ივ.ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის
ზუსტ და საბუნებისმეტყველო მეცნიერებათა ფაკულტეტის
მათემატიკის დეპარტამენტი

სასრული ველები და კრიპტოსისტემები ელიფსურ წირებზე

გეგა გულაღაშვილი

ხელმძღვანელი : თსუ ასოც. პროფ. ქეთევან შავგულიძე

თბილისი 2014

სარჩევი

ანოტაცია

ნაშრომის მიზანს წარმოადგენს ავაგოთ კრიპტოსისტემა ელიფსურ წირზე . შევისწავლეთ სასრული ჯგუფები , რგოლები , ველები , მათი თვისებები . განვმარტეთ ოპერაცია ელიფსური წირის წერტილთა სიმრავლეზე და ამის საშუალებით ავაგეთ ალგორითმი ტექსტის დასაშიფრად და გასაშიფრად.

Abstract

Goal of this thesis is to build a cryptosystem using elliptic curves. We studied finite groups, rings fields and their properties. We defined operation on elliptic curves points and using this we built algorithm for encrypting and decrypting texts.

შინაარსი

კრიპტოგრაფიის შესახებ შეხედულებები დროთა განმავლობაში იცვლებოდა . იცვლებოდა შეხედულებები იმის შესახებ თუ როგორ უნდა და ვიცვათ ინფორმაცია , რომ გარეშე პირების ხელში აღმოჩენის შემთხვევაშიც კი მათ ვერ (პრაქტიკულ დროში) შეძლონ რეალური ინფორმაციის მიღბა . ინფორმაციის დაცულობას განსაზღვრავს ინფორმაციის დაშიფრული ვარიანტის გამშიფრავი ალგორითმის დადგენა , კონკრეტულად ცოდნა .კრიპტოსისტემები ელიფსურ წირზე წარმოადგენენ ინფორმაციის დაშიფვრის მეთოდს და ამ ინფორმაციის დაშიფრული ვარიანტის გამშიფრავი ალგორითმი კარგადაა დაცული .

სასრული ჯგუფები

ვთქვათ G სიმრავლე სასრული ჯგუფია და H , $H \subset G$ ქვეჯგუფია G სიმრავლის . $\forall\, a \neq 0 \in G$ განვიხილოთ სიმრავლეები $\{ a \bullet h \mid h \in H \} = aH$ და $\{ h \bullet a \mid h \in H \} = Ha$. რადგან G სიმრავლე ჯგუფია ე. ი. $aH \subset G$ და $Ha \subset G \quad \forall\, a \in G$.

ლემა 1 :

$$aH \cap bH \neq \varnothing \,(Ha \cap Hb \neq \varnothing) \Leftrightarrow aH = bH \,(Ha = Hb) .$$

დამტკიცება :

$\Leftarrow$. ე. ი. თუ $aH = bH \Rightarrow aH \cap bH \neq \varnothing$.

$\Rightarrow$. ვთქვათ $aH \cap bH \neq \varnothing$ ე. ი. ი. რ. $c \in aH$ და $c \in bH$ ე. ი. $\exists\, h_1, h_2 \in H$ ი. რ. $c = a \bullet h_1$ და $c = b \bullet h_2$ ე. ი. $a \bullet h_1 = b \bullet h_2$ ე. ი. $(a \bullet h_1) \bullet h_2^{-1} = (b \bullet h_2) \bullet h_2^{-1}$ ე. ი. $a \bullet (h_1 \bullet h_2^{-1}) = b \bullet (h_2 \bullet h_2^{-1})$ ე. ი. $a \bullet (h_1 \bullet h_2^{-1}) = b \bullet e$ ე. ი. $a \bullet (h_1 \bullet h_2^{-1}) = b$, $h_1 \bullet h_2^{-1} \in H$ ფიქსირებული ელემენტია . რადგან $a \bullet (h_1 \bullet h_2^{-1}) = b$ ამიტომ $(a \bullet (h_1 \bullet h_2^{-1})) \bullet h = b \bullet h \quad \forall\, h \in H$ ე. ი. $a \bullet ((h_1 \bullet h_2^{-1}) \bullet h) = b \bullet h \quad \forall\, h \in H$. როდესაც $h \in H$ შეიცვლება მთლიან H სიმრავლეზე $(h_1 \bullet h_2^{-1}) \bullet h$ ეს ელემენტიც შეიცვლება მთლიან H სიმრავლეზე , ამიტომ $\{ a \bullet h \mid h \in H \} = \{ a \bullet ((h_1 \bullet h_2^{-1}) \bullet h) \mid h \in H \} = \{ b \bullet h \mid h \in H \}$ ე. ი. $aH = bH$ (ასევე იქნება $Ha \cap Hb \neq \varnothing \Leftrightarrow Ha = Hb$) □

ე. ი. G ჯგუფი იყოფა თანაუკვეთ სიმრავლეებად . დაყოფის შედეგად მიღებული სიმრავლეების კლასს დავარქვათ მარჯვენა და მარცხენა მოსაზღვრე კლასი, შესაბამისად . H , $H \subset G$ ქვეჯგუფს დავარქვათ ნორმალური გამყოფი თუ G ჯგუფის H ქვეჯგუფით დაყოფისას მარჯვენა და მარცხენა მოსაზღვრე კლასებად ერთმანეთს დაემთხვევა . როდესაც მარჯვენა და მარცხენა მოსაზღვრე კლასი ერთმანეთს დაემთხვევა მათ დავარქმევთ მოსაზღვრე კლასს .

ლემა 2 :

თუ G სიმრავლე სასრული ჯგუფია და H , $H \subset G$ ქვეჯგუფი ნორმალური გამყოფია $\Leftrightarrow aH = Ha \quad \forall\, a \in G$.

დამტკიცება :

$\Leftarrow$. თუ $aH = Ha \quad \forall a \in G$, ე. ი. მარჯვენა მოსაზღვრე კლასი ემთხვევა მარცხენა მოსაზღვრე კლასს , ასეთ დროს კი ჩვენ H ქვეჯგუფს ვეძახით ნორმალურ გამოფს □

$\Rightarrow$. H ქვეჯგუფი ნორმალური გამყოფია ე. ი. მარჯვენა მოსაზღვრე კლასი ტოლია მარცხენა მოსაზღვრე კლასის , ე. ი. $\forall aH$ სათვის მარცხენა მოსაზღვრე კლასიდან

$\exists Hb$ ელემენტი მარცხება მოსაზღვრე კლასიდან ი. რ. $aH = Hb \quad \forall a \in G$.

$a \in aH$ ე. ი. $a \in Hb$, ასევე $a \in Ha$, ე. ი. $a \in Ha \cap Hb$ ე. ი.

$Ha \cap Hb \neq \varnothing$ ამიტომ , ლემა $1-$ ის თნახმად $Ha = Hb$ ე. ი.

$aH = Ha \quad \forall a \in G$ □

ლაგრანჟის თორემა :

ვთქვათ , G სიმრავლე სასრული ჯგუფია და H , $H \subset G$ ქვეჯგუფი ნორმალური გამყოფია , მაშინ $|H| \mid |G|$.

დამტკიცება :

რადგან H ქვეჯგუფი ნორმალური გამყოფია ამიტომ ლემა $2-$ ის თანახმად $aH = Ha \quad \forall a \in G$. $|H| = |aH| \quad \forall a \in G$. მოსაზღვრე კლასის ელემენტების რაოდენობა იყოს n რიცხვი , $n \in N$. ე. ი. $|G| = |H| \circ n$ ე. ი. $|H| \mid |G|$ □

$\forall a \in G$ განვსაზღვროთ ასე $\underbrace{a \bullet a \bullet ... \bullet a}_{n} = a^n$, რადგან G ჯგუფია ე. ი.

$a^n \in G \quad \forall n \in N$

G ჯგუფს დავარქვათ სახელი ციკლური თუ მოხდება , რომ $\exists a \in G$ ი. რ.

$\forall b \neq 0 \in G \quad \exists n \in N$ ი. რ. $b = a^n$, ამ a ელემენტს დავარქმევთ ჯგუფის წარმომქმნელს და ჩავწერთ ასე $G = < a >$.

სასრული ველები

ლემა 1:

თუ F სიმრავლე სასრული ველია, მაშინ მას გააჩნია მახასიათებელი.

დამტკიცება :

განვიხილოთ $e \in F$ ერთეულოვანი ელემენტი და შემოვიღოთ აღნიშვნა, $\forall\, n \in N$ და $\forall\, a \in F \quad \underbrace{a + a + \ldots + a}_{n} = n \bullet a$, ე.ი. $n \bullet a \in F \quad \forall\, n \in N$ და $\forall\, a \in F$ განვიხილოთ ელემენტები $0 \bullet e = 0,\ 1 \bullet e = e,\ 2 \bullet e,\ \ldots\ ,\ n \bullet e,\ \ldots$. თითოეული მათგანი წარმოადგენს F ველის ელემენტს , მათი რაოდენობა უსასრულოა ხოლო F ველის ელემენტების რაოდენობა სასრულია , ე.ი. ამ ელემენტებიდან განსხვავებულების რაოდენობა სასრულია , ე.ი. ერთიდაიგივე ელემენტები მეორდებიან $-$ე.ი. $k \bullet e = n \bullet e$ და $k \neq n$. $k \bullet e = n \bullet e \ \Rightarrow$ $k \bullet e + n \bullet (-e) = n \bullet e + n \bullet (-\mathrm{e}) \ \Rightarrow\ \left| k - n \right| \bullet e = 0$ და $\left| k - n \right| \neq 0$ ე.ი. ნულოვანი ელემენტი მიღებადია , ე.ი. არსებობს არანულოვანი რიცხვი , როდესაც პირველად მიღებადია ნულოვანი ელემენტი . p იყოს ეს რიცხვი , ე.ი. $p \bullet e = 0$ □

ლემა 2 :

ველის მახასიათებელი მარტივი რიცხვია.

დამტკიცება :

p რიცხი იყოს ველის მახასიათებელი. ვთქვათ, p არაა მარტივი რიცხვი , მაშინ არსებობს s რიცხვი ი.რ. $s \mid p$, $s \neq 1$ და $s \neq p$ ე.ი. $\exists\ r > 0$

$p = s \circ r$ ე.ი. $0 = p \bullet e = (s \circ r) \bullet e = (s \bullet e) \bullet (\mathrm{r} \bullet e)$ ე.ი. ან $(s \bullet e) = 0$ ან $(\mathrm{r} \bullet e) = 0$, მაგრამ p არის რიცხვი , როდესაც პირველად მიღებადია ნულოვანი ელემენტი ე. ი. თუ $0 < k < p$, $k \bullet e \neq 0$, ე.ი. p მარტივი რიცხვია □

ლემა 3 :

$F_p = \{\ 0 \bullet e = 0,\ 1 \bullet e = e,\ 2 \bullet e,\ \ldots\ ,\ (\mathrm{p} - 1) \bullet e\ \}$ სიმრავლე ველია .

დამტკიცება :

$F_p \subset F$ და F ველია ე.ი. F_p სიმრავლის ელემენტებისთვის სრულდება $-$ ასოციაციურობისა და კომუტაციურობის თვისებები F ველზე განსაზღვრული ორივე $+$ და $\bullet$ ოპერაციის მიმართ, დისტრიბუციულობის თვისება, ნულოვანი ელემენტისა ($0 \bullet e = 0$) და ერთეულოვანი ელემენტის ($1 \bullet e = e$)

არსებობის მოთხოვნები. $k \bullet e + (p-k) \bullet e = p \bullet e = 0$, $k \bullet e \in F$ და $(p-k) \bullet e \in F$, $\forall\ k \in \{0, 1, 2, \ldots, p-1\}$ ე.ი. F_p სიმრავლის ყოველ ელემენტს F_p სიმრავლეში გააჩნია მოპირდაპირე ელემენტი . F_p სიმრავლის ყოველი $k \bullet e$ ელემენტისთვის , $k \in \{1, 2, \ldots, p-1\}$, განვიხილოთ ელემენტი
$k^{\varphi(p)-1} \bullet e$, რომელიც ასევე F_p სიმრავლის ელემენტია , რადგან
$k^{\varphi(p)-1} = p \circ m + r$ და $0 \le r < p$, ე.ი.
$k^{\varphi(p)-1} \bullet e = (p \circ m + r) \bullet e = (p \circ m) \bullet e + r \bullet e = 0 + r \bullet e = r \bullet e$ და $0 \le r \le p-1$.

რადგან p მარტივი რიცხვია და $k \in \{1, 2, \ldots, p-1\}$, ამიტომ $(k, p) = 1$ და ეილერის თეორემის თანახმად $k^{\varphi(p)} \equiv 1 \pmod{p}$, ე. ი. მივიღებთ, რომ
$(k \bullet e) \bullet (k^{\varphi(p)-1} \bullet e) = (k \circ k^{\varphi(p)-1}) \bullet e = k^{\varphi(p)} \bullet e = 1 \bullet e = e$ ე.ი. F_p სიმრავლის ყოველ ელემენტს $k \bullet e$, F_p სიმრავლეში გააჩნია შებრუნებული ელემენტი $k^{\varphi(p)-1} \bullet e$, $\forall\ k \in \{1, 2, \ldots, p-1\}$, ე. ი. F_p სიმრავლე არის ველი □

ლემა 4 :

ვთქვათ $L \subset M$ და L , M სიმრავლეები სასრული ველებია , მათ გააჩნიათ ერთი და იგივე მახასიათებელი .

დამტკიცება :

ლემა 1 − ის თანახმად M ველს გააჩნია მახასათებელი , ვთქვათ ეს მახასიათებელი არის p რიცხვი . რადგან M და L ორივე ველებია და $L \subset M$, ამიტომ $e \in M \Rightarrow e \in L$, ამის გამო $F_p \subset L$. $F_p \subset L$ და $L \subset M$ ე.ი. p რიცხვი არის L ველის მახასიათებელიც □

ვთქვათ $L \subset M$ და L , M ველებია − M სიმრავლე შეიძლება განვიხილოთ როგორც წრფივი სივრცე L ველის მიმართ .

ლემა 5 :

თუ L , M სიმრავლეები სასრული ველებია და $L \subset M$, მაშინ $|M| = |L|^n$, სადაც n რიცხვი წარმადგენს M სიმრავლის , როგორც L ველის მიმართ წრფივი სივრცის განზომილებას.

დამტკიცება :

M ველში ერთი ელემენტი მაინცაა წრფივად დამოუკიდებელი , რადგან თუ $s \in M$ და $s \neq 0$, მაშინ $\alpha \bullet s = 0 \Leftrightarrow \alpha = 0 \quad \forall \ \alpha \in L$ და $\forall \ s \neq 0 \ \in \ M$. M სიმრავლის წრფივად დამოუკიდებელი ელემენტების რაოდენობა უსასრულო ვერ იქნება , რადგან თითოეული წრფივად დამოუკიდებელი ელემენტი M სიმრავლისაა და M სიმრავლის ელემენტების რაოდენობა სასრულია. ე.ი. M სიმრავლის წრფივად დამოუკიდებელი ელემენტის რაოდენობა სასრულია. n იყოს M სიმრავლის წრფივად დამოუკიდებელი ელემენტთა მაქსიმალური რაოდენობა და $a_1, a_2, \ ... \ , a_n$ იყოს M სიმრავლის წრფივად დამოუკიდებელი ელემენტები . $\forall \ s \ \in \ M \ \exists$ $\alpha_i \ \ 1 \leq i \leq n$ სადაც $\alpha_i \in L$ და $s = \alpha_1 \bullet a_1 + \alpha_2 \bullet a_2 + ... + \alpha_n \bullet a_n$. ე.ი. M სიმრავლის ელემენტების რაოდენობა იმდენია , რამდენი განსხვავებული $\alpha_1 \ , \alpha_2 \ , ... , \alpha_n$ სკალარიც შეიძლება ვთქვათ L ველიდან ე.ი.

$$|M| = \underbrace{|\mathrm{L}| \bullet |\mathrm{L}| \bullet \ ... \ \bullet |\mathrm{L}|}_{n} = |\mathrm{L}|^{n} \quad \square$$

ამ ლემებს გამოვიყენებთ სასრული ველების ერთ − ერთი მნიშვნელოვანი თვისების დასამტკიცებლად .

თეორემა 1 :

M სასრული ველის ელემენტების რაოდენობაა p^n . სადაც p რიცხვი არის M სასრული ველის ველის მახასიათებელი და n რიცხვი არის M სასრული ველის , როგორც F_p ველის მიმართ წრფივი სივრცის განზომილება .

დამტკიცება :

ლემა 1 − ის თანახმად $\exists \ M$ ველის მახასიათებელი p რიცხვი . M სასრული ველი წარმოადგენს წრფივ სივრცეს F_p ველის მიმართ . ლემა 5 − ის თანახმად M წფივი სივრცე F_p ველის მიმართ სასრულ განზომილებიანია ე.ი. $\exists \, n$ რიცხვი რომელიც იქნება M წფივი სივრცის განზომილება . ლემა 5 −ის თანახმად $|M| = |F_p|^n = p^n \quad \square$

ე. ი. თუ $L \ , M$ სიმრავლეები სასრული ველებია და $L \subset M$, ლემა 1 − ისა და ლემა 4 − ის თანახმად $\exists \ p$ რიცხვი , რომელიც არის L და M ველის მახასიათებელი . $F_p \subset L$ და $F_p \subset M$, თეორემა 1 − ის თანახმად $\exists \ \ n$ და m რიცხვები ი. რ. $|\mathrm{L}| = p^n$ და $|M| = p^m$.

თეორემა 2 :

ვთქვათ L , M სიმრავლეები სასრული ველებია და $L \subset M$ $|\mathrm{L}| = p^n$ და $|M| = p^m$, მაშინ $n \mid m$.

ამ თეორემის დასამტკიცებლად გამოვიყენებთ შემდეგ სქემას :

ლემა 6 :

ვთქვათ M სიმრავლე სასრული ველია , მაშინ $\forall\ s \neq 0 \in M$ $\exists n \in N$ ი. რ. $s^n = e$.

დამტკიცება :

ნებისმიერი $s \neq 0$ ელემენტისათვის , $s \in M$, განვიხილოთ ელემენტები $s^0 = e$, $s^1 = s, s^2, \ldots, s^m, \ldots$. სადაც ჩანაწერი s^m აღნიშნავს შემდეგ გამოსახულებას $\underbrace{s \bullet s \bullet \ldots \bullet s}_{m} = s^m$ $\forall\ m \in N$. განსახილველი ელემენტების რაოდენობა უსასრულოა და $\forall\ m \in N$ $s^m \in M$, M ველი სასრულია ე.ი. განსახილველი ელემნტებიდან განსხვავებულების რაოდენობა სასრულია . რადგან ყველა ელემენტის რაოდენობა უსასრულოა , ამიტომ ელემენტები მეორდება – ე.ი. $s^k = s^t$ და $k \neq t$. $s^k = s^t \Rightarrow s^k \bullet (s^{-1})^t = s^t \bullet (s^{-1})^t \Rightarrow s^{|k-t|} = e$ და $|k-t| \neq 0$ ე. ი. e ეს ელემენტი მიღებადია, ე. ი. არსებობს არანულოვანი რიცხვი – ი. რ. $s^n = e$ □

შენიშვნა 1 :

თუ $s^n = e \Rightarrow (s^n)^m = e = s^{n \circ m}$ $\forall\ m \in N$, ამიტომ არსებითია $s \neq 0$ ელემენტის ხარისხის როლში განვიხილოთ უმცირესი n რიცხვი, რომლისთვისაც $s^n = e$. ასეთ დროს გამოვა , რომ ყველა განსხვავებული ელემნენტები ესენია $s^0 = e$, $s^1 = s, s^2, \ldots, s^{n-1}$.

შენიშვნა 2 :

მინიმალური ველი , რომელიც მოიცავს L ველს და $M \setminus L$ სიმრავლეს, არის M ველი . $M \setminus L = \{ s_1, s_2, \ldots, s_k \}$.

ავაგოთ მინიმალური ველი , რომელიც მოიცავს L ველსა და $s \in M \setminus L$ ელემენტს , ამ ველს აღვნიშნავთ სიმბოლოებით ასეთნაირად $L(s) : L(s)$ ველი ჩაკეტილი უნდა იყოს M ველზე განსაზღვრული $+$ და $\bullet$ ოპერაციების

მიმართ . ლემა 6 − ისა და შენიშვნა 1 − ის თანახმად $\exists\, n \in N$
$\{ s^0 = e ,\ s^1 = s , s^2 , \ldots , s^{n-1} \} \subset L(s)$ და $s^n = e$. რადგან $L(s)$
ჩაკეტილია $+$ და $\bullet$ ოპერაციების მიმართ, ამიტომ
$\alpha_0 \bullet e + \alpha_1 \bullet s^1 + \ldots + \alpha_{k-1} \bullet s^{k-1} \in L(s) \quad \forall\ \alpha_i \in L \quad 0 \le i \le n-1$ და
$\forall\ k \quad 0 \le k \le n-1$. რადგან $s^n = e$ და n რიცხვი არის s ელემენტის
უმცერესი ხარისხი , ამიტომ
$(\alpha_0 \bullet e + \alpha_1 \bullet s^1 + \ldots + \alpha_{i-1} \bullet s^{i-1}) \bullet (\beta_0 \bullet e + \beta_1 \bullet s^1 + \ldots + \beta_{j-1} \bullet s^{j-1}) =$
$\gamma_0 \bullet e + \gamma_1 \bullet s^1 + \ldots + \gamma_{t-1} \bullet s^{t-1} \in L(s)$ და
$(\alpha_0 \bullet e + \alpha_1 \bullet s^1 + \ldots + \alpha_{i-1} \bullet s^{i-1}) + (\beta_0 \bullet e + \beta_1 \bullet s^1 + \ldots + \beta_{j-1} \bullet s^{j-1}) =$
$\eta_0 \bullet e + \eta_1 \bullet s^1 + \ldots + \eta_{u-1} \bullet s^{u-1} \in L(s)\ \forall \quad 0 \le i, j, t, u \le n-1$,
$\alpha_q, \beta_w, \gamma_r, \eta_c \in L(s)$,
$0 \le q \le i-1,\ 0 \le w \le j-1,\ 0 \le r \le t-1, 0 \le c \le u-1$. რადგან
$L \subset L(s)$ ე. ი. $L(s)$ ველი შეგვიძლია განვიხილოთ L ველის მიმართ
როგორც წრფივი სივრცე .
რადგან $s^0 = e ,\ s^1 = s , s^2 , \ldots , s^{n-1}$ ელემენტებიდან ყველა განსხვავებულია და
$s^n = e$ ამიტომ $e ,\ s^1, s^2 , \ldots , s^{n-1}$ − ეს ელემენტები წრფივად
დამოუკიდებელია, ხოლო $e ,\ s^1, s^2 , \ldots , s^{n-1}, s^n$ − ელემენტები წრფივად
დამოკიდებული. ე. ი. $\alpha_0 \bullet e + \alpha_1 \bullet s^1 + \ldots + \alpha_{n-1} \bullet s^{n-1} + \alpha_n \bullet s^n = 0$ და
$\exists\ \alpha_i \in L$ რომ $\alpha_i \ne 0$, $i > 1$. $\alpha_0 \bullet e + \alpha_1 \bullet s^1 + \ldots + \alpha_{n-1} \bullet s^{n-1} + \alpha_n \bullet s^n$
− ეს გამოსახულება შეგვიძლია განვიხილოთ როგორც L ველის მიმართ n რიგის
პოლინომის ნიშვნელობა s ელემენტზე და რადგან
$\alpha_0 \bullet e + \alpha_1 \bullet s^1 + \ldots + \alpha_{n-1} \bullet s^{n-1} + \alpha_n \bullet s^n = 0$, s ელემენტი არის ამ
პილინომის ფესვი . აღვნიშნოთ ეს n რიგის პოლინომი სიმბოლოთი f , ე. ი.
$\deg(f) = \mathrm{n}$ და $f(s) = 0$ და n რიცხვი არის უმცირესი რიგი პოლინომისა
L ველის მიმართ , რომლის ფესვიც შეიძლება იყოს s ელემენტი . f პოლინომი
L ველის მიმართ დაუყვანადი პოლინომია , რადგან თუ დაყვანადია L ველის
მიმართ ე. ი. $\exists\ g, h$ პოლინომები L ველის მიმართ ი. რ. $f = g \bullet h$ და
$\deg(f) > \deg(h) \ge 1$, $\deg(f) > \deg(h) \ge 1$, მაშინ $f(\mathrm{s}) = g(\mathrm{s}) \bullet h(\mathrm{s})$
ე. ი. $0 = g(\mathrm{s})$, ან $0 = h(\mathrm{s})$ $g(\mathrm{s}), h(\mathrm{s}) \in \mathrm{M}$ ე. ი. s ელემენტი ყოფილა g
ან h პოლინომის ფესვი , რადგან $\deg(g) < \deg(f) = n$ და
$\deg(h) < \deg(f) = n$ და s ელემენტი გამოდის n რიცხვზე უფრო დაბალი
რიგის პოლინომის ფესვი , მაგრამ s ელემენტი n რიცხვზე უფრო დაბალი რიგის
პოლინომის ფესვი არაა ე. ი. არ შეიძლება f პოლინომი იყოს L ველის მიმართ

დაყვანადი ე. ი. f პოლინომი L ველის მიმართ დაუყვანადი პოლინომია . რადგან f პოლინომი L ველის მიმართ დაუყვანადი პოლინომია ე. ი. L ველის მიმართ ყოველი p პოლინომისთვის $(f, \mathrm{p}) = f$ ან $(f, \mathrm{p}) = e$ ე. ი. როდესაც $(f, \mathrm{p}) = f$ გამოვა , რომ $\exists\ q$ პოლინომი L ველის მიმართ ი. რ. $p = f \bullet q$ ე. ი. $p(s) = f(s) \bullet q(s)$ ე. ი. $p(s) = 0 \bullet q(s)$ ე. ი. $p(s) = 0$, $p(s)$ ეს ელემენტი ნულოვანი ელემენტი გამოვიდა . როდესაც $(f, \mathrm{p}) = e$ ე. ი. $\exists\ L$ ველის მიმართ პოლინომები l და r ი. რ. $f \bullet r + \mathrm{p} \bullet l = e$ ე. ი. $f(s) \bullet r(s) + \mathrm{p}(\mathrm{s}) \bullet l(s) = e$ ე. ი. $0 \bullet r(s) + \mathrm{p}(\mathrm{s}) \bullet l(s) = e$ ე. ი. $\mathrm{p}(\mathrm{s}) \bullet l(s) = e$, $p(s)$ არანულოვანი ელემენტი გამოდის , ე. ი. s ელემენტი არაა ამ p პოლინომის ფესვი . რადგან $s^n = e$ ამიტომ $\mathrm{p}(\mathrm{s})$ და $l(\mathrm{s})$ ელემენტების სახე ასეთია $\alpha_0 \bullet e + \alpha_1 \bullet s^1 + \ldots + \alpha_k \bullet s^k$, სადაც $0 < k < n$ ე. ი. $\mathrm{p}(\mathrm{s})$ და $l(\mathrm{s})$ ორივე და $\in L(s)$. რადგან $\mathrm{p}(\mathrm{s}) \bullet l(s) = e$ ყოველი p პოლინომისთვის , რომლის ფესვიც არაა s ელემენტი , ამიტომ ყოველ არანულოვან $\alpha_0 \bullet e + \alpha_1 \bullet s^1 + \ldots + \alpha_k \bullet s^k$ ასეთ ელემენტს გააჩნია შებრუნებული ელემენტი და ესეც $\alpha_0 \bullet e + \alpha_1 \bullet s^1 + \ldots + \alpha_m \bullet s^m$ მასეთივეა $0 < k, m < n$ და რადგან თითოეული მათგანი M ველის ელემენტია ამიტომ მათთვის M ველის $+$, $\bullet$ ოპერაციების მიმართ სრულდება ასოციაციურობისა და კომუტაციურობის თვისებები, ნულოვანი $(0 \bullet e = 0)$ და ერთეულოვანი $(1 \bullet e = e)$ ელემენტის არსებობა, დისტრიბუციულობის თვისება , ყოველი არა ნულოვანი ელემენტისთვის შებრუნებულისა და მოპირდაპირის არსებობა . ე. ი. სიმრავლე $\{ \alpha_0 \bullet e + \alpha_1 \bullet s^1 + \ldots + \alpha_{n-1} \bullet s^{n-1} : \alpha_i \in L, 0 \le i \le n-1 \}$ გამოვიდა ველი და აგების თანახმად უმცირესი ველი რომელიც მოიცავს L ველსა s ელემენტს ამიტომ $L(s) = \{ \alpha_0 \bullet e + \alpha_1 \bullet s^1 + \ldots + \alpha_{n-1} \bullet s^{n-1} : \alpha_i \in L, 0 \le i \le n-1 \}$. $|L(s)| = |L|^n$, სადაც n არის უმცირესი რიგი პოლინომისა L ველის მიმართ , რომლის ფესვიცაა s ელემენტი , ასევე n არის რიცხვი , რომელსაც აქვს სახე: $s^n = e$ და e ელემენტი მიღებადია პირველად .

აქ აღწერილი სქემის გამოყენებით თორემა 2 დამტკიცდება შემდეგნაირად:

დამტკიცება :

თუ $M \setminus L = \varnothing$ ე. ი. $L = M$ ე. ი. $n = m$ და $m \mid m$. თუ $M \setminus L \neq \varnothing$, $M \setminus L = \{ s_1, s_2, \ldots, s_l \}$. $L(s_1, s_2, \ldots s_d)$ განვიხილოთ როგორც $L(s_1, s_2, \ldots s_{d-1})$ ველის მიმართ წრფივი სივრცე $\forall\ d \in \{1, 2, \ldots, \mathrm{k}\}$, $(L(s_0) = L)$.

$L \subset L(s_1) \subset L(s_1, s_2) \subset \ldots \subset L(s_1, s_2, \ldots s_k) = M$ მაშინ ზემოთ აღწერილის თნახმად გვექნება: $\exists\ n_1\ ,\ n_2\ ,\ \ldots\ ,\ n_k \in N$ ი. რ.

$$|L(s_1)| = (\mathrm{p}^{n})^{n_1} = p^{n \circ n_1}$$

$$|L(s_1, s_2)| = (p^{n \circ n_1})^{n_2} = p^{n \circ n_1 \circ n_2}$$

$$\vdots$$

$$|L(s_1, s_2, \ldots s_k)| = (\mathrm{p}^{n \circ n_1 \circ \ldots \circ \mathrm{n}_{k-1}})^{n_k} = \mathrm{p}^{n \circ n_1 \circ \ldots \circ \mathrm{n}_k}$$

მაგრამ $L(s_1, s_2, \ldots s_k) = M$ ე. ი. $|L(s_1, s_2, \ldots s_k)| = |M|$ ე. ი. $m = n \circ n_1 \circ \ldots \circ \mathrm{n}_k$ ე. ი. $n \mid m$ □

ელიფსური წირების მათემატიკური საფუძვლები

მესამე რიგის წირს E -ს, რომელიც მოცემულია განტოლებით

$$E : Y^2 = X^3 + aX + b \qquad (1)$$

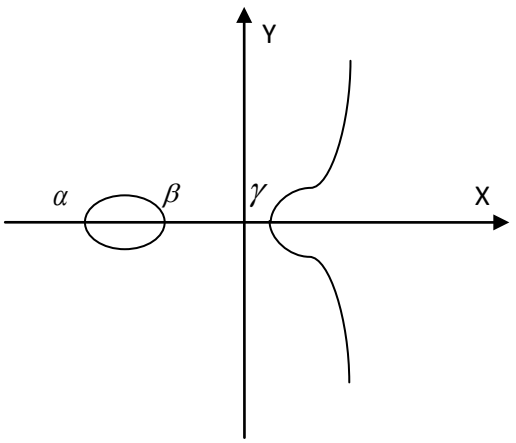
ეწოდება ელიფსური წირი (სინამდვილეში (1) ტიპის განტოლება მიღებულია უფრო ზოგადი სახის განტოლებიდან, რომელიც ჩვენთვის საინტერესო არ არის).

რადგანაც $Y = \pm\sqrt{X^3 + aX + b}$ გრაფიკი სიმეტრიულია აბცისათა ღერძის მიმართ, და რომ ვიპოვოთ მისი თანაკვეთა აბცისათა ღერძთან, საჭიროა ამოვხსნათ განტოლება:

$$X^3 + aX + b = 0 \qquad (2)$$

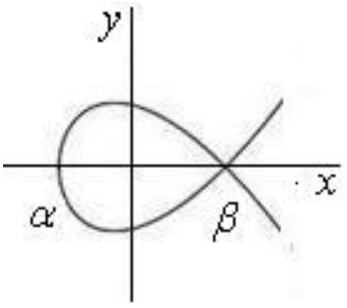
კარდანოს ფორმულებით $D = \left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2$

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



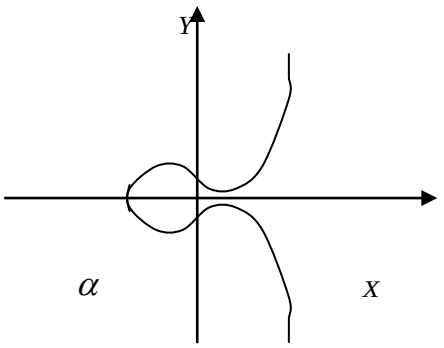
სურ.1. ელიფსური წირი, როცა $D < 0$.

2)თუ $D = 0$, მაშინ (2) განტოლებას აქვს 3 ნამდვილი ფესვი α, β, β , რომელთაგან 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.



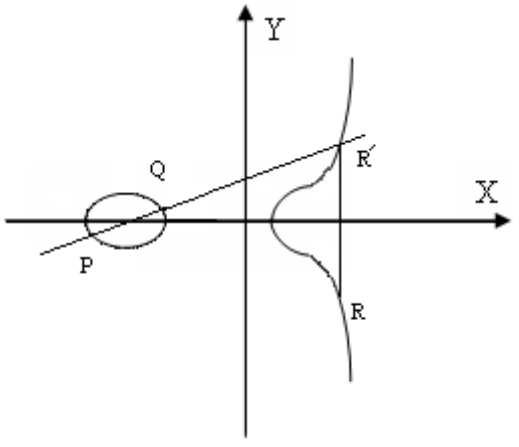
სურ.3. ელიფსური წირი, როცა $D > 0$.

წირს, რომელიც არის ნახ.2 –ზე ეწოდება სინგულარული. $(\beta, 0)$ სინგულარულობის წერტილში აქვს ორი მხები. სინგულარულ წირს გამოვრიცხავთ ჩვენი განხილვიდან ანუ ვიხილავთ $D \neq 0$ შემთხვევას, რაც ექვივალენტურია

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

ვთქვათ ელიფსური E წირი მოცემულია განტოლებით (1), (3) პირობით. განვსაზღვროთ წირზე წერტილთა კომპოზიციის ოპერაცია.

ავიღოთ $P = (x_1, y_1)$, $Q = (x_2, y_2)$ წერტილები E წირიდან. და გავავლოთ ამ წერტილებზე წრფე, ეს წრფე გადაკვეთს წირს მესამე წერტილში, რომელიც აღვნიშნოთ R'-ით. მესამე წერტილი აუცილებლად არსებობს, რადგანაც თუ კუბურ განტოლებას აქვს ორი ნამდვილი ფესვი, რომელიც შეესაბამება P და Q წერტილებს, შესაბამისად მას მესამე ფესვიც აქვს, რომელიც შეესაბამება R'-ს.



სურ.4. წერტილთა კომპოზიცია ც

R წერტილს, კოორდინატებით (x_3, y_3), რომელიც მიიღება R' წერტილის ორდინატის შეცვლით ვუწოდოთ P და Q წერტილების კომბინაცია და

$$R = P + Q$$

ვთქვათ, $P \in E$ წერტილს აქვს კოორდინატები (x, y), მაშინ წერტილები კოორდინატებით (x, y) აღვნიშნოთ $-P$-თი. ჩავთვალოთ, რომ ვერტიკალური წრფე, რომელიც გადის P და $-P$ წერტილებში კვეთს წირს უსასრულოდ დაშორებულ O წერტილში. ე.ი. $P + (-P) = O$

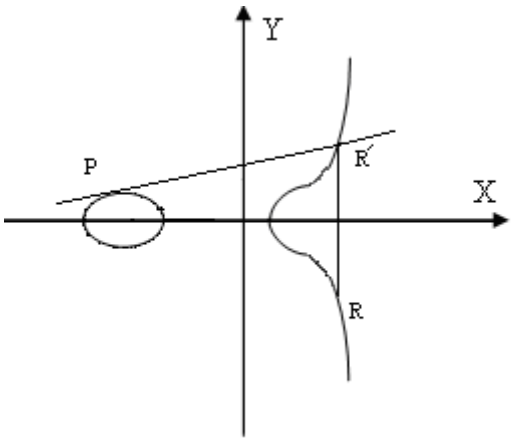
შეთანხმებით

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

O წერტილი ელიფსურ წირზე ასრულებს 0-ის როლს. წარმოვიდგინოთ, რომ P და Q წერტილები ერთმანეთს უახლოვდება $P = Q = (x_1, y_1)$ წერტილში, მაშინ კომპოზიცია

$$R = (x_3, y_3) = P + Q = P + P$$

მიიღება P წერტილში მხების გავლებით და წირთან მისი გადაკვეთის R წერტილის სიმეტრიული ასახვით X ღერძის მიმართ (ნახ.5)



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

ვისარგებლოთ შემდეგი აღნიშვნით $R = P + P = [2]P$

გამოვიყვანოთ ფორმულები, რომლითაც მიიღება $R = (x_3, y_3)$ კოორდინატები $P = (x_1, y_1)$ და $Q = (x_2, y_2)$-ის გამოყენებით.

განვიხილოთ შემთხვევა , როცა $P \neq \pm Q$ და $R = P + Q$ (სურ. 4)

k-თი აღვნიშნოთ P და Q წერტილებზე გამავალი წრფის საკუთხო კოეფიციენტი. ცხადია $k = \dfrac{y_2 - y_1}{x_2 - x_1}$,

მაშინ წრფის განტოლებას აქვს სახე $Y - y_1 = k(X - x_1)$ (6), ანუ მიღებული Y შევიტანოთ წირის განტოლებაში, ანუ ვიპოვოთ წირთან გადაკვეთის წერტილი.

$$(y_1 + k(X - x_1))^2 = X^3 + aX + b$$

თუ ავიყვანთ კვადრატში და დავაჯგუფებთ, მივიღებთ კუბურ განტოლებას

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

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

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

აქედან $x_3 = k^2 - x_1 - x_2$

თუ მიღებულ x_3-ს ჩავსვამთ (6) წრფის განტოლებაში, მივიღებთ R'-სთვის $y_3 = y_1 + k(x_3 - x_1)$, თუ ნიშანს შევცვლით მივიღებთ $y_3 = k(x_1 - x_3) - y_1$.

განვიხილოთ $R = [2]P$ წერტილის მიღება. გავაწარმოვოთ (1) და მივიღებთ

$$2yy' = 3x^2 + a$$

მხების საკუთხო კოეფიციენტი P წერტილში წარმოებულის მნიშვნელობის ტოლია:

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

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

$$[2]P = O$$

ელიფსურ წირებს აქვს შემდეგი თვისებები:

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

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

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

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

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

ჩვენ ვხედავთ, რომ წირზე წერტილების კომპოზიციისას გამოიყენება ოპერაციები: შეკრება, გამოკლება, გამრავლება და გაყოფა რიცხვებზე. ეს ნიშნავს, რომ მიღებული შედეგები იქნება შენარჩუნებული თუ მოქმედებებს ჩავატარებთ მთელ რიცხვებზე მარტივი p მოდულით.

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

$$uv^{-1} \bmod p$$

მოდულით მარტივობა საჭიროა იმისათვის, რომ ნებისმიერი დადებითი $v < p$ რიცხვისათვის არსებობდეს მისი შებრუნებული ისეთი, რომ

$$vv^{-1} \equiv 1 (\bmod p)$$

ასეთნაირად ჩვენ მივიღებთ წირის განტოლებას

$$E : Y^2 = X^3 + aX + b (\bmod p) \qquad (10)$$

სადაც X, Y, a და $b < p$

a და b-სთვის უდნა შესრულდეს პირობა

$$\left(4a^3 + 27b^2\right) \bmod p \neq 0 \qquad (11)$$

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

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

რომელიც აკმაყოფილებს (10) განტოლებას, და O წერტილისაგან უსასრულობაში. ამ სიდიდეს დიდი მნიშვნელობა აქვს კრიპტოგარფიაში.

მაგალითი: განვიხილოთ წირი

$$E_7(2,6): Y^2 = X^3 + 2X + 6 (\bmod 7) \qquad (12)$$

შევამოწმოთ პირობა (11).

$$\left(4 \cdot 2^3 + 27 \cdot 6^2\right) \bmod 7 = 4 \cdot 1 + 6 \cdot 1 = 3 \neq 0$$

ე.ი. მოცემული წირი არასინგულარულია. ავიღოთ ნებისმიერი წერტილი $E_7(2,6)$-დან, მაგალითად $x = 5$, მაშინ

$$y^2 \equiv 1 (\bmod 7) \text{ და } y \equiv 1 (\bmod 7), \quad y \equiv -1 (\bmod 7).$$

ვიპოვეთ 2 წერტილი: (5,1) და (5,6).

ვიპოვოთ წერტილი [2] (5,1)

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

მივიღეთ, რომ [2] (5,1)=(4,6), შეგვიძლია დავრწმუნდეთ, თუ ჩავსვამთ მის კოორდინატებს (12)-ში რომ მოღებული წერტილი ეკუთვნის წირს.

ვიპოვოთ [3] (5,1)=(5,1)+(4,6)

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

მივიღეთ, რომ [2] (5,1)=(2,5), ე.ი. ვნახეთ ოთხი წერტილი.

წირის კრიპტოგარფიული გამოყენებისთვის საჭიროა ვიცოდეთ სულ რამდენი წერტილია $E_7(2,6)$–წირზე.

რამდენიმე სიტყვით დავახასიათოთ $E_p(a,b)$, ცხადია ეს სიმრავლე სარულია და მასში შედიან წერტილები მთელი კოორდინატებით (x,y), სადაც $0 \le x, y < p$. არსებობს პირდაპირი ანალოგია $E_p(a,b)$ სიმრავლესა და მთელი რიცხვის ხარისხების მოდულით p სიმრავლეს შორის, ანუ უფრო ზუსტად $E_p(a,b)$-ში არსებობს წარმომქმნელი G, ისეთი რომ მწკრივი

$G, [2]G, [3]G, \ldots, [n]G$, სადაც $n = \#E_p(a,b)$, არის $E_p(a,b)$-ს ელემენტები, ამასთანავე $[n]G = O$.

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

შებრუნებული ამოცანა, რომელსაც ტრადიციულად ეწოდება დისკრეტული ლოგარითმი ელიფსურ წირებზე ყალიბდება შემდეგნაირად:

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 $O(\sqrt{q}) = O\left(2^{t/2}\right)$).

ელიფსური წირების გამოყენება კრიპტოსისტემებში

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

$$y \equiv g^x \pmod p$$

ოპერაციის შეცვლისა $y \equiv [x]G \pmod p$ ოპერაციით.

ელ-გამელის შიფრი ელიფსურ წირებზე

ვთქვათ გვაქვს არჩეული ელიფსური წირი $E_p(a,b)$ წარმომქმნელი G წერტილით, ისეთი რომ $G, [2]G, [3]G, \ldots, [q]G$ 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 მომხმარებელს. ვთქვათ A მომხმარებელმა უნდა გადასცეს B მომხმარებელს რაიმე m შეტყობინება (m-ს აქვს რიცხვის სახე, $m < p$).

A აკეთებს შემდეგს:

1) ირჩევს შემთხვევით k რიცხვს. $0 < k < q$.

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

3) შიფრავს $e = mx \bmod p$.

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 $m' = ex^{-1} \bmod p$

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 მოწინააღმდეგესათვის არის უცნობი, რადგან მან არ იცის k რიცხვი. მოწინააღმდეგე შეეცდება გამოთვლოს k R წერტილიდან, მაგრამ ამისათვის საჭირო იქნება დისკრეტული ლოგარითმის გამოთვლა წირზე.

ელექტრონულ-ციფული ხელმოწერა

ეს მეთოდი ანალოგიურია, როგორიც იყო ГОСТ Р34.10-94 , მაგრამ ხარისხში აყვანა შეცვლილია წირზე ოპერაციების კომპოზიციით. მომხმარებლები ირჩევენ საერთო ელიფსურ წირს $E_p(a,b)$ და G წერტილს მათზე ისე, რომ $G, [2]G, [3]G, \ldots, [q]G$ არიან განსხვავებული წერტილები და $[q]G = O$ რაიმე მარტივი q-სთვის (q რიცხვის სიგრძე არის 256 ბიტი). ყოველი U მომხმერებელი აირჩევს საიდუმლო x_U გასაღებს $0 < x_U < q$ და გამოთვლის წერტილს წირზე $Y_U = [x_U]G$. წირის პარამეტრები და ღია გასაღების ჩამონათვლალი ყველა მომხმარებლისთვის ცნობილია. იმისთვის რომ A მომხმარებელმა ხელი მოაწეროს m შეტყობინებას, ის აკეთებს შემდეგს:

1. ირჩევს შემთხვევით k რიცხვს, $0 < k < q$.

2. გამოთვლის $P = [k]G = (x, y)$.

3. გამოთვლის $r = x \bmod p$ (თუ $r = 0$-ს უბრუნდება 1-ს).

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

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

რომ შეამოწმოს, A-მ მოაწერა თუ არა ხელი, ნებისმიერი მომხმარებელი იქცევა შემდეგნაირად:

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

2. გამოთვლის $u_1 = sm^{-1} (\bmod q)$ და

$$u_2 = -rm^{-1} (\bmod q)$$

3. გამოთვლის წირზე წერტილების შემდეგ კომბინაციას

$P = [u_1]G + [u_2]Y_A = (x, y)$.

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

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

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

ალგორითმი

პროგრამის ალგორითმი ასეთია , საწყის ეტაპზე ვსაზღვრავთ ელიფსური წირის პარამეტრებს და მარტივ რიცხვს. a, b რიცხვები უნდა შევარჩიოთ შემდეგი წესის დაცვით $4 \circ a^3 + 27 \circ b^2 \neq 0 \pmod{p}$ და p მარტივი რიცხვია (აქ ჩვენ აღებული გვაქვს $p \equiv 3 \pmod{4}$ მარტივი რიცხვი) .

მომდევნო ჯერზე აღვწერთ ელიფსური წირის წერტილების სიმრავლეს . ელიფსური წირის წერტილების სიმრავლეიდან შევარჩევთ ელიფსური წირის წერტილების სიმრავლის, როგორც ჯგუფის წარმომქმნელ ელემენტს .

ნებისმიერი რიცხვისთვის l , ახალ რიცხვს ვსაზღვრავთ შემდეგნაირად : ვპოულობთ ელემენტს ელიფსურ წირზე. ელიფსური წირის წარმომქმნელ G ელემენტს ვკრებთ l ამ რაოდენობით , მიიღება ელიფსური წირის ახალი წერტილი (s,t).

l რიცხვს ვუსაბამებთ s რიცხვს - ამას ვუწოდებთ დაშიფვრას .

რადგან ჩვენთვის ცნობილია წარმომნქმნელი ელემენტი ამიტომ ჩვენ შევძლებთ s რიცხვისაგან (დაშიფრული რიცხვისაგან) განვსაზღვროთ l რიცხვი (რომელი რიცხვიც გარდაიქმნა ამ s რიცხვად) . G წარმომქმნელი ელემენტია , ვიხილავთ ახალ ელემენტებს G , $2 \bullet G$, ..., $n \bullet G$ $n \in N$, $\underbrace{G+G+\ldots+G}_{n} = n \bullet G$, რადგან G წარმომქმნელი ელემენტია ე. ი. $\exists\, k$ ი. რ. $k \bullet G = (s,t)$.

s რიცხვს შევუსაბამებთ k რიცხვს - ამას დავუძახებთ გაშიფვრას .

ჩვენ ვკრებთ ტექსტს , ტექსტის ყოფელ ასოს ვუსაბამებთ ორი ციფრისგან შემდგარ რიცხვს $00, 01, \ldots, 10, 11, \ldots, 20, 21, \ldots 25$ (აქ გვაქვს $00, 01, \ldots, 10, 11, \ldots, 20, 21, \ldots 25, 26$, რადგან 00 გვაქვს ადგილის გამოტოვებისთვის) . მიღებულ რიცხვებს ვაჯგუფებთ ორ - ორად , მიიღება ახალი რიცხვები , ამ რიცხვებისთვის (ესენიც ხომ ნებისმიები რიცხვებია) აღწერილი სქემის მიხედვით ვსაზღვრავთ სხვა რიცხვებს და სხვა რიცხვებიდან ვსაძღვრავთ ამ რიცხვებს .

მიღებილ რიცხვებს ვუსაბამებთ ასეოებს , და გექნება ტექსტი .

```
#include <cstdio>
#include <iostream>
#include <vector>
#include <string>
#include <algorithm>
using namespace std;
string s,s1;
int raod,p=2699,a=7,b=13,xark,n,deg=2709;
//int raod,p=11,a=1,b=6,xark,n,deg=2709;
```

```
int *mas;
pair<int,int> gmas[2709];
vector < pair<int,int> > q;
pair<int,int> g;
pair <int,int> * mas1;
void dasifrva();
void gasifrva();
void gasifruli_teqsti();
int xar(int a,int i);
void texstis_setana();
void texti_ricxvebsi();
void elifsuri_wiri();
pair<int,int> jeradoba(pair<int,int>,int n);
pair<int,int> jami(pair<int,int> w);
pair<int,int> jami(pair<int,int> w,pair<int,int> u);

int main()
{
	texstis_setana();
	texti_ricxvebsi();
	elifsuri_wiri();
	dasifrva();
	gasifrva();
	gasifruli_teqsti();
	return 0;
}

void gasifruli_teqsti()
{
	string s;
	string z=" abcdefghijklmnopqrstuvwxyz";
	for(int i=0;i<raod;i++)
	{
		s.push_back(z[mas[i]/100]);
		s.push_back(z[mas[i]%100]);
	}
	freopen("gasifruli_texti.txt","w",stdout);
	cout<<s;
}

void gasifrva()
{
	freopen("gasifruli_ricxebi.txt","w",stdout);
	for(int i=0;i<raod;i++)
	{
		for(int j=0;j<deg;j++)
		{
			if(mas1[i]==gmas[j])
			{
				mas[i]=j;
				cout<<mas[i]<<" ";
				break;
			}
		}
	}
}

void dasifrva()
{
	freopen("warmomqmnelis_jeradobebi.txt","w",stdout);
	cout<<1<<" "<<gmas[1].first<<" "<<gmas[1].second<<endl;
	cout<<2<<" "<<gmas[2].first<<" "<<gmas[2].second<<endl;
	for(int i=3;i<deg;i++)
	{
```

```
		cout<<i<<" "<<gmas[i].first<<" "<<gmas[i].second<<endl;
	}

	mas1=new pair<int,int> [raod];
	freopen("dasifruli_teqsti.txt","w",stdout);
	for(int i=0;i<raod;i++)
	{
		mas1[i]=gmas[mas[i]];
		cout<<mas1[i].first<<" "<<mas1[i].second<<endl;
	}
}

void elifsuri_wiri()
{
	freopen("wiris_elementebi.txt","w",stdout);
	for(long long i=0;i<p;i++)
	{
		long long tmp=(i*i*i+a*i+b)%p;
		int tmp1=xar(tmp,(p-1)/2)%p;
		if(tmp1==1)
		{
			xark=xar(tmp,(p+1)/4);
			q.push_back(make_pair(i,xark));
			q.push_back(make_pair(i,p-xark));
		}
	}
	n=q.size()+1;
	for(int i=0;i<n-1;i++)
	{
		printf("( %d,%d )\n",q[i].first,q[i].second);
	}
	printf("elementta raodenoba %d",n);
	//g=make_pair(9,2386);
	vector <int> k (n,0);
	pair<int,int> tmp;
	for(int i=0;i<n;i++)
	{
		bool chk=true;
		g=q[i];
		gmas[1]=g;
		gmas[2]=jami(g);
		k[gmas[1].first]++;
		k[gmas[2].first]++;
		for(int j=3;j<n;j++)
		{
			gmas[j]=jami(gmas[j-1],g);
			k[gmas[j].first]++;
			if(k[gmas[j].first]>2)
			{
				chk=false;
				break;
			}
		}
		if(chk)break;
		for(int j=0;j<n;j++)
		{
			k[j]=0;
		}
	}
}

pair<int,int> jami(pair<int,int> w)
{
	int a1,b1;
```

```
	a1=w.first;
	b1=w.second;
	long long tmp=((3*a1*a1+a)%p*(xar((2*b1)%p,p-2)))%p;
	int tmp1=(tmp*tmp-2*a1)%p;
	if(tmp1<0)tmp1+=p;
	tmp=(tmp*(a1-tmp1)-b1)%p;
	if(tmp<0)tmp+=p;
	return make_pair(tmp1,tmp);
}

pair<int,int> jami(pair<int,int> w,pair<int,int> u)
{
	if(w.first>u.first)swap(u,w);

	int tmp=u.first-w.first;
	if(tmp<0)tmp+=p;
	tmp=xar(tmp,p-2);
	int tmp1=(u.second-w.second)%p;
	if(tmp1<0)tmp1+=p;
	tmp=tmp*tmp1%p;
	tmp1=(tmp*tmp-w.first-u.first)%p;
	if(tmp1<0)tmp1+=p;
	tmp=(tmp*(w.first-tmp1)-w.second)%p;
	if(tmp<0)tmp+=p;
	return make_pair(tmp1,tmp);
}

pair<int,int> jeradoba(pair<int,int> w,int n)
{
	if(n==1)return w;
	pair<int,int> tmp=jeradoba(w,n/2);
	if(tmp.first==w.first&&n>3)return make_pair(-1,-1);
	if(tmp.first==-1)return make_pair(-1,-1);
	tmp=jami(tmp);
	if(n%2)return jami(tmp,w);
	else return tmp;
}

int xar(int r,int t)
{
	if(t==0)return 1;
	int tmp=xar(r,t/2)%p;
	tmp=(tmp*tmp)%p;
	if(t%2)return (tmp*r)%p;
	else return tmp%p;
}

void texti_ricxvebsi()
{
	freopen("texti_ricxvebsi.txt","w",stdout);
	int k=s.size();
	s1="";
	string
q[26]={"01","02","03","04","05","06","07","08","09","10","11","12","13",
		"14","15","16","17","18","19","20","21","22","23","24","25","26"};
	for(int i=0;i<k;i++)
	{
		if(s[i]==' ')
		{
			s1+="00";
			if(i%2)s1+=" ";
			continue;
		}
		s1+=q[s[i]-'a'];
```

```
                if(i%2)s1+=" ";
        }
        raod=s1.size()/5+((s1.size()%5)!=0);
        cout<<s1;
        s="";
        s1="";
        mas=new int[raod];
        freopen("texti_ricxvebsi.txt","r",stdin);
        for(int i=0;i<raod;i++)
        {
                cin>>mas[i];
        }
}

void texstis_setana()
{
        printf("texti semoitanet mxolod patara latinuri asoebit\n textis setana
daasrulet sityvit eNd \n");
        while(true)
        {
                 cin>>s1;
                 if(s1=="eNd")break;
                 s+=(s1+" ");
        }
        freopen("semotanili_texti.txt","w",stdout);
        cout<<s;
}
```

გამოყენებული ლიტერატურა

1) Лидл Р., Нидеррайтер Г., Конечные поля, Мир, Москва, 1988 .

2) Журавлев Ю.И., Флеров Ю. А., Вялый М. Н. , Дискретный анализ.Основы высшей алгебры, Мз Пресс, Москва, 2006 .

3) ზურაბ ქოჩლაძე – თანამედროვე კრიპტოგრაფიის საფუძვლები .

4) Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях .