

Cieľom tejto práce je vysvetliť a naimplementovať Schoofov algoritmus na počítanie bodov na eliptických krivkách nad konečnými telesami. Začneme definíciou eliptickej krivky ako množiny bodov spĺňajúcich istú rovnicu a pokračujeme definovaním operácie na tejto množine. Teoretické poznatky potrebné k algoritmu sú predstavené v druhej kapitole. Napokon je prestavený Schoofov algoritmus v tretej kapitole, doplnený o implementáciu v SageMath open-source software.