Zahlentheorie mit dem Interferenzcomputer

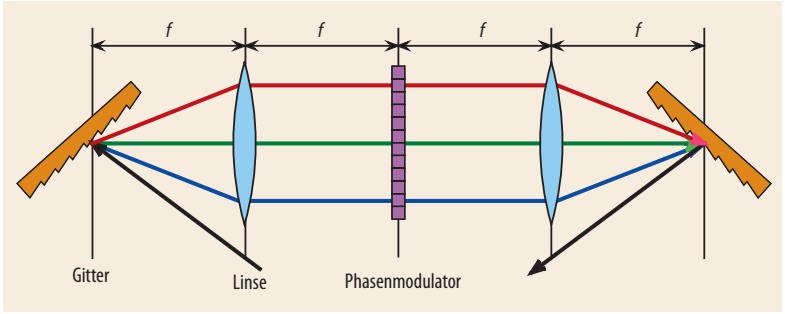
Eine Klasse neuer physikalischer Verfahren, die auf sog. Gauß-Summen beruhen, erlauben es, die Teiler von Zahlen zu bestimmen.

Die Zahlentheorie fasziniert Laien wie Experten gleichermaßen durch das enge Nebeneinander von scheinbar schwierigen Fragen mit einfachen Antworten und scheinbar einfachen, aber trotzdem ungelösten Problemen. Praktische Relevanz hat sie derzeit vor allem zur Verschlüsselung von Daten. Dabei hält sie auch für die Physik Überraschungen bereit: Ein berühmtes Beispiel sind äquivalente statistische Eigenschaften der Nullstellen der Riemannschen Zeta-Funktion und von Eigenwerten hermitischer Zufallsmatrizen, die in der Kernphysik Bedeutung haben. Ein viel älteres Beispiel, dessen Relevanz allerdings erst mit den hier vorgestellten Arbeiten voll erkannt wurde, ist der Talbot-Effekt. Seit Fraunhofer ist das Beugungsbild eines Gitters auf einem Schirm im Fernfeld wohl bekannt. 1836 untersuchte Talbot die Gitterbeugung für kleinere Abstände zwischen Gitter und Schirm, also Bedingungen, die sich nicht mit der Fernfeld-Näherung beschreiben lassen. Er entdeckte, dass in periodischen Abständen z_T auf dem Schirm ein scharfes Selbstabbild des Gitters erscheint und z_T mit der Wellenlänge des Lichtes λ und der Gitterkonstante a gemäß $z_T = a^2/\lambda$ zusammenhängt. Darüber hinaus gibt es bei allen rationalen Vielfachen $(N/\ell)\, z_T$ scharfe ℓ-fach überlagerte Bilder des Gitters (also mit Gitterkonstante a/ℓ), wenn N und ℓ teilerfremd sind [1, 2].

Zur Erklärung ist es hilfreich, Gauß-Summen einzuführen. Das sind Summen über Phasenfaktoren der Form

$$G(N,\ell) := \frac{1}{r}\sum_{m=0}^{r-1} \exp\,(2\pi i\, m^2\, \frac{N}{\ell}).$$

Sie spielen eine wichtige Rolle in der Zahlentheorie und dort insbesondere bei den verschiedensten Problemen im Zusammenhang mit Primzahlen. Aus der Definition der Gauß-Summe folgt schnell, dass $G = 1$ ist, wenn ℓ ein Teiler von N ist. Andernfalls geht G gegen 0 für $r \to \infty$. Gauß-Summen eignen sich also dazu, die Teilbarkeit von Zahlen zu testen. Übrigens ist dazu der Exponent von m nicht entscheidend. Er muss aber so gewählt sein, dass die Phasen hinreichend unregelmäßig werden, wenn ℓ kein Teiler von N ist. Das ist für m^2, also für Gauß-Summen, der Fall. Noch wichtiger im hier zu besprechenden Zusammenhang: Gauß-Summen lassen sich relativ einfach durch verschiedene physikalische Systeme verwirklichen.



Gauß-Summen lassen sich durch Interferenz darstellen, indem man beispielsweise einen Femtosekundenpuls spektral zerlegt und die einzelnen Farben mit einer Linse der Brennweite f auf eine programmierbare Flüssigkristallzeile fokussiert, die jeder spektralen Komponente die passende Phase aufprägt. Eine weitere Linse und ein weiters Gitter fügen die spektralen Anteile wieder zusammen.

Was haben Gauß-Summen, also *Summen* über quadratische Phasen, nun mit dem Talbot-Effekt zu tun? *Integrale* über quadratische Phasen sind von der Beugung an einer Kante oder an einem Spalt bekannt; die Cornu-Spirale stellt sie grafisch dar. Wenn man den Spalt durch ein Gitter mit sehr engen Sub-Spalten ersetzt, gehen diese Fresnel-Integrale in eine Gauß-Summe über. Für bestimmte Abstände des Schirms vom Gitter, die genau der Bedingung entsprechen, dass ℓ Teiler von N ist, entsteht konstruktive Interferenz und infolgedessen ein Bild des Gitters.

Wolfgang Schleich und Kollegen aus Ulm, Hannover und Toulouse haben nun eine ganze Klasse neuer Verfahren ersonnen, um Gauß-Summen durch physikalische Systeme darzustellen. Einige davon wurden kürzlich auch experimentell verwirklicht. Am eindruckvollsten lässt sich dies durch Verwendung der Gauß-Summen zur Überprüfung der Teilbarkeit einer Zahl demonstrieren. Eines der von Schleich et al. vorgestellten Verfahren ist die zeitliche Variante des Talbot-Effekts [3]. Dazu generiert man zu den Zeiten $\tau_m := mT$ ($T \approx 200$ fs) Femtosekundenpulse so, dass der m-te Puls die noch zu definierende Phase ϕ_m hat. Wenn man die Femtosekundenpulse näherungsweise mit δ-Funktionen ausdrückt, lässt sich das elektrische Feld des Lasers durch

$$E(t) = \sum_m e^{i\phi_m}\, e^{i\omega_L t}\, \delta(t - \tau_m) \qquad (1)$$

beschreiben. ω_L ist die Laserfrequenz. Der Grund für dieses Vorgehen sowie die geschickte Wahl der ϕ_m zeigt sich nach einer Fourier-Transformation von $E(t)$, die durch die Approximation der Pulsform durch δ-Funktionen leicht zu berechnen ist:

$$E(\Delta\omega) = \sum_m \exp[i(\phi_m + \tau_m \Delta\omega)] \qquad (2)$$

mit $\Delta\omega := \omega - \omega_L$. Wählt man nun $\phi_m \equiv -2\pi\, m^2\, N/\ell$, so ergibt sich für $\Delta\omega = 0$ bereits eine Gauß-Summe. Wie ist es nun möglich, einen Femtosekundenpuls in m Pulse zu teilen, sodass der Pulsabstand jeweils T ist und die Phasen ϕ_m? Die Antwort haben wir bereits gegeben: Man muss die spektrale Phase der Femtosekundenpulse gemäß Gl. (2) manipulieren. Phasenmanipulation ist für viele Anwendungen

ultrakurzer Pulse ein alltägliches Verfahren geworden, und Flüssigkristall-Arrays, die genauso wie ein Flachbildschirm funktionieren, erlauben es, die Phase sogar frei zu programmieren. Das ist hier auch erforderlich: Um zu überprüfen, ob N durch ℓ teilbar ist, muss für jedes ℓ der durch Gl. (2) definierte Phasenverlauf programmiert und danach die Intensität bei der Zentralwellenlänge ($\Delta\omega = 0$) gemessen werden. Maximale Intensität ist nur dann zu erwarten, wenn ℓ ein Teiler von N ist. Damit hat man einen Analogcomputer zur Division natürlicher Zahlen realisiert. Interessanterweise genügen schon sehr wenige Pulse m, um die Teilbarkeit zu überprüfen. Nach der Faktorisierung von fünfstelligen Zahlen [3] mit diesem Verfahren sind inzwischen erhebliche weitere Fortschritte erzielt worden.

Mithilfe prinzipiell ähnlicher Methoden, die allerdings auf NMR-Techniken beruhen, haben Xinhua Peng und Dieter Suter sogar 17-stellige Zahlen zerlegt [4]. Jedoch sind für die vollständige Faktorisierung von N immer alle Zahlen bis $\ell = \sqrt{N}$ zu testen. Damit wächst auch für dieses auf klassischer Physik beruhende Verfahren der Rechenaufwand mit der Größe der zu faktorisierenden Zahl exponentiell an.

Nun lässt sich aber bekanntlich die quantenmechanische Verschränkung ausnutzen, um Rechenoperationen massiv zu parallelisieren. Diese Tatsache liegt dem Quantencomputer zu Grunde. Im Falle der Faktorisierung bedeutet dies, alle in Frage kommenden möglichen Teiler gleichzeitig zu testen. Zu einer wirklich schnellen Primzahlzerlegung wären die von Schleich et al. vorgestellten Methoden also noch mit quantenmechanischer Verschränkung zu kombinieren. Einen guten Ansatz dazu bietet möglicherweise eine Variante des Verfahrens, die auf kalten Atomen in einer magnetooptischen Falle beruht [5]. Diese werden durch einen $\pi/2$-Puls zunächst polarisiert. Mit einer Serie von π-Pulsen geeigneter Phase prägt man dann Gauß-Summen auf und liest die Polarisation durch einen abschließenden $\pi/2$-Puls aus. Sollte sich ein Weg finden, Gauß-Summen mit verschränkten physikalischen Systemen darzustellen, so wären weitreichende Konsequenzen nicht nur für die wenigen Anwendungen der Zahlentheorie in der Kryptographie, sondern auch für ihr Verhältnis zur Physik zu erwarten.

Gernot Stania und Gerhard G. Paulus

[1] *H. F. Talbot*, Philos. Mag. **9**, 401 (1836)
[2] *M. V. Berry, I. Marzoli* und *W. P. Schleich*, Phys. World, Juni 2001, S. 39
[3] *D. Bigourd, B. Chatel, W. P. Schleich* und *B. Girard*, Phys. Rev. Lett. **100**, 030202 (2008)
[4] *X. Peng* und *D. Suter*, http://arXiv.org/abs/0803.3396
[5] *M. Gilowski, T. Wendrich, T. Müller, Ch. Jentsch, W. Ertmer, E. Rasel* und *W. P. Schleich*, Phys. Rev. Lett **100**, 030201 (2008)

Dr. Gernot Stania, MPI für Quantenoptik, 85748 Garching, und **Prof. Dr. Gerhard G. Paulus**, Institut für Optik und Quantenelektronik, 07743 Jena

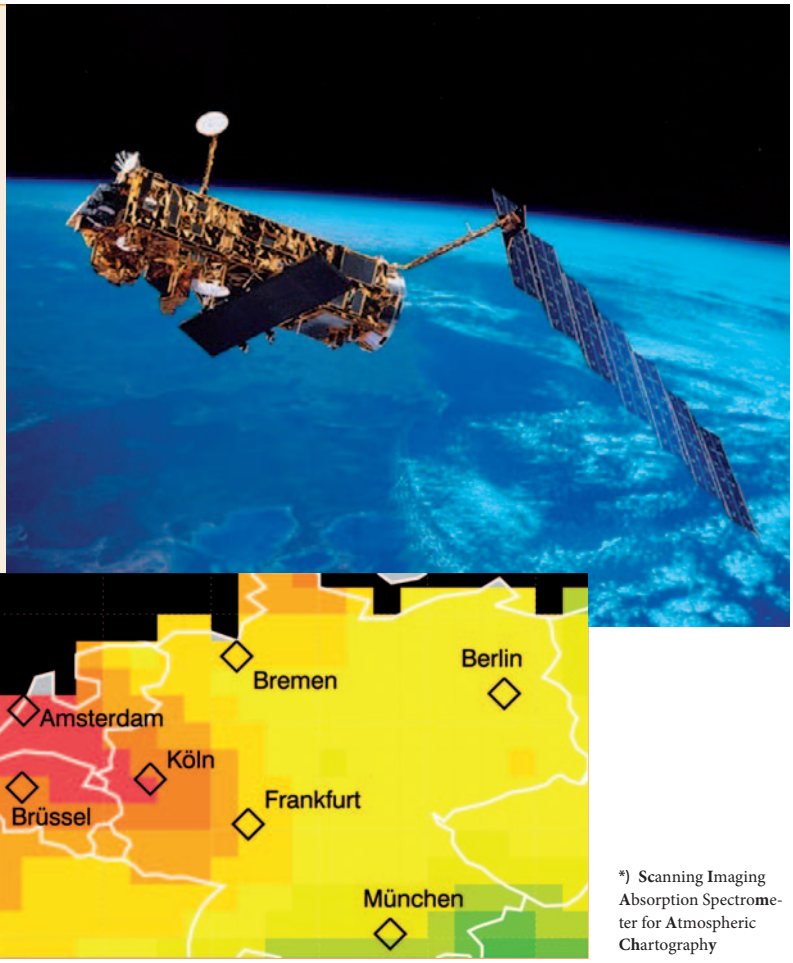
SPÜRNASE IM ALL

Umweltforschern der Universität Bremen ist es erstmals gelungen, mithilfe von Satellitenmessungen erhöhte regionale Konzentrationen des Treibhausgases Kohlendioxid (CO_2) nachzuweisen, die vom Menschen verursacht wurden (**Abb. unten**). Sie verwendeten dazu Daten des Instruments SCIAMACHY*), das unter Federführung des Deutschen Zentrums für Luft- und Raumfahrt (DLR) gebaut wurde und sich auf dem von der ESA betriebenen Umweltsatelliten ENVISAT befindet (**Abb. oben**).

SCIAMACHY misst die von Erdboden und Atmosphäre zurückgestreute Sonnenstrahlung. Daraus lassen sich die Konzentrationen einer Vielzahl von Spurengasen in der Atmosphäre bestimmen, u. a. auch für Kohlendioxid. Hohe Werte (rot) zeigen sich besonders über Europas Hauptballungsgebiet, das sich von Amsterdam bis etwa Frankfurt erstreckt. Richtung Osten nimmt der CO_2-Anteil ab (grün).

Allerdings ist die Zuordnung zwischen einer gemessenen hohen Konzentration in der Atmosphäre und der lokalen Emissionsquelle nicht einfach, da CO_2 eine lange Lebensdauer aufweist und weit transportiert wird. Außerdem führt selbst eine starke anthropogene Quelle nur zu einer kleinen regionalen Erhöhung gegenüber der großen Hintergrundkonzentration. Zusätzlich erschweren auch jahreszeitliche Schwankungen die Interpretation der Daten. Neue mathematisch-physikalische Methoden erlauben aber nun eine Auswertung, die regionale CO_2-Konzentrationsmuster zeigt.

O. Schneising et al., Atmos. Chem. Phys. Discuss. **8**, 5477 (2008)



Bilder: IUP, U Bremen, DLR, ESA

*) **S**canning **I**maging **A**bsorption Spectrom**e**ter for **A**tmospheric **Ch**artography