Domácí úlohy 1.

odevzdat do 12.3. 12:20 (na začátku prosemináře)

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

1. (4 bodů) Popište, jak v grupě odvozené z eliptické křivky najdete bod $-A$. Stačí obrázek a neformální popis konstrukce.

2. (4 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. (4 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. (8 bodů) Připomeňme reprezentaci rotací pomocí kvaternionů. Vektor $u = (u_1, u_2, u_3)$ reprezentujeme jako kvaternion $q_u = u_1 i + u_2 j + u_3 k$. Rotaci o úhel α s osou danou jednotkovým vektorem u reprezentujeme kvaternionem $r_{u,\alpha} = \cos(\alpha/2) + q_u \sin(\alpha/2)$. Rotace $\rho(v)$ vektoru v se pak spočte pomocí konjugace:

$$q_{\rho(v)} = r_{u,\alpha} \cdot q_v \cdot r_{u,\alpha}^{-1}.$$

Dokažte následující fakta:

(1) Je-li u jednotkový vektor, tj. $||u|| = 1$, pak $q_u^2 = -1$.
(2) $r_{u,\alpha} \cdot r_{u,\beta} = r_{u,\alpha+\beta}$. Z tohoto vztahu plyne, že $r_{u,\alpha}^{-1} = r_{u,-\alpha}$.
(3) $r_{u,\alpha} \cdot q_u \cdot r_{u,\alpha}^{-1} = q_u$, tj. u skutečně určuje osu té rotace.

Poznámka: K důkazu, že jde skutečně o rotaci o úhel α, zbývá ověřit, že je to ortogonální zobrazení, tj. že obrazy kolmých vektorů jsou kolmé, a že pro nějaký vektor v kolmý na u platí, že úhel $v, \rho(v)$ je α. Alternativní postup je popsán zde:

`http://www.unizar.es/matematicas/algebra/elduque/Talks/QuaternionsOctonions_handout.pdf`