UNIVERSITÄT KAISERSLAUTERN

EINE BEMERKUNG ÜBER PRIMZAHLEN DER FORM $2^{3n}a + 2^{2n}b + 2^{n}c + 1$

Andreas Guthmann

Preprint Nr. 219

FACHBEREICH MATHEMATIK

EINE BEMERKUNG ÜBER PRIMZAHLEN DER FORM

$$2^{3n}a + 2^{2n}b + 2^{n}c + 1$$

Andreas Guthmann

Preprint Nr. 219

UNIVERSITÄT KAISERSLAUTERN
Fachbereich Mathematik
Erwin–Schrödinger–Straße
6750 Kaiserslautern

Mai 1992

Eine Bemerkung über Primzahlen der Form

$$2^{3n}a + 2^{2n}b + 2^n c + 1$$

von Andreas Guthmann

Abstract. A Remark on Primes of the Form $2^{3n}a+2^{2n}b+2^nc+1$**.** Necessary and sufficient conditions for the numbers in the title to be prime are given. The tests are well suited for practical purposes.

Bekanntlich läßt sich ein Primzahltest für eine natürliche Zahl N dann leicht durchführen, wenn $N-1$ vollständig in Primfaktoren zerlegt ist [4, 5]. In diesem Fall kann man nämlich eine geeignete Umkehrung des Fermatschen Satzes anwenden: Ist $z \in \mathbf{N}$ mit $z^{N-1} \equiv 1 \bmod N$, aber $z^{(N-1)/p} \not\equiv 1 \bmod N$ für jeden Primteiler p von $N-1$, so ist N Primzahl.

Auch wenn $N-1$ nur teilweise faktorisiert ist, kann manchmal ein Primzahltest durchgeführt werden. Ist etwa $N-1 = F \cdot R$, wobei F der vollständig zerlegte Anteil von $N-1$ ist, so folgt aus einem Satz von Pocklington [2, 5], daß $F \geq \sqrt{N}$ ausreicht, um N auf Primzahleigenschaft zu testen. 1975 schließlich konnten Brillhart, Lehmer und Selfridge in einer fundamentalen Arbeit [2] zeigen, daß die Bedingung sogar zu $F \geq \sqrt[3]{N}$ abgeschwächt werden kann.

Ein bekanntes Beispiel für die Anwendung des Falles $F \geq \sqrt{N}$ ist der Satz von Proth [2, 5]. Hier ist $F = 2^n$ und $N = k \cdot 2^n + 1$ mit $0 < k < 2^n$. Ist $z \in \mathbf{N}$ mit $(\frac{z}{N}) = -1$, so ist N genau dann prim, wenn $z^{(N-1)/2} \equiv -1 \bmod N$ gilt.

In dieser Note verallgemeinern wir den Prothschen Test auf den Fall $F \geq \sqrt[3]{N}$. Wir stützen uns dabei auf die oben erwähnte Arbeit von Brillhart et al.[2]. Wir verwenden folgendes

Lemma: *Sei* $N = k \cdot 2^n + 1$ *mit* $n \in \mathbf{N}$ *und ungeradem* k. *Sei* $z \in \mathbf{N}$ *mit* $z^{(N-1)/2} \equiv -1 \bmod N$. *Außerdem sei* $m \in \mathbf{N}$ *mit* $N \not\equiv 0 \bmod \lambda 2^n + 1$ *für* $1 \leq \lambda \leq m-1$. *Man definiere* r, s *durch* $k = 2^{n+1}s + r, 1 \leq r < 2^{n+1}$. *Schließlich gelte*

$$N < (m2^n + 1)[2^{2n+1} + (r-m)2^n + 1]. \tag{1}$$

Dann gilt: Genau dann ist N *prim, wenn* $s = 0$ *oder* $r^2 - 8s$ *kein Quadrat ist.*

Man beachte, daß aus $z^{(N-1)/2} \equiv -1(N)$ sowohl $z^{N-1} \equiv 1(N)$ als auch $(z^{(N-1)/2} - 1, N) = 1$ folgt. Also sind (in den dortigen Bezeichnungen) die Bedingungen (I) des Satzes 5 von Brillhart et al. [2] erfüllt. Unser Lemma ist dann nur eine offenkundige Umformulierung dieses Satzes. Wir beweisen nun folgenden

Satz: *Sei* $N = 2^{3n}a + 2^{2n}b + 2^n c + 1$ *mit* $n \geq 2$, $a, b, c \in \mathbf{N}_0$ *und* $a \leq 4$, $b < 2^n$, $c < 2^n$. *Es seien außerdem die folgenden beiden Bedingungen erfüllt:*

1) $a - b + c \not\equiv 1 \bmod 2^n + 1$.

2) $a - 2b + 4c \not\equiv 8 \bmod 2^{n+1} + 1$.

Schließlich sei $z \in \mathbf{N}$ *mit* $z^{(N-1)/2} \equiv -1(N)$.

Genau dann ist N *prim, wenn*

g) $a = b = 0$ *oder* $c^2 - 2^{n+2}a - 4b$ *kein Quadrat ist, falls* b *gerade,*

u) $a = 0, b = 1$ *oder* $(2^n + c)^2 - 2^{n+2}a - 4(b-1)$ *kein Quadrat ist, falls* b *ungerade.*

Beweis: Zunächst bemerken wir, daß die Bedingung (1) des Lemmas mit $m = 3$ erfüllt ist, denn es gilt

$$\begin{aligned}(3 \cdot 2^n + 1)(2^{2n+1} + (r-3)2^n + 1) &= 6 \cdot 2^{3n} + [3(r-3) + 2]2^{2n} + 2^n r + 1 \\ &\geq 5 \cdot 2^{3n} + 2^n + 1 > 5 \cdot 2^{3n} > N.\end{aligned}$$

Wegen $2^n \equiv -1 \bmod 2^n + 1$ folgt außerdem

$$N \equiv -a + b - c + 1 \not\equiv 0 \bmod 2^n + 1,$$

nach 1). Analog gilt

$$\begin{aligned}8N &= 2^{3(n+1)}a + 2^{2(n+1)} \cdot 2b + 2^{n+1} \cdot 4c + 8 \\ &\equiv -a + 2b - 4c + 8 \not\equiv 0 \bmod 2^{n+1} + 1,\end{aligned}$$

also auch $N \not\equiv 0 \bmod 2^{n+1}+1$. Damit ist $2^n\lambda + 1$ kein Teiler von N für $\lambda = 1, 2$.

Wir können also das Lemma anwenden und somit ist N genau dann prim, wenn $s = 0$ oder $r^2 - 8s$ kein Quadrat ist. In unserem Fall ist nun aber

$$r = c,\ s = 2^{n-1}a + \tfrac{b}{2} \text{ falls } b \text{ gerade},$$

bzw.

$$r = 2^n + c,\ s = 2^{n-1}a + \tfrac{b-1}{2} \text{ falls } b \text{ ungerade}.$$

Damit ist der Satz vollständig bewiesen.

Dieser Satz ist in der Tat eine weitgehende Verallgemeinerung des Prothschen Tests, den wir für $a = b = 0$ erhalten. Da aber über a und b noch verfügt werden kann, hat man eine große Auswahl für N. Der Test ist effektiv in dem Sinne, daß seine Laufzeit durch ein Polynom in n, d.h. durch ein Polynom in $\log N$ beschränkt ist, sobald man ein geeignetes z gefunden hat. In der Praxis ist das kein Problem wie wir gleich sehen werden. In den Anwendungen kann man etwa a, b, c festhalten und damit die Überprüfung der Bedingungen 1), 2), u) und g) erleichtern. Wir geben einige Beispiele dafür.

a) Sei $a = 0, b = 1, c = 2^n - 2$. Dann ist $N = 2^{2n+1} - 2^{n+1} + 1$ und Primzahlen dieser Form wurden von Brillhart et al. [1, 2, 3] untersucht. Offenbar sind 1) und 2) des Satzes erfüllt, falls $n \geq 3$ ist. Da die Bedingung u) immmer gilt, muß nur noch ein geeignetes z mit $z^{(N-1)/2} \equiv -1(N)$ gefunden werden. Für ungerades $n+1$ gilt

$$\left(\frac{3}{N}\right) = \left(\frac{N}{3}\right) = \left(\frac{2}{3}\right)^{n+1} = -1.$$

Aus dem Satz erhalten wir also: *Ist $n \geq 4$ gerade, so ist $N = 2^{2n-1} - 2^n + 1$ genau dann prim, wenn $3^{(N-1)/2} \equiv -1(N)$ ist.*

Ist n ungerade, so findet man in der Praxis ebenfalls mühelos ein geeignetes z.

b) Nun sei $a = 4, b = 17, c = 1$, also $N = 2^{3n+2} + 2^{2n+4} + 2^{2n} + 2^n + 1$. Wie man leicht sieht, sind 1) und 2) für $n \geq 4$ erfüllt. Um die Bedingung u) zu untersuchen, setzen wir

$$Q_n := (2^n + c)^2 - 2^{n+2}a - 4(b-1) = (2^n + 1)^2 - 2^{n+4} - 2^6.$$

Angenommen $Q_n = y^2$ für eine natürliche Zahl y. Es folgt mit $x = 2^n$

$$(x-7)^2 - y^2 = 112.$$

Diese Gleichung ist rasch gelöst für $x, y \in \mathbf{N}$. Da aber x eine Potenz von 2 sein muß gibt es keine Lösung, d.h. Q_n ist niemals ein Quadrat. Somit erhalten wir folgenden Primzahltest: *Ist* $N = 2^{3n+2} + 2^{2n+4} + 2^{2n} + 2^n + 1$ *mit* $n \geq 4$, *so ist* N *genau dann prim, wenn es* $z \in \mathbf{N}$ *gibt mit* $z^{(N-1)/2} \equiv -1(N)$.

Für gerades n kann man wieder $z = 3$ wählen. Man findet so, daß N prim ist für

$$n \in \{1, 3, 6, 9, 10, 11, 21, 33, 43, 55, 73\},$$

und keine weiteren für $n \leq 100$.

Diese Beispiele lassen sich natürlich beliebig vermehren.

Literatur

[1] Brillhart, J., Concerning the Numbers $2^{2p}+1$, p Prime, Math. Comp. **16**, 424-430(1962).

[2] Brillhart, J., Lehmer, D.H., Selfridge, J.L., New Primality Criteria and Factorizations of $2^m \pm 1$, Math. Comp. **29**, 620-647(1975).

[3] Brillhart, J., Selfridge, J.L., Some Factorizations of $2^n \pm 1$ and Related Results, Math. Comp. **21**, 87-96(1967).

[4] Lehmer. D.H., Tests for Primality by the Converse of Fermat's Theorem, Bull. Amer. Math. Soc. **33**, 327-340(1927).

[5] Riesel, H., Prime Numbers and Computer Methods for Factorization, Birkhäuser 1985.

Anschrift des Autors:

Andreas Guthmann

Fachbereich Mathematik

Universität Kaiserslautern

Pfaffenbergstr. 95

D-6750 Kaiserslautern