Optics Letters

Prime number factorization and degree of coherence of speckled light beams

Tianyu Cao,[1,2] Xin Liu,[1,2] Qian Chen,[1,2] Sergey A. Ponomarenko,[3,4] Yangjian Cai,[1,2] and Chunhao Liang[1,2,*]

[1]Shandong Provincial Shandong Provincial Engineering and Technical Center of Light Manipulations & Shandong Provincial Key Laboratory of Optics and Photonic Devices, School of Physics and Electronics, Shandong Normal University, Jinan 250014, China
[2]Collaborative Innovation Center of Light Manipulations and Applications, Shandong Normal University, Jinan 250358, China
[3]Department of Electrical and Computer Engineering, Dalhousie University, Halifax, Nova Scotia, B3J 2X4, Canada
[4]Department of Physics and Atmospheric Science, Dalhousie University, Halifax, Nova Scotia, B3H 4R2, Canada
*chunhaoliang@sdnu.edu.cn

Received 25 July 2024; revised 29 August 2024; accepted 29 August 2024; posted 3 September 2024; published 11 September 2024

We discover a connection between a Gauss sum of number theory and the degree of coherence (DOC) of the field in a transverse plane of structured speckled light beams. We theoretically demonstrate and experimentally validate that prime number factorization can be achieved by manipulating the source beam's DOC in Young's double-slit experiment. The determination of whether a number can be factored is based solely on the visibility of the resulting interference patterns. Our findings offer new insights into information encryption and decryption, data compression, etc.

https://doi.org/10.1364/OL.537537

Partially coherent beams (PCBs), as the dynamic speckles, exhibit statistically stable beam properties despite random fluctuations in an instantaneous phase [1]. Compared to their coherent counterparts, PCBs can eliminate beam interference and remain robust in adverse environment, making them suitable for a wide range of applications across multiple disciplines, such as speckle-free optical imaging and optical communication through turbulent atmospheres [2–5]. A key feature of PCBs is their unique DOC. Gori and collaborators established the sufficient condition for devising this function, leading to the development of numerous PCBs with the prescribed DOC [6]. For further details, refer to review articles [7,8]. Experimentally, PCBs are typically realized using two primary methods: the van Cittert–Zernike theorem and the mode superposition principle [7–10]. Recent advancements in optical systems have led to several remarkable applications utilizing the DOC, including high-capacity and high-fidelity information encryption, robust far-zone optical imaging, imaging beyond the Rayleigh diffraction limit, and prime number factorization [11–16].

Prime number factorization, particularly for large numbers, is an exceedingly challenging problem and is therefore considered a cornerstone of information security [17,18]. This technique has also been employed for dimensionality reduction in machine learning [19], image or data compression [20], efficient color encoding [21], and providing new insights into quantum mechanical systems dynamics [22]. Various protocols for performing prime number factorization have been proposed so far, in both quantum and classical physics. In classical physics, the most popular method involves incomplete or complete Gauss sums. The incomplete Gauss sums, in particular, require fewer Gauss terms, making them more promising for experimental factoring of extremely large numbers [23]. This approach is widely applied in the optical Talbot effect [24], matter waves [25], nuclear spin waves [26], interferometers [27], etc. In optics, Pelka *et al.* established a link between the optical Talbot effect with Gauss sum, achieving factorization up to the value 27 [24]. Bigourd *et al.* factored numbers using a sequence of shaped ultrashort pulses, which demands extremely precise positioning of multiple pulses [27]. Recently, we have advanced number factorization protocols using axial correlation revivals of structured random waves [28] and the periodicity of the OAM phase distribution [29]. The former can be applied to very large numbers, while the latter enables ultrafast factorization.

In this Letter, we establish a link between an incomplete Gauss sum and the periodicity of the two-point field correlation of optical beams in their transverse plane. We provide an alternative method for prime number factorization using PCBs with the prescribed DOC in Young's double-slit experiment.

In the space-frequency domain, the statistical properties of the Schell-model PCBs are typically characterized by the cross-spectral density function. In one dimension, this function is represented as follows:

$$W(x_1, x_2) = \tau^*(x_1)\,\tau(x_2)\,\mu(x_2 - x_1), \tag{1}$$

where τ is the complex amplitude and here is supposed to be $\tau(x) \propto \exp\left(-x^2/2\sigma_0^2\right)$ with the beam width σ_0. $\mu(x_2 - x_1)$ represents the DOC of the field at a pair of points x_1 and x_2 and depends solely on the difference between positional locations. It follows from the optical coherence theory that the DOC of the Schell-model PCBs can be described by the Fourier transform of the spectral density function $Q(v)$ [6] as follows:

$$\mu(x_2 - x_1) = \int Q(v) \exp\left[-i2\pi(x_2 - x_1)v\right] dv. \tag{2}$$

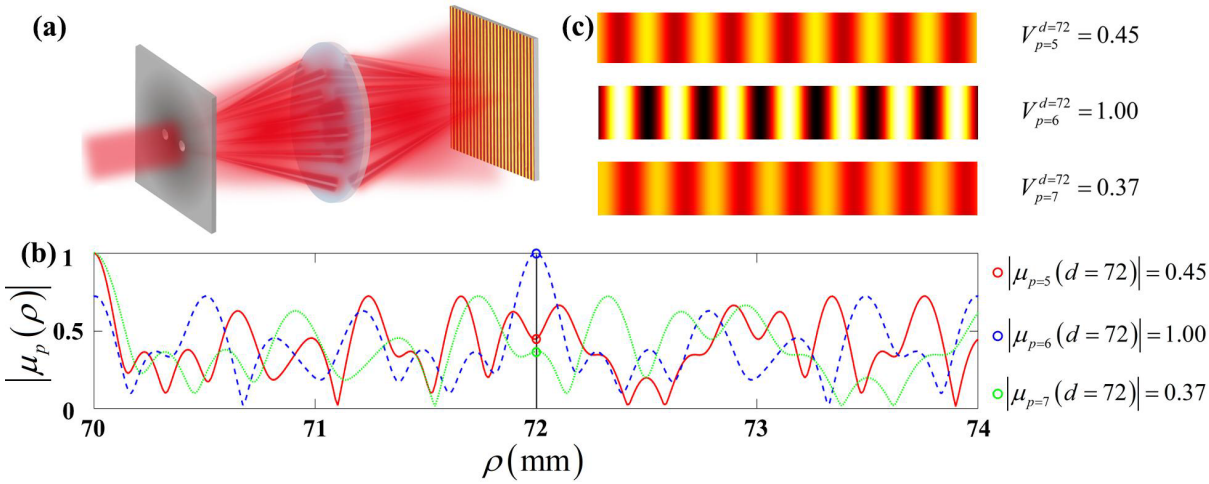

Fig. 1. Schematic illustration of the principle of prime number factorization using two-point correlations of partially coherent beams. (a) Diagram of Young's double-hole experiment with the prescribed PCB. (b) Curves of the DOC for $p = 5$, 6, and 7. (c) Corresponding beam interference fringes, where the distance between two holes is $d = 72$. The parameter M is set to 5.

We can construct the desired DOC by adopting the appropriate $Q(v)$ function. Here we define the spectral density function as follows:

$$Q(v) = \frac{1}{M}\sum_{m}^{M}\delta\left(v - \frac{m^2}{P}\right), \tag{3}$$

where M is a number of Dirac functions and P determines the location of each Dirac function. By substituting Eq. (3) into Eq. (2), the DOC can be expressed as follows:

$$\mu(x_2 - x_1) = \frac{1}{M}\sum_{m}^{M}\exp\left[-i2\pi(x_2 - x_1)\frac{m^2}{P}\right]. \tag{4}$$

Next, we examine a Young's type interference experiment, where the produced beam illuminates a screen with two pinholes, and its transmittance function reads as follows:

$$T(x) = \frac{1}{2}\left[\delta(x + D/2) + \delta(x - D/2)\right]. \tag{5}$$

Here D characterizes the distance between the pinholes. The outgoing beam is focused by a thin lens with the focal length f. The pattern in the rear focal plane of the lens is given by the following:

$$\begin{aligned} I(\rho) = &\iint W(x_1, x_2)\, T^*(x_1)\, T(x_2) \\ &\times \exp\left[-\frac{i2\pi}{\lambda f}(x_2 - x_1)\rho\right] dx_1 dx_2. \end{aligned} \tag{6}$$

By substituting Eqs. (1), (4), and (5) into Eq. (6), we obtain the following:

$$I(\rho) \propto 1 + \mathrm{Re}\left[\mu(D)\exp\left(-\frac{i2\pi}{\lambda f}D\rho\right)\right]. \tag{7}$$

If we take $\mu(D) = |\mu(D)|\exp(i\theta_D)$, where $|\cdot|$ denotes the modulus and θ_D is the angle of $\mu(D)$, the above equation can be rearranged as follows:

$$I(\rho) \propto 1 + |\mu(D)|\cos\left(\theta_D - \frac{2\pi}{\lambda f}D\rho\right). \tag{8}$$

The visibility of the beam interference fringes is determined by the following:

$$V_P^D = \frac{I(\rho)_{\max} - I(\rho)_{\min}}{I(\rho)_{\max} + I(\rho)_{\min}} = |\mu(D)| = \left|\frac{1}{M}\sum_{m}^{M}\exp\left(-i2\pi m^2\frac{D}{P}\right)\right|. \tag{9}$$

The above equation clearly demonstrates that the visibility of beam interference fringes is described by the incomplete Gauss sum. As illustrated in Refs. [28,29], it provides us with a method to factorize a number into prime factors using Young's double-slit interference setup, where the number to be factorized is set as the distance D between the two pinholes, while the trial factor is determined by the parameter P. The parameters D and P are both in meters. For more generality, we define the number D to be factorized and the trial factor P as $d = D/\alpha$ and $p = P/\alpha$, where α is a constant in meters, making d and p dimensionless. The constant α also serves to adjust the values of D and P (especially when they are large) to ensure that they are attainable in the following experiment. Here, if the trial factor p is a true factor of the number d to be factorized, the visibility ideally reaches 1; otherwise, it oscillates rapidly and takes on small values. To eliminate the influence of ghost factors (non-factors with high visibility) and improve factor identification, we adopt the established principle that the parameter M satisfies $M \geq 0.7\sqrt[4]{d}$ [28,29]. All ghost factors are suppressed below the threshold value $1/\sqrt{2}$.

Next, we utilize the theoretical framework of the derived analytical expression to advance and implement a prime number factorization protocol. Figure 1(a) shows the schematic diagram of Young's double-slit interference setup. The PCB with the prescribed DOC illuminates a two-pinhole screen, which is then focused by a thin lens. Here, the distance between the two pinholes is set to $d = 72$, and the trial numbers p are taken as 5, 6, and 7, respectively. Figure 1(b) displays the degrees of coherence for different values of p. The correlation values $|\mu_p(d)|$ at the two pinholes are 0.45, 1.00, and 0.37, respectively, as indicated by the circles. The visibility of the beam interference fringes is determined by the DOC of the source. The corresponding interference patterns and their visibilities at the back focal plane of the lens are presented in Fig. 1(c), where the visibilities match

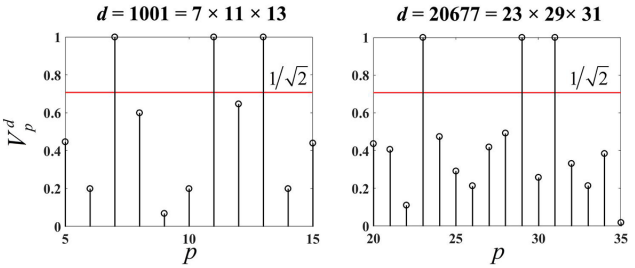

Fig. 2. Visibility as a function of the trial factor p, with the numbers d to be factored set as (a) $d = 1001 = 7 \times 11 \times 13$ and (b) $d = 20677 = 23 \times 29 \times 31$. All factor and non-factors are distinctly distinguished by the threshold value $1/\sqrt{2}$, indicated by the solid red lines. The parameter M is set to 5.

the values $|\mu_p(d)|$. It is observed that only when a trial factor matches the true one, $p = 6$, does the visibility reach 1.00, clearly demonstrating that we can distinguish factors from non-factors solely by the visibility of beam interference fringes. We also factorized the numbers 1001 and 20677, and the corresponding visibilities for the trial factors p are shown in Fig. 2. All factors and non-factors are clearly distinguished by the threshold line $1/\sqrt{2}$, marked by the solid red line.

Finally, we conducted an experimental verification of the aforementioned theoretical results. We exhibit our experimental setup in Fig. 3. A linearly polarized light beam, emitted from a Nd:YAG laser, passes through a half-wave plate and is expanded by a beam expander. The outgoing light beam then traverses a beam splitter and illuminates a phase-only spatial light modulator (SLM). We rotate the half-wave plate to ensure the polarization direction of the beam is horizontal, as the SLM is responsive only to this direction.

To generate a PCB with the prescribed DOC, we utilize the incoherent superposition of customized speckles [30], whose random electric fields are defined by the following:

$$E(x) = \tau(x) F_T[P(v) C_n(v)], \tag{10}$$

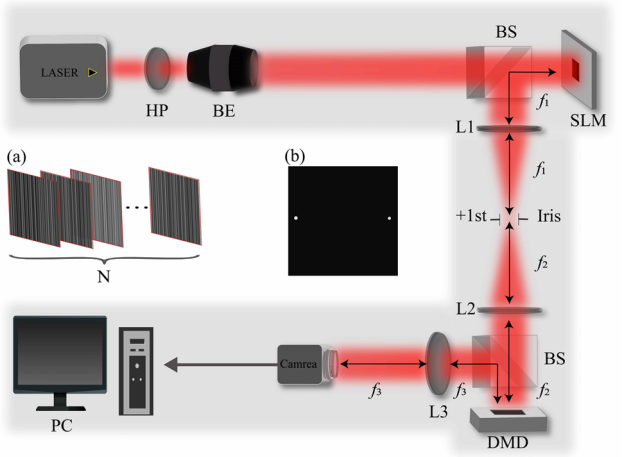

Fig. 3. Experimental setup for prime number factorization with Young's double-hole experiment. HP, half-wave plate; BE, beam expander; BS, beam splitter; SLM, reflective phase-only spatial light modulator; L1–L3, thin lenses with the identical focal length $f_1 = f_2 = f_3 = 25$ cm; DMD, digital micro-mirror device; camera, CCD camera. (a) Holograms for customizing PCBs loaded onto the SLM. (b) Double-hole screen loaded onto the DMD.

where F_T denotes a Fourier transform. $C_n(v)$ is a complex random function, whose real and imaginary parts follow the identical normal distributions. Detailed procedures for obtaining the random electric field are provided in Ref. [30]. In the y-direction, the electric field is supposed to be uniform, and we have $E(y) \propto 1$. To encode a complex random electric field into a hologram grating, we adopt the complex amplitude modulation encoding algorithm [31]. The SLM phase is suggested by the following:

$$\phi_{SLM}(x, y) = A_m \sin\{Arg[E(x)] + 2\pi f_x x\}. \tag{11}$$

Here A_m is attained through numerical inversion: $J_1(A_m) = |E(x)|$, where J_1 characterizes a Bessel function of the first kind and first order. "sin" denotes a sine function, and we adopt "Arg" to attain the phase of $E(x)$. f_x is the frequency of the grating, determining the location of the first-order diffraction light beam.

The beam reflected by the SLM and a beam splitter passes through a modified $4f$ optical imaging system, which comprises two identical lenses and an iris. The iris is used to select the positive or negative first diffraction order. The electric field of the beams transmitted by the order forms our desired signal. By refreshing the complex random function $C_n(v)$ to update the hologram gratings, we generate a speckle ensemble. Due to the ergodic nature of these speckles, we can synthesize the desired PCBs through the incoherent superposition of all speckles, as previously described. The produced beams then illuminate the digital micro-mirror device (DMD), on which the double-hole plate is loaded. Given that the illumination source follows the Schell-model type, its DOC depends only on the coordinate difference, rather than the specific coordinates of the points (as described in Eq. (1)). This feature obviates the need to calibrate for any lateral offset of the two pinholes, significantly simplifying our experimental procedure.

The modulated beams are focused by a thin lens and arrive at its rear focal plane. We use the CCD camera to capture the beam interference fringes. The relevant parameters are set and measured as $\alpha = 0.1$ mm and $\sigma_0 = 2$ mm, respectively. The theoretical and experimental results are exhibited in the left and right panels of Fig. 4. We factorized two numbers, $d = 77$ and 103. For $d = 77$, we tested the trial numbers $p = 6$, 7, and 8. As shown in Figs. 4(a) and 4(b), only the visibility of the true factor $p = 7$ reaches 1 in theory and 0.97 in the experiment. Similarly, for $d = 103$, only the visibility of the true factor $p = 103$ reaches 1 in theory and 0.96 in the experiment, as shown in Figs. 4(c) and 4(d). To provide further details, the experimental results of the fringe visibility for various trial factors p are presented in Fig. 5. The visibilities of the true factors of the numbers being factorized reach or approach 1, while all non-factors are suppressed below the threshold value $1/\sqrt{2}$, marked by the solid red line. The vertical lengths of the error bars indicate the absolute value of the difference between the experimental and theoretical results. The slight differences are mainly due to the deviations in the coherent width, which originally stem from the limited pixel size in SLM and DMD. Overall, Figs. 4 and 5 conspicuously demonstrate that the experimental results are in excellent agreement with the theory, thereby validating our protocol.

To summarize, we have established the relationship between incomplete Gauss sums of the number theory and the DOC of speckled light beams in the transverse plane of a Young's type double-pinhole experiment. The number to be factorized is represented by the distance between the two pinholes, and the

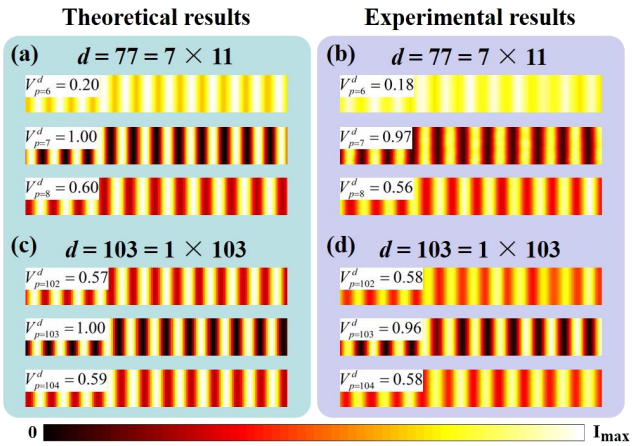

Fig. 4. Theoretical (left panel) and experimental (right panel) results of the interference fringes in the back focal plane of the thin lens. (a) and (b) show the results for $d = 77$, while (c) and (d) show the results for $d = 103$. The fringe visibilities for the trial numbers p are presented in the top left corner of each subplot. The parameters M are set to 5 and 7 for the numbers 77 and 103, respectively.

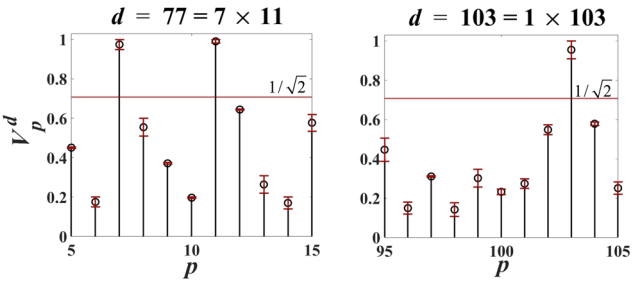

Fig. 5. Experimental fringe visibility for various trial factors p, with the numbers d to be factored set to (a) $d = 77 = 7 \times 11$ and (b) $d = 103 = 1 \times 103$. All factors and non-factors are distinctly distinguished by the threshold value $1/\sqrt{2}$, indicated by the solid red lines. The parameters M are set to 5 and 7 for the numbers 77 and 103, respectively. The vertical lengths of the error bars characterize the absolute differences between the experimental and theoretical results.

trial factor is embedded into the DOC of the field of illuminating beams. We can distinguish factors from non-factors solely via the visibility of the interference fringes. If a trial factor is a true factor, the visibility theoretically reaches 1. All non-factors are suppressed below a threshold value $1/\sqrt{2}$. Further, if we take a small value for α, it provides the possibility for factorizing a large number. The experimental results agree well with the theoretical ones, which proves the feasibility of this proposal. We believe this method has potential applications in optical encryption, information storage, and related fields.

Funding. National Key Research and Development Program of China (2019YFA0705000, 2022YFA1404800); National Natural Science Foundation of China (11974218, 12374311, 92250304); Taishan Scholar Foundation of Shandong Province (tsqn202312163); Qingchuang Science and Technology Plan of Shandong Province (2022KJ246); Natural Science Foundation of Shandong Province (ZR2023YQ006); Natural Sciences and Engineering Research Council of Canada (RGPIN-2018-05497).

Disclosures. The authors declare no conflicts of interest.

Data availability. Data underlying the results presented in this Letter are not publicly available at this time but may be obtained from the authors upon reasonable request.

REFERENCES

1. L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics* (Cambridge University Press, 1995).
2. B. Redding, M. Choma, and H. Cao, Nat. Photonics **6**, 355 (2012).
3. X. Chen, M. E. Kandel, C. Hu, *et al.*, Light: Sci. Appl. **9**, 142 (2020).
4. X. Li, Y. Wang, X. Liu, *et al.*, Appl. Phys. Lett. **124**, 214103 (2024).
5. Z. Shi, Z. Wan, Z. Zhan, *et al.*, Nat. Commun. **14**, 1869 (2023).
6. F. Gori and M. Santarsiero, Opt. Lett. **32**, 3531 (2007).
7. J. Yu, X. Zhu, F. Wang, *et al.*, Prog. Quantum Electron. **91-92**, 100486 (2023).
8. Y. Cai, Y. Chen, and F. Wang, J. Opt. Soc. Am. A **31**, 2083 (2014).
9. Q. Chen, M. Hajati, X. Liu, *et al.*, Opt. Laser Technol. **169**, 110020 (2024).
10. F. Wang, C. Liang, Y. Yuan, *et al.*, Opt. Express **22**, 23456 (2014).
11. C. Liang, G. Wu, F. Wang, *et al.*, Opt. Express **25**, 28352 (2017).
12. C. Liang, Y. E. Monfared, X. Liu, *et al.*, Chin. Opt. Lett. **19**, 052601 (2021).
13. D. Peng, Z. Huang, Y. Liu, *et al.*, PhotoniX **2**, 6 (2021).
14. Y. Liu, Y. Chen, F. Wang, *et al.*, Opto-Electron. Adv. **4**, 210027 (2021).
15. X. Liu, S. A. Ponomarenko, F. Wang, *et al.*, "Incoherent mode division multiplexing for high-security information encryption," arXiv (2023).
16. Y. Liu, X. Zhang, Z. Dong, *et al.*, Phys. Rev. Appl. **17**, 024043 (2022).
17. H. Larocque, A. D'Errico, M. F. Ferrer-Garcia, *et al.*, Nat. Commun. **11**, 5119 (2020).
18. L. Kong, W. Zhang, P. Li, *et al.*, Nat. Commun. **13**, 2705 (2022).
19. X. Lin, Y. Rivenson, N. T. Yardimci, *et al.*, Science **361**, 1004 (2018).
20. M. Sonka, V. Hlavac, and R. Boyle, *Image Processing, Analysis, and Machine Vision* (Springer, 1993).
21. H. L. Li, S. C. Fang, B. M. T. Lin, *et al.*, Light: Sci. Appl. **12**, 32 (2023).
22. G. Mussardo, A. Trombettoni, and Z. Zhang, Phys. Rev. Lett. **125**, 240603 (2020).
23. M. Štefaňák, W. Merkel, and W. P. Schleich, New J. Phys. **9**, 370 (2022).
24. K. Pelka, J. Graf, T. Mehringer, *et al.*, Opt. Express **26**, 15009 (2018).
25. M. Sadgrove, S. Kumar, and K. Nakagawa, Phys. Rev. Lett. **101**, 180502 (2008).
26. M. Mehring, K. Müller, I. Sh. Averbukh, *et al.*, Phys. Rev. Lett. **98**, 120502 (2007).
27. D. Bigourd, B. Chatel, W. P. Schleich, *et al.*, Phys. Rev. Lett. **100**, 030202 (2008).
28. X. Liu, C. Liang, Y. Cai, *et al.*, Phys. Rev. Appl. **20**, L021004 (2023).
29. X. Li, X. Liu, Q. Wu, *et al.*, APL Photonics **9**, 046107 (2024).
30. P. Ma, B. Kacerovská, R. Khosravi, *et al.*, Appl. Sci. **9**, 2048 (2019).
31. C. Rosales-Guzmán and A. Forbes, *How to Shape Light with Spatial Light Modulators* (SPIE, 2017).