Optics EXPRESS

Prime number decomposition using the Talbot effect

KARL PELKA, JASMIN GRAF, THOMAS MEHRINGER, AND JOACHIM VON ZANTHIER[*]

Institut für Optik, Information und Photonik, Universität Erlangen-Nürnberg, 91058 Erlangen, Germany
[*]*joachim.vonzanthier@physik.uni-erlangen.de*

Abstract: We report on prime number decomposition by use of the Talbot effect, a well-known phenomenon in classical near field optics whose description is closely related to Gauss sums. The latter are a mathematical tool from number theory used to analyze the properties of prime numbers as well as to decompose composite numbers into their prime factors. We employ the well-established connection between the Talbot effect and Gauss sums to implement prime number decompositions with a novel approach, making use of the longitudinal intensity profile of the Talbot carpet. The new algorithm is experimentally verified and the limits of the approach are discussed.

OCIS codes: (050.1940) Diffraction; (110.3175) Interferometric Imaging; (200.0200) Optics in computing.

References and links

1. H. F. Talbot, "Facts relating to optical science," Philos. Mag. **9**, 401–407 (1836).
2. L. Rayleigh, "On copying diffraction–gratings, and some phenomena connected therewith," Philos. Mag. **11**, 196–205 (1881).
3. W. D. Montgomery, "Self-imaging Objects of Infinite Aperture," J. Opt. Soc. Am. **57**, 772–775 (1967).
4. L. Liu, "Talbot and Lau effects on incident beams of arbitrary wavefront, and their use," Appl. Opt. **28**, 4668–4678 (1989).
5. K. Banaszek, K. Wódkiewicz, and W. P. Schleich, "Fractional Talbot effect in phase space: A compact summation formula," Opt. Express **2**, 169 –172 (1998).
6. O. Friesch, I. Marzoli, and W. P. Schleich "Quantum carpets woven by Wigner functions," New J. Phys. **2**, 4 (2000).
7. P. Cloetens, J. P. Guigay, C. De Martino, J. Baruchel, and M. Schlenker "Fractional Talbot imaging of phase gratings with hard x rays," Opt. Lett. **22**, 1059–1061 (1997).
8. B. J. McMorran and A. D. Cronin, "An electron Talbot interferometer," New J. Phys. **11**, 033021 (2009).
9. M. S. Chapman, C. R. Ekstrom, T. D. Hammond, J. Schmiedmayer, B. E. Tannian, S. Wehinger, and D. E. Pritchard, "Near–field imaging of atom diffraction gratings: The atomic Talbot effect," Phys. Rev. A **51**, R14–R17 (1995).
10. S. Nowak, C. Kurtsiefer, T. Pfau, and C. David, "High-order Talbot fringes for atomic matter waves," Opt. Lett. **22**, 1430–1432 (1997).
11. M. R. Dennis, N. I. Zheludev, and F. J. G. de Abajo, "The plasmon Talbot effect," Opt. Express **15**, 9692–9700 (2007).
12. S. Cherukulappurath, D. Heinis, J. Cesario, N. F. van Hulst, S. Enoch, and R. Quidant, "Local observation of plasmon focusing in Talbot carpets," Opt. Express **17**, 23772–23784 (2009).
13. P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM Journal on Computing **26**, 1484–1509 (1997).
14. J. F. Clauser and J. P. Dowling, "Factoring integers with Young's N-slit interferometer," Phys. Rev. A **53**, 4587–4590 (1996).
15. M. V. Berry and S. Klein, "Integer, fractional and fractal Talbot effects," J. Mod. Opt. **43**, 2139–2164 (1996).
16. S. Wölk, W. Merkel, W. P. Schleich, I. Sh. Averbukh, and B. Girard, "Factorization of numbers with Gauss sums: I. Mathematical background," New J. Phys. **13**, 103007 (2011).
17. D. Bigourd, B. Chatel, W. P. Schleich, and B. Girard, "Factorization of Numbers with the Temporal Talbot Effect: Optical Implementation by a Sequence of Shaped Ultrashort Pulses," Phys. Rev. Lett. **100**, 030202 (2008).
18. V. Tamma, H. Zhang, X. He, A. Garuccio, and Y. Shih, "Factorization of integers with multi-path optical interference," Int. J. Quantum Inf. **9**, 423–430 (2011).
19. V. Tamma, H. Zhang, X. He, A. Garuccio, W. P. Schleich, and Y. Shih,"Factoring numbers with a single interferogram," Phys. Rev. A **83**, 020304 (2011).
20. V. Tamma, C. O. Alley, W. P. Schleich, and Y. H. Shih, "Prime Number Decomposition, the Hyperbolic Function and Multi-Path Michelson Interferometers," Found. Phys. **42**, 111–121 (2012).
21. M. Gilowski, T. Wendrich, T. Müller, Ch. Jentsch, W. Ertmer, E.M. Rasel, and W.P. Schleich, "Gauss Sum Factorization with Cold Atoms," Phys. Rev. Lett. **100**, 030201 (2008).

#326052 https://doi.org/10.1364/OE.26.015009
Journal © 2018 Received 14 Mar 2018; revised 14 May 2018; accepted 15 May 2018; published 30 May 2018

22. M. Sadgrove, S. Kumar, and K. Nakagawa, "Enhanced Factoring with a Bose-Einstein Condensate," Phys. Rev. Lett. **101**, 180502 (2008).
23. M. Mehring, K. Müller, I. Sh. Averbukh, W. Merkel, and W. P. Schleich, "NMR Experiment Factors Numbers with Gauss Sums," Phys. Rev. Lett. **98**, 120502 (2007).
24. T. S. Mahesh, N. Rajendran, X. Peng, and D. Suter, "Factorizing numbers with the Gauss sum technique: NMR implementations," Phys. Rev. A **75**, 062303 (2007).
25. X. Peng and D. Suter, "NMR implementation of factoring large numbers with Gauß sums: Suppression of ghost factors," Europhys. Lett. **84**, 40006 (2008).
26. M. Berry, I. Marzoli, and W. P. Schleich, "Quantum carpets, carpets of light," Phys. World **14**, 39 (2001).
27. W. B. Case, M. Tomandl, S. Deachapunya, and M. Arndt, "Realization of optical carpets in the Talbot and Talbot-Lau configurations," Opt. Express **17**, 20966–20974 (2009).
28. M. Štefaňák, W. Merkel, W. P. Schleich, D. Haase, and H. Maier, "Factorization with Gauss sums: scaling properties of ghost factors," New J. Phys. **9**, 370 (2007).
29. M. Štefaňák, D. Haase, W. Merkel, M. S. Zubairy, and W. P. Schleich, "Factorization with exponential sums," J. Phys. A **41**, 304024 (2008).
30. V. Tamma, H. Zhang, X. He, A. Garuccio, and Y. Shih, "New factorization algorithm based on a continuous representation of truncated Gauss sums," J. Mod. Opt. **56**, 2125–2132 (2009).
31. W. Merkel, S. Wölk, W. P. Schleich, I. Sh. Averbukh, B. Girard, and G. G. Paulus, "Factorization of numbers with Gauss sums: II. Suggestions for implementation with chirped laser pulses," New J. Phys. **13**, 103008 (2011).

1. Introduction

Diffraction is one of the most fundamental aspects of optics occurring when physical objects are described by waves. The corresponding interferences may lead to surprising phenomena such as a self-imaging of periodic structures as discovered by Talbot [1] and theoretically derived by Rayleigh [2]. The optical Talbot effect was later on studied theoretically in much detail, either by formulations in real space [3,4] or phase space [5,6], and experimentally observed with x-rays [7], electron beams [8], atomic matter waves [9,10] and surface plasmons [11,12]. Although the Talbot effect has been proven to be useful for various applications, we focus on a particular application, namely to decompose composite numbers into their prime factors. Since self-imaging is a general property of diffraction in the near field, the Talbot effect extends prime number decomposition to the field of classical optics, representing an alternative to factorizing algorithms known from quantum computation [13], albeit by purely classical means. This alternative approach was initially developed by Clauser and Dowling [14] and later linked to generalized Gauss sums [15], which constitute a practical tool to perform prime number decompositions [16]. This ability of Gauss sums was already proven in many experiments e.g. by using the temporal Talbot effect [17], different interferometers [18–21], Bose-Einstein condensates [22] or NMR techniques [23–25]. However, up to now there appears to be no experimental realization of the optical Talbot effect with the aim of performing prime number decomposition. This circumstance becomes less surprising when noticing that complete measurements of the two-dimensional intensity profile using coherent illumination, so called Talbot carpets [26], were not recorded until recently [27]. The goal of this paper is to connect the two dots.

2. Prime number decomposition using Gauss sums

Our technique to implement prime number decompositions is based on the properties of Gauss sums, which exist in many different forms [16,28,29]. The discrete Gauss sum, showing the characteristic property of a quadratically occurring summation index, is defined as

$$S_N(l) = \sum_{m=-\infty}^{\infty} w_m \exp\left(i2\pi m^2 \frac{l}{N}\right), \tag{1}$$

with $l, N \in \mathbb{N}$ and weight factors w_m, where the latter is supposed to be a slowly varying function of m [16]. In view of the upcoming discussion, we assume the weight factor to be of the form $w_m = a\,\mathrm{sinc}(ma)$ with $a \in \mathbb{R}^+$. Inserting this weight factor, exploiting the periodicity of the

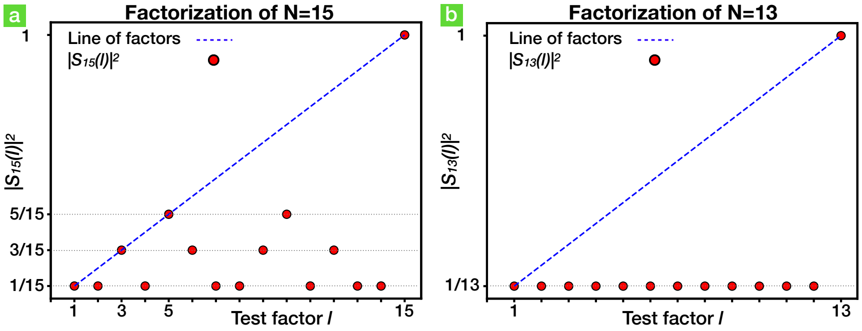

Fig. 1. (a) Evaluation of $|S_{15}(l)|^2$. For $l = 3$ and $l = k \cdot 3$, $|S_{15}(l)|^2$ evaluates to $^3/_{15}$. For $l = 5$ and $l = k \cdot 5$, $|S_{15}(l)|^2$ is equal to $^5/_{15}$. (b) Evaluation of $|S_{13}(l)|^2$. Here $|S_{13}(l)|^2$ evaluates to $^1/_{13}$ for every l since 13 is a prime number. Thus, all prime factors of a number N intersect the line connecting $|S_N(1)|^2$ and $|S_N(N)|^2$ giving rise to the name "line of factors".

exponential function in m with period N and applying the Poisson summation formula, allows us finding the convenient expression

$$S_N(l) = \frac{1}{N}\sum_{m=0}^{N-1} \exp\left(i2\pi m^2 \frac{l}{N}\right) = \frac{1}{N} G(l, N), \tag{2}$$

where $G(l, N)$ represents the so called complete Gauss sum (normalized by N), if the condition $a < {}^2/_N$ holds. Employing the properties of the complete Gauss sum $G(l, N)$ we can perform prime number decomposition [16]. To this aim, we assume that the number N to be factorized is odd and l a test factor. If l is no factor of N, we obtain from Eq. (2) $|S_N(l)|^2 = {}^1/_N$, whereas if l is a prime factor p of N or a multiple kp of a prime factor, we find $|S_N(kp)|^2 = {}^p/_N$. Hence, all prime factors of an odd number N can be uniquely identified by evaluating $|S_N(l)|^2$ for all test factors l and comparing with the "line of factors p", given by $f(p) = {}^p/_N$ (see Fig. 1).

3. The Talbot effect

The Talbot effect is a diffraction phenomenon taking place in the near field behind a grating upon illumination with a plane wave. To derive the Talbot diffraction pattern, we assume an infinite periodic one-dimensional grating with slit width w and period d. The corresponding transmission function reads

$$T(\xi) = \sum_{n=-\infty}^{\infty} \text{rect}\left(\frac{\xi - nd}{w}\right) \qquad \text{with} \qquad \text{rect}(x) = \begin{cases} 1 & \text{for} - 1/2 < x < 1/2, \\ 0 & \text{else.} \end{cases} \tag{3}$$

Within the Fresnel diffraction formalism we can propagate the electric field from the source plane $E(\xi, z = 0) = E_0$ to the detection plane $(x, z > 0)$ via

$$E(x, z) = \frac{\exp(ikz - i\pi/4)}{\sqrt{\lambda z}} \int_{-\infty}^{\infty} T(\xi) E_0 \exp\left\{\frac{ik}{2z}\left[(x - \xi)^2\right]\right\} \mathrm{d}\xi. \tag{4}$$

with λ the wavelength and k the wave number. Since there are infinitely many slits, $T(\xi)$ is a periodic function and can be decomposed into a Fourier series

$$T(\xi) = \sum_{m=-\infty}^{\infty} A_m \exp\left(-im\frac{2\pi}{d}\xi\right) \text{ with } A_m = \frac{w}{d}\text{sinc}\left(m\frac{w}{d}\right). \tag{5}$$

Combining Eqs. (4) and (5) and evaluating the integral yields

$$E(x,z) = E_0 \exp(ikz) \sum_{m=-\infty}^{\infty} A_m \exp\left[-i2\pi\left(m\frac{x}{d} + m^2\frac{z}{L_T}\right)\right], \tag{6}$$

where $L_T = {}^{2d^2}/_{\lambda}$ represents the so-called Talbot length, illustrating the self-imaging effect as $E(x,0) = E(x, nL_T)$ for $n \in \mathbb{N}$. The intensity at the grating is found by calculating the modulus square of the electric field amplitude leading to

$$I(x,z) = I_0\left|\sum_{m=-\infty}^{\infty} A_m \exp\left[-i2\pi\left(m\frac{x}{d} + m^2\frac{z}{L_T}\right)\right]\right|^2, \quad \text{with} \quad I_0 = E_0^2. \tag{7}$$

4. Prime number decomposition using the Talbot effect

In 2009, a precise measurement of a Talbot carpet [27] showed that the intensity distribution along the x-axis at the fractional distances ${}^{z_l}/_{z_T} \approx {}^{l}/_{N}$ contains features of a Gauss sum. This allows to perform prime number decomposition by counting the intensity maxima parallel to the grating at the distinct distances z_l [27]. The properties of the lateral intensity distribution of the Talbot carpet lies also at the heart of [14]. Upon relaxing the assumption of infinitesimal slits to finite slits, it can be shown that the maximal number that can be factored with both methods is given by $N_{\max} < {}^{d}/_{w}$. In this paper, however, we propose a different algorithm for prime number decomposition, based on another appearance of a Gauss sum within the Talbot carpet. Considering the intensity distribution of Eq. (7) at a fixed lateral position $x = qd$, $q \in \mathbb{N}$, and studying the intensity distribution along the z-axis, we obtain after a change of the summation index $n = -m$ and exploiting the symmetry of the Fourier coefficients $A_m = A_{-m}$

$$I(qd,z) = I_0\left|\sum_{n=-\infty}^{\infty} A_n \exp\left(i2\pi n^2\frac{z}{L_T}\right)\right|^2 = I_0|S_{N=L_T}(l=z)|^2. \tag{8}$$

Eq. (8) resembles already the discrete Gauss sum $S_N(l)$. With Fourier coefficients $A_n = ({}^{w}/_{d}) \cdot \operatorname{sinc}[m({}^{w}/_{d})]$ it turns into a complete Gauss sum $G(l,N)$, normalized by N, if the condition $N < {}^{2d}/_{w}$ holds. This can be seen by identifying ${}^{w}/_{d}$ with a in Sec. (2). Note that this condition limits the numbers we can factorize via the dimensions of the used grating. Using this expression we can rewrite Eq. (8) as

$$I(qd,z) = I_0|S_{N=L_T}(l=z)|^2 = \frac{I_0}{N^2}|G(l=z, N=L_T)|^2 \qquad \text{for} \qquad N < \frac{2d}{w}. \tag{9}$$

Altogether, this means that we can perform the prime number decomposition of all odd $N < {}^{2d}/_{w}$ via one measurement of a Talbot carpet when applying the following procedure:

1) Record the intensity profile of the Talbot carpet along the z-axis from any Talbot distance sL_T to the next Talbot distance $(s+1)L_T$ with sufficiently small steps Δz at some fixed slit position $x = qd$ with $s, q \in \mathbb{N}$. This requires ${}^{L_T}/_{\Delta z}$ measurements.

2) Locate the fractional Talbot distances $z_{l,N} = sL_T + {}^{L_T}/_{N} \cdot l$, $l = 1, \ldots, N$ by dividing the measured Talbot length equidistantly into N parts.

3) Draw the line of factors for arbitrary $N < {}^{2d}/_{w}$ from $[1, I(z_{1,N})]$ to $[N, I(z_{N,N})]$ and locate the intensities $I(z_{l,N})$ on or above this line to find the prime factors l of this N.

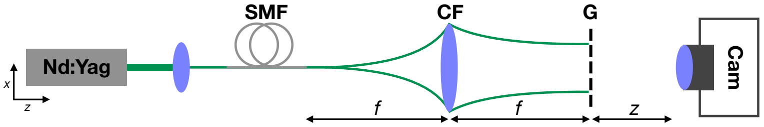

Fig. 2. Experimental setup: Light of a Nd:Yag laser (λ = 532 nm) is coupled into a single mode fiber SMF. A collimation lens CF is placed at its focal length f behind the fiber, such that the beam waist of the resulting Gaussian beam is located at f behind the lens where the grating is located. A CMOS camera with 1280 × 1024 pixels of side length 5.2 µm and a 10× magnifying microscope objective is placed at a distance z behind the grating. The camera was mounted on a translation stage which can travel 150 mm along the z axis.

5. Experimental realization of the Talbot effect with focus on prime number decomposition

To prove the above proposed algorithm for prime number decomposition, we designed the experimental setup shown in Fig. 2. Placing the grating in the focus of the Gaussian beam leads to the following expression for the lateral electric field distribution at the position of the grating

$$E(x, y, z = 0) = E_0 \exp\left(-\frac{x^2+y^2}{2\sigma^2}\right). \tag{10}$$

with the Gaussian beam waist σ. In this case the Fresnel diffraction integral is not calculated using a plane wave as input but a Gaussian distribution, such that the intensity behind the grating reads

$$I(x, z) = \frac{I_0}{\lambda z}\left|\int_{-\infty}^{\infty} T(\xi) \exp\left(-\frac{\xi^2}{2\sigma^2}\right) \exp\left\{\frac{i\pi}{\lambda z}\left[(x-\xi)^2\right]\right\} \mathrm{d}\xi\right|^2. \tag{11}$$

Upon assuming infinitesimal slits, Eq. (11) is the convolution of a fractal curve [15, 26] with the Gaussian beam acting as a Gaussian smoothing filter. This explains why the distribution in Fig. 3(b) is reminiscent of a Gauss sum with a Gaussian smoothing familiar from wave packet dynamics. In order to record the full Talbot carpet for a diffraction grating with a period of d = 200 µm and a slit width of w = 10 µm, the measurement was automated to record with a CMOS camera images between L_T = 150.4 mm and $2L_T$ = 300.8 mm in steps of Δz = 50 µm. From the collected data the Talbot carpet was reconstructed by stacking the measured intensity for each step, whereby each image was averaged over all rows along the y-axis (since the intensity does not depend on y). The resulting Talbot carpet is shown in Fig. 3(a). Besides the experimental data (green line) Fig. 3(b) displays also the theoretical prediction (black dashed line) obtained by numerical evaluation of Eq. (11), demonstrating an excellent agreement between theory and experiment. As an example, Fig. 3(**c**) shows the decomposition of the number N = 27 using our new algorithm. As can be seen, the prime factors 3 and 9 lie above the line of factors connecting $I(z_{1,27})$ and $I(z_{27,27})$ and not as before on this line. The reason for this is due to the reduced intensity at $z = 2L_T$ compared to $z = L_T$, stemming from the Fresnel diffraction of the Gaussian beam. Hence $I(z_{27,27} = 2L_T)$ lies lower than $I(z = L_T)$ (see Fig. 3(b)) causing the slope of the line of factors to be smaller than in the ideal case. This effect is small, but becomes more prominent for Gaussian beams compared to plane waves. This also leads to a slight decrease of the limit up to which numbers can be factorized, theoretically given by $N < {}^{2d}/_{w}$. For the particular grating used, this means that we can decompose only numbers up to N = 29 and not as theoretically predicted up to N = 40. Nevertheless, the application of the discrete Gauss sum $|S_N(l)|^2$ appearing in the Talbot carpet along the z-direction allows us to decompose numbers within the theoretical limit of the approach into their correct prime factors. Our approach reduces also the amount of required experimental data to the measurement of a single Talbot carpet.

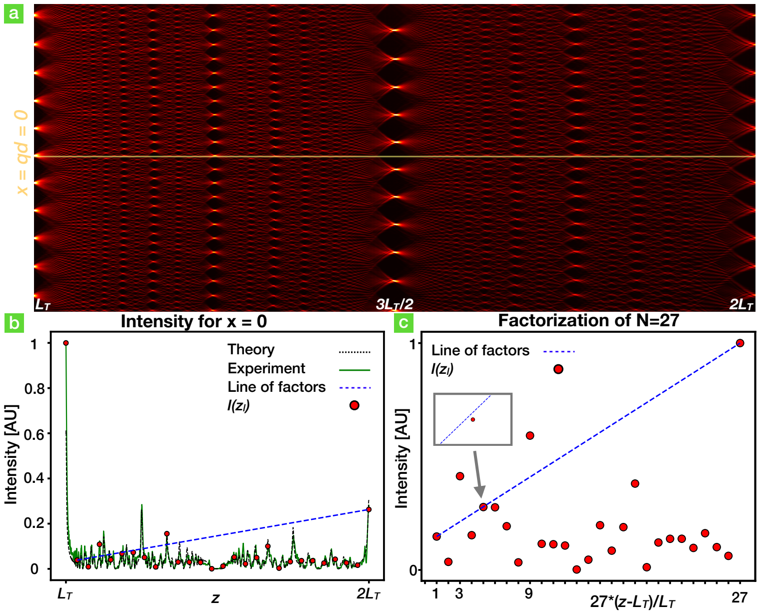

Fig. 3. (a) Measured Talbot carpet for a grating with period $d = 200\,\mu\text{m}$ and a slit width $w = 10\,\mu\text{m}$. The yellow line indicates the line along which the intensity is evaluated for the factorization algorithm. (b) Intensity along the yellow line as measured in the experiment (green line) and as evaluated theoretically (black dashed line) obtained by evaluation of the Fresnel diffraction integral with 250 slits and a Gaussian beam width of $\sigma = 5100\,\mu\text{m}$ measured by the knife-edge method. (c) Result of the proposed factorization algorithm using the experimental data. We see that it finds the correct prime factors 3 and 9 of $N = 27$.

The latter contains the information for all possible numbers since encoding the number to be factorized is done by merely rescaling the z axis through $z_{l,N}$ [16, 19, 30, 31].

6. Conclusion

We theoretically discussed the capabilities of the Talbot effect to perform prime number decomposition based on its mathematical analogy to a Gauss sum. We envisaged at first a diffraction grating with infinitely many slits illuminated by a plane wave. We then found that the properties of the ideal case are still valid for the realistic case of a diffraction grating with finite number of slits illuminated by a Gaussian beam. The theoretical investigations result in the first realization of the discrete Gauss sum $|S_N(l)|^2$ using the longitudinal intensity profile of the Talbot effect. Our novel approach improves the amount of possible numbers that can be experimentally decomposed compared to existing factorization schemes based on the fractional Talbot effect. Nevertheless, we note that the Fourier coefficients of the grating transmission function yield a criterion that, depending on the geometry of the diffraction grating, limits the maximal number N that can be decomposed to rather low values. However, other interference phenomena that can be described by the discrete Gauss sum $|S_N(l)|^2$ might yield less restrictive conditions and therefore enhance the possibility to implement prime number decompositions within a physical realization.

Funding

Erlangen Graduate School in Advanced Optical Technologies (SAOT) by the German Research Foundation (DFG) in the framework of the German excellence initiative, Staedtler Foundation, Universitätsbund Erlangen-Nürnberg e.V.