KAPITEL 4

Primzahltests

Wir erwähnen zwei Grundprobleme:

- Überprüfe, ob eine vorgegebene (große) natürliche Zahl n eine Primzahl ist.
- Konstruiere eine Primzahl einer bestimmten Größenordnung evtl. mit bestimmten Eigenschaften. (Dies ist besonders für die Anwendung wichtig.)

Um eine konkrete Vorstellung zu haben, wollen wir versuchen, eine Primzahl der Gestalt $10^{1000} + r$ mit $r \geq 0$ zu konstruieren.

1. Kleine Teiler

Die Tatsache, dass die Hälfte aller natürlichen Zahlen gerade sind, also 2 als Primteiler haben, wird in folgendem Satz verallgemeinert:

SATZ. *Seien $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $\ldots$, p_r die ersten r Primzahlen und $P = p_1 p_2 \ldots p_r$. Dann gilt:*

(1) *Ist N eine natürliche Zahl, dann haben unter den P Zahlen $N+1$, $N+2$, $N+3$, $\ldots$, $N+P$ genau $P - \varphi(P)$ Zahlen einen Primteiler $\leq p_r$:*

$$\#\{n \in \{N+1, N+2, \ldots, N+P\} : n \text{ hat einen Primteiler } \leq p_r\} = P - \varphi(P).$$

(2) *Für $N \in \mathbb{N}$ gilt*

$$\frac{\#\{n \in \{N+1, \ldots, N+P\} : n \text{ hat einen Primteiler } \leq p_r\}}{P} = 1 - \prod_{i=1}^{r}(1 - \frac{1}{p_i}).$$

In diesem Sinne kann man sagen: Der Anteil der natürlichen Zahlen, die durch einen Primteiler $\leq p_r$ haben, beträgt

$$1 - (1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_r}).$$

Beweis: Sei $M = \{N+1, N+2, N+3, \ldots, N+P\}$. Die folgenden Aussagen ergeben sich direkt auseinander und aus $\varphi(P) = \#(\mathbb{Z}/P\mathbb{Z})^*$:

- Die Zahlen aus M repräsentieren $\mathbb{Z}/P\mathbb{Z}$.
- $\varphi(P)$ der Zahlen aus M repräsentieren $(\mathbb{Z}/P\mathbb{Z})^*$, sind also teilerfremd zu P.
- $P - \varphi(P)$ der Zahlen aus M sind nicht teilerfremd zu P, haben also einen Primteiler p_1 oder p_2 oder $\ldots$ oder p_r.
- $P - \varphi(P)$ der Zahlen aus M haben einen Primteiler $\leq p_r$.

Die letzte Aussage war zu zeigen. Der zweite Teil ergibt sich aus dem ersten Teil durch Division durch P und

$$\frac{P - \varphi(P)}{P} = 1 - \frac{\varphi(P)}{P} = 1 - \prod_{p|P}(1 - \frac{1}{p}) = 1 - \prod_{i=1}^{r}(1 - \frac{1}{p_i}). \blacksquare$$

Beispiel: Bis 10 gibt es die Primzahlen $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$. Sei $P = p_1 p_2 p_3 p_4 = 210$. Dann ist $\varphi(P) = 48$ und $P - \varphi(P) = 162$. Der Satz sagt dann, dass unter 210 aufeinanderfolgenden natürlichen Zahlen $(N+1, N+2, \ldots, N+210)$ 162 Stück einen Primteiler ≤ 10 haben. Dies sind $\frac{162}{210} \approx 77\%$ der Zahlen.

Datei: ki_pzt.tex. Version vom 4.1.2021

Das letzte Beispiel lässt sich sofort verallgemeinern. Sei $K \in \mathbb{N}_{\geq 2}$. Wir wollen den Anteil der natürlichen Zahlen bestimmen, die einen Primteiler $\leq K$ haben. Seien $p_1 < p_2 < p_3 < \cdots < p_r \leq K$ alle Primzahlen $\leq K$. Mit $P = \prod_{i=1}^{r} p_i$ gilt dann

$$\frac{\#\{n \in \{N+1, \ldots, N+P\} : n \text{ hat einen Primteiler } \leq K\}}{P} = 1 - \prod_{i=1}^{r}(1 - \frac{1}{p_i}).$$

Diese Zahl interpretieren wir als den Anteil der natürlichen Zahlen mit einem Primteiler $\leq K$. Für $K \in \{10, 100, 1000, 10000, 100000\}$ haben wir alle Primzahlen $p_1, p_2, \ldots, p_r \leq K$ bestimmt, dann den Anteil $1 - \prod_{i=1}^{r}(1 - \frac{1}{p_i})$ berechnet mit folgendem Ergebnis:

K	10	100	1000	10000	100000
Anteil der Zahlen mit einem Primteiler $\leq K$	77.14%	87.97%	91.90%	93.91%	95.12%

(Die jeweils größten Primzahlen $\leq K$ sind hier $p_4 = 7$, $p_{25} = 97$, $p_{168} = 997$, $p_{1229} = 9973$, $p_{9592} = 99991$.)

Bemerkungen:

(1) Die letzte Tabelle kann man so interpretieren: Die Wahrscheinlichkeit, dass eine zufällig gewählte Zahl einen kleinen Teiler hat, ist recht groß.
(2) Will man testen, ob eine Zahl n prim ist, so sollte man zunächst untersuchen, ob sie kleine Teiler hat.
(3) Will man die Primfaktorzerlegung einer natürlichen Zahl n bestimmen, so sollte man zunächst die kleinen Teiler herausteilen, bevor man aufwändigere Verfahren zu Hilfe zieht.
(4) In der Analytischen Zahlentheorie wird folgende Formel von **Mertens** bewiesen:

$$\prod_{p \leq x}(1 - \frac{1}{p}) \sim \frac{e^{-\gamma}}{\log x}, \quad \text{d.h.} \quad \lim_{x \to \infty} \log x \cdot \prod_{p \leq x}(1 - \frac{1}{p}) = e^{-\gamma},$$

wobei $\gamma = 0.577215664901533$ die Eulersche Konstante bezeichnet.

Beispiel: Wir betrachten $p_1 = 2$, $p_2 = 3$, $p_3 = 5$. Von den Zahlen zwischen 101 und 130 sind genau $8 = \varphi(30)$ Stück weder durch 2 noch durch 3 noch durch 5 teilbar, nämlich

$$101, \quad 103, \quad 107, \quad 109, \quad 113, \quad 119, \quad 121, \quad 127.$$

(Die Zahlen 101, 103, 107, 109, 113, 127 sind sogar prim.)

Beispiel: Wir haben die Zahlen r mit $1 \leq r \leq 1000$ bestimmt, sodass $n = 10^{1000} + r$ keinen Teiler $\leq T$ hat für $T = 10^4, 10^5, 10^6, 10^7, 10^8$

T	r mit $1 \leq r \leq 1000$, sodass $10^{1000} + r$ keinen Teiler $\leq T$ hat
10^4	9, 19, 39, 61, 63, 79, 93, 97, 117, 121, 133, 141, 147, 169, 183, 189, 193, 207, 223, 247, 253, 259, 261, 277, 279, 313, 357, 411, 427, 453, 459, 469, 481, 489, 499, 519, 529, 531, 537, 589, 597, 601, 627, 643, 663, 669, 709, 721, 741, 753, 757, 763, 823, 847, 877, 889, 891, 931, 937, 943, 961, 963, 999
10^5	19, 39, 63, 79, 93, 117, 121, 133, 141, 147, 169, 183, 189, 223, 247, 253, 259, 261, 277, 279, 313, 357, 411, 453, 459, 469, 481, 489, 499, 519, 529, 531, 537, 589, 597, 663, 669, 709, 721, 753, 757, 763, 823, 847, 889, 891, 931, 937, 943, 963, 999
10^6	39, 63, 79, 121, 133, 141, 147, 169, 183, 189, 223, 247, 253, 259, 261, 277, 279, 313, 357, 411, 453, 459, 481, 489, 499, 519, 529, 531, 589, 597, 663, 669, 709, 721, 753, 763, 823, 847, 889, 891, 931, 937, 943, 963, 999
10^7	39, 63, 79, 121, 133, 141, 169, 189, 223, 247, 253, 259, 261, 277, 279, 313, 357, 453, 481, 489, 499, 519, 529, 531, 597, 663, 669, 709, 721, 753, 823, 847, 889, 891, 931, 937, 943, 963
10^8	39, 63, 79, 121, 133, 141, 189, 223, 247, 253, 259, 261, 279, 313, 357, 453, 481, 489, 499, 519, 529, 531, 597, 663, 669, 709, 753, 847, 931, 937, 943, 963

Es ist möglich, dass in der für r's aus der untersten Zeile die Zahl $10^{1000} + r$ prim ist. Doch wie kann man dies feststellen? Wir brauchen eine vernünftige Möglichkeit, Primzahlen von zusammengesetzten Zahlen zu unterscheiden.

2. Der kleine Satz von Fermat und der Satz von Euler

LEMMA. *Für eine Primzahl p und ganze Zahlen a, b gilt*

$$(a+b)^p \equiv a^p + b^p \bmod p.$$

Beweis: Für $1 \le i \le p-1$ ist

$$\binom{p}{i} = \frac{p \cdot (p-1) \cdot (p-2) \cdot \cdots \cdot (p-(i-1))}{1 \cdot 2 \cdot 3 \cdot \cdots \cdot (i-1) \cdot i}.$$

Die Primzahl p im Nenner auf der rechten Seite kürzt sich nicht weg, weswegen $p \mid \binom{p}{i}$, also $\binom{p}{i} \equiv 0 \bmod p$ gilt. Mit dem binomischen Lehrsatz folgt

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i + b^p \equiv a^p + b^p \bmod p,$$

wie behauptet. ■

SATZ (Kleiner Satz von Fermat). *Für eine Primzahl p und eine ganze Zahl a gelten die Aussagen*

$$a^p \equiv a \bmod p$$

und

$$\mathrm{ggT}(a,p) = 1 \quad \Longrightarrow \quad a^{p-1} \equiv 1 \bmod p.$$

Beweis:

(1) Das vorangegangene Lemma liefert $(a+1)^p \equiv a^p + 1 \bmod p$. Mit $0^p \equiv 0 \bmod p$ und $1^p \equiv 1 \bmod p$ folgt durch Induktion sofort, dass $a^p \equiv a \bmod p$ für alle $a \in \mathbb{N}_0$ gilt. Da jede ganze Zahl kongruent zu einer Zahl ≥ 0 ist, folgt sofort die Behauptung.

(2) Nach (1) gilt $a^p \equiv a \bmod p$, also $p \mid a^p - a$, was man auch in der Form

$$p \mid a(a^{p-1} - 1)$$

schreiben kann. Ist nun $\mathrm{ggT}(a,p) = 1$, so folgt $p \mid a^{p-1} - 1$ und damit

$$a^{p-1} \equiv 1 \bmod p,$$

wie behauptet. ■

Der kleine Satz von Fermat ist ein Spezialfall des folgenden Satzes von Euler:

SATZ (Euler). *Ist n eine natürliche Zahl und a eine ganze Zahl mit $\mathrm{ggT}(a,n) = 1$, so gilt*

$$a^{\varphi(n)} \equiv 1 \bmod n.$$

1. Beweis (mit elementaren Methoden):

(1) Die Elemente der Menge $M = \{b : 0 \le b \le n-1, \mathrm{ggT}(b,n) = 1\}$ bilden ein Repräsentantensystem von $(\mathbb{Z}/n\mathbb{Z})^*$. Ist $b \in M$, so gilt $\mathrm{ggT}(ab, m) = 1$ und damit auch $\mathrm{ggT}(ab \bmod m, m) = 1$, also $(ab \bmod m) \in M$. Daher erhalten wir eine wohldefinierte Abbildung

$$f : M \to M \text{ mit } f(b) = ab \bmod m.$$

(2) $f : M \to M$ ist injektiv: $f(b_1) = f(b_2)$ liefert $ab_1 \equiv ab_2 \bmod m$, also $m \mid a(b_1 - b_2)$. Wegen $\mathrm{ggT}(a,m) = 1$ folgt $b_1 \equiv b_2 \bmod m$, also $b_1 = b_2$.

(3) Da M eine endliche Menge ist, ist die injektive Abbildung f sogar bijektiv, also eine Permutation der Menge M. Dies liefert $\prod_{b \in M} b = \prod_{b \in M} f(b)$ und damit

$$\prod_{b \in M} b \equiv \prod_{b \in M} f(b) \equiv \prod_{b \in M} (ab) \equiv a^{\varphi(m)} \prod_{b \in M} b \bmod m,$$

also

$$m \mid (a^{\varphi(m)} - 1) \prod_{b \in M} b.$$

Da alle Zahlen aus M teilerfremd zu m sind, folgt $m \mid a^{\varphi(m)} - 1$ und damit

$$a^{\varphi(m)} \equiv 1 \bmod m,$$

wie behauptet. ■

2. Beweis (mit etwas Gruppentheorie):

(1) Ist G eine endliche (multiplikativ geschriebene) Gruppe, so gilt bekanntlich für jedes $g \in G$

$$g^{\#G} = 1,$$

wenn 1 das neutrale Element von G bezeichnet.

(2) Wir wenden die Aussage aus (1) auf $G = (\mathbb{Z}/n\mathbb{Z})^*$ an: Ist $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$, so ist $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$. Es folgt wegen $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$

$$\overline{a}^{\varphi(n)} = \overline{1},$$

was als Kongruenz geschrieben sofort

$$a^{\varphi(n)} \equiv 1 \bmod n$$

liefert. ■

Für eine Primzahl p ist $\varphi(p) = p - 1$, also erhält man aus dem Satz von Euler unmittelbar den kleinen Satz von Fermat.

Beispiele:

(1) Für $n = 10$ ist $\varphi(n) = \varphi(2 \cdot 5) = 4$.

a	0	1	2	3	4	5	6	7	8	9
$a^4 \bmod 10$	0	1	6	1	6	5	6	1	6	1

(2) Für $n = 11$ ist $\varphi(n) = \varphi(11) = 10$.

a	0	1	2	3	4	5	6	7	8	9	10
$a^{10} \bmod 11$	0	1	1	1	1	1	1	1	1	1	1

(3) Für $n = 12$ ist $\varphi(n) = \varphi(2^2 \cdot 3) = 2 \cdot 2 = 4$.

a	0	1	2	3	4	5	6	7	8	9	10	11
$a^4 \bmod 12$	0	1	4	9	4	1	0	1	4	9	4	1

FOLGERUNG. *Ist $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(n, a) = 1$, so gilt für $x, y \in \mathbb{N}_0$ die Implikation*

$$x \equiv y \bmod \varphi(n) \quad \Longrightarrow \quad a^x \equiv a^y \bmod n.$$

Insbesondere gilt also

$$a^x \equiv a^{(x \bmod \varphi(n))} \bmod n.$$

Beweis: O.E. ist $x \geq y$. Wegen $x \equiv y \bmod \varphi(n)$ existiert dann ein $k \in \mathbb{N}_0$ mit $x = y + k\varphi(n)$. Es folgt mit dem Satz von Euler

$$a^x \equiv a^{y+k\varphi(n)} = a^y \cdot (a^{\varphi(n)})^k \equiv a^y \cdot 1^k \equiv a^y \bmod n,$$

was gezeigt werden sollte. ■

Bemerkung: Mit dem kleinen Satz von Fermat kann man schnell folgende Überlegung anstellen. Ist $n \geq 2$ eine natürliche Zahl und a eine ganze Zahl mit $\mathrm{ggT}(a, n) = 1$, so gelten die Implikationen

$$\begin{aligned} n \text{ prim} \quad &\Longrightarrow \quad a^{n-1} \equiv 1 \bmod n, \\ a^{n-1} \not\equiv 1 \bmod n \quad &\Longrightarrow \quad n \text{ zusammengesetzt.} \end{aligned}$$

Findet man also zu n eine Zahl a mit $1 < a < n$ und $a^{n-1} \not\equiv 1 \bmod n$, so ist n sicher keine Primzahl. Um dies zu einem praktischen Test zu machen, muss man $a^{n-1} \bmod n$ einigermaßen schnell berechnen können. Geht das?

3. Schnelles Potenzieren – Die square-and-multiply-Methode

Frage: Wie kann man schnell $a^d \bmod n$ berechnen?

Berechnet man $a^d \bmod n$ als

$$a^d \bmod n = (\dots(((a \cdot a \bmod n) \cdot a \bmod n) \cdot a \bmod n)\dots) \cdot a \bmod n,$$

so hat man $d-1$ Schritte, was für großes d nicht praktikabel ist.

Obwohl das folgende Lemma mathematisch nur auf den Potenzrechenregeln beruht, ist die Auswirkung auf die schnelle Berechnungsmöglichkeit von $a^d \bmod n$ enorm:

LEMMA. *Sei $a \in \mathbb{Z}$, $d \in \mathbb{N}_0$, $n \in \mathbb{N}$. Sei $d = \sum_{i\geq 0} \delta_i \cdot 2^i$ die Binärentwicklung von d (mit $\delta_i \in \{0,1\}$). Dann gilt:*

$$a^d \equiv \prod_{\substack{i\geq 0\\ \delta_i=1}} a^{2^i} \bmod n$$

und

$$a^{2^0} = a \quad \text{und} \quad a^{2^{i+1}} \equiv (a^{2^i})^2 \bmod n.$$

Beweis: Es gilt

$$a^d \equiv a^{\sum_{i\geq 0}\delta_i\cdot 2^i} \equiv \prod_{i\geq 0} a^{\delta_i\cdot 2^i} \equiv \prod_{i\geq 0}(a^{2^i})^{\delta_i} \equiv \prod_{\substack{i\geq 0\\ \delta_i=1}} a^{2^i} \bmod n.$$

Die zweite Aussage ist unmittelbar klar. ■

Bemerkung: Um $a^d \bmod n$ mit Hilfe des Lemmas zu berechnen, berechnet man die Potenzen $a^{2^i} \bmod n$ durch **sukzessives Quadrieren**, anschließend **multipliziert** man die Potenzen $a^{2^i} \bmod n$ **zusammen**, für die $\delta_i = 1$ gilt. Deswegen spricht man auch von der **square-and-multiply-Methode** zum Potenzieren.

Beispiel: Wir wollen $13^{17} \bmod 19$ berechnen. Die Binärentwicklung von 17 ist $17 = 2^0 + 2^4 = 1 + 16$, sodass wir erhalten

$$13^{17} \equiv 13^1 \cdot 13^{16} \bmod 19.$$

Nun ist modulo 19

$$13^2 \equiv 17, \quad 13^4 \equiv (13^2)^2 \equiv 17^2 \equiv 4, \quad 13^8 \equiv (13^4)^2 \equiv 4^2 \equiv 16, \quad 13^{16} \equiv (13^8)^2 \equiv 16^2 \equiv 9,$$

was man auch in Tabellenform schreiben kann:

i	0	1	2	3	4
$13^{2^i} \bmod 19$	13	17	4	16	9

Es folgt

$$13^{17} \equiv 13^1 \cdot 13^{16} \equiv 13 \cdot 9 \equiv 3 \bmod 19.$$

Um einen zugehörigen Algorithmus zu erhalten, formulieren wir das vorangegangene Lemma noch etwas anders:

LEMMA. *Gegeben seien $a \in \mathbb{Z}$, $d \in \mathbb{N}$, $n \in \mathbb{N}$. Sei $d = \sum_{i\geq 0} \delta_i \cdot 2^i$ die Binärentwicklung von d (mit $\delta_i \in \{0,1\}$) und*

$$b_i = \prod_{j\leq i}(a^{2^j})^{\delta_j} \bmod n, \quad c_i = a^{2^i} \bmod n, \quad d_i = \sum_{j\geq i} \delta_j \cdot 2^{j-i}.$$

Dann gilt:

(1) $c_0 = a \bmod n$ *und* $c_{i+1} = c_i^2 \bmod n$ *für alle* $i \geq 0$.
(2) $d_0 = d$ *und* $d_{i+1} = \left\lfloor \frac{d_i}{2} \right\rfloor$ *für alle* $i \geq 0$.
(3) $\delta_i = d_i \bmod 2$ *für alle* $i \geq 0$.
(4) $b_0 = a^{\delta_0} \bmod n$ *und* $b_{i+1} = b_i c_{i+1}^{\delta_{i+1}} \bmod n$.
(5) *Ist* $d_i \leq 1$, *so ist* $b_i = a^d \bmod n$.

Beweis:

(1) $c_0 = a \bmod n$ ist klar. Für $i \geq 0$ gilt

$$c_{i+1} \equiv a^{2^{i+1}} \equiv a^{2^i \cdot 2} \equiv (a^{2^i})^2 \equiv c_i^2 \bmod n.$$

(2) $d_0 = d$ ist klar. Weiter gilt

$$\left\lfloor \frac{d_i}{2} \right\rfloor = \left\lfloor \sum_{j \geq i} \delta_j \cdot 2^{j-i-1} \right\rfloor = \left\lfloor \sum_{j \geq i+1} \delta_j \cdot 2^{j-(i+1)} + \frac{\delta_i}{2} \right\rfloor = \left\lfloor d_{i+1} + \frac{\delta_i}{2} \right\rfloor = d_{i+1}.$$

(3) Es ist

$$d_i = \sum_{j \geq i} \delta_j \cdot 2^{j-i} = \delta_j + \sum_{j \geq i+1} \delta_j \cdot 2^{j-i} = \delta_j + 2 \sum_{j \geq i+1} \delta_j \cdot 2^{j-(i+1)},$$

woraus sofort $d_i \equiv \delta_i \bmod 2$ folgt.

(4) $b_0 = a^{\delta_0} \bmod n$ ist klar. Weiter gilt

$$b_{i+1} \equiv \prod_{j \leq i+1} (a^{2^j})^{\delta_j} \equiv \prod_{j \leq i} (a^{2^j})^{\delta_j} \cdot (a^{2^{i+1}})^{\delta_{i+1}} = b_i \cdot c_{i+1}^{\delta_{i+1}} \bmod n.$$

(5) Ist $d_i \leq 1$, so gilt $d_{i+1} = \left\lfloor \frac{d_i}{2} \right\rfloor = 0$ und damit wegen $d_{i+1} = \delta_{i+1} + \delta_{i+2} \cdot 2 + \delta_{i+3} \cdot 2^2 + \ldots$ natürlich $\delta_{i+1} = \delta_{i+2} = \delta_{i+3} = \cdots = 0$, was sofort

$$a^d \equiv \prod_{j \geq 0} (a^{2^j})^{\delta_j} \equiv \prod_{j \leq i} (a^{2^j})^{\delta_j} \equiv b_i \bmod n,$$

und somit $b_i = a^d \bmod n$ liefert. ■

Beispiele: Wir verwenden die Bezeichnungen des vorangegangenen Lemmas.

(1) Wir wollen $13^{17} \bmod 19$ berechnen.

i	d_i	δ_i	c_i	b_i
0	17	1	13	13
1	8	0	17	13
2	4	0	4	13
3	2	0	16	13
4	1	1	9	3

Daher ist $13^{17} \equiv 3 \bmod 19$.

(2) Wir berechnen $13^{33} \bmod 37$.

i	d_i	δ_i	c_i	b_i
0	33	1	13	13
1	16	0	21	13
2	8	0	34	13
3	4	0	9	13
4	2	0	7	13
5	1	1	12	8

Folglich ist $13^{33} \equiv 8 \bmod 37$.

(3) Wir wollen $2^{123456789} \bmod 987654321$ berechnen.

i	d_i	δ_i	c_i	b_i
0	123456789	1	2	2
1	61728394	0	4	2
2	30864197	1	16	32
3	15432098	0	256	32
4	7716049	1	65536	2097152
5	3858024	0	344350012	2097152
6	1929012	0	392547562	2097152
7	964506	0	282069526	2097152
8	482253	1	706746679	149611286
9	241126	0	123137257	149611286
10	120563	1	851417971	279277817
11	60281	1	345041113	911451224
12	30140	0	769901713	911451224
13	15070	0	759344764	911451224
14	7535	1	483551350	189213602
15	3767	1	923405899	206271470
16	1883	1	964006387	212405648
17	941	1	91103341	969951539
18	470	0	469653595	969951539
19	235	1	528234745	155914325
20	117	1	142714780	566254001
21	58	0	282045658	566254001
22	29	1	109238839	264855578
23	14	0	982955794	264855578
24	7	1	106586737	970718579
25	3	1	652313308	483053927
26	1	1	924386425	804307517

Also ist

$$2^{123456789} \equiv 804307517 \bmod 987654321.$$

Aus der Darstellung des vorangegangenen Lemmas gewinnt man leicht folgenden Algorithmus:

Potenzieren modulo n mit der square-and-multiply-Methode:
Eingabe: $a \in \mathbb{Z}$, $d \in \mathbb{N}_0$, $n \in \mathbb{N}$
Ausgabe: $a^d \bmod n$

if $d \bmod 2 = 0$ **then**
    $b \leftarrow 1$
else
    $b \leftarrow a \bmod n$
end if
$c \leftarrow a \bmod n$
while $d > 1$ **do**
    $c \leftarrow c^2 \bmod n$
    $d \leftarrow \left\lfloor \frac{d}{2} \right\rfloor$
    if $d \bmod 2 = 1$ **then**
        $b \leftarrow bc \bmod n$
    end if
end while
return b

Bemerkungen:

(1) ℓ gebe an, wie oft die while-Schleife im Algorithmus durchlaufen wird. Wir betrachten den Wert von d_i nach Zeile 9. Beim ersten Durchlauf ist der Wert d_1, beim ℓ-ten Durchlauf dann $d_\ell = 1$. Nun sieht man leicht, dass $d_i = \left\lfloor \frac{d}{2^i} \right\rfloor$ gilt. Aus $d_\ell = 1$ folgt dann $1 \leq \frac{d}{2^\ell} < 2$, also $2^\ell \leq d < 2^{\ell+1}$ und damit $\ell \leq \log_2 d < \ell + 1$, also

$$\ell = \lfloor \log_2 d \rfloor .$$

Daher brauchen wir ℓ Quadratbildungen und höchstens ℓ Multiplikationen. Zusammengefasst: Zur Berechnung von $a^d \bmod n$ hat man mit dem obigen square-and-multiply-Verfahren also

$$\lfloor \log_2 d \rfloor \leq \log_2 d < 3.33 \log_{10} d$$

Quadratbildungen und höchstens soviele Multiplikationen. Dies ist sehr schnell. Für $d \approx 10^{1000}$ sind dies in etwa 3322 Schritte. Die Laufzeit zur Berechnung von $a^d \bmod n$ mit $1 \leq a, d \leq n$ lässt sich dann durch $O((\log n)^3)$ abschätzen.

(2) In Programmpaketen mit Langzahlarithmetik ist das/ein square-and-multiply-Verfahren zur Berechnung von $a^d \bmod n$ normalerweise implementiert. Hier sind ein paar Befehle dafür:
- Python3: `pow(a,d,n)`
- Sage: `pow(a,d,n)` oder `power_mod(a,d,n)`
- Maple: `Power(a,d) mod n`
- Maxima: `power_mod(a,d,n)`

(3) Ist G eine Gruppe, $g \in G$ ein Element und $d \in \mathbb{N}$ groß, so sollte man g^d (bei multiplikativer Schreibweise) bzw. $d \cdot g$ (bei additiver Schreibweise) genauso mit der square-and-multiply-Methode berechnen.

4. Schnelles Potenzieren II — Eine weitere Variante

Wir wollen nochmals $a^d \bmod n$ auf einem anderen Weg berechnen. Die Idee ist, den Exponenten d schrittweise kleiner zu machen. Wir zeigen dies an Hand eines Terms $b \cdot c^d$:

- Ist $d \equiv 0 \bmod 2$, so gilt
$$b \cdot c^d \equiv b \cdot (c^2 \bmod n)^{\frac{d}{2}} \bmod n.$$
- Ist $d \equiv 1 \bmod 2$, so gilt
$$b \cdot c^d \equiv (bc \bmod n) \cdot c^{d-1} \bmod n.$$

Wir beginnen mit kleinen Beispielen:

Beispiel: Wir berechnen $13^{17} \bmod 19$:

$$\begin{aligned} 13^{17} &\equiv 13 \cdot 13^{16} \equiv 13 \cdot (13^2)^8 \equiv 13 \cdot 17^8 \equiv 13 \cdot (17^2)^4 \equiv 13 \cdot 4^4 \equiv 13 \cdot (4^2)^2 \equiv 13 \cdot (-3)^2 \equiv \\ &\equiv 13 \cdot 9 \equiv 3 \bmod 19. \end{aligned}$$

Nun berechnen wir $3^{81} \bmod 100$ und $3^{79} \bmod 100$:

$$\begin{aligned} 3^{81} &\equiv 3 \cdot 3^{80} \equiv 3 \cdot (3^2)^{40} \equiv 3 \cdot 9^{40} \equiv 3 \cdot (9^2)^{20} \equiv 3 \cdot 81^{20} \equiv 3 \cdot (81^2)^{10} \equiv 3 \cdot 61^{10} \equiv \\ &\equiv 3 \cdot (61^2)^5 \equiv 3 \cdot 21^5 \equiv (3 \cdot 21) \cdot 21^4 \equiv 63 \cdot (21^2)^2 \equiv 63 \cdot 41^2 \equiv 63 \cdot 81 \equiv 3 \bmod 100. \\ 3^{79} &\equiv 3 \cdot 3^{78} \equiv 3 \cdot (3^2)^{39} \equiv 3 \cdot 9^{39} \equiv (3 \cdot 9) \cdot 9^{38} \equiv 27 \cdot (9^2)^{19} \equiv \\ &\equiv 27 \cdot 81^{19} \equiv (27 \cdot 81) \cdot 81^{18} \equiv 87 \cdot (81^2)^9 \equiv 87 \cdot 61^9 \equiv (87 \cdot 61) \cdot 61^8 \equiv \\ &\equiv 7 \cdot (61^2)^4 \equiv 7 \cdot 21^4 \equiv 7 \cdot (21^2)^2 \equiv 7 \cdot 41^2 \equiv 7 \cdot 81 \equiv 67 \bmod 100. \end{aligned}$$

Wir bereiten nun die Beispiele algorithmisch auf:

Satz. *Seien $a \in \mathbb{Z}$, $d \in \mathbb{N}_0$, $n \in \mathbb{N}$ gegeben. Rekursiv werden Zahlenfolgen b_i, c_i, d_i wie folgt definiert: Man beginnt mit*

$$b_0 = 1, \quad c_0 = a \bmod n, \quad d_0 = d.$$

Seien nun b_i, c_i, d_i bereits definiert.

- *Ist $d_i = 0$, so bricht man ab. Es gilt dann*
$$b_i = a^d \bmod n.$$

- *Ist* $d_i > 0$ *und* $d_i \equiv 0 \bmod 2$*, so definiert man*

$$b_{i+1} = b_i, \quad c_{i+1} = c_i^2 \bmod n, \quad d_{i+1} = \frac{d_i}{2}.$$

- *Ist* $d_i > 0$ *und* $d_i \equiv 1 \bmod 2$*, so definiert man*

$$b_{i+1} = b_i c_i \bmod n, \quad c_{i+1} = c_i, \quad d_{i+1} = d_i - 1.$$

Beweis: Wir zeigen, dass für alle definierten Indizes i die Beziehung

$$b_i c_i^{d_i} \equiv a^d \bmod n$$

gilt. Für $i = 0$ stimmt dies. Die Beziehung gelte nun für i, d.h.

$$b_i c_i^{d_i} \equiv a^d \bmod n.$$

- Ist $d_i = 0$, so folgt sofort

$$b_i \equiv a^d \bmod n,$$

  also die Behauptung.
- Ist $d_i > 0$ und $d_i \equiv 0 \bmod 2$, so gilt

$$b_{i+1} c_{i+1}^{d_{i+1}} \equiv b_i (c_i^2)^{\frac{d_i}{2}} \equiv b_i c_i^{d_i} \equiv a^d \bmod n.$$

- Ist $d_i > 0$ und $d_i \equiv 1 \bmod 2$, so folgt

$$b_{i+1} c_{i+1}^{d_{i+1}} \equiv (b_i c_i) c_i^{d_i - 1} \equiv b_i c_i^{d_i} \equiv a^d \bmod n.$$

Im Fall $d_i > 0$ gilt also

$$b_{i+1} c_{i+1}^{d_{i+1}} \equiv a^d \bmod n.$$

Daher folgt die Behauptung durch Induktion. ■

Beispiele: Wir verwenden die Bezeichnungen des Satzes.

(1) Wir berechnen $3^{81} \bmod 100$:

i	b_i	c_i	d_i
0	1	3	81
1	3	3	80
2	3	9	40
3	3	81	20
4	3	61	10
5	3	21	5
6	63	21	4
7	63	41	2
8	63	81	1
9	3	81	0

Also ist $b_9 = 3 = 3^{81} \bmod 100$. (Es ist $81 = (1, 0, 1, 0, 0, 0, 1)_3$.)

(2) Wir berechnen $3^{79} \bmod 100$:

i	b_i	c_i	d_i
0	1	3	79
1	3	3	78
2	3	9	39
3	27	9	38
4	27	81	19
5	87	81	18
6	87	61	9
7	7	61	8
8	7	21	4
9	7	41	2
10	7	81	1
11	67	81	0

Also ist $b_{11} = 67 = 3^{79} \bmod 100$. (Es ist $79 = (1,0,0,1,1,1,1)_2$.)

(3) Wir berechnen $13^{17} \bmod 19$:

i	b_i	c_i	d_i
0	1	13	17
1	13	13	16
2	13	17	8
3	13	4	4
4	13	16	2
5	13	9	1
6	3	9	0

Daher ist $b_6 = 3 = 13^{17} \bmod 19$. (Es ist $17 = (1,0,0,0,1)_2$.)

(4) Wir berechnen $13^{33} \bmod 37$:

i	b_i	c_i	d_i
0	1	13	33
1	13	13	32
2	13	21	16
3	13	34	8
4	13	9	4
5	13	7	2
6	13	12	1
7	8	12	0

Also ist $b_7 = 8 = 13^{33} \bmod 37$. (Es ist $33 = (1,0,0,0,0,1)_2$.)

(5) Wir berechnen $2^{123456789} \bmod 987654321$:

i	b_i	c_i	d_i
0	1	2	123456789
1	2	2	123456788
2	2	4	61728394
3	2	16	30864197
4	32	16	30864196
5	32	256	15432098
6	32	65536	7716049
7	2097152	65536	7716048
8	2097152	344350012	3858024
9	2097152	392547562	1929012
10	2097152	282069526	964506
11	2097152	706746679	482253
12	149611286	706746679	482252
13	149611286	123137257	241126
14	149611286	851417971	120563
15	279277817	851417971	120562
16	279277817	345041113	60281
17	911451224	345041113	60280
18	911451224	769901713	30140
19	911451224	759344764	15070
20	911451224	483551350	7535
21	189213602	483551350	7534
22	189213602	923405899	3767
23	206271470	923405899	3766
24	206271470	964006387	1883
25	212405648	964006387	1882
26	212405648	91103341	941
27	969951539	91103341	940
28	969951539	469653595	470
29	969951539	528234745	235
30	155914325	528234745	234
31	155914325	142714780	117
32	566254001	142714780	116
33	566254001	282045658	58
34	566254001	109238839	29
35	264855578	109238839	28
36	264855578	982955794	14
37	264855578	106586737	7
38	970718579	106586737	6
39	970718579	652313308	3
40	483053927	652313308	2
41	483053927	924386425	1
42	804307517	924386425	0

Es folgt $b_{42} = 804307517 = 2^{123456789} \bmod 987654321$.
(Es ist $123456789 = (111010110111100110100010101)_2$.)

Der vorangegangene Satz führt sofort zu folgendem Algorithmus:

Potenzieren modulo n mit der square-and-multply-Methode II:
Eingabe: $a \in \mathbb{Z}$, $d \in \mathbb{N}_0$, $n \in \mathbb{N}$

Ausgabe: $a^d \bmod n$

1: $b \leftarrow 1$, $c \leftarrow a \bmod n$, $(d \leftarrow d)$
2: **while** $d > 0$ **do**
3: **if** $d \bmod 2 = 0$ **then**
4: $c \leftarrow c^2 \bmod n$, $d \leftarrow \lfloor \frac{d}{2} \rfloor$
5: **else**
6: $b \leftarrow bc \bmod n$, $d \leftarrow d - 1$
7: **end if**
8: **end while**
9: **return** b

Bemerkung: Ist e_0 die Anzahl der Nullen, e_1 die Anzahl der Einsen in der Binärdarstellung von d, so wird die while-Schleife in obigem Algorithmus genau $(2e_1 + e_0 - 1)$-mal durchlaufen.

Man kann den Algorithmus noch leicht variieren, da d_{i+1} immer gerade ist, wenn d_i ungerade ist:

Potenzieren modulo n mit der square-and-multply-Methode III:
Eingabe: $a \in \mathbb{Z}$, $d \in \mathbb{N}_0$, $n \in \mathbb{N}$
Ausgabe: $a^d \bmod n$

1: $b \leftarrow 1$, $c \leftarrow a \bmod n$, $(d \leftarrow d)$
2: **while** $d > 0$ **do**
3: **while** $d \bmod 2 = 0$ **do**
4: $c \leftarrow c^2 \bmod n$, $d \leftarrow \lfloor \frac{d}{2} \rfloor$
5: **end while**
6: $b \leftarrow bc \bmod n$, $d \leftarrow d - 1$
7: **end while**
8: **return** b

5. Der Fermatsche Primzahltest (Fermat-Test)

Der kleine Satz von Fermat besagt, dass für eine Primzahl p und eine ganze Zahl a mit $\mathrm{ggT}(a,p)=1$ stets $a^{p-1}\equiv 1 \bmod p$ gilt. Was passiert mit dieser Aussage, wenn p keine Primzahl ist?

Beispiele: Wir betrachten alle ungeraden natürlichen Zahlen mit $1<n<200$. Der Stern bedeutet, dass n eine Primzahl ist.

n	$2^{n-1} \bmod n$	n	$2^{n-1} \bmod n$	n	$2^{n-1} \bmod n$	n	$2^{n-1} \bmod n$
		51	4	$*$ 101	1	$*$ 151	1
$*$ 3	1	$*$ 53	1	$*$ 103	1	153	103
$*$ 5	1	55	49	105	46	155	109
$*$ 7	1	57	4	$*$ 107	1	$*$ 157	1
9	4	$*$ 59	1	$*$ 109	1	159	4
$*$ 11	1	$*$ 61	1	111	4	161	156
$*$ 13	1	63	4	$*$ 113	1	$*$ 163	1
15	4	65	16	115	39	165	16
$*$ 17	1	$*$ 67	1	117	22	$*$ 167	1
$*$ 19	1	69	4	119	30	169	40
21	4	$*$ 71	1	121	56	171	85
$*$ 23	1	$*$ 73	1	123	4	$*$ 173	1
25	16	75	34	125	91	175	134
27	13	77	9	$*$ 127	1	177	4
$*$ 29	1	$*$ 79	1	129	4	$*$ 179	1
$*$ 31	1	81	40	$*$ 131	1	$*$ 181	1
33	4	$*$ 83	1	133	64	183	4
35	9	85	16	135	94	185	16
$*$ 37	1	87	4	$*$ 137	1	187	174
39	4	$*$ 89	1	$*$ 139	1	189	67
$*$ 41	1	91	64	141	4	$*$ 191	1
$*$ 43	1	93	4	143	114	$*$ 193	1
45	31	95	54	145	16	195	4
$*$ 47	1	$*$ 97	1	147	25	$*$ 197	1
49	15	99	58	$*$ 149	1	$*$ 199	1

Ist n eine Primzahl, so ist $2^{n-1}\equiv 1 \bmod n$. Für die ungeraden Zahlen $1<n<200$ gilt auch die Umkehrung. Leider gilt dies aber nicht allgemein.

Definition. *Eine zusammengesetzte natürliche Zahl n heißt* **Fermat-Pseudoprimzahl zur Basis** *a oder einfach* **Pseudoprimzahl zur Basis** *a, wenn gilt* $\mathrm{ggT}(n,a)=1$ *und*

$$a^{n-1}\equiv 1 \bmod n.$$

(Natürlich folgt $\mathrm{ggT}(n,a)=1$ *aus* $a^{n-1}\equiv 1 \bmod n$*.)*

Fermat-Pseudoprimzahlen sind also zusammengesetzte Zahlen, die die Aussage des kleinen Satzes von Fermat erfüllen, obwohl sie keine Primzahlen sind.

Beispiel: Wir betrachten die Zahl $341=11\cdot 31$. Der kleine Satz von Fermat liefert $2^{10}\equiv 1 \bmod 11$, woraus sofort

$$2^{340}\equiv (2^{10})^{34}\equiv 1 \bmod 11$$

folgt. Der kleine Satz von Fermat liefert $2^{30}\equiv 1 \bmod 31$ und damit

$$2^{340}\equiv 2^{30\cdot 11+10}\equiv (2^{30})^{11}\cdot 2^{10}\equiv 2^{10}\equiv (2^5)^2\equiv 32^2\equiv 2^2\equiv 1 \bmod 31.$$

(Mit der Folgerung aus dem Satz von Euler hätten wir natürlich auch kurz

$$2^{340}\equiv 2^{(340 \bmod \varphi(11))}\equiv 2^{(340 \bmod 10)}\equiv 2^0\equiv 1 \bmod 11$$

und

$$2^{340} \equiv 2^{(340 \bmod \varphi(31))} \equiv 2^{(340 \bmod 30)} \equiv 2^{10} \equiv (2^5)^2 \equiv 1 \bmod 31$$

folgern können.) Insgesamt folgt

$$2^{340} \equiv 1 \bmod 341,$$

d.h. 341 ist eine Fermat-Pseudoprimzahl zur Basis 2.

Beispiele: Folgende Tabelle enthält alle Zahlen $n \leq 100000$, die Fermat-Pseudoprimzahlen bzgl. der Basen 2, 3, 5 oder 7 sind.

a	Alle Fermat-Pseudoprimzahlen ≤ 100000 zur Basis a
2	341, 561, 645, 1105, 1387, 1729, 1905, 2047, 2465, 2701, 2821, 3277, 4033, 4369, 4371, 4681, 5461, 6601, 7957, 8321, 8481, 8911, 10261, 10585, 11305, 12801, 13741, 13747, 13981, 14491, 15709, 15841, 16705, 18705, 18721, 19951, 23001, 23377, 25761, 29341, 30121, 30889, 31417, 31609, 31621, 33153, 34945, 35333, 39865, 41041, 41665, 42799, 46657, 49141, 49981, 52633, 55245, 57421, 60701, 60787, 62745, 63973, 65077, 65281, 68101, 72885, 74665, 75361, 80581, 83333, 83665, 85489, 87249, 88357, 88561, 90751, 91001, 93961
3	91, 121, 286, 671, 703, 949, 1105, 1541, 1729, 1891, 2465, 2665, 2701, 2821, 3281, 3367, 3751, 4961, 5551, 6601, 7381, 8401, 8911, 10585, 11011, 12403, 14383, 15203, 15457, 15841, 16471, 16531, 18721, 19345, 23521, 24046, 24661, 24727, 28009, 29161, 29341, 30857, 31621, 31697, 32791, 38503, 41041, 44287, 46657, 46999, 47197, 49051, 49141, 50881, 52633, 53131, 55261, 55969, 63139, 63973, 65485, 68887, 72041, 74593, 75361, 76627, 79003, 82513, 83333, 83665, 87913, 88561, 88573, 88831, 90751, 93961, 96139, 97567
5	4, 124, 217, 561, 781, 1541, 1729, 1891, 2821, 4123, 5461, 5611, 5662, 5731, 6601, 7449, 7813, 8029, 8911, 9881, 11041, 11476, 12801, 13021, 13333, 13981, 14981, 15751, 15841, 16297, 17767, 21361, 22791, 23653, 24211, 25327, 25351, 29341, 29539, 30673, 32021, 35371, 36661, 36991, 38081, 40501, 41041, 42127, 44173, 44801, 45141, 46657, 47641, 48133, 50737, 50997, 52633, 53083, 53971, 56033, 58807, 59356, 63973, 67921, 68101, 68251, 75361, 79381, 80476, 88831, 90241, 91636, 98173
7	6, 25, 325, 561, 703, 817, 1105, 1825, 2101, 2353, 2465, 3277, 4525, 4825, 6697, 8321, 10225, 10585, 10621, 11041, 11521, 12025, 13665, 14089, 16725, 16806, 18721, 19345, 20197, 20417, 20425, 22945, 25829, 26419, 29234, 29341, 29857, 29891, 30025, 30811, 33227, 35425, 38081, 38503, 39331, 45991, 46657, 49241, 49321, 50737, 50881, 58825, 59305, 59641, 62745, 64285, 64681, 65131, 67798, 75241, 75361, 76049, 76627, 78937, 79381, 84151, 87673, 88399, 88831, 89961, 92929, 95821, 97921

Wir zählen noch beispielhaft, wieviele Fermat-Pseudoprimzahlen es gibt: Sei $\pi(x)$ die Anzahl der Primzahlen $\leq x$ und (für folgende Tabelle) $\pi_{\text{Fermat},a}(x)$ die Anzahl der Fermatschen Pseudoprimzahlen $\leq x$ bzgl. der Basis x.

x	$\pi(x)$	$\pi_{\text{Fermat},2}(x)$	$\pi_{\text{Fermat},3}(x)$	$\pi_{\text{Fermat},5}(x)$	$\pi_{\text{Fermat},7}(x)$
10^2	25	0	1	1	2
10^3	168	3	6	5	6
10^4	1229	22	23	20	16
10^5	9592	78	78	73	73
10^6	78498	245	246	248	234
10^7	664579	750	760	745	659
10^8	5761455	2057	2155	1954	1797

Es gibt also deutlich weniger Fermat-Pseudoprimzahlen als Primzahlen. Dies gilt auch allgemein:

Satz. *In Abhängigkeit von $x \in \mathbb{R}$ bezeichne $\pi(x)$ die Anzahl der Primzahlen $\leq x$ und $\pi_{\text{Fermat},a}(x)$ die Anzahl der Fermat-Pseudoprimzahlen $\leq x$. Dann gilt:*

(1) *(Primzahlsatz)*

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1,$$

d.h. $\pi(x) \sim \frac{x}{\log x}$.

(2) *(Erdös)*

$$\lim_{x\to\infty} \frac{\pi_{\text{Fermat},a}(x)}{\pi(x)} = 0.$$

Dies macht klar: Erfüllt eine „zufällig“ gewählte Zahl n die Gleichung $a^{n-1} \equiv 1 \bmod n$, so ist n sehr wahrscheinlich prim. Da man $a^{n-1} \bmod n$ mit der square-and-multiply-Methode schnell berechnen kann, macht man daraus einen Primzahltest:

Fermat-Primzahltest zur Basis a: (Dabei ist $a \in \mathbb{N}_{\geq 2}$.) Sei n eine natürliche Zahl mit $n > a$. Man berechnet (mit der square-and-multiply-Methode)

$$b = a^{n-1} \bmod n$$

(mit $0 \leq b \leq n-1$).

(1) Gilt $b \neq 1$, so ist n zusammengesetzt.
(2) Gilt $b = 1$, so ist n eine Primzahl oder eine Fermat-Pseudoprimzahl zur Basis a. (Man sagt auch, n besteht den Fermat-Primzahltest zur Basis a.)

Bemerkung: Wir haben in der Formulierung des Primzahltests darauf verzichtet, zunächst $\text{ggT}(n,a) = 1$ zu überprüfen. Denn gilt $\text{ggT}(n,a) > 1$, so ist auch $\text{ggT}(n, a^{n-1} \bmod n) > 1$, also $(a^{n-1} \bmod n) > 1$; die Zahl n besteht den Test nicht.

Beispiele:

(1) Die ersten 5 Zahlen $> 10^{100}$, die den Fermatschen Primzahltest zur Basis 2 bestehen, sind:

$$10^{100} + 267, \quad 10^{100} + 949, \quad 10^{100} + 1243, \quad 10^{100} + 1293, \quad 10^{100} + 1983.$$

(Die gleichen Zahlen erhält man, wenn man als Basis 3, 5 oder 7 wählt.) Es handelt es sich sehr wahrscheinlich um Primzahlen.
(2) Unter den Zahlen $10^{1000} + r$ mit $1 \leq r \leq 1000$ erfüllt nur

$$10^{1000} + 453$$

den Fermat-Test zur Basis 2. (Das gleiche Ergebnis erhält man, wenn man den Test zu den Basen $3, 5, 7$ durchführt.)

Bemerkungen:

(1) Man führt folgende Sprechweise ein: Eine natürliche Zahl n, die einen oder mehrere Primzahltests besteht, nennt man eine **wahrscheinliche Primzahl**.
(2) Eine große Zahl n, die kleine Primteiler hat, ist sicher nicht prim. Daher testet man bei einem Primzahltest meist zuerst, ob n kleine Primteiler hat, bevor man einen rechnerisch langsameren Primzahltest durchführt.
(3) In der Praxis braucht man oft große Primzahlen mit bestimmten Eigenschaften. Dabei begnügt man sich meist mit wahrscheinlichen Primzahlen, da deren Konstruktion einfach und schnell geht. Im Gegensatz dazu sind Primzahlbeweise meist komplexer und langsamer.
(4) Die gängigen Computeralgebrasysteme arbeiten mit wahrscheinlichen Primzahlen.
(5) Von Agrawal, Kayal, Saxena wurde 2004 in der Arbeit „PRIMES is in P“ der sogenannte AKS-Primzahltest vorgestellt, der zwar theoretisch schnell ist, für den es aber noch keine praktikable schnelle Variante gibt.

Was passiert, wenn eine Zahl n Fermattests zu verschiedenen Basen erfüllt?

Beispiel: Hier sind alle Zahlen $< 10^6$, die gleichzeitig pseudoprim bzgl. 2, 3, 5 und 7 sind[1]:

n	Faktorisierung	
29341	$13 \cdot 37 \cdot 61$	$(*)$
46657	$13 \cdot 37 \cdot 97$	$(*)$
75361	$11 \cdot 13 \cdot 17 \cdot 31$	$(*)$
115921	$13 \cdot 37 \cdot 241$	$(*)$
162401	$17 \cdot 41 \cdot 233$	$(*)$
252601	$41 \cdot 61 \cdot 101$	$(*)$
294409	$37 \cdot 73 \cdot 109$	$(*)$
314821	$13 \cdot 61 \cdot 397$	$(*)$
334153	$19 \cdot 43 \cdot 409$	$(*)$
340561	$13 \cdot 17 \cdot 23 \cdot 67$	$(*)$
399001	$31 \cdot 61 \cdot 211$	$(*)$
410041	$41 \cdot 73 \cdot 137$	$(*)$
488881	$37 \cdot 73 \cdot 181$	$(*)$
512461	$31 \cdot 61 \cdot 271$	$(*)$
530881	$13 \cdot 97 \cdot 421$	$(*)$
552721	$13 \cdot 17 \cdot 41 \cdot 61$	$(*)$
658801	$11 \cdot 13 \cdot 17 \cdot 271$	$(*)$
721801	$601 \cdot 1201$	
852841	$11 \cdot 31 \cdot 41 \cdot 61$	$(*)$

Leider gibt es auch Zahlen, die Fermat-Pseudoprimzahlen bzgl. jeder Basis a mit $\mathrm{ggT}(a, n) = 1$ sind. Sie haben einen eigenen Namen:

6. Carmichael-Zahlen

DEFINITION. *Eine zusammengesetzte natürliche Zahl n heißt Carmichael-Zahl, wenn für alle natürlichen Zahlen a mit $\mathrm{ggT}(a, n) = 1$ gilt*

$$a^{n-1} \equiv 1 \bmod n.$$

Beispiele: Die folgende Tabelle enthält alle Carmichael-Zahlen ≤ 100000 zusammen mit der Primfaktorzerlegung:

Carmichael-Zahl n	Primfaktorzerlegung von n
561	$3 \cdot 11 \cdot 17$
1105	$5 \cdot 13 \cdot 17$
1729	$7 \cdot 13 \cdot 19$
2465	$5 \cdot 17 \cdot 29$
2821	$7 \cdot 13 \cdot 31$
6601	$7 \cdot 23 \cdot 41$
8911	$7 \cdot 19 \cdot 67$
10585	$5 \cdot 29 \cdot 73$
15841	$7 \cdot 31 \cdot 73$
29341	$13 \cdot 37 \cdot 61$
41041	$7 \cdot 11 \cdot 13 \cdot 41$
46657	$13 \cdot 37 \cdot 97$
52633	$7 \cdot 73 \cdot 103$
62745	$3 \cdot 5 \cdot 47 \cdot 89$
63973	$7 \cdot 13 \cdot 19 \cdot 37$
75361	$11 \cdot 13 \cdot 17 \cdot 31$

[1] $(*)$ bedeutet, dass n eine Carmichael-Zahl ist.

1994 wurde gezeigt, dass es unendlich viele Carmichael-Zahlen gibt. Es ist praktisch auch nicht schwer, große Carmichael-Zahlen zu konstruieren, so ist z.B.

$$n = (6u+1)(12u+1)(18u+1) \quad \text{mit} \quad u = 10^{100} + 289351$$

eine Carmichael-Zahl.

Da jede ganze Zahl a modulo n zu einer Zahl aus $\{0, 1, \ldots, n-1\}$ kongruent ist, muss man die Gleichung $a^{n-1} \equiv 1 \bmod n$ nur für alle $a \in \{0, 1, \ldots, n-1\}$ mit $\mathrm{ggT}(n, a) = 1$ testen. Daher kann man leicht die kleinsten Carmichael-Zahlen angegeben. Für etwas größere natürliche Zahlen hat man folgendes Kriterium:

Satz (Korselt-Kriterium). *Eine natürliche Zahl n ist genau dann eine Carmichael-Zahl, wenn folgende Bedingungen erfüllt sind:*

(1) *n ist zusammengesetzt.*
(2) *n ist quadratfrei, d.h. für jeden Primteiler p von n gilt $p^2 \nmid n$.*
(3) *Für jeden Primteiler p von n gilt $p - 1 \mid n - 1$.*

Alternativ kann man dies auch so formulieren: n ist genau dann eine Carmichael-Zahl, wenn die Primfaktorzerlegung von n die Gestalt $n = p_1 \ldots p_r$ mit $r \geq 2$ hat und $p_i - 1 \mid n - 1$ für $1 \leq i \leq r$ gilt.

Beweis[2]*:*

$\Longrightarrow$ Sei n eine Carmichael-Zahl. Wir überprüfen die angegebenen drei Bedingungen:

(1) Nach Definition der Carmichael-Zahlen ist n zusammengesetzt.

(2) Wir nehmen an, n ist nicht quadratfrei. Dann gibt es einen Primteiler p von n, sodass gilt $n = p^e m$ mit $e \geq 2$ und $p \nmid m$. Wegen $\mathrm{ggT}(n, 1+p^{e-1}m) = 1$ folgt $(1+p^{e-1}m)^{n-1} \equiv 1 \bmod n$ und damit $(1 + p^{e-1}m)^{n-1} \equiv 1 \bmod p^e$. Wegen $e \geq 2$ ist $2(e-1) \geq e$, was zu

$$1 \equiv (1 + p^{e-1}m)^{n-1} \equiv \sum_{i=0}^{n-1} \binom{n-1}{i} (p^{e-1}m)^i \equiv 1 + (n-1)p^{e-1}m \bmod p^e$$

und damit zum Widerspruch $p^e \mid (n-1)p^{e-1}m$ führt. Also muss n doch quadratfrei sein.

(3) Sei p ein Primteiler von n. Wir schreiben $n = pm$. Da wir schon gezeigt habe, dass n quadratfrei ist, gilt $\mathrm{ggT}(p, m) = 1$. Sei g_p eine Primitivwurzel modulo p, d.h. eine Zahl g_p mit $\mathrm{ord}_p(g_p) = p - 1$. Mit dem chinesischen Restsatz findet man eine Zahl g mit

$$g \equiv g_p \bmod p \quad \text{und} \quad g \equiv 1 \bmod m.$$

Man sieht leicht, dass dann $\mathrm{ggT}(g, n) = 1$ gilt, sodass die Carmichael-Eigenschaft nun $g^{n-1} \equiv 1 \bmod n$ und damit

$$g_p^{n-1} \equiv g^{n-1} \equiv 1 \bmod p$$

liefert. Es folgt $\mathrm{ord}_p(g_p) \mid n - 1$, also $p - 1 \mid n - 1$, wie behauptet.

$\Longleftarrow$ Eine natürliche Zahl n erfülle die angegebenen Bedingungen. Wir können dann die Primfaktorzerlegung und die Bedingungen in der Form

$$n = p_1 \ldots p_r \quad \text{mit} \quad r \geq 2 \quad \text{und} \quad p_i - 1 \mid n - 1$$

schreiben. Sei $a \in \mathbb{Z}$ mit $\mathrm{ggT}(n, a) = 1$. Dann gilt auch $\mathrm{ggT}(n, p_i) = 1$. Der kleine Satz von Fermat liefert $a^{p_i - 1} \equiv 1 \bmod p_i$ und damit

$$a^{n-1} \equiv \left(a^{p_i-1}\right)^{\frac{n-1}{p_i-1}} \equiv 1 \bmod p_i \quad \text{wegen} \quad \frac{n-1}{p_i-1} \in \mathbb{N}.$$

Aus $n = p_1 \ldots p_r$ folgt dann sofort

$$a^{n-1} \equiv 1 \bmod n.$$

Da n zusammengesetzt ist, ist n dann eine Carmichael-Zahl. ■

[2]Der Beweis setzt mehr Vorkenntnisse voraus, als im Augenblick zur Verfügung stehen, beispielsweise „Primitivwurzel“ und „Ordnung“.

Beispiel: Es ist $561 = 3 \cdot 11 \cdot 17$. Wegen

$$2 \mid 560, \quad 10 \mid 560, \quad 16 \mid 560$$

ist 561 eine Carmichael-Zahl nach dem Korselt-Kriterium.

Carmichael-Zahlen habe eine Reihe von Eigenschaften, von den wir hier ein paar erwähnen:

FOLGERUNG. *Für eine Carmichael-Zahl n gilt:*

(1) *n ist ungerade.*
(2) *n hat mindestens drei Primteiler.*

Beweis:

(1) Da n zusammengesetzt ist, muss n (mindestens) einen ungeraden Primteiler p haben. Dann ist $p-1$ gerade, sodass aus $p-1 \mid n-1$ folgt, dass auch $n-1$ gerade und damit n ungerade ist.
(2) Da n als Carmichael-Zahl zusammengesetzt und quadratfrei ist, hat n mindestens zwei Primteiler. Wir betrachten den Fall, dass n genau zwei Primteiler p und q hat, also $n = pq$ mit $p < q$. Wegen $q-1 \mid n-1$ folgt aus $n-1 = pq-1 = p(q-1)+(p-1)$ sofort $q-1 \mid p-1$, also $q-1 \leq p-1$, was im Widerspruch zu $p < q$ steht. Daher muss n mindestens drei Primteiler besitzen.

SATZ. *Eine zusammengesetzte natürliche Zahl n ist genau dann eine Carmichael-Zahl, wenn gilt*

$$a^n \equiv a \bmod n \text{ für alle } a \in \mathbb{Z}.$$

7. Der Miller-Rabin-Test

Der Fermatsche Primzahltest untersucht, ob $a^{n-1} \equiv 1 \bmod n$ gilt. Leider gibt es zusammengesetzte Zahlen n, so dass alle a mit $\mathrm{ggT}(a,n) = 1$ diese Bedingung erfüllen, nämlich die Carmichael-Zahlen. Wir werden den Fermattest jetzt etwas verfeinern.

LEMMA. *Ist p eine Primzahl, a eine Zahl mit $a^2 \equiv 1 \bmod p$ und $a \not\equiv 1 \bmod p$, so gilt $a \equiv -1 \bmod p$.*

Beweis: Es ist $0 \equiv a^2 - 1 = (a-1)(a+1) \bmod p$, d.h. $p \mid (a-1)(a+1)$. Nach Voraussetzung ist $a \not\equiv 1 \bmod p$, d.h. $p \not\mid a-1$ und damit $p \mid a+1$, d.h. $a \equiv -1 \bmod p$. ■

Beispiel: Für zusammengesetzte Zahlen n gilt die Aussage des Lemmas im allgemeinen nicht, so ist z.B. $3^2 \equiv 1 \bmod 8$, aber $3 \not\equiv \pm 1 \bmod 8$.

LEMMA. *Sei p eine ungerade Primzahl und $p-1 = 2^\ell q$ mit $q \equiv 1 \bmod 2$. Sei a eine Zahl mit $\mathrm{ggT}(a,p) = 1$ und $b \equiv a^q \bmod p$. Dann gilt für b: Entweder ist $b \equiv 1 \bmod p$ oder es gibt ein i mit $0 \leq i \leq \ell - 1$ und $b^{2^i} \equiv -1 \bmod p$.*

Beweis: Der kleine Satz von Fermat zeigt

$$1 \equiv a^{p-1} \equiv a^{q \cdot 2^\ell} \equiv b^{2^\ell} \bmod p.$$

Ist $b \equiv 1 \bmod p$, so sind wir fertig. Sei also $b \not\equiv 1 \bmod p$. Dann gibt einen Index i mit $0 \leq i \leq \ell - 1$, so dass

$$b^{2^{i+1}} \equiv 1 \bmod p, \quad \text{aber} \quad b^{2^i} \not\equiv 1 \bmod p.$$

Damit gilt $(b^{2^i})^2 \equiv 1 \bmod p$, nach unserem Lemma also $b^{2^i} \equiv -1 \bmod p$, was zu zeigen war. ■

Beispiel: Für $p = 1009$ ist $p - 1 = 2^4 \cdot 63$. Für $a = 2$ ist

$$2^{63} \equiv 192, \quad 192^2 \equiv 540, \quad 540^2 \equiv 1008 \equiv -1 \bmod p.$$

Was passiert nun mit der Aussage des Lemmas, wenn man keine Primzahl hat?

Beispiele:

(1) $341 = 11 \cdot 31$ war eine Pseudoprimzahl zur Basis 2. Nun ist $341 - 1 = 2^2 \cdot 85$. Wählt man $a = 2$ und $b \equiv a^{85} \equiv 32 \bmod 341$, so ist $b^2 \equiv 1 \bmod 341$, also kann 341 nach dem Lemma keine Primzahl sein.
(2) $561 = 3 \cdot 11 \cdot 17$ ist die kleinste Carmichael-Zahl. Nun ist $561 - 1 = 2^4 \cdot 35$. Wir wählen $a = 2$, erhalten $b \equiv a^{35} \equiv 263 \bmod 561$. Nun quadrieren wir:

$$b^2 \equiv 166, \quad b^4 \equiv 67, \quad b^8 \equiv 1 \bmod 561,$$

also kann 561 keine Primzahl sein.
(3) Wir betrachten $n = 10^{1000} + 453$, erhalten $n - 1 = 2^2 \cdot q$ mit einer ungeraden Zahl q. Wir wählen $a = 2$ und berechnen dann $b \equiv a^q \bmod n$ und erhalten:

$$b \not\equiv \pm 1 \bmod n, \quad b^2 \equiv -1 \bmod n,$$

wir erhalten keinen Widerspruch zum Lemma: n ist möglicherweise eine Primzahl.

Die vorstehenden Überlegungen führen zu folgendem Test:

Miller-Rabin-Primzahltest zur Basis a: (Dabei ist $a \in \mathbb{N}_{\geq 2}$.) Sei n eine ungerade natürliche Zahl mit $n > a$. Wir zerlegen

$$n - 1 = 2^\ell q \text{ mit } q \equiv 1 \bmod 2 \quad \text{ und berechnen } \quad b = a^q \bmod n.$$

Gilt

$$b = 1 \quad \text{ oder } \quad b^{2^i} \equiv -1 \bmod n \text{ für ein } i \text{ mit } 0 \leq i \leq \ell - 1,$$

so sagen wir, *n besteht den Miller-Rabin-Test zur Basis a.* Andernfalls ist n zusammengesetzt. (Die Potenzen $b^{2^i} \bmod n$ berechnet man natürlich durch sukzessives Quadrieren: b, b^2, $b^4 = (b^2)^2$, $b^8 = (b^4)^2$, $b^{16} = (b^8)^2$, ...)

Hier ist eine algorithmische Variante:

Miller-Rabin-Primzahltest zur Basis a:
Eingabe: Eine ungerade natürliche Zahl n und eine natürliche Zahl a mit $2 \leq a \leq n - 1$
Ausgabe: (n besteht den Miller-Rabin-Test zur Basis a) oder (n ist zusammengesetzt)

Zerlege $n - 1 = 2^\ell q$ mit einer ungeraden Zahl q
$b \leftarrow a^q \bmod n$
if $b = 1$ oder $b = n - 1$ **then**
    return n besteht den Miller-Rabin-Test zur Basis a
end if
for $i = 1, \ldots, \ell - 1$ **do**
    $b \leftarrow b^2 \bmod n$ ▷ Dann ist $b = (a^q)^{2^i} \bmod n$
    if $b = n - 1$ **then**
        return n besteht den Miller-Rabin-Test zur Basis a
    end if
end for
return n ist zusammengesetzt

Besteht nun eine Zahl n einen Miller-Rabin-Test, so hofft man, dass n prim ist. Leider gibt es auch hier, analog zu den Pseudoprimzahlen beim Fermattest, zusammengesetzte Zahlen, die einen Miller-Rabin-Test bestehen:

Definition. *Eine zusammengesetzte ungerade natürliche Zahl n heißt* **Miller-Rabin-Pseudoprimzahl zur Basis** *a oder eine* **starke Pseudoprimzahl zur Basis** *a, wenn n den Miller-Rabin-Test zur Basis a besteht, d.h. ist $n - 1 = 2^\ell \cdot q$ mit $q \equiv 1 \bmod 2$, so gilt für $b \equiv a^q \bmod n$:*

$$b \equiv 1 \bmod n \quad \textit{oder} \quad b^{2^i} \equiv -1 \bmod n \textit{ für ein } i \textit{ mit } 0 \leq i \leq \ell - 1.$$

Beispiel: Wir betrachten $n = 2047 = 23 \cdot 89$. Es ist

$$n - 1 = 2 \cdot 1023,$$

insbesondere $\ell = 1$.
Wir berechnen für $a = 2$

$$b = (2^{1023} \bmod n) = 1.$$

Also besteht n den Miller-Rabin-Test zur Basis 2. Die Zahl 2047 ist also eine Miller-Rabin-Pseudoprimzahl zur Basis 2.
Nun betrachten wir noch $a = 3$. Wir berechnen

$$b = (3^{1023} \bmod n) = 1565.$$

Da wir nur $b^{2^i} \bmod n$ für $0 \leq i \leq \ell - 1 = 0$ anschauen müssen und $b \not\equiv \pm 1 \bmod n$ ist, besteht n den Miller-Rabin-Test zur Basis 3 nicht.

Beispiele: In der folgenden Liste sind alle starken Pseudoprimzahlen $\leq 10^5$ zu den Basen $a = 2, 3, 5, 7$ aufgeführt.

2	2047, 3277, 4033, 4681, 8321, 15841, 29341, 42799, 49141, 52633, 65281, 74665, 80581, 85489, 88357, 90751
3	121, 703, 1891, 3281, 8401, 8911, 10585, 12403, 16531, 18721, 19345, 23521, 31621, 44287, 47197, 55969, 63139, 74593, 79003, 82513, 87913, 88573, 97567
5	781, 1541, 5461, 5611, 7813, 13021, 14981, 15751, 24211, 25351, 29539, 38081, 40501, 44801, 53971, 79381
7	25, 325, 703, 2101, 2353, 4525, 11041, 14089, 20197, 29857, 29891, 39331, 49241, 58825, 64681, 76627, 78937, 79381, 87673, 88399, 88831

Im folgenden sind die zusammengesetzten Zahlen $n \leq 10^7$ angegeben, die den Miller-Rabin-Test sowohl zur Basis 2 als auch zur Basis 3 bestehen:

$$1373653, 1530787, 1987021, 2284453, 3116107, 5173601, 6787327.$$

(Eine Anwendungsmöglichkeit ist folgende: Besteht eine ungerade Zahl $\leq 10^7$ den Miller-Rabin-Test für $a = 2$ und $a = 3$ und ist sie nicht in obiger Liste, so ist die Zahl prim.)

Für die folgende Tabelle haben wir wieder Primzahlen und Pseudoprimzahlen gezählt, mit folgenden Bezeichnungen:

$$\begin{aligned} \pi(x) &= \#\{p \leq x : p \text{ ist Primzahl}\}, \\ \pi_{\mathrm{F},a}(x) &= \#\{n \leq x : n \text{ ist Fermat-Pseudoprimzahl zur Basis } a\}, \\ \pi_{\mathrm{MR},a}(x) &= \#\{n \leq x : n \text{ ist Miller-Rabin-Pseudoprimzahl zur Basis } a\}. \end{aligned}$$

N	$\pi(N)$	$\pi_{\mathrm{F},2}(N)$	$\pi_{\mathrm{F},3}(N)$	$\pi_{\mathrm{F},5}(N)$	$\pi_{\mathrm{F},7}(N)$	$\pi_{\mathrm{MR},2}(N)$	$\pi_{\mathrm{MR},3}(N)$	$\pi_{\mathrm{MR},5}(N)$	$\pi_{\mathrm{MR},7}(N)$
10^2	25	0	1	1	2	0	0	0	1
10^3	168	3	6	5	6	0	2	1	3
10^4	1229	22	23	20	16	5	6	5	6
10^5	9592	78	78	73	73	16	23	16	21
10^6	78498	245	246	248	234	46	73	64	66
10^7	664579	750	760	745	659	162	207	199	177
10^8	5761455	2057	2155	1954	1797	488	582	475	446

Der entscheidende Unterschied zwischen Fermattest und Miller-Rabin-Test besteht nun darin, dass es beim Miller-Rabin-Test kein Analogon zu den Carmichael-Zahlen gibt:

LEMMA. *Sei eine zusammengesetzte ungerade natürliche Zahl. Dann gilt:*

$$\#\{a \in \{2, 3, \ldots, n-1\} : n \text{ besteht den Miller-Rabin-Test zur Basis } a\} < \frac{1}{4}\varphi(n) < \frac{1}{4}n.$$

Beweis: [Knuth. The Art of Computer Programming. Vol. 2, p.612] ■

Beispiele: Hier sind die zusammengesetzten ungeraden Zahlen n und die Zahlen $a \in \{2, \ldots, n-1\}$, sodass n den Miller-Rabin-Test zur Basis a besteht.

n	$a \in \{2, \ldots, n-1\}$, sodass n den Miller-Rabin-Test zur Basis a besteht
9	8
15	14
21	20
25	7, 18, 24
27	26
33	32
35	34
39	38
45	44
49	18, 19, 30, 31, 48
51	50
55	54
57	56
63	62
65	8, 18, 47, 57, 64
69	68
75	74
77	76
81	80
85	13, 38, 47, 72, 84
87	86
91	9, 10, 12, 16, 17, 22, 29, 38, 53, 62, 69, 74, 75, 79, 81, 82, 90
93	92
95	94
99	98

(Man sieht leicht, dass n den Miller-Rabin-Test zur Basis $n-1$ immer besteht, sodass man sich beim Test auf Zahlen $a \in \{2, \ldots, n-2\}$ beschränken sollte.)

Überlegung: Sei n eine zusammengesetzte ungerade natürliche Zahl und

$$E(n) = \{a \in \{2, \ldots, n-1\} : n \text{ besteht den Miller-Rabin-Test zur Basis } a\}$$

die Menge der Basen, für die n den Miller-Rabin-Test besteht. Dann folgt aus dem Lemma

$$\#E(n) < \frac{1}{4}n.$$

Wählen wir jetzt unabhängig voneinander Zahlen $a_1, \ldots, a_r \in \{2, \ldots, n-1\}$, so gilt für die Wahrscheinlichkeit, dass der Miller-Rabin-Test für alle a_i's funktioniert

$$\text{Wahrscheinlichkeit}(a_1, a_2, \ldots, a_r \in E(n)) \leq (\frac{\#E(n)}{n})^r < (\frac{1}{4})^r.$$

Anders ausgedrückt: Erfüllt eine ungerade natürliche Zahl r (unabhängige) Miller-Rabin-Tests, so ist die Wahrscheinlichkeit, dass n prim ist

$$\geq 1 - (\frac{1}{4})^r.$$

Besteht z.B. eine natürliche Zahl 25 Miller-Rabin-Tests, so ist die Wahrscheinlichkeit, dass n nicht prim ist, $< 10^{-15}$. Für die Praxis genügen diese Anforderungen. (Auch hier spricht man dann wieder von **wahrscheinlichen Primzahlen**.)

Bemerkungen:

(1) Bei vielen Anwendungen werden wahrscheinliche Primzahlen benutzt, da ein Miller-Rabin-Test einfach zu programmieren und schnell in der Ausführung ist. Das BSI empfiehlt den Miller-Rabin-Test.
(2) Natürlich gibt es auch Methoden um zu zeigen, dass eine große Zahl eine Primzahl ist, z.B. der Jacobi-Summen-Test oder ECPP (elliptic curve primality proving) oder der AKS-Test. Für die Praxis haben sie aber zwei Nachteile: sie sind einmal langsamer und zum zweiten sind sie wesentlich komplexer und aufwändiger, so dass Programmierfehler wahrscheinlicher werden.

Mit dem folgenden Algorithmus kann man die auf eine Zahl n folgende Primzahl bestimmen:

Bestimmung der kleinsten Primzahl $p > n$ bei gegebener Zahl n:

Gewählt wird eine natürliche Zahl K, beispielsweise $K = 100000$
Bestimmt werden alle Primzahlen $\leq K$: $\ell_0, \ldots, \ell_{m-1}$, beispielsweise mit dem Sieb des Eratosthenes
Gewählt werden Basen für Miller-Rabin-Tests: $a_0, \ldots, a_{r-1}$
Eingabe: Eine natürliche Zahl n mit $n > K$
Ausgabe: Die kleinste (wahrscheinliche) Primzahl $p > n$

```
p ← n + 1
loop
    i ← 0
    while i < m und p mod ℓ_i ≠ 0 do                ▷ Hat p den Primteiler ℓ_i?
        i ← i + 1
    end while
    if i = m then                                   ▷ p hat keinen Primteiler ≤ K
        j ← 0
        while j < r und p besteht den Miller-Rabin-Test zur Basis a_j do
            j ← j + 1
        end while
        if j = r then                               ▷ p hat alle Miller-Rabin-Tests bestanden
            return p
        end if
    end if
    p ← p + 1
end loop
```

Beispiel: Wir suchen (wahrscheinliche) Primzahlen $p = 10^{1000}+r$. Wir starten mit $n = 10^{1000}$, verwenden verschiedene K und den Miller-Rabin-Test zur Basis 2. Wir finden als erste wahrscheinliche Primzahl $p = 10^{1000} + 453$. Die Laufzeiten waren wie folgt:

K	10	100	1000	10000	100000	1000000
Zeit	8.54 sec	4.32 sec	3.41 sec	2.62 sec	2.40 sec	4.32 sec

Nun haben wir uns auf $K = 10^5$ beschränkt und jeweils gemessen, wie lange wir zum Finden der nächsten (wahrscheinlichen) Primzahl $10^{1000} + r$ gebraucht haben:

r	453	1357	2713	4351	5733	7383	10401	11979	17557	21567
Zeit	2.39 sec	4.21 sec	6.66 sec	7.55	6.87 sec	7.71 sec	14.76 sec	7.74 sec	26.59 sec	18.28 sec

Bemerkung: Die Zahl $n = 10^{1000}+453$ besteht den Miller-Rabin-Test für alle Basen a mit $2 \leq a \leq 3000$, wie wir überprüft haben. (Dies beweist natürlich noch nicht, dass n tatsächlich eine Primzahl ist.)

Erstaunlicherweise gibt es einen Satz, der skizziert, wie aus einer wahrscheinlichen Primzahl eine (bewiesene) Primzahl werden kann:

Satz. *Gilt die erweiterte Riemannsche Vermutung (ERH) und besteht eine Zahl p die Miller-Rabin-Tests bezüglich aller Basen a mit $2 \leq a \leq 2(\ln p)^2$, so ist p eine Primzahl.*

Bemerkungen:

(1) Die (nichtbewiesene) erweiterte Riemannsche Vermutung macht Aussagen über die Lage von Nullstellen meromorpher komplexer Funktionen.
(2) Praktisch ist der Satz nicht von großem Interesse: Braucht man einen Primzahlbeweis, so kann man ihn nicht benutzen, da ERH noch nicht bewiesen ist, andernfalls reichen meistens wahrscheinliche Primzahlen.

Beispiel: Wir wollen sehen, wie weit man mit obigem Satz kommen würde, wenn die Gültigkeit der ERH gezeigt wäre.
Für $p = 10^{1000} + 453$ ist $[2(\ln p)^2] = 10603796$. Wir müssten dann alle Miller-Rabin-Tests bezüglich a mit $2 \leq a \leq 10603796$ durchführen, was ziemlich aufwändig ist.

Bemerkung: Die vorgestellten Primzahltests beruhen darauf, dass es Eigenschaften gibt, die Primzahlen von den meisten zusammengesetzten Zahlen unterscheiden. Daher stellt sich die Aufgabe: Finde gute – einfach und schnell auszuführende – Kriterien, wie sich Primzahlen von zusammengesetzten Zahlen unterscheiden.

Bemerkung: Will man große Primzahlen konstruieren, so ist es sinnvoll zu wissen, wie häufig Primzahlen sind. Obwohl Primzahlen nicht sehr regelmäßig verteilt sind, kann man doch in gewisser Weise eine Dichte angeben:

$$\text{Primzahldichte um } n \approx \frac{1}{\ln n} \approx \frac{1}{2.3 \log_{10} x}.$$

Um 10^ℓ ist also die Primzahldichte $\approx \frac{1}{2.3\ell}$, anschaulich (und mit aller Vorsicht zu genießen): auf 2.3ℓ Zahlen um n kommt eine Primzahl.

Beispiel: Wie oben bereits angegeben gibt es 9 Primzahlen zwischen 10^{1000} und $10^{1000} + 20000$, andererseits ist

$$\frac{20000}{\ln 10^{1000}} = 8.69.$$

Die Teiler ≤ 100000 der ungeraden Zahlen $10^{1000} + r$ für $1 \leq r \leq 200$:

r	Kleine Teiler von $10^{1000} + r$
1	$17 \cdot 16001$
3	$7 \cdot 7 \cdot 7 \cdot 7$
5	$3 \cdot 5 \cdot 43 \cdot 229 \cdot 14387$
7	$23 \cdot 149$
9	$12917 \cdot 42577$
11	$3 \cdot 4621$
13	$1151 \cdot 3793$
15	$5 \cdot 211 \cdot 13397$
17	$3 \cdot 3 \cdot 3 \cdot 7$
19	
21	$11 \cdot 1231$
23	$3 \cdot 13 \cdot 71 \cdot 10159$
25	$5 \cdot 5$
27	$37 \cdot 661$
29	$3 \cdot 19 \cdot 36433$
31	7
33	7417
35	$3 \cdot 3 \cdot 5 \cdot 17 \cdot 631 \cdot 1993 \cdot 3739 \cdot 10937$
37	$53 \cdot 2269$
39	
41	$3 \cdot 12143$
43	$11 \cdot 307$
45	$5 \cdot 7 \cdot 1907$
47	$3 \cdot 571$
49	$13 \cdot 397$
51	$29 \cdot 347$
53	$3 \cdot 3 \cdot 23 \cdot 379 \cdot 92467$
55	$5 \cdot 733 \cdot 6361$
57	31
59	$3 \cdot 7$
61	14249
63	
65	$3 \cdot 5 \cdot 11$
67	$19 \cdot 19$
69	$17 \cdot 47$
71	$3 \cdot 3 \cdot 3 \cdot 3 \cdot 79 \cdot 68161$
73	$7 \cdot 12829$
75	$5 \cdot 5 \cdot 13 \cdot 61 \cdot 1543$
77	3
79	
81	41
83	3
85	$5 \cdot 2381$
87	$7 \cdot 11 \cdot 691$
89	$3 \cdot 3 \cdot 1171 \cdot 5657$
91	$43 \cdot 4493 \cdot 6133$
93	
95	$3 \cdot 5$
97	28111
99	23

r	Kleine Teiler von $10^{1000} + r$
101	$3 \cdot 7 \cdot 7 \cdot 13 \cdot 37 \cdot 59$
103	$17 \cdot 97$
105	$5 \cdot 19$
107	$3 \cdot 3$
109	$11 \cdot 11 \cdot 29 \cdot 113 \cdot 503 \cdot 59419$
111	67
113	$3 \cdot 61211$
115	$5 \cdot 7 \cdot 12659$
117	
119	$3 \cdot 31 \cdot 151 \cdot 367 \cdot 1217$
121	
123	3613
125	$3 \cdot 3 \cdot 3 \cdot 5 \cdot 5 \cdot 5 \cdot 107$
127	$13 \cdot 103 \cdot 1949$
129	$7 \cdot 7933 \cdot 14879 \cdot 22943$
131	$3 \cdot 11$
133	
135	$5 \cdot 83 \cdot 22741$
137	$3 \cdot 17$
139	$89 \cdot 349 \cdot 463$
141	
143	$3 \cdot 3 \cdot 7 \cdot 19 \cdot 53 \cdot 199 \cdot 2309$
145	$5 \cdot 23 \cdot 73 \cdot 1741 \cdot 3691$
147	
149	$3 \cdot 2677 \cdot 6521 \cdot 7753$
151	$7559 \cdot 46141$
153	$11 \cdot 13 \cdot 3061$
155	$3 \cdot 5$
157	$7 \cdot 12641$
159	$173 \cdot 439$
161	$3 \cdot 3$
163	$41 \cdot 47 \cdot 131 \cdot 25463$
165	$5 \cdot 71 \cdot 5081$
167	$3 \cdot 29 \cdot 127$
169	
171	$7 \cdot 17 \cdot 311 \cdot 313$
173	3
175	$5 \cdot 5 \cdot 11 \cdot 37 \cdot 2531$
177	43
179	$3 \cdot 3 \cdot 3 \cdot 13$
181	$19 \cdot 31 \cdot 11159$
183	
185	$3 \cdot 5 \cdot 7$
187	$167 \cdot 20177$
189	
191	$3 \cdot 23 \cdot 18911$
193	18793
195	$5 \cdot 613 \cdot 2837 \cdot 3121$
197	$3 \cdot 3 \cdot 11 \cdot 61$
199	$7 \cdot 7 \cdot 139 \cdot 269 \cdot 617 \cdot 42899$