Miller-Rabin

Algoritmen

Miller-Rabin testen afgør om et givet tal, n, er et sammensat tal eller om det er "nok et primtal". Dette skyldes at det er en probabilistisk algoritme, altså at den afhænger af tilfældighed.
Et kald til Miller-Rabin algoritmen kræver udover tallet n også en parameter k som er antallet af gange algoritmen bliver gentaget. For hver ekstra gang algoritmen bliver kørt hvor der bliver returneret at n nok er primtal, falder sandsynligheden for at n ren faktiskt er et sammensat tal. Altså ses k som en parameter for korrekthed.
Algoritmen kan deles i fire trin for $n \geq 5$.

1. Find de unikke tal r og s, så $n - 1 = 2^r \cdot m$ og m er ulige.
2. Vælg et tilfældigt heltal a, hvor $1 < a < n$.
3. Sæt $b = a^m \pmod{n}$. Hvis $b \equiv \pm 1 \pmod{n}$, så er n nok et primtal.
4. Hvis $b^{2^s} \equiv -1 \pmod{n}$ for et s hvor $1 \leq s \leq r - 1$, så er n nok et primtal. Hvis ikke, så er n et sammensat tal.

Køretid