Nechť $\alpha_1, \alpha_2, \alpha_3 \in \overline{K}$ jsou kořeny polynomu
$$x^3 + Ax + B \qquad P_i = (\alpha_i, 0)$$
$$y^2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$$
$$\operatorname{div}\left(\frac{x}{y}\right) = ?$$
Víme, $\operatorname{ord}_\infty\left(\frac{x}{y}\right) = 1$. Stačí tedy spočítat $\operatorname{ord}_P\left(\frac{x}{y}\right)$ ve vlastních bodech.

Rozlišme dva případy:
1. Nejprve předpokládejme, že $\alpha_i \neq 0$ pro každé i.

Pak
$$\operatorname{ord}_{P_i}(x) = \operatorname{ord}_{P_i}(x - \alpha_i + \alpha_i) =$$
$$\min\{\operatorname{ord}_{P_i}(x-\alpha_i), \operatorname{ord}_{P_i}(\alpha_i)\} = \min\{2, 0\} = 0$$
a tedy
$$\operatorname{ord}_{P_i}\left(\frac{x}{y}\right) = \operatorname{ord}_{P_i}(x) - \operatorname{ord}_{P_i}(y) = 0 - 1 = -1$$
Funkce $\frac{x}{y}$ má nulu v bodech, které mají první složku nulovou (druhá pak musí být nutně nenulová). Buď $c \in K$ libovolný prvek, splňující $c^2 = B \neq 0$. Pak jediné body, které mají první složku nulovou jsou
$Q_1 = (0, c)$, $Q_2 = (0, -c)$, přičemž $c \neq 0$.

V bodech Q_1 a Q_2 je uniformizérem x, tedy

$$\mathrm{ord}_{Q_i}(x) = 1 \quad \text{pro } i = 1,2.$$

Platí

$$2\,\mathrm{ord}_{Q_i}(y) = \mathrm{ord}_{Q_i}(y^2) = \mathrm{ord}_{Q_i}(x^3+Ax+B) = 0$$

$$\mathrm{ord}_{Q_i}(x^3),\ \mathrm{ord}_{Q_i}(Ax),\ \mathrm{ord}_{Q_i}(B)$$

$$\mathrm{ord}_{Q_i}(B) = 0 < \mathrm{ord}_{Q_i}(x^3) = 3$$

$$A \neq 0 \implies \mathrm{ord}_{Q_i}(Ax) = 1$$

$$\mathrm{ord}_{Q_i}\left(\frac{x}{y}\right) = \mathrm{ord}_{Q_i}(x) - \mathrm{ord}_{Q_i}(y) = 1 - 0 = 1$$

Pak

$$\mathrm{div}\left(\frac{x}{y}\right) = [Q_1] + [Q_2] - [P_1] - [P_2] - [P_3] + [\infty]$$

2. BÚNO předpokládejme, že $e_1 = 0$. Pak jediným bodem, který má první složku nulovou je $P_1 = (e_1, 0) = (0,0)$.

$$\mathrm{ord}_{P_1}(x) = \mathrm{ord}_{P_1}(x - e_1) = 2$$

Pak $\mathrm{ord}_{P_1}\left(\frac{x}{y}\right) = \mathrm{ord}_{P_1}(x) - \mathrm{ord}_{P_1}(y) = 2 - 1 = 1$

Podobně jako v předchozím případě lze ukázat, že

$$\mathrm{ord}_{P_2}\left(\frac{x}{y}\right) = \mathrm{ord}_{P_3}\left(\frac{x}{y}\right) = -1.$$

$$\operatorname{div}\left(\frac{x}{y}\right) = [P_1] + [\infty] - [P_2] - [P_3]$$

Tvrzení
Buď E eliptická křivka a $f \in \overline{K}(E)^*$. Pak platí

1. $\operatorname{div}(f) = 0$ právě tehdy, když $f \in \overline{K}^*$
2. $\deg(\operatorname{div}(f)) = 0$.

Protože grupa hlavních divizorů je podgrupou grupy $\operatorname{Div}^0(E)$, můžeme definovat grupu tříd divizorů stupně 0 $\operatorname{Pic}^0(E)$ jako faktorgrupu grupy $\operatorname{Div}^0(E)$ podle podgrupy hlavních divizorů.

Předchozí tvrzení nám dává následující exaktní posloupnost:

$$1 \longrightarrow \overline{K}^* \longrightarrow \overline{K}(E)^* \xrightarrow{\operatorname{div}} \operatorname{Div}^0(E) \longrightarrow \operatorname{Pic}^0(E) \to 0$$

Definujme zobrazení $\varkappa : E \longrightarrow \operatorname{Pic}(E)$

$P \longmapsto$ třída obsahující divizor $[P] - [\infty]$

Tvrzení Pro libovolné $P, Q \in E$ platí

$$\varkappa(P+Q) = \varkappa(P) + \varkappa(Q)$$

Př. Buď $f = ax + by + c \in \overline{K}(E)^*$ nekonstantní funkce (tj. $a \neq 0$ nebo $b \neq 0$). Spočítejme $\mathrm{div}(f)$.

Víme, že $\mathrm{ord}_\infty(x) = -2$ a $\mathrm{ord}_\infty(y) = -3$.

Pak
$$\mathrm{ord}_\infty(f) = \begin{cases} -2, & \text{pokud } b = 0 \\ -3, & \text{pokud } b \neq 0. \end{cases}$$

1. Nejprve předpokládejme $b = 0$. Pak

$$f = a(x - x_0).$$ Označme $P = (x_0, y_0)$ bod na eliptické křivce. Je-li $y_0 \neq 0$, pak $x - x_0$ je uniformizér a platí

$$\mathrm{div}(f) = \mathrm{div}(a) + \mathrm{div}(x - x_0)$$
$$= [P] + [-P] - 2[\infty],$$
kde $-P = (x_0, -y_0)$. Pokud $y_0 = 0$, pak x_0 je kořen polynomu $x^3 + Ax + B$ a podle předchozího příkladu máme

$$\mathrm{div}(f) = \mathrm{div}(a) + \mathrm{div}(x - x_0)$$
$$= 2[P] - 2[\infty].$$

2. $b \neq 0$. Označme $P = (x_0, y_0)$ bod na eliptické křivce. Pak

$$f = ax + by + c = a(x - x_0) + b(y - y_0) + ax_0 + by_0 + c$$

Zřejmě $\mathrm{ord}_P(x - x_0) > 0$, $\mathrm{ord}_P(y - y_0) > 0$. Proto pokud $d = ax_0 + by_0 + c \neq 0$, pak

$$\mathrm{ord}_P(f) = \min\{\underbrace{\mathrm{ord}_P(x-x_0)}_{>0}, \underbrace{\mathrm{ord}_P(y-y_0)}_{>0}, \underbrace{\mathrm{ord}_P(d)}_{=0}\} = 0$$

Předpokládejme, že bod P leží na přímce $f(x,y)=0$, tj. $ax_0+by_0+c=0$. Pak x_0 je kořenem polynomu

$$g = b^2x^3 - a^2x^2 + (b^2A - 2ac)x + b^2B - c^2$$

Platí, že $\mathrm{ord}_P(f)$ je rovna násobnosti x_0 jakožto kořene polynomu.

$$g = b^2(x-x_1)(x-x_2)(x-x_3)$$

$$P_i = (x_i, y_i) \qquad y_i = \frac{-ax_i - c}{b}$$

Pak

$$\mathrm{div}(f) = [P_1] + [P_2] + [P_3] - 3[\infty]$$

<u>Tvrzení</u> Pro libovolné $P, Q \in E$ platí

$$\varkappa(P+Q) = \varkappa(P) + \varkappa(Q)$$

Dk. Je-li některý z bodů roven ∞, pak tvrzení zřejmě platí, neboť $\mathcal{H}(\infty)=0$.
Předpokládejme, že

$$P \neq Q$$

$P=(x_P, y_P)$ a $Q=(x_Q, y_Q)$. Nechť

$$f = ax+by+c \in \bar{K}[x,y]$$

je funkce zadávající přímku, jež prochází body P a Q. Rozlišíme dva případy

(1) $b \neq 0$. Označme $R=(x_R, y_R)$ třetí průsečík přímky f a eliptické křivky. Pak

$$\operatorname{div}(f) = [P]+[Q]+[R]-3[\infty].$$

Nyní označme $g = x - x_R$ funkci zadávající přímku rovnoběžnou s osou y, která prochází bodem R. Pak

$$\operatorname{div}(g) = [R] + [P+Q] - 2[\infty].$$

Proto

$$\operatorname{div}\left(\frac{f}{g}\right) = \operatorname{div}(f) - \operatorname{div}(g)$$

$$= [P]+[Q]-[P+Q]-[\infty]$$

$$= \underbrace{[P]-[\infty]} + \underbrace{[Q]-[\infty]} - ([P+Q]-[\infty])$$

$$0 = \mathcal{H}(P) + \mathcal{H}(Q) - \mathcal{H}(P+Q)$$

(2.) $b=0$. Pak $x_P = x_Q$, $a \neq 0$, a tedy

$f = a(x - x_P)$. Pak

$$\mathrm{div}(f) = \mathrm{div}(x - x_P) = [P] + [Q] - 2[\infty]$$
$$= [P] - [\infty] + [Q] - [\infty]$$

$$0 = \varkappa(P) + \varkappa(Q).$$ Přitom

$\varkappa(P+Q) = 0$, neboť $P+Q = \infty$.

$P = Q \Rightarrow$ pak f zadává tečnu v bodě P.

K tomu, abychom dokázali, že operace na eliptické křivce je asociativní, potřebujeme ukázat, že $\varkappa$ je injektivní.

Tvrzení. Buďte $P, Q \in E(\bar{K})$ a předpokládejme, že existuje funkce $f \in \bar{K}(E)^*$ taková, že

$$\mathrm{div}(f) = [P] - [Q].$$

Pak $P = Q$.