Miller-Rabin-Test

•••

Primzahltest

Janik Mabboux - Mathias Begert

Inhalt

- Einleitung
  - Primzahltests
  - Miller-Rabin-Test
- Grundlagen
  - Der kleine fermatsche Satz
  - Ansatz
- Funktionsweise
- Beispiel
- Quellen / Fragen

Einleitung - Primzahltests

- Asymmetrische Verschlüsselungsverfahren (z.B. RSA) verwenden grosse Primzahlen
  - etwa 1000 Stellen in dualer Form

- Miller-Rabin oder auch Miller-Selfridge-Rabin-Test
  - 1974 von John L. Selfridge bereits verwendet
  - 1976 von Gary L. Miller und Michael O. Rabin veröffentlicht
- Probabilistischer Primzahltest (Monte-Carlo-Algorithmus)
- Auch deterministische Variante möglich
- Fehlerwahrscheinlichkeit nach einem Test ist 1/4
- Starke Pseudoprimzahlen

Der kleine fermatsche Satz

$$a^{p-1} \equiv 1 \pmod{p}$$

Wenn p eine Primzahl ist, dann muss dieser Satz für ein beliebiges a gelten.

Dies kann jedoch auch für nicht prime Zahlen zutreffen:
Beispiel: p=105 (nicht prim) und a=8

Carmichael-Zahlen

Pierre de Fermat

Ansatz

Beispiel n=105 (nicht prim) und a=8

hier gilt auch
$a^{n-1} \equiv 1 \pmod{n}$

	$a^{(n-1)/8}$	$a^{(n-1)/4}$	$a^{(n-1)/2}$	a^{n-1}
	8^{13}	8^{26}	8^{52}	8^{104}
mod 105	8	64	1	1

Vergleich mit einer echten Primzahl mit verschiedenen “Zeugen” a
n=89

Rechts neben einer 1 steht stets eine -1 oder eine weitere 1

	$a^{(n-1)/8}$	$a^{(n-1)/4}$	$a^{(n-1)/2}$	a^{n-1}
	a^{11}	a^{22}	a^{44}	a^{88}
a=3	37	34	-1	1
a=5	55	-1	1	1
a=2	1	1	1	1

Funktionsweise Algorithmus - Vorbereitung

1. Wir definieren n als die zu testende Zahl

2. Nun wählen wir die ganzzahligen d (ungerade) und j, so dass gilt:

$$n - 1 = d \cdot 2^j$$

Beispiel für n=13

$j = 0, \quad d = 12$

$j = 1, \quad d = 6$

$j = 2, \quad d = 3$

Funktionsweise Algorithmus - Test

Nun prüft man mit beliebig vielen, beliebig gewählten
$a \in \{2, 3, ..., n-2\}$

ob entweder

$$a^d \equiv 1 \pmod{n}$$

oder für ein r mit $0 \leq r < j$

$$a^{d \cdot 2^r} \equiv -1 \pmod{n}$$

gilt.

Beispiel

Nun werden wir den Miller-Rabin-Test anhand eines Beispiels testen.

Beispiel

Fragen?

Quellenverzeichnis

- https://de.wikipedia.org/wiki/Miller-Rabin-Test
- G. Teschl und S. Teschl, *Mathematik für Informatiker*, Band 1, 4. Auflage, Springer
- http://www.austromath.at/medienvielfalt/materialien/krypto/lernpfad/content/k_prim_l06.htm
- https://de.wikipedia.org/wiki/Primzahltest
- https://www.youtube.com/watch?v=Tqq6hxxnhEs (Weitz / HAW Hamburg, Der Miller-Rabin-Test)