Test für Mersenne-Strukturen $M=2^p-1$, p ist prim

von

Erich Landhäußer*

(A) Einleitung und Zusammenfassung:

Die Grundmenge $G=\{5,7,9,\cdots\}$ kann in 3 Klassen zerfällt werden, wenn G in Tripel zerteilt und etwa in Spalten geschrieben wird:

.(1) $\begin{matrix}\begin{pmatrix}5\\7\\9\end{pmatrix};\begin{pmatrix}11\\13\\15\end{pmatrix};\begin{pmatrix}17\\19\\21\end{pmatrix};\begin{pmatrix}23\\25\\27\end{pmatrix};\begin{pmatrix}29\\31\\33\end{pmatrix};\begin{pmatrix}35\\37\\39\end{pmatrix};\cdots\end{matrix}\begin{matrix}5-Strang\\7-Strang\\9-Strang\end{matrix}$,

wobei

(2.1) $n_5=5+6\sigma_5\equiv -1_{(mod\,6)}=-1_{(6)}$

(2.2) $n_7=7+6\sigma_7\equiv 1_{(mod\,6)}=+1_{(6)};\quad \sigma_{5,}\sigma_{7,}\sigma_9\in\mathbb{N}_0$

(2.3) $n_9=9+6\sigma_9\equiv 3_{(mod\,6)}=3_{(6)}$

abgelesen werden kann.

Raouf N. Gorgui-Naguib und Satman S. Dlay[1] haben gezeigt, dass für Primzahlen die Äquivalenz

(3) $p^2-1\equiv 0_{(24)}$

zutrifft; der 9-Strang enthält somit nicht prime Elemente (durch 3 teilbar), der 5- und 7-Strang dagegen prime und nicht prime Zahlen. In einer früheren Arbeit[2] wurde gezeigt, dass sowohl für n_5 als auch für n_7 die Äquivalenz (3) gilt, gleichgültig ob prim oder nicht prim.

Die Menge G zerfällt also in 2 Klassen Primzahlen, 2 Klassen nicht primer Elemente, die aber nicht

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

durch 3 teilbar sind und die durch 3 teilbaren im 3-Strang. Das (modulo 24) Regime ergibt die 3 Hauptklassen (1) beschreiben durch (2.1) -(2.3).

Multipliziert man 2 Zahlen aus dem 5-Strang, dann steht das Produkt im 7-Strang: weiter:

(4) $1_{(6)} \cdot 1_{(6)} \equiv 1_{(6)}$; $-1_{(6)} \cdot 1_{(6)} \equiv -1_{(6)}$; $-1_{(6)} \cdot -1_{(6)} \equiv 1_{(6)}$.

(B) Anwendung auf Mersenne-Strukturen

Alle $2^p - 1$, p prim stehen im 7-Strang:

(5) $2^p - 1 = 7 + 6\sigma_0 \Rightarrow \frac{2^2 \cdot (2^{p-3} - 1)}{3} = \frac{2^2 \cdot (2^{\frac{p-3}{2}} - 1) \cdot (2^{\frac{p-3}{2}} + 1)}{3} = \sigma_0 \quad \in \mathbb{N}_g$.

Eine der beiden Klammern spaltet 3 ab, denn das Dreierprodukt $\left(2^{\frac{p-3}{2}} - 1\right) \cdot 2^{\frac{p-3}{2}} \cdot \left(2^{\frac{p-3}{3}} + 1\right)$ von

Zahlen in natürlicher Reihenfolge enthält genau eine durch 3 teilbare Zahl; auf $2^{\frac{p-3}{2}}$ trifft dieses

<u>nicht</u> zu, also wird einer der beiden Faktoren durch 3 teilbar sein, d.h. $\sigma_0 \in \mathbb{N}_g$.

Weiter findet man nach (4), dass alle Quadratzahlen im 7-Strang liegen, nicht aber $n^{3,} n^5$, wenn

$n \in 5 - Strang$ .ist.

Mit (4) resultiert für die drei möglichen Kombinationen:

$n_5 = 5 + 6\sigma_0 = (5 + 6\sigma_5) \cdot (7 + 6\sigma_7) = 35 + 42\sigma_5 + 30\sigma_7 + 36\sigma_5\sigma_5 \in 5 - Strang$

(6.1) $\Rightarrow \sigma_0 = 5 + 7\sigma_5 + 5\sigma_7 + 6\sigma_5 \cdot \sigma_{7,} \sigma_{0,} \sigma_{5,} \sigma_7 \in \mathbb{N}_0$ als Spaltenindizes

$n_7' = 7 + 6\sigma_0' = (5 + 6\sigma_5) \cdot (5 + 6\tilde{\sigma}_5) = 25 + 30\sigma_5 + 30\tilde{\sigma}_5 + 36\sigma_5 \cdot \sigma_7 \in 7 - Strang$

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

oder

$n_7'' = 7 + 6\sigma_0'' = (7 + 6\sigma_7) \cdot (7 + 6\tilde{\sigma}_7) = 49 + 42\sigma_7 + 42\tilde{\sigma}_7 + 36\sigma_7 \cdot \tilde{\sigma}_7$

(6.3) $\Rightarrow \sigma_0'' = 7 + 7\sigma_7 + 7\tilde{\sigma}_7 + 6\sigma_7 \cdot \tilde{\sigma}_7$.

Besitzen diese nichtlinearen diophantischen Gleichungen für die Spaltenindizes Lösungen aus

$\mathbb{N}_0$, dann ist 2^p-1 nicht prim.

Im (modulo 8) Regime haben die Teiler die Struktur

(7.1) $t=1+2\text{pn}\equiv -1_{(8)};\quad pn\equiv -1_{(8)};\quad$ oder $\equiv 3_{(8)}; n\in\mathbb{N}_u$

(7.2) $\tilde{t}=1+8\,p\tilde{n}\equiv 1_{(8)};\quad \tilde{n}\in\mathbb{N}$,

während im (modulo 24)-System

(8.1) $t=5+6\sigma_5, \tilde{t}=5+6\tilde{\sigma}_5$ bzw.

(8.2) $t=7+6\sigma_7; \tilde{t}=7+6\tilde{\sigma}_7$

geschrieben werden kann, so dass für die Differenzen ($t<\tilde{t}$)

(9.1) $\tilde{t}-t=2\,p\cdot(4\,\tilde{n}-n)=\begin{cases}6\cdot(\tilde{\sigma}_5-\sigma_5)\\ 6\cdot(\tilde{\sigma}_7-\sigma_7)\end{cases}$ bzw.

steht. Setzt man

(9.2) $\delta_5=\tilde{\sigma}_5-\sigma_6>\tilde{0}$ bzw. $\delta_7=\tilde{\sigma}_7-\sigma_7>0$

dann resultiert aus (9.1)

(10) $\frac{4\tilde{n}-n}{3}=\frac{\tilde{\sigma}_5-\sigma_5}{p}=\frac{\delta_5}{p}$ bzw. $\frac{\tilde{\sigma}_7-\sigma_7}{p}=\frac{\delta_7}{p}$.

Aus (5), (6.2) bzw. aus (5), (6.3) folgen die Testreihen

(11.1) $\sigma_0-3=2\cdot\sigma_5\cdot(5+3\sigma_5)+\delta_5(5+6\sigma_5), \sigma_5 0,1,2,\cdots$

oder

(11.2) $\sigma_0-7=2\cdot\sigma_7\cdot(7+3\sigma_7)+\delta_7(7+6\sigma_7), \sigma_7 0,1,2,\cdots$.

Da $\sigma_0\in\mathbb{N}_g$, folgt aus (11) in jedem Falle, dass $\delta_5, \delta_7\in\mathbb{N}_u$ sind und zusätzlich Mehrfache von p

(11.3) $\delta=p, 3\text{p}, 5\text{p}\cdots$,

was eine erhebliche Verkürzung der Untersuchung bewirkt.

Dieser Algorithmus bestimmt das kleinste σ durch „Gleichziehen“ mit den konstanten linken Seiten von (11).

Beispiel: $2^{23}-1$: Nach (5) ist $\sigma_0=1398100$ und mit (8.1)

(12.1) $\sigma_0-3=1398097=2\sigma_5\cdot(5+3\sigma_5)+\delta_5\cdot(5+6\sigma_5)$

(12.2) $\sigma_0-7=1398093=2\sigma_7\cdot(7+3\sigma_7)+\delta_7\cdot(7+6\sigma_7)$

mit dem diskreten freien Parameter $\delta_5=23,69,\cdots$:

σ_5: 0, 1, 2, 3, 4, 5, 6,
δ_5: −, −, −, −, −, −, 29739, Ende

Bemerkungen: (a) $\sigma_5=0$ in (12.1) eingesetzt wird durch kein $\delta_5=23,29,\cdots$ erfüllt;

$(\sigma_5=7;\ \delta_5=29739=23\cdot1239)$ wird (12.1) gerecht und der kleinste Teiler von $2^{23}-1$ lautet $t=5+6\cdot7=47$.

(b) Eine Alternative zum divisionsfreien Algorithmus ist die quadratische Gleichung in σ , dann tritt aber δ in der Diskriminante auf.

(c) Gleichung (12.2) muss nicht zum Test herangezogen werden.

Danksagung: Andreas Landhäußer danke ich für wertvolle Quellenhinweise.

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

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