

Zkoušený si vylosuje jedno téma z následujícího seznamu k diskusi. Výsledná známka bude stanovena na základě diskuse a odevzdané implementace Schoofova algoritmu.

- (1) Souřadnicové okruhy a funkční tělesa afinních křivek a jejich projektivním rozšíření. Pojmy hladké a singulární křivky. Jak poznat hladkost u Weierstrasových křivek?
- (2) Rod křivky nad obecným tělesem a pojem obecné (afinní i projektivní) eliptické křivky. Jak popsat struktury grupy na hladké Weierstrasově křivce? A jak to provést na jiných typech křivek (případně obecně)?
- (3) Idea výpočtu grupových operací na Weierstrassově (i Montgomeryho) křivce pomocí geometrické interpretace: opačný prvek, součet dvou různých prvků a zdvojení prvku. Otázka časové složitosti operací.
- (4) Montgomeryho křivky a jejich vztah k Weierstrasovým křivkám. Proč počítat s grupou nad Montgomeryho křivkou? Idea počítání mocnin prvku pomocí Montgomeryho žebříku.
- (5) Ireducibilita a afinní hladkost zobecněných Edwardsových křivek, vztah k Montgomeryho křivkám, pojem racionálního zobrazení a biracionální ekvivalence.
- (6) Popis m -torzní prvků grupy eliptické křivky nad algebraicky uzavřeným a nad konečným tělesem. Význam Hasseovy věty.
- (7) Idea rekurentního výpočtu polynomů, jejichž kořeny tvoří první souřadnici hladké Weierstrassovy křivky. Dichotomie druhé souřadnice prvku křivky. Význam (Schoofův algoritmus) a nevýhody tohoto postupu.
- (8) Základní myšlenky fungování Schoofova algoritmu: detaily využití vztahu $\varphi^2(P) \oplus [q]P = [t]\varphi(P)$.