Zur Teilbarkeit von Mersenne Strukturen

von

Erich Landhäußer*

Einleitung:

Mersenne-Strukturen 2^p-1 - p eine Primzahl - werden auf Teilbarkeit untersucht. Es werden Parameter (n,σ) in mögliche Teiler eingeführt; finden sich keine ganzzahligen Lösungen für (n,σ), dann liegt eine Mersenne Primzahl vor. Die Verwendung dieser Parameter führt gleichzeitig zu einer numerischen Verkleinerung von 2^p-1 .

(a) Voraussetzungen:

Es werden die Mersenne-Strukturen

$$2^p-1\equiv -1_{(mod\,8)};\ p\equiv\begin{pmatrix}+1,+3\\-1,-3\end{pmatrix}_{(mod\,8)},\ p\ Primzahl\ ,$$

auf Teilbarkeit untersucht, die Struktur der Teiler ist

(V1) $t=(1+2pn)\equiv -1_{(mod8)}$ Primzahl,

(V2) $T=(1+8p\sigma)\equiv 1_{(mod\,8)}$ nicht notwendig Primzahl -

und es werden für (n,σ) -Folgen angegeben. Die Beziehung zwischen n,σ folgt aus

(V3) $t\cdot T=2^p-1\equiv -1_{(mod\,8)}$ ==> $4\sigma\cdot t+n=\dfrac{2^{p-1}-1}{p};$

gibt man z. B. $p=11\equiv 3_{(mod\,8)}$ vor, so folgt aus (V1); $n\equiv 1_{(mod\,8)};n:1,9,17,\cdots$; aus (V2): $\sigma\in\mathbb{N}$; es resultiert so für $p\equiv(\pm 1,\pm 3)_{(mod\,8)}$ das Schema:

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

(V4)

p / n	$-3_{(mod\,8)}$	$-1_{(mod\,8)}$	$1_{(mod\,8)}$	$3_{(mod\,8)}$
$-3_{(mod\,8)}$	-	+	-	+
$-1_{(mod\,8)}$	+	-	+	-
$1_{(mod\,8)}$	-	+	-	+
$3_{(mod\,8)}$	+	-	+	-

Wählt man $p=11\equiv 3_{(mod\,8)}$, dann resultieren zwei Stränge für n: $n\equiv 1_{(mod\,8)}$ oder $n\equiv -3_{(mod\,8)}$ mit jeweils $\sigma\in\mathbb{N}$.

(a) Reduktion von 2^p-1

Aus (V3) ergibt sich mit (V1) und (V2) : $t\cdot T=2^p-1$ ==>

$$4\sigma\cdot(1+2\,p\,n)+n=\frac{2^{p-1}-1}{p}\equiv\frac{-1}{p}(mod\,8) \quad .$$

Für $p=11\equiv 3_{(mod\,8)}$ resultiert: $4\sigma\cdot(1+2pn)+n=93\equiv -3_{(mod\,8)}$; mit $n=1$ ergibt sich $\sigma\cdot(23)=23$ also $\sigma=1$.

Probe: $T=89\,;t=23\,;2^{11}-1=2047\equiv -1_{(mod\,8)}$ also eine beachtliche Reduktion von $2^{11}-1\rightarrow 93$.

Der zweite Strang mit $n\equiv -3_{(mod\,8)};5,13,21,\cdots$ liefert kein $\sigma\in\mathbb{N}$.

(b) Beispiel:

$p=17\equiv 1_{(mod\,8)}\,;n\equiv -1_{(mod\,8)}:7,15,23,\cdots;\sigma:2,4,6,\cdots$.

Aus (V3) folgt: $4\sigma\cdot(1+34n)+n=\frac{2^{16}-1}{7}=3855\equiv -1_{(mod\,8)}$;

als Äquivalenz geschrieben:

$4\sigma\cdot(-1_{(mod\,8)})-1_{(mod8)}\equiv-1_{(mod\,8)}$ ==> $4\sigma_{(mod\,8)}\equiv 0_{(mod\,8)}$ ==> $\sigma: 2,4,6,\cdots$

wie oben.

Die vorübergehende Schreibweise als Äquivalenz ergibt oft eine genauere Darstellung von σ . Gleichung (V3) wird nicht durch (n,σ) erfüllt; nach wenigen Schritten wird

$t>\frac{3855-n}{4}$. Hier zeigt sich das hohe Selektionspotential von t als Primzahl.

Der zweite Strang $p=17\equiv 1_{(mod\,8)}; n\equiv 3_{(mod\,8)}$, aber $\sigma: 1,3,5,\cdots$ erfüllt ebenfalls nicht (V3).

Für einige p - sie müssen nicht einmal Primzahlen sein - kann die BSW89 Conjecture[1]als sehr schnelle Alternative gewählt werden:

(V5) Treffen 2 Voraussetzungen zu, so ist die 3. ebenfalls erfüllt.

(1) Für $p=2^k\pm 1$ oder $p=4^k\pm 3$, (p muss keine Primzahl sein, $k=1,2,3,\cdots$)

(2) 2^p-1 eine Mersenne Primzahl, wenn

(3) $\frac{2^p+1}{3}$ eine Primzahl ist. $p=13$ gehört zu (1); $\frac{2^{13}+1}{3}$ ist Primzahl!

Mittels (V1) gelingt es, 2^p-1 erheblich zu reduzieren:

$t=1+2\,p\,n\equiv 0_{(mod\,t)}$

(V6) $-1\equiv 2\,p\,n_{(mod\,t)}$

oder

$pn_{(mod\,t)}\equiv-(1+pn)=-2^{\mu}\cdot\delta_0;\quad \delta_0=\frac{1+pn}{2^{\mu}}\in\mathbb{N}$

(V7) In 2^p-1 eingesetzt ergibt sich mit (V6) die reduzierte Äquivalenzenfolge

(V8)

$$2^p-1\equiv 0_{(mod\,t)};(2^{p-1}+pn)\equiv 0_{(mod\,t)};(2^{p-2}-(pn)^2)\equiv 0_{(mod\,t)};(2^{p-3}+(pn)^3)\equiv 0_{(mod\,t)}\ \cdots$$

bzw. aus (V7):

(V9)
$$\begin{aligned} 2^p-1&\equiv(2^{p-1}-2^{\mu}\cdot\delta_0)_{(mod\,t)}=2^{\mu}\cdot(2^{p-1-\mu}-\delta_0)\equiv 0_{(mod\,t)};\\ 2^{2\mu}(2^{p-2-2\mu}-\delta_0^2)_{(mod\,t)}&\equiv 2^{3\mu}\cdot(2^{p-3-3\mu}-\delta_0^3)_{(mod\,t)}\\ &\cdots \end{aligned}$$

Man findet die Folge

$$(2^p-1)\equiv 0_{(mod\,t)};(2^{p-1-\mu}-\delta_0)\equiv 0_{(mod\,t)};(2^{p-2-2\mu}-\delta_0^2)\equiv 0_{(mod\,t)};(2^{p-3-3\mu}-\delta_0^3)\equiv 0_{(mod\,t)};\cdots$$

Mit $p=11;t=23=1+2\cdot 11$ ==> $pn=11;\delta=pn+1=12=2^2\cdot 3$ d.h. $\mu=2;\delta_0=3$

resultiert

$$(2^{11}-1)\equiv 0_{(mod\,23)};(2^8-3)\equiv 0_{(mod\,23)};(2^5-3^2)\equiv 0_{(mod\,23)};\cdots$$

bzw.

$$(2^{11}-1)\equiv 0_{(mod\,23)};(2^{10}+11)\equiv 0_{(mod\,23)};(2^9-11^2)\equiv 0_{(mod\,23)};\cdots$$ mit starken Reduzierungen.

Literaturverzeichnis

[1] [BSW89] P.T. Bateman, J.L. Selfridge, S.S. Wagstaff, Jr. The new Mersenne Conjecture, *Amer. Math. Monthly*, 96: 125-128, 1989