Altes und Neues vom Logarithmus

Von M. Stifel bis zum Quantencomputer

Vortrag von **Otto Forster** am Mathematischen Institut der LMU München

am Tag der offenen Tür, 15. Januar 1999

Zusammenfassung

Der Logarithmus, entdeckt durch den spielerischen Vergleich von arithmetischen und geometrischen Reihen, erlaubt eine Zurückführung der Multiplikation auf die Addition. Er war deshalb lange Zeit ein wichtiges Hilfsmittel beim numerischen Rechnen. (Auch der Rechenschieber beruht ja auf dem Logarithmus.)

Man sollte glauben, dass heute im Computer-Zeitalter der Logarithmus keine Rolle mehr spielt. Das Gegenteil ist der Fall. Schon Gauß betrachtete eine Verallgemeinerung des Logarithmus auf endliche Körper von Primzahlordnung p, die dem Rechnen mit Kongruenzen modulo p zugrunde liegen. Für seine zahlentheoretischen Untersuchungen berechnete Gauß Tafeln des heute so genannten *diskreten Logarithmus* für alle Primzahlen kleiner als 100.

Für größere Primzahlen wird die Berechnung des diskreten Logarithmus immer schwieriger. Gerade diese Schwierigkeit ist es, die heute für kryptographische Verfahren (Diffie-Hellman, ElGamal) ausgenutzt wird, die zur Sicherung des elektronischen Datenverkehrs eingesetzt werden. Auch die besten Verfahren zur Berechnung des diskreten Logarithmus, von denen eines vorgestellt wird, scheitern bei Primzahlen der Länge von 1024 Bit (über 300 Dezimalstellen), wie sie heute typischerweise benutzt werden.

Bei der Suche nach immer schnelleren Rechnern stieß man auf die Idee des Quantencomputers, dem nicht mehr das traditionelle Modell der Turing-Maschine zugrunde liegt. Diese Theorie erhielt einen enormen Auftrieb durch die Entdeckung von schnellen Algorithmen für Quantencomputer zur Faktorisierung großer ganzer Zahlen und zur Berechnung des diskreten Logarithmus durch Peter Shor. Für diese Leistung wurde Shor auf dem Internationalen Mathematiker-Kongress 1998 in Berlin mit der Nevanlinna-Medaille ausgezeichnet. In dem Vortrag soll auch skizziert werden, wie man mit dem (heute noch hypothetischen) Quantencomputer den diskreten Logarithmus berechnen kann.