Domácí úlohy 2.

odevzdat do 9.4. 10:40

do schránky na KA nebo na stanovsk@karlin.mff.cuni.cz

Úkoly můžete řešit ve dvojici, v takovém případě odevzdávejte jedno řešení se dvěma podpisy. Oba uveďte přezdívku, pod kterou uvidíte výsledky na webu.

1. (5 bodů) Popište, jak v grupě odvozené z eliptické křivky najdete bod $-A$. Stačí obrázek a neformální popis konstrukce.

2. (5 bodů) Nakreslete kružnici $x^2 + y^2 = 2$ (a) v projektivní rovině $\mathcal{P}^2(\mathbb{Z}_3)$, (b) v projektivní rovině $\mathcal{P}^2(\mathbb{Z}_5)$.

Rada: obrázek bude hezčí, pokud si afinní rovinu reprezentujete jako síť se souřadnicemi $-1, 0, 1$, resp. $-2, -1, 0, 1, 2$. A nezapomeňte na body v nekonečnu (tj. rovnici si nejdřív musíte homogenizovat)!

3. (5 bodů) Spočtěte všechny průsečíky křivky dané rovnicí

$$(x^2 - 1)(x - 1)^2 + (y^2 - 1)^2 = 0,$$

a přímky dané rovnicí $y = 1$ v projektivní rovině $\mathcal{P}^2(\mathbb{R})$. Jak je možné, že nevyšla čtyři křížení?

Poznámka: Tato křivka se nazývá "bicuspid curve"(v angličtině *cusp* znamená *hrot*). Najděte si ji na wikipedii nebo si ji nechte nakreslit Wolfram Alphou. Všimněte si, jak jim vykreslování kolem hrotů trochu selhává.

4. (5 bodů) Nechť G je grupa a $X \subseteq G$. Potom je X volná báze grupy G právě tehdy, když $G = \langle X \rangle$ a pro každou grupu H a libovolné zobrazení $\sigma : X \to H$ existuje homomorfismus $\varphi : G \to H$ takový, že $\varphi \restriction X = \sigma$. Dokažte!