

Ačkoli v poslední době byla pozornost upřena především na nový deterministický algoritmus pro testování prvočíselnosti AKS, pravděpodobnostní algoritmy zůstávají efektivním nástrojem pro testování prvočíselnosti. Naše práce se věnuje převážně dvěma nejznámějším probabilistickým algoritmům pro testování prvočíselnosti. Podrobně popisuje princip a důkaz správnosti Solovay-Strassenova a Rabin-Millerova algoritmu. Kromě toho se také pokouší dívat na problematiku pravděpodobnostních testů obecněji. Je představena definice probabilistického algoritmu a různé třídy složitosti odpovídající Monte Carlo či Las Vegas algoritmům. Kromě čistě matematické teorie naznačíme i filosofické aspekty, nad kterými je třeba se při používání pravděpodobnostní metody zamýšlet.