ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი

გიორგი სვანაძე

ელიფსური წირები და კრიპტოსისტემები

ზუსტ და საბუნებისმეტყველო მეცნიერებათა ფაკულტეტის

სამაგისტრო პროგრამა „მათემატიკა“

სამაგისტრო ნაშრომი შესრულებულია მათემატიკის მაგისტრის აკადემიური ხარისხის მოსაპოვებლად

სამაგისტრო ნაშრომის ხელმძღვანელი: თსუ ასოცირებული პროფესორი

ბაჩუკი მესაბლიშვილი

თბილისი

2020

სარჩევი

ანოტაცია

სამაგისტრო ნაშრომი ეხება ალგებრულ მრავალსახეობების კერძო შემთხვევას - ელიფსურ წირებს და კრიპტოსისტემების აგებას ელიფსურ წირებზე. ნაშრომში მოკლედ არის გადმოცემული ორი ცვლადის მესამე ხარისხის ფუნქციის თვისებები, მისი გეომეტრიული შინაარსი და შესაბამისი ალგებრული წირის წერტილებზე მოქმედებები, ამ წერტილებისგან ჯგუფის აგება. დაწერილია პროგრამა ელიფსური წირის წერტილების პოვნისა. ნაშრომში აგრეთვე მოყვანილია ის პრაქტიკული ამოცანები, რომელთა გადაწყვეტა შესაძლებელია ელიფსური წირების გამოყენებით. დაწერილია შესაბამისი პროგრამები.

Abstract

The master thesis is about a particular case of algebraic variety – Elliptic curves and building cryptosystems on elliptic curves. This thesis proposes third-degree function with two variables' properties, its geometric content and algebraic operations on curve points and building a group with these points. This work also represents practical problems that can be solved using elliptic curves, relevant proprietary software codes have been written.

შესავალი

ნაშრომი ეხება ელიფსურ წირებს და მის გამოყენებას პრაქტიკულ ამოცანებში. იგი შედგება ოთხი თავისა და ლიტერატურისაგან.

პირველ თავში მოყვანილია ის თეორიული მათემატიკური საკითხები ალგებრიდან, რომელიც საჭიროა ელიფსური წირის განსაზღვრისა და მისი თვისებების შესწავლისათვის. ელიფსური წირები შეიძლება განხილული იყოს სხვადასხვა ველის მიმართ (ჩვენ ვიხილავთ სასრულ ველთა მიმართ), ამიტომ ნაშრომის პირველ თავში დაწვრილებითაა შესწავლილი სასრული ველისა და მისი ქვეველების თვისებები, ველთა გაფართოებები და გაფართოების ხარისხი, ველის არანულოვან ელემენტთა მიერ შექმნილი ციკლური ჯგუფი და მისი თვისებები, განხილულია ველზე პოლინომთა რგოლის ეკვივალენტობის კლასები.

მეორე თავში განსაზღვრულია მრავალსახეობები, მოყვანილია ელიფსური წირების განსაზღვრება, განხილულია ზოგადი და კონკრეტული სახის ელიფსური წირები და გამოკვლეულია მათი ღერძთან გადაკვეთის წერტილები. გარდა ამისა, შემოტანილია ოპერაციები ელიფსური წირის წერტილებზე. ბოლოს მოყვანილია ელიფსური წირის გომეტრიული და ალგებრული თვისებები.

მესამე თავში ნაჩვენებია, თუ როგორ შეიძლება აიგოს კრიპტოსისტემა ელიფსური წირების გამოყენებით. მოყვანილია ასეთი კრიპტოსისტემის აგების როგორც თეორიული გზა, ასევე კონკრეტული მაგალითი, შესწავლილია ელიფსური წირის წერტილთა ჯგუფი, განხილულია შებრუნებული ამოცანის - დისკრეტული ლოგარითმის პოვნის ალგორითმი.

მეოთხე თავში განხილულია პრაქტიკულ ამოცანებზე მორგებული კრიპტოსქემები. წარმოდგენილია El-Gamal-ის შიფრის, ელექტრონული ხელმოწერის და არჩევნების კრიპტოსქემები. ამავე თავის ბოლოს დაწერელია არჩევნების ჩატარების პროგრამა.

1. სასრულ ველთა თვისებები

გავიხსენოთ, რომ G ჯგუფს ეწოდება ციკლური, თუ არსებობს $a \in G$ ელემენტი ისეთი, რომ G-ს ნებისმიერი b ელემენტისათვის არსებობს ისეთი ნატურალური რიცხვი $i \geq 0$, რომ $b = a^i$. ასეთ a ელემენტს ეწოდება G ციკლური ჯგუფის წარმომქმნელი.

გავიხსენოთ აგრეთვე, რომ ციკლური G ჯგუფის ყოველი ქვეჯგუფი ასევე ციკლურია; ამასთანავე, თუ G არის n რიგის ციკლური ჯგუფი და d ყოფს n-ს, მაშინ G-ს აქვს ერთადერთი d რიგის ქვეჯგუფი.

ვთქვათ G ჯგუფია. თუ $a \in G$ ელემენტის რიგია t, მაშინ a^k ელემენტის რიგი იქნება $\frac{t}{(k,t)}$, სადაც (k,t) არის k და t-ს უდიდესი საერთო გამყოფი. აქედან გამომდინარე, თუ G არის n რიგის ციკლური ჯგუფი და d ყოფს n-ს, მაშინ G-ს აქვს ზუსტად $\varphi(d)$ რაოდენობის ელემენტი, რომელთა რიგია d და, მაშასადამე, G-ს აქვს ზუსტად $\varphi(n)$ წარმომქმნელი.

მაგალითად, განვიხილოთ $\mathbb{Z}_{19}^* = \{1, 2, 3, \dots, 18\}$ მულტიპლიკაციური ჯგუფი, რომლის რიგია 18. ეს ჯგუფი არის ციკლური და მისი წარმომქმნელია, მაგალითად, 2. ქვემოთ ცხრილში მოყვანილია $\mathbb{Z}_{19}^*$ ჯგუფის ყველა ქვეჯგუფი და მათი წარმომქმნელები.

ქვეჯგუფი	წარმომქმნელი	რიგი
{1}	1	1
{1, 18}	18	2
{1, 7, 11}	7, 11	3
{1, 7, 8, 11, 12, 18}	8, 12	6
{1, 4, 5, 6, 7, 9, 11, 16, 17}	4, 5, 6, 9, 16, 17	9
{1, 2, 3, 4, ... , 18}	2, 3, 10, 13, 14, 15	18

ვთქვათ, F ველია, $F[x]$ პოლინომთა რგოლია კოეფიციენტებით F ველიდან, ხოლო $f(x)$ კი - ფიქსირებული პოლინომი $F[x]$-დან. $F[x]$ პოლინომთა რგოლი დავყოთ ეკვივალენტურ კლასებად მოდულით $f(x)$. $g(x) \in F[x]$ პოლინომის ეკვივალენტობის კლასი არის სიმრავლე ყველა იმ პოლინომებისა $F[x]$-დან, რომლებიც $g(x)$-ის სადარია მოდულით $f(x)$, ანუ $f(x)$-ზე გაყოფისას აქვთ იგივე ნაშთი, რაც აქვს $g(x)$-ს $f(x)$-ზე გაყოფისას. ეკვივალენტურ კლასთა ეს

სიმრავლე აღვნიშნოთ $F[x]/(f(x))$-ით. მაშასადამე, $F[x]/(f(x))$ არის n -ზე ნაკლები ხარისხის პოლინომთა სიმრავლე, სადაც $n = \deg(f(x))$.

$F[x]/(f(x))$ პოლინომთა სიმრავლე მასზე განსაზღვრული შეკრებისა და გამრავლების შესაბამისი ოპერაციების მიმართ არის კომუტაციური რგოლი, რომელსაც $F[x]$ პოლინომთა რგოლის ფაქტორ-რგოლი ეწოდება. შევნიშნოთ, რომ როდესაც $f(x)$ დაუყვანადი პოლინომია F ველზე, მაშინ $F[x]/(f(x))$ ველია.

ვთქვათ, E და F ველებია და $E \supset F$. მაშინ E შეგვიძლი განვიხილოთ როგორც ვექტორული სივრცე F ველზე. E ვექტორული სივრცის განზომილებას F ველზე ეწოდება E ველის ხარისხი F-ზე და აღინიშნება $[E:F]$ სიმბოლოთი. თუ ეს ხარისხი სასრულია (და უდრის n -ს), მაშინ E ველს ეწოდება Fველის სასრული (n -ხარისხის) გაფართოება.

ცნობილია (იხ. [3], გვ. 32), თუ $L \supset E \supset F$ ველთა სასრული გაფართოებებია, მაშინ $[L:F] = [L:E][E:F]$.

1.1. სასრულ ველთა არსებობა და ერთადერთობა

ველს ეწოდება სასრული, თუ ის სასრული რაოდენობის ელემენტებისაგან შედგება. ასეთ ველებში ელემენტების რაოდენობაა p^m, სადაც p მარტივი რიცხვია და $m \geq 1$.

ყოველი მარტივი p რიცხვის ნებისმიერი ხარისხისთვის, p^m-სთვის, არსებობს იზომორფიზმამდე სიზუსტით ერთადერთი სასრული ველი, რომლის ელემენტების რაოდენობაა p^m. ასეთი ველი F_{p^m} ან $GF(p^m)$ სიმბოლოთი აღინიშნება. შევნიშნოთ, რომ თუ p მარტივი რიცხვია, მაშინ F_p იზომორფულია $\mathbb{Z}_p$ ველის. ასევე, თუ F_q, $q = p^m$, სასრული ველია (აქ p მარტივი რიცხვია), მაშინ მისი მახასიათებელია p, ის შეიცავს $\mathbb{Z}_p$ ველის იზომორფულ ქვეველს და $F_q \supset \mathbb{Z}_p$ არის m ხარისხის ველთა გაფართოება.

ახლა მოვიყვანოთ რამდენიმე ფაქტი სასრული ველის ქვეველის შესახებ:

1. თუ F_q არის $q = p^m$ რიგის სასრული ველი (p მარტივი რიცხვია), მაშინ მისი ყოველი ქვეველის რიგია p^n, სადაც n არის m-ის გამყოფი და პირიქით, თუ n არის m-ის გამყოფი, მაშინ არსებობს F_q ველის p^n რიგის ქვეველი, სახელდობრ, F_{p^n} ([3], გვ.48).

2. F_q ველის არანულოვანი ელემენტები გამრავლების მიმართ ქმნიან აბელურ ჯგუფს, რომელიც აღინიშნება F_q^* -ით. F_q^* არის $q-1$ რიგის ციკლური ჯგუფი.

2. ელიფსური წირები

არანულოვანი $f_1, \dots, f_m \in F[x_1, \dots, x_n]$ $(n, m \in \mathbb{N})$ მრავალწევრებით წარმოქმნილი მრავალსახეობა F^n სიმრავლეში ეწოდება

$$V(f_1, \dots, f_m) = \{(a_1, a_2, \dots, a_n) : (a_1, a_2, \dots, a_n) \in F^n, f_i(a_1, a_2, \dots, a_n) = 0, i = 1, 2, \dots m\}$$

სიმრავლეს. თუ F ველია, მაშინ მრავალსახეობას ეწოდება აფინური მრავალსახეობა.

ჰიპერზედაპირი ეწოდება მრავალსახეობას, რომელიც წარმოქმნილია ერთი მრავალწევრით (როცა $m = 1$). თუ $n = 2$, მაშინ ჰიპერზედაპირს ეწოდება წირი F ველის მიმართ. მაშასადამე, ნებისმიერი $V(f_1, \dots, f_m)$ $(m \geq 2)$ მრავალსახეობა არის $V(f_i)$ ჰიპერზედაპირების თანაკვეთა $(i = 1, 2, \dots, m)$.

თუ f_i წრფივია, მაშინ გვაქვს წრფივი მრავალსახეობა. თუ $(F, +, \cdot)$ უნულგამყოფო რგოლია, მაშინ ყოველი არაცარიელი სასრული ქვესიმრავლე $S = \{a_1, a_2, \dots, a_n\} \subseteq F$ არის მრავალსახეობა F -ში. მართლაც,

$$S = V\left(\prod_{i=1}^{n}(x - a_i)\right).$$

თუ $(F, +, \cdot)$ უნულგამყოფო სასრული რგოლია, მაშინ

$$F = V\left(\prod_{a \in F}(x - a)\right)$$

და F არის მრავალსახეობა F-ში. ასევე, თუ F ველია, მაშინ F^r მრავალსახეობაა F^n-ში $(r \leq n)$.

$V(f_1, \dots, f_s)$ და $V(g_1, \dots, g_t)$ მრავალსახეობები ტოლია, მაშინ და მხოლოდ მაშინ, როცა ეკვივალენტურია შემდეგი პოლინომიალურ განტოლებათა სისტემები:

$$f_i(x_1, x_2, \dots, x_n) = 0, \ \ i = 1, 2, \dots, s \qquad \text{და} \qquad g_i(x_1, x_2, \dots, x_n) = 0, \ \ i = 1, 2, \dots, t.$$

$V(f)$ მრავალსახეობას F^2-ში (სადაც $f \in F[x, y]$) ეწოდება ბრტყელი ალგებრული წირი, ან მოკლედ წირი და აღინიშნება $\Gamma = V(f)$. მომავალში ვიგულისხმებთ, რომ $\Gamma = V(f)$ წირი მოცემულია ისეთი $g(x, y) = 0$ განტოლებით, რომ g არის უმცირესი დადებითი ხარისხის მრავალწევრი, ანუ $\Gamma = V(g)$. ამასთანავე, $V(g)$ წირის ხარისხი ეწოდება g პოლინომის ხარისხს.

იმის მიხედვით $g(x,y)$ პოლინომი დაუყვანადია, თუ დაყვანადი, გვაქვს ან ერთი დაუყვანადი წირი, ან რამდენიმე წირის გაერთიანება. ნებისმიერ $A(x_0,y_0)$ წერტილს, სადაც (x_0,y_0) არის $g(x,y)=0$ განტოლების ამონახსნი, Γ წირის წერტილი ეწოდება.

განიხილება სხვადასხვა სახის წირები. ვთქვათ, მოცემულია $f(X,Y)=0$ განტოლება, სადაც f ორი X და Y ცვლადის n ხარისხის პოლინომია კოეფიციენტებით F ველიდან. როგორც ვიცით, სიმრავლეს იმ $(x,y)\in F^2$ წყვილებისა, რომელებიც აკმაყოფილებს მოცემულ განტოლებას, ეწოდება n-ური რიგის (ხარისხის) ალგებრული წირი F ველის მიმართ. მაგალითად,

$$a_1X^2+a_2X+a_3XY+a_4Y^2+a_5Y+a_6=0,$$

სადაც $a_1,a_2,a_3,a_4,a_5,\ a_6$ ნამდვილი რიცხვებია, არის მეორე რიგის წირი $\mathbb{R}$-ზე. მომავალში ჩვენ განვიხილავთ წირებს მხოლოდ სასრული ველების მიმართ.

იმ წერტილებს, რომელებშიც $f(X,Y)$-ის ერთი მაინც კერძო წარმოებული $\frac{df}{dX}$ ან $\frac{df}{dY}$ ნულია, ეწოდებათ განსაკუთრებული წერტილები, ანუ E ალგებრული წირის (x_0,y_0) წერტილს ეწოდება განსაკუთრებული, თუ

$$\left.\frac{dE}{dX}\right|_{\substack{X=x_0\\Y=y_0}}=0 \quad \text{ან} \quad \left.\frac{dE}{dY}\right|_{\substack{X=x_0\\Y=y_0}}=0.$$

ალგებრულ წირს ეწოდება გლუვი, თუ მას არა აქვს განსაკუთრებული წერტილები. მესამე რიგის გლუვ წირებს ეწოდებათ ელიფსური წირები.

მათემატიკურ გამოკვლევებში ხშირად გამოიყენება ალგებრულ განტოლებათა სხვადასხვა ფორმები, რომლებიც გვაძლევენ ელიფსურ წირებს და ამ განტოლებებს ნორმალური ანუ სტანდარტული ფორმები ეწოდებათ. უნდა აღინიშნოს, რომ ამ განტოლებათა უმრავლესობა XIX და XX საუკუნეებში იყო მიღებული ელიფსური წირების გამოკვლევებისას კომპლექსურ რიცხვთა ველის მიმართ. ყველაზე ხშირად გავრცელებულია ვაიერშტრასის ნორმალური ფორმის სხვადასხვა მოდიფიკაციები, რომელთა სახელწოდებაც მოდის ვაიერშტრასის ფუნქციის თვისებებიდან. განტოლებას $(\varrho')^2=4\varrho^3-60c_2\varrho-140c_3$ ეწოდება ვეიერშტრასის ნორმალური ფორმა, სადაც

$$\varrho(z) = \frac{1}{z^2} \sum_{\substack{l \in \Lambda, \\ l \neq 0}} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right)$$

ვაიერშტრასის ფუნქციაა. აქ $\Lambda = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}$ მესერია და ω_1, ω_2 ისეთი კომპლექსური რიცხვებია, რომ $\mathrm{Im}\frac{\omega_1}{\omega_2} > 0$.

ელიფსური წირის ვეიერშტრასის ფორმა შეიძლება ჩაიწეროს შემდეგი სახით:

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \text{ სადაც } a_k \in F.$$

თუ F ველის მახასიათებელი:

ა) $char(F) = 2$, მაშინ ნებისმიერ ელიფსურ წირს აქვს სახე

$$Y^2 + cY = X^3 + aX + b \quad \text{ან} \quad Y^2 + cXY = X^3 + aX^2 + b.$$

ბ) $char(F) = 3$, მაშინ ნებისმიერ ელიფსურ წირს აქვს სახე

$$Y^2 = X^3 + aX^2 + bX + c\,.$$

გ) $char(F) \neq 2$ და $char(F) \neq 3$, მაშინ ნებისმიერ ელიფსურ წირს აქვს სახე

$$Y^2 = X^3 + aX + b\,.$$

მომავალში ჩვენ უფრო დაწვრილებით განვიხილავთ ამ მესამე შემთხვევას.

2.1. ელიფსური წირის წერტილები

$Y^2 = X^3 + aX + b$ ელიფსური წირისათვის განვიხილოთ სიმრავლე E, რომელიც შედგება ყველა იმ $P = (x, y)$ წერტილებისაგან, რომლებიც მოცემულ განტოლებას აკმაყოფილებს და ე.წ. „უსასრულოდ დაშორებული წერტილისაგან“ - O. წერტილთა ამ სიმრავლეზე განიმარტება შეკრების ოპერაცია, რომლის ნეიტრალური ელემენტია O. ამიტომ $-O = O$. გარდა ამისა, ადვილი საჩვენებელია, რომ $(x, y) \in E$ მაშინ და მხოლოდ მაშინ, როდესაც $(x, -y) \in E$. ამიტომ $P = (x, y)$ წერტილის მოპირდაპირეა $-P = (x, -y)$ წერტილი. მაშასადამე, $-(x, y) = (x, -y)$, ანუ, თუ $P = (x, y)$, მაშინ $-P = (x, -y)$. ამასთანავე გვაქვს:

$$(x, y) + (x, -y) = 0, \text{ ანუ } P + (-P) = O;$$

$(x, y) + O = O + (x, y) = (x, y)$, ანუ თუ $P \in E$ ნებისმიერი წერტილი, მაშინ $P + O = O$;

$$O + O = O.$$

ზოგად შემთხვევაში, როცა წირს აქვს სახე

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

მაშინ $-(x, y) = (x, \tilde{y})$, სადაც $\tilde{y} = -a_1x - a_3 - y$. მართლაც,

$$(-a_1x - a_3 - y)^2 + a_1x(-a_1x - a_3 - y) + a_3(-a_1x - a_3 - y) = y^2 + a_1xy + a_3y,$$

ე.ი.

$$-(x, y) = (x, \tilde{y}) = (x, -a_1x - a_3 - y).$$

E სიმრავლის ნებისმიერი ორი წერტილის ჯამის განმარტებისათვის დაგვჭირდება რამდენიმე ფაქტი, რომლებსაც ახლა განვიხილავთ. როგორც ზემოთ აღვნიშნეთ, ვაიერშტრასმა აჩვენა, რომ ნებისმიერი ელიფსური წირი შეიძლება ჩაიწეროს შემდეგი სახით:

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \quad \text{სადაც } a_k \in F.$$

ამ ფორმულას ეწოდება ელიფსური წირის ვაიერშტრასის გრძელი ფორმა. წირი გლუვია, თუ $a_1Y = 3X^2 + 2a_2X + a_4$ და $2Y + a_1X + a_3 = 0$ განტოლებებს არა აქვთ ამონახსნი. ეს გამომდინარეობს იმ ფაქტიდან, რომ თუ

$$f(X, Y) = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6,$$

მაშინ

$$\frac{df}{dX} = a_1Y - 3X^2 - 2a_2X - a_4 \quad \text{და} \quad \frac{df}{dY} = 2Y - a_1X - a_3.$$

თუ F ველის მახასიათებელი არ არის 2, $char(F) \neq 2$, მაშინ წრფივი გარდაქმნით

$$Y \to Y - \frac{a_1Y + a_3}{2}$$

წირი შეიძლება მივიყვანოთ სახეზე:

$$Y^2 = X^3 + a_2X^2 + a_4X + a_6$$

და შემდეგ, თუ F ველის მახასიათებელი არ არის არც 3, ანუ $char(F) \neq 2$ და $char(F) \neq 3$, მაშინ წრფივი გარდაქმნით

$$X \to X - \frac{1}{3}a_2$$

წირი შეიძლება მივიყვანოთ სახეზე

$$Y^2 = X^3 + aX + b,$$

რომელსაც ვაიერშტრასის მოკლე ფორმა ეწოდება.

ვთქვათ, E წირი მოცემულია განტოლებით

$$E: Y^2 = X^3 + aX + b. \tag{1}$$

რომლის გრაფიკი სიმეტრიულია აბცისათა ღერძის მიმართ. რომ ვიპოვოთ მისი თანაკვეთა აბცისათა ღერძთან, საჭიროა ამოვხსნათ განტოლება

$$X^3 + aX + b = 0. \tag{2}$$

ამ კუბური განტოლების ამონახსნი ვეძებოთ ასეთი სახით

$$X = u + v.$$

მაშასადამე, უნდა მოვძებნოთ u და v ისეთი, რომ $u + v$ აკმაყოფილებდეს (2) განტოლებას.

მაშინ

$$(u + v)^3 + a(u + v) + b = 0,$$

ანუ

$$u^3 + 3u^2v + 3uv^2 + v^3 + au + av + b = 0,$$

$$u^3 + v^3 + 3uv(u + v) + a(u + v) + b = 0.$$

ეს ტოლობა შესრულდება, თუ ვიპოვეთ u და v ისეთი, რომ

$$\begin{cases} u^3 + v^3 = -b \\ 3uv(u + v) = -a(u + v) \end{cases}, \quad \text{ანუ} \quad \begin{cases} u^3 + v^3 = -b \\ uv = -\dfrac{a}{3} \end{cases}, \quad \text{ე.ი.} \quad \begin{cases} u^3 + v^3 = -b \\ u^3v^3 = -\left(\dfrac{a}{3}\right)^3 \end{cases}.$$

ასეთი u^3 და v^3 არის შემდეგი კვადრატული განტოლების ამონახსნები

$$x^2 + bx - \left(\frac{a}{3}\right)^3 = 0,$$

რომლის დისკრიმინანტი

$$D = 4\left(\frac{a}{3}\right)^3 + 4\left(\frac{b}{2}\right)^2.$$

საიდანაც

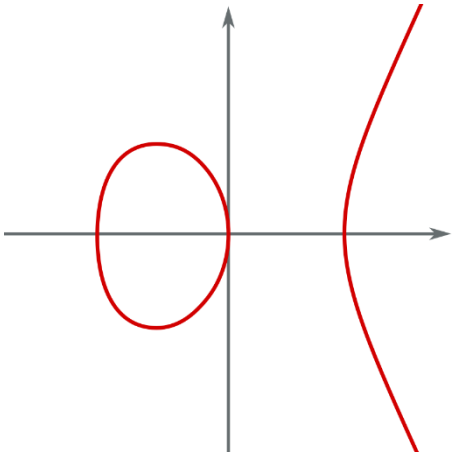
$$u^3, v^3 = -\frac{b}{2} \pm \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}.$$

შევნიშნოთ, რომ აქედან მიიღება კარდანოს ცნობილი ფორმულები.

2.2. გეომეტრია ელიფსურ წირებზე

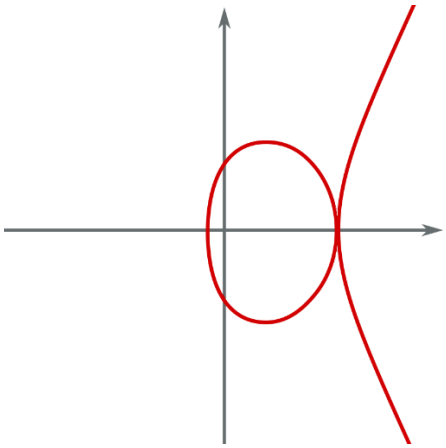
გვაქვს სამი შემთხვევა:

1) თუ $D > 0$, მაშინ (2) განტოლებას აქვს 3 განსხვავებული ნამდვილი ფესვი α, β, γ.



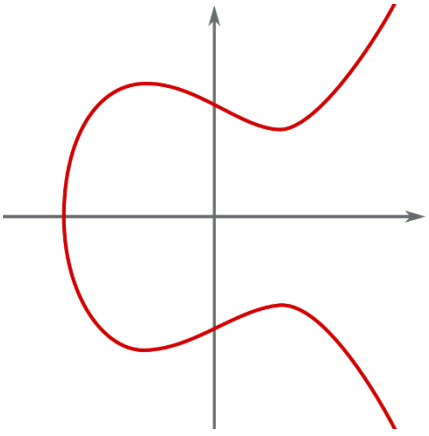
სურ.1. ელიფსური წირი, როცა $D > 0$.

2) თუ $D = 0$, მაშინ (2) განტოლებას აქვს 3 ნამდვილი α, β, β, რომელთგანაც ორი მაინც ერთმანეთის ტოლია.



სურ.2. ელიფსური წირი, როცა $D = 0$.

3) თუ $D < 0$, (2) განტოლებას აქვს ერთი ნამდვილი α და ორი კომპლექსური ფესვი.



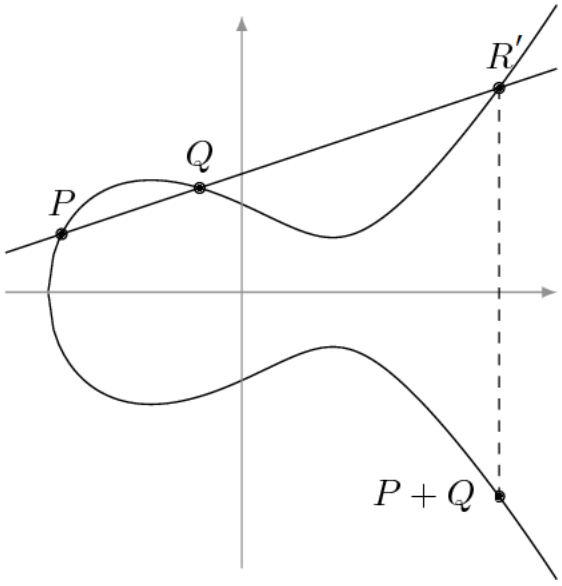
სურ.3. ელიფსური წირი, როცა $D < 0$.

სურ. 2-ზე მოცემული წირი სინგულარულია. სინგულარობის $(\beta,0)$ წერტილში (განსაკუთრებულ წერტილში) მას აქვს ორი მხები. ამ შემთხვევას ჩვენ არ განვიხილავთ ანუ ვიხილავთ მხოლოდ $D \neq 0$ შემთხვევას, რაც ექვივალენტურია შემდეგი პირობის

$$4a^3 + 27b^2 \neq 0 \quad (3)$$

ახლა ვთქვათ, ელიფსური E წირი მოცემულია (1) განტოლებით და შესრულებულია (3) პირობა. განვსაზღვროთ წირზე წერტილთა ჯამის ოპერაცია შემდეგნაირად.

E წირზე ავიღოთ ორი განსხვავებული $P = (x_1, y_1)$, $Q = (x_2, y_2)$ წერტილი და გავავლოთ მათზე წრფე. ეს წრფე წირს გადაკვეთს მესამე, P და Q წერტილებისაგან განსხვავებულ წერტილში, რომელიც აღვნიშნოთ R'-ით. ასეთი წერტილი აუცილებლად არსებობს, რადგანაც თუ კუბურ განტოლებას აქვს ორი ნამდვილი ფესვი, რომელიც შეესაბამება P და Q წერტილებს, შესაბამისად მას მესამე ფესვიც ექნება, რომელსაც შეესაბამება R'.



სურ.4. წერტილთა კომპოზიცია

R წერტილს, კოორდინატებით (x_3, y_3), რომელიც მიიღება R' წერტილის ორდინატის ნიშნის შეცვლით (ანუ R არის R' წერტილის OX ღერძის მიმართ სიმეტრიული წერტილი) ვუწოდოთ P და Q წერტილების ჯამი

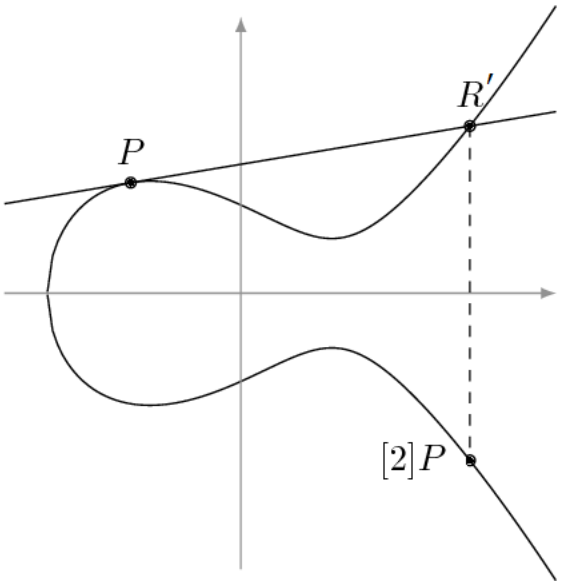
$$R = P + Q.$$

ვთქვათ, $P \in E$ წერტილის კოორდინატებია (x, y), მაშინ $-P$ წერტილის კოორდინატები იქნება $(x, -y)$. ჩავთვალოთ, რომ ვერტიკალური წრფე, რომელიც P და $-P$ წერტილებზე

გადის, E წირს კვეთს უსასრულოდ დაშორებულ O წერტილში, ე.ი. $P + (-P) = O$, ანუ, შეთანხმებით

$$P + O = O + P = P.$$

უსასრულოდ დაშორებული O წერტილი ელიფსურ წირზე ასრულებს 0-ის როლს. წარმოვიდგინოთ, რომ P და Q წერტილები ერთმანეთს უახლოვდება, ანუ $P = Q = (x_1, y_1)$, მაშინ მათი ჯამი $R = (x_3, y_3) = P + Q = P + P$ იქნება, თუ P წერტილში გავავლებთ მხებს და ვიპოვით ამ მხების წირთან გადაკვეთის წერტილის OX ღერძის მიმართ სიმეტრიულ R წერტილს (იხ. სურ. 5)



სურ.5. წერტილის გაორმაგება $R = P + P = [2]P$

ამ შემთხვევაში გამოვიყენებთ შემდეგ აღნიშვნას: $R = P + P = [2]P$.

ახლა გამოვიყვანოთ ფორმულები, რომლითაც გამოითვლება R წერტილის (x_3, y_3) კოორდინატები P და Q წერტილების (x_1, y_1) და (x_2, y_2) კოორდინატების საშუალებით.

განვიხილოთ შემთხვევა, როცა $P \neq \pm Q$ და $R = P + Q$ (იხ. სურ. 4). k-ით აღვნიშნოთ P და Q წერტილებზე გამავალი წრფის საკუთხო კოეფიციენტი. ცხადია,

$$k = \frac{y_2 - y_1}{x_2 - x_1}.$$

მაშინ წრფის განტოლებას ექნება სახე

$$y - y_1 = k(x - x_1). \tag{4}$$

მიღებული y შევიტანოთ წირის განტოლებაში, ანუ ვიპოვოთ წირთან გადაკვეთის წერტილი, ე.ი.

$$\big(y_1 + k(x - x_1)\big)^2 = x^3 + ax + b.$$

მარცხენა მხარეს თუ ავიყვანთ კვადრატში და დავაჯგუფებთ, მივიღებთ კუბურ განტოლებას

$$x^3 - k^2x^2 + \ldots = 0.$$

ცხადია (ვიეტის თეორემით), რომ კუბურ განტოლების ფესვთა ჯამი ტოლია x^2-ის კოეფიციენტის მოპირდაპირე ნიშნით

$$x_1 + x_2 + x_3 = k^2.$$

აქედან $x_3 = k^2 - x_1 - x_2$. თუ x_3-ის მიღებულ მნიშვნელობას ჩავსვამთ (4) განტოლებაში, R'-სთვის მივიღებთ

$$y_3^{'} = y_1 + k(x_3 - x_1).$$

თუ ნიშანს შევცვლით, გვაქვს

$$y_3 = k(x_1 - x_3) - y_1.$$

ახლა განვიხილოთ $R = [2]P$ წერტილის შემთხვევა. (1)-ის გაწარმოებით ვწერთ

$$2yy^{'} = 3x^2 + a.$$

მხების საკუთხო კოეფიციენტი P წერტილში წარმოებულის მნიშვნელობის ტოლია, ანუ

$$k = \frac{3x_1^2 + a}{2y_1},$$

შემდეგ, R წერტილის კოორდინატების მიღება გრძელდება ანალოგიურად. შევნიშნოთ, რომ თუ P წერტილის ორდინატა 0-ია, მაშინ მხები ორდინატთა ღერძის მართობულია და

$$[2]P = O.$$

მაშასადამე, თუ $P = (x_1, y_1)$, $Q = (x_2, y_2)$ წერტილები $Y^2 = X^3 + aX + b$ განტოლებით მოცემული E წირის წერტილებია, მაშინ

- თუ $P \neq Q$ და $x_1 = x_2$, მაშინ $P + Q = 0$,
- თუ $P = Q$ და $y_1 = 0$, მაშინ $P + Q = 2P = 0$,
- თუ $P \neq Q$ და $x_1 \neq x_2$, მაშინ

$$k = \frac{y_2 - y_1}{x_2 - x_1}, \qquad s = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1},$$

- თუ $P = Q$ და $y_1 \neq 0$, მაშინ

$$k = \frac{3x_1^2 + a}{2y_1}, \qquad s = \frac{-x^3 + ax + 2b}{2y},$$

$$P + Q = (k^2 - x_1 - x_2, -k^3 + k(x_1 + x_2) - s).$$

2.3. ალგებრა ელიფსურ წირებზე

ელიფსურ წირის წერტილები ზემოთგანსაზღვრული შეკრების ოპერაციის მიმართ ქმნიან აბელურ ჯგუფს, ანუ ელიფსურ წირის წერტილებს აქვს შემდეგი თვისებები:

1) $P + Q = Q + P$ ნებისმიერი $P, Q \in E$ წერტილისათვის.

2) $P + (Q + S) = (P + Q) + S$ ნებისმიერ $P, Q, S \in E$ წერტილისათვის.

3) არსებობს ნულოვანი ელემენტი O (წერტილი უსასრულობაში), ისეთი რომ $P + O = O + P = P$ ნებისმიერ $P \in E$ წერტილისათვის.

4) ყოველი $P \in E$ წერტილისათვის არსებობს წერტილი $-P \in E$, ისეთი რომ

$$P + (-P) = O.$$

თუ a და b არის F ველის ელემენტები და P და Q წერტილების კოორდინატებიც არის F ველიდან, მაშინ $P + Q$, $2P$, $3P$-ს, ... წერტილების კოორდინატებიც F ველშია. ელიფსური წირის შესაბამისი კუბური განტოლება არის ორი ცვლადის $f(X, Y) = 0$ განტოლება, რომლის

განსაზღვრის არეა F ველი. ჩვეულებრივ, F ველი არის კომპლექსურ რიცხვთა ველი $\mathbb{C}$, ან ნამდვილ რიცხვთა ველი $\mathbb{R}$, ან რაციონალურ რიცხვთა ველი $\mathbb{Q}$ (ამ ველთა მახასიათებელია 0), ან სასრული ველი.

იმის მიხედვით თუ როგორია F ველი, $E(F)$ - ელიფსური წირის წერტილთა სიმრავლეც F ველიდან განსხვავებულია. $E(F)$-ის თვისებები მოცემულია შემდეგ თეორემებში.

თეორემა 1. (H. Poincare, ≈1900) ([6], გვ. 27). ვთქვათ, F ველია და E ელიფსური წირი მოცემულია განტოლებით

$$E: Y^2 = X^3 + aX + b, \text{სადაც } a \text{ და } b \in F.$$

თუ

$$E(F) = \{(x, y) \in E: x, y \in F\} \cup \{0\},$$

მაშინ $E(F)$ არის E-ს ყველა წერტილთა ჯგუფის ქვეჯგუფი.

თეორემა 2. (L.J. Mordell, 1922) ([6], გვ. 38). ვთქვათ, ელიფსური წირი E მოცემულია განტოლებით

$$E: Y^2 = X^3 + aX + b, \text{სადაც } a \text{ და } b \in \mathbb{Q}.$$

მაშინ რაციონალურ წერტილთა $E(\mathbb{Q})$ ჯგუფი არის სასრულად წარმოქმნილი აბელური ჯგუფი, ანუ არსებობს სასრული სიმრავლე $P_1, P_2, \dots, P_t \in E(\mathbb{Q})$ ისეთი, რომ ყოველი $P \in E(\mathbb{Q})$ წერტილი ჩაიწერება შემდეგი სახით: $P = n_1P_1 + n_2P_2 + \dots + n_tP_t$, სადაც $n_1, \dots, n_t \in \mathbb{Z}$.

თეორემა 3. (C.L. Siegel, 1928) ([6], გვ. 41). ვთქვათ, ელიფსური წირი E მოცემულია განტოლებით

$$E: Y^2 = X^3 + aX + b, \qquad \text{სადაც } a \text{ და } b \in \mathbb{Z}.$$

მაშინ E-ს აქვს მხოლოდ სასრული რაოდენობა წერტილებისა, რომელთა კოორდინატები მთელია, ანუ $E(\mathbb{Z})$ სასრულია.

თეორემა 4. (H. Hasse, 1922) ([1], გვ. 26). ვთქვათ, ელიფსური წირი E მოცემულია განტოლებით

$$E: Y^2 = X^3 + aX + b, \qquad \text{სადაც } a \text{ და } b \in F_p.$$

მაშინ

$$\left|\#\, E(F_p) - (p+1)\right| \leq 2\sqrt{p}.$$

პრაქტიკული თვალსაზრისით, რადგან კომპიუტერები უფრო ეფექტურად მუშაობენ ველებზე მახასიათებლით 2, ამიტომ ხშირად გამოიყენება F_q სასრული ველები $q = 2^k$ ელემენტით.

ველისათვის, რომლის მახასიათებელია 2, განტოლება $Y^2 = X^3 + aX + b$ ყოველთვის სინგულარულია (აქვს განსაკუთრებული წერტილები), ამიტომ იხილავენ უფრო ზოგად განტოლებას, $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. მეცნიერთა ჯგუფი (Sato, Kedlaya, Lauder, Wan, Denef, Vercauteren, ...) მუშაობდნენ და აქვთ შედეგები $\#E(F_p)$-ის შეფასებისთვის, როცა $q = p^k$ და p პატარა მარტივი რიცხვია. ერთ-ერთი ყველაზე გავრცელებული და შესწავლილი წირია კობლიცის წირი (Koblitz curve), რომელსაც აქვს სახე

$$y^2 + xy = x^3 + ax^2 + 1, \text{სადაც } a = \ 0 \ \text{ან} \ 1.$$

კობლიცის E წირის კოეფიციენტები ეკუთვნის F_2-ს (პრაქტიკული ამოცანებისთვის გამოიყენება აგრეთვე $E(F_q)$, სადაც $q = 2^k$ და $k \geq 160$).

კობლიცის წირისთვის მიღებულია ზუსტი ფორმულა

$$\#E(F_{2^k}) = 2^k - \left(\frac{-1+\sqrt{-7}}{2}\right)^k - \left(\frac{-1-\sqrt{-7}}{2}\right)^k + 1.$$

3. კრიპტოსისტემები ელიფსურ წირებზე

ვნახეთ, რომ წირზე წერტილების კომპოზიციის განმარტებისათვის გამოიყენება რიცხვებზე შეკრების, გამოკლების, გამრავლებისა და გაყოფის ოპერაციები. ეს ნიშნავს, რომ მიღებული შედეგები ასევე სამართლიანი იქნება, თუ იგივე ოპერაციებს ჩავატარებთ F_p სარულ ველზე ანუ მთელ რიცხვებზე მარტივი p მოდულით.

ამ შემთხვევაში შეკრება, გამოკლება, გამრავლება სრულდება p მოდულით, ხოლო გაყოფა $\frac{u}{v}$ კი - u-ს გამრავლებით v^{-1}-ზე მოდულით p. მაშასადამე,

$$\frac{u}{v} = uv^{-1} \,(mod\, p)$$

მოდულის მარტივობა საჭიროა იმისათვის, რომ ნებისმიერი ნატურალური $v < p$ რიცხვისათვის არსებობდეს მისი შებრუნებული v^{-1} ისეთი, რომ სრულდებოდეს პირობა

$$vv^{-1} \equiv 1(mod\, p).$$

ასეთნაირად ჩვენ მივიღებთ წერტილებს წირზე

$$E: Y^2 = X^3 + aX + b(mod\, p), \tag{5}$$

სადაც X, Y ცვლადებია, ხოლო a და b ორივე ნაკლებია p-ზე. a და b რიცხვებისთვის უნდა სრულდებოდეს პირობა

$$(4a^3 + 27b^2)\, mod\, p \neq 0. \tag{6}$$

სიმრავლე $E_p(a, b)$ შედგება ყველა (x, y) წერტილებისგან

$$0 \leq x, y < p,$$

რომელიც აკმაყოფილებს (5) განტოლებას და O წერტილისაგან უსასრულობაში.

განვიხილოთ ორი მაგალითი:

1. $E_7(2,6): Y^2 = X^3 + 2X + 6(mod\, 7)$. (7)

   შევამოწმოთ პირობა (6).

   $$(4 \cdot 2^3 + 27 \cdot 6^2)\, mod\, 7 = 4 \cdot 1 + 6 \cdot 1 = 3 \neq 0,$$

   ე.ი. მოცემული წირი არასინგულარულია. წირის წერტილებია:

$$(1,\pm 3),\ (2,\pm 2),\ (3,\pm 2),\ (4,\pm 1),\ (5,\pm 1),\ \mathcal{O}.$$

ავიღოთ ნებისმიერი წერტილი $E_7(2,6)$-დან, მაგალითად $x = 5$, მაშინ

$$y^2 \equiv 1(mod\ 7) \Longrightarrow y \equiv 1(mod\ 7) \text{ ან } y \equiv -1(mod\ 7).$$

ვიპოვეთ ორი წერტილი (5,1) და (5,6).

ვიპოვოთ წერტილი [2] (5,1)

$$k = \frac{3 \cdot 5^2 + 2}{2 \cdot 1} = 0(mod\ 7),$$
$$x_3 = -10 = 4(mod\ 7),$$
$$y_3 = 0 \cdot (5-4) - 1 = 6(mod\ 7),$$

მივიღეთ, რომ $[2]\ (5,1) = (4,6)$, შეგვიძლია დავრწმუნდეთ, თუ ჩავსვამთ მის კოორდინატებს (7)-ში, რომ მიღებული წერტილი ეკუთვნის წირს.

ვიპოვოთ $[3]\ (5,1) = (5,1) + (4,6)$,

$$k = \frac{6-1}{4-5} = \frac{5}{6} = 5 \cdot 6 = 2(mod\ 7),$$
$$x_3 = 2^2 - 5 - 4 = 2(mod\ 7),$$
$$y_3 = 2 \cdot (5-2) - 1 = 2 \cdot 3 - 1 = 5(mod\ 7).$$

მივიღეთ, რომ $[3]\ (5,1) = (2,5)$, ე.ი. ვიპოვეთ ოთხი წერტილი.

წირის კრიპტოგრაფიული გამოყენებისთვის საჭიროა ვიცოდეთ სულ რამდენი წერტილია $E_7(2,6)$–წირზე. შევნიშნოთ, რომ მოცემული ჯგუფი ციკლურია ანუ ყოველი წერტილი არის წარმომქნელი.

2. $E_{37}(-5,8): Y^2 = X^3 - 5X + 8(mod\ 37)$.

შევამოწმოთ პირობა (6).

$$(4 \cdot (-5)^3 + 27 \cdot 8^2)\ mod\ 37 = 4 \cdot (-14) + (-10) \cdot (-10) = 18 + 11 = 29 \neq 0,$$

ე.ი. მოცემული წირი არასინგულარულია. წირის წერტილებია:

$$(1,\pm 2), (5,\pm 21), (6,\pm 3), (8,\pm 6), (9,\pm 27), (10,\pm 25),$$
$$(11,\pm 27), (12,\pm 23), (16,\pm 19), (17,\pm 27), (19,\pm 1),$$
$$(20,\pm 8), (21,\pm 5), (22,\pm 1), (26,\pm 8), (28,\pm 8), (30,\pm 25),$$
$$(31,\pm 9), (33,\pm 1), (34,\pm 25), (35,\pm 26), (36,\pm 7), \mathcal{O}.$$

შევნიშნოთ, რომ მოცემული ჯგუფი ორი ციკლური ჯგუფის ნამრავლია

$$E_{37}(-5,8) \cong C_3 \times C_{15}.$$

სამართლიანია შემდეგი

თეორემა 5. სასრულ სივრცეში, ჯგუფი $E_p(a,b)$ ყოველთვის არის ციკლური ჯგუფი ან ორი ციკლური ჯგუფის ნამრავლი.

რამდენიმე სიტყვით დავახასიათოთ $E_p(a,b)$. ცხადია, ეს სიმრავლე სასრულია და მასში შედიან წერტილები მთელი კოორდინატებით (x,y), სადაც $0 \le x, y < p$. არსებობს პირდაპირი ანალოგია $E_p(a,b)$ სიმრავლესა და წერტილის ჯერადებს შორის, ანუ უფრო ზუსტად $E_p(a,b)$-ში არსებობს წარმომქნელი G, ისეთი, რომ მიმდევრობა $G,\ [2]G,\ [3]G, \dots, [n]G$ არის $E_p(a,b)$-ს ელემენტები, სადაც $n = \#E_p(a,b)$. ამასთანავე, $[n]G = \mathcal{O}$.

p, a, b პარამეტრების არჩევისას, წირზე რიცხვთა რაოდენობა შეიძლება იყოს მარტივი რიცხვი, ანუ $\#E_p(a,b)$ იყოს მარტივი. ამ შემთხვევაში ნებისმიერი წერტილი არის მთელი სიმრავლისთვის წარმომქმნელი.

3.1. დისკრეტული ლოგარითმის პოვნის ალგორითმი

ვთქვათ, b არის F_q^*-ის წარმომქმნელი, მაშინ ნებისმიერი x-სთვის ადვილად გამოითვლება $y \equiv [x]b \ (mod\ q)$. შებრუნებული ამოცანა, რომელსაც ტრადიციულად ეწოდება დისკრეტული ლოგარითმი ([2], გვ. 57) ყალიბდება შემდეგნაირად: თუ ვიცით b და y, ვიპოვოთ x რიცხვი, ისეთი რომ, $y \equiv [x]b \ (mod\ q)$, ეს ამოცანა საკმაოდ ძნელია როცა სათანადო პარამეტრებია არჩეული და ამჟამად ცნობილი საუკეთესო ალგორითმებითაც კი გვჭირდება იმ რაოდენობის არითმეტიკული ოპერაცია, რაც დროში ისე გრძელდება რომ თითქმის ამოუხსნელია. განვიხილოთ Silver, Pohlig, Hellman-ის ალგორითმი.

F_q^* არის n რიგის ციკლური ჯგუფი. ვთქვათ,

$$n = \prod_{p|n} p^k$$

და p მარტივი გამყოფები პატარა რიცხვებია. მოცემულია b და y და უნდა ვიპოვოთ x რიცხვი ისეთი, რომ $y \equiv [x]b \ (mod\ q)$.

1. n-ის ყოველი p მარტივი გამყოფისათვის ვიპოვოთ $r_{p,j} = \left[j\frac{n}{p}\right]b$, რომლის p ჯერადი $\mathcal{O}$-ია. მართლაც, $[p]\left(\left[j\frac{n}{p}\right]b\right) = [jn]b = \mathcal{O}$ (როგორც ვიცით, F_q^* არის n რიგის ციკლური ჯგუფი), აქ $j = 0, 1, 2, \dots, p-1$. მაშასადამე, შევადგინეთ $r_{p,j}$-ების ცხრილი.

2. დავუშვათ $x = x_0 + x_1 p + x_2 p^2 + \cdots + x_{k-1}p^{k-1} (mod\ p^k)$, სადაც $0 \le x_i < p$. x_0-ის საპოვნელად გამოვთვალოთ $\left[\frac{n}{p}\right]y$, რადგან $[n]y = \mathcal{O}$, მაშასადამე, თუ გავითვალისწინებთ, რომ $y = [x]b$, მაშინ

$$\left[\frac{n}{p}\right]y = \left[\frac{n}{p}\right][x]b = \left[\frac{n}{p}\right][x_0 + tp]b = \left[\frac{n}{p}\right][x_0]b = r_{p,x_0}.$$

მაგრამ ჩვენ შედგენილი გვაქვს $r_{p,j}$-ები და x_0 არის ის j, რომლისთვისაც დაემთხვევა r_{p,x_0} და $r_{p,j}$.

3. ვიპოვოთ ახლა x_1, განვიხილოთ

$$y_1 = y - [x_0]b = [x]b - [x_0]b = [x_1 p + x_2 p^2 + \cdots + x_{k-1}p^{k-1}]b = [t_1 p]b.$$

რადგან $\left[\frac{n}{p}\right]y_1 = \mathcal{O}$, ამიტომ $\left[\frac{n}{p^2}\right]y_1$ -სთვის გვაქვს

$$\left[\frac{n}{p^2}\right]y_1 = \left[\frac{n}{p^2}\right][x_1 p + x_2 p^2 + \cdots + x_{k-1}p^{k-1}]b = \left[\frac{n}{p}\right][x_1]b = r_{p,x_1},$$

მაგრამ ჩვენ შედგენილი გვაქვს $r_{p,j}$-ები და x_1 არის ის j, რომლისთვისაც დაემთხვევა r_{p,x_1} და $r_{p,j}$.

4. ასე შეგვიძლია ვიპოვოთ x_0, x_1 და ა.შ. x_{k-1}, კერძოდ, ყოველი $i = 1, 2, \dots, k-1$ -სთვის,

$$y_i = y - [x_0 + x_1 p + x_2 p^2 + \cdots + x_{i-1}p^{i-1}]b$$

და რადგან $\left[\frac{n}{p^i}\right]y_i = \mathcal{O}$, ამიტომ $\left[\frac{n}{p^{i+1}}\right]y_1$ -სთვის გვექნება, რომ $\left[\frac{n}{p^{i+1}}\right]y_1 = r_{p,x_i}$. მაგრამ ჩვენ შედგენილი გვაქვს $r_{p,j}$-ები და x_i არის ის j, რომლისთვისაც დაემთხვევა r_{p,x_i} და $r_{p,j}$.

5. ასეთნაირად ვიპოვით x-ს n-ის ყოველი p^k გამყოფისათვის და შემდეგ ნაშთთა შესახებ ჩინური თეორემის ძალით ვიპოვოთ x-ს $mod\ n$, ანუ ვიპოვით x რიცხვს ისეთს, რომ $y \equiv [x]b (mod\ q)$.

თუ ვიცით P და Q წერტილები, ვიპოვოთ m რიცხვი, ისეთი რომ, $Q = [m]P$. ეს ამოცანა საკმაოდ ძნელია. თუ პარამეტრებს ავირჩევთ ისე, როგორც შემდეგშია ნაჩვენები, მაშინ m-ის საპოვნელად ამჟამად ცნობილი საუკეთესო ალგორითმებითაც კი გვჭირდება $O(\sqrt{q})$ ოპერაცია წირებზე, სადაც q არის იმ ქვესიმრავლის სიმძლავრე, რომელსაც ეკუთვნის P და Q წერტილები. წირებზე ყველა გამოთვლა ტარდება მოდულით p (ე.ი. დაახლოებით $log\, p = log\, q$, ანუ $O(\sqrt{q})$).

4. კრიპტოსქემების გამოყენებები

ნებისმიერი კრიპტოსისტემა, რომელიც ეფუძნება დისკრეტულ ლოგარითმს, ადვილად შეიძლება იყოს გადატანილი ელიფსურ წირებზე. ძირითადი პრინციპი მდგომარეობს

$$y \equiv g^x (mod\, p)$$

ოპერაციის შეცვლისა $y \equiv [x]G(mod\, p)$ ოპერაციით.

4.1. El-Gamal-ის შიფრი ელიფსურ წირებზე

ვთქვათ, არჩეული გვაქვს ელიფსური წირი $E_p(a, b)$ წარმომქმნელი G წერტილით ისეთი, რომ G, $[2]G$, $[3]G, \dots, [q]G$ იყოს განსხვავებული და $[q]G = O$ რაიმე q მარტივი რიცხვისთვის. თითოეული მომხმარებელი U ირჩევს შემთხვევით c_U რიცხვს, რომელიც არის მისი საიდუმლო გასაღები და გამოთვლის წირზე $D_U = [c_U]G$, რაც არის მისი ღია გასაღები. წირის პარამეტრები და ღია გასაღებთა ჩამონათვალი აქვს ქსელის ყველა მომხარებელს. ვთქვათ A მომხმარებელმა უნდა გაუგზავნოს B მომხმარებელს m შეტყობინება (m-ს აქვს რიცხვის სახე, $m < p$).

A აკეთებს შემდეგს:

1) ირჩევს შემთხვევით k რიცხვს, $0 < k < q$;

2) გამოთვლის $R = [k]G$, $P = [k]D_B = (x, y)$;

3) დაშიფრავს $e = mx\ (mod\ p)$;

4) უგზავნის B-ს დაშიფრულ ტექსტს (R, e).

B მიიღებს რა (R, e)-ს, აკეთებს შემდეგს:

1) გამოთვლის $Q = [c_B]R = (x, y)$;

2) გაშიფრავს $m' = ex^{-1}(mod\ p)$;

აქ დაგვჭირდა, რომ $[c_B]R = [c_B]([k]G) = [k]([c_B]G) = [k]D_B$,

ე.ი. $Q = P$, ამიტომ $m' = m$.

Q წერტილის x კოორდინატი მოწინააღმდეგისათვის არის უცნობი, რადგან მან არ იცის k რიცხვი. მოწინააღმდეგე შეეცდება k გამოთვალოს $[k]R$ წერტილიდან, მაგრამ ამისათვის საჭირო იქნება დისკრეტული ლოგარითმის გამოთვლა წირზე (იხ. [4], გვ. 485).

4.2. ელექტრონულ-ციფრული ხელმოწერა

მომხმარებლები ირჩევენ საერთო ელიფსურ წირს $E_p(a, b)$ და G წერტილს მასზე ისე, რომ $G,\ [2]G,\ [3]G, \dots, [q]G$ არის განსხვავებული წერტილები და $[q]G = O$ რაიმე მარტივი p-სთვის (p რიცხვის სიგრძე არის 256 ბიტი). ყოველი U მომხმარებელი აირჩევს საიდუმლო x_U გასაღებს $0 < x_U < q$ და გამოთვლის წერტილს წირზე $Y_U = [x_U]G$. წირის პარამეტრები და ღია გასაღების ჩამონათვალი ყველა მომხარებლისთვის ცნობილია. იმისთვის, რომ A მომხმარებელმა ხელი მოაწეროს m შეტყობინებას,

A აკეთებს შემდეგს:

1) ირჩევს შემთხვევით k რიცხვს, $0 < k < q$;

2) გამოთვლის $P = [k]G = (x, y)$;

3) გამოთვლის $r = x\ (mod\ q)$ (თუ $r = 0$-ს უბრუნდება 1-ს);

4) გამოთვლის $s = (km + rx_A)(mod\ q)$ (თუ $s = 0$-ს უბრუნდება ისევ 1-ს);

5) ხელს აწერს შემდეგი შეტყობინებით (r, s)-ით.

ნებისმიერმა მომხარებელმა რომ შეამოწმოს A-მ მოაწერა თუ არა ხელი, იქცევა შემდეგნაირად:

1) ამოწმებს არის თუ არა $0 < r, s < q$;

2) გამოთვლის $u_1 = sm^{-1}(mod\, q)$ და $u_2 = -rm^{-1}(mod\, q)$;

3) გამოთვლის წირზე წერტილების შემდეგ კომბინაციას

$$P = [u_1]G + [u_2]Y_A = (x, y),$$
$$P = [u_1]G + [u_2]Y_A = [(km + rx_A)m^{-1}]G + [-rm^{-1}][x_A]G =$$
$$= [k]G + [rx_A m^{-1}]G + [-rm^{-1}x_A]G = [k]G.$$

თუ $P = O$, მაშინ ხელმოწერა არ მიიღება,

ანუ, თუ $x \equiv r\ (mod\, q)$, მაშინ ხელმოწერა მიიღება, წინააღმდეგ შემთხვევაში არა.

ეს მეთოდი ანალოგიურია, როგორიც იყო P34.10-94-ში, მაგრამ ხარისხში აყვანა შეცვლილია წირზე ოპერაციების კომპოზიციით.

4.3. ელექტორნული არჩევნების კრიპტოსქემა

ელექტრონული არჩევნები ამცირებს ეკონომიკურ ხარჯს და ხმის დათვლის დროს. ეს სისტემა ამომრჩეველს უფლებას აძლევს საარჩევნო ბიულეტენი გააგზავნოს ინტერნეტით. ამ სისტემის დაცვისთვის აუცილებელი თვისებებია:

- **აუთენთიფიკაცია:** მხოლოდ ხმის მიმცემ ამომრჩეველს დართოს ნება არჩევნებში მონაწილეობის;
- **უნიკალურობა:** თითოულ ამომრჩეველს შეეძლოს მხოლოდ ერთხელ ხმის მიცემა;
- **საიდუმლოება:** მიცემული ხმა არ უნდა კავშირდებოდეს ამომრჩეველთან;
- **სამართლიანობა:** შუალედური შედეგები არ უნდა გამოაშკარავდეს არჩევნების დასრულებამდე.

იმისათვის, რომ დავიცვათ ზემოთ აღწერილი თვისებები, საჭიროა გამოვიყენოთ კრიპტოგრაფიული ტექნიკა:

დავყოთ არჩევნები სამ ჯგუფად: ამომრჩეველი, ადგილობრივი კომისია, ცენტრალური კომისია.

1. ამომრჩეველი აირჩევს სასურველ კანდიდატს, დაშიფრავს ბიულეტენს ცენტრალური კომისიის კრიპტოსისტემით, შემდგომ ელექტრონულად მოაწერს ხელს მიღებულს ადგილობრივი კრიპტოსისტემით და გადაუგზავნის ადგილობრივ კომისიას.
2. ადგილობრივი კომისია შეამოწმებს მიღებულს, ნახავს ელექტრონული ხელმოწერა სწორია თუ არა და ასევე აქვს თუ არა უფლება ხმის მიცემის. წარმატების შემთხვევაში დაშიფრულ ბიულეტინს გადაუგზავნის ცენტრალურ კომისიას.
3. ცენტრალური კომისია მიიღებს ბიულეტენებს. დროის გასვლის შემდგომ გაიშიფრება თითოეული ბიულეტენი და გამოცხადდება შედეგები.

საგულისხმობა, რომ ადგილობრივ კომისიას შეუძლია მხოლოდ აუთენთიფიკაცია და უნიკარულობა დაადასტუროს და ვერ შეძლებს ბიულეტენის გაშიფრვას, ასევე ცენტრალურ კომისიას არ შეუძლია ბიულეტენის ამომრჩეველთან დაკავშირება.

უფრო დაწვრილები განვიხილოთ თითოეული ნაბიჯი.

1. ადგილობრივი კომისია გამოიტანს ღიად:
   - ელიფსურ წირს $E_{p_j}(a_j, b_j)$;
   - წარმომქნელს G_j;
   - რაოდენობას q_j .
2. ამომრჩეველი ადგილობრივი კომისიის გამოტანილი მონაცემების მიხედვით აირჩევს დახურულ გასაღებს x_j, გამოთვლის ღია გასაღებს Y_j და მიღებულს შეატყობინებს ადგილობრივ კომისიას.
3. ცენტრალური კომისია გამოიტანს ღიად:
   - ელიფსურ წირს $E_{p_c}(a_c, b_c)$;
   - წარმომქნელს G_c;
   - რაოდენობას q_c ;
   - გასაღებს D_c;
   - კანდიდატთა შესაბამის რიცვებს $c_1, c_2, \dots, c_m$.

4. ამომრჩეველი ირჩევს კანდიდატს c_i-ს და შიფრავს ცენტრალური კომისიისთვის:
   - ირჩევს დახურულ გასაღებს $0 < k_c < q_c$;
   - გამოთვლის
   i. $R_c = [k_c]G_c$;
   ii. $P_c = [k_c]D_c = (x_c, y_c)$;
   iii. $e = c_i * x_c \ (mod\ p_c)$;
   - მივიღეთ (არჩევანის შიფრი) $M = (R_c, e)$.
5. ამომრჩეველი აწერს ხელს ელექტრონულად მიღებულ შიფრს:
   - ირჩევს დახურულ გასაღებს $0 < k_j < q_j$;
   - გამოთვლის
   i. $R_j = [k_j]G_j = (x_j, y_j)$;
   ii. $r = x_j \ (mod\ q_j)$;
   iii. $s = (k_j * M.e + r * x_j)\ mod q_{j;}$
   - მივიღეთ შიფრი $S = (r, s)$ და (ბიულეტინი) (M, S) ეგზავნება ადგილობრივ კომისიას.
6. ადგილობრივი კომისია განიხილავს მიღებულ (M, S) ბიულეტენს:
   - შეამოწმებს მოცემულ ამომრჩეველის ხმის მიცემის უფლებას;
   - გამოთვლის
   i. $u_1 = s * (M.e)^{-1} (mod\ q_j)$;
   ii. $u_2 = -r * (M.e)^{-1} (mod\ q_j)$;
   iii. წირზე:

$$[u_1]G_j + [u_2]Y_j = [(k_j * M.e + r * x_j) * (M.e)^{-1}]G_j + [-r * (M.e)^{-1}][x_j]G_j$$
$$= [k_j]G_j + [r * x_j * (M.e)^{-1}]G_j + [-r * (M.e)^{-1} * x_j]G_j = [k_j]G_j$$
$$= (x_j, y_j);$$

   - თუ გამოთვლილი x_j ემთხვევა r მაშინ ხელმოწერა მიიღება;
   - მიღებულ ხელმოწერილიან ბიულეტენის არჩევანის შიფრები გადაეგზავნება ცენტრალურ კომისიას.
7. ცენტრალური კომისია განიხილავს მიღებულ M არჩევანის შიფრს არჩევნების დასრულების შემდგომ:
   - გამოთვლის
   i. $Q = [x_c]R_c = [x_c][k_c]G_c = [k_c][x_c]G_c = [k_c]D_c = (x'_c, y'_c)$;

ii. $c' = e * {x'}_c^{-1}$;

- ცხადია $Q = P \Rightarrow {x'}_c = x_c \Rightarrow c' = c_i$;
- მიღებული კანდიდატების ხმები შეჯამდება და გამოქვეყნდება შედეგები.

4.4. პროგრამები

1. ხარისხის ნაშთი რეკურსიულად

$$num^{pow} (mod\ prime)$$

```
long PowMod(long num, long pow, long prime)
{
    if (pow == 1)
        return num % prime;
    if (pow % 2 == 1)
    {
        var odd = PowMod(num, pow / 2, prime);
        return odd * odd % prime * num % prime;
    }
    var even = PowMod(num, pow / 2, prime);
    return even * even % prime;
}
```

2. შებრუნებული ნაშთი

$$\frac{1}{num} (mod\ prime) = num^{prime-2}\ (mod\ prime)$$

```
long InverseMod(long num, long prime)
{
    return PowMod(num, prime - 2, prime);
}
```

3. უარყოფითი ნაშთის შეცვლა

$$-num \equiv -num + prime\ (mod\ prime)$$

```
long AbsMod(long num, long prime)
{
    return (num % prime + prime) % prime;
}
```

4. ელიფსური წირის წერტილი ECPoint

```
struct ECPoint
{
    ECPoint(long x, long y)
    {
        X = x;
        Y = y;
    }

    long X { get; set; }
    long Y { get; set; }

    bool IsInfinity()
    {
        return X == 0 && Y == 0;
    }

    ECPoint operator ^(ECPoint a, long pow)
    {
                if (pow == 1)
                    return a;
                var half = a ^ (pow / 2);
                if (pow % 2 == 1)
                    return half + half + a;
                return half + half;
    }

    ECPoint operator -(ECPoint a) => new ECPoint(a.X, Prime - a.Y);

    ECPoint operator +(ECPoint a, ECPoint b)
    {
        if (a.IsInfinity())
            return b;
        if (b.IsInfinity())
            return a;
        long k;
        if (a.X == b.X)
        {
            if (a.Y != b.Y || a.Y == 0)
                return new ECPoint(0, 0);
            k = AbsMod(3 * a.X * a.X + A, Prime) *
            InverseMods[AbsMod(2 * a.Y, Prime)] % Prime;
        }
        else
        {
            k = AbsMod(b.Y - a.Y, Prime) *
            InverseMods[AbsMod(b.X - a.X, Prime)] % Prime;
        }
        long x = AbsMod(k * k - a.X - b.X, Prime);
        long y = AbsMod(k * (a.X - x) - a.Y, Prime);
        return new ECPoint(x, y);
    }

    ECPoint operator -(ECPoint a, ECPoint b)
    {
        return a + (-b);
    }
}
```

5. ელიფსური წირის ჯგუფი `EllipticCurveGroup` შეიცავს:
    - A,B,Prime - პარამეტრებს $E_P(a,b)$
    - Generator - წარმომქმნელი
    - Order - ჯგუფის წერტილთა რაოდენობა.
6. მეთოდები:
    - დაშიფრვა

```
ECPoint Rc = electionGroup.Generator ^ electionRandomKey;
ECPoint Pc = electionGroup.PublicKey ^ electionRandomKey;
long e = candidate * Pc.X % electionGroup.Prime;
var M = new { Rc, e };
```

    - გაშიფრვა

```
ECPoint Q = M.Rc ^ electionGroup.PrivateKey;
long posCandidate = M.e * InverseMod(Q.X, electionGroup.Prime) %
electionGroup .Prime;
```

    - ხელმოწერა

```
ECPoint Rj = signatureGroup.Generator ^ signatureRandomKey;
long r = Rj.X % signatureGroup.Order;
long s = (signatureRandomKey * M.e + r * signatureKey) % signatureGroup.Order;
var S = new { r, s };
var B = new { M, S };
```

    - ხელმოწერის შემოწმება

```
long inverseMod = InverseMod(M.e, signatureGroup.Order);
long u1 = B.S.s * inverseMod % signatureGroup.Order;
long u2 = - B.S.r * inverseMod % signatureGroup.Order;
ECPoint posRj = signatureGroup.Generator ^ u1 + signaturePublicKey ^ u2;
if (posRj.X % signatureGroup.Order == B.S.r)
    return true;
```

ლიტერატურა:

1. El Housni Y., Introduction to the Mathematical Foundations of Elliptic Curve Cryptography, EY Wavespace LAB – Paris, 2018.
2. Koblitz N., Introduction to Elliptic Curves and Modular Forms, Springer, 1993.
3. Lidl R., Niederreiter H., Finite Fields, Cambridge University Press, 2003.
4. Miret J.M., Moreno R., Pujolàs J., Valls M., Algorithms and Cryptographic Protocols Using Elliptic Curves, Contributions to Science, 3(4):481-491 (2007).
5. Silverman J.H., The Arithmetic of Elliptic Curves, Springer, 2009.
6. Silverman J.H., An Introduction to the Theory of Elliptic Curves, University of Wyoming 2006.