Miller-Rabin Test

Effiziente Algorithmen – Sommer 2019

Martin Hoefer

RSA Public-Key Kryptographie

- Alice generiert **öffentlichen** und **privaten Schlüssel**
- Alice gibt öffentlichen Schlüssel bekannt
- Bob verschlüsselt damit Nachricht an Alice
- Alice entschlüsselt Nachricht mit privatem Schlüssel

Implementation

- Alice wählt sowohl (1) zwei sehr große Primzahlen p, q und multipliziert sie zu $n = pq$, als auch (2) Kodierungsexponent c, teilerfremd zu $(p-1)(q-1)$
- Öffentlicher Schlüssel: (n, c)
- Bob verschlüsselt Nachricht x mit: $y = x^c \mod n$
- Betrachte *Eulersche Phi-Funktion* von n:

$$\varphi(n) = |\{a \in \{1, \ldots, n\} \mid ggT(a, n) = 1\}|$$

  d.h. Anzahl Zahlen in $\{1, \ldots, n\}$, die keinen nicht-trivialen gemeinsamen Teiler mit n haben
- Berechnung von $\varphi(n)$ gilt als schwer, aber Alice weiss: $\varphi(n) = (q-1)(p-1)$.
- Alice berechnet multiplikatives Inverses d von c modulo $\varphi(n)$ und dekodiert:

$$y^d \equiv (x^c)^d = x^{c \cdot d \mod \varphi(n)} \equiv x^1 \equiv x \mod n$$

Finde große Primzahlen:

- Sei $\pi(x) = \{p \leq x \mid p \text{ Primzahl}\}$. Nach Primzahlsatz

$$\frac{x}{\pi(x)} = \ln(x) + o(\ln(x))$$

- Also b-Bit Primzahl nach erwartet $O(b)$ zufälligen Versuchen gefunden.
  Aber **ist eine gegebene Zahl n eine Primzahl**?

Lemma 1 (Kleiner Satz von Fermat)**.** *Für jede Primzahl n und jede Zahl $a \in \{1, \ldots, n-1\}$ gilt*

$$a^{n-1} \equiv 1 \mod n \ .$$

Fermat-Test:
Wähle a uniform zufällig und berechne $a^{n-1} \mod n$.
Falls 1, gib aus "n ist prim", andernfalls "n ist nicht prim".

Der Fermat-Test ist extrem schlecht auf Carmichael-Zahlen:

- n heißt **Carmichael-Zahl** wenn n nicht prim und für jede mit n teilerfremde Zahl a gilt

$$a^{n-1} \equiv 1 \mod n \ .$$

- Große Carmichael-Zahlen werden so gut wie immer als Primzahl klassifiziert :(
- Es gibt unendlich viele Carmichael-Zahlen: 561, 1105, 1729, 2465, 2821,... :((

Rekursive Anwendung von Fermat:

- Für jede Zahl n ist die *prime Restklassengruppe*

$$\mathbb{Z}_n^* = \{a \in \{1, \ldots, n-1\} \mid ggT(a, n) = 1\} \cup \{0\} \ .$$

- Wenn n prim, dann ist einfach $\mathbb{Z}_n^* = \{0, 1, \ldots, n-1\}$, und $\mathbb{Z}_n$ ist ein Körper (d.h., Addition und Multiplikation $\mod n$ funktionieren wie gewohnt).
- Es gibt zu $x^2 = 1$ nur zwei Lösungen in jedem Körper: $x \in \{1, -1\}$.
- n prim $\Rightarrow n-1$ gerade $\Rightarrow (n-1)/2$ ganze Zahl. Also, für alle $a \in \mathbb{Z}_n$, $a \neq 0$:

$$a^{n-1} \equiv (a^{(n-1)/2})^2 \equiv 1 \mod n$$

  und damit

$$a^{(n-1)/2} \equiv 1 \mod n \quad \text{oder} \quad a^{(n-1)/2} \equiv -1 \mod n$$

- Wenn $a^{(n-1)/2} \equiv 1 \mod n$ und $(n-1)/2$ gerade, wende das gleiche Argument wieder an.

Erweiterter Fermat-Test:

- Sei n prim und $n - 1 = 2^k \cdot m$ mit k maximal (d.h., m ungerade). Dann gilt für jedes $r = 0, 1, \ldots, k-1$:

$$a^{(n-1)/2^r} \equiv 1 \mod n \quad \Rightarrow \quad a^{(n-1)/2^{r+1}} \equiv -1 \text{ oder } 1 \mod n$$

- Das Zahlenpaar (n, a) mit n ungerade **besteht den erweiterten Fermat-Test** wenn sowohl (1) $a^{n-1} \equiv 1 \mod n$, als auch (2) die obige Implikation für alle $r = 0, 1, \ldots, k-1$ erfüllt ist.

Algorithm 1: Miller-Rabin Primzahltest

```
1 Sei n Eingabezahl und k maximal mit n − 1 = 2^k · m
2 Wähle a ∈ {2, ..., n − 2} zufällig.
3 if n gerade oder ggt(a, n) ≠ 1 oder (n, a) besteht erweiterten Fermat-Test nicht
4     then return("n nicht prim")
5 return("n ist prim")
```

Der Miller-Rabin Test ist ein Monte Carlo Algorithmus mit einseitigem Fehler. Wenn n prim, dann Pr["n ist prim"] $= 1$, wird also immer richtig erkannt. Falls n nicht prim, dann Pr["n nicht prim"] $= q$. Es gilt $q \geq 3/4$. Das q ist in Wirklichkeit oft noch deutlich größer.

Theorem 1. *Wenn die Zahl n zusammengesetzt ist, dann fehlklassifiziert der Miller-Rabin Test sie als Primzahl mit Wahrscheinlichkeit höchstens $1/4$. Im Test werden $O(\log_2 n)$ arithmetische Operationen durchgeführt.*

- Betrachte für ungerades, zusammengesetztes $n \geq 5$ die Menge der *schlechten Teilerreste*

$$G = \{a \in \{2 \ldots, n-2\} \mid (n, a) \text{ besteht erweiterten Fermat-Test}\} \ .$$

- Man kann zeigen, dass $|G| \leq (n-3)/4$.
- Die Wahrscheinlichkeit, einen schlechten Teilerrest zu wählen und fehlerhaft "n ist prim" zu liefern, ist maximal $1/4$.
- Die Schranke an $|G|$ folgt aus gruppen- und zahlentheoretischen Eigenschaften von Teilerresten. Siehe Skript für einen leicht angepassten Test und einen etwas einfacheren Beweis, dass die Wahrscheinlichkeit maximal $1/2$ ist.