the solutions of an equation of the form $ax+by+c=0$ $(a,b\neq 0)$ correspond to the points of a line and those of the eq. of the form $ax^2+bxy+cy^2+dx+ey+f=0$ $(a,b,c\neq 0)$ give a conic section (ellipse, hyperbola, parabola)

we can also take a third grade equation:

$$ax^3+bx^2y+cxy^2+dy^3+ex^2+fxy+gy^2+hx+iy+i=0 \quad (a,b,c,d\neq 0)$$

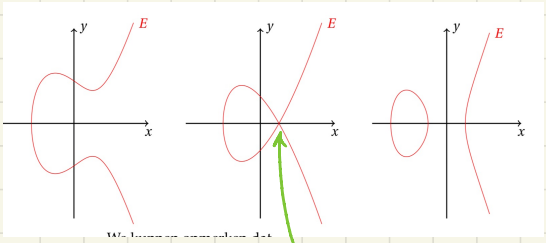
the set of points in the plain that satisfies the equation is an elliptic curve

Via projective transformation we can represent it in the Weierstrass normal form:

$y^2=x^3+ax+b$ $a,b\in\mathbb{R}$ costants

the function has exactly 1 or 2 or 3 zeroes.

We have the following graphs



symmetric from x axis because $y=\sqrt{x^3+ax+b}$ and $y=-\sqrt{x^3+ax+b}$ are both solutions

special happens if discriminant $\Delta=-16(4a^3+27b^2)=0$

we will work only with curves with $\Delta\neq 0$

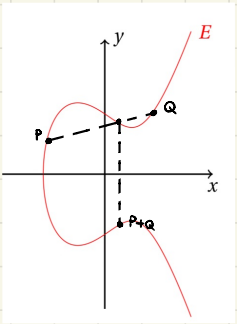
Arithmetical operations

We look at elliptic curves of the form $y^2 = x^3 + ax + b$ (with $a, b \in \mathbb{Z}$, $4a^3 + 27b^2 \neq 0$)

We had a fictional point of infinity on the y-axis ($\mathcal{O}$)

Then the elliptic curve is: $E = \{(x,y) \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$

We'll define "+" using a geometric construct, for $P+Q$



- $P \neq Q$: addition

  Draw line passing through P and Q and take the intersection with E

  Mirror the intersection in respect to the x-axis, that is $P+Q$

- $P = Q$: doubling

  Draw tangent to P and take the intersection with E. Mirror to x-axis: $2P$

special cases

- $\mathcal{O} + P = P$
- if P and Q are symmetrical in respect of the x-axis $P+Q = \mathcal{O}$, $P = -Q$
- if $P \in$ x-axis $2P = \mathcal{O}$

then everything needed for defining addition is:

a) $\forall P, Q \in E : P+Q \in E$

b) $\forall P, Q \in E : P+Q = Q+P$

c) $\forall P, Q \in E : (P+Q)+R = P+(Q+R)$

d) $\forall P \in E : P+\mathcal{O} = \mathcal{O}+P = P$

e) $\forall P \in E, \exists Q : P+Q = \mathcal{O}$

$E+$ is a commutative group

with $P=(x_1,y_1)$, $Q=(x_2,y_2)$ and $R=(x_3,y_3)$ $R = P+Q$ if $\begin{cases} x_3 = s^2 - x_1 - x_2 \\ y_3 = s(x_1 - x_3) - y_1 \end{cases}$

where $s = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & \text{if } P = Q \end{cases}$

special cases:

- $(x_1, y_1) + (x_1, -y_1) = \mathcal{O}$
- $(x_1, y_1) + \mathcal{O} = (x_1, y_1)$
- $2(x_1, 0) = \mathcal{O}$

Elliptic curves modulo P

Do the above work in $\mathbb{F}_p$ instead of $\mathbb{R}$, change the definition to:

an elliptic curve E over $\mathbb{F}_p$, with $p>3$, is the set of points $(x,y) \in \mathbb{F}_p^2$ so that

$E: y^2 \equiv x^3+ax+b \pmod p$ to which we also add $\mathcal{O}$

$\{a,b \in \mathbb{F}_p \mid 4a^3+27b^2 \not\equiv 0 \pmod p\}$

The formulas still work but it's harder to represent geometrically

$(x_3,y_3)=(x_1,y_1)+(x_2,y_2)$ if

$$\begin{cases} x_3 = s^2 - x_1 - x_2 \pmod p \\ y_3 = s(x_1 - x_3) - y_1 \pmod p \end{cases}$$

$$s = \begin{cases} (y_2-y_1)(x_2-x_1)^{-1} \pmod p & \text{if } P \neq Q \\ (3x_1^2+a)(2y_1)^{-1} \pmod p & \text{if } P = Q \end{cases}$$

example:

$y^2 = x^3+2x+2 \pmod{17}$

$E = \{\mathcal{O}, (0,6), (0,11), (3,1), (3,16), (5,1), (5,16), (6,3), (6,14), (7,6), (7,11), (9,1), (9,16), (10,6), (10,11), (13,7), (13,10), (16,4), (16,13)\}$

we find a group of 19 points

take $P=(6,3)$, $Q(16,13)$ $\quad P+Q=(13,7)$

$s = (13-3)(16-6)^{-1} \equiv 10 \cdot 10^{-1} \equiv 1 \pmod{17}$

$x_3 \equiv 1^2 - 16 - 6 \equiv -21 \equiv 13 \pmod{17}$

$y_3 \equiv 1(6-13) - 3 \equiv -10 \equiv 7 \pmod{17}$

$2P \rightarrow \quad s = (3 \cdot 6^2+2)(2 \cdot 3)^{-1} = 8 \cdot 6^{-1} \equiv 8 \cdot 3 \equiv 24 \equiv 7 \pmod{17}$

$x_3 = 7^2 - 2 \cdot 6 \equiv 37 \equiv 3 \pmod{17}$

$y_3 = 7(6-3) - 3 \equiv 18 \equiv -1 \pmod{17}$

Discrete logarithm on elliptic curves

$P=(0,6)$ as a basis point then we calculate all points of E as $K\cdot P = \underbrace{P+P+P\ldots+P}_{K \text{ times}}$

with $1<K\leqslant 19$

$2P=(9,1)$	$8P=(5,16)$	$14P=(10,6)$
$3P=(6,3)$	$9P=(16,13)$	$15P=(7,11)$
$4P=(7,6)$	$10P=(16,4)$	$16P=(6,14)$
$5P=(10,11)$	$11P=(5,1)$	$17P=(9,16)$
$6P=(3,1)$	$12P=(13,7)$	$18P=(0,11)$
$7P=(13,10)$	$13P=(3,16)$	$19P=\mathcal{O}$

we can speak of a cyclic group with 19 elements generated by (0,6).

$(6,3)+(16,13)=3P+9P=12P=(13,7)$ en $2\cdot(6,3)=2\cdot 3P=6P=(3,1)$.

we can also note that $K\cdot P$ is the inverse of $l\cdot p$ if $K+l\equiv 0 \pmod q$ with $q=|E|$

Determining the size of E,+ is difficult, but we get an approximation with the following theorem

Hasse's theorem

given an elliptic curve E modulo p, then the number of points on that curve is named #E and is delimited by:

$$p+1-2\sqrt{p}\leqslant \#E\leqslant p+1+2\sqrt{p}$$

So we see p determine more or less the size of p.

The group is not always cyclical. But we always have sub groups that are.

We can think like powermod to accelerate calculating $K\cdot P$

algorithm: calculating $K\cdot P$ by repeated doubling

write K in binary $K=(K_m K_{m-1}\ldots K_1 K_0)_2$

```
T:=P
for (i=m-1; i>=0; i--){
    T:=2T (mod p)          <- step 1
    if Ki=1{
        T:=T+P (mod p)     <- step 2
    }
}
```

example: $37\cdot P$ $37=(100101)_2$

i	5	4	3	2	1	0
T(at step 1)	$\mathcal{O}$	2P	4P	8P	18P	36P
ui	1	0	0	1	0	1
y (at step 2)	P	2P	4P	9P	18P	37P

this is actually a good one way function (ECDLP)

ECDLP

Given an elliptic curve $E \pmod p$, where P is the generator of $E,+$ and an arbitrary point $Y \in E$ is given

The elliptic curve discrete logarithm problem (ECDLP) consists of the search for

$$d \in \{1, 2, 3 \dots \#E\} \mid Y = d \cdot P$$

In assymmetric cryptography d can serve as the private key, Y part of the public key.

Curve Diffie Hellman (ECDH)

make some adjustments to the previous form

1) Alice and Bob agree on an elliptic curve E over a fixed prime number p and a generator P of (a subgroup of) $E,+$
2) Alice determines a secret key $\underline{a} \in \{1, 2, \dots \#E\}$, Bob same with $\underline{b}$
3) Alice calculates $A = \underline{a} \cdot P$ and sends it to Bob
4) Bob calculates $B = \underline{b} \cdot P$ " "
5) Alice calculates $C_1 = \underline{a} \cdot B$, Bob $C_2 = \underline{b} \cdot A$
6) Since

$$C_1 = a \cdot B = a \cdot b \cdot T = (ab)T$$

and

$$C_2 = b \cdot A = b \cdot a \cdot T = (ab)T$$

if $C_1 = C_2$ they agreed

~ · ~ · ~ · ~ · ~ · ~ · ~ · ~ · ~ · ~

We can also create a variant of ECDH to provide encryption and decryption

- Alice wants to send a message to Bob
- Bob uses an elliptic curve E modulo p and a generator point P
- Bob makes a private key $K_b \in \mathbb{N}$ and a public $K_B = K_b \cdot P \in E$

Alice does the following

- chooses a disposable private key $K_a \in \mathbb{N}$ and a disposable public key $K_A = K_a \cdot P \in E$
- converts m to a point $P_m \in E$ and calculates $Q = P_m + (K_a \cdot K_B)$ in E
- forwards the combination (Q, K_A) to Bob. Encryption twice the size of the message

Bob can then find P_m (therefore m) via $P_m = Q - (K_b \cdot K_A)$

it works because $K_a \cdot K_B = K_a(K_b \cdot P) = K_b(K_a \cdot P) = K_b \cdot K_A$

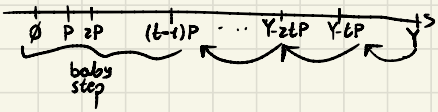
~ · ~ · ~ · ~ · ~ · ~ ·

To solve this we can use Bobs step-Giant step. But not index calculus

example Baby step giant step

replace multiplication with the group's addition, replace exponential with scalar multiplication ($K \cdot P$

well' use an interval of $t = \lceil \sqrt{\#E} \rceil$, so for the theorem of Hasse $t = \lceil \sqrt{p+1+2\sqrt{p}} \rceil = \lceil \sqrt{p}+1 \rceil$



let's take for example $y^2 = x^3 + 3x + 3 \pmod{67}$

$\Delta = -16(4 \cdot 3^3 + 27 \cdot 3^2) \equiv 12 \pmod{67}$

take $P = (3,21)$ as fixed point (generator of E), and $Y = (20,31)$

Determine K for which $Y = K \cdot P$

For the theorem of Hasse we know that $\#E \leq 68 + 2\sqrt{67} = 84.37$. So $K \in \{1, 2, \dots 84\}$

$\lceil \sqrt{84} \rceil = 10$, so we calculate 10 baby steps

i	0	1	2	3	4	5	6	7	8	9
$i \cdot P$	$\mathcal{O}$	(3,21)	(41,38)	(29,52)	(50,8)	(30,5)	(2,33)	(5,3)	(6,6)	(16,44)

sort them by x-coordinate

i	0	6	1	7	8	9	3	5	2	4
$i \cdot P$	$\mathcal{O}$	(2,33)	(3,21)	(5,3)	(6,6)	(16,44)	(29,52)	(30,5)	(41,38)	(50,8)

$Y = (20,31)$ is not in the list so we have to do giant steps

the steps are done by adding multiples of $-10P = -(10P) = -(21,9) = (21,58)$ to Y

until we encounter element from the previous list

j	0	1	2	3	4	5
$(20,31) + j \cdot (21,58)$	(20,31)	(18,23)	(45,64)	(22,59)	(25,5)	(50,8)

so we find

$Y + 5(-10P) = 4P \rightarrow Y = 50P + 4P = Y = 54P$