Modulo $\hat{T}$ - Transformationen von Mersenne-Strukturen auf 3. binomische Gleichungen

von

Erich Landhäußer*

Zusammenfassung

Es wird die Teilbarkeit von Mersenne-Zahlen $\hat{M}=2^p-1$, p Primzahl, durch einen Primzahlteiler $\hat{T}=1+2\ p\cdot n\equiv -1_{(mod\ 8)}$ untersucht. Ziel ist die Verkleinerung des Zahlenwertes von $\hat{M}$ mittels Transformation modulo $\hat{T}$. Dies kann durch Überführung in das Binom $U^2-V^2\equiv 0_{(mod\ \hat{T})}$ oder Parameterdarstellung über eine diophantische Gleichung erfolgen. Auch die Anwendung des Satzes von Euler $\frac{2^{\frac{p-1}{2}}\pm 1}{p}\equiv 0_{(mod\ p)}$ führt zu leicht ausführbaren Tests mit zutreffend gewähltem freien Parameter n in $\hat{T}=1+2\ p\cdot n\equiv -1_{(mod\ 8)}$, p und $\hat{T}$ jeweils Primzahlen.

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

Zur Teilbarkeit von Mersenne-Zahlen, Transformation auf 3. binomische Gleichungen

Die Mersenne-Zahl $\hat{M}=2^p-1\equiv -1_{(mod\ 8)}$, p Primzahl, wird in zwei Schritten numerisch reduziert:

(1) Modulo $\hat{T}=1+2\ p\cdot n\equiv -1_{(mod\ 8)}$, $\hat{T}$ Primzahl, wird $\hat{M}$ auf ein 3.Binom transformiert und

(2) dann wird jeder der beiden Faktoren nochmals verkleinert.

Vorraussetzungen: Es werden die Mersenne-Zahlen $\hat{M}=2^p-1$, p Primzahl auf Teilbarkeit bezüglich einer vorgegebenen Primzahl $\hat{T}=1+2\ p\cdot n\equiv -1_{(mod\ 8)}$ untersucht.

(V1) $\hat{T}=1+\begin{Bmatrix}2\ p_1\cdot n_3\\ 2\ p_3\cdot n_1\end{Bmatrix}\equiv -1_{(mod\ 8)}$; $\begin{cases}p_1\equiv 1_{(mod\ 4)};n_3\equiv 3_{(mod\ 4)}\\ p_3\equiv 3_{(mod\ 4)};n_1\equiv 1_{(mod\ 4)}\end{cases}$

Es folgt aus (V1) mit den Kürzeln

(V2) $\Delta:=-p_{1/3}\cdot n_{3/1}\equiv 1_{(mod\ 8)}$ bzw. $\equiv -3_{(mod\ 8)}$

und

$\delta:=1+p_{1/3}\cdot n_{3/1}\equiv 0_{(mod\ 8)}$ bzw. $\equiv 4_{(mod\ 8)}$

$\Rightarrow \delta+\Delta=1$.

Weiter folgt aus $\hat{T}=1+2\ p_{1/3}\cdot n_{3/1}$;

(V3) $2\cdot\Delta\equiv 1_{(mod\ \hat{T})}$; $2\cdot\delta\equiv 1_{(mod\ \hat{T})}$

(V4) $-\Delta+\delta=\hat{T}\equiv 0_{(mod\ \hat{T})}$

Indizes werden weggelassen!

Ziel der Untersuchung ist die Transformation modulo $\hat{T}$ von $\hat{M}=2^p-1$ in ein 3. Binom, um die Division durch $\hat{T}$ zu vereinfachen.

Da $\hat{T}$ Primzahl ist, muss $\hat{M}\mp\hat{T}\equiv 0_{(mod\ \hat{T})}$ sein;

(V5) $\hat{M} \mp \hat{T} = \begin{cases} 2^p - 2 - 2 \cdot p\, n = 2 \cdot (2^{p-1} - \delta) \equiv 0_{(mod\ \hat{T})} \;;\delta > 0 \\ 2^p + 2\mathrm{p}\, n = 2 \cdot (2^{p-1} - \Delta) \equiv 0_{(mod\ \hat{T})} \;;-\Delta > 0. \end{cases}$

Gelingt es nun[1)]

(V6) $\delta \equiv \frac{x^2}{y^2} (mod\ \hat{T})\,;\, x \in \mathbb{N}_g\,,\, y \in \mathbb{N}_u$

bzw.

$$\Delta \equiv \frac{X^2}{Y^2} (mod\ \hat{T})\,;\, X \in \mathbb{N}_u\,, Y \in \mathbb{N}_u$$

zu lösen, dann entstehen 3. Binome. Die Bedingungen für $x\,, y\,; X\,, Y$ werden unten hergeleitet (A1), wobei die Äquivalenzen (V3), (V4) eine entscheidende Rolle spielen. Es ist dann

(V7) $2^{p-1} \cdot y^2 - x^2 = (2^{\frac{p-1}{2}} \cdot y - x) \cdot (2^{\frac{p-1}{2}} \cdot y + x) \equiv 0_{(mod\ \hat{T})}$

bzw.

$$2^{p-1} \cdot Y^2 - X^2 = (2^{\frac{p-1}{2}} \cdot Y - X) \cdot (2^{\frac{p-1}{2}} \cdot Y + X) \equiv 0_{(mod\ \hat{T})} \quad .$$

Ausführung: Es wird gesetzt mit (V3):

(A1) $x^2 := \delta + h = \delta + h \cdot 1 \equiv \delta \cdot (1 + 2\mathrm{h}) = \delta \cdot y^2_{(mod\ \hat{T})}\,; h \in \mathbb{N}_0$

$X^2 := \Delta + H = \Delta + H \cdot 1 \equiv \Delta \cdot (1 + 2\mathrm{H}) = \Delta \cdot Y^2_{(mod\ \hat{T})}\,; H \in \mathbb{N}_0$

y^2, Y^2 sind jeweils ungerade Quadrate $\equiv 1_{(mod\ 8)}$.

Da $(-\Delta) \in \mathbb{N}_u, \delta \in \mathbb{N}_g$ nach V2 ist, folgt

---

1) Die Äquivalenzen V(6) sind Modulo $\hat{T}$ lösbar, denn $x^2 \equiv \delta\, y^2_{(mod\ \hat{T})} \quad \Leftrightarrow$

$y^2 \equiv 2 \cdot x^2_{(mod\ \hat{T})}$, sodass $y^2 \equiv c_{(mod\ \hat{T})}$ geschrieben werden kann. Definitionsgemäß ist c quadratischer Rest Modulo $\hat{T}$ mit der Bedingung (notwendig und hinreichend)

$c^{\frac{\hat{T}-1}{(2,\hat{T}-1)}} \equiv 1_{(mod\ \hat{T})} \equiv c^{\frac{2\mathrm{pn}}{(2,2\,pn)}} = (2\mathrm{x}^2)^{pn} = 2^{pn} \cdot x^{2\mathrm{pn}} = 2^{\frac{\hat{T}-1}{2}} \cdot x^{\hat{T}-1} \equiv 1_{(mod\ \hat{T})}$, da $\hat{T} \equiv -1_{(mod\ 8)}$ ist.

[1] S. 124

$x^2 \in \mathbb{N}_g^2$ bzw. $X^2 \in \mathbb{N}_u^2 ; Y^2 \in \mathbb{N}_u^2$

wie unter (V6) behauptet.

Mittels (A1) lässt sich $\hat{M}$ in ein 3. Binom transformieren. Die diophantische Gleichung $x^2 = \delta + h$ geht mit $y^2 = 1 + 2$ h in

$$2x^2 = y^2 + \hat{T} \equiv 0_{(mod\,8)} \Rightarrow x^2 \equiv 0_{(mod\,4)} \in \mathbb{N}_g^2$$

nach dem Divisionssatz und entsprechend

(A2) $X^2 = \Delta + H$ folgt

$$2X^2 = Y^2 - \hat{T} \equiv 2_{(mod\,8)} \Rightarrow X^2 \equiv 1_{(mod\,4)} \in \mathbb{N}_u^2 \ .$$

Beide Gleichungen lassen sich als pythagoräische Tripel schreiben: $A^2 + B^2 = C^2$

etwa
$$Y^2 = \hat{T} + 2X^2 \Rightarrow Y^2 = 1 + 2\,p \cdot n + 2\,X^2 \Rightarrow Y^2 = 1 + 2(p \cdot n + X^2)$$
$$\Rightarrow Y^2 + (p \cdot n + X^2)^2 = (p \cdot n + X^2 + 1)^2 \ .$$

Durch Einsetzen von y^2 bzw. $Y^2 = 1, 9, 25, \ldots$ in (A2) ergeben sich zwei Klassen von Lösungen (x^2, y^2) bzw. (X^2, Y^2) .

Beispiel: $\hat{M} = 2^{29} - 1 \equiv 0_{(mod\,1103)}$ soll gezeigt werden:

$p_1 = 29$; $n_3 = 19$; $\delta = 1 + p_1 \cdot n_3 = 552$; $\Delta = -p_1 \cdot p_3 = -551$;

$\hat{T} = 1 + 2\,p_1 n_3 = 1103$.

Man findet aus (A2):

(a) $(2\,4^2 ; 7^2) ; (5\,8^2 ; 7\,5^2)$

$$\delta \equiv \left(\frac{24}{7}\right)^2_{(mod\,1103)} \quad ; \quad \delta \equiv \left(\frac{58}{75}\right)^2_{(mod\,1103)}$$

(b) $(17^2 ; 41^2) ; (31^2 ; 55^2) ; (781^2 ; 1105^2) \Leftrightarrow (781^2 ; 2^2)$

$$\delta \equiv \Delta \equiv \left(\frac{17}{41}\right)^2_{(mod\,1103)} \equiv \left(\frac{31}{55}\right)^2_{(mod\,1103)} \equiv \left(\frac{781}{1105}\right)^2_{(mod\,1103)} \equiv \left(\frac{781}{2}\right)^2_{(mod\,1103)}$$

Nach (V4) ist nämlich $-\Delta + \delta = \hat{T} \equiv 0_{(mod\,\hat{T})}$

Ein zweiter Lösungsweg[2] resultiert aus einer Parameterdarstellung der beiden diophantischen Gleichungen in (A2), der zugleich divisions- und radizierungsfrei ist:

$$\begin{aligned} 2x^2 = y^2 + \hat{T} &\Leftrightarrow y^2 = \hat{T} - 2t \\ x^2 &= \hat{T} - t\,; \qquad t \in \mathbb{Z}\,;\ y^2 \in \mathbb{N}_u^2\,;\ x^2 \in \mathbb{N}_g^2 \\ 2X^2 = Y^2 - \hat{T} &\Leftrightarrow Y^2 = -\hat{T} - 2\xi \\ X^2 &= -\hat{T} - \xi\,; \qquad \xi \in \mathbb{Z}\,;\ Y^2 \in \mathbb{N}_u^2\,;\ X^2 \in \mathbb{N}_u^2 \end{aligned}$$

Es ergeben sich leicht errechenbare Listen für t und ξ und übereinstimmende t_j bzw. ξ_j bringen die Paare (x^2, y^2, t_j) bzw. (X^2, Y^2, ξ_j) .

Aus (V7) folgt aus dem Binom $2^{\frac{p-1}{2}} \cdot y \pm x \equiv 0_{(mod\,\hat{T})}$, dass $2^{\frac{p-1}{2}} \cdot y + x \equiv 0$ bzw. $2^{\frac{p-1}{2}} \cdot y - x \equiv 0$ sein muss.

Mittels (V3) lassen sich die beiden Faktoren weiter reduzieren; es ist nach (V2):

$$2\delta = \begin{cases} 2^4 \cdot \mu \equiv 1_{(mod\,\hat{T})}\,; wenn\ \delta \equiv 0_{(mod\,8)} \\ 2^3 \cdot \rho \equiv 1_{(mod\,\hat{T})}, wenn\ \delta \equiv 0_{(mod\,4)} \end{cases} .$$

Denkt man sich z.B. in $2^{\frac{p-1}{2}} \cdot y \pm x \cdot 1 \equiv 0_{(mod\,\hat{T})}$, dann schreibt sich das Binom $2^{4 \cdot j}(2^{\frac{p-1}{2} - 4 \cdot j} \cdot y \pm \mu^j \cdot x)$ bzw. $2^{3 \cdot j}(2^{\frac{p-1}{2} - 3 \cdot j} \cdot y \pm \rho^j \cdot x) \equiv 0_{(mod\,\hat{T})}$ mit $j \in \mathbb{N}$, wobei j so gewählt wird, dass die Faktoren kleiner werden.

[2] [1] S. 31

Beispiel: $2^{43}-1\equiv 0_{(mod\,431)}$

Aus $2x^2=y^2+\hat{T}$ resultiert $x^2=16^2\,;\,y^2=9^2$

$p=43$; $n_1=5$; $\delta=1+p_3n_1=216\equiv 0_{(mod\,8)}$; $\Delta=-p_3n_1$; $\hat{T}=431=1+2p_3n_1$;

$j=2$; $\mu=27$

$2^{21-8}\cdot 9\pm 27\cdot 16\Rightarrow 2^9 \underset{-}{(+)} 3^4\equiv 0_{(mod\,431)}$; es gilt das Minuszeichen!

Nachtrag

(a) Für $x^2\in \mathbb{N}_g^2$ war $2^{p-1}-\delta=2^{p-1}-(\delta+\xi)+\xi\equiv 0_{(mod\,\hat{T})}$.; $\xi\in\mathbb{N}_g$

Es wird

(N1) $\delta+\xi=x^2$

gesetzt, so dass

$2^{p-1}-x^2+\xi\equiv 0_{(mod\,\hat{T})}$

und

(N2) $2\xi+1=y^2\in\mathbb{N}_u^2$

ist. Dann muss

(N3) $2^{p-1}+\xi\equiv 2^{p-1}\cdot y^2_{(mod\,\hat{T})}$

sein, damit V(7) entsteht; ξ muss so gewählt werden, dass (N1) und (N2) gelten. Für ξ ergibt sich (N4); $2\xi+1=(2n+1)^2=y^2$ als Bedingung für ξ :

(N5) $\xi=2n(n+1)$, d.h. nur solche $\xi=2\cdot n\cdot(n+1)$ sind zulässig, damit (N1), (N2) gelten;

es ist dann

$2^{p-1}-x^2+\xi\equiv 2^{p-1}\cdot y^2-x^2=2^{p-1}\cdot(2\xi+1)-(\delta+\xi)=(2^p-1)\xi+2^{p-1}-\delta\equiv 0_{(mod\,\hat{T})}$.

Ist $\hat{T}$ ein Teiler, dann verschwindet der 1. Summand und es verbleibt

$2^{p-1}-\delta\equiv 0_{(mod\,\hat{T})}$

Beispiel: $p=29$; $\hat{T}=1103=1+2\cdot 551$; $\delta=1+551=552$. Das nächste gerade Quadrat ist $x^2=576$; $y^2=2\xi+1=7^2$; es wird $\delta\equiv\left(\frac{24}{7}\right)^2_{(mod\,1103)}$.

Wählt man $x=26$, dann ist $\xi=124=2\cdot 2\cdot 31$; d.h. $x=26$ erfüllt nicht die

(N2). Erst bei $x=58$ findet sich ein ξ , das (N5) erfüllt.

(b) Für $x^2 \in \mathbb{N}_u^2$ war $2^{p-1}-\Delta \equiv 0_{(mod\,\hat{T})}$; $\Delta = -pn$; da nach (V4) $\Delta \equiv \delta_{(mod\,\hat{T})}$ ist , läuft der analoge Beweis mit $\xi = 2n(n+1) > (-\Delta)$; $2^{p-1}-(\Delta+\xi)+\xi \equiv 0_{(mod\,\hat{T})}$ mit $\xi = 2n(n+1) > (-\Delta)$;

Beispiel: $\Delta = -551$; $2^{(p-1)}-(-551+840)+840 \equiv 0_{(mod\ 1103)}$ mit

$$\xi = 840 = 2 \cdot 20 \cdot 21 \ ; \ \Rightarrow X = 17 \ ; \ Y = 41 \ ; \ \delta \equiv \Delta \equiv \left(\frac{17}{41}\right)^2_{(mod\ 1103)}$$

Die erste Äquivalenz in (V5) lässt sich alternativ

(N6) $2 \cdot p \cdot \left(\frac{2^{p-1}-1}{p} - n\right) \equiv 0_{(mod\,\hat{T})}$; $\hat{T} \equiv -1_{(mod\ 8)}$, p Primzahl

schreiben und da

$p \mid 2^{\frac{p-1}{2}}+1$, wenn $p \equiv \pm 3_{(mod\ 8)}$

und

$p \mid 2^{\frac{p-1}{2}}-1$, wenn $p \equiv \pm 1_{(mod\ 8)}$ ist,

wird aus (N6)

(N7) $\left[\left(2^{\frac{p-1}{2}}-1\right)A - n\right] \equiv 0_{(mod\,\hat{T})}; A = \frac{2^{\frac{p-1}{2}}+1}{p}; p \equiv \pm 3_{(mod\,8)};$

(N8) $\left[\left(2^{\frac{p-1}{2}}+1\right)B - n\right] \equiv 0_{(mod\,\hat{T})}; B = \frac{2^{\frac{p-1}{2}}-1}{p}; p \equiv \pm 1_{(mod\,8)};$

resultieren. Fordert man $n \equiv A\mu_{(mod\,\hat{T})}$ bzw. $n \equiv B\overline{\mu}_{(mod\,\hat{T})}$, dann folgen aus (N7) die Äquivalenzen

(N9) $2^{\frac{p-1}{2}}-1-\mu \equiv 0_{(mod\,\hat{T})}$ und $n \equiv A\mu_{(mod\,\hat{T})}$

und aus (N8)

(N10) $2^{\frac{p-1}{2}}-1-\overline{\mu} \equiv 0_{(mod\,\hat{T})}$ und $n \equiv B\overline{\mu}_{(mod\,\hat{T})}$.

Beide Paare sind bei vorgegebenem p , A , B , sofort lösbar , sodass n als Parameter auftritt, und 2^p-1 auf alle $\hat{T} \equiv -1_{(mod\,8)}$ bei $p = const.$ geprüft

werden kann..

Beispiel: $2^{29}-1;\hat{T}=1103;p\equiv-3_{(mod\,8)};n\equiv+3_{(mod\,8)}$ da

$p=29;n=19;A=565;\quad 2^{14}-1-\mu\equiv 0_{(mod\,\hat{T})}$ und $19\equiv 565_{(mod\,\hat{T})};$ beide Äquivalenzen sind modulo 1103 erfüllt.

Wählt man dagegen $n\equiv 27\equiv 3_{(mod\,8)};\ p=29\Rightarrow\hat{t}=1567\equiv-1_{(mod\,8)}$ dann liefert (N9) einen Widerspruch.

Die Größen A, B müssen offensichtlich nur einmal bestimmt werden, n als freier Parameter und nur solche n, die eine Primzahl $\hat{t}\equiv-1_{(mod\,8)}$ erzeugen.

Literaturverzeichnis

[1] Peter Bundschuh, Einführung in die Zahlentheorie, 4. Auflage – 1991, Verlag: Springer Berlin

[2] Loc. Cit. S. 31