# Глава 10

# Елиптични криви и криптография

## 10.1 Проективно пространство и елиптични криви

**Дефиниция 10.1.1** *Нека $\mathbb{F}$ е поле.* ***Елиптична крива*** *$\mathcal{E}(\mathbb{F})$* ***над*** *$\mathbb{F}$ (зададена с уравнение на Вайерщрас в обобщена форма) наричаме съвкупността от всички точки $(x, y)$ на равнина $\mathbb{F}^2$, които удовлетворяват*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in \mathbb{F}, \tag{10.1}$$

*и една специална точка $\mathcal{O}$, наричана безкрайна точка.*

### 10.1.1 Случаят $\mathrm{char}\,\mathbb{F} \neq 2, 3$.

Когато характеристиката на полето е различна от 2 и 3 (в частност при полето от остатъци по модул просто число $p > 3$: $\mathbb{F} = \mathbb{Z}_p$) горното уравнение може да се трансформира във вида

$$\mathcal{E}: \; y^2 = x^3 + ax + b, \tag{10.2}$$

където $a, b \in \mathbb{F}$, такива че $4a^3 + 27b^2 \neq 0$.

По-точно, ако кривата е зададена с (10.2) се казва, че е представена в редуцирана форма на Вайерщрас (Short Weierstrass form).

За удобство (в частност за равноправно третиране на безкрайната точка) се преминава към проективното пространство $\mathbb{P}_2(\mathbb{F})$, където точките се представят с тройка числа $(x : y : z)$, наречени проективни координати. Две тройки $(x : y : z)$ и $(u : v : w)$ представят една и съща точка, ако

$$\frac{x}{u} = \frac{y}{v} = \frac{z}{w},$$

т.е. точката с афинни координати $(x, y)$ се представя с $(x : y : 1)$. Кривата ще се представя с проективния вариант на редуцираната форма на Вайерщрас

$$\mathcal{E}: \; y^2z = x^3 + axz^2 + bz^3, \tag{10.3}$$

Множеството от точки $(x : y : 0)$ формират така наречената безкрайна права, като точката с координати $(0 : 1 : 0)$ е безкрайната точка $\mathcal{O}$, която лежи на кривата (проективните ѝ координати удовлетворяват (10.3)).

В $\mathcal{E}$ дефинираме операцията събиране и противоположен елемент (т.е. изваждане), с което $\mathcal{E}$ се превръща в адитивна абелева група:
За нулев елемент избираме $\mathcal{O} = (0 : 1 : 0)$. Противоположният елемент на $P = (x, y)$ (т.е. на $P = (x : y : 1)$) се дефинира като $-P = (x, -y)$ и $P + (-P) = \mathcal{O}$. Очевидно, точката $-P$ е симетрична на $P$ относно абцисата.
Нека $P_1(x_1, y_1)$ и $P_2(x_2, y_2)$ не са противоположни, т.е. $P_2 \neq -P_1$. Полагаме

$$m = \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2}, & \text{ако } P_1 \neq P_2 \\ \dfrac{3x_1^2 + a}{2y_1}, & \text{ако } P_1 = P_2 \end{cases}$$

Дефинираме $P(x, y) = P_1 + P_2$ по правилото

$$x = -x_1 - x_2 + m^2; \qquad y = -y_1 + m(x_1 - x). \tag{10.4}$$

Както лесно се вижда второто равенство в (10.4) е уравнението на правата през точките $-P_1$ и $-P_2$. Следователно точката $P$ е пресечната на тази права с кривата. Ако $P_1 \equiv P_2$, то се взема допирателната към $-P_1$.

Стойността на $m$ не се променя при смяна на местата на $P_1$ и $P_2$, следователно и $x$. Ако преобразуваме $y$ от (10.4) във вида

$$y = -mx + \frac{x_2y_1 - x_1y_2}{x_1 - x_2}$$

забелязваме, че и $y$ е инвариантно относно пермутация на $P_1$ и $P_2$. Следователно така дефинираното събиране е комутативно. Проверява се, че са в сила и останалите аксиоми за адитивна абелева група.

Да отбележим, че горното правило за събиране не дефинира сума на точки от вида $(x, y_1)$ и $(x, y_2)$ при $y_1 \neq \pm y_2$. Но наличието такива точки в $\mathcal{E}(\mathbb{Z}_p)$ означава, че $y_1^2 \equiv y_2^2 \pmod{p}$, т.е. поне едно от $p \mid (y_1 - y_2)$ и $p \mid (y_1 + y_2)$ е в сила, което е невъзможно.

Получаването на нула в знаменател при изчисляване на $m$ означава, че $P_1 + P_2 = \mathcal{O}$. В частност при $y = 0$, $P = -P$, т.е. $P + P = \mathcal{O}$.

С $kP$ ще означаваме както обикновено $k$-кратното на точка $P$, т.е. за естествено число $k$:

$$kP \stackrel{\text{def}}{=} \underbrace{P + P + \cdots + P}_{k}.$$

**Пример 10.1.1** Нека $\mathbb{F} = \mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$. Да намерим точките на $\mathcal{E}(\mathbb{Z}_7)$ зададена с уравнението

$$y^2z = x^3 - 2xz^2 + 3z^3.$$

Кривата се състои от $\mathcal{O} = (0 : 1 : 0)$ и точките $(x : y : 1)$ за които двойките $(x, y) \in \mathbb{F}_7^2$ удовлетворяващи $y^2 = x^3 - 2x + 3 = u(x)$. Точни квадрати в $\mathbb{Z}_7$ са $0,\ 1 = (\pm 1)^2,\ 4 = (\pm 2)^2,\ 2 = (\pm 3)^2$. Непосредствената проверка показва, че стойностите на $x$ за които $u(x)$ е точен квадрат са $\ u(1) = 2,\ u(2) = 0,\ u(6) = 4$.

Следователно

$$\mathcal{E}(\mathbb{Z}_7) = \{(0 : 1 : 0),\ (1 : \pm 3 : 1),\ (2 : 0 : 1),\ (6 : \pm 2 : 1)\}$$

Нека $P = (1 : 3 : 1)$. Тогава за $2P$ имаме $m = (3.1 - 2)/2.1 = 1/6 = 6$ в $\mathbb{Z}_7$ и следователно

$$x = -2 + 6^2 = -2 + 1 = 6, \qquad y = -3 + 6(1 - 6) = 2, \text{ т.е.} \quad 2P = (6 : 2 : 1).$$

Аналогично получаваме

$$3P = (2 : 0 : 1) = -3P,\ 4P = (6 : 5 : 1),\ 5P = (1 : 4 : 1) = -P,\ 6P = \mathcal{O}.$$

Следователно $\mathcal{E} \cong Z_6 \cong Z_2 \times Z_3$.

При дефинираните по-горе сумиране и удвояване на точки се налага намиране на обратен елемент в $\mathbb{Z}_p$ (т.е. по модул $p$), което е относително трудоемка операция. Затова в реализациите се използват други форми на кривите и други формули вместо (10.4), с което обръщането се избягва. Такива са формата на Монтгомери и съответните ѝ формули.

**Представяне на Монтгомери**

$$BY^2 = X^3 + AX^2 + X, \qquad BY^2Z = X^3 + AX^2Z + XZ^2, \tag{10.5}$$

където $A, B \in \mathbb{Z}_N$, такива че $B(A^2 - 4)$ е обратим елемент в $\mathbb{F}$

Операциите при тази крива се дават с

$$m = \begin{cases} \dfrac{Y_1 - Y_2}{X_1 - X_2}, & \text{ако } P_1 \neq P_2 \\ \dfrac{3X_1^2 + 2AX_1 + 1}{2BY_1}, & \text{ако } P_1 = P_2 \end{cases}$$

Горните формули също изискват намиране на обратен елемент (даже са малко по-сложни), но могат да се трансформират в еквивалентна форма, при която няма изчисляване на обратен елемент. Нека $P$ е точка от кривата с проективни координати $(X_1 : Y_1 : Z_1)$, а с $(X_n : Y_n : Z_n)$ да означим координатите на точката $nP$, $n$ естествено число.

**Удвояване:**

$$c = \frac{A+2}{4};\ s = (X_n + Z_n)^2,\ r = (X_n - Z_n)^2,\ t = c(s - r) + r,$$

$$X_{2n} = sr, \quad Z_{2n} = (s - r)t.$$

**Събиране:**

$$u = (X_m + Z_m)(X_n - Z_n),\ v = (X_m - Z_m)(X_n + Z_n),\ w = (u + v)^2,\ t = (u - v)^2,$$

$$X_{m+n} = Z_{m-n}w, \qquad Z_{m+n} = X_{m-n}t.$$

(за пресмятането на $(m + n)P$ ни трябват $(m - n)P,\ nP,\ mP.$ )

Интересното е, че не се използва $Y$ координатата. При това

$$-(X : Y : Z) = (X : -Y : Z),$$

т.е. противоположните точки не се различават в $X$ и $Z$ координатите.

Следната трансформация преобразува **формата на Монгомери в редуцирана форма на Вайерщрас**

Делим на $B^3$ и полагаме $x = \frac{X}{B} + \frac{A}{3B}$, $y = \frac{Y}{B}$; $\quad a = \frac{3-A^2}{3B^2}$, $b = \frac{2A^3-9A}{27B^3}$.

Горното преобразувание, обаче, не е обратимо, т.е. не всяко уравнение от Вайещрасов тип може да се получи от уравнение на Монгомери чрез горната трансформация. Такъв първообраз от тип Монгомери съществува тогава и само тогава, когато уравнението

$$Du^3 - 3au - 1 = 0, \qquad D = 27b^2 + 4a^3, \tag{10.6}$$

има решение в $\mathbb{F}$, което е точен квадрат ($u = B^2$).

Наистина, от

$$27bB^3 = A(2A^2 - 9) \quad \text{и} \quad A^2 = 3 - 3aB^2$$

получаваме $9B^3 = A(-1 - 2aB^2)$. Следователно

$$A = -\frac{9B^3}{1 + 2aB^2}.$$

В такъв случай

$$3(1 - aB^2) = \frac{81b^2B^6}{(1 + 2aB^2)^2},$$

откъдето получаваме

$$27b^2B^6 = (1 - aB^2)(1 + 4aB^2 + 4a^2B^4), \qquad \text{т.е.} \qquad (27b^2 + 4a^3)B^6 - 3aB^2 - 1 = 0.$$

Например над $\mathbb{Z}_7$ само следните криви имат съответни криви във с форма на Монгомери

| Вайерщрас | Монтгомери | $\lvert E(\mathbb{Z}_7)\rvert$ |
|---|---|---|
| $y^2 = x^3 - x + 1$ | $3Y^2 = X^3 - 3X^2 + X$<br>$4Y^2 = X^3 + 3X^2 + X$ | 4 |
| $y^2 = x^3 - x - 1$ | $3Y^2 = X^3 + 3X^2 + X$<br>$4Y^2 = X^3 + 4X^2 + X$ | 11 |
| $y^2 = x^3 - 2x + 1$ | $Y^2 = X^3 + 3X^2 + X$<br>$-Y^2 = X^3 + 4X^2 + X$ | 11 |
| $y^2 = x^3 - 2x - 1$ | $Y^2 = X^3 + 4X^2 + X$<br>$-Y^2 = X^3 + 3X^2 + X$ | 3 |

**Пример 10.1.2** Крива 192r1 над $\mathbb{Z}_p$

$$\mathcal{E}: \; y^2 = x^3 - 3x + b, \tag{10.7}$$

където

$$\begin{aligned} p &= 6277101735386680763835789423207666416083908700390324961279 \\ b &= 64210519E59C80E70FA7E9AB72243049FEB8DEECC146B9B1 \\ &= 2455155546008943817740293915197451784769108058161191238065. \end{aligned}$$

Броят на точките е простото число

$$n = 6277101735386680763835789423176059013767194773182842284081,$$

т.е. формират циклична група. За начална точка се взема $G = (G_x, G_y)$, където

$$\begin{aligned}
G_x &= 188DA80E\ B03090F6\ 7CBF20EB\ 43A18800\ F4FF0AFD\ 82FF1012 \\
&= 602046282375688656758213480587526111916698976636884684818 \\
G_y &= 07192B95\ FFC8DA78\ 631011ED\ 6B24CDD5\ 73F977A1\ 1E794811 \\
&= 174050332293622031404857552280219410364023488927386650641.
\end{aligned}$$

Следните формули оперират с $(X : Y : Z)$, където $x = X/Z, \quad y = Y/Z$. След изчисляване на $kG$ се преминава към афинни координати чрез $x = XZ^{-1} \pmod p$ и $y = YZ^{-1} \pmod p$, т.е само с едно обръщане на последното $Z$.

**Събиране на** $(X1 : Y1 : Z1)$ **и** $(X2 : Y2 : Z2)$**. Резултат** $(X3 : Y3 : Z3)$:

$$\begin{aligned}
PX &= X1 * Z2 \\
PY &= Y1 * Z2 \\
PZ &= Z1 * Z2 \\
u &= Y2 * Z1 - PY \\
uu &= u^2 \\
v &= X2 * Z1 - PX \\
vv &= v^2 \\
vvv &= v * vv \\
R &= vv * PX \\
A &= uu * PZ - vvv - 2 * R \\
X3 &= v * A \\
Y3 &= u * (R - A) - vvv * PY \\
Z3 &= vvv * PZ
\end{aligned}$$

**Удвояване на** $(X1 : Y1 : Z1)$**. Резултат** $(X : Y : Z)$:

$$\begin{aligned}
w &= 3 * (X1 - Z1) * (X1 + Z1) \\
s &= 2 * Y1 * Z1 \\
R &= Y1 * s \\
RR &= R^2 \\
B &= 2 * X1 * R \\
h &= w^2 - 2 * B \\
X &= h * s \\
Y &= w * (B - h) - 2 * RR \\
ss &= s^2 \\
Z &= s * ss
\end{aligned}$$

## 10.2 Криптографски протоколи основани на елиптични криви

Нека сме фиксирали криптосистема състояща се от елиптична крива $\mathcal{E}$ над крайното поле $F$ и с базисна точка $G$. (Параметрите им ще дискутираме по-късно.)

Нека даден потребител $U$ притежава

• секретен ключ $d$ - цяло число, съхранява се на смарт-картата;

• публичен ключ точка $Q = dG$ с координати $(Q_x, Q_y)$, съхранява се на защитен сървер.

Процедурата ще се състои в следното:

**Защитен сървер**:

1) Генерира случайно число $k$ и веднага изчислява $kG = (k_x, k_y)$ и $kQ = (K_x, K_y)$

2) Генерира случайно число "съобщиние-ключ" $m = (m_x \mid m_y) \to (m_x, m_y)$ и изчислява $u = m + kQ = (m_x + K_x, m_y + K_y)$.

3) Изпраща на $U$ двойката $\{u, kG\}$.

**Потребител** $U$:

Изчислява $u - d(kG) = m + k(dG) - dkG = m$.

Числата $k$ и $m$ не се съхраняват и след генериране веднага участват в операции. Смарт-картата трябва да съхрани $kG$ и $u$. Ако броят на елементите на $F$ е число с дължина $L$ бита, то $kG$ и $u$ се записват с по $2L$-битови числа. Следователно смарт-картата трябва да съхрани две такива числа след получаването им за да ги обработва. Може да се работи само с едната координата и тогава ще трябва да се съхранят $3L$ бита.

Операциите, които трябва да извърши потребителят са умножение на точка с цяло число. Както при повдигане на степен, $kP$ може да се представи като последователност от умножение на точка по 2 и добавяне на $P$.

Някои стандарти:

http://csrc.nist.gov/groups/ST/toolkit/digital_signatures.html

http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf

http://www.secg.org/index.php?action=secg,docs_secg