Domácí úlohy: Algoritmy na eliptických křivkách
2022/23

1. (odevzdejte do 30.3.) Podrobně ukažte, že výpočet zdvojení bodu na projektivní křivce bez nutnosti invertovat v tělese má časovou složitost 5S+7M (viz strana 17 skript).

6 bodů

2. (odevzdejte do 6.4.) 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.

6 bodů

3. (odevzdejte do 20.4.) Najděte polynom určující zobecněnou Edwardsovu křivku, která je biracionálně ekvivalentní křivce V_f nad tělesem F_5 pro

(a) $f = 2y^2 - (x^3 + x^2 + x)$,
(b) $f = y^2 - (x^3 - x^2 + x)$,
(c) $f = y^2 - (x^3 + x + 2)$.

Které z křivek je nad F_5 biracionálně ekvivalentní nějaké Edwardsově křivce?

6 bodů

4. (odevzdejte do 18.5.) Uvažte nad tělesem $\mathbb{F}_5$ Mongomeryho 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 zobrazení 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: Zobrazte pomocí zobrazení $E_{4,0} \to M_{4,0}$ 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 vzathů ostatních prvků na izomorfismus.

6 bodů