Jouko Teeriaho kevät 2018

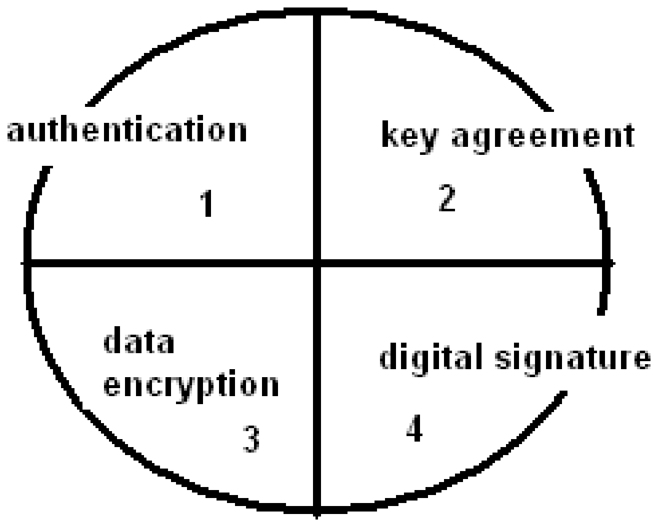
ECC Elliptic Curve Cryptography

"Elliptisten käyrien salaus" lähemmin tarkasteltuna

Yhteys salattu (TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, 256-bittinen avain, TLS 1.2

1. Miksi on siirrytty ECC:hen?

1) käyttäjien autentikointi, **2) symmetrisestä avaimesta sopiminen**
3) symmetrinen salaus (AES) ja **4) digitaalinen allekirjoitus**



Aiempi standardi: RSA autentikointi, RSA Key Exchange,
Sha256RSA digital signature, AES lohkosalaus

V. 2018 Elliptisten käyrien salaus korvannut RSA:n.
Lohkosalaimena edelleen AES256

ECC lyhentää avainpituuksia 90% verrattuna RSA:han

EU suositus v. 2008 arvioi turvallisia avainpituuksia eri järjestelmissä
RSA:n ongelmana ovat liian pitkät avaimet => suorituskykyongelmia

Description	RSA	DH, Elgamal	ECC
Can be broken with basic technologies	816 bits	816	128
Can be broken in short time	1008	1008	144
In theory adequate	1248	1248	160
Generally regarded as absolute minimum	1776	1776	192
Guarantees minimum security	2432	2432	224
Adequate except top secret documents	3248	3248	256
Adequate even for tope secret documents	15424	15424	512

=> ECC (Elliptic Curve Cryptography) tarjoaa saman turvallisuuden selvästi pienemmillä avainpiotuuksialla kuin RSA.

2. Ryhmät ja sykliset ryhmät

ECC kuuluu **syklisten ryhmien salaukset -** menetelmäluokkaan

Ryhmä

Joukko G jossa on määritelty laskutoimitus * , on RYHMÄ , jos

G1 $a*b \in G$ kaikille $a, b \in G$

G2 $a*(b*c) = (a*b)*c$ kaikille $a,b,c \in G$

G3 On olemassa “neutraalialkio” $e \in G$, jolle

$a*e = e*a = a$ kaikille $a \in G$

G4 Kaikilla $a \in G$, on olemassa käänteisalkio $a^{-1} \in G$ jolle $a*a^{-1}=a^{-1}*a = e$

Kommutatiivisia ryhmiä kutsutaan Abelin ryhmiksi

Jos $a*b = b*a$ kaikille $a*b \in G$, G on siis "Abelin ryhmä"

Äärellisiä ryhmiä koskee Eulerin teoreema

Merkitään n = #G = ryhmän G alkoiden lukumäärä . SIlloin

g^n = e for all g ∈ G

Aliryhmät

Ryhmän G osajoukkoa H sanotaan G:n **aliryhmäksi**, jos H on myös ryhmä

Lagrange'n teoreema antaa aliryhmien mahdolliset koot

Ryhmän G aliryhmän H alkioiden lukumäärä on G:n alkioiden lukumäärän **divisori** (tekijä)

ts. #H = #G / d jollakin kokonaisluvulla d

Ryhmä on syklinen jos se voidaan generoida yhdestä alkiosta

Äärellistä ryhmää G (koko n alkiota) sanotaan **sykliseksi** , jos on olemassa alkio g ∈ G jolle

$\{ g, g^2, \ldots, g^n = e\} = G$

Alkiota **g** kutsutaan ryhmän G "**generaattoriksi"** tai generoivaksi alkioksi

(Comment: Fact that g^n= e is called Euler's theorem)

Ryhmän alkion "kertaluku"

Kaikki ryhmän alkiot generoivat jonkin aliryhmän. Merkintä **<a > tarkoittaa alkion a generoimaa aliryhmää.**
Alkion a generoiman aliryhmän kokoa sanotaan a: n **kertaluvuksi** Ord(a)

Jos g on generoiva alkio, Ord(g) = #G = n (G : n alkioiden lukumäärä)

---

3. Sykliset ryhmät Elliptisillä käyrillä

Elliptisen käyrän määritelmä

1880 - luvulla Weierstrass tutki seuraavanlaisia käyriä

$$y^2 + A\,xy = x^3 + B\,x^2 + C\,x + D$$

Niitä kutsutaan elliptisiksi käyriksi.

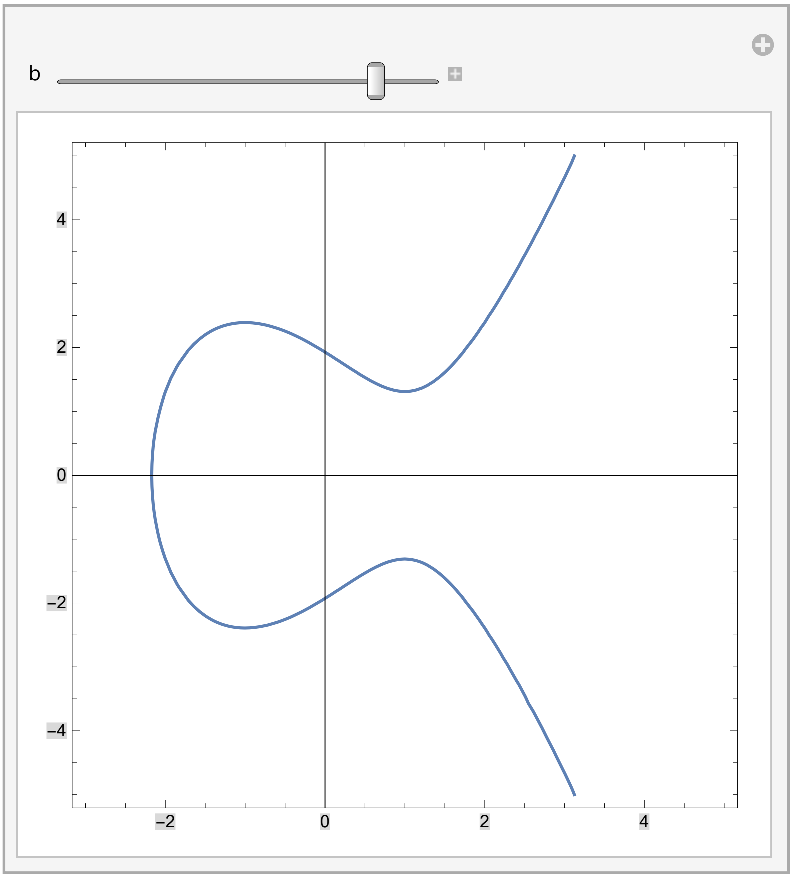
Salauksessa käytettävien käyrien muoto

Yksinkertaisilla koordinaattimuunnoksilla käyrän yhtälö saadaan muotoon

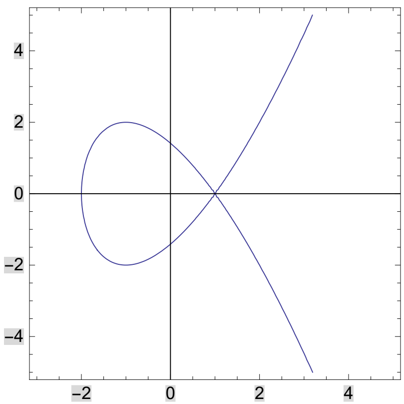
$$y^2 = x^3 + a\,x + b$$

Seuraava animaatio näyttää miltä käyrät näyttävät

```
Manipulate[
 ContourPlot[y^2 == x^3 - 3 x + b, {x, -3, 5}, {y, -5, 5}, Axes → True], {b, -5, 5}]
```



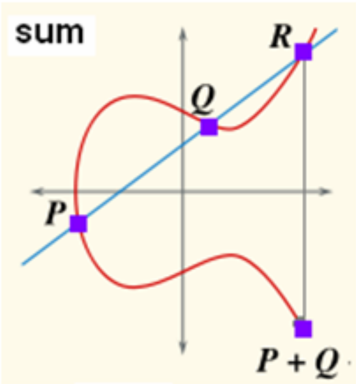
Käyriä, joissa oikean puolen polynomilla on tuplajuuri, ei voi käyttää salauksessa (kuva)



- Ryhmäoperaation (pisteiden summa) määrittely

Addition group on Elliptic Curve

It is possible to define a sum of points in a way, that the group properties are satisfied:

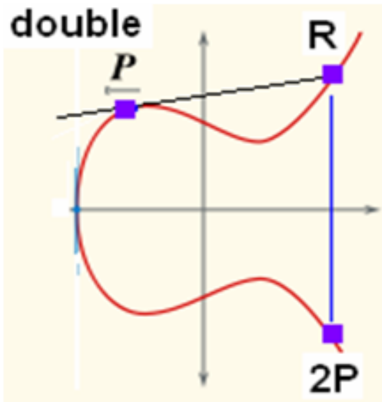


Addition (x1,y1) + (x2,y2)

$\lambda = (y_2 - y_1)/ (x_2 - x_1)$

$x = \lambda^2 - x_1 - x_2$

$y = - y_1 + \lambda(x_1 - x)$



Doubling 2 (x1,y1)

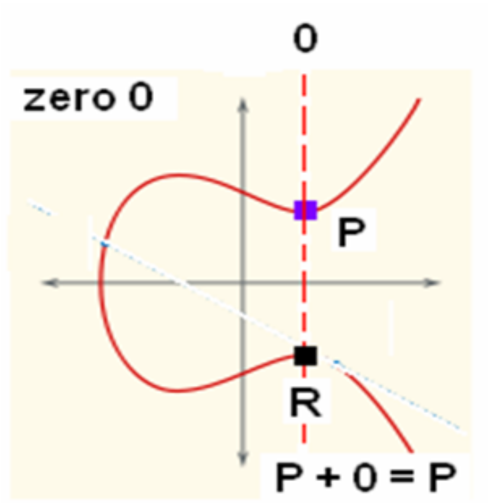
$\lambda = (3 x_1^2 + a)/ (2y_1)$

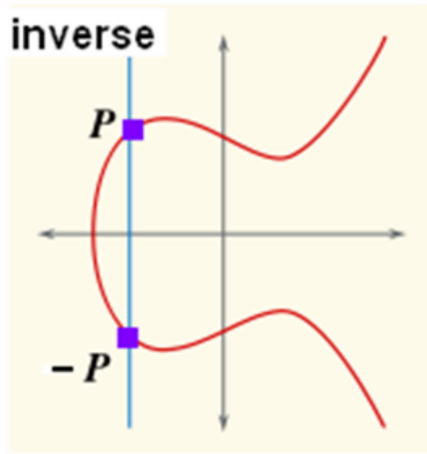
$x = \lambda^2 - 2x_1$

$y = -y_1 + \lambda(x_1 - x)$

Neutraalialkion O ja P:n käänteisalkion -P määrittely

Zero and inverse elements





Zero element 0 is a point with y-coordinate at infinity

Inverse element –P is the symmetric point of P

Neutraalialkio O määritellään alkioksi jolle y = ∞ , joka lisätään käyrän pisteisiin, jotta se toteuttaisi ryhmäaksioomat

4. ECC toteutettuna *Mathematica*- ohjelmalla

Diskreetti Elliptinen käyrä koostuu pisteistä (x,y), joissa x ja y ovat kokonaislukuja välilta 1...(q -1) ja q on alkuluku. Laskutoimitukset suoritetaan mod q.

$E(F_q)$ = kokonaislukuparien (x, y) joukko , missä $0 \le x,y < q$ ja jotka toteuttavat käyrän yhtälön $y^2 = x^3 + a\,x + b \pmod{q}$

Esim : Elliptic Curve $y^2 = x^3 - 3x + 99$ mod 281

Listataan käytän pisteet

```
q = 281; pts = {};
For[x = 0, x < q, x++,
 For[y = 0, y < q, y++,
  If[Mod[y^2 - (x^3 - 3 x + 99), q] == 0, pts = Append[pts, {x, y}]]]]
pts // StandardForm
```

```
{{2, 35}, {2, 246}, {5, 107}, {5, 174}, {6, 4}, {6, 277}, {7, 126}, {7, 155},
 {8, 5}, {8, 276}, {11, 58}, {11, 223}, {13, 3}, {13, 278}, {14, 122}, {14, 159},
 {15, 30}, {15, 251}, {16, 139}, {16, 142}, {19, 88}, {19, 193}, {23, 26},
 {23, 255}, {26, 52}, {26, 229}, {27, 84}, {27, 197}, {28, 7}, {28, 274},
 {30, 95}, {30, 186}, {32, 52}, {32, 229}, {33, 44}, {33, 237}, {34, 47},
 {34, 234}, {35, 88}, {35, 193}, {36, 1}, {36, 280}, {38, 129}, {38, 152},
 {39, 65}, {39, 216}, {42, 57}, {42, 224}, {44, 17}, {44, 264}, {45, 56},
 {45, 225}, {48, 26}, {48, 255}, {49, 108}, {49, 173}, {51, 33}, {51, 248},
 {55, 111}, {55, 170}, {56, 22}, {56, 259}, {57, 137}, {57, 144}, {60, 119},
 {60, 162}, {65, 58}, {65, 223}, {66, 55}, {66, 226}, {67, 122}, {67, 159},
 {68, 13}, {68, 268}, {70, 120}, {70, 161}, {73, 67}, {73, 214}, {74, 112},
 {74, 169}, {75, 116}, {75, 165}, {77, 30}, {77, 251}, {80, 57}, {80, 224},
 {82, 112}, {82, 169}, {84, 22}, {84, 259}, {85, 69}, {85, 212}, {88, 43},
 {88, 238}, {89, 89}, {89, 192}, {90, 14}, {90, 267}, {91, 6}, {91, 275},
 {92, 66}, {92, 215}, {93, 123}, {93, 158}, {98, 107}, {98, 174}, {100, 1},
 {100, 280}, {101, 90}, {101, 191}, {106, 85}, {106, 196}, {107, 137},
 {107, 144}, {108, 56}, {108, 225}, {112, 134}, {112, 147}, {115, 104},
 {115, 177}, {117, 137}, {117, 144}, {119, 5}, {119, 276}, {122, 130},
 {122, 151}, {125, 112}, {125, 169}, {128, 56}, {128, 225}, {129, 70},
 {129, 211}, {130, 91}, {130, 190}, {131, 42}, {131, 239}, {132, 23},
 {132, 258}, {133, 128}, {133, 153}, {134, 21}, {134, 260}, {135, 40},
 {135, 241}, {137, 36}, {137, 245}, {138, 72}, {138, 209}, {140, 41},
 {140, 240}, {141, 22}, {141, 259}, {143, 51}, {143, 230}, {145, 1}, {145, 280},
 {148, 127}, {148, 154}, {149, 136}, {149, 145}, {151, 105}, {151, 176},
 {153, 49}, {153, 232}, {154, 5}, {154, 276}, {156, 115}, {156, 166},
 {159, 57}, {159, 224}, {164, 16}, {164, 265}, {165, 15}, {165, 266},
 {168, 40}, {168, 241}, {171, 37}, {171, 244}, {172, 37}, {172, 244},
 {173, 49}, {173, 232}, {174, 16}, {174, 265}, {175, 29}, {175, 252},
 {176, 60}, {176, 221}, {177, 59}, {177, 222}, {178, 107}, {178, 174},
 {179, 134}, {179, 147}, {180, 99}, {180, 182}, {182, 59}, {182, 222},
 {184, 113}, {184, 168}, {186, 79}, {186, 202}, {189, 30}, {189, 251},
 {190, 64}, {190, 217}, {191, 132}, {191, 149}, {192, 83}, {192, 198},
 {193, 63}, {193, 218}, {197, 41}, {197, 240}, {199, 115}, {199, 166},
 {200, 122}, {200, 159}, {201, 130}, {201, 151}, {203, 59}, {203, 222},
 {204, 66}, {204, 215}, {205, 58}, {205, 223}, {207, 115}, {207, 166},
 {210, 26}, {210, 255}, {212, 75}, {212, 206}, {213, 121}, {213, 160},
 {215, 71}, {215, 210}, {217, 38}, {217, 243}, {218, 98}, {218, 183},
 {219, 37}, {219, 244}, {220, 61}, {220, 220}, {223, 52}, {223, 229},
 {224, 16}, {224, 265}, {225, 41}, {225, 240}, {226, 135}, {226, 146},
 {227, 88}, {227, 193}, {234, 54}, {234, 227}, {236, 49}, {236, 232},
 {239, 130}, {239, 151}, {243, 97}, {243, 184}, {244, 74}, {244, 207},
 {251, 100}, {251, 181}, {253, 46}, {253, 235}, {254, 27}, {254, 254},
 {256, 2}, {256, 279}, {257, 39}, {257, 242}, {259, 40}, {259, 241}, {263, 28},
 {263, 253}, {264, 24}, {264, 257}, {266, 66}, {266, 215}, {271, 134},
 {271, 147}, {274, 45}, {274, 236}, {278, 9}, {278, 272}, {280, 35}, {280, 246}}
```

Lisätään pisteisiin vielä neutraalialkio O , jotta siitä saadaan ryhmä

```
pts = pts ⋃ {O}
```

Lasketaan ryhmän alkioiden lukumäärä

```
n = Length[pts]
Divisors[n]
```

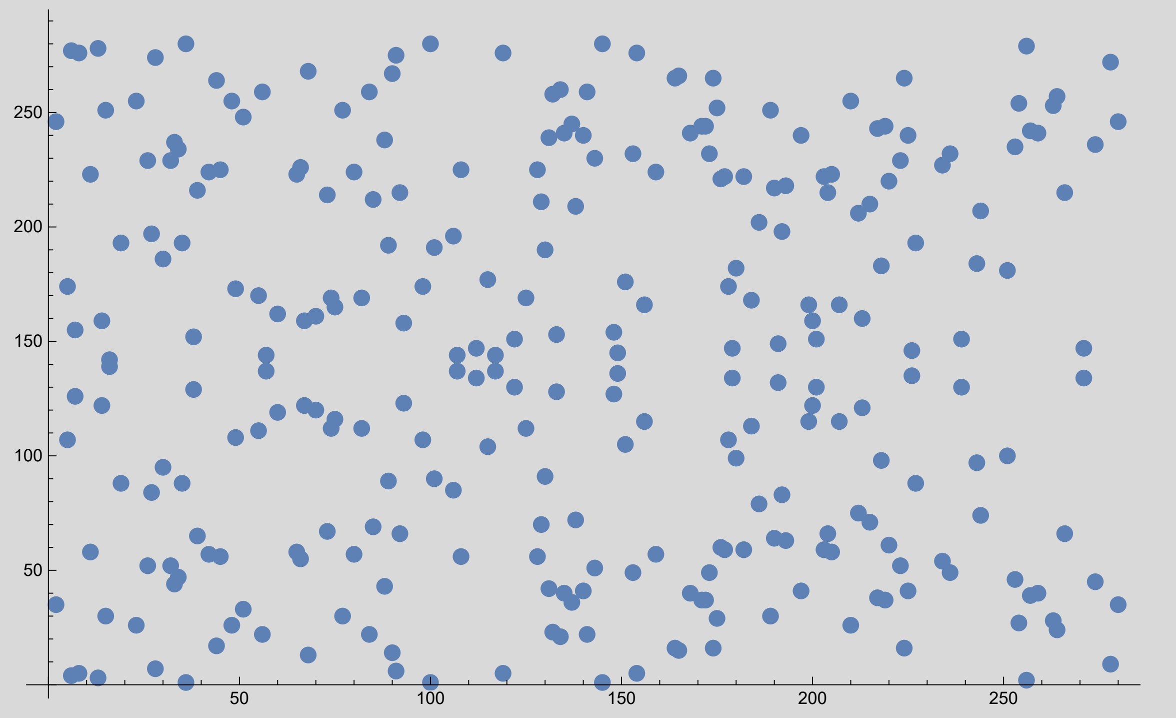
```
291
```

```
{1, 3, 97, 291}
```

Alkioita on yhteensä 291, jonka divisoreita ovat 1, 3 ja 97 ja luku 291 itse

Visualisoidaan ryhmän alkiot

```
ListPlot[pts, PlotStyle -> PointSize[0.015]]
```



Koodataan *Mathematica*lla ryhmäyhteenlasku EllipticSum

Argumentit: q = alkulukumodulus
a, b = käyrän $y^2 = x^3 + a\,x + b$ parametrit
P_list = piste P muodossa { x, y}

Q_list = piste Q muodossa { x, y}
EllipticSum laskee summan P + Q

Funktion pitää toimia myös erikoistapauksissa, joissa joko P tai Q on “nolla-alkio” O,
ja myös tapauksessa jossa P on sama kuin Q.

```
EllipticSum[q_, a_, b_, P_List, Q_List] :=
 Module[ {λ, x3, y3, P3},
  Which[P == {O}, R = Q,
   Q == {O}, R = P,
   P[[1]] ≠ Q[[1]],
   λ = Mod[(Q[[2]] - P[[2]]) * PowerMod[Q[[1]] - P[[1]], -1, q], q];
   x3 = Mod[λ^2 - P[[1]] - Q[[1]], q];
   y3 = Mod[-(λ (x3 - P[[1]]) + P[[2]]), q];
   R = {x3, y3},
   (P == Q) ∧ (P ≠ {O}),
   λ = Mod[ (3 * P[[1]]^2 + a) *
      PowerMod[2 P[[2]], -1, q], q];
   x3 = Mod[λ^2 - 2 P[[1]], q];
   y3 = Mod[-(λ (x3 - P[[1]]) + P[[2]]), q];
   R = {x3, y3},
   (P[[1]] == Q[[1]]) ∧ (P[[2]] ≠ Q[[2]]), R = {O}];
  R]
```

Testi 1: Laske summa (8,5) + (190, 64) (käyrän $y^2 = x^3$ - 3x + 99 pisteitä)

```
q = 281; P = {8, 5}; Q = {190, 64};
EllipticSum[q, -3, 99, P, Q]
```

```
{55, 111}
```

Testi 2. Kokeillaan lisätä nolla-alkio pisteeseen: (8,5) + O pitäisi antaa (8,5)

```
P = {8, 5};
EllipticSum[q, -3, 99, P, {O}]
```

```
{8, 5}
```

Mathematica funktio, joka laskee nopeasti pisteen P monikerran nP

Funktio on ECC - analogia ns. PowerMod- algoritmille, jota RSA käyttää

(11P = 10 P + P = 5*(2P) + P = 4*(2P) + 2P + P = 8P + 2P + P)

```
Mult[n_, P_, q_, a_, b_] := Module[{x, A, B},
  x = n; A = P; B = {O};
  While[x > 1,
   If[OddQ[x],
     B = EllipticSum[q, a, b, A, B];
     x = x - 1,
     A = EllipticSum[q, a, b, A, A];
     x = x / 2;
    ];
  ];
  A = EllipticSum[q, a, b, A, B];
  A
 ]
```

Etsitään käyrän generoiva piste G (ryhmän generaattori)

```
d = Divisors[n]      (* possible subgroup sizes are divisors of n *)
```

```
{1, 3, 97, 291}
```

Lagrangen teoreeman mukaan, G on generaattori, jos G, 3G , 97G ≠ O, mutta 291G = O

```
(* valitaan ehdokkaaksi jokin satunnainen käyrän piste *)
candidate = {135, 241};
Table[Mult[d[[k]], candidate, q, -3, 99], {k, 1, 4}]
```

```
{{135, 241}, {134, 21}, {234, 227}, {O}}
```

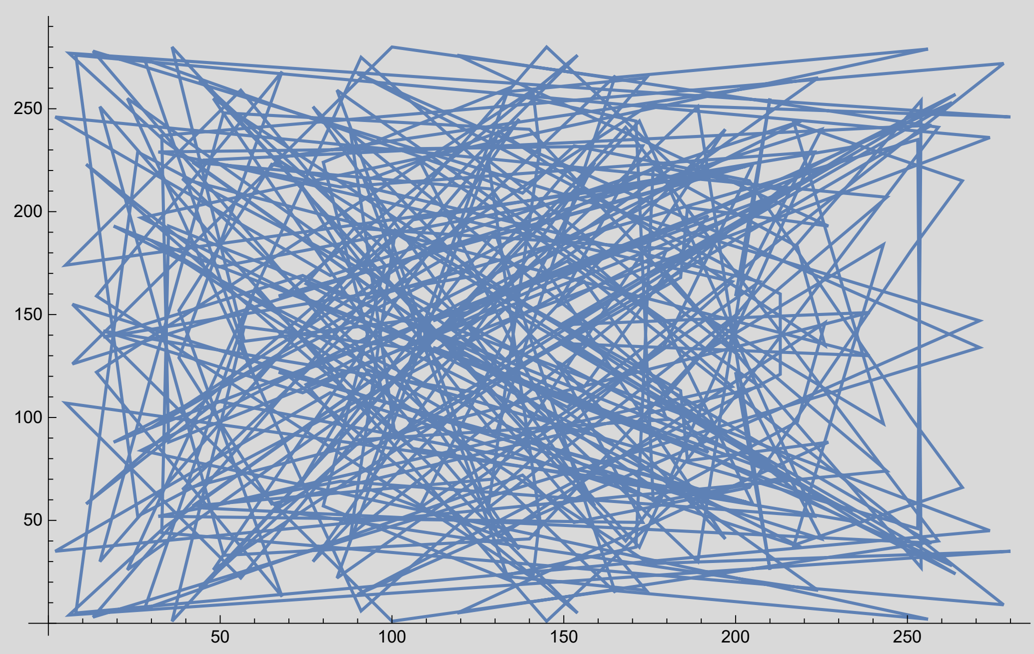
Pisteen (135, 241) kertaluku on siten 291 => piste (135, 241) on generoiva alkio

Visualisoidaan sykli {G, 2G , 3G, ..., 290G} murtoviivalla

```
G = {135, 241}; q = 281;
gr1 = Table[Mult[i, G, q, -3, 99], {i, 1, 291}]
```

```
{{135, 241}, {92, 215}, {134, 21}, {80, 57}, {98, 174}, {56, 259}, {5, 174},
 {190, 217}, {75, 116}, {89, 89}, {180, 99}, {178, 107}, {254, 254},
 {253, 46}, {93, 123}, {73, 67}, {130, 190}, {165, 15}, {39, 216}, {239, 130},
 {149, 136}, {264, 24}, {220, 61}, {88, 238}, {101, 90}, {257, 242}, {45, 225},
 {199, 166}, {91, 6}, {23, 255}, {224, 16}, {66, 55}, {236, 232}, {106, 196},
 {11, 58}, {49, 108}, {203, 59}, {193, 63}, {67, 122}, {205, 58}, {179, 147},
 {108, 225}, {159, 57}, {77, 251}, {197, 41}, {129, 211}, {42, 224},
 {122, 130}, {57, 144}, {36, 1}, {168, 241}, {259, 40}, {119, 5}, {227, 88},
 {186, 79}, {184, 113}, {115, 177}, {30, 95}, {175, 252}, {280, 246}, {6, 277},
 {34, 234}, {182, 59}, {145, 1}, {15, 251}, {51, 33}, {140, 41}, {201, 151},
 {128, 56}, {143, 230}, {141, 259}, {14, 122}, {68, 13}, {38, 152}, {65, 223},
 {207, 166}, {84, 22}, {131, 239}, {226, 135}, {218, 183}, {176, 221},
 {171, 37}, {132, 23}, {174, 16}, {125, 112}, {16, 142}, {74, 112}, {263, 253},
 {133, 128}, {44, 264}, {172, 37}, {223, 229}, {85, 212}, {32, 229},
 {173, 232}, {148, 154}, {234, 227}, {55, 111}, {19, 88}, {177, 222},
 {215, 210}, {112, 147}, {192, 198}, {156, 115}, {26, 229}, {8, 5}, {274, 45},
 {117, 144}, {189, 30}, {210, 255}, {200, 159}, {225, 240}, {7, 126},
 {100, 280}, {164, 265}, {256, 279}, {27, 197}, {219, 37}, {82, 112}, {2, 35},
 {244, 74}, {191, 149}, {243, 97}, {217, 243}, {266, 215}, {251, 181},
 {204, 66}, {153, 49}, {138, 72}, {28, 7}, {60, 162}, {154, 5}, {70, 120},
 {107, 144}, {151, 105}, {278, 272}, {33, 237}, {35, 88}, {212, 206},
 {48, 26}, {137, 245}, {13, 3}, {271, 134}, {90, 267}, {213, 160}, {213, 121},
 {90, 14}, {271, 147}, {13, 278}, {137, 36}, {48, 255}, {212, 75}, {35, 193},
 {33, 44}, {278, 9}, {151, 176}, {107, 137}, {70, 161}, {154, 276}, {60, 119},
 {28, 274}, {138, 209}, {153, 232}, {204, 215}, {251, 100}, {266, 66},
 {217, 38}, {243, 184}, {191, 132}, {244, 207}, {2, 246}, {82, 169},
 {219, 244}, {27, 84}, {256, 2}, {164, 16}, {100, 1}, {7, 155}, {225, 41},
 {200, 122}, {210, 26}, {189, 251}, {117, 137}, {274, 236}, {8, 276},
 {26, 52}, {156, 166}, {192, 83}, {112, 134}, {215, 71}, {177, 59}, {19, 193},
 {55, 170}, {234, 54}, {148, 127}, {173, 49}, {32, 52}, {85, 69}, {223, 52},
 {172, 244}, {44, 17}, {133, 153}, {263, 28}, {74, 169}, {16, 139}, {125, 169},
 {174, 265}, {132, 258}, {171, 244}, {176, 60}, {218, 98}, {226, 146},
 {131, 42}, {84, 259}, {207, 115}, {65, 58}, {38, 129}, {68, 268}, {14, 159},
 {141, 22}, {143, 51}, {128, 225}, {201, 130}, {140, 240}, {51, 248},
 {15, 30}, {145, 280}, {182, 222}, {34, 47}, {6, 4}, {280, 35}, {175, 29},
 {30, 186}, {115, 104}, {184, 168}, {186, 202}, {227, 193}, {119, 276},
 {259, 241}, {168, 40}, {36, 280}, {57, 137}, {122, 151}, {42, 57}, {129, 70},
 {197, 240}, {77, 30}, {159, 224}, {108, 56}, {179, 134}, {205, 223},
 {67, 159}, {193, 218}, {203, 222}, {49, 173}, {11, 223}, {106, 85},
 {236, 49}, {66, 226}, {224, 265}, {23, 26}, {91, 275}, {199, 115}, {45, 56},
 {257, 39}, {101, 191}, {88, 43}, {220, 220}, {264, 257}, {149, 145},
 {239, 151}, {39, 65}, {165, 266}, {130, 91}, {73, 214}, {93, 158}, {253, 235},
 {254, 27}, {178, 174}, {180, 182}, {89, 192}, {75, 165}, {190, 64}, {5, 107},
 {56, 22}, {98, 107}, {80, 224}, {134, 260}, {92, 66}, {135, 40}, {O}}
```

```
ListPlot[gr1, Joined → True, PlotStyle → PointSize[0.03]]
```



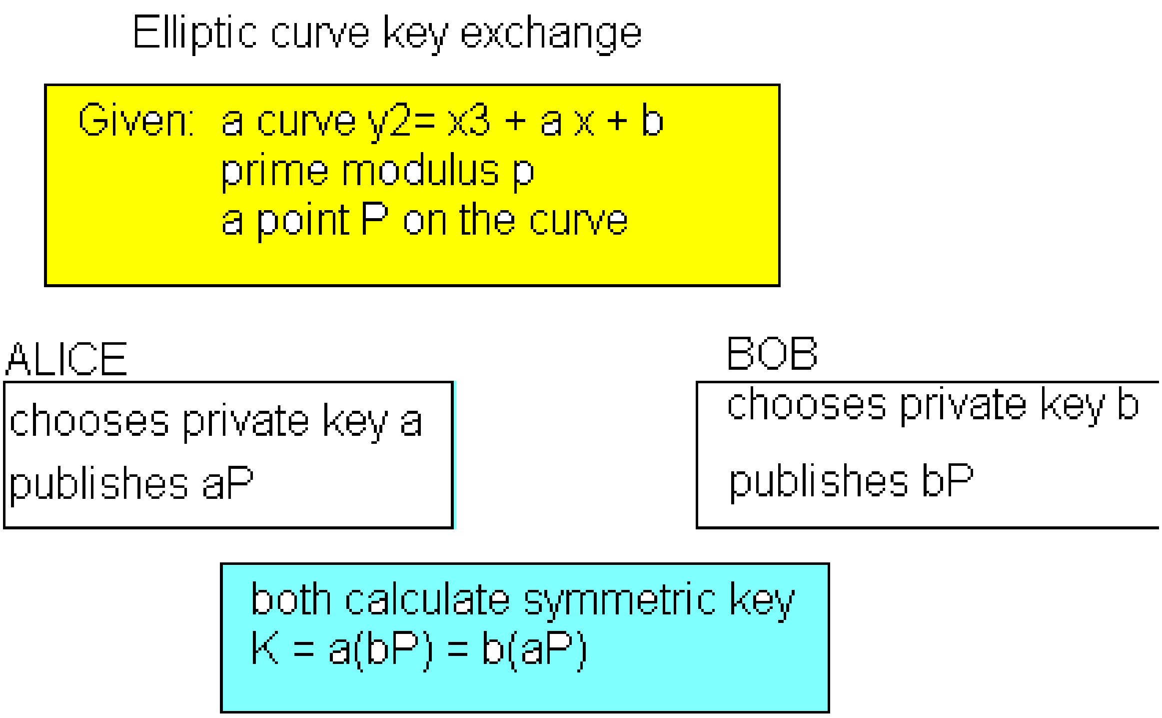
Murtoviiva (g, 2g, ...} käy läpi kaikki käyrän pisteet

5. ECC:hen perustuvia salausalgoritmeja

Aluksi käytetään esimerkkikäyrää $y^2 = x^3 - 3x + 99 \bmod 281$

▪ “ECDHE” = “Elliptic Curve Diffie Hellman Exchange”

Istunnon AES avaimesta sopimisen algoritmi (käyttö: Suomen verkkopankit)



1. Alice ja Bob luovat satunnaiset yksityiset avaimet

Alices private key : ka = 135
Bobs private key: kb = 222

2. Alice ja Bob lähettävät toisilleen julkisina avaimina Ya = *kaG and Yb = *kb**G,**

```
G = {135, 241};      (* käyrän generoiva piste *)
q = 281;              (* käyrän modulus *)
```

```
ka = 135;  kb = 222;
Ya = Mult[ka, G, q, -3, 99]
Yb = Mult[kb, G, q, -3, 99]
```

```
{151, 105}
```

```
{128, 225}
```

3. Sekä Alice että Bob laskevat symmetrisen avaimen,
joka on käyrän piste K = ka*kb*G

```
K = Mult[ka, Yb, q, -3, 99]
K = Mult[kb, Ya, q, -3, 99]
```

```
{134, 260}
```

```
{134, 260}
```

Viestin salaus ElGamal salausta soveltaen

Huom! Dataa ei laajemmin salata EC- salauksella, vaan lohkosalauksella AES, jonka käyttämä istuntoavain sovitaan edellä esitetyllä tavalla.

1. Olkoon K = (K_1,K_2) istuntoavain, joka on sovittu edellä esitetysti

2. Viesti koodataan kok. lukupareiksi, esim. m = (m_1, m_2) = (100, 120)

3. Salakirjoitus on viestin ja avaimen "tulo" c = (m_1*K_1 , m_2* K_2) mod q

Huom: Tulo määritellään seuraavasti (a,b)*(c,d) = (a*c , b*d). *Mathematicalla* asteriksi * toimii juuri näin.

```
m = {100, 120};  K = {134, 260};
c = Mod[m * K, q]        (* salakirjoitus *)
```
```
{193, 9}
```

Salakirjoituksen purkaminen selväkieliseksi

1. Vastaanottaja laske purkuavaimen DK , joka on avaimen K käänteisalkio mod q
Purkuavain DK = (K_1^{-1} mod q , K_2^{-1} mod q)

```
DK = PowerMod[K, -1, q]     (* purkuavaimen laskeminen *)
```
```
{216, 107}
```

2. Seuraavaksi vastaanottaja käyttää purkuavainta DK

```
Mod[c * DK, q]
```
```
{100, 120}
```

Tulos on alkuperäinen viesti

Seuraavaksi kokeillaan toimivatko määritellyt funktiot elliptisillä käyrillä, joita oikeasti käytetään salatuissa yhteyksissä.

6. ECDHE ja salaus Elliptisellä käyrällä P-192

Kryptauksessa käytettävien käyrien vaatimuksia

1. Käyrän pisteiden määrän n tulisi mieluimmin olla alkuluku,
   (tai kahden alkuluvun tulokin käy, joista toinen luvuista pieni)
   ja moduluksen q ≥ 190 bits (tarvittava turvamariginaali)

=> Käyrän pisteiden lukumäärän tunteminen on välttämätöntä, jotta salaus olisi turvallinen.

Toisaalta pisteiden laskeminen on erittäin hankalaa.

NIST (National institute of Standards in USA) on standardoinut joukon käyriä, jotka täyttävät turvallisuusvaatimukset ja joiden pisteiden määrä tunnetaan.

Seuraavassa käytetään käyrää, jonka tunnus on P-192

P-192 parametrit

ECDHE key exchange käyrällä P-192

Alice luo yksityisen avaimen ka ja laskee julkisen avaimen Ya = ka G

```
ka = 2 818 646 689 284 967 968 603 885 680 739 626 753 757 717 668 743 685 369;
Ya = Mult[ka, G, q, -3, b]
```

```
{4 166 887 439 959 785 442 359 358 401 626 820 195 302 130 396 853 922 747 090,
 342 002 490 943 820 139 356 288 313 636 684 834 682 210 773 457 498 261 724}
```

Bob luo yksityisen avaimen kb ja laskee julkisen avaimen Yb = kb G

```
kb = 2 101 924 874 329 080 718 071 957 364 927 874 958 230 913 619 682 994 500;
Yb = Mult[kb, G, q, -3, b]
```

```
{3 197 479 727 310 441 184 166 659 954 176 065 551 017 813 604 210 849 295 027,
 4 546 651 453 263 495 348 932 303 783 137 537 190 292 590 929 227 544 435 757}
```

Sekä Alice ja Bob laskevat tahoillaan symmterisen istuntoavaimen: K = ka*kb*G

```
K = Mult[kb, Ya, q, -3, b]      (* Bob's calculation *)
K = Mult[ka, Yb, q, -3, b]      (* Alice's calculation *)
```

```
{4 569 158 537 909 585 871 329 893 828 249 154 554 821 121 379 238 590 872 510,
 5 889 543 201 412 998 599 750 263 908 982 414 398 530 518 138 795 041 140 383}
```

```
{4 569 158 537 909 585 871 329 893 828 249 154 554 821 121 379 238 590 872 510,
 5 889 543 201 412 998 599 750 263 908 982 414 398 530 518 138 795 041 140 383}
```

This is a symmetric key produced by the key exchange algorithm

AES128-key luodaan tästä avaimesta.

Helpoin tapa on ottaa 128 ensimmäistä bittiä pisteen K x- komponentista

```
AESkey = Take[IntegerDigits[K[[1]], 2], 128]
```

```
{1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0,
 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0,
 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0,
 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1,
 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0}
```

Avaimia esitetään yleensä hex- muodossa

```
BaseForm[FromDigits[AESkey, 2], 16]
```

$\texttt{ba583db1e7aa885b9983b447ea910820}_{16}$

ECC salaus   (ElGamal analogia)

Viesti koodataan kokonaislukupareiksi

Olkoon viesti kaksi sanaa: (“ArcticSeminar”, “Rovaniemi”)

Muunnetaan viesti ASCII -koodien kautta kahdeksi kokonaisluvuksi

```
m01 = ToCharacterCode["ArcticSeminar"]
m02 = ToCharacterCode["Rovaniemi"]
```

```
{65, 114, 99, 116, 105, 99, 83, 101, 109, 105, 110, 97, 114}
```

```
{82, 111, 118, 97, 110, 105, 101, 109, 105}
```

```
{m1, m2} = Mod[{FromDigits[m01, 256], FromDigits[m02, 256]}, q];
m = {m1, m2}
```

```
{5 185 232 087 941 534 446 075 041 964 402, 1 520 664 728 156 487 642 473}
```

Salaus suoritetaan ao. tavalla suoritettavalla kertolaskulla

(c1, c2) = (m1, m2)*(K1, K2) = (m1*K1, m2*K2)

Alice laskee salakirjoituksen

```
c = Mod[K * m, q]     (* ciphertext *)
```

```
{2 461 969 853 658 513 928 470 552 774 196 794 839 821 484 524 954 445 766 793,
 4 922 823 632 219 955 069 517 528 447 511 392 059 330 930 252 067 710 373 849}
```

Bob laskee purkuavaimen DK ja purkaa salauksen

```
DK = PowerMod[K, -1, q]
```

```
Z = Mod[DK * c, q]
```

```
{5 185 232 087 941 534 446 075 041 964 402, 1 520 664 728 156 487 642 473}
```

Tämä pitää vielä muuttaa selväkieliseksi merkkien ASCII koodien kautta

```
FromCharacterCode[IntegerDigits[Z[[1]], 256]]
FromCharacterCode[IntegerDigits[Z[[2]], 256]]
```

```
ArcticSeminar
```

```
Rovaniemi
```

ECC sisältää myös digitaalisen allekirjoituksen ECDSA, joka voidaan demonstroida Mathematicalla.

7. Mihin ECC:n turvallisuus perustuu?

Taitava verkkovakoilija (esim. tiedustelupalvelu)
1) tietää, mitä Elliptistä käyrää yhteys käyttää
2) tietää, mikä on generoiva piste G
3) osaa nappaamaan yhteysdatasta käyttäjien julkiset avaimet Ya ja Yb

Hän ei kykene ratkaisemaan käyttäjien yksityisiä avaimia yhtälöstä, esim. Alicen yksityistä avainta *ka* yhtälöstä

$$\mathbf{Ya} = ka * \mathbf{G}$$

Luvun ka   ratkaisemista yo. yhtälöstä kutsutaan nimellä ECDLP: Elliptic Curve Discrete Logarithm Problem. Käyrillä P-192 tai P-256, jota esim. suomalaiset verkkopankit käyttävät, luvun ka ratkaiseminen kestänee satoja vuosia Brute Force menetelmällä.

ECC:n turvallisuus perustuu siis Ellptisten käyrien Diskreetin Logaritmin ongelman

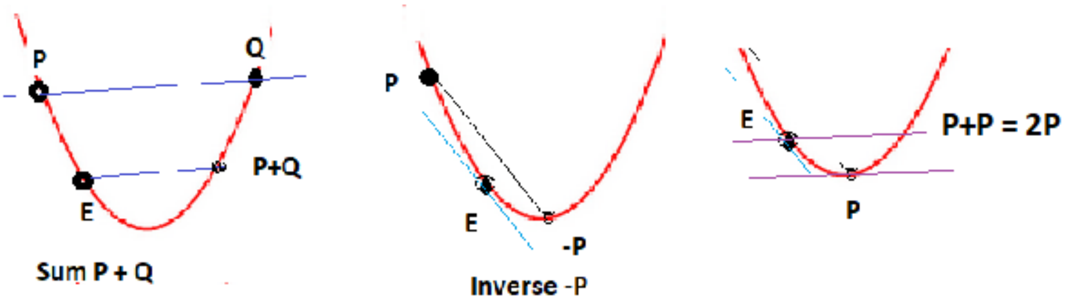
matemaattiseen vaikeuteen.

8. Syklisiä ryhmiä on myös 2. asteen käyrillä (DH and Elgamal)

Myös 2. asteen käyrillä (mm. ellipsi ja parabeli) on syklisiä ryhmiä
kun pisteiden yhteenlasku määritellään sopivalla tavalla.

1. Käyrän mielivaltainen piste E=(e1,e2) otetaan **neutraalialkioksi**.
2. S**um P + Q** on käyrän ja sellaisen suoran leikkauspiste, joka on samansuuntainen janan PQ kanssa
ja kulkee pisteen E kautta.
3. **Tuplaus 2P ja käänteisalkio -P** määritellään kuvan osoittamalla tavalla

Esim: parrabeli $y = x^2$



Voidaan osoittaa, että näin määriteltynä kyseessä on ryhmä.

Piteiden summa kaavoina P + Q

Suoran kulmakerroin $\lambda = \frac{y2-y1}{x2-x1}$

Summan P + Q koordinaatit $x = \lambda - e1$

$y = x^2$

Jos P = Q (kuten on laskettaessa tuloa 2P) , kulmakerroin $\lambda = 2x1$

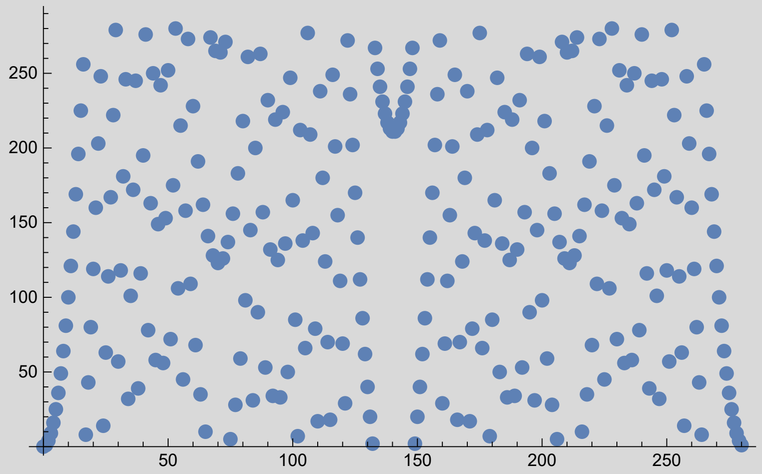
Diskretisointi äärelliseen kuntaan F_q

Alla ovat pisteet käyrälle y = x^2 mod 281

```
q = 281; pts = {};
For[x = 0, x < q, x++,
 For[y = 0, y < q, y++,
  If[Mod[y - x^2, q] == 0, pts = Append[pts, {x, y}]]]]
pts // StandardForm
```

```
{{0, 0}, {1, 1}, {2, 4}, {3, 9}, {4, 16}, {5, 25}, {6, 36}, {7, 49}, {8, 64},
 {9, 81}, {10, 100}, {11, 121}, {12, 144}, {13, 169}, {14, 196}, {15, 225},
 {16, 256}, {17, 8}, {18, 43}, {19, 80}, {20, 119}, {21, 160}, {22, 203},
 {23, 248}, {24, 14}, {25, 63}, {26, 114}, {27, 167}, {28, 222}, {29, 279},
 {30, 57}, {31, 118}, {32, 181}, {33, 246}, {34, 32}, {35, 101}, {36, 172},
 {37, 245}, {38, 39}, {39, 116}, {40, 195}, {41, 276}, {42, 78}, {43, 163},
 {44, 250}, {45, 58}, {46, 149}, {47, 242}, {48, 56}, {49, 153}, {50, 252},
 {51, 72}, {52, 175}, {53, 280}, {54, 106}, {55, 215}, {56, 45}, {57, 158},
 {58, 273}, {59, 109}, {60, 228}, {61, 68}, {62, 191}, {63, 35}, {64, 162},
 {65, 10}, {66, 141}, {67, 274}, {68, 128}, {69, 265}, {70, 123}, {71, 264},
 {72, 126}, {73, 271}, {74, 137}, {75, 5}, {76, 156}, {77, 28}, {78, 183},
 {79, 59}, {80, 218}, {81, 98}, {82, 261}, {83, 145}, {84, 31}, {85, 200},
 {86, 90}, {87, 263}, {88, 157}, {89, 53}, {90, 232}, {91, 132}, {92, 34},
 {93, 219}, {94, 125}, {95, 33}, {96, 224}, {97, 136}, {98, 50}, {99, 247},
 {100, 165}, {101, 85}, {102, 7}, {103, 212}, {104, 138}, {105, 66}, {106, 277},
 {107, 209}, {108, 143}, {109, 79}, {110, 17}, {111, 238}, {112, 180},
 {113, 124}, {114, 70}, {115, 18}, {116, 249}, {117, 201}, {118, 155},
 {119, 111}, {120, 69}, {121, 29}, {122, 272}, {123, 236}, {124, 202},
 {125, 170}, {126, 140}, {127, 112}, {128, 86}, {129, 62}, {130, 40}, {131, 20},
 {132, 2}, {133, 267}, {134, 253}, {135, 241}, {136, 231}, {137, 223},
 {138, 217}, {139, 213}, {140, 211}, {141, 211}, {142, 213}, {143, 217},
 {144, 223}, {145, 231}, {146, 241}, {147, 253}, {148, 267}, {149, 2},
 {150, 20}, {151, 40}, {152, 62}, {153, 86}, {154, 112}, {155, 140}, {156, 170},
 {157, 202}, {158, 236}, {159, 272}, {160, 29}, {161, 69}, {162, 111},
 {163, 155}, {164, 201}, {165, 249}, {166, 18}, {167, 70}, {168, 124},
 {169, 180}, {170, 238}, {171, 17}, {172, 79}, {173, 143}, {174, 209},
 {175, 277}, {176, 66}, {177, 138}, {178, 212}, {179, 7}, {180, 85}, {181, 165},
 {182, 247}, {183, 50}, {184, 136}, {185, 224}, {186, 33}, {187, 125},
 {188, 219}, {189, 34}, {190, 132}, {191, 232}, {192, 53}, {193, 157},
 {194, 263}, {195, 90}, {196, 200}, {197, 31}, {198, 145}, {199, 261},
 {200, 98}, {201, 218}, {202, 59}, {203, 183}, {204, 28}, {205, 156}, {206, 5},
 {207, 137}, {208, 271}, {209, 126}, {210, 264}, {211, 123}, {212, 265},
 {213, 128}, {214, 274}, {215, 141}, {216, 10}, {217, 162}, {218, 35},
 {219, 191}, {220, 68}, {221, 228}, {222, 109}, {223, 273}, {224, 158},
 {225, 45}, {226, 215}, {227, 106}, {228, 280}, {229, 175}, {230, 72},
 {231, 252}, {232, 153}, {233, 56}, {234, 242}, {235, 149}, {236, 58},
 {237, 250}, {238, 163}, {239, 78}, {240, 276}, {241, 195}, {242, 116},
 {243, 39}, {244, 245}, {245, 172}, {246, 101}, {247, 32}, {248, 246},
 {249, 181}, {250, 118}, {251, 57}, {252, 279}, {253, 222}, {254, 167},
 {255, 114}, {256, 63}, {257, 14}, {258, 248}, {259, 203}, {260, 160},
 {261, 119}, {262, 80}, {263, 43}, {264, 8}, {265, 256}, {266, 225}, {267, 196},
 {268, 169}, {269, 144}, {270, 121}, {271, 100}, {272, 81}, {273, 64},
 {274, 49}, {275, 36}, {276, 25}, {277, 16}, {278, 9}, {279, 4}, {280, 1}}
```

```
ListPlot[pts, PlotStyle → PointSize[0.02]]
```



Summafunktio P + Q   (neutraalialkioksi valittu E = (34,32))

```
parabSum[q_, P_List, Q_List] :=
 Module[ {λ, x3, y3, P3},
  Which[P == {34, 32}, R = Q,
   Q == {34, 32}, R = P,
   P ≠ Q,
   λ = Mod[(Q[[2]] - P[[2]]) * PowerMod[Q[[1]] - P[[1]], -1, q], q];
   x3 = Mod[λ - 34, q];
   y3 = Mod[x3 * x3, q];
   R = {x3, y3},
   (P == Q) ∧ (P ≠ {34, 32}),
   λ = Mod[ 2 * P[[1]], q];
   x3 = Mod[λ - 34, q];
   y3 = Mod[x3 * x3, q];
   R = {x3, y3}];
  R]
```

Testi1: Lasketaan summa (281,35) + (225,45).

```
P = {218, 35}; Q = {225, 45}; q = 281;
parabSum[q, P, Q]
```

```
{128, 86}
```

Testi2: Kokeillaan neutraatialkion E = (34,32) lisäämistä

```
e = {34, 32}; P = {218, 35}; q = 281;
parabSum[q, {218, 35}, e]
```

```
{218, 35}
```

```
parabSum[q, e, {218, 35}]
```

```
{218, 35}
```

Testi3: Pisteen tuplaus P + P = 2P

```
P = {218, 35};
parabSum[q, P, P]
```

```
{121, 29}
```

Määritellään nopea vakiolla kertominen n P

```
fastMult[n_, P_, q_] := Module[{x, A, B},
  x = n; A = P; B = {34, 32};
  While[x > 1,
   If[OddQ[x],
     B = parabSum[q, A, B];
     x = x - 1,
     A = parabSum[q, A, A];
     x = x / 2;
    ];
  ];
  A = parabSum[q, A, B];
  A
 ]
```

Testi 4. Laske 6*(225,45)

```
Q = {225, 45};
fastMult[6, Q, q]
```

```
{56, 45}
```

Käytän y = x^2 mod 281 pisteiden lukumäärä on alkuluku 281

```
Length[pts]
```

```
281
```

=> Kaikkien pisteiden (paitsi E:n) kertaluku on 281 ja siten ne ovat ryhmän **generoivia alkioita**

Diffie Hellman key exchange käyrällä $y = x^2$ mod 281

Valitaan G = (218, 35) generoivaksi alkioksi

```
G = {218, 35};  q = 281;
a = 60;  (* Alice:n yksityinen avain *)
b = 16;   (* Bob:n yksityinen avain *)
Ya = fastMult[a, G, q]  (* Alice lähettää julkisen avaimen *)
Yb = fastMult[b, G, q]  (* Bob lähettää julkisen avaimen *)
```

```
{115, 18}
```

```
{168, 124}
```

Alice laskee symmetrisen avaimen K

```
K = fastMult[a, Yb, q]
```

```
{206, 5}
```

Bob **calculates symmetric key** K

```
K = fastMult[b, Ya, q]
```

```
{206, 5}
```

Elgamal salaus käyrällä $y = x^2$ mod 281

Alice salaa viestin m = (100, 120)

```
m = {100, 120};
K = {206, 5};
c = Mod[m * K, q]
```

```
{87, 38}
```

Bob laskee ensin purkuavaimen DK

```
DK = PowerMod[K, -1, q]
```

```
{266, 225}
```

Bob purkaa

```
Mod[c*DK, q]
```

```
{100, 120}
```