Υπολογισμός των Ramanujan t_n αναλλοιώτων

Ελισάβετ Κωνσταντίνου   Αριστείδης Κοντογεώργης

Πανεπιστήμιο Αιγαίου

6 Συνέδριο Άλγεβρας - Θεωρίας Αριθμών
Ιούνιος 2006

Περιεχόμενα

1. Εισαγωγή
2. Ελλειπτικές Καμπύλες
3. Θεωρία κλάσεων σωμάτων
4. Shimura Reciprocity
5. Κρυπτογραφία

Ο Ramanujan στο τρίτο σημειωματάριο του όρισε τις τιμές

$$t_n := \sqrt{3}q_n^{1/18}\frac{f(q_n^{1/3})f(q_n^3)}{f^2(q_n)}$$

όπου

$$q_n = \exp(-\pi\sqrt{n}).$$

Η συνάρτηση f ορίζεται ως

$$f(-q) := \prod_{n=1}^{\infty}(1-q^n) = q^{-1/24}\eta(\tau)$$

όπου $q = \exp(2\pi i\tau)$, $\tau \in \mathbb{H}$ και $\eta(\tau)$ είναι η η-συνάρτηση του Dedekind Χωρίς κανένα επιπλέον σχόλιο στο πως τα υπολόγισε έδωσε μια λίστα πολυωνύμων και ισχυρίστηκε ότι τα t_n αποτελούν ρίζες του.

Ο Ramanujan στο τρίτο σημειωματάριο του όρισε τις τιμές

$$t_n := \sqrt{3} q_n^{1/18} \frac{f(q_n^{1/3}) f(q_n^3)}{f^2(q_n)}$$

όπου

$$q_n = \exp(-\pi\sqrt{n}).$$

Η συνάρτηση f ορίζεται ως

$$f(-q) := \prod_{n=1}^{\infty}(1-q^n) = q^{-1/24}\eta(\tau)$$

όπου $q = \exp(2\pi i\tau)$, $\tau \in \mathbb{H}$ και $\eta(\tau)$ είναι η η-συνάρτηση του Dedekind Χωρίς κανένα επιπλέον σχόλιο στο πως τα υπολόγισε έδωσε μια λίστα πολυωνύμων και ισχυρίστηκε ότι τα t_n αποτελούν ρίζες του.

Ο Ramanujan στο τρίτο σημειωματάριο του όρισε τις τιμές

$$t_n := \sqrt{3} q_n^{1/18} \frac{f(q_n^{1/3}) f(q_n^3)}{f^2(q_n)}$$

όπου

$$q_n = \exp(-\pi\sqrt{n}).$$

Η συνάρτηση f ορίζεται ως

$$f(-q) := \prod_{n=1}^{\infty}(1 - q^n) = q^{-1/24}\eta(\tau)$$

όπου $q = \exp(2\pi i \tau)$, $\tau \in \mathbb{H}$ και $\eta(\tau)$ είναι η η-συνάρτηση του Dedekind Χωρίς κανένα επιπλέον σχόλιο στο πως τα υπολόγισε έδωσε μια λίστα πολυωνύμων και ισχυρίστικε ότι τα t_n αποτελούν ρίζες του.

Οι πίνακες του Ramanujan

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

Shrinvasa Ramanujan

Είχε δίκιο ο Ramanujan;

- Οι Bruce C. Berndt και Heng Huat Chan έκαναν χρήση ad-hoc επιχειρημάτων για να δείξουν ότι τα πολυώνυμα του πίνακα πράγματι μηδενίζονται από τα t_n.
- Οι μέθοδος που χρησιμοποιούν δεν μπορεί να γενικευτεί για κάθε n.
- Ρώτησαν λοιπών πως μπορούμε να υπολογίσουμε τα πολυώνυμα t_n.

Είχε δίκιο ο Ramanujan;

- Οι Bruce C. Berndt και Heng Huat Chan έκαναν χρήση ad-hoc επιχειρημάτων για να δείξουν ότι τα πολυώνυμα του πίνακα πράγματι μηδενίζονται από τα t_n.
- Οι μέθοδος που χρησημοποιούν δεν μπορεί να γενικευτεί για κάθε n.
- Ρώτησαν λοιπών πως μπορούμε να υπολογίσουμε τα πολυώνυμα t_n.

Είχε δίκιο ο Ramanujan;

- Οι Bruce C. Berndt και Heng Huat Chan έκαναν χρήση ad-hoc επιχειρημάτων για να δείξουν ότι τα πολυώνυμα του πίνακα πράγματι μηδενίζονται από τα t_n.
- Οι μέθοδος που χρησημοποιούν δεν μπορεί να γενικευτεί για κάθε n.
- Ρώτησαν λοιπών πως μπορούμε να υπολογίσουμε τα πολυώνυμα t_n.

Τι θα δούμε σε αυτή την διάλεξη:

- Τι σχέση έχουν οι τιμές t_n με την κρυπτογραφία.
- Ελλειπτικές καμπύλες με μιγαδικό πολλαπλασιασμό
- Νόμοι αντιστροφής του Shimura
- Υπολογισμός των τιμών t_n

Τι θα δούμε σε αυτή την διάλεξη:

- Τι σχέση έχουν οι τιμές t_n με την κρυπτογραφία.
- Ελλειπτικές καμπύλες με μιγαδικό πολλαπλασιασμό
- Νόμοι αντιστροφής του Shimura
- Υπολογισμός των τιμών t_n

Τι θα δούμε σε αυτή την διάλεξη:

- Τι σχέση έχουν οι τιμές t_n με την κρυπτογραφία.
- Ελλειπτικές καμπύλες με μιγαδικό πολλαπλασιασμό
- Νόμοι αντιστροφής του Shimura
- Υπολογισμός των τιμών t_n

Τι θα δούμε σε αυτή την διάλεξη:

- Τι σχέση έχουν οι τιμές t_n με την κρυπτογραφία.
- Ελλειπτικές καμπύλες με μιγαδικό πολλαπλασιασμό
- Νόμοι αντιστροφής του Shimura
- Υπολογισμός των τιμών t_n

Ορισμός Ελλειπτικών καμπύλων

Ορισμός

Μία ελλειπτική καμπύλη ορισμένη πάνω από ένα σώμα k είναι μια μη ιδιόμορφη προβολική καμπύλη γένους 1 με ένα ρητό σημείο υπέρ το k.

- Αν το σώμα k έχει χαρακτηρισιστική $\neq 2, 3$ τότε μία ελλειπτική καμπύλη ορίζεται από μία εξίσωση της μορφής
$$zy^2 = x^3 + axz^2 + bz^3, \text{ όπου } a, b \in k$$
- Οι ελλειπτικές καμπύλες αποκτούν δομή αβελιανής ομάδας με βάση τον κανόνα: τρία συνευθειακά σημεία έχουν άθροισμα 0, όπου το 0 της ελλειπτικής καμπύλης είναι το σημείο με προβολικές συντεταγμένες $(x : y : z) = (0 : 1 : 0)$

Ορισμός Ελλειπτικών καμπύλων

Ορισμός

Μία ελλειπτική καμπύλη ορισμένη πάνω από ένα σώμα k είναι μια μη ιδιόμορφη προβολική καμπύλη γένους 1 με ένα ρητό σημείο υπέρ το k.

- Αν το σώμα k έχει χαρακτηρισιακή $\neq 2, 3$ τότε μία ελλειπτική καμπύλη ορίζεται από μία εξίσωση της μορφής

$$zy^2 = x^3 + axz^2 + bz^3, \text{ όπου } a, b \in k$$

- Οι ελλειπτικές καμπύλες αποκτούν δομή αβελιανής ομάδας με βάση τον κανόνα: τρία συνευθειακά σημεία έχουν άθροισμα 0, όπου το 0 της ελλειπτικής καμπύλης είναι το σημείο με προβολικές συντεταγμένες $(x : y : z) = (0 : 1 : 0)$

Ορισμός Ελλειπτικών καμπύλων

Ορισμός

Μία ελλειπτική καμπύλη ορισμένη πάνω από ένα σώμα k είναι μια μη ιδιόμορφη προβολική καμπύλη γένους 1 με ένα ρητό σημείο υπέρ το k.

- Αν το σώμα k έχει χαρακτηρισική $\neq 2, 3$ τότε μία ελλειπτική καμπύλη ορίζεται από μία εξίσωση της μορφής
$$zy^2 = x^3 + axz^2 + bz^3, \text{ όπου } a, b \in k$$
- Οι ελλειπτικές καμπύλες αποκτούν δομή αβελιανής ομάδας με βάση τον κανόνα: τρία συνευθειακά σημεία έχουν άθροισμα 0, όπου το 0 της ελλειπτικής καμπύλης είναι το σημείο με προβολικές συντεταγμένες $(x : y : z) = (0 : 1 : 0)$.

j-αναλλοίωτες ελλειπτικών καμπύλων

- Για κάθε ελλειπτική καμπύλη ορίζεται η j-αναλλοίωτος:

$$j := -1728\frac{4^3a^3}{-16(4a^3+27b^2)}.$$

- Δύο ελλειπτικές καμπύλες με την ίδια j-αναλλοίωτο γίνονται ισόμορφες αν θεωρήσουμε μία το πολύ βαθμού 2 αλγεβρική επέκταση του σώματος ορισμού.
- Δύο ελλειπτικές καμπύλες με διαφορετικές j-αναλλοιώτους δεν μπορεί να είναι ποτέ να είναι ισόμορφες.
- Αν υποθέσουμε ότι το σώμα είναι αλγεβρικά κλειστό τότε το σύνολο των κλάσεων ισοδυναμίας ελλειπτικών καμπύλων δίνεται από το $\mathbb{A}^1(k)$, μέσω της j-αναλλοιώτου.

j-αναλλοίωτες ελλειπτικών καμπύλων

- Για κάθε ελλειπτική καμπύλη ορίζεται η j-αναλλοίωτος:

$$j := -1728 \frac{4^3 a^3}{-16(4a^3 + 27b^2)}.$$

- Δύο ελλειπτικές καμπύλες με την ίδια j-αναλλοίωτο γίνονται ισόμορφες αν θεωρήσουμε μία το πολύ βαθμού 2 αλγεβρική επέκταση του σώματος ορισμού.
- Δύο ελλειπτικές καμπύλες με διαφορετικές j-αναλλοιώτους δεν μπορεί να είναι ποτέ να είναι ισόμορφες.
- Αν υποθέσουμε ότι το σώμα είναι αλγεβρικά κλειστό τότε το σύνολο των κλάσεων ισοδυναμίας ελλειπτικών καμπύλων δίνεται από το $\mathbb{A}^1(k)$, μέσω της j-αναλλοιώτου.

j-αναλλοίωτες ελλειπτικών καμπύλων

- Για κάθε ελλειπτική καμπύλη ορίζεται η j-αναλλοίωτος:
$$j := -1728 \frac{4^3 a^3}{-16(4a^3 + 27b^2)}.$$
- Δύο ελλειπτικές καμπύλες με την ίδια j-αναλλοίωτο γίνονται ισόμορφες αν θεωρήσουμε μία το πολύ βαθμού 2 αλγεβρική επέκταση του σώματος ορισμού.
- Δύο ελλειπτικές καμπύλες με διαφορετικές j-αναλλοιώτους δεν μπορεί να είναι ποτέ να είναι ισόμορφες.
- Αν υποθέσουμε ότι το σώμα είναι αλγεβρικά κλειστό τότε το σύνολο των κλάσεων ισοδυναμίας ελλειπτικών καμπύλων δίνεται από το $\mathbb{A}^1(k)$, μέσω της j-αναλλοιώτου.

j-αναλλοίωτες ελλειπτικών καμπύλων

- Για κάθε ελλειπτική καμπύλη ορίζεται η j-αναλλοίωτος:

$$j := -1728 \frac{4^3 a^3}{-16(4a^3 + 27b^2)}.$$

- Δύο ελλειπτικές καμπύλες με την ίδια j-αναλλοίωτο γίνονται ισόμορφες αν θεωρήσουμε μία το πολύ βαθμού 2 αλγεβρική επέκταση του σώματος ορισμού.
- Δύο ελλειπτικές καμπύλες με διαφορετικές j-αναλλοιώτους δεν μπορεί να είναι ποτέ να είναι ισόμορφες.
- Αν υποθέσουμε ότι το σώμα είναι αλγεβρικά κλειστό τότε το σύνολο των κλάσεων ισοδυναμίας ελλειπτικών καμπύλων δίνεται από το $\mathbb{A}^1(k)$, μέσω της j-αναλλοιώτου.

Ελλειπτικές καμπύλες ορισμένες πάνω από το $\mathbb{C}$

- Οι ελλειπτικές καμπύλες πάνω από το $\mathbb{C}$ ορίζονται ως πηλίκα $E_\Lambda := \mathbb{C}/\Lambda$, όπου το Λ είναι μία διακριτή υποομάδα του $\mathbb{C}$ τάξης 2.
- Δύο ελλειπτικές καμπύλες που αντιστοιχούν σε διαφορετικές υποομάδες Λ_1, Λ_2 η οποίες έχουν βάσεις $\Lambda_i =_{\mathbb{Z}} \langle 1, \tau_i \rangle$ είναι ισόμορφες αν και μόνο αν τα $\mathbb{Z}$-modules είναι ισόμορφα. Δηλαδή ο πίνακας αλλαγής βάσης είναι στοιχείο της $GL_2(\mathbb{Z})$.
- Ο χώρος των κλάσεων ισοδυναμίας ελλειπτικών καμπύλων στο $\mathbb{C}$ είναι ισόμορφος με το $\mathbb{H}/SL_2(\mathbb{Z})$. και η j είναι μια $SL_2(\mathbb{Z})$-αναλλοίωτη συνάρτηση.

$$j : \mathbb{H} \to \mathbb{C}.$$

Ελλειπτικές καμπύλες ορισμένες πάνω από το $\mathbb{C}$

- Οι ελλειπτικές καμπύλες πάνω από το $\mathbb{C}$ ορίζονται ως πηλίκα $E_\Lambda := \mathbb{C}/\Lambda$, όπου το Λ είναι μία διακριτή υποομάδα του $\mathbb{C}$ τάξης 2.
- Δύο ελλειπτικές καμπύλες που αντιστοιχούν σε διαφορετικές υποομάδες Λ_1, Λ_2 η οποίες έχουν βάσεις $\Lambda_i =_{\mathbb{Z}} \langle 1, \tau_i \rangle$ είναι ισόμορφες αν και μόνο αν τα $\mathbb{Z}$-modules είναι ισόμορφα. Δηλαδή ο πίνακας αλλαγής βάσης είναι στοιχείο της $GL_2(\mathbb{Z})$.
- Ο χώρος των κλάσεων ισοδυναμίας ελλειπτικών καμπύλων στο $\mathbb{C}$ είναι ισόμορφος με το $\mathbb{H}/SL_2(\mathbb{Z})$. και η j είναι μια $SL_2(\mathbb{Z})$-αναλλοίωτη συνάρτηση.

$$j : \mathbb{H} \to \mathbb{C}.$$

Ελλειπτικές καμπύλες ορισμένες πάνω από το $\mathbb{C}$

- Οι ελλειπτικές καμπύλες πάνω από το $\mathbb{C}$ ορίζονται ως πηλίκα $E_\Lambda := \mathbb{C}/\Lambda$, όπου το Λ είναι μία διακριτή υποομάδα του $\mathbb{C}$ τάξης 2.
- Δύο ελλειπτικές καμπύλες που αντιστοιχούν σε διαφορετικές υποομάδες Λ_1, Λ_2 η οποίες έχουν βάσεις $\Lambda_i =_{\mathbb{Z}} \langle 1, \tau_i \rangle$ είναι ισόμορφες αν και μόνο αν τα $\mathbb{Z}$-modules είναι ισόμορφα. Δηλαδή ο πίνακας αλλαγής βάσης είναι στοιχείο της $GL_2(\mathbb{Z})$.
- Ο χώρος των κλάσεων ισοδυναμίας ελλειπτικών καμπύλων στο $\mathbb{C}$ είναι ισόμορφος με το $\mathbb{H}/SL_2(\mathbb{Z})$. και η j είναι μια $SL_2(\mathbb{Z})$-αναλλοίωτη συνάρτηση.

$$j : \mathbb{H} \to \mathbb{C}.$$

Η j-συνάρτηση είναι περιοδική και συνεπώς δέχεται ανάπτυγμα Fourier το οποίο υπολογίζεται ως:

$$j(\tau) = \frac{1}{q} + \sum_{n \geq 0} c(n) q^n,$$

όπου $c(n) \in \mathbb{Z}$.

Η j-συνάρτηση είναι περιοδική και συνεπώς δέχεται ανάπτυγμα Fourier το οποίο υπολογίζεται ως:

$$j(\tau) = \frac{1}{q} + \sum_{n \geq 0} c(n) q^n,$$

όπου $c(n) \in \mathbb{Z}$.

Ελλειπτικές Καμπύλες στο $\mathbb{F}_p$.

- Έστω $m = \#E(\mathbb{F}_p)$. Την ποσότητα $t = p + 1 - m$ την ονομάζουμε ίχνος του Frobenious.
- Ισχύει $|t| \leq 2\sqrt{p}$ ή ισοδύναμα $p + 1 - 2\sqrt{p} \leq m \leq p + 1 + 2\sqrt{p}$ (Hasse).
- Αν $j_0 \in \mathbb{F}_p$ τότε υπάρχουν δύο μη ισόμορφες ελλειπτικές καμπύλες με j-αναλλοίωτο j_0 οι

$$E_1 : y^2 = x^3 + ax + b, \quad E_2 : y^2 = x^3 + ac^2x + bc^3,$$

$a = 3k, b = 2k, k = \frac{j_0}{1728 - j_0}$.

Ελλειπτικές Καμπύλες στο $\mathbb{F}_p$.

- Έστω $m = \#E(\mathbb{F}_p)$. Την ποσότητα $t = p + 1 - m$ την ονομάζουμε ίχνος του Frobenious.
- Ισχύει $|t| \leq 2\sqrt{p}$ ή ισοδύναμα $p + 1 - 2\sqrt{p} \leq m \leq p + 1 + 2\sqrt{p}$ (Hasse).
- Αν $j_0 \in \mathbb{F}_p$ τότε υπάρχουν δύο μη ισόμορφες ελλειπτικές καμπύλες με j-αναλλοίωτο j_0 οι

$$E_1 : y^2 = x^3 + ax + b, \quad E_2 : y^2 = x^3 + ac^2x + bc^3,$$

$a = 3k, b = 2k, k = \frac{j_0}{1728 - j_0}$.

Ελλειπτικές Καμπύλες στο $\mathbb{F}_p$.

- Έστω $m = \#E(\mathbb{F}_p)$. Την ποσότητα $t = p + 1 - m$ την ονομάζουμε ίχνος του Frobenious.
- Ισχύει $|t| \leq 2\sqrt{p}$ ή ισοδύναμα $p + 1 - 2\sqrt{p} \leq m \leq p + 1 + 2\sqrt{p}$ (Hasse).
- Αν $j_0 \in \mathbb{F}_p$ τότε υπάρχουν δύο μη ισόμορφες ελλειπτικές καμπύλες με j-αναλλοίωτο j_0 οι

$$E_1 : y^2 = x^3 + ax + b, \quad E_2 : y^2 = x^3 + ac^2x + bc^3,$$

$$a = 3k, b = 2k, k = \frac{j_0}{1728 - j_0}.$$

Ελλειπτικές Καμπύλες στο $\mathbb{F}_p$.

$$\#E_1(\mathbb{F}_p) = p + 1 - t$$

$$\#E_2(\mathbb{F}_p = p + 1 + t$$

Θεωρία κλάσεων σωμάτων

Ορισμός

Έστω K ένα σώμα αριθμών. Το σώμα κλάσεων του *Hilbert* για το K είναι η μέγιστη, αδιακλάδιστη επέκταση του K.

- Το σώμα κλάσεων του Hilbert είναι ένα μέτρο για το αν το K είναι «απλά συνεκτικό» ή όχι.
- Πράγματι αν X επιφάνεια Riemann και $\tilde{X}$ το universal cover τότε το Hilbert class field είναι το σώμα συναρτήσεων της επιφάνειας Riemann $\tilde{X}/[\pi_1(X), \pi_1(X)]$.

Θεωρία κλάσεων σωμάτων

Ορισμός

Έστω K ένα σώμα αριθμών. Το σώμα κλάσεων του *Hilbert* για το K είναι η μέγιστη, αδιακλάδιστη επέκταση του K.

- Το σώμα κλάσεων του Hilbert είναι ένα μέτρο για το αν το K είναι «απλά συνεκτικό» ή όχι.
- Πράγματι αν X επιφάνεια Riemann και $\tilde{X}$ το universal cover τότε το Hilbert class field είναι το σώμα συναρτήσεων της επιφάνειας Riemann $\tilde{X}/[\pi_1(X), \pi_1(X)]$.

Θεωρία κλάσεων σωμάτων

Ορισμός

Έστω K ένα σώμα αριθμών. Το σώμα κλάσεων του *Hilbert* για το K είναι η μέγιστη, αδιακλάδιστη επέκταση του K.

- Το σώμα κλάσεων του Hilbert είναι ένα μέτρο για το αν το K είναι «απλά συνεκτικό» ή όχι.
- Πράγματι αν X επιφάνεια Riemann και $\tilde{X}$ το universal cover τότε το Hilbert class field είναι το σώμα συναρτήσεων της επιφάνειας Riemann $\tilde{X}/[\pi_1(X), \pi_1(X)]$.

Τετραγωνικά μιγαδικά σώματα αριθμών

- Έστω K τετραγωνικό μιγαδικό σώμα αριθμών $K = \mathbb{Q}(\sqrt{-n})$, n θετικός ακέραιος, ελεύθερος τετραγώνου. Έστω $\mathcal{O}_K$ ο δακτύλιος των ακεραίων αλγεβρικών του K.
- Μπορούμε να βρούμε μια ελλειπτική καμπύλη E με $End(E) = \mathcal{O}_K$ και $K(j(E))$ να είναι το σώμα κλάσεων του Hilbert για το K!!
- Επιπλέον μπορούμε να υπολογίσουμε την δράση της ομάδας κλάσεων $Cl(\mathcal{O}_K) = Gal(K(j(E))/K)$

Τετραγωνικά μιγαδικά σώματα αριθμών

- Έστω K τετραγωνικό μιγαδικό σώμα αριθμών $K = \mathbb{Q}(\sqrt{-n})$, n θετικός ακέραιος, ελεύθερος τετραγώνου. Έστω $\mathcal{O}_K$ ο δακτύλιος των ακεραίων αλγεβρικών του K.
- Μπορούμε να βρούμε μια ελλειπτική καμπύλη E με $End(E) = \mathcal{O}_K$ και $K(j(E))$ να είναι το σώμα κλάσεων του Hilbert για το K!!
- Επιπλέον μπορούμε να υπολογίσουμε την δράση της ομάδας κλάσεων $Cl(\mathcal{O}_K) = Gal(K(j(E))/K)$

Τετραγωνικά μιγαδικά σώματα αριθμών

- Έστω K τετραγωνικό μιγαδικό σώμα αριθμών $K = \mathbb{Q}(\sqrt{-n})$, n θετικός ακέραιος, ελεύθερος τετραγώνου. Έστω $\mathcal{O}_K$ ο δακτύλιος των ακεραίων αλγεβρικών του K.
- Μπορούμε να βρούμε μια ελλειπτική καμπύλη E με $End(E) = \mathcal{O}_K$ και $K(j(E))$ να είναι το σώμα κλάσεων του Hilbert για το K!!
- Επιπλέον μπορούμε να υπολογίσουμε την δράση της ομάδας κλάσεων $Cl(\mathcal{O}_K) = Gal(K(j(E))/K)$

Τετραγωνικές μορφες

- Τετραγωνική μορφή: $ax^2 + bxy + cy^2$. $\Delta = b^2 - 4ac$.
- Gauss Δυο τετραγωνικές μορφές είναι ισοδύναμες αν και μόνο αν οι ρίζες τους που ανήκουν στο $\mathbb{H}$ είναι στην ίδια τροχιά της $SL_2(\mathbb{Z})$.
- Η ομάδα $Cl(\mathcal{O}_K) = Gal(K(j(E))/K)$ είναι ισόμορφη με την ομάδα των κλάσεων ισοδυναμίας τετραγωνικών μορφών.
- Τα συζηγή του

$$j(\theta)^{[a,-b,c]} = j(\tau_{[a,b,c]})$$

, $\tau_{[a,b,c]}$) είναι η ρίζα στο $\mathbb{H}$ της τετραγωνικής μορφής $[a, b, c]$ και $[a, b, c]$ διατρέχει τις κλάσεις ισοδυναμίας τετραγωνικών μορφών.

Τετραγωνικές μορφες

- Τετραγωνική μορφή: $ax^2 + bxy + cy^2$. $\Delta = b^2 - 4ac$.
- Gauss Δυο τετραγωνικές μορφές είναι ισοδύναμες αν και μόνο αν οι ρίζες τους που ανήκουν στο $\mathbb{H}$ είναι στην ίδια τροχιά της $SL_2(\mathbb{Z})$.
- Η ομάδα $Cl(\mathcal{O}_K) = Gal(K(j(E))/K)$ είναι ισόμορφη με την ομάδα των κλάσεων ισοδυναμίας τετραγωνικών μορφών.
- Τα συζηγή του

$$j(\theta)^{[a,-b,c]} = j(\tau_{[a,b,c]})$$

, $\tau_{[a,b,c]}$) είναι η ρίζα στο $\mathbb{H}$ της τετραγωνικής μορφής $[a, b, c]$ και $[a, b, c]$ διατρέχει τις κλάσεις ισοδυναμίας τετραγωνικών μορφών.

Τετραγωνικές μορφες

- Τετραγωνική μορφή: $ax^2 + bxy + cy^2$. $\Delta = b^2 - 4ac$.
- Gauss Δυο τετραγωνικές μορφές είναι ισοδύναμες αν και μόνο αν οι ρίζες τους που ανήκουν στο $\mathbb{H}$ είναι στην ίδια τροχιά της $SL_2(\mathbb{Z})$.
- Η ομάδα $Cl(\mathcal{O}_K) = Gal(K(j(E))/K)$ είναι ισόμορφη με την ομάδα των κλάσεων ισοδυναμίας τετραγωνικών μορφών.
- Τα συζηγή του

$$j(\theta)^{[a,-b,c]} = j(\tau_{[a,b,c]})$$

, $\tau_{[a,b,c]})$ είναι η ρίζα στο $\mathbb{H}$ της τετραγωνικής μορφής $[a, b, c]$ και $[a, b, c]$ διατρέχει τις κλάσεις ισοδυναμίας τετραγωνικών μορφών.

Τετραγωνικές μορφες

- Τετραγωνική μορφή: $ax^2 + bxy + cy^2$. $\Delta = b^2 - 4ac$.
- Gauss Δυο τετραγωνικές μορφές είναι ισοδύναμες αν και μόνο αν οι ρίζες τους που ανήκουν στο $\mathbb{H}$ είναι στην ίδια τροχιά της $SL_2(\mathbb{Z})$.
- Η ομάδα $Cl(\mathcal{O}_K) = Gal(K(j(E))/K)$ είναι ισόμορφη με την ομάδα των κλάσεων ισοδυναμίας τετραγωνικών μορφών.
- Τα συζηγή του

$$j(\theta)^{[a,-b,c]} = j(\tau_{[a,b,c]})$$

, $\tau_{[a,b,c]})$ είναι η ρίζα στο $\mathbb{H}$ της τετραγωνικής μορφής $[a, b, c]$ και $[a, b, c]$ διατρέχει τις κλάσεις ισοδυναμίας τετραγωνικών μορφών.

Hilbert εναντίον Ramanujan

- Υπολογισμός αλγεβρικής εξίσωσης για το $j(E)$:

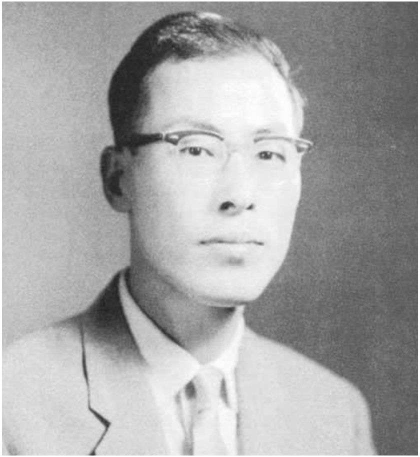
$$f_{-107}(x) = x^3 + 129783279616 \cdot 10^3 x^2 - .$$

$$-6764523159552 \cdot 10^6 x + 337618789203968 \cdot 10^9$$

-

$$p_{-107}(t) = t^3 - 2t^2 + 4t - 1$$

Goro Shimura



Modular συναρτήσεις

Έστω $N \in \mathbb{N}$ και έστω $\Gamma(N)$ η ομάδα

$$\Gamma(N) := \left\{ \gamma \in SL_2(\mathbb{Z}), \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}.$$

Το σώμα των modular functions επιπέδου N αποτελείται από τις μερόμορφες συναρτήσεις g του άνω ημιεπιπέδου $\mathbb{H}$ που παραμένουν αναλλοίωτες κάτω από την δράση της ομάδας $\Gamma(N)$, δηλαδή $g(\gamma\tau) = g(\tau)$ για κάθε $\tau \in \mathbb{H}$ και $\gamma \in \Gamma(N)$. Κάθε modular function είναι περιοδική με περίοδο N και συνεπώς δέχεται ανάπτυγμα Fourier της μορφής

$$g(q) = \sum_{\nu=-i}^{\infty} a_\nu q^\nu,$$

όπου $q = \exp(2\pi i\tau/N)$. Περιοριζόμαστε στις modular functions

Modular συναρτήσεις

Έστω $N \in \mathbb{N}$ και έστω $\Gamma(N)$ η ομάδα

$$\Gamma(N) := \left\{ \gamma \in SL_2(\mathbb{Z}), \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}.$$

Το σώμα των modular functions επιπέδου N αποτελείται από τις μερόμορφες συναρτήσεις g του άνω ημιεπιπέδου $\mathbb{H}$ που παραμένουν αναλλοίωτες κάτω από την δράση της ομάδας $\Gamma(N)$, δηλαδή $g(\gamma\tau) = g(\tau)$ για κάθε $\tau \in \mathbb{H}$ και $\gamma \in \Gamma(N)$. Κάθε modular function είναι περιοδική με περίοδο N και συνεπώς δέχεται ανάπτυγμα Fourier της μορφής

$$g(q) = \sum_{\nu=-i}^{\infty} a_\nu q^\nu,$$

όπου $q = \exp(2\pi i\tau/N)$. Περιοριζόμαστε στις modular functions

Modular συναρτήσεις

Έστω $N \in \mathbb{N}$ και έστω $\Gamma(N)$ η ομάδα

$$\Gamma(N) := \left\{ \gamma \in SL_2(\mathbb{Z}), \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}.$$

Το σώμα των modular functions επιπέδου N αποτελείται από τις μερόμορφες συναρτήσεις g του άνω ημιεπιπέδου $\mathbb{H}$ που παραμένουν αναλλοίωτες κάτω από την δράση της ομάδας $\Gamma(N)$, δηλαδή $g(\gamma\tau) = g(\tau)$ για κάθε $\tau \in \mathbb{H}$ και $\gamma \in \Gamma(N)$. Κάθε modular function είναι περιοδική με περίοδο N και συνεπώς δέχεται ανάπτυγμα Fourier της μορφής

$$g(q) = \sum_{\nu=-i}^{\infty} a_\nu q^\nu,$$

όπου $q = \exp(2\pi i \tau / N)$. Περιοριζόμαστε στις modular functions

Ο νόμος αντιστροφής του Shimura

Θεώρημα (Gee-Shimura)

Έστω $\mathcal{O} = \mathbb{Z}[\theta]$ είναι ο δακτύλιος των ακεραίων αλγεβρικών του τετραγωνικού μιγαδικού σώματος αριθμών K, και $x^2 + Bx + C$ είναι το ελάχιστο πολυώνυμο του θ. Θεωρούμε ένα φυσικό αριθμό $N > 1$ και $x_1, \ldots, x_r$ τους γεννήτορες της $(\mathcal{O}/N\mathcal{O})^*$. Έστω $\alpha_i + \beta_i\theta \in \mathcal{O}$ είναι ένας αντιπρόσωπος της κλάσης του γεννήτορα x_i. Για κάθε γεννήτορα θεωρούμε τον πίνακα

$$A_i := \begin{pmatrix} \alpha_i - B\beta_i & -C\beta_i \\ \beta_i & \alpha_i \end{pmatrix}.$$

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

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

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

Πόρισμα

Τα $t_n = \sqrt{3}\frac{\eta(3\ell_0)\eta(\frac{1}{3}\ell_0+\frac{2}{3})}{\eta^2(\ell_0)}$. Η συνάρτηση

$$\tau \mapsto \frac{\eta(3\tau)\eta(\frac{1}{3}\tau+\frac{2}{3})}{\eta^2(\tau)},$$

είναι *modular* βάρους 72, ισχύουν οι προϋποθέσεις του θεωρήματος *Shimura-Gee* και τα t_n γεννούν το σώμα κλάσεων του *Hilbert*.

Ο νόμος αντιστροφής του Shimura μας επιτρέπει να υπολογίσουμε τα συζηγή του t_n με τρόπο παρόμοιο των σωμάτων του Hilbert.

Με την βοήθεια του gp-pari υπολογίζουμε τους πίνακες

Ο νόμος αντιστροφής του Shimura μας επιτρέπει να υπολογίσουμε τα συζηγή του t_n με τρόπο παρόμοιο των σωμάτων του Hilbert. Με την βοήθεια του gp-pari υπολογίζουμε τους πίνακες

n	$p_n(t)$
107	$x^3 - 2x^2 + 4x - 1$
131	$x^5 + x^4 - x^3 - 3x^2 + 5x - 1$
155	$x^4 + 2x^3 + 5x^2 + 4x - 1$
179	$x^5 - 2x^4 + 5x^3 - x^2 + 6x - 1$
203	$x^4 - 3x^3 + 7x - 1$
227	$x^5 - 5x^4 + 9x^3 - 9x^2 + 9x - 1$
251	$x^7 + 5x^6 + 6x^5 - 2x^4 - 4x^3 + 2x^2 + 9x - 1$
275	$x^4 - x^3 + 6x^2 - 11x + 1$
299	$x^8 + x^7 - x^6 - 12x^5 + 16x^4 - 12x^3 + 15x^2 - 13x + 1$
323	$x^4 - x^3 + 4x^2 + 13x - 1$
347	$x^5 + 7x^4 + 21x^3 + 27x^2 + 13x - 1$
371	$x^8 + 9x^6 - 10x^5 + 14x^4 + 8x^3 - 23x^2 + 18x - 1$
395	$x^8 - x^7 + 5x^6 + 16x^5 + 28x^4 + 24x^3 + 27x^2 + 17x - 1$
419	$x^9 - 6x^8 + 12x^7 - 7x^6 + 12x^5 - 8x^4 + 31x^3 + 10x^2 + 20x - 1$
443	$x^5 - 4x^4 - 3x^3 + 17x^2 + 22x - 1$
467	$x^7 + 6x^6 + 7x^5 - 3x^4 + 3x^3 - 23x^2 + 26x - 1$
491	$x^9 + x^8 + 16x^7 + 2x^6 + 37x^5 - 31x^4 + 44x^3 - 40x^2 + 29x - 1$
515	$x^6 + 8x^5 + 32x^4 + 60x^3 + 68x^2 + 28x - 1$
539	$x^8 - 6x^7 + 28x^6 - 56x^5 + 77x^4 - 56x^3 + 28x^2 - 34x + 1$
563	$x^9 + 4x^8 + 6x^7 - 11x^6 + 44x^5 - 76x^4 + 91x^3 - 64x^2 + 38x - 1$
587	$x^7 + x^6 + 16x^5 - 12x^4 + 20x^3 + 24x^2 + 39x - 1$
611	$x^{10} - 8x^9 + 35x^8 - 62x^7 - x^6 + 116x^5 - 65x^4 - 100x^3 + 125x^2 - 46x + 1$
635	$x^{10} - 11x^9 + 50x^8 - 121x^7 + 201x^6 - 192x^5 + 87x^4 + 51x^3 - 98x^2 + 49x - 1$
659	$x^{11} - 7x^{10} + 7x^9 + 27x^8 + 19x^7 - 43x^6 - 5x^5 + 91x^4 + 157x^3 + 97x^2 + 49x - 1$

n	$p_n(t)$
683	$x^5 + 6x^4 - 5x^3 - 41x^2 + 56x - 1$
707	$x^6 + 4x^5 + 30x^4 + 72x^3 + 108x^2 + 58x - 1$
731	$x^{12} + 7x^{11} + 25x^{10} + 12x^9 + 41x^8 + 9x^7 +$
	$+92x^6 + 73x^5 - 133x^4 + 216x^3 - 153x^2 + 67x - 1$
755	$x^{12} - 2x^{11} + 18x^{10} + 50x^9 + 82x^8 + 182x^7 + 360x^6 + 522x^5 +$
	$+598x^4 + 486x^3 + 262x^2 + 66x - 1$
779	$x^{10} + 8x^9 + 24x^8 - 8x^7 - 11x^6 + 26x^5 + 81x^4 + 220x^3 + 98x^2 + 74x - 1$
803	$x^{10} + 3x^9 + 26x^8 + 11x^7 - 65x^6 + 16x^5 + 7x^4 - 83x^3 + 150x^2 - 83x + 1$
827	$x^7 - 7x^6 + 38x^5 - 54x^4 + 112x^3 - 146x^2 + 89x - 1$
851	$x^{10} - 7x^9 - x^8 + 86x^7 + 69x^6 - 201x^5 - 219x^4 + 94x^3 + 103x^2 - 95x + 1$
875	$x^{10} - 10x^9 + 25x^8 + 10x^7 + 15x^6 + 94x^5 - 35x^4 - 120x^3 + 85x^2 + 100x - 1$
899	$x^{14} + 16x^{13} + 97x^{12} + 308x^{11} + 666x^{10} + 1086x^9 +$
	$+1490x^8 + 1766x^7 + 1800x^6 + 1556x^5 + 998x^4 + 698x^3 + 229x^2 + 106x - 1$
923	$x^{10} - x^9 + 30x^8 - 81x^7 - 29x^6 + 56x^5 + 211x^4 - 27x^3 - 110x^2 - 115x + 1$
947	$x^5 + 5x^4 + 7x^3 - 103x^2 + 125x - 1$
971	$x^{15} - x^{14} + 21x^{13} + 133x^{12} + 264x^{11} + 310x^{10} + 216x^9 +$
	$+62x^8 - 100x^7 - 300x^6 + 152x^5 + 338x^4 + 79x^3 - 285x^2 + 135x - 1$
995	$x^8 + 12x^7 + 59x^6 + 78x^5 + 12x^4 + 66x^3 + 289x^2 + 140x - 1$

Εφαρμογές στην Κρυπτογραφία

- Συστήματα δημοσίου κλειδιού βασισμένα στον διακριτό λογάριθμο σε ελλειπτικές καμπύλες.
- Θα πρέπει να ισχύουν μια σειρά από απαιτήσεις για να είναι ένα κρυπτοσύστημα ασφαλές. Προσπαθούμε να έχουμε ελλειπτικές καμπύλες (ορισμένες πάνω από ένα πεπερασμένο σώμα) με τάξη που να ικανοποιεί μία σειρά από προϋποθέσεις.
- Πως θα κατασκευάσουμε τέτοιες ελλειπτικές καμπύλες;

Εφαρμογές στην Κρυπτογραφία

- Συστήματα δημοσίου κλειδιού βασισμένα στον διακριτό λογάριθμο σε ελλειπτικές καμπύλες.
- Θα πρέπει να ισχύουν μια σειρά από απαιτήσεις για να είναι ένα κρυπτοσύστημα ασφαλές. Προσπαθούμε να έχουμε ελλειπτικές καμπύλες (ορισμένες πάνω από ένα πεπερασμένο σώμα) με τάξη που να ικανοποιεί μία σειρά από προϋποθέσεις.
- Πως θα κατασκευάσουμε τέτοιες ελλειπτικές καμπύλες;

Εφαρμογές στην Κρυπτογραφία

- Συστήματα δημοσίου κλειδιού βασισμένα στον διακριτό λογάριθμο σε ελλειπτικές καμπύλες.
- Θα πρέπει να ισχύουν μια σειρά από απαιτήσεις για να είναι ένα κρυπτοσύστημα ασφαλές. Προσπαθούμε να έχουμε ελλειπτικές καμπύλες (ορισμένες πάνω από ένα πεπερασμένο σώμα) με τάξη που να ικανοποιεί μία σειρά από προϋποθέσεις.
- Πως θα κατασκευάσουμε τέτοιες ελλειπτικές καμπύλες;

Ελλειπτικές καμπύλες με μιγαδικό πολλαπλασιασμό

- Αρκεί να προσδιορίσουμε το j.
- Το θεώρημα του Hasse μας εξασφαλίζει $Z = 4p - (p+1-m)^2 \geq 0 \Rightarrow Z = Dv^2$.
- Η εξίσωση

$$4p = u^2 + Dv^2$$

για κάποιο $u \in \mathbb{Z}$ ικανοποιεί την

$$m = p + 1 \pm u.$$

- Ο αρνητικός αριθμός $-D$ λέγεται CM διακρίνουσα για τον πρώτο p.

Ελλειπτικές καμπύλες με μιγαδικό πολλαπλασιασμό

- Αρκεί να προσδιορίσουμε το j.
- Το θεώρημα του Hasse μας εξασφαλίζει $Z = 4p - (p+1-m)^2 \geq 0 \Rightarrow Z = Dv^2$.
- Η εξίσωση
$$4p = u^2 + Dv^2$$
για κάποιο $u \in \mathbb{Z}$ ικανοποιεί την
$$m = p + 1 \pm u.$$
- Ο αρνητικός αριθμός $-D$ λέγεται CM διακρίνουσα για τον πρώτο p.

Ελλειπτικές καμπύλες με μιγαδικό πολλαπλασιασμό

- Αρκεί να προσδιορίσουμε το j.
- Το θεώρημα του Hasse μας εξασφαλίζει $Z = 4p - (p+1-m)^2 \geq 0 \Rightarrow Z = Dv^2$.
- Η εξίσωση
$$4p = u^2 + Dv^2$$
για κάποιο $u \in \mathbb{Z}$ ικανοποιεί την
$$m = p + 1 \pm u.$$
- Ο αρνητικός αριθμός $-D$ λέγεται CM διακρίνουσα για τον πρώτο p.

Ελλειπτικές καμπύλες με μιγαδικό πολλαπλασιασμό

- Αρκεί να προσδιορίσουμε το j.
- Το θεώρημα του Hasse μας εξασφαλίζει $Z = 4p - (p + 1 - m)^2 \geq 0 \Rightarrow Z = Dv^2$.
- Η εξίσωση
$$4p = u^2 + Dv^2$$
για κάποιο $u \in \mathbb{Z}$ ικανοποιεί την
$$m = p + 1 \pm u.$$
- Ο αρνητικός αριθμός $-D$ λέγεται CM διακρίνουσα για τον πρώτο p.

- Διαλέγουμε ένα πρώτο p. Διαλέγουμε την μικρότερη D μαζί με $u, v \in \mathbb{Z}$ ώστε να έχει λύση η $4p = u^2 + Dv^2$.
- Αν μία από τις τιμές $p+1-u$,$p+1+u$ είναι κατάλληλη τάξη τότε προχωρούμε στην κατασκευή της ελλειπτικής καμπύλης. Αν όχι δοκιμάζουμε με άλλο πρώτο.
- Αν η τιμή είναι κατάλληλη υπολογίζουμε το Hilbert πολυώνυμο, και υπολογίζουμε τις ρίζες του modulo p. Μία από αυτές είναι η j-αναλλοίωτη που ψάχνουμε.

- Διαλέγουμε ένα πρώτο p. Διαλέγουμε την μικρότερη D μαζί με $u, v \in \mathbb{Z}$ ώστε να έχει λύση η $4p = u^2 + Dv^2$.
- Αν μία από τις τιμές $p+1-u, p+1+u$ είναι κατάλληλη τάξη τότε προχωρούμε στην κατασκευή της ελλειπτικής καμπύλης. Αν όχι δοκιμάζουμε με άλλο πρώτο.
- Αν η τιμή είναι κατάλληλη υπολογίζουμε το Hilbert πολυώνυμο, και υπολογίζουμε τις ρίζες του modulo p. Μία από αυτές είναι η j-αναλλοίωτη που ψάχνουμε.

- Διαλέγουμε ένα πρώτο p. Διαλέγουμε την μικρότερη D μαζί με $u, v \in \mathbb{Z}$ ώστε να έχει λύση η $4p = u^2 + Dv^2$.
- Αν μία από τις τιμές $p+1-u$,$p+1+u$ είναι κατάλληλη τάξη τότε προχωρούμε στην κατασκευή της ελλειπτικής καμπύλης. Αν όχι δοκιμάζουμε με άλλο πρώτο.
- Αν η τιμή είναι κατάλληλη υπολογίζουμε το Hilbert πολυώνυμο, και υπολογίζουμε τις ρίζες του modulo p. Μία από αυτές είναι η j-αναλλοίωτη που ψάχνουμε.

Απλοποίηση με τις t_n Ramanujan τιμές

- Αντί να υπολογίσουμε τα πολυώνυμο του Hilbert υπολογίζουμε τα πολυώνυμα $p_n(t)$. και κατασκευάζουμε με διαφορετικό τρόπο το σώμα Hilbert.
- Κάνουμε αναγωγή modulo p και υπολογίζουμε μια ρίζα $t_{0,n}$ των $p_n \mod p$.
- Υπάρχει τύπος που μας εκφράζει τα $j_0 \in \mathbb{F}_p$ συναρτήσει των $t_{n,0}$.

Απλοποίηση με τις t_n Ramanujan τιμές

- Αντί να υπολογίσουμε τα πολυώνυμο του Hilbert υπολογίζουμε τα πολυώνυμα $p_n(t)$. και κατασκευάζουμε με διαφορετικό τρόπο το σώμα Hilbert.
- Κάνουμε αναγωγή modulo p και υπολογίζουμε μια ρίζα $t_{0,n}$ των $p_n \mod p$.
- Υπάρχει τύπος που μας εκφράζει τα $j_0 \in \mathbb{F}_p$ συναρτήσει των $t_{n,0}$.

Απλοποίηση με τις t_n Ramanujan τιμές

- Αντί να υπολογίσουμε τα πολυώνυμο του Hilbert υπολογίζουμε τα πολυώνυμα $p_n(t)$. και κατασκευάζουμε με διαφορετικό τρόπο το σώμα Hilbert.
- Κάνουμε αναγωγή modulo p και υπολογίζουμε μια ρίζα $t_{0,n}$ των $p_n \mod p$.
- Υπάρχει τύπος που μας εκφράζει τα $j_0 \in \mathbb{F}_p$ συναρτήσει των $t_{n,0}$.

Έχει το κινητό σας μια Ελλειπτική καμπύλη;

- Ο αλγορίθμος κατασκευής ελλεπτικών καμπύλων που βασίζεται στην κατασκευή του πολυωνύμου Hilbert δεν μπορεί να εφαρμοστεί σε συσκευές με περιορισμένες υπολογιστικές δυνατότητες: κινητά τηλέφωνα, smart cards, hand held devices.
- Ο αλγόριθμος που βασίζεται στις Ramanujan τιμές υπερτερεί και στην κατασκευή των πολυωνύμων p_n αλλά και στην ποσότητα μνήμης που απαιτείται για τον χειρισμό και την αποθηκευσή τους στην μνήμη.