ΠΥΘΑΓΟΡΕΙΕΣ ΤΡΙΑΔΕΣ, ΤΡΙΓΩΝΟΜΕΤΡΙΑ ΚΑΙ ΥΠΟΛΟΓΙΣΜΟΣ ΟΛΟΚΛΗΡΩΜΑΤΩΝ.

Αριστείδης Κοντογεώργης -Τμήμα Μαθηματικών ΕΚΠΑ

Πρότυπο Λύκειο Ευαγγελικής Σχολής Σμύρνης 21 Οκτωβρίου 2015

ΤΟ ΤΕΛΕΥΤΑΙΟ ΘΕΩΡΗΜΑ ΤΟΥ FERMAT

$$X^n + Y^n = Z^n$$

για $n \geq 3$ δεν έχει λύσεις παρά μόνο τις τετριμμένες, $XYZ = 0$.

ΔΙΟΦΑΝΤΙΚΕΣ ΕΞΙΣΩΣΕΙΣ

Αναζητούμε λύσεις (X, Y, Z) της διοφαντικής εξίσωσης

$$aX + bY + cZ = 0,$$

ή γενικότερα της εξίσωσης

$$F(X, Y, Z) = 0,$$

όπου $F(X, Y, Z) \in \mathbb{Z}[X, Y, Z]$ είναι ένα ***ομογενές πολυώνυμο***, δηλαδή

$$F(\lambda X, \lambda Y, \lambda Z) = \lambda^d \cdot F(X, Y, Z).$$

Παρατήρηση: Ομογενές πολυώνυμο σημαίνει ότι μπορούμε να διαιρέσουμε με Z, θέτοντας

$$x = X/Z, y = Y/Z,$$

και αντί να αναζητήσουμε ακέραιες λύσεις της

$$F(X, Y, Z) = 0$$

να αναζητήσουμε ρητές λύσεις της

$$f(x, y) = F(x, y, 1) = 0.$$

ΤΕΤΡΑΓΩΝΙΚΕΣ ΕΞΙΣΩΣΕΙΣ

Η γραμμική εξίσωση $\boldsymbol{aX} + \boldsymbol{bY} + \boldsymbol{cZ} = 0$ ή ισοδύναμα η $\boldsymbol{ax} + \boldsymbol{by} + \boldsymbol{c} = 0$ είναι εύκολο να λυθεί.

ΤΕΤΡΑΓΩΝΙΚΕΣ ΕΞΙΣΩΣΕΙΣ

Η γραμμική εξίσωση $aX + bY + cZ = 0$ ή ισοδύναμα η $ax + by + c = 0$ είναι εύκολο να λυθεί.

Θα δόσουμε μια μέθοδο επίλυσης της γενικής τετραγωνικής εξίσωσης, η οποία για απλότητα θα δοθεί στην εξίσωση του κύκλου:

Να βρεθούν οι ρητοί αριθμοί που ικανοποιούν την

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

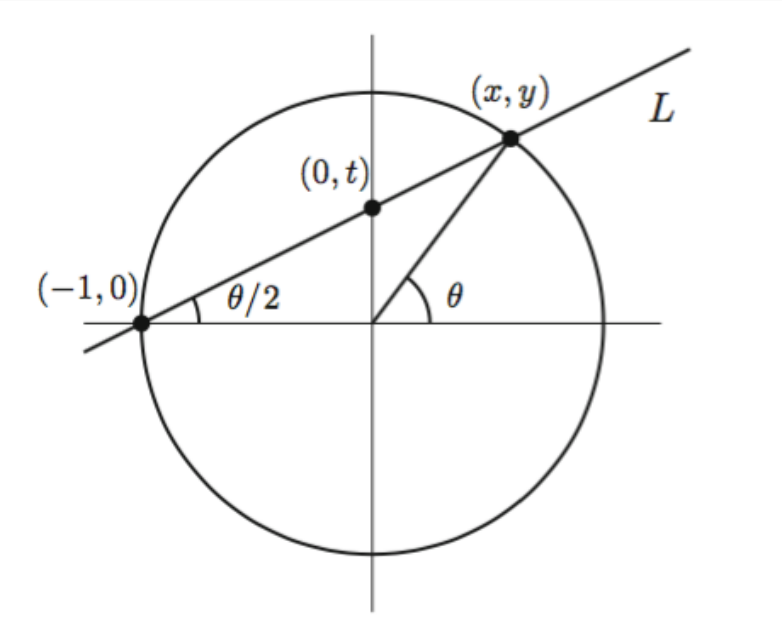
ΤΕΤΡΑΓΩΝΙΚΕΣ ΕΞΙΣΩΣΕΙΣ

Η γραμμική εξίσωση $aX + bY + cZ = 0$ ή ισοδύναμα η $ax + by + c = 0$ είναι εύκολο να λυθεί.

Θα δόσουμε μια μέθοδο επίλυσης της γενικής τετραγωνικής εξίσωσης, η οποία για απλότητα θα δοθεί στην εξίσωση του κύκλου:

Να βρεθούν οι ρητοί αριθμοί που ικανοποιούν την

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



Θεωρούμε μια λύση της τετραγωνικής εξίσωσης $(x, y) = (-1, 0)$ και την ευθεία $y = t(1 + x)$, η οποία περνά από το σημείο $(-1, 0)$. Αυτή η εξίσωση τέμνει τον κύκλο σε άλλο ένα σημείο το οποίο το υπολογίζουμε:

$$1 - x^2 = y^2 = t^2(1 + x)^2.$$

Καταλήγουμε στην εξίσωση $1 - x = t^2(1 + x)$ και με αντικατάσταση υπολογίζουμε

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

Καταλήγουμε στην εξίσωση $1 - x = t^2(1 + x)$ και με αντικατάσταση υπολογίζουμε

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

Παρατηρούμε ότι κάθε τιμή του $t \in \mathbb{Q}$ δίνει μια ρητή λύση του κύκλου και αντιστρόφως κάθε σημείο του κύκλου με ρητές συντεταγμένες οδηγεί σε μια ρητή τιμή του t. Το σημείο $(-1, 0)$ το παίρνουμε για $t = \infty$.

Ας θεωρήσουμε την τιμή $t = m/n$. Με αντικατάσταση υπολογίζουμε

$$\frac{X}{Z} = x = \frac{n^2 - m^2}{n^2 + m^2}, \frac{Y}{Z} = y = \frac{2mn}{n^2 + m^2},$$

και καταλήγουμε στις λύσεις

$$X = n^2 - m^2, Y = 2mn, Z = n^2 + m^2.$$

Σχήμα 1: Βαβυλωνιακή επιγραφή με Πυθαγόρειες Τριάδες γνωστή ως Plimpton 322

ΓΕΝΙΚΗ ΤΕΤΡΑΓΩΝΙΚΗ ΕΞΙΣΩΣΗ

Η παραπάνω μέθοδος μπορεί να χρησιμοποιηθεί για την επίλυση οποιασδήποτε διοφαντικής εξίσωσης που δίνεται από ομογενές πολυώνυμο δευτέρου βαθμού.

ΓΕΝΙΚΗ ΤΕΤΡΑΓΩΝΙΚΗ ΕΞΙΣΩΣΗ

Η παραπάνω μέθοδος μπορεί να χρησιμοποιηθεί για την επίλυση οποιασδήποτε διοφαντικής εξίσωσης που δίνεται από ομογενές πολυώνυμο δευτέρου βαθμού.

Μπορούμε να αποδείξουμε ότι αν η τετραγωνική εξίσωση έχει μια (μη μηδενική) λύση στο $\mathbb{Q}$ τότε έχει τόσες λύσεις όσες και οι ρητές κλίσεις ευθειών.

ΓΕΝΙΚΗ ΤΕΤΡΑΓΩΝΙΚΗ ΕΞΙΣΩΣΗ

Η παραπάνω μέθοδος μπορεί να χρησιμοποιηθεί για την επίλυση οποιασδήποτε διοφαντικής εξίσωσης που δίνεται από ομογενές πολυώνυμο δευτέρου βαθμού.

Μπορούμε να αποδείξουμε ότι αν η τετραγωνική εξίσωση έχει μια (μη μηδενική) λύση στο $\mathbb{Q}$ τότε έχει τόσες λύσεις όσες και οι ρητές κλίσεις ευθειών.

Υπάρχει όμως μία λύση; Πως θα αποφασίσουμε για αυτό;

ΓΕΝΙΚΗ ΤΕΤΡΑΓΩΝΙΚΗ ΕΞΙΣΩΣΗ

Η παραπάνω μέθοδος μπορεί να χρησιμοποιηθεί για την επίλυση οποιασδήποτε διοφαντικής εξίσωσης που δίνεται από ομογενές πολυώνυμο δευτέρου βαθμού.

Μπορούμε να αποδείξουμε ότι αν η τετραγωνική εξίσωση έχει μια (μη μηδενική) λύση στο $\mathbb{Q}$ τότε έχει τόσες λύσεις όσες και οι ρητές κλίσεις ευθειών.

Υπάρχει όμως μία λύση; Πως θα αποφασίσουμε για αυτό;

Είναι σαφές ότι η εξίσωση

$$X^2 + Y^2 + Z^2 = 0,$$

δεν μπορεί να έχει άλλη λύση εκτός από την μηδενική.

Τι γίνεται με την

$$X^2 + Y^2 = 3Z^2$$

Χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι τα $X, Y, Z \in \mathbb{Z}$ δεν έχουν κοινό διαιρέτη. Επιπλέον ούτε το X ούτε το Y είναι διαιρετά με 3. Άρα

$$X \equiv \pm 1 \mod 3, Y \equiv \pm 1 \mod 3,$$

συνεπώς

$$X^2 + Y^2 \equiv 1 + 1 \equiv 2 \mod 3$$

το οποίο δείχνει ότι η αρχική εξίσωση δεν έχει λύση.

Η αρχη του τοπικου-γενικου (local global principle)

Για να δούμε ότι μια διοφαντική εξίσωση δεν έχει λύση στους ρητούς αρκεί να δείξουμε ότι δεν έχει λύση $\mod p^{\ell}$ για κάποια δύναμη πρώτου αριθμού ή ότι δεν έχει λύση στους πραγματικούς αριθμούς.

Η αρχη του τοπικου-γενικου (local global principle)

Για να δούμε ότι μια διοφαντική εξίσωση δεν έχει λύση στους ρητούς αρκεί να δείξουμε ότι δεν έχει λύση $\mod p^\ell$ για κάποια δύναμη πρώτου αριθμού ή ότι δεν έχει λύση στους πραγματικούς αριθμούς.

Τι συμβαίνει όμως αν μπορούμε να δείξουμε ότι μια διοφαντική εξίσωση έχει λύση modulo κάθε πρώτη δύναμη και στο $\mathbb{R}$;

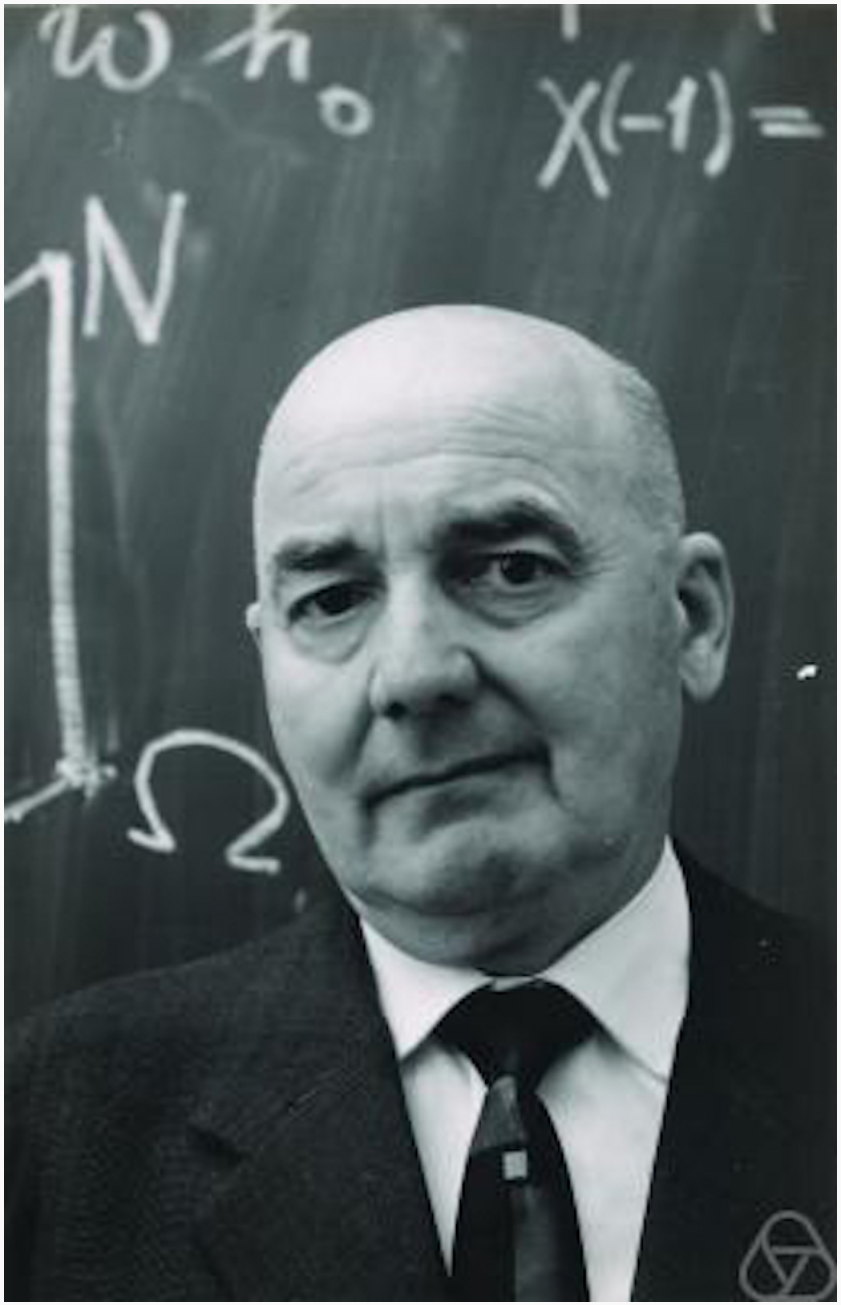
Η αρχη του τοπικου-γενικου (local global principle)

Για να δούμε ότι μια διοφαντική εξίσωση δεν έχει λύση στους ρητούς αρκεί να δείξουμε ότι δεν έχει λύση $\mod p^{\ell}$ για κάποια δύναμη πρώτου αριθμού ή ότι δεν έχει λύση στους πραγματικούς αριθμούς.

Τι συμβαίνει όμως αν μπορούμε να δείξουμε ότι μια διοφαντική εξίσωση έχει λύση modulo κάθε πρώτη δύναμη και στο $\mathbb{R}$;

Αν είναι μια τετραγωνική εξίσωση όπως η παραπάνω, τότε θα έχει λύση και στους ρητούς. Αυτό είναι το περίφημο local-global principle του Hasse.

H. HASSE



Το σώμα των ρητών αριθμών είναι εφοδιασμένο με την απόλυτη τιμή η οποία αποτελεί μια μετρική. Το $\mathbb{Q}$ δεν είναι πλήρες ως προς την μετρική αυτή. Η πλήρωση του $\mathbb{Q}$ ως προς την απόλυτη τιμή δίνει το σώμα των πραγματικών αριθμών.

Το σώμα των ρητών αριθμών είναι εφοδιασμένο με την απόλυτη τιμή η οποία αποτελεί μια μετρική. Το $\mathbb{Q}$ δεν είναι πλήρες ως προς την μετρική αυτή. Η πλήρωση του $\mathbb{Q}$ ως προς την απόλυτη τιμή δίνει το σώμα των πραγματικών αριθμών.

Το σώμα $\mathbb{Q}$ δέχεται και άλλες μετρικές τις λεγόμενες p-αδικές οι οποίες ορίζονται ως εξής:

$$\mathbb{Q} \ni x = a/b, (a, b) = 1.$$

Σύμφωνα με το θεμελιώδες θεώρημα της αριθμητικής $a = p^{\ell} \cdot u_a$, $(u_a, p) = 1$ και $b = p^{\ell'} u_b$, $(u_b, p) = 1$.

Το σώμα των ρητών αριθμών είναι εφοδιασμένο με την απόλυτη τιμή η οποία αποτελεί μια μετρική. Το $\mathbb{Q}$ δεν είναι πλήρες ως προς την μετρική αυτή. Η πλήρωση του $\mathbb{Q}$ ως προς την απόλυτη τιμή δίνει το σώμα των πραγματικών αριθμών.

Το σώμα $\mathbb{Q}$ δέχεται και άλλες μετρικές τις λεγόμενες p-αδικές οι οποίες ορίζονται ως εξής:

$$\mathbb{Q} \ni x = a/b, (a, b) = 1.$$

Σύμφωνα με το θεμελιώδες θεώρημα της αριθμητικής $a = p^{\ell} \cdot u_a$, $(u_a, p) = 1$ και $b = p^{\ell'} u_b$, $(u_b, p) = 1$.

Θέτουμε

$$|x|_p = \frac{1}{p^{\ell - \ell'}}.$$

Η παραπάνω μετρικές είναι μη ισοδύναμες και οι πληρώσεις του $\mathbb{Q}$ ως προς αυτές φτιάχνουν τα $\boldsymbol{p}$-αδικά σώματα $\mathbb{Q}_{\boldsymbol{p}}$.

ΤΟ ΘΕΩΡΗΜΑ ΤΟΠΙΚΟΥ-ΚΑΘΟΛΙΚΟΥ

Η παραπάνω μετρικές είναι μη ισοδύναμες και οι πληρώσεις του $\mathbb{Q}$ ως προς αυτές φτιάχνουν τα p-αδικά σώματα $\mathbb{Q}_p$.

Το local-global principle επαναδιατυπώνεται ως:

Θεώρημα: Μία τετραγωνική μορφή έχει λύση στο $\mathbb{Q}$ αν και μόνο αν έχει λύση σε κάθε $\mathbb{Q}_p$ και στο $\mathbb{R}$.

ΤΟ ΘΕΩΡΗΜΑ ΤΟΠΙΚΟΥ-ΚΑΘΟΛΙΚΟΥ

Η παραπάνω μετρικές είναι μη ισοδύναμες και οι πληρώσεις του $\mathbb{Q}$ ως προς αυτές φτιάχνουν τα p-αδικά σώματα $\mathbb{Q}_p$.

Το local-global principle επαναδιατυπώνεται ως:

Θεώρημα: Μία τετραγωνική μορφή έχει λύση στο $\mathbb{Q}$ αν και μόνο αν έχει λύση σε κάθε $\mathbb{Q}_p$ και στο $\mathbb{R}$.

Παρατήρηση Η ύπαρξη λύσης μπορεί να ελεγχθεί με μεθόδους ***αριθμητικής ανάλυσης*** όπως η μέθοδος του Newton.

Ο παραπάνω τύπος είναι η γνώριμη αναπαράσταση του κύκλου που οδηγεί στους τριγωνομετρικούς τύπους της εφαπτομένης του μισού τόξου.

$$x = \cos(\theta), y = \sin(\theta), t = \tan(\theta/2) = \frac{\sin(\theta)}{1 + \cos(\theta)}$$

οπότε

$$\cos(\theta) = \frac{1 - t^2}{1 + t^2}, \sin(\theta) = \frac{2t}{1 + t^2}.$$

Ο παραπάνω τύπος είναι η γνώριμη αναπαράσταση του κύκλου που οδηγεί στους τριγωνομετρικούς τύπους της εφαπτομένης του μισού τόξου.

$$x = \cos(\theta), y = \sin(\theta), t = \tan(\theta/2) = \frac{\sin(\theta)}{1 + \cos(\theta)}$$

οπότε

$$\cos(\theta) = \frac{1 - t^2}{1 + t^2}, \sin(\theta) = \frac{2t}{1 + t^2}.$$

Μπορούμε να αποδείξουμε τριγωνομετρικές ταυτότητες με αντικατάσταση ανάγωντάς τες σε ένα πρόβλημα ισότητας πολυωνύμων.

Άσκηση 12 σελ. 92 (Βαρουχάκης, Αδαμόπουλος, Γιαννίκος, Μπέτσης, Νοταράς, Φωτόπουλος)

$$\frac{1-\cos(2\theta)+\sin(2\theta)}{1+\cos(2\theta)+\sin(2\theta)}=\tan(\theta)$$

Άσκηση 12 σελ. 92 (Βαρουχάκης, Αδαμόπουλος, Γιαννίκος, Μπέτσης, Νοταράς, Φωτόπουλος)

$$\frac{1-\cos(2\theta)+\sin(2\theta)}{1+\cos(2\theta)+\sin(2\theta)} = \tan(\theta)$$

```
In[1]:= CT := (1 - t^2)/(1 + t^2)

In[2]:= ST := 2*t/(1 + t^2)

In[3]:= Simplify[(1 - CT + ST)/(1 + CT + ST)]

Out[3]= t
```

Αν θέσουμε $\theta = 2\arctan(\boldsymbol{t})$ έχουμε $\boldsymbol{d}\theta = \frac{2\boldsymbol{dt}}{1+\boldsymbol{t}^2}$. Αν έχουμε ένα ολοκλήρωμα που είναι ρητή συνάρτηση των $\cos\theta$ και $\sin\theta$ με τους παραπάνω μετασχηματισμούς καταλήγουμε σε ένα ολοκλήρωμα ρητής συνάρτησης του $\boldsymbol{t}$ το οποίο υπολογίζεται με την βοήθεια στοιχειωδών συναρτήσεων.

$$\int \frac{1}{\sqrt{1-x^2}}dx$$

Έχουμε την μεταβλητή y που ικανοποιεί την εξίσωση:

$$y^2 = 1 - x^2.$$

$$\int \frac{1}{\sqrt{1-x^2}}dx$$

Έχουμε την μεταβλητή y που ικανοποιεί την εξίσωση:

$$y^2 = 1 - x^2.$$

Θα χρησιμοποιήσουμε τον τύπο:

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

παρατηρώντας ότι $dx = -\frac{4t}{(1+t^2)^2}dt$.

$$\int \frac{1}{\sqrt{1-x^2}}dx$$

Έχουμε την μεταβλητή y που ικανοποιεί την εξίσωση:

$$y^2 = 1 - x^2.$$

Θα χρησιμοποιήσουμε τον τύπο:

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

παρατηρώντας ότι $dx = -\frac{4t}{(1+t^2)^2}dt$.

Καταλήγουμε λοιπόν στον υπολογισμό

$$\int -\frac{2}{1+t^2}dt = -2\arctan(t).$$

Κάνοντας τον παραπάνω υπολογισμό με το Mathematica παίρνουμε ως αποτέλεσμα

$$\int \frac{1}{\sqrt{1-x^2}}dx = \arcsin(x).$$

Κάναμε κάπου λάθος;

Κάνοντας τον παραπάνω υπολογισμό με το Mathematica παίρνουμε ως αποτέλεσμα

$$\int \frac{1}{\sqrt{1-x^2}}dx = \arcsin(x).$$

Κάναμε κάπου λάθος;

Όχι, οι δύο συναρτήσεις διαφέρουν κατά σταθερά!

```
In[1]:= FullSimplify[D[(ArcSin[(1 - t^2)/(1 + t^2)] +
        2 ArcTan[t]), t], Assumptions -> Element[t, Reals]]

         2 - 2 Sign[t]
Out[1]= -------------
                 2
            1 + t
```

Προβολικό Επίπεδο:

Είναι εξ ορισμού το σύνολο των κλάσεων ισοδυναμίας

$$\mathbb{R}^3 \backslash \{(0,0,0)\} / \sim,$$

όπου

$$(x, y, z) \sim (x', y', z') \Leftrightarrow (x, y, z) = \lambda(x', y', z'),$$

για κάποιο $\lambda \neq 0$.

Προβολικό Επίπεδο:

Είναι εξ ορισμού το σύνολο των κλάσεων ισοδυναμίας

$$\mathbb{R}^3 \setminus \{(0,0,0)\} / \sim,$$

όπου

$$(x, y, z) \sim (x', y', z') \Leftrightarrow (x, y, z) = \lambda(x', y', z'),$$

για κάποιο $\lambda \neq 0$.

Το προβολικό επίπεδο μπορούμε να το ταυτίσουμε με το σύνολο των μη-τετριμμένων ευθειών στον χώρο $\mathbb{R}^3$. Θα συμβολίζουμε την κλάση ισοδυναμίας του $(x, y, z) \neq (0,0,0)$ με $[x : y : z]$. Παρατηρούμε ότι τα σημεία $[x, y, 1]$ είναι σε ένα προς ένα αντιστοιχία με το επίπεδο $\mathbb{R}^2$, ενώ τα σημεία $[x, y, 0]$ αποτελούν μια ευθεία που την ονομάζουμε την ευθεία στο άπειρο.

Για κάθε πολυώνυμο $f(x, y) \in \mathbb{R}[x, y]$,

$$f = \sum_{i,j} a_{ij} x^i y^j$$

βαθμού n θα συμβολίζουμε με F το αντίστοιχο ομογενές πολυώνυμο

$$F = \sum_{i,j} a_{ij} x^i y^j z^{n-i-j}.$$

Τη διαδικασία αυτή θα την ονομάζουμε ***ομογενοποίηση***.

Για κάθε πολυώνυμο $f(x, y) \in \mathbb{R}[x, y]$,

$$f = \sum_{i,j} a_{ij} x^i y^j$$

βαθμού n θα συμβολίζουμε με F το αντίστοιχο ομογενές πολυώνυμο

$$F = \sum_{i,j} a_{ij} x^i y^j z^{n-i-j}.$$

Τη διαδικασία αυτή θα την ονομάζουμε ***ομογενοποίηση***.

Γεωμετρικά όταν δουλεύουμε πάνω από το σώμα των πραγματικών αριθμών το ομογενοποιημένο σύνολο αντιστοιχεί στον κώνο που γράφουν οι ευθείες που περνούν από το σημείο $(0, 0, 0)$ και από ένα σημείο της καμπύλης $f(x, y), z = 1$.

ΑΠΟΟΜΟΓΕΝΟΠΟΙΗΣΗ

Είναι η αντίστροφη διαδικασία. Από ένα ομογενές πολυώνυμο καταλήγουμε σε ένα μη ομογενές θέτοντας $Z = 1$. Φυσικά θα μπορούσαμε να αποομογενοποίησουμε θέτοντας $= 1$ ή $Y = 1$, ή ακόμα να θεωρήσουμε την τομή με οποιοδήποτε άλλο επίπεδο.

$$X^2 + Y^2 = Z^2 \longrightarrow x^2 + y^2 = 1$$

ΑΠΟΟΜΟΓΕΝΟΠΟΙΗΣΗ

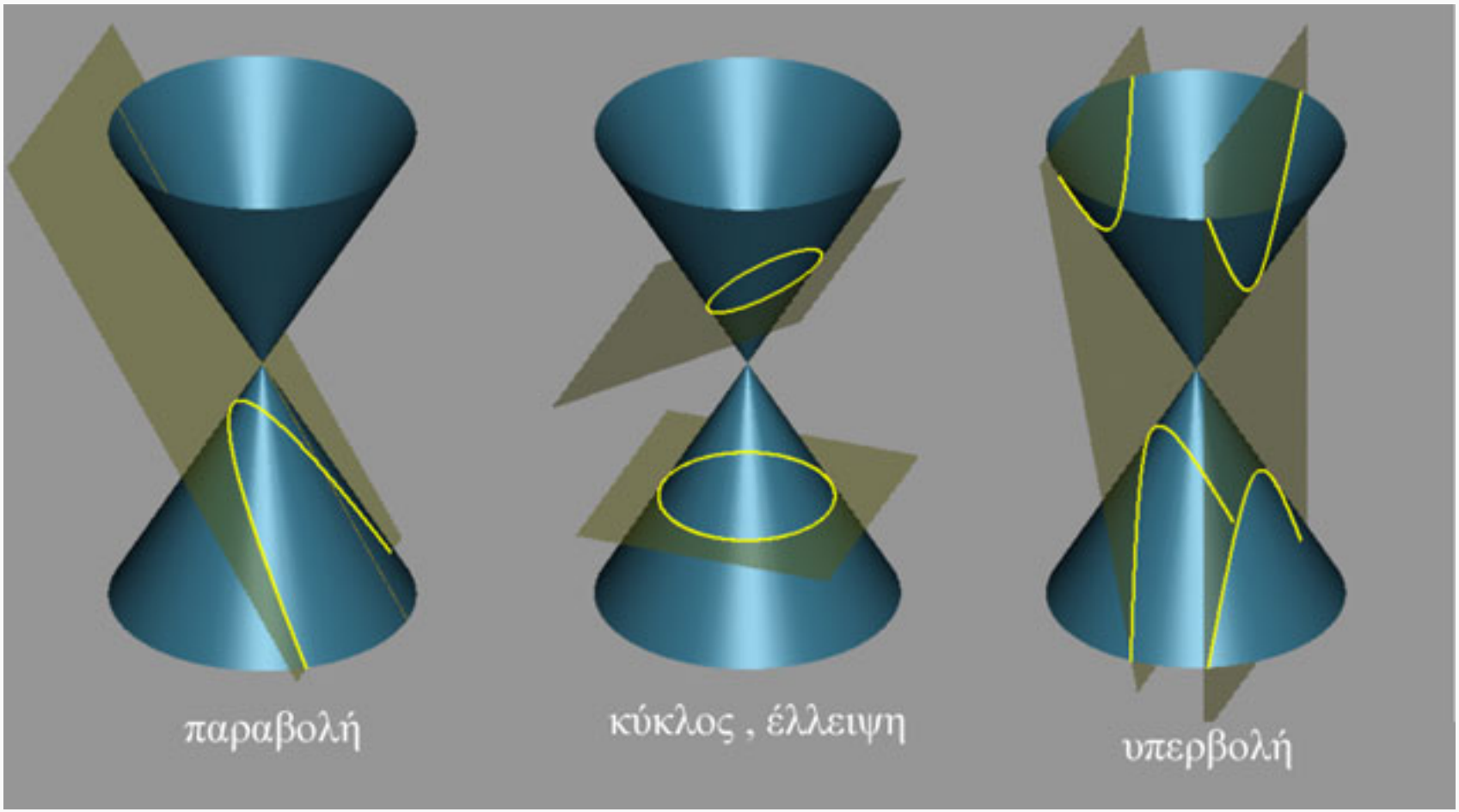
Είναι η αντίστροφη διαδικασία. Από ένα ομογενές πολυώνυμο καταλήγουμε σε ένα μη ομογενές θέτοντας $Z = 1$. Φυσικά θα μπορούσαμε να αποομογενοποίησουμε θέτοντας $= 1$ ή $Y = 1$, ή ακόμα να θεωρήσουμε την τομή με οποιοδήποτε άλλο επίπεδο.

$$X^2 + Y^2 = Z^2 \longrightarrow x^2 + y^2 = 1$$

$$X^2 + Y^2 = Z^2 \longrightarrow x^2 + 1 = z^2$$

ΚΩΝΙΚΕΣ ΤΟΜΕΣ

Προβολικά όλες οι κωνικές τομές ταυτίζονται και αντιστοιχούν σε διαφορετικό επίπεδο τομής.



ΜΙΑ ΑΚΟΜΑ ΡΗΤΗ ΚΑΜΠΥΛΗ

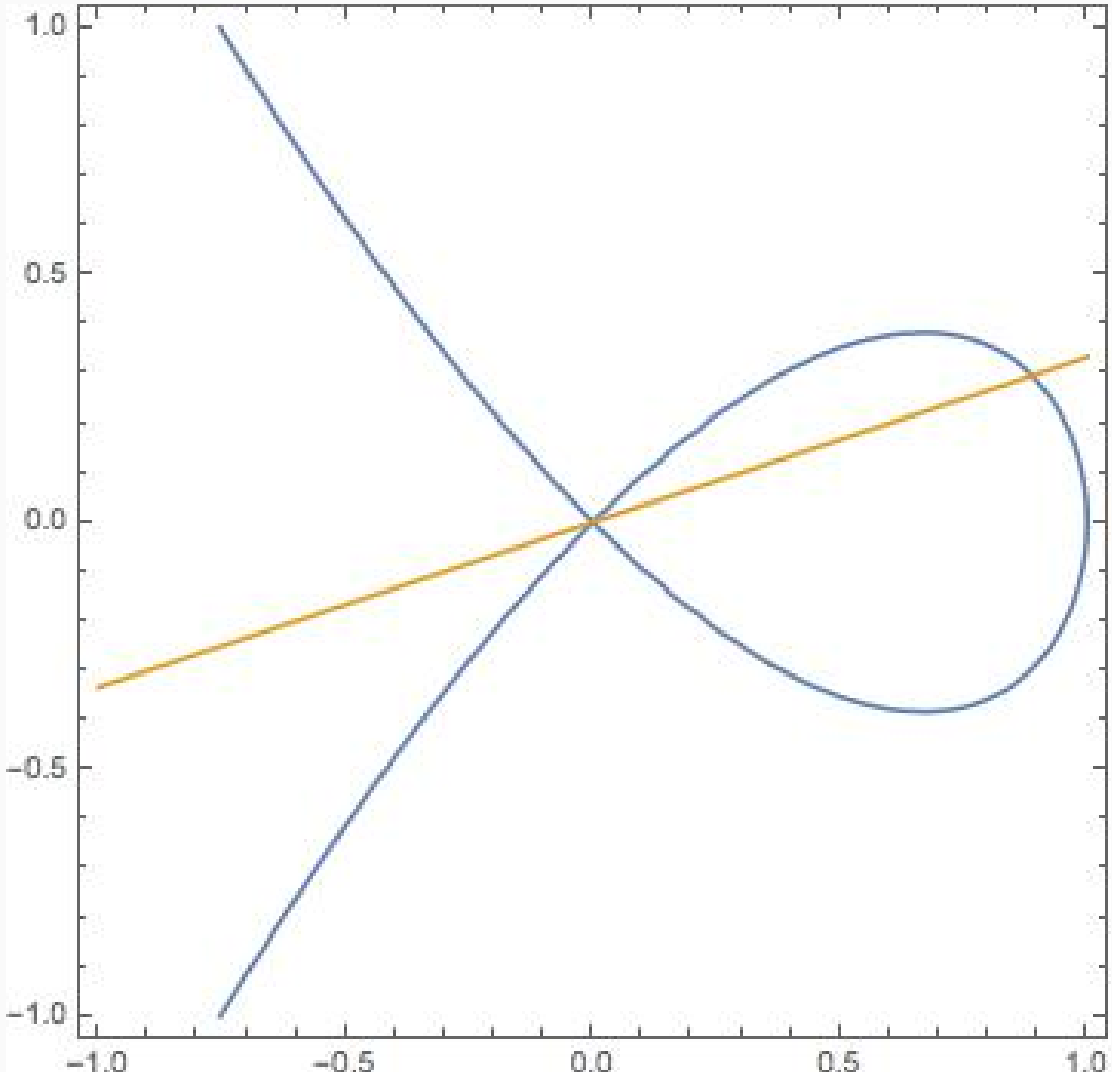
Να υπολογιστεί το ολοκλήρωμα $\int \frac{1}{\sqrt{x^2-x^3}}dx$

Καμπύλη $y^2 = x^2 - x^3$.

ΜΙΑ ΑΚΟΜΑ ΡΗΤΗ ΚΑΜΠΥΛΗ

Να υπολογιστεί το ολοκλήρωμα $\int \frac{1}{\sqrt{x^2-x^3}}\,dx$

Καμπύλη $y^2 = x^2 - x^3$.



ΜΙΑ ΑΚΟΜΑ ΡΗΤΗ ΚΑΜΠΥΛΗ

Καμπύλη $y^2 = x^2 - x^3$.

$y = \lambda \cdot x$, τομή $\lambda^2 x^2 = x^2 - x^3 \Rightarrow x = 0$ ή $\lambda^2 = 1 - x$ και συνεπώς $y = |1 - \lambda^2|\lambda$.

Καμπύλη $y^2 = x^2 - x^3$.

$y = \lambda \cdot x$, τομή $\lambda^2 x^2 = x^2 - x^3 \Rightarrow x = 0$ ή $\lambda^2 = 1 - x$ και συνεπώς $y = |1 - \lambda^2|\lambda$.

Επιπλέον $dx = 2\lambda d\lambda$, άρα το ολοκλήρωμα γίνεται

$$\int \frac{1}{1-\lambda^2} d\lambda = \operatorname{arctanh}(\lambda) = \arctan(\sqrt{1-x}).$$

Καμπύλη $y^2 = x^2 - x^3$.

$y = \lambda \cdot x$, τομή $\lambda^2 x^2 = x^2 - x^3 \Rightarrow x = 0$ ή $\lambda^2 = 1 - x$ και συνεπώς $y = |1 - \lambda^2|\lambda$.

Επιπλέον $dx = 2\lambda d\lambda$, άρα το ολοκλήρωμα γίνεται

$$\int \frac{1}{1-\lambda^2} d\lambda = \operatorname{arctanh}(\lambda) = \arctan(\sqrt{1-x}).$$

Υπολογισμός του ολοκληρώματος

$$\int \frac{1}{\sqrt{x^3 + ax + b}} dx$$

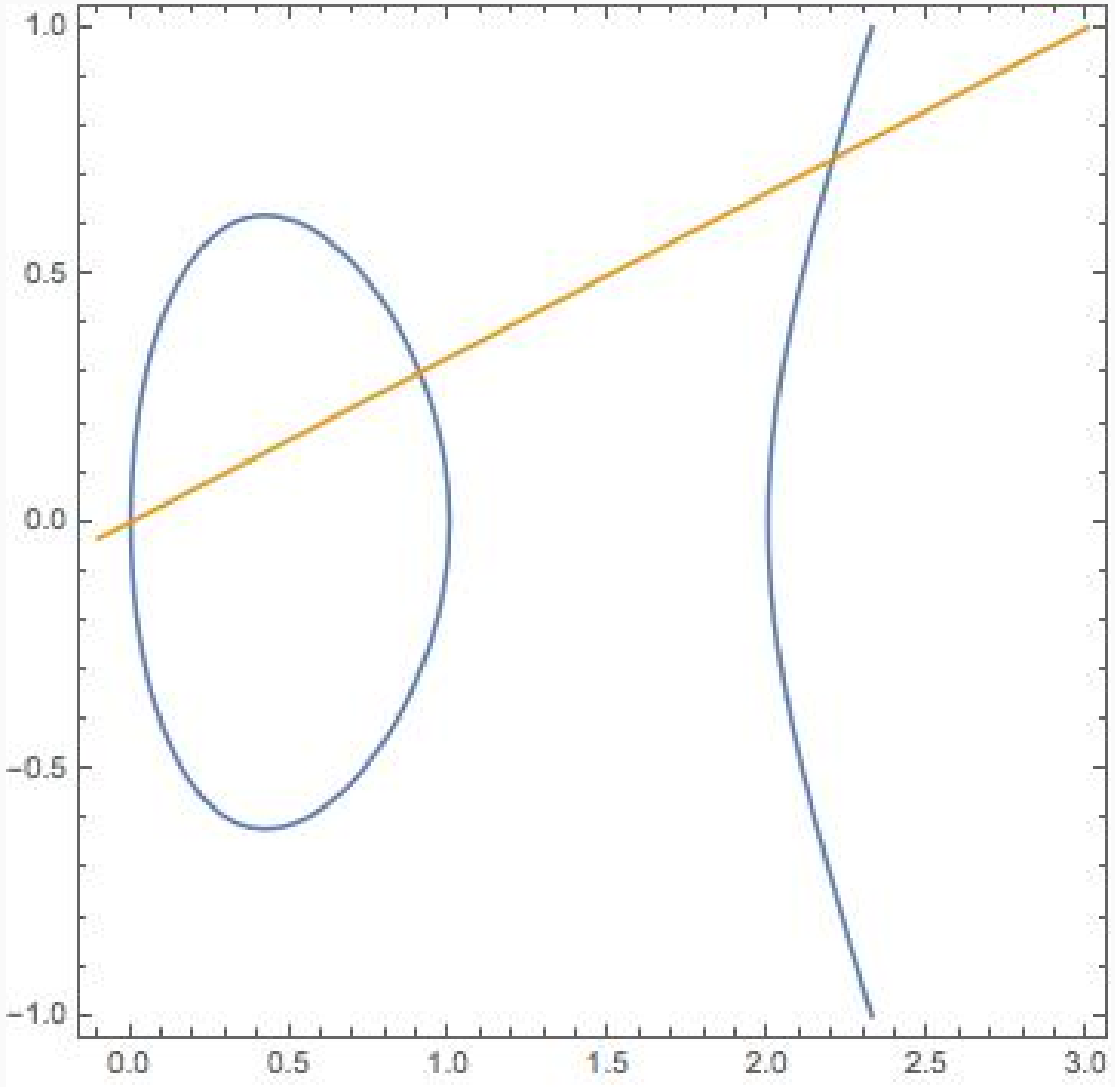
ώστε ο παρονομαστής να μην έχει διπλές ρίζες.

Υπολογισμός του ολοκληρώματος

$$\int \frac{1}{\sqrt{x^3 + ax + b}} dx$$

ώστε ο παρονομαστής να μην έχει διπλές ρίζες.

Η καμπύλη δεν είναι ρητή. Η ευθεία $y = \lambda x$ που περνάει από το σημείο $(0, 0)$ έχει δύο σημεία τομής, εκτός του σημείου $(0, 0)$.



Σχήμα 5: Τομή καμπύλης με ευθεία

WEIERSTRASS

Ο Weierstrass κατασκεύασε την συνάρτηση (το $L \cong \mathbb{Z} \times \mathbb{Z}$, είναι μια διακριτή υποομάδα του $\mathbb{C}$)

$$\mathbb{C} \to \mathbb{C}$$

η οποία ορίζεται από τον τύπο:

$$\wp(z, L) = \frac{1}{z^2} + \sum_{\lambda \in L - \{0\}} \left(\frac{1}{(z+\lambda)^2} - \frac{1}{\lambda^2} \right).$$

Η συνάρτηση του Weierstrass ικανοποιεί τη διαφορική εξίσωση

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L).$$

Δηλαδή το ζευγάρι $(x, y) = (\wp(z), \wp'(z))$ παραμετρίζει την ελλειπτική καμπύλη

$$y^2 = 4x^3 - g_2(L)x - g_3(L).$$

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L).$$

Οι συναρτήσεις $g_2(L), g_3(L)$ εξαρτώνται από το lattice L, και δίνονται από τον τύπο:

$$g_2(L) = 60 \sum_{\lambda \in L - \{0\}} \frac{1}{\lambda^4} \qquad g_3(L) = 140 \sum_{\lambda \in L - \{0\}} \frac{1}{\lambda^6}.$$

Ελλειπτικές Καμπύλες

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L),$$

παραμετρίζει την εξίσωση $y^2 = 4x^3 - g_2(L)x - g_3(L)$.

Τριγωνομετρικός κύκλος

$$(x, y) = (\sin(x), \cos(x)) = (\sin(x), \sin'(x))$$

ικανοποιούν την εξίσωση $x^2 + y^2 = 1$ και συνεπώς παραμετρίζουν τον κύκλο.

Επιπλέον ο κύκλος είναι το πηλίκο του $\mathbb{R}/2\pi\mathbb{Z}$, ενώ η καμπύλη είναι πηλίκο του

$$\mathbb{C}\backslash\{0\}/L,$$

αφού οι συναρτήσεις $\wp$, $\wp'$ είναι L περιοδικές. Τα σημεία του L αποτελούν πόλους της συνάρτησης του Weierstrass και η συνάρτηση του Weierstrass τα στέλνει στο άπειρο.

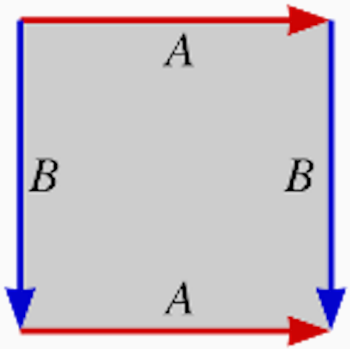
Επιπλέον ο κύκλος είναι το πηλίκο του $\mathbb{R}/2\pi\mathbb{Z}$, ενώ η καμπύλη είναι πηλίκο του

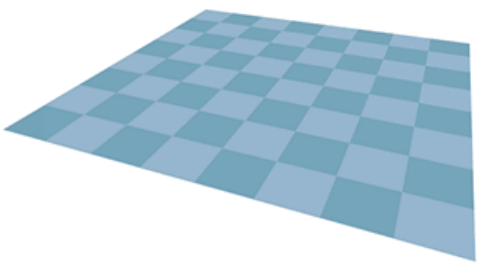
$$\mathbb{C}\backslash\{0\}/L,$$

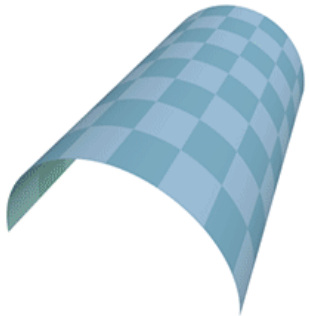
αφού οι συναρτήσεις $\wp$, $\wp'$ είναι L περιοδικές. Τα σημεία του L αποτελούν πόλους της συνάρτησης του Weierstrass και η συνάρτηση του Weierstrass τα στέλνει στο άπειρο.

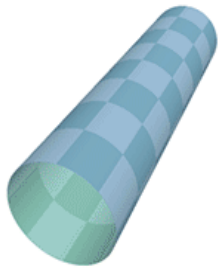
Με αυτό τον τρόπο έχουμε μια προβολική εμφύτευση του $\mathbb{C}/L$ στην καμπύλη $Y^2Z = X^3 + aZ^2X + bX^3$.

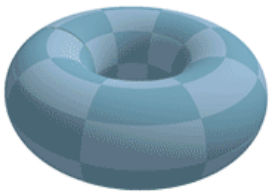
ΤΟΠΟΛΟΓΙΚΗ ΜΟΡΦΗ

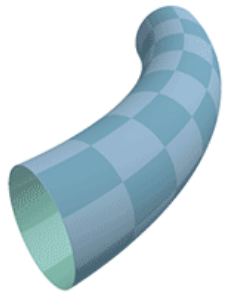












Ισχύει ότι

$$\det \begin{bmatrix} \wp(\boldsymbol{u}) & \wp'(\boldsymbol{u}) & 1 \\ \wp(\boldsymbol{v}) & \wp'(\boldsymbol{v}) & 1 \\ \wp(\boldsymbol{w}) & \wp'(\boldsymbol{w}) & 1 \end{bmatrix} = 0$$

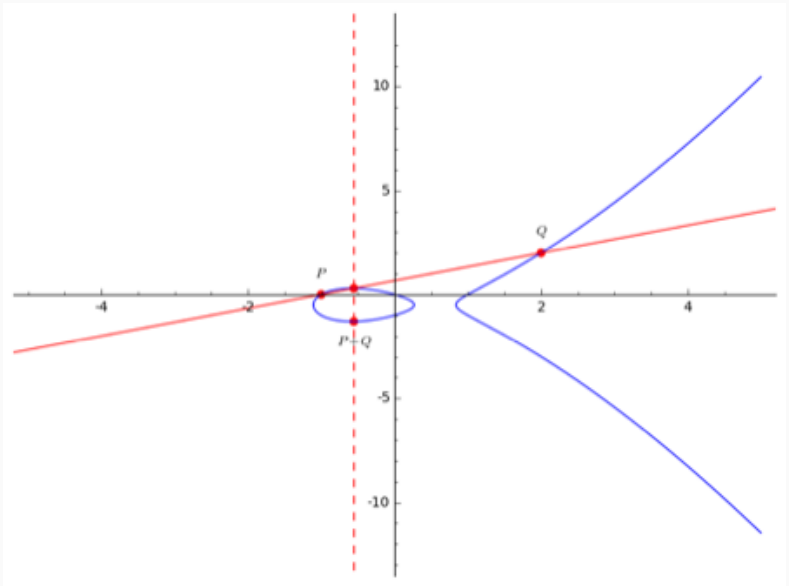
όπου $\boldsymbol{u} + \boldsymbol{v} + \boldsymbol{w} = 0$.

Οι πραξεις δινονται με αλγεβρικο τροπο.

Το σύνολο των σημείων του προβολικού χώρου που ικανοποιούν την

$$Y^2Z = X^3 + aZ^2X + bX^3$$

αποκτά δομή ομάδας αρκεί να απαιτήσουμε συνευθειακά σημεία να έχουν άθροισμα 0.



Σχήμα 7: Πρόσθεση δύο σημείων ελλειπτικής καμπύλης

ΑΛΓΕΒΡΙΚΟΣ ΤΥΠΟΣ ΠΡΟΣΘΕΣΗΣ ΣΗΜΕΙΩΝ

$P = (x_1, y_1), Q = (x_2, y_2)$ σημεία επί της ελλειπτικής καμπύλη και L η ευθεία που τα ενώνει. Έστω PQ το τρίτο σημείο τομής.

Από PQ φέρνουμε την κάθετη ευθεία στον άξονα των x η οποία τέμνει την ελλειπτική καμπύλη στο σημείο $P + Q$. Το σημείο αυτό το ορίζουμε να είναι άθροισμα των σημείων P, Q.

ΑΛΓΕΒΡΙΚΟΣ ΤΥΠΟΣ ΠΡΟΣΘΕΣΗΣ ΣΗΜΕΙΩΝ

$P = (x_1, y_1), Q = (x_2, y_2)$ σημεία επί της ελλειπτικής καμπύλη και L η ευθεία που τα ενώνει. Έστω PQ το τρίτο σημείο τομής.
Από PQ φέρνουμε την κάθετη ευθεία στον άξονα των x η οποία τέμνει την ελλειπτική καμπύλη στο σημείο $P + Q$. Το σημείο αυτό το ορίζουμε να είναι άθροισμα των σημείων P, Q.

Στην περίπτωση που θέλουμε να υπολογίσουμε το σημείο $P + P$, αντί να θεωρήσουμε τη χορδή όπως στην προηγούμενη περίπτωση, θεωρούμε την εφαπτομένη.

$P = (x_1, y_1), Q = (x_2, y_2)$ σημεία επί της ελλειπτικής καμπύλη και L η ευθεία που τα ενώνει. Έστω PQ το τρίτο σημείο τομής.
Από PQ φέρνουμε την κάθετη ευθεία στον άξονα των x η οποία τέμνει την ελλειπτική καμπύλη στο σημείο $P + Q$. Το σημείο αυτό το ορίζουμε να είναι άθροισμα των σημείων P, Q.

Στην περίπτωση που θέλουμε να υπολογίσουμε το σημείο $P + P$, αντί να θεωρήσουμε τη χορδή όπως στην προηγούμενη περίπτωση, θεωρούμε την εφαπτομένη.

Στην περίπτωση που ένας προσθετέος είναι το σημείο στο άπειρο, θέτουμε $P + \mathcal{O} = P$, δηλαδή το σημείο στο άπειρο είναι το ουδέτερο της πράξης.

Ας υποθέσουμε ότι $P_1 = (x_1, y_1)$ και $P_2 = (x_2, y_2)$. Οι παραπάνω κανόνες πρόσθεσης μπορούν να εκφραστούν με τον εξής απλό τρόπο:

Ας υποθέσουμε ότι $P_1, P_2 \neq \mathcal{O}$.

- Αν $x_1 = x_2$ και $y_1 = -y_2$ θέτουμε $P_1 + P_2 = \mathcal{O}$. Δηλαδή συμμετρικά σημεία ως προς τον άξονα των x έχουν άθροισμα $\mathcal{O}$.
- Διαφορετικά θέτουμε

$$\lambda = (3x_1 + a)/(2y_1) \text{ αν } \quad P_1 = P_2$$

$$\lambda = (y_1 - y_2)/(x_1 - x_2) \text{ αν } \quad P_1 \neq P_2$$

Το σημείο $P_1 + P_2$ έχει συντεταγμένες (x_3, y_3) που δίνονται από τους τύπους:

$$(x_3, y_3) = (\lambda^2 - x_1 - x_2, -\lambda x_3 - y_1 + \lambda x_1)$$

Οι ρητές λύσεις μιας κυβικής ελλειπτικής καμπύλης αποτελούν ομάδα.

Θεώρημα Mordell Η ομάδα των σημείων $E(\mathbb{Q})$ είναι μια πεπερασμένα παραγόμενη αβελιανή ομάδα. Δηλαδή

$$E(\mathbb{Q})) = \mathbb{Z}^r \times \prod_{i=1}^{s} \frac{\mathbb{Z}}{n_i\mathbb{Z}}.$$

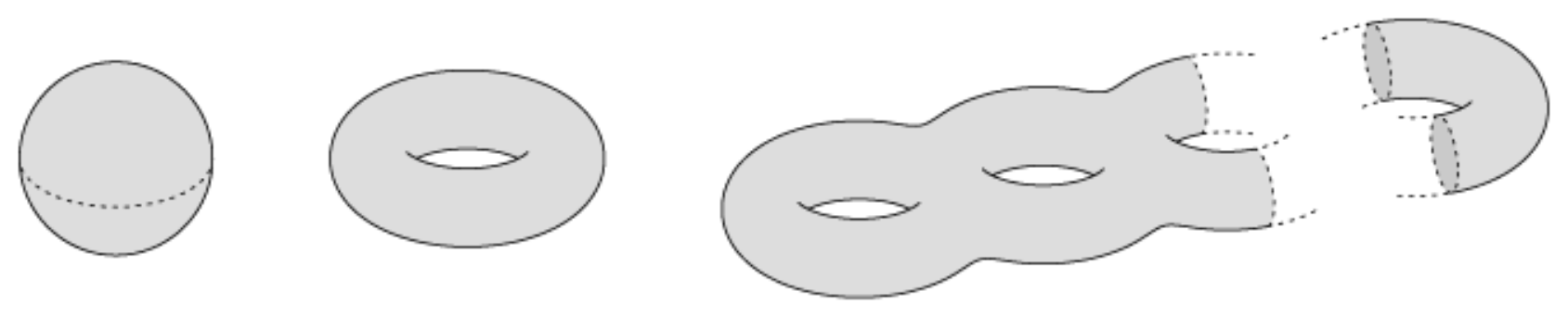
Οι ρητές λύσεις μιας κυβικής ελλειπτικής καμπύλης αποτελούν ομάδα.

Θεώρημα Mordell Η ομάδα των σημείων $E(\mathbb{Q})$ είναι μια πεπερασμένα παραγόμενη αβελιανή ομάδα. Δηλαδή

$$E(\mathbb{Q})) = \mathbb{Z}^r \times \prod_{i=1}^{s} \frac{\mathbb{Z}}{n_i\mathbb{Z}}.$$

Αν βρούμε μερικά σημεία στην Ελλειπτική καμπύλη μπορούμε να κάνουμε πράξεις με αυτά και να βρούμε και άλλα σημεία - λύσεις της διοφαντικής εξίσωσης.

Μια αλγεβρική προβολική καμπύλη, είναι ένα συμπαγές υποσύνολο του $\mathbb{P}^2(\mathbb{C})$, το οποίο αντιστοιχεί σε μια συμπαγή επιφάνεια.



Η τοπολογία της επιφάνειας επηρεάζει το πλήθος των λύσεων

γένος	λύσεις
$g = 0$	καμία λύση ή άπειρες που δίνονται από την ρητή παραμέτριση
$g = 1$	καμία λύση ή οι λύσεις έχουν δομή πεπ. παραγόμενης αβελιανής ομάδας
$g \geq 2$	πεπερασμένες λύσεις

Η περίπτωση $g \geq 2$ ήταν για πολλά χρόνια ανοιχτή εικασία και λύθηκε το 1984 από τον G. Faltings.

Σχήμα 8: G. Faltings

ΤΟ ΤΕΛΕΥΤΑΙΟ ΘΕΩΡΗΜΑ ΤΟΥ FERMAT.

Η καμπύλη του Fermat έχει γένος $\frac{(n-1)(n-2)}{2}$ και για $n \geq 4$ το γένος είναι $g \geq 2$. Το θεώρημα Mordel-Faltings εξασφαλίζει ότι αν έχει μη τετριμμένες λύσεις αυτές είναι πεπερασμένες.

ΤΟ ΤΕΛΕΥΤΑΙΟ ΘΕΩΡΗΜΑ ΤΟΥ FERMAT.

Η καμπύλη του Fermat έχει γένος $\frac{(n-1)(n-2)}{2}$ και για $n \geq 4$ το γένος είναι $g \geq 2$. Το θεώρημα Mordel-Faltings εξασφαλίζει ότι αν έχει μη τετριμμένες λύσεις αυτές είναι πεπερασμένες.

Το τελευταίο θεώρημα του Fermat αποδείχτηκε το 1994 από τον A. Weils χρησιμοποιώντας εργαλεία από την θεωρία των Ελλειπτικών καμπύλων.

ΣΥΜΠΕΡΑΣΜΑΤΑ

- Είδαμε ένα αρχαίο πρόβλημα επίλυσης διοφαντικών εξισώσεων, το οποίο μπορεί να λυθεί με γεωμετρικές τεχνικές.
- Είδαμε ότι η ίδια τεχνική μπορεί να αντιμετωπίσει προβλήματα τριγωνομετρίας, υπολογισμού ολοκληρωμάτων και διοφαντικών εξισώσεων.
- Τα περισσότερο εντυπωσιακά και όμορφα μαθηματικά είναι αυτά που με απροσδόκητο τρόπο συνδέουν διαφορετικούς κλάδους μαθηματικών ή και Φυσικής.

ΕΥΧΑΡΙΣΤΩ ΠΟΛΥ

Ευχαριστώ πολύ!