q'(x) \not\equiv 0$.
Έστω $S = \{x \in \overline{K} \mid (pq' - p'q)q(x) = 0\}$. Έστω $(a, b) \in E(\overline{K})$ τ.ω.
1) $a \neq 0$, $b \neq 0$, $(a, b) \neq \mathcal{O}$
2) $\deg(p(x) - aq(x)) = \max\{\deg(p), \deg(q)\} = \deg(\alpha)$
3) $a \notin r_1(S)$
4) $(a, b) \in \alpha(E(\overline{K}))$

Γιατί υπάρχει το (a, b); Εφόσον το $pq' - p'q$ δεν είναι το μηδενικό πολυώνυμο το S είναι πεπερασμένο οπότε και το $r_1(S)$ είναι πεπερασμένο. Η συνάρτηση $r_1(x)$ παίρνει άπειρο πλήθος τιμών καθώς το $x \in \overline{K}$ (αν όχι τότε για κάποιο $c \in \overline{K}$ θα υπήρχαν άπειρα $x \in \overline{K}$ τ.ω. $r_1(x) = c \;\Rightarrow \dfrac{p(x)}{q(x)} = c \;\Rightarrow\; p(x) - cq(x) = 0$ για άπειρα $x \in \overline{K} \;\Rightarrow\; p(x) - cq(x) \equiv 0 \;\Rightarrow\; p(x) \equiv cq(x) \;\Rightarrow\; p(x), q(x)$ έχουν κοινές ρίζες, άτοπο αφού $(p(x)\,, q(x)) = 1$)
Εφόσον για κάθε $x \in \overline{K}$ υπάρχει $(x, y) \in E(\overline{K})$ άρα το $\alpha(E(\overline{K}))$ είναι άπειρο (η $r_1(x)$ παίρνει άπειρες τιμές). Άρα υπάρχει ένα τέτοιο (a, b).
Θα αποδείξουμε ότι $\deg(a) = \#\{(x_1, y_1) \in E(\overline{K}) \mid \alpha(x_1, y_1) = (a, b)\}$ άρα $\dfrac{p(x_1)}{q(x_1)} = a$ και $y_1 r_2(x_1) = b$. Αφού $(a, b) \neq \mathcal{O} \Rightarrow q(x_1) \neq 0$ άρα το $r_2(x_1)$ ορίζεται. Εφόσον $b \neq 0 \Rightarrow y_1 = \dfrac{b}{r_2(x_1)}$. Οπότε αρκεί να μετρήσουμε τα x_1. Εξ' υποθέσεως το $p(x) - aq(x) = 0$ έχει $\deg(\alpha)$ ρίζες. Αρκεί να δείξουμε ότι δεν έχει ρίζες με πολλαπλότητα. Έστω ότι έχει μια, x_0 τότε

$p(x_0) - aq(x_0) = 0$ και $p'(x_0) - aq'(x_0) = 0 \Rightarrow$

$$p(x_0) = aq(x_0)$$
$$aq'(x_0) = p'(x_0)$$

Άρα $ap(x_0)q'(x_0) = ap'(x_0)q(x_0) \Rightarrow (pq' - p'q)(x_0) = 0$. Συνεπώς το x_0 είναι ρίζα του πολυωνύμου $(pq' - p'q)(x)$. Όμως $x_0 \in S \Rightarrow r_1(x_0) \in r_1(S) \Rightarrow$ $a = \dfrac{p(x_0)}{q(x_0)} \in r_1(S)$, άτοπο. Τελικά αφού υπάρχουν ακριβώς $\deg(\alpha)$ σημεία $(x_1,\, y_1)$ τ.ω. $\alpha(x_1,\, y_1) = (a,\, b)$ τότε $Ker(\alpha) = \deg(\alpha)$. □

Θεώρημα 2.2.1. *Έστω E μια ελλειπτική καμπύλη ορισμένη πάνω από ένα σώμα K. Έστω α, $\alpha \neq 0$ ένας ενδομορφισμός της E.*
Τότε $\alpha : E(\overline{K}) \to E(\overline{K})$ είναι επιμορφισμός.

Απόδειξη. Έστω $(a,\, b) \in E(\overline{K})$. Εφόσον $\alpha(\mathcal{O}) = \mathcal{O}$ υποθέτουμε ότι $(a,\, b) \neq \mathcal{O}$. Έστω $r_1(x) = \dfrac{p(x)}{q(x)}$
Περίπτωση 1) Αν το πολυώνυμο $p(x) - aq(x)$ δεν είναι σταθερό πολυώνυμο τότε έχει μια ρίζα x_0, δηλαδή $p(x_0) - aq(x_0) = 0$. Αν $q(x_0) = 0$, τότε $q(x_0) = 0$ και $p(x_0) - aq(x_0) = 0$ άρα $p(x_0) = 0$ οπότε τα p, q έχουν κοινή ρίζα, άτοπο $\Rightarrow q(x_0) \neq 0$. Επιλέγουμε το $y_0 \in \overline{K}$ να είναι μια από τις τετραγωνικές ρίζες του ${x_0}^3 + Ax_0 + B$. Τότε το $\alpha(x_0,\, y_0)$ ορίζεται και είναι ίσο με $(a,\, b')$ για κάποιο $b' \in \overline{K}$. Όμως ${b'}^2 = a^3 + Aa + B = b^2 \Rightarrow b' = \pm b$. Αν $b' = b$ τελειώσαμε, αν $b' = -b$ τότε $\alpha(x_0,\, -y_0) = (a,\, -b') = (a,\, b)$.
Περίπτωση 2) Έστω ότι το πολυώνυμο $p(x) - aq(x)$ είναι σταθερό πολυώνυμο. Εφόσον ο $Ker(\alpha)$ είναι πεπερασμένος από την πρόταση 2.2.1, μόνο πεπερασμένο το πλήθος σημεία αντιστοιχούν σε ένα σημείο. Άρα είτε $p(x)$ είτε $q(x)$ δεν είναι σταθερό, αφού $E(\overline{K})$ άπειρη. Αν p και q είναι δυο μη σταθερά πολυώνυμα τότε υπάρχει το πολύ ένα a τ.ω. $p(x) - aq(x)$ να είναι σταθερό διότι αν υπήρχαν δυο a, a' τ.ω. $p - aq = c_1$ και $p - a'q = c_2$ τότε $(p - aq) - (p - a'q) = (a' - a)q \Rightarrow c_1 - c_2 = (a' - a)q \Rightarrow q$ σταθερό.

Επίσης $a'(p - aq) - a(p - a'q) = (a' - a)p$ σταθερό $\Rightarrow p$ σταθερό. Άτοπο. Άρα υπάρχουν το πολύ 2 σημεία που δεν είναι στην εικόνα της α (αφού το a είναι 1 το πολύ) τα οποία θα είναι $(a,\, b)\,, (a,\, -b)$ για κάποιο b. Έστω $(a_1,\, b_1)$ ένα οποιοδήποτε άλλο σημείο τ.ω. $(a_1,\, b_1) + (a,\, b) \neq (a,\, \pm b)$ τότε $\exists P_1$ τ.ω. $\alpha(P_1) = (a_1,\, b_1)$ και P_2 τ.ω. $\alpha(P_2) = (a_1,\, b_1) + (a,\, b)$ τότε $\alpha(P_2 - P_1) = \alpha(P_2) - \alpha(P_1) = (a,\, b)$ και $\alpha(P_1 - P_2) = -(a,\, b) = (a,\, -b)$. Άρα η α είναι επί. □

Παρατήρηση : Ο ενδομορφισμός μας απεικονίζει σημεία από το $E(K)$ στο $E(K)$. Αν το σώμα K δεν είναι αλγεβρικά κλειστό τότε ο

ενδομορφισμός δεν είναι κατ' ανάγκη επί.

Τα επόμενα λήμματα θα μας βοηθήσουν στο να διατυπώσουμε μια πρόταση για το πότε ο πολλαπλασιασμός με n είναι διαχωρίσιμος.

Λήμμα 2.2.2. *Έστω E η ελλειπτική καμπύλη $y^2 = x^3 + Ax + B$. Θεωρούμε ένα σταθερό σημείο (u, v) πάνω στην E και θέτουμε $(x, y) + (u, v) = (f(x, y), g(x, y))$ όπου $f(x, y)$, $g(x, y)$ ρητές συναρτήσεις των x, y. Το y θεωρείται συνάρτηση του x με $\frac{dy}{dx} = \frac{3x^2 + A}{2y}$.*
Τότε

$$\frac{\frac{d}{dx}f(x, y)}{g(x, y)} = \frac{1}{y}$$

.

Απόδειξη. Από τους τύπους της πρόσθεσης σημείων έχουμε

$$f(x, y) = \left(\frac{y - v}{x - u}\right)^2 - x - u$$

$$g(x, y) = -\left(\frac{y - v}{x - u}\right)\left[\left(\frac{y - v}{x - u}\right)^2 - x - u\right] + \frac{y - v}{x - u}u - v =$$

$$= \frac{-(y - v)^3 + (x + u)(y - v)(x - u)^2 + u(y - v)(x - u)^2 - v(x - u)^3}{(x - u)^3} =$$

$$= \frac{-(y - v)^3 + x(y - v)(x - u)^2 + 2u(y - v)(x - u)^2 - v(x - u)^3}{(x - u)^3}$$

$$\frac{d}{dx}f(x, y) = \frac{2y'(y - v)(x - u)^2 - (y - v)^2 2(x - u)}{(x - u)^4} - 1 =$$

$$= \frac{2y'(y - v)(x - u) - 2(y - v)^2 - (x - u)^3}{(x - u)^3}$$

$$\begin{aligned}(x - u)^3\Big(y\frac{d}{dx}f(x, y) - g(x, y)\Big) &= 2yy'(y - v)(x - u) - 2y(y - v)^2 - y(x - u)^3 + \\ &\quad (y - v)^3 - x(y - v)(x - u)^2 - 2u(y - v)(x - u)^2 \\ &\quad + v(x - u)^3 \\ &= \dots \\ &= v(Au + u^3 - v^2 - Ax - x^3 + y^2) + \\ &\quad y(-Au - u^3 + v^2 + Ax + x^3 - y^2) \\ &= v(-B + B) + y(B - B) = 0\end{aligned}$$

εφόσον $v^2 = u^3 + Au + B$, $y^2 = x^3 + Ax + B$ άρα $(x-u)^3(y\frac{d}{dx}f(x,\,y) - g(x,\,y)) = 0 \;\Rightarrow\; y\frac{d}{dx}f(x,\,y) - g(x,\,y) = 0 \;\Rightarrow$

$$\frac{\frac{d}{dx}f(x,\,y)}{g(x,\,y)} = \frac{1}{y}$$

□

Λήμμα 2.2.3. *Έστω $\alpha_1,\,\alpha_2,\,\alpha_3$ μη μηδενικοί ομομορφισμοί μιας ελλειπτικής καμπύλης E με $\alpha_1+\alpha_2=\alpha_3$ και $\alpha_j(x,\,y) = \big(R_{\alpha_j}(x),\,yS_{\alpha_j}(x)\big)$. Υποθέτουμε ότι υπάρχουν σταθερές $C_{\alpha_1},\,C_{\alpha_2}$ τ.ω. $\frac{R'_{\alpha_1}(x)}{S_{\alpha_1}(x)} = C_{\alpha_1}$, $\frac{R'_{\alpha_2}(x)}{S_{\alpha_2}(x)} = C_{\alpha_2}$ τότε $\frac{R'_{\alpha_3}(x)}{S_{\alpha_3}(x)} = C_{\alpha_1} + C_{\alpha_2}$.*

Απόδειξη. Έστω $(x_1,\,y_1)$ και $(x_2,\,y_2)$ δύο σημεία της E και $(x_3,\,y_3) = (x_1,\,y_1)+(x_2,\,y_2)$ όπου $\alpha_1(x,\,y) = (x_1,\,y_1)$ και $\alpha_2(x,\,y) = (x_2,\,y_2)$. Τα $x_3,\,y_3$ προκύπτουν ως ρητές συναρτήσεις των $x_1,\,y_1,\,x_2,\,y_2$. Από το προηγούμενο λήμμα,

$$\frac{\frac{dx_3}{dx_1}}{y_3} = \frac{1}{y_1} \;\Rightarrow\; \frac{dx_3}{dx_1} = \frac{y_3}{y_1} \;\Rightarrow\; \frac{\vartheta x_3}{\vartheta x_1} + \frac{\vartheta x_3}{\vartheta y_1}\frac{\vartheta y_1}{\vartheta x_1} = \frac{y_3}{y_1}$$

$$\frac{\frac{dx_3}{dx_2}}{y_3} = \frac{1}{y_2} \;\Rightarrow\; \frac{dx_3}{dx_2} = \frac{y_3}{y_2} \;\Rightarrow\; \frac{\vartheta x_3}{\vartheta x_2} + \frac{\vartheta x_3}{\vartheta y_2}\frac{\vartheta y_2}{\vartheta x_2} = \frac{y_3}{y_2}$$

$\frac{dR_{\alpha_j}(x)}{dx} = C_{\alpha_j}S_{\alpha_j}(x) = C_{\alpha_j}\frac{y_j}{y}$ αφού $yS_{\alpha_j}(x) = y_j$ άρα $\frac{dx_j}{dx} = C_{\alpha_j}\frac{y_j}{y}$

$$\begin{aligned}\frac{dx_3}{dx} &= \frac{\vartheta x_3}{\vartheta x_1}\frac{dx_1}{dx} + \frac{\vartheta x_3}{\vartheta y_1}\frac{dy_1}{dx_1}\frac{dx_1}{dx} + \frac{\vartheta x_3}{\vartheta x_2}\frac{dx_2}{dx} + \frac{\vartheta x_3}{\vartheta y_2}\frac{y_2}{x_2}\frac{dx_2}{dx}\\ &= \left(\frac{\vartheta x_3}{\vartheta x_1} + \frac{\vartheta x_3}{\vartheta y_1}\frac{dy_1}{dx_1}\right)\frac{dx_1}{dx} + \left(\frac{\vartheta x_3}{\vartheta x_2} + \frac{\vartheta x_3}{\vartheta y_2}\frac{dy_2}{dx_2}\right)\frac{dx_2}{dx}\\ &= \frac{y_3}{y_1}\frac{y_1}{y}C_{\alpha_1} + \frac{y_3}{y_2}\frac{y_2}{y}C_{\alpha_2} = \big(C_{\alpha_1}+C_{\alpha_2}\big)\frac{y_3}{y}\end{aligned}$$

$yS_{\alpha_3}(x) = y_3 \;\Rightarrow\; \frac{y_3}{y} = S_{\alpha_3}(x)$ άρα

$\frac{dx_3}{dx} = S_{\alpha_3}(x)\big(C_{\alpha_1}+C_{\alpha_2}\big) \overset{x_3=R_{\alpha_3}(x)}{\Longrightarrow} \frac{R'_{\alpha_3}(x)}{S_{\alpha_3}(x)} = C_{\alpha_1}+C_{\alpha_2}$ □

Πρόταση 2.2.2. *Έστω E μια ελλειπτική καμπύλη ορισμένη πάνω από ένα σώμα K και n ένας μη μηδενικός ακέραιος. Υποθέτουμε ότι ο πολλαπλασιασμός με n πάνω στην E δίνεται με,*
$n(x, y) = (R_n(x), yS_n(x)) \; \forall \; (x, y) \in E(\overline{K})$ *όπου R_n, S_n ρητές συναρτήσεις. Τότε $\frac{R'_n(x)}{S_n(x)} = n$, οπότε ο πολλαπλασιασμός με n είναι διαχωρίσιμος ανν $p \nmid n$ όπου $p = chK$.*

Απόδειξη. Εφόσον $R_{-n}(x) = R_n(x)$ και $S_{-n}(x) = -S_n(x)$ έχουμε ότι $\frac{R'_{-n}(x)}{S_{-n}(x)} = \frac{-R'_n(x)}{S_n(x)}$ οπότε αρκεί να αποδείξουμε για n θετικά.
Επαγωγικά:
Για $k = 1$: Προφανώς ισχύει $R_k(x) = x$, $S_k(x) = 1$, $\frac{R'_k(x)}{S_k(x)} = 1$
Υποθέτουμε ότι ισχύει για $k = n$ και θα αποδείξουμε για $n + 1$. Αν $\frac{R'_n(x)}{S_n(x)} = n$ τότε για $\alpha_1(x, y) = (R_n(x), yS_n(x))$ και $\alpha_2(x, y) = (x, y)$ και $\alpha_3(x, y) = (R_{n+1}(x), yS_{n+1}(x))$ ισχύει $\alpha_3 = \alpha_2 + \alpha_1$ και από το προηγούμενο λήμμα ισχύει $\frac{R'_{n+1}(x)}{S_{n+1}(x)} = n + 1$. Έχουμε ότι $R'_n(x) \neq 0$ ανν $\frac{R'_n(x)}{S_n(x)} = n \neq 0 \quad \Rightarrow \; p \nmid n$. Άρα διαχωρίσιμος $\Leftrightarrow p \nmid n$. □

Πρόταση 2.2.3. *Έστω E μια ελλειπτική καμπύλη υπέρ το $\mathbb{F}_q$ όπου $q = p^l$. Έστω $r, s \in \mathbb{Z}$ όχι και τα δυο μηδέν. Ο ενδομορφισμός $r\phi_q + s$ είναι διαχωρίσιμος ανν $p \nmid s$.*

Απόδειξη. $r(x, y) = (R_r(x), yS_r(x)) \; \Rightarrow \; \big(R_{r\phi_q}(x), yS_{r\phi_q}(x)\big) = (r\phi_q)(x, y) = \big({R_r}^q(x), y^q {S_r}^q(x)\big) = ({R_r}^q(x), y(x^3 + Ax + B)^{\frac{q-1}{2}} {S_r}^q(x))$
Οπότε $C_{r\phi_q} = \frac{R'_{r\phi_q}}{S_{r\phi_q}} = \frac{q{R_r}^{q-1}(x)R'_r(x)}{S_{r\phi_q}} = 0$
$C_s = \frac{R'_s}{S_s} = s$ από την προηγούμενη πρόταση και από το λήμμα 2.2.3 παίρνουμε $\frac{R'_{r\phi_q+s}}{S_{r\phi_q+s}} = C_{r\phi_q} + C_s = 0 + s$ άρα $R'_{r\phi_q+s} = 0$ ανν $p \mid s$. □

2.3 Ιδιάζουσες Καμπύλες

Βασικά ενδιαφερόμαστε για ελλειπτικές καμπύλες ορισμένες υπέρ το σώμα $\mathbb{Q}$ ή κάποιο πεπερασμένο σώμα. Συχνά η μελέτη ελλειπτικών καμπυλών υπέρ το $\mathbb{Q}$ απαιτεί τη γνώση της συμπεριφοράς της ανηγμένης καμπύλης $(mod\, p)$ όπου $p \in \mathbb{P}$. Για τα $p \in \mathbb{P}$ όπου $p \mid \Delta(E)$ όμως,

η ανηγμένη $(mod\, p)$ καμπύλη είναι μια ιδιάζουσα κυβική καμπύλη. Εξ ου και ο λόγος που θεωρείται σκόπιμο να μελετήσουμε και ιδιάζουσες κυβικές καμπύλες. Είναι γνωστό ότι μια κυβική καμπύλη έχει το πολύ ένα ιδιάζον σημείο. Μια ιδιάζουσα κυβική καμπύλη έχει ακριβώς ένα ιδιάζον σημείο το οποίο χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι είναι το $(0,\, 0)$. Αυτό όμως μπορεί να είναι δύο τύπων. Η πρώτη περίπτωση είναι να σχηματίζει κορυφή (cusp) στο σημείο $(0,\, 0)$ (δεν υπάρχει η παράγωγος στο εν λόγω σημείο). Σ' αυτή την περίπτωση η καμπύλη μπορεί να πάρει τη μορφή $y^2 = x^3$. Ειδάλλως μπορεί να σχηματίζει κόμβο (node) στο σημείο $(0,\, 0)$ (η εφαπτομένη στο $(0,\, 0)$ έχει δύο διαφορετικές μεταξύ τους παραγώγους). Αν είμαστε σε αυτή τη περίπτωση η καμπύλη μπορεί να πάρει τη μορφή $y^2 = x^2(x + a)$.

Θεώρημα 2.3.1. *Έστω E η καμπύλη $y^2 = x^3$ και έστω $E_{ns}(K)$ τα μη ιδιάζοντα σημεία πάνω σ' αυτή την καμπύλη με συντεταγμένες από το K συμπεριλαμβανομένου του $\mathcal{O} = [0, 1, 0]$. Η απεικόνιση $E_{ns}(K) \to K$, $(x,\, y) \mapsto \frac{x}{y}$, $\mathcal{O} \mapsto 0$ είναι ισομορφισμός ομάδων ανάμεσα στις $E_{ns}(K)$ και K θεωρούμενη ως προσθετική ομάδα.*

Απόδειξη. Έστω $t = \frac{x}{y}$, τότε $x = \frac{x^3}{x^2} = \left(\frac{y}{x}\right)^2 = \frac{1}{t^2}$ και $y = \frac{x}{t} = \frac{1}{t^2}\frac{1}{t} = \frac{1}{t^3}$
Άρα μπορούμε να εκφράσουμε όλα τα σημεία της $E_{ns}(K)$ συναρτήσει του t. Έστω ότι το $t = 0$ αντιστοιχεί στο $(x,\, y) = \mathcal{O}$. Αυτό σημαίνει ότι η απεικόνιση του θεωρήματος είναι 1-1 και επί. Υποθέτουμε ότι $(x_1,\, y_1) + (x_2,\, y_2) = (x_3,\, y_3)$. Πρέπει να δείξουμε ότι $t_1 + t_2 = t_3$ όπου $t_i = \frac{x_i}{y_i}$
Αν $(x_1,\, y_1) \neq (x_2,\, y_2)$
$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$
Αντικαθιστώντας $x_i = \frac{1}{{t_i}^2}$, $y_i = \frac{1}{{t_i}^3}$ έχουμε

$$
\begin{aligned}
&{t_3}^{-2} = \left(\frac{{t_2}^{-3} - {t_1}^{-3}}{{t_2}^{-2} - {t_1}^{-2}}\right)^2 - {t_1}^{-2} - {t_2}^{-2} \;\Rightarrow \\
&{t_3}^{-2} = (t_1 + t_2)^{-2}
\end{aligned}
$$

Όμοια: $y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$ το οποίο αν αντικαταστήσουμε γίνεται ${t_3}^{-3} = (t_1 + t_2)^{-3}$.
$\frac{x_3}{y_3} = \frac{t_1 + {t_2}^{-2}}{t_1 + {t_2}^{-3}} = \frac{1}{(t_1 + t_2)^{-1}} = t_1 + t_2$.

Αν $(x_1, y_1) = (x_2, y_2)$
$x_3 = \frac{-9{x_1}^4}{4{y_1}^4} - 2x_1 = \frac{9{t_1}^{-8}}{4{t_1}^{-6}} - 2{t_1}^{-2} = \frac{9}{4}{t_1}^{-2} - 2{t_1}^{-2} = \frac{1}{4}{t_1}^{-2}$
$y_3 = \frac{3{x_1}^2}{2y_1}(x_1 - x_3) - y_1 = \frac{-3{t_1}^{-4}}{2{t_1}^{-3}}\left(\frac{1}{4}{t_1}^{-2} - {t_1}^{-2}\right) - {t_1}^{-3} = \frac{1}{8}{t_1}^{-3}$
$\frac{x_3}{y_3} = \frac{4^{-1}{t_1}^{-2}}{8^{-1}{t_1}^{-3}} = 2t_1$ □

Θεωρούμε την περίπτωση όπου $x^3 + Ax + B$ έχει διπλή ρίζα. Υποθέτουμε ότι αυτή η ρίζα είναι το 0 και η καμπύλη E έχει την εξίσωση $y^2 = x^2(x + a)$ για κάποιο $a \neq 0$. Το σημείο $(0, 0)$ είναι το μόνο ιδιάζον σημείο της καμπύλης. Έστω $E_{ns}(K)$ τα μη ιδιάζοντα σημεία της E με συντεταγμένες από το K συμπεριλαμβάνοντας το $\mathcal{O}$. Έστω $\alpha^2 = a$ (άρα το α μπορεί να ανήκει σε επέκταση του K). Η εξίσωση της E μπορεί να γραφεί ως

$$\left(\frac{y}{x}\right)^2 = a + x$$

Όταν το x είναι κοντά στο 0 το δεξί μέλος είναι σχεδόν a. Άρα η E προσεγγίζεται από $\left(\frac{y}{x}\right)^2 = a$ ή $\frac{y}{x} = \pm\alpha$ κοντά στο 0. Αυτό σημαίνει ότι οι δυο εφαπτόμενες της E στο $(0, 0)$ είναι $y = \alpha x$ και $y = -\alpha x$.

Θεώρημα 2.3.2. *Έστω E η καμπύλη $y^2 = x^2(x + a)$ με $a \neq 0$, $a \in K$. Έστω $E_{ns}(K)$ τα μη ιδιάζοντα σημεία της E με συντεταγμένες από το K. Έστω $\alpha^2 = a$, θεωρούμε την απεικόνιση $\psi : (x, y) \mapsto \frac{y + \alpha x}{y - \alpha x}$, $\mathcal{O} \mapsto 1$*
1)Αν $\alpha \in K$ τότε η ψ είναι ισομορφισμός από το $E_{ns}(K)$ στο K^* ως πολλαπλασιαστική ομάδα.
2)Αν $\alpha \notin K$ τότε η ψ δίνει έναν ισομορφισμό $E_{ns}(K) \cong \{u + \alpha v \mid u, v \in K, u^2 - av^2 = 1\}$ όπου το δεξί μέλος είναι ομάδα με πράξη τον πολλαπλασιασμό.

Απόδειξη. Έστω $t = \frac{y + \alpha x}{y - \alpha x}$ το οποίο συνεπάγεται $\frac{y}{x} = \alpha\frac{t+1}{t-1}$ αφού $x + a = \left(\frac{y}{x}\right)^2$ έχουμε $x = \left(\frac{y}{x}\right)^2 - a = \left(\alpha\frac{t+1}{t-1}\right)^2 - a = \frac{4\alpha^2 t}{(t-1)^2}$ και $y = \frac{4\alpha^3 t(t+1)}{(t-1)^3}$. Άρα το (x, y) καθορίζει το t και το t καθορίζει το (x, y) άρα η ψ είναι 1-1 και επί στην πρώτη περίπτωση.
Στην περίπτωση 2 κάνουμε ρητοποίηση του παρονομαστή πολλαπλασιάζοντας αριθμητή και παρονομαστή με $y + \alpha x$ άρα $\frac{y + \alpha x}{y - \alpha x} = u + \alpha v$.

Μπορούμε να αλλάξουμε το πρόσημο του α στην εξίσωση και να διατηρηθεί η ισότητα. Αρα θα έχουμε

$$\frac{y+\alpha x}{y-\alpha x} = u + \alpha v$$
$$\frac{y-\alpha x}{y+\alpha x} = u - \alpha v$$

Οπότε πολλαπλασιάζοντας κατά μέλη $u^2 - av^2 = \frac{(y+\alpha x)(y-\alpha x)}{(y+\alpha x)(y-\alpha x)} = 1$

Αντιστρόφως υποθέτουμε $u^2 - av^2 = 1$. Έστω $x = \left(\frac{u+1}{v}\right)^2 - a$, $y = \left(\frac{u+1}{v}\right)x$ τότε το (x, y) είναι πάνω στην E και $\psi(x, y) = \frac{\frac{y}{x} + \alpha}{\frac{y}{x} - \alpha} = \frac{u+1+\alpha v}{u+1-\alpha v} = \frac{(u+1+\alpha v)(u+1-\alpha v)}{(u+1-\alpha v)^2} = \frac{1}{u-\alpha v} = u + \alpha v$. Άρα είναι 1-1 και επί.

Μένει να δείξουμε ότι η ψ είναι ομομορφισμός. Υποθέτουμε $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ Έστω $t_i = \frac{y_i + \alpha x_i}{y_i - \alpha x_i}$. Πρέπει να δείξουμε οτι $t_1 t_2 = t_3$.

Αν $(x_1, y_1) \neq (x_2, y_2)$ τότε

$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a - x_1 - x_2$ Αντικαθιστώντας $x_i = \frac{4\alpha^2 t_i}{(t_i - 1)^2}$, $y_i = \frac{4\alpha^3 t_i(t_i+1)}{(t_i-1)^3}$ και κάνοντας πράξεις καταλήγουμε οτι

$\frac{4t_3}{(t_3-1)^2} = \frac{4t_1t_2}{(t_1t_2-1)^2}$. (1)

Όμοια $y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$ που έπεται

$\frac{4\alpha^3 t_3(t_3+1)}{(t_3-1)^3} = \frac{4\alpha^3 t_1 t_2(t_1t_2+1)}{(t_1t_2-1)^3}$ (2)

Από τις (1) και (2) έπεται $\frac{t_3 - 1}{t_3 + 1} = \frac{t_1t_2 - 1}{t_1t_2 + 1} \Rightarrow t_1t_2 = t_3$

Η απόδειξη είναι όμοια αν $(x_1, y_1) = (x_2, y_2)$ □

Όταν ανάγουμε την καμπύλη μας $(mod\, p)$ και μας προκύψει μια περίπτωση όπως αυτή του θεωρήματος 2.3.1 λέμε ότι η αναγωγή μας είναι προσθετική. Η δεύτερη περίπτωση είναι να μας προκύψει μια ιδιάζουσα καμπύλη όπως αυτή του θεωρήματος 2.3.2 όπου λέμε ότι η αναγωγή μας είναι πολλαπλασιαστική. Αν είμαστε σ' αυτήν την περίπτωση έχουμε πάλι δύο δυνατότητες. Αν ισχύει το (1) του θεωρήματος 2.3.2 τότε η πολλαπλασιαστική αναγωγή μας λέγεται split και αντίστοιχα αν ισχύει το (2) η αναγωγή μας λέγεται non-split.

2.4 Σημεία Torsion

Έστω E μια ελειπτική καμπύλη ορισμένη υπέρ το K. Έστω n ένας θετικός ακέραιος, ενδιαφερόμαστε για το $E[n] = \{P \in E(\overline{K}) \mid nP = \mathcal{O}\}$ όπου $\overline{K}$ αλγεβρική θήκη του K. Όταν η χαρακτηριστική του K δεν είναι 2, μπορούμε να φέρουμε την E στη μορφή $y^2 =$ πολυώνυνο τρίτου βαθμού και μπορούμε εύκολα να καθορίσουμε την $E[2]$.
Έστω $y^2 = (x - e_1)(x - e_2)(x - e_3)$ με $e_1, e_2, e_3 \in \overline{K}$. Ένα σημείο P ικανοποιεί την $2P = \mathcal{O}$ αν και μόνο αν η εφαπτόμενη στο P είναι κάθετηστον άξονα των x. Εύκολα βλέπουμε ότι αυτό σημαίνει ότι θα πρέπει $y = 0$ άρα $E[2] = \{\mathcal{O}, (e_1, 0), (e_2, 0), (e_3, 0)\}$ Η $E[2]$ είναι ισόμορφη με την $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.
Αν η χαρακτηριστική είναι 2 η κατάσταση είναι λίγο πιο περίπλοκη. Η E μπορούμε να υποθέσουμε ότι έχει μια από τις δύο μορφές:
1) $y^2 + xy + x^3 + a_2x^2 + a_6 = 0$
2) $y^2 + a_3y + x^3 + a_4x + a_6 = 0$
Στην πρώτη περίπτωση $a_6 \neq 0$ και στη δεύτερη $a_3 \neq 0$ (αλλιώς η καμπύλη θα ήταν ιδιάζουσα). Αν το $P = (x, y)$ με $P \in E(\overline{K})$ είναι σημείο τάξης 2 τότε η εφαπτόμενη στο P πρέπει να είναι κάθετη στον άξονα των x το οποίο σημαίνει ότι η μερική παράγωγος ως προς y πρέπει να είναι 0. Στην πρώτη περίπτωση αυτό σημαίνει ότι $x = 0$. Αντικαθιστώντας στην (1) $x = 0$ παίρνουμε $0 = y^2 + a_6 = (y + \sqrt{a_6})^2$. Άρα το $(0, \sqrt{a_6})$ είναι το μόνο σημείο τάξης 2 (οι τετραγωνικές ρίζες είναι μοναδικές σε $chK = 2$) άρα $E[2] = \{\mathcal{O}, (0, \sqrt{a_6})\}$ ισόμορφη με την $\mathbb{Z}_2$. Στην περίπτωση (2) η μερική παράγωγος ως προς y είναι $a_3 \neq 0$, άρα δεν υπάρχουν σημεία τάξης 2 άρα $E[2] = \{\mathcal{O}\}$ Άρα έχουμε την ακόλουθη πρόταση.

Πρόταση:Έστω E μια ελειπτική καμπύλη ορισμένη υπέρ το K. Αν $chK \neq 2$ τότε $E[2] = \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Αν $chK = 2$ τότε $E[2] \cong \{\mathcal{O}\}$ ή $E[2] \cong \mathbb{Z}_2$.

Ας δούμε τώρα την $E[3]$. Αρχικά υποθέτουμε οτι $chK \neq 2, 3$ άρα η E μπορεί να δοθεί στη μορφή $y^2 = x^3 + Ax + B$. Ένα σημείο P ικανοποιεί την $3P = \mathcal{O}$ αν και μόνο αν $2P = -P$. Αυτό σημαίνει ότι η $x-$συντεταγμένη του $2P$ ισούται με αυτή του P (η y-συντεταγμένη διαφέρει ως προς πρόσημο). Από τους τύπους του αθροίσματος σημείων,

$$\lambda^2 - 2x = x \quad \text{όπου } \lambda = \frac{3x^2 + A}{2y}$$

άρα $\lambda^2 4y^2 = (3x^2 + A)^2 \Rightarrow 4\lambda^2(x^3 + Ax + B) = (3x^2 + A)^2$ όμως $\lambda^2 = 3x$ άρα $(3x^2 + A)^2 = 12x(x^3 + Ax + B) \Rightarrow 9x^4 + 6Ax^2 + A^2 = 12x^4 + 12Ax^2 +$

$12Bx \Rightarrow 3x^4 + 6Ax^2 + 12Bx - A^2 = 0$
Η διακρίνουσα του πολυωνύμου είναι $-6912(4A^3 + 27B^2)^2$ η οποία δεν είναι 0. Άρα το πολυώνυμο δεν έχει ρίζες με πολλαπλότητα. Άρα υπάρχουν 4 διαφορετικές τιμές του x στο $\overline{K}$ και κάθε x μας δίνει δυο τιμές του y άρα έχουμε 8 σημεία τάξης 3. Εφ' όσον το $\mathcal{O}$ ανήκει επίσης στην $E[3]$ βλέπουμε λοιπόν ότι η $E[3]$ ειναι ομάδα τάξης 9 στην οποία κάθε στοιχείο είναι 3-torison. Έπεται $E[3] = \mathbb{Z}_3 \oplus \mathbb{Z}_3$
Αν τώρα η χαρακτηριστική είναι 3 υποθέτουμε ότι η E έχει τη μορφή $y^2 = x^3 + a_2x^2 + a_4x + a_6$. Πάλι θέτουμε η $x-$ συντεταγμένη του $2P$ ισούται με αυτή του P. Υπολογίζουμε την $x-$ συντεταγμένη του $2P$ και την θέτουμε ίση με αυτή του P.
$\left(\frac{3x^2 + 2a_2x + a_4}{2y}\right)^2 - a_2 - 2x = x \Rightarrow \left(\frac{2a_2x + a_4}{2y}\right)^2 - a_2 = 3x = 0 \Rightarrow$
$(2a_2x + a_4)^2 - a_2 4y^2 = 0 \Rightarrow 4a_2a_4x + {a_4}^2 + 4{a_2}^2x^2 - 4a_2(x^3 + a_2x^2 + a_4x + a_6) = 0 \Rightarrow 4a_2a_4x + {a_4}^2 + 4{a_2}^2x^2 - 4a_2x^3 - 4a_2x^2 - 4a_2a_4x - 4a_2a_6 = 0 \Rightarrow -a_2x^3 + {a_4}^2 - a_2a_6 = 0 \Rightarrow a_2x^3 + a_2a_6 - {a_4}^2 = 0$
Τα a_2, a_4 δεν μπορούν να είναι ταυτόχρονα 0 καθώς τότε $x^3 + a_6 = (x + \sqrt[3]{a_6})^3$ έχει ρίζα με πολλαπλότητα μεγαλύτερη του 1, άρα ένα τουλάχιστον εκ των a_2, a_4 δεν είναι 0.
Αν $a_2 = 0$ τότε παίρνουμε $-{a_4}^2 = 0$ το οποίο δεν μπορεί να συμβεί άρα δεν υπάρχουν τιμές του x άρα $E[3] = \{\mathcal{O}\}$
Αν $a_2 \neq 0$ τότε παίρνουμε μια εξίσωση της μορφής $a_2(x^3 + a) = 0$ η οποία έχει μια τριπλή ρίζα σε χαρακτηριστική 3. Άρα υπάρχει μία τιμή του x και αντίστοιχα δυο του y. Αυτό μας δίνει 2 σημεία τάξης 3. Εφόσον συμπεριλαμβάνουμε και το σημείο $\mathcal{O}$ βλέπουμε οτι η $E[3]$ έχει τάξη 3 άρα $E[3] \cong \mathbb{Z}_3$

Θεώρημα 2.4.1. *Έστω E μια ελλειπτική καμπύλη ορισμένη σε ένα σώμα K και έστω n ένας θετικός ακέραιος. Αν η χαρακτηριστική του K δεν διαιρεί το n ή είναι 0 τότε $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$*
Αν $chK = p > 0$ και $p \mid n$ τότε γράφουμε $n = p^r n'$ με $p \nmid n'$ τότε $E[n] \cong \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'}$ ή $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_{n'}$

Το θεώρημα θα αποδειχθεί στην συνέχεια στο τέλος της παραγράφου 2.5 .

Ορισμός. *Μια ελλειπτική καμπύλη E σε χαρακτηριστική p λέγεται κανονική (ordinary) αν $E[p] \cong \mathbb{Z}_p$. Ονομάζεται υπεριδιάζουσα (supersingular) αν $E[p] \cong \{\mathcal{O}\}$*

Ένα κριτήριο για το αν μια ελλειπτική καμπύλη ορισμένη πάνω απο ένα σώμα $\mathbb{F}_q$ είναι υπεριδιάζουσα είναι το εξής:

Κριτήριο : Μια ελλειπτική καμπύλη E ορισμένη πάνω απο ένα σώμα $\mathbb{F}_q$ είναι υπεριδιάζουσα αν και μόνο αν $a \equiv 0 \pmod p$ όπου $a = q + 1 - \#E(\mathbb{F}_q)$ και p η χαρακτηριστική του σώματος μας. [4]

Έστω n ένας θετικός ακέραιος που δεν διαιρείται από την χαρακτηριστική του K. Επιλέγουμε μια βάση $\{\beta_1, \beta_2\}$ για την $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$. Αυτό σημαίνει ότι κάθε στοιχείο της $E[n]$ μπορεί να αναπαρασταθεί στη μορφή $m_1\beta_1 + m_2\beta_2$ με $m_1, m_2 \in \mathbb{Z}$. Τα m_1, m_2 είναι μοναδικά καθορισμένα $(mod\, n)$. Έστω $\alpha : E(\overline{K}) \to E(\overline{K})$ ένας ομομορφισμός ομάδων. Τότε ο α απεικονίζει το $E[n]$ στο $E[n]$. Αυτό ισχύει διότι $\mathcal{O} = \alpha(\mathcal{O}) = \alpha(nP) = n\alpha(P)$ οπότε $ord(\alpha(P)) \mid n \;\Rightarrow \alpha(P) \in E[n]$. Άρα υπάρχουν $a, b, c, d \in \mathbb{Z}_n$ τ.ω. $\alpha(\beta_1) = a\beta_1 + c\beta_2$ και $\alpha(\beta_2) = b\beta_1 + d\beta_2$. Άρα κάθε ομομορφισμός $\alpha : E(\overline{K}) \to E(\overline{K})$ περιορισμένος στην $E[n]$ αναπαριστάται από ένα πίνακα 2×2

$$\alpha_n = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Η σύνθεση ομομορφισμών αντιστοιχεί σε πολλαπλασιασμό των αντίστοιχων πινάκων. Σε πολλές περιπτώσεις ο ομομορφισμός α θα είναι ενδομορφισμός το οποίο σημαίνει ότι δίνεται από ρητές συναρτήσεις.

Παράδειγμα :Έστω E η ελλειπτική καμπύλη με εξίσωση $y^2 = x^3 - 2$ ορισμένη υπέρ το $\mathbb{R}$ και έστω $n = 2$ τότε $E[2] = \{\mathcal{O}, (\sqrt[3]{2}, 0), (\omega\sqrt[3]{2}, 0), , (\omega^2\sqrt[3]{2}, 0)\}$ όπου ω μια μη τετριμμένη κυβική ρίζα της μονάδας. Έστω $\beta_1 = (\sqrt[3]{2}, 0)$ και $\beta_2 = (\omega\sqrt[3]{2}, 0)$. Τότε το $\{\beta_1, \beta_2\}$ είναι μια βάση της $E[2]$ και $\beta_3 = \beta_1 + \beta_2$.
Πράγματι,

$$x_3 = \lambda^2 - x_1 - x_2 = \Big(\frac{0-0}{\omega\sqrt[3]{2} - \sqrt[3]{2}}\Big)^2 - \sqrt[3]{2} - \omega\sqrt[3]{2} = \omega^2\sqrt[3]{2}$$
$$y_3 = -\lambda(x_3 - x_1) - y_1 = 0 - 0 = 0$$

Έστω $\alpha : E(\mathbb{C}) \to E(\mathbb{C})$ η μιγαδική συζυγία : $\alpha(x, y) = (\overline{x}, \overline{y})$. Ο α είναι ομομορφισμός.
Πράγματι,
$\alpha(x_1, y_1) = (\overline{x_1}, \overline{y_1}) = P_1$
$\alpha(x_2, y_2) = (\overline{x_2}, \overline{y_2}) = P_2$
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3) \quad P_1 \neq P_2$

$P_4 = (x_4, y_4) = P_1 \oplus P_2$

$$x_4 = \Big(\frac{\overline{y_2} - \overline{y_1}}{\overline{x_2} - \overline{x_1}}\Big)^2 - \overline{x_2} - \overline{x_1} = \overline{\Big(\frac{y_2 - y_1}{x_2 - x_1}\Big)^2} - \overline{x_1} - \overline{x_2}$$
$$= \overline{\Big(\frac{y_2 - y_1}{x_2 - x_1}\Big)^2 - x_1 - x_2} = \overline{x_3}$$

$$y_4 = -\Big(\frac{\overline{y_2} - \overline{y_1}}{\overline{x_2} - \overline{x_1}}\Big)(x_4 - \overline{x_1}) - \overline{y_1} = -\overline{\Big(\frac{y_2 - y_1}{x_2 - x_1}\Big)}(\overline{x_3} - \overline{x_1}) - \overline{y_1}$$
$$= -\overline{\Big(\frac{y_2 - y_1}{x_2 - x_1}\Big)(x_3 - x_1) - y_1} = \overline{y_3}$$

Άρα $P_4 = (\overline{x_3}, \overline{y_3}) = \alpha(x_3, y_3) \Rightarrow \alpha(x_1, y_1) + \alpha(x_2, y_2) = \alpha((x_1, y_1) + (x_2, y_2))$
Έχουμε $\alpha(\beta_1) = 1 \cdot \beta_1 + 0 \cdot \beta_2$, $\alpha(\beta_2) = \beta_3 = 1 \cdot \beta_1 + 1 \cdot \beta_2$ Άρα παίρνουμε τον πίνακα

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

2.5 Division Polynomials

Έστω οι μεταβλητές A, B. Ορίζουμε το πολυώνυμο διαίρεσης $\psi_m \in \mathbb{Z}[x, y, A, B]$ ως
$\psi_0 = 0$
$\psi_1 = 1$
$\psi_2 = 2y$
$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$
$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$
$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3$ για $m \geq 2$
$\psi_{2m} = (2y)^{-1}\psi_m(\psi_{m+2}\psi_{m-1}^2) - \psi_{m-2}\psi_{m+1}^2$ για $m \geq 3$

Λήμμα 2.5.1. *Το ψ_n είναι πολυώνυμο του $\mathbb{Z}[x, y^2, A, B]$ αν το n είναι περιττός και το $\psi_n \in 2y\mathbb{Z}[x, y^2, A, B]$ αν το n είναι άρτιος.*

Απόδειξη. Το λήμμα ισχύει για $n \leq 4$. Επαγωγικά υποθέτουμε ότι ισχύει $\forall\, n < 2m$. Επίσης υποθέτουμε ότι $2m > 4$ άρα $m > 2$. Τότε $2m > m + 2$ άρα όλα τα πολυώνυμα που εμφανίζονται στον ορισμό του ψ_{2m} ικανοποιούν τις υποθέσεις τις επαγωγής.

Αν ο m είναι άρτιος τότε τα $\psi_m,\ \psi_{m+2},\ \psi_{m-2} \in 2y\mathbb{Z}[x,\ y^2,\ A,\ B]$ άρα και το $\psi_{2m} \in 2y\mathbb{Z}[x,\ y^2,\ A,\ B]$ αφού $\psi_{2m} = (2y)^{-1}\psi_m(\psi_{m+2}\psi_{m-1}^2) - \psi_{m-2}\psi_{m+1}^2$

Αν ο m είναι περιττός τότε $\psi_{m-1},\ \psi_{m+1} \in 2y\mathbb{Z}[x,\ y^2,\ A,\ B]$ αφού $m-1$, $m+1$ άρτιοι. Οπότε $\psi_{m-1} = 2yP(x,\ y^2,\ A,\ B)$, $\psi_{m+1} = 2yQ(x,\ y^2,\ A,\ B)$ άρα $\psi_{m-1}^2 = 4y^2P^2(x,\ y^2,\ A,\ B)$, $\psi_{m+1}^2 = 4y^2Q^2(x,\ y^2,\ A,\ B)$
$\psi_{2m} = (2y)^{-1}\psi_m 4y^2(\psi_{m+2}P^2(x,\ y^2,\ A,\ B) + \psi_{m-2}Q^2(x,\ y^2,\ A,\ B) \in 2y\mathbb{Z}[x,\ y^2,\ A,\ B]$
Άρα ισχύει και για $n = 2m$

Ας υποθέσουμε ότι ισχύει για $n < 2m+1$ τώρα.
Αν m είναι άρτιος : $\psi_m,\ \psi_{m+2} \in 2y\mathbb{Z}[x,\ y^2,\ A,\ B], \psi_{m-1},\ \psi_{m+1} \in \mathbb{Z}[x,\ y^2,\ A,\ B]$ άρα
$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \ \Rightarrow$
$\psi_{2m+1} = 16y^4P_1(x,\ y^2,\ A,\ B)P_2(x,\ y^2,\ A,\ B) - P_3(x,\ y^2,\ A,\ B)P_4(x,\ y^2,\ A,\ B)$
Άρα $\psi_{2m+1} \in \mathbb{Z}[x,\ y^2,\ A,\ B]$

Αν m είναι περιττός : $\psi_m,\ \psi_{m+2} \in \mathbb{Z}[x,\ y^2,\ A,\ B], \psi_{m-1},\ \psi_{m+1} \in 2y\mathbb{Z}[x,\ y^2,\ A,\ B]$
$\psi_{2m+1} = P_1(x,\ y^2,\ A,\ B)P_2(x,\ y^2,\ A,\ B) - 16y^4P_3(x,\ y^2,\ A,\ B)P_4(x,\ y^2,\ A,\ B)$
Άρα $\psi_{2m+1} \in \mathbb{Z}[x,\ y^2,\ A,\ B]$ □

Ορίζουμε τα πολυώνυμα $\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}$ και
$\omega_m = (4y)^{-1}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)$.

Λήμμα 2.5.2. *Το $\phi_n \in \mathbb{Z}[x,\ y^2,\ A,\ B]$ για όλα τα n. Αν ο n είναι περιττός τότε $\omega_n \in y\mathbb{Z}[x,\ y^2,\ A,\ B]$. Αν ο n είναι άρτιος τότε $\omega_n \in \mathbb{Z}[x,\ y^2,\ A,\ B]$*

Απόδειξη. Αν ο n είναι περιττός τότε $\psi_{n+1},\ \psi_{n-1} \in y\mathbb{Z}[x,\ y^2,\ A,\ B]$ άρα το γινόμενό τους ανήκει στο $\mathbb{Z}[x,\ y^2,\ A,\ B]$ και $\psi_n \in \mathbb{Z}[x,\ y^2,\ A,\ B]$ οπότε $\phi_n \in \mathbb{Z}[x,\ y^2,\ A,\ B]$

Αν ο n είναι άρτιος τότε $\psi_{n+1},\ \psi_{n-1} \in \mathbb{Z}[x,\ y^2,\ A,\ B]$ και $\psi_n \in y\mathbb{Z}[x,\ y^2,\ A,\ B] \ \Rightarrow$ $\psi_n^2 \in \mathbb{Z}[x,\ y^2,\ A,\ B]$ άρα $\phi_n \in \mathbb{Z}[x,\ y^2,\ A,\ B]$

Αν ο n είναι περιττός : $y^{-1}\omega_n = (4y^2)^{-1}(\psi_{n+2}{\psi^2}_{n-1} - \psi_{n-2}{\psi^2}_{n+1})$ όμως $\psi_{n-1}^2 \in 4y^2\mathbb{Z}[x,\ y^2,\ A,\ B]$ και $\psi_{n+1}^2 \in 4y^2\mathbb{Z}[x,\ y^2,\ A,\ B]$ άρα
$y^{-1}\omega_n \in \mathbb{Z}[x,\ y^2,\ A,\ B] \ \Rightarrow \omega_n \in y\mathbb{Z}[x,\ y^2,\ A,\ B]$.

Αν n είναι άρτιος : $\omega_n = (4y)^{-1}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2) =$
$(4y)^{-1}(2yp_1(x,\ y^2,\ A,\ B){p_2}^2(x,\ y^2,\ A,\ B) - 2yp_3(x,\ y^2,\ A,\ B){p_4}^2(x,\ y^2,\ A,\ B))$
άρα $\omega_n \in \frac{1}{2}\mathbb{Z}[x,\ y^2,\ A,\ B]$. Τώρα για να απαλαγούμε από το 2 στον πα-

ρονομαστή προχωρούμε ως εξής. Με επαγωγή δείχνουμε ότι

$$\psi_n \equiv (x^2+A)^{\frac{n^2-1}{4}} \pmod 2 \quad \text{αν n περιττός}$$
$$(2y)^{-1}\psi_n \equiv \Big(\frac{n}{2}\Big)(x^2+A)^{\frac{n^2-4}{4}} \pmod 2 \quad \text{αν n άρτιος}$$

Περίπτωση 1 : $n \equiv 1 \pmod 4$ δηλαδή $n = 2m+1$ και $m = 2k$

$$\begin{aligned}
\psi_n = \psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \\
&\equiv 2y\Big(\frac{m+2}{2}\Big)(x^2+A)^{\frac{(m+2)^2-4}{4}}\Big(\frac{m}{2}\Big)^3(x^2+A)^{\frac{3(m^2-4)}{4}}2^3y^3 - \\
&\quad (x^2+A)^{\frac{(m-1)^2-1}{4}}(x^2+A)^{\frac{3((m+1)^2-4)}{4}} \pmod 2 \\
&\equiv 0 - (x^2+A)^{\frac{m^2-2m+1-1+3m^2+6m+3-3}{4}} \pmod 2 \\
&\equiv (x^2+A)^{\frac{(2m+1)^2-1}{4}} \pmod 2
\end{aligned}$$

Περίπτωση 2 : $n \equiv 3 \pmod 4$ δηλαδή $n = 2m+1$ και $m = 2k+1$

$$\begin{aligned}
\psi_n = \psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \\
&\equiv (x^2+A)^{\frac{(m+2)^2-1}{4}}(x^2+A)^{\frac{3m^2-3}{4}} - \\
&\Big(\frac{m-1}{2}\Big)2y(x^2+A)^{\frac{(m-1)^2-4}{4}}2^3y^3\Big(\frac{m+1}{2}\Big)^3(x^2+A)^{\frac{3(m+1)^2-12}{4}} \pmod 2 \\
&\equiv (x^2+A)^{\frac{m^2+4m+3+3m^2-3}{4}} \pmod 2 \\
&\equiv (x^2+A)^{\frac{(2m+1)^2-1}{4}} \pmod 2
\end{aligned}$$

Περίπτωση 3 : $n \equiv 0 \pmod 4$ δηλαδή $n = 2m$ και $m = 2k$

$$
\begin{aligned}
\psi_{2m} &= (2y)^{-1}\psi_m(\psi_{m+2}\psi_{m-1}^2) - \psi_{m-2}\psi_{m+1}^2 \\
&\equiv (2y)^{-1}2y\Big(\frac{m}{2}\Big)(x^2+A)^{\frac{m^2-4}{4}} \\
&\quad \Big[2y\Big(\frac{m+2}{2}\Big)(x^2+A)^{\frac{(m+2)^2-4}{4}}(x^2+A)^{\frac{(m-1)^2-1}{2}} - \\
&\quad 2y\Big(\frac{m-2}{2}\Big)(x^2+A)^{\frac{(m-2)^2-4}{4}}(x^2+A)^{\frac{(m+1)^2-1}{2}}\Big] \pmod 2 \\
&\equiv 2y\Big(\frac{m}{2}\Big)(x^2+A)^{\frac{m^2-4}{4}} \\
&\quad \Big[\Big(\frac{m+2}{2}\Big)(x^2+A)^{\frac{3m^2}{4}} - \Big(\frac{m-2}{2}\Big)(x^2+A)^{\frac{3m^2}{4}}\Big] \pmod 2 \\
&\equiv 2ym(x^2+A)^{\frac{(2m)^2-4}{4}} \pmod 2 \qquad \text{και επειδή} \quad n=2m \\
&\equiv 2y\Big(\frac{n}{2}\Big)(x^2+A)^{\frac{n^2-4}{4}} \pmod 2
\end{aligned}
$$

Άρα $(2y)^{-1}\psi_n \equiv \Big(\frac{n}{2}\Big)(x^2+A)^{\frac{n^2-4}{4}} \pmod 2$

Περίπτωση 4 : $n \equiv 2 \pmod 4$ δηλαδή $n = 2m$ και $m = 2k+1$

$$\begin{aligned}
\psi_{2m} &= (2y)^{-1}\psi_m(\psi_{m+2}\psi_{m-1}^2) - \psi_{m-2}\psi_{m+1}^2 \\
&\equiv (2y)^{-1}(x^2+A)^{\frac{m^2-1}{4}} \\
&\Big[(x^2+A)^{\frac{(m+2)^2-1}{4}}\Big(\frac{m-1}{2}\Big)^2(x^2+A)^{\frac{(m-1)^2-4}{2}}(2y)^2 - \\
&(x^2+A)^{\frac{(m-2)^2-1}{4}}\Big(\frac{m+1}{2}\Big)^2(x^2+A)^{\frac{(m+1)^2-4}{2}}(2y)^2\Big] \pmod 2 \\
&\equiv 2y(x^2+A)^{\frac{m^2-1}{4}} \\
&\Big[\Big(\frac{m-1}{2}\Big)^2(x^2+A)^{\frac{3m^2-3}{4}} - \Big(\frac{m+1}{2}\Big)^2(x^2+A)^{\frac{3m^2-3}{4}}\Big] \pmod 2 \\
&\equiv -2ym(x^2+A)^{\frac{4m^2-4}{4}} \pmod 2 \\
&\equiv 2ym(x^2+A)^{\frac{4m^2-4}{4}} \pmod 2
\end{aligned}$$

Άρα $(2y)^{-1}\psi_n \equiv \Big(\frac{n}{2}\Big)(x^2+A)^{\frac{n^2-4}{4}} \pmod 2$

Οπότε αν n άρτιος

$$\begin{aligned}
\omega_n &= (4y)^{-1}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2) \\
&\equiv (4y)^{-1}\Big[2y\Big(\frac{n+2}{2}\Big)(x^2+A)^{\frac{(n+2)^2-4}{4}}(x^2+A)^{\frac{(n-1)^2-1}{4}} - \\
&\equiv 2y\Big(\frac{n-2}{2}\Big)(x^2+A)^{\frac{(n-2)^2-4}{4}}(x^2+A)^{\frac{(n+1)^2-1}{4}}\Big] \pmod 2 \\
&\equiv \frac{1}{2}(x^2+A)^{\frac{3n^2}{4}}2 \pmod 2 \\
&\equiv (x^2+A)^{\frac{3n^2}{4}} \pmod 2
\end{aligned}$$

□

Τώρα θεωρούμε μια ελλειπτική καμπύλη $E : y^2 = x^3 + Ax + B$ $4A^3 + 27B^2 \neq 0$. Δεν προσδιορίζουμε ακόμα σε ποιόν δακτύλιο ή σώμα ανήκουν τα A , B άρα τα θεωρούμε ως μεταβλητές. Θεωρούμε τα πολυώνυμα του $\mathbb{Z}[x,\, y^2,\, A,\, B]$ ως πολυώνυμα του $\mathbb{Z}[x,\, A,\, B]$ αντικαθιστώντας το y^2 με $x^3 + Ax + B$. Άρα γράφουμε $\phi_n(x)$ και $\psi_n^2(x)$. Το ψ_n αν και δεν είναι κατ' ανάγκη μόνο πολυώνυμο του x το ψ_n^2 είναι πάντα πολυώνυμο μόνο του x.

Λήμμα 2.5.3. $\deg(\phi_n(x)) = n^2$ *και* $\deg(\psi_n^2(x)) = n^2 - 1$ *και* $a_{n^2} = 1$ *και* $a_{n^2-1} = n^2$ *αντίστοιχα.*

Απόδειξη. (Θέλουμε $\phi_n(x) = x^{n^2} + \dots \quad , \quad \psi_n^2(x) = n^2 x^{n^2-1} + \dots$)
Αρχικά θα δείξουμε ότι,

$$\psi_n = \begin{cases} y\Big(nx\dfrac{n^2-4}{2} + \dots\Big) & , n \equiv 0 \pmod 2 \\ nx\dfrac{n^2-1}{2} + \dots & , n \equiv 1 \pmod 2 \end{cases}$$

Το αποδεικνύουμε με επαγωγή :
Αν $n = 2m+1$ με $m = 2k$ τότε ο μεγιστοβάθμιος όρος του $\psi_{m+2}{\psi_m}^3$ είναι $y(m+2)x^{\frac{(m+2)^2-4}{2}} y^3 m^3 x^{\frac{3m^2-12}{2}} = (m+2)m^3 y^4 x^{2m^2+2m-6}$ αντικαθιστώντας το y^4 με $\left(x^3+Ax+B\right)^2$ ο μεγιστοβάθμιος όρος θα είναι ο $(m+2)m^3 x^{2m^2+2m-6} x^6 = (m+2)m^3 x^{\frac{4m^2+4m}{2}} = (m+2)m^3 x^{\frac{(2m+1)^2-1}{2}}$
Για το $\psi_{m-1}\psi_{m+1}^3$: $(m-1)x^{\frac{(m-1)^2-1}{2}}(m+1)^3 x^{\frac{3(m+1)^2-3}{2}} = (m-1)(m+1)^3 x^{\frac{(2m+1)^2-1}{2}}$
Άρα ο μεγιστοβάθμιος όρος του ψ_{2m+1} είναι ο
$[(m+2)m^3 - (m-1)(m+1)^3] x^{\frac{(2m+1)^2-1}{2}} = (2m+1)x^{\frac{(2m+1)^2-1}{2}}$.
Ομοίως οι άλλες περιπτώσεις για το $n \pmod 4$
Τώρα όμως για το ψ_n ισχύει,
Αν $n \equiv 0 \pmod 2$: $\psi_n^2 = y^2 n^2 x^{n^2-4} + \dots = x^3 n^2 x^{n^2-4} + \dots = n^2 x^{n^2-1} + \dots$
Αν $n \equiv 1 \pmod 2$: $\psi_n^2 = n^2 x^{n^2-1} + \dots$

Για το ϕ_n ισχύει :
Αν n περιττός : $\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1}$ οπότε ο μεγιστοβάθμιος όρος του ${x\psi_n}^2$ είναι $n^2 x^{n^2}$ και του $\psi_{n+1}\psi_{n-1}$ θα είναι $y(n+1)x^{\frac{(n+1)^2-4}{2}} y(n-1)x^{\frac{(n-1)^2-4}{2}} = y^2(n^2-1)x^{n^2-3}$ όμως $y^2 = x^3+Ax+B$ άρα ο μεγιστοβάθμιος είναι $(n^2-1)x^{n^2-3}x^3 = (n^2-1)x^{n^2}$. Τελικά $\phi_n = n^2 x^{n^2} - (n^2-1)x^{n^2} + \dots = x^{n^2} + \dots$
Αν n άρτιος : Ο μεγιστοβάθμιος του $x\psi_n^2$ είναι $n^2 x^{n^2}$ και του $\psi_{n+1}\psi_{n-1}$ είναι $(n+1)x^{\frac{(n+1)^2-1}{2}}(n-1)x^{\frac{(n-1)^2-1}{2}} = (n^2-1)x^{n^2}$ άρα πάλι $\phi_n = x^{n^2} + \dots$
□

Θεώρημα 2.5.1. *Έστω* $P = (x, y)$ *ένα σημείο στην ελλειπτική καμπύλη* $y^2 = x^3 + Ax + B$ *(πάνω από κάποιο σώμα με* $chK \neq 2$*) και έστω* n *ένας θετικός ακέραιος.Τότε,*

$$nP = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,\, y)}{\psi_n^3(x,\, y)}\right)$$

Το θεώρημα δεν θα το αποδείξουμε εδώ ωστόσο μια απόδειξη δίνεται στο [2]

Παρατήρηση : Έστω ένα σημείο P της ελλειπτικής μας καμπύλης τότε $nP = \mathcal{O} \Leftrightarrow \psi_n(x,\, y) = 0$.

Πόρισμα 2.5.1. *Έστω E μια ελλειπτική καμπύλη. Ο ενδομορφισμός της E που δίνεται από τον πολλαπλασιασμό με n έχει βαθμό n^2.*

Απόδειξη. Από το προηγούμενο λήμμα έχουμε ότι το μέγιστο των βαθμών του αριθμητή καί του παρονομαστή του $\dfrac{\phi_n(x)}{\psi_n^2(x)}$ είναι n^2. Άρα ο βαθμός του ενδομορφισμού είναι n^2 αν αυτή η ρητή συνάρτηση είναι ανάγωγη, δηλαδή αν $\phi_n(x)$ και $\psi_n^2(x)$ δεν έχουν κοινές ρίζες. Θα αποδείξουμε ότι αυτό ισχύει. Έστω ότι δεν ισχύει. Έστω n ο μικρότερος δείκτης για τον οποίο έχουν κοινή ρίζα τα $\phi_n(x)\,,\, \psi_n^2(x)$. Έστω $n = 2m$ άρτιος,

$$\begin{aligned}\phi_2(x) &= x\psi_2(x,\, y)^2 - \psi_3(x)\psi_1(x)\\ &= x(2y)^2 - (3x^4 + 6Ax^2 + 12Bx - A^2)1\\ &= 4x(x^3 + Ax + B) - 3x^4 - 6Ax^2 - 12Bx + A^2\\ &= x^4 - 2Ax^2 - 8Bx + A^2\end{aligned}$$

Υπολογίζοντας την x-συντεταγμένη του $2m(x,\, y)$ σε δύο βήματα πολλαπλασιάζοντας πρώτα με m και μετά με 2 και χρησιμοποιώντας ότι ${\psi_2}^2 = 4y^2 = 4(x^3 + Ax + B)$ παίρνουμε,

$$\frac{\phi_{2m}}{{\psi_{2m}}^2} = \frac{\phi_2\Big(\dfrac{\phi_m}{{\psi_m}^2}\Big)}{{\psi_2}^2\Big(\dfrac{\phi_m}{{\psi_m}^2}\Big)} = \frac{{\phi_m}^4 - 2A{\phi_m}^2{\psi_m}^4 - 8B\phi_m{\psi_m}^6 + A^2{\psi_m}^8}{(4{\psi_m}^2)({\phi_m}^3 + A\phi_m{\psi_m}^4 + B{\psi_m}^6)} = \frac{U}{V}$$

όπου U και V είναι ο αριθμητής και ο παρονομαστής αντίστοιχα. Για να δείξουμε ότι τα U και V δεν έχουν κοινές ρίζες χρειαζόμαστε το εξης λήμμα

Λήμμα 2.5.4. *Έστω $\Delta = 4A^3 + 27B^2$ και έστω*
$F(x,\, z) = x^4 - 2Ax^2z^2 - 8Bxz^3 + A^2z^4$
$G(x,\, z) = 4z(x^3 + Axz^2 + Bz^3)$
$f_1(x,\, z) = 12x^2z + 16Az^3$
$g_1(x,\, z) = 3x^3 - 5Axz^2 - 27Bz^3$
$f_2(x,\, z) = 4\Delta x^3 - 4A^2Bx^2z + 4A(3A^3 + 22B^2)xz^2 + 12B(A^3 + 8B^2)z^3$
$g_2(x,\, z) = A^2Bx^3 + A(5A^3 + 32B^2)x^2z + 2B(13A^3 + 96B^2)xz^2 - 3A^2(A^3 + 8B^2)z^3$
Τότε $Ff_1 - Gg_1 = 4\Delta z^7$ και $Ff_2 - Gg_2 = 4\Delta x^7$.

Απόδειξη. $F(x,\,1) = x^4 - 2Ax^2 - 8Bx + A^2$, $G(x,\,1) = 4(x^3 + Ax + B)$, $f(x,\,1) = 12x^2 + 16A$, $g(x,\,1) = 3x^3 - 5Ax - 27B$

$F(x,\,1)f_1(x,\,1) - G(x,\,1)g_1(x,\,1) =$
$(x^4 - 2Ax^2 - 8Bx + A^2)(12x^2 + 16A^2) - 4(x^3 + Ax + B)(3x^3 - 5Ax - 27B) =$
$12x^6 - 24Ax^4 - 96Bx^3 + 12A^2x^2 + 16Ax^4 - 32A^2x^2 - 128ABx + 16A^3 - 12X^6 -$
$12Ax^4 - 12Bx^3 + 20Ax^4 + 20A^2x^2 + 20ABx + 108Bx^3 + 108ABx + 108B^2 =$
$16A^3 + 108B^2 = 4(4A^3 + 27B^2) = 4\Delta$

$F(\frac{x}{z},\,1)f_1(\frac{x}{z},\,1) - G(\frac{x}{z},\,1)g_1(\frac{x}{z},\,1) =$
$\left[\left(\frac{x}{z}\right)^4 - 2A\left(\frac{x}{z}\right)^2 - 8B\left(\frac{x}{z}\right) + A^2\right]\left[12\left(\frac{x}{z}\right)^2 + 16A\right] -$
$4\left(\left(\frac{x}{z}\right)^3 + A\left(\frac{x}{z}\right) + B\right)\left(3\left(\frac{x}{z}\right)^3 - 5A\left(\frac{x}{z}\right) - 27B\right) = 4\Delta \;\Rightarrow$
$(x^4 - 2Ax^2z^2 - 8Bxz^3 + A^2z^4)(12x^2z + 16Az^3) -$
$4z(x^3 + Axz^2 + Bz^3)(3x^3 - 5Axz^2 - 27Bz^3) = 4\Delta z^7$
Όμοια η δεύτερη ισότητα. □

Το λήμμα έπεται ότι $Uf_1(\phi_m,\,{\psi_m}^2) - Vg_1(\phi_m,\,{\psi_m}^2) = 4\Delta{\psi_m}^{14}$ και $Uf_2(\phi_m,\,{\psi_m}^2) + Vg_2(\phi_m,\,{\psi_m}^2) = 4\Delta{\phi_m}^7$
Αν τα U και V έχουν κοινή ρίζα τότε έχουν και τα ϕ_m και ${\psi_m}^2$. Εφόσον $n = 2m$ είναι ο μικρότερος δείκτης για τον οποίον υπάρχει μια κοινή ρίζα αυτό είναι αδύνατον. Μένει να δείξουμε ότι $U = \phi_{2m}$ και $V = {\psi_{2m}}^2$. Εφόσον $\frac{U}{V} = \frac{\phi_{2m}}{{\psi_{2m}}^2}$ και εφόσον τα U και V δεν έχουν κοινή ρίζα έπεται ότι το ϕ_{2m} είναι πολλαπλάσιο του U και το ${\psi_{2m}}^2$ πολλαπλάσιο του V.

$U = {\phi_m}^4 - 2A{\phi_m}^2{\psi_m}^4 - 8B\phi_m{\psi_m}^6 + A^2{\psi_m}^8$ και από το λήμμα 2.5.3 παίρνουμε ότι $U = x^{4m^2} + \ldots$. Επίσης από το λήμμα 2.5.3 έχουμε ότι $\phi_{2m} = x^{4m^2} + \ldots$ και αφού το ϕ_{2m} είναι πολλαπλάσιο του U έπεται $U = \phi_{2m}$ οπότε και $V = {\psi_{2m}}^2$. Τελικά τα ϕ_{2m} και ${\psi_{2m}}^2$ δεν έχουν κοινές ρίζες.

Τώρα υποθέτουμε ότι ο μικρότερος δείκτης n για τον οποίο τα ϕ_n και ψ_n^2 έχουν κοινή ρίζα είναι περιττός $n = 2m + 1$. Έστω r μια κοινή ρίζα των ϕ_n και ψ_n^2. Εφόσον τώρα $\phi_n = x{\psi_n}^2 - \psi_{n+1}\psi_{n-1}$ και εφόσον $\psi_{n+1}\psi_{n-1}$ είναι πολυώνυμο του x (από λήμμα 2.5.1) έχουμε ότι $(\psi_{n+1}\psi_{n-1})(r) = 0$. Αλλά $\psi_{n\pm1}^2$ είναι πολυώνυμα του x και το γινόμενο τους μηδενίζεται στο r. Άρα $\psi_{n+\delta}^2(r) = 0$ όπου $\delta = 1$ ή -1. Εφόσον το n είναι περιττός και το ψ_n και το $\psi_{n+2\delta}$ είναι πολυώνυμα του x. Επίσης $(\psi_n\psi_{n+2\delta})^2 = \psi_n^2\psi_{n+2\delta}^2$ μηδενίζεται στο r. Άρα και το $\psi_n\psi_{n+2\delta}$ μηδενίζεται στο r. Εφόσον $\phi_{n+\delta} = x\psi_{n+\delta}^2 - \psi_n\psi_{n+2\delta}$ συμπεραίνουμε ότι $\phi_{n+\delta}(r) = 0$.

Οπότε τα $\phi_{n+\delta}$, $\psi^2_{n+\delta}$ έχουν κοινή ρίζα. Το $n+\delta$ είναι άρτιος. Όταν θεωρήσαμε την περίπτωση όπου n ήταν άρτιος είδαμε ότι αν ϕ_{2m} και ψ^2_{2m} έχουν κοινή ρίζα τότε τα ϕ_m και ${\psi_m}^2$ έχουν κοινή ρίζα. Σ' αυτήν εδώ τη περίπτωση το εφαρμόζουμε αυτό στο $2m = n+\delta$ και εφόσον το n έχει υποτεθεί να είναι ο μικρότερος δείκτης για τον οποίο υπάρχει μια κοινή ρίζα έχουμε $\frac{n+\delta}{2} \geq n$. Αυτό έπεται $n = 1$. Αλλά τα $\phi_1 = x$, ${\psi_1}^2 = 1$ δεν έχουν κοινή ρίζα άρα, άτοπο. Αυτό αποδεικνύει ότι τα ϕ_n και ${\psi_n}^2$ δεν έχουν κοινές ρίζες σε όλες τις περιπτώσεις. Άρα όπως είπαμε στην αρχή της απόδειξης ο πολλαπλασιασμός με n έχει βαθμό n^2. □

Έστω $\alpha(x,\, y) = (R(x),\, yS(x))$ ένας ενδομορφισμός μιας ελλειπτικής καμπύλης E, τότε ο α είναι διαχωρίσιμος αν $R'(x)$ δεν είναι ταυτοτικά μηδέν. Έστω ότι το n δεν είναι πολλαπλάσιο της χαρακτηριστικής p του σώματος. Από το Θεώρημα 2.5.1 έχουμε ότι για τον πολλαπλασιασμό με n ισχύει,

$$R(x) = \frac{x^{n^2} + \dots}{n^2 x^{n^2-1} + \dots}$$

Ο αριθμητής της παραγώγου είναι,
$(n^2x^{n^2-1} + \dots)(n^2x^{n^2-1} + \dots) - (x^{n^2} + \dots)(n^2(n^2-1)x^{n^2-2} + \dots) =$
$(n^4x^{2n^2-2} + \dots) - [(n^4 - n^2)x^{2n^2-2} + \dots] = n^2x^{2n^2-2} + \dots \neq 0$
Άρα $R'(x) \neq 0$. Άρα ο πολλαπλασιασμός με n είναι διαχωρίσιμος.

Τώρα είμαστε σε θέση να αποδείξουμε το Θεώρημα 2.4.1. από την προηγούμενη ενότητα.

Θεώρημα 2.4.1. Έστω E μια ελλειπτική καμπύλη ορισμένη σε ένα σώμα K και έστω n ένας θετικός ακέραιος. Αν η χαρακτηριστική του K δεν διαιρεί το n ή είναι 0 τότε $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$
Αν $chK = p > 0$ και $p \mid n$ τότε γράφουμε $n = p^r n'$ με $p \nmid n'$ τότε $E[n] \cong \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'}$ ή $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_{n'}$

Απόδειξη. Από το πόρισμα 2.5.1 $\deg(n) = n^2$ και από την πρόταση 2.2.1 το $E[n]$ όπου $E[n] = Ker(n)$ έχει τάξη n^2. Το Θεμελιώδες Θεώρημα για Πεπερασμένες Αβελιανές Ομάδες μας λέει ότι $E[n] \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ για κάποιους ακέραιους $n_1,\, n_2,\, \cdots, n_k$ με $n_i \mid n_{i+1}\ \forall i$. Έστω $l \in \mathbb{P}$ με $l \mid n_1$. Τότε $l \mid n_i\ \forall i$. Άρα $E[l] \subseteq E[n]$ έχει τάξη l^k. Εφόσον όμως ισχύει και ότι η $E[l]$ έχει τάξη l^2 θα πρέπει $k = 2$ οπότε $E[n] \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ άρα πρέπει $n_2 \mid n$. Εφόσον $n^2 = \#E[n] = n_1 \cdot n_2$ έπεται ότι $n_1 = n_2 = n$ οπότε $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$ όταν η χαρακτηριστική p του σώματος δεν διαιρεί το n.

Μένει η περίπτωση όπου $p \mid n$. Πρώτα καθορίζουμε την p-δύναμη torison

στην E. Από πρόταση 2.2.2 ο πολλαπλασιασμός με p δεν είναι διαχωρίσιμος. Από την πρόταση 2.2.1 τώρα ο πυρήνας $E[p]$ του πολλαπλασιασμού με p έχει τάξη γνησίως μικρότερη από το βαθμό του ενδομορφισμού ο οποίος είναι p^2 από το προηγούμενο πόρισμα. Εφόσον κάθε στοιχείο της $E[p]$ έχει τάξη 1 ή p η τάξη της $E[p]$ είναι δύναμη του p άρα πρέπει να είναι 1 ή p. Αν η $E[p]$ είναι η τετριμμένη τότε και η $E[p^k]$ πρέπει να είναι η τετριμμένη $\forall\, k$. Ας υποθέσουμε τώρα ότι η $E[p]$ έχει τάξη p. Ισχυριζόμαστε ότι $E[p^k] \cong \mathbb{Z}_{p^k}\ \forall k$. Θα δείξουμε ότι η $E[p^k]$ είναι κυκλική. Υποθέτουμε ότι υπάρχει ένα στοιχείο P τάξης p^j. Ο πολλαπλασιασμός με p είναι επί από θεώρημα 2.2.1 άρα υπάρχει ένα σημείο Q τ.ω. $pQ = P$. Εφόσον $p^jQ = p^{j-1}P \neq \mathcal{O}$ αλλά $p^{j+1}Q = p^jP = \mathcal{O}$ άρα το Q έχει τάξη p^{j+1}. Επαγωγικά υπάρχουν σημεία τάξης $p^k\ \forall k$. Οπότε η $E[p^k]$ είναι κυκλική τάξης p^k. Τώρα μπορούμε να συνοψίσουμε.

Έστω $n = p^r \cdot n'$ με $r \geq 0$, $p \nmid n'$ τότε $E[n] \cong E[n'] \oplus E[p^r]$. Έχουμε ότι $E[n'] \cong \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'}$ αφού $p \nmid n'$. Είδαμε επίσης $E[p^r] \cong 0$ ή $\mathbb{Z}_{p^r}$. Επίσης $\mathbb{Z}_{n'} \oplus \mathbb{Z}_{p^r} \cong \mathbb{Z}_{n'p^r} \cong \mathbb{Z}_n$
Άρα $E[n] \cong \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'}$ ή $\mathbb{Z}_n \oplus \mathbb{Z}_{n'}$ □

2.6 Weil Pairing

Έστω E μια ελλειπτική καμπύλη υπέρ το σώμα K και έστω n ένας ακέραιος που δεν διαιρείται από την χαρακτηριστική του K. Τότε $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$. Έστω $\mu_n = \{x \in \overline{K} \mid x^n = 1\}$ η ομάδα των n-ριζών της μονάδας στο $\overline{K}$. Εφόσον η χαρακτηριστική του K δεν διαιρεί το n, η εξίσωση $x^n = 1$ δεν έχει ρίζες με πολλαπλότητα άρα έχει n ρίζες στο $\overline{K}$. Άρα η μ_n είναι κυκλική ομάδα τάξης n. Οποιοσδήποτε γεννήτορας ζ της μ_n ονομάζεται πρωταρχική n-ρίζα της μονάδος. Αυτό είναι ισοδύναμο με το να πούμε ότι $\zeta^k = 1$ ανν $n \mid k$.

Θεώρημα 2.6.1. *Έστω E μια ελλειπτική καμπύλη ορισμένη υπέρ το σώμα K και έστω n ένας θετικός ακέραιος. Υποθέτουμε ότι η χαρακτηριστική του K δεν διαιρεί το n. Τότε υπάρχει μια pairing $e_n : E[n] \times E[n] \to \mu_n$ που ονομάζεται Weil pairing και ικανοποιεί τις ακόλουθες ιδιότητες :*
1) Η e_n είναι διγραμμική ως προς κάθε μεταβλητή. Αυτό σημαίνει ότι $e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T)$ και $e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2)$ $\forall S, S_1, S_2, T, T_1, T_2 \in E[n]$.
2) Η e_n είναι μη ιδιάζουσα ως προς κάθε μεταβλητή. Άρα αν $e_n(S, T) = 1$ για κάθε $T \in E[n]$ τότε $S = \mathcal{O}$ και όμοια αν $e_n(S, T) = 1$ για κάθε

$S \in E[n]$ *τότε* $T = \mathcal{O}$.
3) $e_n(T, T) = 1$ *για κάθε* $T \in E[n]$.
4) $e_n(T, S) = e_n(S, T)^{-1}\ \forall S, T \in E[n]$.
5) $e_n(\sigma S, \sigma T) = \sigma(e_n(S, T))$ *για όλους τους αυτομορφισμούς* σ *του* $\overline{K}$ *που αφήνουν σταθερούς τους συντελεστές της* E.
6) $e_n(\alpha(S), \alpha(T)) = e_n(S, T)^{\deg(\alpha)}$ *για όλους τους διαχωρίσιμους ενδομορφισμούς* α *της* E. *(Αν οι συντελεστές της* E *ανήκουν σε ένα πεπερασμένο σώμα* $\mathbb{F}_q$ *τότε ο ισχυρισμός ισχύει και όταν ο* α *είναι ο ενδομορφισμός του Frobenius* ϕ_q*)*

Καθώς η απόδειξη του θεωρήματος απαιτεί πιο προχωρήμενα εργαλεία από αυτά που αναφέρουμαι εδώ δεν αποδεικνύουμε το θεώρημα. Μια απόδειξη του θεωρήματος δίνεται στο [2].

Πόρισμα 2.6.1. *Έστω* $\{T_1, T_2\}$ *μια βάση της* $E[n]$. *Τότε* $e_n(T_1, T_2)$ *είναι μια πρωταρχική* n*-ρίζα της μονάδας.*

Απόδειξη. Έστω $e_n(T_1, T_2) = \zeta$ με $\zeta^d = 1$. Τότε $e_n(T_1, dT_2) = \zeta^d = 1$. Επίσης $e_n(T_2, dT_2) = e_n(T_2, T_2)^d = 1$. Έστω $S \in E[n]$ τότε $S = aT_1 + bT_2$ για κάποιους $a, b \in \mathbb{Z}$. Οπότε $e_n(S, dT_2) = e_n(aT_1 + bT_2, dT_2) = e_n(aT_1, dT_2)e_n(bT_2, dT_2) = e_n(T_1, dT_2)^a e_n(T_2, dT_2)^b = 1$ Εφόσον αυτό ισχύει για κάθε S έπεται ότι $dT_2 = \mathcal{O}$. Αλλά τώρα $dT_2 = \mathcal{O}$ ανν $n \mid d$ το οποίο έπεται ότι το ζ είναι μια πρωταρχική n-ρίζα της μονάδας. □

Πόρισμα 2.6.2. *Αν* $E[n] \subseteq E(K)$ *τότε* $\mu_n \subset K$.

Απόδειξη. Έστω σ ένας αυτομορφισμός του $\overline{K}$ που αφήνει σταθερά τα στοιχεία του K. Έστω $\{T_1, T_2\}$ μια βάση της $E[n]$. Εφόσον τα T_1, T_2 έχει υποτεθεί ότι έχουν συντεταγμένες στο K έχουμε ότι $\sigma T_1 = T_1$ και $\sigma T_2 = T_2$ άρα $\zeta = e_n(T_1, T_2) = e_n(\sigma T_1, \sigma T_2) = \sigma(e_n(T_1, T_2)) = \sigma(\zeta)$ Από το Θεμελιώδες θεώρημα της θεωρίας Galois έχουμε ότι αν το $x \in \overline{K}$ μένει σταθερό από όλους αυτούς τους αυτομορφισμούς σ τότε x ανήκει σε μια πλήρως διαχωρίσιμη επέκταση του K. Αλλά μια n-ρίζα της μονάδας παράγει μια διαχωρίσιμη επέκταση του K όταν η χαρακτηρισική δεν διαιρεί το n άρα συμπεραίνουμε ότι $\zeta \in K$. Εφόσον τώρα το ζ είναι μια πρωταρχική n-ρίζα της μονάδας έπεται ότι $\mu_n \subset K$. □

Πόρισμα 2.6.3. *Έστω* E *μια ελλειπτική καμπύλη ορισμένη υπέρ το* $\mathbb{Q}$. *Τότε* $E[n] \nsubseteq E(\mathbb{Q})$ *για* $n \geq 3$.

Απόδειξη. Αν $E[n] \subseteq E(\mathbb{Q})$ έπεται $\mu_n \subset \mathbb{Q}$ το οποίο είναι άτοπο για $n \geq 3$. □

Παρατήρηση : Όταν $n = 2$ είναι δυνατόν να έχουμε $E[2] \subseteq E(\mathbb{Q})$. Για παράδειγμα αν E δίνεται από την εξίσωση $y^2 = x(x-1)(x+1)$ τότε $E[2] = \{\mathcal{O}, (0,\, 0),\, (1,\, 0),\, ,\, (-1,\, 0)\}$.
Αν $n = 3, 4, 5, 6, 7, 8, 9, 10, 12$ υπάρχουν ελλειπτικές καμπύλες $E\ |_{\mathbb{Q}}$ τέτοιες ώστε να έχουν σημεία τάξης n με ρητές συντεταγμένες. Το πόρισμα λέει ότι είναι αδύνατο όλα τα σημεία τάξης n να έχουν ρητές συντεταγμένες.

Πρόταση 2.6.1. *Έστω α ένας ενδομορφισμός μιας ελλειπτικής καμπύλης E ορισμένης υπέρ ενός σώματος K. Έστω n ένας θετικός ακέραιος που δεν διαιρείται από την χαρακτηριστική του K. Τότε* $det(\alpha_n) \equiv \deg(\alpha) \pmod{n}$

Απόδειξη. Έστω $T_1,\, T_2$ μια βάση της $E[n]$ τότε από το πόρισμα 2.6.1 έχουμε ότι το $e_n(T_1,\, T_2)$ είναι μια πρωταρχική n-ρίζα της μονάδας. Έστω $e_n(T_1,\, T_2) = \zeta$. Από την ιδιότητα 6 της e_n έχουμε,

$$\begin{aligned}
\zeta^{\deg(\alpha)} &= e_n(\alpha(T_1),\, \alpha(T_2)) \\
&= e_n(aT_1 + cT_2,\, bT_1 + dT_2) \\
&= e_n(aT_1,\, bT_1 + dT_2)e_n(cT_2,\, bT_1 + dT_2) \\
&= e_n(aT_1,\, bT_1)e_n(aT_1,\, dT_2)e_n(cT_2,\, bT_1)e_n(cT_2,\, dT_2) \\
&= e_n(T_1,\, T_1)^{ab}e_n(T_1,\, T_2)^{ad}e_n(T_2,\, T_1)^{cb}e_n(T_2,\, T_2)^{cd} \\
&= \zeta^{ad}\zeta^{-cb} = \zeta^{ad-bc}
\end{aligned}$$

από τις ιδιότητες της Weil pairing. Οπότε $\zeta^{\deg(\alpha)} = \zeta^{ad-bc}$ και αφού η ζ είναι μια πρωταρχική n-ρίζα της μονάδας $\deg(\alpha) \equiv ad - bc \pmod{n}$ Όμως,

$$\alpha_n = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

άρα $\deg(\alpha) \equiv det(\alpha_n) \pmod{n}$ □

Έστω α και β ενδομορφισμοί της E και έστω $a,\, b$ ακέραιοι. Ο ενδομορφισμός $a\alpha + b\beta$ ορίζεται από τη σχέση $(a\alpha + b\beta)(P) = a\alpha(P) + b\beta(P)$. Όπου $a\alpha(P)$ σημαίνει ότι πολλαπλασιάζουμε το $\alpha(P)$ με έναν ακέραιο a πάνω στην E. Το αποτέλεσμα προστίθεται στο $b\beta(P)$ πάνω στην E. Άρα όλη η διαδικασία μπορεί να περιγραφεί από ρητές συναρτήσεις αφού αυτό σημβαίνει και για τα επιμέρους βήματα. Άρα ο $a\alpha + b\beta$ είναι ένας ενδομορφισμός.

Πρόταση 2.6.2. *Ισχύει ότι* $\deg(a\alpha+b\beta) = a^2\deg(\alpha)+b^2\deg(\beta)+ab(\deg(\alpha+\beta) - \deg(\alpha) - \deg(\beta))$.

Απόδειξη. Έστω n ένας ακέραιος που δεν διαιρείται από την χαρακτηριστική του K. Αναπαριστούμε τους α και β από τους πίνακες α_n και β_n (ως προς κάποια βάση του $E[n]$). Τότε ο $a\alpha_n + b\beta_n$ μας δίνει τη δράση του $a\alpha + b\beta$ στην $E[n]$.
$det(a\alpha_n + b\beta_n) = a^2 det(\alpha_n) + b^2 det(\beta_n) + ab(\deg(\alpha_n + \beta_n) - det(\alpha_n) - det(\beta_n))$
Εφόσον αν,

$$\alpha_n = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix},\ \beta_n = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}$$

τότε έχουμε,

$$\begin{aligned} det(a\alpha_n + b\beta_n) &= (aa_1 + bb_1)(aa_4 + bb_4) - (aa_3 + bb_3)(aa_2 + bb_2) \\ &= a^2 a_1 a_4 + aba_1 b_4 + abb_1 a_4 + b^2 b_1 b_4 - \\ &\qquad a^2 a_2 a_3 - aba_3 b_2 - aba_2 b_3 - b^2 b_2 b_3 \\ &= a^2(a_1 a_4 - a_2 a_3) + b^2(b_1 b_4 - b_2 b_3) + ab(a_1 b_4 + b_1 a_4 - a_3 b_2 - a_2 b_3) \\ &= a^2 det(\alpha_n) + b^2 det(\beta_n) + ab(\deg(\alpha_n + \beta_n) - det(\alpha_n) - det(\beta_n)) \end{aligned}$$

Αυτό ισχύει για οποιαδήποτε α_n, β_n Άρα :

$$\deg(a\alpha + b\beta) \equiv a^2 \deg(\alpha) + b^2 \deg(\beta) + ab(\deg(\alpha + \beta) - \deg(\alpha) - \deg(\beta)) \pmod{n}$$

διότι $det(\alpha_n) \equiv \deg(\alpha) \pmod{n}$ και $det(\beta_n) \equiv 0 \deg(\beta) \pmod{n}$
Η ισοτιμία ισχύει όμως για άπειρα n άρα είναι ισότητα. □

2.7 Tate-Lichtenbaum Pairing

Θεώρημα 2.7.1. *Έστω E μια ελλειπτική καμπύλη υπέρ το $\mathbb{F}_q$. Έστω n ένας ακέραιος τ.ω. $n \mid q-1$. Με $E(\mathbb{F}_q)[n]$ δηλώνουμε τα στοιχεία της $E(\mathbb{F}_q)$ που έχουν τάξη που διαιρεί το n , και έστω $\mu_n = \{x \in \mathbb{F}_q \mid x^n = 1\}$. Έστω $P \in E(\mathbb{F}_q)[n]$ και $Q \in E(\mathbb{F}_q)$ και διαλέγουμε $R \in E(\overline{\mathbb{F}_q})$ τέτοιο ώστε $nR = Q$. Με e_n συμβολίζουμε τη n-οστη Weil pairing και με $\phi = \phi_q$ τον q-οστο ενδομορφισμό του Frobenius. Ορίζουμε*

$$\tau_n(P, Q) := e_n(P, R - \phi(R))$$

Ισχύει ότι η $\tau_n : E(\mathbb{F}_q)[n] \times E(\mathbb{F}_q)/nE(\mathbb{F}_q) \to \mu_n$ είναι μια καλώς ορισμένη μη-ιδιάζουσα διγραμμική pairing.

Η pairing του θεωρήματος λέγεται τροποποιημένη Tate-Lichtenbaum pairing. Η αρχική Tate-Lichtenbaum pairing δίνεται αν πάρουμε την n-οστη ρίζα της τ_n καταλήγοντας στην pairing

$< \cdot, \cdot >_n : E(\mathbb{F}_q)[n] \times E(\mathbb{F}_q)/nE(\mathbb{F}_q) \to {\mathbb{F}_q}^*/({\mathbb{F}_q}^*)^n$.
Το γεγονός ότι η τ_n είναι μη-ιδιάζουσα σημαίνει ότι αν $\tau_n(P,\, Q) = 1$ για κάθε Q τότε $P = \mathcal{O}$ και αν $\tau_n(P,\, Q) = 1$ για όλα τα P τότε $Q \in nE(\mathbb{F}_q)$.
Η διγραμμικότητα μας δίνει
$\tau_n(P_1 + P_2,\, Q) = \tau_n(P_1,\, Q)\tau_n(P_2,\, Q)$
$\tau_n(P,\, Q_1 + Q_2) = \tau_n(P,\, Q_1)\tau_n(P,\, Q_2)$

Απόδειξη. Αρχικά θα δείξουμε ότι το $\tau_n(P,\, Q)$ ορίζεται και είναι ανεξάρτητο του R. Εφόσον $nR = Q \in E(\mathbb{F}_q)$ έχουμε ότι $Q - \phi(Q) = \mathcal{O}$ διότι αν $Q = (x,\, y) \in E(\mathbb{F}_q)$ τότε $\phi(Q) = (x^q,\, y^q)$ όμως στο $\mathbb{F}_q$ $x^q = x$ και $y^q = y$. Άρα $\mathcal{O} = Q - \phi(Q) = n(R - \phi(R))$ οπότε $R - \phi(R) \in E[n]$. Εφόσον τώρα $P \in E[n]$ επίσης, η weil pairing $e_n(P,\, R - \phi(R))$ ορίζεται. Υποθέτουμε ότι $nR' = Q$ είναι μια άλλη επιλογή για το R. Έστω $T = R' - R$ τότε $nT = Q - Q = \mathcal{O}$. άρα $T \in E[n]$ οπότε

$$\begin{aligned} e_n(P,\, R' - \phi(R')) &= e_n(P,\, R - \phi(R) + T - \phi(T)) \\ &= e_n(P,\, R - \phi(R))e_n(P,\, T - \phi(T)) \\ &= e_n(P,\, R - \phi(R))e_n(P,\, T)e_n(P,\, \phi(T))^{-1} \end{aligned}$$

Αλλά $P = \phi(P)$ αφού $P \in E(\mathbb{F}_q)$ άρα $e_n(P,\, \phi(T)) = e_n(\phi(P),\, \phi(T)) = \phi(e_n(P,\, T)) = e_n(P,\, T)$ αφού $e_n(P,\, T) \in \mu_n \subset \mathbb{F}_q$ οπότε $e_n(P,\, R' - \phi(R')) = e_n(P,\, R - \phi(R))$. Οπότε η τ_n δεν εξαρτάται από την επιλογή του R.
Εφόσον το Q είναι ένας αντιπρόσωπος ενός συμπλόκου στην $E(\mathbb{F}_q)/nE(\mathbb{F}_q)$ πρέπει να δείξουμε ότι η τ_n εξαρτάται μόνο από το σύμπλοκο και όχι από μια συγκεκριμένη επιλογή αντιπροσώπου. Υποθέτουμε ότι $Q' - Q = nU \in E(\mathbb{F}_q)$. Έστω $nR = Q$ και έστω $R' = R + U$ τότε $nR' = Q'$ αφού $nR' = nR + nU = Q + nU = Q'$ οπότε,

$$\begin{aligned} \tau_n(P,\, Q') &= e_n(P,\, R' - \phi(R')) \\ &= e_n(P,\, R - \phi(R) + U - \phi(U)) \\ &= e_n(P,\, R - \phi(R)) = \tau_n(P,\, Q) \end{aligned}$$

εφόσον $U = \phi(U)$ για $U \in E(\mathbb{F}_q)$. Οπότε η τιμή της τ_n δεν εξαρτάται από την επιλογή του αντιπροσώπου. Αυτό ολοκληρώνει την απόδειξη ότι η τ_n είναι καλώς ορισμένη. Το γεγονός ότι η τ_n είναι διγραμμική στο P έπεται από το ότι η e_n είναι. Για τη διγραμμικότητα στο Q υποθέτουμε ότι $nR_1 = Q_1$ και $nR_2 = Q_2$ τότε $n(R_1 + R_2) = Q_1 + Q_2$ οπότε

$$\begin{aligned} \tau_n(P,\, Q_1 + Q_2) &= e_n(P,\, R_1 + R_2 - \phi(R_1 + R_2)) \\ &= e_n(P,\, R_1 + R_2 - \phi(R_1) - \phi(R_2)) \\ &= e_n(P,\, R_1 - \phi(R_1))e_n(P,\, R_2 - \phi(R_2)) \\ &= \tau_n(P,\, Q_1)\tau_n(P,\, Q_2) \end{aligned}$$

Μένει να αποδείξουμε ότι η τ_n είναι μη-ιδιάζουσα. Πρώτα ας δούμε όμως κάποια γενικά στοιχεία όσον αφορά τις pairings. Έστω $n \geq 1$ και έστω A και B δύο πεπερασμένες αβελιανές ομάδες (θεωρούμενες προσθετικά) τέτοιες ώστε $na = 0$ για όλα τα $a \in A$ και $nb = 0$ για όλα τα $b \in B$. Έστω $<,>: B \times A \to \mu_n$ μια διγραμμική pairing. Αν σταθεροποιήσουμε ένα $a \in A$ τότε

$$\psi_a : b \mapsto (b,\, a)$$

μας δίνει ένα ομομορφισμό από τη B στο μ_n. Με $Hom(B,\, \mu_n)$ θα δηλώνουμε το σύνολο όλων των ομομορφισμών από το B στο μ_n. Το $Hom(B,\, \mu_n)$ γίνεται ομάδα αν το εφοδιάσουμε με ένα γινόμενο των $\alpha, \beta \in Hom(B,\, \mu_n)$, $(\alpha, \beta)(b) = \alpha(b)\beta(b)$ για όλα τα $b \in B$.

Λήμμα 2.7.1. *Αν B μια πεπερασμένη αβελιανή ομάδα τέτοια ώστε $nb = 0$ για όλα τα $b \in B$, τότε $\#Hom(B,\, \mu_n) = \#B$.*

Απόδειξη. Αρχικά ας υποθέσουμε ότι $B = \mathbb{Z}_m$ με $m \mid n$. Αν $\alpha \in Hom(B,\, \mu_n)$ τότε $\alpha(1)^m = \alpha(1 + \cdots + 1) = \alpha(0) = 1$. Άρα το $\alpha(1)$ είναι ένα από τα m στοιχεία στην $\mu_m \subseteq \mu_n$. Όμως το 1 παράγει την $\mathbb{Z}_m$, άρα η τιμή του $\alpha(1)$ καθορίζει το $\alpha(b)$ για κάθε b. Επίσης κάθε επιλογή του $\alpha(1) \in \mu_n$ καθορίζει έναν καλώς ορισμένο ομομορφισμό με $b \mapsto \alpha(1)^b$. Οπότε υπάρχει μια αντιστοιχία 1-1 και επί από το $Hom(\mathbb{Z}_m,\, \mu_n)$ στο μ_m, οπότε $\#Hom(\mathbb{Z}_m,\, \mu_n) = m = \#B$.
Τώρα θεωρούμε μια τυχαία πεπερασμένη αβελιανή ομάδα B. Από το θεμελιώδες θεώρημα των πεπερασμένων αβελιανών ομάδων έχουμε $B \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_s}$. Εφόσον όμως $nb = 0$ για όλα τα $b \in B$, θα έχουμε ότι $m_i \mid n$ για όλα τα i. Υπάρχει μια απεικόνιση

$$\Phi : Hom(\mathbb{Z}_{m_1},\, \mu_n) \oplus \cdots \oplus Hom(\mathbb{Z}_{m_s},\, \mu_n) \to Hom(\mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_s},\, \mu_n)$$

όπου ο ισομορφισμός απεικονίζει την s-άδα $(\alpha_1,\, \alpha_2,\, \cdots, \alpha_s)$ στον ομομορφισμό που δίνεται από την $(b_1,\, b_2, \cdots, b_s) \mapsto \alpha_1(b_1)\alpha_2(b_2)\cdots\alpha_s(b_s)$. Η απεικόνιση $\alpha \mapsto (\alpha_1,\, \alpha_2,\, \cdots, \alpha_s)$ όπου $\alpha_i(b_i) = \alpha(0, \cdots, b_1, \cdots, 0)$ είναι η αντίστροφη της Φ άρα η Φ είναι 1-1.
Εφόσον τώρα η ομάδα $Hom(\mathbb{Z}_{m_1},\, \mu_n) \oplus \cdots \oplus Hom(\mathbb{Z}_{m_s},\, \mu_n)$ έχει τάξη $m_1 m_2 \cdots m_s = \#B$ τότε και η $Hom(\mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_s},\, \mu_n)$ έχει την ίδια τάξη. Αυτό μας δίνει το λήμμα. □

Το μέρος (β) του επόμενου λήμματος θα μας διευκολύνει να αποδείξουμε ότι η Tate-Lichtenbaum pairing είναι μη-ιδιάζουσα καθώς θα μας επιτρέψει να ανάγουμε την ιδιότητα από την μια μεταβλητή στην άλλη.

Λήμμα 2.7.2. *Υποθέτουμε ότι η pairing $<,>: B \times A \to \mu_n$ είναι μη-ιδιάζουσα στο A.*

α) Η απεικόνιση $A \mapsto Hom(B, \mu_n)$ που δίνεται από την $\alpha \mapsto \psi_\alpha$ είναι 1-1.
β) Αν $\#A = \#B$ τότε η pairing είναι επίσης μη-ιδιάζουσα στο B.

Απόδειξη. Υποθέτουμε ότι ψ_α είναι ο τετριμμένος ομομορφισμός. Αυτό σημαίνει ότι $< b, a >= \psi_a(b) = 1$ για όλα τα $b \in B$. Το γεγονός ότι η pairing είναι μη ιδιάζουσα στο A έπεται ότι $a = 0$. Αυτό αποδεικνύει το (α).
Έστω $B_1 = \{b \in B \mid < b, a >= 1 \text{ για κάθε } a \in A\}$. Τότε κάθε $a \in A$ δίνει έναν καλώς ορισμένο ομομορφισμό $\beta_a : B/B_1 \to \mu_n$ που δίνεται από $\beta_a(b \, mod \, B_1) =< b, a >$. Όντως αν $\beta_a(b_1) = \beta_a(b_2)$ τότε
$< b_1, a >=< b_2, a > \Rightarrow < b_1 - b_2, a >= 1$. Αυτό μας λέει όμως ότι $b_1 - b_2 = b \in B_1$ οπότε $b_1 \equiv b_2 \pmod{B_1}$. Αν β_a είναι ο τετριμμένος ομομορφισμός, τότε $< b, a >= 1$ για όλα τα $b \in B$, το οποίο σημαίνει ότι $a = 0$. Οπότε το Α εμφυτεύεται στο $Hom(B/B_1, \mu_n)$ το οποίο έχει τάξη $\#B/\#B_1$, από το λήμμα 2.7.1. Άρα $\#A \mid \#B/\#B_1$ και αφού $\#A = \#B$, θα έχουμε $\#B_1 = 1$. Αλλά $B_1 = \{0\}$ είναι ακριβώς αυτό που θέλουμε, άρα η pairing είναι μη-ιδιάζουσα. □

Ισχύει και το αντίστροφο του (β) στο λήμμα 2.7.2 .

Λήμμα 2.7.3. *Υποθέτουμε $<,>: B \times A \to \mu_n$ είναι μη-ιδιάζουσα και ως προς το A και ως προς το B. Τότε $\#A = \#B$. Συγκεκριμένα $A \cong Hom(B, \mu_n)$ και $B \cong Hom(A, \mu_n)$.*

Απόδειξη. Από το λήμμα 2.7.2 έχουμε μια εμφύτευση από το A στο $Hom(B, \mu_n)$, άρα $\#A \leq \#Hom(B, \mu_n) = \#B$. Αντιστρέφοντας τους ρόλους των A και B έχουμε $\#B \leq \#Hom(A, \mu_n) = \#A$. Οπότε $\#A = \#B$ και οι εμφυτεύσεις είναι ισομορφισμοί. □

Λήμμα 2.7.4. *Έστω M μια πεπερασμένη αβελιανή ομάδα και έστω $\alpha : M \to M$ ένας ομομορφισμός. Τότε $\#Ker(\alpha) = \#M/\#\alpha(M)$.*

Απόδειξη. Το λήμμα είναι άμεση συνέπεια του πρώτου θεωρήματος ισομορφισμών ομάδων. □

Το επόμενο λήμμα θα παίξει σημαντικό ρόλο στο να δείξουμε ότι η Tate-Lichtenbaum pairing είναι μη-ιδιάζουσα.

Λήμμα 2.7.5. *Έστω A και B πεπερασμένες αβελιανές ομάδες τέτοιες ώστε $nx = 0$ για όλα τα $x \in A$ και όλα τα $x \in B$. Υποθέτουμε ότι*

υπάρχει μια μη-ιδιάζουσα (ως προς και τις δυο μεταβλητές) διγραμμική pairing, $<,>: B \times A \to \mu_n$ *.Όπου* μ_n *είναι η ομάδα των n-ριζών της μονάδας (σε κάποιο σώμα). Έστω* C *μια υποομάδα της* B*. Ορίζουμε,*

$$\psi : A \longrightarrow \prod_{c \in C} \mu_n \qquad \textit{όπου} \quad a \mapsto (\cdots, < c, a >, \cdots)$$

Τότε $\#\psi(A) = \#C$*.*

Απόδειξη. Η pairing είναι μη-ιδιάζουσα άρα $A \cong Hom(B, \mu_n)$. Επίσης έχουμε $Ker(\psi) = \{a \in A \mid < c, a >= 1 \text{ για όλα τα } c \in C\}$. Ταυτίζοντας την A με το σύνολο των ομομορφισμών από B στο στο μ_n βλέπουμε ότι $Ker(\psi) = \{f \in Hom(B, \mu_n) \mid f(C) = 1\}$. Αλλά ένας ομομορφισμός που στέλνει το C στο 1 είναι ακριβώς το ίδιο με έναν ομομορφισμό από το B/C στο μ_n. Το σύνολο αυτών των ομομορφισμών έχει τάξη $\#(B/C) = \#B\#C$. Οπότε $\#\psi(A) = \#A/\#Ker(\psi) = \#A/\#(B/C) = \#C$, εφόσον $\#A = \#B$ από λήμμα 2.7.3. □

Τώρα εφαρμόζουμε τα παραπάνω σε μια ελλειπτική καμπύλη E. Έστω

$$\psi : E[n] \longrightarrow \prod_{P \in E(\mathbb{F}_q)[n]} \mu_n \qquad \text{όπου} \quad Q \mapsto (\cdots, e_n(P, Q), \cdots)$$

Λήμμα 2.7.6. *Έστω* $\phi = \phi_q$ *η q-δύναμη του ενδομορφισμού του Frobenius της* E*. Τότε* $Ker(\psi) = (\phi - 1)E[n]$*.*

Απόδειξη. Έστω $Q \in E[n]$. Τότε,

$$\begin{aligned}
\psi(\phi Q) &= (\cdots, e_n(P, \phi Q), \cdots) \\
&= (\cdots, e_n(\phi P, \phi Q), \cdots) && \text{εφόσον } \phi(P) = P \text{ για } P \in E(\mathbb{F}_q)[n] \\
&= (\cdots, e_n(P, Q)^{\deg(\phi)}, \cdots) \\
&= (\cdots, e_n(P, Q)^q, \cdots) && \text{επειδή } \deg(\phi) = q \quad \text{λήμμα 2.2.1} \\
&= (\cdots, e_n(P, Q), \cdots) && \text{επειδή } e_n(P, Q) \in \mu_n \subset \mathbb{F}_q \\
&= \psi(Q)
\end{aligned}$$

Οπότε $\psi((\phi - 1)Q) = 1$ άρα $(\phi - 1)E[n] \subseteq Ker(\psi)$. Από το λήμμα 2.7.5 με $A = B = E[n]$ και $C = E(\mathbb{F}_q)[n]$, έχουμε $\#\psi(E[n]) = \#E(\mathbb{F}_q)[n]$. Με $Ker(\phi - 1)|_{E[n]}$ δηλώνουμε τον πυρήνα του περιορισμού του $\phi - 1$ στο $E[n]$. Τότε,

$$\begin{aligned}
\#E(\mathbb{F}_q)[n] &= \#Ker(\phi - 1)|_{E[n]} && \text{εφόσον } Ker(\phi - 1) = E(\mathbb{F}_q) \\
&= \#E[n]/\#((\phi - 1)E[n]) && \text{από το λήμμα 2.7.4} \\
&\geq \#E[n]/\#(Ker(\psi)) && \text{εφόσον } (\phi - 1)E[n] \subseteq Ker(\psi) \\
&= \#\psi(E[n]) = \#E(\mathbb{F}_q)[n]
\end{aligned}$$

Οπότε πρέπει να έχουμε ισότητα παντού, συνεπώς

$$\#E[n]/\#((\phi-1)E[n]) = \#E[n]/\#(Ker(\psi))$$

. Αυτό σε συνδιασμό με το ότι $(\phi-1)E[n] \subseteq Ker(\psi)$ μας δίνει το αποτέλεσμα, $Ker(\psi) = (\phi-1)E[n]$. □

Τώρα είμαστε σε θέση να αποδείξουμε ότι η Tate-Lichtenbaum pairing είναι μη-ιδιάζουσα. Έστω $Q \in E(\mathbb{F}_q)$. Έχουμε $Q = nR$ με $R \in E(\overline{\mathbb{F}_q})$. Υποθέτουμε ότι $\tau_n(P, Q) = e_n(P, R-\phi R) = 1$ για όλα τα $P \in E(\mathbb{F}_q)[n]$. Τότε $R - \phi R \in Ker(\psi) = (\phi-1)E[n]$. Αυτό σημαίνει ότι υπάρχει ένα $T \in E[n]$ τ.ω. $R - \phi R = \phi T - T$ οπότε $\phi(R+T) = R+T$. Αφού τώρα τα σημεία που μένουν σταθερά από τον ενδομορφισμό ϕ έχουν συντεταγμένες που ανήκουν στο $\mathbb{F}_q$ (λήμμα 3.1.2) έπεται ότι $R+T \in E(\mathbb{F}_q)$. Άρα $Q = nR = n(R+T)$ το οποίο μας δίνει ότι $Q \in nE(\mathbb{F}_q)$. Οπότε η $E(\mathbb{F}_q)[n] \times E(\mathbb{F}_q)/nE(\mathbb{F}_q) \to \mu_n$ είναι μη ιδιάζουσα ως προς τη δεύτερη μεταβλητή. Όμως οι ομάδες $E(\mathbb{F}_q)[n]$ και $E(\mathbb{F}_q)/nE(\mathbb{F}_q)$ έχουν την ίδια τάξη (από το λήμμα 2.7.4 για $\alpha = n$) οπότε από το λήμμα 2.7.2 παίρνουμε ότι είναι μη-ιδιάζουσα και ως προς την πρώτη μεταβλητή. Αυτό ολοκληρώνει την απόδειξη.

□

Κεφάλαιο 3

Επίθεση εναντίον Κρυπτοσυστήματος με την Βοήθεια των Pairings

Ένα πρόβλημα πάνω στο οποίο βασίζεται η ασφάλεια αρκετών κρυπτοσυστημάτων (π.χ. El Gamal) είναι το πρόβλημα του διακριτού λογάριθμου. Αυτό μας καθιστά αναγκαίο να εξετάσουμε τι δυνατότητες έχουμε ενάντια στο πρόβλημα. Μια στρατηγική για να επιτεθούμε στο πρόβλημα του διακριτού λογάριθμου είναι να το ανάγουμε σε ένα ευκολότερο. Σ' αυτό το κεφάλαιο θα δούμε πως μπορούμε να το κάνουμε αυτό για το πρόβλημα του διακριτού λογάριθμου στην ομάδα $E(\mathbb{F}_q)$ δηλαδή στην ομάδα των ρητών σημείων μιας ελλειπτικής καμπύλης. Συγκεκριμένα θα δούμε πως μπορούμε να χρησιμοποιήσουμε τις Weil pairing και Tate-Lichtenbaum pairing που είδαμε στο προηγούμενο κεφάλαιο ώστε να ανάγουμε το πρόβλημα του διακριτού λογάριθμου από την ομάδα $E(\mathbb{F}_q)$ στην πολλαπλασιαστική ομάδα ενός σώματος.

3.1 Η Επίθεση MOV

Η πρώτη επίθεση που θα δούμε θα είναι η MOV που πήρε το όνομα της από τους Menezes, Okamoto και Vanstone. Η επίθεση αυτή χρησιμοποιεί την Weil pairing ώστε να ανάγει το πρόβλημα του διακριτού λογάριθμου από την ομάδα $E(\mathbb{F}_q)$ στην $\mathbb{F}_{q^m}^*$. Από τη στιγμή που το πρόβλημα του διακριτού λογάριθμου πάνω από ένα πεπεραμένο σώμα μπορεί να αντιμετωπισθεί από τον index calculus το πρόβλημα γίνεται αρκετά πιο εύκολο αν το m είναι αρκετά μικρό.

Έστω E μια ελλειπτική καμπύλη υπέρ το $\mathbb{F}_q$.Έστω ότι $P,\, Q \in E(\mathbb{F}_q)$. Έστω N η τάξη του P και υποθέτουμε ότι $MK\Delta(N,\, q) = 1$. Θέλουμε να βρούμε k τ.ω. $Q = kP$. Πρώτα όμως αξίζει να εξετάσουμε αν υπάρχει τέτοιο k .

Λήμμα 3.1.1. *Υπάρχει k τ.ω. $Q = kP$ ανν $NQ = \mathcal{O}$ και η Weil pairing $e_N(P,\, Q) = 1$*

Απόδειξη. Αν $Q = kP$ τότε $NQ = NkP = \mathcal{O}$ επίσης $e_N(P,\, Q) = e_N(P,\, kP) = e_N(P,\, P)^k = 1^k = 1$.
Αντίστροφα : Αν $NQ = \mathcal{O}$ τότε $NQ \in E[N]$. Εφόσον $MK\Delta(N,\, q) = 1$ έχουμε ότι $E[N] \cong \mathbb{Z}_N \oplus \mathbb{Z}_N$ από το θεώρημα 2.4.1. Επιλέγουμε ένα σημείο R τ.ω. το $\{P,\, R\}$ να είναι βάση του $E[N]$. Τότε $Q = aP + bR$ για κάποιους ακέραιους $a,\, b$. Από το πόρισμα της 2.6.1 έχουμε $e_N(P,\, R) = \zeta$ μια πρωταρχική N-ρίζα της μονάδας. Άρα αν $e_N(P,\, Q) = 1$ τότε έχουμε $1 = e_N(P,\, Q) = e_N(P,\, P)^a e_N(P,\, R)^b = \zeta^b$ αφού $Q = aP + bR$. Όμως τώρα έχουμε $1 = zeta^b \Rightarrow b \equiv 0 \pmod{N}$ άρα $bR = \mathcal{O}$ οπότε $Q = aP$. □

Η ιδέα που χρησιμοποιήσαμε για να αποδείξουμε το λήμμα μας δίνει την τακτική της επίθεση MOV για διακριτούς λογάριθμους σε ελλειπτικές καμπύλες. Επιλέγουμε m τ.ω. $E[N] \subseteq E(\mathbb{F}_{q^m})$. Εφόσον όλα τα σημεία του $E[N]$ έχουν συντεταγμένες στο $\overline{\mathbb{F}_q} = \bigcup_{j \geq 1} \mathbb{F}_{q^j}$ ένα τέτοιο m υπάρχει. Από το πόρισμα 2.6.2 η ομάδα μ_N των N-ριζών της μονάδας περιέχεται στο ${\mathbb{F}_q}^m$. Όλοι οι υπολογισμοί μας θα γίνονται στο $\mathbb{F}_{q^m}$. Ο αλγόριθμος είναι ο εξής :

Αλγόριθμος MOV :
Βήμα 1) Επιλέγουμε ένα τυχαίο σημείο $T \in E(\mathbb{F}_{q^m})$.
Βήμα 2) Υπολογίζουμε την τάξη M του T.
Βήμα 3)Έστω $d = MK\Delta(M,\, N)$ και έστω $T_1 = \left(\frac{M}{d}\right)T$. Τότε το T_1 έχει τάξη d η οποία διαιρεί το N έτσι $T_1 \in E[N]$.
Βήμα 4) Υπολογίζουμε $\zeta_1 = e_N(P,\, T_1)$ και $\zeta_2 = e_N(Q,\, T_1)$. Τότε και το ζ_1 και το ζ_2 ανήκουν στην $\mu_d \subseteq \mathbb{F}_{q^m}^*$.
Βήμα 5) Λύνουμε το πρόβλημα του διακριτού λογάριθμου $\zeta_2 = {\zeta_1}^k$ στο $\mathbb{F}_{q^m}^*$. Αυτό θα μας δώσει το $k \pmod{d'}$, όπου d' ένας διαιρέτης του d.
Βήμα 6) Επαναλαμβάνουμε με τυχαία σημεία T μέχρις ότου το ελάχιστο κοινό πολλαπλάσιο των d' να είναι N. Αυτό μας καθορίζει το $k \pmod{N}$.

Παρατήρηση : Αρχικά μπορεί να φαίνεται ότι η περίπτωση $d = 1$ θα συμβαίνει συχνά. Ωστόσο το αντίθετο είναι που συμβαίνει εξαιτίας της

δομής της $E(\mathbb{F}_{q^m})$. Θυμόμαστε ότι $E(\mathbb{F}_{q^m}) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ για κάποιους ακέραιους n_1, n_2 τ.ω. $n_1 \mid n_2$ (πιθανώς $n_1 = 1$ οπότε η ομάδα είναι κυκλική). Τότε $N \mid n_2$ αφού n_2 είναι η μεγαλύτερη πιθανή τάξη ενός στοιχείου στην ομάδα. Έστω B_1, B_2 σημεία τάξης n_1 και n_2 αντίστοιχα τ.ω. τα B_1, B_2 να παράγουν την $E(\mathbb{F}_{q^m})$. Τότε $T = a_1B_1 + a_2B_2$. Έστω l^e μια δύναμη πρώτου που διαιρεί το N. Τότε $l^f \mid n_2$ με $f \geq e$. Αν $l \nmid a_2$ τότε $l^f \mid M$ την τάξη του T. Οπότε $l^e \mid d = MK\Delta(M, N)$. Εφόσον η πιθανότητα του $l \nmid a_2$ είναι $1 - \frac{1}{l}$ η πιθανότητα είναι τουλάχιστον τόσο να είναι όλη η δύναμη l^e μέσα στο d. Μετά από μερικές επιλογές T αυτή θα είναι η περίπτωση. Άρα μερικές δοκιμές του αλγορίθμου θα μας δώσουν το k.

Πιθανώς ο ακέραιος m μπορεί να είναι μεγάλος, και σ' αυτή την περίπτωση το πρόβλημα του διακριτού λογάριθμου στην ομάδα $\mathbb{F}^*_{q^m}$ η οποία έχει τάξη $q^m - 1$ είναι εξίσου δύσκολο με το αρχικό πρόβλημα στην μικρότερη ομάδα $E(\mathbb{F}_{q^m})$, η οποία έχει τάξη περίπου q από το θεώρημα Hasse. [2]

Θεώρημα του Hasse. *Έστω E μια ελλειπτική καμπύλη ορισμένη πάνω από ένα πεπερασμένο σώμα $\mathbb{F}_q$. Τότε για την τάξη της $E(\mathbb{F}_q)$ ισχύει ότι*

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

Ωστόσο για υπεριδιάζουσες καμπύλες μπορούμε συνήθως να πάρουμε $m = 2$ όπως μας δείχνει το παρακάτω αποτέλεσμα. Έστω E ελλειπτική καμπύλη υπέρ το $\mathbb{F}_q$ όπου q είναι δύναμη πρώτου. Τότε $\#E(\mathbb{F}_q) = q + 1 - a$ για κάποιο a. Η καμπύλη E λέγεται υπεριδιάζουσα αν $a \equiv 0 \pmod{p}$ το οποίο είναι ισοδύναμο με $a = 0$ αν $q = p \geq 5$.
Πρώτα θα αποδείξουμε το παρακάτω θεώρημα που θα μας βοηθήσει στη συνέχεια.

Θεώρημα 3.1.1. *Έστω E μια ελλειπτική καμπύλη υπέρ το $\mathbb{F}_q$. Έστω $a = q+1-\#E(\mathbb{F}_q)$ τότε ${\phi_q}^2 - a\phi_q + q = 0$ ως ενδομορφισμός της E και a είναι ο μοναδικός ακέραιος k τ.ω. ${\phi_q}^2 - k\phi_q + q = 0$. Επίσης το a είναι ο μοναδικός ακέραιος που ικανοποιεί την $a \equiv Trace((\phi_q)_m) \pmod{m}$ για όλα τα m με $MK\Delta(m, q) = 1$.*

Απόδειξη. Αν ${\phi_q}^2 - a\phi_q + q$ δεν είναι ο μηδενικός ενδομορφισμός τότε ο πυρήνας του είναι πεπερασμένος ($\#Ker(\phi_q) \leq \deg(\phi_q)$). Θα δείξουμε ότι ο πυρήνας είναι άπειρος οπότε ο ενδομορφισμός είναι ο μηδενικός.

Έστω $m \geq 1$ ένας ακέραιος με $MK\Delta(m, q) = 1$. Ο ϕ_q μας δίνει ένα πίνακα $(\phi_q)_m$ που περιγράφει την δράση του ϕ_q στην $E[m]$. Έστω,

$$(\phi_q)_m = \begin{pmatrix} s & t \\ u & v \end{pmatrix}$$

Ο $\phi_q - 1$ είναι διαχωρίσιμος από πρόταση 2.2.3 αφού $p \nmid -1$. Άρα αφού είναι διαχωρίσιμος έχουμε $\#Ker(\phi_q - 1) = \deg(\phi_q - 1)$. Επίσης $\deg(\phi_q - 1) \equiv det((\phi_q)_m - I) = sv - tu - (s+v) + 1 \pmod m$. Τώρα για τον ϕ_q ισχύει $\deg(\phi_q \equiv det((\phi_q)_m) \pmod m$ άρα $q \equiv sv - tu \pmod m$. $\#Ker(\phi_q - 1) = q + 1 - a$ (από θεωρία) άρα $Trace((\phi_q)_m) = s + v \equiv a \pmod m$ αφού $q + 1 - a \equiv q - (s + v) + 1 \pmod m$. Από το θεώρημα Cayley-Hamilton στη γραμμική άλγεβρα έχουμε ${(\phi_q)_m}^2 - a(\phi_q)_m + qI \equiv O \pmod m$ (το $x^2 - ax + q$ είναι το χαρακτηριστικό πολυώνυμο του $(\phi_q)_m$). Αυτό σημαίνει ότι ο ενδομορφισμός ${\phi_q}^2 - a\phi_q + q$ είναι ταυτοτικά 0 στην $E[m]$. Εφόσον υπάρχουν άπειρα m, ο πυρήνας του ${\phi_q}^2 - a\phi_q + q$ είναι άπειρος άρα ο ενδομορφισμός είναι ο μηδενικός.
Υποθέτουμε ότι υπάρχει $a_1 \neq a$ που ικανοποιεί ${\phi_q}^2 - a\phi_q + q = 0$. Τότε $(a - a_1)\phi_q = ({\phi_q}^2 - a_1\phi_q + q) - ({\phi_q}^2 - a\phi_q + q) = \mathcal{O}$. Από θεώρημα 2.2.1 ο $\phi_q : E(\overline{\mathbb{F}_q}) \to E(\overline{\mathbb{F}_q})$ είναι επί. Άρα το $(a - a_1)$ εκμηδενίζει την $E(\overline{\mathbb{F}_q})$. Συγκεκριμένα το $(a - a_1)$ μηδενίζει την $E[m]$ για κάθε $m \geq 1$. Εφόσον υπάρχουν σημεία τάξης m στην $E[m]$ με $MK\Delta(m, q) = 1$ άρα βρίσκουμε ότι $a - a_1 \equiv 0 \pmod m$ για κάθε τέτοιο m άρα $a - a_1 = 0$. □

Πρόταση 3.1.1. *Έστω E ελλειπτική καμπύλη υπέρ το $\mathbb{F}_q$ και υποθέτουμε ότι $a = q + 1 - \#E(\mathbb{F}_q) = 0$. Έστω N ένας θετικός ακέραιος. Αν υπάρχει σημείο $P \in E(\mathbb{F}_q)$ τάξης N τότε $E[N] \subseteq E(\mathbb{F}_{q^2})$.*

Απόδειξη. Στην αρχή θα διατυπώσουμε και αποδείξουμε μια βοηθητική πρόταση και στη συνέχεια ακολουθεί η απόδειξη της πρότασης.

Λήμμα 3.1.2. *Έστω E ορισμένη υπέρ το $\mathbb{F}_q$ και έστω $(x, y) \in E(\overline{\mathbb{F}_q})$*
1) $\phi_q(x, y) \in E(\overline{\mathbb{F}_q})$
2) $(x, y) \in E(\mathbb{F}_q)$ *ανν* $\phi_q(x, y) = (x, y)$

Απόδειξη. Έχουμε $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ με $a_i \in \mathbb{F}_q$. Υψώνουμε στην q-δύναμη και έχουμε

$$(y^q)^2 + a_1x^qy^q + a_3y^q = (x^q)^3 + a_2(x^q)^2 + a_4x^q + a_6$$

άρα το (x^q, y^q) είναι πάνω στην E οπότε $\phi_q(x, y) \in E(\overline{\mathbb{F}_q})$. Άρα αποδείξαμε το (1). Για το (2) θυμόμαστε ότι $x \in \mathbb{F}_q$ ανν $\phi_q(x) = x$ και όμοια για το y. Άρα $(x, y) \in E(\mathbb{F}_q) \Leftrightarrow x, y \in \mathbb{F}_q \Leftrightarrow \phi_q(x) = x$ και $\phi_q(y) = y \Leftrightarrow \phi_q(x, y) = (x, y)$. □

Και τώρα η απόδειξη της πρότασης.
Ο ενδομορφισμός του Frobenius ϕ_q ικανοποιεί την σχέση ${\phi_q}^2 - a\phi_q + q = 0$ από το προηγούμενο θεώρημα, εφόσον $a = 0$ αυτό μας δίνει ${\phi_q}^2 = -q$. Έστω $S \in E[N]$, εφόσον $\#E(\mathbb{F}_q) = q + 1$ και υπάρχει ένα σημείο τάξης N έχουμε ότι $N \mid q + 1$ ή $-q \equiv 1 \pmod{N}$ οπότε $\phi_q(S)^2 = -qS = 1 \cdot s$. Από το προηγούμενο λήμμα $S \in E(\mathbb{F}_{q^2})$ αφού $\phi_{q^2}(S) = S$. □

Άρα συμπεραίνουμε ότι οι διακριτοί λογάριθμοι υπέρ το $\mathbb{F}_q$ για υπεριδιάζουσες καμπύλες με $a = 0$ μπορούν να αναχθούν σε διακριτούς λογάριθμους στο $\mathbb{F}^*_{q^2}$ οι οποίοι είναι πιο εύκολοι. Όταν η E είναι υπεριδιάζουσα αλλά $a \neq 0$ οι παραπάνω ιδέες δουλεύουν αλλά πιθανώς για $m = 3, 4$ ή 6 το οποίο είναι πάλι αρκετά καλό για να επιταχύνουμε τους υπολογισμούς του διακριτού λογάριθμου. Δεν είναι γνωστά παραδείγματα από τον πραγματικό κόσμο στα οποία να γίνετε η επίθεση μέσω του αλγόριθμου MOV. Ένα πρόβλημα είναι ότι μόλις ανακοινώθηκε η επίθεση με αυτή τη μέθοδο οι επιστήμονες σταμάτησαν να χρησιμοποιούν υπεριδιάζουσες (supersingular) καμπύλες στην κρυπτογραφία. Αυτό άλλαξε όταν η λεγόμενη identity-bas cryptography τους ανάγκασε να επιστρέψουν στο θέμα αλλά με πολύ μεγαλύτερους αριθμούς.

Τέλος ας δούμε ένα παράδειγμα όπου εφαρμόζεται ο αλγόριθμος MOV ώστε να τον κατανοήσουμε καλύτερα. Για το παράδειγμα θα χρησιμοποιήσουμε μια υπεριδιάζουσα ελλειπτική καμπύλη όπου το m που θα πρέπει να πάρουμε είναι 2.

Παράδειγμα : Έστω η ελλειπτική καμπύλη E που δίνεται από την εξίσωση $y^2 = x^3 + 6$ ορισμένη πάνω από το σώμα $\mathbb{F}_{761}$. Να λυθεί το πρόβλημα του διακριτού λογάριθμου $Q = kP$ όπου $P = (117, 690)$ και $Q = (564, 20)$. Τα $P, Q \in E(\mathbb{F}_{761})$, και η τάξη του P δίνεται ότι είναι 381 (για τους παρακάτω υπολογισμούς χρησιμοποιήθηκε το πρόγραμμα PARI GP).

Αρχικά εισάγουμε την καμπύλη μας στο πρόγραμμα με την εντολή ellinit([0,6], ffgen(ffinit(761, 2))).
Επιλέγουμε ένα τυχαίο σημείο $T_1 \in E(\mathbb{F}_{761^2})$ (Μπορούμε να πάρουμε ένα σημείο από την εντολή ellgroup(E, 761, 1)). Εδώ θα πάρουμε $T_1 = (36x + 272,\ 628x + 497)$
Υπολογίζουμε την τάξη του με την εντολή ellorder(E, T_1) και παίρνουμε ως αποτέλεσμα 127, άρα $M = 127$.
Τώρα $d = MK\Delta(127, 381) = 127$ οπότε $\frac{M}{d} = 1$ οπότε υπολογίζουμε τις

Weil pairing
$\zeta_1 = e_{381}(P,\, T_1)$ με την εντολή ellweilpairing(E, P, T_1, 381) και παίρνουμε $\zeta_1 = 219x + 602$
Όμοια $\zeta_2 = e_{381}(Q,\, T_1)$ και παίρνουμε $\zeta_2 = 687x + 318$.
Τώρα υπολογίζουμε την τάξη του ζ_1 η οποία είναι 127 και μπορούμε να την βρούμε με την εντολή fforder(ζ_1). Οπότε λύνουμε το πρόβλημα του διακριτού λογάριθμου $\zeta_2 = {\zeta_1}^k$ στην $\mathbb{F}^*_{761}$ και βρίσκουμε 5.
Άρα $k \equiv 5 \pmod{127}$. Αυτό μπορούμε να το κάνουμε με την εντολή fflog(ζ_2, ζ_1).

Επαναλαμβάνουμε την διαδικασία για διαφορετικό σημείο T_1 αυτή τη φορά. Επιλέγουμε $T_2 = (164x + 143,\, 26x + 518)$ με $M = ord(T_2) = 6$.
$d = MK\Delta(6, 381) = 3$ οπότε $T_3 = \frac{M}{d}T_2$ άρα $T_3 = 2T_2$. Τελικά παίρνουμε $T_3 = (99x + 99,\, 170)$.
Οπότε έχουμε $\zeta_1 = e_{381}(P,\, T_3) = x$ και $\zeta_2 = e_{381}(Q,\, T_3) = 1$ όπου $ord(\zeta_1) = 3$.
Λύνουμαι το πρόβλημα του διακριτού λογάριθμου και παίρνουμε $k \equiv 0 \pmod 3$.

Τώρα όμως ΕΚΠ(127, 3)=381 άρα είμαστε σε θέση να βρούμε το k αν λύσουμε το σύστημα

$$\begin{aligned} k &\equiv 5 \pmod{127} \\ k &\equiv 0 \pmod 3 \end{aligned}$$

Οπότε βρίσκουμε $k \equiv 132 \pmod{381}$ άρα $k = 132$.

3.2 Η Επίθεση Frey-Ruck

Η δεύτερη επίθεση που θα δούμε είναι αυτή των Frey και Ruck. Εδώ θα δούμε πάλι πως ανάγουμε το πρόβλημα του διακριτού λογάριθμου από την ομάδα $E(\mathbb{F}_q)$ στην $\mathbb{F}^*_{q^m}$. Εδω σε αντίθεση με την επίθεση MOV θα κάνουμε χρήση της Tate-Lichtenbaum pairing.

Λήμμα 3.2.1. *Έστω l πρώτος με $l \mid q-1, l \mid \#E(\mathbb{F}_q)$ και $l^2 \nmid \#E(\mathbb{F}_q)$. Έστω P ένας γεννήτορας της $E(\mathbb{F}_q)[l]$. Τότε $\tau_l(P,\, P)$ είναι μια πρωταρχική l-ρίζα της μονάδας.*

Απόδειξη. Αν $\tau_l(P,\, P) = 1$ τότε $\tau_l(uP,\, P) = 1^u = 1$ για όλα τα $u \in \mathbb{Z}$ και αφού τ_l μη-ιδιάζουσα $P \in lE(\mathbb{F}_q)$. Γράφουμε $P = lP_1$ τότε $l^2P_1 = lP = \mathcal{O}$.

Αφού $l^2 \nmid \#E(\mathbb{F}_q)$ δεν υπάρχουν σημεία τάξης l^2 άρα το P_1 έχει τάξη 1 ή l. Αν η τάξη του P_1 ήταν l τότε $\mathcal{O} = lP_1 = P$, αντίφαση. Άρα $\tau_l(P,\, P) \neq 1$ άρα είναι μια πρωταρχική l-ρίζα της μονάδας. □

Έστω $E(\mathbb{F}_q)$ και P όπως στο λήμμα και υποθέτουμε ότι $Q = kP$. Υπολογίζουμε $\tau_l(P,\, Q) = \tau_l(P,\, P)^k$. Αφού το $\tau_l(P,\, P)$ είναι μια πρωταρχική l-ρίζα της μονάδας αυτό καθορίζει το $k \pmod{l}$. Άρα έχουμε ανάγει το πρόβλημα του διακριτού λογάριθμου σε μια πολλαπλασιαστική ομάδα ενός πεπερασμένου σώματος $\mathbb{F}_q$. Τέτοιοι διακριτοί λογάριθμοι είναι συνήθως πιο εύκολο να λυθούν. Οπότε για να επιλέξουμε μια κατάσταση όπου το πρόβλημα του διακριτού λογάριθμου είναι δύσκολο, θα έπρεπε να επιλέξουμε μια κατάσταση όπου υπάρχει ένα σημείο τάξης l όπου l ένας μεγάλος πρώτος τ.ω. $l \nmid q - 1$. Για την ακρίβεια θέλουμε $q^m \not\equiv 1 \pmod{l}$ για μικρές τιμές του m.
Υποθέτουμε ότι η $E(\mathbb{F}_q)$ έχει ένα σημείο τάξης n αλλά $n \nmid q - 1$. Μπορούμε να επεκτείνουμε το σώμα μας στο $\mathbb{F}_{q^m}$ έτσι ώστε $n \mid q^m - 1$. Τότε η Tate-Lichtenbaum pairing μπορεί να χρησιμοποιηθεί. Ωστόσο η ακόλουθη πρόταση μας δείχνει ότι τουλάχιστον στην περίπτωση που το n είναι πρώτος μπορεί να χρησιμοποιηθεί και η Weil pairing.

Πρόταση 3.2.1. *Έστω E μια ελλειπτική καμπύλη υπέρ το $\mathbb{F}_q$. Έστω l ένας πρώτος τ.ω. $l \mid \#E(\mathbb{F}_q)$, $E[l] \nsubseteq E(\mathbb{F}_q)$, και $l \nmid q(q-1)$. Τότε $E[l] \subseteq E(\mathbb{F}_{q^m})$ αν και μόνο αν $q^m \equiv 1 \pmod{l}$.*

Απόδειξη. Αν $E[l] \subseteq E(\mathbb{F}_{q^m})$ τότε $\mu_l \subseteq \mathbb{F}_{q^m}$ από το πόρισμα 2.6.2 οπότε $q^m \equiv 1 \pmod{l}$.
Αντίστροφα, υποθέτουμε ότι $q^m \equiv 1 \pmod{l}$. Έστω $P \in E(\mathbb{F}_q)$ τάξης l και έστω $Q \in E[l]$ με $Q \notin E(\mathbb{F}_q)$. Ισχυριζόμαστε ότι τα P και Q είναι ανεξάρτητα σημεία τάξης l. Αν όχι τότε $uP = vQ$ για κάποιους ακέραιους $u,\, v \not\equiv 0 \pmod{l}$. Πολλαπλασιάζοντας με $v^{-1} \pmod{l}$ έχουμε $Q = V^{-1}uP \in E(\mathbb{F}_q)$ το οποίο είναι άτοπο. Άρα $\{P,\, Q\}$ είναι μια βάση της $E[l]$. Έστω ϕ_q ο ενδομορφισμός του Frobenius. Η δράση του ϕ_q στη βάση $\{P,\, Q\}$ του $E[l]$ μας δίνει ένα πίνακα $(\phi_q)_l$. Εφόσον $P \in E(\mathbb{F}_q)$ έχουμε ότι $\phi_q(P) = P$. Έστω $\phi_q(Q) = bP + dQ$ τότε,

$$(\phi_q)_l = \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}$$

Από το θεώρημα 3.1.1 γνωρίζουμε ότι $Trace((\phi_q)_l) \equiv a = q + 1 - \#E(\mathbb{F}_q) \pmod{l}$. Εφόσον $\#E(\mathbb{F}_q) \equiv 0 \pmod{l}$ εξ υποθέσεως έχουμε ότι $1 + d \equiv q + 1 \pmod{l} \Rightarrow d \equiv q \pmod{l}$. Με επαγωγή διαπιστώνουμε ότι,

$$\begin{pmatrix} 1 & b \\ 0 & q \end{pmatrix}^m = \begin{pmatrix} 1 & b\dfrac{q^m - 1}{q - 1} \\ 0 & q^m \end{pmatrix}$$

Εφόσον $q \not\equiv 1 \pmod{l}$ αφού $l \nmid q(q-1)$ εξ' υποθέσεως έχουμε ${\phi_q}^m = 1$ στην $E[l] \Leftrightarrow {(\phi_q)_l}^m \equiv I \pmod{l} \Leftrightarrow q^m \equiv 1 \pmod{l}$. Εφόσον $E[l] \subseteq E(\mathbb{F}_{q^m})$ ανν ${\phi_q}^m = 1$ στην $E[l]$ από λήμμα 3.1.2 αυτό αποδεικνύει την πρόταση. □

Αν έχουμε $E[n] \subseteq E(\mathbb{F}_{q^m})$ τότε μπορούμε να χρησιμοποιήσουμε την επίθεση MOV ή μπορούμε να χρησιμοποιήσουμε την Tate-Lichtenbaum pairing για να ανάγουμε το πρόβλημα του διακριτού λογάριθμου της $E(\mathbb{F}_{q^m})$ σε συτό της $\mathbb{F}^*_{q^m}$. Η Tate-Lichtenbaum pairing είναι γενικώς πιο γρήγορη. Και στις δύο περιπτώσεις επιλέγουμε τυχαία σημεία R και υπολογίζουμε τις pairings με P και kP. Με μεγάλη πιθανότητα παίρνουμε το k μόνο με λίγες τιμές του R.

Κεφάλαιο 4

Αντιμετωπίζοντας την περίπτωση gcd=N στον αλγόριθμο p-1

Εισαγωγή

Ας υποθέσουμε ότι έχουμε έναν ακέραιο N τον οποίο επιθυμούμε να παραγοντοποιήσουμε. Από εδώ και πέρα ο αριθμός N θα θεωρούμε ότι είναι γινόμενο δυο διαφορετικών πρώτων $N = p \cdot q$. Ο αλγόριθμος $p-1$ [1] είναι ο εξής:
Βήμα 1) Επιλέγουμε έναν ακέραιο B.
Βήμα 2) Επιλέγουμε έναν ακέραιο a τέτοιο ώστε $MK\Delta(a,\, N) = 1$ και υπολογίζουμε το $x \equiv a^m - 1 \pmod N$ και το $g = MK\Delta(x, N)$ όπου m = ΕΚΠ(1, 2, ..., B).
Βήμα 3) Αν $g \neq 1$ και $g \neq N$ τότε βρήκαμε έναν παράγοντα του N οπότε ο αλγόριθμος τερματίζει. Αλλιώς δοκιμάζουμε διαφορετικές τιμές για το a και το B.

Στον αλγόριθμο p-1 του Pollard λοιπόν υπάρχουν τρεις πιθανές περιπτώσεις για κάθε επανάληψη. Η καλύτερη είναι αυτή στην οποία θα πάρουμε έναν μη-τετριμμένο παράγοντα του αριθμού N που προσπαθούμε να παραγοντοποιήσουμε, δηλαδή $MK\Delta(a^m - 1, N) = p$. Η χειρότερη περίπτωση είναι αυτή που μας δίνει $MK\Delta(a^m-1, N) = 1$ καθώς δεν παίρνουμε καμία πληροφορία για την παραγοντοποίηση του N. Ωστόσο όμως έχουμε και μια τρίτη περίπτωση στην οποία $MK\Delta(a^m-1, N) = N$. Αυτή η σχέση μας δίνει κάποιες πληροφορίες για την παραγοντοποίηση του N αλλά όχι την ίδια την παραγοντοποίηση. Το ερώτημα που τίθεται

τώρα, είναι αν μπορούμε να χρησιμοποιήσουμε αυτές τις πληροφορίες για να βρούμε τελικά την παραγοντοποίηση. Η απάντηση είναι ναι σε σχεδόν όλες τις περιπτώσεις. Ωστόσο ο τρόπος με τον οποίο γίνετε αυτό μέχρι τώρα είναι ότι αλλάζουμε τυχαία τις παραμέτρους a και B και κατά πάσα πιθανότητα θα οδηγηθούμε σε αποτέλεσμα. Ο σκοπός μας είναι να δείξουμε ότι υπάρχει ένας εξίσου γρήγορος αλλά πιο αποτελεσματικός τρόπος για να γίνει αυτό.

4.1 Η ιδέα πίσω απ' τον αλγόριθμο

Έστω $N = p \cdot q$ το γινόμενο δυο διαφορετικών πρώτων. Υποθέτουμε ότι καθώς χρησιμοποιούσαμε τον αλγόριθμο p-1 για να παραγοντοποιήσουμε το N βρήκαμε a και B τ.ω. $MK\Delta(a^m - 1, N) = N$ όπου m = ΕΚΠ(1, 2, ..., B). Τότε μπορούμε να παραγοντοποιήσουμε το N δεδομένου ότι $ord_p(\alpha) \neq ord_q(\alpha)$ (θα μελετήσουμε αυτόν τον περιορισμό αργότερα) χρησιμοποιώντας τον παρακάτω αλγόριθμο (για τον τελικό αλγόριθμο που θα δώσουμε αυτό είναι μόνο το πρώτο μερος).

Αλγόριθμος (Μέρος 1) : Για κάθε πρώτο r_i μικρότερο του B κάνουμε τα ακόλουθα μέχρι να βρούμε έναν μη-τετριμμένο παράγοντα του N :

Θέτουμε $U = [log_{r_i} B]$ και L=0. Όσο $U \geqslant L$ θέτουμε $M = \left[\frac{U+L}{2}\right]$ και $m_i = {r_i}^M \prod_{1 \leq j \leq \pi(B)} {r_j}^{a_j}$ με $j \neq i$ και $a_j = [log_{r_j} B]$
$x \equiv a^{m_i} - 1 \pmod{N}$
$g = MK\Delta(x, N)$
Αν g=N τότε $U = \left[\frac{U+L}{2}\right] - 1$
Αν g=1 τότε $L = \left[\frac{U+L}{2}\right] + 1$
Αλλιώς τύπωσε το g και τερμάτισε.

Απόδειξη
Αρχικά θα αποδείξουμε ότι υπάρχει ένας διαιρέτης του m, έστω k τ.ω. $1 < MK\Delta(a^k - 1, N) < N$. Αφού $MK\Delta(a^m - 1, N) = N$ έπεται ότι $ord_p(a)|m$ και $ord_q(a)|m$. Έστω $\gamma = ord_p(a), \delta = ord_q(a)$ και ότι $m = r_1^{a_1} \cdot r_2^{a_2} \cdot \ldots \cdot r_s^{a_s}$ είναι η παραγοντοποίηση του m σε πρώτους. Τότε $W_{r_i}(\gamma) \leq W_{r_i}(m)$ και $W_{r_i}(\delta) \leq W_{r_i}(m) \, \forall i = 1, 2, \ldots, s$. Εφόσον $\gamma \neq \delta$ μπορούμε να υποθέσουμε ότι $\gamma < \delta$ άρα υπάρχει ένας πρώτος που διαιρεί το m, έστω r_j τ.ω. $W_{r_j}(\gamma) < W_{r_j}(\delta)$. Θεωρούμε τον αριθμό $k = r_i^{\ell} \cdot \prod_{1 \leq i \leq s} {r_i}^{a_i}$ με $i \neq j$ και το ℓ να ικανοποιεί $W_{r_j}(\gamma) \leq \ell < W_{r_j}(\delta)$. Μπορούμε να

δείξουμε ότι $gcd(a^k - 1, N) = p$ αφού $\gamma | k$ αλλά $\delta \nmid k$
Τώρα θα δείξουμε ότι ο παραπάνω αλγόριθμος βρίσκει έναν τέτοιο διαιρέτη του m. Από την παραπάνω απόδειξη μπορούμε να συμπεράνουμε ότι αρκεί να μειώσουμε τον εκθέτη ενός πρώτου $r_j \mid m$ τ.ω. $W_{r_j}(\gamma) \leq \ell < W_{r_j}(\delta)$ το οποίο σημαίνει ότι $gcd(r_j^\ell, \gamma) \geq r_j^{W_{r_j}(\gamma)}$ και $gcd(r_j^\ell, \delta) < r_j^{W_{r_j}(\delta)}$.

Έστω $m = m' \cdot r_j^t$ με $gcd(m', r_j) = 1$ για κάποιο $r_j \mid m$. Έστω $m_1 = m' \cdot r_j^{t_1}$ με $t_1 < t$. Μπορούμε να αποδείξουμε ότι :
1) Αν $MK\Delta(a^{m_1} - 1, N) = N$ τότε $\ell < t_1$
2)Αν $MK\Delta(a^{m_1} - 1, N) = 1$ τότε $\ell > t_1$

Αυτό μας δίνει την δυνατότητα να εφαρμόσουμε μια δυαδική αναζήτηση στο σύνολο $\{0, 1, \ldots, W_{r_j}(m)\}$ ώστε να βρούμε το ℓ. Αυτό είναι που κάνει ουσιαστικά ο αλγόριθμος, μια δυαδική αναζήτηση πολλές φορές.

4.2 Βελτιώνοντας τον αλγόριθμο

Στον αλγόριθμο που έχουμε περιγράψει ως τώρα μερικές φορές "ελέγχουμε" εκθέτες για πρώτους $r_i \mid m$ αλλά $r_i \nmid \gamma$ και $r_i \nmid \delta$. Για παράδειγμα αν έχουμε $N = 29 \cdot 53 = 1537$ και έχουμε επιλέξει $\alpha = 2, B = 20$ τότε $m = EK\Pi(1, 2, \ldots, 20) = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$ και $ord_{29}(2) = 28, ord_{53}(2) = 52$. Έστω $m_1 = 2^4 \cdot 3^1 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$ και $m_2 = 2^4 \cdot 3^0 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$ τότε $MK\Delta(a^{m_1} - 1, N) = N$ και $MK\Delta(a^{m_2} - 1, N) = N$.
Το πρόβλημα είναι ότι όσο κι αν αλλάξουμε τον εκθέτη του 3 δεν θα πάρουμε κάποιον παράγοντα του N αφού $3 \nmid ord_{29}(2)$ και $3 \nmid ord_{53}(2)$.

Άρα θέλουμε να είμαστε σε θέση να βρίσκουμε πρώτους r_i με $r_i \mid m$ και $r_i \mid \gamma$ ή $r_i \mid \delta$ έτσι ώστε να μην χρειάζεται να ελέγξουμε εκθέτες για κάθε πρώτο μικρότερο του B μέχρι να πάρουμε αποτέλεσμα. Για να το κάνουμε αυτό θα χρησιμοποιήσουμε πάλι την ιδέα της δυαδικής αναζήτησης. Πάλι υποθέτουμε ότι έχουμε βρεί a και B τ.ω. $MK\Delta(a^m - 1, N) = N$ όπου m = ΕΚΠ(1, 2, ..., B). Επίσης υποθέτουμε ότι $ord_p(\alpha) \neq ord_q(\alpha)$. Έστω $m = r_1^{a_1} \cdot r_2^{a_2} \cdot \ldots r_s^{a_s}$ η παραγοντοποίηση του m σε πρώτους και $m_1 = r_1^{a_1} \cdot r_2^{a_2} \cdot \ldots r_k^{a_k}$ με $k < s$.

Μπορούμε να δείξουμε ότι αν $MK\Delta(a^{m_1}-1,N)=N$ τότε $\forall r_i$ πρώτο με $k<i\leq s$ ισχύει $r_i \nmid \gamma$ και $r_i \nmid \delta$.
Επίσης αν $MK\Delta(a^{m_1}-1,N)=1$ τότε υπάρχουν r_{i_0}, r_{i_1} πρώτοι τ.ω. $r_{i_0} \mid \gamma$ και $r_{i_1} \mid \delta$ $k<i_0,i_1\leq s$.

Αυτό μας δίνει την ικανότητα να εφαρμόσουμε μια δυαδική αναζήτηση στο σύνολο $\{1,2,\ldots,s\}$ έτσι ώστε να βρούμε ένα j τ.ω. $r_j \mid \gamma$ ή $r_j \mid \delta$. Έτσι παίρνουμε τον παρακάτω αλγόριθμο :

Αλγόριθμος (Μέρος 2) : Θέτουμε U=s ,L=1 ,maxp=s. Όσο $U \geq L$ θέτουμε $k=\left[\frac{U+L}{2}\right]$ και $m_k=\prod_{i=1}^{k} r_i^{a_i}$ όπου $a_i=W_{r_i}(m)$
$x \equiv a^{m_k}-1 \pmod N$
$g=MK\Delta(x,N)$
Αν g=N τότε θέτουμε U=k-1 , maxp=k
Αν g=1 τότε L=k+1
Αλλιώς τύπωσε το g, τερματισμός.

Όταν αυτός ο αλγόριθμος θα έχει τερματίσει είτε θα έχουμε βρεί έναν μη-τετριμμένο παράγοντα του N, είτε η μεταβλητή maxp θα είναι ίση με τη "θέση" του του μεγαλύτερου πρώτου r_i που διαιρεί είτε το γ είτε δ στο σύνολο $\{r_1,r_2,\ldots,r_s\}$. Έπειτα θα αναλάβει δράση ο πρώτος αλγόριθμος που περιγράψαμε ώστε να τροποποιήσει τον εκθέτη αυτού του πρώτου.
Έστω maxp=k, αν είμαστε στην περίπτωση όπου $W_{r_k}(\gamma)=W_{r_k}(\delta)$ θα πρέπει να βρούμε έναν άλλο πρώτο r_{i_0} τ.ω. $r_{i_0} \mid \gamma$ ή $r_{i_0} \mid \delta$ καθώς ο πρώτος αλγόριθμος δεν θα καταφέρει να βρεί έναν μη-τετριμμένο παράγοντα του N. Καθώς δεν μπορούμε να χρησιμοποιήσουμε τον αλγόριθμο που περιγράψαμε παραπάνω με τις ίδιες παραμέτρους για να βρούμε έναν πρώτο αφού θα πάρουμε πάλι το ίδιο αποτέλεσμα, κάνουμε την εξής αλλαγή :
Θέτουμε $a' \equiv a^{r_k^{W_{r_k}(m)}} \pmod N$ και $m'=r_1^{a_1}\cdot r_2^{a_2}\cdot \ldots \cdot r_k^{a_k}$ άρα $s'=k$. Και τώρα εφαρμόζουμε τον αλγόριθμο. Αυτή τη φορά δεν θα πάρουμε ως αποτέλεσμα τον ίδιο πρώτο r_k αφού $ord_p(\alpha')=ord_p\left(a^{r_k^{W_{r_k}(m)}}\right)=\frac{\gamma}{MK\Delta\left(\gamma,r_k^{W_{r_k}(m)}\right)}=\frac{\gamma}{r_k^{W_{r_k}(\gamma)}}$ οπότε $r_k \nmid ord_p(\alpha')$. Το ίδιο ιχύει και για το q.

Παράδειγμα : Έστω p=43, q=127 οπότε N=5461. Υποθέτουμε ότι έχουμε επιλέξει a=2 και B=20.

Θα δείξουμε τί θα κάνει ο αλγόριθμος (Μερος 1 και 2 συνδιασμένα) ώστε να παραγοντοποιήσει το N. Έχουμε ότι m=ΕΚΠ(1,2,...,20)=$2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$ $\gamma = ord_{43}(2) = 14$ και $\delta = ord_{127}(2) = 7$. Είμαστε στην περίπτωση όπου $gcd(2^m - 1, 5461) = 5461$.

$$gcd(2^m - 1, 5461) = 5461 \qquad U = 8, L = 1, maxp = 8$$

$$\begin{array}{lll} m_1 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 & gcd(2^{m_1} - 1, 5461) = 5461 & U = 3, L = 1, maxp = 4 \\ m_2 = 2^4 \cdot 3^2 & gcd(2^{m_2} - 1, 5461) = 1 & U = 3, L = 3, maxp = 4 \\ m_3 = 2^4 \cdot 3^2 \cdot 5 & gcd(2^{m_3} - 1, 5461) = 1 & U = 3, L = 4, maxp = 4 \end{array}$$

(Από τους παραπάνω υπολογισμούς ο αλγόριθμος που θεωρήσαμε ως μέρος 2 μας δίνει την πληροφορία ότι το 7 διαιρεί είτε το $\gamma = ord_p(\alpha)$ είτε το $\delta = ord_q(\alpha)$. Τώρα το μέρος 1 του αλγόριθμου αναλαμβάνει δράση)

$$U = 1,\ L = 0$$

$$\begin{array}{lll} m_4 = 2^4 \cdot 3^2 \cdot 5 \cdot 7^0 & gcd(2^{m_4} - 1, 5461) = 1 & U = 1, L = 1 \\ m_5 = 2^4 \cdot 3^2 \cdot 5 \cdot 7^1 & gcd(2^{m_5} - 1, 5461) = 5461 & U = 0, L = 1 \end{array}$$

Και τωρα το ενδιάμεσο βήμα όπου αλλάζουμε α :
$\alpha' \equiv 2^7 (mod\ 5461) \Rightarrow \alpha' \equiv 128 (mod\ 5461)$

$$\begin{array}{lll} m_6 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 & gcd(128^{m_6} - 1, 5461) = 5461 & U = 4, L = 1, maxp = 4 \\ m_7 = 2^4 \cdot 3^2 & gcd(128^{m_7} - 1, 5461) = 5461 & U = 1, L = 1, maxp = 2 \\ m_8 = 2^4 & gcd(128^{m_8} - 1, 5461) = 5461 & U = 0, L = 1, maxp = 1 \end{array}$$

$$U = 4,\ L = 0$$

$$\begin{array}{lll} m_9 = 2^2 & gcd(128^{m_9} - 1, 5461) = 5461 & U = 1, L = 0 \\ m_{10} = 2^0 & gcd(128^{m_{10}} - 1, 5461) = 127 & \end{array}$$

Οπότε βρήκαμε έναν παράγοντα!

4.3 Μελετώντας τον περιορισμό $ord_p(\alpha) \neq ord_q(\alpha)$

Έστω p, q πρώτοι με $N = p \cdot q$. Θέλουμε να βρούμε πόσα α υπάρχουν στο $\mathbb{Z}/N\mathbb{Z}$ με την ιδιότητα $ord_p(\alpha) = ord_q(\alpha)$. Έστω $ord_p(\alpha) = ord_q(\alpha) = \gamma$ τότε αφού το γ είναι τάξη ενός στοιχείου στο $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ αυτό σημαίνει ότι $\gamma \mid p-1$, και όμοια $\gamma \mid q-1$ άρα η μεγαλύτερη δυνατή τιμή του γ θα είναι $MK\Delta(p-1, q-1)$. Είναι γνωστό ότι αν το γ είναι διαιρέτης του $p-1$ τότε υπάρχουν ακριβώς $\phi(\gamma)$ στοιχεία τάξης γ.
Έχουμε ότι $\gamma \mid p-1$ και $\gamma \mid q-1$. Αυτό έπεται ότι υπάρχουν ακριβώς $\phi(\gamma)$ στοιχεία τάξης γ στο $\mathbb{Z}/p\mathbb{Z}$ και άλλα $\phi(\gamma)$ στοιχεία τάξης γ στο $\mathbb{Z}/q\mathbb{Z}$. Έστω x_1 ένα στοιχείο τάξης γ στο $\mathbb{Z}/p\mathbb{Z}$ και x_2 ένα στοιχείο τάξης γ στο $\mathbb{Z}/q\mathbb{Z}$. Από το κινέζικο θεώρημα υπολοίπων έπεται ότι υπάρχει ένα $x_0 \in \mathbb{Z}/N\mathbb{Z}$ τ.ω. $x_0 \equiv x_1 \pmod{p}$ και $x_0 \equiv x_2 \pmod{q}$. Αλλά έχουμε $\phi(\gamma)$ επιλογές για το x_1 και άλλες $\phi(\gamma)$ επιλογές για το x_2. Άρα από στοιχειώδη θεωρία αριθμών συμπεραίνουμε ότι υπάρχουν ακριβώς $\phi(\gamma) \cdot \phi(\gamma)$ στοιχεία στο $\mathbb{Z}/N\mathbb{Z}$ που ικανοποιούν την συνθήκη $ord_p(\alpha) = ord_q(\alpha) = \gamma$. Εφόσον το γ μπορεί να είναι οποιοσδήποτε διαιρέτης του $MK\Delta(p-1, q-1)$ έπεται ότι το πλήθος των $\alpha \in \mathbb{Z}/N\mathbb{Z}$ που έχουν την ιδιότητα $ord_p(\alpha) = ord_q(\alpha)$ είναι

$$\sum_{\gamma \mid d} [\phi(\gamma)]^2 \quad \text{where} \quad d = MK\Delta(p-1, q-1)$$

Θέτουμε $\Delta(n) = \sum_{\gamma \mid n} [\phi(\gamma)]^2$ και θα μελετήσουμε λίγο αυτή τη συνάρτηση. Ξέρουμε ότι η $\phi(n)$ είναι πολλαπλασιαστική συνάρτηση άρα και η $[\phi(n)]^2$ θα είναι πολλαπλασιαστική. Από μια γνωστή πρόταση στη θεωρία αριθμών αν η συνάρτηση $f(n)$ είναι πολλαπλασιαστική τότε και η $F = \sum_{d \mid n} f(n)$ είναι επίσης πολλαπλασιαστική. Αυτό μας δίνει ότι η $\Delta(n)$ είναι πολλαπλασιαστική. Έστω $n = {p_1}^{a_1} \cdot {p_2}^{a_2} \cdot \ldots \cdot {p_s}^{a_s}$ τότε $\Delta(n) = \Delta({p_1}^{a_1}) \cdot \Delta({p_2}^{a_2}) \cdot \ldots \cdot \Delta({p_s}^{a_s})$. Υπολογίζουμε το $\Delta({p_i}^{a_i}) = \sum_{\gamma \mid {p_i}^{a_i}} [\phi(\gamma)]^2$. $\sum_{\gamma \mid {p_i}^{a_i}} [\phi(\gamma)]^2 = \sum_{k=0}^{a_i} [\phi({p_i}^k)]^2 = 1 + \sum_{k=1}^{a_i} [{p_i}^{k-1}(p_i - 1)]^2 = \ldots = \frac{1}{p_i + 1}\left[2 + (p_i - 1) \cdot {p_i}^{2a_i}\right]$. Τελικά

$$\Delta(n) = \prod_{i=1}^{s} \frac{1}{p_i + 1}\left[2 + (p_i - 1) \cdot {p_i}^{2a_i}\right]$$

Αλλά στον αλγόριθμο p-1 δεν επιλέγουμε ποτέ το $\alpha = 1$ ή το $\alpha = N - 1$ τα οποία είναι τα στοιχεία κοινής τάξης 1 και 2 αντίστοιχα (στο $\mathbb{Z}/p\mathbb{Z}$

και $\mathbb{Z}/q\mathbb{Z}$). Οπότε το πλήθος των $\alpha \in \mathbb{Z}/N\mathbb{Z}$ για τα οποία δεν θα δουλέψει ο αλγόριθμος μας είναι $\Delta(MK\Delta(p-1, q-1)) - 2$. Ωστόσο από τον τύπο που βγάλαμε για το $\Delta(n)$ μπορούμε να συμπεράνουμε ότι αν τα $p-1$ και $q-1$ δεν έχουν κάποιον μεγάλο κοινό πρώτο διαιρέτη (το οποίο είναι το σύνηθες) τότε ο $MK\Delta(p-1, q-1)$ δεν θα έχει κάποιο μεγάλο πρώτο διαιρέτη άρα το $\Delta(MK\Delta(p-1, q-1))$ θα είναι μικρό.

4.4 Εξετάζοντας την δύναμη του αλγόριθμου

Μέχρι τώρα έχουμε αποδείξει ότι ο αλγόριθμος μας δουλεύει και είδαμε και ένα παράδειγμα. Το ερώτημα που προκύπτει είναι τι ακριβώς προσθέτει ο αλγόριθμός μας στον αρχικό αλγόριθμο p-1. Με άλλα λόγια πόσο συχνά παίρνουμε την περίπτωση $MK\Delta = N$. Καθώς το N μεγαλώνει η περίπτωση αυτή εμφανίζεται όλο και πιο σπάνια (δεδομένου ότι έχουμε κάποιο λογικό όριο για το B). Για παράδειγμα αν πάρουμε $B = 10^6$ και το N να είναι περίπου 10^{40} δεν θα πάρουμε σχεδόν ποτέ την περίπτωση $MK\Delta = N$. Ωστόσο για μικρότερα N μπορούμε να δούμε ότι ο αλγόριθμος μας αρχίζει να δίνει αποτελέσματα σε περιπτώσεις όπου η κλασική μέθοδος αποτυγχάνει.

Χρησημοποιήσαμε μια γεννήτρια τυχαίων πρώτων για να βρούμε πρώτους p , q ώστε να σχηματίσουμε μερικά N και να δοκιμάσουμε τον αλγόριθμό μας. Σχηματίσαμε 20 N με περίπου 22 δεκαδικά ψηφία το καθένα και προσπαθήσαμε να τα παραγοντοποιήσουμε. Τα αποτελέσματα ήταν τα ακόλουθα : Δεκαέξι από αυτά παραγοντοποιήθηκαν από την κλασική μέθοδο, δηλαδή είτε το N παραγοντοποιήθηκε από την πρώτη επιλογή a και B είτε, αν ο αλγόριθμος αποτύγχανε στο πρώτο βήμα μετά δοκίμαζε κι άλλες τιμές για τα a και B στη τύχη. Δεκαεννέα από αυτά παραγοντοποιήθηκαν από την βελτιωμένη εκδοχή που περιγράψαμε παραπάνω και μια περίπτωση δεν μπορούσε να παραγοντοποιηθεί ούτε με τη μια μέθοδο ούτε με την άλλη. Δύο από αυτές τις τρείς τιμές που έκαναν την διαφορά είναι
$N = 2456056423726817916679$ και $N = 5506696456656507816106 63$
Ο λόγος που ο κλασικός αλγόριθμος απέτυχε να παραγοντοποιήσει αυτές τις τιμές είναι ο εξής. Ας δούμε τι γίνετε με τους πρώτους παράγοντες του πρώτου αριθμού. $N = p \cdot q$ όπου $p = 37676180083$ και $q = 65188573213$. Ας δούμε τώρα την παραγοντοποίηση των $p-1$ και $q-1$.

$p-1 = 2 \cdot 3 \cdot 67 \cdot 809 \cdot 115849$
$q-1 = 2^2 \cdot 3 \cdot 7 \cdot 6473 \cdot 119891$

Το πρόβλημα που αντιμετωπίζει ο κλασικός αλγόριθμος σ' αυτή τη περίπτωση αποκαλύφθηκε. Αν πάρουμε $B > 119891$ τότε για κάθε επιλογή του a θα παίρνουμε $MK\Delta = N$. Αν πάρουμε $B < 115849$ τότε για σχεδόν όλες τις τιμές του a θα πάρουμε $MK\Delta = 1$. Άρα καταλήγουμε ότι θέλουμε $115849 < B < 119891$ ώστε να έχουμε καλές πιθανότητες να βγάλει αποτέλεσμα ο αλγόριθμος. Το πρόβλημα είναι ότι τα 115849 και 119891 είναι πολύ κοντά και δεν μπορούμε να πάρουμε ένα B ενδιάμεσα απλώς επιλέγοντας στην τύχη τιμές. Αυτό το πρόβλημα αντιμετωπίζεται από τον αλγόριθμο που περιγράψαμε.

Βιβλιογραφία

[1] William Stein, Elementary Number Theory: Primes, Congruences and Secrets 2011 http://wstein.org/ent/ent.pdf

[2] Lawrence C. Washington, Elliptic Curves Number Theory and Cryptograhy, Chapman and Hall, London, 2008

[3] Γιάννης Α. Αντωνιάδης, Αριθμητική Ελλειπτικών Καμπυλών, ΕΠΕΑΕΚ "ΠΡΟΜΗΘΕΑΣ", Ηράκλειο, 1999

[4] Christophe Ritzenthaler, Elliptic Curves and Applications to Cryptography 2011 http://iml.univ-mrs.fr/ ritzenth/cours/elliptic-curve-course.pdf