Carmichaelzahlen und andere Pseudoprimzahlen

Christian Glusa

26.05.2008

1 Der fermatsche Primzahltest

Erinnerung 1 (Kleiner Satz von Fermat)**.** *Für p prim, $a \in \mathbb{Z}$, $\mathrm{ggT}(a,p) = 1$ gilt:*
$$a^{p-1} \equiv 1 \pmod{p}$$

Algorithmus 2 (Fermatscher Primzahltest)**.** *Input: $n \in \mathbb{N}$ ungerade*
`Wähle a` $\in \{2, \ldots, \mathtt{n}-2\}$ `# 1 und n-1 machen keinen Sinn`
$\mathtt{b} := \mathtt{a}^{\mathtt{n}-1} \equiv 1 \pmod{\mathtt{n}}$
Output: „zusammengesetzt“, wenn $b \neq 1$, sonst „vielleicht prim“

Dieser Algorithmus benötigt $O((\mathrm{ld}\, n)^3)$ Bitoperationen (Potenzierungsalgorithmus, $\mathrm{ld} = \log_2$)
Falls $\mathrm{ggT}(a,n) \neq 1$ gilt, gibt der Test das richtige Ergebnis aus:
$\mathrm{ggT}(a,n) \neq 1,\ a \in \{2,\ldots,n-2\} \Rightarrow \exists d \in \{2,\ldots n-2\} : d \mid a, d \mid n \Rightarrow d \mid a^{n-1} \Rightarrow d \mid b := a^{n-1} \pmod{n} \Rightarrow b \neq 1$
Für $\mathrm{ggT}(a,n) = 1$ gibt der Algorithmus jedoch manchmal etwas falsches zurück.

Definition 3. *Sei $n \in 2\mathbb{N}+1$ zusammengesetzt , $a \in \mathbb{N}$*

1. *n heißt (fermatsche) Pseudoprimzahl zur Basis a $:\Leftrightarrow$ n ist keine Primzahl und $a^{n-1} \equiv 1 \pmod{n}$*
2. *$psp(a) = \{k \in 2\mathbb{N}+1 : k$ ist Pseudoprimzahl zur Basis $a\}$*
3. *Die Gruppe $F(n) = \{b \in (\mathbb{Z}/n\mathbb{Z})^\times : b^{n-1} \equiv 1 \pmod{n}\}$ sind die Fermat-Lügner von n*
4. *n heisst Carmichael-Zahl $:\Leftrightarrow F(n) = (\mathbb{Z}/n\mathbb{Z})^\times$*

Dass $F(n)$ eine Gruppe ist, lässt sich recht einfach mit dem Untergruppenkriterium zeigen. Für eine Carmichael-Zahl oder eine Primzahl gibt der Algorithmus unabhängig von der Wahl von a immer „vielleicht prim“ zurück. Wenn n weder eine Carmichael-Zahl, noch prim ist, so ist die Wahrscheinlichkeit eines korrekten Resultats größer als $1/2$, denn dann ist $|F(n)| \leq \frac{1}{2}|(\mathbb{Z}/n\mathbb{Z})^\times|$ (Satz von Lagrange).
Wir wissen also, dass der Primzahltest bei Carmichael-Zahlen total versagt. Aber gibt es überhaupt welche? Um die Suche nach ihnen zu vereinfachen, bedienen wir uns der sogenannten Carmichael-Lambda-Funktion:

Definition und Bemerkung 4.

1. $\lambda(n) := \min\{e \in \mathbb{N} : \forall a \in (\mathbb{Z}/n\mathbb{Z})^\times : a^e = 1\}$
2. *n ist Carmichael-Zahl* $\Leftrightarrow \lambda(n) \mid n-1$

Nun müssen wir allerdings auch eine (einfache) Rechenvorschrift für $\lambda(n)$ angeben:

Satz 5. *Der Wert der Lambda-Funktion lässt sich wie folgt bestimmen:*

1. $\lambda(1) = 1$
2. $\lambda(p^e) = (p-1)p^{e-1}$ *für* $p \geq 3$ *prim,* $e \geq 1$
3. $\lambda(2) = 1, \lambda(4) = 2, \lambda(2^e) = 2^{e-2}$ *für* $e \geq 3$
4. $\lambda(n) = \mathrm{kgV}\{\lambda(p_i^{e_i}) : 1 \leq i \leq k\}$, *falls* $n = \prod_{1 \leq i \leq k} p_i^{e_i}$ *Primfaktorzerlegung ist.*

Beweis. 1. ist klar, 2. und 3. folgen aus der stärkeren Aussage über die Struktur von $(\mathbb{Z}/p^e\mathbb{Z})^\times$ durch Satz 7

4. Sei $e := \mathrm{kgV}\{\lambda(p_i^{e_i})\} \Rightarrow \forall a \in (\mathbb{Z}/n\mathbb{Z})^\times : a^e = 1 \Rightarrow \lambda(n) \leq e$
   Wähle $a_i \in (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times$ mit $\mathrm{ord}(a_i) = \lambda(p_i^{e_i})$
   Chinesischer Restsatz $\Rightarrow \exists x \in (\mathbb{Z}/n\mathbb{Z})^\times \, \forall \, 1 \leq i \leq k : x \equiv a_i \pmod{p_i^{e_i}}$
   $\Rightarrow \lambda(n) \geq e$

□

Als Vorbereitung für den Satz über die Struktur von $(\mathbb{Z}/p^e\mathbb{Z})^\times$ benötigen wir:

Definition und Bemerkung 6. *Sei* $n \in \mathbb{Z}$.

1. $\mathrm{ord}_p(n) := \max\{e \in \mathbb{N} : p^e \mid n\}$ *heißt die Ordnung von* p *in* n.
2. *Ist* $n = a_0 + a_1 p + \cdots + a_r p^r$ *die* p*-Entwicklung von* n, *so heißt* $s_p := a_0 + a_1 + \cdots + a_r$ *die* p*-Quersumme von* n.
3. $\mathrm{ord}_p(n!) = \frac{1}{p-1}(n - s_p(n))$

Beweis.

3. $n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n$, also ist $\operatorname{ord}_p(n!) = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \ldots \lfloor \frac{n}{p^r} \rfloor$
$\Rightarrow \operatorname{ord}_p(n!) = (a_1 + a_2 p + \cdots + a_r p^{r-1}) + (a_2 + a_3 p + \cdots + a_r p^{r-2}) + \cdots + a_r$
$= a_1 + a_2(1+p) + a_3(1+p+p^2) + \cdots + a_r(1+p+\cdots+p^{r-1})$
$\Rightarrow (p-1)\operatorname{ord}_p(n!) = a_0(1-1) + a_1(p-1) + a_2(p^2-1) + \cdots + a_r(p^r-1)$
$= n - s_p(n)$

□

Satz 7. *Sei $n \in \mathbb{N}_{>0}$*

1. *Für $p \geq 3$, p prim ist $(\mathbb{Z}/p^n\mathbb{Z})^\times$ zyklisch.*
2. *$(\mathbb{Z}/2\mathbb{Z})^\times$ und $(\mathbb{Z}/4\mathbb{Z})^\times$ sind zyklisch, $(\mathbb{Z}/2^n\mathbb{Z})^\times \cong \langle\overline{5}\rangle \times \langle\overline{-1}\rangle, \operatorname{ord}(\overline{5}) = 2^{n-2}, \operatorname{ord}(\overline{-1}) = 2$ für $n \geq 3$*

Beweis.

1. Wir zeigen die Behauptung, indem wir ein Element mit Ordnung $(p-1)p^{n-1}$ angeben.
Sei $v \in \mathbb{N}$ so, dass v eine Primitivwurzel modulo p ist (Gibt es nach Vortrag 3)
Satz von Fermat $\Rightarrow v^p \equiv v \pmod{p}$
$\Rightarrow v^{p^2} \equiv v^p \equiv v \pmod{p}$
$\ldots \Rightarrow v^{p^{n-1}} \equiv v \pmod{p}$
$\Rightarrow w := v^{p^{n-1}}$ ist Primitivwurzel modulo p
$w^{p-1} = v^{(p-1)p^{n-1}} = v^{\varphi(p^n)} \equiv 1 \pmod{p^n}$
$\Rightarrow \bar{w}^{p-1} = 1$ in $\mathbb{Z}/p^n\mathbb{Z}$
$\Rightarrow \operatorname{ord}(\bar{w}) \mid p-1$, aber $\operatorname{ord}(\bar{w}) \geq p-1$, da w Primitivwurzel modulo p ist.
$\Rightarrow \operatorname{ord}(\bar{w}) = p-1$
Außerdem gilt:
$(1+p)^{p^{n-1}} = 1 + \binom{p^{n-1}}{1}p + \cdots + \binom{p^{n-1}}{p^{n-1}-1}p^{p^{n-1}-1} + p^{p^{n-1}}$

Behauptung. $p^n \mid \binom{p^{n-1}}{m}p^m$ *für* $1 \leq m \leq p^{n-1}$

$\Rightarrow (1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$
$(1+p)^{p^{n-2}} = 1 + \binom{p^{n-2}}{1}p + \cdots + \binom{p^{n-2}}{p^{n-2}-1}p^{p^{n-2}-1} + p^{p^{n-2}}$

Behauptung. $p^n \mid \binom{p^{n-2}}{m}p^m$ *für* $2 \leq m \leq p^{n-2}$

$\Rightarrow (1+p)^{p^{n-2}} \equiv 1 + p^{n-1} \not\equiv 1 \pmod{p^n}$
$\Rightarrow \operatorname{ord}(\overline{1+p}) = p^{n-1}$ in $(\mathbb{Z}/p^n\mathbb{Z})^\times$
Somit hat $\bar{z} := \bar{w}(\overline{1+p})$ Ordnung $(p-1)p^{n-1}$, da $\operatorname{ggT}(p-1, p^{n-1}) = 1$ ist, und erzeugt $(\mathbb{Z}/p^n\mathbb{Z})^\times$, das ja gerade $\varphi(p^n) = (p-1)p^{n-1}$ Elemente hat.

Beweis der Behauptungen.
Für $1 \leq m \leq p^{n-1}$ gilt:
$\operatorname{ord}_p(\binom{p^{n-1}}{m}p^m) = \operatorname{ord}_p(\frac{(p^{n-1})!}{m!(p^{n-1}-m)!}) + \operatorname{ord}_p(p^m)$
$= \frac{1}{p-1}(p^{n-1} - m - p^{n-1} + m - s_p(p^{n-1}) + s_p(m) + s_p(p^{n-1}-m)) + m$
$= \frac{1}{p-1}(-1 + \underbrace{s_p(m)}_{\geq 1} + s_p(p^{n-1}-m)) + m$
$\geq \frac{1}{p-1}s_p(p^{n-1}-m) + m$
Nun gilt aber mit $k := \min\{e \in \mathbb{N} : p^e \geq m\}$
$s_p(p^{n-1}-m) \geq s_p(p^{n-1}-p^k) = s_p(\sum_{j=k}^{n-1}(p-1)p^j) = (p-1)(n-1-k)$
Somit: $\operatorname{ord}_p(\binom{p^{n-1}}{m}p^m) \geq n-1-k+m$
Andererseits gilt:
$m \geq k+1$, denn
$k = 0\ (\Leftrightarrow m = 1):$ $\quad m = 1 \geq 0 + 1 = k + 1$
$k \geq 1\ (\Leftrightarrow p^k \geq m > p^{k-1}):$ $\quad m > p^{k-1} \geq 3^{k-1} \geq k \Rightarrow m \geq k+1$
Also gilt:
$\operatorname{ord}_p(\binom{p^{n-1}}{m}p^m) \geq n$
Die zweite Behauptung lässt sich ähnlich beweisen. □

2. $(\mathbb{Z}/2\mathbb{Z})^\times = \langle\overline{1}\rangle$ und $(\mathbb{Z}/4\mathbb{Z})^\times = \langle\overline{3}\rangle$ sind zyklisch
   Wie bei 1. zeigt man:
   $5^{2^{n-2}} = (1+2^2)^{2^{n-2}} = 1 + \binom{2^{n-2}}{1}2^2 + \cdots + 2^{2^{n-1}} \equiv 1 \pmod{2^n}$
   $5^{2^{n-3}} = (1+2^2)^{2^{n-3}} = 1 + \binom{2^{n-3}}{1}2^2 + \cdots + 2^{2^{n-2}} \equiv 1 + 2^{n-1} \pmod{2^n}$
   Klar ist: $(-1)^2 \equiv 1 \pmod{2^n}$, $\quad -1 \not\equiv 1 \pmod{2^n}$
   Angenommen, es gäbe $i, i' \in \{0,1\}$ und $j, j' \in \{0, 1, \ldots 2^{n-2}-1\}$ mit
   $(-1)^i 5^j \equiv (-1)^{i'} 5^{j'} \pmod{2^n} \Rightarrow (-1)^{i-i'} \equiv 5^{j'-j} \pmod{2^n}$
   Aus $i \neq i'$ folgt der Widerspruch $(-1)^{-1} \equiv -1 \not\equiv 1 \equiv 5^{j'-j} \pmod 4$.
   Also ist $i = i'$ und damit auch $j = j'$. Somit hat das Erzeugnis von $\overline{-1}$ und $\overline{5}$ Ordnung 2^{n-1}

□

Satz 8. *n ist Carmichael-Zahl $\Rightarrow$ n ist ungerade, quadratfrei und enthält mindestens drei Faktoren.*

Beweis. Es gilt $n > 2$, daher $2 \mid \lambda(n)$, da für eine in n enthaltene Primfaktorpotenz p^e gilt: $2 \mid \lambda(p^e) \mid \lambda(n)$.

1. n ist ungerade:
   $2 \mid \lambda(n) \mid n-1 \Rightarrow n$ ungerade

2. n quadratfrei:
   Angenommen, $\exists p$ prim: $p^2 \mid n$
   $\Rightarrow p \mid (p-1)p^{e-1} = \lambda(p^e) \mid \lambda(n) \mid n-1$
   $\Rightarrow p \mid n \ \wedge\ p \mid n-1 \Rightarrow p \mid 1$ $\quad \lightning$

3. n hat mindestens 3 Primfaktoren:
   Angenommen, $n = pq$, p, q verschiedene, ungerade Primzahlen
   $\Rightarrow p - 1 \mid \lambda(n) \mid n - 1$
   $\Rightarrow pq - 1 = n - 1 \equiv 0 \pmod{p-1}$
   Mit $p \equiv 1 \pmod{p-1}$ folgt $q \equiv 1 \pmod{p-1}$ und somit $q \geq p$
   Analog folgt $p \geq q$, womit $p = q$ $\lightning$

□

Dieser Satz schränkt die Menge der infrage kommenden Zahlen schon erheblich ein. Man findet durch Probieren als kleinste Carmichael-Zahl 561:

$$\lambda(561) = \lambda(3 \cdot 11 \cdot 17) = kgV(2, 10, 16) = 80 \text{ und } 80 \mid 560.$$

Es wurde erst vor etwa 10 Jahren gezeigt, dass es sogar unendlich viele Carmichael-Zahlen gibt.

2 Das Jacobi-Symbol

Erinnerung 9 (Legendre-Symbol)**.** *p ungerade Primzahl, $a \in \mathbb{Z}$*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \textit{wenn } a \textit{ ein quadratischer Rest zu } p \textit{ ist} \\ -1 & \textit{wenn } a \textit{ kein quadratischer Rest zu } p \textit{ ist} \\ 0 & \textit{wenn } a \textit{ und } p \textit{ nicht teilerfremd sind} \end{cases}$$

Das Jacobi-Symbol ist eine Erweiterung des Legendre-Symbols auf ungerade positive Zahlen:

Definition 10. *Sei n eine ungerade Zahl mit Primfaktorzerlegung $n = \prod_{i=1}^{k} p_i^{e_i}$, $a \in \mathbb{Z}$*

$$\left(\frac{a}{n}\right) := \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}$$

Insbesondere sei $\left(\frac{a}{1}\right) := 1$

Auch die Eigenschaften des Legendre-Symbols lassen sich übertragen und ähnlich beweisen:

Satz 11. *m, n ungerade und positiv, $a, b \in \mathbb{Z}$*

1. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
2. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$
3. $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$, *wenn* $a \equiv b \pmod{n}$
4. $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2} = \begin{cases} 1 & n \equiv 1 \pmod 4 \\ -1 & n \equiv 3 \pmod 4 \end{cases}$

5. $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8} = \begin{cases} 1 & n \equiv 1 \text{ oder } 7 \pmod 8 \\ -1 & n \equiv 3 \text{ oder } 5 \pmod 8 \end{cases}$

6. *(Quadratische Reziprozitätsgesetz)*
Wenn $\mathrm{ggT}(n,m) = 1$, *dann*
$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}$ *bzw.* $\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}\left(\frac{n}{m}\right)$

Beweis.
1. und 3. folgen aus den Eigenschaften des Legendre-Symbols, 2. aus der Definition des Jacobi-Symbols.
Schreibe $n = n_1 n_2 \cdots n_k$, n_i prim und ungerade und zerlege mit 2.

4. Es gilt mit $4 \mid (n_i - 1)(n_j - 1)$:
$n_1 n_2 \cdots n_k - 1 = (n_1 - 1 + 1) \cdots (n_k - 1 + 1) - 1 \equiv (n_1 - 1) + \cdots + (n_k - 1) \pmod 4$

5. Es gilt mit $16 \mid (n_i^2 - 1)(n_j^2 - 1) = (n_i - 1)(n_i + 1)(n_j - 1)(n_j + 1)$:
$n_1^2 n_2^2 \cdots n_k^2 - 1 = (n_1^2 - 1 + 1) \cdots (n_k^2 - 1 + 1) - 1 \equiv (n_1^2 - 1) + \cdots + (n_k^2 - 1) \pmod{16}$

6. Schreibe $m = m_1 m_2 \cdots m_l$, m_i prim und ungerade und zerlege mit 1. und 2.
$(m_1 m_2 \cdots m_l - 1)(n_1 n_2 \cdots n_k - 1) \mod 8$
$= (m_1 m_2 \cdots m_l - 1 \mod 8)(n_1 n_2 \cdots n_k - 1 \mod 8)$
$= [(m_1 - 1) + \cdots + (m_l - 1) + \sum_{(i,j)}(m_i - 1)(m_j - 1) \mod 8]$
$\cdot[(n_1 - 1) + \cdots + (n_k - 1) + \sum_{(i,j)}(n_i - 1)(n_j - 1) \mod 8]$
$= \sum_{(i,j)}(m_i - 1)(n_j - 1) \mod 8$

□

Es gilt immer noch, dass $\left(\frac{a}{n}\right) = 1$ ist, wenn n prim ist und a ein quadratischer Rest modulo n. Für Nicht-Primzahlen gilt dies allerdings nicht unbedingt:
$\left(\frac{8}{15}\right) = \left(\frac{8}{3}\right)\left(\frac{8}{5}\right) = \left(\frac{2}{3}\right)\left(\frac{3}{5}\right) = (-1)(-1) = 1$, aber $8^{(15-1)/2} \equiv 2 \pmod{15}$

Um das Jacobi-Symbol einer ungeraden, positiven Zahl n und einer ganzen Zahl a zu berechen, verwenden wir die gerade gezeigten Eigenschaften: Wir dürfen o.B.d.A. annehmen, dass $0 < a < n$ ist (Falls $a \geq n$ oder $a < 0$ können wir es mit Eigenschaft 3 reduzieren, falls $a = 0$ ist, folgt $\left(\frac{a}{n}\right) = 0$ für $n \neq 1$).
Wir finden nun $e \geq 0$, $q \in \mathbb{Z}$, n' ungerade und $0 \leq a' < n'$ mit

$$a = 2^e n' \quad n = qn' + a'$$

Durch Eigenschaften 1,5,6 und 3 finden wir:

$$\left(\frac{a}{n}\right) = (-1)^s \left(\frac{a'}{n'}\right) \quad s = e\frac{n^2-1}{8} + \frac{n-1}{2} + \frac{n'-1}{2}$$

Dies gilt auch im Fall $\mathrm{ggT}(a,n) > 1$, da dann beide Seiten 0 sind. Es gilt $0 \leq a' < n' \leq a < n$, wir haben das Problem also auf ein Problem mit kleineren Werten zurückgeführt. Wir müssen dieses Verfahren nur solange durchführen, bis $a = 0$, was nach endlich vielen

Schritten eintritt. Am Schluss erhalten wir also einen Ausdruck der Form

$$\left(\frac{0}{n}\right) = \begin{cases} 1 & n = 1 \\ 0 & sonst \end{cases}$$

Algorithmus 12. *Input:* $0 < a < n, n$ *ungerade*

```
t := 1
solange (a ≠ 0)  {
  solange (a mod 2 = 0)  {
    a := a/2                                  # 2-er Potenz herausdividieren
    wenn (n mod 8 = 3) oder (n mod 8 = 5) dann
      t := −t                                 # Mit (2/n) multipl.
  }
  tausche(a, n)
  wenn (a mod 4 = 3) und (n mod 4 = 3) dann
      t := −t                 # Quadratisches Reziprozitätsgesetz ausnutzen
  a := a mod n
}
```

Output: t wenn $n = 1$*, sonst 0*

Dieser Algorithmus benötigt $O((\mathrm{ld}\, a)(\mathrm{ld}\, n))$ Bitoperationen.

3 Eulersche und Starke Pseudoprimzahlen

Erinnerung 13 (Euler-Kriterium)**.** *p prim,* $a \in \mathbb{Z}, \mathrm{ggT}(a, p) = 1$

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

Da wir durch das Jacobi-Symbol das Legendre-Symbol erweitert haben, können wir jetzt auch beliebige positive ungerade Zahlen einsetzen, was zu folgender Definition Anlass gibt:

Definition 14. *Sei* $n \in 2\mathbb{N} + 1$ *zusammengesetzt,* $a \in \mathbb{N}$ *mit* $\mathrm{ggT}(a, n) = 1$

1. *n heißt eulersche Pseudoprimzahl zur Basis* $a :\Leftrightarrow a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$.
2. $epsp(a) := \{n \in 2\mathbb{N} + 1 : n$ *ist eulersche Pseudoprimzahl zur Basis* $a\}$

Wenn n eine Primzahl ist, dann ist das Euler-Kriterium auf jeden Fall erfüllt, ansonsten wird sich $\left(\frac{a}{n}\right)$ irgendwie zufällig verhalten. Wir haben hiermit einen echt stärkeren Primzahltest als den fermatschen, da es kein Analogon zu den Carmichael-Zahlen gibt. (Ohne Beweis, es gilt $|\{a \in (\mathbb{Z}/n\mathbb{Z})^\times : n$ ist Pseudoprimzahl zur Basis $a\}| \leq 1/2|(\mathbb{Z}/n\mathbb{Z})^\times|$) Dieser Test wird Solovay-Strassen-Test genannt. Eine weitere Verschärfung des Tests erreichen wir durch den Miller-Rabin-Test, der uns auf die sogenannten starken Pseudoprimzahlen führt.

Definition 15. *Sei $n \in 2\mathbb{N}+1$ zusammengesetzt, $n-1 = 2^s d$, wobei $2 \nmid d$ und $a \in \mathbb{Z}$*

1. *n heißt starke Pseudoprimzahl zur Basis a*
   $:\Leftrightarrow a^d \equiv 1 \pmod{n}$ oder $a^{2^r d} \equiv -1 \pmod{n}$ für ein $r \in \{0, \ldots, s-1\}$
2. *$spsp(a) := \{n \in 2\mathbb{N}+1 : n$ ist starke Pseudoprimzahl zur Basis $a\}$*

Dass der Miller-Rabin-Test eine Verschärfung des Solovay-Strassen-Tests ist, der wiederum eine Verschärfung des fermatschen Primzahltest ist, sagt der folgende Satz aus.

Satz 16. *$spsp(a) \subseteq epsp(a) \subseteq psp(a)$*

Beweis. "$epsp(a) \subseteq psp(a)$": $a^{n-1} = (a^{\frac{n-1}{2}})^2 \equiv \left(\frac{a}{n}\right)^2 \equiv 1 \pmod{n}$
"$spsp(a) \subseteq epsp(a)$":
Sei $n \in \mathbb{N}$ ungerade, schreibe $n-1 = 2^s d$, d ungerade (Merke: $s \geq 1$).
$n \in spsp(a) \Rightarrow a^d \equiv 1 \pmod{n} \vee a^{2^r d} \equiv -1 \pmod{n}$ für ein $r \in \mathbb{N}, 0 \leq r < s$
1. Fall: $a^d \equiv 1 \pmod{n}$
Es gilt $a^{\frac{n-1}{2}} = (a^d)^{2^{s-1}} \equiv 1 \pmod{n}$ und $1 = \left(\frac{1}{n}\right) = \left(\frac{a^d}{n}\right) = \left(\frac{a}{n}\right)^d = (\pm 1)^d$.
Daher: $\left(\frac{a}{n}\right) = 1$ (denn d ist ungerade) und somit:
$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$
2. Fall: $a^{2^{s-1}d} \equiv -1 \pmod{n}$ $(r = s-1)$
$a^{\frac{n-1}{2}} = a^{2^{s-1}d} \equiv -1 \pmod{n}$
Also ist zu zeigen: $\left(\frac{a}{n}\right) = -1$
Schreibe $n = p_1 \cdot p_2 \cdots p_l$, p_i prim, ungerade und nicht notwendig verschieden und $p_i - 1 = 2^{s_i} d_i$, wobei d_i ungerade sei.

Behauptung. *$s_i \geq s$ und* $\left(\frac{a}{p_i}\right) = \begin{cases} -1 & \text{wenn } s = s_i \\ 1 & \text{wenn } s < s_i \end{cases}$ *für alle $1 \leq i \leq l$*

Beweis. Aus $a^{2^{s-1}d} \equiv -1 \pmod{n}$ folgt:
$(a^{2^{s-1}d_i})^d \equiv -1 \pmod{n}$
$\overset{p_i \mid n}{\Rightarrow} (a^{2^{s-1}d_i})^d \equiv -1 \pmod{p_i}$
$\Rightarrow a^{2^r d_i} \equiv -1 \pmod{p_i}$
Falls $s_i < s$: $a^{2^{s_i} d_i} = a^{p_i - 1} \not\equiv 1 \pmod{p_i}$ $\quad \lightning$ zum kleinen Satz von Fermat
Somit: $s_i \geq s$
$s_i = s$: $\left(\frac{a}{p_i}\right) \equiv a^{\frac{p_i-1}{2}} \equiv (a^{\frac{p_i-1}{2}})^d \equiv (a^{2^{s-1}d_i})^d \equiv (-1)^{d_i} \equiv -1 \pmod{p_i}$
$s_i > s$: $\left(\frac{a}{p_i}\right)^d \equiv (a^{\frac{p_i-1}{2}})^d \equiv ((a^{2^{s-1}d_i})^d)^{2^{s_i - s}} \equiv (-1)^{2^{s_i - s}} \equiv 1 \pmod{p_i}$ $\square$

Also gilt mit $k := |\{p_i : s_i = s\}|$
$\left(\frac{a}{n}\right) = \prod_{i=1}^{l} \left(\frac{a}{p_i}\right) = (-1)^k$
Wenn wir jetzt zeigen können, dass k ungerade ist, sind wir fertig.
$p_i - 1 = 2^{s_i} d_i \Rightarrow p_i \mod 2^{s+1} = \begin{cases} 1 & \text{wenn } s_i > s \\ 1 + 2^s & \text{wenn } s_i = s \end{cases}$
$n = 1 + 2^s d \equiv 1 + 2^s \pmod{2^{s+1}}$
$\Rightarrow 1 + 2^s \equiv n = \prod_{i=1}^{l} p_i \equiv (1 + 2^s)^k \equiv 1 + k2^s \pmod{2^{s+1}}$
$\Rightarrow k$ ungerade
$\Rightarrow a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$
3. Fall: $a^{2^r d} \equiv -1 \pmod{n}$ $(0 \leq r \leq s-2)$
$a^{\frac{n-1}{2}} = (a^{2^r d})^{2^{s-1-r}} \equiv 1 \pmod{n}$, da $s - 1 - r \geq 1$
Wir können mit p_i, s_i, d_i und k wie im 2. Fall zeigen:

Behauptung. $s_i \geq r + 1$ *und* $\left(\frac{a}{p_i}\right) = \begin{cases} -1 & \text{wenn } r + 1 = s_i \\ 1 & \text{wenn } r + 1 < s_i \end{cases}$ *für alle* $1 \leq i \leq l$

und $\left(\frac{a}{n}\right) = (-1)^k$.
$p_i - 1 = 2^{s_i} d_i \Rightarrow p_i \mod 2^{r+2} = \begin{cases} 1 & \text{wenn } s_i > r + 1 \\ 1 + 2^{r+1} & \text{wenn } s_i = r + 1 \end{cases}$
Mit $n = 1 + 2^s d \equiv 1 \pmod{2^{r+2}}$ (da $s \geq r + 2$)
gilt $1 \equiv n = \prod_{i=1}^{l} p_i \equiv (1 + 2^{r+1})^k \equiv 1 + k2^{r+1} \pmod{2^{r+2}}$.
Daher ist k gerade und $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$ □

Abschließend noch zwei Abschätzungen zur Verteilung der Pseudoprimzahlen:

1. Wenn $C(x)$ die Anzahl der Carmichael-Zahlen $\leq x$ angibt, so gilt für genügend großes x:
$$x^{2/7} < C(x) < xL(x)^{-a}$$
wobei $L(x) = \log\log\log x / \log\log x$ und $a \in \mathbb{R}$ mit $a < 1$

2. Es lässt sich zeigen, dass eine Konstante $c(a)$ existiert, sodass
$$\exp((\log x)^{15/38}) < |psp(a) \cap [1, x]| < xL(x)^{-1/2}$$
für alle $x > c(a)$