

# **Curbe eliptice peste corpuri finite**

ADRIAN MANEA

3 noiembrie 2019

# Cuprins

<b>1</b>	<b>Preliminarii</b>	<b>2</b>
1.1	Varietăți algebrice . . . . .	2
1.2	Varietăți proiective . . . . .	5
1.2.1	Aplicație aritmetică . . . . .	7
<b>2</b>	<b>Curbe algebrice</b>	<b>9</b>
2.1	Divizori . . . . .	10
2.2	Teorema Riemann-Roch . . . . .	11
<b>3</b>	<b>Curbe eliptice</b>	<b>13</b>
3.1	Ecuații Weierstrass . . . . .	13
3.2	Structura de grup . . . . .	15
3.3	Curbe eliptice . . . . .	16
<b>4</b>	<b>Curbe eliptice peste corpuri finite</b>	<b>17</b>
4.1	Numărul punctelor raționale . . . . .	17
<b>5</b>	<b>Algoritmul lui Schoof</b>	<b>19</b>
	<b>Index</b>	<b>21</b>
	<b>Bibliografie</b>	<b>21</b>

## 1.1 Varietăți algebrice

Începem prezentarea cu câteva preliminarii privitoare la varietăți algebrice și alte noțiuni elementare de algebră comutativă.

Vom folosi următoarele notații și obiecte:

- $K$  este un corp perfect, i.e. unul pentru care orice extindere algebrică este separabilă;
- $\overline{K}$  este o închidere algebrică fixată a lui  $K$ ;
- $\text{Gal}(\overline{K}/K) = G_{\overline{K}/K}$  este grupul Galois al extinderii  $K \subseteq \overline{K}$ .

În majoritatea exemplelor,  $K$  va fi (o extindere algebrică a lui)  $\mathbb{Q}$ ,  $\mathbb{Q}$  sau  $\mathbb{F}_p$ .

**Definiție 1.1:** *Spațiul afin* peste corpul  $K$  este mulțimea de  $n$ -tupluri:

$$\mathbb{A}^n = \mathbb{A}^n(K) = \{P = (x_1, \dots, x_n) \in \overline{K}^n\}.$$

Similar, se definește *spațiul punctelor  $K$ -raționale* din  $\mathbb{A}^n$ , care conține restricția  $P \in K^n$ .

Fie  $\overline{K}[X] = \overline{K}[X_1, \dots, X_n]$  un inel de polinoame în  $n$  nedeterminate și fie  $I \trianglelefteq \overline{K}[X]$  un ideal. Putem asocia fiecărui astfel de ideal o submulțime a lui  $\mathbb{A}^n$ :

$$V_I = \{P \in \mathbb{A}^n \mid f(P) = 0, \quad \forall f \in I\}.$$

**Definiție 1.2:** O *mulțime algebrică afină* este o mulțime de forma  $V_I$  ca mai sus.

Dacă  $V$  este o astfel de mulțime, *idealul* lui  $V$  este:

$$I(V) = \{f \in \overline{K}[X] \mid f(P) = 0, \quad \forall P \in V\}.$$

Spunem că o mulțime algebrică este *definită* peste  $K$  dacă idealul său  $I(V)$  poate fi generat de polinoame din  $K[X]$  și notăm aceasta cu  $V/K$ .

Dacă  $V$  este definită peste  $K$ , *mulțimea punctelor  $K$ -raționale* ale lui  $V$  este mulțimea:

$$V(K) = V \cap \mathbb{A}^n(K).$$

**Observație 1.1:** Conform teoremei bazei a lui Hilbert, idealele lui  $\overline{K}[X]$  și  $K[X]$  sînt finit generate.

Fie  $V$  o mulțime algebrică și considerăm idealul:

$$I(V/K) = \{f \in K[X] \mid f(P) = 0, \quad \forall P \in V\} = I(V) \cap K[X].$$

Se poate observa că  $V$  este definită peste  $K$  dacă și numai dacă are loc relația:

$$I(V) = I(V/K) \cdot \overline{K}[X].$$

Presupunem acum că  $V$  este definită peste  $K$  și fie  $f_1, \dots, f_m \in K[X]$ , generatori ai idealului  $I(V/K)$ . Rezultă că  $V(K)$  este mulțimea soluțiilor  $x = (x_1, \dots, x_n)$  pentru ecuațiile polinomiale:

$$f_1(x) = \dots = f_m(x) = 0, \quad x_1, \dots, x_n \in K.$$

**Exemplu 1.1:** Fie  $V$  mulțimea algebrică din  $\mathbb{A}^2$  dată de ecuația  $X^2 - Y^2 = 1$ .

Atunci  $V$  este definită peste orice corp  $K$ .

Presupunem acum  $\text{char} K \neq 2$ . Rezultă  $V(K) \simeq \mathbb{A}^1(K) - \{0\}$ , o bijecție fiind, de exemplu:

$$\begin{aligned} \mathbb{A}^1(K) - \{0\} &\rightarrow V(K) \\ t &\mapsto \left( \frac{t^2 + 1}{2t}, \frac{t^2 - 1}{2t} \right). \end{aligned}$$

**Exemplu 1.2:** Mulțimea algebrică  $V : X^n + Y^n = 1$  este definită peste  $\mathbb{Q}$  și, folosind Marea Teoremă a lui Fermat, pentru orice  $n \geq 3$ , are loc:

$$V(\mathbb{Q}) = \begin{cases} \{(1, 0), (0, 1)\}, & n \text{ impar} \\ \{(\pm 1, 0), (0, \pm 1)\}, & n \text{ par} \end{cases}.$$

**Exemplu 1.3:** Mulțimea algebrică  $V : X^2 = Y^3 + 17$  are multe puncte  $\mathbb{Q}$ -raționale. De fapt, se poate arăta că  $V(\mathbb{Q})$  este infinită. Cîteva exemple sînt:

$$V(\mathbb{Q}) = \{(3, -2), (378661, 5234), \left(\frac{2651}{512}, \frac{137}{64}\right)\}.$$

**Definiție 1.3:** O mulțime algebrică (afină) se numește *varietate algebrică (afină)* dacă  $I(V)$  este un ideal prim al lui  $\overline{K}[X]$ .

Remarcăm că dacă  $V$  este definită peste  $K$ , atunci este suficient să verificăm dacă  $I(V/K)$  este ideal prim al lui  $K[X]$ .

Fie  $V/K$  o varietate, adică  $V$  este varietate definită peste  $K$ . Atunci *inelul coordonatelor afine* al  $V/K$  este:

$$K[V] = \frac{K[X]}{I(V/K)}.$$

De asemenea, deoarece  $I(V/K)$  este ideal prim, rezultă că  $K[V]$  este domeniu de integritate. Corpul său de fracții se notează  $K(V)$  și se numește *corpul de funcții* al lui  $V/K$ .

Similar putem formula înlocuind  $K$  cu  $\bar{K}$ .

În plus, orice element al  $\bar{K}[V]$  se definește pînă la un element din  $I(V/\bar{K})$ , deci pînă la un polinom ce se anulează pe  $V$ . Rezultă că  $f \in \bar{K}[V]$  induce o funcție  $f : V \rightarrow \bar{K}$ .

**Definiție 1.4:** Fie  $V$  o varietate algebrică.

*Dimensiunea* varietății, notată  $\dim V$ , este gradul de transcendență al extinderii  $\bar{K}(V)$  peste  $\bar{K}$ .

**Exemplu 1.4:**  $\dim \mathbb{A}^n = n$ , deoarece  $\bar{K}(\mathbb{A}^n) = \bar{K}(X_1, \dots, X_n)$ .

Dacă  $V \subseteq \mathbb{A}^n$  este dat de o ecuație polinomială neconstantă  $f(X_1, \dots, X_n) = 0$ , atunci  $\dim V = n - 1$ .

Vom fi interesați de proprietatea de *netezime*, care se definește prin analogul condiției de existență a planului tangent:

**Definiție 1.5:** Fie  $V$  o varietate algebrică,  $P \in V, f_1, \dots, f_m \in \bar{K}[X]$  o mulțime de generatori pentru  $I(V)$ .

$V$  se numește *nesingulară (netedă)* în  $P$  dacă matricea jacobiană  $\left( \frac{\partial f_i}{\partial X_j}(P) \right)$  are rangul  $n - \dim V$ .

**Exemplu 1.5:** Fie  $V$  dată de o ecuație polinomială neconstantă  $f(x_1, \dots, x_n) = 0$ .

Atunci  $\dim V = n - 1$ , deci  $P$  este singularitate dacă și numai dacă  $\frac{\partial f}{\partial x_i}(P) = 0, \forall 1 \leq i \leq n$ . Totodată,  $f(P) = 0$ , deci în total obținem  $n + 1$  condiții pe  $n$  nedeterminate.

**Exemplu 1.6:** Fie două varietăți:

$$V_1 : Y^2 = X^3 + X \quad \text{și} \quad V_2 : Y^2 = X^3 + X^2.$$

Punctele lor singulare trebuie să satisfacă:

$$V_1^{\text{sing}} : 3X^2 + 1 = 2Y = 0 \quad \text{și} \quad V_2^{\text{sing}} : 3X^2 + 2X = 2Y = 0.$$

Rezultă că  $V_1$  nu are singularități, dar  $V_2$  are, originea  $(0, 0)$ .

Putem formula și o altă caracterizare a netezimii, prin funcții definite pe varietate. Fie  $P$  un punct arbitrar din  $V$ . Definim idealul  $M_P \triangleleft \bar{K}[V]$  prin:

$$M_P = \{f \in \bar{K}[V] \mid f(P) = 0\}.$$

Se poate observa că  $M_P$  este maximal, deoarece avem izomorfismul:

$$\begin{aligned} \bar{K}[V]/M_P &\rightarrow \bar{K} \\ f &\mapsto f(P). \end{aligned}$$

Rezultă că grupul factor  $M_P/M_P^2$  este un  $\bar{K}$ -spațiu vectorial finit dimensional.

Are loc:

**Propoziție 1.1:** *Fie  $V$  o varietate algebrică.*

*Punctul  $P \in V$  este nesingular dacă și numai dacă  $\dim_{\bar{K}} M_P/M_P^2 = \dim V$ .*

**Exemplu 1.7:** Reluăm cazul anterior al varietăților  $V_1$  și  $V_2$  (exemplul 1.6) și fie  $P = (0, 0)$ .

În ambele cazuri,  $M_P$  este generat de  $X$  și  $Y$ , deci  $M_P^2$  este generat de  $X^2, XY$  și  $Y^2$ .

Pentru  $V_1$  avem:

$$X = Y^2 - X^3 \equiv 0 \pmod{M_P^2},$$

deci  $M_P^2$  este generat doar de  $Y$ .

Dar pentru  $V_2$  nu avem nicio relație netrivială între  $X$  și  $Y$  modulo  $M_P^2$ , deci ambele nedeterminate sînt necesare ca generatori.

Rezultă că  $V_1$  e netedă, dar  $V_2$  nu este, deoarece  $\dim V_{1,2} = 1$ .

Folosind idealul maximal, avem:

**Definiție 1.6:** *Inelul local al varietății  $V$  în  $P$ , notat  $\bar{K}[V]_P$ , este localizatul în  $M_P$ , adică:*

$$\bar{K}[V]_P = \{F \in \bar{K}(V) \mid F = f/g, \quad f, g \in \bar{K}[V], g(P) \neq 0\}.$$

Remarcăm că din  $F = f/g$  rezultă că  $F(P) = f(P)/g(P)$  este corect definită.

Funcțiile din  $\bar{K}[V]_P$  se numesc *regulate* (sau *definite*) în  $P$ .

## 1.2 Varietăți proiective

Definim varietățile proiective ca fiind colecția de linii ce trec prin originea unui spațiu afin de dimensiune imediat superioară.

**Definiție 1.7:** *Spațiul  $n$ -proiectiv peste  $K$ , notat  $\mathbb{P}^n$  sau  $\mathbb{P}^n(\bar{K})$ , este mulțimea tuturor  $(n+1)$ -tuplurilor  $(x_0, \dots, x_n) \in \mathbb{A}^{n+1}$ , astfel încît cel puțin o coordonată  $x_i$  este nenulă modulo echivalența:*

$$(x_0, \dots, x_n) \sim (y_0, \dots, y_n) \iff \exists \lambda \in \bar{K}^\times \text{ a.î. } x_i = \lambda y_i, \forall i.$$

Clasa de echivalență  $\{(\lambda x_0, \dots, \lambda x_n) \mid \lambda \in \bar{K}^\times\}$  se notează  $[x_0, \dots, x_n]$ , iar  $x_0, \dots, x_n$  se numesc *coordonatele omogene* ale punctului respectiv în  $\mathbb{P}^n$ .

De asemenea, mulțimea punctelor  $K$ -raționale din  $\mathbb{P}^n$  este:

$$\mathbb{P}^n(K) = \{[x_0, \dots, x_n] \in \mathbb{P}^n \mid x_i \in K\}.$$

**Observație 1.2:** Pentru  $P = [x_0, \dots, x_n] \in \mathbb{P}^n(K)$ , nu rezultă că fiecare  $x_i \in K$ . În schimb, alegem un  $i$  cu  $x_i \neq 0$  și rezultă că  $x_j/x_i \in K$ , pentru orice  $j$ .

**Definiție 1.8:** Fie  $P = [x_0, \dots, x_n] \in \mathbb{P}^n(\overline{K})$ . Corpul minimal de definiție pentru  $P$  peste  $K$  este corpul:

$$K(P) = K(x_0/x_i, \dots, x_n/x_i), \quad \forall i, \text{ cu } x_i \neq 0.$$

**Definiție 1.9:** Un polinom  $f \in \overline{K}[X]$  se numește *omogen de grad  $d$*  dacă:

$$f(\lambda x_0, \dots, \lambda x_n) = \lambda^d f(x_0, \dots, x_n), \quad \forall \lambda \in \overline{K}.$$

Un ideal omogen al lui  $\overline{K}[X]$  este generat de polinoame omogene.

Fiecărui ideal omogen îi putem asocia o submulțime a  $\mathbb{P}^n$ :

$$V_I = \{P \in \mathbb{P}^n \mid f(P) = 0, \text{ pentru orice } f \in I \text{ omogen}\}.$$

**Definiție 1.10:** O mulțime (algebrică) proiectivă este una de forma  $V_I$  ca mai sus.

Idealul omogen al unei mulțimi proiective, notat  $I(V)$ , este idealul lui  $\overline{K}[X]$  generat de:

$$\{f \in \overline{K}[X] \mid f \text{ omogen}, f(P) = 0, \forall P \in V\}.$$

Similar putem descrie și  $V/K$  și  $V(K) = V \cap \mathbb{P}^n(K)$ .

**Exemplu 1.8:** O dreaptă în  $\mathbb{P}^2$  este o mulțime algebrică dată de  $aX + bY + cZ = 0$ , cu  $a, b, c \in \overline{K}$ , nu toate nule.

Dacă, de exemplu,  $c \neq 0$ , atunci dreapta este definită peste orice corp care conține  $a/c$  și  $b/c$ .

În general, un hiperplan în  $\mathbb{P}^n$  este dat de o ecuație:

$$a_0X_0 + a_1X_1 + \dots + a_nX_n = 0, \quad a_i \in \overline{K}, \text{ nu toate nule.}$$

**Exemplu 1.9:** Fie  $V$  în  $\mathbb{P}^2$  dată de  $X^2 + Y^2 = Z^2$ .

Atunci, pentru orice corp  $K$ , cu  $\text{char} K \neq 2$ , avem  $V(K) \simeq \mathbb{P}^1(K)$ , de exemplu prin:

$$\begin{aligned} \mathbb{P}^1(K) &\rightarrow V(K) \\ [s, t] &\mapsto [s^2 - t^2, 2st, s^2 + t^2]. \end{aligned}$$

### 1.2.1 Aplicație aritmetică

Fie un punct din  $\mathbb{P}^n(\mathbb{Q})$ , de coordonate  $[x_0, \dots, x_n]$ ,  $x_i \in \mathbb{Q}$ .

Putem presupune că am înmulțit cu numitorul comun și am eliminat factorii comuni, deci putem presupune  $x_i \in \mathbb{Z}$ ,  $\gcd(x_i) = 1$ . Rezultă că punctul  $P$  determină coordonatele omogene  $x_i$ , *pînă la un semn*.

În general, dacă un ideal al unei mulțimi algebrice definite peste  $\mathbb{Q}$ ,  $V/\mathbb{Q}$ , este generat de polinoame omogene  $f_1, \dots, f_m \in \mathbb{Q}[X]$ , descrierea  $V(\mathbb{Q})$  revine la a rezolva ecuațiile omogene:

$$f_1(x_0, \dots, x_n) = \dots = f_m(x_0, \dots, x_n) = 0, \quad \gcd(x_i) = 1.$$

**Exemplu 1.10:** Fie  $V : X^2 + Y^2 = 3Z^2$ , definit peste  $\mathbb{Q}$ , dar  $V(\mathbb{Q}) = \emptyset$ . Într-adevăr, presupunem că  $[x, y, z] \in V(\mathbb{Q})$ , cu  $x, y, z \in \mathbb{Z}$  și  $\gcd(x, y, z) = 1$ . Rezultă  $x^2 + y^2 \equiv 0 \pmod{3}$ , dar cum  $-1$  nu este pătrat modulo 3, rezultă că  $x \equiv y \equiv 0 \pmod{3}$ , deci  $x^2, y^2 : 3^2$ , adică  $3 \mid z$ , contradicție cu  $\gcd(x, y, z) = 1$ .

Așadar, ideea generală este că, pentru a arăta că  $V(\mathbb{Q}) = \emptyset$ , este suficient să arătăm că ecuațiile omogene corespunzătoare nu au soluții nenule *modulo*  $p$ , pentru orice prim  $p$  (sau pentru orice putere a unui prim).

Spus mai simplu, avem implicația  $V(\mathbb{Q}) = \emptyset \Rightarrow V(\mathbb{Q}_p) = \emptyset$ , pentru orice corp  $p$ -adic  $\mathbb{Q}_p$ . Mai departe, implicația poate continua cu  $V(\mathbb{R}) = \emptyset$ .

Însă *reciproca este falsă!* Se poate arăta că, pentru varietatea:

$$V : 3X^2 + 4Y^2 + 5Z^3 = 0,$$

avem  $V(\mathbb{Q}_p) \neq \emptyset, \forall p$ , dar  $V(\mathbb{Q}) = \emptyset$ .

**Definiție 1.11:** O mulțime algebrică proiectivă se numește *varietate proiectivă* dacă idealul omogen  $I(V)$  este prim în  $\bar{K}[X]$ .

Fie  $f(Y) \in \bar{K}[Y]$ . Definim:

$$f^*(x_0, \dots, x_n) = x_i^d f\left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i}\right),$$

unde  $d = \deg f$  este cel mai mic întreg care face  $f^*$  polinom.

Spunem că  $f^*$  este *omogenizatul* lui  $f$  în raport cu  $x_i$ .

**Definiție 1.12:** Fie  $V \subseteq \mathbb{A}^n$  o mulțime algebrică afină, cu idealul  $I(V)$  și fie  $V$  o submulțime a  $\mathbb{P}^n$  prin:

$$V \subseteq \mathbb{A}^n \xrightarrow{\phi_i} \mathbb{P}^n$$

$$\phi_i(y_1, \dots, y_n) \mapsto [y_1, \dots, y_{i-1}, 1, y_i, \dots, y_n].$$

*Închiderea proiectivă* a lui  $V$ , notată  $\bar{V}$ , este mulțimea proiectivă al cărui ideal omogen  $I(\bar{V})$  este generat de omogenizatele generatorilor lui  $I(V)$ .

Punctele din  $V - \bar{V}$  se numesc *puncte la infinit* din  $V$ .



**Exemplu 1.11:** Fie  $V$  proiectivă, definită de  $Y^2 = X^3 + 17$ .

Rezultă că  $V$  este dată în  $\mathbb{P}^2$  de:

$$\overline{Y}^2 \overline{Z} = \overline{X}^3 + 17 \overline{Z}^3, \quad X = \overline{X}/\overline{Z}, Y = \overline{Y}/\overline{Z}.$$

Varietatea are un singur punct la infinit,  $[0, 1, 0]$ , obținut din  $\overline{Z} = 0$ . Rezultă:

$$V(\mathbb{Q}) = \{(x, y) \in \mathbb{A}^2(\mathbb{Q}) \mid y^2 = x^3 + 17\} \cup \{[0, 1, 0]\}.$$

**Definiție 1.13:** Fie  $V/K$  o varietate proiectivă și fie  $\mathbb{A}^n \subseteq \mathbb{P}^n$  astfel încât  $V \cap \mathbb{A}^n \neq \emptyset$ . Atunci se definește:

$$\dim V = \dim(V \cap \mathbb{A}^n).$$

*Corpul de funcții*  $K(V)$  este corpul de funcții al  $V \cap \mathbb{A}^n$ .

**Observație 1.3:** Pentru alegeri diferite ale lui  $\mathbb{A}^n$ , obținem izomorfisme canonice între rezultate.

Similar, *netezimea* în varietăți proiective  $V$  se traduce în  $V \cap \mathbb{A}^n$ .

## SECȚIUNEA 2

## CURBE ALGEBRICE

Printr-o *curbă algebrică* vom înțelege o varietate proiectivă de dimensiune 1. Vom lucra, în general, cu curbe netede.

Notățiile specifice sînt:

- $C/K$ : curba  $C$  este definită peste corpul  $K$ ;
- $\overline{K}(C)$ : corpul de funcții al lui  $C$  peste  $K$ ;
- $\overline{K}[C]_P$ : inelul local al lui  $C$  în punctul  $P$ ;
- $M_P$ : idealul maximal al inelului local  $\overline{K}[C]_P$ .

**Definiție 2.1:** Fie  $C$  o curbă și  $P \in C$  un punct neted.

Valuarea normalizată pe  $\overline{K}[C]_P$  este dată de:

$$\begin{aligned}\text{ord}_P : \overline{K}[C]_P &\rightarrow \mathbb{N} \cup \{\infty\} \\ \text{ord}_P(f) &= \sup\{d \in \mathbb{Z} \mid f \in M_P^d\}.\end{aligned}$$

Folosind  $\text{ord}_P(f/g) = \text{ord}_P(f) - \text{ord}_P(g)$ , putem extinde valuarea la  $\mathbb{Z}$ .

Un *uniformizator* pentru  $C$  în  $P$  este orice funcție  $t \in \overline{K}(C)$ , cu  $\text{ord}_P t = 1$ , adică  $t$  este generator pentru dealul  $M_P$ .

Pentru  $C$  și  $P$  ca mai sus, fie  $f \in \overline{K}(C)$ . Se definește *ordinul* lui  $f$  în  $P$  prin  $\text{ord}_P f$ . Dacă ordinul este pozitiv, spunem că  $f$  are zero în  $P$ ; altfel,  $f$  are singularitate (pol) în  $P$ . Dacă ordinul este negativ, spunem că  $C$  este *definită* în  $P$  și putem calcula  $f(P)$ . Altfel,  $f(P) = \infty$ .

**Exemplu 2.1:** Reluăm unul dintre exemplele anterioare (exemplul 1.6):

$$C_1 : Y^2 = X^3 + X, \quad C_2 : Y^2 = X^3 + X^2.$$

Ambele curbe au câte o singularitate la infinit. Fie  $P = (0, 0)$ . Atunci  $C_1$  este netedă în  $P$ , dar  $C_2$  nu este.

Idealul maximal  $M_P$  al lui  $\overline{K}[C_1]_P$  are proprietatea că  $M_P/M_P^2$  este generat de  $Y$ , deci:

$$\text{ord}_P Y = 1, \quad \text{ord}_P X = 2, \quad \text{ord}_P(2Y^2 - X) = 2,$$

ultima egalitate rezultînd din  $2Y^2 - X = 2X^3 + X$ .

## 2.1 Divizori

**Definiție 2.2:** Fie  $C$  o curbă algebrică. *Grupul divizorilor* curbei, notat  $\text{Div}C$ , este grupul abelian liber ( $\mathbb{Z}$ -modulul) generat de punctele de pe  $C$ .

Deci orice  $D \in \text{Div}C$  este o sumă formală:

$$D = \sum_{P \in C} n_P(P),$$

unde  $n_P \in \mathbb{Z}$  și  $n_P = 0$  pentru majoritatea  $P \in C$ .

*Gradul divizorului*  $D$  se definește prin:

$$\deg D = \sum_{P \in C} n_P.$$

Divizorii de grad 0 formează un subgrup al  $\text{Div}(C)$ , pe care îl notăm și definim astfel:

$$\text{Div}^0(C) = \{D \in \text{Div}(C) \mid \deg D = 0\}.$$

Presupunem acum că avem o curbă netedă  $C$  și fie  $f \in \overline{K}(C)^\times$ . Atunci putem asocia un divizor fiecărei funcții  $f$  prin:

$$\text{div}(f) = \sum_{P \in C} \text{ord}_P(f)(P).$$

În plus, cum fiecare  $\text{ord}_P$  definește o valoare, aplicația de mai sus se poate extinde la:

$$\text{div} : \overline{K}(C)^\times \rightarrow \text{Div}(C),$$

care devine un morfism de grupuri abeliene. Acțiunea lui este similară aplicației care trimite un element dintr-un corp de numere în idealul care-l conține. De aceea, noțiunea se poate generaliza și sîntem conduși la definițiile de mai jos.

**Definiție 2.3:** Un divizor  $D \in \text{Div}(C)$  se numește *principal* dacă este de forma  $D = \text{div}f$ , pentru un anumit  $f$  ca mai sus.

Doi divizori se numesc *echivalenți liniar*, notat  $D_1 \sim D_2$ , dacă  $D_1 - D_2$  este un divizor principal.

*Grupul Picard* (sau grupul claselor de divizori) pentru curba  $C$ , notat  $\text{Pic}(C)$ , este grupul factor al  $\text{Div}(C)$  modulo subgrupul divizorilor principali.

Cu aceste noțiuni, se poate demonstra simplu:

**Propoziție 2.1:** Fie  $C$  o curbă netedă și fie  $f \in \overline{K}(C)^\times$ .

- $\operatorname{div} f = 0$  dacă și numai dacă  $f \in \overline{K}^*$ ;
- $\deg(\operatorname{div} f) = 0$ .

**Exemplu 2.2:** În  $\mathbb{P}^1$ , fiecare divizor de grad 0 este principal. Într-adevăr, fie  $D = \sum n_P(P)$  un divizor de grad 0. Atunci fie  $P = [\alpha_P, \beta_P] \in \mathbb{P}^1$  și rezultă că  $D$  este divizor pentru funcția:

$$\prod_{P \in \mathbb{P}^1} (\beta_P X - \alpha_P Y)^{n_P}.$$

Dar  $\sum n_P = 0$ , ceea ce asigură că această funcție aparține  $K(\mathbb{P}^1)$  și rezultă că aplicația  $\deg : \operatorname{Pic}(\mathbb{P}^1) \rightarrow \mathbb{Z}$  este un izomorfism.

Reciproca este de asemenea adevărată, i.e. dacă  $C$  este o curbă netedă iar  $\operatorname{Pic}(C) \simeq \mathbb{Z}$ , atunci  $C \simeq \mathbb{P}^1$ .

**Exemplu 2.3:** Presupunem că lucrăm într-un corp cu  $\operatorname{char} K \neq 2$  și fie  $e_1, e_2, e_3 \in \overline{K}$  trei elemente distincte. Definim curba:

$$C : y^2 = (x - e_1)(x - e_2)(x - e_3).$$

Se poate verifica ușor că această curbă este netedă și că are un singur punct la infinit, pe care îl notăm  $P_\infty$ . Pentru  $i = 1, 2, 3$ , fie  $P_i = (e_i, 0) \in C$ . Atunci obținem:

$$\begin{aligned} \operatorname{div}(x - e_i) &= 2P_i - 2P_\infty \\ \operatorname{div}(y) &= P_1 + P_2 + P_3 - 3P_\infty. \end{aligned}$$

Rezultă din cele de mai sus că grupul divizorilor principali este un subgrup al  $\operatorname{Div}^0 C$ . Definim partea de grad 0 a grupului Picard pentru curba  $C$  ca fiind grupul factor al  $\operatorname{Div}^0 C$  modulo subgrupul divizorilor principali. Notăm acest grup cu  $\operatorname{Pic}^0 C$ .

Observațiile de mai sus pot fi puse în această formă: există un șir exact scurt:

$$1 \rightarrow \overline{K}^\times \rightarrow \overline{K}(C)^\times \xrightarrow{\operatorname{div}} \operatorname{Div}^0 C \rightarrow \operatorname{Pic}^0 C \rightarrow 0.$$

## 2.2 Teorema Riemann-Roch

Fie  $C$  o curbă. Definim o ordine parțială pe grupul divizorilor:

**Definiție 2.4:** Un divizor  $D = \sum n_P(P)$  se numește *efectiv* sau pozitiv, notat  $D \geq 0$ , dacă  $n_P \geq 0$  pentru orice punct  $P \in C$ .

Mai departe, pentru orice divizori  $D_1, D_2 \in \operatorname{Div}(C)$ , putem scrie  $D_1 \geq D_2$  dacă diferența  $D_1 - D_2$  este un divizor efectiv.

**Exemplu 2.4:** Fie  $f \in \overline{K}(C)^\times$  o funcție care este regulată peste tot, mai puțin într-un punct  $P \in C$  și presupunem că acolo are un pol de ordin cel mult  $n$  în  $P$ . Aceste cerințe pot fi puse mai simplu în forma:

$$\operatorname{div} f \geq -n(P).$$

Similar, dacă scriem  $\operatorname{div} f \geq (Q) - n(P)$ , afirmăm că  $f$  are un zero în  $Q$ .

**Definiție 2.5:** Fie  $D \in \operatorname{Div} C$ . Asociem divizorului  $D$  o mulțime de funcții:

$$\mathcal{L}(D) = \{f \in \overline{K}(C)^\times \mid \operatorname{div} f \geq -D\} \cup \{0\}.$$

Mulțimea  $\mathcal{L}(D)$  formează un spațiu vectorial finit dimensional peste  $\overline{K}$  și notăm  $\ell(D) = \dim_{\overline{K}} \mathcal{L}(D)$ .

**Teoremă 2.1** (Riemann-Roch): Fie  $C$  o curbă netedă și fie  $K_C$  un divizor canonic pe  $C$ . Atunci există un întreg  $g \geq 0$ , numit genul curbei  $C$ , astfel încât pentru orice divizor  $D \in \operatorname{Div}(C)$ , are loc:

$$\ell(D) - \ell(K_C - D) = \deg D - g + 1.$$

### 3.1 Ecuații Weierstrass

Vom studia în special curbe eliptice, care sînt curbe de gen 1, cu un punct-bază specificat. Vom vedea că orice astfel de curbă poate fi gîndită ca locul geometric în  $\mathbb{P}^2$  al unei ecuații cubice cu un punct, punctul bază, pe linia de la infinit. Apoi, după o schimbare de coordonate, orice curbă eliptică se poate prezenta sub forma:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

În acest caz, punctul bază este  $O = [0, 1, 0]$ , iar  $a_i \in \overline{K}$ .

Studiem acum curbele eliptice care sînt date cu formule explicite, numite *ecuații Weierstrass*.

Pentru simplificarea notației, vom lucra cu coordonatele neomogene,  $x = X/Z$  și  $y = Y/Z$  și atunci, putem scrie curba:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

ținînd cont și de un punct  $O = [0, 1, 0]$  la infinit. Ca în cazul oricărei varietăți, dacă  $a_i \in K$ , spunem că avem o curbă *E definită peste K*.

Presupunem că lucrăm cu  $\text{char}(\overline{K}) \neq 2$  și atunci putem simplifica ecuația, cu substituția:

$$y \mapsto \frac{1}{2}(y - a_1x - a_3),$$

care conduce la ecuația:

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

cu notațiile:

$$b_2 = a_1^2 + 4a_4, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6.$$

Mai definim și:

$$\begin{aligned}
b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 \\
c_4 &= b_2^2 - 24b_4 \\
c_6 &= -b_2^3 + 36b_2 b_4 - 216b_6 \\
\Delta &= -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 \\
j &= c_4^3 / \Delta \\
\omega &= \frac{dx}{2y + a_1 x + a_3} = \frac{dy}{3x^2 + 2a_2 x + a_4 - a_1 y}.
\end{aligned}$$

Relațiile simple între aceste cantități sînt:

$$4b_8 = b_2 b_6 - b_4^2, \quad \text{și} \quad 1728\Delta = c_4^3 - c_6^2.$$

Mai departe, dacă  $\text{char } \bar{K} \neq 2, 3$ , putem face substituția:

$$(x, y) \mapsto \left( \frac{x - 3b_2}{36}, \frac{y}{108} \right),$$

care elimină termenul cu  $x^2$  și ajungem la:

$$E : y^2 = x^3 - 27c_4 x - 54c_6.$$

**Definiție 3.1:** Cantitatea  $\Delta$  se numește *discriminantul* ecuației Weierstrass, cantitatea  $j$  se cheamă  $j$ -invariantul curbei eliptice, iar  $\omega$  este *invariantul diferențial* asociat ecuației.

Considerăm acum o situație generală. Fie  $P = (x_0, y_0)$  un punct arbitrar care satisface o ecuație de tip Weierstrass:

$$f(x, y) = y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6 = 0$$

și mai presupunem că  $P$  este o singularitate pentru curba  $f(x, y) = 0$ , deci

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.$$

Rezultă că există coeficienți  $\alpha, \beta \in \bar{K}$  astfel încît dezvoltarea Taylor a polinomului  $f(x, y)$  în jurul lui  $P$  se poate scrie:

$$f(x, y) - f(x_0, y_0) = ((y - y_0) - \alpha(x - x_0))((y - y_0) - \beta(x - x_0)) - (x - x_0)^3.$$

**Definiție 3.2:** Folosind notațiile de mai sus, singularitatea  $P$  se numește *nod* dacă  $\alpha \neq \beta$ , iar în acest caz, curbele:

$$y - y_0 = \alpha(x - x_0) \quad \text{și} \quad y - y_0 = \beta(x - x_0)$$

se numesc *tangentele în  $P$* . Reciproc, dacă  $\alpha = \beta$ , spunem că  $P$  este *vîrf* (eng. *cusp*), caz în care tangenta la  $P$  este dată de:

$$y - y_0 = \alpha(x - x_0).$$

## 3.2 Structura de grup

Fie  $E$  o curbă eliptică dată de o ecuație Weierstrass. Rezultă că  $E \subseteq \mathbb{P}^2$  conține puncte  $P = (x, y)$  care satisfac ecuația Weierstrass, împreună cu punctul  $O = [0, 1, 0]$  de la infinit.

Fie  $L \subseteq \mathbb{P}^2$  o dreaptă. Atunci, deoarece ecuația are gradul 3, dreapta  $L$  intersectează  $E$  în exact 3 puncte, pe care le notăm  $P, Q, R$ .

**Definiție 3.3:** Fie  $P, Q \in E$  și fie  $L$  dreapta prin  $P$  și  $Q$  (dacă  $P = Q$ , atunci  $L$  este tangenta în  $P$ ). Fie  $R$  un al treilea punct de intersecție a lui  $L$  cu  $E$ .

Fie  $L'$  dreapta prin  $R$  și  $O$ . Atunci  $L'$  intersectează  $E$  în  $R, O$  și un al treilea punct. Acest al treilea punct se notează  $P \oplus Q$ .

Operația este ilustrată în figura 3.1.

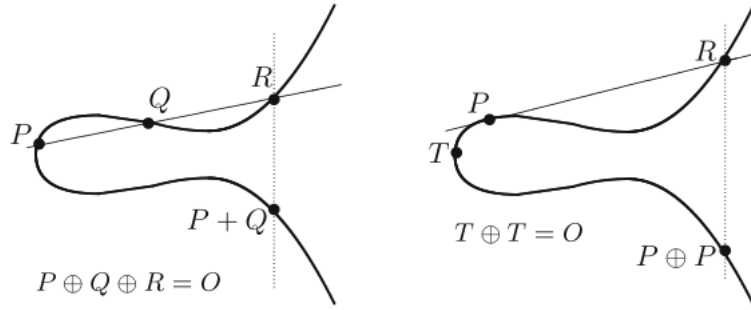


Figura 3.1: Adunarea punctelor pe o curbă eliptică, [Silverman, 2009], p. 51

Cu acestea, se obține că  $(E, \oplus)$  formează un grup abelian, cu elementul neutru  $O = [0, 1, 0]$ . Pentru simplitate, în continuare vom nota operațiile cu notațiile obișnuite,  $\oplus \mapsto +, \ominus \mapsto -$ .

**Exemplu 3.1:** Fie curba eliptică  $E/\mathbb{Q}$ :

$$E : y^2 = x^3 + 17.$$

Calcule simple găsesc câteva puncte cu coordonate întregi:

$$P_1 = (-2, 3), P_2 = (-1, 4), P_3 = (2, 5), P_4 = (4, 9), P_5 = (8, 23).$$

Folosind operația de grup, se pot verifica relațiile:

$$P_5 = -2 \cdot P_1, \quad P_4 = P_1 - P_3.$$

Se poate arăta că orice punct rațional  $P \in E(\mathbb{Q})$  poate fi scris sub forma:

$$P = mP_1 + nP_3, \quad m, n \in \mathbb{Z},$$

ceea ce ne arată că  $E(\mathbb{Q}) \simeq \mathbb{Z} \times \mathbb{Z}$ .

!



### 3.3 Curbe eliptice

Fie  $E$  o curbă netedă de gen 1.

**Definiție 3.4:** O curbă eliptică este o pereche  $(E, O)$ , alcătuită dintr-o curbă nesingulară  $E$  de gen 1 și un punct  $O \in E$ .

Curba se numește *definită peste corpul  $K$* , notat  $E/K$ , dacă  $E$  este o curbă definită peste  $K$ , iar  $O \in E(K)$ .

Relevanța ecuației Weierstrass reiese din:

**Propoziție 3.1:** Fie  $E$  o curbă eliptică definită peste  $K$ .

(a) Există funcțiile  $x, y \in K(E)$  astfel încât aplicația:

$$\phi : E \rightarrow \mathbb{P}^2, \quad \phi = [x, y, 1]$$

dă un izomorfism între  $E/K$  și o curbă dată de o ecuație Weierstrass:

$$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

cu coeficienții  $a_1, \dots, a_6 \in K$  și  $\phi(O) = [0, 1, 0]$ .

Funcțiile  $x, y$  se numesc coordonatele Weierstrass ale curbei eliptice  $E$ .

(b) Orice două ecuații Weierstrass pentru curba fixată  $E$  sînt legate printr-o schimbare de variabile de forma:

$$X = u^2X' + r, \quad Y = u^3Y' + su^2X' + t,$$

pentru  $u \in K^\times, r, s, t \in K$ .

(c) Reciproc, orice curbă cubică netedă  $C$  dată de o ecuație Weierstrass ca în (a) este o curbă eliptică definită peste  $K$ , cu punctul bază  $O = [0, 1, 0]$ .

**Corola 3.1:** Fie  $E/K$  o curbă eliptică cu coordonatele Weierstrass  $x, y$  ca în teoremă. Atunci:

$$K(E) = K(x, y) \quad \text{și} \quad [K(E) : K(x)] = 2.$$

## SECȚIUNEA 4

# CURBE ELIPTICE PESTE CORPURI FINITE

Considerăm acum cazul particular al curbelor eliptice definite peste corpuri finite  $\mathbb{F}_q$ . Cea mai importantă noțiune este aceea a numărului punctelor raționale.

Notățiile pe care le folosim sînt:

- $q$ , o putere a unui prim  $p$ ;
- $\mathbb{F}_q$ , un corp finit cu  $q$  elemente;
- $\overline{\mathbb{F}}_q$ , o închidere algebrică a lui  $\mathbb{F}_q$ .

### 4.1 Numărul punctelor raționale

Fie  $E/\mathbb{F}_q$  o curbă eliptică definită peste un corp finit. Vrem să estimăm numărul punctelor din  $E(\mathbb{F}_q)$  (notat  $\#E(\mathbb{F}_q)$ ) sau, echivalent, una sau mai multe soluții ale ecuației:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad (x, y) \in \mathbb{F}_q^2.$$

Deoarece fiecare valoarea a lui  $x$  conduce la cel mult 2 valori pentru  $y$ , o margine superioară este:

$$\#E(\mathbb{F}_q) \leq 2q + 1.$$

Dar o ecuație pătratică aleatorie are șanse mici de a fi rezolvabilă în  $\mathbb{F}_q$  deci ne așteptăm ca marginea superioară să conțină  $q$ , nu  $2q$ .

Rezultatul de mai jos a fost formulat ca o conjectură de E. Artin și demonstrat de H. Hasse în anii 1930:

**Teoremă 4.1 (Hasse):** Fie  $E/\mathbb{F}_q$  o curbă eliptică definită peste un corp finit. Atunci:

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

*Demonstrație.* Fie o ecuație Weierstrass pentru  $E$  în  $\mathbb{F}_q$  și fie:

$$\phi : E \rightarrow E, \quad (x, y) \mapsto (x^q, y^q)$$

morfismul Frobenius de putere  $q$ . Grupul Galois  $\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$  este generat de aplicația de putere  $q$  pe  $\overline{\mathbb{F}}_q$ , deci pentru orice punct  $P \in E(\overline{\mathbb{F}}_q)$ , are loc:

$$P \in E(\mathbb{F}_q) \iff \phi(P) = P.$$

Rezultă  $E(\mathbb{F}_q) = \ker(1 - \phi)$ , deci:

$$\#E(\mathbb{F}_q) = \#\text{Ker}(1 - \phi) = \deg(1 - \phi).$$

Aplicația de putere pe  $\text{End}(E)$  este o formă pătratică pozitiv definită și cum  $\deg \phi = q$ , rezultă inegalitatea dorită folosind Cauchy-Schwarz.  $\square$

**Exemplu 4.1:** Fie  $\mathbb{F}_q$  un corp finit cu  $q$  impar. Putem folosi teorema Hasse pentru a estima diverse caractere pe  $\mathbb{F}_q$ . Definim:

$$f(x) = ax^3 + bx^2 + cx + d \in K[x]$$

un polinom cubic, cu rădăcini distincte în  $\overline{\mathbb{F}}_q$  și fie:

$$\chi : \mathbb{F}_q^\times \rightarrow \{\pm 1\}$$

caracterul netrivial de ordin 2, adică  $\chi(t) = 1$  dacă și numai dacă  $t$  este un pătrat în  $\mathbb{F}_q^\times$ .

Putem extinde  $\chi$  la  $\mathbb{F}_q$  definind  $\chi(0) = 0$  și putem folosi  $\chi$  pentru a număra punctele  $\mathbb{F}_q$ -raționale de pe curba eliptică:

$$E : y^2 = f(x).$$

Fiecare  $x \in \mathbb{F}_q$  produce 0, 1 sau 2 puncte  $(x, y) \in E(\mathbb{F}_q)$ , în funcție de faptul dacă  $f(x)$  este pătrat, ne-pătrat sau nulă în  $\mathbb{F}_q$ . Rezultă, folosind și punctul de la infinit:

$$\begin{aligned} \#E(\mathbb{F}_q) &= 1 + \sum_{x \in \mathbb{F}_q} (1 + \chi(f(x))) \\ &= 1 + q + \sum_{x \in \mathbb{F}_q} \chi(f(x)) \end{aligned}$$

Ț

Folosind exemplul de mai sus, împreună cu teorema Hasse, obținem:

**Corola 4.1:** Folosind notațiile și contextul de mai sus, avem:

$$\left| \sum_{x \in \mathbb{F}_q} \chi(f(x)) \right| \leq 2\sqrt{q}.$$

## SECȚIUNEA 5

## ALGORITMUL LUI SCHOOOF

Există o abordare algoritmică pentru a număra punctele unei curbe eliptice definită peste un corp finit. Știm din teorema lui Hasse (teorema 4.1) că:

$$\#E(\mathbb{F}_q) = q + 1 - a_1, \quad |a_q| \leq 2\sqrt{q}.$$

Pentru aplicații criptografice, însă, este util să avem o metodă eficientă de a calcula numărul de puncte din  $E(\mathbb{F}_q)$ .

Pentru simplitate, vom presupune că lucrăm cu  $q$  impar și că  $E$  este dată de ecuația Weierstrass de forma:

$$E : y^2 = f(x) = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

pentru care mare parte din rezultatele folosite vor fi valabile și în caracteristică 2, cu mici modificări.

Există o metodă directă, dar deloc simplă, de a calcula numărul de puncte, care folosește simboluri Legendre:

$$a_q = \sum_{x \in \mathbb{F}_q} \left( \frac{f(x)}{q} \right),$$

dar fiecare simbol Legendre se calculează folosind reciprocitatea pătratică în  $O(\log q)$  pași, deci în total avem  $O(q \log q)$  pași, adică un algoritm exponențial.

În continuare, descriem un algoritm care calculează  $\#E(\mathbb{F}_q)$  în timp polinomial, i.e.  $O(\log^c q)$ , cu  $c$  fixat, independent de  $q$ . Ideea acestui algoritm este să se calculeze  $a_q \bmod \ell$  pentru prime mici  $\ell$  și apoi să se folosească lema chineză a resturilor pentru a recompune  $a_q$ .

Fie aplicația:

$$\tau : E(\overline{\mathbb{F}_q}) \rightarrow E(\overline{\mathbb{F}_q}), \quad (x, y) \mapsto (x^q, y^q),$$

aplicația Frobenius de putere  $q$ , deci știm că are loc:

$$\tau^2 - a_q\tau + q = 0$$

în  $\text{End}(E)$ . În particular, pentru  $P \in E(\mathbb{F}_q)[\ell]$ , are loc:

$$\tau^2(P) - [a_q]\tau(P) + [q]P = O,$$

deci dacă punem  $P = (x, y)$  și presupunem  $P \neq O$ , avem:

$$(x^{q^2}, y^{q^2}) - [a_q](x^q, y^q) + [q](x, y) = O.$$

Deoarece am presupus că  $P = (x, y)$  are ordinul  $\ell$ , rezultă:

$$[a_q](x^q, y^q) = [n_\ell](x^q, y^q),$$

pentru un  $n_\ell \equiv a_q \pmod{\ell}$  și  $0 \leq n_\ell < \ell$ .

Similar, putem calcula  $[q](x, y)$  prin a reduce  $q$  modulo  $\ell$  mai întâi.

Nu trebuie să știm exact valoarea lui  $n_\ell$ , deci pentru orice întreg între 0 și  $\ell$  calculăm  $[n](x^q, y^q)$  pentru orice punct  $(x, y) \in E[\ell] - \{O\}$  și verificăm dacă satisface:

$$[n](x^q, y^q) = (x^{q^2}, y^{q^2}) + [q](x, y).$$

Problema care apare este că punctele din  $E[\ell]$  sînt definite peste extinderi destul de mari ale lui  $\mathbb{F}_q$ , deci va trebui să lucrăm cu toate punctele de  $\ell$ -torsione simultan. Pentru aceasta, folosim polinomul  $\psi_\ell(x) \in \mathbb{F}_q[x]$ , ale cărui rădăcini sînt coordonatele  $x$  ale punctelor nenule de  $\ell$ -torsione din  $E$  (presupunem, pentru simplitate,  $\ell \neq 2$ ). Acest polinom are gradul  $\frac{1}{2}(\ell^2 - 1)$  și se poate calcula simplu (**v. Ex. 3.7, pagina 105**). Acum putem lucra în inelul factor:

$$R_\ell = \frac{\mathbb{F}_q[x, y]}{\psi_\ell(x), y^2 - f(x)}.$$

Rezultă că, dacă avem o putere neliniară a lui  $y$ , putem înlocui  $y^2$  cu  $f(x)$  și dacă avem o putere  $x^d$ , mai mare decît  $\frac{1}{2}(\ell^2 - 1)$ , putem împărți la  $\psi_\ell(x)$  și luăm doar restul. Astfel, nu lucrăm niciodată cu polinoame de grad mai mare decît  $\frac{1}{2}(\ell^2 - 3)$ .

Scopul va fi să calculăm  $a_q \pmod{\ell}$  pentru suficiente prime  $\ell$  și apoi să găsim  $a_q$ . Teorema lui Hasse (4.1) ne dă  $|a_q| \leq 2\sqrt{q}$ , deci este suficient să luăm primele  $\ell \leq \ell_{\max}$  astfel încît:

$$\prod_{\ell \leq \ell_{\max}} \ell \geq 4\sqrt{q}.$$

**Teoremă 5.1** (Algoritmul Schoof): *Fie  $E/\mathbb{F}_q$  o curbă eliptică. Algoritmul descris mai jos este unul în timp polinomial pentru a calcula  $\#E(\mathbb{F}_q)$ . Mai precis, calculează  $\#E(\mathbb{F}_q)$  în  $O(\log^8 q)$  pași.*

␣␣␣

**C**

corp

minimal, 6

curbe

divizori, 10

gen, 12

**D**

divizor

echivalență liniară, 10

efectiv, 11

grupul Picard, 10

principal, 10

**I**

invariant Weierstrass

diferențial, 14

discriminant, 14

j, 14

**M**

mulțime

algebrică afină, 2

algebrică definită, 3

proiectivă, 6

**P**

polinom

omogen, 6

omogenizat, 7

**S**

spațiu

afin, 2

proiectiv, 5

spațiul

punctelor raționale, 2

**T**

teorema

Riemann-Roch, 12

**U**

uniformizator, 9

**V**

valuare

normalizată, 9

varietate

afină, 3

dimensiune, 4

netedă, 4

proiectivă, 7

închidere proiectivă, 7

- [Husemoller, 2004] Husemoller, D. (2004). *Elliptic Curves*. Springer.
- [Silverman, 1994] Silverman, J. (1994). *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer.
- [Silverman, 2009] Silverman, J. (2009). *The Arithmetic of Elliptic Curves*. Springer.
- [Washington, 2008] Washington, L. (2008). *Elliptic Curves, Number Theory and Cryptography*. Chapman and Hall.