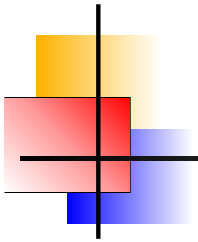
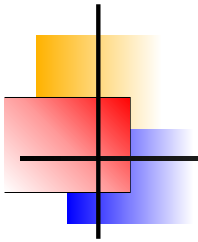


Διοφαντικές εξισώσεις, Θεωρία κλάσεων σωμάτων, κρυπτογραφία

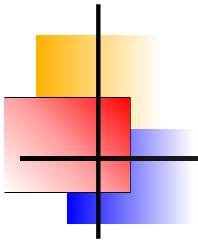
Αριστείδης Κοντογεώργης

Τμήμα Μαθηματικών
Πανεπιστημίου Αθηνών.

Σεμινάριο Τομέα Άλγεβρας και Γεωμετρίας 30/10/2012



Περιεχόμενα



Μία απλή περίπτωση

Θεωρούμε ένα πολυώνυμο $f(x, y) \in \mathbb{Z}[x, y]$.

Στόχος Να βρεθούν οι ρητές λύσεις, δηλαδή τα ζευγάρια

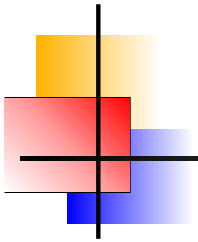
$$\{(x, y) \in \mathbb{Q}^2 : \text{ ώστε } f(x, y) = 0\}.$$

Ισοδύναμα να βρεθούν οι λύσεις του ομογενοποιημένου πολυωνύμου $F(x, y, z) \in \mathbb{Z}[x, y, z]$

$$\{(x, y, z) \in \mathbb{Z}^3 : \text{ ώστε } f(x, y, z) = 0\}.$$

Παράδειγμα

$$f(x, y) = x^n + y^n + 1 = 0, F(x, y, z) = x^n + y^n + z^n = 0.$$



Μία απλή περίπτωση

Θεωρούμε ένα πολυώνυμο $f(x, y) \in \mathbb{Z}[x, y]$.

Στόχος Να βρεθούν οι ρητές λύσεις, δηλαδή τα ζευγάρια

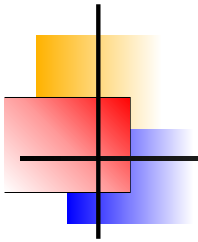
$$\{(x, y) \in \mathbb{Q}^2 : \text{ ώστε } f(x, y) = 0\}.$$

Ισοδύναμα να βρεθούν οι λύσεις του ομογενοποιημένου πολυωνύμου $F(x, y, z) \in \mathbb{Z}[x, y, z]$

$$\{(x, y, z) \in \mathbb{Z}^3 : \text{ ώστε } f(x, y, z) = 0\}.$$

Παράδειγμα

$$f(x, y) = x^n + y^n + 1 = 0, F(x, y, z) = x^n + y^n + z^n = 0.$$



Μία απλή περίπτωση

Θεωρούμε ένα πολυώνυμο $f(x, y) \in \mathbb{Z}[x, y]$.

Στόχος Να βρεθούν οι ρητές λύσεις, δηλαδή τα ζευγάρια

$$\{(x, y) \in \mathbb{Q}^2 : \text{ ώστε } f(x, y) = 0\}.$$

Ισοδύναμα να βρεθούν οι λύσεις του ομογενοποιημένου πολυωνύμου $F(x, y, z) \in \mathbb{Z}[x, y, z]$

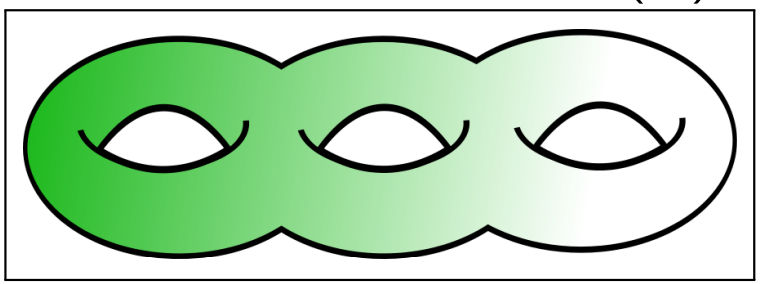
$$\{(x, y, z) \in \mathbb{Z}^3 : \text{ ώστε } f(x, y, z) = 0\}.$$

Παράδειγμα

$$f(x, y) = x^n + y^n + 1 = 0, F(x, y, z) = x^n + y^n + z^n = 0.$$

Αριθμητική Γεωμετρία

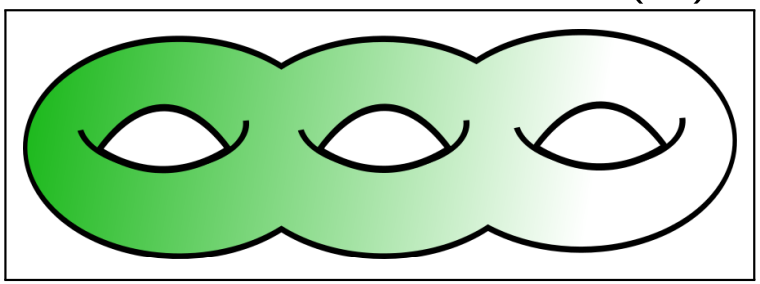
Κάθε ομογενές πολυώνυμο καθορίζει μια συμπαγή επιφάνεια Riemann στο προβολικό επίπεδο $\mathbb{P}^2(\mathbb{C})$ η οποία έχει ένα τοπολογικό γένος g.



Η τοπολογία καθορίζει το πλήθος των λύσεων

1. $g = 0$ Η Διοφαντική εξίσωση έχει καμία ή άπειρες λύσεις.
2. $g = 1$ Το σύνολο λύσεων έχει δομή πεπερασμένα παραγόμενης αβελιανής ομάδας $\mathbb{Z}^r \times \text{torsion}$ (Θεώρημα Mordell)
3. $g \geq 2$ Το σύνολο λύσεων είναι πεπερασμένο. (Εικασία Mordell, Faltings 1984).

Κάθε ομογενές πολυώνυμο καθορίζει μια συμπαγή επιφάνεια Riemann στο προβολικό επίπεδο $\mathbb{P}^2(\mathbb{C})$ η οποία έχει ένα τοπολογικό γένος g.



Η τοπολογία καθορίζει το πλήθος των λύσεων

1. $g = 0$ Η Διοφαντική εξίσωση έχει καμία ή άπειρες λύσεις.
2. $g = 1$ Το σύνολο λύσεων έχει δομή πεπερασμένα παραγόμενης αβελιανής ομάδας $\mathbb{Z}^r \times \text{torsion}$ (Θεώρημα Mordell)
3. $g \geq 2$ Το σύνολο λύσεων είναι πεπερασμένο. (Εικασία Mordell, Faltings 1984).

Ιδέα: λύσεις modulo p^r

Λύνουμε την διοφαντική εξίσωση σε όλους τους δακτύλιους $\mathbb{Z}/p^r\mathbb{Z}$. Αν κάτι δεν λύνεται στο $\mathbb{Z}/p^r\mathbb{Z}$ δεν λύνεται και στο $\mathbb{Q}$.

Σύγκριση δακτυλίων:

$$\begin{aligned} \mathbb{C}[x] &\longleftrightarrow \mathbb{Z} \\ (x-a) &\longleftrightarrow p\mathbb{Z} \text{ πρώτα ιδεώδη} \\ \text{Απόκομα σειρών Taylor} &\longleftrightarrow \mathbb{Z}/p^r\mathbb{Z} \\ \mathbb{C}[[x]] = \varprojlim \mathbb{C}[x]/(x-a)^n &\longleftrightarrow \mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z} \end{aligned}$$

Το σώμα $\mathbb{Q}_p = \mathrm{Quot}(\mathbb{Z}_p)$ είναι η πλήρωση του $\mathbb{Q}$ ως προς την p-αδική μετρική.

Ιδέα: λύσεις modulo p^r

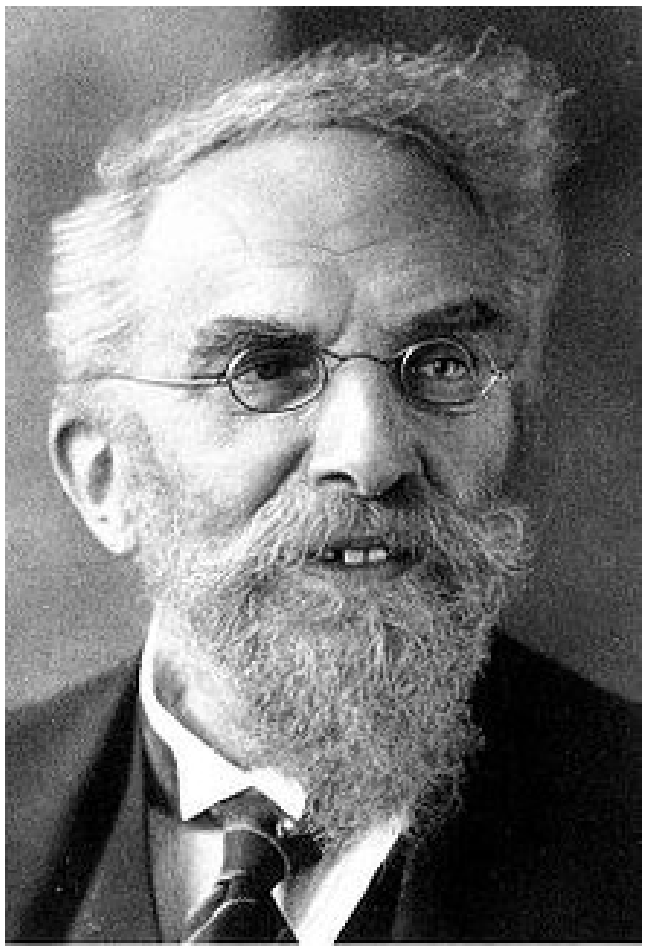
Λύνουμε την διοφαντική εξίσωση σε όλους τους δακτύλιους $\mathbb{Z}/p^r\mathbb{Z}$. Αν κάτι δεν λύνεται στο $\mathbb{Z}/p^r\mathbb{Z}$ δεν λύνεται και στο $\mathbb{Q}$.

Σύγκριση δακτυλίων:

$$\begin{aligned} \mathbb{C}[x] &\longleftrightarrow \mathbb{Z} \\ (x-a) &\longleftrightarrow p\mathbb{Z} \text{ πρώτα ιδεώδη} \\ \text{Απόκομα σειρών Taylor} &\longleftrightarrow \mathbb{Z}/p^r\mathbb{Z} \\ \mathbb{C}[[x]] = \varprojlim \mathbb{C}[x]/(x-a)^n &\longleftrightarrow \mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z} \end{aligned}$$

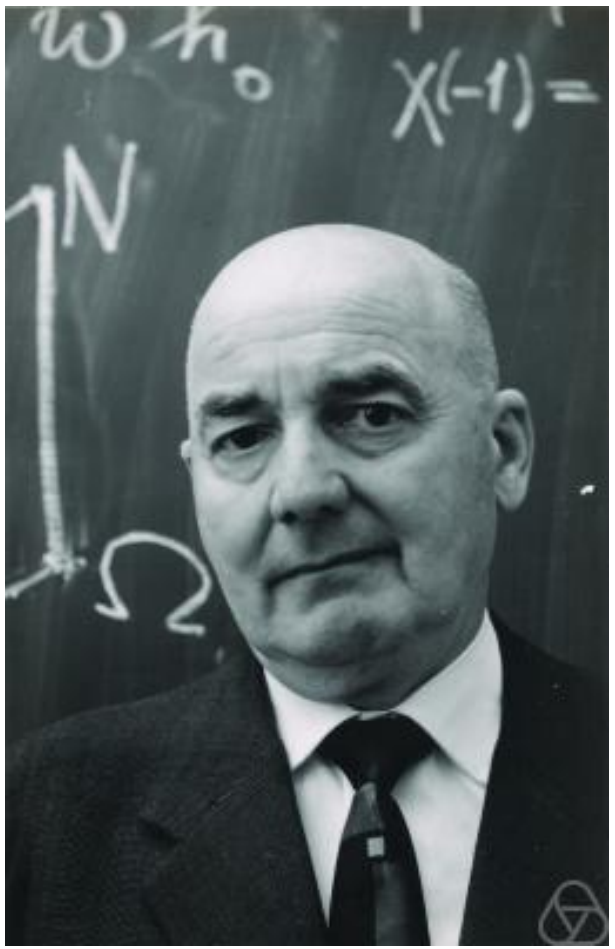
Το σώμα $\mathbb{Q}_p = \mathrm{Quot}(\mathbb{Z}_p)$ είναι η πλήρωση του $\mathbb{Q}$ ως προς την p-αδική μετρική.

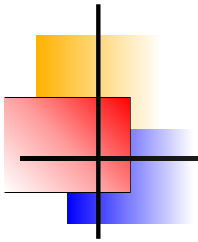
Πρόγονοι



Kurt Hensel

Helmut Hasse





Local Global Principle

Θεώρημα Hasse

Τετραγωνικές μορφές έχουν λύση στο $\mathbb{Q}$ αν και μόνο αν έχουν λύση σε κάθε $\mathbb{Q}_p$ και στο $\mathbb{R}$.

Τι καλό έχει αυτό;

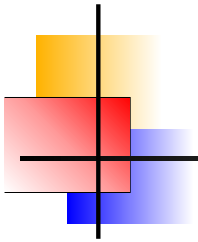
Μπορούμε να χρησιμοποιήσουμε μεθόδους αριθμητικής ανάλυσης (μέθοδος Νεύτωνα, επαναληπτικά σχήματα κτλ) για να δείξουμε ότι διοφαντικές εξισώσεις έχουν λύση.

Λήμμα Hensel - p-αδική μέθοδος Newton

Έστω $f(x) \in \mathbb{Z}_p[x]$. Αν $f(a_0) \equiv 0 \bmod p$ και $f'(a_0) \neq 0 \bmod p$, τότε υπάρχει μοναδικός $a \in \mathbb{Z}_p$ ώστε $f(a) = 0$ και $a \equiv a_0 \bmod p$.

Και για τις μη τετραγωνικές μορφές τι γίνεται;

Η θεωρία διαταραχών μας δίνει συγκεκριμένες obstructions σε ομάδες συνομολογίας ώστε η τοπική λύση να δίνει καθολική.



Local Global Principle

Θεώρημα Hasse

Τετραγωνικές μορφές έχουν λύση στο $\mathbb{Q}$ αν και μόνο αν έχουν λύση σε κάθε $\mathbb{Q}_p$ και στο $\mathbb{R}$.

Τι καλό έχει αυτό;

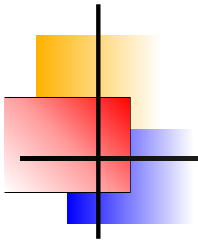
Μπορούμε να χρησιμοποιήσουμε μεθόδους αριθμητικής ανάλυσης (μέθοδος Νεύτωνα, επαναληπτικά σχήματα κτλ) για να δείξουμε ότι διοφαντικές εξισώσεις έχουν λύση.

Λήμμα Hensel - p-αδική μέθοδος Newton

Έστω $f(x) \in \mathbb{Z}_p[x]$. Αν $f(a_0) \equiv 0 \bmod p$ και $f'(a_0) \neq 0 \bmod p$, τότε υπάρχει μοναδικός $a \in \mathbb{Z}_p$ ώστε $f(a) = 0$ και $a \equiv a_0 \bmod p$.

Και για τις μη τετραγωνικές μορφές τι γίνεται;

Η θεωρία διαταραχών μας δίνει συγκεκριμένες obstructions σε ομάδες συνομολογίας ώστε η τοπική λύση να δίνει καθολική.



Local Global Principle

Θεώρημα Hasse

Τετραγωνικές μορφές έχουν λύση στο $\mathbb{Q}$ αν και μόνο αν έχουν λύση σε κάθε $\mathbb{Q}_p$ και στο $\mathbb{R}$.

Τι καλό έχει αυτό;

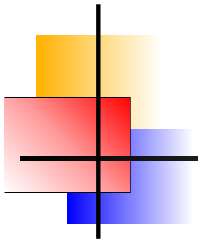
Μπορούμε να χρησιμοποιήσουμε μεθόδους αριθμητικής ανάλυσης (μέθοδος Νεύτωνα, επαναληπτικά σχήματα κτλ) για να δείξουμε ότι διοφαντικές εξισώσεις έχουν λύση.

Λήμμα Hensel - p-αδική μέθοδος Newton

Έστω $f(x) \in \mathbb{Z}_p[x]$. Αν $f(a_0) \equiv 0 \bmod p$ και $f'(a_0) \neq 0 \bmod p$, τότε υπάρχει μοναδικός $a \in \mathbb{Z}_p$ ώστε $f(a) = 0$ και $a \equiv a_0 \bmod p$.

Και για τις μη τετραγωνικές μορφές τι γίνεται;

Η θεωρία διαταραχών μας δίνει συγκεκριμένες obstructions σε ομάδες συνομολογίας ώστε η τοπική λύση να δίνει καθολική.



Local Global Principle

Θεώρημα Hasse

Τετραγωνικές μορφές έχουν λύση στο $\mathbb{Q}$ αν και μόνο αν έχουν λύση σε κάθε $\mathbb{Q}_p$ και στο $\mathbb{R}$.

Τι καλό έχει αυτό;

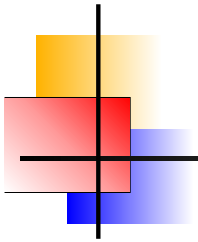
Μπορούμε να χρησιμοποιήσουμε μεθόδους αριθμητικής ανάλυσης (μέθοδος Νεύτωνα, επαναληπτικά σχήματα κτλ) για να δείξουμε ότι διοφαντικές εξισώσεις έχουν λύση.

Λήμμα Hensel - p-αδική μέθοδος Newton

Έστω $f(x) \in \mathbb{Z}_p[x]$. Αν $f(a_0) \equiv 0 \bmod p$ και $f'(a_0) \neq 0 \bmod p$, τότε υπάρχει μοναδικός $a \in \mathbb{Z}_p$ ώστε $f(a) = 0$ και $a \equiv a_0 \bmod p$.

Και για τις μη τετραγωνικές μορφές τι γίνεται;

Η θεωρία διαταραχών μας δίνει συγκεκριμένες obstructions σε ομάδες συνομολογίας ώστε η τοπική λύση να δίνει καθολική.



Γενίκες Διοφαντικές εξισώσεις

Γενικότερα μια διοφαντική εξίσωση ορίζεται ως το σύνολο μηδενισμού ενός συνόλου ομογενών πολυωνύμων που παράγεται από τα $f_1, \ldots, f_r \in \mathbb{Z}[x_1, \ldots, x_r]$. 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

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

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

Γενίκες Διοφαντικές εξισώσεις

Γενικότερα μια διοφαντική εξίσωση ορίζεται ως το σύνολο μηδενισμού ενός συνόλου ομογενών πολυωνύμων που παράγεται από τα $f_1, \ldots, f_r \in \mathbb{Z}[x_1, \ldots, x_r]$. 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

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

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

Γενίκες Διοφαντικές εξισώσεις

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

Θεωρούμε το πλήθος των λύσεων N_r πάνω από κάθε σώμα $\mathbb{F}_{p^r}$.

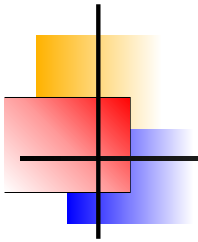
Σχηματίζουμε την «γεννήτρια συνάρτηση»:

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

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 $1 \leq i \leq 2n-1$, $P_i(t) \in \mathbb{Z}[t]$,

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

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

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.

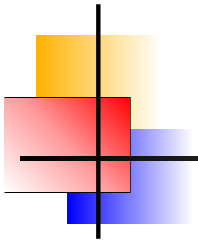
Τύπος σταθερών σημείων του Lefschetz

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

Λήμμα

Αν ϕ ενδομορφισμός πεπερασμένης διάστασης διανυσματικού χώρου

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



Αλγεβρική Τοπολογία εν δράσει

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

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

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

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

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!

Απόδειξη του Λήμματος

Αν $\dim(V) = 1$ τότε

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

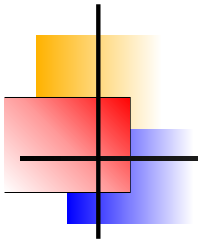
Επαγωγή.

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.

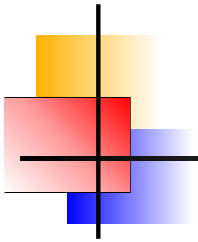
$$N_r = 1 - a_r + q^r.$$

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.



Εξειδίκευση στις Καμπύλες

Θεωρούμε την καμπύλη X γένους g.

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

τότε

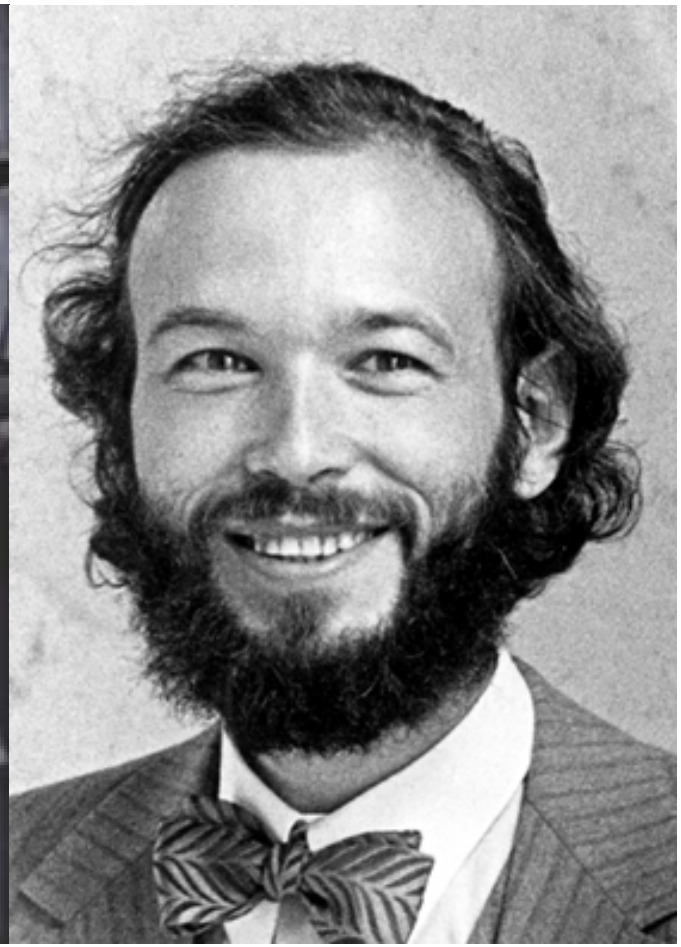
$$|a_r| \leq 2g\sqrt{q^r}$$

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

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

A. Weil -A. Grothendieck - P. Deligne

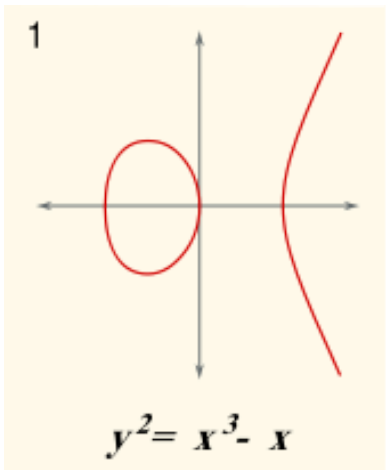


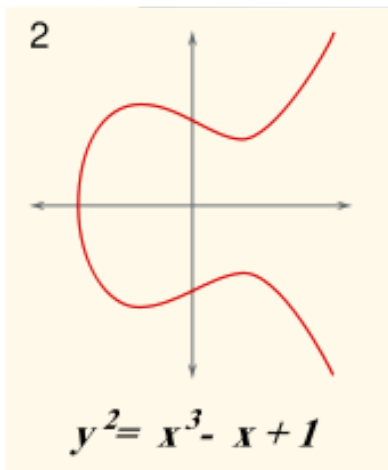


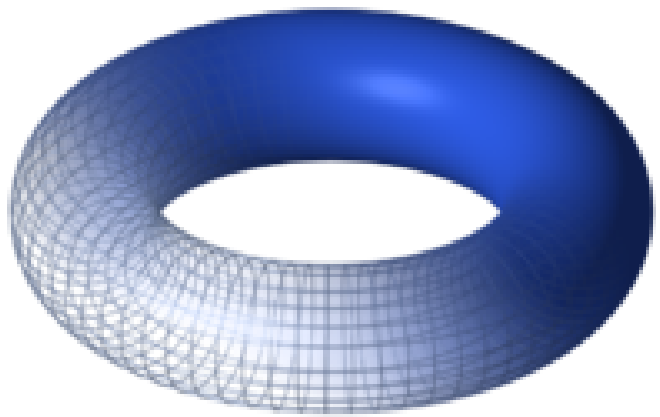
Ελλειπτικές Καμπύλες

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.

Τα σημεία $E(\mathbb{F}_p)$ αποτελούν μια πεπερασμένη ομάδα. Ασφαλώς

$$\#E(\mathbb{F}_p) \leq q + 1 - a_r \leq q + 1 + 2\sqrt{q}.$$

Το πρόβλημα του διακριτού λογαρίθμου

Δίνονται σημεία P, Q σε μία αβελιανή ομάδα για τα οποία γνωρίζουμε ότι $nP = Q$. Να βρεθεί το n.

Το πρόβλημα είναι δύσκολο γιατί το εξυπνότερο που μπορούμε να κάνουμε είναι να εφαρμόζουμε όλα τα n μέχρι να βρούμε το σωστό.

Αβελιανές ομάδες: $\mathbb{F}_{p^r}^*$, E.

Αν η ομάδα E έχει μεγάλη τάξη τότε μπορεί να είναι γινόμενο μικρών κυκλικών για παράδειγμα $(\mathbb{Z}/2\mathbb{Z})^n$ και το πρόβλημα του διακριτού λογαρίθμου εύκολο.

Το πρόβλημα του διακριτού λογαρίθμου είναι δύσκολο αν η ελλειπτική καμπύλη έχει τάξη πρώτο αριθμό, άρα είναι κυκλική.

Τα σημεία $E(\mathbb{F}_p)$ αποτελούν μια πεπερασμένη ομάδα. Ασφαλώς

$$\#E(\mathbb{F}_p) \leq q + 1 - a_r \leq q + 1 + 2\sqrt{q}.$$

Το πρόβλημα του διακριτού λογαρίθμου

Δίνονται σημεία P, Q σε μία αβελιανή ομάδα για τα οποία γνωρίζουμε ότι $nP = Q$. Να βρεθεί το n.

Το πρόβλημα είναι δύσκολο γιατί το εξυπνότερο που μπορούμε να κάνουμε είναι να εφαρμόζουμε όλα τα n μέχρι να βρούμε το σωστό.

Αβελιανές ομάδες: $\mathbb{F}_{p^r}^*$, E.

Αν η ομάδα E έχει μεγάλη τάξη τότε μπορεί να είναι γινόμενο μικρών κυκλικών για παράδειγμα $(\mathbb{Z}/2\mathbb{Z})^n$ και το πρόβλημα του διακριτού λογαρίθμου εύκολο.

Το πρόβλημα του διακριτού λογαρίθμου είναι δύσκολο αν η ελλειπτική καμπύλη έχει τάξη πρώτο αριθμό, άρα είναι κυκλική.

Τα σημεία $E(\mathbb{F}_p)$ αποτελούν μια πεπερασμένη ομάδα. Ασφαλώς

$$\#E(\mathbb{F}_p) \leq q + 1 - a_r \leq q + 1 + 2\sqrt{q}.$$

Το πρόβλημα του διακριτού λογαρίθμου

Δίνονται σημεία P, Q σε μία αβελιανή ομάδα για τα οποία γνωρίζουμε ότι $nP = Q$. Να βρεθεί το n.

Το πρόβλημα είναι δύσκολο γιατί το εξυπνότερο που μπορούμε να κάνουμε είναι να εφαρμόζουμε όλα τα n μέχρι να βρούμε το σωστό.

Αβελιανές ομάδες: $\mathbb{F}_{p^r}^*$, E.

Αν η ομάδα E έχει μεγάλη τάξη τότε μπορεί να είναι γινόμενο μικρών κυκλικών για παράδειγμα $(\mathbb{Z}/2\mathbb{Z})^n$ και το πρόβλημα του διακριτού λογαρίθμου εύκολο.

Το πρόβλημα του διακριτού λογαρίθμου είναι δύσκολο αν η ελλειπτική καμπύλη έχει τάξη πρώτο αριθμό, άρα είναι κυκλική.

Τα σημεία $E(\mathbb{F}_p)$ αποτελούν μια πεπερασμένη ομάδα. Ασφαλώς

$$\#E(\mathbb{F}_p) \leq q + 1 - a_r \leq q + 1 + 2\sqrt{q}.$$

Το πρόβλημα του διακριτού λογαρίθμου

Δίνονται σημεία P, Q σε μία αβελιανή ομάδα για τα οποία γνωρίζουμε ότι $nP = Q$. Να βρεθεί το n.

Το πρόβλημα είναι δύσκολο γιατί το εξυπνότερο που μπορούμε να κάνουμε είναι να εφαρμόζουμε όλα τα n μέχρι να βρούμε το σωστό.
Αβελιανές ομάδες: $\mathbb{F}_{p^r}^*$, E.
Αν η ομάδα E έχει μεγάλη τάξη τότε μπορεί να είναι γινόμενο μικρών κυκλικών για παράδειγμα $(\mathbb{Z}/2\mathbb{Z})^n$ και το πρόβλημα του διακριτού λογαρίθμου εύκολο.

Το πρόβλημα του διακριτού λογαρίθμου είναι δύσκολο αν η ελλειπτική καμπύλη έχει τάξη πρώτο αριθμό, άρα είναι κυκλική.

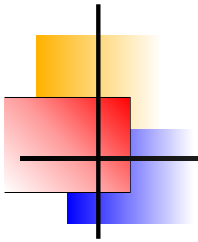
Τα σημεία $E(\mathbb{F}_p)$ αποτελούν μια πεπερασμένη ομάδα. Ασφαλώς

$$\#E(\mathbb{F}_p) \leq q + 1 - a_r \leq q + 1 + 2\sqrt{q}.$$

Το πρόβλημα του διακριτού λογαρίθμου

Δίνονται σημεία P, Q σε μία αβελιανή ομάδα για τα οποία γνωρίζουμε ότι $nP = Q$. Να βρεθεί το n.

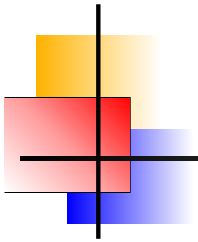
Το πρόβλημα είναι δύσκολο γιατί το εξυπνότερο που μπορούμε να κάνουμε είναι να εφαρμόζουμε όλα τα n μέχρι να βρούμε το σωστό.
Αβελιανές ομάδες: $\mathbb{F}_{p^r}^*$, E.
Αν η ομάδα E έχει μεγάλη τάξη τότε μπορεί να είναι γινόμενο μικρών κυκλικών για παράδειγμα $(\mathbb{Z}/2\mathbb{Z})^n$ και το πρόβλημα του διακριτού λογαρίθμου εύκολο.
Το πρόβλημα του διακριτού λογαρίθμου είναι δύσκολο αν η ελλειπτική καμπύλη έχει τάξη πρώτο αριθμό, άρα είναι κυκλική.



Κατασκευή Ελλειπτικών Καμπυλών με τάξη πρώτο αριθμό

1. Στην τύχη: Κατασκευάζουμε ελλιπτικές καμπύλες στην τύχη μέχρι να πετύχουμε μία που να έχει σωστή τάξη.
2. Η μέθοδος του μιγαδικού πολλαπλασιασμού.

Θα ασχοληθούμε σε αυτή την διάλεξη με την δεύτερη μέθοδο.



Ελλειπτικές καμπύλες ως πηλίκα

Γενικά κάθε ελλειπτική καμπύλη πάνω από το $\mathbb{C}$ είναι πηλίκο του $\mathbb{C}$ modulo μια διακριτή υποομάδα $L = \mathbb{Z} + \tau\mathbb{Z}$, $\Im(\tau) > 0$. Τα L, L' δίνουν την ίδια ελλειπτική καμπύλη αν και μόνο αν

$$\tau' = \frac{a\tau + b}{c\tau + b}, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}).$$

Η συνάρτηση πηλίκο

$$\mathbb{H} \to \mathrm{SL}(2, \mathbb{Z}) \backslash \mathbb{H} \cong \mathbb{C}$$

ονομάζεται j-invariant. Επιπλέον είναι $\mathrm{SL}(2, \mathbb{Z})$- αναλλοίωτη και άρα περιοδική. Έχει ανάπτυγμα Fourier $q = e^{2\pi i \tau}$,

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 +$$

Ελλειπτικές καμπύλες ως πηλίκα

Γενικά κάθε ελλειπτική καμπύλη πάνω από το $\mathbb{C}$ είναι πηλίκο του $\mathbb{C}$ modulo μια διακριτή υποομάδα $L = \mathbb{Z} + \tau\mathbb{Z}$, $\Im(\tau) > 0$. Τα L, L' δίνουν την ίδια ελλειπτική καμπύλη αν και μόνο αν

$$\tau' = \frac{a\tau + b}{c\tau + b}, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}).$$

Η συνάρτηση πηλίκο

$$\mathbb{H} \to \mathrm{SL}(2, \mathbb{Z}) \backslash \mathbb{H} \cong \mathbb{C}$$

ονομάζεται j-invariant. Επιπλέον είναι $\mathrm{SL}(2, \mathbb{Z})$- αναλλοίωτη και άρα περιοδική. Έχει ανάπτυγμα Fourier $q = e^{2\pi i \tau}$,

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 +$$

Ελλειπτικές καμπύλες ως πηλίκα

Γενικά κάθε ελλειπτική καμπύλη πάνω από το $\mathbb{C}$ είναι πηλίκο του $\mathbb{C}$ modulo μια διακριτή υποομάδα $L = \mathbb{Z} + \tau\mathbb{Z}$, $\Im(\tau) > 0$. Τα L, L' δίνουν την ίδια ελλειπτική καμπύλη αν και μόνο αν

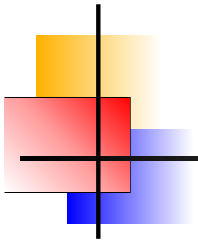
$$\tau' = \frac{a\tau + b}{c\tau + b}, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}).$$

Η συνάρτηση πηλίκο

$$\mathbb{H} \to \mathrm{SL}(2, \mathbb{Z}) \backslash \mathbb{H} \cong \mathbb{C}$$

ονομάζεται j-invariant. Επιπλέον είναι $\mathrm{SL}(2, \mathbb{Z})$- αναλλοίωτη και άρα περιοδική. Έχει ανάπτυγμα Fourier $q = e^{2\pi i \tau}$,

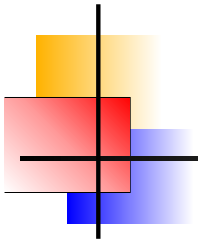
$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 +$$



j-invariant

Παρατηρήσεις: Οι συντελεστές του αναπτύγματος Fourier είναι ακέραιοι.

Σχετίζονται δε με τις διαστάσεις των αναγωγών αναπαραστάσεων του «τέρατος»: της μεγαλύτερης απλής ομάδας με τάξη 808017424794512875886459904961710757005754368000000000.



Σώματα Αριθμών

Ένα σώμα αριθμών είναι μια πεπερασμένη επέκταση του $\mathbb{Q}$, δηλαδή ένα σώμα

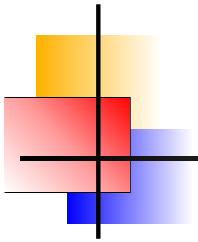
$$K = \mathbb{Q}[x]/f(x),$$

όπου το $f(x)$ είναι ανάγωγο πολυώνυμο του $\mathbb{Q}[x]$. Ο δακτύλιος των ακεραίων αλγεβρικών $\mathcal{O}$ είναι ο δακτύλιος όλων των στοιχείων

$$\mathcal{O} = \{x \in K : \text{ ώστε το } x \text{ ικανοποιεί ένα μονικό πολυώνυμο } f(x) \in \mathbb{Z}[x]\}.$$

Ο δακτύλιος $\mathcal{O}$ δεν είναι περιοχή μονοσήμαντης ανάλυσης αλλά κάθε ιδεώδες του αναλύεται με μοναδικό τρόπο σε γινόμενο πρώτων ιδεωδών.

$$I = P_1^{e_1} \cdots P_r^{e_r}.$$



Σώματα Αριθμών

Ένα σώμα αριθμών είναι μια πεπερασμένη επέκταση του $\mathbb{Q}$, δηλαδή ένα σώμα

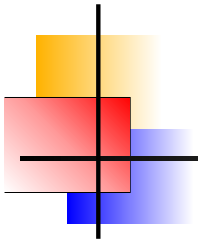
$$K = \mathbb{Q}[x]/f(x),$$

όπου το $f(x)$ είναι ανάγωγο πολυώνυμο του $\mathbb{Q}[x]$. Ο δακτύλιος των ακεραίων αλγεβρικών $\mathcal{O}$ είναι ο δακτύλιος όλων των στοιχείων

$$\mathcal{O} = \{x \in K : \text{ ώστε το } x \text{ ικανοποιεί ένα μονικό πολυώνυμο } f(x) \in \mathbb{Z}[x]\}.$$

Ο δακτύλιος $\mathcal{O}$ δεν είναι περιοχή μονοσήμαντης ανάλυσης αλλά κάθε ιδεώδες του αναλύεται με μοναδικό τρόπο σε γινόμενο πρώτων ιδεωδών.

$$I = P_1^{e_1} \cdots P_r^{e_r}.$$



Σώματα Αριθμών

Ένα σώμα αριθμών είναι μια πεπερασμένη επέκταση του $\mathbb{Q}$, δηλαδή ένα σώμα

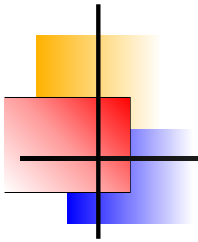
$$K = \mathbb{Q}[x]/f(x),$$

όπου το $f(x)$ είναι ανάγωγο πολυώνυμο του $\mathbb{Q}[x]$. Ο δακτύλιος των ακεραίων αλγεβρικών $\mathcal{O}$ είναι ο δακτύλιος όλων των στοιχείων

$$\mathcal{O} = \{x \in K : \text{ ώστε το } x \text{ ικανοποιεί ένα μονικό πολυώνυμο } f(x) \in \mathbb{Z}[x]\}.$$

Ο δακτύλιος $\mathcal{O}$ δεν είναι περιοχή μονοσήμαντης ανάλυσης αλλά κάθε ιδεώδες του αναλύεται με μοναδικό τρόπο σε γινόμενο πρώτων ιδεωδών.

$$I = P_1^{e_1} \cdots P_r^{e_r}.$$



Ομάδα Κλάσεων

Θεωρούμε την ημιομάδα των ιδεωδών την οποία την εμπλουτίζουμε με τα κλασματικά ιδεώδη τα οποία αποτελούν αβελιανές προσθετικές υποομάδες I του K ώστε για κάποιο $x \in \mathcal{O}$ το xI να γίνεται ιδεώδες του $\mathcal{O}$. Με αυτή την κατασκευή κατασκευάζουμε την ομάδα των κλασματικών ιδεωδών $I(\mathcal{O})$.

Παράδειγμα: Τα κλασματικά ιδεώδη του $\mathbb{Z}$ είναι τα $\frac{1}{n}\mathbb{Z}$.

Θεωρούμε την υποομάδα $PI(\mathcal{O})$ των κυρίων κλασματικών ιδεωδών $a\mathcal{O}$, όπου $a \in K$.

Το πηλίκο το ονομάζουμε ομάδα κλάσεων

$$\mathrm{Cl}(\mathcal{O}) = \frac{I(\mathcal{O})}{PI(\mathcal{O})}.$$

Με μεθόδους κυρτών σωμάτων (γεωμετρία των αριθμών) αποδεικνύεται ότι η ομάδα κλάσεων είναι πεπερασμένη.

Ομάδα Κλάσεων

Θεωρούμε την ημιομάδα των ιδεωδών την οποία την εμπλουτίζουμε με τα κλασματικά ιδεώδη τα οποία αποτελούν αβελιανές προσθετικές υποομάδες I του K ώστε για κάποιο $x \in \mathcal{O}$ το xI να γίνεται ιδεώδες του $\mathcal{O}$. Με αυτή την κατασκευή κατασκευάζουμε την ομάδα των κλασματικών ιδεωδών $I(\mathcal{O})$.

Παράδειγμα: Τα κλασματικά ιδεώδη του $\mathbb{Z}$ είναι τα $\frac{1}{n}\mathbb{Z}$.

Θεωρούμε την υποομάδα $PI(\mathcal{O})$ των κυρίων κλασματικών ιδεωδών $a\mathcal{O}$, όπου $a \in K$.

Το πηλίκο το ονομάζουμε ομάδα κλάσεων

$$\mathrm{Cl}(\mathcal{O}) = \frac{I(\mathcal{O})}{PI(\mathcal{O})}.$$

Με μεθόδους κυρτών σωμάτων (γεωμετρία των αριθμών) αποδεικνύεται ότι η ομάδα κλάσεων είναι πεπερασμένη.

Ομάδα Κλάσεων

Θεωρούμε την ημιομάδα των ιδεωδών την οποία την εμπλουτίζουμε με τα κλασματικά ιδεώδη τα οποία αποτελούν αβελιανές προσθετικές υποομάδες I του K ώστε για κάποιο $x \in \mathcal{O}$ το xI να γίνεται ιδεώδες του $\mathcal{O}$. Με αυτή την κατασκευή κατασκευάζουμε την ομάδα των κλασματικών ιδεωδών $I(\mathcal{O})$.

Παράδειγμα: Τα κλασματικά ιδεώδη του $\mathbb{Z}$ είναι τα $\frac{1}{n}\mathbb{Z}$.

Θεωρούμε την υποομάδα $PI(\mathcal{O})$ των κυρίων κλασματικών ιδεωδών $a\mathcal{O}$, όπου $a \in K$.

Το πηλίκο το ονομάζουμε ομάδα κλάσεων

$$\mathrm{Cl}(\mathcal{O}) = \frac{I(\mathcal{O})}{PI(\mathcal{O})}.$$

Με μεθόδους κυρτών σωμάτων (γεωμετρία των αριθμών) αποδεικνύεται ότι η ομάδα κλάσεων είναι πεπερασμένη.

Ομάδα Κλάσεων

Θεωρούμε την ημιομάδα των ιδεωδών την οποία την εμπλουτίζουμε με τα κλασματικά ιδεώδη τα οποία αποτελούν αβελιανές προσθετικές υποομάδες I του K ώστε για κάποιο $x \in \mathcal{O}$ το xI να γίνεται ιδεώδες του $\mathcal{O}$. Με αυτή την κατασκευή κατασκευάζουμε την ομάδα των κλασματικών ιδεωδών $I(\mathcal{O})$.

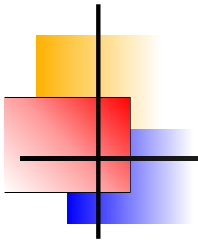
Παράδειγμα: Τα κλασματικά ιδεώδη του $\mathbb{Z}$ είναι τα $\frac{1}{n}\mathbb{Z}$.

Θεωρούμε την υποομάδα $PI(\mathcal{O})$ των κυρίων κλασματικών ιδεωδών $a\mathcal{O}$, όπου $a \in K$.

Το πηλίκο το ονομάζουμε ομάδα κλάσεων

$$\mathrm{Cl}(\mathcal{O}) = \frac{I(\mathcal{O})}{PI(\mathcal{O})}.$$

Με μεθόδους κυρτών σωμάτων (γεωμετρία των αριθμών) αποδεικνύεται ότι η ομάδα κλάσεων είναι πεπερασμένη.

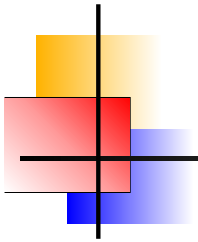


Διακλάδωση (ramification)

Θεωρούμε μια επέκταση σωμάτων αριθμών L/K. Ένα πρώτο ιδεώδες P του $\mathcal{O}_K$ μπορεί να θεωρηθεί ως ιδεώδες του $\mathcal{O}_L$ ως $P\mathcal{O}_L$. Δεν είναι όμως πρώτο κατανάγκη. Έχει μια γραφή στην μορφή:

$$P\mathcal{O}_L = Q_1^{e_1} \cdots Q_r^{e_r},$$

όπου τα Q_i είναι πρώτα ιδεώδη του $\mathcal{O}_L$.
Αν όλα τα $e_i = 1$ τότε θα λέμε ότι το P δεν διακλαδίζεται στην επέκταση L/K. Αν κανένα πρώτο ιδεώδες δεν διακλαδίζεται τότε θα λέμε ότι η επέκταση είναι *αδιακλάδιστη*.



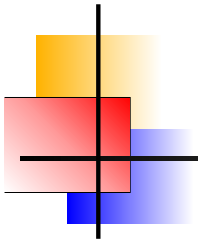
Διακλάδωση (ramification)

Θεωρούμε μια επέκταση σωμάτων αριθμών L/K. Ένα πρώτο ιδεώδες P του $\mathcal{O}_K$ μπορεί να θεωρηθεί ως ιδεώδες του $\mathcal{O}_L$ ως $P\mathcal{O}_L$. Δεν είναι όμως πρώτο κατανάγκη. Έχει μια γραφή στην μορφή:

$$P\mathcal{O}_L = Q_1^{e_1} \cdots Q_r^{e_r},$$

όπου τα Q_i είναι πρώτα ιδεώδη του $\mathcal{O}_L$.

Αν όλα τα $e_i = 1$ τότε θα λέμε ότι το P δεν διακλαδίζεται στην επέκταση L/K. Αν κανένα πρώτο ιδεώδες δεν διακλαδίζεται τότε θα λέμε ότι η επέκταση είναι *αδιακλάδιστη*.

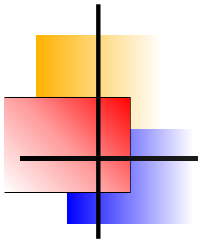


Διακλάδωση (ramification)

Θεωρούμε μια επέκταση σωμάτων αριθμών L/K. Ένα πρώτο ιδεώδες P του $\mathcal{O}_K$ μπορεί να θεωρηθεί ως ιδεώδες του $\mathcal{O}_L$ ως $P\mathcal{O}_L$. Δεν είναι όμως πρώτο κατανάγκη. Έχει μια γραφή στην μορφή:

$$P\mathcal{O}_L = Q_1^{e_1} \cdots Q_r^{e_r},$$

όπου τα Q_i είναι πρώτα ιδεώδη του $\mathcal{O}_L$.
Αν όλα τα $e_i = 1$ τότε θα λέμε ότι το P δεν διακλαδίζεται στην επέκταση L/K. Αν κανένα πρώτο ιδεώδες δεν διακλαδίζεται τότε θα λέμε ότι η επέκταση είναι *αδιακλάδιστη*.

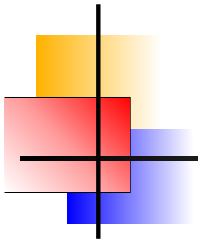


Το σώμα του Hilbert

Θεώρημα

Για κάθε σώμα αριθμών K υπάρχει μια Galois επέκταση H_K το οποίο ορίζεται να είναι η μέγιστη αδιακλάδιστη αβελιανή επέκταση του K. Ισχύει ότι $\mathrm{Gal}(H_K/K) = \mathrm{Cl}(\mathcal{O}_K)$ Το σώμα αυτό το λέμε σώμα του Hilbert.

Παρατηρήσεις: Αδιακλάδιστες επεκτάσεις αντιστοιχούν στην θεωρία επιφανειών Riemann σε τοπολογικά καλύμματα. Σώματα με $\mathrm{Cl}(\mathcal{O}_K) = \{1\}$ δεν μπορούν να έχουν αδιακλάδιστα καλύμματα και είναι «απλά συνεκτικά». Το $\mathbb{Q}$ είναι απλά συνεκτικό. Το γεγονός ότι «κάθε ιδεώδες του $\mathbb{Z}$ είναι κύριο», είναι το ανάλογο του θεωρήματος «κάθε διανυσματική δέσμη είναι καθολικά τετριμμένη». Η ομάδα $\mathrm{Cl}(\mathcal{O}_K)$ θα λέγαμε ότι αντιστοιχεί στην $\pi^1(\mathrm{Spec}\mathcal{O}_K)^{\mathrm{ab}} = H_1(\mathrm{Spec}\mathcal{O}_K)$.



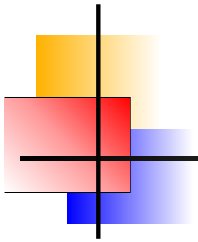
Το σώμα του Hilbert

Θεώρημα

Για κάθε σώμα αριθμών K υπάρχει μια Galois επέκταση H_K το οποίο ορίζεται να είναι η μέγιστη αδιακλάδιστη αβελιανή επέκταση του K. Ισχύει ότι $\mathrm{Gal}(H_K/K) = \mathrm{Cl}(\mathcal{O}_K)$ Το σώμα αυτό το λέμε σώμα του Hilbert.

Παρατηρήσεις: Αδιακλάδιστες επεκτάσεις αντιστοιχούν στην θεωρία επιφανειών Riemann σε τοπολογικά καλύμματα. Σώματα με $\mathrm{Cl}(\mathcal{O}_K) = \{1\}$ δεν μπορούν να έχουν αδιακλάδιστα καλύμματα και είναι «απλά συνεκτικά». Το $\mathbb{Q}$ είναι απλά συνεκτικό. Το γεγονός ότι «κάθε ιδεώδες του $\mathbb{Z}$ είναι κύριο», είναι το ανάλογο του θεωρήματος «κάθε διανυσματική δέσμη είναι καθολικά τετριμμένη». Η ομάδα $\mathrm{Cl}(\mathcal{O}_K)$ θα λέγαμε ότι αντιστοιχεί στην $\pi^1(\mathrm{Spec}\mathcal{O}_K)^{\mathrm{ab}} = H_1(\mathrm{Spec}\mathcal{O}_K)$.

D. Hilbert



Κατασκευή του σώματος του Hilbert

Υποθέτουμε ότι $K = \mathbb{Q}(\sqrt{-d})$, $d > 0$, d ελεύθερος τετραγώνου. Υπολογίζουμε ότι

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{-d}] & \text{αν } -d \equiv 2, 3 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{-d}}{2}] & \text{αν } -d \equiv 1 \bmod 4 \end{cases}$$

Αυτοί είναι ενδομορφισμοί κατάλληλης ελλειπτικής καμπύλης E με μιγαδικό πολλαπλασιασμό.

Τετραγωνικές μορφές διακρίνουσας D

$$ax^2 + bxy + cy^2; b^2 - 4ac = -D, a, b, c \in \mathbb{Z} \ \ (a, b, c) = 1$$

K.F. Gauss Disquisitiones Arithmeticae.

Θα λέμε ότι δυο τετραγωνικές μορφές είναι ισοδύναμες αν υπάρχει μετασχηματισμός της $\mathrm{SL}(2, \mathbb{Z})$ που να στέλνει την μία στην άλλη. Οι κλάσεις ισοδυναμίας είναι σε ένα προς ένα αντιστοιχία με την ομάδα κλάσεων και μπορούμε να τις υπολογίσουμε γρήγορα αφού ένα πλήρες σύστημα αντιπροσώπων είναι τα (a, b, c) ώστε

$$|b| \leq a \leq \sqrt{\frac{D}{3}}, a \leq c, (a, b, c) = 1, b^2 - 4ac = -D$$

$$\text{αν } |b| = a \text{ ή } a = c \text{ τότε } b \geq 0.$$

Τετραγωνικές μορφές διακρίνουσας D

$$ax^2 + bxy + cy^2; b^2 - 4ac = -D, a, b, c \in \mathbb{Z} \ \ (a, b, c) = 1$$

K.F. Gauss Disquisitiones Arithmeticae.

Θα λέμε ότι δυο τετραγωνικές μορφές είναι ισοδύναμες αν υπάρχει μετασχηματισμός της $\mathrm{SL}(2, \mathbb{Z})$ που να στέλνει την μία στην άλλη. Οι κλάσεις ισοδυναμίας είναι σε ένα προς ένα αντιστοιχία με την ομάδα κλάσεων και μπορούμε να τις υπολογίσουμε γρήγορα αφού ένα πλήρες σύστημα αντιπροσώπων είναι τα (a, b, c) ώστε

$$|b| \leq a \leq \sqrt{\frac{D}{3}}, a \leq c, (a, b, c) = 1, b^2 - 4ac = -D$$

αν $|b| = a$ ή $a = c$ τότε $b \geq 0$.

Τετραγωνικές μορφές διακρίνουσας D

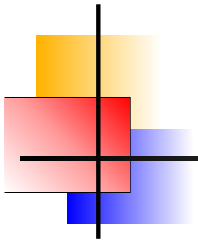
$$ax^2 + bxy + cy^2; b^2 - 4ac = -D, a, b, c \in \mathbb{Z} \ \ (a, b, c) = 1$$

K.F. Gauss Disquisitiones Arithmeticae.
Θα λέμε ότι δυο τετραγωνικές μορφές είναι ισοδύναμες αν υπάρχει μετασχηματισμός της $\mathrm{SL}(2, \mathbb{Z})$ που να στέλνει την μία στην άλλη. Οι κλάσεις ισοδυναμίας είναι σε ένα προς ένα αντιστοιχία με την ομάδα κλάσεων και μπορούμε να τις υπολογίσουμε γρήγορα αφού ένα πλήρες σύστημα αντιπροσώπων είναι τα (a, b, c) ώστε

$$|b| \leq a \leq \sqrt{\frac{D}{3}}, a \leq c, (a, b, c) = 1, b^2 - 4ac = -D$$

$$\text{αν } |b| = a \text{ ή } a = c \text{ τότε } b \geq 0.$$

K.F. Gauss



Μιγαδικός Πολλαπλασιασμός

Θεωρούμε τον δακτύλιο των ενδομορφισμών μιας ελλειπτικής καμπύλης. Στις περισσότερες περιπτώσεις $\mathrm{End}(E) \cong \mathbb{Z}$.

$$[n] : E \to E \qquad P \mapsto nP$$

Υπάρχουν όμως και περιπτώσεις όπου το $\mathrm{End}(E)$ είναι μια τάξη σε ένα μιγαδικό τετραγωνικό σώμα αριθμών. Για παράδειγμα

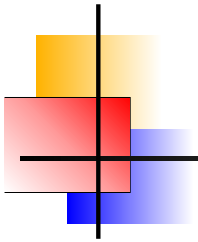
$$\mathrm{End}(\mathbb{C}/\mathbb{Z}[i]) = \mathbb{Z}[i].$$

Πεπερασμένη Χαρακτηριστική

Ο ενδομορφισμός του Frobenious $F : x \mapsto x^p$ είναι στοιχείο του $\mathrm{End}(E)$. Ικανοποιεί δε ένα χαρακτηριστικό πολυώνυμο

$$x^2 - \mathrm{tr}(F)x + q = 0.$$

$$N_p = p + 1 \pm \mathrm{tr}(\mathrm{F})$$



Μιγαδικός Πολλαπλασιασμός

Θεωρούμε τον δακτύλιο των ενδομορφισμών μιας ελλειπτικής καμπύλης. Στις περισσότερες περιπτώσεις $\mathrm{End}(E) \cong \mathbb{Z}$.

$$[n] : E \to E \qquad P \mapsto nP$$

Υπάρχουν όμως και περιπτώσεις όπου το $\mathrm{End}(E)$ είναι μια τάξη σε ένα μιγαδικό τετραγωνικό σώμα αριθμών. Για παράδειγμα

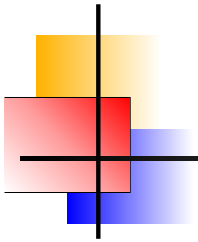
$$\mathrm{End}(\mathbb{C}/\mathbb{Z}[i]) = \mathbb{Z}[i].$$

Πεπερασμένη Χαρακτηριστική

Ο ενδομορφισμός του Frobenious $F : x \mapsto x^p$ είναι στοιχείο του $\mathrm{End}(E)$. Ικανοποιεί δε ένα χαρακτηριστικό πολυώνυμο

$$x^2 - \mathrm{tr}(F)x + q = 0.$$

$$N_p = p + 1 \pm \mathrm{tr}(\mathrm{F})$$



Μιγαδικός Πολλαπλασιασμός

Θεωρούμε τον δακτύλιο των ενδομορφισμών μιας ελλειπτικής καμπύλης. Στις περισσότερες περιπτώσεις $\mathrm{End}(E) \cong \mathbb{Z}$.

$$[n] : E \to E \qquad P \mapsto nP$$

Υπάρχουν όμως και περιπτώσεις όπου το $\mathrm{End}(E)$ είναι μια τάξη σε ένα μιγαδικό τετραγωνικό σώμα αριθμών. Για παράδειγμα

$$\mathrm{End}(\mathbb{C}/\mathbb{Z}[i]) = \mathbb{Z}[i].$$

Πεπερασμένη Χαρακτηριστική

Ο ενδομορφισμός του Frobenious $F : x \mapsto x^p$ είναι στοιχείο του $\mathrm{End}(E)$. Ικανοποιεί δε ένα χαρακτηριστικό πολυώνυμο

$$x^2 - \mathrm{tr}(F)x + q = 0.$$

$$N_p = p + 1 \pm \mathrm{tr}(\mathrm{F})$$

Θεώρημα

Θεωρούμε το $\tau \in \mathbb{H}$, το οποίο ικανοποιεί ένα μονικό πολυώνυμο στο $\mathbb{Z}[x]$ βαθμού 2. Θέτουμε $E_\tau = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$. Τότε

1. $\mathrm{End}(E_\tau) = E_\tau$.
2. $j(\tau) = j(E_\tau)$ είναι ακέραιος αλγεβρικός. Το ελάχιστο πολυώνυμο δίνεται από την εξίσωση

$$H_D(x) = \prod_{[a,b,c] \in \mathrm{CL(K)}} \left(x - j\left(\frac{-b + \sqrt{-D}}{2a} \right) \right) \in \mathbb{Z}[x].$$

3. Το $j(\tau)$ γεννά το σώμα του Hilbert.

Kronecker's Jugendtraum or Hilbert's twelfth problem

* Λατινικά για το «θα αγνοούμε».

Θεώρημα Kronecker-Weber

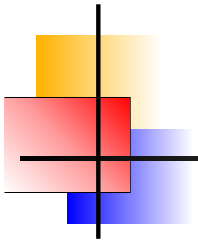
Κάθε αβελιανή επέκταση περιέχεται σε μία κυκλοτομική επέκταση $\mathbb{Q}\left(\exp\left(\frac{2\pi i}{n}\right)\right)$.

Kronecker's Jugendtraum

Να παράγουμε σώματα του Hilbert με την βοήθεια μιγαδικών συναρτήσεων.

Τι είναι γνωστό;

Θεωρία μιγαδικού πολλαπλασιασμού για ελλειπτικές καμπύλες. Γενικεύσεις των μιγαδικών τετραγωνικών επεκτάσεων CM-fields και αβελιανές πολλαπλότητες (Shimura).



Kronecker's Jugendtraum or Hilbert's twelfth problem

Θεώρημα Kronecker-Weber

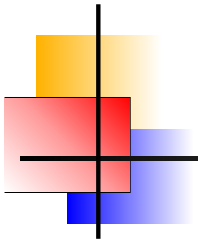
Κάθε αβελιανή επέκταση περιέχεται σε μία κυκλοτομική επέκταση $\mathbb{Q}\left(\exp\left(\frac{2\pi i}{n}\right)\right)$.

Kronecker's Jugendtraum

Να παράγουμε σώματα του Hilbert με την βοήθεια μιγαδικών συναρτήσεων.

Τι είναι γνωστό;

Θεωρία μιγαδικού πολλαπλασιασμού για ελλειπτικές καμπύλες. Γενικεύσεις των μιγαδικών τετραγωνικών επεκτάσεων CM-fields και αβελιανές πολλαπλότητες (Shimura).



Kronecker's Jugendtraum or Hilbert's twelfth problem

Θεώρημα Kronecker-Weber

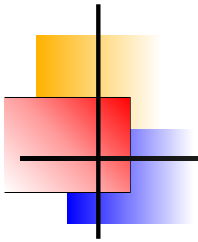
Κάθε αβελιανή επέκταση περιέχεται σε μία κυκλοτομική επέκταση $\mathbb{Q}\left(\exp\left(\frac{2\pi i}{n}\right)\right)$.

Kronecker's Jugendtraum

Να παράγουμε σώματα του Hilbert με την βοήθεια μιγαδικών συναρτήσεων.

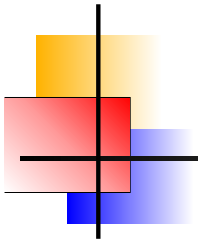
Τι είναι γνωστό;

Θεωρία μιγαδικού πολλαπλασιασμού για ελλειπτικές καμπύλες. Γενικεύσεις των μιγαδικών τετραγωνικών επεκτάσεων CM-fields και αβελιανές πολλαπλότητες (Shimura).



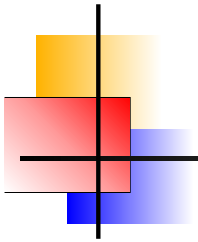
Κατασκευή Ελλειπτικών Καμπυλών

1. Αρκεί να κατασκευάσουμε το j.
2. Το φράγμα του Hasse μας εξασφαλίζει ότι $Z := 4p - (p + 1 - m)^2 \geq 0 \Rightarrow Z = Dv^2$.
3. Η εξίσωση
$$4p = u^2 + Dv^2$$
για κάποιο u ικανοποιεί την $m = p + 1 \pm u$. Ο αρνητικός αριθμός $-D$ λέγεται CM διακρίνουσα για τον πρώτο p.
4. $$x^2 - \mathrm{tr}(F)x + p \mapsto \Delta = \mathrm{tr}(F)^2 - 4p = -Dv^2.$$



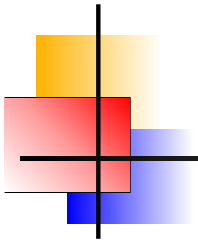
Κατασκευή Ελλειπτικών Καμπυλών

1. Αρκεί να κατασκευάσουμε το j.
2. Το φράγμα του Hasse μας εξασφαλίζει ότι $Z := 4p - (p + 1 - m)^2 \geq 0 \Rightarrow Z = Dv^2$.
3. Η εξίσωση
$$4p = u^2 + Dv^2$$
για κάποιο u ικανοποιεί την $m = p + 1 \pm u$. Ο αρνητικός αριθμός $-D$ λέγεται CM διακρίνουσα για τον πρώτο p.
4. $$x^2 - \mathrm{tr}(F)x + p \mapsto \Delta = \mathrm{tr}(F)^2 - 4p = -Dv^2.$$



Κατασκευή Ελλειπτικών Καμπυλών

1. Αρκεί να κατασκευάσουμε το j.
2. Το φράγμα του Hasse μας εξασφαλίζει ότι $Z := 4p - (p + 1 - m)^2 \geq 0 \Rightarrow Z = Dv^2$.
3. Η εξίσωση
$$4p = u^2 + Dv^2$$
για κάποιο u ικανοποιεί την $m = p + 1 \pm u$. Ο αρνητικός αριθμός $-D$ λέγεται CM διακρίνουσα για τον πρώτο p.
4. $$x^2 - \mathrm{tr}(F)x + p \mapsto \Delta = \mathrm{tr}(F)^2 - 4p = -Dv^2.$$



Κατασκευή Ελλειπτικών Καμπυλών

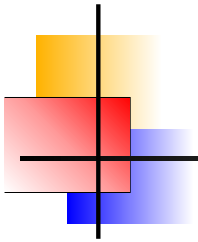
1. Αρκεί να κατασκευάσουμε το j.
2. Το φράγμα του Hasse μας εξασφαλίζει ότι $Z := 4p - (p + 1 - m)^2 \geq 0 \Rightarrow Z = Dv^2$.
3. Η εξίσωση
$$4p = u^2 + Dv^2$$
για κάποιο u ικανοποιεί την $m = p + 1 \pm u$. Ο αρνητικός αριθμός $-D$ λέγεται CM διακρίνουσα για τον πρώτο p.
4. $$x^2 - \mathrm{tr}(F)x + p \mapsto \Delta = \mathrm{tr}(F)^2 - 4p = -Dv^2.$$

Αναγωγή Ελλειπτικής Καμπύλης $\mathrm{mod} p$

$$E(\mathbb{C}) \qquad \tau \in \mathbf{End}(E(\mathbb{C})) \qquad j \text{ ρίζα του } H_D(x) \in \mathbb{Z}[x]$$

$$\downarrow \qquad\qquad \downarrow \qquad\qquad \downarrow$$

$$E(\mathbb{F}_p) \qquad F \in \mathbf{End}(E(\mathbb{F}_p)) \qquad j \text{ ρίζα του } H_D(x) \bmod p \in \mathbb{F}_p[x]$$



Κατασκευή Ελλειπτικών Καμπυλών

1. Διαλέγουμε ένα πρώτο p. Διαλέγουμε την μικρότερη D μαζί με $u, v \in \mathbb{Z}$ ώστε να έχει λύση η $4p = u^2 + Dv^2$.
2. Αν μία από τις τιμές $p + 1 - u$, $p + 1 + u$ έχει τάξη πρώτο αριθμό τότε προχωράμε στην κατασκευή της ελλειπτικής καμπύλης. Αν όχι δοκιμάζουμε άλλο p.
3. Υπολογίζουμε το πολυώνυμο Hilbert $H_D(x) \in \mathbb{Z}[x]$ με χρήση των τιμών της j-invariant. Στην συνέχεια υπολογίζουμε το πολυώνυμο $H_D(x) \bmod p$. Μία λύση του είναι η j-invariant που ψάχνουμε. Η ελλειπτική καμπύλη με αυτή την j-invariant $j \neq 0, 1728$ είναι η

$$y^2 = x^3 + 3kc^2x + 2kc^3, k = j/(1728 - j), c \in \mathbb{F}_p$$

Οι συντελεστές του πολυωνύμου Hilbert γίνονται πολύ μεγάλοι πολύ γρήγορα. Έτσι το πολυώνυμο Hilbert για το $\mathbb{Q}(\sqrt{-299})$ είναι:

$$x^8 + 391086320728105978429440x^7$$

$$-2863528087481612617432616769945 6x^6$$

$$+209405541000632214665149113072113365811 2x^5-$$

$$1865472607707568299619716756851517912965447 68x^4$$

$$+641714127813321866528980865595427518152371811 1232x^3$$

$$-192078394435944888229369889438361771152278772273643 52x^2$$

$$+4579752880821515013624897536320186072435122569480241 1520x-$$

$$1827388396532627222371762662864742290781373101619373 3558272$$

Η συνάρτηση η του Dedekind

$$\eta(\tau) = \exp\left(\frac{2\pi i\tau}{24}\right)\prod_{n=1}^{\infty}(1-q^n), q = \exp(2\pi i\tau), \tau \in \mathbb{H}.$$

Οδηγεί στις συναρτήσεις Weber

$$f(z) = e^{-\pi i/24}\frac{\eta(\frac{\tau+1}{2})}{\eta(\tau)}, f_1(\tau) = \frac{\eta(\frac{\tau}{2})}{\eta(\tau)}, f_2(\tau) = \sqrt{2}\frac{\eta(2\tau)}{\eta(\tau)}.$$

Οι οποίες μπορούν να παράγουν επίσης το σώμα του Hilbert (D. Zagier-N. Yui).

Τι ιδιαίτερο έχουν οι παραπάνω συναρτήσεις;

Είναι modular functions

Η συνάρτηση η του Dedekind

$$\eta(\tau) = \exp\left(\frac{2\pi i\tau}{24}\right)\prod_{n=1}^{\infty}(1-q^n), q = \exp(2\pi i\tau), \tau \in \mathbb{H}.$$

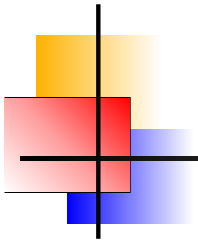
Οδηγεί στις συναρτήσεις Weber

$$f(z) = e^{-\pi i/24}\frac{\eta(\frac{\tau+1}{2})}{\eta(\tau)}, f_1(\tau) = \frac{\eta(\frac{\tau}{2})}{\eta(\tau)}, f_2(\tau) = \sqrt{2}\frac{\eta(2\tau)}{\eta(\tau)}.$$

Οι οποίες μπορούν να παράγουν επίσης το σώμα του Hilbert (D. Zagier-N. Yui).

Τι ιδιαίτερο έχουν οι παραπάνω συναρτήσεις;

Είναι modular functions



Εναλλακτικοί τρόποι να ορίσουμε το σώμα Hilbert

Η συνάρτηση η του Dedekind

$$\eta(\tau) = \exp\left(\frac{2\pi i\tau}{24}\right)\prod_{n=1}^{\infty}(1-q^n), q = \exp(2\pi i\tau), \tau \in \mathbb{H}.$$

Οδηγεί στις συναρτήσεις Weber

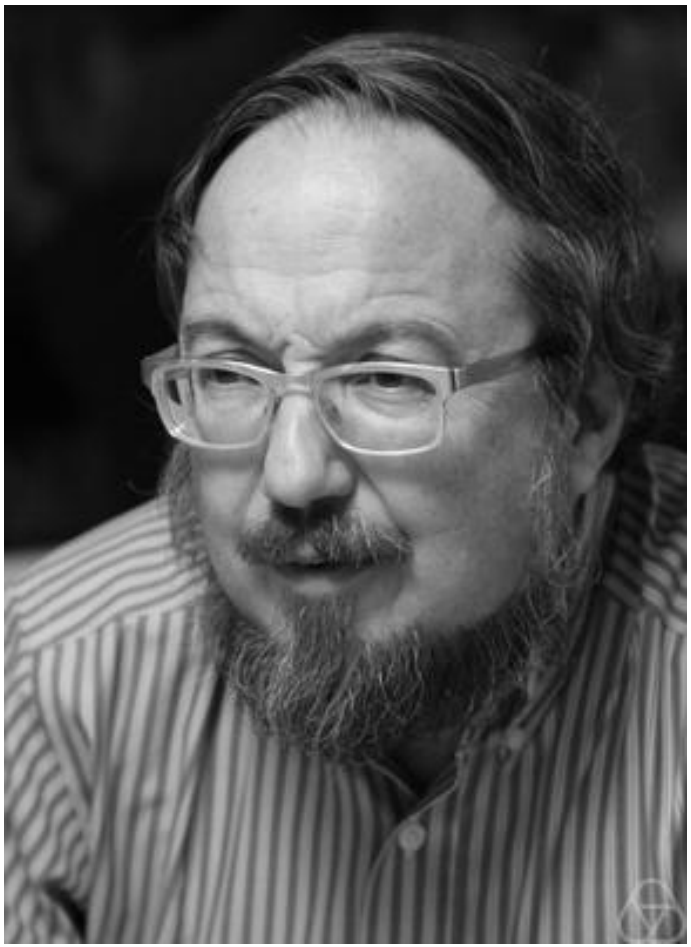
$$f(z) = e^{-\pi i/24}\frac{\eta(\frac{\tau+1}{2})}{\eta(\tau)}, f_1(\tau) = \frac{\eta(\frac{\tau}{2})}{\eta(\tau)}, f_2(\tau) = \sqrt{2}\frac{\eta(2\tau)}{\eta(\tau)}.$$

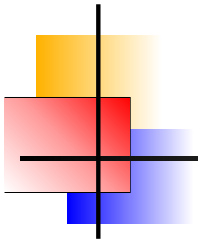
Οι οποίες μπορούν να παράγουν επίσης το σώμα του Hilbert (D. Zagier-N. Yui).

Τι ιδιαίτερο έχουν οι παραπάνω συναρτήσεις;

Είναι modular functions

D. Zagier - N. Yui





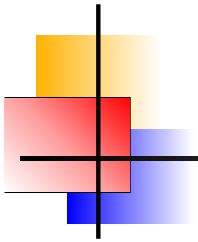
Modular functions επιπέδου N

Θεωρούμε την ομάδα

$$\Gamma(N) = \left\{ A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \text{ ώστε } A \equiv I_2 \bmod N \right\}.$$

Ο χώρος πηλίκο $\Gamma(N)\backslash\mathbb{H}$ είναι επιφάνεια Riemann $Y(N)$ η οποία μπορεί να συμπαγοποιηθεί σε συμπαγή επιφάνεια Riemann $X(N)$ προσθέτοντας σημεία στην ευθεία $\Im(s) = 0$. Τα στοιχεία του σώματος μερομόρφων συναρτήσεων της $X(N)$ τα λέμε modular συναρτήσεις επιπέδου N.

Οι επιφάνειες Riemann $X(N)$ αντιστοιχούν σε αλγεβρικές καμπύλες ορισμένες στο σώμα $\mathbb{Q}(\zeta_N))$. Τα αναπτύγματα Fourier των modular συναρτήσεων έχουν συντελεστές στο $\mathbb{Q}(\zeta_N)$.



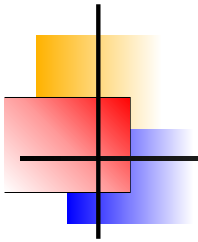
Modular functions επιπέδου N

Θεωρούμε την ομάδα

$$\Gamma(N) = \left\{ A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \text{ ώστε } A \equiv I_2 \bmod N \right\}.$$

Ο χώρος πηλίκο $\Gamma(N)\backslash\mathbb{H}$ είναι επιφάνεια Riemann $Y(N)$ η οποία μπορεί να συμπαγοποιηθεί σε συμπαγή επιφάνεια Riemann $X(N)$ προσθέτοντας σημεία στην ευθεία $\Im(s) = 0$. Τα στοιχεία του σώματος μερομόρφων συναρτήσεων της $X(N)$ τα λέμε modular συναρτήσεις επιπέδου N.

Οι επιφάνειες Riemann $X(N)$ αντιστοιχούν σε αλγεβρικές καμπύλες ορισμένες στο σώμα $\mathbb{Q}(\zeta_N))$. Τα αναπτύγματα Fourier των modular συναρτήσεων έχουν συντελεστές στο $\mathbb{Q}(\zeta_N)$.



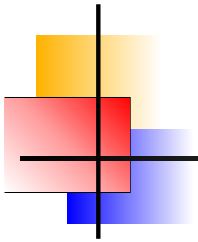
Modular functions επιπέδου N

Θεωρούμε την ομάδα

$$\Gamma(N) = \left\{ A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \text{ ώστε } A \equiv I_2 \bmod N \right\}.$$

Ο χώρος πηλίκο $\Gamma(N)\backslash\mathbb{H}$ είναι επιφάνεια Riemann $Y(N)$ η οποία μπορεί να συμπαγοποιηθεί σε συμπαγή επιφάνεια Riemann $X(N)$ προσθέτοντας σημεία στην ευθεία $\Im(s) = 0$. Τα στοιχεία του σώματος μερομόρφων συναρτήσεων της $X(N)$ τα λέμε modular συναρτήσεις επιπέδου N.

Οι επιφάνειες Riemann $X(N)$ αντιστοιχούν σε αλγεβρικές καμπύλες ορισμένες στο σώμα $\mathbb{Q}(\zeta_N))$. Τα αναπτύγματα Fourier των modular συναρτήσεων έχουν συντελεστές στο $\mathbb{Q}(\zeta_N)$.



Modular functions επιπέδου N

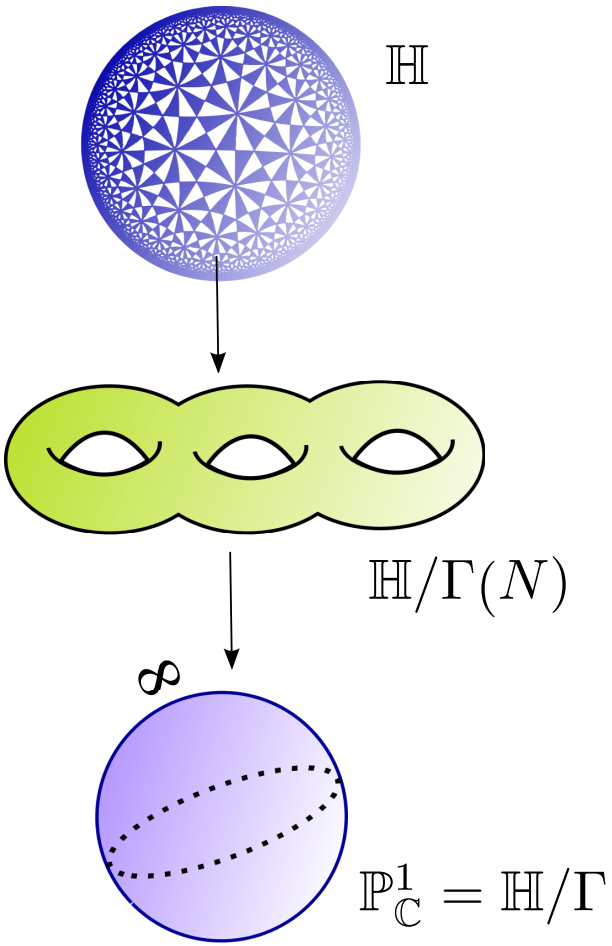
Θεωρούμε την ομάδα

$$\Gamma(N) = \left\{ A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \text{ ώστε } A \equiv I_2 \bmod N \right\}.$$

Ο χώρος πηλίκο $\Gamma(N)\backslash\mathbb{H}$ είναι επιφάνεια Riemann $Y(N)$ η οποία μπορεί να συμπαγοποιηθεί σε συμπαγή επιφάνεια Riemann $X(N)$ προσθέτοντας σημεία στην ευθεία $\Im(s) = 0$. Τα στοιχεία του σώματος μερομόρφων συναρτήσεων της $X(N)$ τα λέμε modular συναρτήσεις επιπέδου N.

Οι επιφάνειες Riemann $X(N)$ αντιστοιχούν σε αλγεβρικές καμπύλες ορισμένες στο σώμα $\mathbb{Q}(\zeta_N))$. Τα αναπτύγματα Fourier των modular συναρτήσεων έχουν συντελεστές στο $\mathbb{Q}(\zeta_N)$.

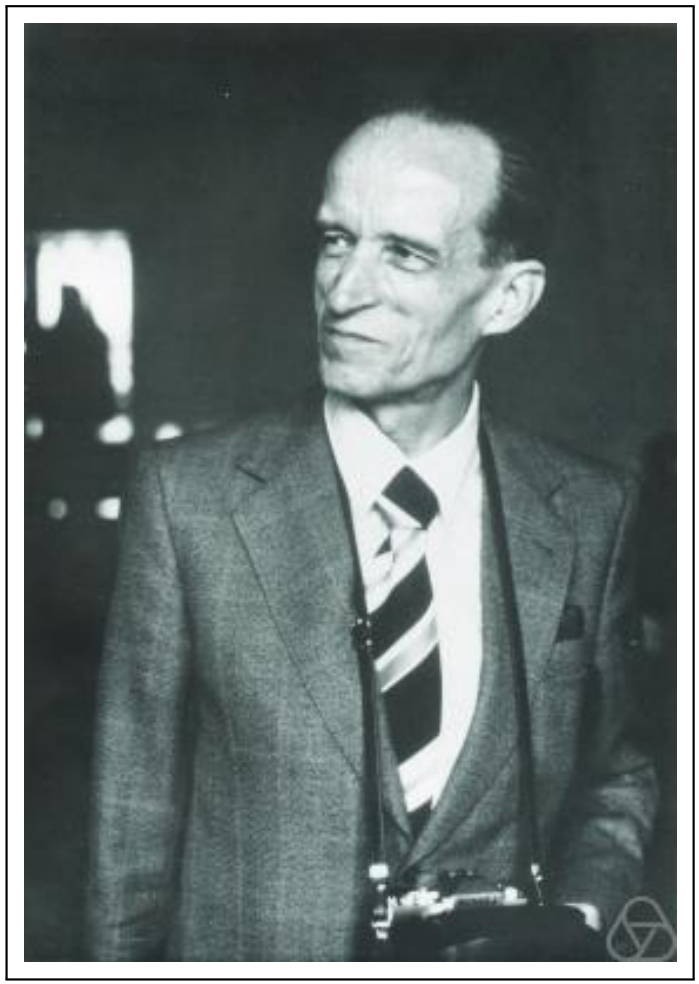
Modular functions επιπέδου N



$$\mathcal{M}(X(N)) \quad \Big\} \; \mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z})$$
$$\uparrow$$
$$\mathbb{C}(t)$$

M. Eichler

``There are five elementary arithmetical operations: addition, subtraction, multiplication, division, and modular forms.''



Θεώρημα

Έστω $\mathcal{O} = \mathbb{Z}[\theta]$ ο δακτύλιος των ακεραίων αλγεβρικών του τετραγωνικού μιγαδικού σώματος αριθμών K, και $x^2 + Bx + C$ το ελάχιστο πολυώνυμο του θ. Θεωρούμε ένα φυσικό αριθμό $N > 1$ και $x_1, \ldots, x_n$ τους γεννήτορες της ομάδας $(\mathcal{O}/N\mathcal{O})^*$, $x_i = a_i + b_i\theta \in \mathbb{Z}[\theta]$. Θεωρούμε τον πίνακα

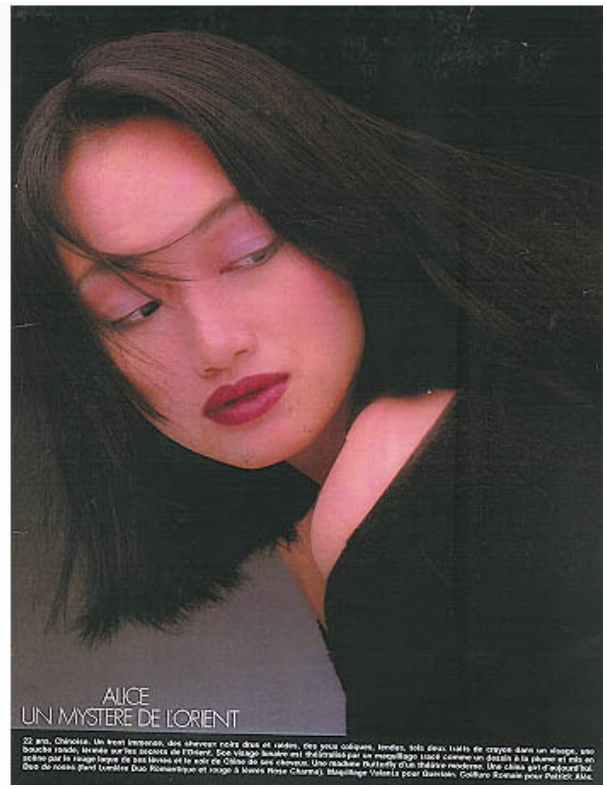
$$A_i = \begin{pmatrix} a_i - Bb_i & -Cb_i \\ b_i & a_i \end{pmatrix}.$$

Αν η f είναι μια modular function επιπέδου N και για όλους τους πίνακες A_i ισχύει ότι

$$f(\theta) = f^{A_i}(\theta), \mathbb{Q}(j) \subset \mathbb{Q}(\theta),$$

τότε το $f(\theta)$ γεννά το σώμα του Hilbert.

G. Shimura - P. Stevenhagen - A. Gee



S. Ramanujan

$$t_n = \sqrt{3}\frac{\eta(3\tau_n)\eta(\frac{1}{3}\tau_n+\frac{2}{3})}{\eta^2(\tau_n)},$$

$$\tau_n = -\frac{1}{2} + i\frac{\sqrt{n}}{2}, n \equiv 11 \bmod 24$$

n	$p_n(t)$
11	$t-1$
35	t^2+1-1
59	t^3+2t-1
83	t^3+2t^2+2t-1
107	t^3-2t^2+4t-1

Τα p_n γενούν το σώμα του Hilbert

S. Ramanujan

$$t_n = \sqrt{3}\frac{\eta(3\tau_n)\eta(\frac{1}{3}\tau_n+\frac{2}{3})}{\eta^2(\tau_n)},$$

$$\tau_n = -\frac{1}{2} + i\frac{\sqrt{n}}{2}, n \equiv 11 \bmod 24$$

n	$p_n(t)$
11	$t-1$
35	t^2+1-1
59	t^3+2t-1
83	t^3+2t^2+2t-1
107	t^3-2t^2+4t-1

Τα p_n γενούν το σώμα του Hilbert

S. Ramanujan

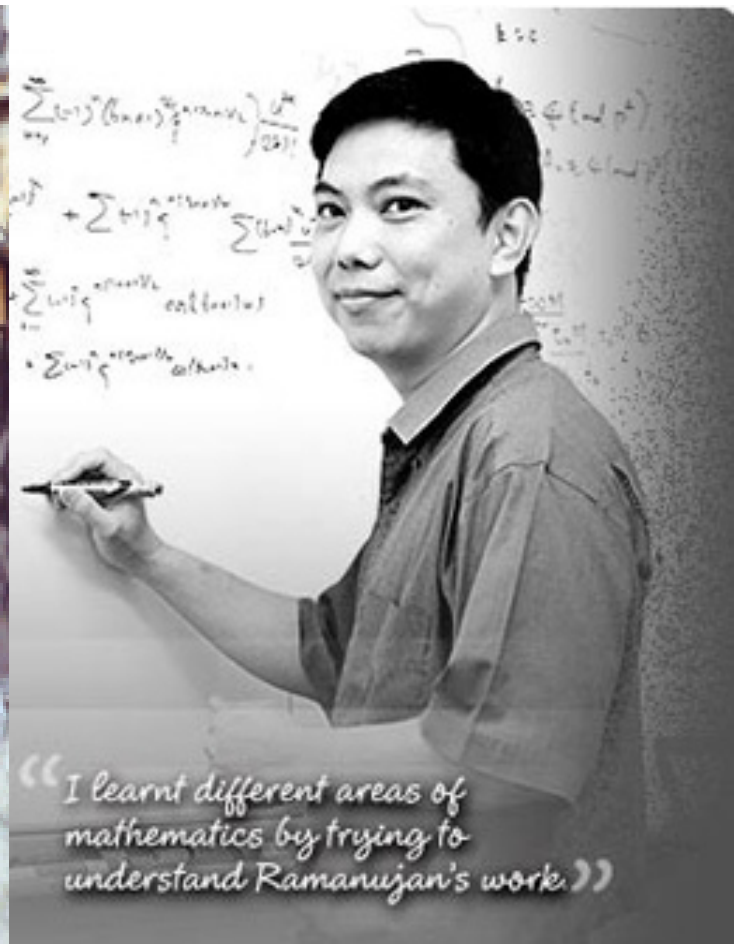
$$t_n = \sqrt{3}\frac{\eta(3\tau_n)\eta(\frac{1}{3}\tau_n+\frac{2}{3})}{\eta^2(\tau_n)},$$

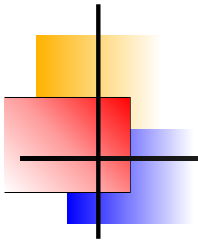
$$\tau_n = -\frac{1}{2} + i\frac{\sqrt{n}}{2}, n \equiv 11 \bmod 24$$

n	$p_n(t)$
11	$t-1$
35	t^2+1-1
59	t^3+2t-1
83	t^3+2t^2+2t-1
107	t^3-2t^2+4t-1

Τα p_n γενούν το σώμα του Hilbert

B. Berndt & Heng Huat Chan





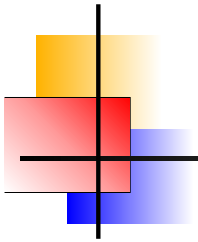
B. Berndt & Heng Huat Chan

Απέδειξαν το ότι ο Ramanujan είχε δίκιο και έθεσαν το ερώτημα πως μπορούν να υπολογιστούν πολυώνυμα για μεγαλύτερες τιμές του n.
Ε. Κωνσταντίνου Α.Κ. απάντηση στο ερώτημα.

$$p_{299}(x) = x^8 + x^7 - x^6 - 12x^5 + 16x^4 - 12x^3 + 15x^2 - 13x + 1.$$

Ε. Κωνσταντίνου

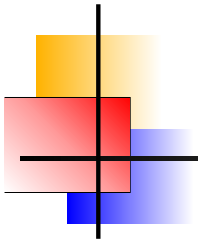
H.H. Chan



Μπορούμε να βρούμε νέες αναλλοίωτες;

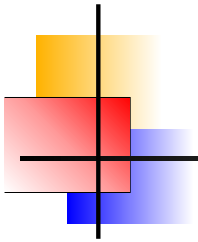
Η μέθοδος της αντιστροφής μας επιτρέπει να επαληθεύσουμε ότι μια modular function κατασκευάζει το σώμα του Hilbert. Πως θα κατασκευάσουμε νέες τέτοιες συναρτήσεις;

Όλες οι γνωστές αναλλοίωτες προέκυψαν από εξαιρετικά έξυπνους μαθηματικούς.



Μπορούμε να βρούμε νέες αναλλοίωτες;

Η μέθοδος της αντιστροφής μας επιτρέπει να επαληθεύσουμε ότι μια modular function κατασκευάζει το σώμα του Hilbert. Πως θα κατασκευάσουμε νέες τέτοιες συναρτήσεις;
Όλες οι γνωστές αναλλοίωτες προέκυψαν από εξαιρετικά έξυπνους μαθηματικούς.



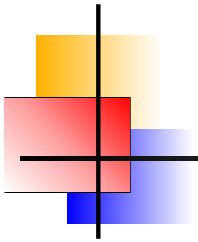
Νέες αναλλοίωτες για κοινούς θνητούς

Μπορούμε να βρούμε ένα πεπερασμένης διάστασης διανυσματικό χώρο V αποτελούμενο από modular συναρτήσεις επιπέδου N ώστε η $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ να δρα στον V. Κάθε στοιχείο $a \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ μπορεί να γραφεί ως ας $b \cdot \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$, $d \in \mathbb{Z}/N\mathbb{Z}^*$ και $b \in \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$.

Η ομάδα $\mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$ παράγεται από τα $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ και

$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Η δράση του S στις συναρτήσεις $g \in V$ ορίζεται $g \circ S = g(-1/z) \in V$ και η δράση του T ορίζεται ως $g \circ T = g(z + 1) \in V$.



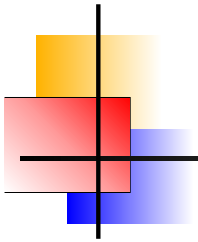
Νέες αναλλοίωτες για κοινούς θνητούς

Μπορούμε να βρούμε ένα πεπερασμένης διάστασης διανυσματικό χώρο V αποτελούμενο από modular συναρτήσεις επιπέδου N ώστε η $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ να δρα στον V. Κάθε στοιχείο $a \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ μπορεί να γραφεί ως ας $b \cdot \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$, $d \in \mathbb{Z}/N\mathbb{Z}^*$ και $b \in \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$.

Η ομάδα $\mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$ παράγεται από τα $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ και

$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Η δράση του S στις συναρτήσεις $g \in V$ ορίζεται $g \circ S = g(-1/z) \in V$ και η δράση του T ορίζεται ως $g \circ T = g(z+1) \in V$.

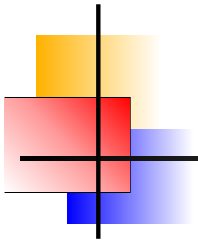


Νέες αναλλοίωτες για κοινούς θνητούς

Μπορούμε να βρούμε ένα πεπερασμένης διάστασης διανυσματικό χώρο V αποτελούμενο από modular συναρτήσεις επιπέδου N ώστε η $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ να δρα στον V. Κάθε στοιχείο $a \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ μπορεί να γραφεί ως ας $b \cdot \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$, $d \in \mathbb{Z}/N\mathbb{Z}^*$ και $b \in \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$.

Η ομάδα $\mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$ παράγεται από τα $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ και $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Η δράση του S στις συναρτήσεις $g \in V$ ορίζεται $g \circ S = g(-1/z) \in V$ και η δράση του T ορίζεται ως $g \circ T = g(z+1) \in V$.

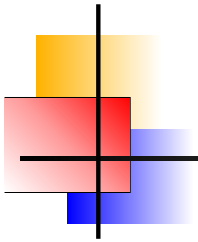


Νέες αναλλοίωτες για κοινούς θνητούς

Μπορούμε να βρούμε ένα πεπερασμένης διάστασης διανυσματικό χώρο V αποτελούμενο από modular συναρτήσεις επιπέδου N ώστε η $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ να δρα στον V. Κάθε στοιχείο $a \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ μπορεί να γραφεί ως ας $b \cdot \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$, $d \in \mathbb{Z}/N\mathbb{Z}^*$ και $b \in \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$.

Η ομάδα $\mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$ παράγεται από τα $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ και $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Η δράση του S στις συναρτήσεις $g \in V$ ορίζεται $g \circ S = g(-1/z) \in V$ και η δράση του T ορίζεται ως $g \circ T = g(z + 1) \in V$.



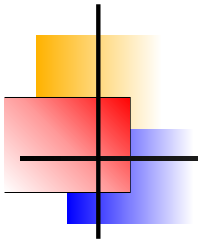
Δράσεις

Η δράση του πίνακα $\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$ δίνεται από την δράση των στοιχείων $\sigma_d \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ στους συντελεστές Fourier.

Αφού κάθε στοιχείο της $\mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$ γράφεται ως λέξη στα S, T έχουμε μια συνάρτηση ρ

$$\left(\frac{\mathcal{O}}{N\mathcal{O}}\right)^* \xrightarrow{\phi} \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}) \longrightarrow \mathrm{GL}(V), \qquad (1)$$

όπου ϕ είναι ο φυσικός ομομορφισμός.

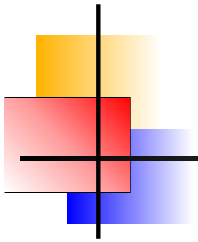


Δράσεις

Η δράση του πίνακα $\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$ δίνεται από την δράση των στοιχείων $\sigma_d \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ στους συντελεστές Fourier.
Αφού κάθε στοιχείο της $\mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$ γράφεται ως λέξη στα S, T έχουμε μια συνάρτηση ρ

$$\left(\frac{\mathcal{O}}{N\mathcal{O}}\right)^* \xrightarrow{\phi} \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}) \longrightarrow \mathrm{GL}(V), \qquad \rho \text{ (overall)} \tag{1}$$

όπου ϕ είναι ο φυσικός ομομορφισμός.



Cocylces

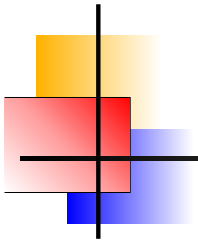
Η συνάρτηση ρ όπως ορίστηκε δεν είναι ομομορφισμός αλλά ικανοποιεί την συνθήκη συνκύκλου:

$$\rho(\sigma\tau) = \rho(\tau)\rho(\sigma)^{\tau} \tag{2}$$

και δίνει μια κλάση στην $H^1(G, \mathrm{GL}(V))$, όπου $G = (\mathcal{O}/N\mathcal{O})^*$. ○ περιορισμός της ρ στην υποομάδα H της G που ορίζεται ως

$$H := \{x \in G : \det(\phi(x)) = 1\}$$

είναι ομομορφισμός.



Cocylces

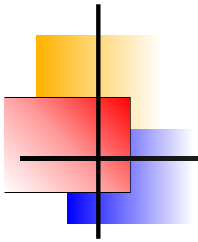
Η συνάρτηση ρ όπως ορίστηκε δεν είναι ομομορφισμός αλλά ικανοποιεί την συνθήκη συνκύκλου:

$$\rho(\sigma\tau) = \rho(\tau)\rho(\sigma)^{\tau} \tag{2}$$

και δίνει μια κλάση στην $H^1(G, \mathrm{GL}(V))$, όπου $G = (\mathcal{O}/N\mathcal{O})^*$. Ο περιορισμός της ρ στην υποομάδα H της G που ορίζεται ως

$$H := \{x \in G : \det(\phi(x)) = 1\}$$

είναι ομομορφισμός.



Invariant Theory

Διαλέγουμε μια βάση $e_1, \ldots, e_m$ του V

Η θεωρία αναλλοίωτων μας δίνει αποτελεσματικούς τρόπους (Reynolds operator, διαγονοποίηση) ώστε να υπολογίσουμε τον δακτύλιο αναλλοίωτων $\mathbb{Q}(\zeta_N)[e_1, \ldots, e_m]^H$.

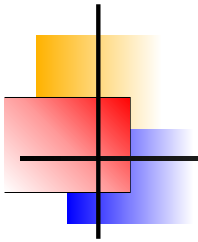
Διαλέγουμε τον διανυσματικό χώρο V_n των αναλλοίωτων πολυωνύμων βαθμού n.

Η δράση του G/H στον V_n δίνει συνκύκλο

$$\rho' \in H^1(\mathrm{Gal}(\mathbb{Q}(\zeta_N))/\mathbb{Q}), \mathrm{GL}(V_n)).$$

Το πολυδιάστατο θεώρημα 90 του Hilbert μας δίνει ότι υπάρχει ένα $P \in \mathrm{GL}(V_n)$ ώστε

$$\rho'(\sigma) = P^{-1}P^{\sigma}. \tag{3}$$



Invariant Theory

Διαλέγουμε μια βάση $e_1, \ldots, e_m$ του V

Η θεωρία αναλλοίωτων μας δίνει αποτελεσματικούς τρόπους (Reynolds operator, διαγονοποίηση) ώστε να υπολογίσουμε τον δακτύλιο αναλλοίωτων $\mathbb{Q}(\zeta_N)[e_1, \ldots, e_m]^H$.

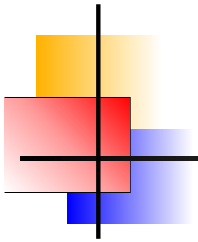
Διαλέγουμε τον διανυσματικό χώρο V_n των αναλλοίωτων πολυωνύμων βαθμού n.

Η δράση του G/H στον V_n δίνει συνκύκλο

$$\rho' \in H^1(\mathrm{Gal}(\mathbb{Q}(\zeta_N))/\mathbb{Q}), \mathrm{GL}(V_n)).$$

Το πολυδιάστατο θεώρημα 90 του Hilbert μας δίνει ότι υπάρχει ένα $P \in \mathrm{GL}(V_n)$ ώστε

$$\rho'(\sigma) = P^{-1}P^{\sigma}. \tag{3}$$



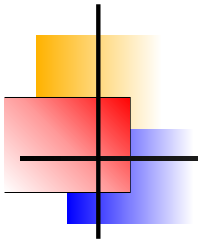
Invariant Theory

Διαλέγουμε μια βάση $e_1, \ldots, e_m$ του V
Η θεωρία αναλλοίωτων μας δίνει αποτελεσματικούς τρόπους (Reynolds operator, διαγονοποίηση) ώστε να υπολογίσουμε τον δακτύλιο αναλλοίωτων $\mathbb{Q}(\zeta_N)[e_1, \ldots, e_m]^H$.
Διαλέγουμε τον διανυσματικό χώρο V_n των αναλλοίωτων πολυωνύμων βαθμού n.
Η δράση του G/H στον V_n δίνει συνκύκλο

$$\rho' \in H^1(\mathrm{Gal}(\mathbb{Q}(\zeta_N))/\mathbb{Q}), \mathrm{GL}(V_n)).$$

Το πολυδιάστατο θεώρημα 90 του Hilbert μας δίνει ότι υπάρχει ένα $P \in \mathrm{GL}(V_n)$ ώστε

$$\rho'(\sigma) = P^{-1}P^{\sigma}. \tag{3}$$

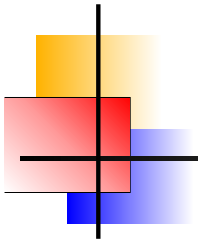


Υπολογισμός του P

Τροποποιημένη μέθοδος του Glasby-Howlett probabilistic algorithm

$$B_Q := \sum_{\sigma \in G/H} \rho(\sigma) Q^{\sigma}. \tag{4}$$

Αν βρούμε ένα 2×2 πίνακα στην $\mathrm{GL}(2, \mathbb{Q}(\zeta_N))$ ώστε B_Q είναι αντιστρέψιμος τότε $P := B_Q^{-1}$.
Οι μη αντιστρέψιμοι πίνακες είναι σπάνιοι (σχηματίζουν ένα Zariski κλειστό σύνολο) στον χώρο των πινάκων. Η πρώτη τυχαία επιλογή του Q δούλεψε πάντα!



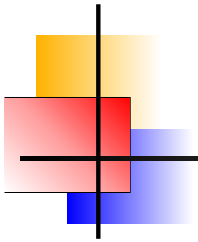
Υπολογισμός του P

Τροποποιημένη μέθοδος του Glasby-Howlett probabilistic algorithm

$$B_Q := \sum_{\sigma \in G/H} \rho(\sigma) Q^{\sigma}. \tag{4}$$

Αν βρούμε ένα 2×2 πίνακα στην $\mathrm{GL}(2, \mathbb{Q}(\zeta_N))$ ώστε B_Q είναι αντιστρέψιμος τότε $P := B_Q^{-1}$.

Οι μη αντιστρέψιμοι πίνακες είναι σπάνιοι (σχηματίζουν ένα Zariski κλειστό σύνολο) στον χώρο των πινάκων. Η πρώτη τυχαία επιλογή του Q δούλεψε πάντα!

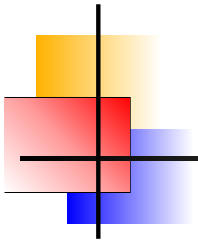


Υπολογισμός του P

Τροποποιημένη μέθοδος του Glasby-Howlett probabilistic algorithm

$$B_Q := \sum_{\sigma \in G/H} \rho(\sigma) Q^{\sigma}. \tag{4}$$

Αν βρούμε ένα 2×2 πίνακα στην $\mathrm{GL}(2, \mathbb{Q}(\zeta_N))$ ώστε B_Q είναι αντιστρέψιμος τότε $P := B_Q^{-1}$.
Οι μη αντιστρέψιμοι πίνακες είναι σπάνιοι (σχηματίζουν ένα Zariski κλειστό σύνολο) στον χώρο των πινάκων. Η πρώτη τυχαία επιλογή του Q δούλεψε πάντα!



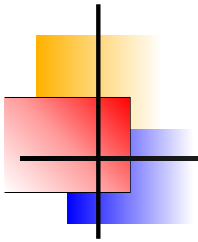
Παραδείγματα

Γενικευμένες συναρτήσεις Weber $\mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3$

$$\mathfrak{g}_0(\tau) = \frac{\eta(\frac{\tau}{3})}{\eta(\tau)},\ \mathfrak{g}_1(\tau) = \zeta_{24}^{-1}\frac{\eta(\frac{\tau+1}{3})}{\eta(\tau)},$$

$$\mathfrak{g}_2(\tau) = \frac{\eta(\frac{\tau+2}{3})}{\eta(\tau)},\ \mathfrak{g}_3(\tau) = \sqrt{3}\frac{\eta(3\tau)}{\eta(\tau)},$$

Είναι modular functions επιπέδου 72.



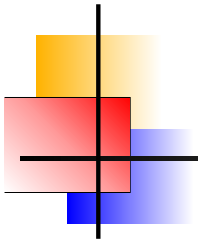
Παραδείγματα

Γενικευμένες συναρτήσεις Weber $\mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3$

$$\mathfrak{g}_0(\tau) = \frac{\eta(\frac{\tau}{3})}{\eta(\tau)},\ \mathfrak{g}_1(\tau) = \zeta_{24}^{-1}\frac{\eta(\frac{\tau+1}{3})}{\eta(\tau)},$$

$$\mathfrak{g}_2(\tau) = \frac{\eta(\frac{\tau+2}{3})}{\eta(\tau)},\ \mathfrak{g}_3(\tau) = \sqrt{3}\frac{\eta(3\tau)}{\eta(\tau)},$$

Είναι modular functions επιπέδου 72.



Παράδειγμα

Για $n = -571$ η ομάδα H έχει τάξη 144 και η G έχει τάξη 3456.
Υπολογίζουμε ότι τα πολυώνυμα

$$I_1 := \mathfrak{g}_0\mathfrak{g}_2 + \zeta_{72}^{6}\mathfrak{g}_1\mathfrak{g}_3, \qquad I_2 := \mathfrak{g}_0\mathfrak{g}_3 + (-\zeta_{72}^{18} + \zeta_{72}^{6})\mathfrak{g}_1\mathfrak{g}_2$$

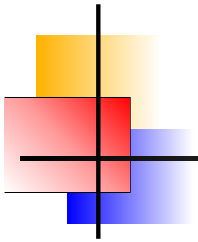
είναι αναλλοίωτα υπό την δράση της H.

Τελικά αναλλοίωτα

$$e_1 := (-12\zeta_{72}^{18} + 12\zeta_{72}^{6})\mathfrak{g}_0\mathfrak{g}_3 + 12\zeta_{72}^{6}\mathfrak{g}_0\mathfrak{g}_3 + 12\mathfrak{g}_1\mathfrak{g}_2 + 12\mathfrak{g}_1\mathfrak{g}_3,$$

$$e_2 := 12\zeta_{72}^{6}\mathfrak{g}_1\mathfrak{g}_2 + (-12\zeta_{72}^{18} + 12\zeta_{72}^{6})\mathfrak{g}_0\mathfrak{g}_3 + (-12\zeta_{72}^{12} + 12)\mathfrak{g}_1\mathfrak{g}_3 + 12\zeta_{72}^{12}\mathfrak{g}_1\mathfrak{g}_3$$

Κάθε $\mathbb{Z}$-γραμμικός συνδιασμός των e_1, e_2 είναι επίσης αναλλοίωτο.



Παράδειγμα

Για $n = -571$ η ομάδα H έχει τάξη 144 και η G έχει τάξη 3456.
Υπολογίζουμε ότι τα πολυώνυμα

$$I_1 := \mathfrak{g}_0\mathfrak{g}_2 + \zeta_{72}^{6}\mathfrak{g}_1\mathfrak{g}_3, \qquad I_2 := \mathfrak{g}_0\mathfrak{g}_3 + (-\zeta_{72}^{18} + \zeta_{72}^{6})\mathfrak{g}_1\mathfrak{g}_2$$

είναι αναλλοίωτα υπό την δράση της H.

Τελικά αναλλοίωτα

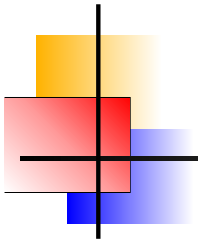
$$e_1 := (-12\zeta_{72}^{18} + 12\zeta_{72}^{6})\mathfrak{g}_0\mathfrak{g}_3 + 12\zeta_{72}^{6}\mathfrak{g}_0\mathfrak{g}_3 + 12\mathfrak{g}_1\mathfrak{g}_2 + 12\mathfrak{g}_1\mathfrak{g}_3,$$

$$e_2 := 12\zeta_{72}^{6}\mathfrak{g}_1\mathfrak{g}_2 + (-12\zeta_{72}^{18} + 12\zeta_{72}^{6})\mathfrak{g}_0\mathfrak{g}_3 + (-12\zeta_{72}^{12} + 12)\mathfrak{g}_1\mathfrak{g}_3 + 12\zeta_{72}^{12}\mathfrak{g}_1\mathfrak{g}_3$$

Κάθε $\mathbb{Z}$-γραμμικός συνδιασμός των e_1, e_2 είναι επίσης αναλλοίωτο.

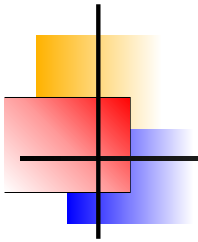
Παραδείγματα

Invariant	polynomial
Hilbert	$t^5 + 400497845154831586723701480652800t^4 +$ $818520809154613065770038265334290448384t^3 +$ $439825075242209481123868941957442230372689510 4t^2$ $-163197309751762039062749137159138628445125423923 20t$ $+152830544536728038180664216500366536462323151924 10112$
$\mathfrak{g}_0^{12}\mathfrak{g}_1^{12} + \mathfrak{g}_2^{12}\mathfrak{g}_3^{12}$	$t^5 - 5433338830617345268674t^4 + 907059135195426583247780 88t^3$ $-304935717753003053581175161972 8t^2$ $-390071826912221442431043741686448t$ - 125099920526477800721478370075114 56
e_1	$t^5 - 936t^4 - 60912t^3 - 2426112t^2 - 40310784t - 3386105856$
e_2	$t^5 - 1512t^4 - 29808t^3 + 979776t^2 + 3359232t - 423263232$



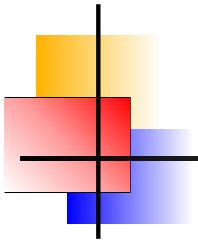
Ερωτήσεις - Προβληματισμοί

1. Επιλογή των καλύτερων invariants Ισοδύναμο πρόβλημα με την ελαχιστοποίηση συνάρτησης ύψους σε ένα lattice.
2. Τα παραδείγματα δείχνουν ότι οι καλύτερες αναλλοίωτες προκύπτουν όταν οι class invariants είναι μονόνυμα.
3. Υπάρχουν τιμές $n \bmod 24$ όπου δεν υπάρχουν μονονυμικά αναλλοίωτα. Σε αυτή την περίπτωση η μέθοδος μας δίνει τα αποτελεσματικότερα αναλλοίωτα.



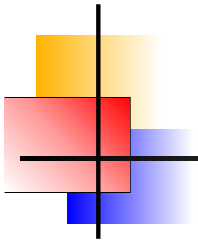
Ερωτήσεις - Προβληματισμοί

1. Επιλογή των καλύτερων invariants Ισοδύναμο πρόβλημα με την ελαχιστοποίηση συνάρτησης ύψους σε ένα lattice.
2. Τα παραδείγματα δείχνουν ότι οι καλύτερες αναλλοίωτες προκύπτουν όταν οι class invariants είναι μονόνυμα.
3. Υπάρχουν τιμές $n \bmod 24$ όπου δεν υπάρχουν μονονυμικά αναλλοίωτα. Σε αυτή την περίπτωση η μέθοδος μας δίνει τα αποτελεσματικότερα αναλλοίωτα.



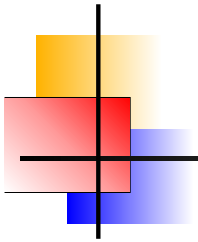
Ερωτήσεις - Προβληματισμοί

1. Επιλογή των καλύτερων invariants Ισοδύναμο πρόβλημα με την ελαχιστοποίηση συνάρτησης ύψους σε ένα lattice.
2. Τα παραδείγματα δείχνουν ότι οι καλύτερες αναλλοίωτες προκύπτουν όταν οι class invariants είναι μονόνυμα.
3. Υπάρχουν τιμές $n \bmod 24$ όπου δεν υπάρχουν μονονυμικά αναλλοίωτα. Σε αυτή την περίπτωση η μέθοδος μας δίνει τα αποτελεσματικότερα αναλλοίωτα.



Ερωτήσεις - Προβληματισμοί

1. Επιλογή των καλύτερων invariants Ισοδύναμο πρόβλημα με την ελαχιστοποίηση συνάρτησης ύψους σε ένα lattice.
2. Τα παραδείγματα δείχνουν ότι οι καλύτερες αναλλοίωτες προκύπτουν όταν οι class invariants είναι μονόνυμα.
3. Υπάρχουν τιμές $n \bmod 24$ όπου δεν υπάρχουν μονονυμικά αναλλοίωτα. Σε αυτή την περίπτωση η μέθοδος μας δίνει τα αποτελεσματικότερα αναλλοίωτα.



Ευχαριστώ πολύ!