Příklad racionální funkce nad hypereliptickou křivkou rodu 3 nad polem $\mathbb{F}_{31}$

Miroslav Kureš

30. března 2022

Rovnice a body hyperelliptické křivky.

Nad polem $\mathbb{F}_{31}$ uvažujeme hypereliptickou křivku rodu 3

$$y^2 = x^7 + 15x.$$

Takto uvažovaná hypereliptická křivka má $32 = 2^5$ bodů: ∞, $[0,0]$, $[1,4]$, $[1,27]$, $[3,0]$, $[4,13]$, $[4,18]$, $[5,7]$, $[5,24]$, $[7,3]$, $[7,28]$, $[12,7]$, $[12,24]$, $[13,0]$, $[15,0]$, $[16,0]$, $[17,9]$, $[17,22]$, $[18,0]$, $[20,15]$, $[20,16]$, $[21,4]$, $[21,27]$, $[22,14]$, $[22,17]$, $[23,8]$, $[23,23]$, $[25,11]$, $[25,20]$, $[28,0]$, $[29,11]$, $[29,20]$.

Tutéž křivku můžeme uvažovat nad rozšířeními $\mathbb{F}_{31^k}$ pole $\mathbb{F}_{31}$ nebo dokonce nad jeho algebraickým uzávěrem $\bar{\mathbb{F}}_{31}$. Obecně se proto budeme zabývat křivkou nad $\bar{\mathbb{F}}_{31}$, kterou označíme C. Bod ∞ nazýváme *bod v nekonečnu*, všechny ostatní body nazýváme *konečné body*.

Splňuje-li konečný bod křivky C její rovnici nad polem $\mathbb{F}_{31^k}$, nazýváme ho $\mathbb{F}_{31^k}$*-racionální*. Bod $[5,24]$ je tedy $\mathbb{F}_{31}$-racionální a bod $[6,341]$ je $\mathbb{F}_{961}$-racionální. Křivka C má 31 $\mathbb{F}_{31}$-racionálních bodů, 1147 $\mathbb{F}_{961}$-racionálních bodů, atd.

Konečný bod $\tilde{P}$ ke konečnému bodu P splňující $P + \tilde{P} = \infty$ nazýváme *opačný bod* k bodu P. Je-li přitom $\tilde{P} \neq P$, řekneme, že P je *obyčejný* bod, je-li $\tilde{P} = P$ řekneme, že P je *speciální* bod. Speciálních bodů na naší křivce je sedm: $[0,0]$, $[3,0]$, $[13,0]$, $[15,0]$, $[16,0]$, $[18,0]$ a $[28,0]$.

Racionální funkce a jí určený divizor.

Vezměme racionální funkci $G = (x-3)(x-5) + (x-3)y$. (Pro jednoduchost pouze polynom.) Norma této funkce je

$$N(G) = -\left(x^9 + 25x^8 + 9x^7 + 30x^4 + 2x^2 + 3x + 23\right).$$

V $\bar{\mathbb{F}}_{31}$ existuje rozklad každého polynomu na kořenové součinitele. V našem příkladu existuje již v $\mathbb{F}_{961}$, a sice

$$x^9 + 25x^8 + 9x^7 + 30x^4 + 2x^2 + 3x + 23 = \\ (x-1)(x-3)^2(x-12)(x-20)(x-22)(x-25)(x-115)(x-890).$$

Z toho je zřejmé, že součet řádů $N(G)$ v konečných bodech křivky C je 18. A tedy součet řádů G v konečných bodech křivky C musí být 9.

Body křivky C, ve kterých nabývá G hodnoty 0, jsou $[1, 27]$, $[3, 0]$, $[12, 7]$, $[20, 15]$, $[22, 17]$, $[25, 20]$, $[115, 110]$, $[890, 885]$. Dále:

$G = (x-1)^0\,((x-3)(x-5) + (x-3)y)$, odtud pro obyčejný bod $P_1 = [1, 27]$ je $r = 0$, $s = 1$ a $\mathrm{ord}_{P_1}(G) = 1$.

$G = (x-3)^1\,((x-5) + y)$, odtud pro speciální bod $P_2 = [3, 0]$ je $r = 1$, $s = 0$ a $\mathrm{ord}_{P_2}(G) = 2$.

Atd. pro ostatní body.

Celkem

$$\begin{aligned} \mathrm{div}\, G \;=\; & [1, 27] + 2[3, 0] + [12, 7] + [20, 15] + \\ & [22, 17] + [25, 20] + [115, 110] + [890, 885] - 9\infty. \end{aligned}$$

(Poznámka: v poli $\mathbb{F}_{961}$ byl použit redukční polynom $t^2 + 1$.)