Sitzungsberichte

der

mathematisch-naturwissenschaftlichen Klasse

der

Bayerischen Akademie der Wissenschaften zu München

Jahrgang 1948

München 1949
Verlag der Bayerischen Akademie der Wissenschaften
In Kommission beim Biederstein Verlag München

Ein Beweis für die Primalität der Zahl $2^{31} - 1 = 2\,147\,483\,647$

Von Oskar Perron, in München

Vorgelegt am 4. Juni 1948

Wenn jemand von einer sehr großen Zahl n (mit 10, 20, 40 oder noch mehr Stellen) durch numerische Rechnung festgestellt hat, daß $3^{n-1} \not\equiv 1 \pmod{n}$ ist, so folgt daraus, daß n keine Primzahl ist. Aber diese Rechnung ist äußerst mühsam und erfordert mehrere Tage oder Wochen oder Monate Zeitaufwand, wobei man nie vor Rechenfehlern sicher ist. Jeder Nachprüfende muß genau so qualvoll rechnen und riskiert Rechenfehler; Sicherheit gewinnt man auf diese Art nicht. Wenn aber jemand eine Faktorzerlegung der Zahl n angibt, so hat er, um sie zu finden, vielleicht viele Jahre mit Versuchen zubringen müssen, aber das Resultat ist in kurzer Zeit (Minuten oder Stunden) nachprüfbar, und man hat Sicherheit.

Hat man für eine andere Zahl n durch numerisches Rechnen festgestellt, daß $3^{n-1} \equiv 1 \pmod{n}$ ist und daß für keinen echten Teiler d von $n-1$, die man zufällig alle kennt, die Kongruenz $3^d \equiv 1 \pmod{n}$ erfüllt ist, so ist damit gezeigt, daß n eine Primzahl ist. Die Nachprüfung der Rechnung ist wieder ebenso qualvoll und gibt keine Sicherheit. Ein Gegenstück zu dem zweiten Verfahren, bei dem die Nachprüfung so einfach ist, gibt es hier nicht.

Nach Kraitchik hat Lucas einmal die Aufgabe gestellt, die Primalität von $2^{31} - 1$ ohne Benutzung von Primzahltafeln zu beweisen, und Kraitchik glaubt, daß Lucas dabei wohl an die Methode der „Lucasschen Reihen" gedacht hat.[1] Diese Methode ist wohl nicht ganz so zeitraubend wie die oben beschriebene, aber sehr viel schneller geht es auch nicht, und die Gefahr der Rechenfehler ist ebenso groß. Nun ist die Zahl $2^{31} - 1$ zwar bloß zehnstellig, aber es gibt doch nur ganz wenig größere

[1] M. Kraitchik, Théorie des nombres, tome II (1926) S. 142.

Zahlen, die heute auf Grund von so mühsamen und unsicheren Rechnungen als Primzahl angesprochen werden; die größte ist $2^{127}-1$ (39-stellig). Aus diesen Gründen dürfte es vielleicht nicht überflüssig sein, wenn im folgenden ein Beweis für die Primalität von $2^{31}-1$ mitgeteilt wird, der keine Primzahltafel benutzt und von jedem, der mit den Elementen der Zahlentheorie vertraut ist, in einer halben Stunde nachgeprüft werden kann.

Es ist zu prüfen, ob $2^{31}-1$ einen Primteiler p hat, der kleiner als $\sqrt{2^{31}-1}$, also gewiß $< 2^{16} < 100000$ ist. Wegen $2^{31} \equiv 1 \pmod{p}$ ist 31 ein Teiler von $p-1$. Daher ist $p-1$ durch 31 und als gerade Zahl sogar durch 62 teilbar. Da somit gewiß $p \neq 3$ und $p \neq 29$ ist, folgt aus der Formel

$$46162^2 + 3 \cdot (3^4 \cdot 29)^2 = 2^{31} - 1,$$

deren Auffindung zeitraubend war[1], deren Nachprüfung aber höchstens 5 Minuten erfordert, daß -3 quadratischer Rest von p ist. Es ist also $\left(\frac{-3}{p}\right) = 1$, folglich nach dem Reziprozitätsgesetz $\left(\frac{p}{3}\right) = 1$, also $p-1$ auch durch 3 teilbar. Somit ist

$$p = 1 + 3 \cdot 62\, n = 1 + 186n, \tag{1}$$

und wegen $p < 100000$ ist gewiß

$$n < 1000. \tag{2}$$

Ferner ist $2 \cdot (2^{31}-1)$ durch p teilbar, also

$$2 \equiv 2^{32} = (2^{16})^2 \pmod{p}.$$

Daher ist 2 quadratischer Rest von p und folglich

$$p \equiv \pm 1 \pmod{8}.$$

In (1) muß daher

$$n \equiv 0 \text{ oder } 3 \pmod{4} \tag{3}$$

[1] Ich verdanke sie Herrn W. Patz. Über die Art der Auffindung vergleiche man dessen Arbeit: Über die Gleichung $X^2 - DY^2 = \pm c \cdot (z^3 - 1)$, wo c möglichst klein. Sitz. Ber. der Bayer. Akademie, Jahrg. 1947.

sein. Mit $2^{31} - 1$ ist nun auch die Zahl

$$2^{31} - 1 - p + 186(n - 33)p$$

durch p teilbar. Diese ist aber nach (1) gleich

$$2^{31} - 2 - 186n + 186(n - 33)(186n + 1) =$$
$$= 186^2 n^2 - 33 \cdot 186^2 n + 2^{31} - 2 - 186 \cdot 33,$$

also, da man in 3 bis 4 Minuten kontrolliert, daß

$$2^{31} - 2 - 186 \cdot 33 = 186^2 \cdot 62073$$

ist, auch durch 186^2 teilbar. Daher ist

$$\frac{n^2 - 33n + 62073}{1 + 186n} = a \tag{4}$$

eine ganze Zahl, und aus (3) entnimmt man sofort:

$$a \equiv 1 \pmod 4. \tag{5}$$

In einer halben Minute kontrolliert man, daß

$$62073 - 186 \cdot 333 = 155$$

ist, worauf sich aus (4) ergibt:

$$an - 333 = \frac{n^3 - 33n^2 + 155n - 333}{1 + 186n}. \tag{6}$$

Im Intervall $1 \leqq n \leqq 10$ kommen wegen (3) nur die Werte $n = 3, 4, 7, 8$ in Frage. Für diese lehrt aber ein Blick auf den Zähler in (6), daß er nicht durch den Nenner teilbar ist; also scheiden diese Werte aus, und wegen (2) sind nur noch die n des Intervalls

$$11 \leqq n \leqq 1000$$

zu prüfen. Nun kann die in (4) auftretende Funktion von n ihr Maximum nur am Anfang oder Ende des Intervalles haben (geometrisch stellt sie einen nach oben konkaven Hyperbelast dar). Für $n = 11$ ist ihr Wert

$$= \frac{121 - 363 + 62073}{2047} < \frac{62000}{2000} = 31;$$

für $n = 1000$ ist er

$$= \frac{1000000 - 33000 + 62073}{186001} < \frac{1800000}{180000} = 10.$$

Da der Zähler in (4) augenscheinlich definit, also $a > 0$ ist, ergibt sich also

(7) $$0 < a < 31.$$

Wenn man die Formel (4) nach n auflöst, muß, da n rational ist, unter der Quadratwurzel eine Quadratzahl A^2 kommen. Es ist also

$$(186a + 33)^2 - 4 \cdot (62073 - a) = A^2.$$

Hieraus folgt nach den Moduln 5 und 13:

(8) $$(a - 2)^2 + 4a - 2 \equiv 0, 1, 4 \pmod 5,$$

(9) $$(4a + 7)^2 - 4 \cdot (11 - a) \equiv 0, 1, 4, 9, 3, 12, 10 \pmod{13}.$$

Nach (8) ist $a^2 \equiv 3, 4, 2 \pmod 5$; da aber 3 und 2 keine quadratischen Reste von 5 sind, bleibt nur $a^2 \equiv 4$, also

(10) $$a \equiv \pm 2 \pmod 5$$

übrig. Zusammen mit (5) ergibt das

$$a \equiv 13, 17 \pmod{20}.$$

Wegen (7) kommen daher für a nur die beiden Werte 13, 17 in Frage. Diese genügen aber nicht der Kongruenz (9), so daß keine Möglichkeit mehr übrig bleibt.