

Probabilistische Primzahltests

Alexander von Felbert

23.01.2006

Motivation und Überblick

- Als **Primzahltest** bezeichnet man ein mathematisches Verfahren, mit dem ermittelt wird, ob eine gegebene Zahl eine Primzahl (prim) ist oder nicht.
- **Probabilistische Algorithmen** sind sog. randomisierte Algorithmen, als Algorithmen welche ein Zufallsexperiment als wesentlichen Bestandteil enthalten. Monte-Carlo-Algorithmen sind rand. Algorithmen, die mit einer nach oben beschränkten Wahrscheinlichkeit ein *falsches Ergebnis liefern dürfen*.
- Alle „naiven“ Verfahren (Brute-Force, Sieb des Eratosthenes) sind **nicht** polynomiell zeitbeschränkt! (Warum?)

Motivation und Überblick

- Im August 2002 wurde das **erste deterministische** und *polynomiell zeitbeschränkte* Verfahren von drei indischen Wissenschaftlern veröffentlicht (AKS-Algorithmus).
- Bei einigen Kryptosystemen, insbesondere bei asymmetrischen Public-Key-Verfahren, werden große Primzahlen **benötigt**.
- Kryptographische Verfahren und damit auch Primzahltests müssen gegenüber der Zeit- und Platzkomplexität gewisse **Anforderungen** erfüllen, insbesondere sollten sie effizient zu berechnen sein.

Grundsätzliches Vorgehen

- 1 Wähle zufällig eine ungerade Zahl $n \in \mathbb{N}$.
- 2 Teste mit einem Verfahren, ob die gegebene Zahl n prim ist oder zusammengesetzt („Black-Box“).
- 3 Ist die Zahl n gemäß Test eine Primzahl, so sind wir bereits fertig. Ansonsten führen wir einen erneuten Test mit der Zahl $(n + 2)$.

Es werden also die Zahlen $n, (n + 2), \dots, (n + 2k)$ getestet, bis im k -ten Schritt wahrscheinlich eine Primzahl gefunden wurde. Beachte das Bertrandsche Postulat: $\forall n \in \mathbb{N}, n > 1 \exists p \in \mathbb{P}$ mit $n < p \leq 2n!$

Grundsätzliches Vorgehen

Input: $n \in \mathbb{N}$, n ungerade!

Output:

- Besteht die Zahl n den Test nicht, so ist diese *nicht* prim, also **bestimmt** zusammengesetzt.
- Besteht die Zahl n den Test, so ist diese **wahrscheinlich** prim.

Grundsätzliches Vorgehen

Die Fehlerwahrscheinlichkeit kann bei allen drei vorgestellten Tests

- durch wiederholtes Durchführen beliebig gesenkt werden.
- exakt beschränkt werden.

Dabei nutzen die vorgestellten Verfahren *notwendige* aber *nicht hinreichenden* Kriterien für Primzahlen aus.

Der Fermat-Test

Satz von Euler und „kleiner“ Satz von Fermat

SATZ

Es sei $b \in \mathbb{Z}$, $n \in \mathbb{N}$. Sei weiter $\text{ggT}(b, n) = 1$, dann gilt:

$$b^{\phi(n)} \equiv 1 \pmod{n}. \quad (1)$$

Folgerung

Es sei p prim und $b \in \mathbb{Z}$ mit $\text{ggT}(b, p) = 1$. Dann gilt:

$$b^{p-1} \equiv 1 \pmod{p}. \quad (2)$$

Satz von Euler

Beispiel:

$$5^{\phi(6)} \bmod 6 = 5^2 \bmod 6 = 25 \bmod 6 = 1.$$

Es ist $\text{ggT}(5, 6) = 1$, d.h. wir können den Satz von Euler anwenden.

$$\text{Es ist } 31^{\phi(853)} \bmod 853 \text{ und } \text{ggT}(853, 31) = 1.$$

Mit dem Satz von Euler folgt

$$31^{\phi(853)} \equiv 1 \pmod{853}$$

853 prim \Rightarrow Kleiner Satz von Fermat.

Pseudoprimzahlen

Der kleine Satz von Fermat ist ein **notwendiges** Kriterium für Primzahlen $p \in \mathbb{P}$. Wir wissen, dass für *geeignete* Zahlen b stets gilt $b^{p-1} \bmod p = 1$. Leider gilt die Umkehrung dieses Sachverhalts nicht, wie uns das folgende Beispiel zeigt:

Beispiel:

$n := 91 = 7 \cdot 13$ und $b := 3$. Obwohl 91 offensichtlich zusammengesetzt ist gilt

$$3^{90} \bmod 91 = 1.$$

Pseudoprimzahlen

Das letzte Beispiel motiviert die folgende

Definition:

Sei $n \in \mathbb{N}$ eine zusammengesetzte Zahl, und sei $b \in \mathbb{Z}_n^*$. Wir nennen n eine **Pseudoprimzahl zur Basis b** , falls $b^{n-1} \bmod n = 1$ gilt.

Beispiel:

Es ist also $n := 91 = 7 \cdot 13$ zur Basis $b := 3$ eine Pseudoprimzahl, da gilt

$$3^{90} \bmod 91 = 1 \text{ aber } 2^{90} \bmod 91 = 64 \neq 1$$

Pseudoprimzahlen

Lemma

Sei $n \in \mathbb{N}$ eine zusammengesetzte Zahl. Die Menge

$$B := \{b \in \mathbb{Z}_n^* \mid n \text{ ist Pseudoprimzahl zur Basis } b\}$$

ist eine Untergruppe von (\mathbb{Z}_n^*, \odot) , wobei \odot die modulare Multiplikation ist.

Beweis:

Seien $a, b \in B$. Dann gilt $a^{n-1} \equiv_n 1 \equiv_n b^{n-1}$. Also

$$(ab^{-1})^{n-1} \equiv a^{n-1}(b^{-1})^{n-1} \equiv 1 \cdot (b^{n-1})^{-1} \equiv 1 \pmod{n},$$

womit auch das Produkt ab^{-1} in B liegt. Mit dem UG-Kriterium folgt damit die Behauptung.

Fehlerwahrscheinlichkeit

Lemma

Sei n eine zusammengesetzte Zahl. Entweder

- *n ist eine Pseudoprimzahl für alle Basen $b \in \mathbb{Z}_n^*$, oder*
- *n ist keine Pseudoprimzahl zur Basis b für mindestens die Hälfte aller $b \in \mathbb{Z}_n^*$.*

Beweis:

Nach einem Korollar aus dem Satz von Lagrange wissen wir, dass die Ordnung einer UG, die Gruppenordnung teilt - vorausgesetzt die UG existiert überhaupt. Diese Erkenntnis angewendet auf \mathbb{Z}_n^* und deren Untergruppe B ergibt die Behauptung.

Carmichael-Zahlen

Die zusammengesetzte Zahl $561 = 3 \cdot 11 \cdot 17$ besitzt eine besondere Eigenschaft, denn sie ist Pseudoprimzahl für alle Basen $b \in \mathbb{Z}_n^*$.
D.h. es gilt für $b \in \{1, 2, 4, \dots, 560\}$ die Kongruenz

$$b^{561-1} \equiv_n 1$$

Definition:

Eine zusammengesetzte Zahl $n \in \mathbb{N}$ heißt **Carmichael-Zahl**, falls $b^{n-1} \pmod n = 1$ für alle Basen $b \in \mathbb{Z}_n^*$ gilt.

Carmichael-Zahlen

7 ersten Carmichael-Zahlen:

$$561 = 3 \cdot 11 \cdot 17$$

$$2465 = 5 \cdot 17 \cdot 29$$

$$8911 = 7 \cdot 19 \cdot 67$$

$$1105 = 5 \cdot 13 \cdot 17$$

$$2821 = 7 \cdot 13 \cdot 31$$

$$1729 = 7 \cdot 13 \cdot 19$$

$$6601 = 7 \cdot 23 \cdot 41$$

SATZ

Sei $n \in \mathbb{N}$ eine ungerade, zusammengesetzte Zahl.

- 1 Sei p prim und $p^2 | n \Rightarrow n$ ist keine Carmichael-Zahl.
- 2 Sei n nicht durch eine Quadratzahl teilbar. Dann gilt:
 n ist eine Carmichael-Zahl \Leftrightarrow Für jeden Primteiler p von n gilt
 $(p-1) | (n-1)$.

Carmichael-Zahlen

Besteht ein zufällig gewähltes ungerades $n \in \mathbb{N}$ den Test, d.h. gilt $b^{n-1} \bmod n = 1$ für ein ebenso zufällig gewähltes $b \in \mathbb{Z}_n^*$, so kann die Zahl n entweder

- 1 eine **Primzahl** sein.
- 2 eine **Carmichael-Zahl** sein.
- 3 eine **zusammengesetzte Zahl** sein, und die Wahrscheinlichkeit ein solches b zu wählen, war höchstens $\frac{1}{2}$.

Carmichael-Zahlen

Carmichael-Zahlen sind innerhalb der natürlichen Zahlen \mathbb{N} recht „weit gestreut liegen“ - es gibt zum Beispiel gerade einmal

- 646 Carmichael-Zahlen kleiner als 10^9 und
- unterhalb von 10^{15} existieren gerade einmal 105212 Carmichael-Zahlen.

Durch **Speicherung** aller Carmichael-Zahlen unterhalb eines maximalen Wertes in einer Datenstruktur kann man das Problem der Carmichael-Zahlen quasi umgehen.

Algorithmus: Fermat-Test

Fermat-Test:

Input: $n \in \mathbb{N}, n \geq 3, n$ ungerade

Output: „ n ist wahrscheinlich prim.“ oder
„ n ist zusammengesetzt!“

Wähle zufällig $b \in \{2, \dots, n-2\}$;

IF ($\text{ggT}(b, n) \neq 1$) **THEN** „ n ist zusammengesetzt!“

$\text{tmp} := b^{n-1} \bmod n$;

IF ($\text{tmp} \neq 1$) **THEN** „ n ist zusammengesetzt!“

ELSE „ n ist wahrscheinlich prim!“

FI

ELSE

FI

Algorithmus: Fermat-Test

- Fermat-Test liefert die richtige Antwort nur mit einer Wahrscheinlichkeit von ≈ 0.5
- Da wir die Basen $b \in \mathbb{Z}_n^*$ stochastisch unabhängig wählen, können wir jedoch den Fermat-Test iterativ ausführen.
- Wähle verschiedene Basen b_0, b_1, \dots, b_k für jeden einzelnen Test stochastisch unabhängig voneinander. Sodann ergibt sich eine Fehlerwahrscheinlichkeit von $\frac{1}{2^k}$.

Bereits für $k > 25$ ist es wahrscheinlicher vom Blitz getroffen zu werden oder aber das ein Hardwarefehler auftritt als dass der Fermat-Test ein falsches Ergebnis „ausspuckt“.

Der Miller-Rabin-Test

Beispiel

Beispiel:

Sei $n = 341 = 31 \cdot 11$, also eine zusammengesetzte Zahl. Wir wählen $b := 2$.

- Wir berechnen $n - 1 = 2^r s$, wobei s ungerade ist: es ist $341 - 1 = 2^2 \cdot 85$, d.h. $r = 2$ und $s = 85$.
- $x_0 = 2^{85} \bmod 341 = 32$,
 $x_1 = 2^{2 \cdot 85} \bmod 341 = 1 = (x_0)^2 \bmod 341$,
 $x_2 = 2^{4 \cdot 85} \bmod 341 = 1 = (x_1)^2 \bmod 341$.
- Also $x = (32, 1, 1) \Rightarrow 341$ ist zusammengesetzt.

Herleitung des Kriteriums

Der Miller-Rabin-Test ist eine **Weiterentwicklung** des Fermat-Tests.

- n prim $\Rightarrow n - 1$ gerade, d.h. $n - 1 = 2t, t \in \mathbb{N}$.

$$\begin{aligned} b^{n-1} \equiv_n 1 &\Leftrightarrow b^{n-1} - 1 \equiv_n 0 \\ &\Leftrightarrow b^{2t} - 1 \equiv_n (b^t - 1)(b^t + 1) \equiv_n 0 \end{aligned}$$

- Der erste Faktor $(b^t - 1)$ kann durch dasselbe Prinzip faktorisiert werden, falls t gerade.

$$\begin{aligned} \Leftrightarrow b^{n-1} - 1 &\equiv (b^s - 1)(b^s + 1)(b^{2s} + 1)(b^{4s} + 1) \dots (b^{2^{r-1}s} + 1) \\ &\equiv 0 \pmod n \end{aligned}$$

Berechnung der charakteristischen Folge

In Restklassenringen kann man leichter quadrieren als Quadratwurzel ziehen, deshalb fängt man andersherum an:

- Berechne $r, s \in \mathbb{N}$, so dass $n - 1 = 2^r s$ und s ungerade.

Nun berechnet man nacheinander die abbrechende Folge

- $x_0 := b^s \pmod n$,
- $x_1 := b^{2^1 s} \pmod n = x_0^2 \pmod n$,
- $x_2 := b^{2^2 s} \pmod n = x_1^2 \pmod n$,
- ...
- $x_r := b^{2^{r-1} s} \pmod n$,

Ist *wahrscheinlich* n prim, so besitzt die Folge $x := (x_0, \dots, x_r)$ eine besondere Form.

Auswertung der charakteristischen Folge

Mögliche Formen der charakteristischen Folge:

- $(x_0, x_1, \dots, x_r) = (1, \dots, 1)$ oder
 $(x_0, x_1, \dots, x_r) = (\star, \dots, \star, n-1, 1, \dots, 1)$,
wobei $\star \neq 1$ bzw. $\star \neq n-1 = -1$ ist. *Dann ist n wahrscheinlich prim.*
- $(x_0, x_1, \dots, x_r) = (\star, \dots, \star, 1, \dots, 1)$ oder
 $(x_0, x_1, \dots, x_r) = (\star, \dots, \star)$ oder
 $(x_0, x_1, \dots, x_r) = (\star, \dots, \star, n-1)$,
wobei $\star \neq 1$ bzw. $\star \neq n-1 = -1$ ist. *Dann ist n zusammengesetzt.*

Beweis

Man kann $b^{\frac{n-1}{2}} = b^t$ als „Variable“ interpretieren und damit $(b^t)^2 - 1$ als Polynom auffassen.

Beweis:

Nach dem kleinen Fermat gilt für Primzahlen n und $b \in \mathbb{Z}_n^*$ stets die Kongruenz

$$\begin{aligned} b^{n-1} \equiv_n 1 &\Leftrightarrow b^{n-1} - 1 \equiv_n 0 \Leftrightarrow b^{2t} - 1 \equiv_n 0 \\ &\Leftrightarrow X^2 - 1 \equiv_n 0 \end{aligned}$$

Das Polynom $X^2 - 1$ besitzt über endlichen Körpern \mathbb{F}_n ausschließlich die beiden Nullstellen ± 1 , wobei in \mathbb{F}_n gilt:
 $-1 \equiv_n n - 1$.

Finden wir also **nicht triviale Wurzeln** von 1 mod n , dann muss n sicher zusammengesetzt sein.

Starke Pseudoprimzahlen

- Ist das Kriterium „ $X^2 - 1 \equiv_n 0$ besitzt nur triviale Wurzeln“ auch *hinreichend* für den Nachweis einer Primzahl?

Nein!

Beispiel:

$n = 2047 = 23 \cdot 89$ ist eine zusammengesetzte Zahl. Wir wählen $b = 2$ mit $ggT(2, 2047) = 1$. Es gilt dann:

$$x_0 := 2^{\frac{2047-1}{2}} = 2^{1023} \pmod{2047} = 1$$

$$x_1 := (x_0)^2 = 2^{2046} \pmod{2047} = 1$$

Starke Pseudoprimzahlen

Definition:

Eine zusammengesetzte ungerade Zahl n heißt **starke Pseudoprimzahl zur Basis** $b \in (\mathbb{Z}/n\mathbb{Z})^*$ mit $n - 1 = 2^r s$ und s ungerade, und falls

- entweder $b^s \pmod n = 1$ ist mit s ungerade, **oder**
- es ein i mit $0 \leq i < r$ gibt, so dass $b^{2^i s} \equiv_n \pm 1$ gilt.

Erfreulich ist aber, dass es zu den *starken* Pseudoprimzahlen **kein** Analogon zu den Carmichael-Zahlen gibt, d.h. der Miller-Rabin-Test ist in der Tat eine Weiterentwicklung des Fermat-Tests!

Beispiel

Beispiel:

$n = 2047 = 23 \cdot 89$ ist eine starke Pseudoprimzahl zur Basis $b = 2$.
Es ist $2047 - 1 = 2^1 \cdot 1023$, d.h. $r = 1$ und $s = 1023$.

$$x_0 := 2^{\frac{2047-1}{2}} = 2^{1023} \pmod{2047} = 1$$

$$x_1 := (x_0)^2 = 2^{2046} \pmod{2047} = 1$$

Fehlerwahrscheinlichkeit

Rabin hat gezeigt, dass eine zusammengesetzte Zahl n für höchstens $\frac{1}{4}$ aller Elemente $b \in (\mathbb{Z}/n\mathbb{Z})^*$ eine starke Pseudoprimzahl zur Basis b ist.

SATZ

Sei n eine zusammengesetzte ungerade Zahl. Dann gilt für höchstens die Hälfte aller $b \in (\mathbb{Z}/n\mathbb{Z})^$, dass n eine starke Pseudoprimzahl zur Basis b ist.*

Beweis: siehe Ausarbeitung!

Der Algorithmus

Miller-Rabin-Test:

Input: $n \in \mathbb{N}, n \geq 3, n$ ungerade.

Output: „ n ist wahrscheinlich prim.“ oder „ n ist zusammengesetzt!“

Bestimme die Zahlen $r, s \in \mathbb{N}$, so dass $n - 1 = 2^r s$ und s ungerade;

Wähle zufällig $b \in \{2, \dots, n - 2\}$;

$x_0 := b^s \pmod n$;

IF ($x_0 = \pm 1$) **THEN** „ n ist wahrscheinlich prim!“

$x_i := (x_{i-1})^2 \pmod n$;

IF $x_i = -1$ **THEN** „ n ist wahrscheinlich prim.“

ELSE „ n ist zusammengesetzt!“

FI

ELSE **FOR** $i := 1$ **TO** $r-1$;
FI

Der Solovay-Strassen-Test

Quadratische Reste

Definition:

Sei $n \in \mathbb{N}$, $n > 1$ vorgegeben. Eine zu n teilerfremde Zahl $a \in \mathbb{Z}_n^*$ heißt **quadratischer Rest** modulo n , wenn es ein $x \in \mathbb{Z}$ gibt, so dass $x^2 \equiv_n a$.

Zwei modulo n quadratische Reste $a, a' \in \mathbb{Z}$ heißen **verschieden**, wenn gilt $a \not\equiv_n a'$. Eine zu n teilerfremde Zahl a heißt **quadratischer Nichtrest** modulo n , wenn a kein quadratischer Rest modulo n ist.

Beispiel

Beispiel:

Wir bestimmen die quadratischen Reste modulo $n := 9$:

$$1^2 \equiv_9 1,$$

$$2^2 \equiv_9 4$$

$$4^2 \equiv_9 7,$$

$$5^2 \equiv_9 7$$

$$7^2 \equiv_9 7,$$

$$8^2 \equiv_9 1.$$

Wir sehen, dass 1,4 und 7 quadratische Reste, dagegen 2,5 und 8 quadratische Nichtreste sind.

Problemreduktion

Für unsere Bedürfnisse reicht es jedoch sich auf quadratische Reste modulo p , p eine **Primzahl**, zu beschränken. Für eine Primzahl p ist $a \in \mathbb{Z}_p^*$ genau dann ein quadratischer Rest \pmod{p} , wenn es ein $x \in \mathbb{Z}$ existiert, so dass die Kongruenz $x^2 \equiv_n a$ lösbar ist.

Wieviele $a \in \mathbb{Z}_p^$ sind Quadratwurzeln, also von der Form $a = b^2 \pmod{p}$ für ein $b \in \mathbb{Z}_p^*$?*

Anzahl der quadratischen Reste?

Lemma

Sei $p > 2$ eine Primzahl. Dann sind die Hälfte der Elemente in \mathbb{Z}_p^ quadratische Reste, und die andere Hälfte sind quadratische Nichtreste modulo p .*

Beweis:

Sei g ein primitives Element von $(\mathbb{Z}/p\mathbb{Z})^*$, dann ist $a = g^j \pmod p$ eine Quadratzahl genau dann, wenn $j \in \mathbb{Z}$ gerade ist:

„ \Rightarrow “: Ist nämlich $j \in \mathbb{Z}$ gerade, d.h. $j = 2k$ für ein $k \in \mathbb{Z}$, dann gilt $a \equiv_p g^j \equiv_p (g^k)^2 \equiv_p g^{2k}$, also eine Quadratzahl.

„ \Leftarrow “: Ist andererseits a eine Quadratzahl, also $a = b^2 \pmod p$ mit $b \in (\mathbb{Z}/p\mathbb{Z})^*$, dann gilt $b = g^k \pmod p$ für ein $k \in \mathbb{Z}$, und $a \equiv_p b^2 \equiv_p (g^k)^2 \equiv_p g^{2k}$, also ist $a = g^j \pmod p$ für ein $k \in \mathbb{Z}$.

Legendre-Symbol

Definition:

Sei $a \in \mathbb{Z}$ und $p > 2$ eine Primzahl. Das **Legendre-Symbol** $\left(\frac{a}{p}\right)$ ist definiert als

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & , \text{ falls } p|a \\ 1 & , \text{ falls } a \pmod{p} \text{ quadratischer Rest modulo } p \\ -1 & , \text{ falls } a \pmod{p} \text{ quadratischer Nichtrest modulo } p \end{cases}$$

Beispiel

Beispiel:

Sei $p = 7$, also prim. Dann besteht die Einheiten-Gruppe $(\mathbb{Z}/7\mathbb{Z})^*$ aus $\phi(7) = 6$ Elementen, nämlich aus den Restklassen $\{1, 2, 3, 4, 5, 6\}$. Es gilt

$$\begin{array}{ll} 1^2 \equiv_7 6^2 \equiv_7 1, & 2^2 \equiv_7 5^2 \equiv_7 4 \\ 3^2 \equiv_7 4^2 \equiv_7 2, & 0^2 \equiv_7 7^2 \equiv_7 0 \end{array}$$

Es sind also $\left(\frac{0}{7}\right) = 0$ und $\left(\frac{1}{7}\right) = \left(\frac{4}{7}\right) = \left(\frac{2}{7}\right) = 1$ und $\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1$.

Kriterium von Euler

Das für Primzahlen notwendige Kriterium für den Solovay-Strassen-Test liefert uns folgender

SATZ

Sei $a \in \mathbb{Z}$ und $p > 2$ eine Primzahl. Dann gilt

$$a^{\frac{p-1}{2}} \equiv_p \left(\frac{a}{p} \right). \quad (3)$$

Beweis: Falls Zeit ausreichend an Tafel, sonst siehe Skript.

Jacobi-Symbol

Die Definition des Legendre-Symbols erweitern wir nun auf beliebige *ungerade* Zahlen.

Definition:

Sei $n > 2$ eine ungerade Zahl und sei $a \in \mathbb{Z}$. Sei $n = \sum_{i=1}^r p_i^{\alpha_i}$ die Primfaktorzerlegung von n , wobei $p_i \neq p_j$ für $j \neq i$ und $1 \leq i, j \leq r$ gilt. Das **Jacobi-Symbol** ist definiert als

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)^{\alpha_1} \cdot \dots \cdot \left(\frac{a}{p_r}\right)^{\alpha_r}.$$

Legendre-Symbol als Spezialfall des Jacobi-Symbols

n **prim** \Rightarrow Jacobi- und Legendre-Symbol stimmen überein.
 n **zusammengesetzt** \Rightarrow Jacobi-Symbol macht **keine** Aussage darüber, ob $a \pmod n$ ein quadratischer Rest ist!

Beispiel:

$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \left(\frac{2}{5}\right) = (-1)(-1) = 1$. Es ist 2 ein quadr. Nichtrest in \mathbb{Z}_3^* und in \mathbb{Z}_5^* .

2 ist aber auch ein quadr. Nichtrest in \mathbb{Z}_{15}^* .

Notwendig aber nicht hinreichend!

Sei $n > 2$ eine ungerade zusammengesetzte Zahl und $a \in \mathbb{Z}_n^*$.
Aufgrund von $\left(\frac{a}{n}\right) = 1$ kann keine Aussage darüber getroffen werden, ob a ein quadratischer Rest bzw. Nichtrest in \mathbb{Z}_n^* ist.

Mit anderen Worten: $\left(\frac{a}{n}\right) = 1$ ist *nicht hinreichend*, wie wir aber noch sehen werden eine *notwendige* Bedingung dafür, dass a ein quadratischer Rest ist.

Notwendig aber nicht hinreichend!

Lemma

Sei $n > 2$ eine ungerade und zusammengesetzt, und sei $a \in \mathbb{Z}_n^*$. Ist a ein quadratischer Rest in \mathbb{Z}_n^* , d.h., es gibt ein $b \in \mathbb{Z}_n^*$ mit $b^2 \bmod n = a$, dann muss $\left(\frac{a}{n}\right) = 1$ gelten.

Beweis:

Sei $n = \sum_{i=1}^r p_i^{\alpha_i}$ die Primfaktorzerlegung von n . Für $1 \leq i \leq r$ gilt dann $b^2 \equiv_{p_i} a$, also ist a ein quadratischer Rest modulo p_i . Es folgt damit

$$\begin{aligned}\left(\frac{a}{n}\right) &= \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_r}\right)^{\alpha_r} \\ &= 1^{\alpha_1} \cdots 1^{\alpha_r} = 1\end{aligned}$$

Idee des Solovay-Strassen-Tests

Für eine ungerade Zahl $n > 2$ wird ein $2 \leq b \leq n - 2$ und $\text{ggT}(b, n) = 1$ gewählt und getestet, ob

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n} \right) \pmod{n} \quad (4)$$

gilt. Ist n prim dann gilt die Bedingung (4) nach dem Kriterium von Euler stets.

Allerdings existieren zusammengesetzte Zahlen n und Zahlen $b \in \mathbb{N}$ mit $0 < b < n$ und $\text{ggT}(b, n) = 1$, so dass Bedingung (4) gilt.

Eulerschen Pseudoprimzahlen

Beispiel:

Die Zahl $n := 2047 = 23 \cdot 89$ ist offensichtlich zusammengesetzt, doch für $b := 2$ gilt $2^{1023} \equiv 1 = \left(\frac{2}{2047}\right) \pmod{2047}$.

Definition:

Sei $n > 2$ ungerade und zusammengesetzt. Sei $b \in (\mathbb{Z}/n\mathbb{Z})^*$. Die Zahl n heißt **Eulersche Pseudoprimzahl zur Basis b** , wenn $b^{\frac{n-1}{2}} \equiv_n \left(\frac{b}{n}\right)$ gilt.

Eulerschen Pseudoprimitiven

Lemma

Sei $n > 2$ eine ungerade, zusammengesetzte Zahl. Dann gilt für mindestens die Hälfte aller $b \in (\mathbb{Z}/n\mathbb{Z})^$, dass n keine Eulersche Pseudoprimitiv zur Basis b ist.*

Das Lemma zeigt, dass es kein Analogon zu den Carmichael-Zahlen gibt! Ein Beweis wird nicht geführt.

Der Algorithmus

Solovay-Strassen-Test:

Input: $n \in \mathbb{N}, n \geq 3, n$ ungerade.

Output: „ n ist wahrscheinlich prim.“ oder „ n ist zusammengesetzt!“

Wähle zufällig $b \in \{2, \dots, n-2\}$;

Berechne $b^{\frac{n-1}{2}} \pmod n$ und $\left(\frac{b}{n}\right)$;

IF $\left(b^{\frac{n-1}{2}} \pmod n \equiv_n \left(\frac{b}{n}\right)\right)$

„ n ist wahrscheinlich prim.“

Else „ n ist zusammengesetzt!“

IF ($\text{ggT}(b, n) = 1$) **THEN**

ELSE „ n ist zusammengesetzt!“

FI