Dreiklassenteilung der Menge der ungeraden Zahlen

von

Erich Landhäußer*

(A) Einleitung und Zusammenfassung

Die Grundmenge G = {5, 7, 9, 11, 13, 15, …} wird als Tripel geschrieben und diese in Spalten angeordnet; es entstehen Stränge von links nach rechts gelesen:

$$\begin{pmatrix}5\\7\\9\end{pmatrix};\begin{pmatrix}11\\13\\15\end{pmatrix};\begin{pmatrix}17\\19\\21\end{pmatrix};\begin{pmatrix}23\\25\\27\end{pmatrix};\begin{pmatrix}29\\31\\33\end{pmatrix};\begin{pmatrix}35\\37\\39\end{pmatrix};\cdots$$

wobei sich die Rekursionsformeln

(1.1) $n_5=5+6\sigma_5\equiv -1(6)$

(1.2) $n_7=7+6\sigma_7\equiv +1(6)$

(1.3) $n_9=9+6\sigma_9\equiv +3(6)$

ablesen lassen, alle $\sigma=0,1,2,3,\cdots$ sind unabhängig voneinander. Im 9- Strang stehen alle durch 3 teilbaren Elemente der Grundmenge, während im 5- und 7-Strang Primzahlen und nicht Primzahlen stehen, mit der gemeinsamen Eigenschaft, dass $n_{5,}n_7$ die Äquivalenz $n^2\equiv 1_{(24)}$ befolgen. Raouf N. Gorgui-Naguib und Satman S. Dlay[1] haben dies für Primzahlen bewiesen; nichtprime Zahlen werden hier mit einbezogen, etwa gilt für

$n_5^2-1=(n_5-1)\cdot(n_5+1)=12\cdot(2+3\sigma_5)\cdot(1+\sigma_5)\equiv 0_{(24)}, \sigma_5\in\mathbb{N}$, da genau eine Klammer den Faktor 2 abspaltet, während für den 9-Strang

$n_9^2-1=(n_9-1)\cdot(n_9+1)=4(4+3\sigma_9)\cdot(5+3\sigma_9) \not\equiv 0$ resultiert; keine der beiden Klammern gibt den Faktor 3 ab.

Für die Zahlen im 5- bzw. 7-Strang werden nicht lineare diophantische Gleichungen gefunden

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

ebenso für Mersenne-Strukturen $2^p-1, p$ Primzahl.

(B) Klasseneinteilung der Grundmenge G, Beziehungen zwischen den Strängen

Es folgt aus (1.1), (1.2):

$$5,11,17,23,29,35,41,47,53,\cdots\equiv -1_{(6)}$$
$$7,13,19,25,31,37,43,49,55,\cdots\equiv +1_{(6)}$$

wobei die untereinander stehenden Zahlen jeweils aus dem gleichen σ folgen. Die multiplikative Verknüpfung der beiden Stränge ergibt:

(2.1)

$$n'_7=(5+6\sigma_5)\cdot(5+6\tilde{\sigma}_5)=25+30\sigma_5+30\tilde{\sigma}_5+36\sigma_5\tilde{\sigma}_5=7+6\cdot(3+5\sigma_5+5\tilde{\sigma}_5+6\sigma_5\tilde{\sigma}_5)\equiv 1_{(6)}\in 7-Strang.$$

Man schreibt $25=7+6\cdot 3$, d.h. das Produkt zweier Zahlen aus dem 5-Strang ergibt ein Element aus dem 7-Strang, da $-1_{(6)}\cdot -1_{(6)}\equiv +1_{(6)}$.

Ebenso findet man für 2 Zahlen aus dem 7-Strang:

(2.2)

$$n''_7=(7+6\sigma_7)\cdot(7+6\tilde{\sigma}_7)=49+42\sigma_7+42\tilde{\sigma}_7+36\sigma_7\tilde{\sigma}_7=7+6\cdot(7+7\sigma_7+7\tilde{\sigma}_7+6\sigma_7\tilde{\sigma}_7)\equiv 1_{(6)}\in 7-Strang$$

mit $49=7+6\cdot 7$ und für je einen Faktor aus 5- und 7-Strang:

(2.3)

$$n'_5=(7+6\sigma_7)\cdot(5+6\sigma_5)=35+30\sigma_7+42\cdot\sigma_5+36\sigma_5\cdot\sigma_7=5+6\cdot(5+5\sigma_7+7\sigma_5+6\sigma_5\sigma_7)\equiv -1_{(6)}\in 5-Strang$$

Additive Verknüpfungen lassen sich ebenfalls einfach realisieren, etwa $1_{(6)}+(-1_{(6)})\equiv 0_{(6)}$, woraus sich Beziehungen zwischen Primzahlen ergeben.

Folgerungen aus (2.1) – (2.3):

(a) Die Verknüpfungen sind kommutativ und assoziativ bzgl. Multiplikation

(b) Quadrate $x^2, x^4, x^6\cdots$ treten nur im 7-Strang auf;

(c) aber $x^3, x^5, x^7,\cdots: (-1_{(6)})^3\equiv(-1_{(6)})^5\equiv -1_{(6)}\in 5-Strang$

(d) nicht prime Zahlen im 7-Strang sind Zweierprodukte aus 5-Strang oder 7-Strang

(e) 2^p-1 p, Primzahl, prim oder nicht prim stehen im 7-Strang.

Beweis: $2^p-1=7+6\sigma\Rightarrow 2^3\cdot(2^{p-3}-1)=2^3\cdot(2^{\frac{p-3}{2}}-1)\cdot(2^{\frac{p-3}{2}}+1)=6\sigma\Rightarrow\sigma\in\mathbb{N}$, da eine Klammer durch 3 teilbar ist. q.e.d.

(f) nicht prime Zahlen im 5-Strang sind Zweierprodukte aus 5-Strang und 7-Strang.

Numerisch sind (2.1)-(2.3) leicht handhabbar, da die linken Seiten ab- und die rechten Seiten zunehmen:

$$n'_7=7+6\cdot\sigma_0=7+6\cdot(3+5\sigma_5+5\tilde{\sigma}_5+6\sigma_5\cdot\tilde{\sigma}_5)\Rightarrow$$

(3.1) $\sigma_0-3-5\sigma_5=\tilde{\sigma}_5\cdot(5+6\sigma_5);\quad 5+6\sigma_5$ prim

und analog

(3.2) $\sigma_0-7-7\sigma_7=\tilde{\sigma}_7\cdot(7+6\cdot\sigma_7);\quad 7+6\sigma_7$ prim

sowie für nicht prime Elemente aus dem 5_Strang:

(3.3) oder $\begin{cases}\sigma_0-5-5\sigma_7=\sigma_5\cdot(7+6\cdot\sigma_7); & 7+6\sigma_7\ prim\\ \sigma_0-5-7\sigma_5=\sigma_7\cdot(5+6\sigma_5); & 5+6\sigma_5\ prim\end{cases}$,

$\sigma_{5,}\sigma_7$ sind freie diskrete Parameter, die Primzahlen $(5+6\sigma_5)$ bzw. $(7+6\sigma_7)$ aufbauen. Finden sich keine ganzzahligen Lösungen für den anderen Partner, dann liegt eine Primzahl vor, andernfalls erfolgt eine Faktorisierung.

Beispiel: $n_7=187=7+6\cdot 30\equiv 1_{(6)}$, 7-Strang; $\sigma_0=30$

Es müssen (3.1) und (3.2) herangezogen werden:

(3.1): $27-5\cdot\sigma_5=\tilde{\sigma}_5\cdot(5+6\sigma_5);$

σ_5:	0,	1,	2,	3,	4,	$\cdots$
$(5+6\sigma_5)$:	5,	11,	17,	23,	29,	$\cdots$
$\tilde{\sigma}_5$:	$-$,	2,	1,	$-$,	$-$,	$\cdots$

Es resultiert das Produkt $(5+6\cdot 1)\cdot(5+6\cdot 1)=11\cdot 17$, beide Faktoren kommen aus dem 5-Strang. (3.2) wird keine Lösung ergeben. Der Test bricht ab, wenn die linken Seiten von

(3.1) – (3.3) negativ werden.

Beispiel: $2^{11}-1=25+30\sigma_5+30\tilde{\sigma}_5+36\sigma_5\cdot\tilde{\sigma}_5$

$$\Rightarrow\frac{2^{10}-13}{3}-5\sigma_5=\tilde{\sigma}_5(5+6\sigma_5)\quad\text{nach (2.1)}\quad\Rightarrow$$

$$337-5\sigma_5=\tilde{\sigma}_5(5+6\sigma_5);(\sigma_5=3;\tilde{\sigma}_5=14)\Rightarrow(23\cdot89)=2^{11}-1\quad.$$

(C) Mersenne-Strukturen, p prim

Der Primzahl-Test für 2^p-1 kann wie oben (2.1), (2.2) durchgeführt werden. Mersenne-Strukturen sind gründlich erforscht, insbesondere sind die Strukturen der Teiler von zusammengesetzten Mersenne-Zahlen bekannt. Speziell für Mersenne-Zahlen lässt sich eine diophantische Gleichung (5) herleiten, die auf (mod 8)-Regime aufbaut. Das Verfahren ist nicht divisionsfrei – im Gegensatz zu (2.1)-(2.3), wo nur durch 3 dividiert wird, muss mittels des „kleinen Fermat“ jeweils durch den Exponenten p dividiert werden.

Zunächst ist wohlbekannt:

(a) $M=2^p-1\equiv-1_{(8)};\ p$ Primzahl

(b) Teiler $t=1+2\mathrm{p}n\equiv-1_{(8)},\ t$ prim, $n\in\mathbb{N}_u$

(c) Teiler $\tilde{t}=1+8\mathrm{p}\tilde{n}\equiv1_{(8)};\tilde{n}\in\mathbb{N};\ p$ Primzahl

(d) $pn\equiv-1_{(8)}$ oder $\equiv3_{(8)}$

(e)
$$\tilde{t}-t=2\ p(4\tilde{n}-n)=6\cdot(\tilde{\sigma}-\sigma)\Rightarrow$$
$$\frac{|4\tilde{n}-n|}{3}=\frac{|\tilde{\sigma}-\sigma|}{p}\quad.$$

Aus (4b;c) ergibt sich speziell für $(x=pn;\ y=4\mathrm{p}\tilde{n})$

$$2^p-1=t\cdot\tilde{t}=(1+2\mathrm{x})\cdot(1+2\mathrm{y})=1+2\mathrm{x}+2\mathrm{y}+4\mathrm{xy}\Rightarrow$$
$$2^{p-1}-1=x+y+2\mathrm{xy}\Rightarrow$$
$$2^{p-1}-1-x=y(1+2\mathrm{x});\ x=pn\equiv-1_{(8)}\,oder\equiv3_{(8)};\ 1+2\mathrm{x}=1+2\mathrm{p}n\equiv-1_{(8)},\ prim$$

und weiter die nichtlineare diophantische Gleichung für die unbekannten $\tilde{n},n$:

(5) $\frac{2^{p-1}-(1+pn)}{p\cdot 4}=\tilde{n}\cdot(1+2\mathrm{pn});\quad 1+2\mathrm{pn}$ Primzahl

n ist der diskrete freie Parameter; resultiert $\tilde{n}\in\mathbb{N}$, dann ist 2^p-1 nicht prim.

Beispiel: Mit p=11 folgt aus (5)

$2^{10}-\frac{(1+11\cdot n)}{44}=\tilde{n}\cdot 23;$ offenbar ist der numerische Aufwand wesentlich größer,als bei

der Anwendung von (2.1), (2.2) , wo nur Division durch 3 auftritt.

Literaturverzeichnis

[1]: 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