Διοφαντικές Εξισώσεις

Μια Διοφαντική εξίσωση} διοφαντική εξίσωση είναι μια εξίσωση της μορφής

$$f(x_1, x_2, \dots, x_n) = 0$$

όπου το $f(x_1, x_2, \dots, x_n)$ είναι ένα πολυώνυμο n μεταβλητών με συντελεστές ακεραίους αριθμούς και n ένας φυσικός αριθμός $n \geq 2$.

Επίλυση μιας διοφαντικής εξίσωσης είναι η εύρεση όλων των n-άδων ακεραίων αριθμών $(x_1, \dots, x_n) \in \mathbb{Z}^n$ οι οποίες επαληθεύουν την εξίσωση.

Παράδειγμα 1

Να λυθεί η διοφαντική εξίσωση

$$y^3 = x^2 - 16.$$

Η εξίσωση γράφεται ως

$$y^3 = (x-4)(x+4).$$

Έστω $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ κάποια λύση αυτής και $d = (x-4, x+4)$. Αν ο x είναι περιττός, τότε $d = 1$ οπότε $x - 4 = a^3, x + 4 = b^3$ με $a, b \in \mathbb{Z}$ περιττούς και $(a, b) = 1$. Επομένως $b^3 - a^3 = 8$, το οποίο είναι αδύνατο.

Αν ο x είναι άρτιος, τότε και ο y είναι άρτιος, συνεπώς $8 \mid x^2$ οπότε $4 \mid x$. Ας γράψουμε το $x = 4x_1$, $x_1 \in \mathbb{Z}$. Η εξίσωση γίνεται $16x_1^2 - 16 = y^3$, άρα $4 \mid y$, δηλαδή $y = 4y_1$, $y_1 \in \mathbb{Z}$.

Παράδειγμα 1

Από τα παραπάνω, προκύπτει ότι

$$x_1^2 = 4y_1^3 + 1, \qquad x_1 \text{ περιττός}$$

Το $x_1 = 2m + 1$ για $m \in \mathbb{Z}$. Συνεπώς $m^2 + m = y_1^3$, δηλαδή $m(m+1) = y_1^3$ και $(m, m+1) = 1$. Επομένως, $m = t^3, m + 1 = s^3$, $t, s \in \mathbb{Z}$ και $(t, s) = 1$. Αλλά οι μόνοι διαδοχικοί κύβοι ακεραίων ανήκουν στο σύνολο $\{-1, 0, 1\}$. Αυτό σημαίνει ότι ο m ή ο $m + 1$ είναι ίσος με μηδέν, δηλαδή $y_1 = 0$ οπότε και $y = 0$. Τελικά η μοναδική λύση της εξίσωσης είναι η $(x, y) = (\pm 4, 0)$.

Παράδειγμα 2

Να λυθεί η διοφαντική εξίσωση

$$Y^3 = X^2 + 1.$$

Παρατηρούμε ότι εδώ το δεξιό μέλος δεν παραγοντοποιείται στο $\mathbb{Z}$. Αν υποθέσουμε ότι $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ λύση της παραπάνω εξίσωσης και μπορούμε να παραγοντοποιήσουμε το δεξιό μέλος

$$y^3 = (x + i)(x - i), \qquad x \in \mathbb{Z}$$

Η παραγοντοποίηση έλαβε χώρα στον δακτύλιο του Gauss

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

και επομένως μας ενδιαφέρει η αριθμητική του δακτυλίου αυτού.

Παράδειγμα 2

Έστω $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ μια λύση της εξίσωσης. Παραγοντοποίηση του δεξιού μέλους δίνει

$$y^3 = (x + i)(x - i),$$

όπου $x + i, x - i \in \mathbb{Z}[i]$ και

$$R = \mathbb{Z}[i] = \{a + bi : (a, b) \in \mathbb{Z} \times \mathbb{Z}\}$$

είναι, όπως θα δούμε αργότερα, ο δακτύλιος των ακεραίων αλγεβρικών αριθμών του σώματος του Gauss

$$\mathbb{Q}(i) = \{a + bi : (a, b) \in \mathbb{Q} \times \mathbb{Q}\}.$$

Αν $\xi = a + bi \in \mathbb{Z}[i]$, η norm του ξ ορίζεται ως

$$N(\xi) = (a + ib)(a - bi) = a^2 + b^2 \in \mathbb{N}.$$

Η ομάδα των μονάδων του $\mathbb{Z}[i]$ είναι η

$$E(\mathbb{Z}[i]) = \{\xi \in \mathbb{Z}[i] : N(\xi) = \pm 1\} = \{\pm 1, \pm i\} = \langle i \rangle.$$

Παράδειγμα 2

Με βάση την παραπάνω norm, ο $\mathbb{Z}[i]$ είναι ευκλείδειος δακτύλιος και συνεπώς δακτύλιος κυρίων ιδεωδών και επομένως δακτύλιος μονοσήμαντης αναλύσης.

Παρατηρούμε ότι $2 = (-i)(1+i)^2$, όπου $-i \in E(\mathbb{Z}[i])$ και $\pi := 1+i$ ανάγωγο στοιχείο του $\mathbb{Z}[i]$. Έστω $d = (x+i, x-i)$, $d \mid 2$. Ισχυριζόμαστε ότι $d \cong 1$. Πράγματι αν $d \ncong 1$, τότε $1+i \mid d$ και συνεπώς $1+i \mid x+i$ άρα $N(1+i) \mid N(x+i)$.

Καταλήγουμε λοιπόν στο συμπέρασμα ότι $2 \mid x^2+1 = y^3$ άρα $2 \mid y$. Τότε $2^3 \mid y^3$ άρα $8 \mid x^2+1$ και $x^2 \equiv -1 \mod 8$, το οποίο είναι άτοπο.

Ώστε $d \cong 1$ οπότε η $y^3 = (x+i)(x-i)$ λόγω της μονοσημάντης αναλύσης δίνει $x+i \cong \xi^3$ και $\xi \in \mathbb{Z}[i]$, δηλαδή $x+i = \epsilon\xi^3$, όπου $\epsilon \in E(\mathbb{Z}[i])$. Αφού $E(\mathbb{Z}[i]) = \langle i \rangle$ κυκλική ομάδα τάξεως 4, έπεται ότι η συνάρτηση $\epsilon \mapsto \epsilon^3$ είναι αυτομορφισμός της ομάδας των μονάδων $E(\mathbb{Z}[i])$.

Παράδειγμα 2

Μπορούμε να αντικαταστήσουμε το ϵ με το ϵ^3 και να πάρουμε $x + i = \eta^3$ με $\eta = a + ib \in \mathbb{Z}[i]$. Καταλήγουμε στη σχέση

$$x + i = (a^3 - 3ab^2) + i(3a^2b - b^3),$$

οπότε $1 = b(3a^2 - b^2)$ συνεπώς το $b \mid 1$, άρα $b = \pm 1$. Έχουμε $3a^2 - 1 = \pm 1$ και $a = 0$ είναι η μόνη λύση στο $\mathbb{Z}$. Τότε $x = a^3 - 3ab^2 = 0$ το οποίο δίνει $y = 1$.

Ώστε το σύνολο λύσεων της είναι το $(x, y) = (0, 1)$.

Αποφασιστικά για την απόδειξη ήταν

1. Το $\mathbb{Z}[i]$ είναι δακτύλιος μονοσήμαντης ανάλυσης
2. Η γνώση της δομής της ομάδας των μονάδων $E(\mathbb{Z}[i])$.

Παράδειγμα 3

Ζητούνται οι ακέραιες λύσεις της εξίσωσης

$$2y^3 = x^2 + 5$$

Και εδώ το δεξιό μέλος δεν παραγοντοποιείται στο $\mathbb{Z}$. Μπορούμε όμως να το παραγοντοποιήσουμε στον δακτύλιο

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in Z\}.$$

Πράγματι, αν $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ λύση της εξίσωσης, τότε παραγοντοποιούμε το δεξιό μέλος και έχουμε

$$2y^3 = (x + \sqrt{-5})(x - \sqrt{-5}).$$

Σε αυτή την περίπτωση θα πρέπει να εργαστούμε στο σύνολο

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\},$$

το οποίο και πάλι αποτελεί ακέραια περιοχή. Η ομάδα των μονάδων του δακτυλίου $\mathbb{Z}[\sqrt{-5}]$ είναι $E(\mathbb{Z}[\sqrt{-5}]) = \{\pm 1\}$.

Παράδειγμα 3

Το 2 είναι ανάγωγο στοιχείο του $\mathbb{Z}[\sqrt{-5}]$. Πράγματι, αν $2 = a \cdot b$ με $a, b \in \mathbb{Z}[\sqrt{-5}]$ όχι μονάδες, τότε $N(a)N(b) = 4$, οπότε $N(a) = N(b) = \pm 2$. Αυτό όμως είναι αδύνατο αφού αν

$$a = \kappa + \lambda\sqrt{-5},\ \kappa, \lambda \in \mathbb{Z}, N(a) = \kappa^2 + 5\lambda^2 \neq \pm 2.$$

«Επομένως»

$$2 \mid (x + \sqrt{-5}) \text{ είτε } 2 \mid (x - \sqrt{-5})$$

που σημαίνει ότι ή

$$\frac{x + \sqrt{-5}}{2} = \frac{x}{2} + \frac{1}{2}\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$$

ή

$$\frac{x - \sqrt{-5}}{2} = \frac{x}{2} - \frac{1}{2}\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}],$$

το οποίο είναι άτοπο, αφού $\frac{1}{2} \notin \mathbb{Z}$.

Παραδείγμα 3

Καταλήξαμε στο συμπέρασμα ότι η διοφαντική εξίσωση

$$2Y^3 = X^2 + 5$$

δεν έχει ακέραια λύση.

Η εξίσωση όμως έχει τουλάχιστον μία λύση, την $(x, y) = (\pm 7, 3)$. Πού είναι το λάθος;

Απάντηση: Το 2 είναι *ανάγωγο στοιχείο* του $\mathbb{Z}[\sqrt{-5}]$ αλλά *όχι πρώτο* στοιχείο αυτού. Αυτό σε αντίθεση προς την περιοχή του Gauss.

Γιατί συμβαίνει αυτό;

Απάντηση: Η περιοχή $\mathbb{Z}[\sqrt{-5}]$ δεν είναι *περιοχή μονοσήμαντης ανάλυσης*. Αποτελεί εύκολη άσκηση η απόδειξη ότι ο

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

έχει δύο διαφορετικές μεταξύ τους γνήσιες αναλύσεις σε γινόμενα

Το τελευταίο θεώρημα του Fermat

Το τελευταίο θεώρημα του Fermat

Cubum in duos cubos aut quadro-quadratum in duos quadro-quadratos et generaliter nullam in infinitum, ultra quadratum, potestam in duas ejusdem nominis fas est dividere. Cujus rei demonstrationem mirabilem sone detexi, hanc marginis exiguitas non caperet

Η διοφαντική εξίσωση

$$X^n + Y^n = Z^n,\ n \in \mathbb{N}, n \geq 3$$

δεν έχει, μη-τετριμμένη, δηλαδή για $xyz \neq 0$, ακέραια λύση. Δεν υπάρχει επομένως τριάδα ακεραίων $(x, y, z) \in \mathbb{Z}^3$ με $xyz \neq 0$, τέτοια ώστε

$$x^n + y^n = z^n,$$

για οποιοδήποτε εκθέτη $n \geq 3$.

Η γέννηση της Αλγεβρικής Θεωρίας Αριθμών

Ο Kummer στα 1837 δέχθηκε ότι ο δακτύλιος

$$\mathbb{Z}[\zeta_p] = \{a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta^{p-2} : a_i \in \mathbb{Z}, i = 0, 1, \ldots, p-1\}$$

είναι περιοχή μονοσήμαντης ανάλυσης, απέδειξε ότι οι $X + \zeta_p^{\mu} Y$ είναι πρώτοι μεταξύ τους ανά δύο, συνεπώς κάθε παράγοντας του γινομένου έχει τη μορφή $\epsilon\alpha^p$, όπου $\alpha \in \mathbb{Z}[\zeta_p]$, ϵ είναι μονάδα του $\mathbb{Z}[\zeta_p]$ και με αυτόν τον τρόπο «απέδειξε» την εικασία Fermat.

Η γέννηση της Αλγεβρικής Θεωρίας Αριθμών

Ο Kummer στην προσπάθειά του να διορθώσει το λάθος του εισήγαγε τους «ιδεώδεις αριθμούς» και κατάφερε να αποδείξει την εικασία του Fermat για τους λεγόμενους «ομαλούς». Περισσότερο συγκεκριμένα, οι μέθοδοι του Kummer αποδεικνύουν την εικασία για όλους τους πρώτους $p < 100$ εκτός από τους $p \neq 37, 59, 67$.

Αλγεβρικά σώματα αριθμών

Ένα σώμα K θα λέγεται αλγεβρικό σώμα αριθμών ακριβώς τότε όταν το K είναι υπόσωμα του $\mathbb{C}$ και $[K : \mathbb{Q}] < \infty$.

Έστω R_K ο δακτύλιος των ακεραίων αλγεβρικών αριθμών του σώματος K, δηλαδή στοιχείων του K τα οποία ικανοποιούν μια μονική εξίσωση με συντελεστές από το K.

Θεώρημα: Ο δακτύλιος R_K είναι *δακτύλιος του Dedekind*, δηλαδή κάθε ιδεώδες του R_K αναλύεται μονοσήμαντα σε γινόμενο πρώτων ιδεωδών αυτού.

Ο δακτύλιος R_K είναι μια ελεύθερη αβελιανή ομάδα δηλαδή υπάρχουν στοιχεία $a_1, \dots, a_n \in R_K$ ώστε

$$R_k = \mathbb{Z}a_1 \oplus \cdots \oplus a_n\mathbb{Z}.$$

Η ομάδα κλάσεων είναι η ομάδα πηλίκο των κλασματικών ιδεωδών προς τα κύρια κλασματικά ιδεώδη. Είναι πεπερασμένη και αποτελεί ένα μέτρο από το πόσο απέχει ο δακτύλιος από το να είναι περιοχή κυρίων ιδεωδών.

Αν p πρώτος του $\mathbb{Z}$, τότε το pR_K είναι ένα κύριο ιδεώδες του R_K το οποίο δέχεται μονοσήμαντη ανάλυση σε πρώτους:

$$pR_K = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_r^{e_r}$$

Νόμος Ανάλυσης: Έστω K αλγεβρικό σώμα αριθμών, $[K : \mathbb{Q}] = n$ και έστω p πρώτος αριθμός, $p \nmid [R_K : \mathbb{Z}[\theta]$ και $f(x) = \mathrm{Irr}(\theta, \mathbb{Q})$. Αν

$$\bar{f}(x) = \bar{f}_1(x)^{e_1} \bar{f}_2(x)^{e_2} \cdots \bar{f}_g(x)^{e_g}$$

είναι η μονοσήμαντη ανάλυση του $\bar{f}(x)$ σε γινόμενο αναγώγων πολυωνύμων του δακτυλίου $\mathbb{F}_p[x]$ τότε ισχύει

$$pR_K = \mathfrak{P}_1^{e_1} \mathfrak{P}_2^{e_2} \cdots \mathfrak{P}_g^{e_g},$$

όπου $\mathfrak{P}_i$ πρώτα ιδεώδη του R_K και μάλιστα $\mathfrak{P}_i = \langle p_i, f_i(\theta) \rangle = pR_K + f_i(\theta) R_K$ για $i = 1, 2, \ldots, g$.

Θεώρημα Μονάδων του Dirichlet Για κάθε αλγεβρικό σώμα αριθμών K υπάρχει ένας φυσικός $r = r(K)$ και μονάδες $\epsilon_1, \epsilon_2, \dots, \epsilon_r$ του R_K (λέγονται θεμελιώδεις μονάδες) έτσι ώστε κάθε μονάδα του R_K να έχει μία μονοσήμαντη παράσταση της μορφής

$$\epsilon = \zeta^s \epsilon_1^{s_1} \epsilon_2^{s_2} \cdots \epsilon_r^{s_r},$$

όπου $s, s_1, s_2, \dots, s_r$ φυσικοί αριθμοί και ζ μία ρίζα της μονάδας του σώματος K.

Η εξίσωση Fermat

Μπορεί να αποδειχθεί ότι η αρχική απόδειξη του Kummer δουλεύει για τις εξισώσεις Fermat, $x^p + y^p = z^p$ αρκεί ο πρώτος p να μην διαιρεί την τάξη του κυκλοτομικού σώματος $\mathbb{Q}(\zeta_p)$. Τους πρώτους αυτούς τους ονομάζουμε «ομαλούς».

Ένας πρώτος p διαιρεί τον αριθμητή της $\zeta(r)$ για ένα περιττό αρνητικό ακέραιο r αν και μόνο αν ο p δεν είναι ομαλός.

Για παράδειγμα η τάξη της ομάδας κλάσεων του $\mathbb{Q}(\zeta_{691})$ διαιρείται από το 691 αφού το $\zeta(-11) = \frac{691}{2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13}$.

Ζήτα συναρτήσεις

Για ένα ιδεώδες $A \lhd R_K$ θα συμβολίζουμε με $N(A) = \#R_K/A$.

Ορίζουμε

$$\zeta_K(s) = \sum_{A \in I_K} \frac{1}{N(A)^s}, \qquad s \in \mathbb{C}, \mathrm{Re}(s) > 1.$$

$$\zeta_K(s) = \prod_{P \in \mathbb{P}(K)} \frac{1}{1 - N(P)^{-s}}.$$

$$\mathrm{Res}_{s=1}\zeta_K(s) = \lim_{s \to 1^+} \zeta_K(s) = \frac{2^s(2\pi^t)\mathrm{Reg}_K}{w\sqrt{|D_K|}} h_K.$$

Παράδειγμα

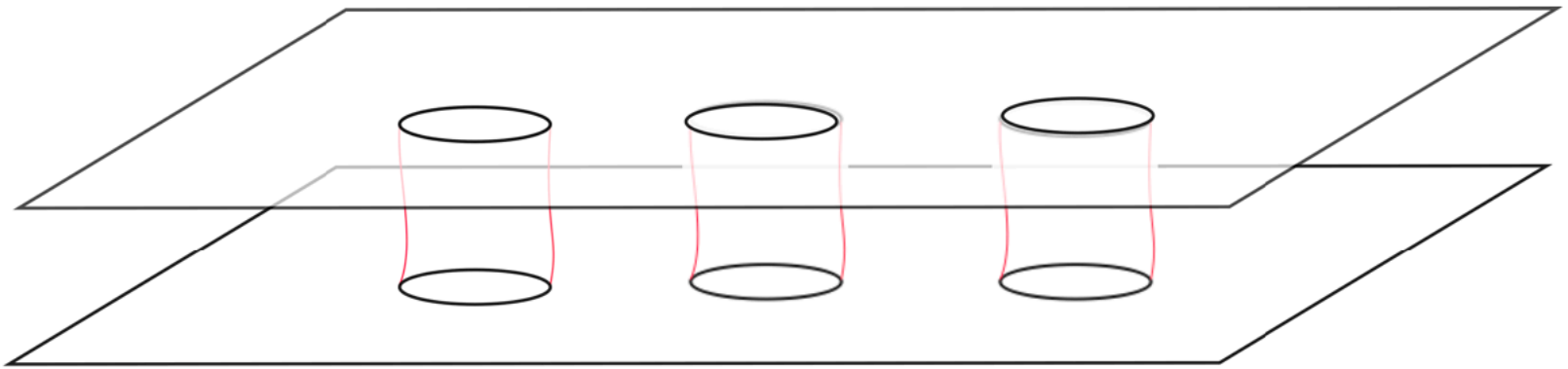
$$x^2 + y^2 = 1$$

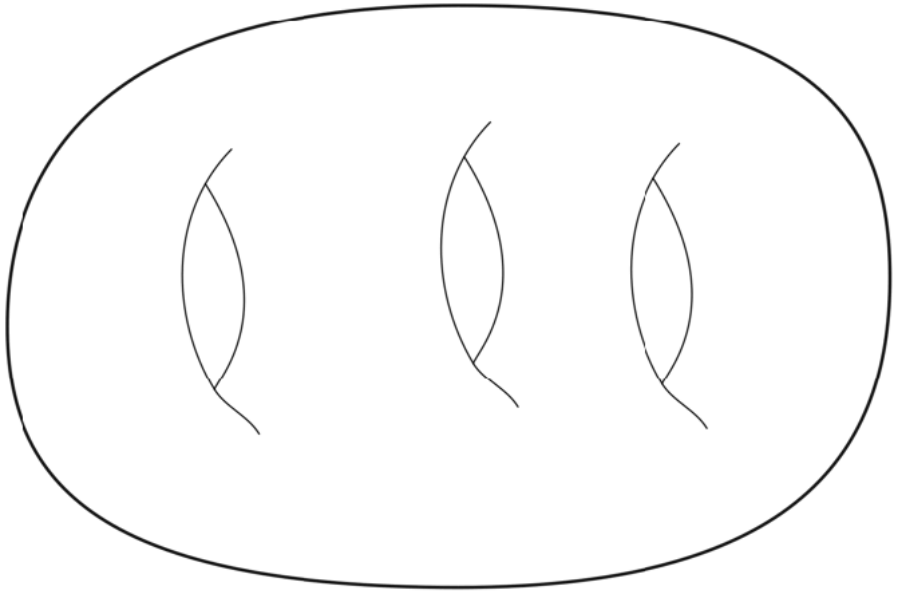
Ορίζει ένα γεωμετρικό σύνολο ως τόπο μηδενισμού. Το σύνολο αυτό αντιστοιχεί σε ένα δακτύλιο φυσιολογικών συναρτήσεων πάνω στο αντικείμενο.

$$k[x, y]/\langle x^2 + y^2 - 1\rangle.$$

Επίσης ορίζεται μια επέκταση σωμάτων $k(x)[\sqrt[2]{1 - x^2}]/k(x)$.

Αλγεβρικές Καμπύλες





Αλγεβρικές Καμπύλες

Γενικότερα θεωρούμε ένα πολυώνυμο δύο μεταβλητών

$$P(x, y) : y^2 - Q(x),$$

όπου το πολυώνυμο $Q(x) \in \mathbb{C}[x]$ πολυώνυμο με απλές ρίζες. Θα θέλαμε να περιγράψουμε τον τόπο μηδενισμού του παραπάνω πολυωνύμου ως υποσύνολο του $\mathbb{C} \times \mathbb{C}$. Ακολουθώντας τον Riemann θεωρούμε το $x \in \mathbb{C}$ ως ελεύθερη μεταβλητή. Για κάθε x έχουμε δύο μιγαδικές τιμές για το y διαφορετικές μεταξύ τους, εκτός από τις πεπερασμένες το πλήθος τιμές του x στις οποίες το Q μηδενίζεται. Συνεπώς μπορούμε να φανταστούμε το σύνολο μηδενισμού του πολυωνύμου $P(x, y)$ ως δύο αντίγραφα του μιγαδικού επιπέδου τα οποία κολλάνε μεταξύ τους στις ρίζες του $Q(x)$. Αν δε θεωρήσουμε αντί για τον τόπο μηδενισμού του $P(x, y)$ τον τόπο μηδενισμού του ομογενοποιημένου πολυώνυμου ως υποσύνολο του προβολικού επιπέδου, καταλήγουμε σε μία συμπαγή επιφάνεια Riemann, με χερούλια.

Διοφαντικές Εξισώσεις Ξανά

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

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

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

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

Διοφαντικές Εξισώσεις Ξανά

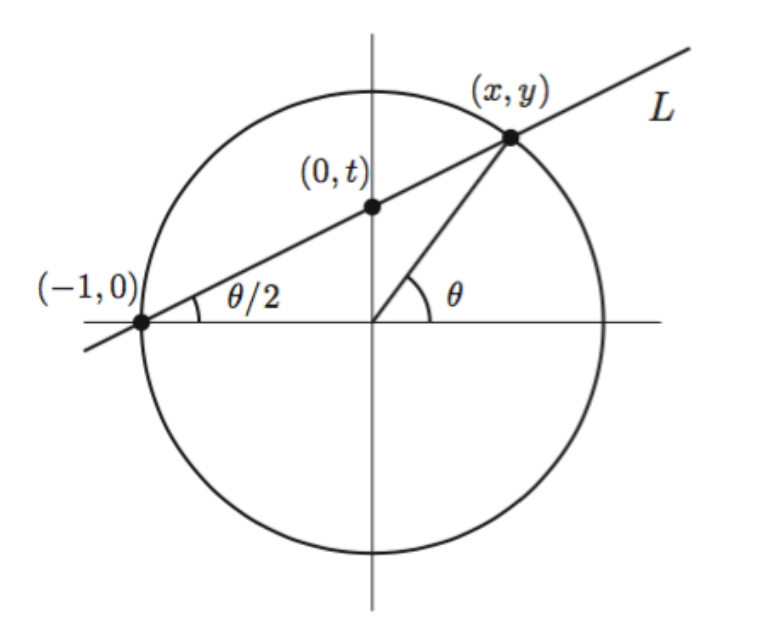
Η γραμμική εξίσωση $aX + bY + cZ = 0$ ή ισοδύναμα η $ax + by + c = 0$ είναι εύκολο να λυθεί.

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

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

Τετραγωνικές εξισώσεις



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:

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

Τετραγωνικές εξισώσεις

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 $t = \infty$.

Πυθαγόρειες τριάδες

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

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

Plimton

Σχήμα 3: Βαβυλωνιακή επιγραφή με Πυθαγόρειες Τριάδες γνωστή ως Plimpton 322

Γενική τετραγωνική εξίσωση

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.

Ύπαρξη λύσης τετραγωνικής εξίσωσης

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.

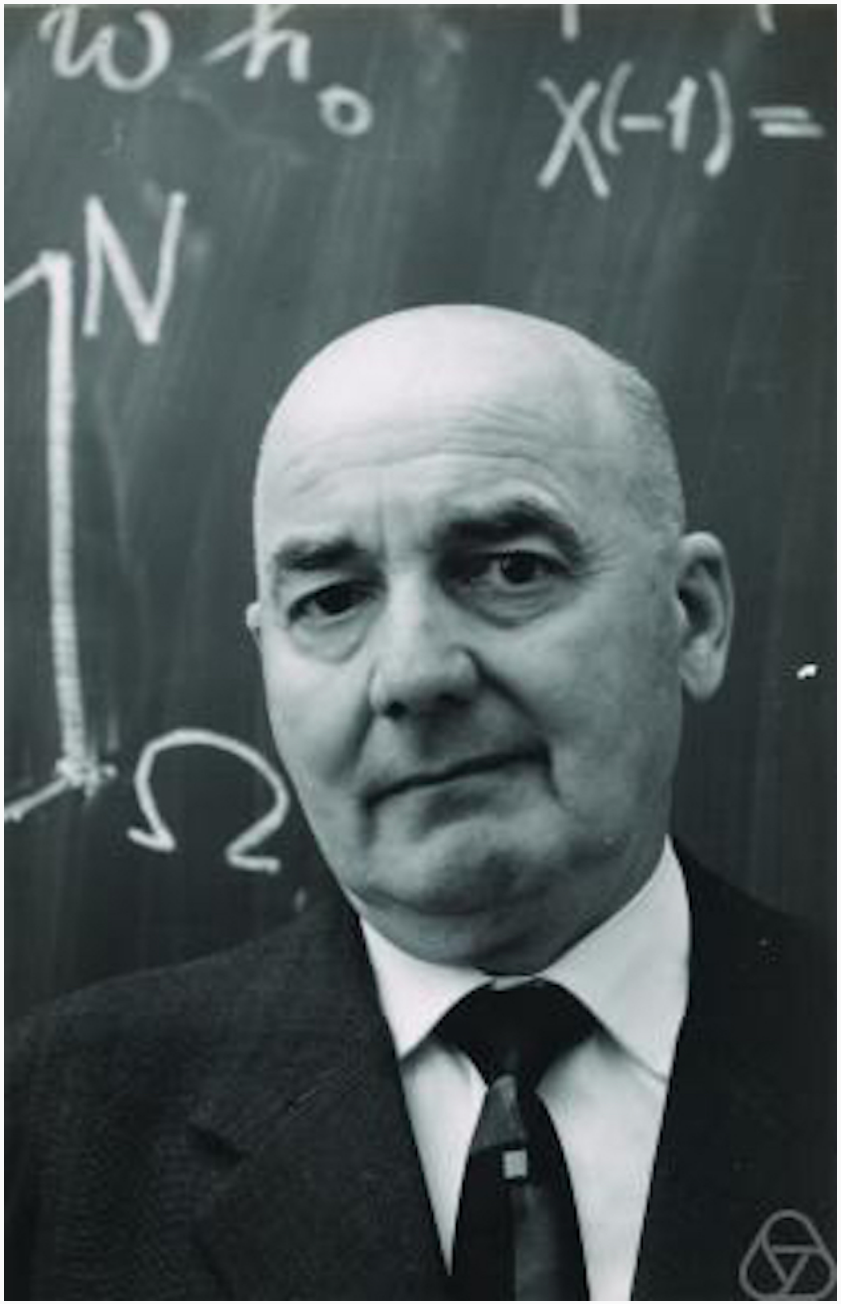
Η αρχή του τοπικού-γενικού (local global principle)

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



Αριθμητική ανάλυση

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

Το θεώρημα τοπικού-καθολικού

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.

Τριγωνομετρία

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)

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

```
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
```

Υπολογισμός ολοκληρωμάτων

Αν θέσουμε $\theta = 2\arctan(t)$ έχουμε $d\theta = \frac{2dt}{1+t^2}$. 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 t το οποίο υπολογίζεται με την βοήθεια στοιχειωδών συναρτήσεων.

Υπολογισμός ολοκληρωμάτων

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

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

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

Συγκρίσεις

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
```

Ενιαία συμπεριφορά τετραγωνικών εξισώσεων.

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 $\lambda \neq 0$.

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.

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 $f(x, y), z = 1$.

Αποομογενοποίηση

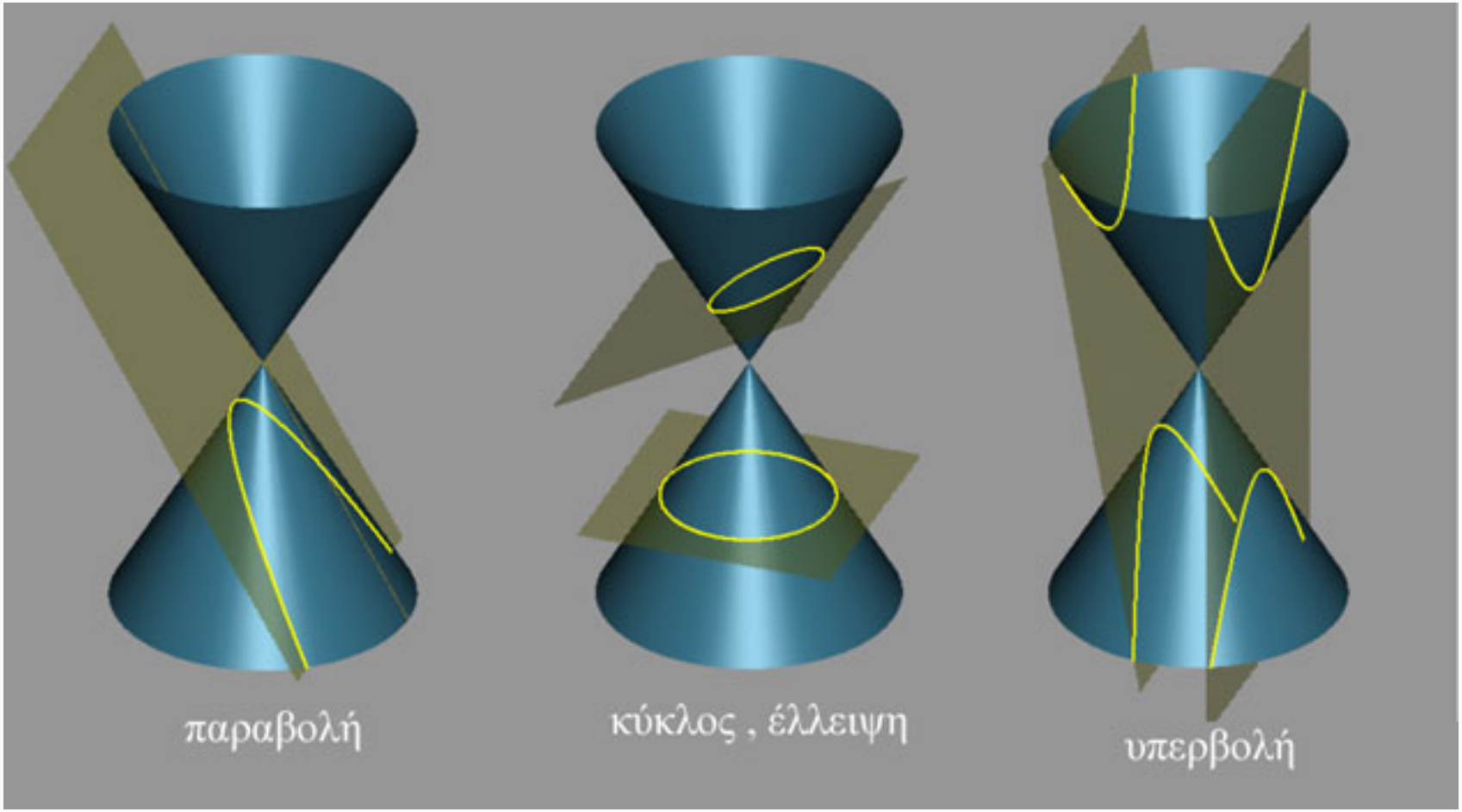
Είναι η αντίστροφη διαδικασία. Από ένα ομογενές πολυώνυμο καταλήγουμε σε ένα μη ομογενές θέτοντας $Z = 1$. Φυσικά θα μπορούσαμε να αποομογενοποίησουμε θέτοντας $\mathrm{X} = 1$ ή $Y = 1$, ή ακόμα να θεωρήσουμε την τομή με οποιοδήποτε άλλο επίπεδο.

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

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

Κωνικές Τομές

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

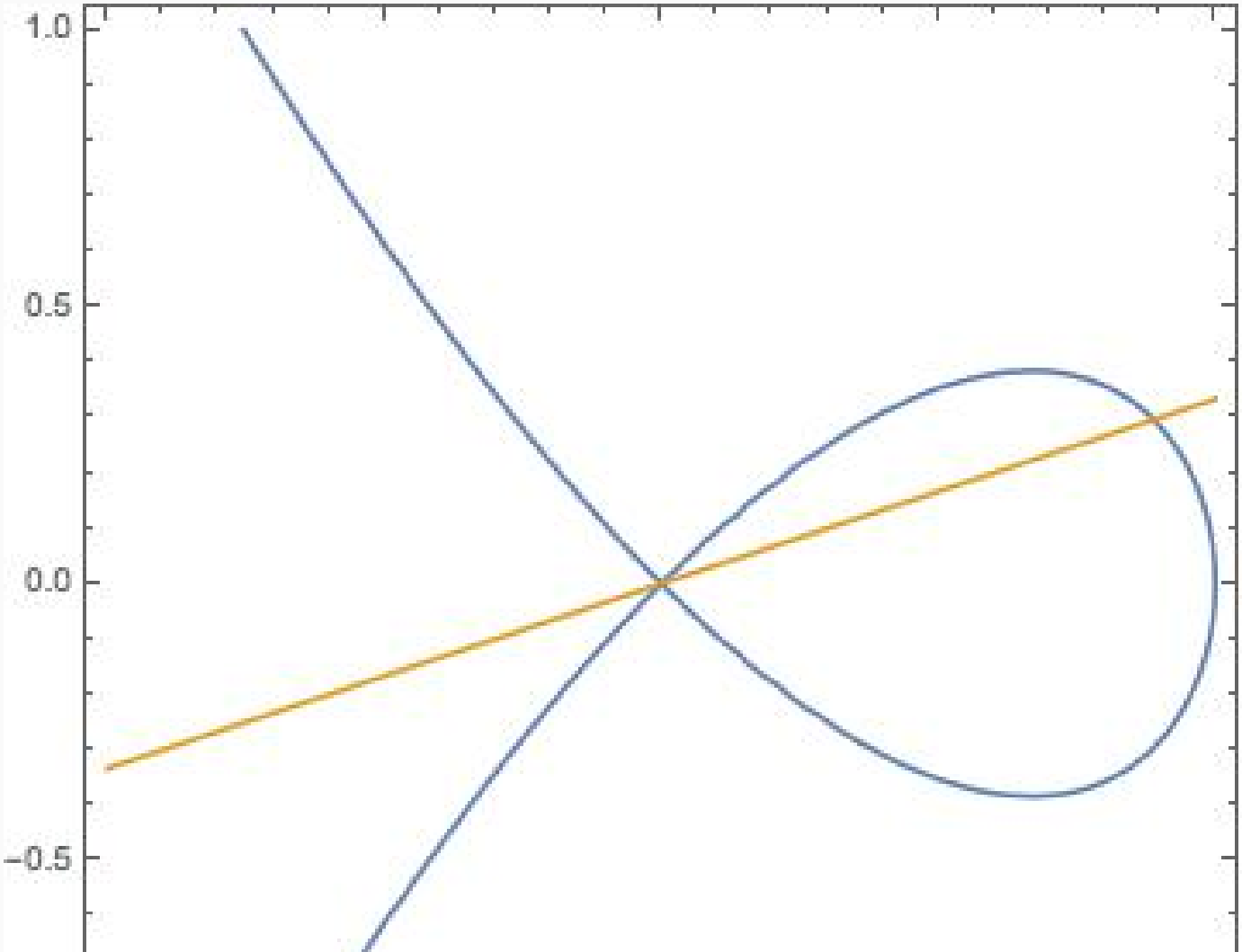


Σχήμα 5: Κωνικές Τομές

Μία ακόμα ρητή καμπύλη

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

Καμπύλη $y^2 = x^2 - x^3$.



Μία ακόμα ρητή καμπύλη

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

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

Ελλειπτικά Ολοκληρώματα

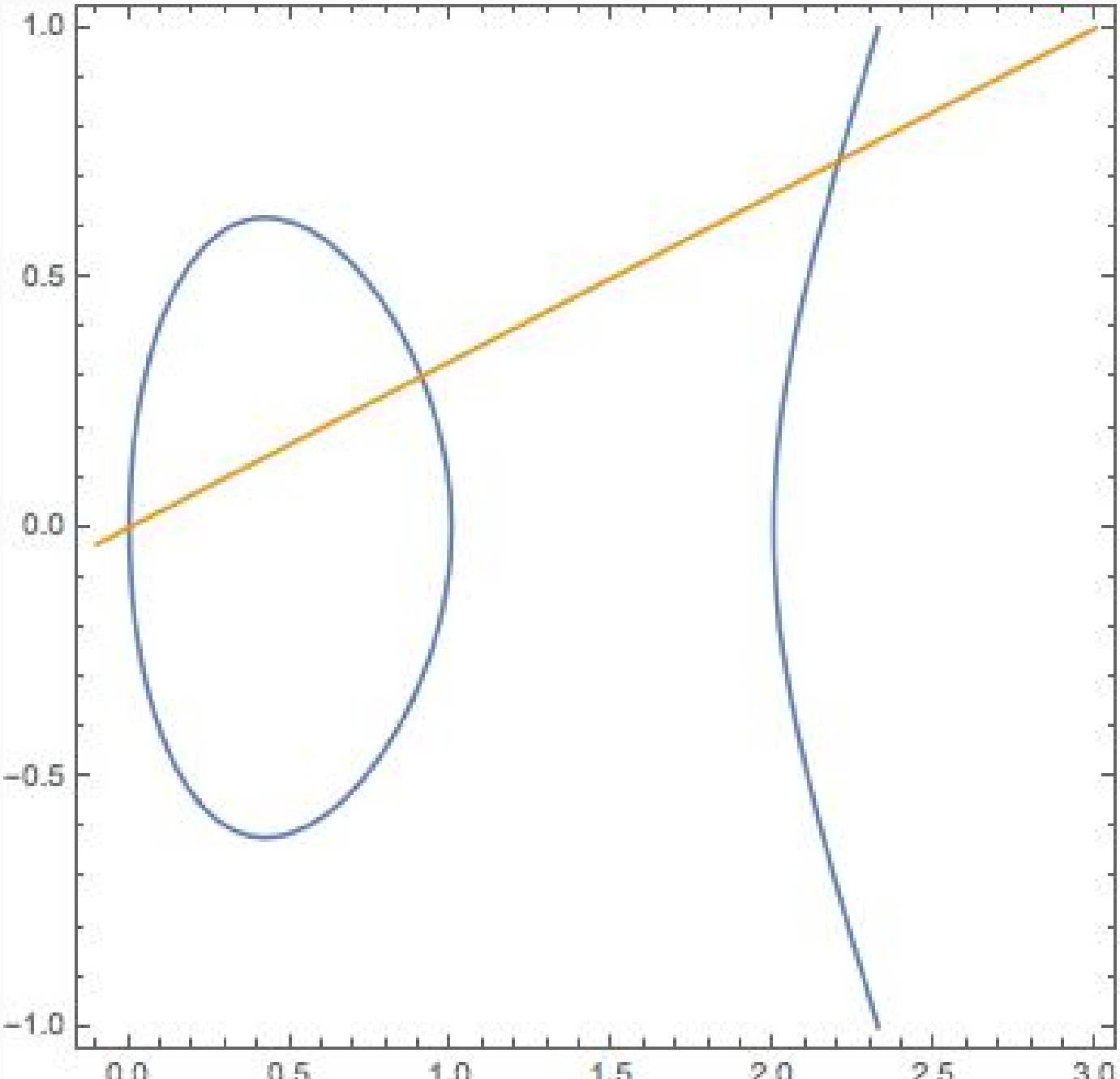
Υπολογισμός του ολοκληρώματος

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

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 $(0, 0)$.

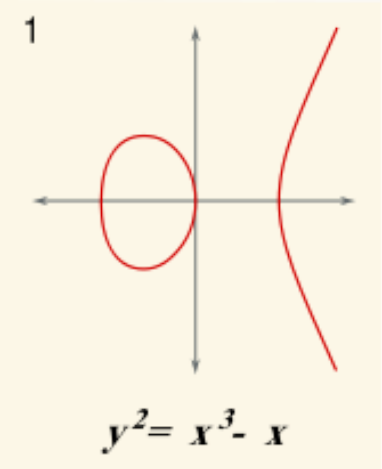
Ελλειπτικά Ολοκληρώματα

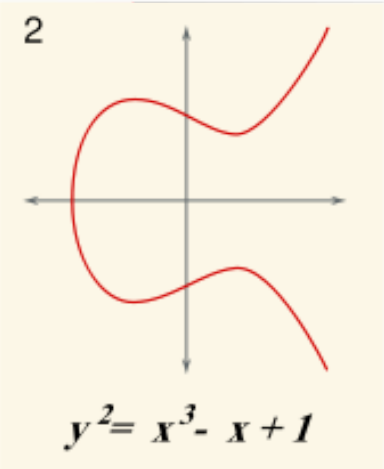


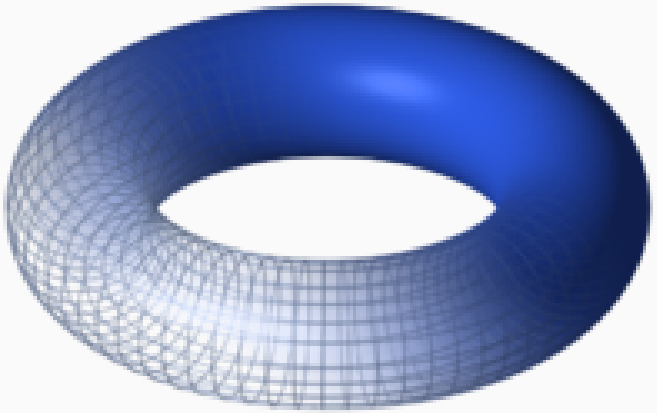
Ελλειπτικές Καμπύλες

Μια ελλειπτική καμπύλη πάνω από ένα σώμα K είναι μια καμπύλη που δίνεται από την εξίσωση

$$E : y^2 = x^3 + ax + b \text{ ώστε } 4a^3 + 27b^2 \neq 0.$$







Το σύνολο των λύσεων $E(K)$ μαζί με ένα επ' άπειρο σημείο είναι αβελιανή ομάδα.

Weierstrass

Υπολογισμός

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

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

Υπολογισμός

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

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

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

Σύγκριση με την υπερβατική παραμέτριση του κύκλου

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.

Σύνολα κλάσεων ισοδυναμίας

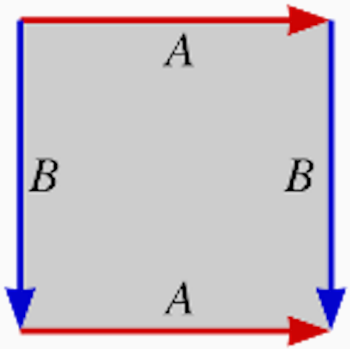
Επιπλέον ο κύκλος είναι το πηλίκο του $\mathbb{R}/2\pi\mathbb{Z}$, ενώ η καμπύλη είναι πηλίκο του

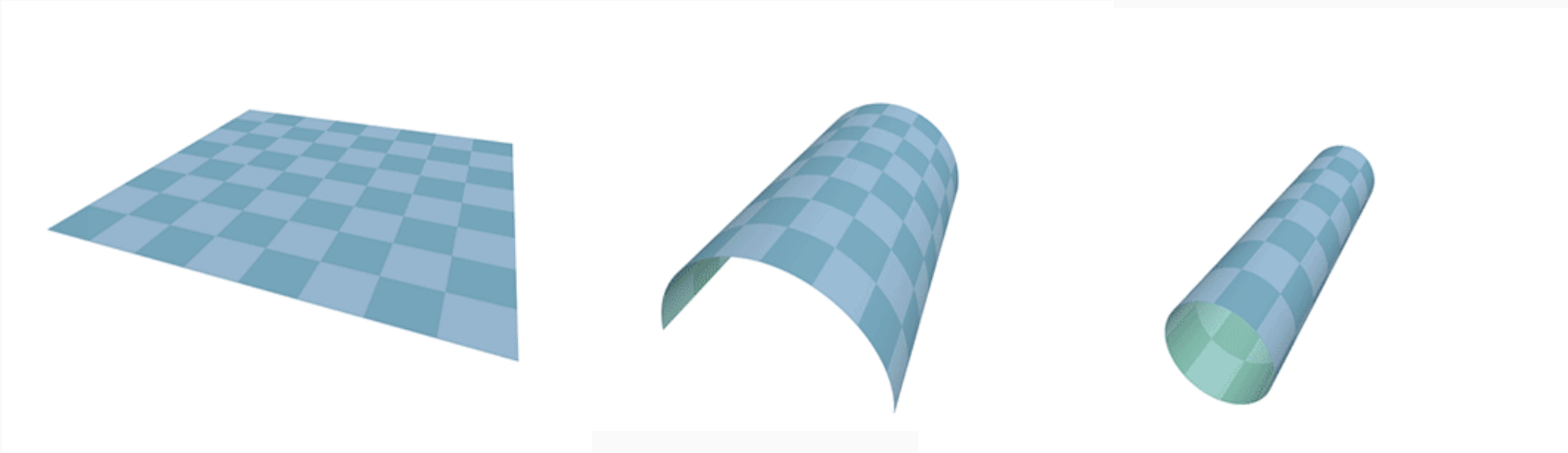
$$\mathbb{C}\backslash\{0\}/L,$$

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

Τοπολογική μορφή





Θεώρημα Poincare

Ισχύει ότι

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

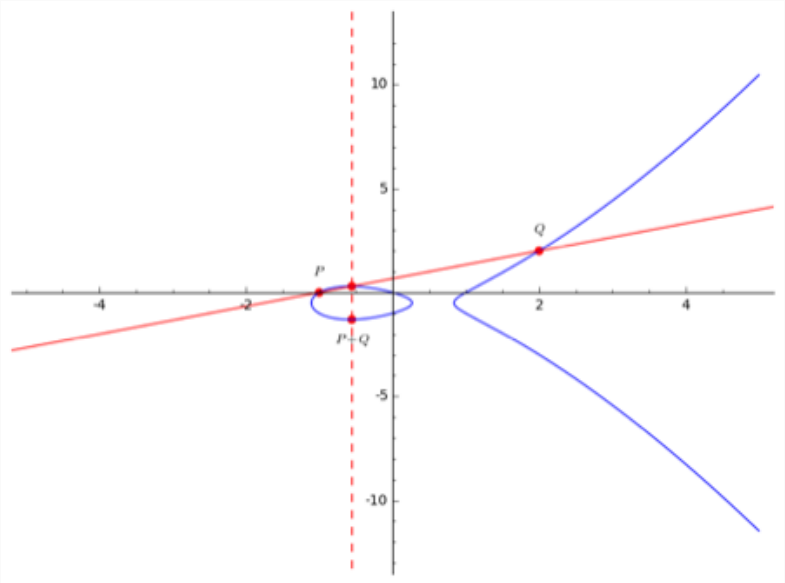
όπου $u + v + w = 0$.

Οι πράξεις δίνονται με αλγεβρικό τρόπο.

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 9: Πρόσθεση δύο σημείων ελλειπτικής καμπύλης

Αλγεβρικός τύπος πρόσθεσης σημείων

$P = (x_1, y_1), Q = (x_2, y_2)$ 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.

Αλγεβρικός τύπος πρόσθεσης σημείων

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:

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

Λύση διοφαντικών εξισώσεων.

Οι ρητές λύσεις μιας κυβικής ελλειπτικής καμπύλης αποτελούν ομάδα.

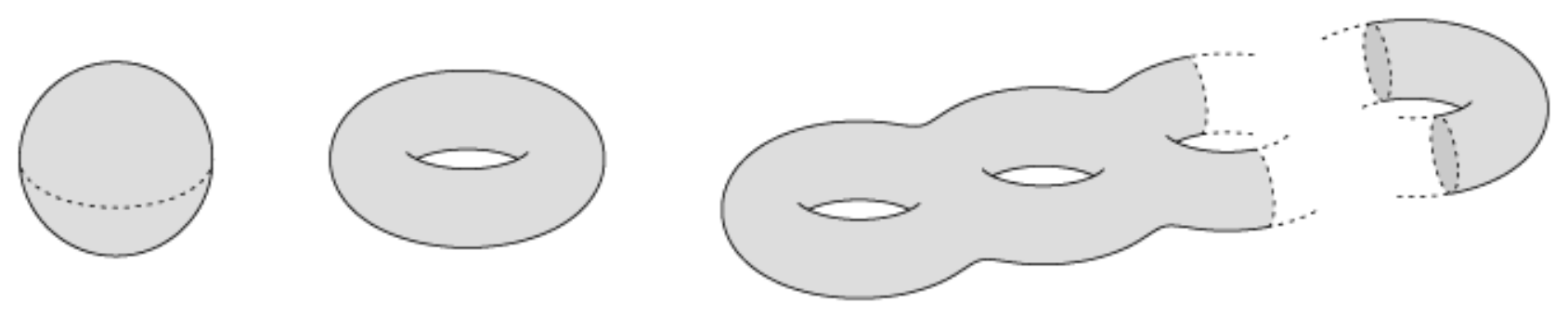
Θεώρημα Mordell Η ομάδα των σημείων $E(\mathbb{Q})$ είναι μια πεπερασμένα παραγόμενη αβελιανή ομάδα. Δηλαδή

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

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

Η γενική περίπτωση

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 εικασία του Mordell

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

Σχήμα 10: G. Faltings

Το τελευταίο θεώρημα 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.

Μέτρημα σημείων σε αλγεβρικές καμπύλες πάνω από πεπερασμένα σώματα. Ζήτα συναρτήσεις, η εικασία του Riemann και η τοπολογική οπτική του A. Weil.

Γενίκες Διοφαντικές εξισώσεις

Γενικότερα μια διοφαντική εξίσωση ορίζεται ως το σύνολο μηδενισμού ενός συνόλου ομογενών πολυωνύμων που παράγεται από τα $f_1, \dots, f_r \in [x_1, \dots, x_r]$. Γεωμετρικά το σύνολο αυτό βρίσκεται μέσα σε ένα προβολικό χώρο.

Θεωρούμε το πλήθος των λύσεων N_r πάνω από κάθε σώμα $\mathbb{F}_{p^r}$. Σχηματίζουμε την «γεννήτρια συνάρτηση»:

$$Z(X,t) = \exp\left(\sum_{r=1}^{\infty} N_r \frac{t^r}{r}\right) \in \mathbb{Q}[[t]].$$

Παράδειγμα
$X = \mathbb{P}^1$, $N_r = \#\mathbb{P}^1(\mathbb{F}_{p^r}) = p^r + 1$.

$$Z(\mathbb{P}^1, t) = \exp\left(\sum_{r=1}^{\infty} (q^r + 1)\frac{t^r}{r}\right) = \frac{1}{(1-t)(1-qt)}.$$

Εικασίες του Weil

1. Η $Z(X,t)$ είναι ρητή συνάρτηση του t.
2. $Z(X, 1/q^n t) = \pm q^{nE/2} t^E Z(X,t)$, $E = \Delta \cdot \Delta, \Delta \subset X \times X$.
3. $P_0(t) = 1 - t$, $P_{2n} = 1 - q^n t$ και για κάθε $1 \leq i \leq 2n-1$, $P_i(t) \in [t]$,

$$P_i(t) = \prod_j (1 - a_{ij} t) \text{ με } |a_{ij}| = q^{1/2}.$$

$$Z(X,t) = \frac{P_1(t) P_3(t) \cdots P_{2n-1}(t)}{P_0(t) P_2(t) \cdots P_{2n}(t)}$$

Θεωρούμε το $x \in \bar{\mathbb{F}}_p$. Είναι γνωστό ότι

$$f : x \in \mathbb{F}_{p^r} \Leftrightarrow x^{p^r} = x.$$

Τα σταθερά σημεία του μορφισμού του Frobenious $x \mapsto x^{p^r}$ του συνόλου V είναι οι λύσεις που ζητάμε.

Τύπος σταθερών σημείων του Lefschetz

$$N_r = \sum_{i=0}^{2n} (-1)^i \mathrm{Tr}(f^{r*}; H^i(X, \mathbb{Q}_l)).$$

Λήμμα
Αν ϕ ενδομορφισμός πεπερασμένης διάστασης διανυσματικού χώρου

$$\exp\left(\sum_{r=1}^{\infty} Tr(\phi^r; V)\frac{t^r}{r}\right) = \det(1 - \phi t; V)^{-1}$$

Απόδειξη του Λήμματος
Αν $\dim(V) = 1$ τότε

$$\exp\left(\sum_{r=1}^{\infty} \lambda^r \frac{t^r}{r}\right) = \frac{1}{1-\lambda t}$$

Επαγωγή.

Απόδειξη εικασιών του Weil
Ρητή συνάρτηση: Λήμμα, τύπος σταθερού σημείου του Lefschetz.

$$P_i(t) = \det(1 - f^* t; H^i(X, \mathbb{Q}_l)).$$

Συναρτησιακή εξίσωση:Poincare duality!

Εξειδίκευση στις Καμπύλες

Θεωρούμε την καμπύλη X γένους g.

$$N_r = 1 - a_r + q^r.$$

τότε

$$|a_r| \leq 2g\sqrt{q^r}$$

$$Z(X,t) = \frac{P_1(t)}{(1-t)(1-qt)}.$$

Καμπύλες με μέγιστο πλήθος σημείων ονομάζονται «μέγιστες» και ο υπολογισμός τους ενδιαφέρει την Θεωρία κωδίκων - Geometric Goppa Codes.

A. Weil -A. Grothendieck - P. Deligne

Ευχαριστώ πολύ!

Ευχαριστώ πολύ!