Εθνικο Μετσοβιο Πολυτεχνειο
Σχολη Ηλεκτρολογων Μηχανικων και Μηχανικων Υπολογιστων
Τομεας Τεχνολογιας Πληροφορικης Και Υπολογιστων

Κρυπτογραφία Ελλειπτικών Καμπυλών

Διπλωματικη Εργασια

του

ΑΝΔΡΕΑ Σ. ΕΥΑΓΓΕΛΑΤΟΥ

Επιβλέπουσα: Σοφία Λαμπροπούλου
Καθηγήτρια Ε.Μ.Π

Αθήνα, Ιούλιος 2023

Εθνικο Μετσοβιο Πολυτεχνειο
Σχολη Ηλεκτρολογων Μηχανικων και Μηχανικων Υπολογιστων
Τομεας Τεχνολογιας Πληροφορικης Και Υπολογιστων

Κρυπτογραφία Ελλειπτικών Καμπυλών

Διπλωματικη Εργασια

του

ΑΝΔΡΕΑ Σ. ΕΥΑΓΓΕΛΑΤΟΥ

Επιβλέπουσα: Σοφία Λαμπροπούλου
Καθηγήτρια Ε.Μ.Π

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 11η Ιουλίου 2023.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Σοφία Λαμπροπούλου	Αριστείδης Κοντογεώργης	Αριστείδης Παγουρτζής
Καθηγήτρια Ε.Μ.Π	Καθηγητής Ε.Κ.Π.Α.	Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2023

Εθνικο Μετσοβιο Πολυτεχνειο
Σχολη Ηλεκτρολογων Μηχανικων και Μηχανικων Υπολογιστων
Τομεας Τεχνολογιας Πληροφορικης Και Υπολογιστων

ΔΗΛΩΣΗ ΜΗ ΛΟΓΟΚΛΟΠΗΣ ΚΑΙ ΑΝΑΛΗΨΗΣ ΠΡΟΣΩΠΙΚΗΣ ΕΥΘΥΝΗΣ

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ενυπογράφως ότι είμαι αποκλειστικός συγγραφέας της παρούσας Πτυχιακής Εργασίας, για την ολοκλήρωση της οποίας κάθε βοήθεια είναι πλήρως αναγνωρισμένη και αναφέρεται λεπτομερώς στην εργασία αυτή. Έχω αναφέρει πλήρως και με σαφείς αναφορές, όλες τις πηγές χρήσης δεδομένων, απόψεων, θέσεων και προτάσεων, ιδεών και λεκτικών αναφορών, είτε κατά κυριολεξία είτε βάσει επιστημονικής παράφρασης. Αναλαμβάνω την προσωπική και ατομική ευθύνη ότι σε περίπτωση αποτυχίας στην υλοποίηση των ανωτέρω δηλωθέντων στοιχείων, είμαι υπόλογος έναντι λογοκλοπής, γεγονός που σημαίνει αποτυχία στην Πτυχιακή μου Εργασία και κατά συνέπεια αποτυχία απόκτησης του Τίτλου Σπουδών, πέραν των λοιπών συνεπειών του νόμου περί πνευματικών δικαιωμάτων. Δηλώνω, συνεπώς, ότι αυτή η Πτυχιακή Εργασία προετοιμάστηκε και ολοκληρώθηκε από εμένα προσωπικά και αποκλειστικά και ότι, αναλαμβάνω πλήρως όλες τις συνέπειες του νόμου στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής άλλης πνευματικής ιδιοκτησίας.

(Υπογραφή)

.....
Ανδρέας Ευαγγελάτος
Διπλωματούχος
Ηλεκτρολόγος Μηχανικός
και Μηχανικός
Υπολογιστών Ε.Μ.Π.

Περίληψη

Η ανάπτυξη των τηλεπικοινωνιών έφερε την ανάγκη για κρυπτογραφημένη επικοινωνία μεταξύ των χρηστών χωρίς την απαίτηση μίας προγενέστερης επικοινωνίας αυτών. Τα ασύμμετρα κρυπτοσυστήματα ή κρυπτοσυστήματα δημοσίου κλειδιού ικανοποιούν αυτήν την απαίτηση, όμως για να υλοποιηθούν θέτουν ισχυρούς περιορισμούς ως προς την απόδοση και την ασφάλεια. Κρυπτοσυστήματα με τις κατάλληλες ιδιότητες προκύπτουν από την μελέτη των αλγεβρικών δομών ορισμένων επίπεδων καμπυλών, των ελλειπτικών καμπυλών. Συγκεκριμένα, τα σημεία μίας ελλειπτικής καμπύλης έχουν αλγεβρική δομή ομάδας και τα κρυπτογραφικά συστήματα, για να πετύχουν τους στόχους τους, εκμεταλλεύονται την ευκολία κάποιων υπολογισμών σε αυτή την δομή αλλά και την δυσκολία άλλων.

Στην παρούσα διπλωματική εργασία εξετάζεται η θεωρία των ελλειπτικών καμπυλών από υπολογιστική σκοπιά και παρουσιάζονται οι εφαρμογές σε σύγχρονα κρυπτογραφικά συστήματα και αποδοτικούς αλγορίθμους. Αρχικά, ορίζεται η κατηγορία των επίπεδων καμπυλών που αποτελούν ελλειπτικές καμπύλες και παρουσιάζεται η πράξη ομάδας των σημείων αυτών. Για εφαρμογές, είναι απαραίτητο οι υπολογισμοί σε αυτή την ομάδα να γίνονται όσο το δυνατόν γρηγορότερα και στην συνέχεια εξετάζονται τεχνικές που επιτυγχάνουν επιτάχυνση των υπολογισμών. Ακολουθεί μία εισαγωγή στους μορφισμούς των ελλειπτικών καμπυλών, που αποτελούν το κλειδί για την ταξινόμηση της ομάδας αλλά και έναν αποδοτικό αλγόριθμο για τον προσδιορισμό του πλήθος των σημείων αυτής, όταν τα σημεία της έχουν συντεταγμένες σε κάποιο πεπερασμένο σώμα.

Η ασφάλεια κρυπτοσυστημάτων που κάνουν χρήση της ομάδας μίας ελλειπτικής καμπύλης βασίζεται στην δυσκολία κάποιων υπολογισμών σε αυτή, με πρωταγωνιστή το πρόβλημα του διακριτού λογαρίθμου. Εξετάζονται αλγόριθμοι που επιλύουν το πρόβλημα και εφαρμόζονται σε ομάδες ελλειπτικών καμπυλών, καθώς επίσης και αλγόριθμος που δεν εφαρμόζεται σε αυτές αλλά, όντας ταχύτερος, καθιστά λιγότερο κατάλληλες άλλες ομάδες πάνω στις οποίες θα μπορούσαν να στηριχθούν αντίστοιχα κρυπτογραφικά συστήματα. Επιπλέον, παρουσιάζονται κρυπτογραφικά συστήματα ελλειπτικών καμπυλών που χρησιμοποιούνται συνεχώς στις δικτυακές επικοινωνίες, καθώς και παρεμφερή προβλήματα στα οποία αυτά στηρίζουν την ασφάλεια τους. Η εργασία ολοκληρώνεται με μία ακόμα σημαντική εφαρμογή, έναν αποδοτικό αλγόριθμο για την παραγοντοποίηση ακεραίων, που στηρίζεται στις ιδιότητες των ομάδων ελλειπτικών καμπυλών.

Λέξεις Κλειδιά

Ελλειπτικές Καμπύλες, Επίπεδες Προβολικές Καμπύλες, Isogenies, Θεώρημα του Hasse, Αλγόριθμος του Schoof, Διακριτός Λογάριθμος, ECIES, ECDSA, Lenstra ECM

Abstract

The development of telecommunications brought the need for encrypted communication between users without the requirement of prior communication between them. Asymmetric cryptosystems or public key cryptosystems satisfy this requirement, but in order to be implemented they impose strong performance and security constraints. Cryptosystems with the appropriate properties are obtained by studying the algebraic structure of certain plane curves, the elliptic curves. In particular, the points of an elliptic curve form a group and cryptographic systems, in order to achieve their goals, exploit the ease of some computations on this structure and the difficulty of others.

In this thesis, the theory of elliptic curves is examined from a computational point of view and applications to modern cryptographic systems and efficient algorithms are presented. Firstly, the class of plane curves that constitute elliptic curves is defined and the group operation on the points of an elliptic curve is presented. For applications, it is necessary that computations on this group be as fast as possible, and techniques that achieve speedup are then considered. This is followed by an introduction to the morphisms of elliptic curves, which are the key to the classification of the group and an efficient algorithm for determining the number of points in this group, when the points have coordinates in a finite field.

The security of cryptosystems that make use of the group of an elliptic curve is based on the difficulty of some computations on it, the main one being the discrete logarithm problem. Algorithms that solve this problem and are applied to elliptic curve groups are considered, as well as an algorithm that does not apply to them but, being faster, makes other groups on which similar cryptographic systems could be based less suitable. In addition, elliptic curve cryptographic systems that are constantly used in network communications are presented, as well as similar problems on which they base their security. The thesis concludes with another important application, an efficient algorithm for integer factorization based on the properties of elliptic curve groups.

Keywords

Elliptic Curves, Plane Projective Curves, Isogenies, Hasse's Theorem, Schoof's Algorithm, Discrete Logarithm, ECIES, ECDSA, Lenstra ECM

Ευχαριστίες

Αρχικά θέλω να ευχαριστήσω την καθηγήτρια κ. Λαμπροπούλου για την ουσιαστική επίβλεψη της εργασίας, την πολλαπλή στήριξη της και, βέβαια, για τη δυνατότητα που μου έδωσε να ασχοληθώ με το πολύ ενδιαφέρον θέμα των Ελλειπτικών Καμπυλών. Επιπλέον, τον καθηγητή κ. Κοντογεώργη για τη συνεχή καθοδήγηση και τον καθοριστικό του ρόλο στην ολοκλήρωση της εργασίας, όπως και τον καθηγητή κ. Παγουρτζή για την όλη του υποστηρικτική φροντίδα. Τέλος, ευχαριστώ την οικογένειά μου για τη συνεχή υποστήριξη και ενθάρρυνση.

Αθήνα, Ιούλιος 2023

Ανδρέας Ευαγγελάτος

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Διοφαντικές Εξισώσεις και Ελλειπτικές Καμπύλες

Οι λύσεις πολυωνυμικών εξισώσεων με ρητούς συντελεστές στους ακεραίους ή τους ρητούς αριθμούς προβλημάτισε από την αρχαιότητα τους μαθηματικούς και απαρτίζει έναν ολόκληρο κλάδο των μαθηματικών που ονομάζεται Διοφαντικές εξισώσεις. Ο κλάδος ονομάζεται έτσι από τον Διόφαντο από την Αλεξάνδρεια (περίπου 210-290 π.χ.) ο οποίος στο έργο του, «Αριθμητικά» όρισε και μελέτησε πολλές τέτοιες εξισώσεις.

Η πιο απλή περίπτωση Διοφαντικής εξίσωσης είναι όταν πρόκειται για μία μόνο μεταβλητή, δηλαδή μία εξίσωση της μορφής:

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0 \tag{1.1}$$

Οι ρητές λύσεις σε τέτοιες εξισώσεις προσδιορίζονται πλήρως με βάση το Λήμμα του Gauss.

Λήμμα (Gauss). *Αν $\frac{a}{b} \in \mathbb{Q}$ είναι λύση της εξίσωσης (1.1) τότε $a \mid a_0$ και $b \mid a_n$.*

Προκύπτει από αυτό ένας εύκολος τρόπος για να βρεθούν όλες οι ρητές λύσεις της εξίσωσης (1.1), αναζητώντας στους διαιρέτες των a_0 και a_n.

Η αμέσως επόμενη περίπτωση είναι αυτή των γραμμικών Διοφαντικών εξισώσεων με δύο μεταβλητές, δηλαδή εξισώσεις της μορφής:

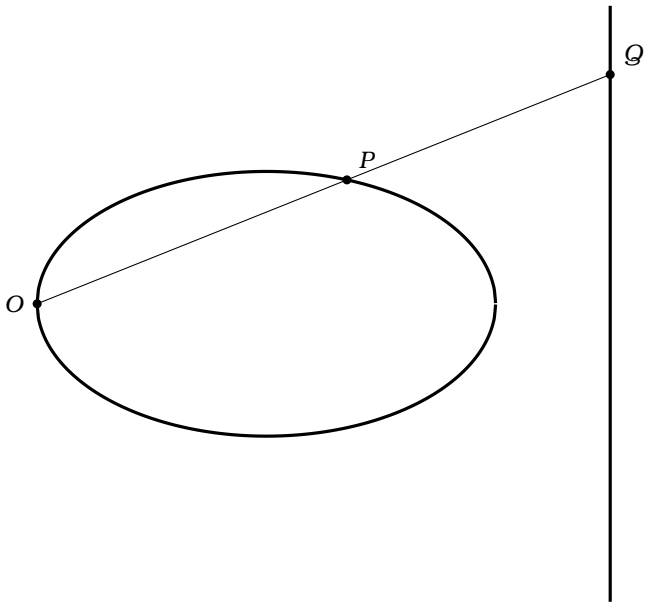
$$ax + by = c \tag{1.2}$$

Από τις ιδιότητες του μέγιστου κοινού διαιρέτη είναι γνωστό πως το σύνολο των πολλαπλασίων του (a, b) είναι ίδιο με το σύνολο των γραμμικών συνδυασμών των a, b. Αν, λοιπόν, οι a, b δεν είναι και οι δύο 0 ισχύει πως η εξίσωση (1.2) έχει ακέραιες λύσεις αν και μόνο αν $(a, b) \mid c$. Αν λοιπόν ισχύει μία τέτοια συνθήκη μπορεί να γραφεί ο (a, b) ως $(a, b) = ax_0 + by_0$ για κάποια $x_0, y_0 \in \mathbb{Z}$ και $c = q(a, b)$. Μία λύση τότε αποτελεί η (qx_0, qy_0). Μάλιστα, οι λύσεις τότε είναι άπειρες και όλες είναι της μορφής $x = qx_0 + k\frac{b}{(a,b)}, y = qy_0 - k\frac{a}{(a,b)}$.
Η αναζήτηση των ρητών λύσεων είναι ακόμα πιο εύκολη.

Η επόμενη περίπτωση είναι αυτή των τετραγωνικών εξισώσεων

$$ax^2 + bxy + cy^2 + dx + ey + f = 0 \tag{1.3}$$

Σε αυτές τις εξισώσεις αν υπάρχει μία λύση στους ρητούς τότε υπάρχουν άπειρες. Ο προσδιορισμός αυτών έρχεται με ικανοποιητικό τρόπο από την γεωμετρία. Όταν είναι δεδομένο ένα σημείο O στους ρητούς και μία ευθεία που διέρχεται από αυτό το σημείο που δίνεται από ρητούς συντελεστές, τότε αυτή τέμνει το γράφημα της (1.3) σε ένα ακόμη σημείο το οποίο είναι σίγουρα ρητό (έχει συντεταγμένες που δίνονται από ρητούς αριθμούς). Αυτό γιατί αν αντικατασταθεί η εξίσωση της ευθείας $y = ax + b$ στην (1.3) για να βρεθούν τα σημεία τομής $ax^2 + bx(ax + b) + c(ax + b)^2 + dx + e(ax + b) + f = 0$ θα προκύψει ένα πολυώνυμο δευτέρου βαθμού ως προς το x με ρητούς συντελεστές. Παρότι στην γενική περίπτωση μπορεί αυτό το πολυώνυμο να έχει άρρητες λύσεις, εξαναγκάζοντας την μία λύση να είναι ρητή θα ισχύει πως και η δεύτερη θα είναι στους ρητούς (το γινόμενο τους θα είναι ο σταθερός όρος). Έτσι, μπορεί να γίνει προβολή των ρητών λύσεων σε μία ευθεία. Επιλέγεται ρητό σημείο της ευθείας Q και σχηματίζεται η εξίσωση της ευθείας που θα έχει ρητούς συντελεστές που ενώνει το O και το Q. Το σημείο P που τέμνει αυτή το γράφημα της εξίσωσης (1.3) έχει ρητές συντεταγμένες.



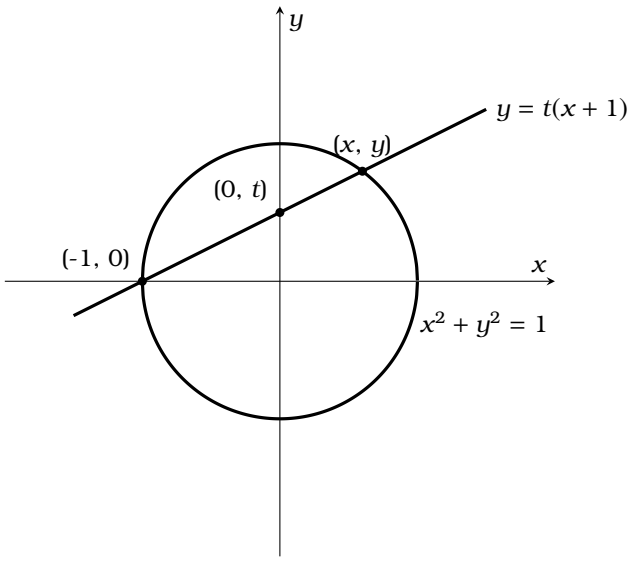
Χαρακτηριστικό παράδειγμα αποτελεί η παραμετρικοποίηση των πυθαγόρειων τριάδων κατ' αυτό τον τρόπο. Αναζητούνται λύσεις στους ακεραίους της εξίσωσης

$$x^2 + y^2 = z^2 \tag{1.4}$$

ή ισοδύναμα ρητές λύσεις της (αφού διαγραφούν κοινοί όροι και γίνει η παρατήρηση ότι πρέπει οι x, z και y, z να είναι πρώτοι μεταξύ τους)

$$x^2 + y^2 = 1 \tag{1.5}$$

Μία λύση αυτής είναι η $(-1, 0)$ οπότε χρησιμοποιώντας αυτή μπορούν να εκφραστούν όλες οι άλλες προβάλοντάς τες στον άξονα των y.



Επιλέγοντας ρητό σημείο $(0, t)$ στον άξονα των y τότε η ευθεία που περνά από τα $(-1, 0)$ και $(0, t)$ είναι η $y = t(x+1)$. Για να βρεθούν τα σημεία τομής της με την (1.5) αντικαθίσταται το y με το $t(x + 1)$ κι προκύτει $x^2 + t^2(x + 1)^2 = 1 \Rightarrow x^2 + t^2(x^2 + 2x + 1) = 1 \Rightarrow x^2(1 + t^2) + 2xt^2 + (t^2 - 1) = 0 \Rightarrow x^2 + \frac{2t}{t^2+1}x + \frac{t^2-1}{t^2+1} = 0$. Είναι γνωστό, όμως, πως η μία λύση της εξίσωσης είναι η -1 άρα η άλλη είναι η $x = -\frac{t^2-1}{t^2+1} = \frac{1-t^2}{t^2+1}$. Βρίσκεται τότε το y από την εξίσωση της ευθείας

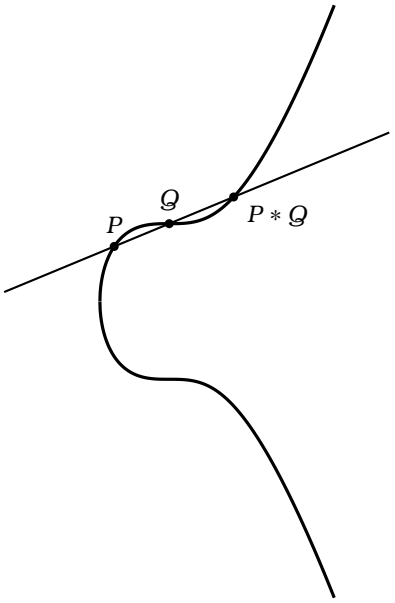
$$x = \frac{1 - t^2}{1 + t^2},\ y = \frac{2t}{1 + t^2}$$

Είναι εμφανές πως αν $t \in \mathbb{Q}$ τότε $x, y \in \mathbb{Q}$ και αντίστροφα αν είναι δεδομένο ένα σημείο με ρητές συντεταγμένες (x, y) τότε η ευθεία που διέρχεται από αυτό και το $(-1, 0)$ δίνεται από ρητούς συντελεστές και τέμνει τον $y'y$ σε ρητό σημείο.

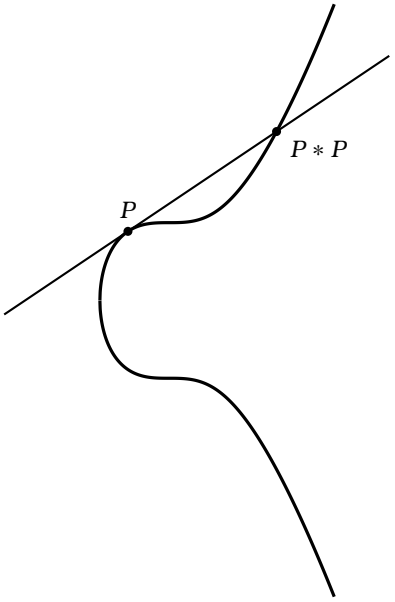
Το επόμενο βήμα είναι η εξέταση κυβικών εξισώσεων με ρητούς συντελεστές της μορφής:

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0 \tag{1.6}$$

Τέτοιες εξισώσεις, υπό κάποιες προϋποθέσεις, περιγράφουν ελλειπτικές καμπύλες. Αυτές είναι πιο σύνθετες για να μπορούν να προβληθούν οι ρητές λύσεις σε μία ευθεία, όταν είναι γνωστό ένα ρητό σημείο. Μία ευθεία με ρητούς συντελεστές που περνάει από αυτό θα τέμνει εν γένει, το γράφημα της εξίσωσης (1.6), σε δύο σημεία τα οποία μπορεί να έχουν άρρητες συντεταγμένες. Ωστόσο, αν είναι γνωστά δύο σημεία με ρητές συντεταγμένες, τότε αντικαθιστώντας την εξίσωση της ευθείας που τα ενώνει $y = ax + b$ στην (1.6) θα προκύψει ένα κυβικό πολυώνυμο με ρητούς συντελεστές. Αυτό, έχει δύο λύσεις στους ρητούς και άρα και η άλλη θα είναι στους ρητούς. Πράγματι, αν $x^3 + ax^2 + bx + c = (x - x_1)(x - x_2)(x - x_3) = x^3 - (x_1 + x_2 + x_3)x^2 + \ldots$ Άρα αφού οι συντελεστές είναι στους ρητούς και οι δύο ρίζες είναι στους ρητούς, τότε θα είναι και η τρίτη. Έτσι, μπορεί να οριστεί μία διμελή πράξη πάνω στο σύνολο των ρητών σημείων.



Ενώνονται τα δύο σημεία με ρητές συντεταγμένες με μία ευθεία που θα έχει ρητούς συντελεστές. Αντικαθίσταται η ευθεία στην εξίσωση της (1.6) και βρίσκεται το τρίτο σημείο τομής της ευθείας και της καμπύλης, το οποίο συμβολίζεται εδώ $P * Q$, που έχει και αυτό συντεταγμένες στους ρητούς. Ακόμα και στην περίπτωση που είναι γνωστό μόνο ένα ρητό σημείο P μπορεί να υπολογιστεί ένα ακόμα, χρησιμοποιώντας την εφαπτομένη της καμπύλης στο σημείο αυτό, υποθέτοντας πως αυτή υπάρχει. Αυτή θα τέμνει την καμπύλη σε ένα επιπλέον σημείο, αφού αντικαθιστώντας την εξίσωσή της στην (1.6) θα προκύψει διπλή ρίζα στο σημείο P και άλλη μία που αναγκαστικά θα είναι στους ρητούς.



Με κάποιες παραλλαγές και με δεδομένο ένα ρητό σημείο στην καμπύλη μπορεί να οριστεί, με αυτό τον τρόπο, μία πράξη ώστε τα ρητά σημεία της καμπύλης να αποτελούν αβελιανή ομάδα. Αυτή η ομάδα μπορεί να οριστεί για μία τέτοια εξίσωση πάνω από αυθαίρετο σώμα, αφού ο ορισμός της πράξης θα δίνεται από ρητές συναρτήσεις με συντελεστές πάνω στο σώμα ορισμού.

Κρυπτογραφία

Η ανάπτυξη των ηλεκτρονικών τηλεπικοινωνιών έφερε την ανάγκη για ασφαλή και με τήρηση της ιδιωτικότητας επικοινωνία μεταξύ των χρηστών. Σε αυτό το πλαίσιο, επήλθε ανάπτυξη των κρυπτογραφικών συστημάτων, που χωρίζονται σε συμμετρικά και ασύμμετρα. Τα κλασσικά κρυπτοσυστήματα βασίζονται στην συμμετρική κρυπτογράφηση. Κατά αυτήν, γίνεται χρήση ενός μυστικού κλειδιού που είναι γνωστό μόνο στον αποστολέα και τον παραλήπτη. Χρησιμοποιείται για να μετασχηματίσει ένα μήνυμα σε κείμενο, από το οποίο δεν μπορεί κανείς να λάβει πληροφορία, παρά μόνο εάν γνωρίζει το μυστικό κλειδί. Έτσι, το μετασχηματισμένο μήνυμα αποστέλλεται σε ένα μη ασφαλές κανάλι και ο παραλήπτης χρησιμοποιεί το μυστικό κλειδι για να αναπαράξει το αρχικό κείμενο. Τέτοιου είδους συστήματα για να λειτουργήσουν πρέπει να έχουν έναν τρόπο ώστε να διανέμεται με ασφάλεια το μυστικό κλειδί σε αποστολέα και παραλήπτη.

Η ασύμμετρη κρυπτογραφία ή κρυπτογραφία δημοσίου κλειδιού έρχεται να λύσει το πρόβλημα της διανομής των κλειδιών. Επινοήθηκε από τους Diffie και Hellman το 1976 στην δημοσίευση τους "New Directions In Cryptography" ενώ ήταν οι Rivest, Shamir και Adleman που έναν χρόνο αργότερα κατασκεύασαν ένα σύστημα δημοσίου κλειδιού, το RSA. Σε ένα σύστημα δημοσίου κλειδιού κάθε χρήστης Α έχει ένα ζεύγος κλειδιών, ένα δημόσιο (public key) και ένα ιδιωτικό (private key). Το δημόσιο κλειδί είναι γνωστό σε όλους τους χρήστες ενώ το ιδιωτικό το γνωρίζει μόνο ο Α. Κάθε χρήστης μπορεί να κρυπτογραφήσει ένα μήνυμα που προορίζεται για τον Α κάνοντας χρήση του δημοσίου κλειδιού του. Η αποκρυπτογράφηση του μηνύματος γίνεται μόνο με την χρήση του αντίστοιχου ιδιωτικού κλειδιού (που γνωρίζει ο Α). Με αυτόν τον τρόπο, δεν υπάρχει ανάγκη για ασφαλή διανομή κλειδιών. Ωστόσο, προκύπτει το πρόβλημα της διασφάλισης της αντιστοιχίας του καθενός δημοσίου κλειδιού με τον εκάστοτε συγκεκριμένο χρήστη. Για αυτό το πρόβλημα έχουν προταθεί λύσεις, που επίσης χρησιμοποιούν κρυπτοσυστήματα δημοσίου κλειδιού. Τα κρυπτοσυστήματα δημοσίου κλειδιού έχουν επιπλέον εφαρμογές, όπως οι ψηφιακές υπογραφές.

Η ασφάλεια της κρυπτογραφίας δημοσίου κλειδιού βασίζεται σε υπολογιστικές υποθέσεις, δηλαδή σε υπολογιστικά προβλήματα για τα οποία δεν υπάρχουν γνωστοί αλγόριθμοι που να τα λύνουν σε λογικό χρόνο, σε σχέση με μία παράμετρο ασφάλειας. Για παράδειγμα, το RSA βασίζεται στην δυσκολία παραγοντοποίησης μεγάλων ακεραίων (χιλιάδων bits). Η γνώση της παραγοντοποίησης από τον χρήστη είναι αυτή που του δίνει την δυνατότητα να αποκρυπτογραφεί μηνύματα. Άλλα κρυπτοσυστήματα δημοσίου κλειδιού βασίζονται στο πρόβλημα του διακριτού λογαρίθμου για αβελιανές ομάδες. Οι ελλειπτικές καμπύλες μπορούν να οριστούν πάνω από πεπερασμένα σώματα και οι λύσεις τους σε αυτά αποτελούν ένα τέτοιο παράδειγμα. Η χρήση των ελλειπτικών καμπυλών σε ασύμμετρα κρυπτοσυστήματα προτάθηκε από τους Neal Koblitz και Victor Miller το 1985 και προσδίδει σε αυτά αρκετά πλεονεκτήματα σε σύγκριση με άλλα ασύμμετρα όπως το RSA. Οι ελλειπτικές καμπύλες προσφέρουν τελικά μεγαλύτερη ασφάλεια για μικρότερα μεγέθη μυστικών κλειδιών, ταχύτερες κρυπτογραφήσεις και αποκρυπτογραφήσεις και απαιτούν λιγότερους υπολογιστικούς πόρους. Την ίδια ασφάλεια που προσφέρει το RSA, για παράδειγμα, με παράμετρο ασφάλειας 3072 bits προσφέρουν συστήματα ελλειπτικών καμπυλών με παράμετρο 256 bits.

Κεφάλαιο 2

Ορισμός Ελλειπτικής Καμπύλης

Στόχος αυτού του κεφαλαίου είναι η παρουσίαση των προαπαιτούμενων εννοιών για τον ορισμό και την μελέτη βασικών ιδιοτήτων των ελλειπτικών καμπυλών.

2.1 Προβολικός Χώρος και Επίπεδες Καμπύλες

Έστω k ένα σώμα και $\overline{k}$ μία αλγεβρική του θήκη. Ορίζεται σε αυτό η σχέση ισοδυναμίας των πλειάδων $(x_0, \ldots, x_n) \in \overline{k}^{n+1}$ με τουλάχιστον ένα $x_i \neq 0$ που δίνεται από την σχέση

$$(x_0, \ldots, x_n) \sim (\lambda x_0, \ldots, \lambda x_n), \forall \lambda \in \overline{k}$$

Ορισμός 2.1. *Ο **προβολικός** $n-$**χώρος** ορίζεται ως το σύνολο των κλάσεων ισοδυναμίας της σχέσης ισοδυναμίας $\sim$, δηλαδή είναι το σύνολο*

$$\mathbb{P}^n = \frac{\{(x_0, \ldots, x_n) \in \overline{k}^{n+1} : \exists i \in \{0, ..., n\}, x_i \neq 0\}}{\sim} = \frac{\overline{k}^{n+1} \setminus \{(0, \ldots, 0)\}}{\sim}$$

*Ένα προβολικό σημείο στο $\mathbb{P}^n$ είναι $k-$**rational** ($k-$**ρητό**) αν περιέχει έναν αντιπρόσωπο με $(x_0, \ldots, x_n) \in k^{n+1}$ ή ισοδύναμα είναι μία πλειάδα $(x_0, \ldots, x_n)$ με $x_i x_j^{-1} \in k, \forall x_j \neq 0$.*

Το σύνολο των k-ρητών προβολικών σημείων στο $\mathbb{P}^n$ συμβολίζεται με $\mathbb{P}^n(k)$.

Συμβολίζεται με $(x_0 : \ldots : x_n)$ η κλάση ισοδυναμίας της πλειάδας $(x_0, \ldots, x_n)$.

Για $n = 2$ χρησιμοποιούνται για συντεταγμένες τα x, y, z αντί των x_0, x_1, x_2 και το $\mathbb{P}^2$ ονομάζεται το **προβολικό επίπεδο**. Το δισδιάστατο ομοπαραλληλικό ή αφινικό επίπεδο πάνω από το σώμα k ορίζεται ως

$$\mathbb{A}^2 = \{(x, y) : x, y \in \overline{k}\}$$

Το σύνολο των $k-$ρητών σημείων στο $\mathbb{A}^2$ συμβολίζεται με $\mathbb{A}^2(k)$ και είναι το σύνολο

$$\mathbb{A}^2(k) = \{(x, y) \in \mathbb{A}^2 \,|\, x, y \in k\}$$

Το $\mathbb{A}^2$ μπορεί να νοηθεί πως εμπεριέχεται στο $\mathbb{P}^2$, αν αντιστοιχθούν τα σημεία $(x, y) \in \mathbb{A}^2$ στα προβολικά σημεία $(x : y : 1) \in \mathbb{P}^2$, δηλαδή από την $1-1$ συνάρτηση $(x, y) \mapsto (x : y : 1)$

$((x_1 : y_1 : 1) = (x_2 : y_2 : 1) \Rightarrow (x_1 = \lambda x_2) \wedge (y_1 = \lambda y_2) \wedge (1 = \lambda 1) \Rightarrow (x_1 = x_2) \wedge (y_1 = y_2))$. Στα παρακάτω, θα ταυτίζεται το $\mathbb{A}^2$ με τα σημεία $(x : y : 1)$ του $\mathbb{P}^2$ ή ισοδύναμα με τα σημεία $(x : y : z), z \neq 0 \Rightarrow (x : y : z) = (xz^{-1} : yz^{-1} : 1) = (x' : y' : 1)$. Τα προβολικά σημεία στο $\mathbb{P}^2$ που δεν βρίσκονται στο $\mathbb{A}^2$ (δηλαδή έχουν $z = 0$) σχηματίζουν την γραμμή στο άπειρο, η οποία είναι ισομορφική με την προβολική γραμμή $\mathbb{P}^1$.

Πίνακας 2.1: *Τα σημεία του προβολικού επιπέδου*

$\mathbb{P}^2$	$\longleftrightarrow$	$\mathbb{A}^2 \cup \mathbb{P}^1$
$(x : y : z)$	$\longrightarrow$	$\begin{cases} \left(\frac{x}{z}, \frac{y}{z}\right) \in \mathbb{A}^2, z \neq 0 \\ (x : y) \in \mathbb{P}^1, z = 0 \end{cases}$
$(x, y, 1)$	$\longleftarrow$	$(x, y) \in \mathbb{A}^2$
$(x : y : 0)$	$\longleftarrow$	$(x : y) \in \mathbb{P}^1$.

Ορισμός 2.2 (Ομογενές πολυώνυμο)**.** *Έστω R ένας αντιμεταθετικός δακτύλιος. Ένα πολυώνυμο $f \in R[x_0, \ldots, x_n]$ είναι ομογενές αν κάθε μη μηδενικός όρος του f έχει τον ίδιο βαθμό.*

Για κάθε μη μηδενικό πολυώνυμο $f \in R[x_0, \ldots, x_n]$ συμβολίζεται με $\deg f$ ο μέγιστος βαθμός των μη μηδενικών του όρων. Ένα ομογενές πολυώνυμο βαθμού n είναι ένα άθροισμα από όρους της μορφής $ax_0^{i_0}x_1^{i_1}\cdots x_n^{i_n}$ όπου $\sum_{k=0}^{n} i_k = n$. Επιπλέον, για κάθε μη μηδενικό πολυώνυμο $f \in R[x_0, \ldots, x_{n-1}]$ υπάρχει ομογενές πολυώνυμο $F \in R[x_0, \ldots, x_n]$ τέτοιο ώστε $\deg f = \deg F$ που ικανοποιεί την

$$F(x_0, \ldots, x_{n-1}, 1) = f(x_0, \ldots, x_{n-1}).$$

Αυτό υπολογίζεται από την

$$F(x_0, \ldots, x_n) = x_n^{\deg f} f\left(\frac{x_0}{x_n}, \ldots, \frac{x_{n-1}}{x_n}\right),$$

δηλαδή αντικαθιστώντας κάθε όρο t της f με $tx_n^{\deg f - \deg t}$. Το πολυώνυμο F καλείται η ομογενοποίηση του f και f η μη ομογενής μορφή του F.

Παράδειγμα 2.1. Αν k σώμα και $f \in k[x, y]$, με

$$f(x, y) = y^2 - x^3 - Ax - B,$$

τότε η ομογενοποίηση του f είναι το πολυώνυμο $F \in k[x, y, z]$ με

$$F(x, y, z) = y^2z - x^3 - Axz^2 - Bz^3.$$

Ορισμός 2.3 (Επίπεδη (προβολική) καμπύλη)**.** *Έστω k ένα σώμα. Μία* ***επίπεδη (προβολική) καμπύλη (plane (projective) curve)*** *X είναι ένα μη μηδενικό ομογενές πολυώνυμο $F \in k[x, y, z]$. Γράφεται X/k για να δηλωθεί πως η X είναι ορισμένη πάνω στο k και $X : F(x, y, z) = 0$.*

Δύο επίπεδες καμπύλες θεωρούνται ίδιες αν είναι η μία πολλαπλάσιο της άλλης. δηλαδή αν X, X' είναι τα F, F' αντίστοιχα και $\exists \lambda \in k, F = \lambda F'$.

Για κάθε επέκταση K/k το σύνολο των K σημείων ή των K ρητών σημείων της X είναι το σύνολο των σημείων μηδενισμού της F στο $\mathbb{P}^2(K)$:

$$X(K) := \{(x : y : z) \in \mathbb{P}^2(K) \,|\, F(x, y, z) = 0\}.$$

Παρατήρηση 1. Επειδή το F στον παραπάνω ορισμό είναι ομογενές ισχύει ότι

$$F(\lambda x, \lambda y, \lambda z) = \lambda^{\deg F} F(x, y, z), \forall \lambda \in k^*.$$

Άρα, αν $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ τότε $F(x_1, y_1, z_1) = 0 \Leftrightarrow F(x_2, y_2, z_2) = 0$. Ένας μηδενισμός του F στο $\mathbb{P}^2$ δεν εξαρτάται από επιλογή αντιπρόσωπου. Επομένως το σύνολο $X(K)$ είναι καλά ορισμένο.

Παρατήρηση 2. Για κάθε σημείο $(x : y : z) \in X(K)$ με $z \neq 0$ ισχύει πως

$$0 = \frac{1}{z^{\deg F}} F(x, y, z) = F\left(\frac{x}{z}, \frac{y}{z}, 1\right) = f\left(\frac{x}{z}, \frac{y}{z}\right)$$

όπου f η μη ομογενής μορφή του F. Μπορεί, λοιπόν, να οριστεί η συνάρτηση

$$\phi : \{(x : y : z) \in X(K) \,|\, z \neq 0\} \longrightarrow \{(x, y) \in \mathbb{A}^2(K) : f(x, y) = 0\}$$

$$\phi(x : y : z) = \left(\frac{x}{z}, \frac{y}{z}\right)$$

Αυτή η συνάρτηση είναι 1-1 και επί αφού $\phi(x_1 : y_1 : z_1) = \phi(x_2 : y_2 : z_2) \Rightarrow \left(\frac{x_1}{z_1}, \frac{y_1}{z_1}\right) = \left(\frac{x_2}{z_2}, \frac{y_2}{z_2}\right) \Rightarrow \left(\frac{x_1}{z_1} : \frac{y_1}{z_1} : 1\right) = \left(\frac{x_2}{z_2} : \frac{y_2}{z_2}, 1\right) \Rightarrow (x_1 : y_1 : z_1) = (x_2 : y_2 : z_2)$ και υπάρχουν $x', y', z \neq 0$ τετοια ώστε $x = \frac{x'}{z}, y = \frac{y'}{z}$ με $f(x, y) = 0 = f\left(\frac{x'}{z}, \frac{y'}{z}\right) = F\left(\frac{x'}{z}, \frac{y'}{z}, 1\right) = F(x', y', z)$. Το πολυωνυμο f τότε λέγεται το αφινικό μέρος του F.

Θα ορίζονται επίπεδες καμπύλες και με την αφινική εξίσωση $g(x, y) = h(x, y)$ με $g, h \in k[x, y]$, η οποία θα ερμηνεύεται σαν την καμπύλη που ορίζεται από το ομογενές πολυώνυμο $F(x, y, z) := G(x, y, z) - H(x, y, z)$ όπου $F, G, H \in k[x, y, z]$ με G, H οι ομογενείς μορφές των g, h αντίστοιχα.

Παράδειγμα 2.2 (Ευθείες στο προβολικό επίπεδο)**.** Μία ευθεία ορισμένη πανω από το σώμα k δίνεται από το μη μηδενικό πολυώνυμο $L = ax + by + cz$. Τα k σημεία της ευθείας είναι το σύνολο

$$L(k) = \{(x : y : z) \in \mathbb{P}^2(k) \,|\, ax + by + cz = 0\}.$$

Δυο διαφορετικές ευθείες τέμνονται σε ένα και μοναδικό σημείο. Πράγματι, αν $L = ax + by + cz$ και $L' = a'x + b'y + c'z$ τότε για να βρεθούν το σημεία τομής των δύο θεωρείται το σύστημα

$$\begin{cases} ax + by + cz = 0 \\ a'x + b'y + cz' = 0 \end{cases} \Leftrightarrow \begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Αφού οι ευθείες είναι διαφορετικές δεν είναι η μία πολλαπλάσιο της άλλης κι επομένως, ο πίνακας συντελεστών A έχει βαθμό 2, δηλαδή $\rho(A) = 2$. Έπεται πως η μηδενικότητά του $\upsilon(A) = 3 - 2 = 1$ και πως ορίζει τότε ένα προβολικό σημείο (μία κλάση ισοδυναμίας).

Επιπλέον, από δύο διαφορετικά σημεία διέρχεται μία και μόνο μία ευθεία. Δηλαδή αν $(x : y : z), (x' : y' : z') \in \mathbb{P}^2(k), (x : y : z) \neq (x' : y' : z')$ και θεωρείται το σύστημα

$$\begin{cases} ax + by + cz = 0 \\ ax' + by' + cz' = 0 \end{cases} \Leftrightarrow \begin{pmatrix} x & y & z \\ x' & y' & z' \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Με το ίδιο επιχείρημα ο χώρος των λύσεων είναι μονοδιάστατος και άρα ορίζει μία ευθεία.

Στο προβολικό επίπεδο παύει να υπάρχει η έννοια της παραλληλίας. Ακόμα και παράλληλες ευθείες τέμνονται. Για τα σημεία τομής αυτών, έστω

$$y = mx + b_1 \text{ και } y = mx + b_2$$

δύο όχι κατακόρυφες ευθείες με $b_1 \neq b_2$. Έχουν ομογενείς μορφές

$$y - mx - b_1 z = 0 \text{ και } y - mx - b_2 z = 0.$$

Εξισώνοντας

$$z = 0 \text{ και } y = mx$$

Αφού δεν μπρούν τα x, y, z να είναι συγχρόνως 0 ισχύει $x \neq 0$, και το σημείο τομής είναι το $(x : mx : 0) = (1 : m : 0)$.
Στην περίπτωση δύο κατακόρυφων ευθειών

$$x = c_1 \text{ και } x = c_2, c_1 \neq c_2$$

Σε ομογενή μορφή

$$x = c_1 z \text{ και } x = c_2 z, c_1 \neq c_2$$

και εξισώνοντας $z = 0 \Rightarrow x = 0$ και επομένως το σημείο τομής είναι το
$(0 : y : 0) = (0 : 1 : 0)$ αφού $y \neq 0$.

Από την παραπάνω ανάλυση φαίνεται πως το προβολικό επίπεδο μπορεί να θεωρηθεί ότι αποτελείται από το σύνηθες επίπεδο, με επιπλέον ένα σημείο στο άπειρο για κάθε διεύθυνση μίας ευθείας, με την έννοια ότι παράλληλες ευθείες έχουν την ίδια διεύθυνση. Έτσι, αυτές οι διευθύνσεις μπορούν να οριστούν ως το σύνολο των ευθειών που διέρχονται από την αρχή των αξόνων, δηλαδή από εξισώσεις της μορφής $Ay = Bx$ με A, B όχι συγχρόνως 0. Δύο

ζεύγη $(A, B), (A', B')$ αντιστοιχούν στην ίδια ευθεία αν και μόνον αν $(A, B) \sim (A', B')$. Αυτά τα σημεία περιγράφονται, λοιπόν, ακριβώς από την προβολική γραμμή $\mathbb{P}^1$.

Παράδειγμα 2.3. Έστω η επίπεδη καμπύλη που ορίζεται από την $E : y^2 = x^3 + Ax + B$ με A, B σε κάποιο σώμα k και ομογενή μορφή $y^2z = x^3 + Axz^2 + Bz^3$. Τα σημεία $(x : y : 1)$ στην προβολική εκδοχή αντιστοιχούν στα σημεία (x, y) της αρχικής. Για τα σημεία στο άπειρο τίθεται $z = 0 \Rightarrow x^3 = 0 \Rightarrow x = 0$ και αφού δεν μπορούν τα x, y, z να είναι συγχρόνως 0 προκύπτει πως $y \neq 0$ και το μοναδικό σημείο στο άπειρο είναι το $(0 : y : 0) = (0 : 1 : 0)$. Κάθε κάθετη ευθεία τέμνει την E στο σημείο $(0 : 1 : 0)$ στο άπειρο.

Ορισμός 2.4 (Λεία επίπεδη (προβολική) καμπύλη)**.** *Μία επίπεδη προβολική καμπύλη X/k που ορίζεται από το $f \in k[x, y, z]$ είναι **λεία (smooth)** σε ένα σημείο $P \in X(\overline{k})$ αν οποιαδήποτε από τις μερικές παραγώγους $\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, \frac{\partial f}{\partial z}$ είναι μη μηδενική στο P. Διαφορετικά, δηλαδή αν $\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = \frac{\partial f}{\partial z}(P) = 0$ το P λέγεται **ιδιάζον (singular)** σημείο της X.*
*Η καμπύλη X είναι **λεία** αν είναι λεία σε κάθε σημείο $X(\overline{k})$*

Παρατήρηση 3. Στο αφινικό επίπεδο ένα σημείο (x_0, y_0) της καμπύλης $f(x, y) = 0$ είναι ιδιάζον αν $f(x_0, y_0) = \frac{\partial f}{\partial x}(x_0, y_0) = \frac{\partial f}{\partial y}(x_0, y_0) = 0$. Αυτό είναι ισοδύναμο με

$$F(x_0, y_0, 1) = \frac{\partial F}{\partial x}(x_0, y_0, 1) = \frac{\partial F}{\partial y}(x_0, y_0, 1) = 0$$

για την ομογενή μορφή της f. Όμως ισχύει πως $x\frac{\partial F}{\partial x} + y\frac{\partial F}{\partial y} + z\frac{\partial F}{\partial z} = (\deg F)F$. Οπότε, ισοδύναμα

$$F(x_0, y_0, 1) = \frac{\partial F}{\partial x}(x_0, y_0, 1) = \frac{\partial F}{\partial y}(x_0, y_0, 1) = \frac{\partial F}{\partial z}(x_0, y_0, 1) = 0$$

.

2.2 Ελλειπτικές Καμπύλες

2.2.1 Εξίσωση Weierstrass

Μπορούν πλέον να μελετηθούν οι κυβικές εξισώσεις που ορίζουν ελλειπτικές καμπύλες. Σε αυτό το πλαίσιο ορίζεται η εξίσωση **Weierstrass** που ορίζει μία επίπεδη καμπύλη:

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \tag{2.1}$$

η οποία έχει ομογενή μορφή:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.2}$$

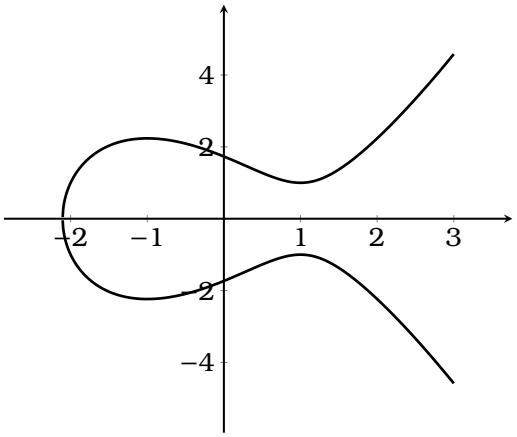
Αν οι συντελεστές $a_1, a_2, a_3, a_4, a_6 \in k$, τότε αυτή είναι ορισμένη πάνω στο k.
Επιπλέον, ορίζονται οι ποσότητες:

$$b_2 = a_1^2 + 4a_2 \tag{2.3}$$
$$b_4 = 2a_4 + a_1a_3 \tag{2.4}$$
$$b_6 = a_3^2 + 4a_6 \tag{2.5}$$
$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \tag{2.6}$$
$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \tag{2.7}$$
$$c_4 = b_2^2 - 24b_4 \tag{2.8}$$
$$c_6 = -b_2^3 + 36b_2b_4 - 216b_6 \tag{2.9}$$
$$j = \frac{c_4^3}{\Delta} \tag{2.10}$$

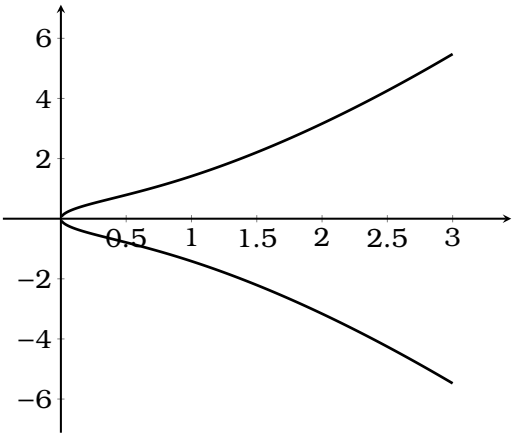
Η Δ ονομάζεται διακρίνουσα της εξίσωσης Weierstrass και το $j = j(E)$ ονομάζεται j-invariant της.

Ορισμός 2.5 (Ελλειπτική Καμπύλη)**.** *Μία **ελλειπτική καμπύλη** E/k είναι μια επίπεδη καμπύλη ορισμένη από την εξίσωση Weierstrass τέτοια ώστε $\Delta \neq 0$.*

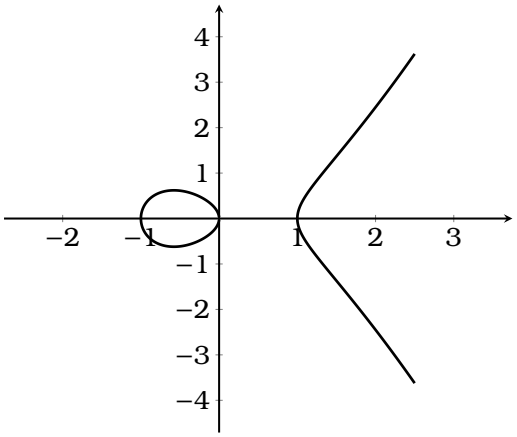
Θέτοντας $z = 0$ στην εξίσωση Weierstrass προκύπτει $x^3 = 0 \Rightarrow x = 0$. Επειδή το y δεν μπορεί να είναι 0, το μοναδικό σημείο της καμπύλης στο άπειρο είναι το $(0 : y : 0) = (0 : 1 : 0) = O$. Αυτό είναι το σημείο στο άπειρο που βρίσκεται σε κάθε κατακόρυφη ευθεία. Στα παρακάτω θα χρησιμοποιείται κυρίως η μη ομογενής μορφή της εξίσωσης Weierstrass γνωρίζοντας πως το O βρίσκεται πάντα πάνω στην καμπύλη.



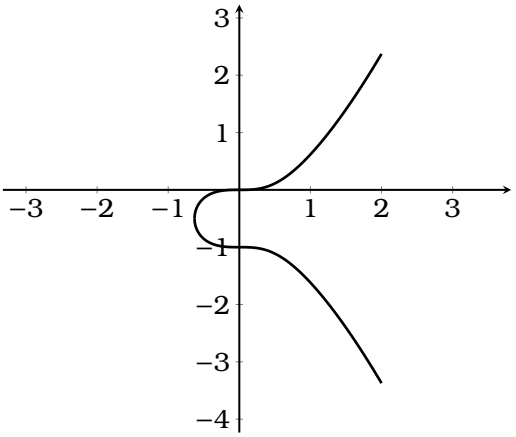
$y^2 = x^3 - 3x + 3$
$\Delta = -2160$



$y^2 = x^3 + x$
$\Delta = -64$



$y^2 = x^3 - x$
$\Delta = 64$



$y^2 + y = x^3$
$\Delta = -27$

Παρατήρηση 4. Σε περισσότερο προχωρημένη γλώσσα ένας ορισμός μίας ελλειπτικής καμπύλης E/k είναι πως είναι μία λεία προβολική καμπύλη γένους 1 ορισμένη πάνω από το k που περιέχει ένα k ρητό σημείο. Ο ορισμός του γένους ξεφεύγει από τα πλαίσια της εργασίας. Ωστόσο, μπορεί να αποδειχθεί πως κάθε ελλειπτική καμπύλη είναι ισόμορφη με μία καμπύλη που δίνεται από μία εξίσωση Weierstrass , αλλά και αντίστροφα, κάθε καμπύλη που ορίζεται από την εξίσωση Weierstrass και έχει $\Delta \neq 0$ ορίζει μία ελλειπτική καμπύλη [1, σ. 59].

2.2.2 Απλοποιημένες εξισώσεις Weierstrass

Η εξίσωση Weierstrass αν και η πιο γενική, μπορεί να απλοποιηθεί υπό ορισμένες προϋποθέσεις σε σχέση με την χαρακτηριστική του σώματος k πάνω στο οποίο είναι ορισμένη.

Θεώρημα 2.1. *Έστω E/k μία ελλειπτική καμπύλη. Με τις επιπλέον προϋποθέσεις που περιγράφονται παρακάτω, υπάρχουν μετασχηματισμοί*

$$x = u^2x' + r \qquad y = u^3y' + u^2sx' + t \qquad \mu\varepsilon\ u \in k^* \ \kappa\alpha\iota\ r, s, t \in k$$

τέτοιοι ώστε η E/k να έχει μία εξίσωση Weierstrass με την ακόλουθη μορφή :

1. *Αν* $\operatorname{char} k \neq 2, 3$

$$y^2 = x^3 + ax + b \qquad \Delta = -16(4a^3 + 27b^2) \qquad j = 1728\frac{4a^3}{4a^3 + 27b^2} \tag{2.11}$$

   Αυτή η εξίσωση ονομάζεται εξίσωση ***short Weierstrass***

2. *Αν* $\operatorname{char} k = 3$ *και* $j(E) \neq 0$

$$y^2 = x^3 + ax^2 + b \qquad \Delta = -a^3b \qquad j = -\frac{a^3}{b} \tag{2.12}$$

3. *Αν* $\operatorname{char} k = 3$ *και* $j(E) = 0$

$$y^2 = x^3 + ax + b \qquad \Delta = -a^3 \qquad j = 0 \tag{2.13}$$

4. *Αν* $\operatorname{char} k = 2$ *και* $j(E) \neq 0$

$$y^2 + xy = x^3 + ax^2 + b \qquad \Delta = b \qquad j = b^{-1} \tag{2.14}$$

5. *Αν* $\operatorname{char} k = 2$ *και* $j(E) = 0$

$$y^2 + cy = x^3 + ax + c \qquad \Delta = a^4 \qquad j = 0 \tag{2.15}$$

Μία καμπύλη που δίνεται την εξίσωση (2.12) ή την (2.14) λέγεται ***non-supersingular****.*
Μία καμπύλη που δίνεται την εξίσωση (2.13) ή την (2.15) λέγεται ***supersingular****.*

Απόδειξη. Έστω ότι η E/k δίνεται από την εξίσωση Weierstrass

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

1. Αφού η χαρακτηριστική του k δεν είναι 2 μπορεί να γίνει η συμπλήρωση του τετραγώνου για το y με την αντικατάσταση $y \mapsto \frac{1}{2}(y - a_1x - a_3)$

$$[\frac{1}{2}(y - a_1x - a_3)]^2 + (a_1x + a_3)[\frac{1}{2}(y - a_1x - a_3)] = x^3 + a_2x^2 + a_4x + a_6$$

   Αναπτύσσοντας το τετράγωνο στο αριστερό μέρος και κάνοντας τις επιμεριστικές πράξεις

$$\frac{1}{4}y^2 - \cancel{\frac{1}{2}y(a_1x + a_3)} + \frac{1}{4}(a_1x+a_3)^2 + \cancel{\frac{1}{2}y(a_1x + a_3)} - \frac{1}{2}(a_1x+a_3)^2 = x^3+a_2x^2+a_4x+a_6 \Rightarrow$$

$$
\begin{aligned}
y^2 - (a_1x + a_3)^2 &= 4x^3 + 4a_2x^2 + 4a_4x + 4a_6 \\
y^2 - a_1^2x^2 - 2a_1a_3 - a_3^2 &= 4x^3 + 4a_2x^2 + 4a_4x + 4a_6 \\
y^2 - a_1^2x^2 - 2a_1a_3 - a_3^2 &= 4x^3 + 4a_2x^2 + 4a_4x + 4a_6 \\
y^2 &= 4x^3 + (4a_2 + a_1^2)x^2 + (4a_4 + 2a_1a_3)x + (4a_6 + a_3^2) \\
y^2 &= 4x^3 + b_2x^2 + 2b_4x + b_6 \qquad (2.16)
\end{aligned}
$$

όπου τα b_2, b_4, b_6 όπως ορίστηκαν στις (1.3)-(1.5).
Αν επιπλέον η χαρακτηριστική του k δεν είναι ούτε 3 μπορεί να εξαφανιστεί ο x^2 όρος με την αντικατάσταση $(x, y) \mapsto (\frac{x - 3b_2}{36}, \frac{y}{108})$ στην (1.16)

$$
\begin{aligned}
\left(\frac{y}{108}\right)^2 =& 4\left(\frac{x - 3b_2}{36}\right)^3 + b_2\left(\frac{x - 3b_2}{36}\right)^2 + 2b_4\left(\frac{x - 3b_2}{36}\right) + b_6 \Rightarrow \\
\frac{y^2}{3^62^4} =& \frac{2^2}{2^63^6}(x^3 - 9x^2b_2 + 3^3xb_2^2 - 3^3b_2^3) + \frac{b_2}{2^43^4}(x^2 - 6xb_2 + 9b_2^2) \\
&+ \frac{2b_4}{2^23^2}x - \frac{1}{2 \cdot 3}b_2 + b_6 \Rightarrow \\
y^2 =& x^3 - \cancel{9x^2b_2} + 3^3xb_2^2 - 3^3b_2^3 + \cancel{3^2b_2x^2} - 3^32xb_2^2 + 3^4b_2^3 + 2^33^4b_4x \\
&- 3^52^3b_2 + 3^62^4b_6 \\
y^2 =& x^3 + (3^3b_2^2 - 3^32b_2^2 + 2^33^4b_4)x + (-3^3b_2^3 - 3^52^3b_2 + 3^62^4b_6) \\
y^2 =& x^3 - 27c_4x - 54c_6 \\
y^2 =& x^3 + ax + b
\end{aligned}
$$

Για την διακρίνουσα, $a_4 = a, a_6 = b, a_1 = a_3 = a_2 = b_2 = 0$
$b_4 = 2a, b_6 = 4b, c_4 = -24b_4 = -48a, c_6 = -216b_6 = -216\,4b$ και
$\Delta = -8b_4^3 - 27b_6^2 = -2^38a^3 - 4^227b^2 = -16(4a^3 + 27b^2)$.

$$
j = \frac{c_4^3}{\Delta} = \frac{-48^3a^3}{-16(4a^3 + 27b^2)} = \frac{(2^43)^3a^3}{16(4a^3 + 27b^2)} = \frac{2^{12}3^3a^3}{2^4(4a^3 + 27b^2)} = 1728\frac{4a^3}{4a^3 + 27b^2}
$$

2. Από την (1.16) και αφού η χαρακτηριστική του k είναι 3

$$
\begin{aligned}
y^2 &= x^3 + b_2x^2 + 2b_4x + b_6 \\
y^2 &= x^3 + a_2x^2 + a_4x + a_6 \qquad (2.17)
\end{aligned}
$$

Για την εξίσωση Weierstrass (1.17) προκύπτουν

$$
\begin{aligned}
&a_1 = a_3 = 0 \quad b_2 = 4a_2 = a_2 \quad b_4 = a_6 \quad b_6 = a_6 \quad b_8 = a_2a_6 - a_4^2 \\
&\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 = -a_2^2(a_2a_6 - a_4^2) - 8b_4^3 = a_2^2a_4^2 - a_2^3a_6 - a_4^3 \\
&c_4 = b_2^2 - \cancel{24b_4} = a_2^2 \quad j = \frac{a_2^6}{\Delta}
\end{aligned}
$$

Αν $j \neq 0$, τότε $a_2 \neq 0$, οπότε με την αντικατάσταση $x \mapsto x + \frac{a_4}{a_2}$ θα εξαφανιστεί ο

γραμμικός όρος

$$y^2 = \left(x + \frac{a_4}{a_2}\right)^3 + a_2\left(x + \frac{a_4}{a_2}\right)^2 + a_4\left(x + \frac{a_4}{a_2}\right) + a_6$$

$$y^2 = x^3 + 3x^2\frac{a_4}{a_2} + 3x\left(\frac{a_4}{a_2}\right)^2 + \left(\frac{a_4}{a_2}\right)^3 + a_2x^2 + 2xa_4 + \left(\frac{a_4}{a_2}\right)^2 + a_4x + \left(\frac{a_4^2}{a_2}\right) + a_6$$

$$y^2 = x^3 + a_2x^2 + \left(\frac{a_4}{a_2}\right)^3 + \frac{a_4^2}{a_2} + a_6$$

$$y^2 = x^3 + a_2x^2 + a_6$$

Για την τελευταία εξίσωση Weierstrass υπολογίζονται $a_1 = a_3 = a_4 = 0$ $b_2 = a_2, b_4 = 0, b_6 = a_6, b_8 = a_2a_6$ $\Delta = -a_2^3a_6$ $c_4 = a_2^2$ $j = \frac{c_4^3}{\Delta} = \frac{a_2^6}{-a_2^3a_6} = -\frac{a_2^3}{a_6}$

3. Από την εξίσωση Weierstrass (1.17) και από τα παραπάνω με $j = 0 \Rightarrow a_2 = 0$ και άρα βρίσκεται στην επιθυμητή μορφή με $a_1 = a_3 = a_2 = 0 = b_2 = b_8$ $b_4 = b_6 = a_6$ $\Delta = -a_4^3$ $j = 0$.

4. Ξεκινώντας πάλι από την εξίσωση Weierstrass υπολογίζονται

$$b_2 = a_1^2 \quad c_4 = b_2^2 - 24b_4 = a_1^4 \quad j = \frac{a_1^{12}}{\Delta} \Rightarrow a_1 \neq 0$$

και με την αντικατάσταση $(x, y) \mapsto \left(a_1^2x + \frac{a_3}{a_1}, a_1^3y + \frac{a_1^2a_4 + a_3^2}{a_1^3}\right)$

$$a_1^6y^2 + \frac{(a_1^2a_4 + a_3^2)^2}{a_1^6} + a_1(a_1^2x + \frac{a_3}{a_1})(a_1^3y + \frac{a_1^2a_4 + a_3^2}{a_1^3}) + a_3(a_1^3y + \frac{a_1^2a_4 + a_3^2}{a_1^3}) =$$
$$(a_1^2x + \frac{a_3}{a_1})^3 + a_2(a_1^2x + \frac{a_3}{a_1})^2 + a_4(a_1^2x + \frac{a_3}{a_1}) + a_6$$
$$a_1^6y^2 + \frac{(a_1^2a_4 + a_3^2)^2}{a_1^6} + a_1^6xy + (a_1^2a_4 + a_3^2)x =$$
$$a_1^6x^3 + a_1^3x^2a_3 + xa_3^2 + \frac{a_3^2}{a_1^3} + a_2a_1^4x^2 + \frac{a_2a_3^2}{a_1^2} + a_4a_1^2x + \frac{a_4a_3}{a_1} + a_6$$
$$y^2 + xy = x^3 + a_2x^2 + a_6 \tag{2.18}$$
$$a_1 = 1 \quad a_3 = a_4 = b_4 = b_6 = 0 \quad b_2 = 1 \quad b_8 = a_6 \quad c_4 = 1 \quad \Delta = a_6$$

5. $j = 0$ άρα $a_1 = 0$ άρα με εφαρμογή στην εξίσωση Weierstrass της αντικατάστασης $x \mapsto x + a_2$ προκύπτει

$$y^2 + a_3y = (x + a_2)^3 + a_2(x + a_2)^2 + a_4(x + a_2) + a_6$$
$$y^2 + a_3y = x^3 + x^2a_2 + a_2^2x + a_2^3 + a_2x^2 + a_2^3 + a_4x + a_4a_2 + a_6$$
$$y^2 + a_3y = x^3 + a_4x + a_6$$
$$a_1 = a_2 = b_2 = b_4 = c_4 = c_6 = 0 \quad b_6 = a_3^2 \quad b_8 = a_4^2 \quad j = 0 \quad \Delta = -27b_6^2 = b_6^2 = a_3^4$$

□

Σε όλες τις παραπάνω απλούστερες μορφές υπάρχει πάντα το σημείο στο άπειρο O.

2.2.3 Η διακρίνουσα

Όπως φάνηκε στην εισαγωγή θα οριστεί η πράξη της ομάδας πάνω σε ελλειπτικές καμπύλες χρησιμοποιώντας εφαπτομένη της καμπύλης σε ένα σημείο. Η απαίτηση $\Delta \neq 0$ εξασφαλίζει πως η εφαπτομένη της καμπύλης σε ένα συγκεκριμένο σημείο μπορεί να οριστεί πάντα.

Θεώρημα 2.2. *Μία καμπύλη E/k που ορίζεται από την εξίσωση Weierstrass είναι λεία αν και μόνο αν $\Delta \neq 0$.*

Απόδειξη. Γίνεται αρχικά η υπόθεση ότι $\Delta \neq 0$. Από την εξίσωση Weierstrass ισχύει

$$F(x,y,z) = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3 = 0$$

$\frac{\partial F}{\partial Z}(O) = 1 \neq 0$. Άρα το σημείο στο άπειρο δεν είναι ποτέ ιδιάζον. Θα γίνει χρήση, στην συνέχεια, των απλοποιημένων μορφών για τα σημεία που δεν είναι στο άπειρο. Αν η χαρακτηριστική του k δεν είναι 2 από την (1.16), $F(x,y,1) = f(x,y) = y^2 - 4x^3 + b_2x^2 + 2b_4x + b_6$ Αν $g(x) = 4x^3 + b_2x^2 + 2b_4x + b_6$ τότε για να είναι ιδιάζον σημείο το (x_0, y_0) εξισώνονται οι παράγωγοι με το 0 και προκύπτει

$$2y_0 = g(x_0) = g'(x_0) = 0$$

Άρα για να μην υπάρχει ιδιάζον σημείο πρέπει το $g(x)$ να μην έχει διπλή ρίζα στο x_0.
Η διακρίνουσα του κυβικού πολυωνύμου $ax^3 + bx^2 + cx + d$ είναι τότε

$$D = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd$$

Άρα στην περίπτωση του $g(x)$ κι αφού $4b_8 = b_2b_6 - b_4^2$

$$\begin{aligned} &4b_2^2b_4^2 - 4\cdot 4\cdot 8b_4^3 - 4b_2^3b_6 - 27\cdot 4^2b_6^2 + 18\cdot 4b_2 2b_4b_6 = \\ &4b_2^2(\cancel{b_2b_6} - 4b_8) + 16(9b_2b_4b_6 - 27b_6^2 - 8b_4^3) - \cancel{4b_2^3b_6} = 16\Delta \end{aligned}$$

Επομένως, το $g(x)$ δεν έχει διπλή ρίζα αν και μόνον αν $D \neq 0 \Leftrightarrow \Delta \neq 0$.

Αν η χαρακτηριστική του k είναι 2 και $j(E) \neq 0$ η E είναι όπως στην εξίσωση (1.14). Εξισώνοντας τις παραγώγους με 0 για να βρεθούν τυχόντα ιδιάζοντα σημεία

$$\begin{aligned} \frac{\partial f}{\partial y}(x_0,y_0) &= \cancel{2y_0} + x_0 = 0 \\ \frac{\partial f}{\partial y}(x_0,y_0) &= y_0 - 3x_0^2 = y_0 = 0 \end{aligned}$$

Αντικαθιστώντας $(x_0, y_0) = (0,0)$ στην (1.16) ισχύει $a_6 = 0$, όμως $\Delta = a_6 \neq 0$, προκύπτει το ζητούμενο.

Αν η χαρακτηριστική του k είναι 2 και $j(E) = 0$ η E είναι όπως στην εξίσωση (1.15). Για

τυχόν ιδιάζον σημείο (x_0, y_0)

$$\frac{\partial f}{\partial y}(x_0, y_0) = \cancel{2y} + a_3 = 0$$

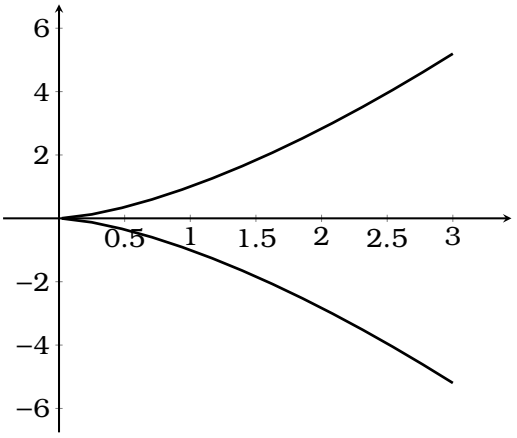
Όμως $\Delta = a_3^4 \neq 0 \Leftrightarrow \frac{\partial f}{\partial y}(x_0, y_0) \neq 0$.

Για την αντίθετη κατεύθυνση γίνται η υπόθεση πως η E δεν είναι λεία κι έχει το (x_0, y_0) ιδιάζον σημείο. Τότε η αντικατάσταση $(x, y) \mapsto (x + x_0, y + y_0)$ δεν μεταβάλλει το Δ, οπότε μπορεί να γίνει επιπλέον η υπόθεση πως $(x_0, y_0) = (0, 0)$. Από τη μη ομογενή μορφή

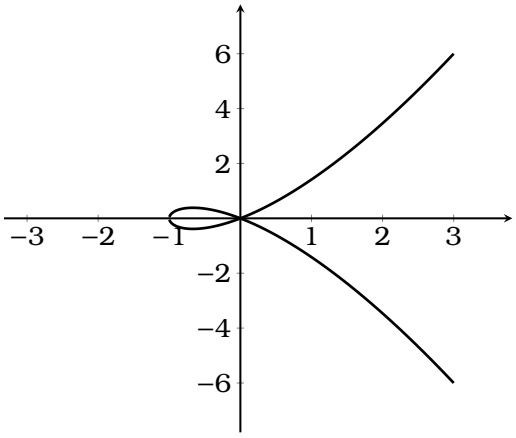
$$f(0,0) = 0 \Rightarrow a_6 = 0$$
$$\frac{\partial f}{\partial x}(0,0) = 0 \Rightarrow a_4 = 0$$
$$\frac{\partial f}{\partial x}(0,0) = 0 \Rightarrow a_3 = 0$$

Οπότε η E παίρνει την μορφή $E : y^2 + a_1xy - a_2x^2 - x^3 = 0$ η οποία έχει $\Delta = 0$.

□



$y^2 = x^3$
$\Delta = 0$



$y^2 = x^3 + x^2$
$\Delta = 0$

Κεφάλαιο 3

Η ομάδα της Ελλειπτικής Καμπύλης

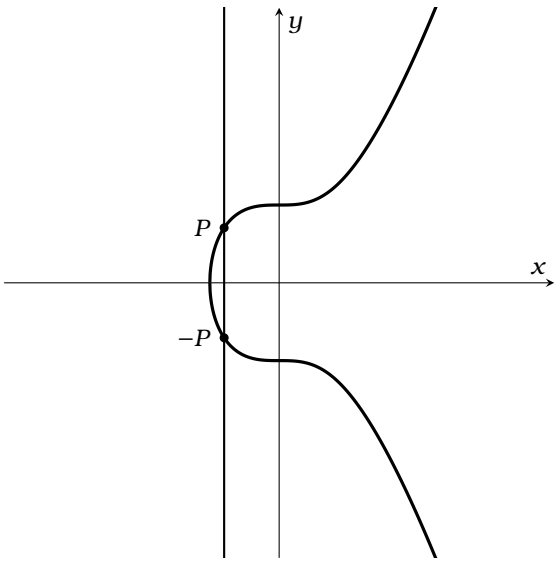
Στόχος αυτού του κεφαλαίου είναι η παρουσίαση της ομάδας των Ελλειπτικών Καμπυλών καθώς και μία ανάλυση της πολυπλοκότητας των υπολογισμών σε αυτή. Η πράξη για μία ελλειπτική καμπύλη E/k ορίζεται πάνω στο σύνολο των σημείων της, δηλαδή αν $k \leq L$ μια επέκταση σώματος του k, η πράξη είναι μία συνάρτηση $+ : E(L) \times E(L) \to E(L)$. Ορίζεται έτσι ώστε τρία σημεία τα οποία βρίσκονται στην ίδια ευθεία να αθροίζουν στο προσθετικό ουδέτερο, το οποίο είναι το μοναδικό σημείο στο άπειρο O. Τα γραφήματα που ακολουθούν αντιστοιχούν σε ελλειπτικές καμπύλες πάνω από το $\mathbb{R}$.

3.1 Short Weierstrass

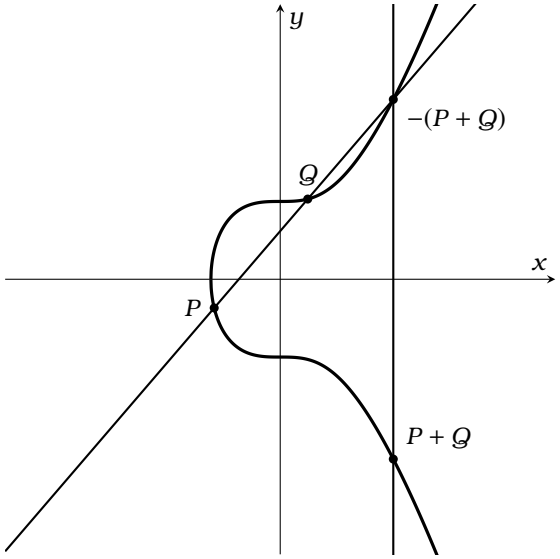
Έστω μία ελλειπτική καμπύλη E/k τέτοια ώστε $\text{char } k \neq 2, 3$ και $k \leq L$, τότε τα σημεία της $E(L)$ στο $\mathbb{A}^2(L)$ ικανοποιούν μία εξίσωση της μορφής $y^2 = x^3 + Ax + B, A, B \in k$ και $O = (0 : 1 : 0) \in E(L)$ το μόνο σημείο στο άπειρο. Το O είναι το προσθετικό ουδέτερο, δηλαδή

$$P + O = O + P = P, \quad \forall P \in E(L)$$

Αν $O \neq P \in E(L)$, τότε αυτό δεν βρίσκεται στο άπειρο, άρα $P = (x_0, y_0) = (x_0 : y_0 : 1)$. Αφού τρία σημεία αθροίζουν στο O, προκύπτει πως $P + -P + O = O$, άρα το $-P$ είναι τρίτο σημείο τομής της κάθετης ευθείας $x = x_0$ και της E. Δηλαδή, $-P = (x_0, -y_0)$.



Έστω τώρα $P = (x_1, y_1) = (x_1 : y_1 : 1) \in E(L)$ και $Q = (x_2, y_2) = (x_2 : y_2 : 1) \in E(L)$, με $x_1 \neq x_2$. Τότε το $R = -(P + Q) \in E(L)$ είναι το τρίτο σημείο τομής της ευθείας $\overline{PQ}$ και της καμπύλης E.



Αυτό προκύπτει αφού $P + Q + R = O \Rightarrow R = -(P + Q)$. Άρα, το $P + Q$ είναι το συμμετρικό του ως προς τον άξονα των x. Η $\overline{PQ}$ έχει κλίση $m = \dfrac{y_2 - y_1}{x_2 - x_1}$ και δίνεται από την εξίσωση $y - y_1 = m(x - x_1)$. Αντικαθιστώντας την εξίσωση της ευθείας στην εξίσωση short Weierstrass προκύπτει

$$\begin{aligned} (m(x - x_1) + y_1)^2 &= x^3 + Ax + B \\ m^2x^2 - 2m^2x_1x + m^2x_1 + y_1^2 + 2mxy_1 - 2mx_1y_1 &= x^3 + Ax + B \\ g(x) = x^3 - m^2x^2 + \ldots &= 0 \end{aligned}$$

Όμως, το μονικό πολυώνυμο $g(x) \in k[x]$ έχει δύο ρίζες στο L άρα και η τρίτη θα είναι στο L αφού το $g(x)$ παραγοντοποιείται ως εξής

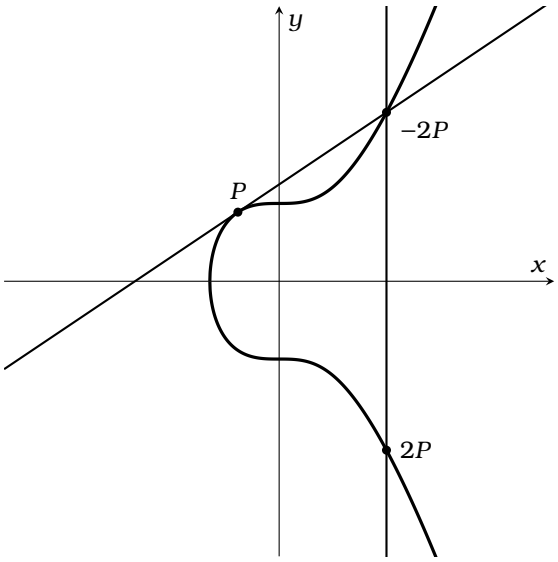
$$\begin{aligned} g(x) &= (x - x_1)(x - x_2)(x - x_3) \\ g(x) &= x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_2x_3 + x_3x_1)x - (x_1x_2x_3) \end{aligned}$$

Εξισώνοντας του συντελεστές του x^2

$$\begin{aligned} x_1 + x_2 + x_3 &= m^2 \\ x_3 &= m^2 - x_1 - x_2 \end{aligned}$$

αντικαθιστώντας το x_3 στην εξίσωση της $\overline{PQ}$ υπολογίζεται το $-y_3$, οπότε $y_3 = m(x_1 - x_3) - y_1$. Επομένως $P + Q = (x_3, y_3) \in E(L)$.

Αν $x_1 = x_2$ από την εξίσωση short Weierstrass προκύπτει πως $y_1 = \pm y_2$. Αν $y_1 = -y_2$, τότε $Q = -P$, οπότε $P + Q = O$. Αν $y_1 = y_2$, τότε $P + Q = 2P$. Η $\overline{PQ}$ είναι η εφαπτομένη της καμπύλης στο σημείο P.



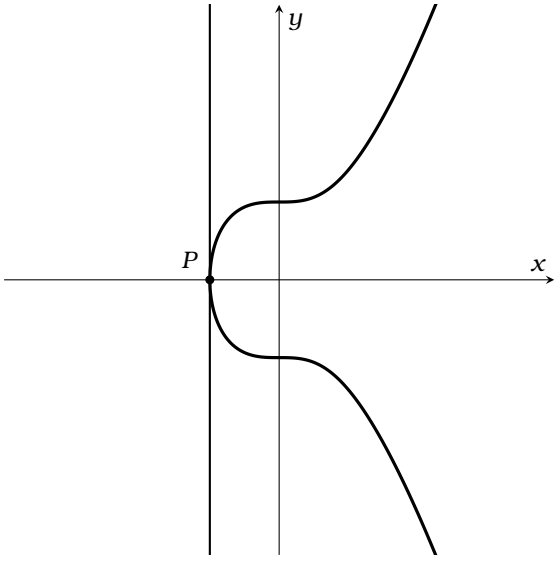
Με διαφόριση της short Weierstrass κατά μέλη

$$2ydy = 3x^2dx + Adx$$
$$m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}$$

Οπότε

$$x_3 = m^2 - 2x_1$$
$$y_3 = m(x_1 - x_3) - y_1$$

όπου $2P = (x_3, y_3)$. Στην περίπτωση που το $y_1 = 0$ οπότε δεν ορίζεται η κλίση της $\overline{PQ}$ και άρα αυτή είναι κατακόρυφη, $2P = O$.



Θεώρημα 3.1. *Έστω E/k μια ελλειπτική καμπύλη με* $\operatorname{char} k \neq 2,3$ *που δίνεται από την εξίσωση short Weierstrass*

$$y^2 = x^3 + Ax + B, \quad A, B \in k$$

με $O = (0:1:0)$ το μοναδικό σημείο στο άπειρο. Η πράξη $+$ ορίζεται στο σύνολο $E(L)$,για $k \leq L$ ως εξής

$$P + O = O + P = P, \quad \forall P \in E(L)$$

Για $P = (x_1, y_1), Q = (x_2, y_2) \in E(L)$. Τότε

$$P + Q = \begin{cases} (m^2 - x_1 - x_2, m(x_1 - x_3) - y_1) & m = \frac{y_2 - y_1}{x_2 - x_1}, x_1 \neq x_2 \\ (m^2 - 2x_1, m(x_1 - x_3) - y_1) & m = \frac{3x_1^2 + A}{2y_1}, x_1 = x_2, y_1 = y_2 \neq 0 \\ O & x_1 = x_2, y_1 = y_2 = 0 \\ O & x_1 = x_2, y_1 \neq y_2 \end{cases}$$

και $-P = (x, -y)$. Το $(E(L), +)$ είναι αβελιανή ομάδα.

Απόδειξη. Είναι εμφανές από τους τύπους πως αφού $A, B \in L$, τότε το $P + Q$ έχει πάντα συντεταγμένες στο L. Το O από τον ορισμό του δρα ως προσθετικό ουδέτερο και όπως αναφέρθηκε $P + (-P) = O$, οπότε υπάρχουν αντίθετα στοιχεία. Μένει να δειχθεί πως η $+$ έχει την προσεταιριστική ιδιότητα, το οποίο αφήνεται για το παράρτημα Α΄. □

Για τον υπολογισμό της $+$ χρειάζονται από τους τύπους οι εξής υπολογισμοί στο σώμα L:

1. 3 πολλαπλασιασμοί και 1 αντιστροφή, αν $x_1 \neq x_2$
2. 4 πολλαπλασιασμοί και 1 αντιστροφή, για τον υπολογισμό του $2P$ (λόγω του επιπλέον x_1^2 στον αριθμητή του m).

Για την αποφυγή της χρονοβόρας αντιστροφής οι πράξεις μπορούν να γίνουν χρησιμοποιώντας προβολικές συντεταγμένες.

Παράδειγμα 3.1. Έστω $E/\mathbb{Q}$ η ελλειπτική καμπύλη

$$y^2 = x^3 + 17$$

Έχει τα σημεία με ακέραιες συντεταγμένες $P_1 = (-2, 3), P_2 = (-1, 4), P_3 = (2, 5), P_4 = (4, 9), P_5 = (8, 23), P_6 = (43, 282), P_7 = (52, 375), P_8 = (5234, 378661)$ όπου

$$P_2 = -2P_1 + P_3 \quad P_4 = P_1 - P_3 \quad P_5 = -2P_1 \quad P_6 = -P_1 + 2P_3 \quad P_7 = 3P_1 - P_3$$

Παράδειγμα 3.2. Έστω $E/\mathbb{F}_5$ η ελλειπτική καμπύλη

$$y^2 = x^3 + x + 1$$

Για την εύρεση όλων των σημείων της $E(\mathbb{F}_5)$ επιλέγονται όλες οι πιθανές τιμές για το x και

λύνεται η εξίσωση ως προς y.

$$x = 0 \Rightarrow y^2 = 1 \Rightarrow y = 1, 4$$
$$x = 1 \Rightarrow y^2 = 3, \left(\frac{3}{5}\right) = -1$$
$$x = 2 \Rightarrow y^2 = 1 \Rightarrow y = 1, 4$$
$$x = 3 \Rightarrow y^2 = 1 \Rightarrow y = 1, 4$$
$$x = 4 \Rightarrow y^2 = 4 \Rightarrow y = 2, 3$$

Άρα συνολικά $E(\mathbb{F}_5) = \{O, (0,1), (0,4), (2,1), (2,4), (3,1), (3,4), (4,2), (4,3)\}$. Η $E(\mathbb{F}_5)$ είναι κυκλική τάξης 9 και παράγεται από το $P = (0,1)$. Για τον υπολογισμό του $2P$

$$m = \frac{3x_1^2 + a}{2y_1} = \frac{1}{2} = 2^{-1} \equiv 3 \mod 5$$

αφού $2 \cdot 3 = 6 \equiv 1 \mod 5$, άρα $2^{-1} \equiv 3 \mod 5$.

$$x_3 = m^2 - 2x_1 \equiv 4 \mod 5$$
$$y_3 = m(x_1 - x_3) - y_1 \equiv 3(0-4) - 1 \equiv 2 \mod 5$$

Άρα $2P = (4, 2)$.

3.1.1 Η Πράξη Ομάδας σε προβολικές συντεταγμένες

Στους τύπους του Θεωρήματος 3.1 μπορούν να αντικατασταθούν τα x_1, y_1, x_2, y_2 με $x_1/z_1, y_1/z_1, x_2/z_2, y_2/z_2$ οπότε προκύπτουν

$$P = (x_1 : y_1 : z_1), Q = (x_2 : y_2 : z_2), P + Q = (x_3 : y_3 : z_3)$$

Αν $P \neq \pm Q$,

$$x_3 = (x_2z_1 - x_1z_2)((y_2z_1 - y_1z_2)^2 z_1z_2 - (x_2z_1 - x_1z_2)^2(x_2z_1 + x_1z_2))$$
$$y_3 = (y_2z_1 - y_1z_2)((x_2z_1 - x_1z_2)^2(x_2z_1 + 2x_1z_2) - (y_2z_1 - y_1z_2)^2 z_1z_2) - (x_2z_1 - x_1z_2)^3 y_1z_2$$
$$z_3 = (x_2z_1 - x_1z_2)^3 z_1z_2$$

Αν $P = Q$,

$$x_3 = 2y_1z_1(A^2(z_1^2 + 3x_1^2)^2 - 8x_1y_1^2z_1)$$
$$y_3 = A(z_1^2 + 3x_1^2)(12x_1y_1^2z_1 - A^2(z_1^2 + 3x_1^2)^2) - 8y_1^4z_1^2$$
$$z_3 = (2y_1z_1)^3$$

Αν $P = -Q, P + Q = O$.

Οι υπολογισμοί για την περίπτωση $P_1 \neq \pm Q$, γίνονται χρησιμοποιώντας τα ακόλουθα

ενδιάμεσα αποτελέσματα :

$$u = y_2z_1 - y_1z_2 \qquad v = x_2z_1 - x_1z_2 \qquad w = u^2z_1z_2 - v^3 - 2v^2x_1z_2$$
$$x_3 = vw \qquad y_3 = u(v^2x_1z_2 - w) - v^3y_1z_2 \qquad z_3 = v^3z_1z_2$$

Οπότε απαιτούνται 14 πολλαπλασιασμοί και καμία αντιστροφή. Ομοίως για την περίπτωση $P = Q$:

$$t = Az_1^2 + 3x_1^2 \qquad u = y_1z_1 \qquad v = ux_1y_1 \qquad w = t^2 - 8v$$
$$x_3 = 2uw \qquad y_3 = t(4v - w) - 8y_1^2u^2 \qquad z_3 = 8u^3$$

Οπότε απαιτούνται 12 πολλαπλασιασμοί και καμία αντιστροφή.

3.2 Πράξη Ομάδας σε Γενικές Εξισώσεις Weierstrass

Σε αντιστοιχία με την προηγούμενη ενότητα μπορεί να οριστεί η πράξη ομάδας για ελλειπτικές καμπύλες στην μορφή Weierstrass δηλαδή η E/k να δίνεται από εξίσωση της μορφής

$$F(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0 \tag{3.1}$$

με $O = (0 : 1 : 0)$ το μόνο σημείο στο άπειρο. Σε αυτή την περίπτωση για $P = (x_0, y_0) \in E(L)$ η ευθεία που διέρχεται από το P είναι η $L : x - x_0 = 0$ και αντικαθιστώντας στην εξίσωση της καμπύλης $F(x_0, y) = c(y - y_0)(y - y_0') = y^2 + (a_1x_0 + a_3)y - x_0^3 - a_2x_0^2 - a_4x_0 - a_6$. Αφού ο συντελεστής του y είναι το αντίθετο του αθροίσματος των ριζών της εξίσωσης, οι ρίζες της είναι y_0 και $y_0' = -a_1x_0 - a_3 - y_0$. Οπότε, $-P = (x_0, -y_0 - a_1x_0 - a_3)$. Για την πρόσθεση δύο σημείων $P = (x_1, y_1), Q = (x_2, y_2) \in E(L)$ προκύπτει πως αν $x_1 = x_2$ και $y_1 + y_2 + a_1x_2 + a_3 = 0$, τότε $P = -Q$ και άρα $P + Q = O$. Διαφορετικά, η ευθεία που διέρχεται από τα P, Q (εφαπτομένη αν $P = Q$) έχει εξίσωση $y = \lambda x + \nu$. Αντικαθιστώντας στην εξίσωση της E και παραγοντοποιώντας $F(x, \lambda x + \nu) = c(x - x_1)(x - x_2)(x - x_3)$ οπότε $c = -1$ και $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$, $y_3 = \lambda x_3 + \nu$. Τέλος με εφαρμογή του τύπου της $P + Q = -(x_3, y_3)$.

Έστω, λοιπόν, μία Ελλειπτική καμπύλη E/k και L/k που ορίζεται από την εξίσωση Weierstrass. Στο σύνολο $E(L)$ ορίζεται η πράξη + ως εξής:

$$P + O = O + P = P, \quad \forall P \in E(L)$$

Αν $P = (x_1, y_1), Q = (x_2, y_2) \in E(L)$, τότε $-P = (x_0, -y_0 - a_1x_0 - a_3)$ και $(x_3, y_3) = (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, -(\lambda + a_1)x_3 - \nu - a_3)$

$$P + Q = \begin{cases} (x_3, y_3) & \lambda = \frac{y_2 - y_1}{x_2 - x_1}, \nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}, x_1 \neq x_2 \\ (x_3, y_3) & \lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}, P = Q, y_1 + y_2 + a_1x_2 + a_3 \neq 0 \\ O & x_1 = x_2, y_1 + y_2 + a_1x_2 + a_3 = 0 \end{cases}$$

Παράδειγμα 3.3. Έστω η καμπύλη $E/\mathbb{F}_2$

$$y^2 + xy = x^3 + 1$$

με $E(\mathbb{F}_2) = \{O, (0,1), (1,0), (1,1)\}$. Για τα σημεία $E(\mathbb{F}_4)$ με το ανάγωγο πολυώνυμο $x^2 + x + 1 \in \mathbb{F}_2[x]$ σχηματίζεται το $\mathbb{F}_2[x]/\langle x^2 + x + 1\rangle$ το οποίο είναι σώμα με 4 στοιχεία και $a = x + \langle x^2 + x + 1\rangle$, τότε το $\mathbb{F}_4 = \{0, 1, a, 1 + a\}$ με $a^2 + a + 1 = 0 \Rightarrow (a + 1)(a^2 + a + 1) = a^3 + a^2 + a + a^2 + a + 1 = a^3 + 1 = 0 \Rightarrow a^3 = 1$.

$$\begin{aligned}
&x = 0 \Rightarrow y^2 = 1 \Rightarrow y = 1\\
&x = 1 \Rightarrow y^2 + y = 0 \Rightarrow y = 0, 1\\
&x = a \Rightarrow y^2 + ay = a^3 + 1 = 0 \Rightarrow y = 0, a\\
&x = a^2 \Rightarrow y^2 + a^2 y = a^6 + 1 = 0 \Rightarrow y = 0, a^2
\end{aligned}$$

Επομένως $E(\mathbb{F}_4) = \{O, (0,1), (1,0), (1,1), (a,0), (a,a), (1+a,0), (1+a, 1+a)\}$ κυκλική τάξης 8 που με γεννήτορες τα $(a,0), (a,a), (1+a,0), (1+a, 1+a)$.

3.3 Πολλαπλασιασμός ακέραιου με σημείο

Έστω E/k μία Ελλειπτική καμπύλη, L/k και $P \in E(L)$. Ορίζεται για $n \in \mathbb{Z}$ η πράξη $nP = P + P + ... + P$, n φορές αν $n > 0$, διαφορετικά ορίζεται $nP = (-P) + (-P) + \ldots + (-P)$, $|n|$ φορές αν $n < 0$. Αν $n = 0$ τότε $nP = O$. Στις κρυπτογραφικές εφαρμογές των ελλειπτικών καμπυλών υπάρχει συνεχής ανάγκη για τον υπολογισμό ποσοτήτων nP για γνωστό ακέραιο n και γνωστό σημείο $P \in E(L)$. Στην περίπτωση που ο $n < 0$ μπορεί να υπολογιστεί πρώτα το $Q = |n|P$ και τότε το αποτέλεσμα θα είναι το $nP = -Q$.

3.3.1 Επαναλαμβανόμενος Διπλασιασμός

Ένας τρόπος να υπολογιστεί σε πολυωνυμικό χρόνο ως προς την δυαδική αναπαράσταση του n είναι η μέθοδος του επαναλαμβανόμενου διπλασιασμού. Αν η δυαδική αναπαράσταση του $n \in \mathbb{N}$ είναι $n = \sum_{i=0}^{l-1} a_i 2^i, a_i \in \{0,1\}$ τότε

$$nP = (\sum_{i=0}^{l-1} a_i 2^i)P = \sum_{i=0}^{l-1} a_i 2^i P$$

όπου το δεύτερο άθροισμα αναφέρεται σε πρόσθεση σημείων. Επομένως αρκεί να υπολογιστούν τα $2^i P$ για $i = 0, 1, \ldots, l-1$ και να προστεθούν στο O όσα από αυτά αντιστοιχούν σε μη μηδενικό a_i. Για παράδειγμα, για τον υπολογισμό του $19P$ με $19 = 1 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4$, υπολογίζονται πρώτα τα

$$2P = P + P, \quad 4P = 2P + 2P, \quad 8P = 4P + 4P, \quad 16P = 8P + 8P$$

και $19P = 16P + 2P + P$. Ο υπολογισμός των $2^i P$ γίνεται με διπλασιασμό και απαιτεί $l - 1$ διπλασιασμούς. Αν με $n = (a_{l-1}, a_{l-1}, \ldots, a_1, a_0)$ συμβολίζεται η δυαδική αναπαράσταση

του n η παραπάνω διαδικασία περιγράφεται από τον παρακάτω αλγόριθμο.

Αλγοριθμος 3.1: *Double and Add*

Input $n = (a_{l-1}, a_{l-1}, \ldots, a_1, a_0), P \in E(L)$
Output nP
  $Q \leftarrow O$
  for $i \leftarrow 0$ **to** $l-1$ **do**
    if $a_i = 1$ **then**
      $Q \leftarrow Q + P$
    end if
    $Q \leftarrow 2Q$
  end for
  return Q

Ο αλγόριθμος 3.1 απαιτεί στην χειρότερη $\log_2 n$ προσθέσεις σημείων και $\log_2 n$ διπλασιασμούς. Ωστόσο, ο αναμενόμενος αριθμός άσων στην δυαδική αναπαράσταση του n είναι $\frac{\log_2 n}{2}$ οπότε τόσος είναι κι ο αναμενόμενος αριθμός προσθέσεων.

3.3.2 Non-Adjacent Form

Η αντιστροφή στην περίπτωση της εξίσωσης short Weierstrass δίνεται από $-P = (x, -y)$ και στην περίπτωση της γενικότερης εξίσωσης Weierstrass από $-P = (x, -y - a_1 x - a_3)$. Είναι κατ' αυτόν τον τρόπο η αφαίρεση σημείων ουσιαστικά η ίδια από άποψη υπολογισμών με την πρόσθεση σημείων. Επομένως, μπορεί να χρησιμοποιηθεί μία αναπαράσταση για τους ακεραίους που επιτρέπει στα ψηφία να έχουν αρνητικές τιμές.

Ορισμός 3.1 (Non-Adjacent Form)**.** *Έστω $n \in \mathbb{N}$. Τότε η n Non-Adjacent Form αναπαράσταση του n είναι η (μοναδική) ακολουθία $n = \sum_{i=0}^{l-1} a_i 2^i$ με $a_i \in \{-1, 0, 1\}$, $a_{l-1} \neq 0$ και $a_{i+1} a_i = 0$ για $0 \leq i \leq l-1$. Συμβολίζεται NAF(n)*

Η NAF αναπαράσταση ενός φυσικού n είναι στην χειρότερη κατά ένα ψηφίο μεγαλύτερη από την δυαδική αναπαράσταση του n, ενώ η μέση πυκνότητα των μη μηδενικών στοιχείων στην NAF είναι $\frac{1}{3}$. Η NAF αναπαράσταση ενός φυσικού n μπορεί να υπολογιστεί με διαδοχικές διαιρέσεις με το 2, επιτρέποντας τα υπόλοιπα να είναι $0, \pm 1$. Αν ο αριθμός k που είναι να διαιρεθεί είναι μονός, το υπόλοιπο r επιλέγεται ώστε το πηλίκο $\frac{k-r}{2}$ να είναι ζυγός, επιβάλλοντας το επόμενο ψηφίο να είναι 0. Αυτή η διαδικασία αποτυπώνεται στον αλγόριθμο 3.2.

Αλγοριθμος 3.2: *Υπολογισμός NAF αναπαράστασης φυσικού αριθμού*

Input $k \in \mathbb{N}$
Output NAF(k)
  $i \leftarrow 0$
  while $k \geq 1$ **do**
    if $k \equiv 1 \mod 2$ **then**
      $k_i \leftarrow 2 - (k \mod 4)$
      $k \leftarrow k - k_i$
    else
      $k_i \leftarrow 0$
    end if
    $k \leftarrow \frac{k}{2}$
    $i \leftarrow i + 1$
  end while
  return $(k_{i-1}, k_{i-2}, \ldots, k_1, k_0)$

Παράδειγμα 3.4 (Εφαρμογή του Αλγορίθμου 3.2)**.** Για τον υπολογισμό του NAF(29)

29		$29 = 4 \cdot 7 + 1$
14	1	
7	0	$7 = 2 \cdot 4 - 1$
4	-1	
2	0	
1	0	$1 = 0 \cdot 4 + 1$
0	1	

οπότε $29 = 2^5 - 2^2 + 2^0$

Κατ' αντιστοιχία με τον αλγόριθμο 3.1 ο ακόλουθος αλγόριθμος υπολογίζει το $nP, n \in \mathbb{N}, P \in E(k)$ χρησιμοποιώντας την NAF αναπαράσταση του n και αφαιρέσεις όπου αυτές χρειάζονται.

Αλγοριθμος 3.3: *Addition Subtraction*

Input NAF$(n), n \in \mathbb{N}, P \in E(k)$
Output nP
  $Q \leftarrow O$
  for $i \leftarrow l-1$ **downto** 0 **do**
    $Q \leftarrow 2Q$
    if $n_i = 1$ **then**
      $Q \leftarrow Q + P$
    end if
    if $n_i = -1$ **then**
      $Q \leftarrow Q - P$
    end if
  end for
  return Q

Ο αλγόριθμος 3.3 απαιτεί στην χειρότερη $\log_2 n$ προσθέσεις σημείων και $\log_2 n$ διπλασιασμούς όπως και ο 3.1. Ωστόσο, επειδή ο αναμενόμενος αριθμός μη μηδενικών ψηφίων στην NAF αναπαράσταση του n είναι $\frac{\log_2 n}{3}$ οπότε τόσος είναι κι ο αναμενόμενος αριθμός προσθέσεων.

3.4 Καμπύλες Koblitz

Οι καμπύλες Koblitz είναι ελλειπτικές καμπύλες που ορίζονται πάνω από το $\mathbb{F}_2$:

$$E_0 : y^2 + xy = x^3 + 1$$
$$E_1 : y^2 + xy = x^3 + x^2 + 1$$

οπότε για κρυπτογραφικές εφαρμογές χρησιμοποιούνται οι ομάδες $E_0(\mathbb{F}_{2^m})$ και $E_1(\mathbb{F}_{2^m})$.

Προκύπτει πως για κάθε $l \mid m \Rightarrow \mathbb{F}_{2^l} \leq \mathbb{F}_{2^m}$ και άρα $E_a(\mathbb{F}_{2^l}) \leq E_a(\mathbb{F}_{2^m})$, επομένως $|E_a(\mathbb{F}_{2^l})| \mid |E_a(\mathbb{F}_{2^m})|$. Συγκεκριμένα, για $l = 1, |E_0(\mathbb{F}_2)| = 4$ και $|E_1(\mathbb{F}_2)| = 2$ κι αφού για κρυπτογραφικές εφαρμογές είναι επιθυμητά σημεία με μεγάλη πρώτη τάξη, επιλέγονται m τέτοια ώστε η τάξη του $E_0(\mathbb{F}_{2^m}) = 4p$ και $E_1(\mathbb{F}_{2^m}) = 2q$, όπου p, q πρώτοι.

Χρησιμοποιώντας τον αυτομορφισμό του Frobenius $\phi_2(x) = x^2$ (για τον οποίο ισχύει πως $\phi_2(x+y) = \phi_2(x) + \phi_2(y)$ και $\phi_2(xy) = \phi_2(x)\phi_2(y), \forall x, y \in \mathbb{F}_{2^m}$) προκύπτει πως αν $(x, y) \in E_a(\mathbb{F}_{2^m}), a \in \{0, 1\}$ τότε και $(x^2, y^2) \in E_a(\mathbb{F}_{2^m})$, διότι

$$y^2 + xy = x^3 + ax^2 + 1 \Rightarrow$$
$$\phi_2(y^2 + xy) = \phi_2(x^3 + ax^2 + 1) \Rightarrow$$
$$\phi_2(y)^2 + \phi_2(x)\phi_2(y) = \phi_2(x)^3 + \phi_2(a)\phi_2(x)^2 + \phi_2(1)$$

Όμως $\phi_2(0) = 0, \phi_2(1) = 1$ άρα και $\phi_2(a) = a \in \{0, 1\}$ αφού ο ϕ_2 αφήνει τα στοιχεία του $\mathbb{F}_2$ σταθερά. Τελικά,

$$\phi_2(y)^2 + \phi_2(x)\phi_2(y) = \phi_2(x)^3 + a\phi_2(x)^2 + 1$$

άρα τα $(x^2, y^2) = (\phi_2(x), \phi_2(y)) \in E_a(\mathbb{F}_{2^m})$.

Επιπλέον, επιβεβαιώνεται πως $(x^4, y^4)+2(x, y) = (-1)^{1-a}(x^2, y^2)$ ή συμβολίζοντας $\tau(x, y) = (x^2, y^2)$,

$$\begin{aligned} \tau(\tau(P)) + 2P = (-1)^{1-a}\tau(P), \quad \forall P \in E_a(\mathbb{F}_{2^m}) \iff \\ (\tau^2 + 2)P = (-1)^{1-a}\tau(P), \quad \forall P \in E_a(\mathbb{F}_{2^m}) \end{aligned}$$

Βλέποντας το τ σαν τον μιγαδικό αριθμό που ικανοποιεί την $\tau^2 + 2 = (-1)^{1-a}\tau$ δηλαδή τον $\tau = \frac{(-1)^{1-a}+\sqrt{-7}}{2}$, μπορεί να οριστεί ο πολλαπλασιασμός ενός σημείου P με ένα στοιχείο του $\mathbb{Z}[\tau]$ ως εξής: αν $u_{l-1}\tau l - 1 + \ldots + u_1\tau_1 + u_0 \in \mathbb{Z}[\tau], u_i \in \mathbb{Z}$ και $P \in E_a(\mathbb{F}_{2^m})$, τότε

$$(u_{l-1}\tau^{l-1} + \ldots + u_1\tau + u_0)(P) = u_{l-1}\tau^{l-1}(P) + \ldots + u_1\tau_1(P) + u_0P$$

Ο στόχος είναι, λοιπόν, ο υπολογισμός του nP χρησιμοποιώντας μία αναπαράσταση του $n \in \mathbb{N}$ σαν στοιχείο του $\mathbb{Z}[\tau]$, με τελικά λιγότερες πράξεις. Αξίζει να σημειωθεί πως ο υπολογισμός του $\tau(P)$ χρησιμοποιώντας μια Normal Basis, δηλαδή μία βάση του $\mathbb{F}_{2^m}$ σαν διανυσματικό χώρο πάνω από το $\mathbb{F}_2$ της μορφής $\{a, a^2, a^{2^2}, \ldots, a^{2^{m-1}}\}$, απαιτεί απλά μία αριστερή ολίσθηση.

Παράδειγμα 3.5 ($a = 0$)**.**

$$\begin{aligned} 9 = \tau^5 - \tau^3 + 1, \quad \text{επομένως} \\ 9P = \tau^5(P) - \tau^3(P) + P = (x^{32}, y^{32}) - (x^8, y^8) + (x, y) \end{aligned}$$

για τον υπολογισμό του $9P$ απαιτούνται 5 ολισθήσεις, 2 προσθέσεις και μία αφαίρεση στην $E_0(\mathbb{F}_{2^m})$.

Κάθε στοιχείο του $\mathbb{Z}[\tau]$ μπορεί να γραφεί στη μορφή $x + y\tau$ αφού κάθε δύναμη του τ μεγαλύτερη του 2 μπορεί να γραφεί από μικρότερες χρησιμοποιώντας τη σχέση $\tau^2 = (-1)^{1-a} - 2$ και ο δακτύλιος είναι $\mathbb{Z}[\tau]$ είναι Ευκλείδια περιοχή με Ευκλείδια εκτίμηση την

$$N(x + y\tau) = (x + y\tau)\overline{(x + y\tau)} = x^2 + (-1)^{1-a}xy + 2y^2$$

δηλαδή $\forall a, b \in \mathbb{Z}[\tau], a \neq 0$ υπάρχουν $q, r \in \mathbb{Z}[\tau]$ τέτοια ώστε $b = qa + r$ με $N(r) < N(a)$. Αφού $N(\tau) = 2$ το υπόλοιπο r μετά από διαίρεση με τ θα είναι $r = 0, \pm 1$.

Θεώρημα 3.2 (Κριτήρια διαιρετότητας με τ και τ^2)**.** *Έστω* $x + y\tau \in \mathbb{Z}[\tau]$.

1. $\tau \mid x + y\tau \iff x \equiv 0 \mod 2$.
2. $\tau^2 \mid x + y\tau \iff x \equiv 2y \mod 4$.

Απόδειξη. 1. Αν $x \equiv 0 \mod 2 \Rightarrow x = 2v, v \in \mathbb{Z}$, τότε

$$\begin{aligned} (y + (-1)^{1-a}v - \tau v)\tau = y\tau + (-1)^{1-a}v\tau + \tau^2 v = y\tau + v((-1)^{1-a}\tau + \tau^2) = y\tau + 2v \\ = x + y\tau \end{aligned}$$

Αντίστροφα,

$$\begin{aligned}(u + v\tau)\tau &= u\tau + v\tau^2 = u\tau + v((-1)^{1-a}\tau - 2)\\ &= -2v + (u + (-1)^{1-a}v)\tau\end{aligned}$$

2. Λύνοντας την απο πάνω σχέση ως προς u, v για την εύρεση του πηλίκου $(u, v) = (y + \frac{(-1)^{1-a}x}{2}, -\frac{x}{2})$. Το πηλίκο διαιρείται από το τ αν και μόνο αν ο $y + \frac{(-1)^{1-a}x}{2}$ είναι ζυγός ή ισοδύναμα

$$y + \frac{(-1)^{1-a}x}{2} = 2k \iff 2y + (-1)^{1-a}x = 4k \iff 2y \equiv x \mod 4$$

αφού ο x είναι ζυγός.

□

Σε αντιστοιχία με την NAF αναπαράσταση ορίζεται η TNAF αναπαράσταση για ένα θετικό ακέραιο.

Ορισμός 3.2 (TNAF)**.** *Έστω $n \in \mathbb{N}$. Τότε η n τ-αδική Non-Adjacent Form αναπαράσταση του n είναι η (μοναδική) ακολουθία $n = \sum_{i=0}^{l-1} a_i\tau^i$ με $a_i \in \{-1, 0, 1\}$, $a_{l-1} \neq 0$ και $a_{i+1}a_i = 0$ για $0 \leq i \leq l-1$. Συμβολίζεται TNAF(n)*

Ο υπολογισμός της TNAF αναπαράστασης ενός θετικού ακεραίου n είναι ακριβώς ανάλογος με τον αλγόριθμο 3.2 όπου το υπόλοιπο μετά από διαίρεση με τ επιλέγεται έτσι ώστε το πηλίκο να διαρείται από το τ δηλαδή να είναι της μορφής $2v + y\tau$.

Αλγοριθμος 3.4: *Υπολογισμός τ-αδικής NAF αναπαράστασης φυσικού αριθμού*

Input $x + y\tau \in \mathbb{N}$
Output TNAF$(x + y\tau)$
  $i \leftarrow 0$
  while $x \neq 0$ **or** $y \neq 0$ **do**
    if $x \equiv 1 \mod 2$ **then**
      $u_i \leftarrow 2 - (x - 2y \mod 4)$
      $x \leftarrow x - u_i$
    else
      $u_i \leftarrow 0$
    end if
    $(x, y) \leftarrow (y + \frac{(-1)^{1-a}x}{2}, -\frac{t}{2})$
    $i \leftarrow i + 1$
  end while
  return $(u_{i-1}, \ldots, u_1, u_0)$

Παράδειγμα 3.6 (Εφαρμογή του αλγορίθμου 3.2)**.** Για τον υπολογισμό του TNAF(9) με κάνοντας χρήση του αλγορίθμου για $a = 1$. Σε κάθε βήμα χρησιμοποιείται το θεώρημα διαιρετότητας και το πηλίκο υπολογίζεται από τον τύπο $\frac{x+y\tau}{\tau} = u + v\tau = y + \frac{(-1)^{1-a}x}{2} + \frac{-x}{2}\tau$ όπως στην απόδειξή του.

$9+0\tau$		$1 : 8+0\tau+1$ με $8 \equiv 2 \cdot 0 \mod 4$, $-1 : 10+0\tau$ με $2 \not\equiv 2 \cdot 0 \mod 4$
$-4-4\tau$	1	
$-2-2\tau$	0	
$-3+\tau$	0	$1 : -4+1\tau$ με $-4 \not\equiv 2 \cdot 1 \mod 4$, $-1 : -2+1\tau-1$ με $-2 \equiv 2 \cdot 1 \mod 4$
$0+\tau$	-1	
1	0	
0	1	

οπότε $9 = \tau^5 - \tau^3 + \tau^0$

Ο αλγόριθμος 3.4 μπορεί, λοιπόν, να χρησιμοποιηθεί για τον υπολογισμό της TNAF αναπαράστασης ενός φυσικού n θέτοντας $x = n, y = 0$, η οποία έχει μέση πυκνότητα μη μηδενικών ψηφίων $\frac{1}{3}$. Ωστόσο, το μήκος αυτής είναι κατά προσέγγιση $\log_2(N(n)) = 2log_2(n)$, δηλαδή διπλάσιο της δυαδικής αναπαράστασης του n. Για την αντιμετώπιση αυτού του προβλήματος χρησιμοποιείται πως ο $\phi_{2^m}(x) = x^{2^m}$ είναι ταυτοτική συνάρτηση στο $\mathbb{F}_{2^m}$, οπότε εφαρμογή του $\tau^m(P) = P \iff (\tau^m - 1)(P) = 0, \forall P \in E_a(\mathbb{F}_{2^m})$. Συνεπάγεται, λοιπόν, πως αν $a, b \in \mathbb{Z}[\tau]$ με $a \equiv b \mod (\tau^m - 1)$ τότε $aP = bP, \forall P \in E_a(\mathbb{F}_{2^m})$. Το υπόλοιπο έχει μήκος κατά προσέγγιση m και διατηρεί μέση πυκνότητα μη μηδενικών ψηφίων $\frac{1}{3}$. Άρα για τον υπολογισμό του nP αρκεί να υπολογιστεί το υπόλοιπο της διαίρεσης του n με το $\tau^m - 1$, έστω k, και τελικά υπολογισμός του kP.

Αλγοριθμος 3.5: *Διαίρεση στον δακτύλιο* $\mathbb{Z}[\tau]$

Input $u + v\tau, w + z\tau \in \mathbb{N}$
Output $q, r \in \mathbb{Z}[\tau]$, τέτοια ώστε $u + v\tau = q(w + z\tau) + r, N(r) < N(w + z\tau)$
$k \leftarrow wu + zu + 2zv$
$l \leftarrow wv - zu$
$h \leftarrow w^2 + (-1)^{1-a}wz + 2z^2$
$m \leftarrow \lfloor \frac{k}{h} \rfloor$
$n \leftarrow \lfloor \frac{l}{h} \rfloor$
$o \leftarrow u - wm + 2zn$
$p \leftarrow v - sm - wn - zn$
return $q = m + n\tau, r = o + p\tau$

Για τον υπολογισμό του υπολοίπου με διαίρεση με τον $\tau^m - 1$ πρέπει να βρεθεί η μορφή του σαν $a + b\tau$ η οποία προκύπτει από

$$U_k = (-1)^{1-a}U_{k-1} - 2U_{k-1}$$
$$\tau^m = U_m\tau - 2U_{m-1}$$

Συνδυάζοντας τα παραπάνω, για τον υπολογισμό του nP χρησιμοποιείται ο ακόλουθος

αλγόριθμος ο οποίος είναι ακριβώς ανάλογος του αλγορίθμου 3.3 που χρησιμοποιεί προσθέσεις και αφαιρέσεις.

Αλγοριθμος 3.6: *Υπολογισμός $nP, n \in \mathbb{N}, P \in E_a(\mathbb{F}_{2^m})$*

Input $n \in \mathbb{N}, P \in E_a(\mathbb{F}_{2^m})$
Output nP
  $r \leftarrow n/(U_m\tau - (2U_{m-1} + 1))$ (αλγόριθμος 3.5, διατηρείται το υπόλοιπο)
  $(u_{l-1}, \ldots, u_1, u_0) \leftarrow \text{TNAF}(r)$ (αλγόριθμος 3.4)
  $Q \leftarrow u_l P$
  for $i \leftarrow l - 2$ **downto** 1 **do**
    $Q \leftarrow \tau Q$
    if $u_i = 1$ **then**
      $Q \leftarrow Q + P$
    end if
    if $u_i = -1$ **then**
      $Q \leftarrow Q - P$
    end if
  end for
  return Q

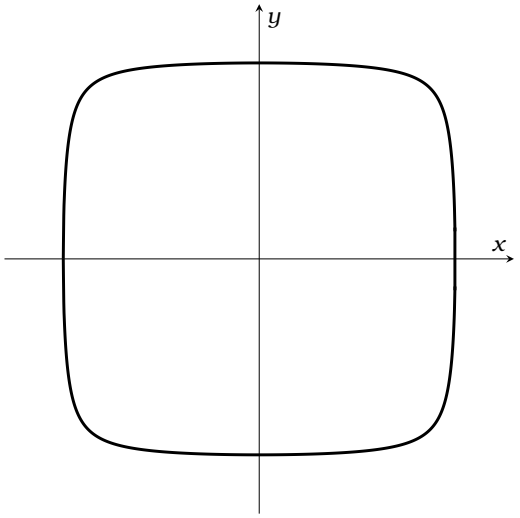
Ο αλγόριθμος 3.6 αποφεύγει τελείως τους διπλασιασμούς και τους αντικαθιστά με ολισθήσεις. Αφού το μήκος του υπολοίπου μετά από διαίρεση είναι κατά προσέγγιση m και έχει πυκνότητα μη μηδενικών ψηφίων $\frac{1}{3}$, το αναμενόμενο πλήθος πράξεων για τον υπολογισμό του nP είναι $\frac{m}{3}$ προσθέσεις σημείων της $E_a(\mathbb{F}_{2^m})$

3.5 Καμπύλες Edwards

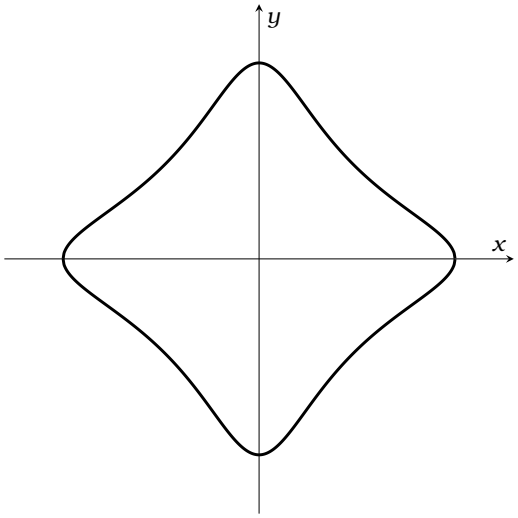
Οι καμπύλες Edwards είναι καμπύλες που ορίζονται πάνω από ένα σώμα k χαρακτηριστικής όχι 2, από εξισώσεις της μορφής

$$x^2 + y^2 = 1 + ax^2y^2 \tag{3.2}$$

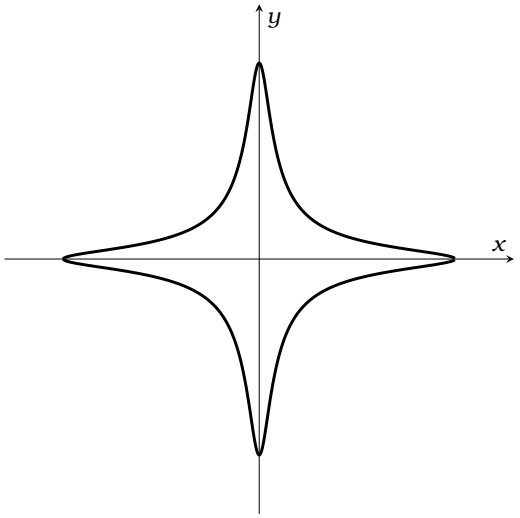
όπου a δεν είναι τετράγωνο στο k. Σε αυτές τις καμπύλες ορίζεται πράξη ομάδας τέτοια ώστε το σημείο $(0, 1)$ να είναι το προσθετικό ουδέτερο.



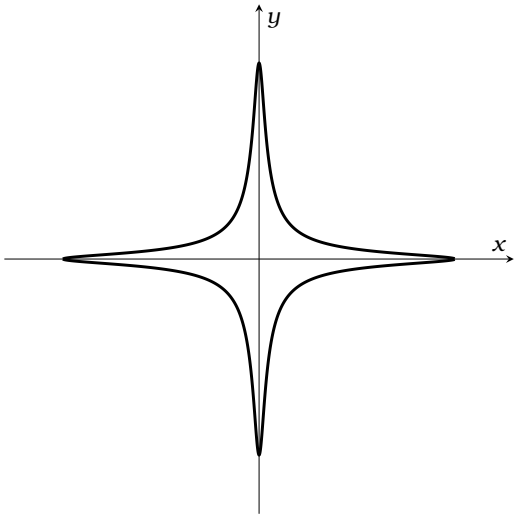
$x^2 + y^2 = 1 + 0.9x^2y^2$



$x^2 + y^2 = 1 - 10x^2y^2$



$x^2 + y^2 = 1 - 300x^2y^2$



$x^2 + y^2 = 1 - 1200x^2y^2$

Μία καμπύλη Edwards μπορεί να μετασχηματιστεί σε μία καμπύλη σε μορφή Weierstrass :

$$w = (ax^2 - 1)y \qquad X = \frac{-2(w-1)}{x^2} \qquad Y = \frac{4(w-1) + 2(a+1)x^2}{x^3}$$

οπότε για κάθε λύση της αρχικής εξίσωσης (x_0, y_0) με $x_0 \neq 0$ αντιστοιχεί ένα αφινικό σημείο (X_0, Y_0) στην καμπύλη E/k:

$$Y^2 = (X - a - 1)(X^2 - 4a)$$

Αν γίνει αντιστοίχιση του $(0, 1)$ της 3.2 με το O της E/k και του $(0, -1)$ (του άλλου σημείου της 3.2 με $x = 0$) στο $(a + 1, 0)$ της E/k, τότε προκύπτει μία 1-1 και επί αντιστοιχία μεταξύ των k-ρητών σημείων της 3.2 και του $E(k)$ (και ομοίως για κάθε επέκταση L/k παρότι το a μπορεί να είναι σε αυτή τετράγωνο). Αξίζει να σημειωθεί πως δεν μπορεί κάθε ελλειπτική καμπύλη να αναπαρασταθεί σε μορφή Edwards. Συγκεκριμένα, μία Edwards καμπύλη έχει πάντα ένα ρητό σημείο τάξης 4, το $(1, 0)$.

Η αντιστοίχηση των k-ρητών σημείων της 3.2 με το $E(k)$ δίνει την δυνατότητα χρήσης της πράξης ομάδας στην $E(k)$ για να αποκτήσουν οι k-ρητές λύσεις της 3.2 δομή ομάδας ισόμορφης με της $E(k)$. Για την πρόσθεση, λοιπόν, των σημείων $(x_1, y_1), (x_2, y_2)$ της 3.2:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + a x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - a x_1 x_2 y_1 y_2} \right) \tag{3.3}$$

ενώ $-(x_1, y_1) = (-x_1, y_1)$.

Σε αντίθεση με καμπύλες σε μορφή Weierstrass η 3.3 είναι καλά ορισμένη για κάθε ζεύγος σημείων της 3.2. Πράγματι, αν οποιοσδήποτε από τους παρονομαστές είναι 0 προκύπτει πως

$$\begin{aligned}(1 + a x_1 x_2 y_1 y_2)(1 - a x_1 x_2 y_1 y_2) = 1 - a^2 x_1^2 x_2^2 y_1^2 y_2^2 = 0 \\ \Rightarrow a^2 x_1^2 x_2^2 y_1^2 y_2^2 = 1\end{aligned}$$

επομένως τα x_1, y_1, x_2, y_2 είναι όλα μη μηδενικά. Από την εξίσωση 3.2 για το (x_1, y_1):

$$x_1^2 + y_1^2 = 1 + a x_1^2 y_1^2 = 1 + \frac{1}{a x_2^2 y_2^2} = \frac{x_2^2 + y_2^2}{a x_2^2 y_2^2}$$

Προσθέτοντας ή αφαιρόντας $2x_1 y_1 = \pm \dfrac{2}{a x_2 y_2}$ στην παραπάνω εξίσωση προκύπτει:

$$(x_1 \pm y_1)^2 = \frac{(x_1 \pm y_2)^2}{a x_2^2 y_2^2}$$

με οποιαδήποτε επιλογή προσήμου στο αριστερό μέρος. Αφού τα x_1, y_1 δεν είναι μηδέν τουλάχιστον ένα από τα $(x_1 + y_1)$ και $(x_1 - y_1)$ είναι μη μηδενικό και άρα και το τετράγωνό του. Επομένως από την τελευταία εξίσωση έπεται πως το a θα έπρεπε να είναι τετράγωνο κάτι που από υπόθεση δεν ισχύει. Επομένως, η πρόσθεση των σημείων με χρήση της 3.3 είναι καλά ορισμένη σε κάθε επέκταση L/k για την οποία το a δεν είναι τετράγωνο.

Από την 3.3 που ορίζει την πράξη ομάδας απαιτούνται 5 πολλαπλασιασμοί και 2 αντιστροφές στο σώμα k για τον υπολογισμό του $(x_1, y_1) + (x_2, y_2)$, χωρίς να προσμετρούνται οι προσθέσεις και οι πολλαπλασιασμοί με το a το οποιο μπορεί να επιλεγεί μικρό. Η πράξη ομάδας είναι κατά αυτόν τον τρόπο λιγότερο αποδοτική από τον υπολογισμό της πράξης ομάδας σε καμπύλες short Weierstrass. Ωστόσο, μπορούμε και σε αυτή την περίπτωση να χρησιμοποιήσουμε προβολικές συντεταγμένες. Αντικαθιστώντας x_3 και y_3 με x_3/z_3 και y_3/z_3, οπότε προκύπτει

$$\frac{x_3}{z_3} = \frac{z_1 z_2 (x_1 y_1 + x_2 y_1)}{z_1^2 z_2^2 + a x_1 x_2 y_1 y_2} \qquad \frac{y_3}{z_3} = \frac{z_1 z_2 (y_1 y_2 - x_1 x_2)}{z_1^2 z_2^2 - a x_1 x_2 y_1 y_2}$$

$$r = z_1 z_2 \qquad s = x_1 y_2 + x_2 y_1 \qquad t = a x_1 x_2 y_1 y_2 \qquad u = y_1 y_2 - x_1 x_2$$

$$x_3 = rs(r^2 - t) \qquad y_3 = ru(r^2 + t) \qquad z_3 = (r^2 + t)(r^2 - t)$$

Για τον υπολογισμό των x_3, y_3, z_3 χρειάζονται συνολικά 12 πολλαπλασιασμοί. Αν υπολογιστεί το $s = (x_1 + y_1)(x_2 + y_2) - x_1 x_2 - y_1 y_2$ χρειάζονται τελικά 11 πολλαπλασιασμοί και καμία

αντιστροφή.

Στην περίπτωση του διπλασιασμού $1 + ax_1^2y^2 = x_1^2 + y_1^2$ από την 3.2 οπότε,

$$2(x_1, y_1) = \left(\frac{2x_1y_1}{1 + ax_1^2y_1^2}, \frac{y_1^2 - x_1^2}{1 - ax_1^2y_1^2}\right) = \left(\frac{2x_1y_1}{x_1^2 + y_1^2}, \frac{y_1^2 - x_1^2}{2 - (x_1^2 + y_1^2)}\right)$$

Χρησιμοποιώντας πάλι προβολικές συντεταγμένες, ο διπλασιασμός γίνεται

$$b = (x_1 + y_1)^2 \quad c = x_1^2 \quad d = y_1^2 \quad e = c + d \quad h = z_1^2 \quad j = e - 2h$$
$$x_3 = (b - e)j \qquad y_3 = e(c - d) \qquad z_3 = ej$$

οπότε απαιτούνται 7 πολλαπλασιασμοί και καμία αντιστροφή.

Η έκφραση 3.3 είναι καλώς ορισμένη για οποιαδήποτε δύο σημεία $(x_1, y_1), (x_2, y_2)$ που ικανοποιούν την 3.2. Δεν χρειάζεται να γίνει διάκριση των περιπτώσεων για όταν ένα από τα δύο είναι το προσθετικό ουδέτερο ή όταν το ένα είναι το αντίθετο του άλλου. Η υλοποίηση της πρόσθεσης τότε μπορεί να υλοποιηθεί χωρίς διακλαδώσεις σε straight-line code. Υπάρχει, επιπλέον, προστασία απέναντι σε side-channel attacks. Τέτοιες επιθέσεις εκμεταλλεύονται την περίπτωση που χρησιμοποιούνται διαφορετικοί τύποι για τον διπλασιασμό και την πρόσθεση παρατηρώντας την διαφορά σε χρόνο και ενέργεια που απαιτούν οι διαφορετικές πράξεις. Μπορούν με αυτό τον τρόπο να ανακτήσουν ιδιωτικά κλειδιά τα οποία χρησιμοποιούνται σαν ακέραιοι για τον πολλαπλασιασμό με ένα σημείο της καμπύλης σε διάφορα κρυπτοσυστήματα (δηλαδή υπολογίζονται ποσότητες nP για P σημείο της καμπύλης και $n \in \mathbb{Z}$). Η ακολουθία πολλαπλασιασμών και διπλασιασμών, σε αυτή την περίπτωση, ουσιαστικά κωδικοποιεί την δυαδική αναπαράσταση του n.

3.6 Συντεταγμένες Jacobian

Οι συντεταγμένες Jacobian είναι μια παραλλαγή των προβολικών συντεταγμένων που οδηγούν τελικά σε ταχύτερο διπλασιασμό σημείων. Έστω k σώμα και $\overline{k}$ μία αλγεβρική του θήκη. Χρησιμοποιείται η σχέση ισοδυναμίας

$$(x, y, z) \sim (\lambda^2 x, \lambda^3 y, \lambda z), \forall \lambda \in \overline{k}^*$$

οπότε ως σημεία στο επίπεδο θεωρούνται κατ' αναλογία με τον ορισμό του προβολικού επιπέδου το σύνολο

$$\frac{\overline{k}^3 \setminus \{(0,0,0)\}}{\sim}$$

Η κλάση ισοδυναμίας του (x, y, z) συμβολίζεται πάλι ως $(x : y : z)$. Κάθε σημείο $(x : y : z)$ με $z \neq 0$ αντιστοιχεί στο αφινικό σημείο $\left(\frac{x}{z^2}, \frac{y}{z^3}\right)$.

3.6.1 Η πράξη ομάδας σε συντεταγμένες Jacobian

Έστω $k \leq L$. Η ομογενής εξίσωση short Weierstrass έχει πλέον τη μορφή

$$E/k : y^2 = x^3 + Axz + Bz^6$$

Το σημείο στο άπειρο αντιστοιχεί πλέον στο $(1:1:0)$. Το αντίθετο σημείο του $P=(x:y:z)$ είναι το $-P=(x:-y:z)$. Για τα αφινικά σημεία $P=(x_1,y_1), Q=(x_2,y_2)\in E(L)$ με $P_1\neq\pm Q$ υπολογίζεται το $(x_3,y_3)=P+Q$ από τους τύπους

$$\begin{aligned} x_3 &= m^2-x_1-x_2 \\ y_3 &= m(x_1-x_3)-y_1 \\ m &= \frac{y_2-y_1}{x_2-x_1} \end{aligned}$$

Αντικαθιστώντας, λοιπόν, $(x_i,y_i)\mapsto\left(\frac{x_i}{z_i^2},\frac{y_i}{z_i^3}\right)$ προκύπτουν τα x_3,y_3 και z_3 από τους ακόλουθους υπολογισμούς

$$\begin{gathered} r=x_1z_2^2 \quad s=x_2z_1^2 \quad t=y_1z_2^3 \quad u=y_2z_1^3 \quad v=s-r \quad w=u-t \\ x_3=-v^3-2rv^2+w^2 \quad y_3=-tv^3+(rv^2-x_3)w \quad z_3=vz_1z_2 \end{gathered}$$

Στην περίπτωση που $P=Q$ οι τύποι για τον διπλασιασμό $2P=(x_3,y_3)$

$$\begin{aligned} x_3 &= m^3-2x_1 \\ y_3 &= m(x_1-x_3)-y_1 \\ m &= \frac{3x_1^2+A}{2y_1} \end{aligned}$$

Αντικαθιστώντας στα παραπάνω $(x_1,y_1)\mapsto\left(\frac{x_1}{z_1^2},\frac{y_1}{z_1^3}\right)$

$$\begin{aligned} \frac{x_3}{z_3^2} &= \left(\frac{3(\frac{x_1}{z_1^2})^2+A}{2\frac{y_1}{z_1^3}}\right)^2-2\frac{x_1}{z_1^2}=\frac{(3x_1^2+Az_1^4)^2-8x_1y_1^2}{(2y_1z_1)^3} \\ \frac{y_3}{z_3^3} &= \left(\frac{3(\frac{x_1}{z_1^2})^2+A}{2\frac{y_1}{z_1^3}}\right)\frac{3x_1}{z_1^2}-\left(\frac{3(\frac{x_1}{z_1^2})^2+A}{2\frac{y_1}{z_1^3}}\right)^3-\frac{y_1}{z_1^3}=\frac{12x_1y_1^2(3x_1^2+Az_1^4)-(3x_1^2+Az_1^4)^3-8y_1^4}{(2y_1z_1)^3} \end{aligned}$$

οπότε $z_3=2y_1z_1$.
Τα παραπάνω υπολογίζονται αποδοτικά από τους

$$\begin{gathered} v=4x_1y_1^2 \quad w=3x_1^2+Az_1^4 \\ x_3=-2v+w^2 \quad y_3=-8y_1^4+(v-x_3)w \quad z_3=2y_1z_1 \end{gathered}$$

Από τους παραπάνω τύπους φαίνεται πως η πρόσθεση διαφορετικών σημείων απαιτεί 16 πολλαπλασιασμούς ενώ ο διπλασιασμός σημείων απαιτεί 9 πολλαπλασιασμούς. Αν $A=-3$ μπορεί να γίνει ο υπολογισμός $w=3(x_1^2-z_1^4)=(x_1+z_1^2)(x_1-z_1^2)$ απαιτώντας τελικά 8 πολλαπλασιασμούς για τον διπλασιασμό σημείων. Οι ελλειπτικές καμπύλες που προτείνονται από το NIST στο FIPS 186-4 πάνω από σώματα $\mathbb{Z}_p$ για p πρώτο είναι όλα αυτής της μορφής ($A=-3$) για την αξιοποίηση των αποδοτικότερων αυτών τύπων.

Κεφάλαιο 4

Η δομή της $E(\mathbb{F}_q)$

Ο προσδιορισμός της δομής των ελλειπτικών καμπυλών πάνω από πεπερασμένα σώματα προκύπτει από την μελέτη των μορφισμών ελλειπτικών καμπυλών, τις isogenies.

4.1 Μορφισμοί ελλειπτικών καμπυλών

Ορισμός 4.1. *Έστω C/k μία επίπεδη προβολική καμπύλη που ορίζεται από την $f(x,y,z)=0$, όπου f ένα μη σταθερό ομογενές πολυώνυμο του $k[x,y,z]$ το οποίο είναι ανάγωγο σαν στοιχείο του $\overline{k}[x,y,z]$. Το **σώμα συναρτήσεων** $k(C)$ είναι το σύνολο των κλάσεων ισοδυναμίας των ρητών συναρτήσεων $\frac{g}{h}$ τέτοια ώστε :*

- *$g,h \in k[x,y,z]$ είναι ομογενή πολυώνυμα τέτοια ώστε $\deg(g)=\deg(h)$*
- *H h δεν διαιρείται από το το f ή ισοδύναμα $h \notin (f)$*
- *$\frac{g_1}{h_1} \sim \frac{g_2}{h_2} \iff g_1h_2 - g_2h_1 \in (f)$*

Αφού $\deg(g)=\deg(h)$ μπορεί να οριστεί η τιμή μίας συνάρτησης από το σώμα συναρτήσεων σε ένα προβολικό σημείο εφόσον δεν μηδενίζεται ο παρονομαστής. Έτσι αν $P=(\lambda x,\lambda y,\lambda z)\in C, \lambda \in k^*$

$$\frac{g(\lambda x,\lambda y,\lambda z)}{h(\lambda x,\lambda y,\lambda z)} = \frac{\lambda^{\deg(g)}g(x,y,z)}{\lambda^{\deg(h)}h(x,y,z)} = \frac{g(x,y,z)}{h(x,y,z)}$$

Επιπλέον, αν $\frac{g_1}{h_1}$ είναι ισοδύναμη με την $\frac{g_2}{h_2}$ και $h_1(P)\neq 0, h_2(P)\neq 0$ τότε

$$g_1(P)h_2(P) - g_2(P)h_1(P) \in (f), \quad f(P)=0$$
$$(\frac{g_1}{h_1})(P) = (\frac{g_2}{h_2})(P)$$

Υπάρχει περίπτωση μία συνάρτηση από το σώμα συναρτήσεων μίας καμπύλης C να μην ορίζεται για ένα στοιχείο της κλάσης ισοδυναμίας αλλά να ορίζεται για κάποια άλλη συνάρτηση της ίδιας κλάσης. Δηλαδή, αν $a=\frac{g_1}{h_1}$ με $h_1(P)=0$, μπορεί να ισχύει πως $\frac{g_2}{h_2}\sim\frac{g_1}{h_1}$ με $h_1(P)\neq 0$. Η a ορίζεται στο $P\in C(\overline{k})$ αν μπορεί να παρασταθεί σαν $\frac{g}{h}$ για κάποια $g,h\in k[x,y,z]$ με $h(P)\neq 0$.

Παράδειγμα 4.1. Έστω C/k η $f(x,y,z)=zy^2-x^3-z^2x=0, P=(0:0:1)\in C$

$$a = \frac{3xz}{y^2} \in k(C)$$

Ο παρονομαστής μηδενίζεται στο P ωστόσο

$$a = \frac{3xz}{y^2} = \frac{3xz^2}{zy^2} = \frac{3xz^2}{x^3 + z^2x} = \frac{3z^2}{x^2 + z^2}$$

Επομένως, $a(P) = 3$

Ορισμός 4.2 (Ρητή συνάρτηση)**.** *Έστω C_1, C_2 δύο επίπεδες προβολικές καμπύλες ορισμένες στο k. Μία **ρητή συνάρτηση (rational map)** $\phi : C_1 \to C_2$ είναι μία τριάδα $(\phi_x : \phi_y : \phi_z) \in \mathbb{P}^2(k(C_1))$ έτσι ώστε $\forall P \in C_1(\bar{(k)})$ όπου ϕ_x, ϕ_y, ϕ_z ορίζονται και δεν είναι και οι τρεις 0 το προβολικό σημείο $(\phi_x(P) : \phi_y(P) : \phi_z(P)) \in C_2(\bar{k})$. Η ρητή συνάρτηση ϕ ορίζεται στο $P \in C_1(\bar{k})$ αν υπάρχει $\lambda \in k(C_1)^*$ τέτοιο ώστε $\lambda\phi_x, \lambda\phi_y, \lambda\phi_z$ όλες ορίζονται και είναι μη μηδενικές στο P.*

Μία ρητή συνάρτηση δεν είναι μία συνάρτηση από το $C_1(\bar{k})$ στο $C_2(\bar{k})$ που δίνεται από ρητες συναρτήσεις αφού μπορεί να μην ορίζεται παντού. Μία ρητή συνάρτηση που ορίζεται σε όλο το $C_1(\bar{k})$ λέγεται **μορφισμός** και δύο προβολικές καμπύλες λέγονται **ισόμορφες** αν υπάρχουν μορφισμοί $\phi : C_1 \to C_2, \phi^{-1} : C_2 \to C_1$ τέτοιοι ώστε $\phi \circ \phi^{-1} = id$ και $\phi^{-1} \circ \phi = id$. Δύο σημαντικές ιδιότητες των μορφισμών είναι οι ακόλουθες [1, σ. 19-20, 2.1, 2.3]:

1. Αν C_1 είναι μία λεία προβολική καμπύλη, τότε κάθε ρητή συνάρτηση από την C_1 στην προβολική καμπύλη C_2 είναι μορφισμός.

2. Ένας μορφισμός προβολικών καμπυλών είναι είτε επί είτε σταθερός.

Ορισμός 4.3 (Isogeny)**.** *Μία **isogeny** $\phi : E_1 \to E_2$ από ελλειπτικές καμπύλες ορισμένες πάνω από το k είναι ένας επί μορφισμός καμπυλών που είναι και ομομορφισμός ομάδων $E_1(\bar{k})$ και $E_2(\bar{k})$. Οι E_1 και E_2 λέγονται τότε isogenous πάνω από το k (σώμα ορισμού του ϕ), ενώ αν επιπλέον ο ϕ είναι ισομορφισμός τότε λέγονται ισόμορφες.*

Παράδειγμα 4.2. Αν E/k ελλειπτική καμπύλη ορισμένη από την $y^2 = x^3 + Ax + B$ τότε ο $\phi : E \to E$ που δίνεται από

$$(x : y : z) \mapsto (x : -y : z)$$
$$\phi(P) = -P$$

είναι ρητή συνάρτηση και ορίζεται σε κάθε προβολικό σημείο $P \in E(\bar{k})$ οπότε είναι μορφισμός. Είναι προφανώς ενδομορφισμός της $E(\bar{k})$, μη σταθερός (άρα είναι επί) κι επομένως isogeny και μάλιστα ισομορφισμός.

Παράδειγμα 4.3 (Διπλασιασμός)**.** Αν E/k ελλειπτική καμπύλη ορισμένη από την $y^2 = x^3 + Ax + B$ τότε ο $\phi : E \to E$ που δίνεται από

$$\phi(P) = 2P$$

Για τον διπλασιασμό του $P = (x, y)$ έχουμε

$$\phi_x(x, y) = (m(x, y))^2 - 2x = \frac{(3x^2 + A)^2 - 8xy^2}{4y^2}$$
$$\phi_y(x, y) = m(x, y)(x - \phi_x(x, y)) - y = \frac{12xy^2(3x^2 + A) - (3x^2 + A)^3 - 8y^4}{8y^4}$$

Ομογενοποιώντας και διαγράφοντας τους παρανομαστές $\phi = (\frac{\psi_x}{\psi_z} : \frac{\psi_y}{\psi_z} : 1) = (\psi_x : \psi_y : \psi_z)$ όπου

$$\psi_x(x, y, z) = 2yz((3x^2 + Az^2)^2 - 8xy^2z)$$
$$\psi_y(x, y, z) = 12xy^2z(3x^2 + Az^2) - (3x^2 + Az^2)^3 - 8y^4z^2$$
$$\psi_z(x, y, z) = 8y^3z^3$$

Αν $y = 0$ τότε $3x^2 + Az^2 \neq 0$ αφού η E είναι λεία. Οπότε το μόνο σημείο στο οποίο ψ_x, ψ_y, ψ_z μηδενίζονται ταυτόχρονα είναι το $O = (0 : 1 : 0)$. Ωστόσο, αφού $f(x, y, z) = y^2z - x^3 - Axz^3 - Bz^3$ μπορούν να χρησιμοποιηθούν οι ισοδύναμες εκφράσεις $\psi_x + 18xyzf$, $\psi_y + (27f - 18y^2z)f$ οπότε μετά την διαγραφή των κοινών όρων προκύπτουν

$$\psi_x(x, y, z) = 2y(xy^2 - 9Bxz^2 + A^2z^3 - 3Ax^2z)$$
$$\psi_y(x, y, z) = y^4 - 12y^2z(2Ax + 3Bz) - A^3z^4 + 27Bz(2x^3 + 2Axz^2 + Bz^3) + 9Ax^2(3x^2 + 2Az^2)$$
$$\psi_z(x, y, z) = 8y^3z$$

οπότε $\phi(O) = O$ και ο ϕ είναι isogeny.

Παράδειγμα 4.4 (Ο ενδομορφισμός του Frobenius)**.** Σε ένα σώμα $\mathbb{F}_p$ χαρακτηριστικής p η συνάρτηση $\pi : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ με $x \mapsto x^p$ είναι αυτομορφισμός σώματος ο οποίος αφήνει σταθερό το υπόσωμα $\mathbb{F}_p$. Επιπλέον, κάθε δύναμη αυτού π^n είναι επίσης αυτομορφισμός που διατηρεί το $\mathbb{F}_{p^n}$ σταθερό.
Αν $E/\mathbb{F}_q$ ($\mathbb{F}_q = \mathbb{F}_{p^n}$) ελλειπτική καμπύλη τότε ο

$$\pi_E : (x : y : z) \mapsto (x^q : y^q : z^q)$$

είναι μορφισμός $\pi_E : E \to E$. Αν υψωθεί η εξίσωση της καμπύλης της E στην q-οστή δύναμη

$$y^2z = x^3 + Axz^2 + Bz^3$$
$$(y^q)^2(z^q) = (x^q)^3 + A^q(x^q)(z^q)^2 + B^q(z^q)^3$$

όμως $A, B \in \mathbb{F}_q$ οπότε $A^q = A, B^q = B$, άρα το $(x^q : y^q : z^q) \in E(\overline{\mathbb{F}}_q)$.
Η συνάρτηση π_E είναι ομομορφισμός ομάδων αφού η πράξη ομάδας δίνεται από ρητές συναρτήσεις με συντελεστές στο $\mathbb{F}_q$ το οποίο μένει σταθερό κάτω από την ύψωση στην q-οστή δύναμη, δηλαδή $\pi_E(P + Q) = \pi_E(P) + \pi_E(Q), \forall P, Q \in E(\overline{\mathbb{F}}_q)$.
Τα παραπάνω ισχύουν και στην περίπτωση της γενικής εξίσωσης Weierstrass και άρα και ελλειπτικές καμπύλες πάνω από σώματα χαρακτηριστικής 2 ή 3.

4.2 Κανονική μορφή των isogenies

Αν οι ελλειπτικές καμπύλες ορίζονται πάνω από σώματα όχι χαρακτηριστικής 2 ή 3 μπορούν να γραφούν στην μορφή $y^2 = f(x)$ όπου $f(x)$ ένα κυβικό πολυώνυμο. Σε αυτή την περίπτωση μία isogeny $\phi = (\phi_x : \phi_y : \phi_z)$ μπορεί να γραφεί σε αφινική μορφή για το αφινικό σημείο $(x : y : 1) \in E(\overline{k})$ ώστε $\phi(x, y) = \left(\frac{\phi_x(x, y, 1)}{\phi_z(x, y, 1)}, \frac{\phi_y(x, y, 1)}{\phi_z(x, y, 1)}\right) = (r_1(x, y), r_2(x, y))$. Με εφαρμογή της $y^2 = f(x)$, βλέποντας δηλαδή τα $r_1(x, y), r_2(x, y)$ σαν στοιχεία του σώματος κλασμάτων του $k[x, y]/(y^2 - f(x))$ (το οποίο είναι ακεραία περιοχή στην προκειμένη περίπτωση) προκύπτει πως

$$r_1(x, y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y} \qquad r_2(x, y) = \frac{q_1(x) + q_2(x)y}{q_3(x) + q_4(x)y}$$

με $p_i, q_i \in k[x], i \in \{1, \ldots, 4\}$. Πολλαπλασιάζοντας αριθμητές και παρονομαστές με $p_3(x) - p_4(x)y$ και $q_3(x) - q_4(x)y$ στα r_1 και r_2 αντίστοιχα και εφαρμόζοντας την $y^2 = f(x)$, αυτά γράφονται στη μορφή

$$r_1(x, y) = \frac{p_1(x) + p_2(x)y}{p_3(x)} \qquad r_2(x, y) = \frac{q_1(x) + q_2(x)y}{q_3(x)}$$

με $p_i, q_i \in k[x], i \in \{1, \ldots, 3\}$.
Επιπλέον, αφού η ϕ είναι και ομομορφισμός ομάδων $\phi(-P) = -\phi(P), \forall P \in E(\overline{k})$, δηλαδή

$$\begin{gathered}
(r_1(x, -y), r_2(x, -y)) = (r_1(x, y), -r_2(x, y)) \\
r_1(x, -y) = r_1(x, y) \qquad r_2(x, -y) = -r_2(x, y) \\
\frac{p_1(x) - p_2(x)y}{p_3(x)} = \frac{p_1(x) + p_2(x)y}{p_3(x)} \qquad \frac{q_1(x) - q_2(x)y}{q_3(x)} = -\frac{p_1(x) + p_2(x)y}{p_3(x)} \\
p_2(x) = 0 \qquad q_1(x) = 0
\end{gathered}$$

οπότε, τελικά η ϕ γράφεται

$$\phi(x, y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right) \tag{4.1}$$

με $u, v, s, t \in k[x]$ και $(u, v) = 1$ και $(s, t) = 1$. Η μορφή 4.1 λέγεται η **κανονική μορφή** της isogeny ϕ και είναι μοναδική εκτός πολλαπλασιασμού με σταθερά στο k^*, αφού έχουν διαγραφεί όλοι οι κοινοί όροι από τα κλάσματα.

Λήμμα 4.1. *Έστω $E_1/k : y^2 = f_1(x)$ και $E_2/k : y^2 = f_2(x)$ δύο ελλειπτικές καμπύλες σε short Weierstrass και $\phi(x, y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$ μία isogeny σε κανονική μορφή. Τότε $v^3 \mid t^2$ και $t^2 \mid v^3 f_1$. Τα πολυώνυμα $v(x)$ και $t(x)$ έχουν το ίδιο σύνολο ριζών στο $\overline{k}$.*

Απόδειξη. Αντικαθιστώντας το $\left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$ στην E_2 προκύπτει $\left(\frac{s(x)}{t(x)}y\right)^2 = f_2\left(\frac{u(x)}{v(x)}\right)$ και από την

$y^2 = f_1(x)$

$$\left(\frac{s(x)}{t(x)}\right)^2 f_1(x) = f_2\left(\frac{u(x)}{v(x)}\right)$$
$$\left(\frac{s(x)}{t(x)}\right)^2 f_1(x) = \left(\frac{u(x)}{v(x)}\right)^3 + A\left(\frac{u(x)}{v(x)}\right) + B$$
$$v^3(x)s^2(x)f_1(x) = t^2(x)u^3(x) + t^2(x)Au(x)v^2(x) + Bt^2(x)v^3(x)$$
$$v^3(x)s^2(x)f_1(x) = t^2(x)(u^3(x) + Au(x)v^2(x) + Bv^3(x))$$
$$v^3(x)s^2(x)f_1(x) = t^2(x)w(x) \tag{4.2}$$

όπου $w(x) = u^3(x)+A(x)u(x)v^2(x)+Bv^3(x)$. Επιπλέον, $(v(x), w(x)) = 1$ γιατί αν $(v(x), w(x)) = d(x) \neq 1$ τότε $(d(x) \mid v(x)) \wedge (d(x) \mid w(x)) \Rightarrow d(x) \mid u(x)$, κι άρα $d(x) \mid (u(x), v(x)) \neq 1$ το οποίο δεν ισχύει από την κανονική μορφή. Άρα $(v(x), w(x)) = 1$ και $v^3(x) \mid t^2(x)$.
$t^2(x) \mid v^3(x)s^2(x)f_1(x)$ αλλά αφού $(t(x), s(x)) = 1$ προκύπτει πως $t^2(x) \mid v^3(x)f_1(x)$. Για το δεύτερο σκέλος κάθε ρίζα του $v(x)$ είναι ρίζα του $t(x)$ αφού $v^3(x) \mid t^2(x)$ και κάθε ρίζα του $t(x)$ είναι διπλή ρίζα του $t^2(x) \mid v^3(x)f_1(x)$, όμως το $f_1(x)$ δεν έχει πολλαπλές ρίζες άρα είναι ρίζα του $v(x)$. □

Κάνοντας χρήση του παραπάνω λήμματος μπορούν πλέον να προσδιοριστούν ακριβώς τα αφινικά σημεία τα οποία βρίσκονται στον πυρήνα μιας isogeny ϕ σε κανονική μορφή. Αν $P = (x_0 : y_0 : 1) \in E_1(\overline{k})$ με $v(x_0) \neq 0 \Rightarrow t(x_0) \neq 0$ η $\phi(x_0, y_0)$ είναι αφινικό σημείο κι άρα $P \notin \ker\phi$. Αν τώρα $v(x_0) = t(x_0) = 0$ τότε ομογενοποιώντας και γράφοντας την ϕ σε προβολική μορφή

$$\phi = (u(x, z)t(x, z) : v(x, z)s(x, z)y : v(x, z)t(x, z))$$

με $u, v, t, s \in k[x, z]$ ομογενή. Με την υπόθεση ότι $y_0 \neq 0$, $v(x_0, 1) = t(x_0, 1) = 0$ όμως $v^3|t^2$ η πολλαπλότητα του x_0 σαν ρίζα του t είναι γνήσια μεγαλύτερη από την πολλαπλότητα του x_0 σαν ρίζα του v, άρα μπορεί να μετασχηματιστεί η ϕ με διαίρεση με κατάλληλη δύναμη του $x - x_0z$ ώστε η ϕ_y να μην μηδενίζεται στο $(x_0 : y_0 : 1)$ (αφού $(t, s) = 1$). Σε αυτή την περίπτωση, ϕ_x, ϕ_z μηδενίζονται κι άρα $\phi(P) = (0 : 1 : 0) = O \Rightarrow P \in \ker\phi$.
Αν $y_0 = 0$ τότε $y_0^2 = f_1(x_0) = 0$ οπότε

$$\begin{aligned}\phi &= (u(x, z)t(x, z) : v(x, z)s(x, z)y : v(x, z)t(x, z)) \\ &= (u(x, z)t(x, z)yz : v(x, z)s(x, z)y^2z : v(x, z)t(x, z)yz) \\ &= (u(x, z)t(x, z)yz : v(x, z)s(x, z)f_1(x, z) : v(x, z)t(x, z)yz)\end{aligned}$$

Αφού $v^3 \mid t^2$ και το $(x_0, 1)$ είναι ρίζα πολλαπλότητας 1 του f_1, σαν ρίζα του vf_1 δεν έχει μεγαλύτερη πολλαπλότητα από σαν ρίζα του t. Οπότε διαιρώντας με κατάλληλη δύναμη του $x - x_0z$ ώστε να μη μηδενίζεται η ϕ_y στο $(x_0 : y_0 : 1)$ και τότε τα ϕ_x, ϕ_y μηδενίζονται αφού έχουν ως παράγοντα το y. Άρα και σε αυτή την περίπτωση $P \in \ker\phi$. Από αυτή την παράγραφο αποδείχθηκε το ακόλουθο

Θεώρημα 4.1. *Έστω E_1, E_2 ελλειπτικές καμπύλες ορισμένες πάνω από ένα σώμα k και $\phi : E_1 \to E_2$ isogeny σε κανονική μορφή. Τα αφινικά σημεία $(x_0 : y_0 : 1) \in E_1(\overline{k})$ που ανήκουν στον $\ker\phi$ είναι ακριβώς αυτά για τα οποία $v(x_0) = 0$. Επιπλέον, $\ker\phi$ είναι πεπερασμένη υποομάδα της $E_1(\overline{k})$.*

4.3 Πυρήνες των isogenies

Ορισμός 4.4. *Έστω $\phi(x, y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)y}{t(x)}\right)$ μία isogeny σε κανονική μορφή. Ο **βαθμός** της ϕ ορίζεται ως $\deg\phi = \max\{\deg u, \deg v\}$.*
*Η ϕ λέγεται **διαχωρίσιμη** αν $\left(\frac{u(x)}{v(x)}\right)' \neq 0$, διαφορετικά λέγεται **μη διαχωρίσιμη**.*

Παράδειγμα 4.5. Η κανονική μορφή του $\phi(x : y : z) = (x : -y : z)$ είναι η $\phi(x, y) = (x, -y)$ άρα είναι διαχωρίσιμη βαθμού 1.

Παράδειγμα 4.6. Η κανονική μορφή της isogeny του διπλασιασμού είναι

$$\phi(x, y) = \left(\frac{x^4 + 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}, \frac{x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2}{8(x^3 + Ax + B)^2}y\right)$$

είναι διαχωρίσιμη βαθμού 4.

Παράδειγμα 4.7. Η κανονική μορφή ενδομορφισμού του Frobenius για την $E/\mathbb{F}_q : y^2 = f(x)$ είναι

$$\pi_E(x, y) = (x^q, (f(x))^{\frac{q-1}{2}}y)$$

είναι μη διαχωρίσιμη βαθμού q.

Έστω ϕ μη διαχωρίσιμη isogeny σε κανονική μορφή. Αν $\left(\frac{u}{v}\right)' = \left(\frac{u'v - uv'}{v^2}\right) = 0 \Rightarrow u'v = uv'$. Αφού $(u, v) = 1$ κάθε ρίζα του u πρέπει να είναι ρίζα του u' με τουλάχιστον την ίδια πολλαπλότητα όμως $\deg u' < \deg u$ επομένως $u' = 0$. Αντίστοιχα $v' = 0$. Επομένως,

$$\left(\frac{u}{v}\right)' = 0 \iff u' = v' = 0 \iff u = f(x^p) \wedge v = g(x^p) \tag{4.3}$$

όπου $\operatorname{char} k = p$.
Από την 4.2 με $u' = v' = 0 \Rightarrow w' = 0 \Rightarrow \left(\frac{w}{v^3}\right)' = \left(\frac{s^2 f_1}{t^2}\right)' = 0 \Rightarrow s^2(x)f_1(x) = g(x^p) \wedge t^2(x) = h(x^p)$. Για $x_0 \in \overline{k}$ με $f_1(x_0) = 0 \Rightarrow g(x_0^p) = 0 \Rightarrow (x - x_0^p) \mid g(x) \Rightarrow (x - x_0)^p = (x^p - x_0^p) \mid g(x^p)$. Οι ρίζες του $f_1(x)$ είναι διαφορετικές μεταξύ τους άρα $f_1^p(x) \mid g(x^p) \Rightarrow g(x^p) = g_1(x^p)f_1^p(x)$.

$$s^2(x)f_1(x) = g_1(x^p)f_1^p(x)$$
$$s^2(x) = g_1(x^p)f_1^{p-1}(x)$$

Άρα $g_1(x^p)$ είναι τετράγωνο $g_1(x^p) = h_1(x)^2, h_1(x) = \dfrac{s(x)}{f_1^{\frac{p-1}{2}}(x)}$.

Αφού $h_1^2(x) = g_1(x^p)$ και $(g_1(x^p))' = 0$

$$(h_1^2)' = 2h_1h_1' = 0$$
$$h_1' = 0$$

αφού $p \neq 2$ και $h_1 = 0 \Rightarrow s = 0$ το οποίο δεν ισχύει. Τελικά, $h_1(x) = g_2(x^p) \Rightarrow$

$$(s(x)y)^2 = s^2(x)f_1(x) = g_2^2(x^p)f_1^p(x) = (g_2(x^p)y^p)^2$$

οπότε και για την ϕ_y ισχύει $\frac{s(x)y}{t(x)} = b(x^p)y^p$. Άρα η $\phi = (a(x^p), b(x^p)y^p) = \phi' \circ \pi$. Επαναλαμβάνοντας την διαδικασία, η οποία τερματίζει αφού μικραίνει ο βαθμός των πολυωνύμων στις ρητές συναρτήσεις a, b, η ϕ γράφεται ως

$$\phi = \phi_{sep} \circ \pi^n$$

για κάποιο $n \geq 0$, $\pi : (x : y : z) \mapsto (x^p, y^p, z^p)$ και ϕ_{sep} κάποια διαχωρίσιμη isogeny.

$$\deg \phi = p^n \deg \phi_{sep}$$
$$\deg_s \phi := \deg \phi_{sep} \quad \deg_i \phi := p^n$$

όπου $\deg_s \phi$ και $\deg_i \phi$ λέγονται ο **διαχωρίσιμος** και **μη διαχωρίσιμος βαθμός** της ϕ αντίστοιχα.

Θεώρημα 4.2. $|\ker \phi| = \deg_s \phi$

Απόδειξη. Έστω $\phi = \phi_{sep} \circ \pi^n$. $\ker \phi = \ker \phi_{sep}$ αφού

$$(x : y : z) = (0 : 1 : 0) \iff (x^p : y^p : z^p) = (0 : 1 : 0)$$

κι άρα ο π και οι δυνάμεις του έχουν τετριμμένο πυρήνα. Αρκεί λοιπόν να αποδειχθεί το ζητούμενο στην περίπτωση που $\phi = \phi_{sep}$ δηλαδή η ϕ να είναι διαχωρίσιμη.
Έστω $\phi(x, y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$ και $(a, b) \in \phi(E_1(\overline{k})), a, b \neq 0$. Το $\overline{k}$ είναι άπειρο σύνολο άρα τετοια a, b υπάρχουν (επιλέγεται ως a τετμημένη που δεν μηδενίζει το $f_1(x)$). Το σύνολο

$$S(a, b) = \{(x_0, y_0) \in E_1(\overline{k}) : \phi(x_0, y_0) = (a, b)\}$$

για το οποίο ισχύει $|S(a, b)| = |\ker \phi|$ αφού ϕ ομομορφισμός ομάδων. Αν $(x_0, y_0) \in S(a, b)$

$$\frac{u(x_0)}{v(x_0)} = a \qquad \frac{s(x_0)}{t(x_0)} = b$$

$t(x_0), s(x_0) \neq 0$ αφού $y_0 \neq 0$ άρα το

$$y_0 = \frac{t(x_0)}{s(x_0)}b$$

καθορίζεται από το x_0. Άρα αρκεί να καθοριστεί το πλήθος των x_0 στο $S(a, b)$.

$$g(x) = u(x) - av(x) = 0 \iff \phi(x_0, y_0) = (a, b)$$

Για να έχει λοιπόν το $g(x)$ πολλαπλή ρίζα πρέπει

$$g(x_0) = g'(x_0) = 0$$
$$av(x_0) = u(x_0) \qquad av'(x_0) = u'(x_0)$$

Πολλαπλασιάζοντας τις δύο τελευταίες σχέσεις κατά μέλη

$$av(x_0)u'(x_0) = u(x_0)av'(x_0)$$
$$v(x_0)u'(x_0) = u(x_0)v'(x_0) \tag{4.4}$$

Όμως αφού η ϕ είναι διαχωρίσιμη $uv' - v'u \neq 0$ και η παραπάνω σχέση έχει πεπερασμένο αριθμό ριζών. Αν λοιπόν το (a, b) επιλεχθεί ώστε επιπλέον να μην ικανοποιείται η 4.4 για κανένα $(x_0, y_0) \in S(a, b)$ τότε κάθε ρίζα της g είναι απλή και $|\ker \phi| = |S(a, b)| = \deg g = \deg \phi$ □

4.4 Υποομάδες Στρέψης και Πολυώνυμα Διαίρεσης

Έστω E/k μία ελλειπτική καμπύλη που δίνεται από την εξίσωση $y^2 = x^3 + Ax + B$. Η συνάρτηση $[n] : P \mapsto nP$ είναι isogeny $E \to E$ με πυρήνα την **n-υποομάδα στρέψης** της E

$$E[n] = \{P \in E(\overline{k}) : nP = O\}$$

Εκφράζοντας το nP σε Jacobian συντεταγμένες σαν συνάρτηση του $P = (x : y : 1) \in E(\overline{k})$ (δουλεύοντας στο $k[x, y]/\langle y^2 - x^3 - Ax - B\rangle$, λαμβάνοντας δηλαδή υπόψιν την εξίσωση της καμπύλης) τότε το nP μπορεί να γραφεί στη μορφή $nP = (\phi_n : \omega_n : \psi_n)$ με $\phi_n, \omega_n, \psi_n \in \mathbb{Z}[x, y, A, B]$ και

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

να είναι η κανονική μορφή της $[n]$.

Τα ψ_n ονομάζονται **πολυώνυμα διαίρεσης** και ορίζονται ως εξής

$$\psi_0 = 0$$
$$\psi_1 = 1$$
$$\psi_2 = 2y$$
$$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$$
$$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2)$$
$$\psi_{2n} = \frac{1}{2y}\psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2)$$
$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3$$

με τους αναδρομικούς τύπους να ισχύουν για $n > 4$. Επιπλέον, $\psi_{-n} = -\psi_n$. Τα ϕ_n, ω_n

ορίζονται ως εξής

$$\begin{aligned}
\phi_n &= x\psi_n^2 - \psi_{n+1}\psi_{n-1} \\
\phi_n &= \phi_{-n} \\
\omega_n &= \frac{1}{4y}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2) \\
\omega_n &= \omega_{-n}
\end{aligned}$$

Λήμμα 4.2. $\forall n \in \mathbb{Z}$

$$\psi_n \in \begin{cases} \mathbb{Z}[x, A, B] & n \equiv 1 \mod 2 \\ 2y\,\mathbb{Z}[x, A, B] & n \equiv 0 \mod 2 \end{cases}$$

$$\phi_n \in \mathbb{Z}[x, A, B]$$

$$\omega_n \in \begin{cases} \mathbb{Z}[x, A, B] & n \equiv 0 \mod 2 \\ y\,\mathbb{Z}[x, A, B] & n \equiv 1 \mod 2 \end{cases}$$

Θεώρημα 4.3. *Έστω E/k μία ελλειπτική καμπύλη ορισμένη από την εξίσωση $y^2 = x^3 + Ax + B$ και $n \in \mathbb{Z} \setminus \{0\}$. Τότε για την isogeny $[n]$ ισχύει*

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

Απόδειξη. Για $n \in \{1, \ldots, 4\}$ οι τύποι ισχύουν. Για $n = 2m + 1 > 4$, υποθέτοντας ότι οι τύποι ισχύουν για m και $m + 1$ αρκεί να δειχθεί $P_n = P_m + P_{m+1}$ με $P_i = (\phi_i, \omega_i, \psi_i)$ σε Jacobian συντεταγμένες. Από την πράξη ομάδας προκύπτει πως $z_3 = x_1 z_2^2 - x_2 z_1^2$, δηλαδή

$$\begin{aligned}
\phi_m\psi_{m+1}^2 - \phi_{m+1}\psi_m^2 &= (x\psi_m^2 - \psi_{m+1}\psi_{m-1})\psi_{m+1}^2 - (x\psi_{m+1}^2 - \psi_{m+2}\psi_m)\psi_m^2 \\
&= x\psi_m^2\psi_{m+1}^2 - \psi_{m+1}^2\psi_{m-1} - x\psi_m^2\psi_{m+1}^2 + \psi_m^3\psi_{m+2} \\
&= \psi_m^3\psi_{m+2} - \psi_{m+1}^3\psi_{m-1} \\
&= \psi_{2m+1}
\end{aligned}$$

Για $n = 2m > 4$, υποθέτοντας ότι ισχύουν για m, αρκεί να δειχθεί ότι $P_n = P_m + P_m$ με $P_i = (\phi_i, \omega_i, \psi_i)$ σε Jacobian συντεταγμένες. Από την πράξη ομάδας για τον διπλασιασμό $z_3 = 2y_1 z_1$, οπότε

$$\begin{aligned}
2\omega_m\psi_m &= 2\left(\frac{1}{4y}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)\right)\psi_m \\
&= \frac{1}{2y}\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \\
&= \psi_{2m}
\end{aligned}$$

Με αντίστοιχο τρόπο για τα ϕ_n, ω_n □

Για να προσδιοριστεί η δομή των n-υποομάδων στρέψης θα πρέπει να δειχθεί ότι η έκφραση της isogeny $[n]$ μέσω των πολυωνύμων ϕ_n, ω_n, ψ_n είναι πράγματι σε κανονική

μορφή, να προσδιοριστεί ο βαθμός της, καθώς και αν αυτή είναι διαχωρίσιμη. Το παρακάτω λήμμα αποδεικνύει πως το κλάσμα της τετμημένης $\frac{\phi_n}{\psi_n^2}$ είναι όπως στην κανονική μορφή.

Λήμμα 4.3. *Έστω E/k μία ελλειπτική καμπύλη ορισμένη από $y^2 = x^3 + Ax + B$. Τότε $(\phi_n(x), \psi_n^2(x)) = 1$*

Απόδειξη. Έστω πως $(\phi_n(x), \psi_n^2(x)) = d(x) \neq 1$ και $x_0 \in \overline{k}$ τέτοιο ώστε $d(x_0) = 0$. $P = (x_0, y_0) \in E(\overline{k}), P \neq O$. Τότε $nP = O$ αφού $\psi_n^2(x_0) = 0$ και άρα

$$\begin{aligned}
\phi_n(x_0) &= x_0\psi_n^2(x_0) - \psi_{n+1}(x_0, y_0)\psi_{n-1}(x_0, y_0) = 0 \\
0 &= 0 - \psi_{n+1}(x_0, y_0)\psi_{n-1}(x_0, y_0) \\
\psi_{n+1}(x_0, y_0) &= 0 \text{ ή } \psi_{n-1}(x_0, y_0) = 0 \\
(n-1)P &= O \text{ ή } (n+1)P = O \\
-P &= O \text{ ή } P = O
\end{aligned}$$

το οποίο έρχεται σε αντίθεση με την υπόθεση πως το P είναι αφινικό σημείο. □

Αρκεί, λοιπόν, σύμφωνα με τα παραπάνω να εξεταστεί η μορφή των ϕ_n, ψ_n για να προσδιοριστεί η αν είναι διαχωρίσιμη και ο βαθμός της isogeny $[n]$ $(\max\{\deg \phi_n, \deg \psi_n\})$. Αυτά προκύπτουν άμεσα από τους μεγιστοβάθμιους όρους ως προς τη μεταβλητή x (lt_x) των ϕ_n και ψ_n.

Λήμμα 4.4. *Για κάθε $n \in \mathbb{Z}^+$*

$$\begin{aligned}
\phi_n &= x^{n^2} + \cdots \\
\psi_n &= \begin{cases} nx^{\frac{n^2-1}{2}} + \cdots & n \equiv 1 \mod 2 \\ y(nx^{\frac{n^2-4}{2}} + \cdots) & n \equiv 0 \mod 2 \end{cases}
\end{aligned}$$

Ο βαθμός λοιπόν της isogeny $[n]$ είναι n^2. Αν η $\operatorname{char} k \nmid n$, τότε $lt_x\phi_n'(x) = n^2x^{n^2-1} \neq 0$, άρα από 4.3 η $[n]$ είναι διαχωρίσιμη. Αν $\operatorname{char} k \mid n$ τότε ο όρος $n^2x^{n^2-1}$ είναι 0 και $\deg \psi_n^2 < n^2 - 1$. Άρα $|\ker[n]| = |\{O\} \cup \{(x_0 : y_0 : 1) \in E(\overline{k}) : \psi(x_0) = 0\}| < \deg[n]$, επομένως από το θεώρημα 4.2 η $[n]$ είναι μη διαχωρίσιμη. Τελικά, $[n]$ διαχωρίσιμη αν και μόνον αν $\operatorname{char} k \nmid n$

4.4.1 Η δομή της $E[l^e]$

Έστω l πρώτος. Αν $\operatorname{char} k \nmid l$, τότε σύμφωνα με τα παραπάνω

$$|E[l]| = |\ker[l]| = \deg[l] = l^2$$

Αφού η $E[l]$ είναι αβελιανή, από το Θεμελιώδες Θεώρημα των Πεπερασμένα Παραγόμενων Αβελιανών Ομάδων

$$E[l] \cong \mathbb{Z}_l \times \mathbb{Z}_l \text{ ή } E[l] \cong \mathbb{Z}_{l^2}$$

Στην $E[l]$ ωστόσο κάθε στοιχείο έχει τάξη το πολύ l, οπότε ισχύει πως $E[l] \cong \mathbb{Z}_l \times \mathbb{Z}_l$
Για $e > 1$, $E[l^e] \cong \mathbb{Z}_{l^{e_1}} \times \mathbb{Z}_{l^{e_2}} \times \cdots \times \mathbb{Z}_{l^{e_r}}$ με $\sum_{i=1}^{r} e_i = e$ και $|E[l^e]| = l^{e2}$. Όμως $E[l] \leq E[l^e]$ οπότε

$r \neq 2$, γιατί αλλιώς θα υπήρχαν είτε λιγότερα είτε περισσότερα στοιχεία στην $E[l]$ (ανάλογα με το αν $r = 1$ ή $r > 2$). Επιπλέον, αφού κάθε στοιχείο της $E[l^e]$ έχει το πολύ τάξη l^e.

$$E[l^e] \cong \mathbb{Z}_{l^e} \times \mathbb{Z}_{l^e}$$

Αν τώρα $\operatorname{char} k \mid l$, $|E[l]| = \deg_s[l] < l^2$

$$\begin{aligned} \deg[l] &= (\deg_s[l])(\deg_i[l]) \\ l^2 &= (\deg_s[l])(\deg_i[l]) \\ \deg_s[l] = l \text{ ή } \deg_s[l] &= 1 \\ |E[l]| = l \text{ ή } |E[l]| &= 1 \\ E[l] \cong \mathbb{Z}_l \text{ ή } E[l] &= \{O\} \end{aligned}$$

Για $e > 1$, $E[l^e] \cong \mathbb{Z}_{l^{e_1}} \times \mathbb{Z}_{l^{e_2}} \times \cdots \times \mathbb{Z}_{l^{e_r}}$. Κατ' αντιστοιχία με την περίπτωση που $\operatorname{char} k \nmid l$, $r = 1$ ή $r = 0$ ανάλογα με το αν $E[l] \cong \mathbb{Z}_l$ ή $E[l] = \{O\}$. Αν $E[l] = \{O\}$ τότε και $E[l^e] = \{O\}$ γιατί αλλιώς θα υπήρχε στοιχείο τάξης l στην $E[l^e]$ και άρα και στην $E[l]$.
Αν $E[l] \cong \mathbb{Z}_l$ τότε $E[l^e] = \mathbb{Z}_{l_1^e}$, με $e_1 \leq e$. Επομένως, υπάρχει $P \in E[l^e], P \neq O$ τέτοιο ώστε $E[l^e] =< P >$. Όμως η $[l]$ είναι επί, άρα υπάρχει $Q \in E(\overline{k})$ τέτοιο ώστε $lQ = P$. Τότε, αν $e_1 < e$, το Q έχει τάξη l^{e_1+1} και $Q \notin< P >$. Όμως $Q \in E[l^e]$, άρα αναγκαστικά $e_1 = e$ και $E[l^e] \cong \mathbb{Z}_{l^e}$.

Συνοπτικά,

Θεώρημα 4.4. *Έστω E/k ελλειπτική καμπύλη. Τότε για κάθε πρώτο l και $e \geq 1$:*

$$E[l^e] \cong \begin{cases} \mathbb{Z}_{l^e} \times \mathbb{Z}_{l^e}, & \operatorname{char} k \neq l \\ \mathbb{Z}_{l^e} \text{ ή } \{O\}, & \operatorname{char} k = l \end{cases}$$

4.4.2 Πεπερασμένες υποομάδες της $E(\overline{k})$

Σαν άμεσο πόρισμα από την δομή των $E[l^e]$ για πρώτους l, μπορεί να καθοριστεί η δομή οποιασδήποτε πεπερασμένης υποομάδας της $E(\overline{k})$ και κατ' επέκταση η δομή της $E(\mathbb{F}_q)$.

Λήμμα 4.5. *Έστω μία πεπερασμένη αβελιανή ομάδα G, τότε η G είναι ισόμορφη με το ευθύ γινόμενο των διαφορετικών Sylow υποομάδων της.*

Απόδειξη. Αφού η G είναι αβελιανή, τότε κάθε μία από τις p-Sylow υποομάδες της είναι κανονική, οπότε για κάθε πρώτο p υπάρχει μία και μόνο μία p-Sylow υποομάδα, έστω H_p, αφού αυτές είναι μεταξύ τους συζυγείς.
Τότε ορίζεται $\phi : \prod_p H_p \to G$ με $\phi(h_1, h_2, \ldots, h_r) = h_1 h_2 \cdots h_r$, $h_i \in H_p$.

$$\begin{aligned} \phi((h_1, h_2, \ldots, h_r)(h_1', h_2', \ldots, h_r')) &= \phi(h_1 h_1', h_2 h_2', \ldots, h_r h_r') \\ &= (h_1 h_1')(h_2 h_2') \cdots (h_r h_r') \\ &= (h_1, h_2, \ldots, h_r)(h_1', h_2', \ldots, h_r') \\ &= \phi(h_1, h_2, \ldots, h_r)\phi(h_1', h_2', \ldots, h_r') \end{aligned}$$

όπου στο τελευταίο βήμα χρησιμοποιήθηκε πως η G είναι αβελιανή. Άρα ο ϕ είναι ομομορφισμός ομάδων. Ακόμη,

$$\begin{aligned}(h_1, h_2, \dots, h_r) \in \ker \phi &\iff \\ \phi(h_1, h_2, \dots, h_r) = e &\iff \\ h_1 h_2 \cdots h_4 = e &\iff \\ h_1 = (h_2 \cdots h_r)^{-1}\end{aligned}$$

Όμως το h_1 έχει τάξη σχετικά πρώτο ως προς τις τάξεις των $h_2, \dots, h_r$ άρα $\ker \phi = \{e\}$ και ο ϕ είναι μονομορφισμός. Τέλος, λόγω ισότητας του πλήθους των στοιχείων των $\prod_p H_p$ και G ο ϕ είναι επί και άρα ισομορφισμός. □

Θεώρημα 4.5. *Έστω E/k μία ελλειπτική καμπύλη. Κάθε πεπερασμένη υποομάδα της $E(\overline{k})$ είναι ισόμορφη με το γινόμενο δύο (πιθανώς τετριμμένων) κυκλικών ομάδων, με το πολύ μία από αυτές να έχει τάξη την οποία διαιρεί η* $\operatorname{char} k$.
Ειδικότερα, αν $k = \mathbb{F}_q$ με $\operatorname{char} \mathbb{F}_q = p$ τότε

$$E(\mathbb{F}_q) \cong \mathbb{Z}_m \times \mathbb{Z}_n$$

για $n, m \in \mathbb{Z}^+$ με $m \mid n$ και $p \nmid m$.

Απόδειξη. Έστω T μία πεπερασμένη υποομάδα της $E(\overline{k})$. Από το Λήμμα 4.5, η T είναι το ευθύ άθροισμα των l-Sylow υποομάδων της T_l με $T_l \leq E[l^e]$ για κάποιο $e \geq 1$. Άρα είναι το γινόμενο δύο κυκλικών ομάδων από το Θεώρημα 4.4, δηλαδή

$$T_l \cong T_{l,1} \times T_{l,2}$$

με $T_{l,1}, T_{l,2}$ ομάδες τάξης δύναμης του l και $T_{l,2}$ τετριμμένη αν $\operatorname{char} k = l$. Οι ομάδες $T_1 = \prod_l T_{l,1}$ και $T_2 = \prod_l T_{l,2}$ είναι κυκλικές αφού οι $T_{l,i}$ είναι κυκλικές για σταθερό i με σχετικά πρώτες τάξεις. Επίσης, με $\operatorname{char} k \nmid |T_{l,2}|$ γιατί αν $\operatorname{char} k = l$ τότε $T_l \cong T_{l,1} \times T_{l,2} \leq E[l^e] \cong \mathbb{Z}_{l^e} \times \{O\}$ και η $T_{l,2}$ είναι τετριμμένη. Τελικά,

$$G_1 \cong T_1 \times T_2 \cong \mathbb{Z}_m \times \mathbb{Z}_n$$

με $\operatorname{char} k \nmid n$. □

4.5 Το Θεώρημα του Hasse

Το θεώρημα του Hasse δίνει ένα φράγμα για το μέγεθος της ομάδας $E(\mathbb{F}_q)$. Συγκεκριμένα,

Θεώρημα 4.6 (Θεώρημα του Hasse)**.** *Έστω $E/\mathbb{F}_q$ μία ελλειπτική καμπύλη. Τότε*

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

όπου $|t| \leq 2\sqrt{q}$

Κάνοντας χρήση του ενδομορφισμού του Frobenius για μία ελλειπτική καμπύλη ορισμένη στο $\mathbb{F}_q$ προκύπτει πως

$$E(\mathbb{F}_q) = \{P \in E(\overline{\mathbb{F}}_q) : \pi_E(P) = P\} = \{P \in E(\overline{\mathbb{F}}_q) : (\pi_E - 1)(P) = O\} = \ker(\pi_E - 1)$$

όπου -1 είναι η isogeny $[-1]$ και για τις isogenies $(\phi + \psi)(P) := \phi(P) + \psi(P)$. Η $\pi_E - 1$ είναι διαχωρίσιμη και γενικότερα

Λήμμα 4.6. *Αν $\phi, \psi : E_1 \to E_2$ isogenies με ϕ διαχωρίσιμη, τότε η $\phi + \psi$ είναι διαχωρίσιμη αν και μόνον αν η ψ είναι διαχωρίσιμη.*

Απόδειξη. Αν η ψ είναι μη διαχωρίσιμη μπορεί να γραφεί ως $\psi = \psi_{sep} \circ \pi^n$ και $\phi = \phi_{sep} \circ \pi^m, n, m > 0$. Τότε $\phi + \psi = \phi_{sep} \circ \pi^n + \psi_{sep} \circ \pi^m = (\phi_{sep} \circ \pi^{n-1} + \psi_{sep} \circ \pi^{m-1}) \circ \pi$. Άρα η $\phi + \psi$ είναι μη διαχωρίσιμη. Αν $\phi + \psi$ είναι μη διαχωρίσιμη, τότε το ίδιο ισχύει για την $-(\phi + \psi)$, την $\phi - (\phi + \psi) = -\psi$ και την ψ. □

Επιπλέον, ισχύει πως

$$\deg(r\pi_E - s) = r^2 q + s^2 - rst$$

όπου $t = q + 1 - \deg(\pi^n - 1)$ όταν $(r, s) = 1$. Το t ονομάζεται το ίχνος του ενδομορφισμού του Frobenius. Όντας βαθμός, η παραπάνω ποσότητα είναι θετική, δηλαδή

$$r^2 q + s^2 - rst \geq 0$$
$$q(\frac{r}{s})^2 - t\frac{r}{s} + 1 \geq 0$$

Αυτή η σχέση ισχύει για όλους τους ρητούς $\frac{r}{s}$. Αφού το $\mathbb{Q}$ είναι πυκνό στο $\mathbb{R}$

$$qx^2 - tx + 1 \geq 0, \forall x \in \mathbb{R}$$

Έπεται ότι η διακρίνουσα δεν μπορεί να είναι θετική, άρα $\Delta = t^2 - 4q \leq 0 \Rightarrow |t| \leq 2\sqrt{q}$.

4.6 Ο αλγόριθμος του Schoof

Ο αλγόριθμος του Schoof είναι ένας αλγόριθμος πολυωνυμικού χρόνου που υπολογίζει το $|E(\mathbb{F}_q)|$ για κάποια ελλειπτική καμπύλη $E/\mathbb{F}_q$ της μορφής $y^2 = f(x)$. Αυτός υπολογίζει το ίχνος του ενδομορφισμού του Frobenius t (όπως στο θεώρημα του Hasse) modulo κάποιων μικρών πρώτων και χρησιμοποιεί το Κινεζικό Θεώρημα Υπολοίπων για να το υπολογίσει modulo έναν αριθμό που υπερβαίνει το διπλάσιο του φράγματος του Hasse (για να βρεθεί και το πρόσημό του). Έτσι, προσδιορίζεται πλήρως το t και κατ' επέκταση το $|E(\mathbb{F}_q)|$.

4.6.1 Το υπόλοιπο του ίχνους του Frobenius σε διαίρεση με το 2

Η $E(\mathbb{F}_q)$ είναι αβελιανή ομάδα, οπότε το $2 \mid |E(\mathbb{F}_q)|$ αν και μόνον αν η $E(\mathbb{F}_q)$ έχει ένα στοιχείο τάξης 2. Αν η $E : y^2 = f(x)$, τότε τα στοιχεία τάξης 2 στο $E(\mathbb{F}_q)$ είναι ακριβώς τα αφινικά σημεία της μορφής $(x_0, 0)$. Αυτό γιατί αν $P \neq O$ δηλαδή $P = (x, y)$ τότε

$$2P = O \Rightarrow P = -P \Rightarrow (x, y) = (x, -y) \Rightarrow y = 0$$

Για να υπάρχει ένα τέτοιο σημείο πρέπει να υπάρχει ρίζα του $f(x)$ στο $\mathbb{F}_q$.
Το $\mathbb{F}_q$ είναι το σώμα ριζών του $x^q - x \in \mathbb{F}_p[x]$, οπότε μπορεί να εξεταστεί αν ο μέγιστος κοινός διαιρέτης του $f(x)$ και του $x^q - x$ έχει βαθμό μεγαλύτερο του μηδέν οπότε και τα δύο πολυώνυμα θα έχουν κοινή ρίζα. Συγκεκριμένα,

$$t_2 = \begin{cases} 0 & \deg((f(x), x^q - x)) > 0 \\ 1 & \text{διαφορετικά} \end{cases}$$

με $t_2 \equiv t \mod 2$.

4.6.2 Το υπόλοιπο του ίχνους του Frobenius σε διαίρεση με περιττό πρώτο

Έστω περιττός πρώτος l. Ο ενδομορφισμός του Frobenius ικανοποιεί την εξίσωση

$$\pi_E^2 - t\pi_E + q = 0$$

υπό την έννοια ότι $\pi_E^2(P) - [t] \circ \pi_E(P) + [q](P) = O, \forall P \in E(\overline{\mathbb{F}}_q)$. Θεωρώντας την παραπάνω εξίσωση για τα στοιχεία της $E[l]$, επειδή αυτά έχουν τάξη το πολύ l

$$\pi_l^2 - t_l\pi_l + q_l = 0 \tag{4.5}$$

με π_l ο ενδομορφισμός του Frobenius σαν συνάρτηση $\pi_l : E[l] \to E[l]$ και $t_l, q_l \in \mathbb{Z}_l$ τέτοια ώστε $t_l \equiv t \mod l$ και $q_l \equiv q \mod l$. Η εξίσωση 4.5 ερμηνεύεται ως $\pi_l^2(P) - [t_l] \circ \pi_l(P) + [q_l](P) = O, \forall P \in E[l]$.
Για να υπολογιστεί τότε το t_l δοκιμάζονται όλες οι τιμές $c = 0, 1, \ldots l-1$ για τον υπολογισμό της $\pi_l^2 - c\pi_l + q_l$ και ελέγχεται για ποια τιμή του c η ποσότητα μηδενίζεται. Αν για κάποιο c ισχύει ότι $\pi_l^2 - c\pi_l + q_l = 0$, τότε επιλέγοντας $P \in E[l], P \neq O$ θα ισχύει πως

$$\pi_l^2(P) - c\pi_l(P) + q_l(P) = O \text{ και}$$
$$\pi_l^2(P) - t_l\pi_l(P) + q_l(P) = O$$

αφαιρώντας τις δύο σχέσεις κατά μέλη, προκύπτει πως

$$(c - t_l)\pi_l(P) = O$$

Το $\pi_l(P) \neq O$ και άρα έχει τάξη τον πρώτο l. Επομένως από την παραπάνω σχέση $l \mid c - t_l \iff c \equiv t_l \mod l$. Αυτό επαληθεύει πως αν η σχέση 4.5 ισχύει για κάποιο $P \in E[l] \neq O$ τότε θα ισχύει για κάθε $O \neq P \in E[l]$.

Η προηγούμενη παράγραφος δίνει έναν τρόπο υπολογισμού του ζητούμενου t_l, όμως απαιτείται ο υπολογισμός isogenies σαν συναρτήσεις από το $E[l]$ στο $E[l]$. Αν G μία αβελιανή ομάδα, τότε το σύνολο $\mathrm{End}(G) = \{\phi : G \to G, \phi \text{ ομομορφισμός}\}$ είναι δακτύλιος με πρόσθεση και πολλαπλασιασμό τις

$$+ : \mathrm{End}(G) \to \mathrm{End}(G), \quad (\phi + \psi)(P) = \phi(P) + \psi(P) \forall P \in G$$
$$\cdot : \mathrm{End}(G) \to \mathrm{End}(G), \quad (\phi\psi)(P) = (\phi \circ \psi)(P)) \forall P \in G$$

Έτσι, η εξίσωση 4.5 μπορεί να νοηθεί σαν εξίσωση στο $\mathrm{End}(E[l])$. Για την εύρεση του t_l χρειάζεται να μπορούν να γίνουν πράξεις στον δακτύλιο ενδομορφισμών $\mathrm{End}(E[l])$ και να μπορεί να ελεγχθεί η ισότητα στοιχείων του.

Υπολογισμοί στο $\mathrm{End}(E[l])$

Ένα σημείο $P \neq O, P = (x_0, y_0) \in E(\overline{\mathbb{F}}_q)$ ανήκει στην $E[l]$ αν και μόνον αν $\psi_l(x_0) = 0$ (Ο l είναι περιττός, άρα από το Λήμμα 4.2 το ψ_l είναι συνάρτηση μόνο του x). Για την αναπαράσταση των στοιχείων του $\mathrm{End}(E[l])$ σαν ρητές συναρτήσεις, αυτά νοούνται σαν στοιχεία του δακτυλίου

$$\mathbb{F}_q[x, y]/\langle \psi_l(x), y^2 - f(x) \rangle$$

Σε αυτή την περίπτωση

$$\begin{aligned} \pi_l &= (x^q \mod \psi_l(x), y^q \mod (\psi_l(x), y^2 - f(x))) \\ &= (x^q \mod \psi_l(x), (f(x)^{\frac{q-1}{2}} \mod \psi_l(x))y) \end{aligned}$$

και

$$[1]_l = (x \mod \psi_l, (1 \mod \psi_l(x))\, y)$$

Επομένως, μπορούν να αναπαρασταθούν τα στοιχεία της εξίσωσης 4.5 με μοναδικό τρόπο στη μορφή $(a(x), b(x)y)$ με $a(x), b(x) \in \mathbb{F}_q[x]/\langle \psi_l(x) \rangle$, δηλαδή σαν πολυώνυμα βαθμού το πολύ $\deg \psi_l = \frac{l^2-1}{2}$.

Για τον πολλαπλασιασμό $\phi_1 = (a_1(x), b_1(x)y), \phi_2 = (a_2(x), b_2(x)y) \in \mathrm{End}(E[l])$ από τον ορισμό

$$\phi_1\phi_2 = \phi_1 \circ \phi_2 = (a_1(a_2(x)), b_1(a_2(x))b_2(x)y)$$

Στην επιθυμητή μορφή

$$\phi_1\phi_2 = \phi_1 \circ \phi_2 = (a_1(a_2(x)) \mod \psi_l(x), (b_1(a_2(x))b_2(x) \mod \psi_l(x))\, y)$$

Η πρόσθεση για τα $\phi_1 = (a_1(x), b_1(x)y), \phi_2 = (a_2(x), b_2(x)y) \in \mathrm{End}(E[l])$ ορίζεται σημειακά, άρα θα πρέπει να χρησιμοποιηθούν οι τύποι για την πρόσθεση σημείων στην E. Θέτοντας

$x_1 = a_1(x), y_1 = b_1(x)y, x_2 = a_2(x), y_2 = b_2(x)y,$

$$(x_3, y_3) = (m^2 - x_1 - x_2, m(x_1 - x_3) - y_1)$$

όπου

$$m = \frac{y_1 - y_2}{x_1 - x_2} = \frac{b_1(x) - b_2(x)}{a_1(x) - a_2(x)}y = r(x)y, \quad \text{αν } x_1 \neq x_2$$

και

$$m = \frac{3x_1^2 + A}{2y_1} = \frac{3a_1^2(x) + A}{2b_1(x)y} = \frac{3a_1^2(x) + A}{2b_1(x)f(x)}y = r(x)y, \quad \text{αν } x_1 = x_2$$

Τελικά, για το x_3 ισχύει

$$\begin{aligned} x_3 =& r^2(x)y^2 - a_1(x) - a_2(x) \\ =& r^2(x)f(x) - a_1(x) - a_2(x) \end{aligned}$$

Άρα είναι μόνο συνάρτηση του x και άρα στην επιθυμητή μορφή, αγνοώντας την ρητή συνάρτηση r.
Τότε το y_3

$$\begin{aligned} y_3 =& m(a_1(x) - x_3) - b_1(x)y \\ =& r(x)y(a_1(x) - x_3(x)) - b_1(x)y \\ =& (r(x)(a_1(x) - x_3(x)) - b_1(x))y \end{aligned}$$

Άρα είναι και αυτό στην επιθυμητή μορφή, αγνοώντας την ρητή συνάρτηση r.

Αν $r(x) = \frac{u(x)}{v(x)}$ με $v(x)$ αντιστρέψιμη σαν στοιχείο του $\mathbb{F}_q[x]/\langle\psi_l(x)\rangle$, τότε μπορεί να γραφεί στην επιθυμητή μορφή σαν το πολυώνυμο $u(x)(v(x))^{-1} \mod \psi_l$. Αν $v(x)$ δεν είναι αντιστρέψιμο στοιχείο του $\mathbb{F}_q[x]/\langle\psi_l(x)\rangle$ τότε $(v(x), \psi_l(x)) \neq 1$ είναι ένας μη τετριμμένος παράγοντας του $\psi_l(x)$. Αν $v(x) = a_1(x) - a_2(x)$, τότε $\deg(v(x)) < \deg(\psi_l(x))$ και αν $v(x) = 2b_1(x)f(x)$, τότε $(\psi_l(x), f(x)) = 1$ αφού οι ρίζες του $f(x)$ δίνουν την 2-υποομάδα στρέψης και οι ρίζες του $\psi_l(x)$ δίνουν την l-υποομάδα στρέψης ($l \neq 2$). Επομένως, $(v(x), \psi_l(x)) \mid b_1(x)$. Σε κάθε περίπτωση, λοιπόν, ισχύει πως $\deg((v(x), \psi_l(x))) < \deg(\psi_l(x))$. Μπορεί, λοιπόν, να αντικατασταθεί ο δακτύλιος $\mathbb{F}_q[x]/\langle\psi_l(x)\rangle$ με τον $\mathbb{F}_q[x]/\langle g(x)\rangle$, όπου $g(x) = (v(x), \psi_l(x))$. Αυτό γιατί η σχέση 4.5 θα ισχύει και για όλα τα $P \in E[l]$ που έχουν ως τετμημένη ρίζα του $g(x)$. Τελικά, ο αλγόριθμος για τον υπολογισμό του t_l:

Αλγοριθμος 4.1: *Υπολογισμός του υπολοίπου της διαίρεσης με το l του ίχνους του Frobenius*

Input $E/\mathbb{F}_q : y^2 = f(x), l$ περιττός πρώτος
Output $t_l \equiv t \mod l$

```
h ← ψ_l ∈ F_q[x] (Double and Add)
while true do
try:
    π_l ← (x^q mod h, (f^((q−1)/2)(x) mod h)y)
    π_l^2 ← π_l ∘ π_l
    q_l ← (q mod l)[1]_l (Double and Add)
    s ← π_l^2 + q_l
    for t_l ← 0 to l − 1 do
        w ← t_l π_l (Double and Add)
        if w = s then
            return t_l
        end if
    end for
catch division by υ(x):
    h ← gcd(υ(x), h)
end while
```

Για τον υπολογισμό των π_l, π_l^2 απαιτείται ύψωση σε δύναμη στον δακτύλιο $\mathbb{F}_q[x]/\langle \psi_l(x), y^2 - f(x)\rangle$, δηλαδή $\log q$ πολλαπλασιασμοί. Όλα τα πολυώνυμα έχουν βαθμό που φράσσεται από τον βαθμό του ψ_l (μικρότερο δηλαδή από l^2), οπότε ο πολλαπλασιασμός των πολυωνύμων απαιτεί l^4 πολλαπλασιασμούς στο $\mathbb{F}_q$ το οποίο απαιτεί $\log^2 q$ πράξεις. Ο εσωτερικός βρόχος επαναλαμβάνεται το πολύ l φορές. Σε αυτόν γίνεται πολλαπλασιασμός σημείου με φυσικό αριθμό, άρα απαιτούνται $\log l$ πολλαπλασιασμοί στον δακτύλιο $\mathbb{F}_q[x]/\langle \psi_l(x), y^2 - f(x)\rangle$. Ο εξωτερικός βρόχος δεν μπορεί να επαναληφθεί πάνω από l^2 φορές αφού μία τέτοια επανάληψη σημαίνει επανεκκίνηση της διαδικασίας με h μικρότερου βαθμού (ωστόσο αυτή η επανεκκίνηση μπορεί να συμβεί μόνο μία φορά). Συνεπώς, ο αλγόριθμος είναι πολυωνυμικός ως προς το $\log q$ και το l, με πολυπλοκότητα $O(l^4 \log^3 q)$. Ακολουθεί ο αλγόριθμος του Schoof που χρησιμοποιεί τον αλγόριθμο 4.1.

Αλγοριθμος 4.2: *Αλγόριθμος του Schoof*

Input $E/\mathbb{F}_q : y^2 = f(x)$
Output $|E(\mathbb{F}_q)|$
  $M \leftarrow 1$
  $t \leftarrow 0$
  $l \leftarrow 2$
  while $M \leq 4\sqrt{q}$ **do**
    $t_l \leftarrow t \mod l$ (είτε υπολογίζοντας $(f(x), x^q - x)$ αν $l = 2$ είτε με τον αλγόριθμο 4.1 αν l περιττός)
    $t_t \leftarrow (M(M^{-1} \mod l)t_l + l(l^{-1} \mod M)t_t) \mod lM$
    $M \leftarrow lM$
    $l \leftarrow \text{nextprime}(l)$
  end while
  if $t > \frac{M}{2}$ **then**
    $t \leftarrow t - M$
  end if
  return $q + 1 - t$

Σαν αναλλοίωτη του βρόχου του αλγορίθμου 4.2 είναι πως στην μεταβλητή t_t είναι αποθηκευμένη η ποσότητα $t \mod M$. Σε κάθε επανάληψη του βρόχου το νέο M' προκύπτει από το προηγούμενο M μετά από πολλαπλασιασμό με τον πρώτο l. Από την προηγούμενη επανάληψη στην t_t είναι αποθηκευμένο το $t \mod M$, οπότε για το νέο t_t συνδυάζεται με το Κινέζικο Θεώρημα Υπολοίπων το $t \mod M$ και το $t \mod l$ για την αποθήκευση στην μεταβλητή t_t της ποσότητας $t \mod lM$, δηλαδή της $t \mod M'$, εξασφαλίζοντας την αναλλοίωτη.

Από το Θεώρημα των πρώτων αριθμών το l_{max} που χρειάζεται είναι $O(\log q)$, οπότε το πλήθος των πρώτων που θα χρειαστούν είναι $O\left(\frac{\log q}{\log(\log q)}\right)$. Έτσι, ο αλγόριθμος 4.2 έχει πολυπλοκότητα $O(\log^8 q)$ (αφού αντικατασταθεί το l στην πολυπλοκότητα του αλγορίθμου 4.1).

Παράδειγμα 4.8. Έστω $E/\mathbb{F}_{19}$ η ελλειπτική καμπύλη $y^2 = x^3 + 2x + 1$. Τότε $|E(\mathbb{F}_{19})| = 19 + 1 - t$. Θα προσδιοριστεί το t με τον αλγόριθμο 4.2. Αφού $2\sqrt{19} < 9$, $-9 < t < 9$. Για αυτό θα χρησιμοποιηθούν οι πρώτοι $l = 2, 3, 5$.

Για $l = 2$, γίνεται ο υπολογισμός του

$$(x^{19} - x, x^3 + 2x + 1) = 1$$

Άρα η $|E(\mathbb{F}_{19})|$ δεν έχει σημεία τάξης 2 και $t_2 = 1$.

Για $l = 3$, γίνεται η διαδικασία υπολογισμού όπως στον αλγόριθμο 4.2. $q_l = 1 \equiv q \mod 3$ και $q^2 = 361$. Πρέπει να ελεγχθεί αν

$$(x^{361}, y^{361}) + (x, y) = (x^{19}, y^{19})$$

$h(x) = \psi_3(x) = 3x^4 + 12x^2 + 12x - 4$ και $f(x) = x^3 + 2x + 1$.

$\pi_3 = (x^{19} \mod \psi_3(x), (f^9(x) \mod \psi_3(x))y) = (4x^3 - 9x^2 + 3x - 6, (-8x^3 - x^2 - 6x - 9)y)$
$\pi_3^2 = (a_2(a_1(x)) \mod \psi_3, (b_1(a_2(x))b_2(x) \mod \psi_l)y)$

όπου $a_1(x) = a_2(x) = 4x^3 - 9x^2 + 3x - 6, b_1(x) = b_2(x) = -8x^3 - x^2 - 6x - 9$

$$\pi_3^2 = (6x^3 - 6x^2 - 8x + 6, 8x^3 - 8x^2 + 2x - 8)$$

Για τον υπολογισμό του $(x^{361}, y^{361}) + (x, y)$ εφαρμόζεται η πράξη ομάδας.

$$m = \frac{b_1(x) - b_2(x)}{a_1(x) - a_2(x)} = \frac{8x^3 - 8x^2 + 2x - 8 - 1}{6x^3 - 6x^2 - 8x + 6 - x} = \frac{8x^3 - 8x^2 + 2x - 9}{6x^3 - 6x^2 - 9x + 6}$$

Ωστόσο $(6x^3 - 6x^2 - 9x + 6, \psi_l) = x - 8 \neq 1$, οπότε το νέο $h(x) = x - 8$. Είναι εμφανές πως για $x = 8$ είναι ένα σημείο της $E[3]$, οπότε $3 \mid |E(\mathbb{F}_{19})| = 19 + 1 - t \Rightarrow t \equiv 2 \mod 3$. Ωστόσο, ο αλγόριθμος συνεχίζει την διαδικασία

$$\pi_3 = (x^{19} \mod h(x), (f^9(x) \mod h(x))y) = (8, y)$$

$$\pi_3^2 = (8, y)$$

$$(x, y) = (8, y)$$

Για τον υπολογισμό του $(x^{361}, y^{361}) + (x, y) = 2(8, y)$ εφαρμόζεται η πράξη ομάδας

$$m = \frac{3a_1^2(x) + A}{2b_1(x)f(x)}y = \frac{3 \cdot 8^2 + 2}{2(x^3 + 2x + 1)} = \frac{4}{-6} = 12$$

$$(x_3, y_3) = (m^2 - 2a_1(x), m(a_1(x) - x_3) - b_1(x)y) = \ldots$$

Όταν, λοιπόν, $c = 2$

$$t_l\pi_l = 2(8, y) = (x^{361}, y^{361}) + (x, y)$$

οπότε ο αλγόριθμος αφού επαναλάβει τον παραπάνω υπολογισμό θα επιστρέψει $t_l = 2$.

Για $l = 5$, $q_l = 4 \equiv -1 \equiv q \mod 5, c = 3$. Πρέπει να ελεγχθεί αν

$$(x^{361}, y^{361}) - (x, y) = 3(x^{19}, y^{19})$$

$h(x) = \psi_5(x) = 5x^{12} + 10x^{10} + 17x^8 + 5x^7 + x^6 + 9x^5 + 12x^4 + 2x^3 + 5x^2 + 8x + 8.$

$$\begin{aligned}\pi_5 &= (x^{19} \mod \psi_5(x), (f^9(x) \mod \psi_5(x))y) \\ &= (-8x^{11} - 6x^{10} + 9x^8 - x^7 - x^6 - x^5 + 4x^4 + 5x^3 + 9x^2 - 2, \\ &\quad (-7x^{11} + x^{10} + 8x^9 - 9x^8 - 4x^7 + 4x^6 - x^5 + 7x^4 - 2x^2 + 5x - 8)y) \\ \pi_5^2 &= \ldots\end{aligned}$$

Στην συνέχεια υπολογίζεται το $(x^{361}, y^{361}) + (x, -y)$

$$m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{y^{361} + y}{x^{361} + x}$$

$$(x_3, y_3) = (m^2 - x_1 - x_2, m(x_1 - x_3) - y_1) = \dots$$

Τέλος, υπολογίζεται το $3\pi_l$ και προκύπτει ίσο με το παραπάνω (x_3, y_3), οπότε $t \equiv 3 \mod 5$.

Άρα,

$$t \equiv \begin{cases} 1 \mod 2 \\ 2 \mod 3 \\ 3 \mod 5 \end{cases} \Rightarrow t \equiv 23 \mod 30 \Rightarrow t = -7$$

$|E(\mathbb{F}_{19})| = 19 + 1 - t = 27$.

Κεφάλαιο 5

Το πρόβλημα του Διακριτού Λογαρίθμου

Η ασφάλεια των κρυπτογραφικών συστημάτων που χρησιμοποιούν ελλειπτικές καμπύλες στηρίζεται στο πρόβλημα του Διακριτού Λογαρίθμου. Στόχος αυτού του κεφαλαίου είναι η παρουσίαση του προβλήματος, αλγορίθμων που το επιλύουν και η ανάλυση της πολυπλοκότητας αυτών. Αν και το πρόβλημα είναι εύκολο σε ορισμένες περιπτώσεις, σε άλλες φαίνεται να είναι υπολογιστικά απρόσιτο.

Ορισμός 5.1 (Διακριτός Λογάριθμος)**.** *Έστω G ομάδα με $|G| = n \in \mathbb{N}$, $g \in G, y \in \langle g \rangle$ και $q = \text{ord}(g)$. Ζητείται να βρεθεί $x \in \mathbb{Z}_q$ τέτοιο ώστε $g^x = y$ (σε προσθετικό συμβολισμό $xg = y$). Αυτό το x λέγεται ο* ***διακριτός λογάριθμος*** *του y με βάση g και συμβολίζεται* $\log_g y$.

Μία περίπτωση στην οποία είναι εύκολο να υπολογιστεί ο διακριτός λογάριθμος είναι η ομάδα $(\mathbb{Z}_p, +)$ για p πρώτο. Δοθέντων $g, y \in \mathbb{Z}_p \setminus \{0\}$ αναζητείται $x \in \mathbb{Z}_p$ τέτοιο ώστε

$$xg = y$$
$$x = yg^{-1}$$

όπου g^{-1} ο πολλαπλασιαστικός αντίστροφος του $g \mod p$. Υπολογίζεται, λοιπόν, σε πολυωνυμικό χρόνο ο διακριτός λογάριθμος στην ομάδα $(\mathbb{Z}_p, +)$. Η ασφάλεια των συστημάτων που κάνουν χρήση ελλειπτικών καμπυλών βασίζεται στην υπόθεση ότι δεν υπάρχει αποτελεσματικός αλγόριθμος που να επιλύει το πρόβλημα του Διακριτού Λογαρίθμου στην ομάδα μίας ελλειπτικής καμπύλης. Η αντίθετη κατεύθυνση δηλαδή από το g και το x να βρεθεί το y είναι εύκολη στην γενική περίπτωση, υπό την έννοια ότι υπάρχει πολυωνυμικός αλγόριθμος ως προς την αναπαράσταση του x που να το επιλύει (παρότι οι πράξεις της ομάδας μπορεί να είναι υπολογιστικά ακριβές). Ένας τέτοιος είναι η εφαρμογή του αλγορίθμου 3.1 σε γενική ομάδα.

5.1 Brute Force

Η πιο απλή μέθοδος επίλυσης του προβλήματος του διακριτού λογαρίθμου είναι να υπολογιστούν σειριακά οι τιμές

$$g^0, g^1, g^2, \ldots, g^{q-1}$$

και να συγκριθούν με το y. Αν βρεθεί ισότητα, τότε έχει βρεθεί το $\log_g y$. Αυτός ο αλγόριθμος απαιτεί $O(q)$ πράξεις ομάδας. Είναι δηλαδή εκθετικός ως προς την δυαδική αναπαράσταση του q. Κατά μέση τιμή θα χρειαστεί $\frac{q}{2}$ πράξεις ομάδας ενώ καταλαμβάνει $O(1)$ χώρο.

5.2 Baby-Step Giant-Step

Ο αλγόριθμος Baby-Step Giant-Step του Shanks επιλύει τον διακριτό λογάριθμο με αρκετά λιγότερες πράξεις ομάδας απ' ότι η Brute Force προσέγγιση όμως αρκετά περισσότερες απαιτήσεις σε μνήμη. Είναι επιθυμητό να υπολογιστεί το $x \in \mathbb{Z}_q$ όταν $g^x = y$ με $\text{ord}(g) = q$. Στον αλγόριθμο, γράφεται ο x από την Ευκλείδια Διαίρεση ως

$$x = mk + r, \quad 0 \leq r < k \tag{5.1}$$

για κάποιο $k \in \mathbb{N}$. Τότε

$$\begin{aligned} g^x &= y \\ g^{mk+r} &= y \\ g^r &= yg^{-mk} \end{aligned}$$

Αρχικά υπολογίζονται τα Baby Steps g^r για $r \in \{0, \ldots, k-1\}$ και αποθηκεύονται. Στην συνέχεια υπολογίζονται τα Giant Steps yg^{-mk} για $m \in \{0, \ldots, k-1\}$ και κάθε ένα από αυτά ελέγχεται για ισότητα με τα Baby Steps. Όταν πετύχει η ισότητα για δεδομένα r και m τότε αυτά συδυάζονται όπως στην 5.1 για τον υπολογισμό του x.
Αν $k = \lceil \sqrt{q} \rceil$, τότε θα υπάρχει ένα Baby-step στο οποίο θα πετύχει η ισότητα. Σε αυτή την περίπτωση απαιτούνται $O(\sqrt{q})$ πράξεις ομάδας και $O(\sqrt{q})$ αποθηκευτικός χώρος.

Παράδειγμα 5.1. Ζητείται να βρεθεί ο $\log_5 3$ στην ομάδα $\mathbb{Z}_{37}^*$. Επιλέγεται $k = \lceil \sqrt{37} \rceil = 7$ και υπολογίζονται τα Baby-Steps 5^r για $r \in \{0, \ldots, 6\}$:

$$\begin{aligned} 5^0 &\mod 37 = 1 \\ 5^1 &\mod 37 = 5 \\ 5^2 &\mod 37 = 25 \\ 5^3 &\mod 37 = 14 \\ 5^4 &\mod 37 = 33 \\ 5^5 &\mod 37 = 17 \\ 5^6 &\mod 37 = 11 \end{aligned}$$

Στην συνέχεια υπολογίζονται τα Giant-Steps $3 \cdot 5^{-7m}$ για $m \in \{0, \ldots, 6\}$:

$$\begin{aligned} 3 \cdot 5^{-7 \cdot 0} &\mod 37 = 3 \\ 3 \cdot 5^{-7 \cdot 1} &\mod 37 = 31 \\ 3 \cdot 5^{-7 \cdot 2} &\mod 37 = 12 \\ 3 \cdot 5^{-7 \cdot 3} &\mod 37 = 13 \\ 3 \cdot 5^{-7 \cdot 4} &\mod 37 = 11 \end{aligned}$$

Προκύπτουν ίδιες τιμές για $r = 6, m = 4$, οι υπολογισμοί των Giant-Steps σταματούν και $\log_5 3 = 4 \cdot 7 + 6 = 34$

5.3 Ο αλγόριθμος ρ του Pollard

Έστω $G = \langle g \rangle, y \in G, |G| = n \in \mathbb{N}$. Ο αλγόριθμος ρ του Pollard πετυχαίνει τον υπολογισμό του διακριτού λογαρίθμου $\log_g y$ σε αναμενόμενο χρόνο $O(\sqrt{n})$ όπως και ο αλγόριθμος Baby-step Giant-step του Shanks όμως σε σταθερό $O(1)$ χώρο αντί του $O(\sqrt{n})$. Προς αυτή την κατεύθυνση επιλέγεται συνάρτηση $f : G \to G$ και υπολογίζεται η ακολουθία $\beta_{i+1} = f(\beta_i)$ για $i = 0, 1, \ldots$ Αφού η G είναι πεπερασμένη ομάδα θα υπάρχουν $i, m \in \mathbb{N}$ τέτοια ώστε $\beta_i = \beta_{i+m}$. Εκφράζοντας τα β_i και β_{i+m} σαν δυνάμεις του g και του y, δηλαδή

$$\beta_i = g^{k_i} y^{l_i} \text{ και } \beta_{i+m} = g^{k_{i+m}} y^{l_{i+m}}$$

το $x = \log_g y$ υπολογίζεται από την σχέση

$$k_i + x l_i \equiv k_{i+m} + x b_{i+m} \mod n$$

Αν τα στοιχεία της ακολουθίας (β_i) είναι τυχαία επιλεγμένα στοιχεία της G, τότε χρειάζεται να υπολογιστούν $O(\sqrt{|G|}) = O(\sqrt{n})$ για να είναι η πιθανότητα σύγκρουσης μεγαλύτερη του $\frac{1}{2}$ (Παράδοξο Γενεθλίων).

Ως προσέγγιση των παραπάνω απαιτήσεων, χωρίζεται η G σε τρία ξένα υποσύνολα $G = G_1 \cup G_1 \cup G_3$. Η συνάρτηση $f : G \to G$ ορίζεται τότε ως εξής:

$$f(\beta) = \begin{cases} g\beta & \text{αν } b \in G_1 \\ \beta^2 & \text{αν } b \in G_2 \\ y\beta & \text{αν } b \in G_3 \end{cases}$$

Επιλέγεται τυχαίο $k_0 \in \{1, \ldots, n\}, l_0 = 0$ και $\beta_0 = g^{k_0}$. Τα στοιχεία της ακολουθίας είναι τα $\beta_{i+1} = f(\beta_i), i \geq 0$ τα οποία γράφονται ως

$$\beta_i = g^{k_i} y^{l_i}$$

οπότε για τα k_i, l_i ισχύουν οι ακόλουθες σχέσεις:

$$k_{i+1} = \begin{cases} k_i + 1 \mod n & \text{αν } \beta_i \in G_1 \\ 2k_i \mod n & \text{αν } \beta_i \in G_2 \\ k_i & \text{αν } \beta_i \in G_3 \end{cases}$$

και

$$l_{i+1} = \begin{cases} l_i & \text{αν } \beta_i \in G_1 \\ 2l_i \mod n & \text{αν } \beta_i \in G_2 \\ l_i + 1 \mod n & \text{αν } \beta_i \in G_3 \end{cases}$$

Όταν, λοιπόν, δύο στοιχεία της ακολουθίας β_i και β_{i+m} είναι ίσα τότε

$$\begin{aligned} \beta_i &= \beta_{i+m} \\ g^{k_i} y^{l_i} &= g^{k_{i+m}} y^{l_{i+m}} \\ k_i + x l_i &\equiv k_{i+m} + x l_{i+m} \mod n \end{aligned} \tag{5.2}$$

Αν $(l_i - l_{i+m}, n) = d$, η 5.2 έχει d λύσεις, οι οποίες μπορούν να δοκιμαστούν αν το d είναι μικρό. Διαφορετικά, επιλέγεται καινούργιο k_0 και η διαδικασία επαναλαμβάνεται από την αρχή.

Με μία μικρή αύξηση των υπολογισμών, η ανίχνευση της σύγκρουσης μπορεί να επιτευχθεί σε σταθερό χώρο χρησιμοποιώντας μία μέθοδο εύρεσης συγκρούσεων όπως του Floyd. Σε αυτή, διατηρούνται δύο τριάδες (β_i, k_i, l_i) και $(\beta_{2i}, k_{2i}, l_{2i})$. Σε κάθε επανάληψη ελέγχεται αν $\beta_i = \beta_{2i}$. Αν η σύγκρουση συμβεί στα I, J τότε η ακολουθία $\beta_I, \beta_{I+1}, \ldots$ επαναλαμβάνεται με περίοδο $\Delta = J - I$, δηλαδή

$$\beta_i = \beta_{i+k\Delta}, k \in \mathbb{N}, i \geq I$$

Αν i είναι το μικρότερο πολλαπλάσιο του Δ μεγαλύτερο ή ίσο του I, τότε $i < J$ γιατί διαφορετικά αν $i \geq J$ τότε $i = q\Delta \geq I + \Delta \Rightarrow q(\Delta - 1) \geq I$, το οποίο δεν ισχύει αφού το i επιλέχθηκε ως ελάχιστο πολλαπλάσιο του Δ μεγαλύτερο ή ίσο του I. Άρα $i < J$ και αφού το i είναι πολλαπλάσιο του Δ, το ίδιο θα ισχύει και για το $2i$. Επομένως, η σύγκρουση ανιχνεύεται για $I \leq i < J$. Μόλις, λοιπόν, ανιχνευτεί η συγκρουση αναζητείται το ελάχιστο j τέτοιο ώστε $\beta_i = \beta_{i+j}$.

Παράδειγμα 5.2. Έστω $E/\mathbb{F}_{1093} : y^2 = x^3 + x + 1$, $P = (0, 1) \in E(\mathbb{F}_{1093}), Q = (240, 229)$. Η τάξη του P είναι 1067 και ζητείται ο $\log_P Q$, δηλαδή το $x \in \mathbb{Z}_{1067}$ τέτοιο ώστε $xP = Q$. Για τον ορισμό των τριών συνόλων επιλέγεται πως $P = (x, y) \in G_{i+1}$ αν $x \equiv i \mod 3$. Έπομένως,

$$f(x, y) = \begin{cases} P + (x, y) & \text{αν } x \equiv 0 \mod 3 \\ 2(x, y) & \text{αν } x \equiv 1 \mod 3 \\ Q + (x, y) & \text{αν } x \equiv 2 \mod 3 \end{cases}$$

μπορεί να οριστεί και το $f(O) = O$, ωστόσο αν προκύψει $f(O)$ τότε έχει βρεθεί μία σχέση της μορφής $aP + bQ = O$, απ' όπου μπορεί να βρεθεί εύκολα το $\log_P Q$ (εκτός αν προκύψει κάτι τετριμμένο όπως π.χ. $1067P + 2000Q = O$). Επιλέγεται $k_0 = 13$ οπότε $\beta_1 = 13P =$

(290, 799).

$\beta_1 = 13P + 0Q = (290, 799)$ $\beta_2 = 13P + 1Q = (999, 81)$
$\beta_2 = 13P + 1Q = (999, 81)$ $\beta_4 = 15P + 1Q = (969, 838)$
$\beta_3 = 14P + 1Q = (21, 575)$ $\beta_6 = 17P + 1Q = (853, 1088)$
$\beta_4 = 15P + 1Q = (969, 838)$ $\beta_8 = 34P + 3Q = (448, 14)$
$\beta_5 = 16P + 1Q = (921, 1024)$ $\beta_{10} = 68P + 7Q = (596, 750)$
$\beta_6 = 17P + 1Q = (853, 1088)$ $\beta_{12} = 136P + 16Q = (483, 611)$
$\beta_7 = 34P + 2Q = (671, 25)$ $\beta_{14} = 137P + 17Q = (1068, 980)$
$\beta_8 = 34P + 3Q = (448, 14)$ $\beta_{16} = 276P + 34Q = (619, 633)$
$\beta_9 = 68P + 6Q = (1016, 281)$ $\beta_{18} = 553P + 68Q = (472, 1004)$
$\beta_{10} = 68P + 7Q = (596, 750)$ $\beta_{20} = 39P + 137Q = (530, 1)$
$\beta_{11} = 68P + 8Q = (523, 938)$ $\beta_{22} = 78P + 276Q = (934, 696)$
$\beta_{12} = 136P + 16Q = (483, 611)$ $\beta_{24} = 156P + 553Q = (515, 587)$
$\beta_{13} = 137P + 16Q = (611, 610)$ $\beta_{26} = 157P + 554Q = (448, 14)$
$\beta_{14} = 137P + 17Q = (1068, 980)$ $\beta_{28} = 314P + 42Q = (596, 750)$
$\beta_{15} = 138P + 17Q = (838, 506)$ $\beta_{30} = 628P + 86Q = (483, 611)$
$\beta_{16} = 276P + 34Q = (619, 633)$ $\beta_{32} = 629P + 87Q = (1068, 980)$
$\beta_{17} = 552P + 68Q = (324, 858)$ $\beta_{34} = 193P + 174Q = (619, 633)$
$\beta_{18} = 553P + 68Q = (472, 1004)$ $\beta_{36} = 387P + 348Q = (472, 1004)$

Αφού βρέθηκε σύγκρουση στο β_{18},

$$\begin{aligned} 553 + 68x &\equiv 387 + 348x && \mod 1067 \\ x &\equiv (68 - 348)^{-1}(387 - 553) && \mod 1067 \\ x &\equiv 999 && \mod 1067 \end{aligned}$$

Τελικά, $\log_P Q = 999$.

5.4 Ο αλγόριθμος Pohling-Hellman

Ο αλγόριθμος Pohling-Hellman μετατρέπει το πρόβλημα του διακριτού λογαρίθμου από κυκλικές ομάδες με σύνθετη τάξη n σε κυκλικές ομάδες με τάξη πρώτων παραγόντων του n. Έστω $G = \langle g \rangle, y \in G, |G| = n \in \mathbb{N}$ και ζητείται το $x = \log_g y$. Η παραγοντοποίηση του n σε πρώτους είναι

$$n = \prod_{i=1}^{m} p_i^{e_i}$$

Στον αλγόριθμο Pohling-Hellman υπολογίζεται το $x \mod p_i^{e_i}$ για κάθε πρώτο παράγοντα p_i του n. Το x γράφεται ως $x \equiv x_0 + x_1 p_i + x_2 p_i^2 \ldots$ και άρα $\mod p_i^{e_i}$ ισχύει

$$x \equiv x_0 + x_1 p_i + \ldots + x_{e_i-1} p^{e_i-1} \mod p_i^{e_i}$$

Τότε

$$\begin{aligned} g^x &= y \\ (g^x)^{\frac{n}{p_i}} &= y^{\frac{n}{p_i}} \\ (g^{x_0+x_1 p_i+\cdots+x_{e_i-1}p_i^{e_i-1}+\cdots})^{\frac{n}{p_i}} &= y^{\frac{n}{p_i}} \\ (g^{x_0})^{\frac{n}{p_i}} g^{nq} &= y^{\frac{n}{p_i}} \\ (g^{x_0})^{\frac{n}{p_i}} &= y^{\frac{n}{p_i}} \\ g^{x_0 \frac{n}{p_i}} &= y^{\frac{n}{p_i}} \end{aligned}$$

Το $g^{\frac{n}{p_i}}$ έχει πλέον τάξη p_i οπότε μπορεί να υπολογιστεί το x_0 χρησιμοποιώντας κάποιον αλγόριθμο για τον διακριτό λογάριθμο όπως ο αλγόριθμος Baby-step Giant-step του Shanks ή ο αλγόριθμος ρ του Pollard. Γνωρίζοντας τα $x_0, x_1, \ldots x_j, j < e_i - 1$ υπολογίζεται το x_{j+1} ως εξής

$$\begin{aligned} g^{x_0+x_1 p_i+\cdots+x_{e_i-1}p_i^{e_i-1}+\cdots} &= y \\ g^{-x_0-x_1 p_i+\cdots-x_j p_i^j} g^{x_0+x_1 p_i+\cdots+x_{e_i-1}p_i^{e_i-1}+\cdots} &= g^{-x_0-x_1 p_i+\cdots-x_j p_i^j} y = y_j \\ g^{x_{j+1}p_i^{j+1}+x_{j+2}p_i^{j+2}\cdots} &= y_j \\ (g^{x_{j+1}p_i^{j+1}+x_{j+2}p_i^{j+2}\cdots})^{\frac{n}{p_i^{j+2}}} &= (y_j)^{\frac{n}{p_i^{j+2}}} \\ g^{x_{j+1}\frac{n}{p_i}} &= y_j^{\frac{n}{p_i^{j+2}}} \end{aligned}$$

Το x_{j+1} είναι τελικά το $\log_{g^{\frac{n}{p_i}}} y_j^{\frac{n}{p_i^{j+2}}}$ και χρειάζεται να λυθεί ο διακριτός λογάριθμος για στοιχείο με τάξη p_i. Μόλις, λοιπόν, υπολογιστούν όλα τα $x_j, 0 \le j < e_i$ είναι γνωστό το $x \mod p_i^{e_i}$. Αυτή η διαδικασία επαναλαμβάνεται για κάθε p_i πρώτο διαιρέτη του n και το συνολικό x υπολογίζεται $\mod n$ με το Κινέζικο Θεώρημα Υπολοίπων. Η παραπάνω διαδικασία μπορεί να υλοποιηθεί αναδρομικά επιτυγχάνοντας $O(k \log k + \sum_{p|n} v_p(n) \sqrt{p})$ όπου $k = log_2 n$ εφόσον χρησιμοποιηθεί κάποιος αλγόριθμος που επιλύει τον διακριτό λογάριθμο σε χρόνο $O(\sqrt{p})$ για στοιχείο με τάξη p, όπως ο αλγόριθμος Baby-step Giant-step του Shanks. Ο αλγόριθμος Pohling-Hellman είναι λοιπόν πολύ αποδοτικός αν η τάξη του στοιχείου βάσης για τον υπολογισμό του διακριτού λογαρίθμου έχει μικρούς πρώτους παράγοντες.

Παράδειγμα 5.3. Έστω $E/\mathbb{F}_{599} : y^2 = x^3 + 1, P = (60, 19), Q = (277, 239) \in E(\mathbb{F}_{599})$ με $\text{ord}(P) = 600 = n$. Αναζητείται $x \in \mathbb{Z}_{600}$ τέτοιο ώστε $xP = Q$. Η παραγοντοποίηση του n σε πρώτους είναι

$$n = 600 = 2^3 \cdot 3 \cdot 5^2$$

Το x γράφεται $x = x_0 + x_1 2 + x_2 2^2 + \ldots$, οπότε

$$\frac{n}{2}(xP) = \frac{n}{2}Q$$
$$x_0(\frac{n}{2}P) = \frac{n}{2}Q =$$
$$x_0(598, 0) = O$$

Άρα $x_0 = 0$.
Για το x_1 υπολογίζεται το $Q_1 = Q - x_0 P = Q$ και τότε

$$x_1(\frac{n}{2}P) = Q_1 \frac{n}{2^2} = Q\frac{n}{4}$$
$$x_1(598, 0) = (598, 0)$$

οπότε $x_1 = 1$.
Για το x_2 υπολογίζεται το $Q_2 = Q_1 - (1 \cdot 2)P = Q - 2P = (35, 243)$. Τότε

$$x_2(\frac{n}{2}P) = \frac{n}{2^3}Q_2$$
$$x_2(598, 0) = \frac{n}{2^3}(35, 243)$$
$$x_2(598, 0) = O$$

οπότε $x_2 = 0$. Τελικά, $x = x_0 + x_1 2 + x_2 2^2 + \ldots \equiv 2 \mod 8$.

Το x γράφεται $x = x_0 + x_1 3 + \ldots$, οπότε

$$x_0(\frac{n}{3}P) = \frac{n}{3}Q$$
$$x_0(0, 1) = (0, 598)$$

Αφού $2(0, 1) = (0, 598)$, $x_0 = 2$ και $x \equiv 2 \mod 3$.

Το x γράφεται $x = x_0 + x_1 5 \ldots$, οπότε για το x_0

$$x_0(\frac{n}{5}P) = \frac{n}{5}Q$$
$$x_0(84, 179) = (84, 179)$$

άρα $x_0 = 1$.
Για το x_1 υπολογίζεται το $Q_1 = Q - x_0 P = Q - P = (130, 129)$. Τότε

$$x_1(\frac{n}{5}P) = \frac{n}{5^2}Q_1$$
$$x_1(84, 179) = (491, 465)$$

Δοκιμάζοντας τις δυνατές τιμές για το x_1, προκύπτουν $2(84, 179) = (491, 134), 3(84, 179) = (491, 465)$, οπότε $x_1 = 3$. Τελικά, $x = 1 + 3 \cdot 5 + \ldots \equiv 16 \mod 25$.

Συνδυάζοντας τις ισοδυναμίες

$$x \equiv \begin{cases} 2 & \mod 8 \\ 2 & \mod 3 \\ 16 & \mod 25 \end{cases}$$

οπότε από το Κινέζικο Θεώρημα Υπολοίπων $x \equiv 266 \mod 600$, κι άρα $\log_P Q = 266$.

5.5 Index Calculus

Ο αλγόριθμος Index Calculus. σε αντίθεση με τους προηγούμενους αλγορίθμους που παρουσιάστηκαν, είναι ειδικού σκοπού και αφορά επίλυση του διακριτού λογαρίθμου στην πολλαπλασιαστική ομάδα ενός πεπερασμένου σώματος. Η απουσία ενός τέτοιου αλγορίθμου στην γενική περίπτωση για ελλειπτικές καμπύλες είναι αυτό που τις καθιστά περισσότερο ελκυστικές για κρυπτογραφικές εφαρμογές από τις πολλαπλασιαστικές ομάδες πεπερασμένων σωμάτων. Για την περιγραφή του αλγορίθμου γίνεται η υπόθεση πως το πεπερασμένο σώμα είναι το $\mathbb{F}_p = \mathbb{Z}_p, g, y \in \mathbb{F}_p$ με $\langle g \rangle = \mathbb{F}_p^*$, και ζητείται ο $\log_g y$.

Τα στοιχεία του $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ θεωρούνται ως οι ακέραιοι $0, \ldots, p-1 = N$ (χρησιμοποιούνται αυτοί οι ακέραιοι ως αντιπρόσωποι των συμπλόκων). Τότε, για κάθε ακέραιο e,

$$g^e y^{-1} \in \{1, \ldots, N\} \subseteq \mathbb{Z}$$

όπου στην παραπάνω σχέση το αποτέλεσμα θεωρείται ως στοιχείο του $\mathbb{Z}$ με χρήση των μοναδικών αντιπρόσωπων. Το αποτέλεσμα, ως ακέραιος, έχει μοναδική παραγοντοποίηση σε πρώτους

$$\prod_{i=1}^{m} p_i^{e_i} = g^e y^{-1}$$

με $e_i \geq 0$. Πολλαπλασιάζοντας και τα δύο μέλη της παραπάνω εξίσωσης με y και εφαρμόζοντας την συνάρτηση του διακριτού λογαρίθμου ως προς g προκύπτει πως

$$\sum_{i=1}^{m} e_i \log_g p_i + \log_g y \equiv e \mod N$$

όπου $\log_g p_i$ ο διακριτός λογάριθμος ως προς g της εικόνας του ακεραίου p_i μέσω του κανονικού ομομορφισμού $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. Ο διακριτός λογάριμος $log_g y$ καθορίζεται, τότε, από τους $\log_g p_i$. Στόχος του αλγορίθμου είναι η εύρεση αρκετών εξισώσεων που θα επιτρέψουν τον υπολογισμό του $\log_g y$, χωρίς τον υπολογισμό των $\log_g p_i$.

Για την δημιουργία του γραμμικού συστήματος εξισώσεων, επιλέγεται φυσικός B ως άνω όριο των πρώτων αριθμών που θα χρησιμοποιηθούν. Το πλήθος των πρώτων μέχρι το B είναι τότε $b = \pi(B) = O\left(\frac{B}{\log B}\right)$. Το σύνολο

$$P_B = \{p : p \leq B \text{ και } p \text{ πρώτος}\} = \{p_1, p_2, \ldots p_b\}$$

λέγεται factor base, και είναι το σύνολο από το οποίο θα προέρχονται τα p_i. Επιλέγοντας,

λοιπόν, e είναι επιθυμητό το αποτέλεσμα $g^e y^{-1} \in \{1, \ldots, N\}$ ως ακέραιος να μπορεί να παραγοντοποιηθεί από πρώτους που ανήκουν στο σύνολο P_B, πράγμα το οποίο θα συμβαίνει μόνο για μερικές τιμές του e. Αν αυτό συμβαίνει, ωστόσο, ο αριθμός $g^e y^{-1} \in \{1, \ldots, N\}$ λέγεται B-λείος (B-smooth) και γίνεται γνωστή μία γραμμική εξίσωση της μορφής

$$e_1 \log_g p_1 + e_2 \log_g p_2 + \ldots + e_b \log_g p_b + \log_g y \equiv e \mod N$$

Αφού κανένας διακριτός λογάριθμος δεν είναι γνωστός η παραπάνω νοείται σαν μία εξίσωση σε $b+1$ μεταβλητές

$$e_1 x_1 + e_2 x_2 \ldots + e_b x_b + x_{b+1} \equiv e \mod N$$

Η παραπάνω εξίσωση έχει λύση $x_i = \log_g p_i$, $1 \leq i \leq b$ και $x_{b+1} = \log_g y$. Επιλέγοντας τυχαία e, συγκεντρώνεται ένα σύστημα από $b+1$ γραμμικές εξισώσεις το οποίο αν επιλύεται γίνεται γνωστός ο $\log_g y$.

Συνοπτικά, ο αλγόριθμος Index Caclulus

Αλγοριθμος 5.1: *Index Calculus*

Input $y \in < g >= \mathbb{Z}_p^*$
Output $\log_g y$
  Επίλεξε όριο B
  $P_B \leftarrow \{p_1, p_2, \ldots, p_b\}$ (οι πρώτοι έως το B, $b = \pi(B)$)
  $N \leftarrow p - 1$
  $f \leftarrow$ **false**
  while not f **do**
    for i = 1 **to** b+1 **do**
      $e_i \leftarrow_R \{1, \ldots, N\}$ τέτοιο ώστε $g^{e_i} y^{-1} = \prod p_j^{e_{i,j}}$
      $R_i = (e_{i,1}, e_{i,2}, \ldots, e_{i,b}, 1, e_i)$
    end for
    if Solvablefor$x_{b+1}(R_1, \ldots, R_{b+1}) \mod N$ **then**
      $x \leftarrow x_{b+1}$
      $f \leftarrow$ **true**
    end if
  end while
  return x

Αν το e επιλέγεται τυχαία και ομοιόμορφα από το $\mathbb{Z}_p^*$, το g^e είναι ένα ομοιόμορφα επιλεγμένο στοιχείο του $\mathbb{Z}_p^*$ και το ίδιο ισχύει για το $g^e y^{-1}$. Για την κατάλληλη επιλογή της τιμής του B είναι αναγκαία η γνώση της πιθανότητας ενός ομοιόμορφα επιλεγμένου στοιχείου του $\mathbb{Z}_p^*$, το οποίο θεωρείται ως το σύνολο των ακεραίων $\{1, \ldots, N\}$, να είναι B-λείο. Αν $\psi(N, B)$ είναι το πλήθος των B-λείων ακεραίων στο διάστημα $\{1, \ldots, N\}$ τότε η πιθανότητα να είναι ένας ομοιόμορφα επιλεγμένος ακέραιος στο διάστημα να είναι B-λείος είναι $\frac{\psi(N,B)}{N}$. Θέτοντας $u = \frac{\log N}{\log B}$ και αντικαθιστώντας το B με $N^{\frac{1}{u}}$ (αφού $\frac{1}{u} = \frac{\log B}{\log N} = \log_N B$), προκύπτει πως

$$\frac{1}{N} \psi(N, N^{\frac{1}{u}}) = u^{-u+o(u)} \tag{5.3}$$

καθώς $N, u \to \infty$ εφόσον $u < (1-\epsilon)\frac{\log N}{\log \log N}$ για κάποιο $\epsilon > 0$ [2].

Η χρονική πολυπλοκότητα του αλγορίθμου, αγνοώντας το κόστος για την επίλυση του συστήματος γραμμικών εξισώσεων, είναι τότε κατά προσέγγιση

$$(b+1)\cdot u^u \cdot b \cdot \mathrm{M}(\log N)$$

αφού ζητείται να παραχθούν $(b+1)$ εξισώσεις, $u^u \approx \frac{N}{\psi(N,B)}$ είναι η αναμενόμενη τιμή των e που θα πρέπει να δοκιμαστούν μέχρι να προκύψει ένας B-λείος αριθμός, b ο αριθμός των διαιρέσεων που πρέπει να γίνουν ώστε να καθοριστεί αν ένας αριθμός είναι B-λείος και $\mathrm{M}(\log N)$ η πολυπλοκότητα της διαίρεσης. Αντικαθιστώντας b με $\frac{B}{\log B}$ και αγνοώντας λογαριθμικούς όρους, ζητείται η τιμή του u που ελαχιστοποιεί την ποσότητα $B^2u^u = N^{\frac{2}{u}}u^u$. Ως προσέγγιση αυτού επιλέγεται η τιμή

$$u = \sqrt{\frac{\log N}{\log\log N}}$$

οπότε για το B που πρέπει να επιλεγεί ισχύει

$$B = N^{\frac{1}{u}} = exp(\frac{1}{u}\log N) = \exp\left(\frac{1}{2}\sqrt{\log N \log\log N}\right) = L_N\left[\frac{1}{2},\frac{1}{2}\right]$$

όπου

$$L_N[a,c] = \exp\left((c+o(1))(\log N)^a(\log\log N)^{1-a}\right)$$

Οι τιμές $L_N[0,c] = \log N^{c+o(1)}$ είναι πολυωνυμικές ως προς $\log N$ και οι τιμές $L_N[1,c] = N^{c+o(1)}$ είναι εκθετικές ως προς $\log N$, ενώ για $0 < a < 1$ οι τιμές $L_N[a,c]$ είναι υποεκθετικές ως προς $\log N$. Η συνολική, λοιπόν, χρονική πολυπλοκότητα του αλγορίθμου είναι κατά προσέγγιση

$$B^2u^u = L_N\left[\frac{1}{2},\frac{1}{2}\right]^2 L_N\left[\frac{1}{2}\right] = L_N\left[\frac{1}{2},2\right]$$

Παράδειγμα 5.4. Έστω $p = 1217$ και αναζητείται ο $\log_3 37$ στην $\mathbb{Z}_p^*, N = 1216$. Τότε $37^{-1} = 921 \mod 1217$. Επιλέγεται $B = \exp(\frac{1}{2}\sqrt{\log N \log\log N}) = 6.46$. Οπότε $P_B = \{2,3,5,7,11,13,17\}$.

Για $e = 12$

$$3^{12}37^{-1} \equiv 450 \mod N$$

με $450 = 2\cdot 3^2\cdot 5^2$ οπότε προκύπτει η εξίσωση

$$x_1 + 2x_2 + 2x_3 + x = 12$$

Για $e = 191$

$$3^{191}37^{-1} \equiv 5 \mod N$$

οπότε προκύπτει η εξίσωση

$$x_3 + x = 191$$

Για $e = 885$

$$3^{885}37^{-1} \equiv 1384 \mod N$$

με $1384 = 2^7 \cdot 3 \cdot 7$ οπότε προκύπτει η εξίσωση

$$7x_1 + x_2 + x = 885$$

Για $e = 917$

$$3^{917}37^{-1} \equiv 14 \mod N$$

με $14 = 2 \cdot 7$ οπότε προκύπτει η εξίσωση

$$x_1 + x_4 + x = 917$$

Για $e = 928$

$$3^{928}37^{-1} \equiv 1029 \mod N$$

με $1029 = 3 \cdot 7^3$ οπότε προκύπτει η εξίσωση

$$x_2 + 3x_4 + x = 928$$

Καλείται, λοιπόν, να εξεταστεί αν υπάρχει λύση ως προς x του συστήματος

$$\begin{cases} x_1 + 2x_2 + 2x_3 + x = 12 \\ x_3 + x = 191 \\ 7x_1 + x_2 + x = 885 \\ x_1 + x_4 + x = 917 \\ x_2 + 3x_4 + x = 928 \end{cases}$$

στον δακτύλιο $\mathbb{Z}_N$.

$$x_3 = 191 - x$$

Αντικαθιστώντας το παραπάνω στην πρώτη εξίσωση

$$\begin{aligned} x_1 + 2x_2 + 2(191 - x) + x &= 12 \\ x_1 &= 846 + x - 2x_2 \end{aligned}$$

Αντικαθιστώντας το x_1 στη τρίτη και την τέταρτη σχέση προκύπτει

$$\begin{aligned} 7(846 + x - 2x_2) + x_2 + x &= 885 \\ 8x - 13x_2 &= 1043 \\ x_2 &= (-13)^{-1}(1043 - 8x) \\ x_2 &= 481 - 280x \end{aligned}$$

και

$$\begin{aligned}(846 + x - 2x_2) + x_4 + x &= 917\\ -2x_2 + x_4 + 2x &= 71\\ -2(481 - 280x) + x_4 + 2x &= 71\\ x_4 &= 1033 - 562x\end{aligned}$$

Τέλος, στην τελευταία εξίσωση

$$\begin{aligned}(481 - 280x) + 3(1033 - 562x) + x &= 928\\ 467x &= 996\end{aligned}$$

Η τελευταία εξίσωση είναι η ισοδυναμία $467x \equiv 996 \mod 1216$ η οποία έχει μοναδική λύση αφού $(467, 1216) = 1$ και αυτή είναι η $x \equiv 588 \mod 1216$. Ελέγχοντας, προκύπτει πράγματι πως $3^{588} \equiv 37 \mod 1217$, άρα $\log_3 37 = 588$.

Κεφάλαιο 6

Κρυπτοσυστήματα Ελλειπτικών Καμπυλών

Οι ελλειπτικές καμπύλες χρησιμοποιούνται σε συστήματα ασύμμετρης κρυπτογραφίας, δηλαδή συστήματα στα οποία ο κάθε χρήστης διαθέτει ένα δημόσιο κι ένα ιδιωτικό κλειδί. Το ιδιωτικό κλειδί χρησιμοποιείται για την αποκρυπτογράφηση μηνυμάτων ενώ το δημόσιο μπορεί να χρησιμοποιηθεί από οποιονδήποτε για να κρυπτογραφήσει ένα μήνυμα που προσδιορίζεται για τον κάτοχο του αντίστοιχου ιδιωτικού κλειδιού. Σε αυτά τα συστήματα, πληροφορίες κρύβονται σε στοιχεία μίας ομάδας. Οι ομάδες των ελλειπτικών καμπυλών προσφέρουν αντίστοιχη ασφάλεια με άλλες ομάδες π.χ. η $\mathbb{Z}_n^*$ χρησιμοποιώντας πολύ λιγότερα bits πληροφορίας. Για παράδειγμα, την ίδια ασφάλεια που προσφέρει το RSA με κλειδιά των 3072 bits μπορεί να προσφέρει ένα σύστημα ελλειπτικών καμπυλών με κλειδιά μήκους 256 bits. Υλοποιήσεις κρυπτοσυστημάτων ελλειπτικών καμπυλών απαιτούν λιγότερη υπολογιστική ισχύ, λιγότερη κατανάλωση ενέργειας και είναι κατάλληλες για συσκευές IoT (Internet Of Things). Σε αυτό το κεφάλαιο θα παρουσιαστούν οι υποθέσεις πολυπλοκότητας για προβλήματα τα οποία χρησιμοποιούνται σε τέτοια συστήματα, καθώς και συστήματα ασύμμετρης κρυπτογραφίας που κάνουν χρήση ελλειπτικών καμπυλών.

6.1 Κρυπτογραφικές Υποθέσεις

Η ασφάλεια των κρυπτοσυστημάτων ελλειπτικών καμπυλών βασίζεται στην δυσκολία να λυθούν ορισμένα προβλήματα πάνω στην ομάδα μίας ελλειπτικής καμπύλης σε λογικό χρόνο.

6.1.1 ECDLP

Το ECDLP (Elliptic Curve Discrete Logarithm Problem) είναι η ειδική περίπτωση του προβλήματος του διακριτού λογαρίθμου πάνω στην ομάδα μίας ελλειπτικής καμπλύλης.

Ορισμός 6.1 (ECDLP)**.** *Έστω $E/\mathbb{F}_q$ μία ελλειπτική καμπύλη $P \in E(\mathbb{F}_q), Q \in \langle P \rangle, \mathrm{ord}(P) = k$. Ζητείται να βρεθεί $n \in \mathbb{Z}_k$ τέτοιο ώστε $nP = Q$. Το πρόβλημα αυτό ονομάζεται* ***ECDLP (Elliptic Curve Discrete Logarithm Problem)***

Αποτελώντας ειδική περίπτωση του προβλήματος του Διακριτού Λογαρίθμου μπορούν να χρησιμοποιηθούν όλοι οι αλγόριθμοι του προηγούμενου κεφαλαίου που το επιλύουν για γενικές ομάδες. Αυτοί απαιτούν εκθετικό χρόνο ως πως την δυαδική αναπαράσταση του μεγαλύτερου πρώτου που διαιρεί την τάξης του σημείου P. Συγκεκριμένα, απαιτούν χρόνο $O(\sqrt{\mathrm{ord}(P)})$ όταν η τάξη είναι πρώτος αριθμός. Σε αντίθεση με την πολλαπλασιαστική

ομάδα $\mathbb{Z}_n^*$ δεν είναι γνωστός κάποιος υποεκθετικός αλγόριθμος που να επιλύει το πρόβλημα του διακριτού λογαρίθμου για ελλειπτικές καμπύλες στη γενική περίπτωση. Η υπόθεση του διακριτού λογαρίθμου για ελλειπτικές καμπύλες είναι, λοιπόν, πως το ECDLP απαιτεί εκθετικό χρόνο για την επίλυση του στη γενική περίπτωση. Αξίζει να τονιστεί πως υπάρχουν ελλειπτικές καμπύλες στις οποίες το πρόβλημα ECDLP μπορεί να λυθεί σε υποεκθετικό (Επίθεση MOV) ή και σε πολυωνυμικό χρόνο (Επίθεση του Smart για $E(\mathbb{F}_p) = p$). Για κρυπτογραφικά συστήματα τέτοιες καμπλύλες πρέπει να αποφεύγονται. Για την αποφυγή όλων των πιθανά αδύναμων καμπυλών δεν προτείνεται η χρήση τυχαίων αλλά συγκεκριμένων οι οποίες έχουν περάσει ειδικό έλεγχο και είναι ασφαλείς. Για παράδειγμα, το πρότυπο FIPS 186-4 προτείνει αρκετές ελλειπτικές καμπύλες που μπορεί κανείς να χρησιμοποιήσει όπως η $P-256$ η οποία είναι μία ελλειπτική καμπύλη $E/\mathbb{F}_p$ της μορφής

$$y^2 = x^3 - 3x + b$$

με τις εξής παραμέτρους των 256 bits

$$\begin{aligned} p =& 115792089210356248762697446949407573530086143415290314195533631308867097853951 \\ b =& 41058363725152142129326129780047268409114441015993725554835256314039467401291 \end{aligned}$$

Το σημείο βάσης που χρησιμοποιείται είναι το $P = (P_x, P_y)$ με συντεταγμένες 256 bits

$$\begin{aligned} P_x =& 48439561293906451759052585252797914202762949526041747995844080717082404635286 \\ P_y =& 36134250956749795798585127919587881956611106672985015071877198253568414405109 \end{aligned}$$

το οποίο έχει πρώτη τάξη 256 bits

$$\text{ord}(P) = 115792089210356248762697446949407573529996955224135760342422259061068512044369$$

6.1.2 ECDH

Το πρόβλημα ECDH (Elliptic Curve Diffie-Hellman) είναι ένα πρόβλημα παρεμεφερές με του διακριτού λογαρίθμου, αν και ασθενέστερο από αυτό. Η ασφάλεια ορισμένων κρυπτογραφικών συστημάτων βασίζεται πάνω στην υπόθεση πως αυτό το πρόβλημα είναι υπολογιστικά απρόσιτο για μία ομάδα ελλειπτικών καμπυλών στη γενική περίπτωση.

Ορισμός 6.2 (ECDH)**.** *Έστω $E/\mathbb{F}_q$ μία ελλειπτική καμπύλη $P \in E(\mathbb{F}_q), \text{ord}(P) = k, a, b \in \mathbb{Z}_k$. Δίνονται $P, aP, bP \in E(\mathbb{F}_q)$ και ζητείται να υπολογιστεί το σημείο abP. Το πρόβλημα αυτό ονομάζεται* ***ECDH (Elliptic Curve Diffie-Hellamn)***

Το πρόβλημα αυτό είναι ασθενέστερο από το ECDLP αφού το ECDH ανάγεται σε πολυω-

νυμικό χρόνο στο ECDLP. Αν, λοιπόν, κανείς μπορεί να λύσει το πρόβλημα του διακριτού λογαρίθμου μπορεί να βρει το $a \in \mathbb{Z}_k$ από τα P, aP. Έπειτα υπολογίζει το $a(bP) = abP$ σε πολυωνυμικό χρόνο. Ισχύει, δηλαδή, πως

$$\text{ECDH} \leq \text{ECDLP}$$

ωστόσο δεν είναι γνωστό αν ισχύει και η αντίθετη κατεύθυνση.

6.1.3 ECDDH

Άλλο ένα πρόβλημα στην δυσκολία του οποίου βασίζουν την ασφάλεια τους ορισμένα κρυπτοσυστήματα ελλειπτικών καμπυλών είναι το πρόβλημα ECDDH (Elliptic Curve Decision Diffie-Hellman).

Ορισμός 6.3 (ECDDH)**.** *Έστω $E/\mathbb{F}_q$ μία ελλειπτική καμπύλη $P, Q \in E(\mathbb{F}_q)$, $\text{ord}(P) = k$, $a, b \in \mathbb{Z}_k$. Δίνονται $P, aP, bP, Q \in E(\mathbb{F}_q)$ και ζητείται να εξεταστεί αν $Q = abP$. Το πρόβλημα αυτό ονομάζεται* ***ECDDH (Elliptic Curve Decision Diffie-Hellamn)***

Το πρόβλημα αυτό είναι ευκολότερο από το ECDH και ανάγεται πολυωνυμικά σε αυτό. Αν κανείς μπορεί να λύσει το ECDH τότε μπορεί να υπολογίσει το abP από τα P, aP, bP και να εξετάσει αν $Q = abP$. Ισχύει, δηλαδή, πως

$$\text{ECDDH} \leq \text{ECDH}$$

χωρίς να είναι γνωστό αν ισχύει η αντίθετη κατεύθυνση. Συνολικά, λοιπόν, ισχύει πως

$$\text{ECDDH} \leq \text{ECDH} \leq \text{ECDLP}$$

Δεν είναι γνωστός κάποιος αλγόριθμος που να λύνει αποδοτικά το ECDDH στη γενική περίπτωση. Η υπόθεση Diffie-Hellman είναι πως το ECDDH είναι υπολογιστικά απρόσιτο.

6.2 Ανταλλαγή Κλειδιού Diffie-Hellamn

Η ανταλλαγή κλειδιών Diffie-Hellman (DHKE-Diffie Hellman Key Exchange) χρησιμοποιείται στην περίπτωση που ο Bob και η Alice θέλουν να συμφωνήσουν πάνω σε ένα μυστικό κλειδί, το οποίο έπειτα θα χρησιμοποιήσουν για ένα σύστημα συμμετρικής κρυπτογράφησης όπως το AES ή το DES. Η ανταλλαγή πληροφοριών γίνεται πάνω από ένα δημόσιο κανάλι, στο οποίο μπορεί να έχει πρόσβαση οποιοσδήποτε.

1. Αρχικά, η Alice κι ο Bob συμφωνούν σε μία ελλειπτική καμπύλη $E/\mathbb{F}_q$ που θα χρησιμοποιήσουν για την ανταλλαγή κλειδιού, τέτοια ώστε το πρόβλημα του διακριτού λογαρίθμου να είναι δύσκολο στην $E(\mathbb{F}_q)$. Έπειτα συμφωνούν σε ένα σημείο $P \in E(\mathbb{F}_q)$ με μεγάλη, συνήθως πρώτη, τάξη n.

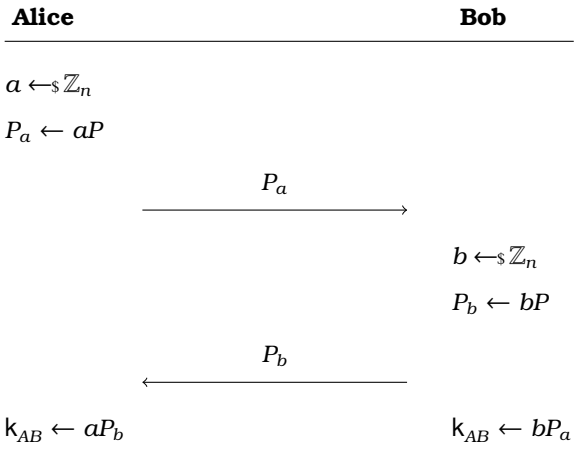
2. Η Alice επιλέγει ακέραιο $a \in \mathbb{Z}_n$ και υπολογίζει το $P_a = aP$ το οποίο αποστέλλει στον Bob.

3. Ο Bob επιλέγει ακέραιο $b \in \mathbb{Z}_n$ και υπολογίζει το $P_b = bP$ το οποίο αποστέλλει στην Alice.

4. Η Alice υπολογίζει το $aP_b = abP$.

5. Ο Bob υπολογίζει το $bP_a = abP$.

Σχηματικά η παραπάνω διαδικασία



Το κοινό μυστικό είναι τότε το

$$k_{AB} = abP$$

από το οποίο μπορούν ο Bob κι η Alice να αντλήσουν ένα μυστικό κλειδί. Για να παράδειγμα μπορούν να χρησιμοποιηθούν τα 256 bits της x συντεταγμένης του abP (στην περίπτωση της P-256) (ή κάποιο hash αυτής) σαν κλειδί για κρυπτογράφηση με ένα συμμετρικό σύστημα. Από την υπόθεση DH είναι υπολογιστικά απρόσιτο να μπορεί κάποιος κακόβουλος χρήστης που έχει πρόσβαση στο κανάλι να λάβει πληροφορία για το abP, αφού δεν μπορεί να το διακρίνει από τυχαίο σημείο της $\langle P \rangle$.

6.3 Συμπίεση Σημείων

Σε κρυπτοσυστήματα στα οποία χρησιμοποιούνται ελλειπτικές καμπύλες απαιτείται συχνά η αποθήκευση και η μεταφορά μέσω του δικτύου σημείων μίας ελλειπτικής καμπύλης. Στην περίπτωση που χρησιμοποιείται μία καμπύλη σε short Weierstrass μορφή, δηλαδή

$$E/\mathbb{Z}_p : y^2 = x^3 + ax + b$$

και χρησιμοποιείται η $E(\mathbb{Z}_p)$ τότε γνωρίζοντας την x συντεταγμένη ενός αφινικού σημείου $P = (x, y)$ υπάρχουν μόνο δύο περιπτώσεις για την τιμή του y (εκτός αν $x^3 + ax + b \equiv 0 \mod p$). Αυτές οι δύο είναι αντίθετες $\mod p$ και αφού ο p είναι μονός μία από τις δύο είναι μονή και η άλλη είναι ζυγή. Συνεπώς για να αποθηκευτεί ένα σημείο της καμπύλης αρκεί να αποθηκευτεί η x συντεταγμένη και ένα bit που να δηλώνει αν είναι άρτιο ή περιττό το $y \mod p$. Αυτό οδηγεί σε μία μείωση του μεγέθους που απαιτεί το σημείο για αποθήκευση κατά

σχεδόν 50%. Ωστόσο, για την ανακατασκευή του σημείου χρειάζονται επιπλέον υπολογισμοί αφού θα πρέπει να υπολογιστεί η τετραγωνική ρίζα $\mod p$

$$y = \pm \sqrt{x^3 + ax + b} \mod p$$

και να διατηρηθεί η λύση που συμφωνεί με το bit προσήμου.

6.4 Κρυπτοσυστήματα Δημοσίου Κλειδιού

Ένα σύστημα δημοσίου κλειδιού αποτελείται τρία σύνολα $\mathcal{M}, \mathcal{K}, C$ μηνυμάτων, κλειδιών και κρυπτοκειμένων και μία τριάδα PPT (Propabilistic Polynomial Time) αλγορίθμων

$$(\text{KeyGen}, \text{Enc}, \text{Dec})$$

όπου

- KeyGen είναι ο αλγόριθμος παραγωγής κλειδιών ο οποίος παίρνει σαν είσοδο την παράμετρο ασφάλειας 1^n και δίνει έξοδο ένα ζεύγος κλειδιών $(\mathsf{pk}, \mathsf{sk}) \in \mathcal{K}^2$ (Δημόσιο και Ιδιωτικό κλειδί).
- Enc είναι ο αλγόριθμος κρυπτογράφησης ο οποίος παίρνει σαν είσοδο ένα μήνυμα $m \in \mathcal{M}$ και ένα δημόσιο κλειδί pk και δίνει έξοδο ένα κρυπτοκείμενο $c \in C$.
- Dec είναι ο αλγόριθμος αποκρυπτογράφησης ο οποίος παίρνει σαν είσοδο ένα κρυπτοκείμενο $c \in C$ και ένα ιδιωτικό κλειδί sk και δίνει έξοδο ένα μήνυμα $m \in \mathcal{M}$.

από το οποίο απαιτείται να ισχύει

$$\text{Dec}(\mathsf{sk}, \text{Enc}(\mathsf{pk}, m)) = m, \forall m \in \mathcal{M}$$

Σε αυτό ο Bob εκτελεί τον αλγόριθμο KeyGen και δημιουργεί ένα ζεύγος δημόσιου ιδιωτικού κλειδιού $(\mathsf{pk}, \mathsf{sk})$. Η Alice θέλει να στείλει ένα μήνυμα $m \in \mathcal{M}$ στον Bob πάνω από μη ασφαλές κανάλι και έχει γνώση του δημοσίου κλειδιού pk του Bob. Εκτελεί τότε τον αλγόριθμο $\text{Enc}(\mathsf{pk}, m)$ ο οποίος δίνει σαν έξοδο το κρυπτοκείμενο c. Η Alice έπειτα στέλνει το κρυπτοκείμενο c στον Bob. Ο Bob αφού λάβει το κρυπτοκείμενο c εκτελεί τον αλγόριθμο $\text{Dec}(\mathsf{sk}, c)$ ο οποίος δίνει σαν έξοδο το μήνυμα m, οπότε ο Bob λαμβάνει το μήνυμα της Alice.

6.4.1 Το Κρυπτοσύστημα ElGamal

Το κρυπτοσύστημα ElGamal είναι ένα κρυπτοσύστημα δημοσίου κλειδιού που χρησιμοποιεί ελλειπτικές καμπύλες. Το κρυπτοσύστημα ElGamal αποτελείται από τους ακόλουθους αλγορίθμους:

- **KeyGen**$(1^n) = (\mathsf{pk}, \mathsf{sk})$
  Επιλέγεται πεπερασμένο σώμα $\mathbb{F}_q$, ελλειπτική καμπύλη $E/\mathbb{F}_q$ τέτοια ώστε το πρόβλημα του διακριτού λογαρίθμου να είναι δύσκολο, ένα σημείο $P \in E(\mathbb{F}_q)$ με $\text{ord}(P) = n$. Έπειτα, επιλέγεται τυχαίος ακέραιος $x \in \{1, \ldots, n-1\}$ και υπολογίζεται το σημείο $Q = xP$. Τα κλειδιά είναι τα $(\mathsf{pk}, \mathsf{sk}) = (\{E, P, Q, n\}, \{x\})$.

- **Enc**$(\mathsf{pk}, m) = c$
  Επιλέγεται τυχαίος ακέραιος $r \in \{1, \ldots, n-1\}$. Το κρυπτοκείμενο είναι το ζεύγος

$$(rP, m + rQ) = (R, S)$$

  .

- **Dec**$(\mathsf{sk}, (R, S)) = m$
  Το μήνυμα υπολογίζεται από τη σχέση

$$m = S - xR$$

  Αν το ζεύγος (R, S) έχει προέλθει από τον αλγόριθμο Enc τότε

$$S - xR = m + rQ - xrP = m + r(xP) - xrP = m$$

Σχηματικά, η διαδικασία αποστολής ενός μηνύματος m από την Alice στον Bob

Alice		**Bob**
		$(\{E, P, Q, n\}, \{x\}) \leftarrow \text{KeyGen}(1^{\lambda})$
	$\{E, P, Q, n\}$ $\longleftarrow$	
$r \leftarrow_{\$} \{1, \ldots, n-1\}$		
$R \leftarrow rP$		
$S \leftarrow m + rQ$		
	(R, S) $\longrightarrow$	
		$m \leftarrow S - xR$

Από τα παραπάνω είναι εμφανές πως στην περιγραφή του κρυπτοσυστήματος το μήνυμα είναι ένα στοιχείο της $E(\mathbb{F}_q)$. Είναι, ωστόσο, επιθυμητό να μπορεί να κρυπτογραφηθεί ένα μήνυμα το οποίο προέρχεται από το σύνολο $\{0,1\}^s$. Για να πραγματοποιηθεί αυτό χρησιμοποιείται μία συνάρτηση $f : \{0,1\}^s \to E(\mathbb{F}_q)$ η οποία κωδικοποιεί τα μηνύματα σαν σημεία της $E(\mathbb{F}_q)$. Αυτή μπορεί έπειτα να αντιστραφεί και να υπολογιστεί το μήνυμα από το σημείο στο οποίο κωδικοποιείται. Για παράδειγμα, έστω πως μία βάση για το $\mathbb{F}_q = \mathbb{F}_{p^k}$ πάνω από το $\mathbb{F}_p$ να είναι η $\{b_0, \ldots, b_{k-1}\}$, κι έστω πως $s = k - 1 - l, l \in \mathbb{N}$. Τότε ένα μήνυμα $m = m_0 \ldots m_{s-1}$ μπορεί να αναπαρασταθεί από το $x = m_0 b_0 + m_1 b_1 + \ldots + m_{s-1} b_{s-1} + 0 b_s + \ldots + 0 b_{k-1} \in \mathbb{F}_{p^k}$. Αν $x' = x^3 + ax + b$ είναι τετράγωνο τότε μπορεί να υπολογιστεί το $\sqrt{x'}$ και άρα το $P_m = (x, \sqrt{x'}) \in E(\mathbb{F}_{p^k})$. Αν το x' δεν είναι τετράγωνο, μπορούν να αυξηθούν τα ψηφία των συντελεστών $b_s, \ldots, b_{k-1}$ έως ότου αυτό να είναι τετράγωνο. Φυσικά, υπάρχει και η ελάχιστη πιθανότητα το x' να μην είναι ποτέ τετράγωνο οπότε το μήνυμα απορρίπτεται σαν μη κωδικοποιήσιμο. Η διαδικασία αντιστρέφεται εύκολα διατηρώντας τους συντελεστές των

$b_0, \dots b_{s-1}$ από την x-συντεταγμένη του P_m. Τέλος, ο χώρος των μηνυμάτων μπορεί να μεγαλώσει κατάλληλα ώστε να αξιοποιούνται καλύτερα οι συντελεστές των $b_0, \dots, b_{s-1}$, δηλαδή να κωδικοποιείται ένα μήμυμα το οποίο νοείται σαν ακέραιος στο $\{0, \dots, p^k - 1\}$

Είναι σημαντικό να μην χρησιμοποιείται η ίδια τιμή για την τυχαιότητα r πάνω από μία φορά. Αν $(R, S) = (rP, m_1 + rQ), (R, S') = (rP, m_2 + rQ)$ τότε με γνώση του m_1 υπολογίζεται το $S - m_1 = rQ$ και τότε μπορεί να υπολογιστεί το $m_2 = S' - rQ$.

Η εξαγωγή ενός μηνύματος m από τις δημόσιες πληροφορίες (R, S) είναι ισοδύναμη με το πρόβλημα ECDH αφού αν μπορεί να λυθεί το ECDH από τα rP, xP μπορεί να υπολογιστεί το $rxP = rQ$ και άρα και το μήνυμα $m = S - rQ$. Αντίστροφα, αν μπορεί να υπολογιστεί το μήνυμα από μία δυάδα $(R, S) = (rP, m + rQ)$, τότε επιλέγοντας $r = a, x = b, m$ μπορεί να υπολογιστεί από το $(R, S) = (aP, m + aQ) = (aP, m + abP)$ το μήνυμα m. Έπειτα γίνεται γνωστό το $S - m = abP$. Υποθέτοντας, λοιπόν, πως το ECDH είναι υπολογιστικά απρόσιτο δεν είναι δυνατόν από ένα κρυπτοκείμενο να εξαχθεί το μήνυμα από έναν PPT αντίπαλο παρά μόνο με αμελητέα πιθανότητα.

6.4.2 ECIES

Ένα ακόμη κρυπτοσύστημα δημοσίου κλειδιού που κάνει χρήση ελλειπτικών καμπυλών είναι το ECIES (Elliptic Curve Integrated Encryption Scheme) που επινοήθηκε από τους Bellare και Rogaway. Ενσωματώνει συμμετρική κρυπτογράφηση και MAC (Message Authentication Code). Σε αντίθεση με το κρυπτοσύστημα ElGamal τα μηνύματα δεν χρειάζεται να είναι σημεία μίας ελλειπτικής καμπύλης αλλά μπορούν να προέρχονται από το $\{0, 1\}^*$. Για να επιτευχθούν αυτά, χρησιμοποιείται ένα κρυπτοσύστημα συμμετρικής κρυπτογράφησης με αλγορίθμους $\text{Enc}'(k, m) : \{0, 1\}^m \times \{0, 1\}^* \to \{0, 1\}^*, \text{Dec}'(k, c) : \{0, 1\}^m \times \{0, 1\}^* \to \{0, 1\}^*$ και μία συνάρτηση σύνοψης $H : \{0, 1\}^* \to \{0, 1\}^k$ (ή κάποια άλλη μέθοδο για παραγωγή Message Authentication Code). Επιπλέον, χρησιμοποιείται μία Key Derivation Function (KDF) με χρήση της οποίας μπορεί να παραχθεί ένα κλειδί από ένα σημείο μίας ελλειπτικής καμπύλης, όπως για παράδειγμα αναφέρθηκε στην περίπτωση του DHKE μπορούν να χρησιμοποιηθούν κάποια bits (ή κάποιο hash αυτών) από την x-συντεταγμένη του σημείου.

Το κρυπτοσύστημα ECIES αποτελείται από τους ακόλουθους αλγορίθμους:

- **KeyGen**$(1^\lambda) = (\mathsf{pk}, \mathsf{sk})$
  Επιλέγεται πεπερασμένο σώμα $\mathbb{F}_q$, ελλειπτική καμπύλη $E/\mathbb{F}_q$ τέτοια ώστε το πρόβλημα του διακριτού λογαρίθμου να είναι δύσκολο, ένα σημείο $P \in E(\mathbb{F}_q)$ με $\text{ord}(P) = n$. Έπειτα, επιλέγεται τυχαίος ακέραιος $x \in \{1, \dots, n-1\}$ και υπολογίζεται το σημείο $Q = xP$. Τα κλειδιά είναι τα $(\mathsf{pk}, \mathsf{sk}) = (\{E, P, Q, n\}, \{x\})$.

- **Enc**$(\mathsf{pk}, m) = c$
  Επιλέγεται τυχαίος ακέραιος $r \in \{1, \dots, n-1\}$. Υπολογίζονται τα

$$U = rP$$
$$T = rQ$$

  Στη συνέχεια, χρησιμοποιείται η KDF πάνω στα U, T για την παραγωγή του $k_1 \| k_2$ με k_1, k_2 να έχουν ορισμένο μήκος.

Κρυπτογραφείται το μήνυμα μέσω του συμμετρικού αλγορίθμου κρυπτογράφησης με κλειδί το k_1, οπότε παράγεται το

$$c = \mathrm{Enc}'(k_1, m)$$

Τέλος, υπολογίζεται το MAC για το c με το κλειδί k_2

$$t = H(c \| k_2)$$

Το κρυπτοκείμενο είναι τότε το

$$(U, c, t)$$

- **Dec**$(\mathsf{sk}, (U, c, t)) = m$
  Υπολογίζεται το $T = xU$ με γνώση του ιδιωτικού κλειδιού $\mathsf{sk} = x$. Χρησιμοποιείται η KDF πάνω στα U, T για την παραγωγή του $k_1 \| k_2$.
  Χρησιμοποιώντας το k_2 ελέγχεται πως δεν έχει αλλοιωθεί το μήνυμα εξετάζοντας πως

  $$t = H(c \| k_2)$$

  Αν αυτό δεν ισχύει το μήνυμα απορρίπτεται. Αν ισχύει, τότε αποκρυπτογραφείται το c με το k_1 με χρήση του αλγορίθμου Enc′ οπότε παράγεται το

  $$m = \mathrm{Dec}'(k_1, c)$$

Σχηματικά, η διαδικασία αποστολής ενός μηνύματος m από την Alice στον Bob με χρήση του ECIES

Alice		**Bob**
		$(\{E, P, Q, n\}, \{x\}) \leftarrow \text{KeyGen}(1^{\beta})$
	$\xleftarrow{\{E, P, Q, n\}}$	
$r \leftarrow_{\$} \{1, \ldots, n-1\}$		
$U \leftarrow rP$		
$T \leftarrow rQ$		
$k_1 \| k_2 \leftarrow \text{KDF}(U, T)$		
$c \leftarrow \text{Enc}'(k_1, m)$		
$t \leftarrow H(c \| k_2)$		
	$\xrightarrow{(U, c, t)}$	
		$T \leftarrow xU$
		$k_1 \| k_2 \leftarrow \text{KDF}(U, T)$
		if $t \neq H(c \| k_2)$ then reject
		$m \leftarrow \text{Dec}'(k_1, c)$

Το σύστημα ECIES είναι ένα παράδειγμα Hybrid Encytption συστήματος όπου χρησιμοποιείται ένα σύστημα δημοσίου κλειδιού μαζί με ένα συμμετρικό σύστημα για την αποστολή κρυπτογραφημένων μηνυμάτων. Το σύστημα δημοσίου κλειδιού χρησιμοποιείται για τον προσδιορισμό του κλειδιού που θα χρησιμοποιήσει το συμμετρικό σύστημα για την κρυπτογράφηση του μηνύματος. Έτσι το ECIES μπορεί να κρυπτογραφεί αυθαίρετου μήκους μηνύματα (π.χ. σε Blocks από έναν Block Cipher όπως ο AES) εκτελώντας πράξεις πάνω στην ελλειπτική καμπύλη μία μόνο φορά.

Ένα ακόμη σημαντικό πλεονέκτημα του αλγορίθμου ECIES είναι πως έχει αντίσταση πάνω σε επιθέσεις CCA (Chosen Ciphertext Attacks), όπου ο αντίπαλος έχει την δυνατότητα να ζητήσει την αποκρυπτογράφηση μηνυμάτων της επιλογής του. Εκείνος όμως, δεν γνωρίζει το $T = xU$ ώστε να έχει στη διάθεση του το κλειδί k_2. Υποθέτωντας πως η συνάρτηση σύνοψης που χρησιμοποιείται έχει ανοχή στις συγκρούσεις είναι σχεδόν αδύνατον να παραχθεί μία σωστή τιμή y ώστε $H(c\|y) = H(c\|k_2)$. Έτσι, οι αποκρυπτογραφήσεις του επιτυθέμενου θα απορρίπτονται αιρώντας το πλεονέκτημα της αποκρυπτογράφησης κατά ζήτηση. Συγκεκριμένα το ECIES παρέχει ασφάλεια IND-CCA2.

6.5 Ψηφιακές Υπογραφές

Τα συστήματα ψηφιακών υπογραφών επιτρέπουν σε έναν χρήστη S που διαθέτει ένα δημόσιο κλειδί pk να υπογράψει ένα μήνυμα με το ιδιωτικό κλειδί του sk έτσι ώστε οποιοσδήποτε έχει πρόσβαση στο δημόσιο κλειδί pk να μπορεί να επιβεβαιώσει πως το μήνυμα προέρχεται από τον S και δεν έχει αλλοιωθεί. Σε αντίθεση με τα συστήματα δημοσίου κλειδιού, σε αυτή την περίπτωση ο κάτοχος του δημοσίου κλειδιού δρα σαν αποστολέας και όχι σαν παραλήπτης.

Ένα σύστημα ψηφιακών υπογραφών αποτελείται απο τρία σύνολα $\mathcal{M}, \mathcal{K}, \mathcal{S}$ μηνυμάτων, κλειδιών και υπογραφών αντίστοιχα και μία τριάδα PPT αλγορίθμων

$$(\text{KeyGen}, \text{Sign}, \text{Vf})$$

όπου

- KeyGen είναι ο αλγόριθμος παραγωγής κλειδιών ο οποίος παίρνει σαν είσοδο την παράμετρο ασφάλειας 1^η και δίνει έξοδο ένα ζεύγος κλειδιών $(\mathsf{pk}, \mathsf{sk}) \in \mathcal{K}^2$ (Δημόσιο και Ιδιωτικό κλειδί).

- Sign είναι ο αλγόριθμος υπογραφής ο οποίος παίρνει σαν είσοδο ένα μήνυμα $m \in \mathcal{M}$ και ένα ιδιωτικό κλειδί sk και δίνει έξοδο μία υπογραφή $\sigma \in \mathcal{S}$.

- Vf είναι ο αλγόριθμος ελέγχου της υπογραφής ο οποίος παίρνει σαν είσοδο ένα μήνυμα $m \in \mathcal{M}$, μία υπογραφή $\sigma \in \mathcal{S}$ και ένα ιδιωτικό κλειδί pk και δίνει έξοδο ένα bit $b \in \{0, 1\}$ που φανερώνει αν η υπογραφή είναι έγκυρη ή όχι.

Αν η Alice θέλει να υπογράψει ένα μήνυμα και να το στείλει υπογεγραμμένο στον Bob, πρώτα εκτελεί τον αλγόριθμο KeyGen και δημιουργεί ένα ζεύγος δημόσιου και ιδιωτικου κλειδιού $(\mathsf{pk}, \mathsf{sk})$. Επιλέγει το μήνυμα $m \in \mathcal{M}$ που θέλει να υπογράψει και εκτελεί τον αλγόριθμο Sign με είσοδο το μήνυμα m και το ιδιωτικό κλειδί sk και παίρνει ως έξοδο την υπογραφή $\sigma \in \mathcal{S}$. Έπειτα στέλνει το ζεύγος (m, σ) στον Bob. Ο Bob εκτελεί τον αλγόριθμο Vf με είσοδο το μήνυμα m, την υπογραφή σ και το δημόσιο κλειδί pk της Alice και παίρνει ως έξοδο ένα bit $b \in \{0, 1\}$ που φανερώνει αν η υπογραφή είναι έγκυρη.

6.5.1 Ψηφιακές Υπογραφές ElGamal

Το σύστημα ψηφιακών υπογραφών ElGamal αποτελείται από τους ακόλουθους αλγορίθμους

- **KeyGen**$(1^\eta) = (\mathsf{pk}, \mathsf{sk})$
  Επιλέγεται πεπερασμένο σώμα $\mathbb{F}_q$, ελλειπτική καμπύλη $E/\mathbb{F}_q$ τέτοια ώστε το πρόβλημα του διακριτού λογαρίθμου να είναι δύσκολο, ένα σημείο $P \in E(\mathbb{F}_q)$ με $\text{ord}(P) = n$. Έπειτα, επιλέγεται τυχαίος ακέραιος $x \in \{1, \ldots, n-1\}$ και υπολογίζεται το σημείο $Q = xP$. Τέλος, επιλέγεται συνάρτηση $f : \mathbb{F}_q \to \mathbb{Z}$. Αυτή δεν χρειάζεται συγκεκριμένες ιδιότητες εκτός από το ότι το σύνολο τιμών της θα πρέπει να είναι μεγάλο και μόνο μικρό πλήθος εισόδων να αντιστοιχίζονται στην ίδια έξοδο. Για παράδειγμα αν $\mathbb{F}_q = \mathbb{F}_p$ μπορεί να χρησιμοποιηθεί η x συντεταγμένη του σημείο σαν στοιχείο του $\mathbb{Z}_p$. Σε αυτή το πολύ δύο είσοδοι δίνουν την ίδια έξοδο. Τα κλειδιά είναι τα $(\mathsf{pk}, \mathsf{sk}) = (\{f, E, P, Q, n\}, \{x\})$.

- **Sign**$(\mathsf{sk}, m) = \sigma = (R, s)$
  Επιλέγεται τυχαίος ακέραιος $k \in \{1, \ldots, n-1\}$ με $(k, n) = 1$ και υπολογίζεται το $R = kP$ και το $r = f(R)$. Η υπογραφή είναι η δυάδα

$$(R, s) = (R, (m - xr)k^{-1} \mod n)$$

.

- **Vf**(pk, m, (R, s)) = b
  Υπολογίζεται το $r = f(R)$. Το b είναι 1 αν

$$rQ + sR = mP$$

  διαφορετικά είναι 0.
  Αν το ζεύγος (R, s) έχει προέλθει από τον αλγόριθμο Sign τότε

$$rQ + sR = r(xP) + (m - xr)k^{-1}(kP) = (rx + m - xr)P = mP$$

  και άρα η υπογραφή θα θεωρηθεί έγκυρη.

Σχηματικά, η διαδικασία υπογραφής ενός μηνύματος m από την Alice και αποστολή του υπογεγραμμένου μηνύματος στον Bob με χρήση ψηφιακών υπογραφών ElGamal

Alice		**Bob**
$(\{f, E, P, Q, n\}, \{x\}) \leftarrow \text{KeyGen}(1^n)$		
$k \leftarrow_{\$} \{1, \ldots, n-1\}, (k, n) = 1$		
$R \leftarrow kP$		
$r \leftarrow f(R)$		
$s \leftarrow (m - xr)k^{-1} \mod n$		
	$\xrightarrow{\{f, E, P, Q, n\}, m, (R, s)}$	
		$r \leftarrow f(R)$
		if $rQ + sR = mP$ then $b \leftarrow 1$
		else $b \leftarrow 0$

Οι ψηφιακές υπογραφές ElGamal διαθέτουν το ίδιο πρόβλημα με την κρυπτογράφηση ElGamal στην περίπτωση που επαναληφθεί η τυχαιότητα k. Επιπλέον, αν για την f μπορεί να προσδιοριστεί εύκολα σημείο για συγκεκριμένη εικόνα τότε οι ψηφιακές υπογραφές ElGamal δεν έχουν αντίσταση έναντι της υπαρξιακής πλαστογράφησης, δηλαδή της επίθεσης στην οποία καλείται ένας αντίπαλος να παράξει μία έγκυρη υπογραφή για ένα οποιοδήποτε μήνυμα. Αυτό μπορεί να αποφευχθεί χρησιμοποιώντας το πρότυπο Hash-and-Sign δηλαδή υπογράφοντας το Hash ενός μηνύματος.

6.5.2 ECDSA

Το σύστημα ECDSA (Elliptic Curve Digital Signature Algorithm) αποτελεί μία παραλλαγή των ψηφιακών υπογραφών ElGamal και ενσωματώνει το πρότυπο Hash-and-Sign.

Το σύστημα ψηφιακών υπογραφών ECDSA αποτελείται από τους ακόλουθους αλγορίθμους

- **KeyGen**$(1^\beta) = (\mathsf{pk}, \mathsf{sk})$
  Επιλέγεται πεπερασμένο σώμα $\mathbb{F}_p$, ελλειπτική καμπύλη $E/\mathbb{F}_p$ τέτοια ώστε το πρόβλημα του διακριτού λογαρίθμου να είναι δύσκολο, ένα σημείο $P \in E(\mathbb{F}_p)$ με $\mathrm{ord}(P) = n$. Έπειτα, επιλέγεται τυχαίος ακέραιος $x \in \{1, \ldots, n-1\}$ και υπολογίζεται το σημείο $Q = xP$. Τέλος, επιλέγεται συνάρτηση σύνοψης $H : \{0,1\}^* \to \{0, \ldots, n-1\}$. Τα κλειδιά είναι τα $(\mathsf{pk}, \mathsf{sk}) = (\{H, E, P, Q, n\}, \{x\})$.

- **Sign**$(\mathsf{sk}, m) = \sigma = (r, s)$
  Υπολογίζεται το $h = H(m)$. Επιλέγεται τυχαίος ακέραιος $k \in \{1, \ldots, n-1\}$ με $(k, n) = 1$ και υπολογίζεται το $R = kP = (x_R, y_R)$. Αν $r = x_R \equiv 0 \mod n$ επιλέγεται νέο k. Η υπογραφή είναι η δυάδα

$$(r, s) = (r, (h + xr)k^{-1} \mod n)$$

  .

- **Vf**$(\mathsf{pk}, m, (r, s)) = b$
  Υπολογίζεται τα $u_1 = s^{-1}h \mod n$ και $u_2 = s^{-1}r \mod n$. Έπειτα, υπολογίζεται το σημείο $u_1P + u_2Q = (x_1, y_1)$. Αν $r \equiv x_1 \mod n$ τότε η υπογραφή θεωρείται έγκυρη.
  Αν το ζεύγος (r, s) έχει προέλθει από τον αλγόριθμο Sign τότε

$$\begin{aligned}(x_1, y_1) &= u_1P + u_2Q = s^{-1}hP + s^{-1}rkP = s^{-1}(h + rk)P \\ &= (h + rk)^{-1}k(h + rk)P = kP = R \\ &= (x_R, y_R)\end{aligned}$$

  και άρα η υπογραφή θα θεωρηθεί έγκυρη.

Σχηματικά, η διαδικασία υπογραφής ενός μηνύματος m από την Alice και αποστολή του υπογεγραμμένου μηνύματος στον Bob με χρήση ψηφιακών υπογραφών ECDSA

Alice		**Bob**
$(\{H, E, P, Q, n\}, \{x\}) \leftarrow \text{KeyGen}(1^\eta)$		
$h \leftarrow H(m)$		
$k \leftarrow_\$ \{1, \ldots, n-1\}, (k, n) = 1$		
$(x_R, y_R) = R \leftarrow kP$		
$r \leftarrow x_R \mod n$		
$s \leftarrow (h + xr)k^{-1} \mod n$		
	$\{H, E, P, Q, n\}, m, (r, s) \longrightarrow$	
		$u_1 \leftarrow s^{-1}h \mod n$
		$u_2 \leftarrow s^{-1}r \mod n$
		$(x_1, y_1) = u_1P + u_2Q$
		if $r \equiv x_1 \mod n$ then $b \leftarrow 1$
		else $b \leftarrow 0$

Σε αντίθεση με τις ψηφιακές υπογραφές ElGamal, μόνο δύο πολλαπλασιασμοί ακεραίων με σημεία της E χρειάζονται για την επιβεβαίωση μίας υπογραφής. Αν πρέπει να γίνουν πολλές επαληθεύσεις ο ECDSA είναι αρκετά πιο αποδοτικός. Οι ψηφιακές υπογραφές ECDSA έχουν το ίδιο πρόβλημα με τις ψηφιακές υπογραφές ElGamal σε σχέση με την επανάληψη της τυχαιότητας k, η οποία θα πρέπει να αποφεύγεται.

Οι ψηφιακές υπογραφές ECDSA χρησιμοποιούνται περισσότερο από τις ψηφιακές υπογραφές ElGamal. Για παράδειγμα, το Bitcoin χρησιμοποιεί ECDSA πάνω από την καμπύλη secp256k1 η οποία είναι η $E/\mathbb{F}_p : y^2 = x^3 + 7$ με $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$. Το σημείο βάσης είναι το $P = (P_x, P_y)$ όπου

$$P_x = 55066263022277343669578718895168534326250603453777594175500187360389116729240$$

$$P_y = 32670510020758816978083085130507043184471273380659243275938904335757337482424$$

το οποίο έχει πλήρη τάξη

$$n = 11579208923731619542357098500868790785283756427907490438260516314151816149433 7$$

6.5.3 Ψηφιακές Υπογραφές Schnorr

Το σύστημα ψηφιακών υπογραφών Schnorr αποτελείται από τους ακόλουθους αλγορίθμους

- **KeyGen**$(1^\eta) = (\mathsf{pk}, \mathsf{sk})$

  Επιλέγεται πεπερασμένο σώμα $\mathbb{F}_q$, ελλειπτική καμπύλη $E/\mathbb{F}_q$ τέτοια ώστε το πρόβλημα

του διακριτού λογαρίθμου να είναι δύσκολο, ένα σημείο $P \in E(\mathbb{F}_q)$ με $\text{ord}(P) = n$. Έπειτα, επιλέγεται τυχαίος ακέραιος $x \in \{1, \ldots, n-1\}$ και υπολογίζεται το σημείο $Q = xP$. Τέλος, επιλέγεται συνάρτηση σύνοψης $H : \{0,1\}^* \to \{0, \ldots, n-1\}$. Τα κλειδιά είναι τα $(\mathsf{pk}, \mathsf{sk}) = (\{H, E, P, Q, n\}, \{x\})$.

- **Sign**$(\mathsf{sk}, m) = \sigma = (R, s)$
  Επιλέγεται τυχαίος ακέραιος $k \in \{1, \ldots, n-1\}$ και υπολογίζεται το $R = kP = (x_R, y_R)$. Η υπογραφή είναι το ζεύγος

$$(R, s) = (R, k + x \cdot H(R\|Q\|m) \mod n)$$

- **Vf**$(\mathsf{pk}, m, (R, s)) = b$
  Ελέγχεται αν

$$sP = R + H(R\|Q\|m) \cdot Q$$

  οπότε θεωρείται έγκυρη η υπογραφή.
  Αν το ζεύγος (R, s) έχει προέλθει από τον αλγόριθμο Sign τότε

$$sP = (k + x \cdot H(R\|Q\|m))P = kP + x \cdot H(R\|Q\|m)P = R + H(R\|Q\|m) \cdot Q$$

  και άρα η υπογραφή θα θεωρηθεί έγκυρη.

Σχηματικά, η διαδικασία υπογραφής ενός μηνύματος m από την Alice και αποστολή του υπογεγραμμένου μηνύματος στον Bob με χρήση ψηφιακών υπογραφών Schnorr

Alice		**Bob**
$(\{H, E, P, Q, n\}, \{x\}) \leftarrow \text{KeyGen}(1^\beta)$		
$k \leftarrow_\$ \{1, \ldots, n-1\}$		
$R \leftarrow kP$		
$s \leftarrow k + xH(R\|Q\|m) \mod n$		
	$\xrightarrow{\{H, E, P, Q, n\}, m, (R, s)}$	
		if $sP = R + H(R\|Q\|m) \cdot Q$
		then $b \leftarrow 1$
		else $b \leftarrow 0$

Οι υπογραφές Schnorr έχουν το ίδιο πρόβλημα με τις υπογραφές ElGamal και DSA σχετικά με την επανάληψη της τυχαιότητας. Σε αυτή την περίπτωση μπορεί να εξαχθεί το sk από την σχέση $s' - s = (k - k') - x(H(R\|Q\|m) - H(R'\|Q\|m'))$, οπότε αν $k = k'$ προκύπτει το $\mathsf{sk} = x = (s' - s)\,(H(R\|Q\|m) - H(R'\|Q\|m'))^{-1} \mod n$. Η επανάληψη του ίδιου k πρέπει και εδώ να αποφεύγεται.

Ένα πλεονέκτημα των υπογραφών Schnorr είναι πως δίνουν την δυνατότητα για μαζική επαλήθευση υπογραφών. Έτσι μπορούν να επαληθευτούν οι υπογραφές $(R_1, s_1), \ldots, (R_n, s_n)$

για τα μηνύματα $m_1, \ldots, m_n$ που υπογράφηκαν από τα ιδιωτικά κλειδιά $x_1, \ldots, x_n$ με αντίστοιχα δημόσια $Q_1, \ldots, Q_n$ από τη σχέση

$$(s_1 + \ldots + s_n)P = R_1 + H(R_1 \| Q_1 \| m) \cdot Q_1 + \ldots R_n + H(R_n \| Q \| m) \cdot Q_n$$

Κεφάλαιο 7

Παραγοντοποίηση Ακεραίων με Ελλειπτικές Καμπύλες

Στόχος αυτού του κεφαλαίου είναι η παρουσίαση του αλγορίθμου του Lenstra (ή Elliptic-Curve Factorization Method (ECM)) για την παραγοντοποίηση ακεραίων με ελλειπτικές καμπύλες. Αυτός αποτελεί έναν από τους πιο αποδοτικούς αλγορίθμους παραγοντοποίησης ακεραίων όντας υποεκθετικού χρόνου και έχει πολλές εφαρμογές στην κρυπτογραφία. Για διαιρέτες που δεν υπερβαίνουν τα 60 δεκαδικά ψηφία είναι ο πιο αποδοτικός, ενώ ο μεγαλύτερος παράγοντας που έχει βρεθεί μέσω αυτού του αλγορίθμου είχε 78 ψηφία. Βασίζεται σε ιδέες του αλγορίθμου $p-1$ του Pollard για την παραγοντοποίηση ακεραίων, ο οποίος είναι ένας ειδικού σκοπού αλγόριθμος παραγοντοποίησης, δηλαδή είναι ικανός να παραγοντοποιεί ακεραίους συγκεκριμένης μορφής.

7.1 Ο αλγόριθμος $p-1$ του Pollard

Έστω n ο σύνθετος αριθμός του οποίου ζητείται η παραγοντοποίηση και p ένας πρώτος του παράγοντας. Από το μικρό θεώρημα του Fermat αν a ένας ακέραιος με $p \nmid a$ δηλαδή $(p, a) = 1$, τότε

$$a^{p-1} \equiv 1 \mod p$$

Δηλαδή $p \mid a^{p-1} - 1$ και $p \mid n$, απ' όπου έπεται πως $p \mid (a^{p-1} - 1, n)$. Ωστόσο, δεν είναι γνωστή η τιμή του p για να μπορεί να υπολογιστεί το a^{p-1}. Αντί αυτού επιλέγεται

$$k = 2^{e_2} \cdot 3^{e_3} \cdot 5^{e_5} \cdots r^{e_r}$$

ένα γινόμενο αρκετών μικρών πρώτων και υπολογίζεται το $(a^k - 1, n) = (a^k - 1 \mod n, n)$. Το δεύτερο μέρος της ισότητας απαιτει πολυωνυμικό χρόνο ως προς τις δυαδικές αναπαραστάσεις των k, n για να υπολογιστεί. Αν, λοιπόν, ο $p-1$ έχει μικρούς πρώτους παράγοντες, έτσι ώστε $p-1 \mid k$ δηλαδή $k = (p-1)q$ τότε θα ισχύει πως

$$a^k \equiv a^{(p-1)q} \equiv (a^{p-1})^q \equiv 1^q \equiv 1 \mod p$$

άρα $p \mid (a^k - 1) \Rightarrow p \mid (a^k - 1, n)$. Επομένως ισχύει

$$(a^k - 1, n) \geq p > 1$$

Αν ισχύει πως $(a^k - 1, n) \neq n$ τότε έχει βρεθεί ένας μη τετριμμένος παράγοντας του n οπότε η διαδικασία μπορεί να επαναληφθεί για τους παράγοντες. Θα πρέπει να υπάρχει κάποιος έλεγχος πρώτων αριθμών για να οριστεί σε ποιους παράγοντες είναι να επαναληφθεί η διαδικασία. Αν, όμως, ισχύει πως $(a^k - 1, n) = n$, τότε θα πρέπει να επιλεγεί ένα νέο a και να πραγματοποιηθεί η διαδικασία από την αρχή. Αξίζει να τονιστεί πως η επιλογή του $a \in \{1, \ldots, n-1\}$ είναι τυχαία και για να λειτουργήσει ο αλγόριθμος θα πρέπει να ισχύει το μικρό θεώρημα του Fermat για τον a, δηλαδή να ισχύει πως $(a, n) = 1$. Αν $(a, n) = d > 1$, τότε ο d είναι αυτομάτως ένας μη τετριμμένος παράγοντας και ο n έχει παραγοντοποιηθεί σε γινόμενο μικρότερων ακεραίων.

Παράδειγμα 7.1. Έστω $n = 246082373$ ο οποίος είναι σύνθετος αφού $(n, 2) = 1$ και $2^{n-1} \equiv 180137693$. Επιλέγεται $a = 2$ και $k = 5! = 120 = 2^3 \cdot 3 \cdot 5$, οπότε

$$2^{120} \equiv 153677509 \mod n$$

και

$$(2^{120} - 1, n) = 1$$

Σε αυτή την περίπτωση ο αλγόριθμος δεν δίνει παράγοντα του n, ωστόσο η διαδικασία μπορεί να επανεκκινήσει για μεγαλύτερο k. Αν $k = 7! = 5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$ τότε

$$2^{5040} \equiv 101220672 \mod n$$

και

$$(2^{5040} - 1, n) = 2521$$

Βρέθηκε ένας μη τετριμμένος παράγοντας του n και η διαδικασία μπορεί να επαναληφθεί για τους 2521 και $\frac{n}{2521} = 97613$. Ωστόσο, με κάποιο έλεγχο πρώτων αριθμών μπορεί να επαληθευτεί πως

$$n = 246082373 = 2521 \cdot 97613$$

η παραγοντοποίηση του n σε πρώτους αριθμούς.

Ισχύει ο ισομορφισμός δακτυλίων $\mathbb{Z}_{246082373} \simeq \mathbb{Z}_{2521} \times \mathbb{Z}_{97613}$. Η πολλαπλασιαστικές τάξεις του 2 είναι

$$\begin{aligned} \mathrm{ord}_{\mathbb{Z}^*_{246082373}}(2) &= 30747780 = 2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 23 \cdot 1061 \\ \mathrm{ord}_{\mathbb{Z}^*_{2521}}(2) &= 1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7 \\ \mathrm{ord}_{\mathbb{Z}^*_{97613}}(2) &= 97612 = 2^2 \cdot 23 \cdot 1061 \end{aligned}$$

Ο αλγόριθμος πέτυχε επειδή η τάξη $\mathrm{ord}_{\mathbb{Z}^*_{2521}}(2)$ η οποία είναι ένας διαιρέτης του $p - 1 = 2521 - 1 = 2520$ διαιρούσε το $k = 5040$ αλλά η τάξη $\mathrm{ord}_{\mathbb{Z}^*_{97613}}(2)$ δεν διαιρούσε το k. Αν οι τάξεις διαρούσαν συγχρόνως το k θα ίσχυε πως $(2^k - 1, n) = n$ και ο αλγόριθμος δεν θα είχε αποτέλεσμα.

Στην πράξη, χρησιμοποιείται ένα άνω φράγμα B και γινόμενα πρώτων αριθμών μικρότερων του B για τον προσδιορισμό της τιμής του k.

Αλγοριθμος 7.1: *Ο αλγόριθμος $p-1$ του Pollard*

Input n σύνθετος, B όριο
Output Ένας γνήσιος παράγοντας του n ή failure

```
a ←_R {1, ..., n − 1}
d ← gcd(a, n)
if d ≠ 1 then
    return d
end if
b ← a
for l πρώτος με l ≤ B do
    e ← ⌈log_l n⌉ δηλαδή l^{e−1} < n ≤ l^e
    b ← b^{l^e} mod n
    if b = 1 (η περίπτωση που (b − 1, n) = n) then
        return failure
    end if
    d ← gcd(b − 1, n)
    if d ≠ 1 then
        return d
    end if
end for
return failure
```

Αν p, q είναι δυο πρώτοι παράγοντες του n με l_p και l_q οι μεγαλύτεροι πρώτοι παράγοντες των $p-1$ και $q-1$ αντίστοιχα, τέτοιοι ώστε $l_p < l_q, l_p \leq B$, τότε ο αλγόριθμος 7.1 όταν φτάσει στο l_p θα ισχύει πως $b = a^m$ με $m = \prod_{l \text{ πρώτος } \leq l_p} l^e$. Τότε $p-1 \mid m$ οπότε από το μικρό θεώρημα του Fermat $b = a^m \equiv 1 \mod p \Rightarrow p \mid b-1$. Όμως $l_q \nmid m$, οπότε με πιθανότητα τουλάχιστον $1 - \frac{1}{l_q}$ θα ισχύει $b \neq 1 \mod q$ και άρα $1 < (b-1, n) < n$ (Το πλήθος των στοιχείων της $\mathbb{Z}_q^*$ που έχουν τάξη που δεν διαιρείται από το l_q είναι το πλήθος των λύσεων ως προς e της εξίσωσης

$$g^{e\frac{q-1}{l_q^k}} \equiv 1 \mod q$$

όπου g ένας γεννήτορας της $\mathbb{Z}_q^*$ και k η μεγαλύτερη δύναμη του l_q που διαιρεί το $q-1$. Άρα το πλήθος των λύσεων είναι μικρότερο από το πλήθος των λύσεων της

$$g^{e\frac{q-1}{l_q}} \equiv 1 \mod q$$

που είναι ισοδύναμο με το πλήθος των λύσεων της $e\frac{q-1}{l_q} \equiv 0 \mod (q-1)$ η οποία έχει λύσεις όλα τα πολλαπλάσια του l_q μέχρι το $q-1$, δηλαδή $\frac{q-1}{l_q}$. Άρα υπάρχουν το πολύ $\frac{q-1}{l_q}$ στοιχεία στην $\mathbb{Z}_q^*$ με τάξη που δεν διαιρείται από το l_q, και άρα τουλάχιστον $q-1-\frac{q-1}{l_q} = \frac{(l_q-1)(q-1)}{l_q}$ στοιχεία με τάξη που διαιρείται από το l_q. Η πιθανότητα το a να είναι ένα από αυτά είναι, λοιπόν, τουλάχιστον $\frac{\frac{(l_q-1)(q-1)}{l_q}}{q-1} = \frac{l_q-1}{l_q} = 1 - \frac{1}{l_q}$).

Στην περίπτωση που $B = \sqrt{n}$, σύμφωνα με την παραπάνω παράγραφο, ο αλγόριθμος 7.1 είναι πολύ πιθανό ότι θα επιτύχει. Ωστόσο, είναι πιθανότερο πως θα αποτύχει αν ο n είναι δύναμη πρώτου ή αν ο μέγιστος πρώτος που διαιρεί το $p-1$ είναι ο ίδιος για

κάθε πρώτο παράγοντα p του n. Το κόστος χρόνου για την εκτέλεση του αλγορίθμου είναι $O(\pi(B)\mathrm{M}(\log N)\log N)$ όπου $\mathrm{M}(\log N)$ το κόστος πολλαπλασιασμού δυαδικών αριθμών με μήκος $\log N$. Αν επιλεγεί $B = \sqrt{n}$ το κόστος είναι $O(\sqrt{n}\mathrm{M}(\log N))$ δηλαδή ίδια με το να δοκιμαστούν όλοι οι πιθανοί παράγοντες του n από το 1 έως το $\sqrt{n}$, χωρίς να είναι σίγουρη η επιτυχία. Ωστόσο, ο αλγόριθμος $p-1$ του Pollard είναι ιδιαίτερα αποδοτικός στην περίπτωση που ο σύνθετος αριθμός n έχει πρώτους παράγοντες p τέτοιους ώστε το $p-1$ να είναι το γινόμενο μικρών παραγόντων.

Η ύπαρξη του αλγορίθμου $p-1$ του Pollard οδήγησε κρυπτογραφικά συστήματα τα οποία βασίζονται στην δυσκολία του προβλήματος της παραγοντοποίησης (π.χ. RSA) να χρησιμοποιούν **Safe Primes**. Αυτοί είναι πρώτοι p, τέτοιοι ώστε ο $p-1 = 2q$ με q επίσης πρώτο. Αν p Safe prime τότε το $p-1$ δεν έχει πολλούς μικρούς παράγοντες και είναι δύσκολο (πολύ μικρή πιθανότητα) να παραγοντοποιηθεί από τον αλγόριθμο 7.1.

7.2 Ο αλγόριθμος του Lenstra

Ο αλγόριθμος $p-1$ του Pollard εργάζεται στην ομάδα $\mathbb{Z}_n^*$ αλλά μπορεί να νοηθεί σαν να κάνει ταυτόχρονα τους υπολογισμούς στις ομάδες $\mathbb{Z}_p^*$ για κάθε $p \mid n$. Είναι απίθανο πως αυτός θα παραγοντοποιήσει τον n αν για κάθε $p \mid n$, το $p-1$ δεν είναι λείο. Ο αλγόριθμος του Lenstra θεωρεί μία ελλειπτική καμπύλη $E/\mathbb{Q}$ που ορίζεται από μία εξίσωση με ακέραιους συντελεστές της μορφής $y^2 = x^3 + Ax + B$ και έχει την ευκαιρία να παραγοντοποιήσει τον n αν για κάποιο πρώτο $p \mid n$ η $E(\mathbb{F}_p)$ έχει λεία τάξη. Το πλεονέκτημα αυτής της μεθόδου σε σχέση με τον αλγόριθμο $p-1$ του Pollard είναι πως στην περίπτωση που η $E(\mathbb{F}_p)$ δεν έχει λεία τάξη για κανένα $p \mid n$, τότε είναι εφικτό να δοκιμαστεί μία νέα ελλειπτική καμπύλη $E'/\mathbb{Q}$ για την οποία μπορεί η $E(\mathbb{F}_p)$ να έχει λεία τάξη για κάποιο $p \mid n$.

Ο αλγόριθμος του Lenstra ακολουθεί τα βήματα του αλγορίθμου $p-1$ του Pollard ωστόσο αντί για να υψώνεται ένα τυχαίο στοιχείο $a \in \mathbb{Z}_n^*$ σε μία μεγάλη λεία δύναμη k ελπίζοντας πως το $a^k \equiv 1 \mod p$, επιλέγεται ένα τυχαίο σημείο P σε μία ελλειπτική καμπύλη $E/\mathbb{Q}$ και υπολογίζεται το γινόμενο ενός μεγάλου λείου φυσικού k και του σημείου ελπίζοντας πως το $kP = O$ στην ομάδα $E(\mathbb{Z}/p\mathbb{Z})$. Συγκεκριμένα, ένα σημείο $P \in \mathbb{P}^2(\mathbb{Q})$ μπορεί να αναπαρασταθεί από τριάδα ακεραίων σχετικά πρώτων μεταξύ τους. Εφαρμόζοντας σε κάθε στοιχείο της τριάδας τον ομομορφισμό $x \mapsto x \mod p$ προκύπτει μία συνάρτηση $\mathbb{P}^2(\mathbb{Q}) \to \mathbb{P}^2(\mathbb{F}_p)$ η οποία είναι ομομορφισμός ομάδων από την $E(\mathbb{Q})$ στην $\overline{E}(\mathbb{F}_p)$ όπου η εξίσωση της $\overline{E}$ είναι η εξίσωση της $E \mod p$ όταν αυτή ορίζει ελλειπτική καμπύλη, δηλαδή ο p δεν διαιρεί την διακρίνουσα Δ. Αυτό ελέγχεται από το αν $(n, \Delta) = 1$. Αν $P \in E(\mathbb{Q})$ και $k \in \mathbb{N}$ τέτοιο ώστε το $kP = (Q_x : Q_y : Q_z)$ να είναι μέσω του ομομορφισμού το $O \in \overline{E}(\mathbb{F}_p)$ τότε $p \mid (Q_z, n)$. Στην περίπτωση που αυτός είναι n η διαδικασία γίνεται από την αρχή για νέα ελλειπτική καμπύλη E. Οι υπολογισμοί γίνονται όχι πάνω από το $\mathbb{Q}$ αλλά οι τριάδες διατηρούνται σαν στοιχεία του $\mathbb{Z}_n$ αφού ο αλγόριθμος ενδιαφέρεται μόνο για τις εικόνες αυτών των σημείων modulo πρώτων που διαιρούν τον n. Οι πράξεις γίνονται σε προβολικές συντεταγμένες οπού δεν υπάρχουν αντιστροφές και μπορούν να διατηρηθούν οι συντεταγμένες σαν στοιχεία του $\mathbb{Z}_n$.

Για να προκύψει μη τετριμμένος διαιρέτης του n θα πρέπει να ισχύει πως $(Q_z, n) \neq n$. Αυτό είναι πολύ πιθανό να ισχύει δεδομένου πως το $P \notin T(E(\mathbb{Q}))$, δηλαδή την υποομάδα

στρέψης της $E(\mathbb{Q})$. Αυτό ισχύει διότι ο ομομορφισμός που αναφέρθηκε στην προηγούμενη παράγραφο απεικονίζει ισομορφικά το $T(E(\mathbb{Q}))$ σε υποσύνολο του $E(\mathbb{F}_p)$ αν ο p δεν διαιρεί το διπλάσιο της διακρίνουσας της E κι οπότε θα ισχύει πως $(Q_z, n) = n$. Το να βρεθεί ένα σημείο που δεν ανήκει στο $T(E(\mathbb{Q}))$ για δεδομένη ελλειπτική καμπύλη E είναι δύσκολο. Για να αποφευχθεί αυτό επιλέγονται $x_0, y_0, a \in \{1, \ldots, N-1\}$ και $b = y_0^2 - x_0^3 - ax_0$, οπότε το $P = (x_0, y_0) \in E(\mathbb{Q})$ με $E : y^2 = x^3 + ax + b$. Η πιθανότητα το $P \in T(E(\mathbb{Q}))$ είναι αμελητέα (από το θεώρημα Nagell-Lutz [3, σ. 56, 2.5] θα πρέπει το $y_0^2 \mid \Delta = 4a^3 + 27b^2 = 4a^3 + 27(x_0^3 + ax_0)^2$ το οποίο έχει αμελητέα πιθανότητα).

Αλγοριθμος 7.2: *Ο αλγόριθμος του Lenstra*

Input n σύνθετος, B όριο, M όριο
Output Ένας γνήσιος παράγοντας του n ή failure

$a, x_0, y_0 \leftarrow_R \{0, \ldots, n-1\}$
$b \leftarrow y_0^2 - x_0^3 - ax_0$
$d \leftarrow \gcd(4a^3 + 27b^2, n)$
if $d \neq 1$ **and** $d \neq n$ **then**
  return d
else if $d = n$ **then**
  return failure
end if
$P \leftarrow (x_0 : y_0 : 1)$
$Q \leftarrow P$
for l πρώτος με $l \leq B$ **do**
  $Q \leftarrow l^e Q$ δηλαδή $l^{e-1} \leq (\sqrt{M} + 1)^2 < l^e$
  $d \leftarrow (Q_z, n)$
  if $d = n$ **then**
    return failure
  else if $d \neq 1$ **then**
    return d
  end if
end for
return failure

Ο παραπάνω αλγόριθμος υπολογίζει το $Q = mP$ όπου $m = \prod_{l \leq B} l^e$. Έστω πρώτοι $p, q \mid n$ τέτοιοι ώστε η εικόνα του P μέσω του ομομορφισμού που περιγράφηκε να είναι P_p και P_q αντίστοιχα, κι έστω πως η $\mathrm{ord}(P_p) \leq (\sqrt{p}+1)^2 \leq (\sqrt{M}+1)^2$ (Η αριστερή ανισότητα προκύπτει από το θεώρημα του Hasse 4.6) είναι B-λεία αλλά η $\mathrm{ord}(P_q)$ δεν είναι. Τότε $P_p = O$ αλλά $P_q \neq O$ οπότε $p \mid Q_z$ και $q \nmid Q_z$ και προκύπτει μη τετριμμένος παράγοντας του n.

Αν ο αλγόριθμος 7.2 αποτύχει μπορεί να επανεκκινήσει με άλλη καμπύλη. Ο αριθμός των φορών που θα πρέπει να επαναληφθεί ο αλγόριθμος εξαρτάται από την πιθανότητα το $|E(\mathbb{F}_p)|$ να είναι B-λείο. Είναι γνωστό πως $|E(\mathbb{F}_p)| = p + 1 - t, |t| \leq 2\sqrt{p}$ και προκύπτει πως $|E(\mathbb{F}_p)|$ κατανέμεται σχεδόν ομοιόμορφα στο διάστημα $\{p + 1 - 2\sqrt{p}, \ldots, p + 1 + 2\sqrt{p}\}$, οπότε η πιθανότητα ένας ακέραιος να είναι B-λείος σε αυτό το διάστημα προσεγγίζεται από την πιθανότητα ένας ακέραιος να είναι λείος στο $\{p, \ldots, 2p\}$ η οποία ασυμπτωτικά αντικαθίσταται από την πιθανότητα ένας ακέραιος στο $\{1, \ldots, p\}$ να είναι B-λείος. Κάτω από αυτές τις υποθέσεις, η χρονική πολυπλοκότητα του αλγορίθμου είναι $O(\pi(B)(\log M)\mathrm{M}(\log n))$ για κάθε

ελλειπτική καμπύλη και θα χρειαστούν $O(u^u)$ (5.3) καμπύλες για να βρεθεί ένας παράγοντας $p \leq M$ του n, όπου $u = \frac{\log M}{\log B}$. Ο αναμενόμενος χρόνος, λοιπόν, για να βρει ο αλγόριθμος παράγοντα του n είναι

$$O\left(u^u \cdot \pi(B) \cdot \log M \cdot \mathrm{M}(\log N)\right)$$

Αυτή η ποσότητα ελαχιστοποιείται για $u = \sqrt{\frac{2\log N}{\log\log N}}$ και άρα η βέλτιστη τιμή για το B είναι η $L_M\left[\frac{1}{2}, \frac{1}{\sqrt{2}}\right]$ οπότε ο αναμενόμενος χρόνος γίνεται $O\left(L_M\left[\frac{1}{2}, \frac{1}{\sqrt{2}}\right]\mathrm{M}(\log N)\right)$. Επειδή γενικά το όριο M δεν είναι γνωστό επιλέγεται ένα αρχικό και περιοδικά διπλασιάζεται οπότε επιτυγχάνεται αναμενόμενος χρόνος

$$O\left(L_p\left[\frac{1}{2}, \frac{1}{\sqrt{2}}\right]\mathrm{M}(\log N)\right)$$

που εξαρτάται δηλαδή από τον μικρότερο πρώτο παράγοντα p του n.

Παραρτήματα

Παράρτημα Α΄

Υπολογιστική Απόδειξη της Προσεταιριστικότητας

Η απόδειξη της προσεταιριστικότητας της πράξης ομάδας για ελλειπτικές καμπύλες στην εξίσωση short Weierstrass $E/k : y^2 = x^3 + Ax + B$ (Θεώρημα 3.1) μπορεί να γίνει με συμβολικούς υπολογισμούς. Σε αυτή την περίπτωση θεωρούνται τα σημεία

$$P = (P_x, P_y)$$
$$Q = (Q_x, Q_y)$$
$$R = (R_x, R_y)$$

Οι μεταβλητές τότε είναι οι $P_x, P_y, Q_x, Q_y, R_x, R_z, A, B$. Αυτές μπορούν να προστεθούν και να πολλαπλασιαστούν μεταξύ τους δηλαδή οι υπολογισμοί να γίνουν στον δακτύλιο

$$\mathbb{Z}[P_x, P_y, Q_x, Q_y, R_x, R_z, A, B]$$

Ωστόσο, τα P, Q, R είναι σημεία της καμπύλης οπότε για να αποδειχθεί η προσεταιριστικότητα θα πρέπει να μπορούν να εφαρμοστούν και οι σχέσεις

$$P_y^2 = P_x^3 + AP_x + B$$
$$Q_y^2 = Q_x^3 + AQ_x + B$$
$$R_y^2 = R_x^3 + AR_x + B$$

Τελικά, οι υπολογισμοί πρέπει να γίνουν στον δακτύλιο

$$R = \frac{\mathbb{Z}[P_x, P_y, Q_x, Q_y, R_x, R_z, A, B]}{\langle P_y^2 - P_x^3 - AP_x - B, Q_y^2 - Q_x^3 - AQ_x - B, R_y^2 - R_x^3 - AR_x - B\rangle}$$

Για την απόδειξη θα πρέπει να εξεταστούν οι ακόλουθες περιπτώσεις:

- Και τα τρία σημεία είναι διαφορετικά μεταξύ τους, δηλαδή να εξεταστεί αν

$$P + (Q + R) = (P + Q) + R$$

- Τα σημεία P, Q είναι ίδια, δηλαδή να εξεταστεί αν

$$P + (P + Q) = (P + P) + Q$$
$$P + (Q + P) = (P + Q) + P$$
$$Q + (P + P) = (Q + P) + P$$

- Το ένα σημείο είναι το $S = -P$

$$P + (S + Q) = (P + S) + Q$$
$$P + (Q + S) = (P + Q) + S$$
$$Q + (P + S) = (Q + P) + S$$

- Τα τρία σημεία είναι ίδια

$$P + (P + P) = (P + P) + P$$

Επιπλέον μπορούν να εξεταστούν και οι περιπτώσεις που $R = P + Q, R = P - Q, R = -(P + Q), R = 2P, R = -2P$.

Οι υπολογισμοί στον δακτύλιο R μπορούν να γίνουν μέσω αντιπροσώπων όπως οι κανονικοί υπολογισμοί στον δακτύλιο $\mathbb{Z}[P_x, P_y, Q_x, Q_y, R_x, R_z, A, B]$, δηλαδή πολυωνυμικό δακτύλιο με 8 μεταβλητές και συντελεστές στο $\mathbb{Z}$. Ο έλεγχος των παραπάνω ισοτήτων, ωστόσο, δεν γίνεται με απλό έλεγχο της ισότητας των συντεταγμένων των σημείων που προκύπτουν σαν αποτέλεσμα πράξεων στο αριστερό και το δεξί μέλος. Οι ισότητες θα πρέπει να εξεταστούν στον δακτύλιο πηλίκο R όπου εφαρμόζεται η εξίσωση της ευθείας για τα σημεία. Άρα είναι επιθυμητό να μπορεί να γίνει έλεγχος ισότητας των στοιχείων f, g modulo το ιδεώδες

$$I = \langle P_y^2 - P_x^3 - AP_x - B, Q_y^2 - Q_x^3 - AQ_x - B, R_y^2 - R_x^3 - AR_x - B \rangle$$

ή ισοδύναμα να εξεταστεί αν

$$f - g \in I$$

Αφού η πράξη ομάδας εκφράζεται από ρητές συναρτήσεις είναι επιθυμητό να μπορεί να εξεταστεί και η ισότητα δύο ρητών συναρτήσεων modulo I, δηλαδή για τις $\frac{f_1}{g_1}, \frac{f_2}{g_2}$ ισχύει $\frac{f_1}{g_1} = \frac{f_2}{g_2} \mod I$ ή ισοδύναμα αν $f_1 g_2 - f_2 g_1 \in I$. Τελικά, απαιτείται η δυνατότητα εξέτασης για το αν ένα πολυώνυμο ανήκει σε ένα ιδεώδες $I \triangleleft \mathbb{Z}[P_x, P_y, Q_x, Q_y, R_x, R_z, A, B]$.

Α΄.1 Αναπαράσταση και Πράξεις Πολυωνύμων

Τα πολυώνυμα του δακτυλίου $k[x_1, \ldots, x_n]$ πάνω από ένα αντιμεταθετικό δακτύλιο συντελεστών k μπορούν να αναπαρασταθούν σαν αθροίσματα μονωνύμων πολλαπλασιασμένα με σταθερές του k. Ένα μονώνυμο είναι τότε ένα γινόμενο της μορφής

$$x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$$

όπου $a_1, \ldots, a_n \in \mathbb{Z}_{\geq 0}$. Αυτό μπορεί να αναπαρασταθεί από ένα διάνυσμα $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n_{\geq 0}$ και συμβολίζεται x^a. Η ισότητα μονωνύμων μπορεί να εξεταστεί από την ισότητα των αντίστοιχων διανυσμάτων.

```
data Monomial = Monomial {
     getDegrees :: [Integer]
 } deriving (Eq)
```

Ο βαθμός του μονωνύμου είναι τότε το $|a| = a_1 + a_2 + \cdots + a_n$. Ένα πολυώνυμο $f \in k[x_1, \ldots, x_n]$ είναι τότε ένα γραμμικός συνδυασμός μονωνύμων με συντελεστές στο k

$$f = \sum_a b_a x^a, b_a \in k, a \in \mathbb{Z}^n_{\geq 0}$$

οπότε μπορεί να αναπαρασταθεί από ένα λεξικό με κλειδιά μονώνυμα και τιμές συντελεστές στο k.

```
data Polynomial a = Polynomial {
   getMonomials :: Map.Map Monomial a
 }
```

Για τα μονώνυμα χρησιμοποιείται μία διάταξη, δηλαδή μία σχέση $>$ στο σύνολο $\mathbb{Z}^n_{\geq 0}$ η οποία έχει τις εξής ιδιότητες:

1. $>$ είναι ολική διάταξη στο $\mathbb{Z}^n_{\geq 0}$, δηλαδή $a > b$ ή $a = b$ ή $b > a$.
2. $c \in \mathbb{Z}^n_{\geq 0} \wedge a > b \Rightarrow a + c > b + c$.
3. $>$ είναι καλή διάταξη, δηλαδή κάθε μη κενό υποσύνολο του $\mathbb{Z}^n_{\geq 0}$ έχει ελάχιστο στοιχείο ως προς την $>$.

Σε όλα τα παρακάτω θεωρείται πως υπάρχει μία σταθερή διάταξη $>$. Η πιο συνηθισμένη διάταξη είναι η λεξικογραφική, για την οποία αν $a, b \in \mathbb{Z}^n_{\geq 0}$, τότε $a > b$ αν η πρώτη μη μηδενική συντεταγμένη (από αριστερά) της διαφοράς $a - b \in \mathbb{Z}^n$ είναι θετική. Υλοποιείται άμεσα από τον ορισμό

```
-- zip two lists together up to the longest one by repeating the element a if the left one
 ends first or b if the right list ends second. Apply the function f to the zipped
 elements.
zipWithPadding :: a -> b -> (a -> b -> c) -> [a] -> [b] -> [c]
zipWithPadding a b f (x:xs) (y:ys) = f x y : zipWithPadding a b f xs ys
zipWithPadding a _ f []     ys     = zipWith f (repeat a) ys
zipWithPadding _ b f xs     []     = zipWith f xs (repeat b)

instance Ord (Monomial) where
 compare (Monomial l1) (Monomial l2) =
     case (dropWhile (==0) (zipWithPadding 0 0 (-) (l1) (l2))) of
         []                -> EQ
         (x:xs) | x > 0    -> GT
         (x:xs) | otherwise -> LT
```

Οι πράξεις των πολυωνύμων μπορούν να γίνουν με τις προφανείς απλές μεθόδους αν και υπάρχουν και αποδοτικότεροι μέθοδοι. Για την πρόσθεση απλά προστίθενται οι συντελεστές των μονωνύμων με τους ίδιους βαθμούς

```
addPoly :: (Num a, Eq a) => Polynomial a -> Polynomial a -> Polynomial a
addPoly (Polynomial p1) (Polynomial p2) = filterOutZeros $ Polynomial $
      Map.foldrWithKey f p1 p2
 where
     f :: (Num a, Eq a) => Monomial -> a -> Map.Map Monomial a -> Map.Map Monomial a
     f key coeff prevMap =
         if Map.member key prevMap
             then Map.update (\pval ->
                        if (coeff + pval /= 0)
                           then Just (coeff + pval)
                           else Nothing) key prevMap
             else Map.insert key coeff prevMap
```

Για τον πολλαπλασιασμό πολυωνύμων μπορούν να πολλαπλασιαστούν όλα τα μονώνυμα των δύο πολυωνύμων μεταξύ τους και στη συνέχεια να προστεθούν τα μονώνυμα με τους ίδιους βαθμούς.

```
multMonoms :: Monomial -> Monomial -> Monomial
multMonoms m1 m2 = Monomial (zipWithPadding 0 0 (+) (getDegrees m1) (getDegrees m2))

multiplyByMonom :: (Num a, Eq a) => Monomial -> Polynomial a -> Polynomial a
multiplyByMonom m = Polynomial . Map.mapKeys (multMonoms m) . getMonomials

zeroPolynomial :: (Num a) => Polynomial a
zeroPolynomial = Polynomial (Map.fromList [])

multiplyPolys :: (Num a, Eq a) => Polynomial a -> Polynomial a -> Polynomial a
multiplyPolys a (Polynomial b) = filterOutZeros $
   Map.foldrWithKey (\key coeff prevPoly -> addPoly (prevPoly) (Polynomial $ Map.map (\x
 -> x * coeff) ( getMonomials (multiplyByMonom key a)))) zeroPolynomial b
```

Η αφαίρεση πολυωνύμων πραγματοποιείται από πρόσθεση του αντίθετου πολυωνύμου που υπολογίζεται με τα αντίθετα των συντελεστών.

```
negatePoly :: (Num a, Eq a) => Polynomial a -> Polynomial a
negatePoly = Polynomial . Map.map negate . getMonomials
```

Υπάρχουν, λοιπόν, οι απαραίτητες συναρτήσεις για τον ορισμό των πολυωνύμων ως δακτυλίου (Num).

```
instance (Num a, Eq a) => Num (Polynomial a) where
 (+)           = addPoly
 (*)           = multiplyPolys
 fromInteger i = Polynomial $ Map.fromList [(Monomial [], fromInteger i)]
 negate        = negatePoly
```

```
instance (Num a, Eq a) => Eq (Polynomial a) where
 p1 == p2 = all (==0) (Map.elems $ getMonomials (p1 - p2))
```

Οι ρητές συναρτήσεις υλοποιούνται εύκολα ως ένα ζεύγος πολυωνύμων και ικανοποιούν τις ιδιότητες του δακτυλίου αλλά και του σώματος (Fractional).

```
data RationalFunction a = RF {
   getNumerator :: Polynomial a,
   getDenominator :: Polynomial a
 }

instance (Num a, Eq a) => Eq (RationalFunction a) where
   (RF n1 d1) == (RF n2 d2) = (n1 * d2 == n2 * d1)

instance (Num a, Eq a) => Num (RationalFunction a) where
   (RF n1 d1) + (RF n2 d2) = RF (n1 * d2 + n2 * d1) (d1 * d2)
   (RF n1 d1) * (RF n2 d2) = RF (n1 * n2) (d1 * d2)
   fromInteger i = RF (fromInteger i) (fromInteger 1)
   negate (RF n d) = RF (negate n) d

instance (Num a, Eq a) => Fractional   (RationalFunction a) where
   fromRational r = RF (fromInteger (numerator r)) (fromInteger (denominator r))
   (RF n1 d1) / (RF n2 d2) = RF (n1 * d2) (d1 * n2)
```

Α΄.2 Διαίρεση στον $k[x_1, \ldots, x_n]$

Η διαίρεση στον $k[x_1, \ldots, x_n]$ δεν ορίζεται όσο εύκολα όσο στον $k[x]$ αφού ο $k[x]$ είναι Ευκλείδια Περιοχή ενώ ο πολυωνυμικός δακτύλιος σε πάνω από μία μεταβλητές δεν είναι ούτε Περιοχή Κυρίων Ιδεωδών. Ωστόσο, υπάρχει μία διαδικασία διαίρεσης η οποία φέρει ομοιότητες με την περίπτωση της μίας μεταβλητής. Για το πολυώνυμο $f \in k[x_1, \ldots, x_n]$ σε σχέση με την $>$ ορίζονται ο μεγιστοβάθμιος συντελεστής του f ως $\mathrm{LC}(f)$, το μεγιστοβάθμιο μονώνυμο του f ως $\mathrm{LM}(f)$ και ο μεγιστοβάθμιος όρος του f ως $\mathrm{LT}(f) = \mathrm{LC}(f) \cdot \mathrm{LM}(f)$. Επιπλέον, ορίζεται ο μεγιστος βαθμός ως προς την διάταξη μονωνύμων του f ως $\mathrm{multideg}(f) = \max\{a \in \mathbb{Z}^n_{\geq 0} | b_a \neq 0\}$.
Είναι επιθυμητό να διαιρεθεί το $f \in k[x_1, \ldots, x_n]$ από τα $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, δηλαδή να γραφεί στη μορφή

$$f = q_1 f_1 + q_2 f_2 + \ldots + q_s f_s + r, \quad q_i, r \in k[x_1, \ldots, x_n]$$

Η διαίρεση στην περίπτωση της μίας μεταβλητής γίνεται με διαδοχική διαίρεση του LT του διαρετέου στο LT του διαιρέτη, ώστε τελικά το υπόλοιπο να έχει μικρότερο βαθμό από τον διαιρέτη. Αυτή η διαδικασία επεκτείνεται στις περισσότερες μεταβλητές επιτυγχάνοντας τον βαθμό multideg του υπολοίπου r να είναι μικρότερος από όλα τα πολυώνυμα που δρουν ως διαιρέτες.

Παράδειγμα 1.1. Έστω ότι είναι επιθυμητή η διαίρεση του $f = x^2y + xy^2 + y^2$ από τα $f_1 = xy - 1$ και $f_2 = y^2 - 1$. Ακολουθώντας την περίπτωση της μίας μεταβλητής, ο $\mathrm{LT}(f_1)$ διαιρεί τον $\mathrm{LT}(f)$ ενώ ο $\mathrm{LT}(f_2)$ όχι. Τότε $\frac{\mathrm{LT}(f)}{\mathrm{LT}(f_1)} = x$ οπότε το νέο

$$f' = f - xf_1 = x^2y + xy^2 + y^2 - x(xy - 1) = x^2y + xy^2 + y^2 - x^2y + x = xy^2 + x + y^2$$

Συνεχίζοντας την ίδια διαδικασία για το f', προκύπτει πως $\mathrm{LT}(f_1) \mid \mathrm{LT}(f')$ αλλά και $\mathrm{LT}(f_2) \mid \mathrm{LT}(f')$. Έστω ότι επιλέγεται το f_1 τότε $\frac{\mathrm{LT}(f')}{\mathrm{LT}(f_1)} = y$, οπότε το νέο

$$f'' = f' - yf_1 = x + y^2 + y$$

Τώρα, κανένας LT δεν διαιρεί τον $\mathrm{LT}(f'')$. Ωστόσο, ο $\mathrm{LT}(f_2)$ διαιρεί τον δεύτερο μεγαλύτερο όρο, άρα ο μεγιστοβάθμιος x απομακρύνεται και προστίθεται στο υπόλοιπο. Έτσι,

$$f''' = f'' - x = y^2 + y$$

Η διαδικασία συνεχίζεται αφού $\mathrm{LT}(f_2) \mid \mathrm{LT}(f''')$, οπότε

$$f'''' = f''' - \frac{\mathrm{LT}(f''')}{\mathrm{LT}(f_2)} f_2 = f''' - f_2 = y + 1$$

Ο $\mathrm{LT}(f'''')$ δεν διαιρείται από κανέναν LT οπότε προστίθεται στο υπόλοιπο.

$$f''''' = f'''' - y = 1$$

Ομοίως για το f''''', οπότε $f'''''' = 0$ και

$$f = (x + y)f_1 + f_2 + (x + y + 1)$$

		q_1 :	x	$+y$					
		q_2 :	1						r
xy	-1		x^2y	$+xy^2$	$+y^2$				
y^2	-1		$-x^2y$	$+x$					
				xy^2	$+x$	$+y^2$			
				$-xy^2$	$+y$				
					x	$+y^2$	$+y$		
						$+y^2$	$+y$	$\rightarrow$	x
						$-y^2$	$+1$		
							$+y$	$+1$	
								$+1$ $\rightarrow$	$x + y$
								0 $\rightarrow$	$x + y + 1$

Από την παραπάνω διαδικασία προκύπτει ο αλγόριθμος της διαίρεσης

Αλγοριθμος Α΄.1: *Ο αλγόριθμος διαίρεσης στον* $k[x_1, \ldots, x_n]$

Input $f_1, \ldots, f_s, f \in k[x_1, \ldots, x_n]$
Output $q_1, \ldots, q_s, r \in k[x_1, \ldots, x_n]$

$q_1 \leftarrow 0; \ldots; q_s \leftarrow 0; r \leftarrow 0$
$p \leftarrow f$
while $p \neq 0$ **do**
  $i \leftarrow 1$
  divisionOccured $\leftarrow$ false
  while $i \leq s$ **and** divisionOccured = false **do**
    if $\mathrm{LT}(f_i) \mid \mathrm{LT}(p)$ **then**
      $q_i \leftarrow q_i + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}$
      $p \leftarrow p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i$
      divisionOccured $\leftarrow$ true
    else
      $i \leftarrow i + 1$
    end if
  end while
  if divisionOccured = false **then**
    $r \leftarrow r + \mathrm{LT}(p)$
    $p \leftarrow p - \mathrm{LT}(p)$
  end if
end while

Είναι εμφανές πως ο multideg του πολυωνύμου p σε κάθε βήμα μειώνεται. Αφού η $>$ είναι καλή διάταξη ο αλγόριθμος θα τερματίσει.

Η εφαρμογή του αλγορίθμου της διαίρεσης δίνει έναν τρόπο έκφρασης του πολυωνύμου f στη μορφή

$$f = q_1 f_1 + q_2 f_2 + \ldots + q_s f_s + r \tag{Α΄.1}$$

με κάθε όρο του r να μην διαιρείται από κανέναν από τους $\mathrm{LT}(f_i), 1 \leq i \leq s$. Το υπόλοιπο της διαίρεσης του f από τα πολυώνυμα $S = \{f_1, \ldots, f_s\}$ συμβολίζεται ως $\overline{f}^S$
Η υλοποίηση του αλγορίθμου Α΄.1

```
-- Get the Leading Term of a polynomial
getLT :: (Num a, Eq a) => Polynomial a -> (Monomial, a)
getLT (Polynomial p) | Map.null p = (Monomial [], 0)
getLT (Polynomial p) | otherwise   = (head . Map.toDescList) p

-- Get the Leading Monomial of a Polynomial
getLM :: (Num a, Eq a) => Polynomial a -> Monomial
getLM = fst . getLT

-- check division of leading terms
ltDivideslt :: (Num a, Eq a) => Polynomial a -> Polynomial a -> Bool
ltDivideslt p1 p2 = all (>=0) $ zipWithPadding 0 0 (-) (f p2) (f p1)
   where f = getDegrees . fst . getLT
```

```
   -- Perform monomial division (subtraction of degrees)
   monomialQuotient :: Monomial -> Monomial -> Maybe Monomial
   monomialQuotient m1 m2 =
      case (all (>=0) res) of
         True -> Just $ Monomial res
         _    -> Nothing
      where res = zipWithPadding 0 0 (-) (getDegrees m1) (getDegrees m2)

   -- Divide leading terms if possible
   ltQuotient :: (Fractional a, Eq a) => Polynomial a -> Polynomial a -> Maybe (Polynomial a)
   ltQuotient p1 p2 = do
      let (lm1, lc1) = getLT p1
      let (lm2, lc2) = getLT p2
      lm <- lm1 `monomialQuotient` lm2
      let lc = lc1 / lc2
      return $ Polynomial $ Map.fromList [(lm, lc)]
   -- Divide leading terms if possible and return quotient and remainder
   ltQuotientRem :: (Fractional a, Eq a) => Polynomial a -> Polynomial a -> Maybe (Polynomial
    a, Polynomial a)
   ltQuotientRem p1 p2 = do
      quotient <- p1 `ltQuotient` p2
      return (quotient, p1 - quotient * p2)

   -- Apply leading term division by a list of polynomials where possible and return the
    results
   oneStepDiv' :: (Fractional a, Eq a) => Polynomial a -> [Polynomial a] -> [Maybe
    (Polynomial a)]
   oneStepDiv' f ps = map (ltQuotient f) ps

   -- Returns the list of quotients while performing division by only the fst element in
   -- the list that can divide f and returns 0 elsewhere for the quotients. The third element
    of the returned tuple is the remainder
   -- The boolean indicates if at least one division was done
   oneStepDiv :: (Fractional a, Eq a) => Polynomial a -> [Polynomial a] -> (Bool, [Polynomial
    a], Polynomial a)
   oneStepDiv f ps = (not $ all isNothing filtered, quotients, f - sum (zipWith (*) ps
    quotients))
    where
        filtered = getOnlyFstJust (oneStepDiv' f ps)
        quotients = map (filterOutZeros . maybe 0 id) $ getOnlyFstJust (oneStepDiv' f ps)


-- From a list get all of the list up to and including the fst element of
-- the list which satisfies the predicate
splitAtFirst :: (a -> Bool) -> [a] -> [a]
splitAtFirst pred = uncurry (flip (++) . take 1) . swap . break pred

getOnlyFstJust :: [Maybe a] -> [Maybe a]
```

```
getOnlyFstJust a = zipWithPadding Nothing Nothing (<|>) (splitAtFirst isJust a) (map (\_ ->
    Nothing) a)

-- Apply the onestep division by adding the leading terms to the remainder whenever it is not
    possible. Finish when there is nothing left to divide
division :: (Fractional a, Eq a) => Polynomial a -> [Polynomial a] -> ([Polynomial a],
    Polynomial a)
division f ps =
    if filterOutZeros f == zeroPolynomial then (map (\_ -> zeroPolynomial) ps, zeroPolynomial)
    else case oneStepDiv f ps of
        (False, _ , _) -> fmap (+ltp) (division (filterOutZeros (f - ltp)) ps)
        (True,  qs, r) -> (swap . fmap (zipWith (+) qs) . swap) (division (filterOutZeros r)
    ps)
    where
        ltp = (Polynomial . Map.fromList) [getLT f]
```

Εκτελώντας την διαίρεση του παραδείγματος 1.1 με την σειρά των f_1, f_2 ανεστραμμένη προκύπτει το αποτέλεσμα

$$f = (x + y)(y^2 - 1) + x(xy - 1) + (2x + 1)$$

δηλαδή διαφορετικό r. Το υπόλοιπο του αλγορίθμου Α΄.1 σε αντίθεση με την περίπτωση της μίας μεταβλητής δεν είναι μοναδικό. Ωστόσο, αν $r = 0$ ισχύει πως $f \in \langle f_1, \ldots, f_s \rangle$, όμως αν $f \in \langle f_1, \ldots, f_s \rangle$ μπορεί να ισχύει $r \neq 0$.

Α΄.3 Gröbner Bases

Για να μπορεί να ελεγχτεί αν ένα πολυώνυμο ανήκει σε ένα ιδεώδες $I \triangleleft k[x_1, \ldots, x_n]$ είναι επιθυμητό το υπόλοιπο της διαίρεσης του αλγορίθμου Α΄.1 να είναι μοναδικό. Η εφαρμογή της διαίρεσης από ένα τυχαίο σύνολο γεννητόρων του I δεν είναι βέβαιο πως θα οδηγήσει σε μοναδικό υπόλοιπο. Ωστόσο, υπάρχουν κατάλληλα σύνολα γεννητόρων για κάθε ιδεώδες διαιρώντας με τα οποία δίνει πάντα μοναδικό υπόλοιπο. Τα σύνολα αυτά ονομάζονται Gröbner Bases.

Για ένα ιδεώδες $I \triangleleft k[x_1, \ldots, x_n]$ με $I \neq \{0\}$ ορίζονται τα σύνολα

1. $\mathrm{LT}(I) = \{\mathrm{LT}(f) : f \in I \setminus \{0\}\}$

2. $\langle \mathrm{LT}(I) \rangle$ το ιδεώδες που παράγεται από τα μονώνυμα του $\mathrm{LT}(I)$.

Από το Θεώρημα Βάσης του Hilbert κάθε ιδεώδες του $k[x_1, \ldots, x_n]$ είναι πεπερασμένα παραγόμενο οπότε υπάρχουν πολυώνυμα $f_1, \ldots, f_s \in I$ τέτοια ώστε $I = \langle f_1, \ldots, f_s \rangle$. Τότε, ισχύει πως $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle \subseteq \langle \mathrm{LT}(I) \rangle$, αφού το $\langle \mathrm{LT}(I) \rangle$ σίγουρα περιλαμβάνει τα $\mathrm{LT}(f_i)$. Το αντίστροφο δεν ισχύει στην γενική περίπτωση. Όταν αυτό ισχύει, τότε το σύνολο γεννητόρων λέγεται **Gröbner Basis** για το I. Οι βάσεις Gröbner έχουν την επιθυμητή ιδιότητα σχετικά με την μοναδικότητα του υπολοίπου. Συγκεκριμένα, ισχύει το ακόλουθο

Θεώρημα 1.1. *Έστω $I \triangleleft k[x_1, \ldots, x_n]$ ένα ιδεώδες με $I \neq \{0\}$ και $G = \{f_1, \ldots, f_s\}$ μία βάση Gröbner του I. Τότε υπάρχει μοναδικό $r \in k[x_1, \ldots, x_n]$ τέτοιο ώστε κανένας όρος του r να μην διαιρείται από κανέναν από τους $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$, $g \in I$ τέτοιο ώστε $f = g + r$ και r είναι το υπόλοιπο της διαίρεσης του f από την G ανεξαρτήτως σειράς των πολυωνύμων της G.*

Απόδειξη. Από την Α΄.1 η f γράφεται στην επιθυμητή μορφή

$$f = q_1 f_1 + q_2 f_2 + \ldots + q_s f_s + r$$

με κάθε όρο του r να μην διαιρείται από κανέναν από τους $\mathrm{LT}(f_i)$, $1 \leq i \leq s$ και

$$g = q_1 f_1 + q_2 f_2 + \ldots + q_s f_s \in I$$

Για την μοναδικότητα του υπολοίπου r, έστω πως $f = g' + r'$ με κάθε όρο του r' να μην διαιρείται από κανέναν από τους $\mathrm{LT}(f_i)$, $1 \leq i \leq s$ και $g' \in I$. Τότε

$$r - r' = g' - g \in I$$

οπότε αν $r \neq r' \Rightarrow \mathrm{LT}(r - r') \in < \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) >$. Ο $\mathrm{LT}(r)$ διαιρείται τότε από κάποιο $\mathrm{LT}(f_i)$, το οποίο δεν ισχύει. Άρα $r - r' = 0 \Rightarrow r = r'$. □

Οι βάσεις Gröbner δίνουν έναν αλγόριθμο για τον έλεγχο σχετικά με το αν ένα πολυώνυμο ανήκει στο ιδεώδες I αφού από το παραπάνω θεώρημα προκύπτει άμεσα πως αν G μία βάση Gröbner του I τότε

$$f \in I \iff r = 0$$

αφού αν $r = 0 \Rightarrow f = g \in I$ και αν $f \in I \Rightarrow f = f + 0$, οπότε λόγω μοναδικότητας $r = 0$. Δημιουργείται, ωστόσο, η ανάγκη υπολογισμού μίας βάσης Gröbner από ένα σύνολο γεννητόρων του I.

Α΄.4 Ο αλγόριθμος του Buchberger

Ο αλγόριθμος του Buchberger είναι ένας αλγόριθμος για τον υπολογισμό μίας βάσης Gröbner από ένα σύνολο γεννητόρων ενός μη μηδενικού ιδεώδους $I \triangleleft k[x_1, \ldots, x_n]$. Για την επίτευξη αυτού του σκοπού ορίζεται το S-πολυώνυμο των $f, g \in k[x_1, \ldots, x_n]$ ως

$$S(f, g) = \frac{\mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LT}(f)} f - \frac{\mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LT}(g)} g$$

όπου το $\mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))$ υπολογίζεται ως x^γ όπου $\gamma = (\gamma_1, \ldots, \gamma_n)$, $\gamma_i = \max\{a_i, b_i\}$, $a = \mathrm{multideg}(f)$, $b = \mathrm{multideg}(g)$.

Παράδειγμα 1.2. Έστω $f = x^3y^2 - x^2y^3 + x, g = 3x^4y + y^2 \in \mathbb{R}[x, y]$. Τότε $\gamma = (4, 2)$ και

$$S(f, g) = \frac{x^4y^2}{x^3y^2} f - \frac{x^4y^2}{3x^4y} g = -x^3y^3 + x^2 - \frac{1}{3}y^3$$

```
monomialLCM :: Monomial -> Monomial -> Monomial
monomialLCM (Monomial m1) (Monomial m2) = Monomial $ zipWithPadding 0 0 max m1 m2

ltLCM :: (Num a, Eq a) => Polynomial a -> Polynomial a -> Polynomial a
ltLCM f g = Polynomial $ Map.fromList [(monomialLCM (getLM f) (getLM g), 1)]

sigmaPolynomial :: (Fractional a, Eq a) => Polynomial a -> Polynomial a -> Polynomial a
sigmaPolynomial f g =
     (fromJust (lcmp `ltQuotient` f)) * f - (fromJust (lcmp `ltQuotient` g)) * g
   where
      lcmp = ltLCM f g
```

Θεώρημα 1.2 (Κριτήριο του Buchberger)**.** *Έστω $I \triangleleft k[x_1,\dots,x_n]$ ένα μη μηδενικό ιδεώδες και $G = \{f_1,\dots,f_s\}$ ένα σύνολο γεννητόρων του I. Τότε G είναι βάση Gröbner του I αν και μόνο αν για κάθε $i \neq j$ ισχύει $\overline{S(f_i,f_j)}^{G} = 0$ (με κάποια διάταξη).*

Το κριτήριο του Buchberger δίνει έναν τρόπο υπολογισμού μίας βάσης Gröbner ενός ιδεώδους I από ένα σύνολο γεννητόρων του F. Μπορούν να υπολογιστούν τα S-πολυώνυμα για ζεύγη πολυωνύμων από το F και αν αυτά δεν δίνουν μηδενικό υπόλοιπο μετά από διαίρεση με το F τότε να προστεθούν τότε να προστεθούν τα υπόλοιπα στο σύνολο. Αν η διαδικασία επαναληφθεί, τα υπόλοιπα των S-πολυωνύμων που προστέθηκαν θα είναι μηδέν μετά από διαίρεση με το νέο σύνολο F'. Αυτή η διαδικασία θα τερματίσει αφού τα ιδεώδη $\langle \mathrm{LT}(F')\rangle$ θα είναι μία αύξουσα ακολουθία ιδεωδών του $k[x_1,\dots,x_n]$ που τελικά θα πρέπει να σταθεροποιείται (Θεώρημα Βάσης Hilbert).

Αλγοριθμος Α΄.2: *Ο αλγόριθμος του Buchberger*

Input $F = \langle f_1,\dots,f_s\rangle$
Output $G = \langle g_1,\dots,g_t\rangle$ βάση Gröbner του I με $F \subseteq G$

```
G ← F
while G ≠ G' do
    G' ← G
    for (f, g) ∈ G', f ≠ g do
        r ← S(f, g)^G
        if r ≠ 0 then
            G ← G ∪ {r}
        end if
    end for
end while
return G
```

```
-- Multivariate Division but keep only the remainder
reduce :: (Fractional a, Eq a) => Polynomial a -> [Polynomial a] -> Polynomial a
reduce f ps = snd (division f ps)
-- Get remainders of sigma polynomials to add from pairs in ps
toAdd ps =
   filter (/=0) [reduce (sigmaPolynomial p q) ps | (p:ys) <- tails ps, q <- ys]
```

```
-- Buchberger's algorithm
grobnerBasis :: (Fractional a, Eq a) => [Polynomial a] -> [Polynomial a]
grobnerBasis fs =
   case toAdd fs of
      []     -> fs
      (r:rs) -> grobnerBasis ([r] ++ fs)
```

Για τον έλεγχο αν ένα πολυώνυμο $f \in k[x_1, \ldots, x_n]$ ανήκει στο μη μηδενικό ιδεώδες $I \triangleleft k[x_1, \ldots, x_n]$ αρκεί λοιπόν να υπολογιστεί μία βάση Gröbner για το I με τον αλγόριθμο Α΄.2 και στη συνέχεια να εξεταστεί αν το υπόλοιπο της διαίρεσης του f από τη βάση είναι 0 (από τον αλγόριθμο Α΄.1).

```
-- Check if f is in the ideal generated by ps
isInIdeal f ps =
 reduce f (grobnerBasis ps) == zeroPolynomial

-- Check if n1/d1 = n2/d2 modulo the ideal generated by ps
eqModIdeal (RF n1 d1) (RF n2 d2) i =
   ((reduce n1 i)*(reduce d2 i) - (reduce n2 i)*(reduce d1 i)) `isInIdeal` i
```

Α΄.5 Απόδειξη Της Προσεταιριστικότητας

Για την απόδειξη της προσεταιριστικότητας πρέπει να υλοποιηθεί η πράξη ομάδας της $E : y^2 = x^3 + Ax + B$ πάνω από οποιοδήποτε σώμα k. Η αναπαράσταση της καμπύλης και των σημείων:

```
-- defines the elliptic curve y^2 = x^3 + Ax + B, over a
data EC a = EC {
   getA :: a,
   getB :: a
   }
   deriving (Eq)
-- defines a projective point on an elliptic curve
data ECPoint a = ECPoint {
   getEC :: EC a,
   getX  :: a,
   getY  :: a,
   getZ  :: a
   }
```

Η ισότητα προβολικών σημείων:

```
instance (Fractional a, Eq a) => Eq (ECPoint a) where
     -- same equivalence class as projective coordinates
     (ECPoint ec x1 y1 z1)  == (ECPoint ec' x2 y2 z2) =
      case (x1, x2, y1, y2, z1, z2) of
```

```
            (0, _, 0, _, 0, _)       -> error "(0 : 0 : 0) is not  projective point"
            (_, 0, _, 0, _, 0)       -> error "(0 : 0 : 0) is not  projective point"
            (0, 0, y, z, 0, 0)       -> True
            (0, 0, 0, 0, z1, z2)     -> z1 == z2
            (0, 0, 0, y2, z1, z2)    -> False
            (0, 0, y1, 0, z1, z2)    -> False
            (x1, 0, _, _, _, _)      -> False
            (0, x2, _, _, _, _)      -> False
            (x1, x2, y1, y2, z1, z2) -> y1 / x1 == y2 / x2 &&  z1/x1 == z2/x2

  makeAffine :: (Fractional a, Eq a) => ECPoint a -> ECPoint a
  makeAffine (ECPoint ec x y z) = if z /= 0 then ECPoint ec x y z else ECPoint ec (x/z)
(y/z) 1

  -- constructs the point O on an elliptic curve given as input
  o :: Fractional a => EC a -> ECPoint a
  o ec = ECPoint ec 0 1 0
```

Η πρόσθεση σημείων:

```
-- one of them is the identity element O
p@(ECPoint ec x1 y1 z1) <+> q@(ECPoint ec' x2 y2 z2) | p == o ec = q
p@(ECPoint ec x1 y1 z1) <+> q@(ECPoint ec' x2 y2 z2) | q == o ec = p
p@(ECPoint ec x1 y1 z1) <+> q@(ECPoint ec' x2 y2 z2) | ec /= ec' = error "Adding Points
 from Different Curves"
p@(ECPoint ec x1 y1 z1) <+> q@(ECPoint ec' x2 y2 z2) | x1 == x2 && y1 /= y2 = (o ec)
-- The general case no overhead if given in affine form
p@(ECPoint ec x1 y1 z1) <+> q@(ECPoint ec' x2 y2 z2) | x1/z1 == x2/z2 && y1/z1 == y2/z2 =
    let
            p'@(ECPoint _ x1' y1' _) = makeAffine p
            q'@(ECPoint _ x2' y2' _) = makeAffine q
            m = (3*x1'^2+ (getA ec)) / (2 * y1')
            x3 = m^2 - 2 * x1'
            y3 = m * (x1' - x3) - y1'
    in
            (ECPoint ec x3 y3 1)

p@(ECPoint ec x1 y1 z1) <+> q@(ECPoint ec' x2 y2 z2) | x1/z1 == x2/z2 && y1/z1 /= y2/z2 =
            (o ec)
-- The doubling case
p@(ECPoint ec x1 y1 z1) <+> q@(ECPoint ec' x2 y2 z2) =
    let
            p'@(ECPoint _ x1' y1' _) = makeAffine p
            q'@(ECPoint _ x2' y2' _) = makeAffine q
            m = (y2'-y1') / (x2' - x1')
            x3 = m^2 -  x1' - x2'
            y3 = m * (x1'-x3) - y1'
    in
            (ECPoint ec x3 y3 1)
```

```
invertElem :: (Fractional a, Eq a) => ECPoint a -> ECPoint a
invertElem p@(ECPoint ec x1 y1 z1) | p == o ec = p
invertElem p@(ECPoint ec x1 y1 z1) | otherwise = ECPoint ec x (-y) 1
     where
             (ECPoint _ x y _) = makeAffine p
```

οπότε η πρόσθεση των σημείων πληροί της προϋποθέσεις μίας ομάδας, εφόσον τα σημεία της καμπύλης θεωρούνται πάνω από σώμα.

```
instance (Fractional a, Eq a) => Semigroup (ECPoint a) where
     p <> q = p <+> q

instance (Fractional a, Eq a) => Monoid (ECPoint a) where
     mempty = o'

instance (Fractional a, Eq a) => Group (ECPoint a) where
     invert = invertElem
```

Για την απόδειξη της προσεταιριστικότητας, λοιπόν, αρκεί να εξεταστούν οι περιπτώσεις που αναφέρθηκαν με σημεία τις ρητές συναρτήσεις.

```
-- to construct the variables
xivar i = Polynomial $ Map.fromList [(Monomial (take (i-1) (repeat 0) ++ [1]), 1)]
(px:py:qx:qy:rx:ry:a:b:_) = map (\i -> xivar i) [1..10] :: [Polynomial Rational]
idealI = [py^2-px^3-a*px-b, qy^2-qx^3-a*qx-b, ry^2-rx^3-a*rx-b]
ec = EC (RF a 1) (RF b 1)
p = ECPoint ec (RF px 1) (RF py 1) 1
q = ECPoint ec (RF qx 1) (RF qy 1) 1
r = ECPoint ec (RF rx 1) (RF ry 1) 1
s = invert p
-- Check whether the points are equal modulo the idealI
equal p1 p2 = eqModIdeal (getX p1) (getX p2) idealI && eqModIdeal (getY p1) (getY p2)
 idealI

cases = [
 ((p <> p) <> q, p <> (p <> q)),
 ((p <> q) <> p, p <> (q <> p)),
 ((q <> p) <> p, q <> (p <> p)),
 ((p <> s) <> q, p <> (s <> q)),
 ((p <> q) <> s, p <> (q <> s)),
 ((q <> p) <> s, q <> (p <> s)),
 ((p <> p) <> p, p <> (p <> p)),
 ((p <> q) <> r, p <> (q <> r))
 ]

isAssociative = all (==True) $ map (\(l, r) -> equal l r) cases
```

Η εκτέλεση της συνάρτησης isAssociative δίνει έξοδο True.

Βιβλιογραφία

[1] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer Science+Business Media, LLC, 2η έκδοση, 2009.

[2] Carl Pomerance E.R. Canfield, Paul Erdös. *On a problem of Oppenheim concerning "factorisatio numerorum"*, 1983.

[3] John T. Tate Joseph H. Silverman. *Rational Points on Elliptic Curves*. Springer International Publishing Switzerland, 2η έκδοση, 2015.

[4] Anthony W. Knapp. *Elliptic Curves*. Princeton University Press, 1992.

[5] Lawrence C. Washington. *Ellptic Curves : Number Theory And Cryptography*. Taylor & Francis Group, LLC, 2008.

[6] Vanstone Darrel Hankerson, Alfred Menezes. *Guide to Elliptic Curve Cryptography*. Springer-Verlag New York, Inc, 2004.

[7] Johannes A. Buchmann. *Introduction to Cryptography*. Springer New York, 2001.

[8] Yehuda Lindell Jonathan Katz. *Introduction to Modern Cryptography 2nd Edition*. 2015.

[9] Douglas R. Stinson. *Cryptography: Theory and Practice*. Chapman & Hall/CRC, 2006.

[10] Donal O'Shea David A. Cox, John Little. *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer International Publishing Switzerland, 2015.

[11] John B. Fraleigh. *A First Course in Abstract Algebra, 7th Edition*. 2002.

[12] Tanja Lange Daniel J. Bernstein. *Faster Addition and Doubling On Elliptic Curves*. 2007.

[13] Jerome A. Solinas. *An Improved Algorithm for Arithmetic on a Family of Elliptic Curves*. 1997.

[14] René Schoof. *Ellitptic Curves Over Finite Fields and the Computation of Square Roots mod p*. 1985.

[15] Andrew Sutherland. *Elliptic Curves*. *https://math.mit.edu/classes/18.783/*.

[16] J.M. Pollard. *Monte Carlo Methods for Index Computation mod p*. 1978.

[17] Jr. H. W. Lenstra. *Factoring Integers With Elliptic Curves*. 1987.

[18] Neal Koblitz. *Elliptic Curve Cryptosystems*. 1987.

[19] *Secp256k1, https://en.bitcoin.it/wiki/Secp256k1*.

[20] Mike Burmester, Στέφανος Γκρίτζαλης, Σωκράτης Κάτσικας, Βασίλης Χρυσικόπουλος. *Σύγχρονη Κρυπτογραφία: Θεωρία και Εφαρμογές*. Παπασωτηρίου, 2011.

[21] Ευστάθιος Ζάχος, Αριστείδης Παγουρτζής, Παναγιώτης Γροντάς. *Υπολογιστική Κρυπτογραφία*. Kallipos, 2015.

[22] Γιάννης Αντωνιάδης, Αριστείδης Κοντογεώργης. *Θεωρία Αριθμών και εφαρμογές*. Kallipos, 2015.

[23] Γιάννης Αντωνιάδης, Αριστείδης Κοντογεώργης. *Πεπερασμένα Σώματα & Κρυπτογραφία*. Kallipos, 2015.