Elliptiset käyrät

11. helmikuuta 2014

Huomatkaa, että tässä on skipattu ihan valtavasti kunnon teoriaa, koska kurssin aiheena on krypto, ei elliptiset käyrät!

1 Perusmääritelmät

Kunta $\mathbb{Z}_p = \{01, 2, 3, \ldots, p-1\}$. Sen *karakteristika* on p, koska $pa = 0$ kaikilla $a \in \mathbb{Z}_p$.

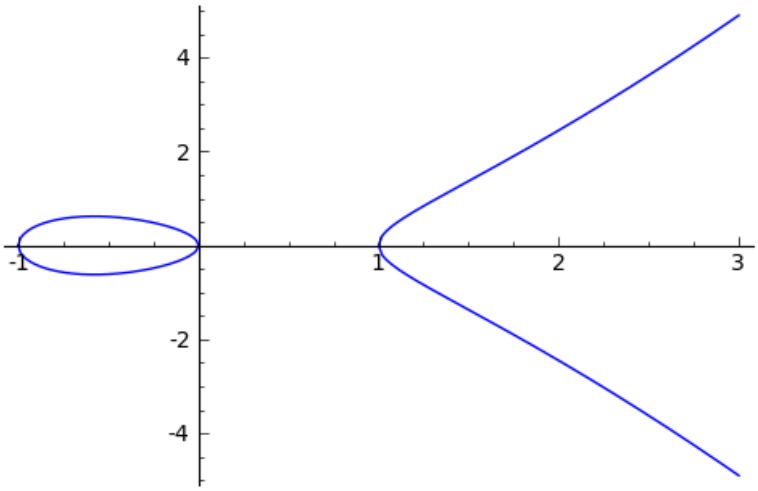
Oletetaan, että kunnan karakteristika on $p > 3$. Kutsutaan nyt elliptiseksi käyräksi käyrää, joka toteuttaa yhtälön

$$y^2 = x^3 + ax + b,$$

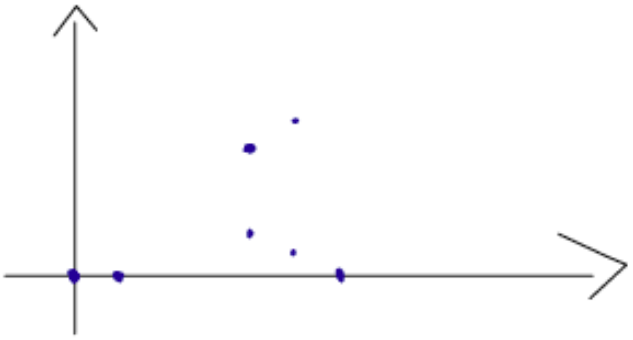
kun *diskriminantti* $-16(4a^3 + 27b^2) \neq 0$. (JOssain lähteissä diskriminantti on $4a^3 + 27b^2$.) Elliptiseen käyrään lasketaan lisäksi kuuluvan äärettömyyspisteen. Samaistetaan kaikki mahdolliset sellaiset äärettömät keskenään, joissa molemmat koordinaatit ovat itseisarvoltaan äärettömän suuria, eli esimerkiksi $(\infty, \infty) = (-\infty, \infty)$.

Itse asiassa, elliptinen käyrä on hieman yleisempi otus kuin ylläoleva, mutta kun karakteristika $p > 3$, niin yksinkertaisillä muuttujanvaihdoksilla käyrä voidaan aina saattaa ylläolevaan muotoon.

Reaalilukujen joukossa elliptinen käyrä $y^2 = x^3 - x$ näyttää tältä:



Kunnassa $\mathbb{Z}_p$ elliptinen käyrä näyttää tältä (esimerkkinä käyrä $y^2 = x^3 - x$ ja kunta $\mathbb{Z}_7$):



2 Yhteenlasku

Äärettömyyspisteeseen suhtaudutaan yhteenlaskun neutraalialkiona (eli nollana!), ja kirjoitetaan tyypillisesti $(\infty, \infty) = O$. Tämä ei ole yhtään niin sairasta kuin miltä kuulostaa. Katsotaan siis yhteenlaskun määritelmää, ja huomataan, että ääretön tosiaan toimii sympaattisesti yhteenlaskussa.

Vastaavasti voidaan vasta-alkioksi valita piste, joka on peilaus x-akselin suhteen: Jos $P = (x, y)$, niin $-P = (x, -y)$.

Yhteenlasku voidaan määritellä geometrisesti tai kaavoin.

2.1 Geometrinen määrittely yhteenlaskulle

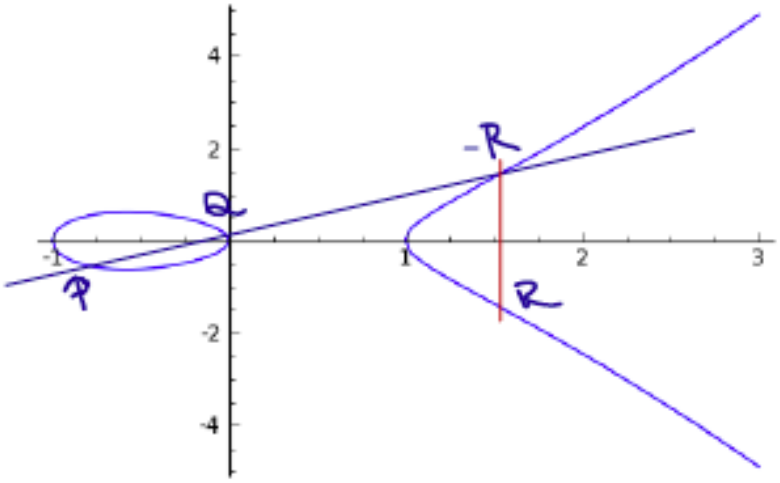
Seuraavat määritelmät voidaan tehdä äärellisissä kunnissa, mutta jotta asiat on helppo hahmottaa, eletään nyt kunnassa $\mathbb{R}$.

Kun lasketaan yhteen kaksi keskenään erisuurta pistettä, joiden x-koordinaatit ovat erisuuret, toimitaan seuraavasti

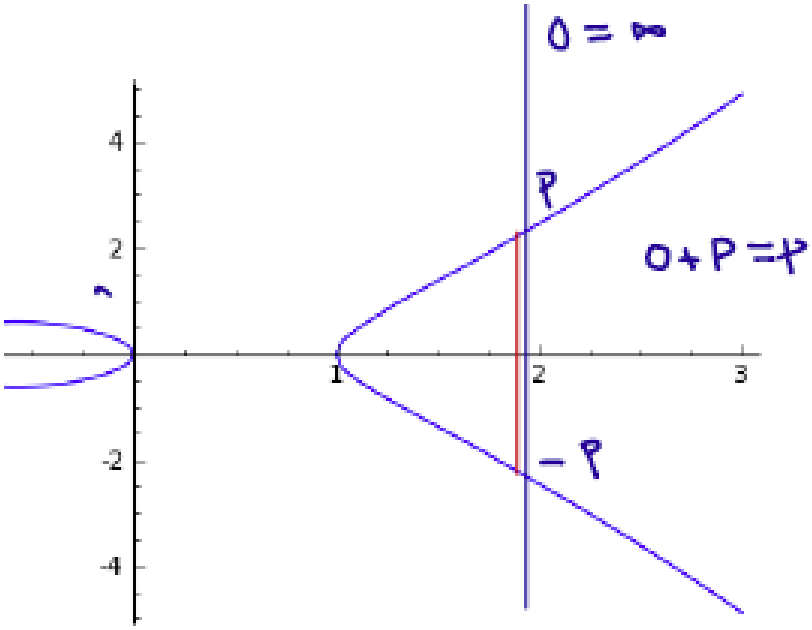
1. Piirretään suora pisteiden kautta.

2. Haetaan suoran ja elliptisen käyrän kolmas leikkauspiste

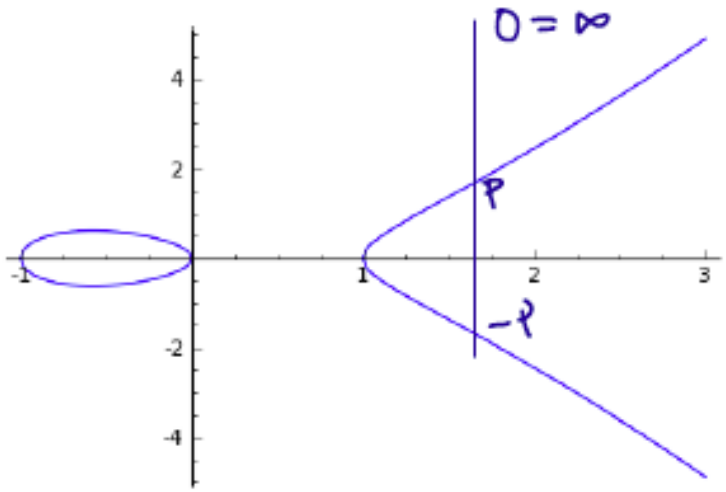
3. Peilataan se x-akselin suhteen. VALMIS!



Jos toinen pisteistä onkin äärettömyyspiste O, on ylläoleva geometrinen konstruktio ensisilmäyksellä omituinen. Se kuitenkin järkevöityy, kun ajatellaan äärettömyyspisteen olevan jossain sairaan korkealla, eli alkuperäisestä pisteestä $y-$akselin suuntaisesti ylöspäin. Tällöin suoraksi muodostuu y-akselin suuntainen suora ja yhteenlaskun tulos on alkuperäinen piste P. Kas näin:



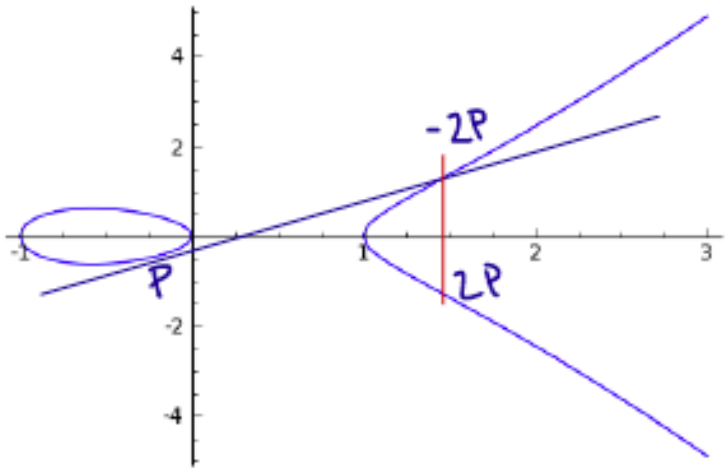
Jos taas pisteiden $x-$koordinaatit ovat yhtäsuuret, on suora y-akselin suuntainen, jolloin kolmas käyrän leikkauspiste on ääretönpiste, eli $P + (-P) = O$:



Pisteen kahdentaminen:

1. Piirretään pisteen tangentti.
2. Katsotaan missä tangentti leikkaa käyrän.
3. Peilataan x-akselin suhteen.

Operaatio näyttää siis tältä:



Ylläolevassa geometrisessa konstruktiossa oletettiin, että kolmas käyrän piste löytyy suoralta, jos kaksi pistettä on jo löytynyt (paitsi silloin, kun kyseessä on y-akselin suuntainen suora, jolloin on selvää, että pistettä ei voi löytyä, sillä kun x-koordinaatti on vakio,

on y-koordinaatilla korkeintaan kaksi vaihtoehtoa $\pm\sqrt{x^3+ax+b}$. Osoitetaan nyt ylläoleva implisiittinen väite:

Lause 1. *Kun $y = cx+d$, niin suoralla on elliptisen käyrän kanssa 1 tai 3 leikkauspistettä, kun leikkauspisteet lasketaan monikerroittain.*

Ennen kuin siirrytään todistukseen, selvennetään, mitä monikerroittain laskeminen tässä tarkoittaa. Sillä tarkoitetaan yksinkertaisesti sitä, että polynomilla $x^2-2x+1 = (x-1)^2$ on nollakohtana vain piste $x = 1$, mutta pisteessä on kaksinkertainen nollakohta. Nyt voimmekin siirtyä todistukseen.

Todistus. Tarkastelemme yhtälöryhmän

$$\begin{cases} y = cx + d \\ y^2 = x^3 + ax + b \end{cases}$$

ratkaisujen lukumäärää. Sijoitetaan eka yhtälö toiseen. Saadaan

$$(cx + d)^2 = x^3 + ax + b,$$

eli

$$x^3 - c^2x^2 + (a + 2cd)x + (b - d^2) = 0.$$

Tämä on kolmannen asteen polynomi. Sillä on vähintään yksi juuri reaalilukujen joukossa, sillä

$$\lim_{x\to-\infty} x^3 - c^2x^2 + (a + 2cd)x + (b - d^2) = -\infty$$

ja

$$\lim_{x\to\infty} x^3 - c^2x^2 + (a + 2cd)x + (b - d^2) = \infty.$$

Toisaalta, mikäli sillä on kaksi reaalista juurta, olkoot α ja β, niin funktio

$$\frac{x^3 - c^2x^2 + (a + 2cd)x + (b - d^2)}{(x - \alpha)(x - \beta)}$$

on reaalikertoiminen ensimmäisen asteen polynomi, jolla on siis selvästi reaalinen nollakohta. Todistus on valmis. □

2.2 Yhteenlasku kaavoin

Esitetään nyt ylläoleville laskutoimituksille kaavat.

Kahden erisuuren pisteen $P = (x_P, y_P)$ ja $Q = (x_Q, y_Q)$ yhteenlasku, kun $x_P \neq x_Q$:

$$P + Q = R = (x_r, y_R),$$

missä

$$\begin{cases} x_R = s^2 - x_P - x_Q \\ y_R = -y_P + s(x_P - x_R), \end{cases}$$

missä $s = \frac{y_P - y_Q}{x_P - x_Q}$. Osoitetaan nyt, että tämä tuottaa saman tuloksen kuin ylläoleva geometrinen konstruktio:

Todistus. Ylläolevassa geometrisessa konstruktiossa tuotettiin kahden pisteen $P = (x_P, y_P)$ ja $Q = (x_Q, y_Q)$ kautta kulkeva suora. Tällaisen suoran yhtälö on

$$y - y_P = \frac{y_P - y_Q}{x_P - x_Q}(x - x_P) = s(x - x_P).$$

Koska $-R = (x_R, -y_R) = (x_R, y_P - s(x_P - x_R)) = (x_R, y_P + s(x_R - x_P))$, huomataan, että $-R$ todellakin sijaitsee suoralla, kuten pitikin.

Seuraavaksi osoitetaan, että $-R$ (tai R) todellakin myös sijaitsee elliptisellä käyrällä. Tämä on hieman vaikeampi tehtävä. Ensinnäkin, koska pisteet P ja Q sijaitsevat käyrällä, tiedetään, että

$$\begin{cases} y_P^2 = x_P^3 + ax_P + b \\ y_Q^2 = x_P^3 + ax_P + b. \end{cases}$$

Vähennetään yhtälöt toisistaan ja saadaan

$$y_P^2 - y_Q^2 = a(x_P - x_Q) + x_P^3 - x_Q^3,$$

joten

$$a = \frac{y_P^2 - y_Q^2}{x_P - x_Q} - \frac{x_P^3 - x_Q^3}{x_P - x_Q} = s(y_P - y_Q) - (x_P^2 + x_P x_Q + x_Q^2).$$

Ratkaistaan vielä parametrin b arvo ensimmäisestä yhtälöstä:

$$b = y_P^2 - x_P^3 - ax_P = y_P^2 - x_P^3 - x_P\left(s(y_P + y_Q) - (x_P^2 + x_P x_Q + x_Q^2)\right).$$

Tämän jälkeen voidaan osoittaa, että $y_R^2 = x_R^3 + ax_R + b$ sijoittamalla yhtälöön luvuille a ja b ratkaistut lausekkeet sekä luvun s lauseke. Tämä on ihan rehellisesti vain raakaa työtä. □

Pisteen kahdentaminen on ikäänkuin raja-arvo edellisestä operaatiosta. Muuten kaikki toimii samoin, mutta pisteiden kautta kulkevan suoran sijaan käytetään tangenttia. Nyt siis kulmakerroin on

$$s = \frac{3x_P^2 + a}{2y_P},$$

ja pisteen $(x_R, y_R) = R = 2P$ koordinaatit ovat

$$\begin{cases} x_R = s^2 - 2x_P \\ y_R = -y_P + s(x_P - x_R). \end{cases}$$

Yhteenlasku äärellisissä kunnissa

Yllä on esitetty laskutoimitukset reaalilukujen kunnassa, eli miten kaikki toimii, kun $x, y \in \mathbb{R}$. Kryptografian kannalta äärelliset kunnat ovat oleellisia. Voisimme määritellä yhteenlaskun äärellisissä kunnissa geometrisesti, ja konstruktio olisi varsin samanlainen kuin reaaliluvuillakin. Kyseinen konstruktio ei kuitenkaan välttämättä ole ehkä kätevin mahdollinen.

Yhteenlaskukaavat siirtyvät suoraan, mutta jokainen operaatio pitää suorittaa modulo p, kun eletään kunnassa $\mathbb{Z}_p$. Yhteenvedettynä, laskutoimitukset siis toimivat seuraavasti:

Pisteen vasta-alkio: Kun $P = (x_P, y_P)$, niin $-P = (x_P, p - y_P)$.

Vasta-alkion summaus: $P + (-P) = O$, ja neutraalialkion summaus $O + P = P$.

Kahden erisuuren pisteen $P = (x_P, y_P)$ ja $Q = (x_Q, y_Q)$ summaus, kun $P \neq -Q$:

$$s = \frac{y_P - y_Q}{x_P - x_Q} \pmod{p}$$

ja

$$P + Q = R = (x_r, y_R),$$

missä

$$\begin{cases} x_R = s^2 - x_P - x_Q \pmod{p} \\ y_R = -y_P + s(x_P - x_R) \pmod{p}. \end{cases}$$

Lopulta vielä pisteiden kahdennus: Jos $R = 2P$, niin

$$s = \frac{3x_P^2 + a}{2y_P} \pmod{p},$$

ja

$$\begin{cases} x_R = s^2 - 2x_P \pmod{p} \\ y_R = -y_P + s(x_P - x_R) \pmod{p}. \end{cases}$$

2.3 Elliptisen käyrän rakenteesta

Elliptisen käyrän pisteet muodostavat ylläolevan laskutoimituksen suhteen ryhmän, sillä

1. Laskutoimitus on suljettu.
2. Laskutoimituksella on neutraalialkio.
3. Kaikilla alkioilla on vasta-alkio.
4. Laskutoimitus on assosiatiivinen. Tämän todistaminen vaatisi pitkällisiä laskuja useine tapaustarkasteluineen. Sivuutetaan.

Ryhmä on peräti Abelin ryhmä, sillä alkiot kommutoivat laskutoimituksen suhteen.

Viitteet

[1] SAGE. `http://www.sagemath.org`

[2] Batten Lynn Margaret. Public Key Cryptography: Applications and Attacks (IEEE Press Series on Information and Communication Networks Security) [Kindle Edition]