ELGAMAL ENCRYPTION SCHEME	**ELLIPTIC CURVE ENCRYPTION SCHEME**
SETUP: **1. p is a prime.** **2. g is an element of prime order q in F_p^*.** **3. The group used is $\{g^0, g^1, g^2, ..., g^{q-1}\}$.**	**SETUP:** **1. E is an elliptic curve defined over the field F_q.** **2. P is a point of prime order n in $E(F_q)$.** **3. The group used is $\{\mathcal{O}, P, 2P, ..., (n-1)P\}$.**
KEY GENERATION: **1. Select a random integer x in the interval $[2, q-2]$.** **2. Compute $y = g^x \bmod p$.** **3. The private key is x.** **4. The public key is y.**	**KEY GENERATION:** **1. Select a random integer d in the interval $[2, n-2]$.** **2. Compute $Q = dP$.** **3. The private key is d.** **4. The public key is Q.**
ENCRYPTION: **1. Represent the message M as an integer m in the interval $[2, p-2]$.** **2. Select a random integer k in the interval $[2, q-2]$.** **3. Compute $g^k \bmod p$.** **4. Compute $y^k \bmod p$.** **5. Compute ciphertext $c = m * y^k \bmod p$.** **6. Transmit $(g^k \bmod p, c)$.**	**ENCRYPTION:** **1. Represent the message M as a field element m in F_q.** **2. Select a random integer k in the interval $[2, n-2]$.** **3. Compute $kP = (x_1, y_1)$.** **4. Compute $kQ = (x_2, y_2)$.** **5. Compute ciphertext $c = m \oplus x_2$.** **6. Transmit (x_1, y_1, c).**
DECRYPTION: **1. Compute $y^k = (g^k)^x \bmod p$.** **2. Compute $m = c * (y^k)^{-1} \bmod p$.**	**DECRYPTION:** **1. Compute $(x_2, y_2) = d(x_1, y_1)$.** **2. Compute $m = c \oplus x_2$.**

Charakterystyka ciała

Jeśli wielokrotne dodawanie jedynki do siebie w ciele F_p nigdy nie da zera, to mówimy, że ciało F ma charakterystykę *zero*; w takim przypadku ciało F zawiera kopię ciała liczb wymiernych. W przeciwnym razie istnieje taka liczba pierwsza p, że suma 1+1+ ... +1 (p razy) jest równa) i liczbę p nazywamy *charakterystyka ciała F*. W tym przypadku ciało F zawiera kopię ciała $\mathbb{Z}/p\mathbb{Z}$, które nazywamy jego podciałem prostym.

Elementami $\mathbb{Z}/m\mathbb{Z}$ mającymi elementy odwrotne ze wzgledu na mnożenie są klasy liczb względnie pierwszych z m, tzn. liczbami a, dla których $\exists$ liczba b taka, że $ab \equiv 1 (mod\ m)$, są dokładnie te liczby a, dla których $NWD(a,m)=1$. Ponadto, jesli $NWD(a,m)=1$, to taka liczba odwrotna b może być znaleziona za pomocą 0(log m) operacji na bitach.

The Weierstrass equation for an elliptic curve:

$$y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6 \qquad (2.1)$$

If $a_1, a_2, a_3, a_4, a_6 \in K$, then E is said to be defined over K.

Define the quantities: $d_2 = a_1^2+4a_2$ $\qquad d_4 = 2a_4+a_1a_3$ $\qquad d_6 = a_3^2+4a_6$

$$d_8 = a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2 \qquad c_4 = d_2^2-24d_4$$

$$\Delta = -d_2^2d_8-8d_4^3-27d_6^2+9d_2d_4d_6 \qquad (2.9)$$

$$j(E) = c_4^3/\Delta \qquad (2.10)$$

If $char(K) \neq 2$, then admissible change of variables

$$(x,y) \rightarrow (x, y - a_1x/2 - a_3/2)$$

transforms E/K to the curve

$$y^2 = x^3+b_2x^2+b_4x+b_6.$$

If $char(K) \neq 2,3$, then admissible change of variables

$$(x,y) \rightarrow ((x-3b_2)/36, y/216)$$

futher transforms E/K to the curve

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

$$\Delta = -16(4a^3+27b^2)$$

$char(K) = 2 \rightarrow j(E) = (a_1)^{12}/\Delta$

If $j(E)\neq 0$, then admissible change of variables

$$(x,y) \rightarrow (a_1^2 x+a_3/a_1, a_1^3 y+(a_1^2 a_4+a_3^2)/a_1^3)$$

transforms E to the curve

$$y^2+xy = x^3+a_2x^2+a_6 \qquad (2.12)$$

If $j(E)=0$, then admissible change of variables

$$(x,y) \rightarrow (x+a_2, y)$$

transforms E to the curve

$$y^2+a_3y = x^3+a_4x+a_6 \qquad (2.13)$$

We denote the number of points in $E(F_q)$ by $\#E(F_q)$.
Th. 2.8 (Hasse) Let $\#E(F_q)=q+1-t$. Then $|t| \leq 2\sqrt{q}$.
The elliptic curve E is said to be supersingular if p divides t, where $\#E(F_q)=q+1-t$. Otherwise, it is called non-supersingular.
It is well-known that if $p=2$ or if $p=3$, then E is supersingular $\Leftrightarrow j(E)=0$.
The curve E/F_p: $y^2=x^3+ax+b$ is said to be supersingular if $\#E/F_p=p+1$; otherwise it is non-supersingular.

$\forall P,Q \in K$

- $\vartheta+P = P$ **and** $P+\vartheta=P$. **(So ϑ serves as the identity element.)**
- $-\vartheta=\vartheta$.
- **If** $P=(x_1,y_1)\neq\vartheta$, **then** $-P=(x_1,-y_1-a_1x_1-a_3)$
- **If** $Q=-P$, **then** $P+Q=\vartheta$.
- **If** $P\neq\vartheta$, $Q'\neq\vartheta$, $Q\neq -P$, **then let R be the third point of intersection (counting multiplicities) of either the line PQ if $P\neq Q$, or the tangent line to the curve at P if $P=Q$, with the curve. Then $P+Q=R$.**

$P(x_1,y_1)$ $Q(x_2,y_2)$ $R(x_3,y_3)$

$x_3=\lambda^2+a_1\lambda-a_2-x_1-x_2$ $\qquad y_3=-(\lambda+a_1)x_3-\beta-a_3$ $\qquad \beta=y_1-\lambda x_1$

$$\lambda = \begin{cases} \dfrac{y_2-y_1}{x_2-x_1}, & P \neq Q \\ \dfrac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3}, & P = Q \end{cases}$$

Elliptic Curves over F_p

$p>3$ - a prime number $a,b \in F_p$ such that $4a^3+27b^2 \neq 0$ in F_p
An elliptic curve $E(F_p)$ over F_p is the set solutions (x,y) $(x,y \in F_p)$ to the equation

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

together with an extra point ϑ, the point at *infinity*.

Rule for adding two distinct points that are not inverses of each other:

$(x_1,y_1), (x_2,y_2) \in E(F_p)$, $x_1 \neq x_2$. **Then** $(x_3,y_3) = (x_1,y_1) + (x_2,y_2)$, **where**
$x_3 = \lambda^2 - x_1 - x_2$ $\quad y_3 = \lambda(x_1-x_3)-y_1$ $\quad \lambda = (y_2-y_1)/(x_2-x_1)$.

Rule for doubling a point:

$(x_1,y_1) \in E(F_p)$ **be a point with** $y_1 \neq 0$. **Then** $(x_3,y_3) = 2(x_1,y_1)$, **where**
$x_3 = \lambda^2 - 2x_1$ $\quad y_3 = \lambda(x_1-x_3)-y_1$ $\quad \lambda = (3x_1^2+a)/(2y_1)$

The curve is said to be *supersingular* if $\#E(F_p) = p+1$; otherwise it is *non-supersingular*.

Division in a Finite Field
$a,b \in F_q$, $b \neq 0$, then the quotient a/b is the element c such that $a = bc$. The quotient can be found efficiently using exponentiation $c = ab^{q-2} \pmod q$.

Finding Square Roots Modulo a Prime
p - odd prime g - an integer $0<g<p$.
If $g^{(p-1)/2} = 1 \pmod p$ then g has a square root (mod p), i.e., there exists an integer y such that $y^2 = g \pmod p$.
If $g^{(p-1)/2} = -1 \pmod p$ then g does not have a square root (mod p). (One of the above two possibilities must hold.)
If a square root does exist, it can be found efficiently as follows.

- **If $p=3 \pmod 4$, that is $p=4u+3$ then a square root of g modulo p can be obtained by computing $y = g^{u+1} \bmod p$.**
- **If $p=5 \pmod 8$, that is $p=8u+5$ then a square root of g modulo p can be obtained by computing $\gamma = (2g)^u \bmod p$, $i = 2g\gamma^2 \bmod p$, $y = g\gamma(i-1) \bmod p$.**

A general method: find $\wp$ such that $\wp^2-4g$ does not have a square root (mod p). Set $\wp=g$; then a square root y of g modulo p is found using the Lucas sequence: $y = \frac{1}{2} V_{(p+1)/2} \pmod p$.

Generating Lucas Sequences

$\mathcal{P}$ and $\mathcal{Q}$ - nonzero integers such that $\Delta = \mathcal{P}^2-4\mathcal{Q}$ is nonzero. The *Lucas sequence* V_k for $\mathcal{P}$, $\mathcal{Q}$ is defined by $V_0 = 2$, $V_1 = \mathcal{P}$, and $V_k = \mathcal{P}V_{k-1} - \mathcal{Q}V_{k-2}$ for k≥2.

Elliptic Curves over K=2^m

j(E)≠0

$$y^2+xy = x^3+a_2x^2+a_6 \qquad \Delta = a_6 \qquad j(E) = 1/a_6$$

***P* = $(x_1,y_1)\in E$; then *-P* = (x_1,y_1+x_1).**

If *Q* = $(x_2,y_2)\in E$ and $Q \neq -P$, then *P+Q* = (x_3,y_3), where

$$x_3 = \begin{cases} \left(\frac{y_1 + y_2}{x_1 + x_2}\right)^2 + \frac{y_1 + y_2}{x_1 + x_2} + x_1 + x_2 + a_2, P \neq Q \\ x_1^2 + \frac{a_6}{x_1^2}, P = Q \end{cases}$$

and

$$y_3 = \begin{cases} \left(\frac{y_1 + y_2}{x_1 + x_2}\right)(x_1 + x_3) + x_3 + y_1, P \neq Q \\ x_1^2 + \left(x_1 + \frac{y_1}{x_1}\right)x_3 + x_3, P = Q \end{cases}$$

Elliptic Curves over $K=2^m$

j(E)=0

$$y^2+a_3y = x^3+a_4x+a_6 \qquad \Delta = a_3^4$$

***P* = $(x_1,y_1)\in E$; then *-P* = (x_1,y_1+a_3).**

If *Q* = $(x_2,y_2)\in E$ and $Q \neq -P$, then $P+Q = (x_3,y_3)$, where

$$x_3 = \begin{cases} \left(\dfrac{y_1+y_2}{x_1+x_2}\right)^2 + x_1 + x_2, P \neq Q \\ \dfrac{x_1^4 + a_4^2}{a_3^2}, P = Q \end{cases}$$

and

$$y_3 = \begin{cases} \left(\dfrac{y_1+y_2}{x_1+x_2}\right)(x_1+x_3) + y_1 + a_3, P \neq Q \\ \left(\dfrac{x_1^2 + a_4}{a_3}\right)(x_1+x_3) + y_1 + a_3, P = Q \end{cases}$$

m=4

Field $F(2^m)$ has type I

Non-reducible polinom (from m to 0)
1 1 1 1 1

If $F(2^m)$ has a type I ONB then f(x) = x^m + ... + x + 1.
If $F(2^m)$ has a type II ONB then compute $f(x)=f_m(x)$ using following recursive formulae: $f_0(x) = 1$, $f_1(x) = x + 1$, $f_{i+1}(x) = xf_i(x) + f_{i-1}(x)$, $i \geq 1$.

Matrix A

0 0 1 0
0 1 0 0
1 1 1 1
1 0 0 0

i-th row of matrix A, $0 \le i \le m-1$ is the bit string corresponding to the polynomial $x^{2^{\wedge}i}$ mod f(x).

Matrix Am1

0 0 0 1
0 1 0 0
1 0 0 0
1 1 1 1

The inverse matrix A^{-1} of A.

Matrix V

0 1 0 0
1 0 0 0
0 0 0 1
1 1 1 1

i-th row of matrix V is obtained as follows. First compute the polynomial $x*x^{2^{\wedge}i}$ mod f(x) and the corresponding bit string is i-th row of matrix V.

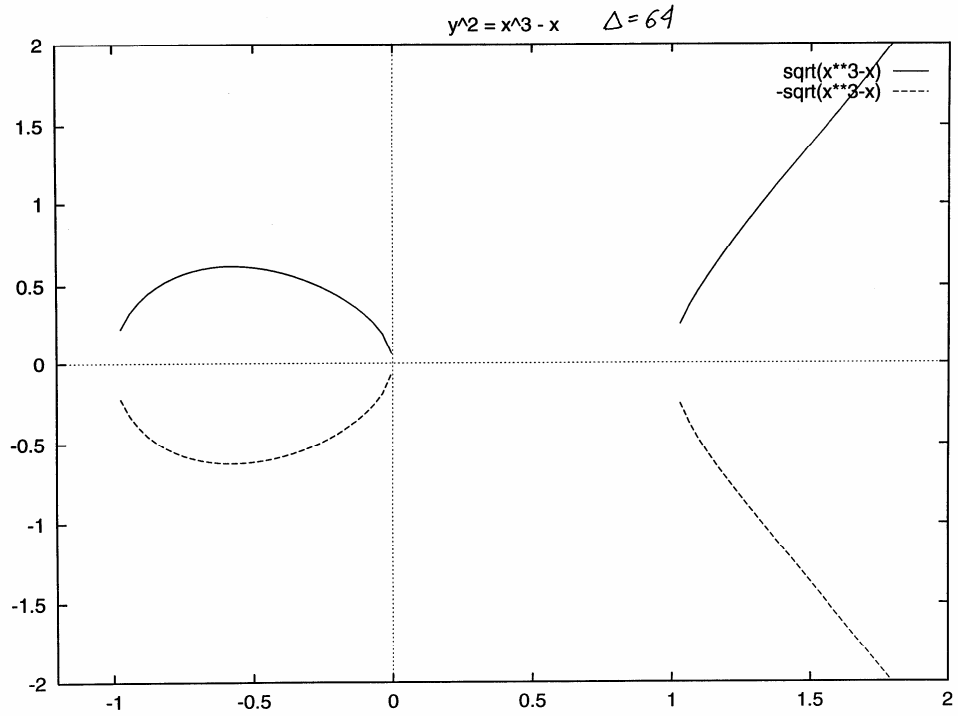
Matrix T

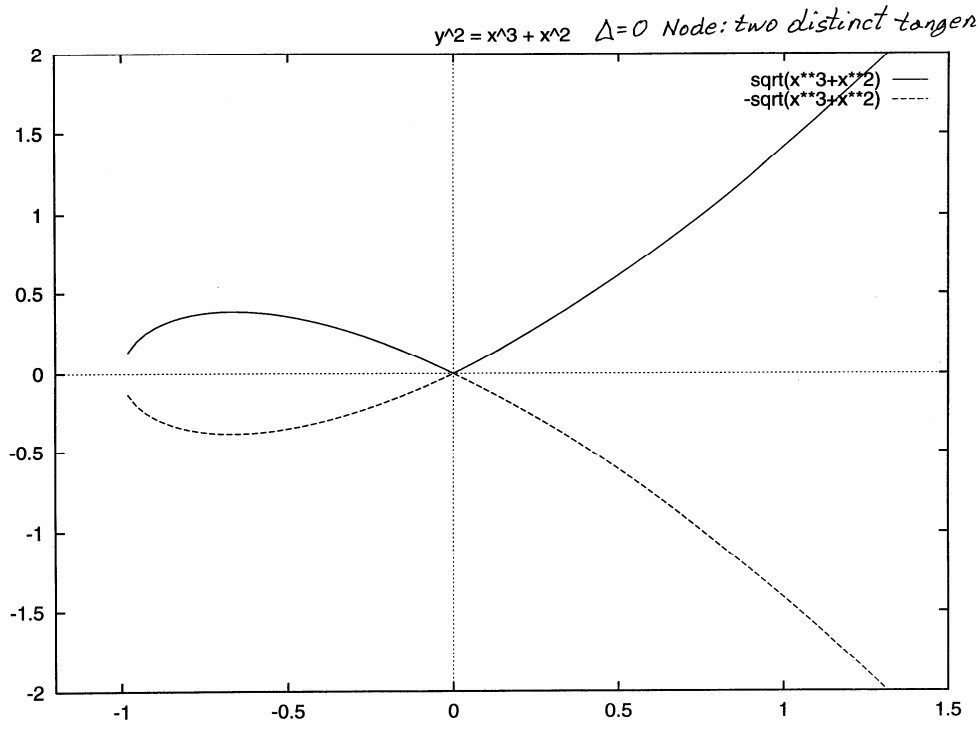
0 1 0 0
0 0 0 1
1 1 1 1
0 0 1 0

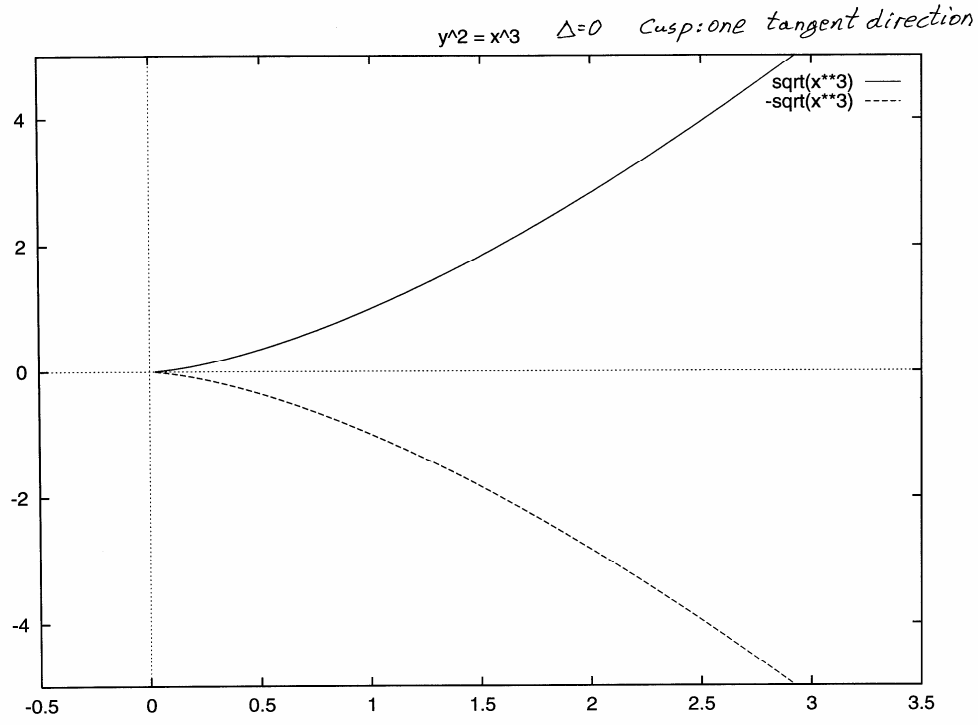
The matrix $T = V*A^{-1}$

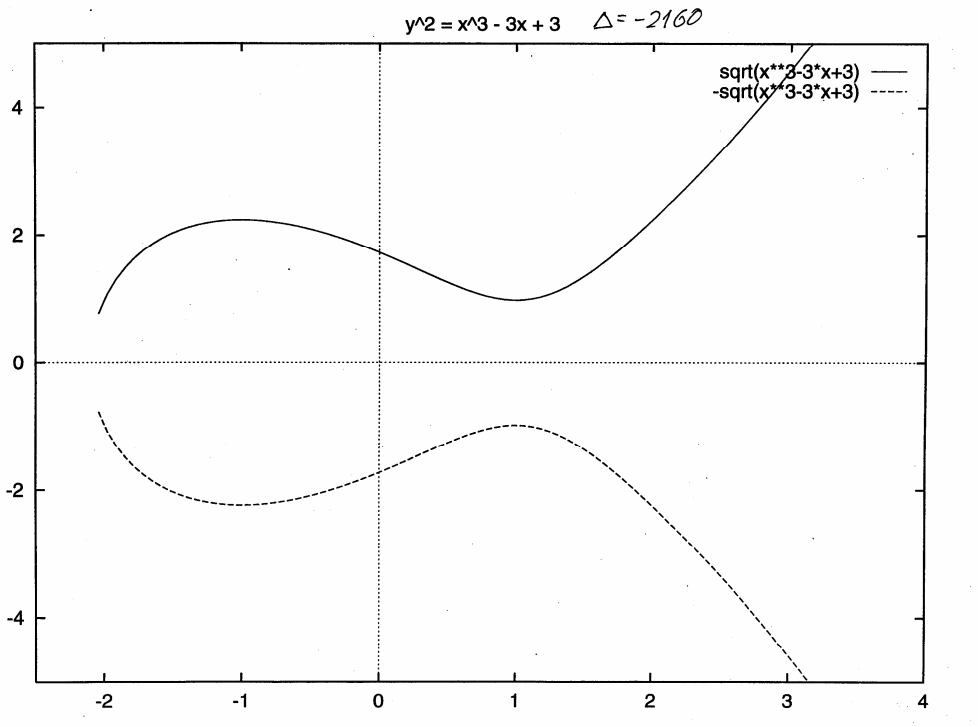
Non-zero lambda
L[0,2]=1
L[1,2]=1 L[1,3]=1
L[2,0]=1 L[2,1]=1
L[3,1]=1 L[3,3]=1

The product terms λ_{ij}, for $0 \le i,j \le m-1$: $\lambda_{ij}=T(j-i,-i)$. Here, T(i,j) denotes (i,j)-entry of T with indices reduced modulo m. Each product term λ_{ij} is an element of F_2. It should also be the case that $\lambda_{ij}=1$ for precisely one j, $0 \le j \le m-1$ and that for each i, $0 \le i \le m-1$, $\lambda_{ij}=1$ for precisely two distinct j, $0 \le j \le m-1$. Hence exactly 2m-1 of the m^2 entries of the matrix T are 1, the rest being 0.


y^2 = x^3 - x
Δ = 64
sqrt(x**3-x)
-sqrt(x**3-x)
2
1.5
1
0.5
0
-0.5
-1
-1.5
-2
-1
-0.5
0
0.5
1
1.5
2


y^2 = x^3 + x^2
Δ = 0 Node: two distinct tangent dir.
sqrt(x**3+x**2)
-sqrt(x**3+x**2)
2
1.5
1
0.5
0
-0.5
-1
-1.5
-2
-1
-0.5
0
0.5
1
1.5


y^2 = x^3 Δ=0 Cusp: one tangent direction
sqrt(x**3)
-sqrt(x**3)
4
2
0
-2
-4
-0.5
0
0.5
1
1.5
2
2.5
3
3.5


y^2 = x^3 - 3x + 3 Δ = -2160
sqrt(x**3-3*x+3)
-sqrt(x**3-3*x+3)
4
2
0
-2
-4
-2
-1
0
1
2
3
4