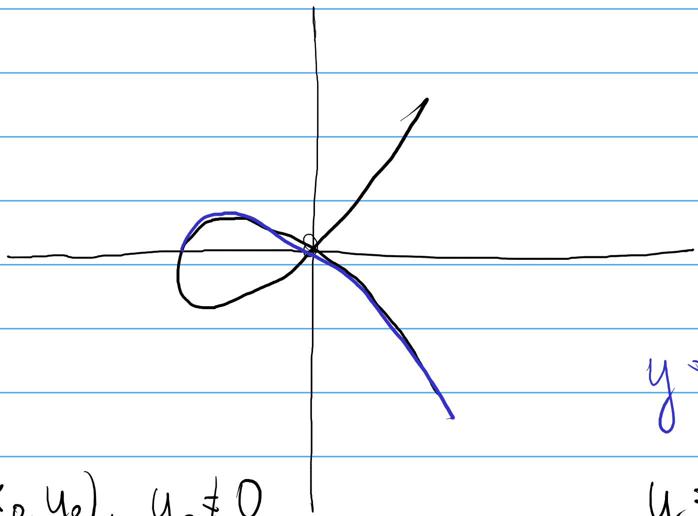
Tečna v nesingulárním bodě P:

$$\frac{\partial F}{\partial X}(P)X + \frac{\partial F}{\partial Y}(P)Y + \frac{\partial F}{\partial Z}(P)Z = 0$$

nad $\mathbb{R}$:

$$y^2 = x^2 \cdot (x+a), \quad a \neq 0, a > 0$$



$y = -x\sqrt{x+a}$

$y = x\sqrt{x+a}$

$P = (x_0, y_0), \ y_0 \neq 0$

$$2yy' = 3x^2 + 2ax$$

$$y' = \frac{3x^2+2ax}{2y}$$

$y' = -\sqrt{x+a} - x \cdot \frac{1/2}{\sqrt{x+a}}$

v bodě $(0,0)$ je směrnice tečny: $-\sqrt{a}$

$y' = \sqrt{x+a} + x\frac{1/2}{\sqrt{x+a}}$

směrnice: $\sqrt{a}$

Buď C křivka zadaná Weierstrassovou rovnicí:

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

pro vhodná $a_1, a_2, a_3, a_4, a_6 \in K$. Předpokládejme, že bod $P = (x_0, y_0)$ je singulární bod křivky C, tedy

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.$$

Pak Taylorův rozvoj polynomu $f(x,y)$ v P je tvaru

$$f(x,y) - f(x_0,y_0) = \big((y-y_0) - \alpha(x-x_0)\big)\cdot\big((y-y_0) - \beta(x-x_0)\big) - (x-x_0)^3$$

pro vhodná $\alpha, \beta \in \overline{K}$. Pokud $\operatorname{char} K \neq 2$, pak α a β jsou kořeny polynomu

$$t^2 + \frac{\partial^2 f}{\partial x \partial y}(P)\, t + \frac{1}{2}\frac{\partial^2 f}{\partial x^2}(P) \in K[t].$$

Speciálně, je-li křivka zadaná rovnicí

$$y^2 = x^2(x+a), \quad a \neq 0,$$

pak tečny v bodě $P = (0,0)$ jsou kořeny polynomu

$$t^2 - a.$$

<u>Definice</u>

Singulární bod P se nazývá uzel (node), jestliže $\alpha \neq \beta$. V takovém případě jsou přímky dané rovnicemi

$$y - y_0 = \alpha(x - x_0) \qquad y - y_0 = \beta(x - x_0)$$

tečnami v bodě P.

Singulární bod P se nazývá hrot (cusp), jestliže $\alpha = \beta$. V takovém případě je tečna v bodě P daná rovnicí

$$y - y_0 = \alpha (x - x_0).$$

Eliptická křivka $E/\mathbb{Q}$ zadaná Weierstrassovou rovnicí

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

kde $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$, má aditivní, resp. multiplikativní redukci modulo p, jestliže modulo p má hrot, resp. uzel.

Nechť E je eliptická křivka nad $\mathbb{Q}$ daná rovnicí

$$y^2 = x(x+35)(x-55)$$

Pak

$$E \pmod 2: \quad y^2 \equiv x(x+1)^2$$
$$E \pmod 3: \quad y^2 \equiv x(x-1)^2$$
$$E \pmod 5: \quad y^2 \equiv x^3$$
$$E \pmod 7: \quad y^2 \equiv x^2 \cdot (x+1)$$
$$E \pmod{11}: \quad y^2 \equiv x^2 (x+2)$$

Křivka E má zřejmě aditivní redukci modulo 5 a multiplikativní redukci mod 7, 11. Protože 2 není kvadratický zbytek modulo 11, je tato redukce neštěpící se. Naopak, modulo 7 se jedná o štěpící se redukci. Pro $p = 3$

$$y^2 - x^3 + 2x^2 - x = 0$$

$$\underline{P = (1,0)}$$

jsou směrnice tečen kořeny polynomu

$$t^2 + 2 \in \mathbb{F}_3[t]$$
$$t^2 - 1 = (t-1)(t+1)$$

Jedná se tedy o štěpící se multiplikativní redukci.

Redukce modulo 2: Singulární bod $(1,0)$

$$f(x,y) = y^2 + x^3 + x$$

$$y^2 + x^3 + x = \big(y - \alpha(x-1)\big)\big(y - \beta(x-1)\big) - (x-1)^3$$

$$= \big(y + \alpha(x+1)\big)\big(y + \beta(x+1)\big) + x^3 + x^2 + x + 1$$

$$= y^2 + (\alpha+\beta)y(x+1) + \alpha\beta(x^2+1) + x^3 + x^2 + x + 1$$

Odtud dostaneme

$$(\alpha+\beta)y(x+1) + \alpha\beta(x^2+1) + x^2 + 1 = 0,$$

tedy $\alpha\beta = 1$ a $\alpha + \beta = 0$, neboli $\alpha = \beta$. To znamená, že E má aditivní redukci modulo 2. Pro ostatní prvočísla má E dobrou redukci.

$$(x,y) \longmapsto \left(\frac{x'}{u^2}, \frac{y'}{u^3}\right), \quad u \neq 0$$

$$y^2 = x^3 + Ax + B$$

$$\frac{(y')^2}{u^6} = \frac{(x')^3}{u^6} + A\cdot\left(\frac{x'}{u^2}\right) + B \quad \Big| \cdot u^6$$

$$(y')^2 = (x')^3 + Au^4 \cdot x' + Bu^6$$

Weierstrassova rovnice zadávající křivku E

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

se nazývá minimální Weierstrassova rovnice (minimální model), jestliže $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$ a ze všech takových rovnic má nejmenší hodnotu $|\Delta|$.

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

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

Buď $E/\mathbb{Q}$. Definujme L-funkci eliptické křivky E nekonečným součinem

$$L_E(s) = \prod_{p \mid \Delta(E)} (1 - a_p p^{-s})^{-1} \cdot \prod_{p \nmid \Delta(E)} (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

Pro libovolné p platí

$$a_p = 1 + p - A_p, \text{ kde}$$

A_p je počet bodů křivky E modulo p.

Pokud $p \mid \Delta(E)$, pak

$$a_p = \begin{cases} 0 & \text{má-li } E \text{ aditivní redukci modulo } p \\ 1 & \text{má-li } E \text{ štěpící se multiplikativní redukci mod } p \\ -1 & \text{má-li } E \text{ neštěpící se multiplikativní redukci mod } p \end{cases}$$