Eine optische Faktorenzerlegung ganzer Zahlen mit Gaußschen Summen.

E.Frins*, B.Hils, H.Schmitzer**, W.Dultz

Universidad de la República Montevideo[*], Xavier Univ. Cincinnati[**], Univ. Frankfurt(Main)

requalivahanus(affenschaukel)t-online.de

Das schnelle Faktorisieren großer Zahlen ist ein ernstes Hindernis beim Knacken der modernen Nachrichtenverschlüsselung, die auf der Falltüreigenschaft eines Produktes aus großen Primzahlen beruht. Wir zeigen, daß Gaußsche Summen zur Faktorisierung mit einer Anzahl harmonischer Gitter optisch realisiert werden können.

Endliche Gaußsche Summen *C* sind Reihen mit Summanden aus trigonometrischen Funktionen, deren Phase proportional zur ν-ten Potenz des Summationsindexes m ist. Z.B.:

$$C = 1/(M+1)\sum_{m=0}^{M}\cos(2\pi m^{\nu} N/l)$$

N, l und ν sind ganze Zahlen. Infolge der Normierung der Summe, ist *C* immer gleich 1, wenn l ein Teiler von N ist. Ist l kein Teiler von N, so fluktuieren die Phasen und die Summanden heben sich bei größerem M gegenseitig fast weg. In Abbildung 1 wird die Zahl N= 27 in ihre Faktoren l=1,3,9 und 27 zer-

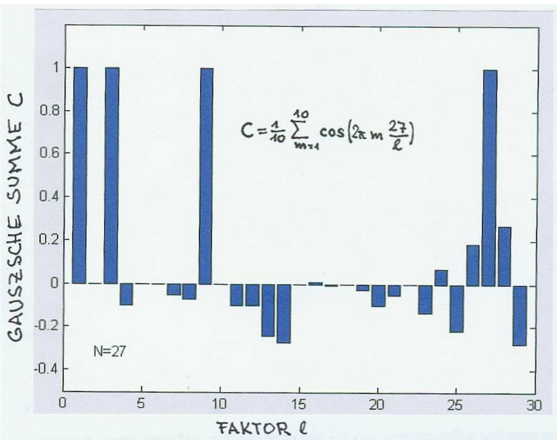

Abb.1 Faktorenzerlegung mit Gaußscher Summe.

legt, M ist gleich 10 und $\nu = 1$.

Für eine Anwendung muß diese Kreidemathematik als physikalischer Aufbau verwirklicht werden. Dafür wurden der Talboteffekt [1] und in letzter Zeit besonders von Schleich et al. [2-5] andere Interferenzsysteme wie NMR Echos, der zeitliche Talbot Effekt und frequenzgeschneiderte Impulse, sowie kalte Atome vorgeschlagen und erprobt. Hier beschreiben wir einen Demonstrationsversuch zur Faktorenzerlegung mit Gaußschen Summen, bei dem eine größere Anzahl harmonischer Ronchigitter gleichzeitig mit monochromatischem Licht beleuchtet wird.

Im Fernfeld eines Gitters addieren sich die Amplituden der Wellen, die aus den einzelnen Spalten kommen, in einer Gaußschen Summe,

$$C = \sum_{m=1}^{M}\cos(2\pi m d \sin\varphi/\lambda)$$

wobei M die Zahl der Spalte des Gitters, d die Gitterkonstante und φ der Beugungswinkel des Strahles ist. Nur wenn $d\sin\varphi/\lambda$ ganzzahlig ist, hat man eine konstruktive Interferenz der M Wellen, und ein helles Fernfeld unter dem Winkel φ. Im Gegensatz zum Talboteffekt, der ein Nahfeldeffekt mit $\nu = 2$ ist, finden wir hier im Fernfeld $\nu = 1$. Abb.2 zeigt eine Periode eines Ronchigitters mit seiner N-ten konstruktiven Ordnung unter dem Winkel φ. Dabei gilt $N = \frac{d}{\lambda}\sin\varphi$

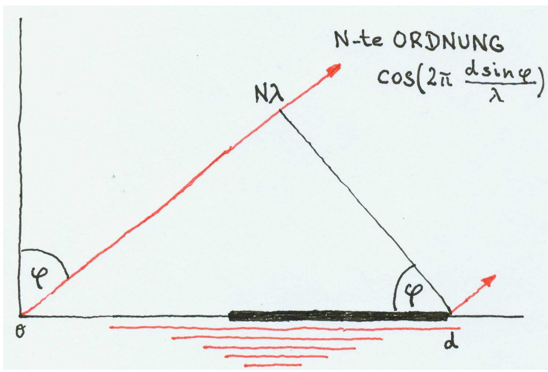

Abb.2 Eine Periode d eines Ronchigitters mit der konstruktiven Interferenzordnung N

Wir ersetzen jetzt das Gitter durch ein anderes mit der Gitterkonstanten d' und fragen erneut nach einer konstruktiven Ordnung unter dem selben Winkel φ. Diese Ordnung sei die *N'*-te des Gitters *d'* also gilt $N' = \frac{d'}{\lambda}\sin\varphi$. Damit finden wir $N = N'\frac{d}{d'}$ und für harmonische

Gitter mit $d' = d/l$ (l ganzzahlig) $N = N'l$. In diesem Fall sind also N' und l Faktoren von N und beide Gitter d, d' haben ein helles Fernfeld unter dem Winkel φ. Wir erwarten daher nur dann eine konstruktive Ordnung unter dem selben Winkel φ bei beiden Gittern wenn l ein Faktor von N ist. Bilden wir also die Fernfelder vieler harmonischer Gitter mit $d' = d/l$ und $l = 1,2,3,4,...$ übereinander ab, so treten helle Ordnungen unter dem Beugungswinkel φ nur bei den Gittern auf, deren l ein Faktor der Grundgitterordnung $N = \frac{d}{\lambda}\sin\varphi$ ist.

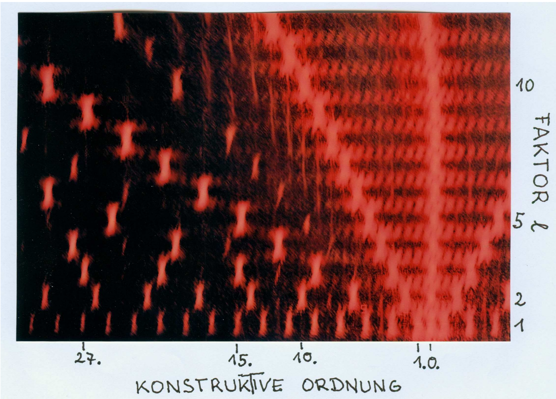

Abb.3 Das Fernfeld von 12 Ronchigittern mit harmonischen Gitterkonstanten zwischen d_0=0,2 mm (Grundgitter ganz unten) und d=d_0/12 (oben).

Abb.3 zeigt das Fernfeld von 12 harmonischen Ronchigittern übereinander, der Faktor l bestimmt die Gitterkonstante: $d = d_0 / l$. Betrachten wir für N=27 die 27-te Ordnung des Grundgitters $(l = 1)$. Über dem hellen Fleck dieser Ordnung finden wir weitere konstruktive Ordnungen für $l = 3,9$, die die Faktoren $l = 1,3,9$ anzeigen; die helle Ordnung bei $l = 27$ liegt nicht mehr auf unserer Photographie. Ein Ronchigitter zeigt bestenfalls nur sehr schwache gerade höhere Ordnungen, so daß manche Faktoren ausfallen oder sehr schwach angezeigt werden. Als Beispiel hierfür sei der Fall N=10 angeführt, bei dem die Faktoren $l = 1,5$ als gerade Ordnungen des Grundgitters und des Gitters mit $l = 5$ schwach angezeigt werden, der Faktor $l = 2$ als ungerade Ordnung des Gitters mit $l = 2$ aber stark. Der Faktor 10 ist hier auch noch sichtbar.
In Abb.4 ist der experimentelle Aufbau gezeigt, bei dem zwei Zylinderlinsen eine diagonale Lichtlinie über die nebeneinander liegenden, harmonischen Ronchigitter Abb.5 von jeweils

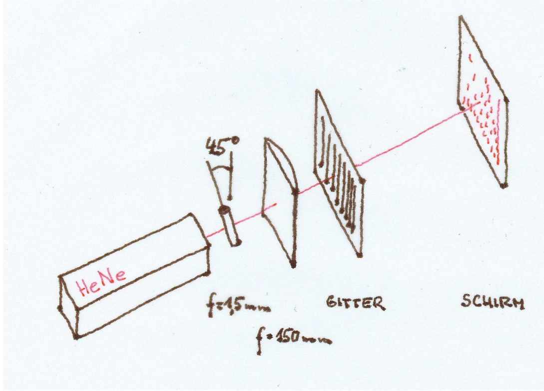

Abb.4 Experimenteller Aufbau

1 mm Breite zeichnen und die verschiedenen Ordnungen auf dem Schirm übereinander abbilden. Beachten Sie auch den Zwiestreit zweier Motive der Tiefenwahrnehmung am Gitter der Abbildung 4.

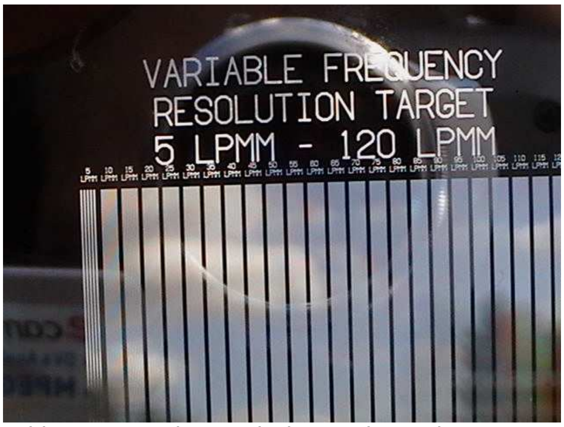

Abb.5 Satz harmonischer Gitter (Nr.V38-582 Edmund Optics)

Unsere Anordnung realisiert das Sieb des griechischen Gelehrten Erathostenes 284 – 202 v.Chr., der als erster auch den Erdumfang gemessen hat. Wir glauben, daß sie sich sehr gut als Beispiel für eine Gitteranwendung in einem Praktikum eignet. Um sie zu einem Quantenrechner zu entwickeln, müßte man sie mit einem einzelnen Photon betreiben und erreichen, daß dieses nicht alle, sondern nur die für die Faktorisierung relevanten Ordnungen beleuchtet. Wie das gehen soll wissen wir nicht, aber wenn man ein Problem benennen kann, kann man es vielleicht lösen.

[1] J.Clauser, J.Dowling; Phys.Rev.A **53** 4587 (1996)
[2] M.Mehring et al.; PRL **98** 120502 (2007)
[3] D.Bigourd et al.; PRL **100** 030202 (2008)
[4] W.Merkel et al. Fortschr.Phys. **54** 856 (2006)
[5] M.Gilowski et al.; PRL **100** 030201 (2008)