Η Μέθοδος του Chabauty και Ακέραια σημεία επί Ελλειπτικών Καμπύλων

Δραζιώτης Κ.

18 Νοεμβρίου 2008, Ιωάννινα

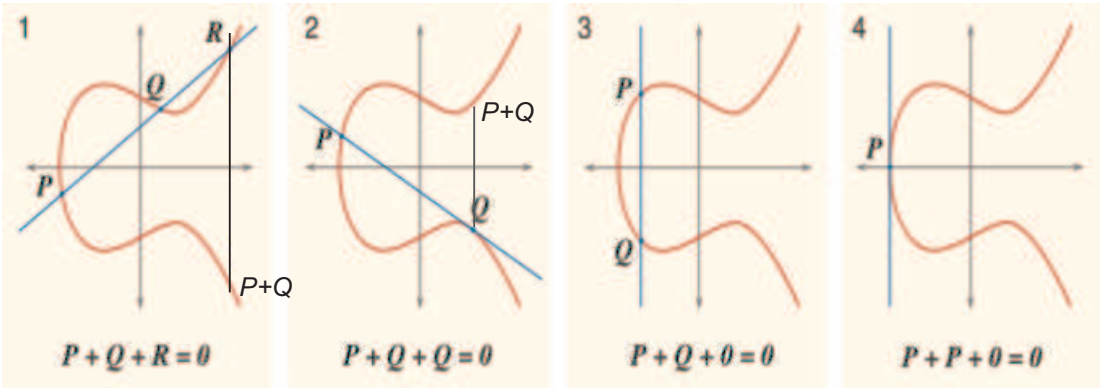
Ελλειπτικές καμπύλες πάνω σε σώματα αριθμών

Έστω K ένα σώμα αριθμών και $\overline{K}$ μια αλγεβρική του θήκη. Ας είναι E η αλγεβρική καμπύλη που ορίζεται από την εξίσωση

$$E : y^2 = x^3 + Ax + B, \quad A, B \in K, \quad 4A^3 + 27B^2 \neq 0.$$

Ελλειπτική καμπύλη επί του K είναι το σύνολο των σημείων της E με συντεταγμένες από το K μαζί με το σημείο $[0 : 1 : 0]$, στο άπειρο του προβολικού της μοντέλου.

Επί των $K-$σημείων της μπορούμε να ορίσουμε μια πράξη ως εξής :



Σχημα 1. Το ουδέτερο στοιχείο της πρόσθεσης είναι το σημείο στο άπειρο, το οποίο σε προβολικές συν/νες είναι το σημείο $\mathbf{0} = [0 : 1 : 0]$.

Η πράξη αυτή είναι αβελιανή. Ο Mordell απέδειξε ότι αν $K = \mathbb{Q}$ τότε είναι πεπερασμένα παραγόμενη και ο Neron γενίκευσε για την περίπτωση όπου $K \neq \mathbb{Q}$. Άρα

$$E(K) \simeq E_{torsion}(K) \oplus \mathbb{Z}^r.$$

Το r ονομάζεται τάξη (rank) της ελλειπτικής πάνω στο K. Το σύνολο $E_{torsion}(\mathbb{Q})$ ελέγχεται από το θέωρημα των Lutz-Nagel :
Αν $(a, b) \in E_{torsion}(\mathbb{Z})$ *τότε είτε* $b = 0$ *είτε* $b|\Delta_E$ *όπου* $\Delta_E = -16(4A^3 + 27B^2)$.

EIlisabeth Lutz (1937). Sur L'equation $y^2 = x^2 - Ax - B$ *dans les corps p-adiques. J. Reine Angew. Math. 177:* 237 – 247.

Επίσης ο *Mazur* απόδειξε ότι η ομάδα $E_{torsion}(\mathbb{Q})$ είναι ισόμορφη με μία από τις παρακάτω :

$$\mathbb{Z}/m\mathbb{Z}, \quad 1 \leq m \leq 10 \text{ ή } m = 12$$

είτε

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Η εύρεση της τάξης μιας ελλειπτικής επί του $\mathbb{Q}$ είναι, στην πράξη, τις περισσότερες φορές εύκολος. Γενικά όμως, δεν υπάρχει αλγόριθμος για την εύρεση της τάξης μιας ελλιπτικής καμπύλης. Η διαδικασία αυτή είναι ακόμη δυσκολότερη επί ενός σώματος αριθμών αν ο βαθμός του είναι μεγάλος. Ακόμη όμως και αν έχουμε βρεί την τάξη η εύρεση μιας βάσης δηλ. r ανεξάρτητων σημείων, άπειρης τάξης, επί της ελλειπτικής δεν είναι εύκολο πρόβλημα. Ειδικότερα, δεν υπάρχει αλγόριθμος που να μας δίνει αυτή την βάση

στους ρητούς. Στην πράξη όμως συνήθως μπορούμε να τη βρούμε (2-descend method).
Αν η καμπύλη μας έχει τάξη μηδέν, τότε ο προσδιορισμός των ακέραιων (και ρητών) σημείων του είναι πολύ απλός (εφαρμογή του Lutz-Nagel θεωρήματος). Τα ακέραια σημεία μιας ελλειπτικής (επί ενος τυχαίου σώματος αριθμών) είναι πάντα πεπερασμένα (θεώρημα του Siegel). Τα ρητά είναι άπειρα αρκεί να έχει τάξη τουλάχιστον ένα (επί του σώματος αριθμών).

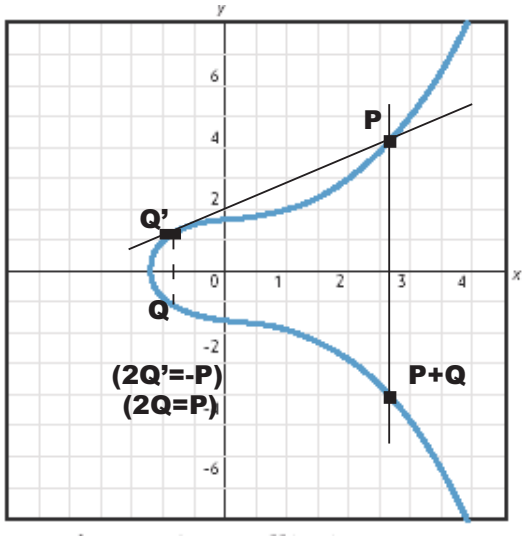
Η μελέτη των ακέραιων σημείων μιας ελλειπτικής γίνεται με αρκετές μεθόδους. Η πιο γενική είναι αυτή των Tzanakis-Stroker και Gebel-Petho-Zimmer- η οποία ονομάζεται *μέθοδος των ελλειπτικών λογαρίθμων*. Η μέθοδος αυτή είναι γνώστη από παλαιότερα για παραδειγμα από τον Serge Lang. Το μειονέκτημα αυτής της μεθόδου είναι ότι απαιτεί την εύρεση μιας βάσης της ελλειπτικής. Κατόπιν, υπάρχεί η *μέθοδος Thue* η οποία τελικά χρησιμοποιεί την μέθοδο του Baker. Αυτή η μέθοδος δεν δουλευει πάντα. Μέτα υπάρχουν μέθοδοι ad hoc που χρησιμοποίουν στοιχειώδη θεωρία αριθμών (σύμβολο Legendre, αναγωγή $\mod p$ κ.α.).

Σε αύτη την ομιλία θα ασχοληθούμε με μια "νέα" τεχνική για την επίλυση των ελλειπτικών επί των ακεραίων την μέθοδο διπλασιασμού σημείου του Chabauty. Η μέθοδος αύτη πρώτη φορά εμφανίζεται στην εργασία του Chabauty

Démonstration de quelques lemmes de rehaussement. (French) C. R. Acad. Sci. Paris 217, (1943) 413 – 415.

Η μέθοδος του Chabauty σε σώματα αριθμών

Η μέθοδος του Chabauty ισχυρίζεται στην ουσία ότι η επίλυση της εξίσωσης $2Q = P$, όπου $P \in E(\mathbb{Z})$, $Q \in E(\overline{\mathbb{Q}})$, μας προσδιορίζει το σύνολο $E(\mathbb{Z})$. Αν $P = (a, b)$, $Q = (s, t)$ τότε μπορούμε να βρούμε μια σχέση $\Theta(a, s) = 0$ και κατόπιν μια σχέση $R(s) = 0$. Οπότε λύνοντας την τελευταία μπορούμε να βρούμε το a. Επομένως, αρχικά αναζητούμε σημείο Q τέτοιο ώστε $2Q = P$.



Σχημα 2. Το σημείο που ψάχνουμε είναι το $Q = (s, t)$

Αν βρούμε το Q τότε πολύ εύκολα βρίσκουμε το P. Από την σχέση $2(s, t) = (a, b)$ βρίσκουμε ότι

$$a = \frac{s^4 - 2As^2 - 8Bs + A^2}{4(s^3 + As + B)}.$$

Από όπου προκύπτει

$$\Theta_a(s) = s^4 - 4as^3 - 2As^2 - (4Aa + 8B)s - 4Ba + A^2 = 0.$$

Αν $S = \{p \in \text{spec}(\mathbb{Z}) : p \big| \Delta_E\}$, και e_1, e_2, e_3 οι ρίζες του $X^3 + AX + B$. Για την εύρεση του s η μέθοδος του Chabauty ισχυρίζεται ότι τα $s_1 = s - e_1,\ s_2 = s - e_2$ είναι $S-units$ στο σώμα $\mathbb{Q}(s)$ και παρατηρούμε ότι ικανοποιούν την εξίσωση $s_1 - s_2 = e_2 - e_1$. Το σώμα που ορίζει το s είναι (το πολύ) τετάρτου βαθμού και από το γενικό θεώρημα Neron-Ogg-Shafarevich βρίσκουμε ότι το σώμα $\mathbb{Q}(e_1, e_2, e_3)(2^{-1}(E(\mathbb{Z}))$ είναι μη διακλαδιζόμενο εξω από το σύνολο των πρώτων που διαιρούν την διακρίνουσα Δ_E, επομένως, το ίδιο θα συμβαίνει και με το σώμα $\mathbb{Q}(s)$. Άρα από το θεώρημα του Hermite προκύπτει ότι υπάρχουν πεπερασμένα σώματα $\mathbb{Q}(s)$. Σε κάθε ένα από τα σώματα λύνουμε την εξίσωση των μονάδων

$$X - Y = e_2 - e_1.$$

Υπάρχουν δύο μέθοδοι να βρίσκουμε σώματα συγκεκριμένου βαθμού μη διακλαδιζόμενα έξω από ένα σύνολο S πρώτων αριθμών. Υπάρχει η μέθοδος του Hunter και η μέθοδος που χρησιμοποιεί Class field Theory. Αυτές περιγράφονται στο βιβλίο του H.Cohen

Advance Topics in Computational Number Theory.

Αν εφαρμόσουμε τις μεθόδους αυτές προκύπτουν αρκετά σώματα αριθμών. Αυτό είναι αρκετά δαπανηρό, έτσι αποφεύγουμε αυτές τις μεθόδους.

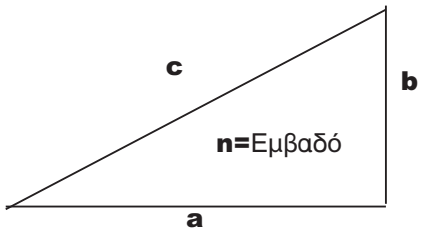
Παρακάτω θα εφαρμόσουμε την μέθοδο του Chabauty για να λύσουμε εξισώσεις της μορφής

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

Αυτές οι ελλειπτικές καμπύλες συνδέονται με το πρόβλημα εύρεσης ορθογωνίων αριθμών (congruent numbers).

Ορθογώνιοι Αριθμοί (Congruent Numbers)

Έστω n ένας φυσικός αριθμός. Αν υπάρχει ορθογώνιο τρίγωνο με πλευρές ρητού μήκους εμβαδού n, τότε ο n ονομάζεται ορθογώνιος αριθμός. Σύμφωνα



Σχημα 3. $a, b, c \in \mathbb{Q}$

με την Ιστορία του Dickson το πρόβλημα πρώτη φορά εμφανίζεται σε ένα χειρόγραφο ενός ανώνυμου Άραβα το 962 μ.χ. Για παράδειγμα αν $n = 1131$, τότε

$$a = 104,\ b = \frac{87}{4},\ c = \frac{425}{4}.$$

Δηλαδή ο n είναι ορθογώνιος αριθμός.
Ενώ, αν $n = 469409$, τότε

$$a = \frac{89880}{29},\ b = \frac{127223}{420},\ c = \frac{37929467}{12180}.$$

Το πρόβλημα εύρεσης ορθογώνιων αριθμών συνδέεται άμεσα με την ελλειπτική καμπύλη $y^2 = x^3 - n^2x$. Ισχύει

$$c^2 = a^2 + b^2, \quad n = \frac{ab}{2}.$$

Αν θέσουμε

$$x = n(a+c)/2, \quad y = 2n^2(a+c)/b^2$$

παρατηρούμε ότι το $(x, y) \in \mathbb{Q}^2$ ικανοποιει την εξίσωση:

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

Και αντίστροφα αν (x, y) με $y \neq 0$ ρητή λύση της $y^2 = x^3 - n^2x$, τότε οι αριθμοί

$$a = (x^2 - n^2)/y, \ b = 2n/y, \ c = (x^2 + n^2)/y,$$

είναι πλευρές ορθογωνίου τριγώνου εμβαδού n. Επομένως, ο φυσικός αριθμός n είναι ορθογώνιος αν-ν υπάρχει ρητή λύση της εξίσωσης $y^2 = x^3 - n^2x$ ισοδύναμα αν-ν η τάξη της ελλειπτικής καμπύλης $y^2 = x^3 - n^2x$ είναι θετική.

Η μέθοδος του Chabauty στην ελλειπτική $E_n : y^2 = x^3 - n^2x$.

Πριν περιγράψουμε τον αλγόριθμο για την εύρεση των ακέραιων σημείων της E_n χρειαζόμαστε ένα αλγόριθμο που να αποφαίνεται για την επιλυσιμότητα μιας *index equation* σε ένα σώμα τετάρτου βαθμου και ένα αλγόριθμο που να μας δίνει τις λύσεις μιας εξίσωσης μονάδων επί ενός σώματος αριθμών τετάρτου βαθμού. Το δεύτερο μπορεί να γίνει με τον αλγόριθμο του *Wildanger*

Wildanger, K., Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern. (German) [Solving unit and index form equations in algebraic number fields] J. Number Theory 82 (2000), no. 2, 188–224.

Ο αλγόριθμος αυτός έχει υλοποιηθεί στον αλγεβρικό υπολογιστικό πακέτο *magma* και *Kash*.

Η εξίσωση των μονάδων σε ένα σώμα αριθμών K, αφορά εξισώσεις της μορφής $aX + bY = c$ όπου τα $a, b, c \in K$, και οι λύσεις (x, y) που αναζητούμε είναι μονάδες του σώματος αριθμών δηλ. $|N_K(x)|$, $|N_K(y)| = 1$.

Όσον αφορά το πρώτο αλγόριθμο χρειαζόμαστε μόνο αν μια *index equation* έχει λύση σε ένα σώμα αριθμών K και όχι την ακριβή επιλυσιμότητα της. Βεβαίως υπάρχει αλγόριθμος για την ακριβή επιλυσημότητα της υλοποιημένος στον $Magma$, $Kash$, αλλά είναι αρκετά δαπανηρός. Η *index form* ορίζεται ως εξής. Έστω $B = \{\omega_1 = 1, \omega_2, \omega_3, \omega_4\}$ μια βάση ακεραιότητας του σώματος K. Τότε θέτουμε

$$l(x, y, z) = x\omega_2 + y\omega_3 + z\omega_4.$$

και $l_i(x, y, z),\ (i = 1, 2, 3, 4)$ οι συζυγείς του επί του K. Τότε

$$D_{K/\mathbb{Q}}(x, y, z) = \prod_{1 \le j,i \le 4} (l_i(x, y, z) - l_j(x, y, z)) =$$

$$= I(x, y, z)^2 D_K.$$

Η *index form* $I(x, y, z)$ ως προς την βάση B ορίζεται από την προηγούμενη σχέση.
Αν $a \in \mathbb{O}_K$ τότε αυτός γράφεται

$$a = z_1 + z_2\omega_2 + z_3\omega_3 + z_4\omega_4,\ \ z_1, z_2, z_3, z_4 \in \mathbb{Z}.$$

Τότε ο δείκτης ($index$) του a, $I(a)$ είναι ο δείκτης του $\mathbb{Z} - module\ \mathbb{Z}[a]$ στην ακεραία περιοχή $\mathbb{O}_K$.
Το κριτήριο που αποφαίνεται για την επίλυση ή όχι μιας index equation σε ένα σώμα τετάρτου βαθμού δίνεται στην παρακάτω εργασία.
I. Gaal, A. Petho, M. Pohst, On the Resolution of Index Form Equations in Biquadratic Fields III. The Bicyclic Biquadratic case, J. Number Theory, 53 (1995), 100-114.

Ο παρακάτω αλγόριθμος είναι σε συνεργασία με τον Κ.Πουλάκη.

Είσοδος : n φυσικός
Έξοδος : Οι ακέραιες λύσεις της εξίσωσης $E_n : y^2 = x^3 - n^2 x$.

Βήμα 1 : Υπολογίζουμε τις ακέραιες λύσεις με $|x| \leq n$.

Βήμα 2 : Υπολογίζουμε τα σώματα $K = \mathbb{Q}(s)$ όπου s ρίζα του πολυωνύμου $\Theta_a(T)$.
Ισχύει το εξής :αν (x, y) ακέραια λύση της E_n, τότε
$x = dwA^2,\ x + n = 2^e duB^2,\ x - n = 2^e dvC^2$, όπου $d = \gcd(x, n),\ d_1 = \mathrm{sf}(d),\ wuv = d_1,\ e \in \{0, 1\}$. Επίσης $K = \mathbb{Q}(\sqrt{x}, \sqrt{x - n})$ από όπου προκύπτει $K = \mathbb{Q}(\sqrt{uv}, \sqrt{2^e wv})$

Βήμα 2 (i) : Αν $[K : \mathbb{Q}] = 1$, τότε $x = W^2$.

Βήμα 2 (ii) : Αν $[K : \mathbb{Q}] = 2$, τότε
είτε $uv = 1$, είτε $2^e wv = 1$, είτε $B^2 - A^2 = m$.

Βήμα 2 (iii) : Αν $[K : \mathbb{Q}] = 4$, τότε ορίζουμε τα εξής σύνολα :
$D = \{d \in \mathbb{Z}_{\geq 0} :\ d|n,\ \mathrm{ord}_p(d) = \mathrm{ord}_p(n), \forall p \text{ odd prime}\}$.
Για κάθε $d \in D$ θέτουμε $m = n/d$ και $d = d_1 d_2^2$,

$$D(d) = \left\{(u, v, w, e) \in \mathbb{Z}^4_{\geq 0} :\ uvw = d_1,\ e \in \{0, 1\}\ \right\}.$$

Υπολογίζουμε τα σώματα $\mathbb{Q}(\sqrt{uv}, \sqrt{2^e wv})$ για τα οποία η $index\ form$ εξίσωση $I_K(x_2, x_3, x_4) = \pm 2^7 n^3/\Delta_K$ έχει λύση.
Για την περίπτωση όπου $d = n$ μπορούμε να δουλέψουμε απλούστερα λύνοντας την διοφαντική $w^2 X^4 - uvY^2 = 1$. Αυτή έχει μελετηθεί από τους $Benett - Walsh$.

Βήμα 3 : Για κάθε σώμα που προέκυψε από το *Βήμα 2 (iii)* λύνουμε τις εξισώσεις των μονάδων (unit equations)

$$aX - bY = m,\ N_K(a) = 4m^4,\ N_K(b) = m^4.$$

Βήμα 4 : Οι ακέραιες λύσης της E_n προκύπτουν από τα βήματα 1, 2 (i,ii) και 3 με χρήση της σχέσης $\Theta_a(s) = 0$.

Παραδείγματα

1. Θεωρούμε την καμπύλη $E : y^2 = x^3 - (1131)^2 x$.
Πρώτα βρίσκουμε τις ακέραιες λύσεις
(x, y) με $|x| \leq n$. Αυτές είναι :
$(0, 0),\ (\pm 1131, 0),\ (-117, \pm 12168)$.
Το βήμα 2 (i) και (ii) δίνουν ξανά το σημείο $(-117, \pm 12168)$.
Για την υλοποίηση του βήματος (iii) διακρίνουμε δύο περιπτώσεις αν $d = n$ και αν $d < n$.
Στη πρώτη περίπτωση έχουμε τις τετράδες $(w, u, v, e) = (1, 1, 1131, 1), (1, 13, 87, 1), (13, 29, 3, 0)$. Για κάθε μία από αυτές λύνουμε την διοφαντική

$$w^2 X^4 - uvY^2 = 1.$$

Καμία από αυτές δεν έχει λύσεις.

Συνεχίζουμε με τους υπόλοιπους διαιρέτες d του n.
Για κάθε διαιρέτη d βρίσκουμε τις τετράδες (u, v, w, e).
Κάθε τετράδα δίνει ένα σώμα τετάρτου βαθμού στο οποίο ελέγχουμε αν η *index equation* έχει λύση.
Στις μόνες περιπτώσεις που συνέβη αυτό είναι όταν $d = 377$. Στη περίπτωση αυτή το σώμα που προκύπτει είναι το $\mathbb{Q}(\sqrt{13}, \sqrt{58})$. Μια βάση αυτού είναι η
$\omega_0 = 1$, $\omega_1 = \theta$, $\omega_2 = (\theta^2+2\theta+3)/4$, $\omega_3 = (\theta^3+83\theta+90)/180$,
όπου $\theta = \sqrt{13} + \sqrt{58}$. Αν $z = \sum_{i=0}^{3} z_i \omega_i$ στοιχείο του $\mathbb{O}_K$ τότε το συμβολίζουμε $z = [z_0; z_1; z_2; z_3]$.

Συνεχίζουμε στο βήμα 3.
Λύνουμε τις εξισώσεις νόρμας

$N_K(t) = m^4,\ N_K(t) = 4m^4,\ m = n/d = 1131/377 = 3.$

Αυτές δίνονται αντίστοιχα στους δύο παρακάτω πίνακες.

$[46; -30; -17; 70],\ [4; 2; -1; -4],\ [4; 1; 0; -1],\ [28; -16; -1; 14],$
$[646; 236; -17; -196],\ [-19; -2; 4; 0],\ [-167254; 78936; 55361; -193688],$
$[8; 3; 0; -2],\ [-116; -47; 17; 70],$
$[12; 5; -2; -8],\ [3; 0; 0; 0],\ [54; -27; -2; 24],$
$[-123378; 33167; 35564; -92558],\ [-6; 3; 0; -2],$
$[-1330901358; 626185105; 49998419; -561048396],\ [129; 2; -4; 0],\ [3; -1; 0; 1],$
$[-2352490266; 1106839766; 88376795; -991704638],\ [-450; 219; 17; -196]$
(19 λύσεις)

$[-78; 39; 3; -35],\ [18; 7; -1; 7],$
$[75450997426395; 26966216894344; -1993938001999; -22374625065691],$
$[9874766665; 3529245596; -260959765; -2928313929],$
$[-9; 6; 3; -13],\ [-64259; 39638; 23153; -92919],\ [498; 191; -13; -159],\ [30; -3; -1; 3]$
$[-18; 9; 1; -9],\ [1856475641909; 663505142760; -49060946289; -550528791509],$
$[27; 10; -1; -9],\ [-391; 234; 125; -515],$
$[4671; 1670; -125; -1389],\ [-11; 6; 1; -7]$
$[875811; 313018; -23153; -259737],\ [113; 42; -3; -35]$
(15 λύσεις)

Κατόπιν λύνουμε τις εξισώσεις των μονάδων $aX - bY = m$. Το a παίρνει τις τιμές του πρώτου πίνακα ενώ το b του δεύτερου πίνακα. Η εξίσωση με

$a = [12; 5; -2; -8]$ και
$b = [75450997426395; 26966216894344; -1993938001999; -22374625065691]$
έχει μόνο μία λύση $X = [-1; 0; 0; 0]$,
$Y = [290305319644; -179246403758; -104979192791; 420989904480]$.

Αυτή η λύση δίνει το σημείο $(10933, \pm 1137032)$ της E.
Δουλεύοντας παρόμοια στο σώμα $\mathbb{Q}(\sqrt{3}, \sqrt{87})$ παίρνουμε τη λύση $(1392, \pm 30276)$. Άρα :

$$E(\mathbb{Z}) = \{(0, 0),\ (\pm 1131, 0),\ (-117, \pm 12168),$$
$$(1392, \pm 30276),\ (10933, \pm 1137032)\}.$$

2. Σε αυτό το παράδειγμα θα μελετήσουμε μια ελλειπτική καμπύλη που δεν είναι της μορφής

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

Η ελλειπτική με την οποία θα ασχοληθούμε είναι η $y^2 = x^3 - 2x$ και επίλυση της μας δίνει τους όρους της ακολουθίας P_n, των $Pell$ αριθμών, που είναι τετράγωνα. Η ακολουθία $Pell$ ορίζεται από τον αναγωγικό τύπο :

$$P_0 = 0,\ P_1 = 1,\ P_n = 2P_{n-1} + P_{n-2}.$$

Μερικοί όροι αυτής της ακολουθίας είναι :

$0, 1, 2, 5, 12, 29, 70, 169, 408, 985, 2378, 5741, 13860, ...$

Οι αριθμοί αυτοί ονομάζονται *αριθμοί Pell* (επίσης μερικές φορές τους ονομάζουμε και *αριθμούς λάμδα*.)
Ο γενικός όρος γράφεται

$$P_n = \frac{\epsilon^n - \overline{\epsilon}^n}{2\sqrt{2}},\ \epsilon = 1 + \sqrt{2}.$$

Επίσης παρατηρούμε ότι

$$\epsilon^n = S_n + P_n\sqrt{2},$$

όπου

$$S_n = \frac{\epsilon^n + \overline{\epsilon}^n}{2},$$

Οι αριθμοί S_n/P_n είναι τα συγκλίνωντα κλάσματα του αριθμού $\sqrt{2}$. Το πρόβλημα με το οποίο θα ασχοληθούμε είναι η εύρεση τετραγώνων των αριθμών $Pell$.

Δηλ. ενδιαφερόμαστε για την λύση της διοφαντικής εξίσωσης :

$$P_n = x^2 \ \ (x > 0).$$

Εφόσον $S_n^2 - 2P_n^2 = 1$, και $P_n = x^2$ προκύπτει η διοφαντική εξίσωση $L : y^2 = 2x^4+1$. Για να λύσουμε την εξίσωση $L : y^2 = 2x^4-1$ είναι αρκετό να λύσουμε την ελλειπτική $C : y^2 = x^3-2x$. Πράγματι, αν (x, y) ακέραια λύση της L, τότε το ακέραιο σημείο

$$P = (a, b) = (2x^2, 2xy)$$

ανήκει στην C. Υποθέτουμε ότι $|a| \geq 2$. Έστω $R = (s, t)$ σημείο της C τέτοιο ώστε $2R = P$. Τότε

$$a = \frac{(s^2+2)^2}{4s(s^2-2)} \text{ (duplication formula)}$$

επομένως το s είναι ρίζα του πολυωνύμου

$$\Theta_a(S) = S^4 - 4aS^3 + 4S^2 + 8aS + 4.$$

Οι ρίζες του $\Theta_a(S)$ είναι:

$$a \pm \sqrt{a^2-2} \pm \sqrt{2a^2 \pm 2a\sqrt{a^2-2}},$$

όπου το πρώτο $\pm$ συμπίπτει με το τρίτο.

Θα υπολογίσουμε τα πιθανά σώματα $L = \mathbb{Q}(s)$. Κατόπιν τα στοιχεία (του L)

$$u = \frac{s + \sqrt{2}}{2},\ v = \frac{\sqrt{2} - s}{2},$$

θα αποδείξουμε ότι είναι μονάδες στο σώμα L και ικανοποιουν την εξίσωση των μονάδων

$$X + Y = \sqrt{2}.$$

Μετά θα κάνουμε χρήση του αλγορίθμου του Wildanger για να λύσουμε τις εξισώσεις των μονάδων. Επομένως θα βρούμε τα s και αυτές τις τιμές θα τις αντικαταστήσουμε στη σχέση

$$\frac{(s^2 + 2)^2}{4s(s^2 - 2)}$$

και θα πάρουμε τα ακέραια σημεία της καμπύλης C.

Πρώτο Βήμα. Υπολογισμός των σωμάτων L

Θέτουμε $L = \mathbb{Q}(s)$. Εφόσον, $a = 2x^2$, προκύπτει $a^2-2 = 4x^4-2 = 2y^2$ επομένως $L = \mathbb{Q}(\sqrt{2x^2 \pm y\sqrt{2}})$. Επίσης, $K = \mathbb{Q}(\sqrt{2}) \subset L$ και $N_K(2x^2 \pm y\sqrt{2}) = 2$. Συνεπάγεται ότι οι πρώτοι αριθμοί που διαιρούν την διακρίνουσα του σώματος L είναι μόνο ο 2. Άρα ο μοναδικός διακλαδιζόμενος πρώτος αριθμός στο L είναι ο 2. Επιπλεόν, από

Cohen, Henri; Advanced topics in computational number theory. Graduate Texts in Mathematics, 193. Springer-Verlag, New York, 2000. [Chapter 9, Proposition 9.4.1, p.461]

προκύπτει ότι το σώμα L είναι ολικα πραγματική επέκταση (τετάρτου βαθμου) πάνω στο $\mathbb{Q}$. Κάνουμε χρήση των πινάκων του Jones

Jones, W.J., http://math.la.asu.edu/~jj/numberfields/.

Tables of number fields with prescribed ramification.

ή της βάσης δεδομένων των Jürgen Klüners and Gunter Malle,

http://www.mathematik.uni-kassel.de/~klueners/minimum/minimum.html

και καταλήγουμε ότι $L = \mathbb{Q}(\sqrt{2+\sqrt{2}})$.

Δεύτερο Βήμα. Απόδειξη ότι $u = \frac{s+\sqrt{2}}{2}$, $v = \frac{\sqrt{2}-s}{2}$ *είναι μονάδες του* L

Τα στοιχεία $u = \frac{s+\sqrt{2}}{2}$, $v = \frac{\sqrt{2}-s}{2}$ είναι ρίζες του πολυωνύμου με ακέραιους συντελεστές :

$$\begin{aligned} \lambda(S) &= \frac{1}{256}\mathrm{res}_W\big(\Theta_a(2S \mp W), W^2 - 2\big) \\ &= S^8 - 4aS^7 + \cdots + 1, \end{aligned}$$

όπου $\mathrm{res}_W(\cdot,\cdot)$ συμβολίζει την απαλείφουσα των δύο πολυωνύμων ως προς την μεταβλητή W. Επομένως u, v είναι μονάδες του L. Επίσης $u + v = \sqrt{2}$. Καταλήγουμε ότι τα u και v ικανοποιούν την εξίσωση των μονάδων $X + Y = \sqrt{2}$ στο L.

Τρίτο Βήμα. Η λύση της εξίσωσης των μονάδων

Ο αλγόριθμος του Wildanger είναι υλοποιημένος στο αλγεβρικό σύστημα Magma. Οι λύσεις που προέκυψαν δίνονται στον πίνακα 1, όπου έχουμε θέσει
$[a_0\ a_1\ a_1\ a_3] = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3$,
$\theta = \sqrt{2+\sqrt{2}}$. Αντικαθιστούμε στην σχέση

$$a = \frac{(s^2+2)^2}{4s(s^2-2)}$$

κάθε λύση της εξίσωσης των μονάδων και ελεγχουμε αν μας δίνει ακέραια τιμή. Μέτα την εκτέλεση αύτής της διαδικασίας προέκυψε $a = 2,338$. Άρα για $|a| \geq 2$, έχουμε $|a| = 2$ ή 338. Επειδή $a = 2x^2$ παίρνουμε ότι $|x| = 1$ ή 13. Επομένως τα τετράγωνα των Pell αριθμών είναι $P_1 = 1,\ P_7 = 169$.

Ευχαριστώ

Πίνακας 1-Οι 44 λύσεις της εξίσωσης των μονάδων $X + Y = \sqrt{2}$ στο σώμα αριθμών $L = \mathbb{Q}(\sqrt{2+\sqrt{2}})$.

[-1,0,0,0] [-1,0,1,0]	[1,0,0,0] [-3 0,1,0]	[-1,-1,0,0] [-1,-1,1,0]
[-1,1,0,0] [-1,-1,1,0]	[-1,-1,1,0] [-1,1,0,0]	[-3,0,1,0] [1,0,0,0]
[407,533,-119,-156] [-409,-533,120,156]	[-1,1,1,0] [-1,-1,0,0]	[-1,0,1,0] [-1,0,0,0]
[-409,533,120,-156] [407,-533,-119,156]	[5,7,-1,-2] [-7,-7,2,2]	[1,4,0,-1] [-3,-4,1,1]
[-71,39,120,-65] [69,-39,-119,65]	[-1,-1,-1,1] [-1,1,2,-1]	[1,2,-3,-2] [-3,-2,4,2]
[69,39,-119,-65] [-71,-39,120,65]	[-7,7,2,-2] [5,-7,-1,2]	[-3,2,4,-2] [1,-2,-3,2]
[-71,-39,120,65] [69,39,-119,-65]	[-1,2,0,-1] [-1,-2,1,1]	[1,3,0,-1] [-3,-3,1,1]
[11,14,-3,-4] [-13,-14,4,4]	[-1,2,1,-1] [-1,-2,0,1]	[-3,3,1,-1] [1,-3,0,1]
[-1,1,-1,-1] [-1,-1,2,1]	[-1,1,2,-1] [-1,-1,-1,1]	[-3,-4,1,1] [1,4,0,-1]
[11,-14,-3,4] [-13,14,4,-4]	[1,-3,0,1] [-3,3,1,-1]	[-1,-2,0,1] [-1,2,1,-1]
[-13,14,4,-4] [11,-14,-3,4]	[-3,-3,1,1] [1,3,0,-1]	[-1,-2,1,1] [-1,2,0,-1]
[-409,-533,120,156] [407,533,-119,-156]	[1,-2,-3,2] [-3,2,4,-2]	[5,-7,-1,2] [-7,7,2,-2]
[69,-39,-119,65] [-71,39,120,-65]	[-1,-1,2,1] [-1,1,-1,-1]	[1,-4,0,1] [-3,4,1,-1]
[-13,-14,4,4] [11,14,-3,-4]	[-3,-2,4,2] [1,2,-3,-2]	[-3,4,1,-1] [1,-4,0,1]
[407,-533,-119,156] [-409,533,120,-156]	[-7,-7,2,2] [5,7,-1,-2]	