Curbe eliptice

0.1 Forma Weierstrass

Fie $\mathbb{K}$ un corp comutativ. De exemplu $\mathbb{K}$ poate fi corpul numerelor reale $\mathbb{R}$, corpul numerelor complexe $\mathbb{C}$, corpul numerelor raţionale $\mathbb{Q}$, unul din corpurile $\mathbb{F}_p$, unde p este un număr prim sau unul din corpurile $\mathbb{F}_{p^k}$, cu $k \geq 1$. Pentru început vom considera doar cazul corpului numerelor reale $\mathbb{R}$. Fie $a, b \in \mathbb{K}$ două elemente din $\mathbb{K}$ şi $f(x) = x^3 + ax + b$ un polinom cu coeficienţi din $\mathbb{K}$. Acest polinom defineşte o curbă (o cubică) peste corpul $\mathbb{K}$:

$$E(\mathbb{K}) = \{(x, y) \in \mathbb{K}^2 : y^2 = f(x)\}.$$

Dorim că polinomul f să definească o curbă netedă (pentru a putea "construi" tangenta în fiecare punct). Pentru aceasta punem condiţia ca polinomul f să nu aibă rădăcini multiple. Reamintim că dacă x_2, x_2, x_3 sunt rădăcinile polinomului cubic f, atunci discriminatul său este

$$\Delta_E = [(x_1 - x_2)(x_2 - x_3)(x_3 - x_1)]^2 = -4a^3 - 27b^2.$$

Demonstraţie: Avem relaţiile lui Viète $x_1+x_2+x_3 = 0$, $x_1x_2+x_2x_3+x_3x_1 = a$ şi $x_1x_2x_3 = -b$. Cum $f'(x) = 3x^2 + a$, avem $f'(x_1) = 3x_1^2 + a = (x_1 - x_2)(x_1 - x_3)$, $f'(x_2) = 3x_2^2 + a = (x_2 - x_1)(x_2 - x_3)$ şi $f'(x_3) = 3x_3^2 + a = (x_3 - x_1)(x_3 - x_2)$. Făcând produsul celor trei relaţii şi utilizând relaţiile lui *Viète* obţinem expresia discriminantului.

Observaţia 1. *Polinomul f nu are rădăcini multiple dacă şi numai dacă $\Delta_E \neq 0$.*

Definiţia 1. *Fie $F(x, y) = x^3 + ax + b - y^2$ şi $P(x_0, y_0) \in E(\mathbb{K})$ un punct pe curbă. Punctul se numeşte singular dacă*

$$\frac{\partial F}{\partial x}(x_0, y_0) = \frac{\partial F}{\partial y}(x_0, y_0) = 0.$$

Observaţia 2. *O curbă $E(\mathbb{K})$ cu $\Delta_E \neq 0$ nu are puncte singulare. Într-adevăr, să presupunem că există un punct $P(x_0, y_0)$ pe curbă, în care derivatele parţiale ale lui f se anulează. Atunci avem $3x_0^2 + a = 0$ şi $-2y_0 = 0$. Atunci $y_0 = 0$ şi $x_0^3 + ax_0 + b = 0$, de unde rezultă $b = 2x_0^3$ şi $a = -3x_0^2$ şi deci $4a^3 + 27b^2 = 0$, contradicţie.*

Exerciţiul 1. *Următoarele curbe au $\Delta_E = 0$ (au puncte singulare):*

1. *Curba $y^2 = x^3 - 3x + 2 = (x - 1)^2(x + 2)$ are un nod în punctul de coordonate $(1, 0)$.*
2. *Curba $y^2 = x^3$ are un punct de inflexiune (vârf) în punctul de coordonate $(0, 0)$.*
3. *Curba $y^2 = x^3 - 3x - 2 = (x + 1)^2(x - 2)$ are un punct izolat în $(-1, 0)$.*

Exerciţiul 2. *Următoarele curbe au $\Delta_E \neq 0$ (nu au puncte singulare):*

1. *$y^2 = x^3 - 1$.*
2. *$y^2 = x^3 - 3x + 3$.*
3. *$y^2 = x^3 - 4x$.*

0.2 Legea de grup

Una din cele mai importante proprietăţi ale curbelor de mai sus este aceea că dacă se adaugă încă un punct special, noua mulţime de puncte admite o structură de grup comutativ.

Fie $P_1(x_1, y_1)$ şi $P_2(x_2, y_2)$ două puncte distincte pe curba $E(\mathbb{R})$. Considerăm dreapta $d = P_1P_2$, având ecuaţia $y = y_1 + m(x - x_1)$, unde $m = \frac{y_2 - y_1}{x_2 - x_1}$ este panta dreptei. Dreapta d intersectează curba $E(\mathbb{R})$ într-un al treilea punct P_3'. Coordonatele lui P_3' se găsesc rezolvând sistemul

$$\begin{cases} y &= y_1 + m(x - x_1) \\ y^2 &= x^3 + ax + b \end{cases}$$

Dacă înlocuim prima ecuaţie în cea de-a doua obţinem ecuaţia cubică în x

$$x^3 + ax + b - (y_1 + m(x - x_1))^2 = 0.$$

Cele trei soluţii ale ecuaţiei de mai sus corespund celor trei puncte de intersecţie ale dreptei d cu $E(\mathbb{R})$. Dar două din cele trei puncte sunt chiar $P_1(x_1, y_1)$ şi $P_2(x_2, y_2)$ şi deci două dintre cele trei soluţii sunt x_1 şi x_2. Folosind prima relaţie a lui Viète, se obţine cu uşurinţă a treia soluţie $x_3 = m^2 - x_1 - x_2$ şi deci $y_3 = y_1 + m(x_3 - x_1)$. Am arătat astfel că dreapta d intersectează curba în trei puncte. Definim $P_1 + P_2 = P_3$, unde P_3 are coordonatele $(x_3, -y_3)$, adică P_3 este simetricul lui P_3' faţă de axa Ox.

Apar însă în definiţia de mai sus cel puţin două probleme.

1. Dacă dreapta d este verticală, adică $x_2 = x_1$ şi $y_1 = -y_2$, cine este al treilea punct de intersecţie al dreptei d cu curba $E(\mathbb{R})$.

2. Cum definim suma a două puncte dacă P_1 coincide cu P_2?

Cum se pot rezolva cele două probleme?

1. Pentru prima problemă se mai adaugă curbei încă un punct pe care-l notăm cu ∞ şi se numeşte punctul de la infinit (vom explica ceva mai târziu cine este acest punct). Aşadar, dacă P_1 şi P_2 sunt distincte, dar P_1 are coordonatele (x_1, y_1) iar P_2 coordonatele $(x_1, -y_1)$, definim adunarea lor prin $P_1 + P_2 = \infty$.

2. Pentru problema a doua, dacă $P_1 = P_2$, în loc să considerăm dreapta determinată de cele două puncte ca mai sus, vom considera tangenta în punctul P_1 la curba $E(\mathbb{R})$. De aceea legea definită astfel se mai numeşte şi "coardă-tangentă".

Dacă derivăm implicit ecuaţia $y^2 = x^3 + ax + b$ obţinem $2y\frac{dy}{dx} = 3x^2 + a$ şi deci panta tangentei în punctul $P_1(x_1, y_1)$ este $m = \frac{3x_1^2+a}{2y_1}$ iar ecuaţia tangentei este $y = y_1 + m(x - x_1)$. Ca mai sus, al treilea punct al intersecţiei tangentei în P_1 la curbă (P_1 este punct dublu) are coordonatele $x_3 = m^2 - 2x_1$ şi $y_3 = y_1 + m(x_3 - x_1)$. Definim acum $P_1 + P_1 = 2P_1$ ca fiind punctul punctul P_3, de coordonate $(x_3, -y_3)$.

Calculul de mai sus nu funcţionează dacă $y_1 = 0$. În acest caz tangenta în P_1 este verticală. Definim în acest caz $P_1 + P_1 = \infty$.

Definiţia 2. *Fie $\mathbb{K}$ un corp oarecare având caracteristica diferită de 2 sau 3 şi fie $f = x^3 + ax + b \in \mathbb{K}[X]$ un polinom cu coeficienţi în $\mathbb{K}$ fără rădăcini multiple. Se numeşte curbă eliptică peste corpul $\mathbb{K}$ mulţimea punctelor*

$$E(\mathbb{K}) = \{(x, y) \in \mathbb{K} \times \mathbb{K} : y^2 = x^3 + ax + b\} \cup \{\infty\}$$

Legea de grup Fie $E(\mathbb{K})$ o curbă eliptică definită de ecuaţia $y^2 = x^3 + ax + b$ şi $P_1(x_1, x_2)$, $P_2(x_2, y_2)$ două puncte pe curbă diferite de ∞. Definim $P_1 + P_2 = P_3(x_3, y_3)$ prin:

1. Dacă $x_1 \neq x_2$ atunci
$$x_3 = m^2 - x_1 - x_2,\ y_3 = -y_1 - m(x_3 - x_1), \text{ unde } m = \tfrac{y_2 - y_1}{x_2 - x_1}.$$

2. Dacă $x_1 = x_2$ dar $y_1 \neq y_2$, atunci $P_1 + P_2 = \infty$.

3. Dacă $P_1 = P_2$ şi $y_1 \neq 0$, atunci
$$x_3 = m^2 - 2x_1,\ y_3 = -y_1 - m(x_3 - x_1), \text{ unde } m = \tfrac{3x_1^2 + a}{2y_1}.$$

4. Dacă $P_1 = P_2$ şi $y_1 = 0$, atunci $P_1 + P_1 = 2P_1 = \infty$.

Mai mult, pentru orice punct P de pe curbă definim $P + \infty = \infty$.

Formulele de mai sus rămân valabile şi în cazul unui corp oarecare având caracteristica diferită de 2 sau 3.

Teorema 1. *Legea de adunare a punctelor unei curbe eliptice $E(\mathbb{K})$ satisface următoarele proprietăţi:*

1. *Dacă punctele $P, Q, R \in E(\mathbb{K})$ sunt pe o dreaptă, atunci $(P + Q) + R = \infty$.*

2. *(comutativitatea) $P + Q = Q + P$ pentru orice două puncte $P, Q \in E(\mathbb{K})$.*

3. *(existenţa elementului neutru) Pentru orice $P \in E(\mathbb{K})$ avem $P + \infty = P$.*

4. *(existenţa inversului) Pentru orice $P \in E(\mathbb{K})$ există $P' = -P \in E(\mathbb{K})$ astfel încât $P + P' = \infty$.*

5. *(asociativitatea) $(P + Q) + R = P + (Q + R)$ pentru orice trei puncte $P, Q, R \in E(\mathbb{K})$.*

Cu alte cuvinte, punctele unei curbe eliptice formează un grup abelian având element neutru punctul de la infinit ∞.

Demonstraţie: Vom nota cu O punctul de la infinit.

(1) Considerând dreapta $l = PQ$, aceasta intersectează curba E în punctele $\{P, Q, R\}$. Pe de altă parte, dreapta OR intersectează curba în punctele $\{O, R, R'\}$. Evident $R' = P + Q$. Adunâm acum punctele R' şi R. Dreapta $R'R$ intesectează curba a treia oară în punctul O. Se duce acum tangenta la curbă în punctul O care va intersecta a treia oară curba tot în punctul O (punctul de la infinit este un punct triplu, iar tangenta în O este dreapta punctelor de la infinit). Se obţine în final că $R' + R = O$.

(2) Comutativitatea este evidentă pentru că dreapta PQ coincide cu dreapta QP.

(3) Fie P un punct oarecare pe curbă. Dacă dreapta PO intersectează curba în punctul Q, atunci al treilea punct de intersecţie al dreptei OQ cu $E(\mathbb{K})$ va fi evident P şi deci $P + O = P$.

(4) Fie P un punct oarecare pe curbă şi fie P' al treilea punct de interesecţie al dreptei PO cu E. Folosind punctul (1), avem $(P + P') + O = O$, adică $P + P' = O$.

(5) Demonstrarea asociativităţii nu mai este aşa de simplă şi va fi discutată în paragraful 0.4.

0.3 Planul proiectiv şi punctul de la infinit

Planul proiectiv ne va permite să interpretăm punctul de la infinit al unei curbe eliptice.

Fie $\mathbb{K}$ un corp comutativ. Planul proiectiv $\mathbb{P}^2(\mathbb{K})$ peste corpul $\mathbb{K}$ este dat de clasele de echivalenţă ale tripletelor $(x, y, z) \in \mathbb{K}^3$, astfel încât cel puţin una din coordonatele x, y, z este nenulă. Două triplete (x_1, y_1, z_1) şi (x_2, y_2, z_2) sunt echivalente dacă există un element nenul $\lambda \in \mathbb{K}$ astfel încât $(x_1, y_1, z_1) = \lambda(x_2, y_2, z_2)$. Vom nota cu $[x : y : z]$ clasa de echivalenţă a lui (x, y, z)

Dacă $[x : y : z]$ este un punct din planul proiectiv cu $z \neq 0$, atunci $[x : y : z] = [x/z : y/z : 1]$. Acestea sunt punctele "finite" din $\mathbb{P}^2(\mathbb{K})$. Dacă $z = 0$ nu mai putem împărţi prin z si punctele de acest tip se vor numi "punctele de la infinit". Vom vedea că punctul de la infinit al unei curbe eliptice se identifică cu unul din aceste puncte.

Notăm cu $\mathbb{A}^2(\mathbb{K})$ planul afin $\{(x, y) \in \mathbb{K} \times \mathbb{K}\}$ peste corpul $\mathbb{K}$. Există o scufundare naturală $\mathbb{A}^2(\mathbb{K}) \hookrightarrow \mathbb{P}^2(\mathbb{K})$ a lui $\mathbb{A}^2(\mathbb{K})$ în $\mathbb{P}^2(\mathbb{K})$ dată de $(x, y) \mapsto [x : y : 1]$. În acest fel, planul afin $\mathbb{A}^2(\mathbb{K})$ se identifică cu punctele finite din planul proiectiv $\mathbb{P}^2(\mathbb{K})$. Adăugarea punctelor de la infinit pentru a obţine planul proiectiv se numeşte compactificarea planului afin.

Considerăm din nou polinomul $f(x, y) = x^3 + ax + b - y^2$. Corespondentul său omogen în planul proiectiv este polinomul $F(x, y, z) = z^3 f(\frac{x}{z}, \frac{y}{z}) = x^3 + axz^2 + bz^3 - y^2 z$. Aşadar, zerourile acestui polinom sunt punctele curbei noastre reprezentate în planul proiectiv. Pentru a vedea care sunt punctele de la infinit care aparţin curbei E, intersectăm curba cu dreapta punctelor de la infinit, adică dreapta de ecuaţie $z = 0$. Obţinem $x = 0$ şi deci y poate fi orice număr real nenul. Am găsit că punctul de la infinit al al curbei E este $[0 : 1 : 0]$. Se poate vedea uşor că acest punct se află pe orice dreaptă verticală. Acesta este punctul ∞ adăugat mai sus.

0.4 Asociativitatea legii de adunare

Am folosit de mai multe ori până acum faptul că o dreaptă interesectează o curbă eliptică în exact trei puncte. Acest rezultat este o consecinţă a Teoremei următoare:

Teorema 2. *(**Bezout**) Dacă C şi D sunt două curbe proiective plane de grade c şi respectiv d, presupunând că C şi D nu au o infinitate de puncte în comun (nu au componente comune), atunci card$(C \cap D) \leq c \cdot d$.*

Dacă se lucrează într-un corp algebric închis, iar punctele de intersecţie sunt numărate cu "multiplicităţile" lor, avem egalitatea $\sum_{P \in C \cap D} I_P(C, D) = c \cdot d$, unde $I_P(C, D)$ este multiplicitatea interescţiei curbelor C şi D în punctul P.

Lema 1. *Fie $P_1, \ldots, P_8$ opt puncte distincte din planul proiectiv $\mathbb{P}(\mathbb{K})$, astfel încât oricare patru nu se află pe o aceeaşi dreaptă şi oricare şapte nu se află pe o aceeaşi conică. Atunci există un al nouălea punct Q astfel încât orice cubică care trece prin punctele $P_1, \ldots, P_8$, conţine şi punctul Q.*

Folosind această lemă suntem în măsură să demonstrăm asociativitatea legii de adunare a punctelor unei curbe eliptice. Trebuie să arătăm că $(A+B)+C = A+(B+C)$, pentru orice trei puncte A, B, C de pe curbă. De fapt e suficient să arătăm că $-((A+B)+C) = -(A+(B+C))$.

Considerăm acum dreptele l_1, l_2, l_3 şi m_1, m_2, m_3 determinate în felul următor:

l_1	determinată de	A,	B,	$-(A+B)$
l_2	determinată de	$A+B$,	C,	$-((A+B)+C)$
l_3	determinată de	O,	$-(B+C)$,	$B+C$
m_1	determinată de	O,	$-(A+B)$,	$A+B$
m_2	determinată de	B,	C,	$-(B+C)$
m_3	determinată de	A,	$B+C$,	$-(A+(B+C))$.

Ştim că punctul $-((A+B)+C)$ se află pe dreapta l_2 iar punctul $-(A+(B+C))$ pe dreapta m_3 şi ne propunem să arătăm că cele două puncte coincid cu punctul $\{D\} = l_2 \cap m_3$.

Considerăm acum cubicele $l_1 l_2 l_3 = 0$ şi $m_1 m_2 m_3 = 0$. Din Teorema lui Bezout, cele două cubice se intersectează în nouă puncte. Pe de altă parte, din construcţie, ştim că aceste cubice trec prin punctele $O, A, B, C, A+B, -(A+B), B+C$ şi $-(B+C)$. Vom face demonstraţia în cazul când aceste 8 puncte sunt distincte. Fie D cel de-al nouălea punct. Presupunând că sunt îndeplinite condiţiile, Lema 1 ne spune că orice altă cubică ce trece prin cele 8 puncte de mai sus, va trece şi prin punctul D. Deoarece curba eliptică E conţine cele 8 puncte, va trece şi ea prin punctul D.

Astfel, interesecţia curbelor E şi $m_1 m_2 m_3$ va conţine punctele $O, A, B, C, A+B, -(A+B), B+C, -(B+C), -(A+(B+C))$ şi D. Dar cum această interescţie trebuie să conţină doar nouă puncte, două dintre acestea trebuie să fie egale. Singura variantă posibilă este $D = -(A+(B+C))$. Analog, considerând intersecţia $l_1 l_2 l_3 \cap E$, se obţine $D = -((A+B)+C)$, şi deci asociativitatea este demonstrată.

Observaţia 3. *Dacă suntem atenţi la multiplicităţi, putem adapta demostraţia şi la cazul când cele* 8 *puncte nu sunt neapărat distincte, dar impunând condiţia ca* $l_1 l_2 l_3$ *şi* $m_1 m_2 m_3$ *să fie cubice distincte.*

Observaţia 4. *Să remarcăm că dacă curba* E *este ireductibilă (cum este cazul unei curbe eliptice), dacă ne uităm la punctele* $O, A, B, C, A+B, -(A+B), B+C$ *şi* $-(B+C)$*, oricare patru nu sunt coliniare şi oricare şapte nu sunt pe o conică. Într-adevăr, dacă ar exista patru puncte din cele de mai sus pe o aceeaşi dreaptă* d*, ar însemna că* $card(D \cap E) \geq 4$*, ceea ce ar contrazice Teorema lui Bezout (o dreaptă este o curbă de grad* 1 *pe când o curbă eliptică o curbă de grad* 3*). Analog se verifică şi condiţia legată de conică, aceasta fiind o curbă de grad* 2*.*

Ne propunem acum să dăm o schiţă de demonstraţie a lemei (1).

Demonstraţie: (Demonstraţia Lemei (1))

În primul rând, nu este greu de văzut că spaţiul cubicelor proiective admite o structură de spaţiu vectorial de dimensiune 10. Pe de altă parte spaţiul cubicelor ce trec prin 8 puncte date formează un subspaţiu vectorial de dimensiune 2, aceasta cu condiţia ca cele 8 ecuaţii liniare implicate să fie independente. Acest lucru se întâmplă deoarece oricare 4 puncte nu sunt coliniare şi oricare 7 nu sunt pe o conică (R.Hartshone,Algebraic Geometry, Springer, 1977, pagina 400). Acest spaţiu 2-dimensional va fi generat de două cubice F_1 şi F_2. Aceasta înseamnă că cele opt puncte $P_1, \ldots, P_8$ se află pe F_1 şi F_2 şi orice altă cubică G, ce conţine cele opt puncte, se poate exprima prin $G = \mu F_1 + \nu F_2$. Din Teorema lui Bezout, intersecţia $F_1 \cap F_2$ are exact 9 puncte. Aşadar, există un al nouălea punct Q pe cele două cubice, adică $F_1(Q) = 0$ şi $F_2(Q) = 0$. Atunci $G(Q) = \mu F_1(Q) + \nu F_2(Q) = 0$, adică, există un al nouălea punct Q ce se găseşte pe orice cubică ce conţine cele opt puncte $P_1, \ldots, P_8$.

0.5 Structura grupului

Exemplul 1. *Fie curba eliptică* $E(\mathbb{F}_5)$ *definită de polinomul* $y^2 = x^3 + 1$*. Să remarcăm că pătratele în* $\mathbb{F}_5$ *sunt* $0 = 0^2$*,* $1 = 1^2 = 4^2$ *şi* $4 = 2^2 = 3^2$ *şi deci doar* 1 *şi* 4 *sunt resturi pătratice. Atunci elementele lui* $E(\mathbb{F}_5)$ *sunt date de următorul tabel*

x	x^3+1	$y=\pm\sqrt{x^3+1}$	*puncte*
0	*1*	$\pm 1 = 1, 4$	*(0,1),(0,4)*
1	*2*	-	-
2	*4*	$\pm 2 = 2, 3$	*(2,2),(2,3)*
3	*3*	-	-
4	*0*	*0*	*(4,0)*

Evident la punctele listate mai sus se adaugă şi punctul de la infinit. Deci cardinalul lui $E(\mathbb{F}_5)$ *este 6. Fie* $G = (2, 3)$. *Calculăm* $2G$, *folosind formulele explicite ale legii de grup în care* $a = 0$ *şi* $b = 1$. *Cum panta tangentei la curbă în punctul* G *este* $m = \dfrac{3x_1^2}{2y_1} = 2$, *rezultă* $x_3 = m^2 - 2x_1 = 0$ *şi* $y_3 = -y_1 - m(x_3 - x_1) = 1$, *de unde rezultă atunci* $2G = (0, 1)$. *Calculăm acum* $3G = 2G + G$. *Panta dreptei ce trece prin punctele* $2G$ *şi* G *este* $m = \dfrac{y_2 - y_1}{x_2 - x_1} = 1$ *şi deci* $x_3 = m^2 - x_1 - x_2 = 4$ *şi* $y_3 = -y_1 - m(x_3 - x_1) = 0$. *Obţinem astfel* $3G = (4, 0)$. *Pentru calculul lui* $4G = 2G + 2G$ *se folosesc formulele tangentei având panta* $m = 0$. *Se obţine* $4G = (0, 4)$. *Cum* $4G = -2G$, *rezultă* $6G = O$. *Este clar că* $5G = (2, 2)$. *Am arătat astfel că* $E(\mathbb{F}_5)$ *este un grup ciclic, izomorf cu grupul aditiv* $\mathbb{Z}_6$, *generat de punctul* G, *care este evident element de ordin 6.*▪

Exemplul 2. *Considerăm acum curba eliptică* $E(\mathbb{F}_7)$ *dată de ecuaţia* $y^2 = x^3+1$. *Avem* $0^2 = 0$, $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$ *şi* $(\pm 3)^2 = 2$. *Atunci elementele lui* $E(\mathbb{F}_5)$ *sunt date de următorul tabel*

x	x^3+1	$y=\pm\sqrt{x^3+1}$	*puncte*
0	*1*	± 1	*(0,1),(0,6)*
1	*2*	± 3	*(1,3),(1,4)*
2	*2*	± 3	*(2,3),(2,4)*
3	*0*	*0*	*(3,0)*
4	*2*	± 3	*(4,3),(4,4)*
5	*0*	*0*	*(5,0)*
6	*0*	*0*	*(6,0)*
			O

Deci $E(\mathbb{F}_7)$ *are 12 puncte. Grupul nu este ciclic, în schimb dacă notăm* $Q = (1, 3)$ *şi* $R = (5, 0)$ *atunci vom avea* $2Q = (0, 1)$, $3Q = (3, 0)$, $4Q = (0, 6)$, $5Q = (1, 4)$, $6Q = O$, $2R = O$, $Q + R = (2, 3)$, $2Q + R = (4, 4)$, $3Q + R = (6, 0)$, $4Q + R = ((4, 3)$ *şi* $5Q + R = (2, 4)$. *Deci toate punctele sunt de forma* $nQ + mR$ *cu* $n \in \mathbb{Z}/6\mathbb{Z}$ *şi* $m \in \mathbb{Z}/2\mathbb{Z}$. *În acest caz grupul nu mai este ciclic dar este izomorf cu suma directă a două grupuri ciclice* $\mathbb{Z}_2 \oplus \mathbb{Z}_6$.▪

În general este adevărată următoarea teoremă:

Teorema 3. *Fie* $E(\mathbb{F}_q)$ *o curbă eliptică peste un corp finit* $\mathbb{F}_q$. *Atunci grupul* $E(\mathbb{F}_q)$ *este izomorf cu* $\mathbb{Z}_n$ *pentru un anumit întreg* $n \geq 1$, *sau este izomorf cu grupul* $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ *unde* $n_1, n_2 \geq 1$ *sunt întregi astfel încât* n_1 *divide pe* n_2 *şi* n_1 *divide* $q - 1$.

Corolarul 1. *Dacă ordinul grupului* $E(\mathbb{F}_q)$ *este liber de pătrate atunci* $E(\mathbb{F}_q)$ *este grup ciclic.*

0.6 Ordinul grupului

Fie p un număr prim şi $E(\mathbb{F}_p)$ o curbă eliptică peste un corp finit $\mathbb{F}_p$, dată de ecuaţia $y^2 = x^3 + ax + b$. Dacă vrem să listăm toate punctele curbei, încercăm toate valorile $x \in \mathbb{F}_p$ şi găsim rădăcinile pătrate y ale lui $x^3 + ax + b$ (dacă ecestea există). Această procedură stă la baza unui algoritm simplu de numărare a punctelor unei curbe eliptice.

Propoziţia 1. *(Metoda Lang-Trotter) Fie* $p \neq 2, 3$ *un număr prim şi* $E(\mathbb{F}_p)$ *o curbă eliptică, peste corpul* $\mathbb{F}_p$, *definită de ecuaţia* $y^2 = x^3 + ax + b = f(x)$. *Atunci numărul de puncte al curbei eliptice* $E(\mathbb{F}_p)$ *este*

$$card\ E(\mathbb{F}_p) = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{f(x)}{p} \right).$$

Demonstraţie:

Fixăm $x_0 \in \mathbb{F}_p$ şi fie $f(x_0) = x_0^3 + ax_0 + b$. Distingem trei cazuri:

1. Dacă $f(x_0)$ este rest pătratic modulo p atunci numărul de puncte $(x, y) \in E(\mathbb{F}_p)$, având prima coordonată x_0 este $2 = 1 + \left(\frac{f(x)}{p}\right)$, pentru că simbolul lui Legedre $\left(\frac{f(x)}{p}\right)$ este 1.

2. Dacă $f(x_0)$ nu este rest pătratic modulo p atunci numărul de puncte $(x, y) \in E(\mathbb{F}_p)$, având prima coordonată x_0 este $0 = 1 + \left(\frac{f(x)}{p}\right)$, pentru că simbolul lui Legedre $\left(\frac{f(x)}{p}\right)$ este -1.

3. Dacă $f(x_0) \equiv 0 \pmod{p}$ atunci numărul de puncte $(x, y) \in E(\mathbb{F}_p)$, având prima coordonată x_0 este $1 = 1 + \left(\frac{f(x)}{p}\right)$ pentru că simbolul lui Legedre $\left(\frac{f(x)}{p}\right)$ este 0.

Adăugând şi punctul de la infinit, obţinem

$$\text{card } E(\mathbb{F}_p) = 1 + \sum_{x \in \mathbb{F}_p} \left(1 + \left(\frac{f(x)}{p}\right)\right) = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{f(x)}{p}\right). \blacksquare$$

Exerciţiul 3. *Fie $E(\mathbb{F}_{11})$ curba eliptică determinată de ecuaţia $y^2 = x^3 + x + 1 = f(x)$. Ne propunem să determinăm numărul punctelor curbei folosind propoziţia de mai sus. În tabelul de mai jos sunt listate toate valorile lui $f(x)$ pentru $x \in \mathbb{F}_{11}$.*

x	0	1	2	3	4	5	6	7	8	9	10
$f(x)$	1	3	0	9	3	10	3	10	4	2	10
$\left(\frac{f(x)}{11}\right)$	1	1	0	1	1	-1	1	-1	1	-1	-1

Am folosit pentru calculul simbolurilor câteva proprietăţi generale ale acestora:

$$\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right), \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

$$\left(\frac{3}{p}\right) = (-1)^{\lfloor \frac{p+1}{6} \rfloor}, \text{ pentru } p \neq 3 \text{ şi } \left(\frac{5}{p}\right) = (-1)^{\lfloor \frac{p-2}{5} \rfloor}, \text{ pentru } p \neq 5.$$

De exemplu $\left(\frac{10}{11}\right) = \left(\frac{2}{11}\right) \cdot \left(\frac{5}{11}\right) = (-1)^{120/8} \cdot (-1)^{\lfloor 9/5 \rfloor} = 1.$

Folosind acum formula din propoziţia precedentă, obţinem card $E(\mathbb{F}_{11}) = 11 + 1 + 2 = 14$.

Să remarcăm că deoarece 14 este liber de pătrate, atunci grupul $E(\mathbb{F}_{11})$ este izomorf cu $\mathbb{Z}_{14}$.

Observaţia 5. *Metoda descrisă mai sus funcţionează pentru valori mici ale lui p (de exemplu $p < 200$), dar este foarte lentă pentru valori foarte mari ale lui p.*

Teorema 1. *(H.Hasse, 1933) Fie $E(\mathbb{F}_q)$ o curbă eliptică peste un corp finit $\mathbb{F}_q$. Atunci*

$$|q + 1 - \text{card} E(\mathbb{F}_q)| < 2\sqrt{q}.$$

Algoritmul lui Shanks: paşi de copil-paşi de uriaş

Se alege mai întâi un punct $P \in E(\mathbb{F}_p)$. Pentru a alege un punct $P = (x, y) \in E(\mathbb{F}_p)$, se rulează valorile $x \in \mathbb{F}_p$ până când $x^3 + ax + b$ este un pătrat perfect în $\mathbb{F}_p$, după care se calculează rădăcinile pătrate y ale lui $x^3 + ax + b$. Se încearcă determinarea ordinului lui P în grupul $E(\mathbb{F}_p)$. Mai întâi se caută un întreg k astfel încât $kP = O$. Fie $N =$ card $E(\mathbb{F}_p)$. Din Teorema lui Lagrange, ştim că $NP = O$. Bineânţeles că nu-l ştim încă pe N, dar ştim că $N \in (p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$. Putem încerca toate valorile lui N din acest interval, care verifică condiţia $NP = O$. Acest lucru se poate face în aproximativ $4\sqrt{p}$ paşi. Totuşi, este posibil să mărim viteza până la aproximativ $4\sqrt[4]{p}$ paşi urmând următorul algoritm:

1. Se alege un întreg m astfel încât $m \geq \sqrt[4]{p}$.

2. Se calculează punctele jP pentru $j = 0, 1, \ldots, m$. Deoarece inversul unui punct se obţine schimbând semnul coordonatei y, avem practic şi coordonatele punctelor $-jP$. Obţinerea acestei liste reprezintă "paşii de copil".

3. Se calculează punctul $Q = (p + 1)P$.

4. Se calculează punctele $Q + k(2mP)$ pentru $k = -m, -(m-1), \ldots, m$ până cand se obţine o egalitate cu unul din cele $2m + 1$ din punctele din lista găsită la pasul (2), adică $Q + k(2mP) = \pm jP$. Aceştia sunt paşi de uriaş.

5. Obţinem $(p+1+2km \mp j)P = O$. Fie $M = p+1+2km \mp j$.

6. Se descompune M în factori primi. Fie $p_1, p_2, \ldots, p_r$ factorii primi distincţi ai lui M.

7. Se calculează $(M/p_i)P$ pentru $i = 1, \ldots, r$. Dacă există un i pentru care $(M/p_i)P = O$, atunci se înlocuieşte M cu M/p_i şi se revine la pasul precedent. Dacă $(M/p_i)P \neq O$ pentru orice i, atunci M este ordinul lui P.

8. Dacă căutăm ordinul grupului $E(F_p)$, se repetă paşii precedenţi cu diferite puncte P alese la întâmplare în $E(F_p)$, până când cel mai mic multiplu comun al ordinelor găsite divide doar un singur număr N din intervalul $(p+1-2\sqrt{p}, p+1+2\sqrt{p})$. Atunci $N = \text{card } E(F_p)$.

Observaţia 6. *Dacă există cel puţin o potrivire de puncte la pasul (4), atunci este clar că se obţine un număr M astfel încât $MP = O$. Să arătăm că există cel puţin o astfel de potrivire.*

Fie a un întreg astfel încât $|a| \leq 2m^2$. Atunci există întregii a_0 şi a_1 cu $-m < a_0 \leq m$ şi $-m \leq a_1 \leq m$ astfel încât $a = a_0 + 2ma_1$. Pentru a arăta acest lucru, fie $a_0 \equiv a \pmod{2m}$, cu $-m < a_0 \leq m$, şi fie $a_1 = (a-a_0)/2m$. Atunci $|a_1| \leq (2m^2+m)/2m < m+1$.

Fie acum $a = p+1-N$, unde N este ordinul grupului. Din Teorema lui Hasse, este clar că $|a| \leq 2m^2$. Atunci există a_0 şi a_1 ca mai înnainte. Fie $k = -a_1$ şi $j = |a_0|$. Atunci $Q + k(2mP) = (p+1-2ma_1)P = (p+1-a+a_0)P = NP + a_0P = a_0P = \pm jP$, şi deci există o potrivire între cele două liste.

Observaţia 7. *Pasul (6) ne dă ordinul lui P. Fie k ordinul punctului P şi M dat de pasul (6), astfel încât $(M/p_i)P \neq O$ pentru orice i. Deoarece $MP = O$ este clar că k divide pe M. Presupunem că $k \neq M$ şi fie p_i un număr prim ce divide pe M/k. Atunci kp_i divide pe M şi deci k divide pe M/p_i. Dar atunci $(M/p_i)P = O$, ceea ce contrazice presupunerrea făcută.*

Exemplul 3. *Fie curba eliptică $E = E(\mathbb{F}_{31})$ de ecuaţie $y^2 = x^3 + x + 13$. Punctele curbei $E(\mathbb{F}_{31})$ sunt listate în tabelul de mai jos.*

k	kP	k	kP	k	kP	k	kP	k	kP	k	kP
1	(9,10)	7	(6,24)	13	(27,10)	19	(5,22)	25	(16,23)	31	(23,12)
2	(18,29)	8	(24,29)	14	(26,21)	20	(26,10)	26	(24,2)	32	(18,2)
3	(23,19)	9	(16,8)	15	(5,9)	21	(27,21)	27	(6,7)	33	(9,21)
4	(4,22)	10	(20,2)	16	(19,3)	22	(28,18)	28	(17,13)	34	O
5	(25,16)	11	(22,22)	17	(10,0)	23	(22,9)	29	(25,15)		
6	(17,18)	12	(28,13)	18	(19,28)	24	(20,29)	30	(4,9)		

Fie $P = (9,10) \in E(\mathbb{Z}_{31})$. Este uşor de văzut că $\sqrt[4]{31}$ este aproximativ 2 şi putem alege $m = 3 > \sqrt[4]{31}$.

Facem lista paşilor mici:

$$-3P = (23,12), -2P = (18,2), -P = (9,21), O,$$
$$P = (9,10), 2P = (18,29),\ 3P = (23,19).$$

Calculăm $Q = (31+1)P = (18,2)$, după care facem lista paşilor mari calculând punctele $Q + k(2mP)$ pentru $k = -3, \ldots, 3$.

$$14P = (26,21), 20P = (26,10), 26P = (24,2), 32P = (18,2)$$
$$38P = (4,22), 44P = (20,2), 50P = (19,3).$$

Ne uităm după potriviri şi observăm că $32P = -2P$, adică $34P = O$. Acesta este numărul M din algoritm.

Se descompune M în factori primi, $M = 2 \cdot 17$.

Se calculează $2P = (18,29) \neq O$ şi $17P = (10,0) \neq O$. Este clar că $M = 34$ este ordinul punctului P.

Ne uităm acum în intervalul $(31+1-2\sqrt{31}, 31+1+2\sqrt{31}) \subset (20,44)$ şi observăm că 34 este singurul număr din interval divizibil cu 34.

Concluzionăm că $N = 34$ este ordinul grupului. Deci grupul $E(\mathbb{F}_{31})$ este ciclic, generat de $P = (9,10)$.∎

Exemplul 4. *Fie curba eliptică $E = E(\mathbb{F}_{23})$ de ecuaţie $y^2 = x^3 + x + 1$. Punctele curbei $E(\mathbb{F}_{23})$ sunt listate în tabelul de mai jos.*

k	kP	k	kP	k	kP	k	kP	k	kP
1	(3,10)	7	(11,3)	13	(1,7)	19	(0,22)	25	(19,18)
2	(7,12)	8	(13,16)	14	(4,0)	20	(13,7)	26	(7,11)
3	(19,5)	9	(0,1)	15	(1,16)	21	(11,20)	27	(3,13)
4	(17,3)	10	(6,4)	16	(5,19)	22	12,19)	28	O
5	(9,16)	11	(18,20)	17	(18,3)	23	(9,7)		
6	(12,4)	12	(5,4)	18	(6,19)	24	(17,20)		

Fie $P = (3, 10) \in E(\mathbb{Z}_{23})$. *Calculăm* $\sqrt[4]{23}$ *şi alegem* $m = 3 > \sqrt[4]{23}$.

Facem lista paşilor mici:

$$-3P = (19, 18), -2P = (7, 11), -P = (3, 13), O,$$
$$P = (3, 10), 2P = (7, 12),\ 3P = (19, 5).$$

Calculăm $Q = (23 + 1)P = (17, 20)$, *după care facem lista paşilor mari calculând punctele* $Q + k(2mP)$ *pentru* $k = -3, \ldots, 3$.

$$6P = (12, 4), 12P = (5, 4), 18P = (6, 19), 24P = (17, 20)$$
$$30P = (7, 12), 36P = (13, 16), 42P = (4, 0).$$

Ne uităm după potriviri şi observăm că $30P = 2P$, *adică* $28P = O$. *Acesta este numărul* M *din algoritm.*

Se descompune M *în factori primi,* $M = 2^2 \cdot 7$.

Se calculează $2P = (7, 12) \neq O$ *şi* $7P = (11, 3) \neq O$. *Este clar că* $M = 28$ *este ordinul punctului* P.

Ne uităm acum în intervalul $(23 + 1 - 2\sqrt{23}, 23 + 1 + 2\sqrt{23}) \subset (14, 34)$ *şi observăm că* 28 *este singurul număr din interval divizibil cu* 28.

Concluzionăm că $N = 28$ *este ordinul grupului. Deci grupul* $E(\mathbb{F}_{23})$ *este ciclic, generat de* $P = (3, 10)$.∎

Exemplul 5. *Exemplificăm aplicarea algoritmului Paşi de copil paşi de uriaş pentru calculul ordinului grupului* $E(\mathbb{F}_{11})$ *dat de ecuaţia* $y^2 = x^3 + x + 6$. *Dacă* $R = (2, 7)$, *puterile punctului* R *sunt listate în tabelul de mai jos*

k	kP	k	kP
1	(2,7)	8	(3,5)
2	(5,2)	9	(10,9)
3	(8,3)	10	(8,8)
4	(10,2)	11	(5,9)
5	(3,6)	12	(2,4)
6	(7,9)	13	O
7	(7,2)		

Fie $P = (5, 2) \in E(\mathbb{Z}_{11})$. *Calculăm* $\sqrt[4]{11}$ *şi alegem* $m = 2 > \sqrt[4]{11}$.

Facem lista paşilor mici:

$$-2P = -4R = (10, 9), -P = -2R = (5, 9), O,$$
$$P = 2R = (5, 2), 2P = 4R = (10, 2).$$

Calculăm $Q = (11 + 1)P = (5, 9)$, *după care facem lista paşilor mari calculând punctele* $Q + k(2mP)$ *pentru* $k = -2, \ldots, 2$.

$$4P = 8R = (3, 5), 8P = 3R = (8, 3), 18P = (6, 19), 12P = 11R = (5, 9)$$
$$16P = 6R = (7, 9), 20P = R = (2, 7).$$

Ne uităm după potriviri şi observăm că $12P = -P$, *adică* $13P = O$. *Acesta este numărul* M *din algoritm.*

Ne uităm acum în intervalul $(11 + 1 - 2\sqrt{11}, 11 + 1 + 2\sqrt{11}) \subset (4, 20)$ *şi observăm că* 13 *este singurul număr din interval divizibil cu* 13.

Concluzionăm că $N = 13$ *este ordinul grupului. Deci grupul* $E(\mathbb{F}_{13})$ *este ciclic, generat de* $R = (2, 7)$.∎

1 Criptosisteme pe curbe eliptice

În 1985 Lenstra a arătat cum pot fi folosite curbele eliptice pentru realizarea unui algoritm de factorizare. Rezultatul lui Lenstra a sugerat posibilitatea folosirii curbelor eliptice la criptografia cu cheie publică. Miller şi Koblitz au fost primii care propun folosirea curbelor eliptice în

sistemele criptografice. Ei nu inventează noi algoritmi criptografici, dar au fost primii care au propus folosirea grupului punctelor unei curbe eliptice peste corpuri finite în implementarea criptosistemelor cu cheie publică bazate pe problema logaritmului discret în varianta curbelor eliptice. Astfel, Miller (Victor S. Miller, Use of elliptic curves in cryptography, pp. 417-426, LNCS 218, Advances in Cryptology Crypto 85, Santa Barbara, California, Hugh C. Williams (ed.), Springer-Verlag, 1986) a propus în 1985 un analog al protocolului Diffie-Hellman iar în 1987, Koblitz (Neal Koblitz, Elliptic curve cryptosystems, pp. 203-209, Mathematics of Computation, 48, 177, January 1987) prezintă analoage ale criptosistemelor El Gamal şi Massey-Omura. Primul analog al schemei RSA a fost introdus în 1991 de Koyama, Mauer, Okamoto, Vanstone.

Folosirea curbelor eliptice în implementarea criptosistemelor le face mult mai protejate. De asemenea criptosisteme pe curbe eliptice sunt mai eficiente decât cele clasice şi pentru motivul că în cele clasice se fac înmulţiri cu numere de 1024 biţi, pe când la primele cu numere de 163 biţi. Acesta este un avantaj, deşi operaţia de grup este mult mai complicată. De asemenea mărimea cheilor în cazul folosirii curbelor eliptice este mult mai mică decât în cazul clasic.

1.1 Scufundarea unui text necifrat într-o curbă eliptică

A scufunda un text simplu într-o curbă eliptică E, înseamnă a reprezenta textul simplu ca puncte din E. Abia după scufundare putem efectua calculele în E. Să remarcăm deci că scufundarea se va face înainte de criptare (scufundarea nu face parte din criptare). Cum se poate scufunda un text într-o curbuă eliptică? Ideal ar fi să scufundăm de exemplu, mesajele numerice $m \in \mathbb{F}_p$, ca prima coordonată a punctului unei curbe eliptice. Însă nu toate elementele lui $\mathbb{F}_p$ pot fi privite ca prima coordonată a unui punct al curbei.

Vom prezenta în cele ce umează două metode de reprezentare a unui mesaj în punctele unei curbe eliptice.

Metoda 1

Fie $E(\mathbb{F}_p)$ o curbă eliptică şi P un punct al său astfel încât ordinul n al lui P este suficient de mare. Subgrupul lui $E(\mathbb{F}_p)$ generat de P are n elemente şi deci orice număr $m \in \{1, \ldots, n\}$ poate fi reprezentat în curba $E(\mathbb{F}_p)$ prin punctul corespunzător nP.

Exemplul 6. *Fie curba eliptică $E = E(\mathbb{F}_{31})$ de ecuaţie $y^2 = x^3 + x + 13$. Am văzut în exemplul 3, că $P = (9, 10) \in E(\mathbb{F}_{31})$ este un generator al grupului. Dacă Alice vrea să trimită lui Bob mesajul HELLO, înainte de criptare, folosind corespondenţa numere $\longleftrightarrow$ cifre ($1 \leftrightarrow A$, $2 \leftrightarrow B$, $\ldots, 26 \leftrightarrow Z$), va sufunda textul simplu în curbă prin:*

$$(24, 29),\ (25, 16),\ (28, 13),\ (28, 13),\ (5, 9).\blacksquare$$

Metoda 2 (Metoda lui Koblitz) Fie acum p un număr prim astfel încât $p \equiv 3 (\mathrm{mod}\, 4)$ şi $E(\mathbb{F}_p)$ o curbă eliptică dată de ecuaţia $y^2 = x^3 + ax + b$. Prezentăm acum o metodă probabilistică de scufundare a unui text simplu într-o curbă eliptică $E(\mathbb{F}_p)$, metodă propusă de Koblitz.

- presupunem că mesajul necifrat m, este un număr între $0 \leq m \leq \frac{p}{1000} - 1$;
- se calculează $x_j = 1000m + j$ pentru $j = 0, 1, \ldots, 999$, adică se adăugă lui m trei cifre şi se obţine valoarea x_j astfel încât $1000m \leq x_j < 1000(m + 1) < p$);
- pentru $j = 0, \ldots, 999$, se calculează $s_j = x_j^3 + ax_j + b$ până obţinem $s_j^{\frac{p-1}{2}} \equiv 1$ mod p, adică s_j este pătrat modulo p;
- se calculează o rădăcină pătrată y_j a lui s_j prin $y_j \equiv s_j^{\frac{p+1}{4}} \pmod{p}$;
- punctul $P_m = (x_j, y_j)$ este punctul de pe curbă, ce corespunde textului m;
- invers, pentru a reconstitui mesajul m, dacă avem un punct (x_j, y_j) pe curbă, atunci $m = \left[\frac{x_j}{1000}\right]$.

Observaţia 8. *Cum s_j este practic un element oarecare din grupul ciclic F_p^*, probabilitatea ca s_j să fie pătrat este de aproximativ $1/2$. Astfel, probabilitatea de a nu fi capabili să găsim un punct pentru reprezentarea lui m este de aproximativ 2^{-1000}.*

Exemplul 7. *Fie curba eliptică $E = E(\mathbb{F}_{31})$ de ecuaţie $y^2 = f(x) = x^3 + x + 13$. Pentru uşurinţa vom înlocui pe 1000 din algoritmul precedent, cu 10. În practică numerele sunt evident mult mai mari.*

Presupunem că vrem să scufundăm mesajul $m = 2$ corespunzător literei B. Avem $0 \leq 2 < \frac{31}{10} - 1$. Căutăm acum x astfel încât

$$10 \cdot 2 = 20 \leq x < 30 < 31.$$

Luăm $x_0 = 20$, rezultă $f(20) \equiv 4 (mod 31)$.

Testăm dacă 4 este pătrat:

$$4^{\frac{31-1}{2}} = 4^{15} = 4^{1+2+2^2+2^3} \equiv 1 \, (mod 31).$$

deci 4 este pătrat. Calculăm rădăcina pătrată a lui 4:

$$4^{\frac{31+1}{4}} = 4^8 = 4^{2^3} \equiv 2 \, mod 31.$$

Deci mesajul $m = 2$ se scufundă în punctul $P = (20, 2)$.∎

1.2 Protocolul Diffie-Hellmann pe curbe eliptice

Presupunem că Alice şi Bob vor să genereze o cheie comună secretă pe care să o folsească la un sistem simetric precum DES sau AES. De exemplu Alice şi Bob pot fi două bănci ce vor să facă un transfer de bani. Protocolul Diffie-Hellmann poate fi implementat folosind curbe eliptice.

1. Alice şi Bob cad de acord asupra unei curbe eliptice $E = E(\mathbb{F}_p)$, de ecuaţie $y^2 = x^3 + ax + b$ peste un corp $\mathbb{F}_p$, unde p este număr prim $p \cong 10^{150}$ astfel încât problema logaritmului discret este dificilă în $E = E(\mathbb{F}_p)$. Ei aleg şi un punct $P \in E = E(\mathbb{F}_p)$ astfel încât subgrupul generat de P să aibă ordinul n suficient de mare (de obicei, curba şi punctul sunt alese astfel încât ordinul este un număr prim foarte mare).

   Să remarcăm că punctul P joacă rolul rădăcinii primitive din sistemul Diffie-Hellman clasic, in cazul acesta nu mai este în mod necesar un generator al grupului $E = E(\mathbb{F}_p)$. Toate calculele se vor face în grupul generat de P.

2. Alice alege un întreg $a \in \{0, 1, \ldots, (n-1)\}$ (secret), şi calculează $Q = aP \in E$, pe care-l trimite lui Bob.

3. Bob alege un întreg $b \in \{0, 1, \ldots, (n-1)\}$ (secret), şi calculează $R = bP \in E$, pe care-l trimite lui Alice.

4. Alice calculează cheia secretă $aR = a(bP) \in E$.

5. Bob calculează cheia secretă $bQ = b(aP) \in E$.

Observaţia 1. *Oscar (atacatorul) ştie aP şi pe bP. Fără rezolvarea problemei logaritmului discret (adică găsirea lui a ştiind P şi aP sau a lui b ştiind P şi bP) nu se poate calcula abP.*

Este clar că problema logaritmului discret este mult mai dificilă în contextul curbelor eliptice, datorită dificultăţii sporite a calculului în grupul $E(\mathbb{F}_p)$ faţă de grupul $\mathbb{F}_p^*$. În plus, un alt avantaj, îl constitue faptul că pentru un corp $\mathbb{F}_p$ dat pot exista mai multe curbe eliptice asociate.

Exemplul 8. *Fie curba eliptică $E(\mathbb{F}_{31})$ de ecuaţie $y^2 = x^3 + x + 13$. Punctul bază ales este $P = (9, 10)$. Aşa cum am vazut mai sus $ord(P) = 34$.*

Alice alege $a = 11$ şi calculează $Q = aP = 11(9, 10) = (22, 2)$ şi trimite rezultatul lui Bob.

Bob alege $b = 2$ şi calculează $R = bP = 2(9, 10) = (18, 29)$ şi trimite rezultatul lui Alice.

Alice calculează $11R = 11(18, 29) = (28, 18)$

Bob calculează $2Q = 2(22, 22) = (28, 18)$

Cheia comună secretă va fi $(28, 18)$.

1.3 Criptosistemul ElGamal pe curbe eliptice

Într-u articol publicat în1987, Koblitz propune implementarea analogului criptosistemului El-Gamal într-o curbă eliptică peste un corp $\mathbb{F}_p$ de caracteristică diferită de 2 sau 3.

Presupunem că Bob vrea să trimită un mesaj lui Alice.

1. **Generarea cheilor**

   - Alice alege un corp $\mathbb{F}_p$ (de caracteristică diferită de 2 sau 3) şi o curbă eliptică $E(\mathbb{F}_p)$.
   - Alice alege apoi un punct bază $P \in E(\mathbb{F}_p)$, având ordinul n suficient de mare (de preferinţă un număr prim foarte mare) astfel încât problema logaritmului discret (varianta pe curbe eliptice) este dificilă în $E(\mathbb{F}_p)$.

- Alice alege acum un întreg $a \in \{0, 1, \ldots, (n-1)\}$ la întâmplare şi calculează aP.

Corpul $\mathbb{F}_p$, curba $E(\mathbb{F}_p)$ şi punctele P şi aP reprezintă cheia publică. Întregul a este cheia secretă a lui Alice.

2. **Criptarea**

   - Presupunem că Bob vrea să trimită mesajul m lui Alice.
   - Mai întâi, el scufundă mesajul în curba eliptică $E(\mathbb{F}_p)$ aleasă de Alice. Aceasta este doar o "codificare" a mesajului m şi nu o criptare. Modalitatea de scufundare este (evident) ştiută şi de Alice. Fie $M \in E(\mathbb{F}_p)$ punctul ce reprezintă pe m în curba eliptică.
   - Apoi Bob alege un întreg $b \in \{0, 1, \ldots, (n-1)\}$ (astfel încât $b(aP) \neq O$) la întâmplare şi calculează bP.
   - Mesajul criptat şi trimis lui Alice de către Bob este
   $$(C_1, C_2) = (bP, M + b(aP)).$$

   Este important ca Bob să folosească de fiecare dată (când va trimite mesaje criptate ElGamal lui Alice) o altă valoare a lui b. Oscar va şti dacă Bob a folosit acelaşi b deoarece "vede" pe bP. El va calcula atunci $C_2' - C_2 = M' - M$. Dacă deja el ştie pe M atunci va găsi $M' = C_2' - C_2 + M$.

3. **Decriptarea** Pentru decriptare, Alice calculează
$$C_2 - aC_1 = M + b(aP) - a(bP) = M.$$

Observaţia 9. *Oscar cunoaşte informaţiile publice ale lui Alice precum şi punctele C_1 şi C_2. Dacă el ar putea calcula eficient logaritmul discret, atunci ar putea folosi punctele P şi aP pentru a afla valoarea lui a, care mai apoi poate fi folosită pentru a decripta mesajul prin $C_2 - aC_1$. De asemenea, Oscar ar putea folosi punctele P şi C_1 pentru a-l descoperi pe b.*

Este important pentru Bob să folosească de fiecare dată (când va trimite mesaje criptate ElGamal lui Alice) o altă valoare pentru a. Presupunem că Bob foloseşte aceeaşi valoare a pentru a cripta mesajele M şi M'. Oscar poate recunoaşte acest lucru din egalitatea $C_1 = C_1' = bP$. Oscar calculează atunci $C_2' - C_2 = M' - M$ şi dacă el ştie textul M, poate calcula pe M' prin $M' = (M' - M) + M$.

Observaţia 10. *În principiu, sistemul ElGamal funcţionează bine. Există însă cel puţin două inconveniente.*

Mesajul ce urmează a fi criptat este un punct de pe curba eliptică aleasă, lucru care limitează spaţiul textelor simple. De asemenea, Oscar ar putea descoperi mesajul dacă ştie doar o parte a sa, adică una din coordonatele punctului M.

Sistemul ElGamal cu curbe eliptice realizează o expandare a mesajului de 1 la 4 spre deosebire de sistemul ElGamal clasic care realizează o expandare a mesajului de 1 la 2. Pentru a remedia acest lucru, Bob ar putea trimite lui Alice doar primele coordonate ale punctelor C_1 şi C_2. Din păcate, deoarece Alice trebuie să calculeze diferenţa $C_2 - aC_1$, ea are nevoie de ambele coordonate ale punctelor C_1 şi C_2. Totuşi, coordonata x a unui punct determină coordonata y a sa până la o schimbare de semn, aşa înncât Bob ar putea să mai trimită încă un bit. De exemplu, Bob ar mai putea trimite pe 0 dacă $0 \leq y \leq \frac{1}{2}p$ şi 1 dacă $\frac{1}{2}p \leq y \leq p$. Astfel, Bob poate trimite doar coordonatele x ale punctelor C_1 şi C_2, plus încă doi biţi suplimentari. Se realizează astfel o "comprimare" a punctelor.

Exemplul 9. *Alegem din nou curba eliptică $E(\mathbb{F}_{31})$ de ecuaţie $y^2 = x^3 + x + 13$ şi punctul $P = (22, 22) = 11 \cdot (9, 10)$. Presupunem că cheia secretă a lui Alice este $a = 3$. Ea calculează şi face public punctul $aP = 33 \cdot (9, 10) = (9, 21)$.*

Presupunem că Bob vrea să trimită mesajul O (litera O). Mai întâi el scufundă mesajul în curba aleasă. Presupunem că mesajul este reprezentat de punctul $M = (5, 9) = 15 \cdot (9, 10)$. Apoi, Bob alege $b = 7$, după care calculează

$$C_1 = bP = 7(22, 22) = 77(9, 10) = 9(9, 10) = (16, 8)$$
$$b(aP) = 231(9, 10) = 27(9, 10) = (6, 7)$$
$$C_2 = M + b(aP) = (5, 9) + (6, 7) = 42(9, 10) = (24, 29)$$

şi trimite lui Alice mesajul cifrat

$$(C_1, C_2) = ((16, 8), (24, 29)).$$

Pentru decriptare Alice calculează $aC_1 = 3(16, 8) = (6, 7)$*, după care calculează*

$$C_2 - aC_1 = (24, 29) - (6, 7) = 15(9, 10) = (5, 9).\blacksquare$$

Exemplul 10. *Considerăm curba eliptică* $E(\mathbb{F}_{11})$ *dată de ecuaţia* $y^2 = x^3+x+6$ *(vezi Exemplul 5). Fie* $P = (2, 7)$ *punctul ales de Alice pe curba eliptică. Presupunem că exponentul secret al lui Alice este* $a = 7$*, deci cheia sa publică va fi* $aP = 7(2, 7) = (7, 2)$*. Presupunem că Bob vrea să cripteze mesajul* $M = (10, 9)$ *(care este un punct de pe curbă). Dacă Bob alege cheia secretă* $b = 3$*, atunci el calculează* $C_1 = 3(2, 7) = (8, 3)$ *şi* $C_2 = M + b(aP) = (10, 9) + 3(7, 2) = (10, 9) + (3, 5) = (10, 2)$ *şi trimite lui Alice mesajul cifrat* $C = ((8, 3), (10, 2))$*. Alice primeşte mesajul cifrat* C*, pe care-l decriptează prin* $M = (10, 2) - 7(8, 3) = (10, 2) - (3, 5) = (10, 2) + (3, 6) = (10, 9).\blacksquare$

1.4 Criptosistemul Menezes-Vanstone

O variantă a analogului criptosistemului ElGamal, pentru curbe eliptice este criptosistemul Menezes-Vanstone. Are particularitatea de a "masca" textul mesajului în loc să-l "scufunde". A fost introdus în 1990 de către Alfred J. Menezes şi Scott A. Vanstone în articolele

Alfred J. Menezes şi Scott A. Vanstone, The implementation of elliptic curve cryptosystems, pp. 2-13, LNCS 453, Advances in Cryptology Auscrypt 90, Sydney, Australia, Josef Pieprzyk and Jennifer Seberry (eds.), Springer-Verlag, 1990.

Alfred J. Menezes şi Scott A. Vanstone, Elliptic curve cryptosystems and their implementation, pp. 209-224, Journal of Cryptology, 6, 4, 1993.

Presupunem că Bob vrea să trimită un mesaj lui Alice.

1. **Generarea cheilor:** Alice alege un corp $\mathbb{F}_p$ cu p număr prim $p > 3$, o curbă eliptică $E(\mathbb{F}_p)$ peste corpul $\mathbb{F}_p$ şi un punct $P \in E(\mathbb{F}_p)$ de ordin n suficient de mare (e preferabil să fie un generator al lui $E(\mathbb{F}_p)$). Aceste date sunt fixate şi publice. Alice alege un întreg $a \in \{1, \ldots, n\}$ (pe care-l ţine secret) şi calculează aP (pe care-l face public).

2. **Criptarea:** Presupunem că Bob vrea să trimită lui Alice mesajul $m = (m_1, m_2) \in \mathbb{F}_p^* \times \mathbb{F}_p^*$. Bob alege un întreg $b \in \{1, \ldots, n\}$ astfel încât $b(aP) = (c_1, c_2)$, cu $c_1 \neq 0$ şi $c_2 \neq 0$, şi trimite lui Alice mesajul criptat
$$(bP, y_1, y_2) = (bP, c_1 m_1 (\mathrm{mod}\, p),\ c_2 m_2 (\mathrm{mod}\, p)).$$

3. **Decriptarea:** Pentru decriptare, Alice calculează
$$(y_1 c_1^{-1} (\mathrm{mod}\, p), y_2 c_2^{-1} (\mathrm{mod}\, p)) = (m_1, m_2),$$
unde $(c_1, c_2) = a(bP)$.

Observaţia 2. *Decriptarea este corectă. Într-adevăr, Alice poate calcula*

$$a(bP) = b(aP) = (c_1, c_2),$$

după care obţine

$$\begin{array}{rcccl} y_1 c_1^{-1} & \equiv & (c_1 m_1) c_1^{-1} & \equiv & m_1 \ (mod p) \\ y_2 c_2^{-1} & \equiv & (c_2 x_2) c_2^{-1} & \equiv & m_2 \ (mod p). \end{array}$$

Exerciţiul 4. *Alice şi Bob decid să comunice folosind criptosistemul cu curbe eliptice Menezes-Vanstone. Aleg curba eliptică* $E(\mathbb{F}_{31})$ *de ecuaţie* $y^2 = x^3 + x + 13$*. Punctul bază ales este* $P = (9, 10)$ *iar cheia secretă a lui Bob este* $b = 12$*. Ţinând seama că scufundarea mesajului s-a făcut după corespondenţa litere* $\leftrightarrow$ *numere (*$A \leftrightarrow 1$*,* $B \leftrightarrow 2$*,* $\ldots$*,* $Z \leftrightarrow 26$*), să decriptăm mesajul primit de Bob*

$$((6, 24),\ 26,\ 23);\ ((25, 15),\ 11,\ 30);\ ((9, 10),\ 2,\ 9).$$

$b \cdot aP = 12 \cdot (6, 24) = 16 \cdot (9, 10) = (19, 3)$ *aici* $a = 7$*. Atunci :*

$$\begin{array}{l} y_1 \cdot c_1^{-1} (mod 31) = 26 \cdot 19^{-1} (mod 31) = 26 \cdot 18 = 3 \mapsto C \\ y_2 \cdot c_2^{-1} (mod 31) = 23 \cdot 3^{-1} (mod 31) = 23 \cdot 21 = 18 \mapsto R \end{array}$$

$b \cdot aP = 12 \cdot (25, 15) = 8 \cdot (9, 10) = (24, 29)$ *aici* $a = 29$*. Atunci :*

$$\begin{array}{l} y_1 \cdot c_1^{-1} (mod 31) = 11 \cdot 24^{-1} (mod 31) = 11 \cdot 22 = 25 \mapsto Y \\ y_2 \cdot c_2^{-1} (mod 31) = 30 \cdot 29^{-1} (mod 31) = 30 \cdot 15 = 16 \mapsto P \end{array}$$

$b \cdot aP = 12 \cdot (9,10) = 12 \cdot (9,10) = (28,13)$ *aici* $a = 1$. *Atunci :*

$$y_1 \cdot c_1^{-1} (mod 31) = 2 \cdot 28^{-1} (mod 31) = 2 \cdot 10 = 20 \mapsto T$$
$$y_2 \cdot c_2^{-1} (mod 31) = 9 \cdot 13^{-1} (mod 31) = 9 \cdot 12 = 15 \mapsto O$$

Deci mesajul decriptat este CRYPTO.

Exerciţiul 5. *Alice şi Bob decid să comunice folosind criptosistemul cu curbe eliptice Menezes-Vanstone. Aleg curba eliptică* $E(\mathbb{F}_{31})$ *de ecuaţie* $y^2 = x^3 + x + 13$. *Punctul bază ales este* $P = (9,10)$ *iar cheia secretă a lui Bob este* $b = 25$. *Ţinând seama că scufundarea mesajului s-a făcut după corespondenţa litere* $\leftrightarrow$ *numere (*$A \leftrightarrow 1$, $B \leftrightarrow 2$, $\ldots$, $Z \leftrightarrow 26$*), să decriptăm mesajul primit de Bob*

$$((4,9),\ 28,\ 7);\ ((5,22),\ 9,\ 13);\ ((5,22),\ 20,\ 17);\ ((25,16),\ 12,\ 27).$$

$b \cdot aP = 25 \cdot (4,9) = (34 \cdot 22 + 2) \cdot (9,10) = (18,29)$ *aici* $a = 30$. *Atunci :*

$$y_1 \cdot c_1^{-1} (mod 31) = 28 \cdot 19^{-1} (mod 31) = 28 \cdot 19 = 5 \mapsto E$$
$$y_2 \cdot c_2^{-1} (mod 31) = 7 \cdot 29^{-1} (mod 31) = 7 \cdot 15 = 12 \mapsto L$$

$b \cdot aP = 25 \cdot (18,28) = 8 \cdot (9,10) = (24,29)$ *aici* $a = 18$. *Atunci :*

$$y_1 \cdot c_1^{-1} (mod 31) = 9 \cdot 24^{-1} (mod 31) = 9 \cdot 22 = 12 \mapsto L$$
$$y_2 \cdot c_2^{-1} (mod 31) = 13 \cdot 29^{-1} (mod 31) = 13 \cdot 15 = 9 \mapsto I$$

$b \cdot aP = 25 \cdot (5,22) = 33 \cdot (9,10) = (9,21)$ *aici* $a = 1$. *Atunci :*

$$y_1 \cdot c_1^{-1} (mod 31) = 20 \cdot 9^{-1} (mod 31) = 20 \cdot 7 = 16 \mapsto P$$
$$y_2 \cdot c_2^{-1} (mod 31) = 17 \cdot 21^{-1} (mod 31) = 17 \cdot 3 = 20 \mapsto T$$

$b \cdot aP = 25 \cdot (25,16) = 23 \cdot (9,10) = (22,9)$ *aici* $a = 1$. *Atunci :*

$$y_1 \cdot c_1^{-1} (mod 31) = 12 \cdot 22^{-1} (mod 31) = 12 \cdot 24 = 9 \mapsto I$$
$$y_2 \cdot c_2^{-1} (mod 31) = 27 \cdot 9^{-1} (mod 31) = 27 \cdot 7 = 3 \mapsto C$$

Deci mesajul decriptat este ELLIPTIC.

1.5 Criptosistemul cu curbe eliptice Massey-Omura

([MO86] James L. Massey şi James K. Omura, U.S. Patent No. 4,567,600, Method and apparatus for maintaining the privacy of digital messages conveyed by public transmission, 28 January 1986.)

Reamintim scenariul lacătelor. Presupunem că Alice vrea să trimită, printr-un canal nesigur, un mesaj lui Bob. Ea ar putea proceda astfel. Alice pune mesajul său într-o cutie pe care o închide cu lacătul său, după care trimite cutia lui Bob. Bob ataşează la cutie lacătul său şi o trimite înapoi lui Alice. Alice scoate lacătul ei şi trimite cutia înapoi lui Bob. Acum Bob scoate lacătul lui şi citeşte mesajul. La momentul respectiv se părea că metoda nu funcţionează în criptografie pentru că criptările nu comută decât în cazul unor sisteme criptografice foarte simple. Folosirea curbelor eliptice permite implementarea matematică a acestei proceduri.

1. Alice şi Bob se înţeleg asupra unei curbe eliptice $E(\mathbb{F}_p)$ peste un corp finit $\mathbb{F}_p$ astfel încât problema logaritmului discret este dificilă în $E(\mathbb{F}_p)$. Fie n ordinul grupului $E(\mathbb{F}_p)$.

2. Alice reprezintă mesajul ei printr-un punct $M \in E(\mathbb{F}_p)$.

3. Alice alege un întreg secret $a \in (1,n)$ astfel încât cmmdc $(a,n) = 1$. Alice calculează apoi $M_1 = aM$, şi trimite pe M_1 lui Bob.

4. Bob alege un întreg secret $b \in (1,n)$ astfel încât cmmdc $(b,n) = 1$. Bob calculează apoi $M_2 = bM_1$, şi trimite pe M_2 lui Alice.

5. Alice calculează inversul a^{-1} modulo n, calculează $M_3 = a^{-1}M_2$ şi trimite pe M_3 lui Bob.

6. Bob calculează inversul b^{-1} modulo n, calculează $M_4 = b^{-1}M_3$. Atunci $M_4 = M$ este mesajul necriptat.

Observaţia 11. *Punctul M_4 obţinut în final de către Bob este chiar mesajul m iniţial. În primul rând avem $a^{-1} \cdot a \equiv 1 \pmod n$, adică există un întreg k astfel încât $a^{-1} \cdot a = 1 + kn$. Pe de altă parte, grupul $E(\mathbb{F}_p)$ are ordinul n, şi aplicând Teorema lui Lagrange, avem $nR = \infty$, pentru orice punct $R \in E(\mathbb{F}_p)$. Atunci $a^{-1}aR = (1 + kn)R = R + R\infty = R$. Aplicând acest lucru pentru $R = bM$, găsim că $M_3 = a^{-1}baM = bM$.*

Analog, $b^{-1} \cdot b \equiv 1 \pmod n$ şi deci $M_4 = b^{-1}bM = M$.

Aşadar, sistemul funcţionează pentru că aici criptarea comută cu decriptarea.

Observaţia 12. *Securitatea sistemului se bazează pe dificultatea problemei logaritmului discret pe curbe eliptice. Sistemul Massey-Omura pe curbe eliptice poate fi considerat ca o variantă a protocolului Diffie-Hellman.*

Exerciţiul 6. *Alice doreşte să trimită mesajul $m = 15$ lui Bob folosind sistemul Massey-Omura.*

Cei doi se hotărăsc asupra curbei eliptice $E(\mathbb{F}_{31})$ definită de ecuaţia $y^2 = x^3 + x + 13$.

Ordinul grupului este $n = 34$ (vezi exemplul (3)).

Alice reprezintă mesajul m prin punctul $M = (5, 9) = 15P$, unde $P = (9, 10)$ este un generator al grupului.

Alice alege $a = 7$ şi calculează $M_1 = 7M = 105P = (3 + 3 \cdot 34)P = (23, 19)$ şi trimite rezultatul lui Bob.

Bob alege $b = 3$ şi calculează $M_2 = 3M_1 = 9P = (16, 8)$ şi trimite rezultatul lui Alice.

Alice calculează $a^{-1} = 7^{-1} = 5 \pmod{34}$, calculează $M_3 = 5M_2 = 45P = (11 + 34)P = 11P = (22, 22)$ şi trimite rezultatul lui Bob.

Bob calculează $b^{-1} = 3^{-1} = 23 \pmod{34}$ şi calculează $M_4 = 23M_3 = 253P = (15+7\cdot34)P = 15P = (5, 9) = M$.

1.6 Criptosistemul RSA cu curbe eliptice (ECRSA)

Până acum am considerat curbe eliptice definite peste un corp. Vom considera acum curbe eliptice definite peste inelul $\mathbb{Z}/n\mathbb{Z}$ unde $n = pq$, cu p şi q două numere prime distincte. Similar cu cazul curbelor eliptice peste corpuri, definim $E(\mathbb{Z}/n\mathbb{Z})$ ca fiind mulţimea punctelor de coordonate $(x, y) \in (\mathbb{Z}/n\mathbb{Z})^2$ astfel încât $y^2 = x^3 + ax + b$, la care se mai adaugă un punct O_n de la infinit. Presupunem în plus că cmmdc$(n, 4a^3 + 27b^2) = 1$. Acum am putea defini o lege de compoziţie pe $E(\mathbb{Z}/n\mathbb{Z})$ exact ca în cazul curbelor eliptice $E(\mathbb{F}_q)$, înlocuind calculele din corpul $\mathbb{F}_q$ cu cele din inelul $\mathbb{Z}/n\mathbb{Z}$ (vezi formulele din paragraful 0.2). Apar însă două probleme. Prima problemă constă în faptul că pentru calculul pantelor m din formule, trebuie să facem împărţiri în inelul $\mathbb{Z}/n\mathbb{Z}$. Aceste împărţiri sunt definite doar dacă împărţitorul este inversabil faţă de legea multiplicativă. Aşadar, operaţia în $E(\mathbb{Z}/n\mathbb{Z})$ nu este mereu definită. A două problemă, legată strâns de prima, este aceea că $E(\mathbb{Z}/n\mathbb{Z})$ nu mai este grup. Se pare că este imposibil să avem un criptosistem în $E(\mathbb{Z}/n\mathbb{Z})$. Prezentăm în cele ce urmează un sistem criptografic pe $E(\mathbb{Z}/n\mathbb{Z})$, introdus de K.Koyama, U.Maurer, T.Okamoto şi S.Vanstone în 1992 (Kenji Koyama, Ueli M. Maurer, Tatsuaki Okamoto şi Scott A. Vanstone, New public-key scheme based on elliptic curves over the ring $\mathbb{Z}_n$, pp. 252-266, LNCS 576, Advances in Cryptology,Crypto,91.Santa Barbara. California, Joan Feigenbaum (ed.), Springer-Verlag, 1992).

Operaţia de adunare, propusă mai înainte, este echivalentă (atunci când este definită) cu operaţia grupală pe $E(\mathbb{Z}/p\mathbb{Z}) \times E(\mathbb{Z}/q\mathbb{Z})$ (adunarea se face pe componente). Să explicăm mai clar acest lucru. Folosind Lema Chineză a resturilor, orice element $c \in \mathbb{Z}/n\mathbb{Z}$ se poate reprezenta în mod unic printr-o pereche $[c_p, c_q]$, unde $c_p \in \mathbb{Z}/p\mathbb{Z}$ iar $c_q \in \mathbb{Z}/q\mathbb{Z}$. Acest lucru rezultă uşor din faptul că sistemul de congruenţe $c \equiv c_p \pmod p$, $c \equiv c_q \pmod q$ admite o soluţie unică modulo $n = pq$. Astfel, orice punct $P = (x, y)$ din $E(\mathbb{Z}/n\mathbb{Z})$ se poate reprezenta în mod unic printr-o pereche de puncte $[P_p, P_q] = [(x_p, y_p), (x_q, y_q)]$, unde $P_p \in E(\mathbb{Z}/p\mathbb{Z})$ şi $P_q \in E(\mathbb{Z}/q\mathbb{Z})$, cu convenţia că punctul de la infinit O_n este reprezentat de $[O_p, O_q]$, unde O_p şi O_q sunt punctele de la infinit ale curbelor $E(\mathbb{Z}/p\mathbb{Z})$ şi respectiv $E(\mathbb{Z}/q\mathbb{Z})$.

De exemplu punctul $(11, 32)$ de pe curba $E(\mathbb{Z}/35\mathbb{Z})$ dată de ecuaţia $y^2 = x^3 + 8$ este reprezentat de perechea de puncte $(1, 2) \in E(\mathbb{Z}/5\mathbb{Z})$, $(4, 4) \in E(\mathbb{Z}/7\mathbb{Z})$.

Prin aplicaţia $E(\mathbb{Z}/n\mathbb{Z}) \mapsto E(\mathbb{Z}/p\mathbb{Z}) \times E(\mathbb{Z}/q\mathbb{Z})$, $P \mapsto (P_p, P_q)$, astfel definită, sunt acoperite toate punctele din $E(\mathbb{Z}/p\mathbb{Z}) \times E(\mathbb{Z}/q\mathbb{Z})$, cu excepţia perechilor (P_p, P_q) pentru care exact unul din punctele P_p şi P_q este punctul de la infinit. Remarcăm că adunarea pe $E(\mathbb{Z}/n\mathbb{Z})$ nu este definită dacă şi numai dacă punctul rezultat (văzut ca element din $E(\mathbb{Z}/p\mathbb{Z}) \times E(\mathbb{Z}/q\mathbb{Z})$) este unul din aceste puncte speciale.

Este important să remarcăm, că dacă numerele prime p şi q sunt foarte mari, probabilitatea ca suma a două puncte din $E(\mathbb{Z}/n\mathbb{Z})$ să nu fie definită este foarte mică. De fapt, dacă probabilitatea ca adunarea în $E(\mathbb{Z}/n\mathbb{Z})$ să nu fie definită nu este mică, atunci executarea operaţiei de

adunare pe $E(\mathbb{Z}/n\mathbb{Z})$ ar putea da un algoritm eficient de factorizare. Un astfel de algoritm este presupus a nu exista. Se poate demonstra că dacă $P, Q \in E(\mathbb{Z}/n\mathbb{Z})$ sunt puncte pentru care adunarea nu este definită în $E(\mathbb{Z}/n\mathbb{Z})$, atunci cunoaşterea lor, e suficientă pentru a descompune pe n.

A doua problemă, adică $E(\mathbb{Z}/n\mathbb{Z})$ nu este grup, poate fi rezolvată de următoarea lemă. Adică, deşi nu pot fi folosite proprietăţile grupurilor finite, se poate utiliza o proprietate a lui $E(\mathbb{Z}/n\mathbb{Z})$, analoagă Teoremei lui Lagrange din teoria grupurilor.

Lema 2. *Fie $E(\mathbb{Z}/n\mathbb{Z})$ o curbă eliptică astfel încât $cmmdc(4a^3 + 27b^2, n) = 1$ şi $n = pq$ cu p şi q numere prime astfel încât $p \equiv q \equiv 2 \pmod 3$, $p, q \geq 5$. Fie $m = (p+1)(q+1)$. Atunci pentru orice punct $P \in E(\mathbb{Z}/n\mathbb{Z})$ şi orice întreg $k \in \mathbb{Z}$, avem $(1 + km)P = P$.*

Demonstraţie: În primul rând reamintim că dacă p este un număr prim impar astfel încât $p \equiv 2 \pmod 3$, iar $E(\mathbb{F}_p)$ este o curbă eliptică peste corpul $\mathbb{F}_p$, atunci ordinul grupului $E(\mathbb{F}_p)$ este $p + 1$. Folosind această observaţie, este clar că $(p + 1)P_p = O_p$ şi $(q + 1)P_q = O_q$ pentru orice punct $P \in E(\mathbb{Z}/n\mathbb{Z})$ şi deci $(1 + km)P_p = P_p$ şi $(1 + km)P_q = P_q$. Folosind acum Lema Chineză a resturilor, rezultă afirmaţia din enunţ.

Suntem în măsură să descriem acum unul din criptosistemele descoperite de K.Koyama, U.Maurer, T.Okamoto şi S.Vanstone bazate pe curbe eliptice peste inele. Vom descrie sistemul, numit chiar de autori, schema de tip 1.

Presupunem că Bob vrea să trimită un mesaj lui Alice.

1. **Generarea cheilor:**

   (a) Alice alege două numere prime diferite, foarte mari, astfel încât $p \equiv q \equiv 2 \pmod 3$ şi o curbă eliptică $E(\mathbb{Z}/n\mathbb{Z})$ dată de o ecuaţie de forma $y^2 = x^3 + b$. Deocamdată elementul $b \in \mathbb{Z}/n\mathbb{Z}$ este oarecare.

   (b) Alice calculează $n = pq$ şi $m = \text{card } E(\mathbb{Z}/p\mathbb{Z}) \times \text{card } E(\mathbb{Z}/q\mathbb{Z}) = (p + 1)(q + 1)$.

   (c) Alice alege un întreg e prim cu m şi calculează unicul întreg d, $1 \leq d < m$ astfel încât $de \equiv 1 \pmod m$.

   Cheia secretă este tripletul (p, q, d) iar cheia publică este perechea (n, e).

2. **Criptarea:**

   (a) Bob reprezintă mesajul său ca o pereche de întregi $(m_1, m_2) \pmod n$. El priveşte perechea (m_1, m_2) ca un punct M pe curba eliptică $E(\mathbb{Z}/n\mathbb{Z})$, dată de ecuaţia $y^2 = x^3 + b$, unde $b \equiv m_2^2 - m_1^3 \pmod n$. El nu are nevoie de calculul lui b.

   (b) Bob criptează textul simplu M prin $C = eM$ în $E(\mathbb{Z}/n\mathbb{Z})$ şi trimite textul cifrat $C = (c_1, c_2)$ lui Alice.

3. **Decriptarea:** Pentru decriptare, Alice calculează $M = dC$ în $E(\mathbb{Z}/n\mathbb{Z})$. Decriptarea este corectă datorită lemei de mai sus. Aceasta se poate aplica pentru că $ed = 1 + k(p+1)(q+1)$ pentru un întreg k.

Observaţia 13. *Să remarcăm că valoarea lui b nu apare în formulele legii de adunare, şi deci aceasta nu este necesară. Ea poate fi calculată de Oscar prin $b \equiv c_2^2 - c_1^3 \pmod n$.*