III Anwendungen

7 Der Primzahltest von M. O. Rabin

(7.1) In Abschnitt (2.4) wurde der Primzahltest behandelt, der wohl jedem aus der Schule bekannt ist; es wurde dort auch bemerkt, daß dieser Test nur für kleine Zahlen brauchbar ist. In diesem Paragraphen wird ein wirklich brauchbarer Primzahltest vorgestellt, nämlich der Primzahltest von M. O. Rabin. In den beiden ersten Abschnitten dieses Paragraphen wird die Behandlung dieses Tests vorbereitet: In (7.2) wird eine Eigenschaft aller ungeraden Primzahlen bewiesen, und in (7.3) wird gezeigt, daß diese Eigenschaft umgekehrt die Primzahlen unter allen ungeraden natürlichen Zahlen > 1 charakterisiert. In Wirklichkeit wird in (7.3) wesentlich mehr bewiesen; dieses schärfere Ergebnis wird nachher bei der Diskussion des Rabinschen Tests benötigt. Die dabei benötigten Resultate über Potenzreste wurden in § 6 hergeleitet. Von Zufallszahlen, wie sie der Test von Rabin benötigt, ist im nächsten Paragraphen die Rede.

(7.2) Satz: *Es sei p eine ungerade Primzahl, es seien $\alpha := v_2(p-1)$ und $q := (p-1)/2^\alpha$. Für jedes $a \in \mathbb{Z} \setminus p\mathbb{Z}$ gilt: Es ist entweder $a^q \equiv 1 \pmod p$, oder es gibt ein $\beta \in \{0, 1, \ldots, \alpha-1\}$ mit $a^{2^\beta q} \equiv -1 \pmod p$.*

Beweis: Es sei $a \in \mathbb{Z} \setminus p\mathbb{Z}$. Die Ordnung $d := \operatorname{ord}([a]_p)$ von $[a]_p$ in der Gruppe $\mathbb{F}_p^\times$ ist nach (4.21) ein Teiler von $p-1 = 2^\alpha q$, also gibt es ein $\gamma \in \{0, 1, \ldots, \alpha\}$ und einen Teiler $d' \in \mathbb{N}$ von q mit $d = 2^\gamma d'$.
(a) Ist $\gamma = 0$, so ist $d = d'$ ein Teiler von q, und daher gilt $[a]_p^q = [1]_p$ (vgl. (3.5)(3)), also $a^q \equiv 1 \pmod p$.
(b) Es gelte $\gamma \geq 1$. Es ist $d/2 = 2^{\gamma-1}d' < d = \operatorname{ord}([a]_p)$, und daher gilt $[a]_p^{d/2} \neq [1]_p$. Im Körper $\mathbb{F}_p$ gilt

$$[0]_p \;=\; [a]_p^d - [1]_p \;=\; \left([a]_p^{d/2} - [1]_p\right)\left([a]_p^{d/2} + [1]_p\right),$$

und somit ist $[a]_p^{d/2} = -[1]_p = [-1]_p$. Für $\beta := \gamma - 1 \in \{0, 1, \ldots, \alpha-1\}$ gilt daher

$$a^{2^\beta q} \;=\; a^{2^{\gamma-1}q} \;=\; \left(a^{d/2}\right)^{q/d'} \;\equiv\; (-1)^{q/d'} \;=\; -1 \pmod p,$$

denn q/d' ist ungerade.

(7.3) Satz: *Es sei $m > 1$ eine ungerade natürliche Zahl, die keine Primzahl ist, und es seien $\alpha := v_2(m-1)$ und $q := (m-1)/2^\alpha$; es seien*

$$E(m) := \{a \in \mathbb{Z} \mid 0 \le a \le m-1;\ \mathrm{ggT}(a,m) = 1\}$$

und

$$A(m) := \left\{ a \in E(m) \;\middle|\; \begin{array}{l} \text{Es gilt } a^q \equiv 1 \pmod m, \text{ oder es existiert ein} \\ \beta \in \{0,1,\ldots,\alpha-1\} \text{ mit } a^{2^\beta q} \equiv -1 \pmod m \end{array} \right\}.$$

Es gilt

$$A(m) \subsetneqq E(m),$$

und ist $m \neq 9$, so gilt

$$\#\big(A(m)\big) \le \frac{1}{4}\varphi(m) = \frac{1}{4}\#\big(E(m)\big).$$

Beweis: Es gilt

$$A(9) = \{1,8\} \subsetneqq \{1,2,4,5,7,8\} = E(9).$$

Es sei von jetzt an $m \ge 15$, und es sei $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ die Primzerlegung von m. Für jedes $i \in \{1,2,\ldots,r\}$ ist $p_i = 1 + 2^{\beta_i} q_i$ mit einem $\beta_i \in \mathbb{N}$ und einem ungeraden $q_i \in \mathbb{N}$. Durch eine Umnumerierung von $p_1, p_2, \ldots, p_r$ erreicht man, daß $\beta_1 = \min(\{\beta_1, \beta_2, \ldots, \beta_r\})$ gilt. Für jedes $i \in \{1,2,\ldots,r\}$ sei $q_i' := \mathrm{ggT}(q, q_i)$.
(1) Für die Menge

$$\mathcal{M} := \{a \in E(m) \mid a^q \equiv 1 \pmod m\}$$

gilt nach (6.14)(2) und (6.16)(2): Es ist

$$\begin{aligned} \#(\mathcal{M}) = N_q(1,m) &= \prod_{i=1}^r N_q(1, p_i^{\alpha_i}) = \prod_{i=1}^r \mathrm{ggT}\big(q, \varphi(p_i^{\alpha_i})\big) = \\ &= \prod_{i=1}^r \mathrm{ggT}\big(q, p_i^{\alpha_i - 1}(p_i - 1)\big) = \prod_{i=1}^r \mathrm{ggT}(q, p_i - 1) = \\ &= \prod_{i=1}^r \mathrm{ggT}(q, 2^{\beta_i} q_i) = \prod_{i=1}^r \mathrm{ggT}(q, q_i) = \prod_{i=1}^r q_i'. \end{aligned}$$

(Dabei ist zu beachten: $q = (m-1)/2^\alpha$ ist ungerade und durch keinen der Primteiler $p_1, p_2, \ldots, p_r$ von m teilbar).

Nach (6.17)(2) gilt für $\beta \in \{0, 1, \ldots, \alpha - 1\}$ und für die Menge

$$\mathcal{M}_\beta := \left\{a \in E(m) \mid a^{2^\beta q} \equiv -1 \pmod m\right\} :$$

Ist

$$\begin{aligned}\beta &= v_2(2^\beta q) \geq \min\left(\left\{v_2(p_1 - 1), v_2(p_2 - 1), \ldots, v_2(p_r - 1)\right\}\right) = \\ &= \min\left(\{\beta_1, \beta_2, \ldots, \beta_r\}\right) = \beta_1,\end{aligned}$$

so ist $\mathcal{M}_\beta = \varnothing$, und ist $\beta \leq \beta_1 - 1$, so ist

$$\begin{aligned}\#(\mathcal{M}_\beta) &= N_{2^\beta q}(-1, m) = \prod_{i=1}^{r} \mathrm{ggT}\left(2^\beta q, \varphi(p_i^{\alpha_i})\right) = \\ &= \prod_{i=1}^{r} \mathrm{ggT}\left(2^\beta q, p_i^{\alpha_i - 1}(p_i - 1)\right) = \prod_{i=1}^{r} \mathrm{ggT}(2^\beta q, p_i - 1) = \\ &= \prod_{i=1}^{r} \mathrm{ggT}(2^\beta q, 2^{\beta_i} q_i) = \prod_{i=1}^{r} (2^\beta q_i') = 2^{r\beta} \prod_{i=1}^{r} q_i'.\end{aligned}$$

Es gilt

$$A(m) = \mathcal{M} \cup \bigcup_{\beta=0}^{\alpha-1} \mathcal{M}_\beta = \mathcal{M} \cup \bigcup_{\beta=0}^{\beta_1 - 1} \mathcal{M}_\beta,$$

und die Mengen $\mathcal{M}$, $\mathcal{M}_0$, $\mathcal{M}_1, \ldots, \mathcal{M}_{\beta_1 - 1}$ sind paarweise disjunkt. Also gilt

$$\begin{aligned}\#\left(A(m)\right) &= \#(\mathcal{M}) + \sum_{\beta=0}^{\beta_1 - 1} \#(\mathcal{M}_\beta) = \\ &= \left(1 + \sum_{\beta=0}^{\beta_1 - 1} 2^{r\beta}\right) \cdot \prod_{i=1}^{r} q_i' = \left(1 + \frac{2^{r\beta_1} - 1}{2^r - 1}\right) \cdot \prod_{i=1}^{r} q_i' = \\ &= \frac{\varphi(m)}{p_1^{\alpha_1 - 1}(p_1 - 1) p_2^{\alpha_2 - 1}(p_2 - 1) \cdots p_r^{\alpha_r - 1}(p_r - 1)} \left(1 + \frac{2^{r\beta_1} - 1}{2^r - 1}\right) \cdot \prod_{i=1}^{r} q_i' = \\ &= \frac{\varphi(m)}{2^{\beta_1 + \beta_2 + \cdots + \beta_r} \cdot p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdots p_r^{\alpha_r - 1}} \left(1 + \frac{2^{r\beta_1} - 1}{2^r - 1}\right) \cdot \underbrace{\prod_{i=1}^{r} \frac{q_i'}{q_i}}_{\leq 1}.\end{aligned}$$

(2) Ist $r \geq 3$, so folgt aus (1): Es ist

$$\#\left(A(m)\right) \leq \frac{\varphi(m)}{2^{\beta_1 + \beta_2 + \cdots + \beta_r}} \left(1 + \frac{2^{r\beta_1} - 1}{2^r - 1}\right) \leq \frac{\varphi(m)}{2^{r\beta_1}} \left(1 + \frac{2^{r\beta_1} - 1}{2^r - 1}\right) =$$

$$= \varphi(m)\cdot\left(\frac{1}{2^r-1}+\frac{2^r-2}{2^{r\beta_1}(2^r-1)}\right) \le \varphi(m)\cdot\left(\frac{1}{2^r-1}+\frac{2^r-2}{2^r(2^r-1)}\right) =$$
$$= \varphi(m)\cdot\frac{2\cdot(2^r-1)}{2^r\cdot(2^r-1)} = \frac{\varphi(m)}{2^{r-1}} \le \frac{\varphi(m)}{4}.$$

(3) Gilt $r=2$ und $\alpha_1>1$ oder $\alpha_2>1$, so ist $p_1^{\alpha_1-1}p_2^{\alpha_2-1}\ge 3$, und wegen (1) gilt

$$\begin{aligned}\#(A(m)) &= \frac{\varphi(m)}{2^{\beta_1+\beta_2}p_1^{\alpha_1-1}p_2^{\alpha_2-2}}\cdot\left(1+\frac{2^{2\beta_1}-1}{2^2-1}\right)\cdot\frac{q_1'q_2'}{q_1q_2} \le\\ &\le \frac{\varphi(m)}{2^{2\beta_1}\cdot 3}\cdot\frac{2^{2\beta_1}+2}{3} = \frac{\varphi(m)}{9}\cdot\left(1+\frac{1}{2^{2\beta_1-1}}\right) \le\\ &\le \frac{\varphi(m)}{9}\cdot\frac{3}{2} = \frac{\varphi(m)}{6} < \frac{\varphi(m)}{4}.\end{aligned}$$

(4) Gilt $r=2$, $\alpha_1=1$, $\alpha_2=1$ und $\beta_1<\beta_2$, so ergibt sich aus (1): Es gilt

$$\begin{aligned}\#(A(m)) &\le \frac{\varphi(m)}{2^{\beta_1+\beta_2}}\cdot\left(1+\frac{2^{2\beta_1}-1}{2^2-1}\right) \le \frac{\varphi(m)}{2^{2\beta_1+1}}\cdot\frac{2^{2\beta_1}+2}{3} \le\\ &\le \frac{\varphi(m)}{6}\cdot\left(1+\frac{1}{2^{2\beta_1-1}}\right) \le \frac{\varphi(m)}{6}\cdot\frac{3}{2} = \frac{\varphi(m)}{4}.\end{aligned}$$

(5) Es gelte $r=2$, $\alpha_1=1$, $\alpha_2=1$ und $\beta_1=\beta_2$. Für $q_1'=\mathrm{ggT}(q,q_1)$ und $q_2'=\mathrm{ggT}(q,q_2)$ gilt $q_1'<q_1$ oder $q_2'<q_2$. (Angenommen, es ist $q_1'=q_1$ und $q_2'=q_2$. Dann gilt $q_1\mid q$ und $q_2\mid q$, wegen $p_1\equiv 1 \pmod{q_1}$ gilt

$$0 \equiv 2^\alpha q = m-1 = p_1p_2-1 \equiv p_2-1 = 2^{\beta_2}q_2 \pmod{q_1},$$

und daraus folgt $q_1\mid q_2$. Ebenso folgt $q_2\mid q_1$. Also gilt $q_1=q_2$ und daher $p_1=1+2^{\beta_1}q_1=1+2^{\beta_2}q_2=p_2$, aber das ist falsch). Wegen $q_1'\mid q_1$ und $q_2'\mid q_2$ und weil q_1 und q_2 ungerade sind, folgt $q_1'\le q_1/3$ oder $q_2'\le q_2/3$, also in jedem Fall $q_1'q_2'\le q_1q_2/3$. Hieraus und aus (1) folgt

$$\begin{aligned}\#(A(m)) &\le \frac{\varphi(m)}{2^{2\beta_1}}\cdot\left(1+\frac{2^{2\beta_1}-1}{2^2-1}\right)\cdot\frac{q_1'q_2'}{q_1q_2} \le \varphi(m)\cdot\frac{2^{2\beta_1}+2}{3\cdot 2^{2\beta_1}}\cdot\frac{1}{3} =\\ &= \frac{\varphi(m)}{9}\cdot\left(1+\frac{1}{2^{2\beta_1-1}}\right) \le \frac{\varphi(m)}{9}\cdot\frac{3}{2} = \frac{\varphi(m)}{6} < \frac{\varphi(m)}{4}.\end{aligned}$$

(6) Es gelte $r=1$. Nach (1) gilt

$$\#(A(m)) = \frac{\varphi(m)}{2^{\beta_1}p_1^{\alpha_1-1}}\cdot\left(1+\frac{2^{\beta_1}-1}{2-1}\right)\cdot\frac{q_1'}{q_1} = \frac{\varphi(m)}{p_1^{\alpha_1-1}}\cdot\frac{q_1'}{q_1} \le \frac{\varphi(m)}{p_1^{\alpha_1-1}}.$$

Da m keine Primzahl ist, ist $\alpha_1 \geq 2$. Ist $p_1 \geq 5$, so gilt somit

$$\#\big(A(m)\big) \leq \frac{\varphi(m)}{5} < \frac{\varphi(m)}{4}.$$

Ist $p_1 = 3$, so ist $\alpha_1 \geq 3$, denn es ist $m = p_1^{\alpha_1} \geq 15$, und es gilt

$$\#\big(A(m)\big) \leq \frac{\varphi(m)}{9} < \frac{\varphi(m)}{4}.$$

Damit ist der Satz bewiesen.

(7.4) Bemerkung: (1) Es sei $m > 1$ eine ungerade natürliche Zahl, und es seien $\alpha := v_2(m-1)$ und $q := (m-1)/2^\alpha$. Wenn m eine Primzahl ist, so gilt nach (7.2) für jedes $a \in E(m) = \{a \in \mathbb{Z} \mid 0 \leq a \leq m-1;\ \mathrm{ggT}(a,m) = 1\}$:

$$(*) \qquad \begin{cases} \text{Entweder ist } a^q \equiv 1 \pmod m, \\ \text{oder es gibt ein } \beta \in \{0,1,\ldots,\alpha-1\} \text{ mit } a^{2^\beta q} \equiv -1 \pmod m. \end{cases}$$

Ist m keine Primzahl und ist $m \neq 9$, so gilt $(*)$ nach (7.3) nur für höchstens ein Viertel aller $a \in E(m)$. Für $m = 9$ gilt $(*)$ für genau ein Drittel aller $a \in E(m) = \{1,2,4,5,7,8\}$.
(2) Die Abschätzung in (7.3) läßt sich nicht verbessern: Ist $m = 91 = 7 \cdot 13$, so gilt $(*)$ für genau $18 = \varphi(m)/4$ aller Elemente von $E(m)$.

(7.5) Der Primzahltest von M. O. Rabin (1976/1980): (1) Es sei m eine ganze Zahl , und es sei $k_{\max}$ eine natürliche Zahl (etwa $k_{\max} = 20$).
(RABIN 1) Ist $m < 2$, so gibt man FALSE aus und bricht ab.
(RABIN 2) Ist m eine der 25 Primzahlen < 100, so gibt man TRUE aus und bricht ab.
(RABIN 3) Ist m durch eine der 25 Primzahlen < 100 teilbar, so gibt man FALSE aus und bricht ab.
(RABIN 4) Ist $m < 10201 = 101^2$, so gibt man TRUE aus und bricht ab. (In diesem Fall ist m nach (2.3) eine Primzahl).
(RABIN 5) Man setzt

$$\alpha := v_2(m-1), \quad q := \frac{m-1}{2^\alpha} \quad \text{und} \quad k := 1.$$

(RABIN 6) Man wählt eine Zufallszahl $a \in \{1,2,\ldots,m-1\}$. Wenn $d := \mathrm{ggT}(a,m) > 1$ ist, so gibt man FALSE aus und bricht ab. (Ist $d > 1$, so ist d ein nichttrivialer Teiler von m).
(RABIN 7) Gilt sowohl $a^q \not\equiv 1 \pmod m$ als auch $a^{2^\beta q} \not\equiv -1 \pmod m$ für jedes $\beta \in \{0,1,\ldots,\alpha-1\}$, so gibt man FALSE aus und bricht ab. (In diesem Fall weiß man nach (7.2), daß m keine Primzahl ist, kennt aber keinen nichttrivialen Teiler von m).

(RABIN 8) Ist $k < k_{\max}$, so setzt man $k := k + 1$ und geht zu (RABIN 6). Ist $k = k_{\max}$, so gibt man TRUE aus und bricht ab.

(2) Es sei m eine ganze Zahl. Liefert der Algorithmus RABIN für m die Ausgabe FALSE, so ist m keine Primzahl. Liefert er dagegen die Ausgabe TRUE, so ist entweder m eine Primzahl, oder m ist keine Primzahl, und während des Algorithmus wurde $k_{\max}$-mal eine Zufallszahl gewählt, die in der in (7.3) erklärten Teilmenge $A(m)$ von

$$E(m) := \{b \mid 1 \leq b \leq m-1;\ \mathrm{ggT}(b,m) = 1\}$$

liegt. Ist m keine Primzahl und ist $m > 9$, so ist $\#(A(m))/\#(E(m)) \leq 1/4$, und daher ist die Wahrscheinlichkeit dafür, daß RABIN bei Anwendung auf m das falsche Ergebnis TRUE liefert, höchstens gleich $1/4^{k_{\max}}$. (Dabei ist vorausgesetzt, daß der Zufallszahlengenerator, der im Schritt (RABIN 6) jeweils eine Zufallszahl liefert, hinreichend gut ist, also die von ihm gelieferten Zufallszahlen unabhängig voneinander sind). Der Algorithmus RABIN ist ein stochastischer Test: Zum einen verwendet er zufällig gewählte Zahlen, und zum anderen liefert er mit einer gewissen kleinen Wahrscheinlichkeit bisweilen ein inkorrektes Ergebnis, doch läßt sich diese Wahrscheinlichkeit durch Vergrößerung von $k_{\max}$ beliebig klein machen.

(3) Es sei $m > 1$ eine ungerade natürliche Zahl, die keine Primzahl ist, und es sei a eine natürliche Zahl. Man nennt m eine starke Pseudoprimzahl zur Basis a, wenn $a \bmod m$ in der in (7.3) erklärten Ausnahmemenge $A(m)$ liegt, also wenn a und m teilerfremd sind und mit $\alpha := v_2(m-1)$ und $q := (m-1)/2^\alpha$ gilt: Entweder ist $a^q \equiv 1 \pmod m$, oder es gibt ein $\beta \in \{0, 1, \ldots, \alpha - 1\}$ mit $a^{2^\beta q} \equiv -1 \pmod m$.

(4) Mit der in (3) eingeführten Sprechweise gilt: Liefert der Algorithmus RABIN für eine ungerade natürliche Zahl m die Ausgabe TRUE, so ist m entweder eine Primzahl oder für $k_{\max}$ Zahlen a aus der Menge

$$\{b \mid 1 \leq b \leq m-1;\ \mathrm{ggT}(b,m) = 1\}$$

eine starke Pseudoprimzahl zur Basis a.

(5) Der Primzahltest `isprime` aus dem MuPAD-Kern ist im wesentlichen der Primzahltest RABIN (mit $k_{\max} = 10$).

(7.6) Der in (7.5)(1) beschriebene stochastische Primzahltest wurde von M. O. Rabin 1976 in [86] angegeben. Eine deterministische Variante des Rabinschen Tests hat G. L. Miller 1975 in [70] publiziert. Er zeigte: Unter der Voraussetzung der Richtigkeit der verallgemeinerten Riemannschen Vermutung, von der bereits in (5.5)(2) die Rede war, gibt es zu jeder ungeraden

Nichtprimzahl $m > 1$ eine natürliche Zahl a mit $1 < a < 2 \cdot \log(m)^2$, für die m nicht starke Pseudoprimzahl zur Basis a ist. Wüßte man also, daß die verallgemeinerte Riemannsche Vermutung richtig ist, so könnte man für jede natürliche Zahl $m > 1$ in höchstens $\lfloor 2 \cdot \log(m)^2 \rfloor$ Schritten vom Typ (RABIN 7) entscheiden, ob sie eine Primzahl ist oder nicht.

(7.7) Man könnte eine deterministische Variante von RABIN folgendermaßen implementieren: Man führt den Schritt (RABIN 7) jeweils mit einer Zahl a aus einer von Anfang an festgewählten endlichen Menge $\mathcal{M}$ durch und nicht mit einer zufällig gewählten Zahl a. Solche Primzahltests waren in älteren Versionen mancher Computeralgebra-Systemen enthalten, wobei $\mathcal{M}$ die Menge der ersten 5 oder der ersten $k_{\max}$ Primzahlen war. Ein solcher Test wird immer gewisse Nichtprimzahlen als Primzahlen deklarieren. Es gilt nämlich (vergleiche dazu Granville [45]): Zu jeder endlichen Menge $\mathcal{M}$ gibt es unendliche viele ganze Zahlen, die für jedes $a \in \mathcal{M}$ starke Pseudoprimzahlen zur Basis a sind. In [5] gibt F. Arnault die Zahlen

$$n := 1\,19506\,87687\,95265\,79251\,83613\,15725\,11635\,18982\,45581$$

und

$$\begin{aligned} N := \quad & 80\,38374\,57453\,63949\,12570\,79614\,34194\,21081\,38837\,68828 \\ & 75581\,45837\,48891\,75222\,97427\,37653\,33652\,18650\,23361\,63960 \\ & 04545\,79150\,42023\,60320\,87665\,69966\,76098\,72840\,43965\,40823 \\ & 29287\,38791\,85086\,91668\,57328\,26776\,17710\,29389\,69773\,94701 \\ & 67082\,30428\,68710\,99974\,39976\,54414\,48453\,41155\,87245\,06334 \\ & 09279\,02227\,52962\,29414\,98423\,06881\,68540\,43264\,57534\,01832 \\ & 97861\,11298\,96064\,48452\,16191\,65287\,25975\,34901 \end{aligned}$$

an, für die gilt: n ist für jede Primzahl $p \leq 31$ eine starke Pseudoprimzahl zur Basis p, und N ist für jede Primzahl $p \leq 200$ eine starke Pseudoprimzahl zur Basis p. In [6] konstruiert Arnault große Carmichael-Zahlen, die starke Pseudoprimzahlen zu vielen Basen sind.

Die folgende Liste (vgl. dazu die Arbeit [50] von G. Jaeschke) enthält zu jedem $k \in \{1, 2, \ldots, 8\}$ in der ersten Spalte die kleinste natürliche Zahl m_k, die eine starke Pseudoprimzahl zu den Basen p_1, $p_2, \ldots, p_k$ ist, wobei p_1, $p_2, \ldots, p_k$ die ersten k Primzahlen sind. In der zweiten Spalte steht für jedes k die Primzerlegung von m_k und in der dritten der Quotient $\#(A(m_k))/\varphi(m_k)$, wobei wie bisher $A(m_k)$ die Menge der zu m_k teilerfremden natürlichen Zahlen $a < m_k$ ist, für die m_k eine starke Pseudoprimzahl zur Basis a ist.

k	m_k	Primzerlegung	$\#(A(m_k))/\varphi(m_k)$
1	2047	$23 \cdot 89$	1/8
2	13 73653	$829 \cdot 1657$	3/16
3	253 26001	$2251 \cdot 11251$	1/10
4	32150 31751	$151 \cdot 751 \cdot 28351$	1/4
5	215 23028 98747	$6763 \cdot 10627 \cdot 29947$	1/4
6	347 47496 60383	$1303 \cdot 16927 \cdot 157543$	1/4
7	34155 00717 28321	$10670053 \cdot 32010157$	1/8
8	34155 00717 28321	$10670053 \cdot 32010157$	1/8

(7.8) Bemerkung: Es gibt eine Reihe von deterministischen Primzahltests, also von Primzahltests, die mit Sicherheit ein korrektes Ergebnis liefern. Darauf kann hier nicht eingegangen werden. Ein solcher Test ist in der MuPAD-Funktion `numlib::proveprime` enthalten, ein anderer, der Hilfsmittel aus der Algebraischen Zahlentheorie verwendet, wird in Abschnitt 9.6 des Buchs [10] von E. Bach und J. Shallit beschrieben.

(7.9) Aufgaben:

Aufgabe 1: Man schreibe eine MuPAD-Funktion, die für natürliche Zahlen m und a entscheidet, ob m eine starke Pseudoprimzahl zur Basis a ist. Man bestätige mit ihrer Hilfe, was in (7.7) über die beiden von F. Arnault angegebenen Zahlen n und N und über die Zahlen $m_1, m_2, \ldots, m_8$ ausgesagt ist. (Man vgl. auch Aufgabe 7).

Aufgabe 2: Es sei $m > 1$ eine ungerade natürliche Zahl, und es seien $\alpha := v_2(m-1)$ und $q := (m-1)/2^\alpha$; es sei $A(m)$ die Menge der $a \in \{0, 1, 2, \ldots, m-1\}$ mit $\mathrm{ggT}(a, m) = 1$, für die gilt: Es ist $a^q \equiv 1 \pmod{m}$, oder es gibt ein $\beta \in \{0, 1, \ldots, \alpha - 1\}$ mit $a^{2^\beta q} \equiv -1 \pmod{m}$.

(a) Man schreibe eine MuPAD-Funktion, die die Menge $A(m)$ berechnet.

(b) Im Beweis von (7.3) wurde die Anzahl der Elemente der Menge $A(m)$ berechnet. Man schreibe eine MuPAD-Funktion, die $\#(A(m))/\varphi(m)$ (oder $\#(A(m))$ selbst) berechnet. Man schreibe diese Funktion so, daß man ihr statt m auch eine Liste $[p_1, p_2, \ldots, p_r]$ paarweise verschiedener ungerader Primzahlen und eine Liste $[\alpha_1, \alpha_2, \ldots, \alpha_r]$ natürlicher Zahlen übergeben kann, zu denen sie dann $\#(A(m))/\varphi(m)$ [oder $\#(A(m))$] für $m := p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ berechnet. Auf diese Weise kann man $\#(A(m))/\varphi(m)$ auch für solche m ausrechnen, die `ifactor` nicht mehr faktorisieren will (vgl. Aufgabe 3).

Aufgabe 3: Die Zahlen n und N aus (7.7) sind keine Primzahlen, und man kann ihre Primzerlegungen mit Hilfe der in (4.29) beschriebenen Methode berechnen (vgl. (4.30), Aufgabe 9). Man ermittle die Anzahl der Elemente der Mengen $A(n)$ und $A(N)$. (Dazu lese man den Beweis in (7.3) oder bearbeite zuerst Aufgabe 2(b)).

Aufgabe 4: Es seien p_1, p_2, p_3 paarweise verschiedene ungerade Primzahlen, es sei $m := p_1p_2p_3$, und es gelte für jedes $i \in \{1,2,3\}$

$$p_i \equiv 3 \pmod 4 \quad \text{und} \quad p_i - 1 \,|\, m - 1.$$

Man zeige: Für die in (7.3) definierte Menge $A(m)$ gilt

$$\#(A(m)) = \frac{\varphi(m)}{4}.$$

(Nach dem Kriterium von Korselt ist m eine Carmichael-Zahl, vgl. dazu Aufgabe 7 in (5.26)).

Aufgabe 5: (1) Man zeige, daß die Zahl

$$m := 1253\,07596\,07784\,49601\,05845\,73923$$

eine Carmichael-Zahl ist und daß sie für genau ein Viertel aller zu m teilerfremden natürlichen Zahlen $b < m$ eine starke Pseudoprimzahl zur Basis b ist. (m ist eine der von F. Arnault in [6] angegebenen großen Carmichael-Zahlen, die zu vielen Basen starke Pseudo-Primzahlen sind).

(2) Man zeige, daß `isprime` bei Anwendung auf m bisweilen die falsche Ausgabe `TRUE` liefert.

Aufgabe 6: Man schreibe zu dem Algorithmus RABIN aus (7.5) eine MuPAD-Funktion `rabin`. Dabei sollte die Zahl $k_{\max}$ vom Benutzer frei gewählt werden können. Man überlege sich auch noch, ob man den Schritt (RABIN 3) folgendermaßen implementieren sollte: Man prüft nach, ob das Produkt der 25 Primzahlen < 100 und die Zahl m, von der festzustellen ist, ob sie eine Primzahl ist oder nicht, teilerfremd sind. Ist es sinnvoll, nach (RABIN 4) noch einen weiteren ähnlichen Test durchzuführen, etwa festzustellen, ob m und das Produkt der Primzahlen zwischen 100 und 1000 teilerfremd sind?

Aufgabe 7: Man ändere den Algorithmus RABIN folgendermaßen ab: Man führt den Schritt (RABIN 7) nicht mit einer zufällig aus der Menge $E(m) = \{b \mid 1 \le b \le m-1;\ \mathrm{ggT}(b,m) = 1\}$ ausgewählten Zahl a durch, sondern wählt darin als a der Reihe nach $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$ und so fort. Man schreibe dazu eine MuPAD-Funktion. Diese Funktion wird eine natürliche Zahl m, die keine Primzahl ist, als Primzahl deklarieren, wenn m eine starke Pseudoprimzahl zu jeder der Basen $p_1, p_2, \ldots, p_{k_{\max}}$ ist.