Prof. Dr. Alfred Schreiber – Institut für Mathematik und ihre Didaktik

"Algorithmen" : Sieb des Eratosthenes
Nachtrag zur Verfahrensbegründung
und Lösung von Aufgabe 25

Nachtrag zu "Das Sieb des Eratosthenes"

Es folgt hier eine Zusammenstellung sämtlicher Teilaussagen (und Beweise), die zum Nachweis der Gültigkeit des in der Vorlesung angegebenen Algorithmus "Sieb des Eratosthenes" notwendig und hinreichend sind (einschließlich einer Beantwortung der Frage in A25).

Behauptung 1. Die Siebzahlen sind genau diejenigen Zahlen in {1, 2, …, n}, die nicht gestrichen werden.

Beweis: Es werden ausschließlich die *echten* Vielfachen einer Siebzahl gestrichen.

Behauptung 2. Die Primzahlen in {1, 2, …, n} werden nicht gestrichen.

Beweis: Eine Primzahl ist niemals echtes Vielfache einer Zahl.

Behauptung 3. Eine Zahl in {1, 2, …, n} , die nicht gestrichen wird, ist notwendig prim.

Beweis: Sei m eine beliebige Zahl, die nicht gestrichen wird. Man betrachte den kleinsten Primteiler q von m. Es gilt $m = k\,q$ mit ganzem $k \geq 1$. Wäre $k \geq 2$, so wäre m echtes Vielfache einer Primzahl $q \in \{1, 2, \ldots, n\}$. Nach Behauptung 2 wird q nicht gestrichen, ist also nach Behauptung 1 eine Siebzahl. Bei einem Siebschritt mit q müsste m jedoch gestrichen werden. Infolgedessen kann nur $k = 1$ sein, d.h. m ist prim.

Behauptung 4. Alle im Siebverfahren auftretenden Siebzahlen sind prim.

Beweis: Folgt unmittelbar aus Behauptung 1 und Behauptung 3.

Behauptung 5. Wurde mit allen Primzahlen kleiner als p schon gesiebt, so ist p^2 die (beim Siebschritt mit p) nächste zu streichende Zahl.

Beweis: Alle Vielfachen $k \cdot p$ mit $2 \leq k < p$ sind bereits gestrichen. Sei nämlich q kleinster Primteiler eines solchen k, dann hat man $k \cdot p = q \cdot (k' \cdot p)$ mit ganzem $k' \geq 1$. Wegen $q \leq k < p$ ist q eine vor p benutzte Siebzahl, also muss $k \cdot p$ als ein echtes Vielfaches von q gestrichen worden sein. Beim Siebschritt mit p ergibt sich daher als nächste zu streichende Zahl p^2.

Behauptung 6. Wurde mit allen Primzahlen $p \leq \lfloor \sqrt{n} \rfloor$ gesiebt, so bewirken weitere Siebschritte keine Streichungen in der Liste {1, 2, …, n}.

Beweis: Sei p_m die größte der Primzahlen $p \leq \lfloor \sqrt{n} \rfloor$. Beim Siebschritt mit p_m ist nach Behauptung 5 die nächste zu streichende Zahl $p_m{}^2 \leq n$. Die nachfolgende Siebzahl p_{m+1} ist (da Primzahl gemäß Behauptung 4) größer als $\lfloor \sqrt{n} \rfloor$; mithin wäre nun die erste zu streichende Zahl $p_{m+1}{}^2$ größer als n.

Bemerkung. Behauptung 6 besagt, dass man die Siebzahlen durch $\lfloor \sqrt{n} \rfloor$ beschränken kann (wie im Algorithmus in funclib.js dann auch tatsächlich geschehen).

Aufgabe 25

In beiden Varianten des Siebverfahrens (siehe Aufgabe 24) wird die jeweils nächste Siebzahl (bzw. ihre Position **`i`**) mittels der Schleife

```
while ( tab[i]==0 ) i=i+1
```

gesucht. Es ist nachzuweisen, dass die Schleife terminiert. Man zeige dazu, dass zu jeder Siebzahl $p \le \lfloor \sqrt{n} \rfloor$ eine noch nicht gestrichene Zahl q mit $p < q \le n$ existiert.

Lösung

Mit den oben dargelegten Aussagen ergibt sich die Begründung unmittelbar: Die nächste mit einer Siebzahl $p \le \lfloor \sqrt{n} \rfloor$ zu streichende Zahl ist (laut Behauptung 5) $p^2 (\le n)$, man kann (in der Behauptung der Aufgabe) also $q = p^2$ wählen, wenn q nicht schon vorher gestrichen wurde. Dies ist aber klar, weil q ein echtes Vielfaches von p und außerdem keiner anderen Siebzahl ist.