

Domácí úlohy 3.

odevzdat do 10.5. ve formě PDF 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) Načrtněte eliptickou křivku $y^2 = x^3 + 4x$ v projektivní rovině $\mathcal{P}^2(\mathbb{R})$. Tato křivka obsahuje přesně tři afinní body s racionálními souřadnicemi. Dokažte, že grupa $E_{\mathbb{Q}}(f)$ je čtyřprvková cyklická.

Rada: diskutujte řady prvků

2. (5 bodů) Uvažujte ElGamalovy protokoly s grupou $\mathbb{Z}_{29}^* = \langle 2 \rangle$ a tajným klíčem $k = 8$. Zašifujte zprávu 10. Digitálně podpište zprávu m , jejíž hash je 10. Jako náhodné číslo l zvolte 9.

3. (5 bodů) Vysvětlete nějaké geograficky vzdálené osobě (humanitně založené sestře, spolužákovi, který nemá rád algebru, rodičům, zvidavému dědečkovi, ...), jak hrát kámen-nůžky-papír v době karantény, a zahrajte si. Jako důkaz mi pošlete printscreen komunikace :-) (aspoň fragment, z kterého je vidět, jak hraje)

4. (5 bodů) Napište nějakou věrnou maticovou reprezentaci grupy D_{10} . Jde to udělat lépe (tj. v menší dimenzi), než pomocí reprezentace grupy S_{10} popsané v komentáři?