Miller Rabin Test

Übersicht

Wer sich in der Welt der Verschlüsselung bewegt, trifft früher oder später auf grosse Primzahlen. Je grösser eine Zahl, umso schwerer ist es, zu bestimmen, ob sie prim ist oder nicht. Genau diesem Problem stellt sich der Miller-Rabin-Test (MRT) - der Algorithmus prüft Zahlen darauf, ob sie Prim sind oder nicht.

Funktionsweise

Eingabewerte sind die zu prüfende, natürliche Zahl $n \geq 5$ und eine aus der Menge $a \in \{2, 3, 4 \ldots, n-2\}$ frei wählbaren Zahl. Das Resultat des Algorithmus sagt aus, ob die Zahl *n* zusammengesetzt (aus mehreren Faktoren bestehend) oder *wahrscheinlich* eine Primzahl ist. Eine Zahl *n* kann also durch den Algorithmus als *wahrscheinlich* Prim bezeichnet werden, obwohl *n* zusammengesetzt ist.
In den meisten Fällen der Anwendung des Algorithmus wird *a* zufällig gewählt, weswegen der Algorithmus zu den Monte-Carlo-Algorithmen zählt. Monte-Carlo-Algorithmen wiederum bezeichnen Algorithmen, die mit einer gewissen Wahrscheinlichkeit ein falsches Ergebnis liefern. Die Wahrscheinlichkeit eines Fehlers kann durch mehrfaches Anwenden des Algorithmus mit verschiedenen *a*'s beliebig minimiert werden. In diesem Kontext sprechen wir vom probabilistischen MRT.
Der MRT bietet auch eine deterministische Variante, mit dieser kann ein Fehler ausgeschlossen werden. Dafür muss *a* bestimmt gewählt werden. Wie *a* festgelegt werden muss wird hier aus platzgründen nicht angegeben. Die deterministische Variante wird trotz Fehlerausschluss seltener angewendet, da die Berechnung länger dauert, als bei der probabilistischen Variante.

Algorithmus

Wir bestimmen eine ungerade Zahl n von der wir wissen möchten ob diese eine Primzahl ist. Zusätzlich wird *a* wie oben beschrieben festgelegt. Nun werden noch *d* (ungerade) und *j* so bestimmt, dass gilt: $n - 1 = d * 2^j$
Letztendlich wird geprüft ob gilt:
$a^d \equiv 1 \ (mod\ n)$
oder
$a^{d*2^r} \equiv -1\ (mod\ n)$ für ein *r* mit 0 ≤ *r* < *j*

Trifft keiner der beiden Prüfungen zu, muss die Zahl zusammengesetzt sein. Wie bereits beschrieben, kann auch eine zusammengesetzte Zahl mit einer bestimmten Wahrscheinlichkeit diese Bedingungen erfüllen.
Wird das *a* zufällig gewählt, so ist die Wahrscheinlichkeit, dass ein Resultat eine Zahl zu Prim bestimmt zu mehr als 75% korrekt ist. Mit jedem weiteren *a*, das zur Prüfung angewendet wird, verringert sich die Wahrscheinlichkeit, ein falsches Resultat zu haben, um 25% → (1/4)^i wobei die Anzahl Iterationen bezeichnet. Damit liegt die Fehlerquote bei fünf Prüfungen bereits bei unter 0.1%.

Quellen

http://www.austromath.at/medienvielfalt/materialien/krypto/lernpfad/content/k_prim_l06.htm
https://de.wikipedia.org/wiki/Miller-Rabin-Test