Teză de Licență

Sisteme de criptare hibride folosind curbe eliptice și jocuri combinatoriale

Student:
Ștefan M. Cobeli

Îndrumător științific:
Conf. dr. Cătălin Gherghe

16 Iunie, 2016

Cuprins

Lista Figurilor

Lista Tabelelor

Prefață

Sistemele criptografice se bazează pe încredere. Încrederea utilizatorilor și a factorilor de decizie că funcționarea lor este în deplină siguranță. Aceasta este condiția esențială, față de care, altele, legate de spațiu, memorie, timp, viteză, complexitate, ușurință în utilizare devin secundare.

Nu există însă siguranță absolută. Pentru aceasta am avea nevoie de chei unice, bine alese și de lungime egală cu cea a mesajelor de criptat, iar păstrarea lor, inclusiv din punct de vedere fizic, să se poată face într-un perfect secret.

Un sistem de criptare hibrid este compus din două criptosisteme, unul care folosește cheie publică, iar altul care folosește cheie privată. Primul dintre acestea este folosit pentru transmiterea cheii secrete corespunzătoare criptosistemului simetric, iar al doilea este folosit pentru criptarea și mai apoi decriptarea mesajelor transmise. Avantajele unui sistem hibrid sunt date de faptul că îmbină beneficiile date de către ambele sisteme constituente. Marea parte a mesajelor urmează a fi criptate de un sistem simetric și nu de unul asimetric, iar dimensiunea cheilor unui sistem care folosește cheie de criptare publică este aproape dublă față de cazul folosirii unei chei secrete [BCC'09]. De asemenea, vom vedea pe parcursul lucrării faptul că o criptare asimetrică implică mult mai multe calcule decât una simetrică și, prin urmare, și timpul necesar unei astfel de criptări este mai mare. Așadar, pentru a cripta mesaje lungi este indicat să folosim un sistem de criptare simetric.

Însă un sistem hibrid are avantajul că e mai sigur și mai flexibil. Pentru ca un atacator să reușească să înțeleagă un mesaj cifrat, el ar trebui să reușească să spargă ambele sisteme de criptare care formează sistemul hibrid, sisteme care sunt diferite unul de altul. Mai mult, dacă sistemul asimetric, care folosește chei publice și private e public cunoscut și se bazează pe dificultatea rezolvării unei probleme a cărei complexitate depinde de lungimea cheilor, sistemul simetric poate fi menținut privat de cei doi comunicatori. Mai mult, aceștia pot cădea de acord să-l schimbe periodic fără ca atacatorul să fie la curent cu aceste schimbări. Folosirea sistemelor hibride ar putea contribui la aducerea noțiunii de "încredere în siguranța sistemului" mai aproape de realitate, în condițiile în care "demonstrațiile matematice despre securitatea sistemelor" sunt de fapt altceva decât ceea ce în folclor se transmite ca fiind "siguranță demonstrată", după cum constată Koblitz și Menezes în articolele [KM'07], [KM'10].

Lucrarea de față este împărțită în două părți. În prima parte vom introduce noțiunea de curbă eliptică, prezentând câteva rezultate generale privitoare la structura de grup care este indusă de acest obiect matematic. Apoi, adaptând o metodă utilizată în [CZ'01] pentru numărarea anumitor puncte speciale aflate pe o curbă mai

generală, și folosind estimarea sumelor exponențiale pe curbe eliptice [KS'00], vom demonstra trei teoreme despre uniformitatea distribuției locale, în pătrate mici incluse în $\mathbb{F}_p^2$, a punctelor unei curbe eliptice peste corpul finit $\mathbb{F}_p$. În încheierea primei părți vom prezenta sistemul de criptare bazat pe curbe eliptice, care a fost introdus de V. Miller [Mil'85] și N. Koblitz [Kob'87].

În partea a doua a lucrării vom prezenta o serie de metode propuse recent pentru mai multe sisteme simetrice folosite la criptarea imaginilor și vom exemplifica un astfel de sistem bazat pe permutările generate de drumul unui cal pe o tablă de șah de dimensiune $m \times n$.

PARTEA I
Sistem de criptare bazat pe curbe eliptice

1 Istoric

Pentru început vom prezenta câteva dintre cele mai importante momente în care au apărut curbele eliptice în matematică și în criptografie, din antichitate și până în prezent, folosind datele prezentate în enciclopedia [MOV'96], tratatele [Sil'95] și [Was'08] și în articolul [BM'14]. Curbele eliptice apar pentru prima dată în istorie în lucrarea lui Diophant *"Arithmetica"*, unde acesta propune următorul exercițiu:

> *Să se împartă un număr dat în alte două numere, cu proprietatea că produsul acestora este egal cu diferența dintre un cub și latura sa.*

Problema a fost scrisă de Diophant sub forma $Y(a-Y) = X^3 - X$, aceasta fiind chiar ecuația unei curbe eliptice. O rezolvare completă a problemei nu a fost găsită decât abia după 1500 de ani, Diophant prezentând doar o soluție în cazul $a = 6$.

În anul 1621 matematicianul francez Claude Gaspard Bachet de Méziriac a tradus în limba latină *Arithmetica* lui Diophant, traducere care a ajuns și în mâinile lui Fermat, oferindu-i inspirație. Astfel, Fermat abordează multe probleme legate de curbe eliptice. Spre exemplu, el conjecturează faptul că singurele perechi de numere întregi (x, y) care satisfac ecuația $y^2 = x^3 - 2$ sunt perechile $(3, 5)$, și $(3, -5)$ și, la fel, singurele perechi de numere întregi care satisfac ecuația $y^2 = x^3 - 4$ sunt $(2, 2), (2, -2), (5, 11), (5, -11)$.

De asemenea în probleme legate de curbe eliptice s-au implicat mulți alți matematicieni, inclusiv Leonhard Euler sau Issac Newton, fără a avea noțiunile de curbe definite cum sunt astăzi. Un caz interesant este al problemei pătratului egal cu o piramidă formată din pătrate consecutive. Conjectura lui É. Lucas (1875) spune că singurele soluții ale ecuației diofantice:

$$\sum_{n=0}^{N} n^2 = M^2$$

sunt cele triviale $0^2 = 0^2$, $0^2 + 1^2 = 1^2$ și

$$0^2 + 1^2 + \cdots + 24^2 = 70^2$$

Conjectura lui Lucas a fost rezolvată în 1918 de Watson [Wat'18] folosind curbe eliptice, dar mai recent s-au găsit și soluții elementare: Ma [Ma'85], Anglin [Ang'90], [Ang'95], Bennett [Ben'02]. Interesantă este legătura încă puțin înțeleasă a ecuației lui Lucas cu teoria bosonică a stringurilor într-un spațiu cu 26 dimensiuni (cf. John Baez http://math.ucr.edu/home/baez/week95.html).

Apariția curbelor eliptice în criptografie a fost precedată de începuturile criptografiei asimetrice în anii '70 când au fost propuse mai multe astfel de scheme de criptare, precum protocolul lui W. Diffie și M. Hellman [DH'76] sau criptosistemul `RSA`, descoperit de R. Rivest, A. Shamir, L. Adleman [RSA'78].

Folosind grupul punctelor unei curbe eliptice, definite peste un corp finit, Victor Miller [Mil'85] și Neal Koblitz [Kob'87] au propus independent unul de altul un criptosistem care își bazează securitatea pe dificultatea rezolvării problemei logaritmului discret în grupul curbei eliptice. Printre avantajele puse în evidență de Miller și de Koblitz se numără faptul că dimensiunea cheilor unui criptosistem pe curbe eliptice este considerabil mai mică decât cea a criptosistemelor clasice care oferă un nivel de siguranță asemănătoare.

Curbele eliptice sunt considerate o alternativă viabilă pentru înlocuirea metodelor de criptare existente. În anul 2005 *United States National Security agency* a publicat un articol în care recomandă trecerea treptată de la primele criptosisteme asimetrice către folosirea curbelor eliptice.

2 Generalități

Fie $\mathbb{K}$ un corp, care poate fi finit, adică, $\mathbb{K} = \mathbb{F}_q$ cu $q = p^m$, unde $p > 3$ este număr prim și $m \in \mathbb{N}^*$ sau dacă este infinit, atunci $\mathbb{K} = \mathbb{R}$, corpul numerelor reale. Considerăm ecuația:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

unde $a_1, \ldots, a_6 \in \mathbb{K}$. Ecuația (1) se poate rescrie sub forma:

$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(a_6 + \frac{a_3^2}{4}\right). \tag{2}$$

Prin urmare, schimbarea de variabile:

$$\begin{cases} y_1 = y + \dfrac{a_1x}{2} + \dfrac{a_3}{2} \\ x_1 = x + \dfrac{a_2 + \frac{a_1^2}{4}}{3} \end{cases} \tag{3}$$

transformă ecuația (2) în

$$y_1 = x_1^3 + Ax_1 + B, \tag{4}$$

unde coeficienții A, B sunt elemente ale corpului $\mathbb{K}$. În continuare vom lua în considerare doar ecuațiile de forma (4), cu proprietatea $4A^3 + 27B^2 \neq 0$.

Definiția 2.1. *Fie $A, B \in \mathbb{K}$ fixate. Presupunem că elementele A, B satisfac proprietatea $4A^3 + 27B^2 \neq 0$ și fie $E(\mathbb{K}; A, B) = E(\mathbb{K})$ mulțimea punctelor*

$$E(\mathbb{K}) := \{(x, y) \in \mathbb{K}^2 \ : \ y = x^3 + Ax + B\} \cup \{\mathcal{O}\}.$$

Aici $\mathcal{O}$ se numește punctul de la infinit și în reprezentarea sa din spațiul proiectiv este egal cu $(0 : 1 : 0)$. Mulțimea $E(\mathbb{K}; A, B)$ se numește curbă eliptică de parametrii A, B peste corpul $\mathbb{K}$.

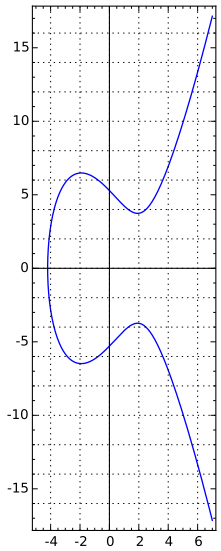


Figura 2.1: Două curbe eliptice peste $\mathbb{R}$: $E(\mathbb{R}; -1, 0)$ (stânga) și $E(\mathbb{R}; -11, 28)$ (dreapta). În ambele cazuri se observă simetria punctelor față de dreapta $y = 0$.

Eae33be84pesteF101.pdf

Figura 2.2: Curba eliptică $E(\mathbb{F}_p; 33, 84)$, $p = 101$ (punctele colorate în albastru). Cu excepția punctului $(10, 0)$ și a punctului de la infinit, toate punctele curbei sunt situate simetric față de dreapta $y = p/2$, cea punctată, roșie.

Ecuația (1) se numește *ecuația Weierstrass generală*, iar ecuația (4) se numește *ecuația Weierstrass* sau simplu *ecuația curbei eliptice*. În Figura 2.1 sunt reprezentate graficele a două curbe eliptice peste $\mathbb{R}$, iar în Figura 2.2 se pot vedea punctele unei curbe eliptice peste un corp finit. Pentru a compara aspectele geometrice și distribuția punctelor, în Figura 2.3 este reprezentată o aceeași curbă peste două corpuri finite.

Observația 2.1. *La început am exclus corpurile* $\mathbb{K}$ *de caracteristică* 2 *sau* 3*, deoarece în aceste cazuri nu am fi putut efectua schimbarea de variabile* (3) *pentru care e nevoie ca elementele* 2 *și* 3 *să fie inversabile. De aceea, pentru a putea dezvolta teoria curbelor eliptice în aceste corpuri se folosesc ecuații mai generale. Astfel, în cazul corpurilor de caracteristică* 2 *se folosește ecuația* (1)*, iar în cazul corpurilor de caracteristică* 3 *se folosește ecuația*

$$y^2 = x^3 + a_2x^2 + a_4x + a_6,$$

deoarece, în acest caz, schimbarea de variabilă $y \to y_1 := y + a_1x/2 + a_3/2$ *din relațiile* (3) *este încă posibilă.*

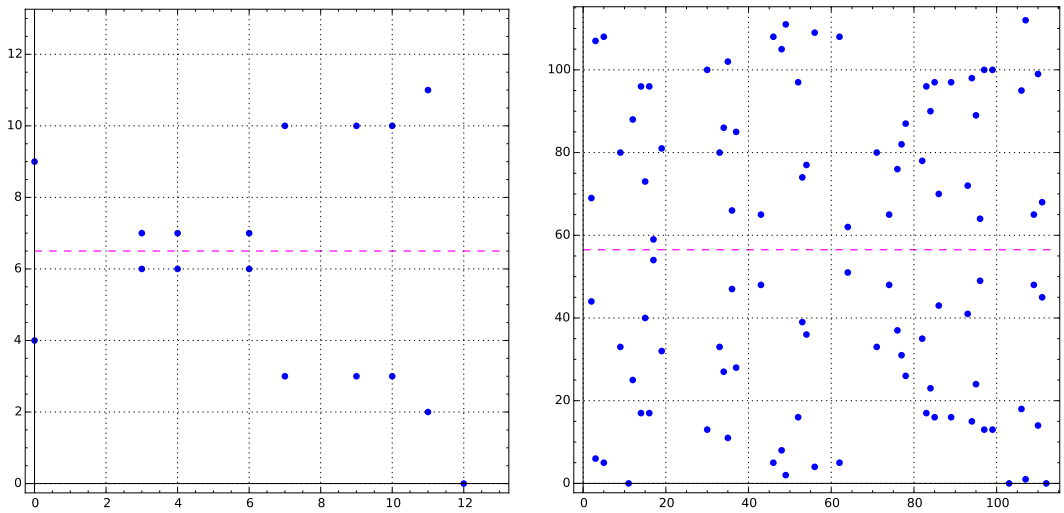


Figura 2.3: Curba eliptică $E: \ y^2 = x^3 + 2x + 3$ peste $\mathbb{F}_p$. În figura din partea stângă $p = 13$, discriminantul este egal cu $-16(4 \cdot 2^3 + 27 \cdot 2^2) \pmod{13} \equiv 7$ și curba este formată din următoarele 18 puncte (în coordonate proiective): $(0:1:0), (0:4:1), (0:9:1), (3:6:1), (3:7:1), (4:6:1), (4:7:1), (6:6:1), (6:7:1), (7:3:1), (7:10:1), (9:3:1), (9:10:1), (10:3:1), (10:10:1), (11:2:1), (11:11:1), (12:0:1)$. În figura din partea dreaptă $p = 113$, discriminantul este egal cu $-16(4 \cdot 2^3 + 27 \cdot 2^2) \pmod{113} \equiv 7$, iar cardinalul curbei este egal cu 100. De remarcat cele patru puncte care nu au un simetric față de dreapta $y = p/2$: $(0:1:0), (11:0:1), (103:0:1), (112:0:1)$.

3 Legea de grup

Fie $E = E(\mathbb{R}; A, B)$. Pe mulțimea punctelor lui E definim o operație care va satisface axiomele unui grup comutativ. În cele ce urmează vom descrie această relație.

Fie $P_1, P_2 \in E$ de coordonate (x_1, y_1), respectiv (x_2, y_2). Definim $P_1 + P_2 := P_3$ (prescurtat vom folosi notația multiplicativă $P_1P_2 = P_3$) astfel:

(i) Construim dreapta d care trece prin P_1 și prin P_2;

(ii) Fie punctul $P_3' = d \cap E \setminus \{P_1, P_2\}$;

(iii) Fie P_3 simetricul față de axa OX a lui P_3'. Definim $P_1 + P_2 := P_3$.

În continuare vom arăta corectitudinea construcției de mai sus. Împărțim demonstrația în 4 cazuri:

Cazul I. $P1 \neq P_2$, $P_1, P_2 \in E \setminus \mathcal{O}$ și $x_1 \neq x_2$;

Cazul II. $P1 \neq P_2$, $P_1, P_2 \in E \setminus \mathcal{O}$ și $x_1 = x_2$;

Cazul III. $P_1 = P_2$;

Cazul IV. $P_1 = \mathcal{O}$ sau $P_2 = \mathcal{O}$.

Cazul I. $P1 \neq P_2$, $P_1, P_2 \in E \setminus \mathcal{O}$ și $x_1 \neq x_2$.
Dreapta d, care trece prin punctele P_1 și P_2, are panta $m_d = \frac{y_2 - y_1}{x_2 - x_1}$ și are ecuația $d : y = m(x - x_1) + y_1$. Pentru a găsi un al treilea punct în care dreapta d intersectează curba E îl înlocuim în ecuația curbei pe y din ecuația dreptei și obținem

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B \tag{5}$$

Ecuația (5) are gradul al 3-lea în x și prin urmare are 3 soluții, dintre care știm deja două și anume x_1 și x_2. Printr-un calcul simplu (împărțind polinomul de mai sus prin $(x - x_1)$ și $(x - x_2)$ sau și mai simplu din relațiile lui Viète) putem obține și cea de-a treia soluție care este:

$$x_3' = m^2 - x_1 - x_2$$

și înlocuind în ecuația dreptei îl aflăm și pe

$$y_3' = m(x - x_1) + y_1.$$

Așadar cel de-al treilea punct al intersecției dintre dreapta d și curba E este $P_3' = (x_3', y_3')$. În cele din urmă, luăm simetricul față de axa OX al punctului P_3' și obținem:

$$\begin{aligned} P_3 &= P_1 + P_2 \\ &= (x_3' - y_3') \\ &= (m^2 - x_1 - x_2, m(x_1 - x) - y_1). \end{aligned} \tag{6}$$

Cazul II. $P1 \neq P_2$, $P_1, P_2 \in E \setminus \mathcal{O}$ și $x_1 = x_2$.
Deoarece $x_1 = x_2$, panta dreptei d care trece prin ele este ∞ și prin P_1, P_2urmare este verticală, intersectând curba E în punctul de la infinit $\mathcal{O}$, iar simetricul său față de axa OX este de asemenea $\mathcal{O}$. Așadar

$$P_3 = P_1 + P_2 = \mathcal{O}. \tag{7}$$

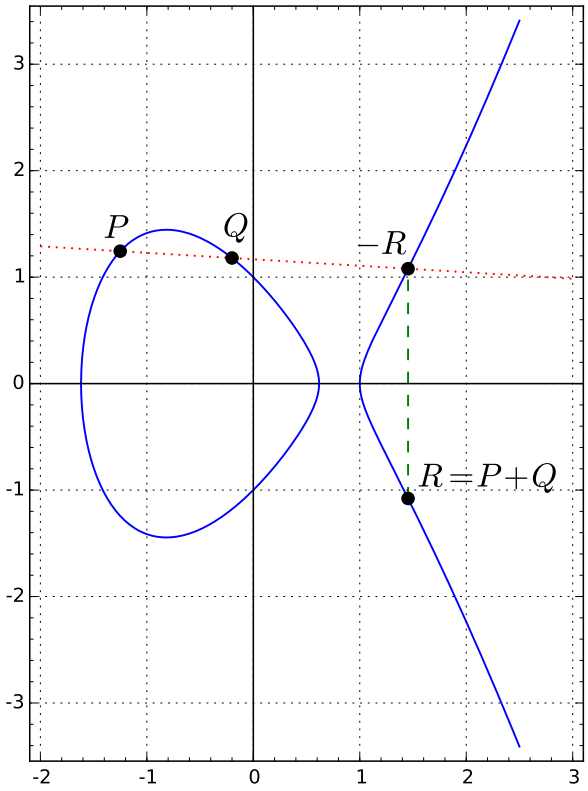


Figura 3.4: Curba eliptică $E(\mathbb{R}; -2, 1)$ peste corpul numerelor reale. Sunt evidențiate punctele P; Q; $-R = E \cap \overline{PQ}$ și suma $P + Q = R$.

Cazul III. $P_1 = P_2$.
Dreapta care trece prin două puncte aproximează din ce în ce mai bine o tangentă la curbă pe măsură ce acestea se apropie unul de celălalt. Prin urmare, în acest caz, luăm dreapta d să fie tangenta la curbă în P_1. Știm că există această tangentă deoarece am exclus din definiție curbele care ar putea avea puncte singulare (acestea ar avea proprietatea $4A^3 + 27B^2 = 0$). Panta tangentei în punctul P_1 este

$$m_d = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}$$

Dacă $y_1 = 0$, atunci suntem siguri că $3x_1^2 + A \neq 0$ și prin urmare dreapta d este verticală și din nou P_3 ar fi $\mathcal{O}$.

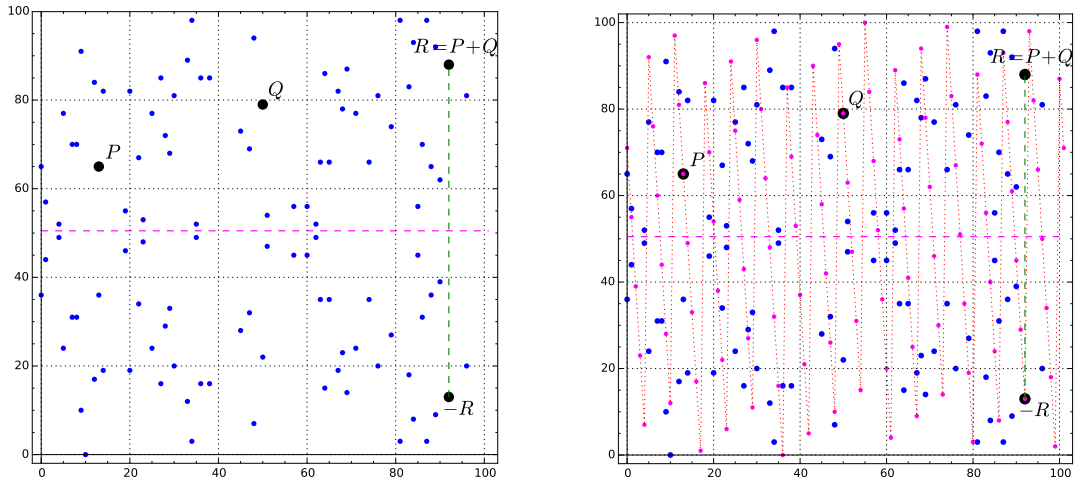


Figura 3.5: Curba eliptică $E: \ y^2 = x^3 + 33x + 84$ peste $\mathbb{F}_p$, cu $p = 101$. Curba are discriminantul 93 și conține 108 puncte. Sunt evidențiate punctele $P = (13, 65)$; $Q = (50, 79)$; $-R = (92, 13)$ și suma $P + Q = R = (92, 88)$. În figura din partea dreaptă este reprezentată și dreapta PQ precum și punctele $(x, y) \in \mathbb{F}_p^2$ care aparțin acestei drepte.

Explicație: Punctul $P_1 = (x_1, 0)$ respectă ecuația curbei, așadar $x_1^3 + Ax + B = 0$, deci x_1 este rădăcină pentru polinomul $M = X^3 + AX + B$. Dacă $3x_1^2 + A = 0$, atunci x_1 este rădăcină și pentru polinomul $N = 3X^2 + A$. Să observăm că polinomul N este derivata polinomului M, iar cum x_1 este rădăcină pentru amândouă deducem că este rădăcină dublă pentru polinomul M.
Acest lucru nu este posibil, deoarece $x_1^3 + Ax + B = 0$ nu are rădăcini multiple, din definiția curbei eliptice, unde ne asigurăm că discriminantul acesteia $\triangle = -16(4A^3 + 27B^2)$ este nenul.

Dacă $y_1 \neq 0$, ecuația tangentei este

$$y = m(x - x_1) + y_1.$$

Înlocuind în ecuația curbei, obținem

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B,$$

ecuație de gradul al treilea în x. Știm două rădăcini ale acesteia și anume x_1 rădăcină dublă și o găsim ușor pe cea de-a treia ca fiind

$$x_3' = m^2 - 2x_1,$$

iar ordonata corespunzătoare este

$$y_3' = m(x_3' - x_1) + y_1.$$

În final, luăm simetricul punctului (x_3', y_3') față de axa OX și obținem

$$P_3 = (m^2 - 2x_1, m(x_1 - x_3') - y_1)$$

Cazul IV. $P_1 = \mathcal{O}$ sau $P_2 = \mathcal{O}$ Presupuneam că $P_1 = \mathcal{O}$ (raționamentul este analog pentru $P_2 = \mathcal{O}$). Dacă $P_2 \neq \mathcal{O}$ atunci dreapta d care trece prin $\mathcal{O}$ și P_2 este o dreaptă verticală, și prin urmare intersectează curba E în simetricul lui P_2 față de axa OX. Punctului astfel obținut trebuie să-i luăm iarăși simetricul față de aceeași axă și prin urmare îl obținem pe P_2.

În concluzie $P + \mathcal{O} = \mathcal{O} + P = P$ pentru orice $P \in E \setminus \{\mathcal{O}\}$. Extindem acest fapt și pentru punctul de la infinit astfel încât $\mathcal{O} + \mathcal{O} = \mathcal{O}$.

Rezumatul 1. Rezumăm argumentele de mai sus în următoarele formule:
Fie E o *curbă eliptică* dată de ecuația $y^2 = x^3 + Ax + B$ cu $A, B \in \mathbb{R}$ și fie $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E$. Definim operația de adunare $P_1 + P_2 = P_3 = (x_3, y_3)$ astfel:

(1) Dacă $P_1 = \mathcal{O}$, atunci $P_1 + P_2 = P_2$ (analog pentru cazul $P_2 = \mathcal{O}$, avem $P_1 + P_2 = P_1$);

(2) Dacă $x_1 \neq x_2$, atunci fie $x_3 = m^2 - x_1 - x_2$ și $y_3 = m(x_1 - x_3) - y_1$, unde $m = (y_2 - y_1)/(x_2 - x_1)$;

(3) Dacă $x_1 = x_2$ și $y_1 \neq y_2$, atunci $P_3 = \mathcal{O}$;

(4) Dacă $P_1 = P_2$ și $y_1 \neq 0$, atunci $x_3 = m^2 - 2x_1$, $y_3 = m(x_1 - x_3) - y_1$, unde $m = (3x_1^2 + A)/(2y_1)$;

(5) Dacă $P_1 = P_2$ și $y_1 = 0$, atunci $P_3 = \mathcal{O}$.

Observația 3.1. *În exact același mod, cu aceleași formule, putem defini operația de adunare a punctelor unei curbe eliptice definite peste un corp finit $\mathbb{F}_q$, unde $q = p^m$, $p > 3$ este prim, $m \in \mathbb{N}^*$ și $char(\mathbb{F}) > 3$.*

Următoarea teoremă stabilește faptul că mulțimea punctelor curbei împreună cu operația de adunare formează un grup abelian.

Teorema 3.1. *Fie $\mathbb{K}$ un corp, care, în cazul infinit, poate fi $\mathbb{Q}$ sau $\mathbb{R}$, iar în cazul finit, $\mathbb{F}_q$, unde $q = p^m$, $m \in \mathbb{N}^*$, iar $p > 3$ este un număr prim și fie E o curbă eliptică de ecuație $y^2 = x^3 + Ax + B$, cu $A, B \in \mathbb{K}$ și $4A^3 + 27B^2 \neq 0$. Atunci, punctele lui E împreună cu operația de adunare definită în Rezumatul 1 formează un grup comutativ.*

3.1 Calculul rapid al multiplilor unui punct

Pe parcursul lucrării vom folosi de multe ori adunarea succesivă a unui singur punct cu el însuși. Aceasta poate fi folosită în diverse sisteme de criptare la calcularea

cheilor publice, a semnăturilor, a mesajelor criptate sau la protocolul de schimb al cheilor. Pe scurt, notăm $0P = \mathcal{O}$ și :

$$dP \coloneqq \underbrace{P + P + \cdots + P}_{\text{d ori}}, \quad \text{unde } d \in \mathbb{N} \setminus \{0\}.$$

Să observăm un fapt elementar, dar extrem de util: pentru a obține multiplul dP, nu sunt neapărat necesare efectuarea a $d-1$ operații de adunare, cum ar părea la prima vedere, ci, numărul acestora poate fi redus calculând succesiv dublurile $2P = P + P$, $2P + 2P = 4P$, $4P + 4P = 8P$, etc. Din acestea se obține apoi multiplul dorit. De exemplu, $13P = P + 4P + 8P$. În general, numărul operațiilor necesare pentru a-l calcula pe dP este cel mult egal cu $2\log_2 d$. Într-adevăr:

Exponențierea rapidă. Fie $\overline{d_{n-1}d_{n-2}\dots d_0}$ scrierea în baza 2 a lui d. Atunci

$$d = d_{n-1}2^{n-1} + d_{n-2}2^{n-2} + \cdots + d_1 2 + d_0\,, \tag{8}$$

unde cifrele $d_1, \dots, d_{n-1} \in \{0, 1\}$ și $d_{n-1} = 1$. De aici rezultă că $2^{n-1} \leq d < 2^n$ și, prin urmare, $n - 1 = \lfloor \log_2 d \rfloor$. Folosim scrierea lui d în forma (8) în calculul lui dP astfel. Să observăm că, pe de o parte, în scrierea (8) se efectuează $\log_2 d$ operații de adunare, iar, pe de altă parte, pentru a afla toți termenii sumei, efectuăm de asemenea $\log_2 d$ operații de adunare, calculând recursiv $2^{n-1}P = 2(2(\dots 2(P)))$ și observând că toți termenii sumei sunt obținuți pe parcurs. Prin urmare, dP se poate obține prin efectuarea a $\log_2 d + \log_2 d = 2\log_2 d$ adunări. Acest procedeu de calcul a fost denumit *Double-and-Add algorithm* sau *Exponențiere rapidă*.

Exemplu:

Fie curba eliptică $E : y^2 = x^3 + 3x + 45$ peste corpul $\mathbb{F}_{8831}$ și punctul $P = (4, 11) \in E$. Vrem să calculăm $2502P$.

Pasul 1: Îl descompunem pe 2502 în sumă de puteri ale lui 2 și obținem $2502 = 2^{11} + 2^8 + 2^7 + 2^6 + 2^2 + 2^1$.

Pasul 2: Calculăm multiplii dP, unde d sunt puterile lui 2 (până la puterea maximă apărută în descompunerea lui 2502, i.e., 2^{11}) și reținem informațiile într-un table/vector. Obținem:

i	0	1	2	3
2^iP	$(4, 11)$	$(7168, 3452)$	$(5169, 3357)$	$(5415, 6321)$
i	4	5	6	7
2^iP	$(2061, 7304)$	$(6380, 1218)$	$(5878, 8657)$	$(3423, 6675)$
i	8	9	10	11
2^iP	$(7902, 4842)$	$(227, 5624)$	$(3369, 3686)$	$(748, 2458)$

Pasul 3: Calculăm $2502P = 2^{11}P + 2^8P + 2^7P + 2^6P + 2^2P + 2^1P = (748, 2458) + (7902, 4842) + (3423, 6675) + (5878, 8657) + (5169, 3357) + (7168, 3452)$ și obținem $2502P = (5592, 7900)$.

În continuare prezentăm un algoritm care este și mai eficient decât *Exponențierea rapidă* din punct vedere al spațiului de memorie necesar. Trebuie să remarcăm faptul că algoritmul anterior are complexitatea de ordinul $O(\log n)$ atât pentru timp cât și pentru spațiu. Următorul algoritm, care se numește *Left-to-right Montgomery ladder,* fiind prezentat în [Mon'87], are complexitatea $O(\log n)$ pentru timp și $O(1)$ pentru spațiu.

Date de intrare: E, $P = (x, y) \in E$, $d = (1, d_{n-2}, \ldots, d_0)$;
Date de ieșire: $Q = dP$;
1: $R_0 \leftarrow P$, $R_1 \leftarrow 2P$;
2: **pentru** i **de la** $n-2$ **la** 0
3: **dacă** $k_i = 1$ **atunci**
4: $R_0 \leftarrow R_0 + R_1$, $R_1 \leftarrow 2R_1$;
5: **altfel**
6: $R_1 \leftarrow R_0 + R_1$, $R_0 \leftarrow 2R_0$;
7: **întoarce rezultatul** $Q = R_0$.

Se observă în această situație că nu mai este solicitată memoria decât cu scrierea lui $d = \overline{1, d_{n-2}, \ldots, d_0}$ în baza 2 și cu valorile variabilelor P, R_0 și R_1, iar timpul de execuție este proporțional cu numărul de cifre ale lui d în baza 2, așadar avem complexitatea timp $O(\log n)$, iar complexitatea spațiu $O(1)$.

3.2 Ordinul grupului, Teorema lui Hasse

Având intenția de a folosi structura descrisă mai sus într-un protocol de criptare, securitatea acestuia va fi dependentă de numărul de elemente ale grupului. În continuare vom prezenta câteva rezultate care estimează acest număr în funcție de corpul peste care lucrăm. Este evident că în cazul unui corp infinit, vom avea o infinitate de puncte într-o curbă eliptică și prin urmare ne punem această problemă doar în cazul în care lucrăm într-un $\mathbb{F}_q$.

Teorema 3.2 (Hasse 1933)**.** *Fie E o curbă eliptică peste corpul finit $\mathbb{F}_q$. Atunci*

$$\big||E| - (q+1)\big| \leq 2\sqrt{q}\,. \tag{9}$$

Succint, Teorema lui Hasse spune că ordinul de mărime al abaterii față de p al numărului de puncte de pe o curbă eliptică peste $\mathbb{F}_p$ este de ordinul $\sqrt{p}$, adică $|E| = p + O(\sqrt{p})$.

Teorema lui Hasse [Has'33] este un caz particular al unei conjecturi din 1924 a lui Emil Artin, care este un enunț mai general formulat pentru curbe algebrice.

André Weil [Wei'49] a completat demonstrația conjecturii lui Artin pentru curbe algebrice peste corpuri finite, iar în estimarea sa corespunzătoare inegalității (9) apare în plus doar un factor multiplicativ g, care este genul curbei algebrice.

Rezultatul lui Hasse a fost fost dezvoltat de André Weil [Wei'49], [Wei'79] într-un cadru mai general și este cunoscut sub numele de Conjecturile lui Weil.

3.3 Sume exponențiale

O consecință importantă a demonstrării conjecturilor lui Weil [Del'74], [Del'80] este obținerea de către Bombieri [Bom'66] și Deligne [Del'74, Section 8] a estimărilor pentru diverse sume exponențiale a unor combinații de caractere aditive și multiplicative. (Pentru noi, de interes sunt cazul particular în care caracterele multiplicative sunt triviale, constante egale cu 1, iar caracterele aditive sunt funcțiile $e_p(t) := e^{2\pi it/p}$). Aceste estimări sunt de mare interes în teoria numerelor, deoarece ele pot fi folosite pentru a obține informații despre distribuția unor șiruri, proprietățile unor numere, soluțiile unor ecuații, etc. Vom prezenta o exemplificare a acestui fapt, analizând în cele ce urmează distribuția punctelor unei curbe eliptice peste un corp finit. Obiectivul nostru este de a extinde rezultatul lui Hasse pentru a obține o estimare locală a numărului de puncte de pe o curbă eliptică peste un corp finit.

Întrebarea fundamentală este legată de observația sugerată de Figurile 3.5, 2.3:

> *Este adevărat că punctele unei curbe eliptice peste $\mathbb{F}_p$ sunt uniform distribuite în pătratul $\mathbb{F}_p \times \mathbb{F}_p$? Oare cât de mult poate fi micșorat un pătrat oarecare inclus în $\mathbb{F}_p \times \mathbb{F}_p$ pentru a putea fi siguri că acesta încă conține puncte ale curbei? Depinde mărimea acestui pătrat de curbă sau doar de p, la fel ca marginea termenului eroare din Teorema lui Hasse?*

Pentru a investiga această problemă, avem nevoie de următoarea estimare a unor sume exponențiale de caractere aditive pe grupul punctelor curbei. Rezultatul datorat lui Kohel și Shparlinski [KS'00] este o consecință a estimării sumelor exponențiale datorate lui Bombieri [Bom'66]. În forma particulară de care vom avea în continuare nevoie, rezultatul este prezentat în teorema care urmează (a se vedea și enunțul din prezentarea [LS'06] lucrării [LS'07]).

Teorema 3.3 (Kohel, Shparlinski)**.** *Fie E o curbă eliptică peste $\mathbb{F}_p$, $p > 3$ prim și $H \subset E$ un subgrup al grupului format din punctele curbei. Atunci, pentru orice funcție neconstantă $f : E \to \{0, \ldots, p-1\}$, avem:*

$$\sum_{P \in H} e_p\big(f(P)\big) = O(\sqrt{p}),$$

unde $e_p(t) \coloneqq e^{\frac{2\pi it}{p}}$, pentru orice $t \in \mathbb{R}$.

În particular, din Teorema 3.3 rezultă următoarea formă particulară a estimării, cea pe care o vom aplica în demonstrațiile Teoremelor 3.4, 3.5 și 3.6:

$$S_p(u, v) := \sum_{(x,y) \in E} e_p\big(ux + vy\big) = O(\sqrt{p}), \tag{10}$$

pentru orice $u, v \in \mathbb{Z}$, nedivizibile simultan cu p.

Câteva proprietăți ale funcției e_p de care vom avea nevoie sunt prezentate în lema care urmează.

Lema 3.1. *Fie p un număr prim și fie funcția $e_p : \mathbb{R} \to \mathbb{R}$, definită prin $e_p(t) = e^{\frac{2\pi i t}{p}}$. Atunci, pentru orice $\alpha, \beta \in \mathbb{R}$ și orice $u \in \mathbb{Z}$, au loc următoarele egalități:*

$$e_p(\alpha)e_p(\beta) = e_p(\alpha + \beta), \tag{i}$$

$$\sum_{x \in \{0,\ldots,p-1\}} e_p(ux) = \begin{cases} p & \text{dacă } u \equiv 0 \pmod{p}; \\ 0 & \text{dacă } u \not\equiv 0 \pmod{p}, \end{cases} \tag{ii}$$

$$|e_p(\alpha)| = 1. \tag{iii}$$

Demonstraţie. Să observăm că $e_p(t)$ este o formă particulară a notației lui Euler $\exp(\alpha) := \cos\alpha + i\sin\alpha$, care reprezintă punctul de pe cercul unitate aflat la capătul unui arc de lungime $\alpha \pmod{2\pi}$, măsurat în sens trigonometric începând cu punctul $(0, 1)$. Astfel, pentru $\alpha = 2\pi t/p$, avem $\exp(\alpha) = e_p(t)$. Atunci egalitatea (iii) rezultă din definiție (formula rezultă din Teorema lui Pitagora scrisă sub forma $\cos^2\alpha + \sin^2\alpha = 1$), iar relația (i) este o proprietate de bază a funcției exponențiale, care rezultă direct din definiția sa.

Pentru a demonstra formula (ii), să observăm că dacă x este număr întreg și $p \mid u$, atunci există $k \in \mathbb{Z}$ astfel încât $u = kp$. Atunci $e_p(ux) = e_p(kpx) = \exp(2\pi ikpx/p) = \exp(2\pi ikx) = 1$, deoarece produsul kx este număr întreg. Aceasta argumentează prima parte a formulei (ii), deoarece, în acel caz, în suma din partea stângă se adună p numere care sunt egale toate cu 1.

Să presupunem acum că $u \not\equiv 0 \pmod{p}$. Să observăm că în acest caz, dacă $x \in \{0, 1, \ldots, p-1\}$, atunci numerele $ux/p \pmod 1$ sunt diferite două câte două. Într-adevăr, dacă $x_1, x_2 \in \{0, 1, \ldots, p-1\}$ și $ux_1/p = ux_2/p \pmod 1$, atunci $u(x_1 - x_2)/p = 0 \pmod 1$. Ținând cont de ipoteza că u este relativ prim cu p, rezultă că $u(x_1 - x_2)/p = 0 \pmod 1$, ceea ce implică $x_1 = x_2$. Aceasta înseamnă că numerele care se adună în partea stângă a formulei (ii) sunt exact rădăcinile de ordinul p din 1. Indiferent de ordinea în care acestea sunt scrise, suma lor este egală cu suma unei progresii geometrice:

$$\sum_{x \in \{0,\ldots,p-1\}} e_p(ux) = \sum_{y=0}^{p-1} e_p(y) = \frac{\exp(2\pi ip/p) - 1}{\exp(2\pi i/p) - 1} = \frac{1-1}{\exp(2\pi i/p) - 1} = 0,$$

ceea ce încheie demonstrația lemei.

□

În sfârșit un rezultat elementar care aproximează funcția $\sin(\cdot)$ cu o dreaptă:

Lema 3.2. *Pentru orice $t \in [0, 1]$ are loc inegalitatea*

$$2\|t\| \leq \sin \pi t\,. \tag{11}$$

Demonstraţie. Vezi Figura 3.6.

□

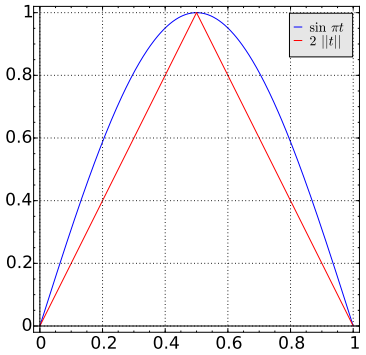


Figura 3.6: Comparație între funcțiile $t \mapsto \sin \pi t$ și dublul distanței de la t la cel mai apropiat număr întreg, pentru $t \in [0, 1]$.

3.4 Distribuția punctelor unei curbe eliptice în $\mathbb{F}_p^2$

Fie E o curbă eliptică peste $\mathbb{F}_p$. Dorim să estimăm numărul punctelor lui E care au abscisa sau ordonata într-un subinterval al lui $[0, p-1]$. Atunci, dacă $I \subset [1, p-1]$ este un subinterval de numere întregi fixat, ceea ce vrem este să calculăm cardinalul mulțimii

$$E_I = \left\{(x, y) \in E : x \in I\right\}.$$

Să observăm că punctele din mulțimea E_I sunt situate într-o bandă verticală, așa cum se poate vedea în imaginea din partea stângă a Figurii 3.7.

Metoda folosită în demonstrația teoremei următoare este o adaptare în cazul nostru particular al aceleia utilizate în lucrarea [CZ'01].

Teorema 3.4. *Fie E o curbă eliptică peste $\mathbb{F}_p$, $p > 3$ prim și fie $I \subset [1, p-1] \cap \mathbb{N}$ un interval de numere întregi. Atunci numărul punctelor din E care au abscisa în intervalul I este dat de estimarea:*

$$|E_I| = |I| + O(\sqrt{p} \log p).$$

Demonstrație. Definim funcția caracteristică a intervalului I:

$$\varphi_I(x) := \begin{cases} 1 & \text{dacă } x \in I; \\ 0 & \text{dacă } x \in [1, p-1] \setminus I. \end{cases}$$

Transformata Fourier a lui φ_I este definită astfel:

$$\hat{\varphi}_I(u) := \frac{1}{p} \sum_{x=0}^{p-1} \varphi_I(x) e_p(-ux), \quad \forall u \in [0, p-1] \cap \mathbb{N}.$$

Din definiția de mai sus putem deduce că

$$\varphi_I(x) = \sum_{u=0}^{p-1} \hat{\varphi}_I(x) e_p(ux). \tag{12}$$

Într-adevăr, această egalitate poate fi verificată prin calcul direct. Astfel, pentru orice $x \in [0, p-1] \cap \mathbb{N}$ fixat, avem:

$$\begin{aligned}\sum_{u=0}^{p-1} \hat{\varphi}_I(u) e_p(ux) =& \sum_{u=0}^{p-1} \left(\frac{1}{p} \sum_{x'=0}^{p-1} \varphi_I(x') e_p(-ux') \right) e_p(ux) \\ =& \frac{1}{p} \sum_{u=0}^{p-1} \sum_{x'=0}^{p-1} \varphi_I(x') e_p(-ux') e_p(ux).\end{aligned}$$

De aici, schimbând ordinea de sumare, folosind proprietățile (i) și (ii) din Lema 3.1 și izolând termenii pentru care $x' = x$, obținem:

$$\begin{aligned}\sum_{u=0}^{p-1} \hat{\varphi}_I(u) e_p(ux) =& \frac{1}{p} \sum_{x'=0}^{p-1} \varphi_I(x') \sum_{u=0}^{p-1} e_p(u(x-x')) \\ =& \frac{1}{p} \varphi_I(x) \sum_{u=0}^{p-1} e_p(0) + \frac{1}{p} \sum_{x' \in \{0,\ldots,p-1\} \setminus x} \varphi_I(x') \sum_{u=0}^{p-1} e_p(u(x-x')) \\ =& \frac{1}{p} \varphi_I(x) p + \frac{1}{p} \sum_{x' \in \{0,\ldots,p-1\} \setminus x} 0 \\ =& \varphi_I(x).\end{aligned}$$

Folosind funcția caracteristică, să observăm că putem scrie $|E_I|$ sub forma unei sume exponențiale, astfel:

$$|E_I| = \sum_{(x,y) \in E} \varphi_I(x).$$

Înlocuind $\varphi_I(x)$ cu expresia sa dată de formula (12), schimbând ordinea de sumare și izolând termenul principal, putem scrie:

$$\begin{aligned}|E_I| =& \sum_{(x,y) \in E} \sum_{u=0}^{p-1} \hat{\varphi}_I(u) e_p(ux) \\ =& \sum_{u=0}^{p-1} \hat{\varphi}_I(u) \sum_{(x,y) \in E} e_p(ux) \\ =& \hat{\varphi}_I(0) \sum_{(x,y) \in E} e_p(0) + \sum_{u=1}^{p-1} \hat{\varphi}_I(u) \sum_{(x,y) \in E} e_p(ux) \\ =& M + err,\end{aligned} \tag{13}$$

unde

$$\begin{aligned}M :=& \hat{\varphi}_I(0) \sum_{(x,y) \in E} e_p(0) \\ err :=& \sum_{u=1}^{p-1} \hat{\varphi}_I(u) \sum_{(x,y) \in E} e_p(ux).\end{aligned}$$

În continuare trebuie să îi estimăm pe M și pe err. Folosind doar definiția transformatei Fourier a lui φ_I și faptul că $\varphi_I(x) = 0$ pentru orice $x \notin I$, termenul principal se obține imediat:

$$\begin{aligned} M =& \hat{\varphi}_I(0) \sum_{(x,y)\in E} e_p(0) \\ =& \left(\frac{1}{p} \sum_{x=0}^{p-1} \varphi_I(x) e_p(0) \right) \sum_{(x,y)\in E} 1 \\ =& \frac{1}{p} |E| \sum_{x\in I} 1 \\ =& \frac{|I||E|}{p}. \end{aligned}$$

De aici, aplicând Teorema lui Hasse, rezultă că

$$M = \frac{|I|}{p}(p + O(\sqrt{p})) = |I| + O(\sqrt{p}). \tag{14}$$

Pentru a găsi un majorant pentru $|err|$ avem nevoie de o estimare a lui $|\hat{\varphi}_I(u)|$ pentru $u \neq 0$. Vom nota cu i_s și i_d capetele stâng și respectiv drept ale intervalului I. Fie $u \in \{1, \ldots, p-1\}$, atunci:

$$\begin{aligned} |\hat{\varphi}_I(u)| &= \left| \frac{1}{p} \sum_{x=0}^{p-1} \varphi_I(x) e_p(-ux) \right| \\ &= \frac{1}{p} \left| \sum_{x=i_s}^{i_d} e_p(-ux) \right| \\ &= \frac{1}{p} \left| \sum_{x=0}^{i_d - i_s} e_p(-ui_s - ux) \right| \\ &= \frac{1}{p} |e_p(-ui_s)| \left| \sum_{x=0}^{i_d - i_s} e_p(-ux) \right| \\ &= \frac{1}{p} \left| \sum_{x=0}^{i_d - i_s} e_p(-ux) \right|. \end{aligned}$$

Continuăm evaluarea adunând termenii progresiei geometrice:

$$\begin{aligned} |\hat{\varphi}_I(u)| &= \frac{1}{p} \left| \frac{e_p(-u)^{i_d - i_s + 1} - 1}{e_p(-u) - 1} \right| \\ &\leq \frac{|e_p(u)^{i_d - i_s + 1}| + 1}{p \cdot |1/e_p(u) - 1|} \\ &= \frac{2}{p \cdot |1 - e_p(u)|/|e_p(u)|} \\ &= \frac{2}{p \cdot |e_p(u) - 1|}. \end{aligned}$$

Așadar

$$|\hat{\varphi}_I(u)| \leq \frac{2}{p \cdot |e_p(u) - 1|}. \tag{15}$$

Numitorul fracției din (15) se poate majora astfel:

$$\begin{aligned} p \cdot |e_p(u) - 1| =& p \left| 1 - e^{\frac{-2\pi iu}{p}} \right| = p \left| e^{\frac{-\pi iu}{p}} \left(e^{\frac{-\pi iu}{p}} - e^{\frac{\pi iu}{p}} \right) \right| \\ =& p \left| e^{\frac{-\pi iu}{p}} \right| \left| e^{\frac{-\pi iu}{p}} - e^{\frac{\pi iu}{p}} \right| \\ =& p \left| 2i \sin\left(\frac{\pi u}{p} \right) \right| = 2p \left| \sin\left(\frac{\pi u}{p} \right) \right| \\ \geq& 2p \cdot 2 \left\| \frac{u}{p} \right\| = 4p \cdot \left\| \frac{u}{p} \right\|. \end{aligned}$$

Pentru obținerea ultimei inegalități am aplicat Lema 3.2. Folosind această estimare în inegalitatea, rezultă

$$|\hat{\varphi}_I(u)| \leq \frac{2}{p \cdot |e_p(u) - 1|} \leq \frac{2}{4p \cdot ||\frac{u}{p}||} = \frac{1}{2p \cdot ||\frac{u}{p}||}. \tag{16}$$

Folosind inegalitatea (16) în definiția *err*, rezultă:

$$\begin{aligned} |err| &= \left| \sum_{u=1}^{p-1} \hat{\varphi}_I(u) \sum_{(x,y) \in E} e_p(ux) \right| \\ &\leq \sum_{u=1}^{p-1} |\hat{\varphi}_I(u)| \left| \sum_{(x,y) \in E} e_p(ux) \right| \\ &\leq \sum_{u=1}^{p-1} \frac{1}{2p \cdot \|\frac{u}{p}\|} |S_p(u, 0)| \end{aligned}$$

Știind din Teorema 3.3 (Kohel, Shparlinski) că $|S_p(u, 0)| = O(\sqrt{p})$, putem continua majorarea astfel:

$$\begin{aligned} |err| &\ll \sqrt{p} \sum_{u=1}^{p-1} \frac{1}{2p \cdot \|\frac{u}{p}\|} \\ &= \sqrt{p} \cdot 2 \cdot \sum_{u=1}^{(p-1)/2} \frac{1}{2p \cdot \frac{u}{p}} \\ &= \sqrt{p} \cdot \sum_{u=1}^{(p-1)/2} \frac{1}{u} \\ &\ll \sqrt{p} \log p, \end{aligned} \tag{17}$$

deoarece $1 + 1/2 + \cdots + 1/N = O(\log N)$. Așadar $|err| = O(\sqrt{p} \log p)$. În concluzie, din 13, 14 și (17) obținem $|E_I| = |I| + O(\sqrt{p}) + O(\sqrt{p} \log p) = |I| + O(\sqrt{p} \log p)$, ceea ce era de demonstrat. □

Să observăm că rezultatul Teoremei 3.4 este netrivial pentru intervale a căror lungime are un ordin de mărime mai mare decât $\sqrt{p}\log p$.

Raționând similar vom arăta că putem aproxima și numărul punctelor unei curbe eliptice care au ordonata într-un anumit interval.

Teorema 3.5. *Fie E o curbă eliptică peste $\mathbb{F}_p$, $p > 3$ prim și $J \subset \{1, \dots, p-1\}$ un interval de numere întregi. Atunci numărul punctelor de pe curba E care au ordonata în intervalul J este egal cu:*

$$|E_J| = |J| + O(\sqrt{p}\log p),$$

unde $E_J \coloneqq \{(x, y) \in E : y \in J\}$.

Demonstraţie. La fel cum am procedat în demonstrația Teoremei 3.4, vom defini funcția caracteristică a intervalului J, transformata sa Fourier și vom pune din nou în evidență legătura dintre acestea:

$$\varphi_J(y) = \begin{cases} 1 & \text{dacă } y \in J; \\ 0 & \text{dacă } y \in [1, p-1] \setminus J. \end{cases}$$

$$\hat{\varphi}_J(v) \coloneqq \frac{1}{p}\sum_{y=0}^{p-1} \varphi_J(y) e_p(-vy), \quad \forall v \in [0, p-1] \cap \mathbb{N};$$

$$\varphi_J(y) = \sum_{v=0}^{p-1} \hat{\varphi}_J(v) e_p(vy).$$

Observăm că $|E_J| = \sum_{(x,y)\in E} \varphi_J(y)$. Folosindu-ne de scrierea lui φ_J în funcție de transformata sa Fourier obținem:

$$\begin{aligned} |E_J| &= \sum_{(x,y)\in E} \sum_{v=0}^{p-1} \hat{\varphi}_J(v) e_p(vy) \\ &= \sum_{v=0}^{p-1} \hat{\varphi}_J(v) \sum_{(x,y)\in E} e_p(vy) \\ &= \hat{\varphi}_J(0) \sum_{(x,y)\in E} e_p(0) + \sum_{v=1}^{p-1} \hat{\varphi}_J(v) \sum_{(x,y)\in E} e_p(vy). \end{aligned}$$

După cum am văzut anterior, în demonstrația Teoremei 3.4, primul termen de pe ultimul rând, adică, $\hat{\varphi}_J(0) \sum_{(x,y)\in E} e_p(0)$, este egal cu

$$\frac{|I|}{p} \cdot |E| = \frac{|I|}{p}(p + O(\sqrt{p}) = |I| + O(1),$$

conform Teoremei lui Hasse. De asemenea, procedând tot la fel ca în demonstrația Teoremei 3.4, vedem că valoarea absolută a celui de-al doilea termen este

$$\begin{aligned}
&\leq \sum_{v=1}^{p-1} \left|\hat{\varphi}_J(v)\right| \cdot \Big| \sum_{(x,y)\in E} e_p(vy)\Big| \\
&\leq \sum_{v=1}^{p-1} \frac{2}{p\cdot|e_p(v)-1|} \cdot |S_p(0,v)| \\
&\ll \sqrt{p}\log p,
\end{aligned}$$

fiindcă, din Teorema Kohel-Shparlinski 3.3 știm că $|S_p(0,v)| \leq 2\sqrt{p}$. Prin urmare

$$|E_J| = |J| + O(\sqrt{p}\log p),$$

ceea ce încheie demonstrația teoremei. □

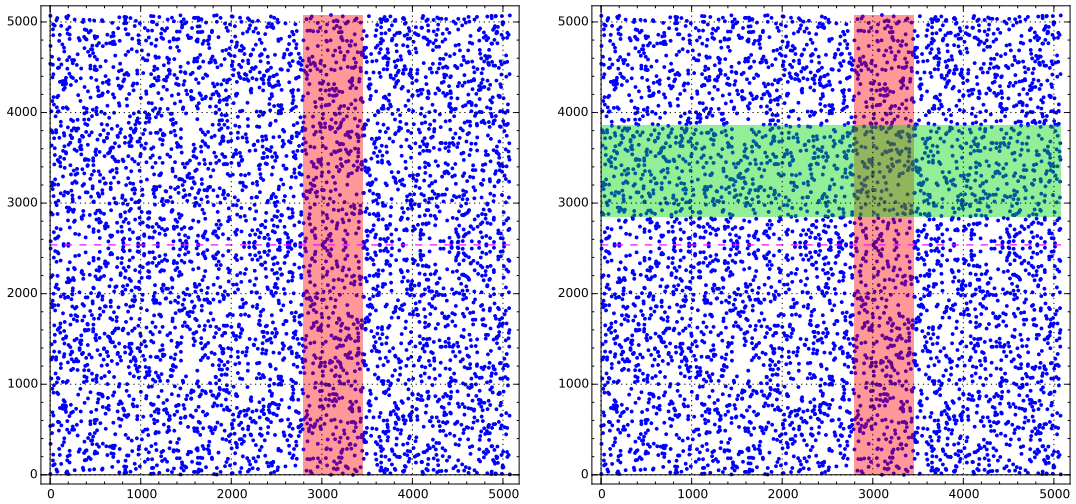


Figura 3.7: Distribuția uniformă a punctelor unei curbe eliptice peste un corp finit. Curba eliptică $E: y^2 = x^3 + 7x + 33$ peste $\mathbb{F}_p$, cu $p = 5077$, al 679-lea număr prim. E are discriminantul 69 și conține 5126 puncte. Intervalele $I = [2793, 3452]$, $J = [2844, 3858]$ au lungimile $|I| = 659$ și $|J| = 1014$. Banda verticală roșie $I \times [0, p-1]$ conține 657 puncte, iar banda orizontală verde $[0, p-1] \times J$ conține 1023 puncte ale curbei. Intersecția celor două benzi, dreptunghiul $I \times J$, are aria $|I \times J| = 668226$ și conține 137 puncte, număr care este bine aproximat de raportul $|I \times J|/p \approx 131.62$.

În cele din urmă vom generaliza rezultatele de mai sus estimând numărul de puncte ale unei curbe eliptice care se află într-un produs de intervale de forma $I \times J$, unde I și J sunt două subintervale de numere întregi, incluse în $[0, p-1]$.

Teorema 3.6. *Fie E o curbă eliptică peste $\mathbb{F}_p$, $p > 3$ prim și $I, J \subset \{1, \ldots, p-1\}$, două intervale de numere întregi. Atunci numărul punctelor de pe curba E care au abscisa în intervalul I și ordonata în intervalul J este:*

$$|E_{I\times J}| = \frac{|I \times J|}{p} + O(\sqrt{p}\log^2 p),$$

unde

$$E_{I\times J} = \{(x,y) \in E : x \in I \text{ și } y \in J\}.$$

Demonstrație. Definim funcțiile caracteristice ale intervalelor I și J și transformatele lor Fourier:

$$\varphi_I(x) \coloneqq \begin{cases} 1 \text{ dacă } x \in I; \\ 0 \text{ dacă } x \in [1, p-1] \setminus I. \end{cases}$$

$$\hat{\varphi}_I(u) \coloneqq \frac{1}{p}\sum_{x=0}^{p-1} \varphi_I(x) e_p(-ux),\ \forall u \in [0, p-1] \cap \mathbb{N};$$

$$\varphi_J(y) \coloneqq \begin{cases} 1 \text{ dacă } y \in J; \\ 0 \text{ dacă } y \in [1, p-1] \setminus J. \end{cases}$$

$$\hat{\varphi}_J(v) \coloneqq \frac{1}{p}\sum_{y=0}^{p-1} \varphi_J(y) e_p(-vy),\ \forall v \in [0, p-1] \cap \mathbb{N};$$

Atunci, $|E_{I\times J}|$ se poate scrie astfel:

$$\begin{aligned} |E_{I\times J}| &= \sum_{(x,y)\in E} \varphi_I(x)\varphi_J(y) \\ &= \sum_{(x,y)\in E} \sum_{v=0}^{p-1} \varphi_I(x)\hat{\varphi}_J(v) e_p(vy) \\ &= \sum_{v=0}^{p-1} \hat{\varphi}_J(v) \sum_{(x,y)\in E} \varphi_I(x) e_p(vy) \\ &= \sum_{v=0}^{p-1}\sum_{u=0}^{p-1} \hat{\varphi}_J(v)\hat{\varphi}_I(u) \sum_{(x,y)\in E} e_p(ux) e_p(vy) \end{aligned}$$

Separând în aceste sume termenii în care u sau v sunt egali cu 0, rezultă

$$\begin{aligned} |E_{I\times J}| =& \hat{\varphi}_I(0)\hat{\varphi}_J(0) \sum_{(x,y)\in E} e_p(0) + \hat{\varphi}_I(0) \sum_{v=1}^{p-1} \hat{\varphi}_J(v) \sum_{(x,y)\in E} e_p(vy) \\ &+ \hat{\varphi}_J(0) \sum_{u=1}^{p-1} \hat{\varphi}_I(u) \sum_{(x,y)\in E} e_p(ux) \\ &+ \sum_{u=1}^{p-1}\sum_{v=1}^{p-1} \hat{\varphi}_I(u)\hat{\varphi}_J(v) \sum_{(x,y)\in E} e_p(ux+vy). \end{aligned} \tag{18}$$

Notăm cei patru termeni scoși în evidență în partea dreaptă a egalității anterioare, în ordine, cu M, err_I, err_J și respectiv $err_{I\times J}$, și îi analizăm pe fiecare în parte.

Folosind Teorema lui Hasse, M este

$$\begin{aligned} M =& \hat{\varphi}_I(0)\hat{\varphi}_J(0) \sum_{(x,y)\in E} 1 = \frac{|I|}{p} \cdot \frac{|J|}{p} \cdot |E| \\ =& \frac{|I \times J|}{p^2}(p + O(\sqrt{p})) \\ =& \frac{|I \times J|}{p} + O(\sqrt{p}). \end{aligned} \tag{19}$$

Termenii err_I și err_J pot fi majorați ca în demonstrațiile Teoremelor 3.4 și 3.5:

$$\begin{aligned} |err_I| =& \Big|\hat{\varphi}_I(0) \sum_{v=1}^{p-1} \hat{\varphi}_J(v) \sum_{(x,y)\in E} e_p(vy)\Big| \\ \leq& \frac{|I|}{p} \left| \sum_{v=1}^{p-1} \hat{\varphi}_J(v) O(\sqrt{p}) \right| \leq \frac{|I|}{p}\sqrt{p}\log p = O(\sqrt{p}\log p); \end{aligned} \tag{20}$$

Analog avem:

$$|err_J| = O(\sqrt{p}\log p). \tag{21}$$

În sfârșit, ne rămâne să estimăm ultimul termen. Avem:

$$\begin{aligned} |err_{I\times J}| =& \left| \sum_{u=1}^{p-1}\sum_{v=1}^{p-1} \hat{\varphi}_I(u)\hat{\varphi}_J(v) \sum_{(x,y)\in E} e_p(ux+vy) \right| \\ \leq& \sum_{u=1}^{p-1}\sum_{v=1}^{p-1} |\hat{\varphi}_I(u)| \cdot |\hat{\varphi}_J(v)| \cdot \Big| \sum_{(x,y)\in E} e_p(ux+vy)\Big| \\ \leq& \sum_{u=1}^{p-1}\sum_{v=1}^{p-1} |\hat{\varphi}_I(u)| \cdot |\hat{\varphi}_J(v)| \cdot |S_p(u,v)| \,. \end{aligned}$$

Folosind aici inegalitatea (16) și Teorema Kohel-Shparlinski, putem continua majorarea pentru a obține

$$\begin{aligned} |err_{I\times J}| \ll& \sum_{u=1}^{p-1}\sum_{v=1}^{p-1} \frac{1}{2p \cdot ||\frac{u}{p}||} \cdot \frac{1}{2p \cdot ||\frac{v}{p}||}\sqrt{p} \\ =& \sqrt{p}\,\Big(\sum_{u=1}^{p-1} \frac{1}{2p \cdot ||\frac{u}{p}||}\Big)^2 \\ =& \sqrt{p}\,\Big(\sum_{u=1}^{\frac{p-1}{2}} \frac{1}{p \cdot \frac{u}{p}}\Big)^2 \\ \ll& \sqrt{p}\log^2 p \,. \end{aligned} \tag{22}$$

Inserând în egalitatea (18) estimările (19), (20), (21) și (22) obținem concluzia:

$$\begin{aligned}|E_{I\times J}| =& \frac{|I\times J|}{p} + O(\sqrt{p}\log p) + O(\sqrt{p}\log p) + O(\sqrt{p}\log^2 p)\\ =& \frac{|I\times J|}{p} + O(\sqrt{p}\log^2 p),\end{aligned}$$

ceea ce încheie demonstrația teoremei. □

În particular, dacă presupunem că intervalele I și J sunt egale, atunci din Teorema 3.6 rezultă că pătratul $I \times I$ conține cel puțin un punct al curbei dacă termenul principal al estimării are un ordin de mărime mai mare decât termenul eroare, adică, de exemplu, dacă $\frac{|I|^2}{p} \gg \sqrt{p}\log^{2+\epsilon} p$ (care este $\gg \sqrt{p}\log^2 p$, pentru orice $\epsilon > 0$ fixat), estimare care este echivalentă cu condiția $\frac{|I|}{p} \gg p^{3/4}\log^{1+\epsilon} p$. În consecință, am obținut următorul corolar.

Corolarul 3.1. *Fie E o curbă eliptică peste $\mathbb{F}_p$, $p > 3$ prim și fie $\mathcal{P} \subset [1, p-1]^2$ un pătrat cu latura $l(p)$. Fie $\epsilon > 0$ un număr real fixat. Presupunem că există $C > 0$ și $p_0 > 0$ astfel încât*

$$l(p) > Cp^{3/4}\log^{1+\epsilon} p, \qquad \textit{pentru orice } p > p_0.$$

Atunci, pătratul $\mathcal{P}$ conține cel puțin un punct al curbei E, pentru orice $p \geq p_0$.

3.5 Corpurile infinite și sistemele criptografice

Din cauza faptului că nu este cunoscută o metodă de reprezentare a tuturor numerelor reale într-un limbaj mașină, trebuie să excludem încă de la început folosirea unor curbe eliptice peste $\mathbb{R}$ în algoritmii de criptare. Curbele eliptice peste corpul numerelor raționale sunt ineficiente deoarece, în general acestea au puține puncte de coordonate mici, acestea crescând foarte repede prin multiplicarea punctelor. Mai mult decât atât, se cunosc puține exemple de astfel de curbe care să aibă unu număr semnificativ de coordonate întregi. Spre exemplu, în lucrarea [Wim'53], Wiman analizează următoarele curbe eliptice peste $\mathbb{Q}$:

$$y^2 = x^3 - 7x + 10, \qquad (e_1)$$
$$y^2 = x^3 - 172x + 820, \qquad (e_2)$$
$$y^2 = x^3 - 172x + 505, \qquad (e_3)$$
$$y^2 = x^3 - 112x + 2320, \qquad (e_4)$$

El a demonstrat că (e_1), (e_2), (e_3) și (e_4) au câte cel puțin $24, 60, 58$ și respectiv 70 puncte de coordonate întregi. Metoda sa pleacă de la găsirea prin verificare directă a unor soluții și apoi adunarea repetată a acestora în grupul curbelor. Procedeul este apoi repetat, incluzând în operațiile de adunare și punctele noi obținute. Mai târziu,

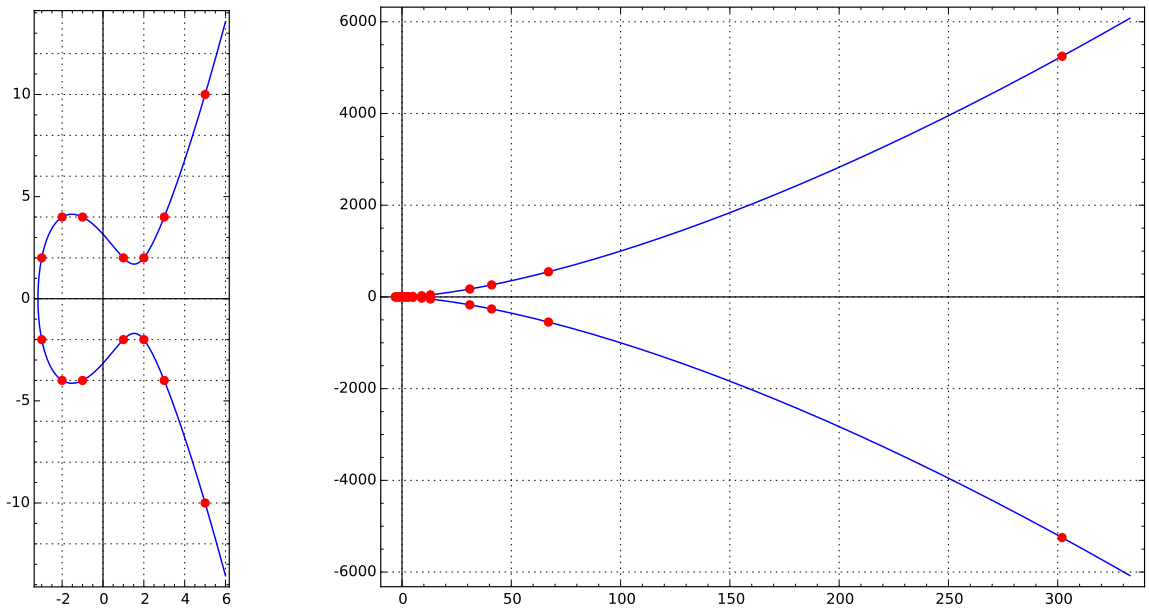


Figura 3.8: Curba eliptică $y^2 = x^3 - 7x + 10$ definită peste corpul numerelor raționale are discriminantul -21248. Pe ea se găsesc exact 26 puncte de coordonate întregi dispuse simetric față de axa Ox. Cele 13 puncte de coordonate întregi care au ordonata pozitivă sunt: $(-3, 2)$,$(-2, 4)$,$(-1, 4)$,$(1, 2)$,$(2, 2)$,$(3, 4)$,$(5, 10)$,$(9, 26)$,$(13, 46)$, $(31, 172)$,$(41, 262)$,$(67, 548)$,$(302, 5248)$. În imaginea din partea dreaptă, raportul dintre scara orizontală și cea verticală este ales să fie subunitar pentru a putea reprezenta toate aceste puncte.

Tabelul 1: Cele 13 puncte de coordonate întregi ale curbei eliptice $y^2 = x^3 - 7x + 10$ definită peste $\mathbb{Q}$. Pe lângă acestea, mai sunt opusele lor: $\bar{M}_3 = (-3, -2)$, $\bar{M}_2 = (-2, 4)$,..., $\bar{P}_{10} = (302, -5248)$.

M_3	M_2	M_1	P_1	P_2	P_3	P_4
$(-3, 2)$	$(-2, 4)$	$(-1, 4)$	$(1, 2)$	$(2, 2)$	$(3, 4)$	$(5, 10)$

P_5	P_6	P_7	P_8	P_9	P_{10}
$(9, 26)$	$(13, 46)$	$(31, 172)$	$(41, 262)$	$(67, 548)$	$(302, 5248)$

Bremner și Tzanakis [BT'83] au demonstrat că ecuația (e_1) are exact 26 de puncte de coordonate întregi.

Aceste puncte sunt listate în Tabelul 1 și prezentate în formă grafică în imaginile din Figura 3.8.

Tehnica cea mai des întâlnită pentru găsirea unor puncte de coordonate întregi este cea de realizare a unor combinații liniare între puncte cu aceeași proprietate, care sunt deja cunoscute. (Să remarcăm faptul că nu întotdeauna suma a două puncte de coordonate întregi are coordonate întregi, dar ne așteptăm ca aceasta să se întâmple mai des decât în cazul în care am lucra cu fracții, deoarece în acele cazuri ar trebui sa fie îndeplinite un număr mai mare de condiții pentru ca simplificările să reducă

Tabelul 2: Extras din tabla adunării punctelor de coordonate întregi ale curbei eliptice $y^2 = x^3 - 7x + 10$ definită peste $\mathbb{Q}$. Rezultatul "$*$" reprezintă sumele care nu aparțin lui $\mathbb{Z} \times \mathbb{Z}$.

$+$	M_3	M_2	M_1	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}
M_3	$\bar{P}_7$	$\bar{P}_5$	$\bar{P}_4$	$\bar{P}_2$	$\bar{P}_1$	$*$	$\bar{M}_1$	$\bar{M}_2$	$*$	$\bar{M}_3$	$*$	$*$	$*$
M_2	$\bar{P}_5$	$*$	$\bar{P}_3$	$*$	$*$	$\bar{M}_1$	$*$	$\bar{M}_3$	$*$	$*$	M_3	$*$	$*$
M_1	$\bar{P}_4$	$\bar{P}_3$	$*$	$\bar{P}_1$	$*$	$\bar{M}_2$	$\bar{M}_3$	$*$	M_3	$*$	$*$	M_2	$*$
P_1	$\bar{P}_2$	$*$	$\bar{P}_1$	$\bar{M}_1$	$\bar{M}_3$	M_3	M_2	M_1	$*$	$*$	$*$	$*$	$*$
P_2	$\bar{P}_1$	$*$	$*$	$\bar{M}_3$	$*$	M_1	$*$	$*$	P_1	$*$	$*$	$*$	$*$
P_3	$*$	$\bar{M}_1$	$\bar{M}_2$	M_3	M_1	$*$	P_1	$*$	$*$	P_2	$*$	$*$	$*$
P_4	$\bar{M}_1$	$*$	$\bar{M}_3$	M_2	$*$	P_1	$*$	P_2	$*$	$*$	P_3	$*$	$*$
P_5	$\bar{M}_2$	$\bar{M}_3$	$*$	M_1	$*$	$*$	P_2	$*$	P_3	$*$	$*$	P_4	$*$
P_6	$*$	$*$	M_3	$*$	P_1	$*$	$*$	P_3	$*$	P_4	$*$	$*$	P_5
P_7	$\bar{M}_3$	$*$	$*$	$*$	$*$	P_2	$*$	$*$	P_4	$*$	P_5	$*$	$*$
P_8	$*$	M_3	$*$	$*$	$*$	$*$	P_3	$*$	$*$	P_5	$*$	P_6	$*$
P_9	$*$	$*$	M_2	$*$	$*$	$*$	$*$	P_4	$*$	$*$	P_6	$*$	P_7
P_{10}	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	P_5	$*$	$*$	P_7	$*$

complet toți numitorii rezultatelor finale.) Să verificăm, în continuare, cum se pot obține din aproape în aproape cele 26 de puncte de coordonate întregi ale curbei (e_1) pornind doar de la P_1 și P_2. Să remarcăm faptul că în momentul în care aflăm un punct de coordonate întregi $P = (a, b)$, l-am aflat și pe opusul său $\bar{P} = (a, -b)$, care, de asemenea, și el are coordonatele tot întregi.

Faptul că $P_1(1, 2), P_2(2, 2) \in E(-7, 10; \mathbb{Q})$ e ușor de verificat. Apoi, obținem:

$$\begin{aligned} M_3 &= \bar{P}_1 + \bar{P}_2 & M_2 &= 4P_1 + P_2 \\ M_1 &= 2\bar{P}_1 & P_1 &= P_1 \\ P_2 &= P_2 & P_3 &= 2\bar{P}_1 + \bar{P}_2 \\ P_4 &= 3P_1 + P_2 & P_5 &= 3\bar{P}_1 \\ P_6 &= P_1 + \bar{P}_2 & P_7 &= 2P_1 + 2P_2 \\ P_8 &= 5\bar{P}_1 + 2\bar{P}_2 & P_9 &= 6P_1 + P_2 \\ P_{10} &= 4\bar{P}_1 + P_2. \end{aligned}$$

Din aceste relații constatăm că toate punctele de coordonate întregi de pe curba $E(-7, 10; \mathbb{Q})$ sunt combinații liniare de P_1, P_2 cu coeficienți întregi, adică aparțin laticii

$$\mathcal{L} := \{mP_1 + nP_2 \in E(-7, 10; \mathbb{Q}) : m, n \in \mathbb{Z}\}.$$

Acestea sunt însă cazurile fericite, deoarece punctele din $\mathcal{L}$ au coordonate raționale al căror numărători și numitori sunt foarte mari, chiar și atunci când coeficienții m, n sunt mici. Spre exemplu: $P_{10} = (302, 5248)$, iar

$$2P_{10} = 2(4\bar{P}_1 + P_2) = -8P_1 + 2P_2 = \left(\frac{8319422361}{110166016}, \frac{758364692181827}{1156302503936}\right).$$

În general se poate observa că numitorii și numărătorii coordonatelor multiplilor unui

punct cresc extrem de repede. De exemplu primii 10 multiplii ai lui $P_3 = (3, 4)$ sunt:

$$
\begin{aligned}
P_3 &= (3, 4) \\
2P_3 &= \left(\frac{1}{4}, \frac{23}{8}\right) \\
3P_3 &= \left(\frac{-373}{121}, \frac{-2012}{1331}\right) \\
4P_3 &= \left(\frac{7649}{8464}, \frac{-1635631}{778688}\right) \\
5P_3 &= \left(\frac{11877595}{2601769}, \frac{-35902154780}{4196653397}\right) \\
6P_3 &= \left(\frac{6952604481}{122456356}, \frac{579110076716617}{1355102035496}\right) \\
7P_3 &= \left(\frac{36681371788147}{16667630925201}, \frac{155970574432300561852}{68047286682856527801}\right) \\
8P_3 &= \left(\frac{-57460606348173951}{90574576534858816}, \frac{10266715726529942217923475 1}{27258971675380929453412864}\right) \\
9P_3 &= \left(\frac{-15352751249805244187117}{6501363482485826934001}, \frac{-191617050069573888160185355635859 6}{52421165349480827006523762609899 9}\right) \\
10P_3 &= \left(\frac{11739276579402254068145207 69}{83839711124706782119620490 0}, \frac{-41651117362798067806164416865307974822647}{24275861992635817390490143289660101343000}\right),
\end{aligned}
$$

iar primii 4 multiplii ai lui $P_{10} = (302, 5248)$ sunt:

$$
\begin{aligned}
P_{10} &= (302, 5248) \\
2P_{10} &= \left(\frac{8319422361}{110166016}, \frac{758364692181827}{1156302503936}\right) \\
3P_{10} &= \left(\frac{20914488463760924189518}{15532771693159987631759885909111}, \frac{3015626391486754911805515405629056}{1553277169315998763175988590911 1}\right) \\
4P_{10} &= \Bigg(\frac{48012874930273480241619554313734833202 89}{25343339729283987879151650639148456345 6}, \\
&\qquad \frac{32967428745922959748469756823964879056495659938159042618964 9}{40345561873355502056443129411401170237563098778276242391 04}\Bigg).
\end{aligned}
$$

În concluzie, chiar și un domeniu aparent propice cum este laticea $\mathcal{L}$, care totuși are câteva puncte de coordonate întregi mici, se dovedește a fi puțin convenabil, deoarece are puține puncte cu care s-ar putea identifica "atomii" unui mesaj de criptat în condițiile în care spațiul și timpul necesar operațiunilor de criptare și decriptare este redus.

4 Criptare folosind curbe eliptice

4.1 Introducere

În continuare ne vom referi la trei persoane imaginare, *Alice*, *Bob* și *Eve*.
Alice și *Bob* își trimit mesaje unul altuia, iar *Eve* primește o copie a acestora, de fiecare dată. Căutăm o modalitatea de comunicare care să le permită lui *Alice* și *Bob* să se înțeleagă, iar *Eve* să întâmpine dificultăți cât mai mari în deslușirea mesajelor.

4.2 Problema logaritmului discret

Enunț Fie $E(\mathbb{K}_q) = \{(x, y) \in \mathbb{K}_q^2 \ : \ y = x^3 + Ax + B\} \cup \{\mathcal{O}\}$ o curbă eliptică și două puncte $P, Q \in E(\mathbb{K}_q)$. Vrem să găsim $n \in \mathbb{N}$ cu proprietatea că $nP = Q$.
Problema logaritmului discret este greu de rezolvat și nu se cunoaște un algoritm polinomial care să obțină soluția problemei în cazul general. Cu toate acestea, există anumite *curbe eliptice* pentru care se cunosc rezolvări admisibile .

4.3 Protocolul Diffie-Hellman

Algoritmul pe care îl vom descrie în cele ce urmează îi ajută pe *Alice* și pe *Bob* să stabilească un punct comun P de pe o curbă eliptică, în timp ce *Eve* va trebui să rezolve *problema logaritmului discret* pentru a-l descoperi.

Fie E o *curbă eliptică* peste un corp $\mathbb{K}$ dată de ecuația $y^2 = x^3 + Ax + B$, cu $A, B \in \mathbb{K}$.

Observația 4.1. *Fie $P \in E$ și $d \in \mathbb{N}$, dacă* problema logaritmului discret *este dificilă, atunci Eve va întâmpina dificultăți în aflarea lui d, chiar dacă aceasta cunoaște punctele P și dP.*

Vrem să folosim această observație pentru a interschimba mesaje între *Alice* și *Bob*.

Algoritm

Pasul 1. *Alice* și *Bob* se pun de acord asupra unei *curbe eliptice* E și asupra unui punct $P \in E$ (le presupunem pe cele din notația anterioară).

Pasul 2. *Alice* și *Bob* aleg câte un număr natural $a \in \mathbb{N}$, respectiv $b \in \mathbb{N}$ astfel încât $a \nmid ord(P)$ și $b \nmid ord(P)$.

Pasul 3. *Alice* calculează aP și îi trimite rezultatul lui *Bob*, iar acesta calculează bP și îi trimite rezultatul lui *Alice*.

Pasul 4. După ce mesajele ajung, *Alice* îl primește pe bP și calculează $a(bP)$, iar *Bob* primește aP și calculează $b(aP)$. Dar $a(bP) = abP = baP = b(aP)$.

Așadar și *Alice* și *Bob* au intrat în posesia punctului $Q \coloneqq abP$, fără ca vreunul dintre ei să afle numărul la care s-a gândit celălalt, inițial. Cum am stabilit anterior, *Eve* cunoaște conversația pe care *Alice* și *Bob* au avut-o și prin urmare știe *curba eliptică* E, punctul P și mesajele aP și bP.

Exemplu:

Pasul 1. *Alice* și *Bob* aleg curba eliptică $E : y^2 = x^3 + x + 7206$ peste corpul $\mathbb{F}_{7211}$ și punctul $P = (3, 5) \in E$ cu $ord(P) = 7223 = 31 \times 233$;

Pasul 2. *Alice* alege $a = 32 \nmid 7223$ și *Bob* alege $b = 17 \nmid 7223$.

Pasul 3. *Alice* calculează $aP = 32(3,5) = (4470, 5283)$, iar *Bob* calculează $bP = 17(3,5) = (1352, 6299)$ și interschimbă rezultatele obținute.

Pasul 4. *Alice* calculează $a(bP) = 32(1352, 6299) = (855, 979)$, iar *Bob* calculează $b(aP) = 17(4470, 5283) = (855, 979)$. Punctul comun obținut este $Q = (855, 979)$

Întrebare Poate *Eve* să găsească punctul Q, având informațiile anterior precizate?

4.4 Scufundarea mesajelor într-o curbă eliptică

Pentru ca *Alice* și *Bob* să poată cripta conversația lor cu ajutorul curbelor eliptice, trebuie să găsim o modalitate prin care unui mesaj să îi asociem un punct de pe o curbă, iar după aceea să îl criptăm folosind metode de manipulare ale punctelor. În continuare vom prezenta un algoritm de scufundare a unui mesaj într-o curbă eliptică, propus de matematicianul Neal Koblitz.

Fie E o curbă eliptică peste $\mathbb{F}_q$, $q > 3$ număr prim, dată de ecuația $y^2 = x^3 + Ax + B$, cu $A, B \in \mathbb{F}_p$ (similar se tratează cazul în care $q = p^k$, cu $p > 3$ număr prim și $k \in \mathbb{N}$). Putem presupune că mesajele pe care dorim să le scufundăm sunt numere (spre exemplu reprezentare lor în codul ASCII).

Pasul 1. Fie $m \in \mathbb{N}$, $0 \leq m < q/100$ reprezentarea mesajului dorit. Vrem să îi asociem lui m un punct de pe curba E.

Pasul 2. Calculăm pe rând $x_j = 100m + j$ pentru orice $j \in \{0, 1, \ldots, 99\}$.

Pasul 3. Dacă $s_j := x_j^3 + Ax_j + B$ are proprietatea că $s_j^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, atunci s_j este rest pătratic modulo p. Dacă s_j nu satisface această condiție, ne întoarcem la pasul anterior.

Pasul 4. Calculăm $y_j := s_j^{\frac{1}{2}}$ și asociem mesajului m punctul de (x_j, y_j).

Observația 4.2. *Punctul (x_j, y_j) este pe curba E din felul în care l-am construit. Deoarece s_j este un element din $\mathbb{F}_q$, dat de o funcție cu un grad mare de entropie, probabilitatea ca acesta să fie rest pătratic modulo q este aproximativ $\frac{1}{2}$ și prin urmare probabilitatea ca nici unul dintre s_j calculați să nu respecte condiția din "Pasul 3" este aproximativ 2^{-100} .*

Regăsirea mesajului m se face prin simpla calculare a lui $x_j/100$.

Exemplu: Vom folosi aceeași curbă eliptică pe care am prezentat-o în exemplificarea protocoluluiDiffie-Hellman și anume $E : y^2 = x^3 + x + 7206$ peste corpul $\mathbb{F}_{7211}$. *Alice* poate alege $m \in \mathbb{N}$, $0 \leq m < 7211/100$, așadar are la dispoziție 72 de mesaje (numere) pe care le poate scufunda cu ajutorul metodei lui Koblitz.

Pasul 1. *Alice* alege mesajul $m = 27$.

Pasul 2. Parcurgerea lui x_j începe de la 2701 și până la 2705, *Alice* descoperind că nu există nici un punct din E cu aceste abscise.

Pasul 3. *Alice* îl găsește pe primul x_j, $x_6 = 2706$ cu proprietatea că $s_6 = x_6^3 + x_6 + 7206$ ($s_j = 6130$) și $s_6^{\frac{7211-1}{2}} \equiv 1 \pmod{7211}$.

Pasul 4. *Alice* calculează $y_j = s_j^{\frac{1}{2}}$. Deoarece $7211 \equiv 3 \pmod 4$, o rădăcină a lui s_j este $s_j^{\frac{7212}{4}} = 6636$.

Prin urmare scufundarea lui $m = 27$ în curba E rezultă în punctul $P_m = (2706, 6636)$. Se observă faptul că $x_j/100 = 2706/100 = 27 = m$, prin urmare algoritmul se verifică.

4.5 Criptosistemul Massey-Omura

Sistemul propus se bazează pe dificultatea rezolvării problema logaritmului discret și pe una dintre primele idei ale criptografiei folosind cheie publică. *Alice* pune mesajul pentru *Bob* într-o cutie pe care o sigilează cu un lacăt pentru care doar ea are cheia și îi trimite cutia lui *Bob* . Deoarece *Bob* nu are nici o idee cum ar putea desface lacătul lui *Alice* , sigilează cutia cu un alt lacăt al cărui cheie este deținută doar de el și trimite cutia înapoi. În final *Alice* primește cutia cu cele două lacăte și îl desface pe cel pe care ea la pus inițial și astfel îi trimite cutia lui *Bob* având doar lacătul pe care acesta știe să îl desfacă și deci va putea citi fără probleme mesajul din interior. Algoritmul folosind curbe eliptice este următorul:

Pasul 1. *Alice* și *Bob* se pun de acord asupra unei curbe eliptice E cu $k := ord(E)$ peste un corp $\mathbb{K}$.

Pasul 2. *Alice* scufundă mesajul său m în E (folosind spre exemplu algoritmul prezentat anterior) și obține un punct $M \in E$.

Pasul 3. *Alice* alege un număr natural a, $0 \leq a < k$, $(a, k) = 1$, calculează $M_1 := aM$ și trimite punctul astfel obținut lui *Bob* .

Pasul 4. *Bob* alege $b \in \mathbb{N}$, $0 \leq b < k$, $(b, k) = 1$, calculează $M_2 := bM_1$ și trimite rezultatul lui *Alice* .

Pasul 5. *Alice* calculează a^{-1} în $\mathbb{Z}_k$ și trimite $M_3 = a^{-1}M_2$ lui *Bob* .

Pasul 6. În final *Bob* calculează b^{-1} în $\mathbb{Z}_k$ și găsește mesajul inițial $M = b^{-1}M_3$.

Observația 4.3. *Bob obține la "Pasul 6" mesajul lui Alice deoarece* $b^{-1}M_3 = b^{-1}a^{-1}baM = (ik+1)(jk+1)M$, *unde* $ik+1 = a*a^{-1}$, *iar* $jk+1 = b*b^{-1}$. *Cum* $tkP = \mathcal{O}$ *pentru orice* $P \in E$ *și* $t \in \mathbb{N}$, *deducem că* $(ik+1)(jk+1)M = \mathcal{O}+M = M$, *așadar algoritmul are rezultatul dorit.*

Rămâne să stabilim dificultățile pe care le întâmpină *Eve* în momentul în care dorește să îl afle pe M. Ea are la dispoziție toate informațiile transmise între *Alice* și *Bob* . Prin urmare, cunoaște cine este curba E, punctele $\{M_1, M_2, M_3\}$ și vrea să îl obțină pe M. Observăm că $M_3 = bM$ și deci *Eve* cunoaște aM, bM și abM, iar atunci ne aflăm în ipotezele problemei Diffie-Hellman, echivalentă cu problema logaritmului discret. Așadar *Eve* va trebui să rezolve una dintre aceste probleme dificile pentru a îl găsi pe M.

Exemplu:

Pasul 1. *Alice* și *Bob* aleg curba eliptică $E : y^2 = x^3 + 4x + 144$ peste corpul $\mathbb{F}_{601}$, având $ord(E) = 563 = 3 \times 191$.

Pasul 2. *Alice* alege mesajul ei să fie corespunzător punctului $M = (5, 17) \in E$.

Pasul 3. *Alice* alege $a = 10$, $(10, 563) = 1$ și calculează $M_1 = aM = 10(5, 17) = (569, 253)$ și îi trimite rezultatul lui *Bob* .

Pasul 4. *Bob* alege $b = 100$, $(100, 563) = 1$ și calculează $M_2 = bM_1 = 100(569, 253) = (254, 318)$, iar rezultatul îl înapoiază lui *Alice* .

Pasul 5. *Alice* calculează $a^{-1} = 10^{-1}$ în $\mathbb{Z}_5 63$ și anume $10^{-1} = 169$ și $M_3 = a^{-1}M_2 = 169(254, 318) = (497, 202)$ și trimite din nou rezultatul lui *Bob* .

Pasul 6. *Bob* calculează $b^{-1} = 100^{-1}$ în $\mathbb{Z}_5 63$ și anume $100^{-1} = 411$ și obține $411M_3 = M = (5, 17)$. Prin urmare, algoritmul se verifică, *Alice* și *Bob* reușind să comunice informația dorită.

4.6 Avantaje ale criptării folosind curbe eliptice

Unul dintre cele mai cunoscute criptosisteme asimetrice care nu folosește curbe eliptice este `RSA`, propus de matematicienii Ron Rivest, Adi Shamir, și Leonard Adleman în anul 1977, ale căror inițiale dau și numele criptosistemului. Ulterior s-a aflat că această idee fusese folosită încă din 1973 de către *UK intelligence agency GCHQ* la propunerea lui Clifford Cocks, dar a informația a fost ținută secretă până în anul 1973. Criptosistemul `RSA` își bazează securitatea pe dificultatea factorizării numerelor întregi în produs de factori primi. Pentru această problemă nu se cunoaște un algoritm polinomial care să o rezolve (la fel ca și problema logaritmului discret). Cea mai eficientă metodă pentru abordarea acestei probleme se numește *General Number Field Sieve* (`GNFS`), care, pentru factorizarea unui număr n, având $\lfloor \log_2(n) \rfloor + 1$ biți, are nevoie de un număr de pași de ordinul

$$\exp\left((64/9)^{1/3} + o(1))(\log n)^{1/3}(\log\log n)^{2/3}\right),$$

Tabelul 3: Comparație între dimensiunile cheilor care oferă același nivel de securitate pentru criptosistemul `RSA` și pentru problema logaritmului discret.

Lungime chei `RSA`	Chei folosite pentru criptare cu logaritmul discret
1024 biți	160 biți
2048 biți	224 biți
3072 biți	256 biți
7680 biți	384 biți
15360 biți	512 biți

asimptotic, pentru $n \to \infty$. (Aici am notat $exp(x) = e^x$, iar $\log x$ este logaritmul natural.) Pentru descompunerea în factori a unor numere mari există o competiție numită *RSA-factoring-challenge* (vezi `RSA Laboratories` la adresa http://www.emc.com/emc-plus/rsa-labs/historical/a-cost-based-security-analysis-key-lengths.htm). Aceasta propune o listă de numere mari care sunt considerate a fi greu de descompus în factori primi. Cel mai mare număr de pe această listă care a fost factorizat este

$$\begin{aligned}\texttt{RSA-769} =& 12301866845301177551304949583849627207728535695953347921973\\ & 24521517264005072636575187452021997864693899564749427740638\\ & 45925192557326303453731548268507917026122142913461670429214\\ & 31602221240479274737794080665351419597459856902143413.\end{aligned}$$

Numărul `RSA-768` are 768 de biți, iar reprezentarea sa zecimală are 232 cifre. Descompunerea lui `RSA-768` a fost încheiată la data de 12 Decembrie 2009 după peste doi ani de calcule efectuate în paralel pe serverele mai multor universități [KAFa'10]. Descompunerea obținută este $\texttt{RSA-768} = p \cdot q$, unde:

$$\begin{aligned}p =& 33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489\\ q =& 36746043666799590428244633799627952632279158164343087642676032283815739666511279233373417143396810270092798736308917.\end{aligned}$$

De asemenea, autorii [KAFa'10] estimează că. pentru un calculator obișnuit, aceeași operațiune ar fi durat aproximativ 2000 de ani.

Următorul număr din `RSA`-challenge-list are 1024 de biți, iar dificultatea pentru factorizarea sa cu același algoritm este de 1000 de ori mai mare decât a fost pentru `RSA-768`. Așadar, deocamdată, pentru folosirea criptosistemului `RSA` este recomandată o cheie de aproximativ 1000 de biți.

Comparativ, pentru problema logaritmului discret pe curbe eliptice, cel mai bun rezultat a fost obținut în Iulie 2009 când, după trei luni de rulare continuă a fost rezolvată pentru un corp finit $\mathbb{F}_p$, unde p este un prim de 112 biți [BCC'09]. Pentru calcul a fost folosit cel mai eficient algoritm de rezolvare a problemei logaritmului discret peste curbe eliptice cunoscut, și anume *Pollard's rho algorithm.* Conform *National Institute of Standards and Technology* (NIST) siguranța este de același nivel pentru chei de lungime sunt în Tabelul 3.

4.7 Conjectura Sato-Tate

Pentru curba eliptică E peste $\mathbb{F}_p$, notăm cu $a_p(E) := p + 1 - |E|$ termenul eroare din Teorema lui Hasse. Să observăm că a_p depinde de doi parametrii: numărul prim p și curba eliptică E. O problemă naturală care se pune este studierea mai aprofundată a lui $a_p(E)$. Întrebarea care se pune este dacă nu cumva $a_p(E)$ poate fi mărginit de o funcție cu ordinul de mărime mai mic decât $\sqrt{p}$ și aceasta fie în cazul general sau în cazuri particulare, variind doar unul dintre cei doi parametri.

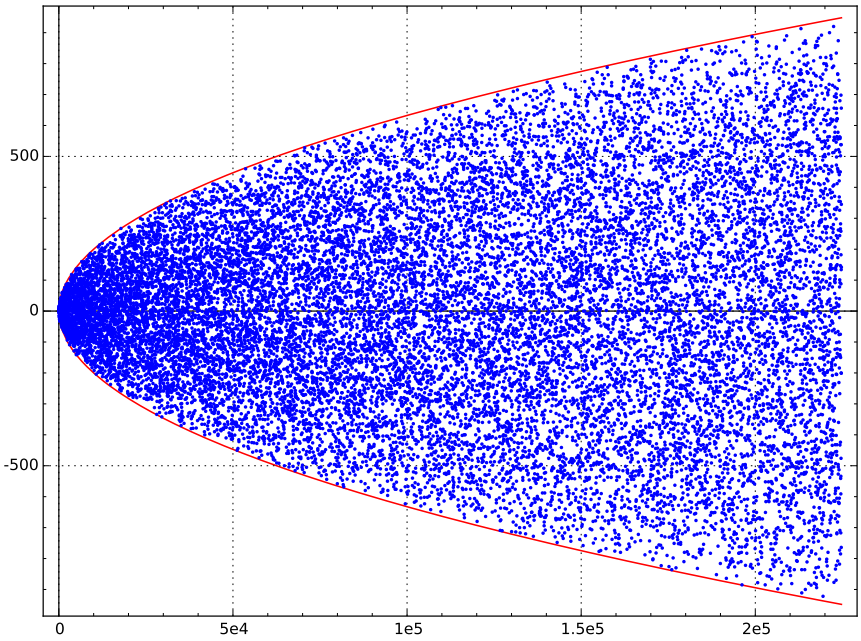


Figura 4.9: Distribuția termenilor eroare $a_p(E) = p+1-|E|$ din Teorema lui Hasse. În imagine, curba eliptică este menținută fixată, $E : y^2 = x^3 - 7x + 10$. Punctele albastre corespund perechilor $(p, a_p(E))$ pentru cele 78497 numere prime p pentru care $5 \leq p \leq 1000033$, iar cu roșu sunt desenate graficele funcțiilor $x \mapsto \pm 2\sqrt{x}$.

Diversele observații, raționamente euristice și calule arată că rezultatul general valabil pentru toate numerele prime și toate curbele posibile nu poate fi îmbunătățit. Mai mult, există observații și argumente care arată valabilitatea acestui lucru chiar și atunci când se fixează unul dintre parametri (curba E sau numărul prim p) iar celălalt parametru este lăsat liber. Acesta este un atu al unui sistem criptografic bazat pe curbe eliptice, deoarece sunt disponibile o varietate suficient de mare de grupuri în care se poate face criptarea, grupuri al căror cardinal poate fi suficient de departe de departe de numărul prim p. Imaginile prezentate în Figurile 4.9 și 4.10 confirmă această varietate.

Deoarece, din Teorema lui Hasse știm că

$$-1 \leq \frac{a_p(E)}{2\sqrt{p}} \leq 1\,,$$

iar restricția funcției $\theta \mapsto \cos\theta$ la intervalul $[0, \pi]$ este bijectivă, rezultă că pentru

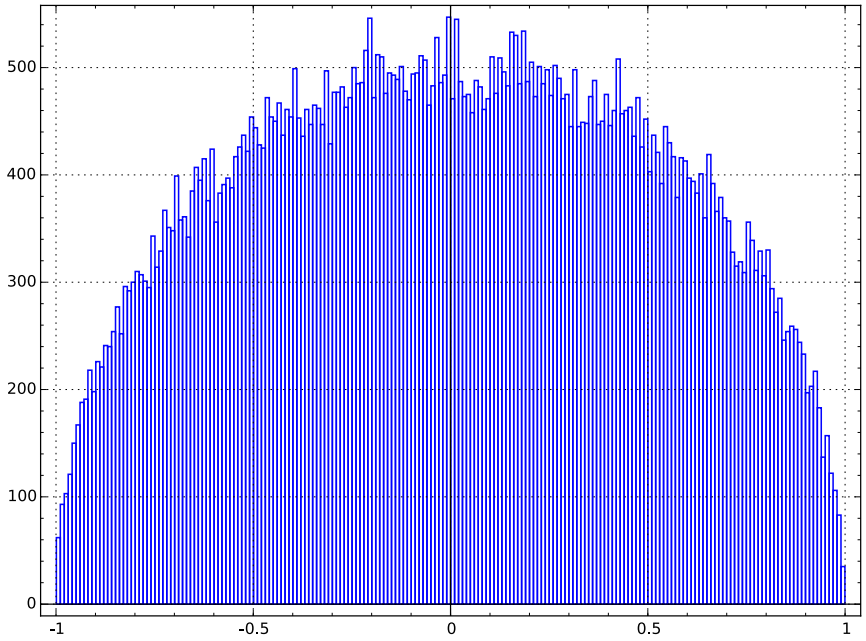


Figura 4.10: Histograma frecvenței rapoartelor $\frac{a_p(E)}{2\sqrt{p}}$ în 200 de intervale egale de lungime 0.01, unde curba $E : y^2 = x^3 - 7x + 10$ este fixată, iar $p \in [5, 1000033]$.

orice p și orice E, curbă eliptică peste $\mathbb{F}_p$, ecuația

$$\cos\theta = \frac{a_p(E)}{2\sqrt{p}} \tag{23}$$

are o unică soluție în intervalul $[0, \pi]$. Notăm cu $\theta_p(E) := \arccos a_p(E)/(2\sqrt{p})$ soluția ecuației (23).

Independent unul de altul, la începutul anilor 1960, Mikio Sato și John Tate au fosrmulat următoarea conjectură cu privire la distribuția unghiurilor $\theta_p(E)$.

Conjectura (Sato-Tate, 21.1. [Sil'95])**.** *Fie E o curbă eliptică peste corpul numerelor raționale și fie unghiurile $\theta_p \in [0, \pi]$ definite ca soluții ale ecuației* (23) *pentru curbele corespunzătoare lui E definite peste $\mathbb{F}_p$. Atunci, mulțimea $\{\theta_p\}$ este echidistribuită față de o probabilitatea cu densitatea $\frac{2}{\pi}\sin^2\theta$. Mai precis, pentru orice $\alpha, \beta \in [0, \pi]$, $\alpha \leq \beta$, avem:*

$$\lim_{X\to\infty} \frac{|\{p \leq X : \alpha \leq \theta_p(E) \leq \beta\}|}{|\{p : p \leq X\}|} = \frac{2}{\pi}\int_\alpha^\beta \sin^2\theta\, d\theta.$$

Recent, Richard Taylor și colaboratorii săi au publicat o serie de lucrări în care demonstrează Conjectura Sato-Tate în ipoteze suplimentare sau într-un cadru mai general decât cel din enunțul prezentat mai sus.

Fixând un număr prim suficient de mare, analogul conjecturii lui Sato-Tate a fost demonstrat de Birch [Bir'68] (vezi și tratatul lui Silverman [Sil'95, Theorem 21.4]).

Teorema 4.1 (Birch(1968)). *Fie $p \geq 5$ un număr prim și fie $\mathbf{E}_p$ mulțimea claselor de curbe eliptice izomorfe, definite peste $\mathbb{F}_p$. Pentru orice $E \in \mathbf{E}_p$, fie $a_p(E) = p+1-|E|$ și $\cos\theta_p(E) = \frac{a_p(E)}{2\sqrt{p}}$. Atunci, pentru orice $\alpha, \beta \in [0,\pi]$, $\alpha \leq \beta$, avem:*

$$\lim_{p\to\infty} \frac{|\{E \in \mathbf{E}_p : \alpha \leq \theta_p(E) \leq \beta\}|}{|\mathbf{E}_p|} = \frac{2}{\pi}\int_\alpha^\beta \sin^2\theta\, d\theta.$$

PARTEA a II-a
Alte sisteme de criptare

4.8 Criptarea imaginilor

Necesitatea transmiterii la distanță a imaginilor într-un sistem securizat, care să asigure acuratețea și să permită accesul la informație doar a celor care dețin cheia, a devenit o problemă mult studiată odată cu dezvoltarea transmisiilor TV digitale, a comunicațiilor prin internet sau a teleconferințelor, În ultimii ani au fost studiate și propuse diverse noi metode pentru criptarea imaginilor. Să remarcăm că, în format digital, orice imagine este o matrice de numere și, prin urmare, problema criptării imaginilor coincide cu cea a criptării oricărui mesaj.

În fapt, obiectivul tehnicilor de criptare a imaginilor este de a înlocui o imagine cu o alta care este de greu înțeles. Toate metodele de criptare folosesc în diverse feluri funcții bazate pe substituții sau transpoziții ori combinații ale acestora, care, înglobate într-un algoritm, transformă imaginea într-una criptată. Cheia este incorporată în funcția de criptare și aceeași cheie este utilizată și la decriptare, sistemul fiind simetric. Pentru scăderea semnificativă a timpului necesar efectuării operațiunilor necesare se construiesc și procesoare dedicate, precum cele folosite în sistemele Data Encryption Standard `DES` și Advanced Encryption Standard `AES`.

Prezentăm în continuare succint câteva metode de criptare a imaginilor propuse în ultimii ani.

- Algoritmi inspirați din limbajul folosit în genetică: informația care, mai întâi, este transformată în binar și perechile de biți 00, 01, 10, 11 sunt înlocuite cu A, C, G, T, se descompune în blocuri în care elementele se combină urmând un algoritm ce combină încrucișarea (cross-over) și mutația. Un exemplu de aplicare al acestei proceduri este analizat în lucrarea [Hus'06].
- Scheme de criptare bazate pe introducerea de zgomot-haos, prin *difuzie* (modificarea pixelilor imaginii se face folosind șiruri cu un nivel ridicat de iregularitate) și *confuzie* (ordinea pixelilor este schimbată). Parametrii de control ai operațiunii formează cheia simetrică [CMC'04], [ARa'08], [Dia'16], [FHa'16].
- Transformarea șirurilor de pixeli conform cu evoluția unor celulare automate e folosită în algoritmii propuși de Ye et al. [YL'08] și X. Wang și Luan [WL'13].
- O serie de autori folosesc o serie de scheme bazate pe combinarea permutărilor folosite în jocuri matematice, de exemplu Wu et al. [WZa'14] folosesc pătratele latine, Y. Y. Wang et alea [WWS'12] și Diaconu, Loukhaoukha [Dia'15], sudoku, respectiv KenKen, iar Zhang et al. [ZTX'11], Diaconu [Dia'13], cubul Rubick.

În afară de aceste metode, există o mare varietate de posibilități de alegere a unor scheme de permutare care ar putea fi folosite la criptare, puțin testate fiind jocurile combinatoriale [BCG'04].

Metode de criptare a imaginilor bazate pe o problemă care a stârnit un larg interes de-a lungul timpului sunt analizate de Delei et al. [DSW'08] și Diaconu et al. [Dia'14]. În esență, se face permutarea pixelilor dintr-un bloc dreptunghiular în lungul unui drum ce corespunde unui tur al calului de șah care parcurge o singură dată toate pătratele unei table cu dimensiunile egale cu ale blocului de pixeli. Cheia criptării este dată de succesiunea pătratelor, iar diferența dintre operațiunile de criptare și decriptare constă doar în parcurgerea drumului în sensuri opuse.

4.9 Drumul calului pe tabla de șah

Un drum complet al calului pe tabla pe o tablă dreptunghiulară formată din $m \times n$ pătrate este o înșiruire fără repetiții a tuturor pătratelor tablei astfel încât orice două pătrate consecutive se pot obține unul din altul prin săritura calului (două pătrate într-o direcție și unul într-o direcție perpendiculară pe aceasta). Vom nota un astfel de drum prin KT, de la Knight's-Tour (en.) sau Keima-Tour (în "*jocul împrejmuirii*", în varianta goului pe tabla 19×19, *keima* (jp.) este mutarea analoagă săriturii calului). Întotdeauna există astfel de KT-uri dacă tabla nu are una din dimensiuni foarte mici. Un exemplu de problemă construită în lungul unui astfel de drum este criptograma din Tabelul 4.

Tabelul 4: Criptograma unei celebre reflecții despre vreme. Realizarea ei s-a făcut după modelul unei probleme din 1870. (*Cheia folosită pentru criptare se găsește în tabelul Tabelul 5, iar soluția problemei în Tabelul 6.*)

cum	îns	n-a	ce	di	pă	bă	schim
tru	ne	a	în	cli	bă	rii	ei
din	nici	re	ei	mas	lim	te	naș
cea	tea	ce	se	gân	pa	rii	se
pre	pen	pen	ri	cli	pă	fe	ne
moar	toa	ca	tru	cli	te	o	ci
vechi	și	no	te-s	toa	te	ți	uă
ci	și	o	cu	noaș	ne	te	poa

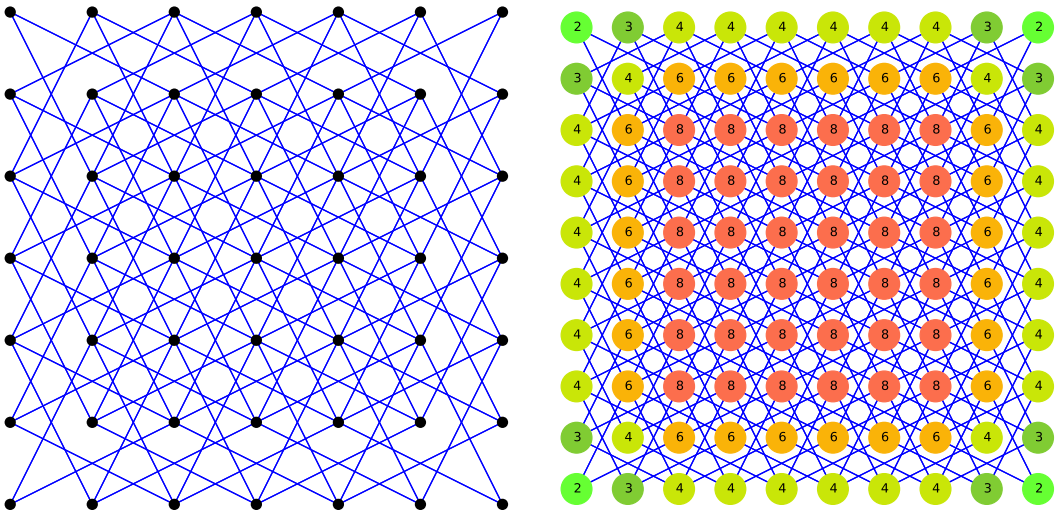
KT este o problemă clasică, fiind investigată de Euler în 1759, dar sub diferite forme apare și mai înainte, de exemplu, pe o tablă 4×4 apare la începutul secolului al IX-lea, în Kavyalankara, o lucrare despre poezie a poetului Rudrata, din Kashmir.

Formal, problema revine la parcurgerea unui unui drum hamiltonian într-un graf cu o formă particulară (două exemple sunt prezentate în Figura 4.11). Timpul necesar găsirii unui astfel de drum în cazul particular al acestui graf pe o tabla de dimensiune $n \times n$ este de ordinul $O(n)$ [CHa'94]. Pentru criptare, însă este nevoie de o bază largă de astfel de drumuri, condiție îndeplinită chiar și pentru table relativ mici [HK'05].

Există mai mulți algoritmi pentru găsirea unui singur drum sau pentru numărarea tuturor drumurilor. Forța brută sau back-tracking pot fi folosite doar pentru table mici, succesul lor fiind redus pe table de dimensiuni mai mari de 8×8. Algoritmii pentru generarea KT-urilor se bazează pe construirea unor drumuri de o formă particulară pe table mici și lipirea acestora într-un drum pe reuniuni de table care

formează un bloc dreptunghiular mai mare. Un exemplu este algoritmul lui Lin și Wei [LW'05] care construiește un drum pe tabla $m \times n$ în $O(mn)$ pași.

Ideea descoperită de H. C. von Warnsdorf în 1823 poate scurta semnificativ căutarea unui KT. Astfel, folosind-o pe tabla 8×8, se poate găsi ușor o soluție, indiferent de locul de plecare, deși numărul estimat al mutărilor posibile în arborele asociat grafului este în jur de 4×10^{51}. Folosirea ideii lui Warnsdorf este de folos în special în apropierea colțurilor și a marginilor tablei și spune că atunci când calul poate sări în mai multe locuri, e de preferat să se aleagă un pătrat din care se va putea continua drumul în cât mai puține feluri. Într-adevăr această regulă impusă alegerii corespunde bunului simț, fiindcă de-a lungul drumului, e de preferat să eliminăm cât mai repede pătratele problematice, păstrând-le pentru viitor pe cele care ne oferă mai multe posibilități de alegere neatinse. În cazul în care minimul numărului de continuări se atinge în mai multe pătrate, atunci se alege unul dintre acestea, conform unei strategii (alegerea pătratului se face aleatoriu, se face sortare și alegere în funcție de anumite criterii, etc.).



]

Figura 4.11: Graful corespunzător săriturii calului (mutarea keima) pe tabla 7×7 (stânga) și pe tabla 10×10 (dreapta). În imaginea din partea dreaptă, fiecare nod este etichetat cu ordinul acestuia (numărul de arce de care este acesta legat).

Cull și De Curtis [CD'78, Theorem 2] au demonstrat existența drumurilor KT pe orice tablă dreptunghiulară de de dimensiuni $m \times n$ cu $\min(m, n) \geq 5$. Rezultatul construit prin inducție a fost demonstrat în diferite alte moduri de autorii unor algoritmi care generează KT-uri (a se vedea lucrările Parberry [Par'97], Lin și Wei [LW'05] precum și articolele pe care aceștia le citează).

Există și drumuri pe unele table cu dimensiuni mai mici, pentru unele dintre acestea numărul drumurilor fiind calculat cu exactitate (vezi [HK'05] și [OEIS, A165134]). Astfel, dacă $\texttt{KT}(n)$ este numărul drumurilor calului care trece exact o dată prin fiecare pătrat al tablei pătrate $n \times n$, atunci $\texttt{KT}(1) = 1$, $\texttt{KT}(2) = \texttt{KT}(3) = \texttt{KT}(4) = 0$, $\texttt{KT}(5) = 1728$, $\texttt{KT}(6) = 6637920$, $\texttt{KT}(7) = 165575218320$, $\texttt{KT}(8) = 19591828170979904$.

Observăm creșterea exponențială a lui $\texttt{KT}(n)$, $\texttt{KT}(8)$ are deja 17 cifre, și este cea mai mare dintre valorile exacte, precis calculate până în prezent.

Există cazuri particulare de drumuri cu proprietăți interesante din punct de vedere teoretic: circuite (un KT pentru care punctul de plecare și de sosire coincid) sau drumuri care produce pătrate magice. în urma unei lung proces de verificare, folosind un software scris de J. C. Meyrignac, în 2003 s-a constat că nu există KT-uri care să genereze pătrate perfect magice pe tabla 8×8.

4.10 Criptarea folosind KT-uri

Pentru criptare, sunt mai multe variante posibile. În forma elementară informația de criptat este aranjată într-o matrice $A = (a_{i,j})$ de dimensiune $m \times n$. Apoi se alege un circuit KT pe tabla de dimensiune $m \times n$:

$$\texttt{KT}: \quad t_{i_1,j_1} \to t_{i_2,j_2} \to \cdots \to t_{i_m,j_n}\,,$$

care, în fapt, furnizează o permutare a mulțimii de indici a matricii. Circuitul KT este cheia de criptare. Matricea criptată $C = C(A, \texttt{KT}) = (c_{i,j})$ se obține făcând substituțiile corespunzătoare circuitului KT, adică:

$$c_{i_2,j_2} := a_{i_1,j_1},\ c_{i_3,j_3} := a_{i_2,j_2}, \ldots, c_{i_m,j_n} := a_{i_{m-1},j_{n-1}},\ c_{i_1,j_1} := a_{i_m,j_n}. \tag{24}$$

4.11 Procedura de criptare, variante, generalizări

Folosind un canal de comunicare secretizat, cei doi comunicatori se pun de acord asupra procedurii de criptare/decriptare.

Se alege un circuit KT pe o tablă de dimensiune $m \times n$. Aceasta este cheia privată, care e comună celor care comunică.

Informația de criptat se aranjează într-o matrice. După caz, se aplică peste aceasta un filtru de zgomot, care este cunoscut atât de A cât și de Z, pentru a ascunde particularitățile geometrice ale distribuției datelor de criptat. Matricea se descompune în blocuri dreptunghiulare de dimensiuni $m \times n$.

Fiecare bloc B se înlocuiește cu blocul CB obținut prin substituțiile corespunzătoare circuitului KT.

Informația astfel criptată se transmite destinatarului pe un canal care poate fi nesecretizat. Acesta o decriptează urmând în sens invers pașii de la criptare și efectuând operațiunile opuse la fiecare moment.

(P1) Să observăm că pentru a obține matricea C nu este neapărat necesar să avem la dispoziție un circuit KT complet, deoarece un circuit aproape complet este suficient fiind simplu de completat cu substituții particulare definite pentru arcele care îi lipsesc. Ba chiar mai mult, folosirea unor astfel de circuite incomplete furnizează o bază de alegere a cheilor mult mai mare.

(P2) Procedura de descompunere/criptare se poate aplica repetat, pe blocuri de dimensiuni diferite, folosind aceeași cheie sau, chiar într-o variantă mai complexă, cu mai multe chei diferite pentru blocuri diferite.

(P3) Substituția (24) poate fi înlocuită cu una de tipul $c_{i,j} := a_{i+d,j+d}$ (corespunzătoare la $d \geq 1$ sărituri ale calului la fiecare pas). Mai general, drumul KT (care în fapt corespunde unei permutări a unei mulțimi cu mn elemente) se poate compune cu o altă permutare fixată, pentru a ascunde apropierea geometrică dintre elementele care se substituie.

(P4) Regula săriturii calului, notată pe scurt $2 \perp 1$, poate fi înlocuită cu alte reguli mai generale, de tipul $e \perp f$, cu $e, f \geq 1$ (se sar e pași într-o direcție urmați de f pași într-o direcție perpendiculară pe aceasta). De exemplu, folosind termeni din go: $1 \perp 2$ (*keima*, e săritura calului și în shogi), șahul chinezesc), $1 \perp 3$ (*ogeima*), $1 \perp 4$ (*oogeima*), $2 \perp 3$. De remarcat faptul că nu toate mutările de acest fel sunt folositoare. De exemplu, mutările pe diagonală $1 \perp 1$ (*kosumi*) sau $2 \perp 2$ (*hazama tobi*), pasul elefantului în xiangqi, păstrează culoarea pătratelor tablei și nu oferă varietatea necesară unei criptări eficiente.

(P5) Pentru siguranță suplimentară, informația esențială care trebuie transmisă, poate fi ascunsă de exemplu într-o imagine, care la rândul ei se poate insera/ascunde într-o succesiune de imagini/film.

În același context este interesantă o problema înrudită, anume cea a găsirii claselor de tururi parțiale (incomplete), dar a căror reuniune disjunctă să acopere întreaga tablă.

Definiția 4.1. *Fie o tablă de șah de dimensiune $m \times n$ fixată și fie $c \geq 1$ un număr natural.*

1. *Numim* călătorie *a calului pe această tablă un șir de pătrate care nu se autointersectează și în care termenii consecutivi se obțin unul din altul prin săritura calului.*
2. *O călătorie se numește* netrivială *dacă conține cel puțin două pătrate.*
3. *Numim* c-Keima-Tour-pe-Bucăți *o mulțime compusă din exact c călătorii disjuncte a căror reuniune acoperă întreaga tablă.*
4. *Notăm cu* c-KTB *o astfel de descompunere a tablei în călătorii disjuncte.*
5. *Un c-Keima-Tour-pe-Bucăți se numește* netrivial *dacă toate călătoriile din care este format sunt netriviale.*

Să observăm că dacă $c = 1$, 1-KTB-urile coincid cu drumurile complete formate dintr-o singură bucată, iar acestea sunt exact KT-urile. Presupunem în continuare că tabla este pătrată, de dimensiune $n \times n$ și, pentru orice $c \geq 1$ fixat, notăm cu c-KTB(n) numărul c-KTB-urilor care pot acoperi această tablă.

Problemă. *1. Să se calculeze numerele c-KTB(n), unde $c, n \geq 1$ și să se compare cu valorile cunoscute ale KTB(n).*

2. Fie $C(n)$ valoarea maximă a numerelor naturale $c \geq 1$ pentru care există c-KTB format doar din călătorii netriviale, adică,

$$C(n) := \max\{c : \text{ există } c\text{-KTB netrivial pe tabla } n \times n \}.$$

Să se estimeze $C(n)$.

Tabelul 5: Drumul folosit pentru obținerea criptogramei din Tabelul 4.

30	11	64	35	28	13	52	47
61	36	29	12	63	48	27	14
10	31	62	57	34	53	46	51
37	60	33	54	49	58	15	26
32	9	38	59	56	25	50	45
39	6	55	24	1	44	19	16
8	23	4	41	18	21	2	43
5	40	7	22	3	42	17	20

Tabelul 6: Soluția criptogramei din Tabelul 4 este strofa a treia din *Glossa* lui Mihai Eminescu.

nici	în	cli	ne	a	ei	lim	bă
re	cea	cum	pă	n-a	gân	di	rii
îns	pre	cli	pa	ce	se	schim	bă
pen	tru	mas	ca	fe	ri	ci	rii
ce	din	moar	tea	ei	se	naș	te
și	o	cli	pă	ți	ne	poa	te
pen	tru	ci	ne	o	cu	noaș	te
toa	te-s	vechi	și	no	uă	toa	te

Notă de final: Calculele și figurile din aceasta lucrare au fost realizate folosind `FOSMSS` (Free Open-Source Mathematical Software System – sistemul de programe matematice cu sursă liberă și deschisă) `SageMath`[SAGE], versiunile 6.8-7.2.

Bibliografie

[Ang'90] W. S. Anglin, *The Square Pyramid Puzzle*, American Mathematical Monthly **97**, no. 2 (1990), 120–124. 6

[Ang'95] W. S. Anglin, *The Queen of Mathematics –An introduction to Number Theory*, Springer-Science+Business Media, B.V. Dordrecht, Netherlands: Kluwer, 1995, X+389 pp. 6

[ARa'08] D. Arroyo, R. Rhouma, G. Alvarez, S. Li, V. Fernandez, *On the security of a new image encryption scheme based on chaotic map lattices*, Chaos, **18** (2008), no. 3, Article ID 033112. 38

[BCC'09] J. W. Bos, M. E. Kaihara, T. Kleinjung, A. K. Lenstra and P. L. Montgomery, *PlayStation 3 computing breaks* 2^{60} *barrier 112-bit prime ECDLP solved*, EPFL IC LACAL,CH-1015 Lausanne (2009). 4, 34

[BCG'04] R. Berlekamp, John H. Conway, Richard K. Guy, *Winning Ways for your Mathematical Plays*, 2nd edition, Wellesley, Massachusetts: A. K. Peters Ltd., 4 vols., 2001-2004. 38

[Ben'02] M. A. Bennett, *Lucas' square pyramid problem revisited*, Acta Arith. **105**, (2002) no. 4, 341–347. 6

[Bir'68] B. J. Birch. *How the number of points of an elliptic curve over a fixed prime field varies*, J. London Math. Soc., **43** (1968), 57–60. 36

[BM'14] M. W. Barsagade, S. Meshram, *Overview of history of elliptic curves and its use in cryptography*, International Journal of Scientific & Engineering Research **5**, Issue 4 (2014), 467–471. 6

[Bom'66] E. Bombieri, *On exponential sums in finite fields*, Amer. J. Math. **88** (1966), 71–105. 16

[BT'83] A. Bremner, N. Tzanakis, *Integer Points on* $y^2 = x^3 - 7x + 10$, Math. of Comp. **41**, no. 164 (1983), 731–741. 27

[CMC'04] G. Chen, Y. Mao, C. K. Chui, *A symmetric image encryption scheme based on 3D chaotic cat maps*, Chaos, Solitons and Fractals, **21** (2004), no. 3, 749–761. 38

[CZ'01] C. Cobeli, A. Zaharescu, *Generalization of a problem of Lehmer*, Manuscripta Math. **104** (2001), 301–307. 4, 18

[HB'05] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, F. Vercauteren, *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Mathematics and its Applications **34** 2005, pp. 848.

[CHa'94] A. Conrad, T. Hindrichs, H. Morsy, I. Wegener, Solution of the Knight's Hamiltonian Path Problem on Chessboards, Discrete Applied Mathematics **50** (1994), no. 2, 125–134. 39

[CD'78] P. Cull, J. De Curtins, *Knight's Tour revisited*, Fibonacci Quart. **16** (1978), 276–285. 40

[DSW'08] J. Delei, B. Sen, D. Wenming, *An image encryption algorithm based on Knight's tour and slip encryption filter*, Proceedings of the International Conference on Science and Software Engineering, vol. 1, 2008, Wuhan, China 251–255. 39

[Del'74] P. Deligne, *La conjecture de Weil. I. (French)*, Inst. Hautes Études Sci. Publ. Math. **43** (1974), 273–307. 16

[Del'80] P. Deligne, *La conjecture de Weil. II. (French) [Weil's conjecture. II]*, Inst. Hautes Études Sci. Publ. Math. **52** (1980), 137–252. 16

[Dia'13] A.-V. Diaconu, K. Loukhaoukha, *An improved secure image encryption algorithm based on Rubik's Cube principle and digital chaotic cipher*, Mathematical Problems in Engineering, vol. **2013**, Article ID 848392, pp. 1–10. 38

[Dia'14] A.-V. Diaconu, A. Costea, M.-A. Costea, *Color image scrambling technique based on transposition of pixels between RGB channels using Knight's moving rules and digital chaotic map*, Mathematical Problems in Engineering, vol. **2014**, Article ID 932875, pp. 1–15. 39

[Dia'15] A.-V. Diaconu, *KenKen puzzle-based image encryption algorithm*, Proceedings of the Romanian Academy, Series A **16** (2015), Special Issue: Cryptology, 271–286. 38

[Dia'16] A.-V. Diaconu, *Circular inter-intra pixels bit-level permutation and chaos-based image encryption*, Information Sciences, in press (2016) DOI:10.1016/j.ins.2015.10.27. 38

[DH'76] W. Diffie, M. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory 22 (1976), no. 6, 644–654. 7

[FHa'16] C. Fu, J. B. Huang, N. N. Wang, Q. B. Hou, W. M. Lei, *A symmetric chaos-based image cipher with an improved bit-level permutation strategy*, Entropy, **16** (2014), 2, 770–788. 38

[Has'33] H. Hasse, *Zur Theorie der abstrakten elliptischen Funktionenkörper. I. Die Struktur der Gruppe der Divisorenklassen endlicher Ordnung*, J. Reine Angew. Math. **175** (1936), 55–62. 15

[HK'05] P. Hingston, G. Kendall, *Enumerating knight's tours using an ant colony algorithm*, The 2005 IEEE Congress on Evolutionary Computation, **2** (2006), 1003–1010. 39, 40

[Hus'06] M. Husainy, *Image encryption using Genetic Algorithm*, Information Technology Journal 5 (2006), no. 3, 516–519. 38

[KAFa'10] T. Kleinjung, K. Aoki, J. Franke, A. K. Lenstra, E. Thomé, J. W. Bos, P. Gaudry, A. Kruppa, P. L. Montgomery, D. A. Osvik, H. te Riele, A. Timofeev, P. Zimmermann, *Factorization of a 768-bit RSA modulus*, Springer, Lecture Notes in Computer Science,**6223** (2010), 333–350. 34

[Kob'87] N. Koblitz, *Elliptic curve cryptosystems*, Math. of Comp. **48** (1987) no. 177, 203–209. 5, 7

[KM'07] N. Koblitz, A. Menezes, *Another look at "provable security"*, J. of Cryptology, **20** (2007), 3–37. 4

[KM'10] N. Koblitz, A. Menezes, *The brave new world of bodacious assumptions in cryptography* Neal Koblitz and Alfred Menezes Notices of the AMS, **57** (2010), 357–365. 4

[KS'00] D. R. Kohel, I. E. Shparlinski, *On exponential sums and group generators for elliptic curves over finite fields*, Algorithmic Number Theory, 4th International Symposium, ANTS-IV Leiden, The Netherlands, July 2-7, 2000 Volume **1838** of the series Lecture Notes in Computer Science, 395–404. 5, 16

[LS'06] T. Lange, I. E. Shparlinski, *Distribution of some sequences of points on elliptic curves*, AMS 2006 Spring Central Sectional Meeting Notre Dame, IN, April 8-9, 2006. 16

[LS'07] T. Lange, I. E. Shparlinski, *Distribution of some sequences of points on elliptic curves*, J. of Math. Crypt., **1** (2007), no. 1, 1–11. 16

[LW'05] S. S. Lin, C. L. Wei, *Optimal algorithms for constructing knight's tours on arbitrary $n \times m$ chessboards*, Discrete Appl. Math. **146** (2005) 219–232. 40

[Ma'85] D. G. Ma, *An elementary proof of the solutions to the diophantine equation*, Sichuan Daxue Xuebao **4** (1985), 107–116. 6

[MOV'96] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, *Handbook of applied cryptography*, CRC Press, 1996, Fifth Printing (August 2001), pp. 816. Online: http://cacr.uwaterloo.ca/hac 6

[Mil'85] V. Miller, *Use of elliptic curves in cryptography*, CRYPTO. Lecture Notes in Computer Science **85** (1985), 417–426. 5, 7

[Mon'87] P. L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization*, Math. of Comp. **48** (1987), 243–264. 15

[OEIS] N. J. A. Sloane and OEIS foundation, *On-Line Encyclopedia of Integer Sequences*, published electronically, sequence http://oeis.org/A165134. 40

[Par'97] I. Parberry, *An efficient algorithm for the Knight's tour problem*, Discrete Appl. Math. **73** (1997), 251–260. 40

[RSA'78] R. Rivest, A. Shamir, L. Adleman, , *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM **21** (1978), no. 2, 120–126. 7

[Sil'95] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, Berlin 1995, 2nd ed. 2005. 6, 36

[SAGE] W. Stein et al., *Sage Mathematics Software* , The Sage Development Team, 2015. http://www.sagemath.org. 43

[WL'13] X. Wang, D. Luan, *A novel image encryption algorithm using a chaos and reversible cellular automata*, Commun. Nonlinear Sci. Numer. Simulat., **18** (2013), 3075–3085. 38

[WWS'12] Y. Y. Wang, D. Wan, H. Y. Sheng, *An encryption algorithm by scrambling image with sudoku grids matrix*, Advanced Materials Research, **433** (2012), 4645–4650. 38

[Was'08] L. C. Washington, *Elliptic curves: number theory and cryptography*, CRC press, 2008 Apr 3. 6

[Wat'18] G. N. Watson, *The problem of the square pyramid*, Messenger of Math. **48** (1918), 1–22. 6

[Wei'49] A. Weil, *Numbers of solutions of equations in finite fields*, Bull. A.M.S **55** (1949), 497–508. 15, 47

[Wei'79] A. Weil, *Comments on* [Wei'49], Collected Works, vol. I, Springer 1979, 568–569. 15

[Wim'53] A. Wiman, *Über die Punkte mit ganzzahligen Koordinaten auf gewissen Kurven dritter Ordnung*, 12te Skand. Matematikerkongressen, Lund, (1953-1954), 317–323. 26

[WZa'14] Y. Wu, Y. Zhou, J. P. Noonan, S. Agaian, *Design of image cipher using Latin squares*, Inform. Sci., **264** (2014), 317–339. 38

[YL'08] R. Ye, H. Li, *A novel image scrambling and watermarking scheme based on cellular automata*, Proceedings of the International Symposium on Electronic Commerce and Security, 2008, Guangzhou, China, 938–941. 38

[ZTX'11] L. Zhang, X. Tian, S. Xia, *A scrambling algorithm of image encryption based on Rubik's cube rotation and logistic sequence*, Proc. of the IEEE 2011 Int. Conf. on Multimedia and Signal Processing (CMSP), **1**, Guilin, China, 2011, 312–315. 38