

Domácí úlohy: Algoritmy na eliptických křivkách

2023/24

Domácí úkoly budou zadány celkem čtyři za 20 bodů a k získání zápočtu z nich bude třeba získat aspoň 12 bodů.

1. (odevzdejte do 26.3.) Uvažte polynomy

$$u = x_2^2 - (x_1^3 + 2), v = x_2^2 - (x_1^3 + 3x_1^2 + x_1) \in \mathbb{F}_5[x_1, x_2]$$

nad pětivrčkovým tělesem. Spočítejte (explicitně je napište) všechny $\mathbb{F}_5$ -racionální body afinních křivek $V_u(\mathbb{F}_5)$ a $V_v(\mathbb{F}_5)$ a všechny $\mathbb{F}_5$ -racionální body jejich projektivního rozšíření (tj. $V_U(\mathbb{F}_5)$ a $V_V(\mathbb{F}_5)$ pro homogenizované polynomy $U, V \in \mathbb{F}_5[X_1, X_2, X_3]$). Rozhodněte, zda jsou křivky hladké či singulární a u singulárních najděte singularity.

5 bodů

2. (odevzdejte do 16.4.) (a) Odhadněte v závislosti na počtu operací invertování, násobení a čtverců (I, M, S) v tělese (tedy sčítání a odčítání zanedbáváme) a binární délce $k = l_2(n)$ časovou složitost výpočtu mocniny $[n]P$ prvku Montgomeryho křivky pomocí Montgomeryho žebříku.

3 body

(b) Rozhodněte, zda je polynom $y^2 - (x^3 + 3x + 5) \in \mathbb{F}_7[x, y]$ $\mathbb{F}_7$ -ekvivalentní nějakému Montgomeryho polynomu.

2 body

3. (odevzdejte do 7.5.) Najděte polynom určující zobecněnou Edwardsovu křivku, která je biracionálně ekvivalentní křivce V_f nad tělesem $\mathbb{F}_5$ pro Montgomeryho křivky určené polynomem (a) $f = 2y^2 - (x^3 + x^2 + x)$, (b) $f = y^2 - (x^3 - x^2 + x)$. Které z křivek jsou nad $\mathbb{F}_5$ biracionálně ekvivalentní nějaké Edwardsově křivce?

3 body

Pro Edwardsovu křivu určenou rovnicí (c) $y^2 + x^2 = 1 + 2x^2y^2$ nad tělesem $\mathbb{F}_5$ najděte biracionálně ekvivalentní Montgomeryho křivku. Kam se příslušnou biracionální ekvivalencí zobrazí bod $(2, 2)$ Edwardsovy křivky?

2 body

4. (odevzdejte do 26.5.) Uvažte nad tělesem $\mathbb{F}_5$ Montgomeryho křivku

$$M_{4,0} = \{(0, 0), (1, \pm 1), (2, 0), (-2, 0), (-1, \pm 2)\}$$

danou rovnicí $2y^2 = x^3 + x$ a Edwardsovu křivku v zúplněných souřadnicích

$$E_{4,0} = \{((\pm 1 : 1), (0 : 1)), ((0 : 1), (\pm 1 : 1)), ((\pm 2 : 1), (1 : 0)), ((1 : 0), (\pm 2 : 1))\}$$

danou rovnicí $x^2 + y^2 = 1 + 4x^2y^2$. Popište (tak, aby bylo jasné jak vypadají obrazy všech prvků) izomorfismus grupy $M_{4,0}(\mathbb{F}_5)$ a $E_{4,0}(\mathbb{F}_5)$, který je indukován biracionálním zobrazením z Věty E.7 (viz skripta části G.3 a G.4, ověřovat ekvivalenci křivek nemusíte, pozor na odlišné značení Montgomeryho křivky než na přednášce). Vysvětlete, proč jde o izomorfismus.

Návod: Zobraďte pomocí zobrazení $E_{4,0} \rightarrow M_{4,0}$ z E.7 F_5 -racionální body do grupy $M_{4,0}$, zjistěte, které z nich jsou involuce a proveďte diskuzi jejich vztahu k prvkům grupy $\mathbb{Z}_4 \times \mathbb{Z}_2$ a dodefinujte pomocí vztahů ostatních prvků na izomorfismus.

5 bodů