Anwendung des „Eratosthenes“ auf Dreiklassenteilung von

$\mathbb{N}_u$

von

Erich Landhäußer*

(A) Einleitung:

Zerlegt man die Menge $\mathbb{N}_u = \{5, 7, 9, 11, \cdots\}$ in Tripel und schreibt diese in Spalten, so erhält man

formal $3\,x\,1$ Spalten: Landhäußer [1]

$$
\text{.(I)} \qquad \begin{array}{ccccccccc}
\sigma: \; 0, & 1, & 2, & 3, & 4, & 5, & 6, & 7, & \cdots \\
\begin{pmatrix}5\\7\\9\end{pmatrix}, & \begin{pmatrix}11\\13\\15\end{pmatrix}, & \begin{pmatrix}17\\19\\21\end{pmatrix}, & \begin{pmatrix}23\\25\\27\end{pmatrix}, & \begin{pmatrix}29\\31\\33\end{pmatrix}, & \begin{pmatrix}35\\37\\39\end{pmatrix}, & \begin{pmatrix}41\\43\\45\end{pmatrix}, & \begin{pmatrix}47\\49\\51\end{pmatrix}, & \cdots
\end{array} ,
$$

es bilden sich 3 Zeilen, wobei jede eine Rekursion befolgt - σ ist der Spaltenindex;

$$
\text{(II)} \quad \begin{array}{l}
n_5 = 5 + 6\sigma \equiv -1_{(mod\,6)}; \sigma \in \mathbb{N}_0; 5-Strang \\
n_7 = 7 + 6\sigma \equiv 1_{(mod\,6)}; \quad \sigma \in \mathbb{N}_0; 7-Strang \\
n_9 = 9 + 6\sigma \equiv 3_{(mod\,6)}; \quad \sigma \in \mathbb{N}_0; 9-Strang
\end{array}
$$

Im 9-Strang stehen nur nicht prime Zahlen, die den Faktor 3 abspalten, im 5- und 7-Strang auch Primzahlen, für die

$$
\text{(III)} \quad n_{(5,7)}^2 - 1 \equiv 0_{(mod\,24)} \equiv 0_{(24)}
$$

gilt; Gorgui-Naguib, Dlay[2] haben dies für Primzahlen gezeigt, aber auch die nicht primen Elemente besitzen diese Eigenschaft, wie in [1] gezeigt.

---

*Erich Landhäußer, Hünensand 45; 49716 Meppen; E-Mail: alandhae@gmx.de

(B) Ein „schneller Eratosthenes“

Aus den Äquivalenzen

$$-1_{(6)}\cdot -1_{(6)} \equiv 1_{(6)};\ -1_{(6)}\cdot 1_{(6)} \equiv -1_{(6)};\ 1_{(6)}\cdot 1_{(6)} \equiv 1_{(6)}$$

folgert man:

(1) $\begin{cases} n_5 \cdot n_7 \text{ liegt im 5-Strang,} \\ n_5 \cdot n'_5\, und\, n_7 \cdot n'_7 \text{ liegen im 7-Strang,} \end{cases}$ woraus divisionsfrei sämtliche Primzahlen in den

beiden Strängen stehen bleiben, wenn die nichtprimen Elemente (1) gestrichen werden:

(2.1) : $1_{(6)}\cdot 1_{(6)} \equiv -1_{(6)}$

$$\left.\begin{array}{cccc} 5\cdot 7=35, & 5\cdot 13 & 5\cdot 19, & \cdots, \\ 11\cdot 7=77, & 11\cdot 13, & 11\cdot 19 & \cdots, \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \\ 35\cdot 7=245, & 35\cdot 13, & 35\cdot 19, & \cdots, \end{array}\right\} \in \text{5-Strang, nicht prime Elemente}$$

35 ist offenbar die kleinste nicht prime Zahl im 5-Strang.Es bleiben die Primzahlen

$5,, 11, 17, 23, 29, 41, 47\cdots$ zurück.

(2.2): $-1_{(6)}\cdot -1_{(6)} \equiv 1_{(6)}$

$$\left.\begin{array}{ccccc} 5\cdot 5=25, & 5\cdot 11 & 5\cdot 17, & 5\cdot 23, & \cdots \\ -, & 11\cdot 11, & 11\cdot 17, & 11\cdot 23 & \cdots \\ -, & -, & 17\cdot 17, & 17\cdot 23, & \cdots \\ -, & -, & -, & 23\cdot 23, & \cdots \end{array}\right\} \in \text{7-Strang, nicht prime Elemente}$$

25 ist die kleinste nicht prime Zahl, es folgen zwanglos die primen Elemente

$7, 13, 19, 31, 37, 43. 61, 67, \cdots$

(2.3) $1_{(6)}\cdot 1_{(6)} \equiv 1_{(6)}$

$$\left.\begin{array}{ccccc} 7\cdot 7=49, & 7\cdot 13 & 7\cdot 19, & 7\cdot 25, & \cdots \\ -, & 13\cdot 13, & 13\cdot 19, & 13\cdot 25 & \cdots \\ -, & -, & 19\cdot 19, & 19\cdot 25, & \cdots \\ -, & -, & -, & 25\cdot 25, & \cdots \end{array}\right\} \in \text{7-Strang,nicht prime Elemente}$$

Es ergeben sich dieselben Primzahlen, allerdings mit anderen nicht primen Elementen als in (2.2). Mittels der Möbius-Funktion kann man die Anzahl von Primzahlen unterhalb einer Grenze bestimmen, nicht aber ihre eigentlichen Werte, vgl. Bundschuh [3].

(C) Numerische Beschreibung des „schnellen Eratosthenes“

Die Rekursionsformeln (II) erlauben eine Untersuchung der nicht primen Zahlen in den beiden Strängen; was zu nicht linearen diophantischen Gleichungen führt: Findet man Lösungen, so ist die Zahl nicht prim, im anderen Fall liegt eine Primzahl vor. Landhäußer [1], [4].

(3.1) $n_5 \cdot n'_7 = 5+6\sigma_0 = (5+6\sigma_5)\cdot(7+6\sigma_7) = 35+42\sigma_5+30\sigma_7+36\sigma_5\sigma_7 \Rightarrow$

(3.2) $\sigma_0 = 5+7\sigma_5+5\sigma_7+6\sigma_5\cdot\sigma_7; \quad \sigma_{5,}\sigma_7 \in \mathbb{N}_0$, 5-Strang

(4.1) $n_7 \cdot n'_7 = 7+6\overset{*}{\sigma_0} = (5+6\sigma_5)\cdot(5+6\tilde{\sigma}_5) = 25+30\sigma_5+30\tilde{\sigma}_5+36\sigma_5\tilde{\sigma}_5 \Rightarrow$

(4.2) $\overset{*}{\sigma_0} = 3+5(\sigma_5+\tilde{\sigma}_5)+6\sigma_5\cdot\tilde{\sigma}_5; \quad \sigma_{5,}\tilde{\sigma}_5 \in \mathbb{N}_0$, 7-Strang

(5.1) $\bar{n}_7 \cdot \bar{n}'_7 = 7+6\bar{\sigma}_7 = (7+6\sigma_7)\cdot(7+6\tilde{\sigma}_7) = 49+42\sigma_7+42\tilde{\sigma}_7+36\sigma_7\cdot\tilde{\sigma}_7 \Rightarrow$

(5.2) $\bar{\sigma}_7 = 7+7\cdot(\sigma_7+\tilde{\sigma}_7)+6\sigma_7\cdot\tilde{\sigma}_7; \quad \sigma_{7,}\tilde{\sigma}_7 \in \mathbb{N}_0$, 7-Strang

Es resultieren drei nicht lineare diophantische Gleichungen für die jeweiligen Spaltenindizes

$\sigma_{0,}\overset{*}{\sigma_0}, \bar{\sigma}_0$ mit den unbekannten $\sigma_{5,}\tilde{\sigma}_{5,}\sigma_{7,}\tilde{\sigma}_7$.

Findet man Lösungen $(\sigma_{5,}\tilde{\sigma}_5), (\sigma_{5,}\sigma_7), (\sigma_{7,}\tilde{\sigma}_7)$ für die betreffende Spalte, dann sind beide Elemente nicht prim. [1].

Aus der Primzahlmenge und der Menge der zusammengesetzten Zahlen ermitteln sich die Strukturen der Spalten,wenn man Zahlenpaare,die sich um 2 unterscheiden – sie besitzen den gleichen Spaltenindex σ_0 - zusammensetzt: $\begin{pmatrix}5\\7\end{pmatrix}, \begin{pmatrix}17\\19\end{pmatrix}$ - Zwillinge - und gemischte Spalten

$\begin{pmatrix}35\\37\end{pmatrix},\begin{pmatrix}23\\25\end{pmatrix}$ oder „leere“ Spalten $\begin{pmatrix}119\\121\end{pmatrix},\begin{pmatrix}185\\187\end{pmatrix}$.

Bemerkung: Im 7-Strang finden sich die Quadrate und die Mersenne-Strukturen [4].

Literaturverzeichnis

[1]: Erich Landhäußer, Dreiklassenteilung der Menge der ungeraden Zahlen http://www.primzahlen.de/referenten/Erich_Landhaeusser/Dreiklassenteilung_der_Menge_der_ungeraden_Zahlen.pdf, 2011

[2]: Raouf N. Gorgui-Naguib and Satnam S. Dlay, Properties of the Euler Totient Function Modulo 24 and Some of Its Cryptographic Implications , Advances in Cryptology — EUROCRYPT ’88 Lecture Notes in Computer Science, 1988, Volume 330/1988, 267-274

[3]: Peter Bundschuh: Einführung in die Zahlentheorie, 1991, Seite 45, Seite 289

[4]: Erich Landhäußer, Test für Mersenne-Strukturen http://www.primzahlen.de/referenten/Erich_Landhaeusser/Test _fuer_Mersenne-Strukturen.pdf, 2011