Elliptiset käyrät kryptografiassa

Aleksander Peltoinen

Pro gradu -tutkielma
Kesäkuu 2025

MATEMATIIKAN JA TILASTOTIETEEN LAITOS

Tarkastajat:
Dos. Jyrki Lahtonen
FT. Arto Leppistö

TURUN YLIOPISTO
Matematiikan ja tilastotieteen laitos

Aleksander Peltoinen: Elliptiset käyrät kryptografiassa
Pro gradu -tutkielma, 46 s.
Matematiikka
Kesäkuu 2025

Kryptografia, eli viestin salaus, on tärkeä osa nykyistä yhteiskuntaa. Sen avulla Internetissä voidaan asioida turvallisesti ja yksityisesti. Internetin kannalta erityisen tärkeä on yleisen avaimen kryptografia, koska se sallii suojatun kanavan luomisen ilman ennalta sovittua salaista avainta. Sen avulla voidaan myös allekirjoittaa viesti ja sitä kautta varmistua, että viesti ei ole väärennetty.

Elliptinen käyrä on tietyn muotoisen yhtälön muodostama pistejoukko, jonka pisteille voidaan määritellä yhteenlaskuoperaation. Tämä joukko ja laskutoimitus muodostavat vaihdannaisen, eli Abelin ryhmän. Jos elliptinen käyrä on määritelty äärellisen kunnan yli, niin ryhmän jokainen alkio virittää äärellisen syklisen aliryhmän. Tähän sykliseen aliryhmään liittyy elliptisen käyrän diskreetin logarithmin ongelma, jolle ei tunneta tehokasta ratkaisualgoritmia.

Elliptisen käyrän kryptosysteemi on tyypiltään yleisen avaimen kryptografia, joka perustuu elliptisen käyrän diskreetin logarithmin ongelmaan. Koska elliptisen käyrän yhteenlaskuoperaatio on hyvin monimutkainen, tietyn suojaustason saavuttamiseen vaaditaan huomattavasti lyhyempi avain kuin muissa yleisesti käytetyissä yleisen avaimen kryptosysteemeissä. Tämän lisäksi, koska laskutoimitukset suoritetaan huomattavasti pienemmissä kunnissa, salaus ja purku ovat huomattavasti nopeampia ja vaativat vähemmän laskentaresursseja.

Tutkielmassa perehdytään perusteellisesti elliptisen käyrän keskeisiin käsitteisiin. Näytetään, miten elliptisen käyrän ominaisuudet periytyvät kuutiollisista käyristä ja määritellään elliptisen käyrän laskutoimituksia. Sen jälkeen esitetään Edwardsin käyrää, näytetään, miten sen laskut periytyvät elliptisestä käyrästä ja millainen elliptinen käyrä voidaan esittää Edwardsin käyränä. Lopuksi näytetään, miten elliptisen käyrän muodostama ryhmä käytetään kryptografiassa.

Asiasanat: Kryptografia, elliptinen käyrä, Edwardsin käyrä.

Sisällys

1 Johdanto

Kryptografia on tärkeä osa nykyistä yhteiskuntaa. Se tulee vastaan, kun luetaan sähköpostia, kirjaudutaan sosiaaliseen mediaan tai maksetaan ostoksia pankkikortilla tai nettipankin välityksellä. Kryptografian avulla voidaan lähettää yksityisiä viestejä julkisia kanavia pitkin. Sen avulla voidaan myös varmistaa viestin aitous.

Kryptosysteemit voidaan jakaa symmetriseen ja julkisen avaimen salaukseen. Symmetrisessä salausmenetelmässä samaa salaista avainta käytetään sekä salaukseen että salauksen purkaamiseen. Julkisen avaimen salauksessa käytetään kahta avainta, julkista ja yksityistä. Käyttötarkoituksesta riippuen toisella salataan, toisella puretaan salausta. Julkisen avaimen salaus mahdollistaa avaintenvaihdon ja digitaalisen allekirjoituksen.

Yleisimmin käytetyt julkisen avaimen kryptosysteemit ovat: kokonaislukujen tekijöihinjaon ongelmaan perustuva RSA, diskreettiin logaritmin ongelmaan perustuva Diffie-Hellman ja elliptisen käyrän diskreetti logaritmiin perustuvat EC-kryptosysteemit. Mihinkään näistä ongelmista ei tunneta tehokasta ratkaisualgoritmia. Taulukosta 1 nähdään, että elliptisillä käyrillä on selvä etu; samaan suojaustasoon päästään pienemmällä avaimella kuin RSA:lla. Laskutoimitukset elliptisessä käyrässä ovat huomattavasti monimutkaisempia, mutta koska ne tehdään paljon pienemmässä äärellisessä kunnassa, ne ovat huomattavasti nopeampia.

Taulukko 1: NIST:n suosittelemat avainkoot bitteinä [7]

.

Suojaustaso	Moduluksen tekijöihinjako (RSA), pq=n	Diskreetti logaritmi(D-H), $a^k \ mod \ p$	Elliptinen käyrä, $E(\mathbb{F}_q)$
128	n=3072	k=256 p=3072	q=256
192	n=7680	k=384 p=7680	q=384
256	n=15360	k=512 p=15360	q=512

Edwardsin käyrät ovat elliptiset käyrät, joilla on tietyt hyvät ominaisuudet. Sen laskutoimitukset ovat nopeita ja laskentakustannus summalle ja tuplaukselle on sama, mikä auttaa tietynlaisia sivukanavahyökkäyksiä vastaan [2].

Elliptisin käyrien keskeiset käsitteet voivat tuntua epäintuitiivisilta, erityisesti kun kyse on Edwardsin käyristä. Tässä tutkielmassa pyrin luomaan tätä intuitiota ja visualisoimaan kuvien avulla, mitä niissä tapahtuu.

2 Algebra

Tässä kappaleessa käydään läpi algebran perusteita, erityisesti äärellisten ryhmien ja kuntien kannalta. Jos lukija tuntee nämä käsitteet hyvin, niin tämän kappaleen

voi ohittaa.

2.1 Ryhmät

Ryhmä on algebrallinen rakenne, joka muodostuu yhdestä joukosta ja yhdestä laskutoimituksesta. Laskutoimituksen pitää olla liitännäinen, joukossa suljettu ja jokaisella joukon alkiolla pitää olla käänteisalkio joukossa. Elliptisten käyrien kryptografian kannalta on myös tärkeää, että ryhmän laskutoimitus on vaihdannainen siis ryhmä on Abelin ryhmä. Määritellään ryhmä seuraavasti:

Määritelmä 1. Pari $(A, \oplus)$, on *(Abelin) ryhmä* jos se täyttää seuraavat ehdot:

1. Joukko A on epätyhjä ja laskutoimitus $\oplus$ on suljettu joukossa A, eli $a \oplus b \in A$, kaikilla $a, b \in A$;

2. Laskutoimitus on vaihdannainen $a \oplus b = b \oplus a$, kaikilla $a, b \in A$;

3. Joukossa A on neutraalialkio e, jolle $e \oplus a = a \oplus e = a$ jokaisella $a \in A$;

4. Jokaisella joukon A alkiolla on olemassa vasta-alkio, $a \oplus -a = e$;

5. Laskutoimitus on liitännäinen: $(a \oplus b) \oplus c = a \oplus (b \oplus c)$, kaikilla $a, b, c \in A$.

vasta-alkiota joskus kutsutaan myös käänteisalkioksi ja merkitään a^{-1}, näin tehdään varsinkin kertolaskuun rinnastettavan laskutoimituksen yhteydessä.

Esimerkki 1. Pari $(\mathbb{Z}_n, +)$, missä $+$ laskutoimitus on määritelty $a+b = c \pmod n$ on ryhmä kaikilla $n \in \mathbb{N}, n > 1$. Laskutoimitus on selvästi liitännäinen ja vaihdannainen joukossa $\mathbb{Z}_n$, neutraalialkio on 0 ja alkion a vasta-alkio on $-a = n - a$.

Esimerkki 2. Pari $(\mathbb{Z}_6 \setminus \{0\}, *)$, ei ole ryhmä, koska $2, 3 \in \mathbb{Z}_6 \setminus \{0\}$, mutta $2 * 3 = 6 = 0 \notin \mathbb{Z}_6 \setminus \{0\}$. Myöskään $(\mathbb{Z}_6, *)$ ei ole ryhmä, koska $0 \in \mathbb{Z}_6$ ja nollalla ei ole käänteisalkiota $0^{-1} = a \in \mathbb{Z}_6$, joka toteuttaa ehdon $0 * a = 1$

Lause 1. *Olkoon $(A, \oplus)$ ryhmä. Jos jollain $a, a_1, b \in A$ pätee $a \oplus b = a_1 \oplus b$, niin $a = a_1$*

Todistus. Koska A on ryhmä, on alkiolla $b \in A$ olemassa vasta-alkio $-b$, eli:

$$a \oplus b = a_1 \oplus b \quad || : \oplus - b$$

$$\Leftrightarrow a \oplus b \oplus -b = a_1 \oplus b \oplus -b.$$

Ryhmän liitännäisyydestä seuraa:

$$a \oplus b \oplus -b = a_1 \oplus b \oplus -b$$

$$\Leftrightarrow a \oplus e = a_1 \oplus e \Leftrightarrow a = a_1.$$

□

Tästä lauseesta seuraa suoraan eräs neutraalialkion ominaisuus.

Seuraus 1. *Jos ryhmän A alkioille a ja b pätee $a \oplus b = b$, niin $a = e$ on ryhmän neurtaalialkio.*

Määritelmä 2. Olkoon $(A, \oplus)$ on ryhmä ja joukko B on joukon A osajoukko, silloin $(B, \oplus)$ on ryhmän A *aliryhmä*, jos

1. Ryhmän A neutraalialkio e on myös ryhmän B neutraalialkio, eli $e_G = e_H$;

2. Laskutoimitus $\oplus$ on suljettu joukossa B, eli $a \oplus b \in B$ kaikilla $a, b \in B$;

3. Jokaisella alkiolla $a \in B$ on olemassa käänteisalkio $-a \in B$ eli $a \oplus -a = e$.

Huomautus 1. Aliryhmän vaihdannaisuus periytyy vaihdannaisesta ryhmästä. Eli jos ryhmä $(A, \oplus)$ on vaihdannainen ryhmä ja $(B, \oplus)$ on ryhmän A aliryhmä, niin $a \oplus b = b \oplus a$ kaikilla $a, b \in A$, eli myös kaikilla $a, b \in B \subset A$

Kryptografian kannalta erityisen tärkeä on yhden alkion virittämä aliryhmä.

Määritelmä 3. Olkoon $(G, \oplus)$ ryhmä ja $a \in G$ sen mielivaltainen alkio, silloin ryhmä $\langle a \rangle$ on pienin mahdollinen ryhmän G aliryhmä, joka sisältää alkion a.

Yhden alkion virittämä aliryhmä on aina *syklinen*, siis jokainen sen alkio $b \in \langle a \rangle$ voidaan ilmoittaa muodossa $b = a^k$, missä $k \in \mathbb{N}$. Tähän liittyy kryptografian kannalta tärkeä diskreetin logaritmin ongelma. Tästä lisää Kryptografia-kappaleessa.

Määritelmä 4. Olkoon $(A, \oplus)$ äärellinen ryhmä. Ryhmän *kertaluku* on alkioiden määrä ryhmässä: $ord(A) = |A|$. Alkion *kertaluku* $ord(a) = ord(\langle a \rangle) = |\langle a \rangle|$, $a \in A$.

Esimerkki 3. Yhden alkion $2 \in \mathbb{Z}_6$ virittämä ryhmä $(\langle 2 \rangle, +)$ on ryhmän $(\mathbb{Z}_6, +)$ aliryhmä.

Muodostetaan ryhmätaulu:

$+$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

Siitä nähdään suoraan, että $e_{\mathbb{Z}_6} = 0 = e_{\langle 2 \rangle}$, laskutoimitus on suljettu ryhmässä ja $2 + 4 = 0 = 4 + 2$, eli jokaisella ryhmän alkiolla on vasta-alkio.

Esimerkki 4. Tutkitaan ryhmän $(\mathbb{Z}_7 \setminus \{0\}, \cdot)$ aliryhmää $\langle 3 \rangle$.

$$3^2 = 2, 3^3 = 6, 3^4 = 3 \cdot 6 = 4, 3^5 = 3 \cdot 4 = 5, 3^6 = 3 \cdot 5 = 15 = 1$$

Eli aliryhmä $\langle 3 \rangle$ on ryhmä $\mathbb{Z}_7 \setminus \{0\}$ itse.

Lause 2. *(Lagrangen lause): Olkoon G äärellinen ryhmä ja H sen aliryhmä. Silloin ryhmän H kertaluku jakaa ryhmän G kertaluvun eli*

$$ord(G) = n \cdot ord(H), n \in \mathbb{N}.$$

Todistus. Lagrangen lauseen todistus on suoraviivainen, mutta siihen tarvitaan sivuluokkien määritelmää. Tarkemmin todistukseen voi perehtyä esimerkiksi Jokke Häsän Algebra II -kurssimonisteessa [1]. □

2.2 Kunnat

Määritelmä 5. Kolmikko $F = (A, \oplus, \otimes)$ on *kunta*, jos se täyttää seuraavat ehdot:

1. $(A, \oplus)$ on ryhmä;

2. $(A \setminus \{0\}, \otimes)$ on ryhmä ja 0 on ryhmän $(A, \oplus)$ neutraalialkio;

3. Kaikille $a, b, c \in A$ on voimassa osittelulaki: $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$.

Määritelmä 6. Kunnan $(\mathbb{F}, +, \times)$ karakteristikka $char(\mathbb{F}) = k$, missä $k \in \mathbb{N}$ on pienin mahdollinen, joka toteuttaa ehdon

$$k \cdot 1_F = \underbrace{1_F + ... + 1_F}_{k} = 0, \text{ missä } 1_F \text{ kunnan } \mathbb{F} \text{ kertolaskun neutraalialkio.}$$

Jos sellaista positiivista kokonaislukua k ei ole olemassa, niin $char(\mathbb{F}) = 0$

Esimerkki 5. Alkukunnan $\mathbb{Z}_p$, karakteristikka on $char(\mathbb{Z}_p) = p$, missä $p \in \mathbb{P}$.

Esimerkki 6. Reaalilukujoukon muodostaman kunnan karakteristikka on nolla, $char(\mathbb{R}) = 0$, koska $k \cdot 1 = 0$ jos ja vain jos $k = 0$

3 Elliptiset käyrät

Tästä lähtien oletamme, että tutkittavan kunnan karakteristikka on nolla tai suurempi kuin 3 $char(\mathbb{F}) \notin \{2, 3\}$. Tutkitaan ensin kolmannen asteen polynomifunktioita ja niiden juuria. Kunnan $\mathbb{F}$ yli määritelty kolmannen asteen funktiot ovat muotoa:

$$p(x) = x^3 + ax^2 + bx + c. \tag{1}$$

Koska $char(\mathbb{F}) \neq 3$, laskutoimitus $a(1+1+1)^{-1} = \frac{a}{3}$ on määritelty, voidaan tehdä muuttujanvaihto $x \mapsto u = x + \frac{a}{3}$ ja saadaan:

$$p(x + \frac{a}{3} - \frac{a}{3}) = (x + \frac{a}{3} - \frac{a}{3})^3 + a(x + \frac{a}{3} - \frac{a}{3})^2 + b(x + \frac{a}{3} - \frac{a}{3}) + c$$

$$\Leftrightarrow p(u - \frac{a}{3}) = (u - \frac{a}{3})^3 + a(u - \frac{a}{3})^2 + b(u - \frac{a}{3}) + c$$

$$= u^3 - \frac{3a}{3}u^2 + \frac{3a^2}{9}u - \frac{a^3}{27} + au^2 - \frac{2a^2}{3}u + \frac{a^3}{9} + bu - \frac{ba}{3} + c$$

$$= u^3 + (a - a)u^2 + (\frac{a^2}{3} - 2\frac{a^2}{3} + b)u - \frac{a^3}{27} + \frac{3a^3}{27} + c - \frac{ab}{3}$$

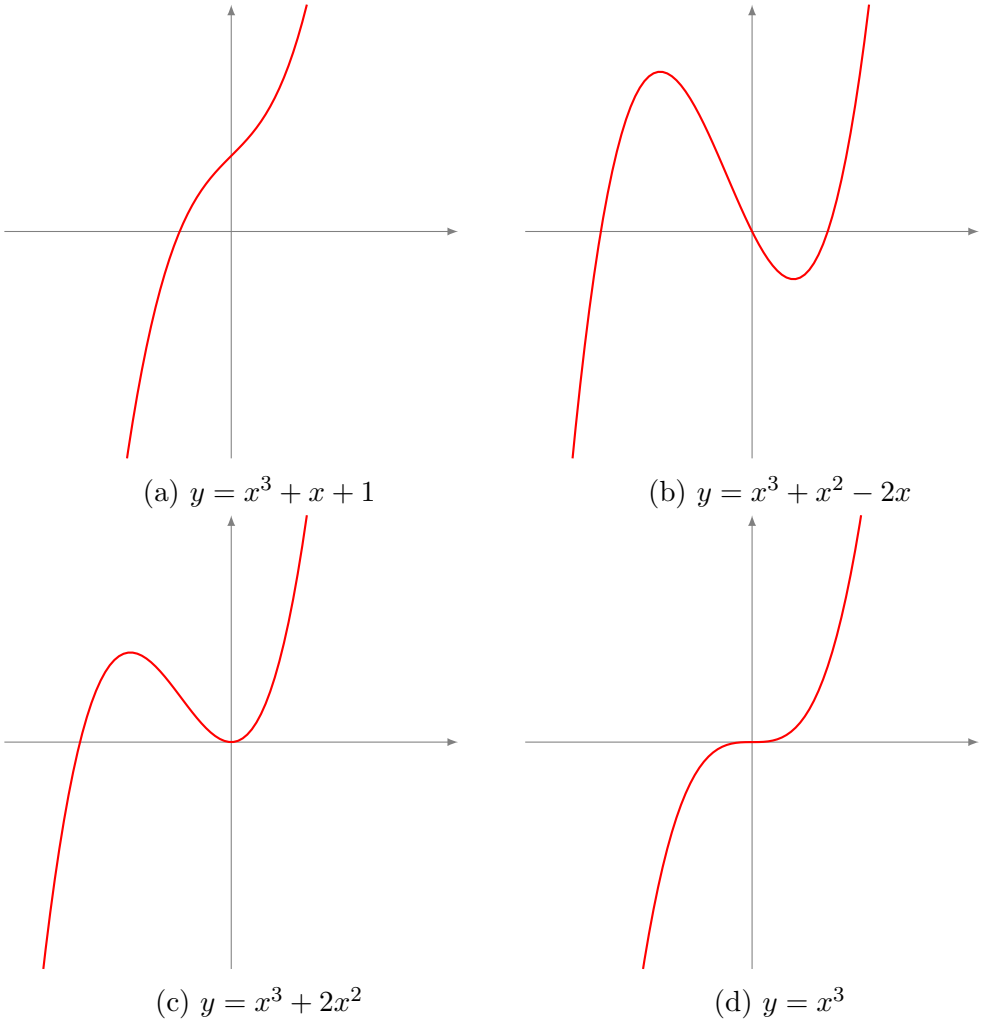
$$= u^3 + (b - \frac{a^2}{3})u + (c - \frac{ab}{3} + \frac{2a^3}{27}). \tag{2}$$

Merkitään $s = b - \frac{a^2}{3}$ ja $t = c - \frac{ab}{3} + \frac{2a^3}{27}$. Nyt funktio voidaan esittää muodossa:

$$p'(u) = u^3 + su + t \tag{3}$$

ja, jos (x_1, y_1) on yhtälön $p(x)$ ratkaisu, niin $(x_1 + \frac{a}{3}, y_1)$ on $y = p'(x)$ rakaisu. Näin todettiin, että kaikki kolmannen asteen polynomit voidaan esittää yksinkertaisemmassa muodossa.

Seuraavaksi tutkitaan polynomin $p(x)$ juuria. Reaalilukujoukon kunnassa $\mathbb{R}$ kolmannen asteen polynomifunktiolla on yksi tai kolme juurta, osa juurista voi olla moninkertaisia.



(a) $y = x^3 + x + 1$ (b) $y = x^3 + x^2 - 2x$

(c) $y = x^3 + 2x^2$ (d) $y = x^3$

Kuva 1: Kolmannen asteen yhtälöitä kunnan $\mathbb{R}$ yli.

Kuvissa 1a ja 1b nähdään käyrät, joilla ei ole moninkertaisia juuria, kuvan 1c käyrällä on kaksinkertainen juuri ja kuvan 1d käyrällä kolminkertainen juuri. Moninkertaisten juurien olemassaolo voidaan tutkia diskriminantin avulla. Olkoon x_1, x_2 ja x_3 polynomin $p(x) = x^3 + Ax + B$ juuret, osa juurista voi olla kompleksisia. Nyt saadaan diskriminantti [3, s.9]

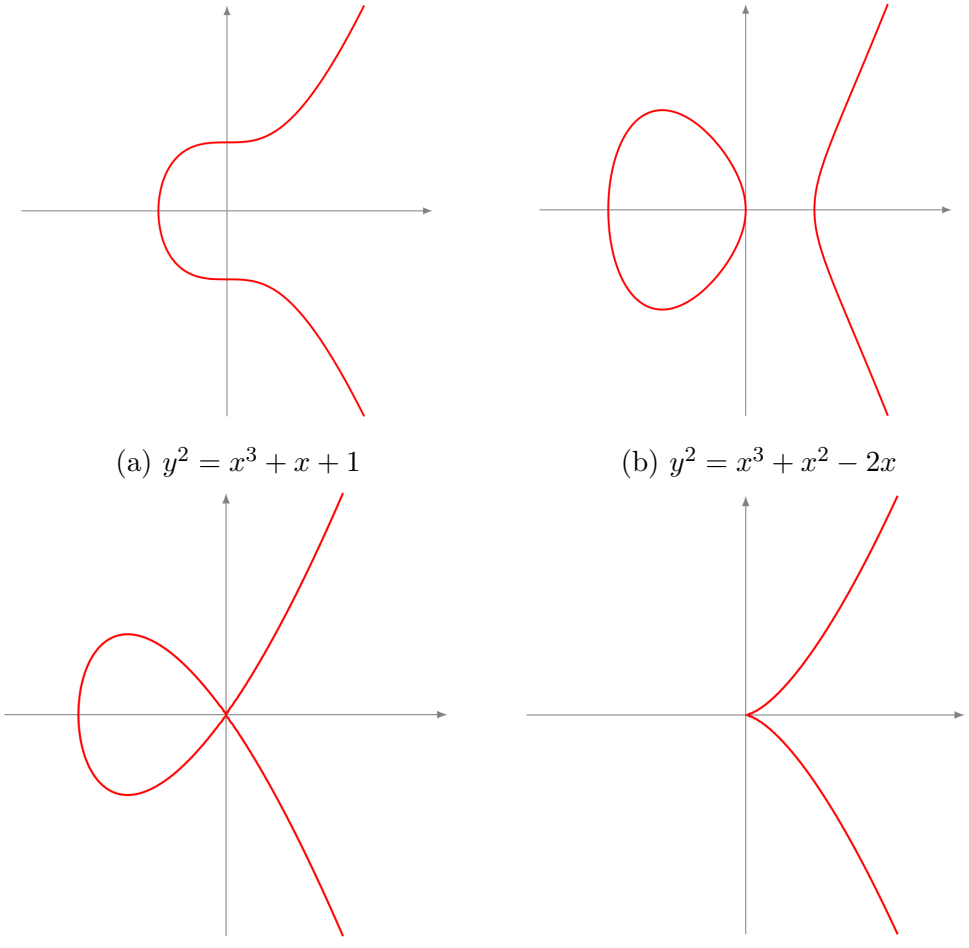
$$\Delta = ((x_1 - x_2)(x_1 - x_3)(x_2 - x_3))^2 = -(4A^3 + 27B^2). \tag{4}$$

Tästä suoraan nähdään, että diskriminantti $\Delta = 0$ täsmälleen silloin, kun polynomilla on moninkertainen juuri.

Tutkitaan nyt yhtälöä

$$y^2 = p(x) = x^3 + ax^2 + bx + c,$$

,missä p(x) on kolmannen asteen polynomi ja kertoimet a, b, c, d kuuluvat kuntaan, jonka yli yhtälö on määritelty. Tämä yhtälö kuvaa elliptistä käyrää. Kuvassa 2 nähdään kuvan 1 polynomija vastaavat käyrät.



(a) $y^2 = x^3 + x + 1$ (b) $y^2 = x^3 + x^2 - 2x$

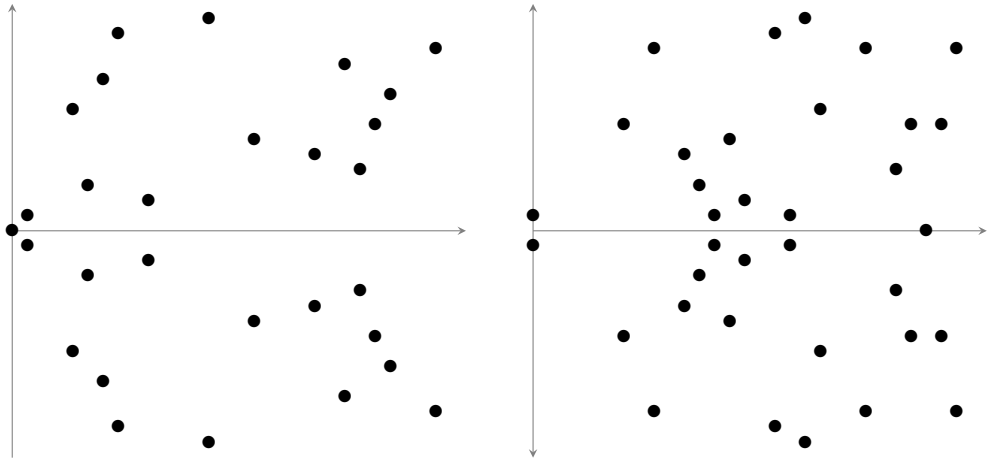
(c) $y^2 = x^3 + 2x^2$ (d) $y^2 = x^3$

Kuva 2: Yhtälöt $y^2 = p(x)$ kunnan $\mathbb{R}$ yli.

Kuvassa 2 nähdään kaikki yhtälön $y^2 = p(x)$ käyrän tyypit. Kuvien 2a ja 2b ovat sileitä ja epäsingulaarisia. Jokaiselle epäsingulaarisen käyrän pisteelle voidaan määritellä yksikäsitteinen kulmakerroin ja sen avulla piirtää tangenttisuora. Kuvien 2c ja 2d käyrissä on singulaaripiste $(0, 0)$, joka on myös moninkertainen polynomin $p(x)$ juuri. Näille pisteille ei voida määritellä yksikäsitteistä kulmakerrointa. Visuaalisesti se nähdään itseään leikkaavana käyränä tai terävänä kärkenä. Tämä on elliptisten käyrien aritmetiikassa, sillä singulaarisesta käyrästä ei saada muodostettua ryhmää, tästä puhutaan enemmän aritmetiikkaosiossa.

Kuitenkin kryptografian kannalta meitä kiinnostaa nämä yhtälöt äärellisissä kunnissa ja tämän tutkielman kannalta alkulukukunnassa $\mathbb{Z}_p$, missä p on alkuluku.

Tällöin käyrä on joukko pisteitä ja singulaarisuus ei näy suoraan kuvaajasta. Kuvan 3a yhtälö on singulaarinen ja kuvan 3b on epäsingulaarinen kunnan $\mathbb{Z}_{29}$ yli.



(a) $y^2 = x^3$ (b) $y^2 = x^3 + x + 1$

Kuva 3: Yhtälöt kunnan $\mathbb{Z}_{29}$ yli.

3.1 Elliptisten käyrien aritmetiikkaa

Yleisesti elliptiset käyrät määritellään Weierstrassin yleisellä muodolla:

Määritelmä 7. Weierstrassin yhtälön yleinen muoto:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{5}$$

missä $y, x, a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}$, ja $\mathbb{F}$ on kunta, oletetaan myös, että kunnan karakteristikka $char(\mathbb{F}) > 3$. Tämän lisäksi elliptisen käyrän pitää olla epäsingulaarinen, eli sen diskriminantti $\Delta \neq 0$.

Määritelmä 8. Yhtälön 5 *diskriminantti* Δ on [4, s.72]

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \tag{6}$$

missä

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2. \end{aligned} \tag{7}$$

Kolmannen asteen yhtälön tavoin sopivalla muuttujanvaihdolla Weierstrassin yhtälö voidaan muuttaa yksinkertaisempaan muotoon. Muuttujanvaihdosta puhutaan myöhemmin enemmän. Sallitun muuttujavaihdon avulla yhtälö voidaan muuttaa muotoon (seuraus 2)

$$y^2 = x^3 + Ax + B. \tag{8}$$

Tätä yhtälöä kutsutaan Weierstrassin lyhyeksi muodoksi, tai yksinkertaisesti Weierstrassin muodoksi. Tällöin yhtälön diskriminantti on:

$$\Delta = -8b_4^3 - 27b_6^2 = -8(2A)^3 - 27(4B)^2 = -16(4A^3 + 27B^2). \tag{9}$$

Tässä kohdassa huomataan, että Weierstrassin yhtälön diskriminantin arvo on nolla täsmälleen silloin, kun oikeanpuolisen kolmannen asteen polynomin diskriminantin (yhtälön 4) arvo on nolla, eli kun yhtälöllä $0 = x^3 + Ax + B$ on olemassa moninkertainen juuri.

3.1.1 Elliptisen käyrän ja suoran leikkauspisteet

Katsotaan seuraavaksi, mitä tapahtuu, kun piirretään suora, joka kulkee kahden käyrän pisteen kautta. Olkoon E elliptinen käyrä Weierstrassin muodossa, ja $P = (x_1, y_1)$ ja $Q = (x_2, y_2)$ pisteet käyrällä. Oletetaan ensin, että $x_1 \neq x_2$, silloin kahden pisteen välinen suoran kulmakerroin on

$$k = \frac{y_2 - y_1}{x_2 - x_1}, \tag{10}$$

jollain $k \in \mathbb{F}$. Jos $P = Q$ eli $x_1 = x_2$ ja $y_1 = y_2$, lisäksi vaaditaan, että $y_1 \neq 0$ pisteen P kohdalle piirretään tangenttisuora. Esittämällä elliptisen käyrän yhtälö muodossa:

$$0 = \pm\sqrt{x^3 + Ax + B} - y. \tag{11}$$

Derivoimalla yhtälö muuttujan x suhteen, saadaan kulmakerroin k:

$$\frac{d}{dx} = \pm\frac{3x^2 + A}{2\sqrt{x^3 + Ax + B}}. \tag{12}$$

Sijoittamalla $x = x_1$ ja $y_1^2 = x_1^3 + Ax_1 + B$ saadaan kulmakerroin k pisteessä (x_1, y_1)

$$k = \frac{3x_1^2 + A}{2y_1}. \tag{13}$$

Tässä kohtaa plusmiinusmerkkiä ei enää tarvita, koska se sisältyy vakiossa y_1. Nyt saadaan suoran yhtälö

$$y = k(x - x_1) + y_1 = kx + b, \tag{14}$$

missä $b = y_1 - kx_1$. Käyrän E ja suoran leikkauspisteiden x-koordinaatit saadaan sijoittamalla $y = kx + b$ elliptisen käyrän yhtälöön:

$$\begin{aligned} (kx + b)^2 &= x^3 + Ax + B \\ &\Leftrightarrow 0 = x^3 - k^2x^2 + (A - 2kb)x + (B - b^2). \end{aligned} \tag{15}$$

Koska yhtälö 15 on kolmannen asteen yhtälö ja meillä on jo tiedossa kaksi yhtälön juurta (x_1 ja x_2), yhtälö voidaan esittää muodossa:

$$\begin{aligned} 0 &= (x - x_1)(x - x_2)(x - x_3) \\ &= x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - (x_1x_2x_3), \end{aligned} \tag{16}$$

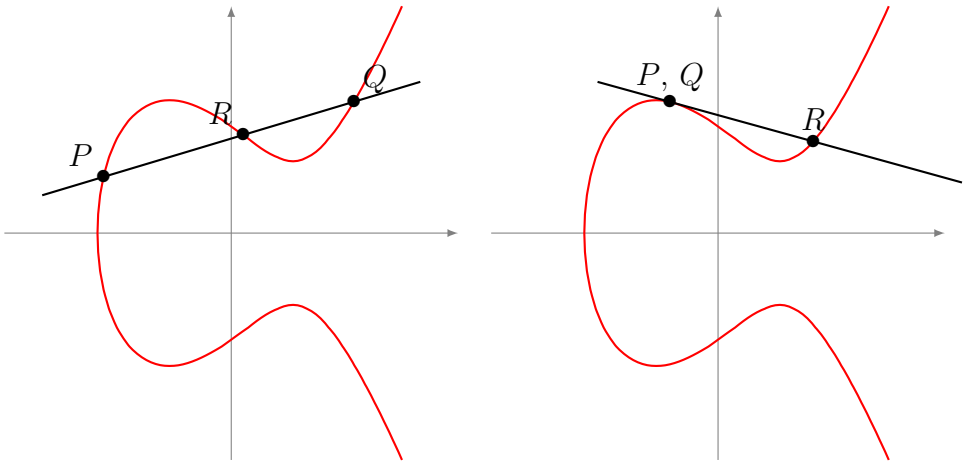
missä x_3 on yhtälön,eli kolmannen leikkauspisteen x-koordinaatti. Yhdistämällä yhtälöt 15 ja 16 saadaan x_3:

$$\begin{aligned} -k^2 &= -(x_1 + x_2 + x_3) \\ \Leftrightarrow x_3 &= k^2 - x_1 - x_2. \end{aligned} \tag{17}$$

Kolmannen leikkauspisteen y-koordinaatti saadaan sijoittamalla $x = x_3$ suoran yhtälöön:

$$y_3 = k(x_3 - x_1) + y_1. \tag{18}$$

Tässä voidaan huomata, ettei suoran yhtälön vakiotermiä b tarvitse laskea. Nyt kolmannen leikkauspisteen R koordinaatit ovat $R = (x_3, y_3)$.



(a) $P \neq Q$ (b) $P = Q$

Kuva 4: Elliprisen käyrän ja suoran leikkauspisteet P, Q ja R kunnassa $\mathbb{R}$.

Esimerkki 7. Olkoon elliptinen käyrä $E : y^2 = x^3 - 2x + 4$ kunnan $\mathbb{Q}$ yli. Käyrän pisteet $P = (0, -2)$, $Q = (3, 5)$. Lasketaan pisteiden P ja Q läpi kulkevan suoran kolmannen leikkauspisteen koordinaatit.

Katsotaan ensin, että pisteet ovat käyrällä E.

$$0^3 - 2 \cdot 0 + 4 = 4 = (-2)^2$$

$$3^3 - 2 \cdot 3 + 4 = 27 - 6 + 4 = 25 = 5^2$$

lasketaan kulmakerroin

$$k = \frac{5 - (-2)}{3 - 0} = \frac{7}{3}.$$

Sijoitetaan $k = \frac{7}{3}$ yhtälöön 17

$$x_3 = \frac{7^2}{3^2} - 0 - 3$$

$$= \frac{49}{9} - \frac{27}{9} = \frac{22}{9}.$$

Sijoitetaan $x_3 = \frac{22}{3}$ ja $k = \frac{7}{3}$ suoran yhtälöön ja saadaan:

$$y_3 = \frac{7}{3}(\frac{22}{9} - 0) + (-2) = \frac{154}{27} - \frac{54}{27} = \frac{100}{27}.$$

Näin saatiin laskettua kolmas leikkauspiste on $R = (\frac{22}{9}, \frac{100}{27})$.

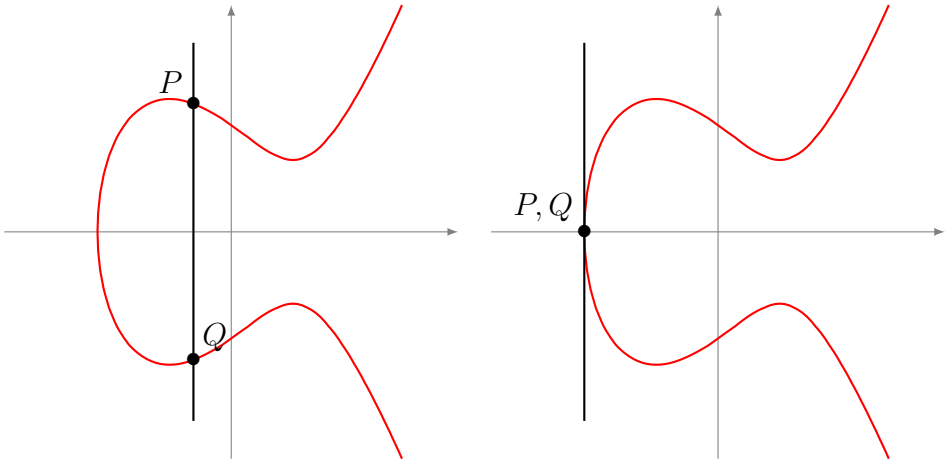
Tutkimatta jäi tapaukset, kun käyrän pisteet $P = (x_1, y_1)$ ja $Q = (x_1, -y_1)$. Oletetaan ensin, että $P \neq Q$, eli $y_1 \neq 0$. Silloin pisteitä yhdistävä suora on pystysuora ja yhtälö on $x = x_1$. Jos $y_1 = 0$, silloin derivaatan raja-arvo kasvaa tai vähenee rajatta:

$$\lim_{x \to x_1} \frac{3x^2 + A}{2y} = \pm\infty. \tag{19}$$

Kun x lähestyy arvoa x_1, lähestyy y arvoa 0 ja $3x_1^2 + A \neq 0$, koska muuten kolmannen asteen yhtälöllä on kaksinkertainen juuri x_1, eli käyrä ei olisi elliptinen, koska sen diskriminantti $\Delta = 0$. Siis tässäkin tapauksessa käyrän tangenttisuora on pystysuora $x = x_1$. Sijoitetaan nyt tangenttisuoran yhtälö elliptisen käyrän yhtälöön ja saadaan

$$y^2 = x_1^3 + Ax_1 + B = b, \tag{20}$$

jollain vakiolla $b \in \mathbb{F}$. Todetaan, että kyseessä on toisen asteen yhtälö ja kolmatta juurta sillä ei voi olla, eli muita leikkauspisteitä kuin P ja Q ei ole.



(a) $P \neq Q$ (b) $P = Q$

Kuva 5: Elliptisen käyrän ja pystysuoran leikkauspisteet P, Q kunnassa $\mathbb{R}$.

3.1.2 Elliptsen käyrän pisteiden muodostama ryhmä

Määritellään seuraavaksi elliptisen käyrän pisteiden joukko $E(\mathbb{F})$.

Määritelmä 9. Olkoon E elliptinen käyrä kunnan $\mathbb{F}$ yli, silloin joukko $E(\mathbb{F})$ on

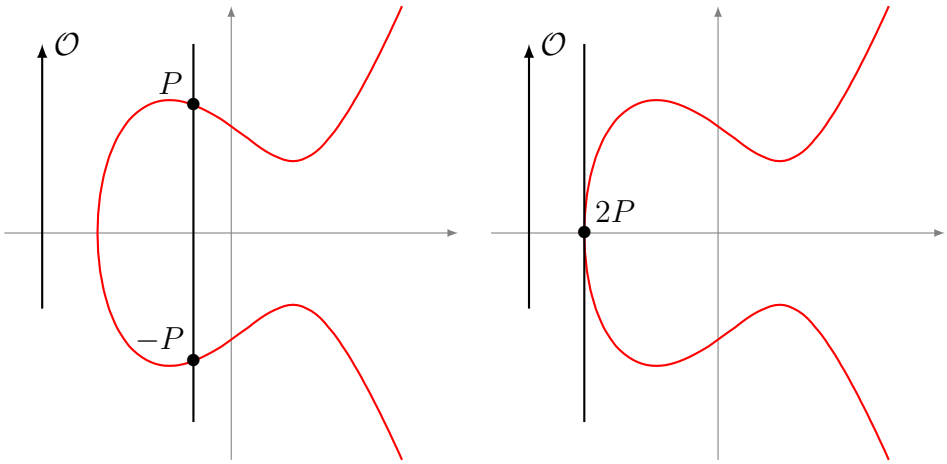
$$E(\mathbb{F}) = \{(x, y) \in \mathbb{F} \times \mathbb{F} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}, \tag{21}$$

missä $\mathcal{O}$ on äärettömyyspiste.

Käyttäen kappaleen 3.1.1 operaatioita määritellään ryhmän laskuoperaatio Weierstrassin muodossa olevan elliptisen käyrän pisteille. Olkoon P, Q ja $T = (x_T, y_T)$ kolme joukon $E(\mathbb{F})$ alkiota, jotka ovat yhdellä suoralla. Jos suora on pystysuora, niin kolmas alkio on $T = \mathcal{O}$, nimetään $\mathcal{O}$ neutraalialkioksi. Määritellään yhtälö

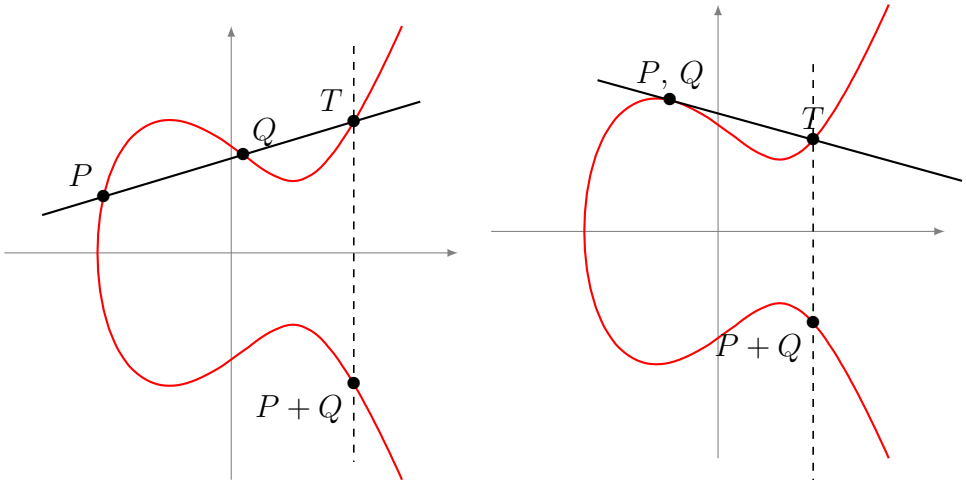
$$P + Q + T = \mathcal{O}. \tag{22}$$

Tästä määritellään laskusääntö, $P + Q = -T$, missä $-T = (x_T, -y_T)$ on alkion T vasta-alkio.



(a) $P \neq -P$ (b) $P = -P$

Kuva 6: Neutraali- ja vasta-alkiot ryhmässä $E(\mathbb{R})$, $P + -P = \mathcal{O}$.



(a) $P \neq Q$ (b) $P = Q$

Kuva 7: $P + Q$ laskutoimitus ryhmässä $E(\mathbb{R})$.

Yhdistetään tämä periaate kappaleen 3.1.1 laskutoimituksiin ja luodaan elliptisen käyrän pisteiden ryhmän laskulait Weierstrassin muodolle kunnan $\mathbb{F}$ yli.

Määritelmä 10. Elliptisen käyrän $E_{A,B}(\mathbb{F}) : y^2 = x^3 + Ax + B$ pisteiden ryhmän laskulait:

Olkoon $P = (x_1, y_1)$ ja $Q = (x_2, y_2)$ mielivaltaiset pisteet käyrällä $E_{A,B}(\mathbb{F})$

1. Neutraalialkio:
$P + \mathcal{O} = \mathcal{O} + P = P$, kaikilla pisteillä P käyrällä $E(\mathbb{F})$

2. Vasta-alkio:
$-P = (x_1, -y_1)$ on alkion P vasta-alkio, $P + -P = -P + P = \mathcal{O}$

3. Yhteenlasku:
Olkoon: $P + Q = U = (x_3, y_3)$, ja $\pm P \neq Q$, silloin
$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1$, missä $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$

4. Tuplaus:
Olkoon: $2P = P + P = U = (x_3, y_3)$ ja $y_1 \neq 0$, silloin
$x_3 = \lambda^2 - 2x_1, \quad y_3 = \lambda(x_1 - x_3) - y_1, \qquad$ missä $\lambda = \dfrac{3x_1^2 + A}{2y_1}$

Lause 3. *Määritelmän 10 laskulait muodostavat ryhmän $E_{A,B}(\mathbb{F})$.*

Todistus. Olkoon $P = (x_1, y_1)$ ja $Q = (x_2, y_2)$ mielivaltaiset pisteet käyrällä, eli käyrän $E_{A,B}(\mathbb{F})$ pisteet ja $R = (x_3, y_3)$ pisteiden P ja Q läpi kulkevan suoran ja elliptisen käyrän $E_{A,B}$ kolmas leikkauspiste.

Epätyhjyys ja neutraalialkio: Joukko $E_{A,B}(\mathbb{F})$ on epätyhjä, koska se sisältää neutraalialkion $\mathcal{O}$.

Vasta-alkio: Jos P kuuluu ryhmään niin myös $-P = (x_1, -y_1)$ kuuluu ryhmään, koska $-y_1 \in \mathbb{F}$ ja $y_1^2 = (-y_1)^2$. Eli mielivaltaisella alkiolla P on vasta-alkio $-P$ ja $P + (-P) = \mathcal{O} \in E(\mathbb{F})$.

Ryhmän sulkeneisuus: Jos $Q \neq -P$, niin piste R saadaan kolmannen leikkauspisteen laskuista, eli se on joukossa $E_{A,B}(\mathbb{F})$, silloin myös $-R = (x_3, -y_3)$, eli $P + Q = -R \in E_{A,B}(\mathbb{F})$. Jos $Q = -P$, silloin $P + Q = \mathcal{O} \in E(\mathbb{F})$.

Vaihdannaisuus: Tämä periytyy suoraan kunnan $\mathbb{F}$ vaihdannaisuudesta, sekä kulmakertoimen ominaisuudesta:

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

.

Liitännäisyys: Liitännäisyyden voi todistaa suoraan laskuilla, mutta se on pitkä ja sotkuinen, hienostuneempaan todistukseen voi tutustua Lawrence C. Washingtonin teoksessa [3]. □

Huomautus 2. Jos käyrän diskriminantti $\Delta = 0$, niin käyrä ei ole elliptinen, ja näillä laskutoimituksilla ei saada aikaan ryhmää.

Esimerkki 8. Olkoon $a \neq b$ ja $y^2 = (x-a)^2(x-b) = x^3 + Ax + B$, jonka oikeanpuolen polynomilla on kaksinkertainen juuri $x = a$, eli käyrän diskriminantti $\Delta = 0$. Lasketaan $P + Q$, missä $P = (a, 0)$ ja $Q = (b, 0)$. Lasketaan suoran kulmakerroin

$$\lambda = \frac{0-0}{a-b} = 0,$$

nyt saadaan x-koordinaatiksi:

$$x_3 = 0^2 - a - b.$$

Mutta koska käyrä on Weierstrassin muodossa, toisen asteen termin kerroin on

$$-2a - b = 0,$$

eli $x_3 = a$, y-koordinaatti on:

$$y_3 = 0(0-0) - 0 = 0.$$

Tällöin $P + Q = (a, 0) = P$ ja seurauksen 1 nojalla tämä tarkoittaisi, että $Q = (b, 0) \neq \mathcal{O}$ on myös neutraalialkio.

Esimerkki 9. Tutkitaan elliptista käyrää alkulukukunnan $\mathbb{Z}_{13}$ yli

$$E_{1,5}(\mathbb{Z}_{13}) : y^2 = x^3 + x + 5.$$

Todetaan ensin sen olevan elliptinen käyrä laskemalla diskriminantti

$$\Delta = -16(4 \cdot 1^3 + 27 \cdot 5^2) = -3(4 + 1 \cdot (-1)) = -9 = 4 \neq 0.$$

Käyrän pisteet voidaan laskea käymällä kaikki mahdolliset arvot, joita funktiot $p(x) = x^3 + x + 5$ ja $g(y) = y^2$ voivat saada kunnassa $\mathbb{Z}_{13}$. Käyttäen taulukon

x	$x^3 + x + 5 \pmod{13}$
0	5
1	7
2	2
3	9
4	8
5	5
6	6
7	4
8	5
9	2
10	1
11	8
12	3

y	$y^2 \pmod{13}$
0	0
1	1
2	4
3	9
4	3
5	12
6	10
7	10
8	12
9	3
10	9
11	4
12	1

arvoja muodostetaan elliptisen käyrän joukon

$$E_{1,5}(\mathbb{Z}_{13}) = \{\mathcal{O}, (10,1), (10,12), (7,2), (7,11), (3,3), (3,10), (12,4), (12,9)\}.$$

Lasketaan nyt $P + Q = (x_R, y_R) = R$, kun $P = (10, 1)$ ja $Q = (7, 2)$

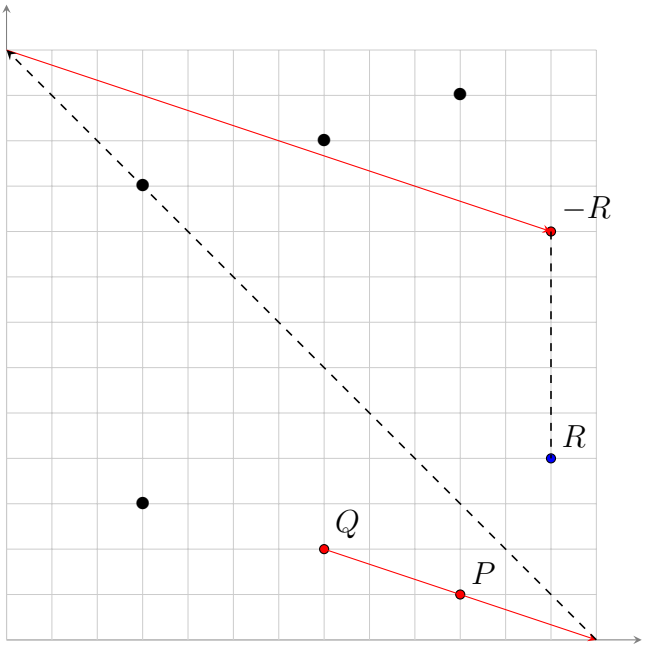
$$\lambda = \frac{2-1}{7-10} = \frac{1}{-3} = \frac{1}{10} = 10^{-1} = 4,$$

koska $10 \cdot 4 = 1$ kunnassa $\mathbb{Z}_{13}$. Yleisesti alkulukukunnan käänteisalkiot voidaan laskea Eukleideen algoritmin avulla. Sijoitetaan $\lambda = 4$ yhteenlaskukaavaan ja saadaan pisteen R koordinaatit

$$x_R = 4^2 - 10 - 7 = 16 - 17 = -1 = 12$$

$$y_R = 4(10 - 12) - 1 = 4(-2) - 1 = -9 = 4,$$

eli $R = (12, 4)$. Kuvassa 8 visualisoidaan kyseinen laskutoimitus.



Kuva 8: $P + Q = R$ lasku, punainen linja on pisteiden P ja Q läpi kulkeva suora ja diagonaali katkoviiva kuvaa $(13, 0) = (0, 13)$ joukossa $\mathbb{Z}_{13} \times \mathbb{Z}_{13}$.

Lasketaan nyt $2P = T = (x_T, y_T)$

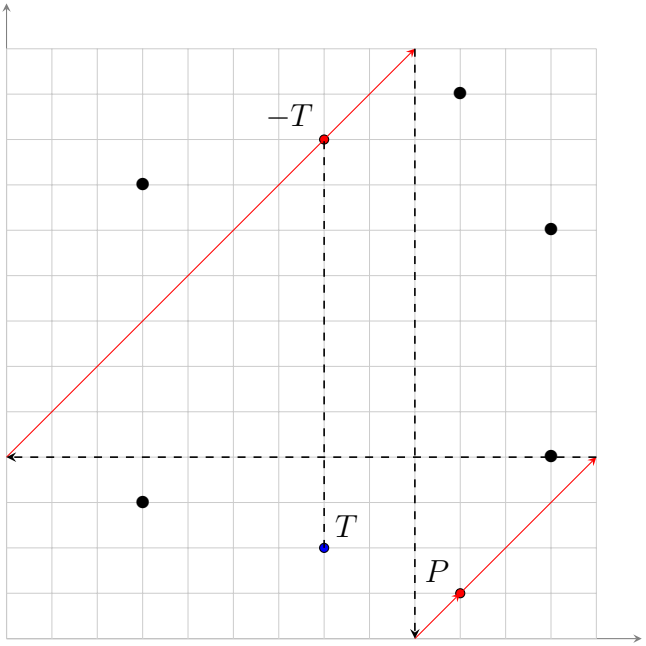
$$\lambda = \frac{2 \cdot 10^2 + 1}{2 \cdot 1} = \frac{301}{2} = \frac{2}{2} = 1,$$

eli kulmakerroin on 1.

$$x_T = 1^2 - 2 \cdot 10 = -19 = 7$$

$$y_T = 1(10 - 7) - 1 = 3 - 1 = 2,$$

Näin saatiin tulos $T = (7, 2)$. Tuplauksen visualisointi äärellisessä kunnassa on paljon vaikeampi esittää graafisesti, käytännössä pitää löytää suora, joka kulkee vain kahden pisteen kautta, kuvassa 9 näkyy tilanne $2P = T$.



Kuva 9: $2P = T$ lasku, punainen linja on pisteen P tangenttisuora, se leikka vain pisteitä P ja T.

Laskemalla pisteet yhteen, voidaan muodostaa ryhmätaulu, itse laskut jätetään väliin.

$+$	$(10,1)$	$(7,2)$	$(3,3)$	$(12,4)$	$(12,9)$	$(3,10)$	$(7,11)$	$(10,12)$
$(10,1)$	$(7,2)$	$(12,4)$	$(3,10)$	$(3,3)$	$(7,11)$	$(12,9)$	$(10,12)$	$\mathcal{O}$
$(7,2)$	$(12,4)$	$(3,3)$	$(12,9)$	$(3,10)$	$(10,12)$	$(7,11)$	$\mathcal{O}$	$(10,1)$
$(3,3)$	$(3,10)$	$(12,9)$	$(10,12)$	$(7,11)$	$(10,1)$	$\mathcal{O}$	$(7,2)$	$(12,4)$
$(12,4)$	$(3,3)$	$(3,10)$	$(7,11)$	$(12,9)$	$\mathcal{O}$	$(10,12)$	$(10,1)$	$(7,2)$
$(12,9)$	$(7,11)$	$(10,12)$	$(10,1)$	$\mathcal{O}$	$(12,4)$	$(7,2)$	$(3,3)$	$(3,10)$
$(3,10)$	$(12,9)$	$(7,11)$	$\mathcal{O}$	$(10,12)$	$(7,2)$	$(10,1)$	$(12,4)$	$(3,3)$
$(7,11)$	$(10,12)$	$\mathcal{O}$	$(7,2)$	$(10,1)$	$(3,3)$	$(12,4)$	$(3,10)$	$(12,9)$
$(10,12)$	$\mathcal{O}$	$(10,1)$	$(12,4)$	$(7,2)$	$(3,10)$	$(3,3)$	$(12,9)$	$(7,11)$

Taulukko 2: $E(\mathbb{Z}_{13})$:n ryhmätaulu.

Ryhmätaulusta nähdään suoraan, että ryhmä on syklinen, eli se on yhden alkion virittämä ja eräs virittävä alkio on $(10,1)$ ja ryhmän kertaluku on 9. Itse asiassa se on isomorfinen ryhmän $(\mathbb{Z}_9, +)$ kanssa.

Määritelmä 11. Ryhmät $\mathbb{G}$ ja $\mathbb{S}$ ovat isomorfisia, jos ja vain jos on olemassa kuvaus $f : \mathbb{G} \mapsto \mathbb{S}$ joka toteuttaa seuraavat ehdot:

I1: neutraalialkio kuvautuu neutraalialkioksi: $f(e_{\mathbb{G}}) = e_{\mathbb{S}}$;

I2: $f(P + Q) = f(P) + f(Q)$ kaikilla $P, Q \in \mathbb{G}$;

I3: kuvaus f on bijektio.

Bijektio tarkoittaa, että jokaista maalijoukon alkiota kohti on tasan yksi lähtöjoukon alkio. Sen seuraus on, että voidaan myös muodostaa käänteiskuvauksen $f^{-1} : \mathbb{S} \mapsto \mathbb{G}$, joka myös toteuttaa isomorfismin ehtoja.

Esimerkki 10. Todetaan, että esimerkin 9 ryhmä $E_{1,5}(\mathbb{Z}_{13})$ ja $(\mathbb{Z}_9, +)$ ovat isomorfisia. Muodostetaan kuvaus $f : E_{1,5}(\mathbb{Z}_{13}) \mapsto \mathbb{Z}_9$. Ryhmätaulusta Taulukko 2 todettiin jo, että $E_{1,5}(\mathbb{Z}_{13}) = \langle(10, 1)\rangle$, voidaan jokainen ryhmän alkio ilmaista muodossa $P = n(10, 1) = \underbrace{(10, 1) + ... + (10, 1)}_{n}, n \in \mathbb{N}$. Eli $f(n(10, 1)) = n$

$P \in E(\mathbb{Z}_{13})$	$f(P) \in \mathbb{Z}_9$
$(10, 1)$	1
$2(10, 1) = (7, 2)$	2
$3(10, 1) = (12, 4)$	3
$4(10, 1) = (3, 3)$	4
$5(10, 1) = (3, 10)$	5
$6(10, 1) = (12, 9)$	6
$7(10, 1) = (7, 11)$	7
$8(10, 1) = (10, 12)$	8
$9(10, 1) = \mathcal{O}$	$9 = 0$

Taulukko 3: isomorfinen kuvaus f.

Ryhmäisomorfismin $E_{1,5}(\mathbb{Z}_{13}) \simeq \mathbb{Z}_9$ avulla voidaan helpottaa laskuja huomattavasti. Yleisesti tällaisia ryhmätauluja ja isomorfismeja ei pystytä luomaan suurissa äärellisissä kunnissa. Kuitenkin tiedetään, että elliptinen käyrä luo vain tietyn tyyppisiä ryhmiä.

Lause 4. *Elliptisen käyrän muodostama ryhmä $E(\mathbb{Z}_p)$ on aina isomorfinen ryhmän $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ kanssa, jollain kokonaisluvuilla $n_1, n_2 \geq 1$ ja n_1 jakaa n_2.*

Todistus. Todistukseen voi tutustua teoksessa [3]. □

Huomautus 3. Kokonaisluku n_1 voi olla 1, silloin ryhmä on syklinen.

Seuraavaksi käydään läpi, millaisia isomorfismeja voidaan muodostaa elliptisten käyrien välillä ja miten niitä voidaan hyödyntää.

3.1.3 Muuttujanvaihto

Kirjallisuudessa muuttujanvaihto määritellään kuvauksena

$$f : (x, y) \mapsto (u, v) = (f_1(x, y), f_2(x.y)),$$

missä $(x, y), (u, v) \in \mathbb{F} \times \mathbb{F}$. Tässä kuvauksessa $f_1(x, y)$ korvataan muuttujalla u ja $f_1(x, y)$ muuttujalla v. Erityisesti meitä kiinnostavat tapaukset, jolloin kuvaus f on bijektio; silloin sillä on käänteiskuvaus g:

$$g : (u, v) \mapsto (x, y) = (g_1(u, v), g_2(u, v)).$$

Tätä käänteiskuvausta voidaan hyödyntää myös yhtälön muuttamiseen, jolloin (x, y) tilalle sijoitetaan $(g_1(u, v), g_2(u, v))$. Merkitään tällaista muutosta

$$(x, y) \mapsto (g_1(u, v), g_2(u, v)).$$

Kappaleen 3 alussa nähtiin, miten muuttujanvaihdolla voidaan yleistä kolmannen asteen yhtälöä (yhtälö 1) voidaan muuttaa yksinkertaisempaan muotoon (yhtälö 8). Tällainen muuttujanvaihto toimii myös elliptisille käyrille.

Esimerkki 11. Olkoon

$$E_1(\mathbb{F}) : y^2 = x^3 + ax^2 + bx + c$$

elliptinen käyrä jonka diskriminantti on

$$\Delta_{E_1} = -(4a)^2 \cdot (4ac - b^2) - 8(2b)^3 - 27(4c)^2 + 9(4a \cdot 2b \cdot 4c).$$

$$= 16a^2b^2 - 16(4a^3c) - 16(4b^3) - 16(27c^2) + 16(18abc)$$

$$= -16(-a^2b^2 + 4a^3c + 4b^3 + 27c^2 - 18abc) \neq 0.$$

Tehdään muuttujanvaihto $f : (x, y) \mapsto (u, v) = (x + \frac{a}{3}, y)$, yhtälöiden 2 tapaan saadaan elliptisen käyrän:

$$E_2(\mathbb{F}) : y^2 = u^3 + Au + B,$$

missä $A = b - \frac{a^2}{3}$ ja $B = -c - \frac{ab}{3} + \frac{2a^3}{27}$. Diskriminantti on nyt:

$$\Delta_{E_2} = -16(4A^3 + 27B^2) = -16(4(b - \frac{a^2}{3})^3 + 27(c - \frac{ab}{3} + \frac{2a^3}{27})^2)$$

$$= -16(4(b^3 - a^2b^2 + \frac{a^4b}{3} - \frac{a^6}{27}) + 27(c^2 - 2\frac{abc}{3} + \frac{a^2b^2}{9} + 4\frac{a^3c}{27} - \frac{4}{3}\frac{a^4b}{27} + 4\frac{a^6}{27^2}))$$

$$= -16(4b^3 - 4a^2b^2 + \frac{4}{3}a^4b - \frac{4}{27}a^6 + 27c^2 - 18abc + 3a^2b^2 + 4a^3c - \frac{4}{3}a^4b + \frac{4}{27}a^6)$$

$$= -16((-4 + 3)a^2b^2 + 4a^3c + 4b^3 + 27c^2 - 18abc + (\frac{4}{3} - \frac{4}{3})a^4b + (\frac{4}{27} - \frac{4}{27})a^6)$$

$$= -16(-a^2b^2 + 4a^3c + 4b^3 + 27c^2 - 18abc) = \Delta_{E_1} \neq 0,$$

eli E_2 on myös elliptinen käyrä. Koordinaatistossa, kyseinen muuttujanvaihto siirsi kaikki elliptisen käyrän pisteet $\frac{a}{3}$ verran vasemmalle. Muuttujanvaihtoa voidaan ajatella myös koordinaatiston vaihtona eli y-akselia siirrettiin $\frac{a}{3}$ verran oikealle.

Tutkitaan seuraavaksi muuttujanvaihtoa, missä siirretään x-akselia.

Esimerkki 12. Olkoon $E(\mathbb{R})$ elliptien käyrä

$$E(\mathbb{R}) : y^2 = x^3 - 2x + 2.$$

Tekemällä muuttujanvaihto

$$f : (x, y) \mapsto (u, v) = (x, y - x - 1),$$

saadaan käyrä $E_2(\mathbb{R})$ muodosta

$$E(\mathbb{R}) : (y - x - 1 + x + 1)^2 = x^3 - 2x + 2$$

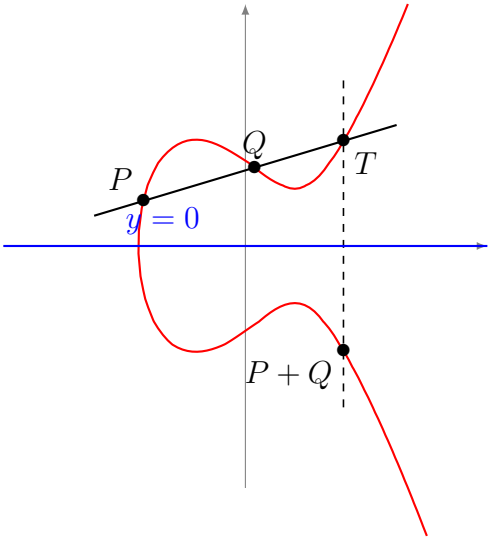
tuottaen

$$E_2(\mathbb{R}) : (v + u + 1)^2 = u^3 - 2u + 2,$$

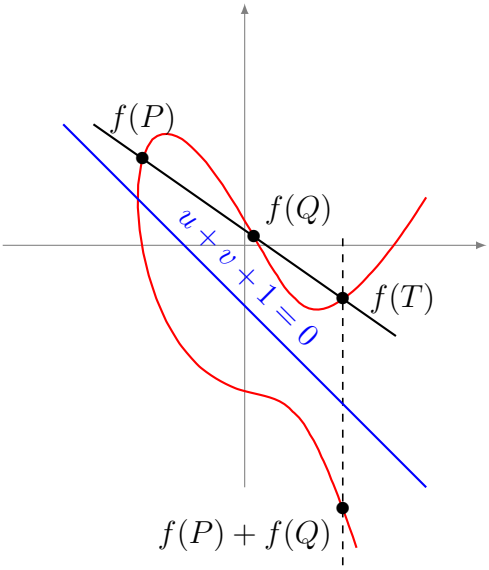
avataan sulkeet ja muokataan Weierstrassin yleiseksi muotoon:

$$v^2 + 2uv + 2v = u^3 - u^2 - 4u - 1. \tag{23}$$

Katsotaan miltä se näyttää koordinaatistossa.



Kuva 10: Käyrä $E(\mathbb{R}) : y^2 = x^3 - 2x + 2$ ja kahden pisteen laskutoimitus.



Kuva 11: Käyrä $E(\mathbb{R})$ muuttujanvaihdon jälkeen, kuvan 11 x-akseli kuvautui siniseksi suoraksi $v + u + 1 = 0$.

Määritelmä 12. Olkoon $a, b, c, d, e \in \mathbb{F}$ ja $a, c \neq 0$, niin muuttujanvaihto

$$f : \begin{cases} (x, y) \mapsto (u, v) = (ax + b, cy + dx + e) \\ \mathcal{O} \mapsto \mathcal{O}, \end{cases} \tag{24}$$

on lineaarinen muuttujanvaihto.

Lemma 1. *Lineaarinen muuttujanvaihto kuvaa suorat suoriksi, ja vain pystysuorat pystysuoriksi.*

Todistus. Jokainen suora voidaan esittää muodossa $sy+tx+k = 0$, missä $s, t, k \in \mathbb{F}$, $s \neq 0$ tai $t \neq 0$, ja $s = 0$ jos ja vain jos kyseessä on pystysuora. Tehdään nyt määritelmän 12 muuttujanvaihto, saadaan:

$$\begin{aligned} s(\frac{1}{c}(cy + dx + e - dx - e)) + t(\frac{1}{a}(ax + b - b)) + k &= \frac{s}{c}(v - dx - e) + \frac{t}{a}(u - b) + k \\ &= \frac{s}{c}v - \frac{sd}{ca}(ax + b - b) - \frac{s}{c}e + \frac{t}{a}u - \frac{t}{a}b + k \\ &= \frac{s}{c}v - \frac{sd}{ca}(u - b) + \frac{t}{a}u - \frac{se}{c} - \frac{tb}{a} + k \\ = \frac{s}{c}v + (\frac{t}{a} - \frac{sd}{ca})u - (\frac{se}{c} - \frac{tb}{a} + k + \frac{sdb}{ca}) &= 0. \end{aligned} \tag{25}$$

Näin saatiin suoran yhtälön, eli suorat kuvautuvat aina suoriksi. Lisäksi huomataan, koska $c \neq 0$, y kerroin on $\frac{s}{c} = 0$, jos ja vain jos $s = 0$ ja jos $s = 0$, niin u kerroin on $\frac{t}{a} \neq 0$, koska $t \neq 0$. Eli pystysuorat kuvautuvat pystysuoriksi ja vain pystysuora voi kuvautua pystysuoraksi. □

Lause 5. *Jos $E(\mathbb{F})$ on elliptinen käyrä ja kuvaus $f : E(\mathbb{F}) \mapsto E_1(\mathbb{F})$ on lineaarinen muuttujanvaihtokuvaus, niin $E_1(\mathbb{F})$ on elliptinen käyrä ja käyrät E ja E_1 ovat isomorfisia.*

Todistus. Todistetaan ensin, määritelmän 11 **I3** ehto, eli että lineaarinen muuttujanvaihto on bijektio. Bijektio on kuvaus, joka on surjektio ja injektio. Olkoon $f(x, y) = f(x', y')$, tämä pätee, jos ja vain jos

$$\begin{cases} ax + b = ax' + b \\ cy + dx + e = cy' + dx' + e. \end{cases}$$

Tämän yhtälöparin ainoa ratkaisu on $(x, y) = (x', y')$. Määritellään myös $f(\mathcal{O}) = \mathcal{O}$ eli kuvaus on injektio. Tämän lisäksi

Olkoon alkio (x, y) mielivaltainen alkio joukossa $\in \mathbb{F} \times \mathbb{F}$, silloin on olemassa alkio

$$(x', y') = (\frac{x - b}{a}, \frac{y - e}{c} - d\frac{(x - b)x}{ac}),$$

joka kuvautuu alkioksi (x, y)

$$f : (x', y') \mapsto (ax' + b, cy' + dx' + e) = (a\frac{x - b}{a} + b, c(\frac{y - e}{c} + d\frac{(x - b)x}{ac}) - d\frac{x - b}{a} + e)$$

$$= (x - b + b, y - e + d\frac{(x-b)x}{ac} - d\frac{(x-b)x}{ac} + e) = (x, y).$$

Tämän lisäksi äärettymyyspisteen $\mathcal{O}$ alkukuva on $\mathcal{O}$, näin todistettiin, että jokaisella alkiolla on alkukuva, eli kuvaus on myös surjektio. Tästä seuraa, että kuvaus on bijektio.

Ehto **I1** on triviaali, neutraalialkio kuvautuu neutraalialkioksi $\mathcal{O} \mapsto \mathcal{O}$.

Ehto **I2** todistetaan lemman 1 avulla, ja suoran ja käyrän leikkauspisteiden avulla. Olkoon $P + Q = R$, missä $P, Q, R \in E(\mathbb{F})$, silloin pisteet $P, Q, -R$ ovat eräällä suoralla. Koska suorat kuvautuvat suoriksi, niin myös pisteet $f(P), f(Q), f(-R)$ ovat eräällä suoralla.

Alkio R ja sen käänteisalkio $-R$, ovat pystysuoralla, koska pystysuorat kuvautuvat pystysuoriksi, myös $f(R)$ ja $f(-R)$ ovat pystysuoralla, eli $f(-R) = -f(R)$. Nyt saadaan

$$f(P) + f(Q) = f(R) = f(P + Q),$$

koska $f(P), f(Q), f(-R)$ ovat suoralla ja $f(-R) = -f(R)$ on alkion $f(R)$ käänteisalkio. □

Huomautus 4. Lineaarinen muuttujanvaihto voi tuottaa elliptisen käyrän epätavallisessa muodossa

$$c^2y^2 + a'xy + b'y = a^3x^3 + c'x^2 + d'x + e',$$

missä c ja a ovat lineaarisen (kuvauksen 12) kertoimet, ja a', b', c', d', e' eräitä vakioita. Tällainen muoto voidaan palauttaa yleiseen Weierstrassin muotoon, esimerkiksi muuttujanvaihdolla $(x, y) \mapsto (u, v) = (ax, cy)$.

Seuraus 2. *Jokainen käyrä yleisessä Weierstrassin muodossa voidaan esittää Weierstrassin lyhyenä muotona.*

Todistus. Olkoon

$$E(\mathbb{F}) : y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5$$

elliptinen käyrä. Esitetään lineaarinen muuttujanvaihto $f : E(\mathbb{F}) \mapsto E_{A,B}(\mathbb{F})$ yhdistettynä funktiona $f = g(h)$. Seurataan esimerkkiä 12 ja täydennetään yhtälön vasen puoli trinomin neliöön.

$$y^2 + a_1xy + a_2y + \frac{a_1^2x^2}{4} + \frac{a_1a_2x}{2} + \frac{a_2^2}{4} = x^3 + a_3x^2 + \frac{a_1^2x^2}{4} + a_4x + \frac{a_1a_2x}{2} + \frac{a_2^2}{4} + a_5$$

$$\Leftrightarrow (y + \frac{a_1x}{2} + \frac{a_2}{2})^2 = x^3 + (a_3 + \frac{a_1^2}{4})x^2 + (a_4 + \frac{a_1a_2}{2})x + (\frac{a_2^2}{4} + a_5).$$

Tehdään muuttujanvaihto $h : (x, y) \mapsto (u, v) = (x, y + \frac{a_1x}{2} + \frac{a_2}{2})$, saadaan

$$v^2 = u^3 + (a_3 + \frac{a_1^2}{4})u^2 + (a_4 + \frac{a_1a_2}{2})u + (\frac{a_2^2}{4} + a_5).$$

Merkitään $a = a_3 + \frac{a_1^2}{4}$, $b = a_4 + \frac{a_1 a_2}{2}$ ja $c = \frac{a_2^2}{4} + a_5$, nyt

$$v^2 = u^3 + au^2 + bu + c.$$

Esimerkin 11 mukaan, tehdään muuttujanvaihto $g : (u, v) \mapsto (s, t) = (u + \frac{a}{3}, v)$, tuloksena on

$$t^2 = s^3 + (b - \frac{a^2}{3})s + (c - \frac{ab}{3} + \frac{2a^3}{27}).$$

Seuraavaksi merkitään $A = b - \frac{a^2}{3}$ ja $B = c - \frac{ab}{3} + \frac{2a^3}{27}$ ja näin saatiin aikaiseksi Weierstrassin lyhyt muoto:

$$t^2 = s^3 + As + B.$$

□

3.2 Neljännen kertaluvun pisteet

Neljännen kertaluvun pisteet ovat ne elliptisen käyrän $E_{A,B}(\mathbb{F})$ pisteet, joille pätee $4P = \mathcal{O}$ ja $2P \neq \mathcal{O}$. Määritelmän 10 ryhmän laskulaista nähdään, että kaikki toisen kertaluvun pisteet ovat muotoa $P = (a, 0)$, missä $x_p \in \mathbb{F}$ ovat yhtälön

$$0 = x^3 + Ax + B \tag{26}$$

juuret kunnassa $\mathbb{F}$. Jos tällaista juurta ei ole, niin myöskään neljännen kertaluvun pistettä ei voi olla, sillä jos $4P = \mathcal{O}$, niin $2Q = \mathcal{O}$ missä $Q = 2P$.

Oletetaan nyt, että yhtälöllä 26 on juuri a, yritetään nyt löytää käyrän piste P, jolle pätee $2P = (a, 0)$, pisteelle pätee myös $(a, 0) + P = -P$, kuvassa 12 nähdään miltä se näyttää kunnassa $\mathbb{R}$. Vastaavasti kuin kappaleessa 3.1.1. Tehdään ensin lineaarinen muuttujanvaihto, niin että $(x, y) \mapsto (x - a, y)$, saadaan yhtälö

$$y^2 = (x + a)^3 + A(x + a) + B = x^3 + 3ax^2 + 3a^2x + a^3 + Ax + aA + B$$

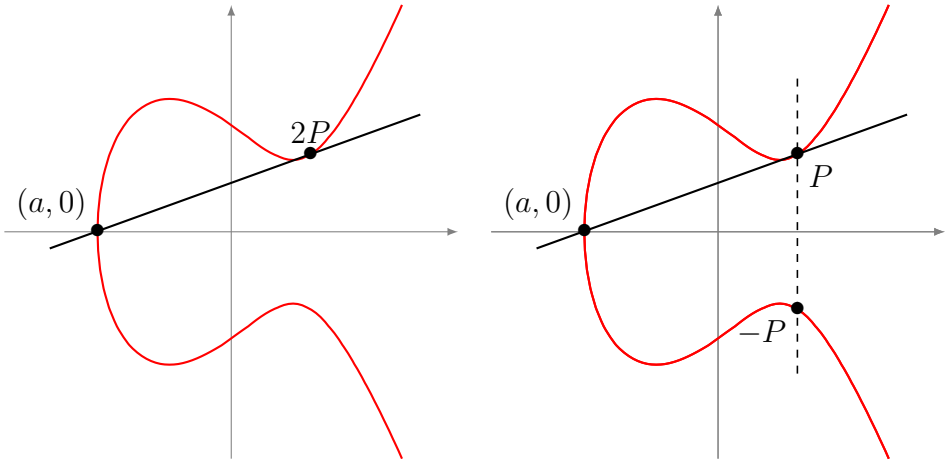
$$\Leftrightarrow y^2 = x^3 + 3ax^2 + (3a^2 + A)x + (B + a^3 + aA) \tag{27}$$

ja $(0, 0)$ on sen juuri. Tämä tarkoittaa, että vakiotermi on nolla, eli $0 = B + a^3 + aA$, eli yhtälö 27 voidaan esittää muodossa

$$y^2 = x^3 + 3ax^2 + (3a^2 + A)x. \tag{28}$$

Olkoon $P = (x_P, y_P)$, piste käyrällä ja $x_P, y_P \neq 0$ muodostetaan nyt suora, joka kulkee pisteiden $(0, 0)$ ja P läpi ja P on kaksoispiste, eli se on samalla käyrän tangentti. Koska suora kulkee pisteen $(0, 0)$ läpi, suoran yhtälö on muotoa $y = kx$, missä

$$k = \frac{y_P}{x_P}.$$



(a) $2P = (a,0)$ (b) $P + (a,0) = -P$

Kuva 12: tangentti, joka sivuaa käyrän pisteessä P ja leikkaa käyrän toisen kertaluvun pisteessä $(a,0)$.

Tangentin kulmakerroin saadaan derivaatan avulla

$$k = \frac{3x_P^2 + 6ax_P + 3a^2 + A}{2y_P},$$

ja yhdistämällä nämä yhtälöt saadaan

$$\frac{y_P}{x_P} = \frac{3x_P^2 + 6ax_P + 3a^2 + A}{2y_P}$$

$$\Leftrightarrow \frac{2y_P^2}{x_P} = 3x_P^2 + 6ax_P + 3a^2 + A,$$

koska $\frac{y^2}{x} = x^2 + 3ax + 3a^2 + A$ yhtälö voidaan esittää muodossa

$$2x_P^2 + 6ax_P + 6a^2 + 2A = 3x_P^2 + 6ax_P + 3a^2 + A,$$

yhtälö voidaan nyt sieventää muotoon

$$x_P^2 = 3a^2 + A.$$

Ratkaisu voi olla olemassa jos ja vain jos $\sqrt{3a^2 + A}$ on olemassa kunnassa $\mathbb{F}$. Tämä tarkoittaa, että Weierstrassin muodossa $E_{A,B}$ neljännen kertaluvun pisteen koordinaatti on aina muotoa

$$x = a \pm \sqrt{3a^2 + A},$$

missä a on eräs kuutiollisen polynomin nollakohta. Tämän neliöjuuren olemassaolo kunnassa ei kuitenkaan tarkoita, että elliptisellä käyrällä on neljännen kertaluvun alkio.

Esimerkki 13. Olkoon elliptinen käyrä $E_{11,9}(\mathbb{Z}_{13})$

$$E_{11,9}(\mathbb{Z}_{13}) : y^2 = x^3 + 11x + 9. \tag{29}$$

Kuutiollisen polynomin nollakohdat ovat $2, 4$ ja 7, erityisesti meitä kiinnostaa ensin mainittu juuri. Varmistetaan, että $(2, 0)$ on käyrällä

$$0^2 = 2^3 + 11 \cdot 2 + 9 = 8 + 22 + 9 = 39 = 3 \cdot 13 = 0.$$

Tarkistetaan seuraavaksi, että $3a^2 + A = 3 \cdot 2^2 + 11$ on neliö kunnassa $\mathbb{Z}_{13}$

$$3 \cdot 2^2 + 11 = 23 = 10 = 36 = 6^2.$$

Muille nollakohdille tämä ei päde, $3 \cdot 4^2 + 11 = 7$ ja $3 \cdot 7^2 + 11 = 2$ eivät ole neliöitä, eli kaikki mahdolliset neljännen kertaluvun pisteet ovat muotoa (x', y), missä $x' = 2 \pm 6$. Tällaisia pisteitä ei kuitenkaan ole käyrällä, koska

$$(-4)^3 + 11 \cdot (-4) + 9 = -99 = 5$$

ja

$$(8)^3 + 11 \cdot 8 + 9 = 609 = 11$$

eivät ole neliöitä. Näin todettiin, että käyrällä $E_{11,9}(\mathbb{Z}_{13})$ ei ole neljännen kertaluvun pisteitä, vaikka kunnassa $3a^2 + A$ on neliö.

Weierstrassin muodosta olevasta käyrästä on hyvin hankala nähdä suoraan, onko käyrällä toisen ja neljännen kertaluvun pisteitä. Tämän takia joskus halutaan esittää käyrä muodossa, neljännen kertaluvun piste on helposti löydettävissä, mikäli sellainen on.

3.2.1 Montgomeryn muoto

Yhdysvaltalainen matemaatikko Peter Lawrence Montgomery osoitti, että jos elliptinen käyrä toteuttaa tiettyjä ehtoja, niin sen luomassa ryhmässä laskutoimitukset voidaan nopeuttaa. Nämä käyrät voidaan aina esittää muodossa:

$$\mathcal{M}_{A,B}(\mathbb{F}) : By^2 = x^3 + Ax^2 + x, \tag{30}$$

diskriminantti on tällöin:

$$\Delta = B(A^2 - 4) \neq 0.$$

Tämä muoto myöhemmin nimettiin hänen mukaansa *Montgomeryn muodoksi* tai *Montgomeryn käyräksi*.

Määritelmä 13. Montgomery käyrän $\mathcal{M}_{A,B} : By^2 = x^3 + Ax^2 + x$ pisteiden ryhmän laskulait:

Olkoon $P = (x_1, y_1)$ ja $Q = (x_2, y_2)$ mielivaltaiset pisteet käyrällä $\mathcal{M}_{A,B}(\mathbb{F})$.

1. Neutraalialkio:
$P + \mathcal{O} = \mathcal{O} + P = P$, kaikilla pisteillä P käyrällä $\mathcal{M}_{A,B}(\mathbb{F})$.

2. Vasta-alkio:
$-P = (x_1, -y_1)$ on alkion P vasta-alkio, $P + -P = -P + P = \mathcal{O}$.

3. Yhteenlasku:
Olkoon: $P + Q = U = (x_3, y_3)$, ja $\pm P \neq Q$, silloin
$x_3 = B\lambda^2 - A - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1$, missä $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$.

4. Tuplaus:
Olkoon: $2P = P + P = U = (x_3, y_3)$ ja $y_1 \neq 0$, silloin
$x_3 = B\lambda^2 - A - 2x_1, \quad y_3 = \lambda(x_1 - x_3) - y_1, \qquad$ missä $\lambda = \dfrac{3x_1^2 + 2Ax_1 + 1}{2By_1}$.

Tutkitaan millaisen ryhmän Montgomeryn käyrä muodostaa. Huomataan, että Montgomeryn muodossa on aina alkio $P = (0, 0)$, jolle pätee $2P = \mathcal{O}$, eli esimerkin 9 käyrää ei voida esittää Montgomeryn muodossa. Jos $A^2 - 4$ ei ole neliö, niin piste $(0, 0)$ on ainoa toisen kertaluvun piste.

Vastaavasti potentiaalisen neljännen kertaluvun alkion Q x koordinaatti saadaan yhtälöstä

$$\frac{y_Q}{x_Q} = \frac{3x_Q^2 + 2Ax_Q + 1}{2By_Q}$$
$$\Leftrightarrow 2x_Q^2 + 2Ax_Q + 2 = 3x_Q^2 + 2Ax_Q + 1$$
$$\Leftrightarrow x_Q^2 = 1 \Leftrightarrow x_Q = \pm 1.$$

Sijoitetaan x_Q Montgomery käyrän yhtälöön ja saadaan y-koordinaatti:

$$By^2 = (\pm 1)^3 + A(\pm 1)^2 \pm 1 = A \pm 2$$
$$\Leftrightarrow y^2 = \frac{A \pm 2}{B}.$$

Jos $B(A + 2)$ tai $B(A - 2)$ on neliö, niin käyrällä on neljännen kertaluvun pisteet ja ne ovat muotoa $(1, \pm\sqrt{\frac{A+2}{B}})$ tai $(-1, \pm\sqrt{\frac{A-2}{B}})$.

Jos kuitenkin molemmat $B(A + 2)$ ja $B(A - 2)$ ovat neliöitä, niin molemmat $A + 2$ ja $A - 2$ ovat neliöitä tai eivät ole. Jos molemmat ovat neliöitä, niin myös

$$(A + 2)(A - 2) = A^2 - 4 \tag{31}$$

on neliö. Jos kunta on äärellinen, niin kahden ei neliön tulo on neliö, eli $A^2 - 4$ on neliö. Tämä pätee myös reaalilukukunnassa, koska silloin $A < -2$, mikä tarkoittaa,

että $A^2 - 2^2 > 0$, eli on $A^2 - 4$ neliö. Jos $A^2 - 4$ on neliö, käyrällä on kaksi muuta toisen kertaluvun pistettä

$$(\frac{-A \pm \sqrt{A^2-4}}{2}, 0) \in \mathcal{M}_{A,B}.$$

Nämä kolme toisen kertaluvun pistettä muodostavat aliryhmän, merkitään $P = (\frac{-A+\sqrt{A^2-4}}{2}, 0)$ ja $Q = (\frac{-A-\sqrt{A^2-4}}{2}, 0)$, ja muodostetaan ryhmätaulu.

$+$	$\mathcal{O}$	$(0,0)$	P	Q
$\mathcal{O}$	$\mathcal{O}$	$(0,0)$	P	Q
$(0,0)$	$(0,0)$	$\mathcal{O}$	Q	P
P	P	Q	$\mathcal{O}$	$(0,0)$
Q	Q	P	$(0,0)$	$\mathcal{O}$

Taulukko 4: Toisen kertaluvun pisteiden muodostama ryhmätaulu.

Näin todettiin, että Montgomeryn käyrällä on aina neljännen kertaluvun aliryhmä, mikä tarkoittaa, että ryhmän kertaluku on aina neljällä jaollinen. Palataan yhtälöön 28 ja oletetaan, että kunnassa $\mathbb{F}$ on olemassa neliöjuuri $\sqrt{3a^2 + A} \neq 0$, tehdään muuttujavaihto $x \mapsto \frac{x}{\sqrt{3a^2+A}}$ ja saadaan

$$y^2 = (x\sqrt{3a^2 + A})^3 + 3a(x\sqrt{3a^2 + A})^2 + (3a^2 + A)x\sqrt{3a^2 + A}$$

$$= (3a^2 + A)^{3/2}x^3 + 3a(3a^2 + A)x^2 + (3a^2 + A)^{3/2}x$$

$$\Leftrightarrow \frac{1}{(3a^2 + A)^{3/2}}y^2 = x^3 + \frac{3a}{\sqrt{3a^2 + A}}x^2 + x,$$

tehdään vielä yksi muuttujanvaihto, $y \mapsto y\sqrt{3a^2 + A}$, saadaan:

$$\frac{1}{\sqrt{3a^2 + A}}y^2 = x^3 + \frac{3a}{\sqrt{3a^2 + A}}x^2 + x. \tag{32}$$

Merkitään $B' = \frac{1}{\sqrt{3a^2+A}}$ ja $A' = \frac{3a}{\sqrt{3a^2+A}}$ ja saadaan Montgomeryn käyrä

$$\mathcal{M}_{A',B'} : B'y^2 = x^3 + A'x^2 + x. \tag{33}$$

Yhdistetään muuttujanvaihdot ja esitetään lauseena.

Lause 6. *Olkoon $E_{A,B}(\mathbb{F})$ elliptinen käyrä Weierstrassin lyhyessä muodossa, jolla on juuri $(a, 0)$ ja $\sqrt{3a^2 + A}$ on olemassa kunnassa $\mathbb{F}$, tällöin elliptinen käyrä voidaan esittää Montgomeryn käyränä $\mathcal{M}_{A',B'}$ muuttujanvaihdolla*

$$(x, y) \mapsto (a + x\sqrt{3a^2 + A}, y\sqrt{3a^2 + A}). \tag{34}$$

Missä $A' = \frac{3a}{\sqrt{3a^2+A}}$ ja $B' = \frac{1}{\sqrt{3a^2+A}}$.

Todistus. Olkoon $E_{A,B}(\mathbb{F})$ elliptinen käyrä, $(a,0) \in E_{A,B}(\mathbb{F})$ ja $\sqrt{3a^2+A} \in \mathbb{F}$.Tehdään yhtälön 34 lineaarinen muuttujanvaihto

$$\begin{aligned} E : (y\sqrt{3a^2+A})^2 &= (a+x\sqrt{3a^2+A})^3 + A(a+x\sqrt{3a^2+A}) + B \\ \Leftrightarrow (3a^2+A)y^2 =& (3a^2+A)x^3\sqrt{3a^3+A} + 3a(3a^2+A)x^2 + 3a^2x\sqrt{3a^2+A} \\ &+ a^3 + Ax\sqrt{3a^2+A} + aA + B. \end{aligned} \tag{35}$$

Aikaisemmin ollaan jo todettu, että jos a on kuutiollisen käyrän juuri, niin $a^3+aA+B=0$. Jaetaan molemmat puolet polynomilla $(3a^2+A)x^3\sqrt{3a^3+A}$ ja saadaan

$$\Leftrightarrow \frac{1}{\sqrt{3a^2+A}}y^2 = x^3 + \frac{3a}{\sqrt{3a^2+A}}x^2 + x.$$

Tämä vastaa Montgomeryn käyrää

$$\mathcal{M}_{A',B'} : B'y^2 = x^3 + A'x^2 + x.$$

□

Seuraus 3. *Olkoon $E_{A,B}(\mathbb{F})$ elliptinen käyrä, $(a,0) \in E_{A,B}(\mathbb{F})$ on käyrän ainoa toisen kertaluvun alkio ja $\sqrt{3a^2+A} \in \mathbb{F}$. Silloin käyrällä on olemassa neljännen kertaluvun alkio.*

Todistus. Koska tällainen käyrä voidaan esittää Montgomeryn käyränä, sillä on aliryhmä, jonka kertaluku on neljä. Koska ryhmässä on vain yksi toisen kertaluvun alkio, ryhmässä on olemassa alkio P, jolle pätee $2P \neq \mathcal{O}$ ja $4P = \mathcal{O}$. □

3.2.2 Elliptisen käyrän kertaluku ja kierrot

Palautetaan mieleen määritelmää 9 ja esitetään se Weierstrassin muodossa:

$$E(\mathbb{F}) = \{(x,y) \in \mathbb{F} \times \mathbb{F} : y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}.$$

Tätä määritelmää voidaan esittää myös muodossa

$$E(\mathbb{F}) = \{(x,y') \in \mathbb{F} \times \mathbb{F} : \pm y' = x^3 + Ax + B\} \cup \{\mathcal{O}\},$$

missä y' on neliö kunnassa $\mathbb{F}$. Eli joukossa on vain x-koordinaatit, jotka tuottavat neliön polynomin x^3+Ax+B yli. Tutkitaan nyt käyrää

$$E_k(\mathbb{F}) : ky^2 = x^3 + Ax + B,$$

missä $0 \neq k \in \mathbb{F}$. Tätä muotoa sanotaan myös käyrän $E : y^2 = x^3+Ax+B$ *kierroksi* ja yleisesti *kierreryiksi elliptiseksi käyräksi*

Jos k on neliö, voidaan tehdä lineaarinen muuttujanvaihto $y \mapsto \frac{y}{\sqrt{k}}$ ja saadaan käyrä

$$E_{k'}(\mathbb{F}) : y^2 = x^3 + Ax + B,$$

joka on lausen 24 nojalla isomorfinen käyrien E_k ja E_n kanssa. Tällaista kiertoa kutsutaan triviaaliksi kierroksi. Oletetaan, että k ei ole neliö, tehdään lineaarinen muuttujanvaihto $(x,y) \mapsto (kx,ky)$, saadaan

$$k^3y^2 = k^3x^3 + Akx + B,$$

jakamalla yhtälö vakiolla k^3 saadaan Weierstrassin muoto

$$E_{k''}(\mathbb{F}) : y^2 = x^3 + \frac{A}{k^2}x + \frac{B}{k^3}. \tag{36}$$

Tämäkin elliptinen käyrä on isomorfinen käyrän E_k kanssa. Tutkitaan seuraavaksi millaisen joukon ja ryhmän kierretty käyrä muodostaa ja miten se liittyy alkuperäiseen, kiertämättömään käyrään. Olkoon käyrä

$$E : y^2 = x^3 + Ax + B,$$

ja sen epätriviaali kierto

$$E_k : ky^2 = x^3 + Ax + B.$$

Muodostetaan joukot X_E, X_{Ek}, joihin kuuluu elliptisten käyrien pisteiden x-koordinaatit

$$X_E = \{x : y^2 = x^3 + Ax + B, x, y \in \mathbb{F} \times \mathbb{F}\},$$

$$X_{Ek} = \{x : ky^2 = x^3 + Ax + B, x, y \in \mathbb{F} \times \mathbb{F}\}.$$

Koska k ei ole neliö, niin myös ky^2 ei ole neliö. Koska kunnan jokainen alkio on joko neliö tai ei ole ja polynomi on määritelty jokaiselle alkiolle, joukkojen unioni on koko kunta

$$X_E \cup X_{Ek} = \mathbb{F}.$$

Tämän avulla nyt voidaan laskea E ja E_k yhteenlaskettujen alkioiden määrää $|E| + |E_k|$.

Lause 7. *Olkoon $\mathbb{F}$ äärellinen kunta, jonka keraluku $|\mathbb{F}| = q$, $E(\mathbb{F})$ elliptinen käyrä ja $E_k(\mathbb{F})$ sen epätriviaali kierto, silloin näiden joukkojen yhteenlaskettu alkioiden määrä on*

$$|E| + |E_k| = 2q + 2.$$

Todistus. Olkoon $x \in \mathbb{F}$, $E : y^2 = x^3 + Ax + B$ ja $E_k : ky^2 = x^3 + Ax + B$. Jos x polynomin $x^3 + Ax + B$ nollakohta, niin alkio $(x, 0)$ kuuluu molempiin joukkoihin, eli se lasketaan kaksi kertaa. Oletetaan nyt, että x ei ole polynomin nollakohta, nyt jos $x^3 + Ax + B$ on neliö, niin $(x, \pm\sqrt{x^3 + Ax + B}) \in E$, jos ei, niin $(x, \pm\sqrt{\frac{x^3+Ax+B}{k}})$. Kummassakin tapauksessa alkio lasketaan kahteen kertaan. Tämän lisäksi kumpaankin joukkoon kuuluu äärettömyyspiste $\mathcal{O}$. Näin saatiin

$$|E| + |E_k| = 2|\mathbb{F}| + 2|\{\mathcal{O}\}| = 2q + 2.$$

□

Esimerkki 14. Elliptisen käyrän kierrot reaalilukukunnassa

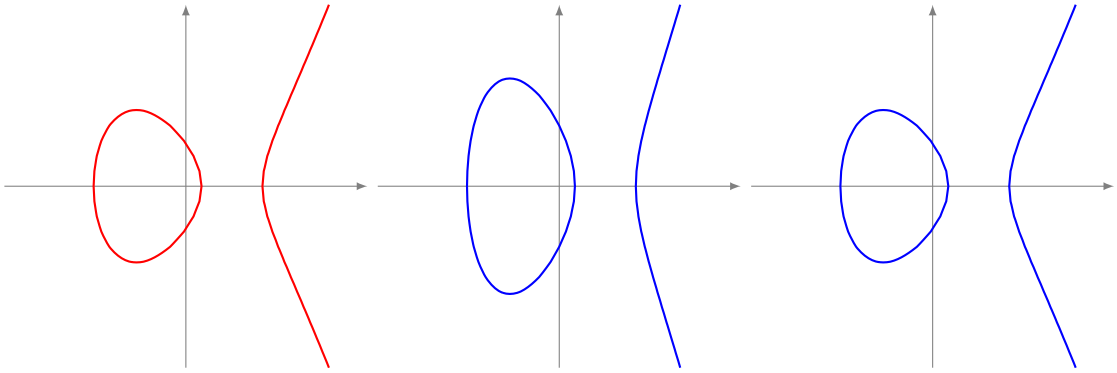
Olkoon elliptinen käyrä

$$E_{-2,\frac{1}{2}}(\mathbb{R}) : y^2 = x^3 - 2x + \frac{1}{2},$$

ja sen kierrot

$$Ek_{-2,\frac{1}{2}}(\mathbb{R}) : ky^2 = x^3 - 2x + \frac{1}{2},$$

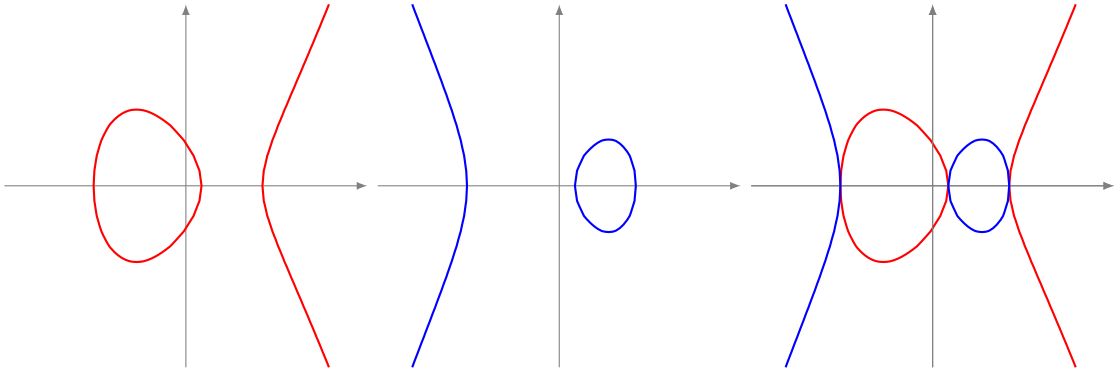
missä $k \neq 0$. Tutkitaan ensin tapaukset, missä k on neliö, reaalilukukunnassa se tarkoittaa, että $k > 0$. Jos $(x_1, y_1) \in E_{-2,\frac{1}{2}}$, niin $(x_1, \frac{1}{\sqrt{k}}y_1) \in Ek_{-2,\frac{1}{2}}$, eli y-akseli skaalataan vakiolla $\frac{1}{\sqrt{k}}$.



(a) $y^2 = x^3 - 2x + \frac{1}{2}$ (b) $\frac{1}{2}y^2 = x^3 - 2x + \frac{1}{2}$ (c) $\frac{1}{2}y^2 = x^3 - 2x + \frac{1}{2}$

Kuva 13: Käyrä $E_{-2,\frac{1}{2}}(\mathbb{R})$ ja sen kierto $k = \frac{1}{2}$, kuvassa (c) y-akseli on skaalattu näyttämään samalta kuin käyrä kuvassa (a).

Oletetaan nyt, että k ei ole neliö, eli $k < 0$. Tätä kiertoa voidaan ajatella kahdeksi peräkkäiseksi kierroksi, missä $k_1 = |k|$ ja $k_2 = -1$. Eli riittää näyttää, miltä kierto näyttää, kun $k = -1$.



(a) $y^2 = x^3 - 2x + \frac{1}{2}$ (b) $-y^2 = x^3 - 2x + \frac{1}{2}$ (c) käyrät (a) ja (b) yhdessä

Kuva 14: Käyrä $E_{-2,\frac{1}{2}}(\mathbb{R})$ ja sen kierto, kun $k = -1$.

Yhdistetään nämä käyrät yhdeksi kuvaksi ja huomataan, että jokainen arvo $x \in R$ on käyrällä $E_{-2,\frac{1}{2}}(\mathbb{R})$ tai sen kierolla $Ek_{-2,\frac{1}{2}}(\mathbb{R})$, kun $k < 0$.

3.3 Edwardsin Käyrä

Yhdysvaltalainen matemaatikko Harold Mortimer Edwards, Jr. esitti elliptisen käyrän, joka on muotoa

$$E : x^2 + y^2 = a^2(1 + x^2y^2),$$

hän kutsui tätä muotoa elliptisen käyrän normaalimuodoksi. Tällaisen muodon eräs etu on, että tuplauksen ja summan algoritmi on sama. Olkoon $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$, silloin laskukaava on

$$(x_3, y_3) = (\frac{1}{a} \cdot \frac{x_1y_2 + x_2y_1}{1 + x_1y_1x_2y_2}, \frac{1}{a} \cdot \frac{y_1y_2 - x_1x_2}{1 - x_1y_1x_2y_2}).$$

Myöhemmin tätä käyrää yleistettiin muotoon

$$Ed_{a,d}(\mathbb{F}) : ax^2 + y^2 = 1 + dx^2y^2,$$

tätä käyrää kutsutaan *kierretyksi Edwardsin käyräksi* jos $a \neq 1$ ja *Edwardsin käyräksi* jos $a = 1$, parametri $a \neq 0$ on kiertoparametri, jos se on neliö, niin voidaan tehdä muuttujanvaihto $x \mapsto \frac{x}{\sqrt{a}}$ ja saadaan

$$\frac{a}{a}x^2 + y^2 = 1 + \frac{d}{a}x^2y^2$$

Määritelmä 14. Olkoon $(a - d)ad \neq 0$, silloin

$$Ed_{a,d}(\mathbb{F}) = ax^2 + y^2 = 1 + dx^2y^2$$

on Edwardsin käyrä ja sen pisteiden ryhmän laskulait ovat:

Olkoon $P = (x_1, y_1)$ ja $Q = (x_2, y_2)$ mielivaltaiset pisteet käyrällä $Ed_{a,d}(\mathbb{F})$

1. Neutraalialkio:
$(0, 1) + P = P + (0, 1) = P$, kaikilla $P \in Ed_{a,d}$.

2. Vasta-alkio:
$-P = (-x_1, y_1) \in Ed_{a,d}$, kaikilla $P \in Ed_{a,d}$.

3. Yhteenlasku ja tuplaus:
olkoon: $P + Q = U = (x_3, y_3)$, silloin

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \quad y_3 = \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}.$$

Huomautus 5. Ehto $(a - d)ad \neq 0$ tarkoittaa, että $a, d \neq 0$ ja $a \neq d$. Jos $a = d$, niin yhtälö on muotoa

$$ax^2 + y^2 = 1 + ax^2y^2$$

$$\Leftrightarrow y^2 - 1 = ax^2(y^2 - 1)$$

$$\Rightarrow \frac{y^2 - 1}{y^2 - 1} = 1 = ax^2, \text{kun } y \neq \pm 1.$$

Eli käyrän äärelliset pisteet ovat silloin suorilla $y = \pm 1$ ja $x = \pm\sqrt{a^{-1}}$, jos a on neliö.

Tästä määritelmästä nähdään suoraan eräs Edwardsin käyrän vahvimmista puolista, ryhmäoperaatiot ovat samoja summaukselle ja tuplaukselle. Kyseisistä kaavoista ei kuitenkaan aukea, mitä ryhmäoperaatioissa tehdään ja miltä ryhmäoperaatiot näyttävät graafisesti. Tutkitaan tätä muuttujanvaihdon kautta. Bernstein, Birkner, Joye, Lange ja Peters osoittivat, että jokainen Montgomeryn käyrä voidaan esittää kierrettynä Edwardsin käyränä ja jokainen kierretty Edwardsin käyrä voidaan esittää Montgomeryn käyränä [9].

Tämä vastaavuus voidaan esittää muuttujanvaihtona $f : \mathcal{M}_{A,B} \mapsto Ed_{a,d}$.

Lause 8. *Jokainen Montgomeryn käyrä $\mathcal{M}_{A,B} : Bv^2 = u^3 + Au^2 + u$ on isomorfinen Edwardsin käyrän $Ed_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$ kanssa, kun*

$$\begin{cases} a = (A+2)/B \\ d = (A-2)/B. \end{cases}$$

Muuttujanvaihtokuvaus on silloin

$$f : \begin{cases} (u,v) \mapsto (x,y) = (\frac{u}{v}, \frac{u-1}{u+1}), & \text{kun } u \neq -1 \text{ ja } v \neq 0 \\ (0,0) \mapsto (0,-1) \\ \mathcal{O} \mapsto (0,1), \end{cases} \tag{37}$$

ja käänteiskuvaus on

$$g : \begin{cases} (x,y) \mapsto (u,v) = (\frac{1+y}{1-y}, \frac{1+y}{(1-y)x}), & \text{kun } x \neq 0 \text{ ja } y \neq 1 \\ (0,-1) \mapsto (0,0) \\ (0,1) \mapsto \mathcal{O}. \end{cases} \tag{38}$$

Tämän lisäksi muut toisen kertaluvun alkiot $(u,v) \in \{(u_1,0),(u_2,0)\} \subset \mathcal{M}_{A,B}$, sekä neljännen kertaluvun alkiot $(u,v) = (-1, \pm\sqrt{\frac{A-2}{B}})$ kuvautuvat poikkeuspisteisiin, jos sellaisia on käyrällä.

Todistus. Todistus esitetään Bernsteinin, Birknerin, Joyen, Langen ja Peterin julkaisussa "Twisted Edwards Curves"[9]. □

Huomautus 6. Edellisessä lauseessa mainituille poikkeuspisteille ei päde määritelmän 14 ryhmän laskulait, vaan ne pitää laskea erikseen. Kryptografiassa tällaisia käyriä pyritään välttämään.

Tutkitaan seuraavaksi, miten muuttujanvaihtokuvaus f kuvaa suoria, tätä kautta saadaan selville, miten Edwardsin käyrän ryhmäoperaatiot toimivat. Ensiksi tutkitaan pystysuoraa (a', t), missä a' on vakio ja t muuttuja.

$$f : (a', t) \mapsto (\frac{a'}{t}, \frac{a'-1}{a'+1}), \tag{39}$$

Tämä on vaakasuora $y = \frac{a'-1}{a'+1}$, kun $a' \neq -1$. Kun $a' = -1$, silloin pystysuora leikkaa ne neljännen kertaluvun pisteet, jotka kuvautuvat poikkeuspisteisiin. Eli vastaalkiot Edwardsin käyrällä löytyvät vaakatasolla, tämä nähdään myös määritelmästä

14. Oletetaan nyt, että kyseessä ei ole pystysuora, tutkitaan miten kyseinen muuttujanvaihto muuttaa suoran yhtälön $v = a'u + b'$. Tehdään sijoitus

$$(u, v) \mapsto (\frac{1+y}{1-y}, \frac{1+y}{(1-y)x}),$$

näin suoran yhtälö muuttuu muotoon

$$\frac{1+y}{(1-y)x} = a'\frac{1+y}{1-y} + b'$$

$$\Leftrightarrow 1 + y = a'(1+y)x + b'(1-y)x$$

$$\Leftrightarrow \frac{1+y}{(a'+b') + (a'-b')y} = x.$$

Tästä nähdään, että jos $a' \neq b'$, niin kyseessä on hyperbeli, jonka asymptootit ovat

$$y = -\frac{a'+b'}{a'-b'}$$

ja

$$x = \lim_{y\to\infty} \frac{1+y}{(a'+b') + (a'-b')y} = \frac{1}{a'-b'}.$$

Tässä voidaan huomata myös, että vaikka saatu käyrä ei ole määritelty kun $x = 0$, sen raja-arvo siinä pisteessä on aina piste $(0, -1)$. Erikoistapaus on $a' = b'$, kyseessä on suora $y = 2a'x - 1$, eli pisteen $(-1, 0)$ läpi kulkevat suorat kuvautuvat pisteen $(0, -1)$ läpi kulkeviksi suoriksi, joista puuttuu itse piste $(0, -1)$. Jos $a' \neq 0$ ja $b' = 0$, eli suora kulkee origon kautta, niin se kuvautuu pystysuoraksi $x = \frac{1}{a'}$.

Tästä havaittiin, että poikkeustapauksia lukuun ottamatta Edwardsin käyrän summaus $P+Q$ tapahtuu hyperbelin avulla, kyseinen hyperbeli määritellään kolmen pisteen avulla P, Q ja $(0, -1)$. Katsotaan esimerkistä, miltä tuo näyttää.

Esimerkki 15. Olkoon $\mathcal{M}_{-1,1} : v^2 = u^3 - u^2 + u$ Montgomeryn käyrä kunnan $\mathbb{R}$ yli, tällöin $A = -1$ ja $B = 1$ ja

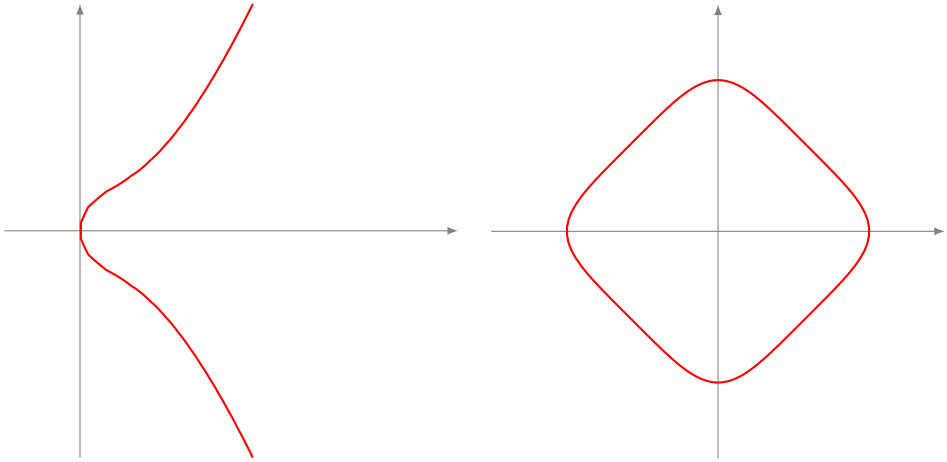
$$\begin{cases} a = (-1+2)/1 = 1 \\ d = (-1-2)/1 = -3, \end{cases}$$

eli käyrä $\mathcal{M}_{-1,1}$ on isomorfinen Edwardsin käyrän $Ed_{1,-3} : x^2 + y^2 = 1 - 3x^2y^2$ kanssa.

Valitaan pisteet Montgomeryn käyrästä $P = (1, 1)$, $Q = (2, \sqrt{6})$ ja $T = (0, 0)$, lasketaan vastaavat pisteet Edwardsin käyrällä

$$f(P) = (\frac{1}{1}, \frac{1-1}{1+1}) = (1, 0), \quad f(Q) = (\frac{2}{\sqrt{6}}, \frac{2-1}{2+1}) = (\frac{\sqrt{6}}{3}, \frac{1}{3}), \quad f(T) = (0, -1).$$

Merkitään $f(P) = P', f(Q) = Q'$ ja $f(T) = T'$ ja katsotaan miltä näiden pisteiden eräät laskutoimitukset näyttävät Edwardsin käyrällä.



(a) $\mathcal{M}_{-1,1}$ (b) $Ed_{1,-3}$

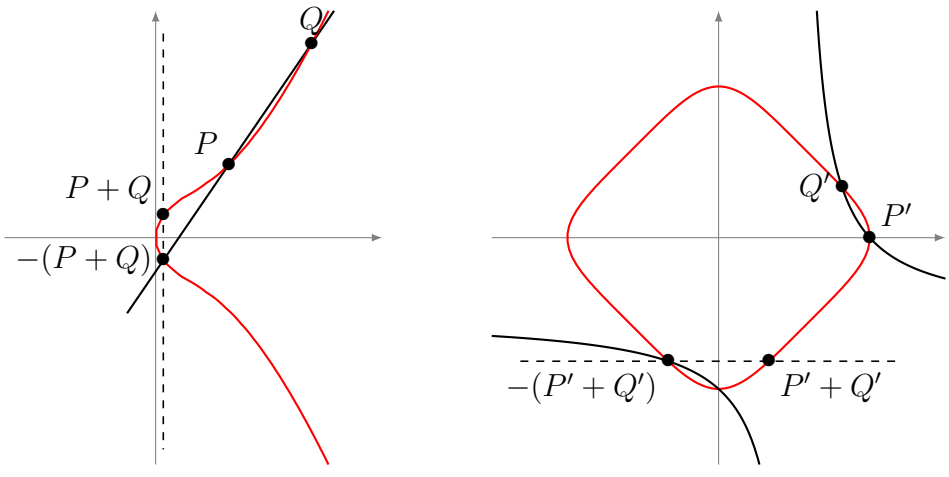
Kuva 15: Isomorfiset käyrät.

Pisteet P ja Q muodostavat suoran $y = (\sqrt{6}-1)x - \sqrt{6} + 2$, muuttujavaihdon jälkeen saadaan hyperbeli

$$\frac{1+y}{((\sqrt{6}-1)+(-\sqrt{6}+2))+((\sqrt{6}-1)-(-\sqrt{6}+2))y} = x$$

$$\Leftrightarrow \frac{1+y}{1+(2\sqrt{6}-3)y} = x.$$

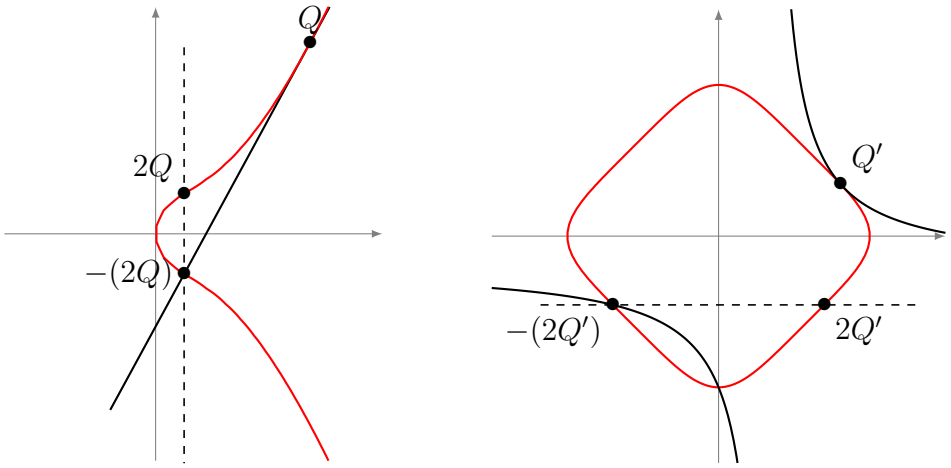
Nyt tämän hyperbelin avulla saadaan visualisoitua, miltä pisteiden summaus näyttää Edwardsin käyrällä.



(a) $P + Q$ (b) $P' + Q'$

Kuva 16: Summaus Montgomeryn- ja Edwardsin käyrällä.

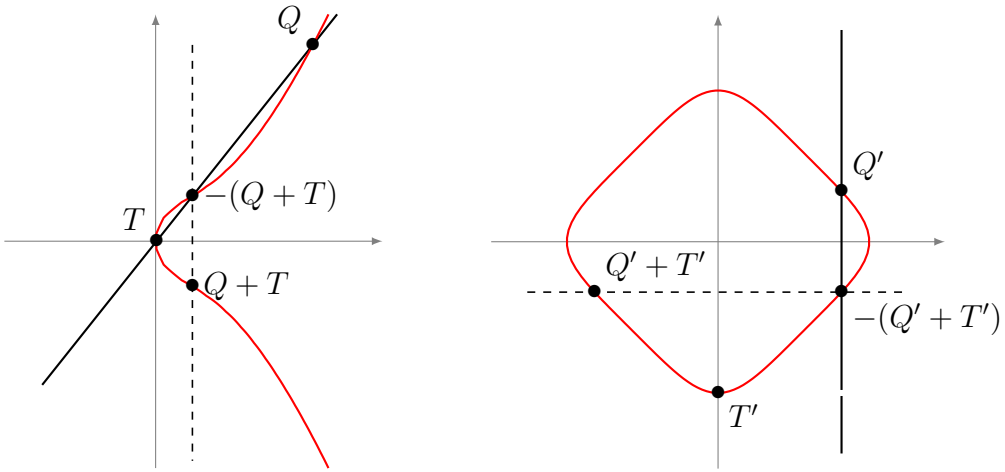
Vastaavasti pisteen tuplauksessa tangenttisuora kuvautuu hyperbeliksi, joka sivuaa Edwardsin käyrää pisteessä Q'.



(a) $2Q$ (b) $2Q'$

Kuva 17: Tuplaus Montgomeryn- ja Edwardsin käyrällä.

Katsotaan seuraavaksi miltä näyttää pisteiden yhteenlasku Edwardsin käyrällä, kun toinen pisteistä on toisen kertaluvun piste.



(a) $Q+T$ (b) $Q'+T'$

Kuva 18: Yhteenlasku Montgomeryn- ja Edwardsin käyrällä, kun toinen pisteistä on toisen kertaluvun piste.

Tätä poikkeustapausta voidaan myös ajatella nopeasti asymptootteja lähestyvien hyperbelien raja-arvona, tällöin tapauksessa $Q'+T'$ summauskäyrä on

$$x = \frac{\sqrt{6}}{3} \vee y = -1$$

ja pisteiden summaa saadaan leikkauspisteistä.

3.3.1 Kierretyn Edwardsin käyrän poikkeuspisteet

Esimerkissä 15 tutkittiin Edwardsin käyrää, jossa kerroin a on neliö ja d ei ole neliö. Tällaisilla käyrillä ei ole poikkeuspisteitä, ja määritelmän 14 laskukaavoja voidaan

käyttää kaikille laskutoimituksille. Esitetään väite lauseena ja todistetaan.

Lause 9. *Olkoon $Ed_{a,d}(\mathbb{F}) : ax^2+y^2 = 1+dx^2y^2$ kierretty Edwardsin käyrä, käyrällä ei ole poikkeuspisteitä jos ja vain jos a on neliö ja d ei ole neliö.*

Todistus. Lauseen 8 mukaan, käyrällä $Ed_{a,d}$ on birationaalisesti ekvivalentti Montgomeryn käyrä $\mathcal{M}_{A,B}$, missä $a = \frac{A+2}{B}$ ja $d = \frac{A-2}{B}$.

Jos a on neliö, ja d ei ole neliö, niin

$$\frac{A+2}{B} \cdot \frac{A-2}{B} = \frac{A^2-4}{B^2}$$

ei ole neliö, ja koska B^{-2} on neliö, A^2-4 ei ole neliö. Tämä tarkoittaa, että käyrällä on vain yksi toisen kertaluvun piste. Koska $\frac{A+2}{B}$ on neliö ja $\frac{A-2}{B}$ ei ole neliö, ainoat Montgomeryn käyrän neljännen kertaluvun pisteet ovat $(1, \pm\sqrt{\frac{A+2}{B}})$. Näin mikään käyrän $\mathcal{M}_{A,B}$ piste ei kuvaudu poikkeuspisteeksi.

Jos $d = \frac{A-2}{B}$ on neliö, niin piste $(-1, \pm\sqrt{\frac{A-2}{B}})$ on käyrällä $\mathcal{M}_{A,B}$ ja se kuvautuu poikkeuspisteeksi.
Jos $a = \frac{A+2}{B}$ ei ole neliö, niin käyrällä on joko toisen kertaluvun piste $(x', 0)$, $x' \neq 0$, kun d ei ole neliö. Tai $(-1, \pm\sqrt{\frac{A-2}{B}})$, kun d on neliö. Molemmat näistä pisteistä kuvautuvat poikkeuspisteisiin Edwardsin käyrällä. □

Seuraus 4. *Edellisen lauseen todistuksesta seuraa, että äärelliset neljännen kertaluvun pisteet Edwardsin käyrällä ovat aina x-askelilla, tarkemmin:*

$$f((1, \pm\sqrt{\frac{A+2}{B}})) = (\pm\sqrt{a^{-1}}, 0) \in Ed_{a,d}.$$

Nämä ovat myöskin ainoat Edwardsin käyrän pisteet x-akselilla, koska jos $y = 0$, silloin yhtälö on

$$ax^2 + 0^2 = 1 + dx^2 0^2 \Leftrightarrow x = \pm\sqrt{a^{-1}}.$$

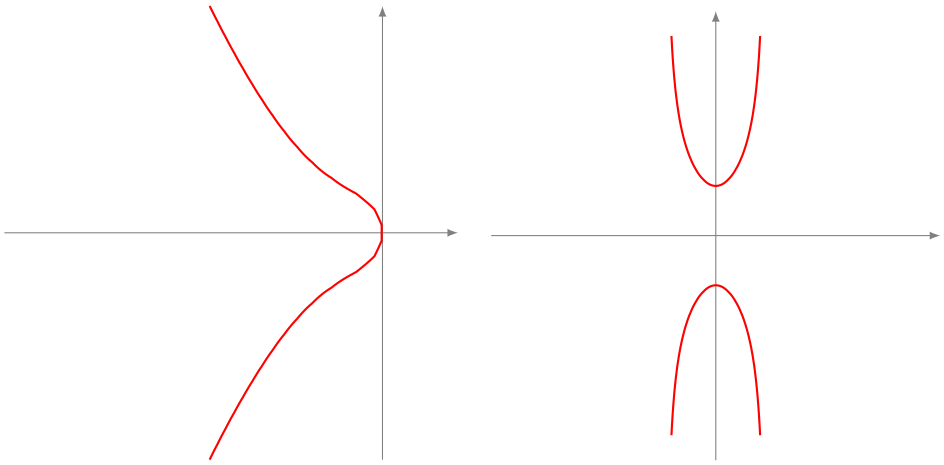
Katsotaan seuraavaksi, mitä sitten tapahtuu, kun sellaisia pisteitä on käyrällä.

Esimerkki 16. Tehdään aikaisemmin esitetylle Montgomeryn käyrälle $\mathcal{M}_{-1,1}$ muuttujan vaihto $(x, y) \mapsto (-x, y)$, saadaan käyrä

$$\mathcal{M}_{1,-1} : -y^2 = x^3 + x^2 + x,$$

tämä käyrä vastaa Edwardsin käyrää

$$Ed_{-3,1} : -3x^2 + y^2 = 1 + x^2y^2,$$



(a) $\mathcal{M}_{1,-1}$ (b) $Ed_{-3,1}$

Kuva 19: Isomorfiset käyrät.

Kuvasta 19 nähdään, ettei Edwardsin käyrä leikkaa x-akselia (seuraus 4), mikä tarkoittaa, että Montgomeryn käyrän neljännen kertaluvun pisteet $(-1, \pm 1)$ kuvautuvat Edwardsin käyrän poikkeuspisteisiin $(\mp 1, \infty)$. Erityisesti meitä kiinnostaa, miltä näyttää yhteenlasku, kun toinen pisteistä on poikkeuspiste. Valitaan Montgomeryn käyrästä pisteet $Q = (-2, \sqrt{6})$ ja $T = (-1, 1)$, nämä pisteet muodostavat suoran

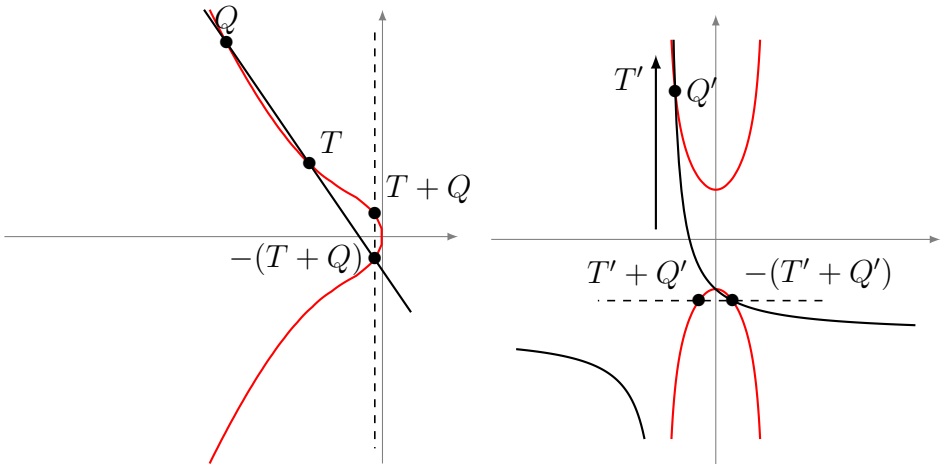
$$y = (-\sqrt{6} + 1)x - \sqrt{6} + 2.$$

Montgomeryn laskukaavoja käyttäen saadaan

$$R = (T + Q) = (2\sqrt{6} - 5, 15 - 6\sqrt{6}).$$

Pisteet Q ja R kuvautuvat pisteisiin $Q' = (-\frac{\sqrt{6}}{3}, -3)$, $R' = (-\frac{1}{3}, \frac{1}{5} - \frac{3\sqrt{6}}{10})$, suora kuvautuu hyperbeliksi

$$\frac{1 + y}{-2\sqrt{6} + 3 - y} = x.$$



(a) $T + Q$ (b) $T' + Q'$

Kuva 20: Yhteenlasku Montgomeryn käyrällä ja Edwardsin käyrällä, kun toinen pisteistä on poikkeuspiste.

Tässä voidaan ajatella, että hyperbelin ja kierretyn Edwardsin käyrän kolmas leikkauspiste T' sijaitsee äärettömyyspisteessä $(-1, -\infty)$, joka tässä tapauksessa on sama alkio kuin $(-1, \infty)$.

Katsotaan vielä miltä poikkeuspisteen näyttävät äärellisessä kunnassa.

Esimerkki 17. Olkoon $\mathcal{M}_{1,1}(\mathbb{Z}_5) : v^2 = u^3 + u^2 + u$, lauseen 8 mukaan se vastaa käyrää

$$Ed_{3,4}(\mathbb{Z}_5) : 3x^2 + y^2 = 1 + 4x^2y^2.$$

Kirjataan ensin kaikki Montgomeryn käyrän pisteet

u	$u^3 + u^2 + u$	v	v^2
0	0	0	0
1	3	1	1
2	4	2	4
3	4	3	4
4	4	4	1

Tästä saadaan käyrän pisteet:

$$\mathcal{O}, (0,0), (2,2), (3,2), (4,2), (2,3), (3,3), (4,3).$$

Tehdään muuttujanvaihdot:

(u,v)	$(x,y)=(\frac{u}{v},\frac{u-1}{u+1})$	apu
$\mathcal{O}$	$(0,1)$	
$(0,0)$	$(0,4)$	$(0,-1)$
$(2,2)$	$(1,2)$	(1,1/3)
$(3,2)$	$(4,3)$	(3/2,2/4)
$(4,2)$	P_4	(2,3/0)
$(2,3)$	$(4,2)$	-(1,2)
$(3,3)$	$(1,3)$	-(4,3)
$(4,3)$	$-P_4$	(3,3/0)

Taulukko 5: Muuttujanvaihto.

$+$	$\mathcal{O}$	$(0,0)$	$(2,2)$	$(3,2)$	$(4,2)$	$(2,3)$	$(3,3)$	$(4,3)$
$\mathcal{O}$	$\mathcal{O}$	$(0,0)$	$(2,2)$	$(3,2)$	$(4,2)$	$(2,3)$	$(3,3)$	$(4,3)$
$(0,0)$	$(0,0)$	$\mathcal{O}$	$(3,2)$	$(2,2)$	$(4,3)$	$(3,3)$	$(2,3)$	$(4,2)$
$(2,2)$	$(2,2)$	$(3,2)$	$(4,2)$	$(4,3)$	$(3,3)$	$\mathcal{O}$	$(0,0)$	$(2,3)$
$(3,2)$	$(3,2)$	$(2,2)$	$(4,3)$	$(4,2)$	$(2,3)$	$(0,0)$	$\mathcal{O}$	$(3,3)$
$(4,2)$	$(4,2)$	$(4,3)$	$(3,3)$	$(2,3)$	$(0,0)$	$(2,2)$	$(3,2)$	$\mathcal{O}$
$(2,3)$	$(2,3)$	$(3,3)$	$\mathcal{O}$	$(0,0)$	$(2,2)$	$(4,3)$	$(4,2)$	$(3,2)$
$(3,3)$	$(3,3)$	$(2,3)$	$(0,0)$	$\mathcal{O}$	$(3,2)$	$(4,2)$	$(4,3)$	$(2,2)$
$(4,3)$	$(4,3)$	$(4,2)$	$(2,3)$	$(3,3)$	$\mathcal{O}$	$(3,2)$	$(2,2)$	$(0,0)$

Taulukko 6: Montgomeryn käyrän $\mathcal{M}_{1,1}$ ryhmätaulu.

$+$	$(0,1)$	$(0,4)$	$(1,2)$	$(4,3)$	P_4	$(4,2)$	$(1,3)$	$-P_4$
$(0,1)$	$(0,1)$	$(0,4)$	$(1,2)$	$(4,3)$	P_4	$(4,2)$	$(1,3)$	$-P_4$
$(0,4)$	$(0,4)$	$(0,1)$	$(4,3)$	$(1,2)$	$-P_4$	$(1,3)$	$(4,2)$	P_4
$(1,2)$	$(1,2)$	$(4,3)$	P_4	$-P_4$	$(1,3)$	$(0,1)$	$(0,4)$	$(4,2)$
$(4,3)$	$(4,3)$	$(1,2)$	$-P_4$	P_4	$(4,2)$	$(0,4)$	$(0,1)$	$(1,3)$
P_4	P_4	$-P_4$	$(1,3)$	$(4,2)$	$(0,4)$	$(1,2)$	$(4,3)$	$(0,1)$
$(4,2)$	$(4,2)$	$(1,3)$	$(0,1)$	$(0,4)$	$(1,2)$	$-P_4$	P_4	$(4,3)$
$(1,3)$	$(1,3)$	$(4,2)$	$(0,4)$	$(0,1)$	$(4,3)$	P_4	$-P_4$	$(1,2)$
$-P_4$	$-P_4$	P_4	$(4,2)$	$(1,3)$	$(0,1)$	$(4,3)$	$(1,2)$	$(0,4)$

Taulukko 7: Edwardsin käyrän $Ed_{3,4}$ ryhmätaulu.

Yritetään summata $Ed_{3,4}$ käyrän pisteet $(1,2)$ ja $(4,3)$ määritelmän 14 laskukaavojen avulla

$$x_3 = \frac{1\cdot 3 + 2\cdot 4}{1 + 4\cdot 1\cdot 2\cdot 3\cdot 4} = \frac{3+8}{1+96} = \frac{1}{2} = 3,$$

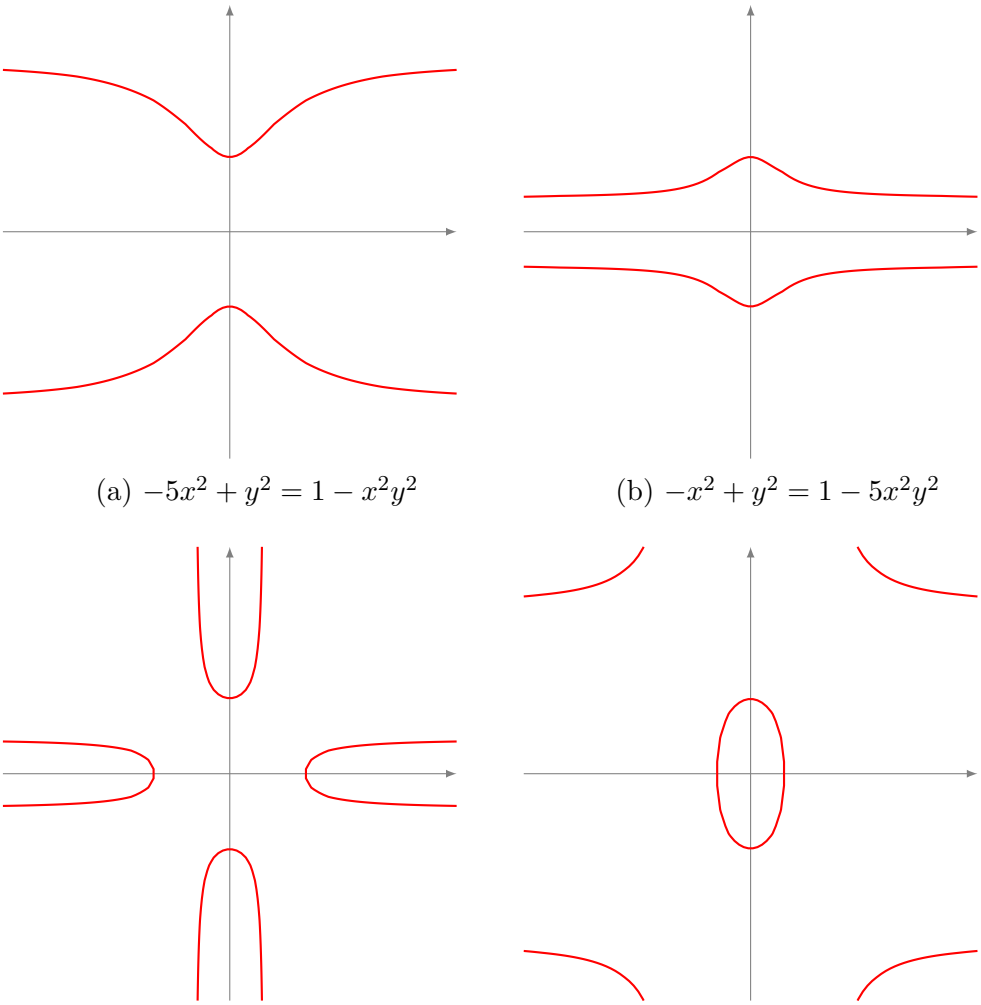
$$y_3 = \frac{2\cdot 3 - 3\cdot 1\cdot 4}{1 - 4\cdot 1\cdot 2\cdot 3\cdot 4} = \frac{6-12}{1-96} = \frac{4}{0}.$$

Tässä jouduttiin jakamaan nollalla, mikä ei ole sallittua, ryhmätaulusta 7 nähdään kuitenkin, että $(1,2)+(4,3) = -P_4$, eli toinen neljännen kertaluvun poikkeuspisteistä.

Huomautus 7. Edellä mainittu Montgomeryn käyrä $\mathcal{M}_{1,1}$ on birationaalisesti ekvivalentti käyrän $\mathcal{M}_{4,4}$, jonka Edwardsin käyrän esitys ei sisällä poikkeuspisteitä.

Edellisissä esimerkeissä todettiin, että eräillä käyrillä voi olla esityksiä, joissa ei ole poikkeuspisteitä ja joissa on poikkeuspisteitä. Tutkitaan seuraavaksi, millaisilla kierretyillä Edwardsin käyrillä ei ole poikkeuspisteitä.

Eräs edellisen lauseen seuraus



(a) $-5x^2 + y^2 = 1 - x^2y^2$ (b) $-x^2 + y^2 = 1 - 5x^2y^2$

(c) $x^2 + y^2 = 1 + 5x^2y^2$ (d) $5x^2 + y^2 = 1 + x^2y^2$

Kuva 21: Edwardsin käyrät kunnan $\mathbb{R}$ yli.

Kuvien 21a ja 21b käyrillä on kaksi toisen kertaluvun ja kaikki neljä neljännen kertaluvun poikkeuspistettä ovat poikkeuspisteitä. Kuvien 21c ja 21d käyrillä on kaksi toisen kertaluvun, kaksi neljännen kertaluvun pistettä ja kaksi neljännen kertaluvun pistettä ovat rationaalisia. Katsotaan seuraavaksi esimerkin äärellisessä kunnassa.

Esimerkki 18. Valitaan Montgomeryn käyrä $\mathcal{M}_{1,1}(\mathbb{Z}_7) : y^2 = x^3 + x^2 + x$, listataan alkiot ja muodostetaan ryhmätaulun

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

$+$	$\mathcal{O}$	$(0,0)$	$(2,0)$	$(4,0)$	$(5,1)$	$(3,2)$	$(3,5)$	$(5,6)$
$\mathcal{O}$	$\mathcal{O}$	$(0,0)$	$(2,0)$	$(4,0)$	$(5,1)$	$(3,2)$	$(3,5)$	$(5,6)$
$(0,0)$	$(0,0)$	$\mathcal{O}$	$(4,0)$	$(2,0)$	$(3,5)$	$(5,6)$	$(5,1)$	$(3,2)$
$(2,0)$	$(2,0)$	$(4,0)$	$\mathcal{O}$	$(0,0)$	$(3,2)$	$(5,1)$	$(5,6)$	$(3,5)$
$(4,0)$	$(4,0)$	$(2,0)$	$(0,0)$	$\mathcal{O}$	$(5,6)$	$(3,5)$	$(3,2)$	$(5,1)$
$(5,1)$	$(5,1)$	$(3,5)$	$(3,2)$	$(5,6)$	$(4,0)$	$(0,0)$	$(2,0)$	$\mathcal{O}$
$(3,2)$	$(3,2)$	$(5,6)$	$(5,1)$	$(3,5)$	$(0,0)$	$(4,0)$	$\mathcal{O}$	$(2,0)$
$(3,5)$	$(3,5)$	$(5,1)$	$(5,6)$	$(3,2)$	$(2,0)$	$\mathcal{O}$	$(4,0)$	$(0,0)$
$(5,6)$	$(5,6)$	$(3,2)$	$(3,5)$	$(5,1)$	$\mathcal{O}$	$(2,0)$	$(0,0)$	$(4,0)$

Taulukko 8: Montgomeryn käyrän $\mathcal{M}_{1,1}$ ryhmätaulu.

Taulusta nähdään, että neljännen kertaluvun alkiot ovat $(5,1), (3,2), (3,5)$ ja $(5,6)$ ja ne tuplaantuvat alkioon $(4,0)$. Tehdään muuttujanvaihdot lauseen 8 mukaan, saadaan

(u,v)	$(x,y) = (\frac{u}{v}, \frac{u-1}{u+1})$	apu
$\mathcal{O}$	$(0,1)$	
$(0,0)$	$(0,6)$	$(0,-1)$
$(2,0)$	P_2	
$(4,0)$	P_2'	
$(5,1)$	$(5,3)$	(5,4/6)
$(3,2)$	$(5,4)$	(3/2,2/4)
$(3,5)$	$(2,4)$	-(5,4)
$(5,6)$	$(2,3)$	-(5,3)

Taulukko 9: Muuttujanvaihto.

ja Edwardsin käyrän

$$Ed_{3,6}(\mathbb{Z}_7) : 3x^2 + y^2 = 1 + 6x^2y^2.$$

$+$	$(0,1)$	$(0,6)$	P_2	P_2'	$(5,3)$	$(5,4)$	$(2,4)$	$(2,3)$
$(0,1)$	$(0,1)$	$(0,6)$	P_2	P_2'	$(5,3)$	$(5,4)$	$(2,4)$	$(2,3)$
$(0,6)$	$(0,6)$	$(0,1)$	P_2'	P_2	$(2,4)$	$(2,3)$	$(5,3)$	$(5,4)$
P_2	P_2	P_2'	$(0,1)$	$(0,6)$	$(5,4)$	$(5,3)$	$(2,3)$	$(2,4)$
P_2'	P_2'	P_2	$(0,6)$	$(0,1)$	$(2,3)$	$(2,4)$	$(5,4)$	$(5,3)$
$(5,3)$	$(5,3)$	$(2,4)$	$(5,4)$	$(2,3)$	P_2'	$(0,6)$	P_2	$(0,1)$
$(5,4)$	$(5,4)$	$(2,3)$	$(5,3)$	$(2,4)$	$(0,6)$	P_2'	$(0,1)$	P_2
$(2,4)$	$(2,4)$	$(5,3)$	$(2,3)$	$(5,4)$	P_2	$(0,1)$	P_2'	$(0,6)$
$(2,3)$	$(2,3)$	$(5,4)$	$(2,4)$	$(5,3)$	$(0,1)$	P_2	$(0,6)$	P_2'

Taulukko 10: Edwardsin käyrän $Ed_{3,6}$ ryhmätaulu.

4 Elliptisen käyrän kryptografia

Kryptografian keskeinen tarkoitus on mahdollistaa suojatun vuorovaikutuksen suojaamattoman kanavan yli. Matemaattisesti kaikki kryptografia perustuu johonkin laskennalliseen ongelmaan, jonka ratkaisu voidaan tarkistaa *tehokkaasti*, eli polynomisessa ajassa. Keskeinen laskentaongelma EC-kryptosysteemissä on elliptisen käyrän pisteen monikerta

$$sP = Q.$$

Jos s tiedetään, niin sP voidaan laskea tehokkaasti ynnäys- ja tuplausalgoritmilla.

Algoritmi 1 Ynnäys- ja tuplausalgoritmi

Olkoon $P \in E(\mathbb{F})$ ja $s \geq 1$, merkitään $Q = e$ siis käyrän neutraalialkio.
1. Jos s ei ole kahdella jaollinen, niin laske ja merkitse $Q = P + Q$.
2. Laske ja merkitse $P = 2P$.
3. Merkitse $s = \lfloor s/2 \rfloor$.
4. Jos $s > 0$, hyppää askeleeseen 1.
5. Palauta Q.

Koska kerroin s jaetaan joka kerta kahdella, algoritmia ajetaan enintään $\log_2(N)$ kierrosta, missä N on pisteen P kertaluku. Kryptografiassa avainkoot ja pisteiden kertalukujen suuruudet ilmaistaan bitteinä ja ajokertoja tulee olla enintään logaritmisessa suuruusluokassa. Eli ynnäys- ja tuplausalgoritmi on tehokas.

Oletetaan seuraavaksi, että tiedetään P ja Q, ja että $sP = Q$, mutta itse s ei tiedetä. Eräs tapa yrittää ratkaista tuo ongelma on summata $P+P+...+P$, kunnes saadaan aikaan Q. Tämä veisi s askelta, mikä bittien suuruusluokassa tarkoittaisi N askelta, eli algoritmi ei ole tehokas. Kyseessä on elliptisen käyrän logaritmin ongelma ja sen ratkaisuun ei tunneta tehokasta ratkaisualgoritmia. Tunnetaan kuitenkin tehokkaammat $\sqrt{N}$ -luokan algoritmit, kuten Baby step, Giant step, sekä Pollardin ρ- ja λ-algoritmit. Näihin voi tutustua teoksessa [3]. Elliptisen logaritmin ongelmaan liittyy myös Diffie-Hellman ongelma, missä tunnetaan aP ja bP, ja yritetään laskea abP. Tähänkään ongelmaan ei löydy tehokasta ratkaisualgoritmia klassisilla menetelmillä. Katsotaan seuraavaksi, miltä näyttää elliptisen käyrän kryptosysteemit.

4.1 Diffie-Hellman avaintenvaihto

Eräs suhteellisen yksinkertainen, mutta erittäin käytännöllinen elliptisen käyrän sovellus on Diffie-Hellman-avaintenvaihto EC-kryptosysteemissä. Sillä ei ole tarkoitus vaihtaa varsinaista tietoa, vaan jakaa yhteinen *siemen*, minkä avulla molemmat osapuolet voivat luoda saman avaimen symmetristä kryptosysteemiä varten. Seuraava algoritmi on kuvattu lähteessä [3].

Salakuuntelija Eve tietää elliptisen käyrän $E(\mathbb{F})$, ja pisteet P, aP ja bP. Ratkaistaakseen abP, hänen pitää joko ratkaista elliptisen käyrän diskreetin logaritmin

Algoritmi 2 Diffie-Hellman avaintenvaihto

1. Alice ja Bob sopivat julkisesti, mitä elliptistä käyrää E yli kunnan $\mathbb{F}$ he käyttävät. He myös valitsevat pisteen $P \in E(\mathbb{F})$, niin että sen kertaluku on suuri, yleensä halutaan, että se on alkuluku.

2. Alice valitsee satunnaisesti kokonaisluvun a ja laskee pisteen $P_a = aP$ ja lähettää P_a Bobille.

3. Bob valitsee satunnaisesti kokonaisluvun b satunnaisesti ja laskee pisteen $P_b = bP$ ja lähettää sen Alicelle.

4. Alice laskee $aP_b = abP$.

5. Bob laskee $bP_a = baP$.

6. Alice ja Bob käyttävät alkion $baP = abP \in E(P)$ generoidakseen avaimen julkisesti sovitulla menetelmällä.

ongelma tai elliptisen käyrän Diffie-Hellman ongelma. Tässä voidaan myös huomata, ettei Alicen eikä Bobin tarvitse luoda ja pitää yllä omia elliptisen käyrän avaimia, vaan sessioavaimet a ja b arvotaan prosessin aikana.

Tämä algoritmi on kuitenkin haavoittuvainen väliintulohyökkäykselle. Jos Eve onnistuu tunkeutumaan Alicen ja Bobin kommunikaation väliin, hän voi välittäjänä lukea, muuttaa ja väärentää yksityisiä viestejä. Näin se toimii:

Algoritmi 3 Even väliintulo

1. Eve onnistuu tunkeutumaan Alice ja Bobin kommunikaation väliin, hän esittää Bobia Alicelle ja Alicea Bobille.

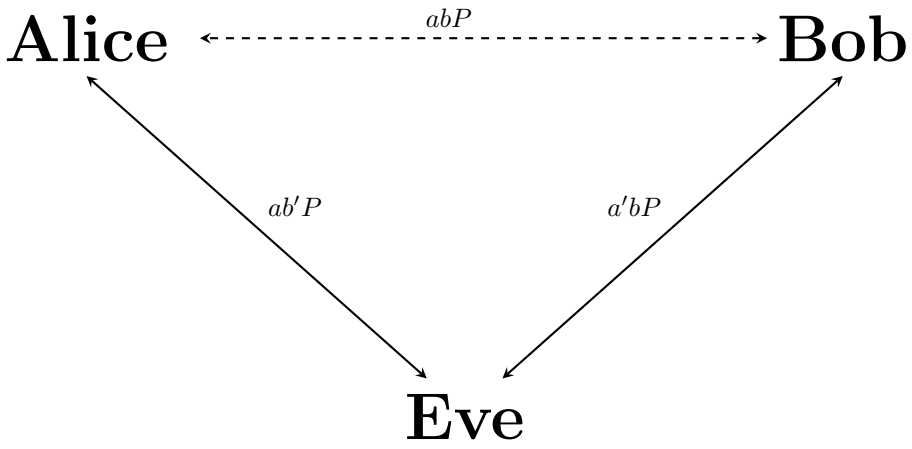
2. Alice ja Bob seuraavat EC Dilfie-Hellman avaintenvaihtoalgoritmia.

3. Eve kaappaa viestit aP ja bP ja ottaa itselleen talteen, niiden tilalle hän valitse satunnaisesti luvut a' ja b', lähettäen sen jälkeen pisteen $a'P$ Bobille ja pisteen $b'P$ Alicelle.

4. Alice ja Eve muodostavat yhteisen avaimen $ab'P$ avulla.

5. Bob ja Eve muodostavat yhteisen avaimen $a'bP$ avulla.

Tämä väliintulo-ongelma on erityisen hankala, jos Alice ja Bob eivät tunne toisiaan ja he kommunikoivat internetin kautta, missä tieto kulkee monien palvelimien läpi. Tämän algoritmin avulla Alice ja Bob eivät voi olla varmoja, että he kommunikoivat suoraan. Eräs tapa varmistua, että kommunikaatio tapahtuu juuri kyseisen tahon kanssa, on sähköinen allekirjoitus. Katsotaan seuraavaksi, miten se toimii.



Kuva 22: Even väliintulo, katkoviiva kuvaa miten Alice ja Bob näkevät kommunikaation ja mitkä siemenet he loivat.

4.2 Sähköinen allekirjoitus

Sähköinen allekirjoitus on tarkoitukseltaan hyvin samanlainen kuin normaali käsin tehty allekirjoitus eli lyhyesti sanottuna sitä ei voida väärentää ja allekirjoittaja ei voi kiistää allekirjoitustaan. Tarkemmin ilmaistuna sähköisen allekirjoituksen pitää täyttää seuraavat ehdot [4]:

1. **Luotettavuus**: allekirjoitus on sidottu käyttäjään ja kukaan muu ei voi luoda niitä;

2. **Kiistämättömyys**: allekirjoittaja ei voi kiistää allekirjoituksensa;

3. **Aitous**: allekirjoitus on sidottu allekirjoitettuun viestiin, ulkopuolinen ei voi kopioida sitä toiseen viestiin.

Käytännössä kryptografisessa allekirjoituksessa allekirjoittaja salaa viestin tunnisteen yksityisellä avaimella ja tarkistaja purkaa salauksen yleisen avaimen avulla ja tarkistaa, että tunnisteet täsmäävät. Tunnisteet useimmiten luodaan *hajautusfunktion* avulla. Hajautusfunktio ottaa mielivaltaisen pitkän viestin ja palauttaa vakiopituisen bittijonon, tunnisteen. Oletuksena on, ettei tunnisteesta voi laskea lähdeviestiä, ei osata luoda lähdeviestiä, jolla on haluttu tunniste, ja yhteentörmäykset ovat harvinaisia. Yhteen törmäyksellä tarkoitetaan, että kahdella viestillä on sama tunniste. Tarkemmin hajautusfunktioihin voi tutustua Fergusonin, Schneierin ja Kohnon teoksessa [6]. Seuraava algoritmi on esitetty teoksissa [3, 5].

Elliptisen käyrän digitaalinen allekirjoitus ECDCA: Bob on julkaissut avaimen $(\mathbb{F}, E, N, P, Q, H)$, jossa $\mathbb{F}$ on äärellinen kunta, E on elliptinen käyrä, P, Q ovat pisteet käyrällä $E(\mathbb{F})$ ja $Q = kP$, missä k on salainen avain. Piste P valitaan niin, että sen kertaluku N on suuri alkuluku ja H on hajautusfunktio. Nyt Bob haluaa allekirjoittaa viestin m joka tapahtuu algoritmin 4 mukaisesti.

Algoritmi 4 Viestin allekirjoitus

1. Bob valitsee satunnaisen kokonaisluvun $a \in [1, N-1]$ ja laskee $R = aP = (x, y)$.

2. Bob käyttää ennalta sovitun hajautusfunktion H ja laskee $H(m)$.

3. Bob laskee $s = a^{-1}(H(m) + kx) \pmod N$.

4. Bob lähettää allekirjoitetun viestin(m, R, s).

Algoritmi 5 Allekirjoituksen vahvistus

1. Alice lataa Bobin julkisen avaimen ja vastaanottaa viestin (m, R, s).

2. Alice ottaa talteen x, $R = (x, y)$.

3. Alice laskee $u_1 = s^{-1}H(m) \pmod N$ ja $u_2 = s^{-1}x \pmod N$.

4. Alice laskee $V = u_1P + u_2Q$.

5. Alice vahvistaa viestin, jos $V = R$.

Oletetaan Alicen saavan kolmikon (m, R, s), algoritmin 5 avulla hän laski arvon V. Seurataan nyt algoritmeja taaksepäin

$$V = u_1P + u_2Q = s^{-1}H(m)P + s^{-1}xQ = s^{-1}(H(m)P + xQ),$$

koska $Q = kP$, tästä saadaan

$$= s^{-1}(H(m)P + xkP) = s^{-1}(H(m) + xk)P,$$

koska $s = a^{-1}(H(m) + kx) \pmod N$ ja ja pisteen P virittämän elliptisen käyrän aliryhmän kertaluku on N

$$= (a^{-1}(H(m) + kx))^{-1}(H(m) + xk)P$$

$$= a(H(m) + kx)^{-1}(H(m) + xk)P = aP = R = V.$$

Siis allekirjoitus vahvistuu jos ja vain jos allekirjoittaja tietää Bobin yksityisen avaimen k. Tärkeä oletus on, että $a^{-1} \pmod N$ ja $s^{-1} \pmod N$ ovat olemassa, tämä on aina totta, jos N on alkuluku ja $s \neq 0$. Jos kuitenkin $s = 0$, niin

$$(H(m) + kx) = 0 \mod N,$$

silloin Bobin pitää valita arvo a uudestaan.

Jos Alice saa väärän viestin $m' \neq m$, niin $H(m') \neq H(m)$, koska oletetaan, että hajautusfunktion yhteentörmäykset ovat harvinaisia ja niiden tahallinen luonti on vaikeaa. Nyt saadaan

$$(H(m) + kx)^{-1}(H(m') + xk) = h \neq 1 \pmod N,$$

eli

$$V = ahP \neq aP = R.$$

Näin olleen väärän viestin allekirjoitus ei vahvistu. Myöskin askel

$$s^{-1}(H(m)P + xQ) = s^{-1}(H(m)P + xkP)$$

voidaan tehdä vain, jos viestin allekirjoittaja tietää Bobin salaisen avaimen k, eli allekirjoituksen väärentäminen on vaikeaa. Näin ECDCA täyttää kiistämättömyys- ja aitous-ehtoja, luotettavuus riippuu yleisen avaimen julkaisijan luotettavuudesta. Julkisten avaimien infrastruktuuriin ja julkaisijan luotettavuuteen voi tutustua lähteessä [6].

Sähköisen allekirjoituksen avulla voidaan myös estää Even väliintulohyökkäyksen avaintenvaihdossa (algoritmi 3). Alice ja Bob sopivat, että Bob allekirjoittaa viestin P_b, koska Eve ei kykene luomaan Bobin allekirjoitusta viestille $P_{b'}$, hän ei pysty uskottamaan Alicelle, että hän on Bob. Tällainen protokolla toimii esimerkiksi, kun Bob on palvelin ja Alice asiakkaan käyttämä selain. Bobin pitää taas varmistaa Alicen henkilöllisyys toisella tavalla. Jos Bob on palvelin, hän voi esimerkiksi kysyä käyttäjätunnuksen ja salasanan sen jälkeen, kun suojattu yhteys on luotu avaintenvaihdon avulla.

4.3 ECIES -salaus ja -purku

Yleisen avaimen kryptografian avulla voidaan myös luoda kryptosysteemi, missä yleinen avain käytetään viestin salaukseen ja salauksen voi purkaa vain yksityisen avaimen haltija. Elliptisen käyrän kryptografiassa eräs tällainen kryptosysteemi on Bellare'n ja Rogawayn ehdottama ECIES(The Elliptic Curve Integrated Encryption Scheme). Tämä osuus perustuu lähteisiin [3, 5]. ECIES-protokolla: Bob on julkaissut

avaimen $(\mathbb{F}, E, N, P, Q)$, jossa $\mathbb{F}$ on äärellinen kunta, E on elliptinen käyrä, P, Q ovat pisteet käyrällä $E(\mathbb{F})$ ja $Q = kP$, missä k on salainen avain. Piste P valitaan niin, että sen kertaluku N on suuri alkuluku. Erikseen on myös määritelty hajautusfunktiot H_1, H_2, sekä symmetrinen kryptosysteemi S, johon liittyy E_r ja D_r ovat salaus- ja salauksen purkualgoritmit avaimella r. Nyt Alice salaa viestin m algoritmin 6 mukaisesti.

Algoritmi 6 ECIES-salaus

1. Alice lataa Bobin julkisen avaimen.

2. Alice valitsee satunnaisen kokonaisluvun $a \in [1, N-1]$.

3. Alice laskee $R = aP$ ja $Z = aQ$.

4. Alice laskee $H_1(R, Z) = k_1||k_2$, missä $k_1||k_2$ on bittijono. Ennalta sovittu määrä biteistä arvoksi k_1 ja loput k_2.

5. Alice laskee $C = E_{k_1}(m)$ ja $t = H_2(C, k_2)$.

6. Alice lähettää salatun viestin (R, C, t) Bobille.

Algoritmi 7 ECIES-salauksen purku

1. Bob saa Alicen salatun viestin (R, C, t).

2. Bob laskee $Z = kR$. Jos Z on käyrän ryhmän neutraalialkio, viesti hylätään.

3. Bob laskee $H_1(R, Z) = k_1||k_2$.

4. Bob laskee $t' = H_2(C, k_2)$. Jos $t' \neq t$, viesti hylätään.

5. Bob purkaa viestin salauksen k_1 avaimen avulla $m = D_{k_1}(C)$.

Oletetaan Alicen lähettäneen kolmikon (R, C, t). Koska

$$Z = kR = k(aP) = a(kP) = aQ,$$

Alicella ja Bobilla on samat R ja Z ja he käyttävät samoja hajautusfunktioita H_1 ja H_2, he luovat samat avaimet k_1 ja k_2. Koska vain Bob tietää yksityisen avaimen k, vain hän osaa laskea $Z = kR$.

Myös ECIES-protokolla estää Even algoritmin 3 väliintulohyökkäykseen. Jos Alice ja Bob sopivat että Alice salaa viestinsä P_a Bobin yleisellä avaimella, Eve ei saa selville P_a ja hän ei pysty luomaan yhteistä avainta Alicen kanssa.

Viitteet

[1] Jokke Häsä, Algebra II, Helsingin Yliopisto, 2010.

[2] Daniel J. Bernstein, Tanja Lange, Faster addition and doubling on elliptic curves, Advances in Cryptology, ASIACRYPT, 2007.

[3] Lawrence C. Washington, Elliptic Curves: Number Theory and Cryptography, 2nd edition, CRC Press, 2008.

[4] Henri Cohen, Gerhard Frey, Handbook of Elliptic and Hyperelliptic Curve Cryptography, CRC Press, 2006.

[5] Darrel Hankerson, Alfred Menezes, Scott Vanstone, Gerhard Frey, Guide to Elliptic Curve Cryptography, Springer, 2004.

[6] Niels Ferguson, Bruce Schneier, Tadayoshi Kohno, Cryptography Engineering Design Principles and Practical Applications, Wiley Publishing, Inc, 2010.

[7] Recommendation for Key Management: Part 1 – General, `https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf`, luettu 21.2.2024.

[8] Harold M. Edwards, A normal form for elliptic curves, Bulletin (New Series) of the American Mathematical Society Volume 44, Number 3, July 2007.

[9] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, Christiane Peters, Twisted Edwards Curves, 2008.