Factorization of Numbers with the temporal Talbot effect: Optical implementation by a sequence of shaped ultrashort pulses

Damien Bigourd\textsuperscript{1}, Béatrice Chatel\textsuperscript{1,*}, Wolfgang P. Schleich\textsuperscript{2} and Bertrand Girard\textsuperscript{1,*}

\textsuperscript{1}\textsuperscript{*} Laboratoire de Collisions, Agrégats, Réactivité (UMR 5589, CNRS - Université de Toulouse, UPS), IRSAMC, Toulouse, France

\textsuperscript{2} Institut für Quantenphysik, Universität Ulm, Albert-Einstein-Allee 11, D-89081 Ulm, Germany

(Dated: February 1, 2008)

We report on the successful operation of an analogue computer designed to factor numbers. Our device relies solely on the interference of classical light and brings together the field of ultrashort laser pulses with number theory. Indeed, the frequency component of the electric field corresponding to a sequence of appropriately shaped femtosecond pulses is determined by a Gauss sum which allows us to find the factors of a number.

PACS numbers: 02.10De, 42.65Re, 42.79Kr

In 1836 Henry Fox Talbot used "a magnifying glass of considerable power" \cite{1} to investigate the interference pattern of light emerging from a diffraction grating produced by Joseph Fraunhofer. Talbot noticed "a curious effect": the interference patterns in planes parallel to the grating repeated themselves periodically as the distance between the plane and the grating increased. Almost fifty years later this self-imaging effect was rediscovered and explained by Lord Rayleigh \cite{2}. Today the Talbot effect was rediscovered fifty years later this self-imaging effect was rediscovered and explained by Lord Rayleigh \cite{2}. T oday the T albot ef-...
The experimental data indicated by black dots are compared with the expected values $|A^M_N(l)|^2$ depicted by crosses and the agreement is very good, particularly for the factors whose Gauss sum comes out very clearly. The experimental contrast is in general smaller than expected. This reduction could be due to several experimental limitations: (i) Our shaper is pixellated in...
the spectral domain and therefore introduces temporal replica. These replica are separated by 35 ps and are particularly broad and weak due to the nonlinear dispersion in the mask plane \[23\] \[24\] which was carefully calibrated. This time window of 35 ps is restricted down to 28 ps by the effect of the gaussian envelope due to the spatial beam profile in the mask plane \[22\] \[23\] \[24\]. Its consequences are limited here by working on only a fraction (3 to 7 ps) of the shaping window. (ii) Another consequence of pixellation is the hole in amplitude associated to large phase steps between consecutive pixels \[24\] which may induce small distortions as compared to the ideal transmission \(H_0(\omega)\). (iii) The main limitation to the extinction ratio (currently of 20 dB) is due to the gaps between pixels in the LCD (3% of the pixel width) adding a non programmable pulse at \(t = 0\), which participates also to this loss of contrast. This contribution is difficult to compensate and produces undesired interferences with the pulse train \[22\]. (iv) Finally the resolutions of both pulse shaper and spectrometer limit the ultimate contrast which can be achieved. Both are carefully calibrated following the procedure described in \[22\].

A key issue in the efficiency and reliability of this scheme is the choice of the truncation parameter \(M\) of the Gauss sum. This question is closely related to the phenomenon of ghosts factors \[26\]. Indeed, for certain integer arguments \(l\), the Gauss sum can take values close to unity even when \(l\) is not a factor of \(N\). Ghosts can be suppressed \[26\] below the threshold of \(1/\sqrt{2}\) by choosing \(M \approx 0.7 \sqrt{N}\).

The example \(N = 19043 = p(p + 2)\) with \(p = 137\) is perfectly suited to test the predictions of Ref. \[26\] concerning ghost factors. In this case, \(N\) consists of the product of twin primes which are approximately equal and of the order of \(\sqrt{N} \approx 137.996\). In this way we can test our method at the upper boundary \(\sqrt{N}\) of our set of trial factors. For this purpose we first note that for any integer number \(N\) consisting of the product of twin primes the elementary relation \(N = p(p + 2) = (p + 1)^2 - 1\) yields the approximation \(p + 1 \approx \sqrt{N}\) together with the decomposition \(N/(p + 1) = (p + 1) - 1/(p + 1)\). As a result the truncated Gauss sum reduces to

\[
A_{l=0}^{\text{trunc}}(p+1) = \frac{1}{M+1} \sum_{m=0}^{M} \exp\left(-2\pi i \frac{m^2}{p+1}\right)
\]

Since \(1 \ll M\) and \(1 \ll (p + 1)\) we can approximate this sum by a Fresnel integral which yields \[24\] the scaling \(M \propto \sqrt{p + 1} \approx \sqrt{N}\).

In Fig. 3, we display by crosses the exact sum \(\left|A_{19043}^{(138)}(M)\right|^2\) as a function of \(M\). We note the slow decay and the oscillations due to the Fresnel integral. Solid dots representing our measurements follow this behavior. The general trend is well reproduced. However the experimental uncertainties do not allow to reproduce fully the expected oscillations. Moreover, we find the predicted threshold \(M \approx 0.7 \sqrt{19043} \approx 8\). In the insert, an experimental realization of factoring \(N = 19043 = 137 \times 139\) with a 9 pulses sequence is shown as an example. Theory and experiments are also in excellent agreement.

Our work clearly demonstrates that we can use shaped femtosecond pulses to implement Gauss sums and factor numbers. However, many generalizations offer themselves: (i) So far we have only made use of the phases \(\theta_m\) in the frequency representation Eq. \[24\] of the electric field. The second contribution to the phase, that is the product \(\tau_m \Delta \omega\) did not enter since we set \(\Delta \omega = 0\). (ii) Since we have only the single parameter \(\theta_m\) at our disposal, the number \(N\) to be factored and the trial factor \(l\) cannot be varied independently. (iii) Finally we have pursued a sequential rather than a parallel approach. Indeed, we have only used a single spectral component.

The activation of the so far unused phase \(\tau_m \Delta \omega\) solves all three problems. Since now we have two parameters we can encode \(N\) in \(\tau_m\) and \(l\) in \(\Delta \omega\). By recording the complete spectrum we achieve a massive parallelism.

The choice of \(\theta_m = 0\) and \(\tau_m = 2\pi m^2 N \alpha\) with the numerical constant \(\alpha\) also yields the Gauss sum \(A_N^{(M)}\) and illustrates this new approach. Here the spacing between pulses increases quadratically and \(l\) is inversely proportional to \(\Delta \omega\) such that a single spectrum directly contains all the information.

However, some remaining difficulties need to be overcome: (i) The Gaussian shape of the spectral profile leads to ponderations in the Gauss terms which have to be taken into account. (ii) The variation of \(l\) between 2 and \(\sqrt{N}\) i. e. on several orders of magnitudes puts severe constraints on the spectral resolution necessary to carry the experiment. (iii) Finally, the number of pulses is limited by \(\sqrt{T_w/3\tau_L} \approx 10\) with our present set-up.

The quadratic spacing of the pulses required in the above approach might represent a severe problem. The
might be an interesting way around, since it also allows us to factor numbers. In contrast to the truncated Gauss sum $A_N^M$, which only needs to be recorded at integer arguments, the sum $S_N$ relies on a continuous argument. Here we need the complete spectrum. In return $S_N$ displays interesting scaling properties which enable us to use the interference pattern for $N$ to factor the number $N'$ by rescaling the frequency axis [27].

We conclude by noting that our implementation is closely connected to the Talbot effect [28]. Indeed, an initial wave function consisting of an array of sharp maxima located at integer multiples $m$ of a period $d$ accumulates quadratic phases in its time evolution. On first sight this behavior is surprising since the energy spectrum of the harmonic oscillator is linear. However, due to the quadratic dependence of the energy on the position, the maxima at $md$ translate into quadratic phases $(md)^2$. A similar behavior was noted [29] in the quantum carpets woven by a wave packet moving in a harmonic oscillator and consisting only on energy eigenstates with quadratic quantum numbers.

Although the electromagnetic field represents a harmonic oscillator it might be easier to realize a factorization scheme based on this effect using a mechanical oscillator. A laser cooled atom into an optical lattice and prepared in its motional ground state offers a possible realization. An absorption grating [30] produced by a standing light wave can prepare the periodic array of narrow wave packets. Moreover, the coupling of the center-of-mass motion to a quantized standing light field [31] can introduce entanglement into the Talbot effect making factorization with entangled Gauss sums viable.

In summary, we have factorized numbers through the implementation of a Gauss sum with optical interferences produced by a sequence of shaped short laser pulses. This work opens the route to further promising developments based on the wide flexibility offered by optical interferences.

E. Baynard and S. Faaure are acknowledged for their technical help. We enjoyed fruitful discussions with G.S. Agarwal, A. Mommayrant and I. Walmsley. This work has been supported by the Agence Nationale de la Recherche (Contract ANR - 06-BLAN-0004) and the Del Duca foundation. WPS is grateful to the Max Planck Society and the A. von Humboldt Stifung for their support. Moreover, he acknowledges the support by the Ministerium für Wissenschaft und Kunst, Baden-Württemberg and the Landesstiftung Baden-Württemberg in the framework of the Quantum Information Highway A8 and the Center for Quantum Engineering.

* Member of the Institut Universitaire de France
** corresponding author: beatrice@irsamc.ups-tlse.fr

[1] H. F. Talbot, Philos. Mag. 9, 401 (1836).
[2] L. Rayleigh, Philos. Mag. 11, 196 (1881).
[3] M. J. Berry et al., Physics World 14, 39 (2001).
[4] K. Patorski, in Progress in Optics, edited by E. Wolf (North-Holland, Amsterdam, 1989), vol. 28, p. 1.
[5] B. Brezger et al., Phys. Rev. Lett. 88, 100404 (2002).
[6] S. Nowak et al., Opt. Lett. 22, 1430 (1997).
[7] N. Koblitz, A Course in Number Theory and Cryptography (Springer, New York, 1994).
[8] L. M. K. Vandersypen et al., Nature 414, 883 (2001).
[9] W. Merkel et al., Fortschr. Phys. 54, 856 (2006); Int. J. Mod. Phys. B 20, 1893 (2006); Phys. Rev. A 76, 033417, (2007). J. Clausner et al., Phys. Rev. A 53, 4587 (1996).
[10] W. Harter, Phys. Rev. A 64, 012312 (2001).
[11] M. Mehring et al., Phys. Rev. Lett. 98, 120502 (2007).
[12] T. S. Mahesh et al., Phys. Rev. A 75, 062303 (2007).
[13] M. Gomis et al., quant-ph/0709.1424v1 (2007).
[14] A. M. Weiner, Rev. Sci. Instr. 71, 1929 (2000).
[15] D. Meshulach et al., Nature 396, 239 (1998); N. Dudovich et al., Phys. Rev. Lett. 86, 47 (2001); J. Degert et al., Phys. Rev. Lett. 89, 203003 (2002); B. Chatel et al., Phys. Rev. A 68, 041402 (2003); A. Mommayrant et al., Phys. Rev. Lett. 96, 103002 (2006); Opt. Lett. 31, 410 (2006); Opt. Commun. 264, 256 (2006). A. Assion et al., Science 282, 919 (1998). C. Daniel et al., Science 299, 536 (2003). K. Ohmori et al., Phys. Rev. Lett. 91, 243003 (2003); 96, 093002 (2006). H. Katsuki et al., Science 311, 1589 (2006).
[16] J. Ahn et al., Science 287, 463 (2000).
[17] Z. Zheng et al., Opt. Lett. 25, 984 (2000).
[18] Z. Amitay et al., Chem. Phys. Lett. 359, 8 (2002).
[19] N. Bhattacharya et al., Phys. Rev. Lett. 88, 137901 (2002).
[20] E. Brainis et al., Phys. Rev. Lett. 90, 157901 (2003).
[21] P. Londero et al., Phys. Rev. A 69, 010302 (2004).
[22] For an instructive explanation of the temporal Talbot effect see F. Mitschke and U. Morgner, Optics and Photonics News 9 (6), 45 (1998).
[23] A. Mommayrant et al., Rev. Sci. Instr. 75, 2668 (2004).
[24] H. Wang et al., IEEE J. Sel. Top. Quantum Electron. 7, 718 (2001).
[25] J. Vaughan et al., Optics Express 14, 1314 (2006).
[26] M. Wohlenhein et al., Appl. Phys. B 79, 435 (2004).
[27] M. Štefanák et al., New J. Phys. 9 370 (2007).
[28] W. Merkel et al., Phys. Rev. A in preparation (2007).
[29] G. S. Agarwal, Phys. Rev. B 203030 (1999).
[30] O. M. Friesch et al., New J. Phys. 2, 1 (2000).
[31] For an introduction to atom optics in quantized light fields see Chapt. 20 in: W. P. Schleich, Quantum optics in phase space (Wiley-VCH, Berlin, 2001).
