Algorithmen zwischen Mersenne-Primzahlexponenten

von

Erich Landhäußer*

(I) Einleitung und Zusammenfassung

Zur Zeit sind 47 Primzahlen p bekannt,die als Exponent in 2^p-1 wieder eine Primzahl erzeugen: $2,3,5,7,13,17,19,31,\cdots$, die Zahlen 2 und 3 werden weggelassen, und die restlichen 45 werden in dieser Arbeit auf Strukturen untersucht,die zum Teil Algorithmen darstellen.

Die Menge $G=5,7,9,11,13,15,\cdots$ lässt sich in 3 Klassen zerlegen, Landhäußer, [1], deren Elemente durch die Basisgleichungen

$$(A)\quad \begin{array}{ll} x^{(5)}=5+6\sigma=5,11,17,23,35,41,\cdots & 5-Strang, (x^{(5)})^2\equiv +1_{(mod\,24)} \\ x^{(7)}=7+6\sigma=7,13,19,25,31,43,\cdots & 7-Strang, (x^{(7)})^2\equiv +1_{(mod\,24)} \\ x^{(9)}=9+6\sigma=9,15,21,27,33,39,\cdots & 9-Strang, (x^{(9)})^2\not\equiv +1_{(mod\,24)} \end{array}$$

gegeben sind, wobei $\sigma=0,1,2,3,\cdots$ als Parameter auftritt; 5- und 7-Strang enthalten keine durch 3 teilbaren Zahlen, sind teilerfremd und bestehen jeweils aus Primzahlen und zusammen gesetzten Zahlen, die hier nicht interessieren, Naguib, Dlay, [2]

$$(B)\quad \begin{array}{l} p^{(5)}=5,11,17,23,29,41,47,53,59,71,\cdots \\ p^{(7)}=7,13,19,31,37,43,61,67,73,79,\cdots \end{array}$$

Die Primzahlen in (B) werden als bekannt vorausgesetzt, Euler, [3].Weisstein, [4]

(II) Mersenne-Primes: 2^p-1 ist prim und p nach (C) ist ebenfalls prim

Es interessieren nur die Exponenten p für die 2^p-1 Primzahl bleibt.Zur Zeit sind 47 solcher Primzahlen bekannt; mit (A) sind das 22 aus dem 5-Strang und 23 aus dem 7-Strang, wenn die

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

Primzahlen 2 und 3 weggelassen werden:

(C)

5, 17, 89, 107, 521, 4.253, 9.689, 9.941, 11.213, 19.937, 21.701, 86.243, 756.839, 859.433, 1.398.269, 2.976.221, 3.021.377, 6.972.593, 25.964.951, 32.582.657, 37.156.667, 43.112.609

bzw.

7, 13, 19, 31, 61, 127, 607, 1.279, 2.203, 2.281, 3.217, 4.423, 23.209, 44.497, 110.503, 132.049, 216.091, 1.257.787, 13.466.917, 20.996.011, 24.036.583, 30.402.457, 42.643.801.

(III) Erzeugende Funktionen für die Stränge (C), Sequenzen

Basierend auf (A) kann man erzeugende Funktionen definieren; die entstehenden Teilmengen werden hier Sequenzen genannt, mit den Startprimzahlen $p_0 : 5, 17, 107, 756.839$; $p_{(n)}^{(p_0)} = p_0 + 24n$

(D)

$p_{(n)}^{(5)} = 5 + 24n$: 5, 4.253, 9.941, 11.213, 27.701, 1.398.269, 2.976.221 aus 5-Sequenz, 7 Elemente;

$p_{(n)}^{(17)} = 17 + 24n$: 17, 89, 521, 9.689, 19.937, 859.433, 3.021.377, 6.972.593, 32.589.657, 43.112.609 aus 17-Sequenz, 10 Elemente;

$p_{(n)}^{(107)} = 107 + 24n$: 107, 86.243, 37.156, 667.107 aus 107-Sequenz, 3-Elemente;

$p_{(n)}^{(756.839)} = 756.839 + 24n$: 756.839, 25.964.951 aus 756.839-Sequenz, 2 Elemente;

Der 5-Strang zerfällt in vier Sequenzen,die erzeugenden Funktionen sind bijektiv mit den Startprimzahlen p_0 $5, 17, 107,$ und 756.839 ; das lineare n im Gegensatz zu den Euler Erzeugenden Funktionen Euler, [3] lässt Erweiterungen zu; keine Primzahl im 5-Strang wird ausgelassen und alle p_n bleiben in der jeweiligen Sequenz; in (C) sind die Startprimzahlen für den 5- und 7-Stränge gekennzeichnet (jeweils 4 Stück). Die entstehenden Primzahlpaaresummen haben die Struktur $p + p' = 24 \cdot (\mu), \mu \in \mathbb{N}$ und bei Übereinstimmung von $24(\mu)$ resultieren Quadrupel von Primzahlen etwa $5 + 19 = 24 \cdot (1) = 17 + 7$.

Der 7-Strang zerfällt ebenfalls in vier Sequenzen mit den Startprimzahlen

$p_0 : 7, 13, 19, 2281 : p_{(n)}^{(p_0)} = p_0 + 24n$ wird analog zum 5-Strang:

$p_{(n)}^{(7)}$: 7, 31, 127, 607, 1.279, 4.423, 110.503,
24.036.583; 7-Sequenz, 8 Elemente

(E) $p_{(n)}^{(13)}$: 13, 61, 13.466.917; 13-Sequenz, 3 Elemente

$p_{(n)}^{(19)}$: 19, 2203, 216.091, 1.257.787, 20.996.011; 19-Sequenz, 5 Elemente

$p_{(n)}^{(2281)}$: 2.281, 3.217, 23.209, 44.497, 132.049,
30.402.457, 42.643.801; 2281-Sequenz, 7 Elemente

Man unterscheide streng zwischen Strang und Sequenzen (D) und (E). Die acht Sequenzen (D), (E) sind trivialerweise teilerfremd,aber addiert man z.B. die Elemente der 5-Sequenz zu denen der 19-Sequenz in beliebiger Reihenfolge, dann spaltet die Summe den Faktor 24 ab; dies gilt auch für die (17 – 7) Sequenzen, (107 – 13) Sequenz und die (756.839 – 2.281) Sequenz; der Beweis ist einfach. Der Algorithmus lässt sich auf Mehrfachsummen ausdehnen.

(IV) Zusammenfassung

Die Basisgleichungen (A) erzeugen aus der Grundmenge $5,7,9,11,\cdots$ zwei Klassen,deren Primzahlen in (C) aufgelistet sind und als bekannt vorausgesetzt werden; mittels der dualen Paare (5 – 19) , (17 – 7),(107 – 13), (756.839 – 2.281) lassen sich algorithmische Strukturen zwischen den primen Exponenten p in 2^p-1 aufbauen.

Man zeigt einfach, dass die Summe aus den α Primes p aus einer der Sequenzen (D) derselben Anzahl aus der zugehörigen dualen Sequenz (E) den Faktor 24 abgibt – darunter dürfen auch gleiche p sein:

(a) $(7+31+607)+(17+89+521)=24\cdot(53)$,
(b) $(31+31+607)+(17+89+521)=24\cdot(54)=2\cdot31+607+17+89+521$,
(c) $(607+607+607)+(89+89+521)=24\cdot(105)=3\cdot607+2\cdot89+521$
(d) The new Mersenne Conjecture [5] ist leider nicht durchgehend anwendbar.

(V) Literaturverzeichnis

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

[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] Leonhard Euler, Nouveaux Mémoires de l'Académie royale des Sciences. Berlin, p. 36, 1772.

[4] Weisstein, Eric W. "Prime-Generating Polynomial." From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/Prime-GeneratingPolynomial.html

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

[6] Table of Known Mersenne Primes http://primes.utm.edu/mersenne/index.html#known