Miller Rabin Primzahl-Test

Recap: Fermat Test

- Muster für die Erzeugung grosser Primzahlen:

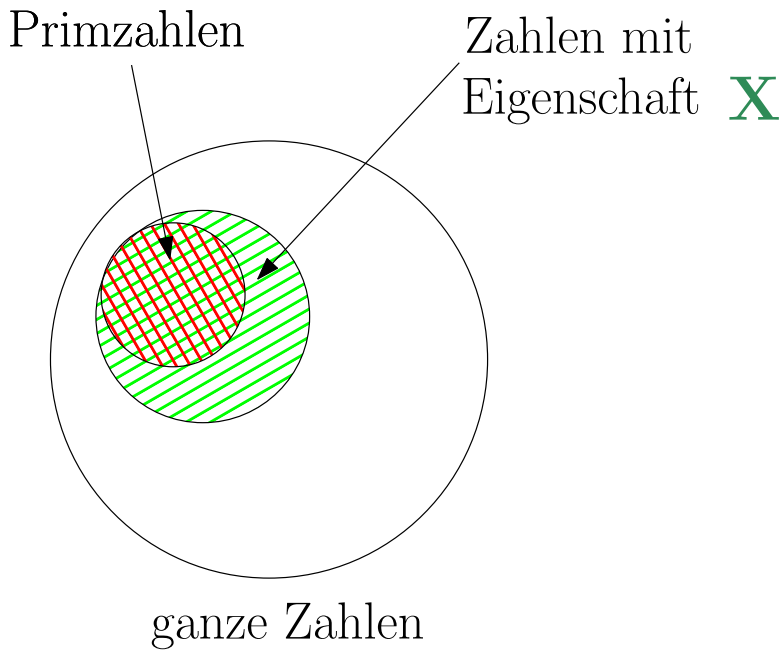
  while (noch keine Primzahl gefunden) **do**
  Wähle (zufällig) eine grosse Zahl z
  Teste, ob z eine Primzahl ist
  Falls ja: **return** z
  Falls nein: Mache weiter
  end

- Letzte Woche: Fermat Test
- Heute: Miller Rabin Test

Recap: Fermat Test

Strategie, um zu testen, ob eine gegebene Zahl prim ist

- Tests mit einer Zufallskomponente:
  Grundidee: Teste auf eine Eigenschaft **X** (die **effizient** prüfbar ist).



- Einige Zahlen werden fälschlicherweise als Primzahlen klassifiziert!
- Aber: Wird eine Zahl als nicht-prim klassifiziert wird, dann stimmt es!

Recap: Fermat Test

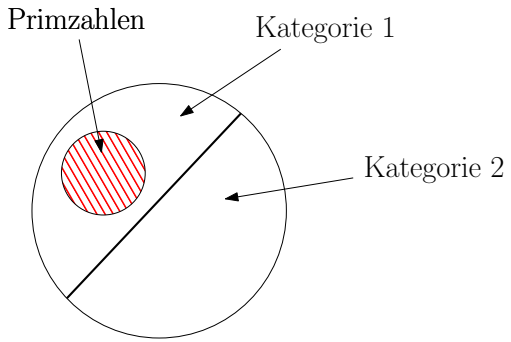
Eigenschaft X

- $a^{n-1} = 1 \pmod{n}$, und
- $\mathrm{ggT}(a, n) = 1$

Recap: Fermat Test

Analyse

- **Kategorie 1** $\mathrm{FL}(n) = \mathbb{Z}_n^*$ (alle El. von $\mathbb{Z}_n^*$ sind Fermat-Lügner)
- **Kategorie 2** $|\mathrm{FL}(n)| < |\mathbb{Z}_n^*|$ und somit $|\mathrm{FL}(n)| \leq \frac{|\mathbb{Z}_n^*|}{2}$



Kategorie 2

- Fermat Test funktioniert in der Regel zufriedenstellend.

Kategorie 1

- Fermat Test versagt fast **immer**.
- Name dieser Zahlen: Carmichael-Zahlen.
- Für genügend grosse n gilt:
  $\#$ Carmichael Zahlen in $\{1, 2, \ldots, n\} \geq n^{2/7}$.

Miller Rabin Test – Grundidee

- Ziel: Verschärfung des Kriteriums des kleinen Satzes von Fermat (zur Behebung der Schwäche mit den Carmichael-Zahlen)
- Hilfs-Beobachtung: Für jede ungerade Primzahl n gilt: $n-1$ kann man darstellen als: $n-1 = 2^r \cdot u$ (mit u ungerade).
- "Faktorisiere" damit das Fermat-Kriterium:
- $$a^{n-1} = 1 \Leftrightarrow a^{n-1} - 1 = 0 \Leftrightarrow a^{u \cdot 2^r} - 1 = 0 \pmod{n}$$
- $$(a^{u \cdot 2^{r-1}} + 1) \cdot (a^{u \cdot 2^{r-1}} - 1) = 0 \pmod{n}$$
- $$(a^{u \cdot 2^{r-1}} + 1) \cdot (a^{u \cdot 2^{r-2}} + 1) \ldots (a^{u} + 1) \cdot (a^{u} - 1) = 0 \pmod{n}$$
- Falls n prim ist, so MUSS eine der obigen Klammern Null sein $\pmod{n}$
  Grund: n kann nicht in Faktoren über mehrere Klammern verteilt werden!

Miller Rabin Test – explizite Form

Satz (Begründung: Siehe vordere Folie)

Wir betrachten eine ungerade Primzahl n und wählen r und u so, dass $n-1 = 2^r \cdot u$. Dann gilt für jedes $a \in \mathbb{Z}_n^*$

(1) $a^u = 1 \pmod{n}$, oder

(2) $a^{2^k \cdot u} = -1 \pmod{n}$ für ein $k \in \{0, 1, \ldots, r-1\}$

Miller Rabin Test: Verwende das Kriterium vom obigen Satz als Test, ob eine Zahl n prim ist.

Aufgabe Prüfe den Satz für $n = 29$ und $a = 7$.

Aufgabe Prüfe den Satz für $n = 29$ und $a = 15$.

Miller Rabin Test – Beispiel

Aufgabe Belege mithilfe des Satzes von der letzten Folie mit $a = 2$, dass $n = 561$ zusammengesetzt ist.

Lügner

- **Recap:** Fermat: $\mathrm{FL}(n) = \{a \in \mathbb{Z}_n^* \mid a^{n-1} = 1 \pmod{n}\}$
- Miller Rabin: $\mathrm{SL}(n) = \{a \in \mathbb{Z}_n^* \mid a$ erfüllt Bed (1) oder (2) vom vorherigen Satz$\}$

Bem: Für **nicht-prime** Zahlen n verwendet man die Bezeichnungen:

- Fermat-Lügner = Elemente von $\mathrm{FL}(n)$
- starke Lügner = Elemente von $\mathrm{SL}(n)$

Aufgabe: Wir setzen $n := 85$. Entscheide für die Zahlen 13 und 14, ob sie jeweils ein starker Lügner für n sind.

Vergleich Fermat Test vs Miller Rabin Test

- **Recap:** Es gibt zusammengesetzte Zahlen n mit der Eigenschaft $\mathrm{FL}(n) = \mathbb{Z}_n^*$
  $\Rightarrow$ Fermat Test liefert für diese n fast immer das falsche Ergebnis.
- Miller Rabin: Man kann zeigen: $|\mathrm{SL}(n)| \leq \frac{1}{4}|\mathbb{Z}_n^*|$
- Folgerung: Der Miller Rabin Test hat die folgenden Eigenschaften:
  1. Falls n eine Primzahl ist, liefert der Test: n ist prim.
  2. Falls n nicht-prim ist, dann ist $\Pr(n \text{ wird als prim eingeschätzt}) \leq \frac{1}{4}$
- Somit: Macht man t Durchläufe vom Miller Rabin Test, so beträgt die Wahrscheinlichkeit für ein falsches Resultat höchstes $\left(\frac{1}{4}\right)^t$.
  Dies tendiert schnell gegen 0.