Θεωρία Κλάσεων Σωμάτων και Εφαρμογές στην Κρυπτογραφία

Νίκος Γκερπινής

27/6/05

- Ανάλυση στοιχείων μέσα σε έναν δακτύλιο ακεραίων $\mathfrak{D}_K$, ενός σώματος K.
- Σε κάθε $\mathfrak{D}_K$ είναι δυνατή η ανάλυση ενός στοιχείου, αλλά δεν είναι πάντα περιοχή μοναδικής ανάλυσης.

- Δουλεύουμε σε τετραγωνικά μιγαδικά σώματα αριθμών, $\mathbb{Q}(\sqrt{d})$. Είναι $d < 0$ και ελεύθερος τετραγώνων.
- Ο δακτύλιος ακεραίων ενός $\mathbb{Q}(\sqrt{d})$ είναι

1. $\mathfrak{D}_K = \mathbb{Z}[\sqrt{d}]$, αν $d \not\equiv 1 \bmod 4$ και $D = 4d$
2. $\mathfrak{D}_K = \mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{d}]$, αν $d \equiv 1 \bmod 4$ και $D = d$.

- Ανάλυση ιδεωδών σε δακτυλίους ακεραίων τετραγωνικών μιγαδικών σωμάτων αριθμών.

• **Θεώρημα:** Τα μη μηδενικά κλασματικά ιδεώδη ενός δακτυλίου ακεραίων, έχουν μονοσήμαντη ανάλυση σε γινόμενο πρώτων ιδεωδών.
• Αν $\mathfrak{a} \subseteq \mathfrak{D}_K$ ορίζεται η νόρμα του ιδεώδους να είναι

$$N(\mathfrak{a}) = |\mathfrak{D}_K/\mathfrak{a}|.$$

• Αν έχουμε $\mathfrak{a} = \langle \alpha \rangle$ τότε $N(\mathfrak{a}) = |N(\alpha)|$.
• Αν $K = \mathbb{Q}(\sqrt{d})$ είναι $|N(\alpha)| = |x^2 - dy^2|$.

Ορισμός: Class group $\mathcal{H}$, είναι το πηλίκο της ομάδας $\mathcal{F}$ των κλασματικών ιδεωδών, προς την ομάδα $\mathcal{P}$ των κύριων κλασματικών ιδεωδών.

- Δύο $\mathfrak{x},\ \mathfrak{y} \in \mathcal{F}$ είναι ισοδύναμα αν

$$\mathfrak{x}\mathfrak{d} = \mathfrak{y}\mathfrak{e},$$

με $\mathfrak{d},\ \mathfrak{e} \in \mathcal{P}$. Το σύνολο αυτών των κλάσεων $[\mathfrak{x}]$, είναι η class group.

- Αν $\mathfrak{D}_K$ είναι ΠΜΑ, τότε η $h = |\mathcal{H}| = 1$.

Θεώρημα: Κάθε μη μηδενικό ιδεώδες $\mathfrak{a}$ του $\mathfrak{D}_K$, είναι ισοδύναμο με ένα ιδεώδες του οποίου η νόρμα είναι $\leq (\frac{2}{\pi})^t \sqrt{|D|}$.

Παράδειγμα: Έστω $\mathbb{Q}(\sqrt{-5})$. Τότε $t = 1$ και $D = 4d = 4(-5) = -20$. Η νόρμα κάθε ιδεώδους του $\mathbb{Z}[\sqrt{-5}]$ είναι ≤ 2.85. Όλα δηλαδή τα ιδεώδη έχουν νόρμα 1 ή 2. Τα ιδεώδη με νόρμα 1 είναι όλος ο $\mathfrak{D}_K$ και ένα ιδεώδες του $\mathbb{Q}(\sqrt{-5})$ που έχει νόρμα 2, είναι το $\langle 2, 1 + \sqrt{-5} \rangle$. Άρα $h = 2$.

Νόμος ανάλυσης σε έναν $\mathfrak{D}_K$.

Θεώρημα: Έστω K ένα σώμα αριθμών βαθμού n και $\mathfrak{D}_K = \mathbb{Z}[\theta]$, ο οποίος παράγεται από το $\theta \in \mathfrak{D}_K$. Έστω ότι έχουμε έναν πρώτο αριθμό p και το ελάχιστο πολυώνυμο f του θ στο $\mathbb{Q}$, έχει ανάλυση σε ανάγωγα πάνω από το $\mathbb{Z}_p$,

$$f = f_1^{e_1} ... f_r^{e_r}.$$

Τότε αν f_i ένα οποιοδήποτε από αυτά τα πολυώνυμα $\mathrm{mod} p$, το ιδεώδες $\mathfrak{p}_i = \langle p \rangle + \langle f_i(\theta) \rangle$ θα είναι πρώτο ιδεώδες και η ανάλυση του $\langle p \rangle$ σε πρώτα ιδεώδη στον $\mathfrak{D}_K$ είναι

$$\langle p \rangle = \mathfrak{p}_1^{e_1} ... \mathfrak{p}_r^{e_r}.$$

Παράδειγμα: Έχουμε $\mathbb{Q}(\sqrt{-1})$. Είναι $\theta = \sqrt{-1}$ με ελάχιστο πολυώνυμο το $t^2 + 1$.

Ζητάμε ανάλυση του $\langle 2 \rangle$. Είναι

$$t^2 + 1 = (t+1)^2 \bmod 2,$$

άρα

$$\langle 2 \rangle = \mathfrak{p}^2,$$

και το $\mathfrak{p}$ είναι ένα πρώτο ιδεώδες. Είναι

$$\mathfrak{p} = \langle 2 \rangle + \langle \sqrt{-1} + 1 \rangle = \langle 1 + \sqrt{-1} \rangle.$$

Η ανάλυση του $\langle 2 \rangle$ στον $\mathfrak{D}_K$ είναι

$$\langle 2 \rangle = \langle 1 + \sqrt{-1} \rangle^2$$

Ανάλυση ιδεωδών σε επεκτάσεις Galois.

Έστω $\mathfrak{p}$ πρώτο ιδεώδες του $\mathfrak{D}_K$. Σαν ιδεώδες μιας επέκτασης $K \subset L$ έχει ανάλυση σε πρώτα ιδεώδη

$$\mathfrak{p} = \mathfrak{B}_1^{e_1} ... \mathfrak{B}_g^{e_g}.$$

Τα e_i λέγονται δείχτες διακλάδωσης. Κάθε πρώτο ιδεώδες $\mathfrak{B}_i$ δίνει μία επέκταση $\mathfrak{D}_K/\mathfrak{p} \subset \mathfrak{D}_L/\mathfrak{B}_i$, με βαθμό f_i που ονομάζεται βαθμός αδράνειας.

1. Αν $e_i = 1$, τότε το $\mathfrak{p}$ είναι αδιακλάδωτο πάνω από το $\mathfrak{B}$.

2. Αν και το $f_i = 1$, τότε το $\mathfrak{p}$ διασπάται πλήρως πάνω από το $\mathfrak{B}$.

Θεώρημα: Έστω επέκταση Galois $K \subset L$, με $L = K(\alpha),\ \alpha \in \mathfrak{D}_L$ και $f(x)$ το ελάχιστο πολυώνυμο του α πάνω από το K, τέτοιο ώστε $f(x) \in \mathfrak{D}_K[x]$. Αν το $\mathfrak{p}$ είναι πρώτο στο $\mathfrak{D}_K$ και το $f(x)$ αναλύεται πλήρως $\mathrm{mod}\mathfrak{p}$, τότε έχουμε:

1. Το $\mathfrak{p}$ είναι αδιακλάδωτο στο L.

2. Αν $f(x) \equiv f_1(x)...f_g(x) \bmod \mathfrak{p}$, όπου τα $f_i(x)$ είναι ανάγωγα $\mathrm{mod}\mathfrak{p}$ τότε το $\mathfrak{B}_i = \mathfrak{p}\mathfrak{D}_L + f_i(\alpha)\mathfrak{D}_L$ είναι πρώτο ιδεώδες του $\mathfrak{D}_L$ με $\mathfrak{B}_i \neq \mathfrak{B}_j,\ i \neq j$, και $\mathfrak{p}\mathfrak{D}_L = \mathfrak{B}_1...\mathfrak{B}_g$. Επιπλέον όλα τα $f_i(x)$, έχουν τον ίδιο βαθμό, ο οποίος είναι ο βαθμός αδράνειας f.

3. Το $\mathfrak{p}$ διασπάται πλήρως στο L, αν και μόνο αν η $f(x) \equiv 0 \bmod \mathfrak{p}$ έχει $\deg f$ το πλήθος λύσεις στο $\mathfrak{D}_K$.

Θεώρημα: Αν έχουμε ένα σώμα αριθμών K, τότε υπάρχει μία πεπερασμένη επέκταση Galois L, για την οποία θα είναι:

1. Η L είναι αδιακλάδωτη αβελιανή επέκταση του K.
2. Κάθε αδιακλάδωτη αβελιανή επέκταση του K, βρίσκεται μέσα στην L.

Ένα τέτοιο σώμα L, λέγεται σώμα κλάσεων του Hilbert, για το K. Είναι η μέγιστη αβελιανή επέκταση για το K και είναι μοναδική.

1. Ομάδα διακλάδωσης του $\mathfrak{B}$, $D_{\mathfrak{B}} = \{\sigma \in Gal(L/K) : \sigma(\mathfrak{B}) = \mathfrak{B}\}$, με τάξη $|D_{\mathfrak{B}}| = e_{\mathfrak{B}|\mathfrak{p}} f_{\mathfrak{B}|\mathfrak{p}}$.

2. Ομάδα αδράνειας του $\mathfrak{B}$, $I_{\mathfrak{B}} = \{\sigma \in Gal(L/K) : \sigma(\alpha) \equiv \alpha \bmod \mathfrak{B}\}$, με τάξη $|I_{\mathfrak{B}}| = e_{\mathfrak{B}|\mathfrak{p}}$.

Έστω επέκταση Galois $K \subset L$, και $\mathfrak{p}$ ένα πρώτο ιδεώδες του $\mathfrak{D}_K$, αδιακλάδωτο στο L. Αν το $\mathfrak{B}$ είναι πρώτο του $\mathfrak{D}_L$ και το οποίο να περιέχει το ιδεώδες $\mathfrak{p}$, τότε υπάρχει ένα μοναδικό στοιχείο $\sigma \in D_{\mathfrak{B}}$, τέτοιο ώστε για κάθε $\alpha \in \mathfrak{D}_L$ να είναι,

$$\sigma(\alpha) = \alpha^{N(\mathfrak{p})} \bmod \mathfrak{B},$$

όπου $N(\mathfrak{p}) = |\mathfrak{D}_K/\mathfrak{p}|$, η νόρμα του ιδεώδους $\mathfrak{p}$.
Το μοναδικό στοιχείο σ του προηγούμενου λήμματος, καλείται σύμβολο του Artin και θα το συμβολίζουμε από εδώ και πέρα $\left(\frac{L/K}{\mathfrak{B}}\right)$.

• Αν $K \subset L$ αβελιανή επέκταση Galois επέκταση, το σύμβολο Artin εξαρτάται μόνο από το ιδεώδες $\mathfrak{p}$, οπότε γράφουμε $(\frac{L/K}{\mathfrak{p}})$.
• Το $\mathfrak{p}$ διασπάται πλήρως στο L, αν και μόνο αν $((L/K)/\mathfrak{B}) = 1$.
• Σε ένα τετραγωνικό σώμα $\mathbb{Q}(\sqrt{d})$, ένα p διασπάται πλήρως αν έχουμε

$$t^2 - d \equiv 0 \bmod p.$$

Δηλαδή το d γράφεται σαν τετράγωνο mod$p$. Άρα το σύμβολο του Legendre δίνει

$$\left(\frac{d}{p}\right) = 1,$$

που το ίδιο μας λέει και το σύμβολο Artin.

- Έστω $\mathfrak{a} \in \mathcal{F}$ και η ανάλυσή του σε πρώτα ιδεώδη $\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{r_i}$.
- $\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_{i=1}^{r} \left(\frac{L/K}{\mathfrak{p}_i}\right)^{r_i}$.
- Το σύμβολο του Artin ορίζει ομομορφισμό :

$$\left(\frac{L/K}{\cdot}\right) : \mathcal{F} \longrightarrow Gal(L/K).$$

Θεώρημα: Έστω L το σώμα κλάσεων του Hilbert ενός σώματος αριθμών, K. Τότε ο ομομορφισμός Artin

$$\left(\frac{L/K}{\cdot}\right) : \mathcal{F} \longrightarrow Gal(L/K),$$

είναι επί και έχει πυρήνα την ομάδα των κύριων κλασματικών ιδεωδών $\mathcal{P}$. Επομένως, σύμφωνα με το θεμελιώδες θεώρημα του ισομορφισμού, θα έχουμε:

$$\mathcal{H} \cong Gal(L/K).$$

Θεώρημα: Αν έχουμε ένα σώμα αριθμών K, τότε υπάρχει μία ένα προς ένα αντιστοιχία μεταξύ των αδιακλάδωτων αβελιανών επεκτάσεων του K, και των υποομάδων H της ομάδας κλάσεων ιδεωδών $\mathcal{H}$. Επιπλέον, αν μία επέκταση M, αντιστοιχεί σε μία υποομάδα $H \subset \mathcal{H}$, ο Artin ομομρφισμός θα επάγει ισομορφισμό

$$\mathcal{H}/H \cong Gal(M/K).$$

Θεώρημα: Έστω L το σώμα κλάσεων του Hilbert, ενός σώματος αριθμών K. Έστω επίσης ένα πρώτο ιδεώδες $\mathfrak{p}$, του K. Τότε το $\mathfrak{p}$ θα διασπάται πλήρως στο L, αν και μόνο αν είναι κύριο ιδεώδες.

Ελλειπτικές Καμπύλες

• Μία ελλειπτική καμπύλη ορισμένη στο K, είναι το αλγεβρικό σύνολο $V(f)$ ενός f ομογενούς πολυωνύμου βαθμού $\deg f = 3$, τέτοιο ώστε το $V(f)$ να είναι παντού ομαλό.
• Μία ελλειπτική καμπύλη πάνω από το K ορίζεται να είναι το σύνολο των λύσεων στο προβολικό επίπεδο $\mathbb{P}^2(K)$, της ομογενούς μακράς εξίσωσης του Weierstrass,

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

με $a_1, a_2, a_3, a_4, a_6 \in K$ μαζί με το σημείο στο άπειρο $\mathcal{O}$.
• Μετά από αποομογενοποίηση και κατάλληλη αλλαγή συντεταγμένων, η εξίσωση μιας ελλειπτικής καμπύλης θα δίνεται από

$$Y^2 = X^3 + aX + b,\ \ a, b \in K.$$

Νόμος ομάδας

• Τα ρητά σημεία μιας ελλειπτικής καμπύλης, μαζί με το σημείο $\mathcal{O}$, έχουν δομή αβελιανής ομάδας, με πράξη την πρόσθεση σημείων ορισμένη ως εξής.
• $P, Q \in E(K)$ και R το τρίτο σημείο της $E(K)$ που τέμνει η PQ την $E(K)$. Το σημείο $P + Q$ είναι το συμμετρικό του R. Ουδέτερο στοιχείο της πράξης είναι το $\mathcal{O}$.

• Οι εφαρμογές της θεωρίας των Ε.Κ. στην κρυπτογραφία, είναι για Ε.Κ. ορισμένες πάνω από πεπερασμένα σώματα, $E(\mathbb{F}_q)$.

• Πολύ σημαντικό ζήτημα είναι η εύρεση της τάξης $|E(\mathbb{F}_q)|$.

• Ένα φράγμα για την τάξη έδωσε ο Hasse :

$$||E(\mathbb{F}_q)| - q - 1| \leq 2\sqrt{q}.$$

• Η τάξη μιας $E(\mathbb{F}_q)$ υπολογίζεται από

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

με t να είναι το ίχνος του Frobenius.
Θα δούμε δύο μεθόδους υπολογισμού της τάξης $|E(\mathbb{F}_q)|$.

1. Αλγόριθμος του Schoof,
2. Ε.Κ. με μιγαδικό πολλαπλασιασμό.

ΠΔΛΕΚ

• Τα κρυπτοσυστήματα είναι βασισμένα στο πρόβλημα του διακριτού λογάριθμου για ελλειπτικές καμπύλες (ΠΔΛΕΚ).

• Αν έχουμε $Q, P \in \mathbb{F}_q$ με $Q = \langle P \rangle$, το ΠΔΛΕΚ είναι η εύρεση ενός ακεραίου αριθμού m τέτοιου ώστε

$$Q = mP.$$

• Ζήτημα για κρυπταναλυτές : εύρεση κατάλληλης Ε.Κ.
• Η τάξη $|E(\mathbb{F}_q)|$ πρέπει να πληρεί κάποιες προυποθέσεις για την αποφυγή επιθέσεων στα κρυπτοσυστήματα.

1. $|E(\mathbb{F}_q)| = rs$, με r έναν μεγάλο πρώτο αριθμό.
2. $t \neq 1$ (συνθήκη ανωμαλίας).
3. $t \neq 0, 2$ και το t να μην διαιρεί την χαρακτηριστική του σώματος $\mathbb{F}_q$ (συνθήκη MOV).

Ο Αλγόριθμος του Schoof

- Η $E(\mathbb{F}_q)$ είναι γνωστή και αναζητούμε την τάξη της.
- Ενδομορφισμός του Frobenius : $\phi : (x, y) \mapsto (x^q, y^q)$.
- Ικανοποιεί : $\phi^2(P) - t\phi(P) + qP = \mathcal{O},\ P \in E(\mathbb{F}_q)$.
- $P \in E[l] = \{P \in E(\mathbb{F}_q) : lP = \mathcal{O}\}$.
- Δοκιμάζει τις τιμές $\tau \in \{2, ..., l-1\}$ για l πρώτους με $l \leq l_{max}$ ο μικρότερος πρώτος όπου $\prod l > 4\sqrt{q}$.
- Με κινέζικο θεώρημα υπολογίζει το ίχνος του Frobenius t.

Μιγαδικός Πολλαπλασιασμός

- Κατασκευή ελλειπτικών καμπύλων με γνωστή τάξη.
- Η εύρεση της τάξης $E(\mathbb{F}_q)$ είναι πάλι το πρόβλημα.
- Μειονέκτημα της μεθόδου : Συγκεκριμένη οικογένεια καμπύλων, δηλ. λίγες επιλογές στην κατασκευή ενός κρυπτοσυστήματος.

Ορίζουμε την j αναλλοίωτο μιας Ε.Κ.

- $\mathbb{H} = \{z \in \mathbb{C} : Im(z) > 0\}$.
- $E_\tau \cong \mathbb{C}/\Lambda,\ \Lambda = \mathbb{Z} + \tau\mathbb{Z},\ \tau \in \mathbb{H}$.
- Η j είναι μία συνάρτηση $j : \mathbb{H} \longrightarrow \mathbb{C}$, περιοδική και δέχεται ανάλυση Fourier

$$j(q) = \frac{1}{q} + \sum c(n)q^n,\ q = e^{2\pi iz}.$$

$$j(q) = \frac{1}{q} + 744 + 19688q + 21493760q^2 + 864299970q^3 + 20245856256q^4$$

• $End(E)$ είναι ο δακτύλιος όλων των ισογενειών από την E στον εαυτό της.
• Αν ο $End(E) \cong \mathbb{Z} + \tau\mathbb{Z}$, δηλαδή έχει δομή μιας order τετραγωνικού μιγαδικού σώματος, λέμε ότι η E.K. έχει μιγαδικό πολλαπλασιασμό.

Θεώρημα: Έστω $\tau \in \mathbb{H}$ να είναι ένας μιγαδικός αλγεβρικός αριθμός. Τότε αν θέσουμε $E_\tau = \frac{\mathbb{C}}{\mathbb{Z}+\tau\mathbb{Z}}$, η ελλειπτική καμπύλη E_τ έχει μιγαδικό πολλαπλασιασμό, και το $j(\tau)$ είναι ακέραιος αλγεβρικός. Επιπλέον το σώμα $K(j(\tau))$ είναι το Hilbert class field του σώματος $\mathbb{Q}(\tau)$.

Θεώρημα: Αν το K είναι το πεπερασμένο σώμα $\mathbb{F}_p$, και $j_0 \in \mathbb{F}_p$, $j \neq 0, 1728 \bmod p$, τότε οι δύο ελλειπτικές καμπύλες E_1, E_2 που έχουν j-ανναλοίωτο j_0 θα έχουν τάξεις

$$|E_1| = p + 1 - t, \ |E_2| = p + 1 + t.$$

Θεώρημα: Έστω τ όπως ορίστηκε πριν και με διακρίνουσα $-D$. Δηλαδή $-D$ είναι η διακρίνουσα της πρωταρχικής τετραγωνικής μορφής $Q(x, y)$, η οποία έχει το τ σαν ρίζα της $Q(x, 1) = 0$. Έστω h_D ο αριθμός κλάσεων της order με διακρίνουσα $-D$. Τότε το $j(\tau)$ είναι ακέραιος αλγεβρικός και το ελάχιστο πολυώνυμό του δίνεται από

$$H_D(x) = \prod(x - j(\alpha)),$$

όπου το α διατρέχει όλους τους μιγαδικούς αριθμούς τέτοιους ώστε, το $(\alpha, 1)$ να είναι μία ρίζα μιας εκ των h_D το πλήθος ανηγμένων πρωταρχικών μορφών διακρίνουσας $-D$.

1. Επιλέγουμε έναν μεγάλο πρώτο.
2. Βρίσκουμε την λύση της $4p = u^2 + Dv^2$ για την μικρότερη τιμή της D.
3. Υπολογίζουμε την τάξη της $p + 1 \pm u$ και ελέγχουμε αν πληρεί τις προϋποθέσεις μας.
4. Υπολογίζουμε το πολυώνυμο Hilbert και μία ρίζα του $\mathrm{mod} p$, έστω j. Αυτή είναι η j αναλλοίωτος που χαρακτηρίζει την ελλειπτική καμπύλη που ψάχνουμε.
5. Παίρνουμε δύο ελλειπτικές καμπύλες με την ίδια j και επιλέγουμε ποια έχει την τάξη που έχουμε βρει.