Primzahl-Tests

Grund-Thematik (Repetition)

- Bei vielen Verschlüsselungs-Systemen (z.B. RSA) werden grosse Primzahlen benötigt!

  $\uparrow$

  $\approx 10000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000$

- Vorgehensweise, um grosse Primzahlen zu erzeugen:

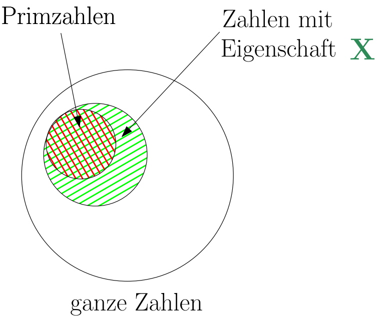
  while (noch keine Primzahl gefunden) **do**
      Wähle (zufällig) eine grosse Zahl z
      Teste, ob z eine Primzahl ist
      Falls ja: **return** z
      Falls nein: Mache weiter
  end

- In diesem Modul betrachten wir zwei solche Tests
  - Fermat Test (heute)
  - Miller Rabin Test (nächste Woche)

Primzahl-Tests (Repetition)

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!

Hintergrund:

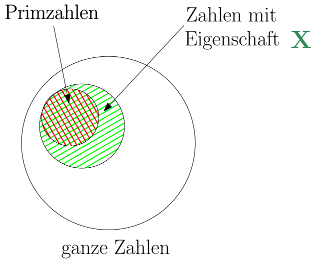
Satz von Fermat $\quad n$ prim $\Rightarrow \quad a^{n-1} = 1 \pmod{n} \quad$ für alle $a \in \mathbb{Z}_n^*$

Eigenschaft **X**

Folge: Wenn eine Zahl Eigenschaft **X** NICHT hat $\Rightarrow$ KEINE Primzahl.

resp. Wenn $a^{n-1} \neq 1 \pmod{n}$ für *irgendein* $a \Rightarrow n$ ist KEINE Primzahl

Bsp $n = 391$, $a = 3 \qquad 3^{390} = 151 \pmod{391} \Rightarrow 391$ ist nicht prim.



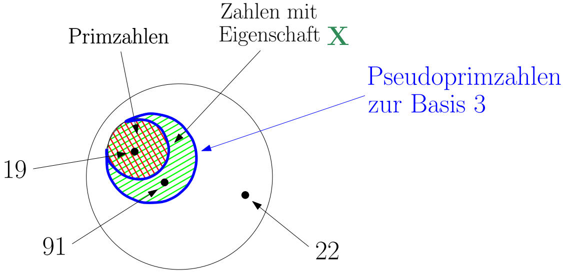
Definition

Eine nicht-prime Zahl n heisst Pseudoprimzahl zur Basis a, wenn

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

Bsp: $a = 3$

1. $n = 19$:
   $3^{18} = 1 \pmod{19}$
2. $n = 22$:
   $3^{21} = 3 \pmod{22}$
3. $n = 91$:
   $3^{90} = 1 \pmod{91}$



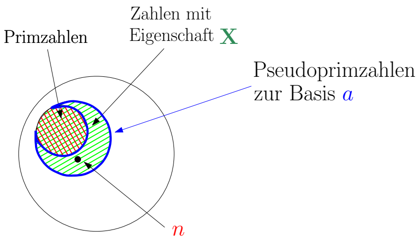
Fermat Test: Analyse

Definition

Eine Zahl a heisst Fermat-Lügner der nicht-primen Zahl n, wenn

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

Notation: $\underset{\text{Fermat-Lügner}}{\underset{\uparrow}{FL(n)}} = \{a \in \mathbb{Z}_n^* : \underset{n \text{ ist Pseudoprimzahl zur Basis } a}{\underset{\uparrow}{a^{n-1}}} = 1 \pmod{n}\}$



- Viele Fermat-Lügner → Risiko für falsche Klassifizierung als "prim"

Fermat-Lügner

Aufgabe Bestimme $\mathrm{FL}(15)$

Abschätzung der Fehlerwahrscheinlichkeit des Fermat Tests

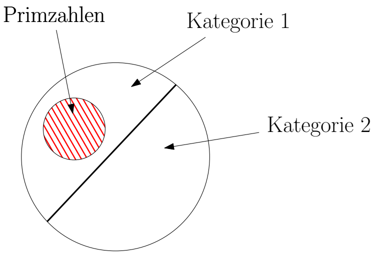
Satz: $\mathrm{FL}(n)$ ist eine Untergruppe von $\mathbb{Z}_n^*$

Satz von Lagrange: $|U|$ teilt $|G|$ (für jede Untergruppe U von G)

Folgerung: $|\mathrm{FL}(n)|$ teilt $|\mathbb{Z}_n^*|$

Es gibt also 2 Kategorien

- **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 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 $|\mathrm{FL}(n)| \leq \frac{|\mathbb{Z}_n^*|}{2}$

Fermat Test

for $i = 1$ **to** t **do**
  Erzeuge eine Zufallszahl a mit $1 \leq a \leq n-1$
  Berechne $r := a^{n-1} \pmod{n}$
  if $((r \neq 1)$ **or** $(\mathrm{ggT}(a, n) \neq 1))$ **then return** "nicht prim"
end
return "prim"

Analyse für Kategorie 2

- $\Pr(\text{Test versagt}) = \Pr(a \text{ ist in } \mathrm{FL}(n)) \leq \frac{|\mathrm{FL}(n)|}{n-1} \leq \frac{|\mathrm{FL}(n)|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$
- $\Pr(\text{alle } t \text{ Test-Durchläufe versagen}) \leq \left(\frac{1}{2}\right)^t \to 0$
- n wird mit hoher Wahrscheinlichkeit als nicht-prim erkannt
  $\Rightarrow$ sehr kleine Fehler-Rate

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 $|\mathrm{FL}(n)| \leq \frac{|\mathbb{Z}_n^*|}{2}$

Bem: Da für ungerade n die Zahlen 1 und $n-1$ immer Fermat-Lügner sind, könnte man den Bereich einschränken auf $2 \leq a \leq n-2$.

Analyse für Kategorie 1

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

Carmichael Zahlen

Definition

Eine zusammengesetzte natürliche Zahl n heisst **Carmichael Zahl**, wenn für alle $a \in \mathbb{Z}_n^*$ gilt: $a^{n-1} = 1 \pmod{n}$.

Bem: Zwischen 1 und 100'000 gibt es 16 Carmichael Zahlen, z.B. 561, 1105, 1729.

Satz (ohne Herleitung)

Für jede zusammengesetzte Zahl $n \geq 3$ gilt: n ist Carmichael Zahl $\Leftrightarrow$

(1) n ist quadratfrei, und

(2) für jeden Primteiler p von n gilt $(p-1)|(n-1)$

Folgerung

Für jede Carmichael-Zahl n gilt:

(1) n besitzt mindestens 3 Primfaktoren.

(2) n ist ungerade.

Fazit

Fermat Test . . .

- ist effizient,
- klassifiziert viele Zahlen richtig als ”prim”/”nicht prim”,
- liefert fälschlicherweise ”prim” für eine relativ substantielle Menge von zusammengesetzten Zahlen .

Die letzte Schwäche lässt sich beheben, indem man eine stärkere Form des kleinen Satzes von Fermat verwendet (s. nächste Woche – Miller Rabin Test).