# SOBRE TESTES DE PRIMALIDADE

LUCAS MACHADO FERNANDES, PAULO CÉSAR CAVALCANTE DE OLIVEIRA

A teoria dos números, quando se diz respeito à criptografia, possui uma aplicabilidade imensa no meio científico, tal que os números primos são o grande mistério circundado. Sabe-se que os criptossistemas de curvas elípticas, usados em sistemas de segurança, são dependentes desses números, que por sua vez asseguram o seu funcionamento. Dessa forma, foram desenvolvidas várias técnicas para determiná-los, denominadas de teste de primalidade, aos quais conseguimos classificá-los, rapidamente, como primo ou composto. Esta produção científica objetiva estudar a fundamentação teórica que possibilita alguns desses testes importantes, além de proporcionar soluções eficazes para a sua aplicabilidade. Quanto à metodologia, o projeto é desenvolvido através de seminários voltados para a resolução de problemas da temática, além do uso do software SAGE para a aplicação dos estudos realizados. Mesmo com a dificuldade de produção relevante, o projeto Curvas Maximais está despertando o interesse pela pesquisa na álgebra, através de conteúdos fundamentais para a qualificação do profissional. Portanto, é evidente que se pode trabalhar com diversos testes como o crivo de Erastóstenes, o teste probabilístico de Miller-Rabin e o teste determinístico de Agrawal, Kayal e Saxena, de modo que os números primos estão sendo desmistificados de forma contínua.

**PALAVRAS-CHAVE:** NÚMEROS PRIMOS; TESTE DE PRIMALIDADE; CURVAS MAXIMAIS

**ÀREA TEMÀTICA:** MATEMÁTICA

**FORMA DE APRESENTAÇÃO:** PÔSTER