Factoring numbers with interfering random waves

Sébastien J. Weber, Béatrice Chatel, Bertrand Girard

Factoring numbers with interfering random waves

Sébastien Weber, Béatrice Chatel* and Bertrand Girard**

Laboratoire Collisions, Agrégats, Réactivité - IRSAMC-(CNRS, Université de Toulouse, UPS)- France

PACS 42.65.Re – Ultrafast processes; optical pulse generation and pulse compression
PACS 02.10.De – Algebraic structures and number theory
PACS 42.79.Kr – Display devices, liquid-crystal devices

Abstract. - We report on a new implementation of the factorisation of numbers using Gauss sums which improves tremendously the efficiency to eliminate all "ghost" factors. We show that by choosing randomly the terms in the Gauss sum, the required number of terms varies as $\ln N$ instead of $\sqrt[4]{N}$. As an illustration, we present experimental results obtained by interfering thirty ultrashort laser pulses where we factorise $1,340,333,404,807$. This new approach is totally general and can be implemented for all the experiments based on the Gauss sum.

Introduction. – Factorisation of numbers has attracted a wide interest in pure arithmetics as well as for applications, particularly because it is much easier to multiply two large prime numbers than doing the reverse operation [1]. This difficulty is at the basis of encryption systems. A competition exists permanently to promote new algorithms in order to factorize large numbers. For instance, J. Franke (Bonn's university) was able to factorize the RSA-640 (193 digits) in 5 months with 80 processors. Besides improving mathematical algorithms, several physical approaches to factorisation have been introduced [2,3]. In particular, quantum systems offer strong promises due to the large-scale parallelism offered by the use of entangled states. Indeed, the Shor's factorisation algorithm is one of the two pillars of quantum computing [2]. Despite the difficulties to manipulate the required large number of qubits [4] and in particular to preserve them from decoherence [5–7], the factorisation of 15 has been achieved [3]. However, large scale demonstrations based on quantum algorithms are still not in view.

Recently a very different approach based on Gauss Sums has been proposed theoretically [8, 9] and experimentally implemented by several groups in NMR [10, 11], with cold atoms [12] and ultrashort pulses [13]. This method which presents strong interest as underlined by reference [14] is based on multiple-wave interferences with relative phases depending on the number N to be factorised and another integer l. These interferences reproduce the Gauss sum [15] given by:

$$\mathcal{A}_N^{(l)}(l) = \frac{1}{l}\sum_{m=0}^{l-1} \exp\left(-2\pi i m^2 \frac{N}{l}\right) \qquad (1)$$

where N is the number to be factored. The argument l scans through all integers between two and $\sqrt{N}$ for possible factors. When l is not a factor, the quadratic phases take quasi-random values (modulo 2π) and the resulting sum remains small. When l is a factor, then all the phases are multiples of 2π and the sum is equal to unity.

It has been shown [9] that in most cases only the first few terms are necessary to discriminate factors, for which the normalized Gauss sum is always equal to 1, from non-factors for which it is strictly smaller than 1. This leads to the truncated Gauss sum consisting of the first M terms :

$$\mathcal{A}_N^{(M)}(l) = \frac{1}{M}\sum_{m=0}^{M-1} \exp\left(-2\pi i m^2 \frac{N}{l}\right) \qquad (2)$$

This sequential approach has so far been used for the experimental demonstrations [10–13]. However for large numbers, "ghost" factors appear [16]. These "ghost" factors are trial numbers leading to a high value of the Gauss sum even though they are not factors. They are the main limitation for the determination of factors. They correspond to a value of l such that $\frac{N}{l} = q + \frac{k}{l} (k << l)$ where q and k are integers, for which the phase remains small for all the terms of the truncated Gauss Sum.

The proposed implementations of $\mathcal{A}_N^{(M)}$ are based on multipath interferences [9]. Each path produces one term in the Gauss sum. The difficulty is in finding a system that is experimentally accessible and in which the required phase in Eq. (2) is obtained by a simple variation of a physical parameter. So far this strict condition has not been fulfilled yet. Nevertheless, several experiments in which each phase of the Gauss sum is separately

determined have recently succeeded in demonstrating the ability of Gauss sums to factorise numbers with physical systems as mentioned above. They have achieved factorisation of the numbers 157,573 [10], 52,882,363 [11], and 263,193 [12] respectively, with up to $M = 15$ terms in the Gauss sum.

Recently our group has introduced [13] an all optical approach towards factoring numbers based on modern pulse-shaping technology [17]. The number 19,043 was factorised with $M = 9$ terms. This approach has the advantage of providing the modulus square of the Gauss sum which increases the contrast to discriminate factors from non-factors. We present here significant improvements which allow factorising considerably larger numbers. First, the pulse shaper was operated close to its technical limits in order to produce up to 30 pulses, and second we introduce a new way of truncating the Gauss sum, based on a random choice of M terms instead of choosing the first M terms. This approach is directly analogous to the Monte-Carlo method used to calculate integrals. This leads to a drastic suppression of the ghost factors. These two improvements lead to a significant increase of the largest numbers factored. Moreover, the scaling law of the number of pulses required to eliminate all "ghost" factors as a function of N is now logarithmic instead of $\sqrt[4]{N}$ [13,16].

Experimental Set-up. – The Gauss sum (Eq.2) is implemented through multiple wave interferences produced by a sequence of M ultrashort pulses generated by a high-resolution pulse shaper (HRPS) [17]. The complex spectral mask

$$H_\theta(\omega) = w_m \sum_{m=0}^{M-1} \exp\left[i\left(\theta_m + \tau_m \Delta\omega\right)\right] \tag{3}$$

is applied with the pulse shaper to modify the Fourier-transform-limited input laser pulse: $E_{out}(\omega) = H_\theta(\omega) E_{in}(\omega)$, with $\theta_m = -2\pi i m^2 \frac{N}{l}$ and $\Delta\omega = \omega - \omega_0$ (ω_0 is the carrier frequency of the input electric field). Each term of the sum in Eq. 3 is therefore produced by an ultrashort pulse delayed by τ_m and with an extra phase shift θ_m. Here we choose $T = 200\,\text{fs}$ in order to produce a sequence of well-separated pulses.

The laser system is a conventional Ti: Sapphire laser delivering 30 fs at 805 nm with 80 MHz repetition rate. The pulse shaping device is defined to avoid chromatic as well as off-axis aberrations. The 4f set-up is thus composed of one pair each of reflective gratings and cylindrical mirrors. Its active elements -two 640 pixels liquid crystal mask- are installed in the common focal plane of both mirrors. This provides high resolution pulse shaping in phase and amplitude [17]. This is used to generate the shaped pulse sequence.

The interference produced by the pulse sequence is analyzed with a high resolution spectrometer. We measure the spectral intensity at the central wavelength $\lambda_0 = 2\pi\, c/\omega_0$ and thus retrieve the Gauss sum for each l. The experiment is performed for l ranging between 2 and $\sqrt{N}$ in order to discriminate factors from non-factors.

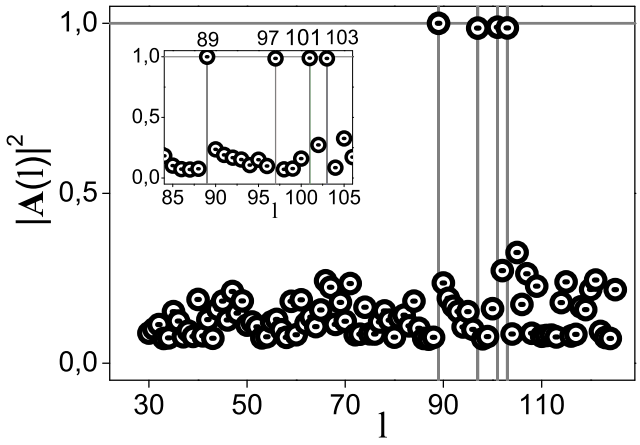

Fig. 1: Experimental factorization of $N = 89,809,099$ with $M = 30$ shaped pulses used to calculate the sequentially truncated Gauss sum. The plot shows the value of the Gauss sum as a function of l and the inset is a zoom around the factors (pointed by vertical lines).

Results and discussions. – In Fig. 1 we display the results of our optical implementation of the factorization scheme based on the Gauss sum for $N = 89,809,099 = 89 \times 97 \times 101 \times 103$ obtained with a sequence of $M = 30$ pulses. The contrast between factors and non-factors is excellent.

Two other examples are displayed in Fig. (2-a) and (2-b) ($N = 1,340,333,404,807 = 11003 \times 11027 \times 11047$) (Fig. 2-b is a zoom around the factors), and Fig. (3-a) ($N = 2,499,200,063 = 49,991 \times 49,993$) obtained with $M = 30$ shaped pulses. Here, the limits of this approach are clearly seen. In both cases "ghost" factors remain. The truncated Gauss sum has insufficient terms to lead to destructive interferences and eliminate these factors. These ghosts factors are located near the two twin prime factors (Fig. (3-a)) or worst spread on the whole interval $[2, \sqrt{N}]$ (Fig. (2-a)) even no ghost factors appear close to the real factors. It can be easily demonstrated [13,16] that the required number of pulses to eliminate them scales as $\sqrt[4]{N}$. In the last example ($N = 2,499,200,063$), this gives $M \simeq 220$. Indeed, for the number $(p+1)$ lying between two twin prime factors p and $p+2$, the residual phase is $\theta_m = -2\pi m^2/(p+1)$. Hence, for $m^2 \ll (p+1) \simeq \sqrt{N}$, all the phases are close to 0. Therefore the Gauss sum adds vectors pointing in the same direction that interfere constructively. This property is illustrated in Fig. 4 which displays the phase values of the M first factors, for $M =$ 30, 100 and 200 (from the inner to the last but one outer circle).

These examples show that, although it has demonstrated to be quite efficient, truncating the Gauss sum

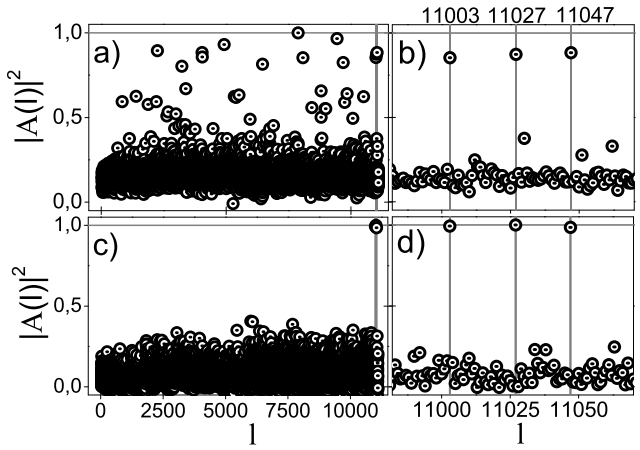

Fig. 2: Experimental factorization of $N = 1,340,333,404,807 = 11003 \times 11027 \times 11047$ with $M = 30$ shaped pulses: (a) is obtained with a sequential truncated Gauss Sum, (b) is the zoom around the factors. (c) is made with random choice of terms, (d) is the zoom. Vertical lines indicate the different factors of N.

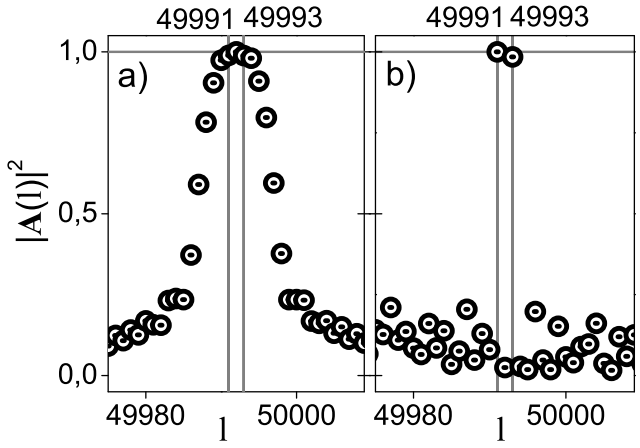

Fig. 3: Experimental factorization of $N = 2,499,200,063 = 49,991 \times 49,993$ with $M = 30$ shaped pulses. (a) with sequential terms and (b) with random choice of terms. Vertical lines point the factors of N.

to its first M terms is certainly not the best strategy to estimate this sum. Here we investigate an alternative way consisting of choosing randomly M terms to achieve a better estimate of the Gauss sum:

$$\mathcal{A}'^{(M)}_N(l) = \frac{1}{M}\sum_{m=0}^{M-1} \exp\left(-2\pi i \mu(m)^2 \frac{N}{l}\right) \tag{4}$$

where $\mu(m)$ is an integer randomly chosen in the interval $[0, l-1]$. In this case, the phases of the terms used to calculate $\mathcal{A}'^{(M)}_N(l)$ are distributed quasi-homogeneously in the $[0, 2\pi]$ interval as can be seen in the example plotted in Fig. 4 (circles). This method is applied to the two numbers already studied with the sequential truncation

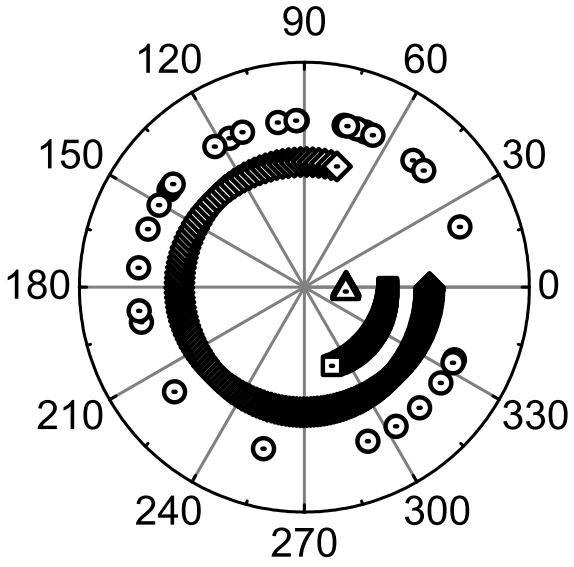

Fig. 4: Phases (in degree) of the different terms in the Gauss sum for the ghost factor $l = 49,992$ of the number $N = 49,991 \times 49,993$. Different radii are used for clarity. From the inner to the outer circle : triangles are used for the sum with $M = 30$ consecutive terms, squares for $M = 100$ consecutive terms, diamonds for $M = 200$ consecutive terms, circles for 30 terms randomly chosen in the interval $[0, l-1]$.

for which many ghost factors have been encountered. The results are presented on Fig. 2-c,d and 3-b. All the ghosts factors which are close to the real factors (Fig. 3) as well as those which are spread on the whole interval (Fig. 2) have been clearly eliminated. The same number of pulses (30) has been used for both the sequential and the random methods.

This new approach of estimating the Gauss sum is extremely powerful and opens possibilities to factorize larger numbers. The number of pulses required to find the factors while eliminating all the ghosts can be evaluated with a simple model based on the random walk. We assume that for non-factors, the phases of the M terms in the Gauss sum $\mathcal{A}'^{(M)}_N(l)$ are homogeneously distributed in the $[0, 2\pi]$ interval. We can write

$$\left|\mathcal{A}'^{(M)}_N(l)\right| = \frac{L_M}{M} \tag{5}$$

where L_M is the length of the random walk after M steps of length 1. In the large numbers limit, the probability distribution of the random walk length is given by

$$P(L_M(M\to\infty)) = \frac{2\,L_M}{M(1-e^{-M})}\, e^{-\frac{L_M^2}{M}} \simeq \frac{2\,L_M}{M}\, e^{-\frac{L_M^2}{M}} \tag{6}$$

with an average value of $\sqrt{\langle L_M^2\rangle} = \sqrt{M}$

We find a ghost when $\left|\mathcal{A}'^{(M)}_N(l)\right|^2 > S$ where $S < 1$ is the threshold value, depending on the signal to noise ratio of the experiment, for which the experimental estimate

of the Gauss sum is clearly different from one, so that the trial number l is unambiguously a non-factor. The probability of finding a ghost is therefore given by

$$\begin{aligned} P_{ghost} &= P\left(\left|\mathcal{A}'^{(M)}_N(l)\right| > \sqrt{S}\right) \\ &= \int_{\sqrt{S}\,M}^{M} P(L)\,dL \simeq e^{-SM} \end{aligned} \tag{7}$$

We can consider that all ghost factors are eliminated if the probability of finding a ghost within the $\sqrt{N}$ numbers tested is much smaller than one:

$$P_{ghost}\sqrt{N} = \epsilon \ll 1 \tag{8}$$

This gives

$$M = -\frac{\ln \epsilon}{S} + \frac{\ln N}{2S} \tag{9}$$

As an example, for very conservative numbers such as $\epsilon = 0.01$, $S = 0.5$, and the number $N = 2,499,200,063$, one gets $M = 31$ (which is already in the large numbers limit) in good agreement with our experimental findings.

If technical limits prevent using a larger number of pulses (or terms in the Gauss sum), then several sequences of M random pulses could be used to improve the discrimination between ghosts and real factors. In this case, the results of several sequences would be combined incoherently, so that p sequences of M pulses would be equivalent to a single sequence of $\sqrt{p}\,M$ pulses. Since these extended experiments could be applied only to a small fraction of numbers, the penalty cost in terms of total duration of the experiment would be very small.

Conclusion. – The use of pulse shapers to produce multiple-pulse interferences, together with a random choice of the term, opens new opportunities in factorising numbers through the Gauss sum. Other variants of the Gauss sums are also currently investigated theoretically [18] or very recently experimentally [19]. These new approaches should now be implemented with physical systems in which the phases of the terms of the Gauss sum (Eq. 2) result directly from a physical process. Several have been considered [8, 9, 20] and are currently investigated. Parallel approaches in which all trial numbers are tested at once [13] will also improve tremendously the efficiency of these methods.

Here we have demonstrated the tremendous improvement introduced by the term's random choice in the Gauss sum. Since random processes are inherent to quantum mechanics, starting from entangled states could be a way to implement the term's random choice in the Gauss sum. This could be a significant milestone towards the design of a physical process able to implement directly the term's phases of the Gauss sum (Eq. 2).

* * *

E. Baynard and S. Faure are acknowledged for their technical help. We enjoyed fruitful discussions with W.P. Schleich and C. Sire. This work has been supported by the Agence Nationale de la Recherche (Contract ANR - 06-BLAN-0004) and the Del Duca foundation.

* *corresponding author: Beatrice@irsamc.ups-tlse.fr*

** Member of the Institut Universitaire de France

REFERENCES

REFERENCES

[1] Koblitz N., *A Course in Number Theory and Cryptography* (Springer, New York) 1994.

[2] Ekert A. and Jozsa R., *Reviews of Modern Physics* , **68** (1996) 733.

[3] Vandersypen L. M. K., Steffen M., Breyta G., Yannoni C. S., Sherwood M. H. and Chuang I. L., *Nature* , **414** (2001) 883.

[4] Haffner H., Hansel W., Roos C. F., Benhelm J., Chek-al kar D., Chwalla M., Korber T., Rapol U. D., Riebe M., Schmidt P. O., Becher C., Guhne O., Dur W. and Blatt R., *Nature* , **438** (2005) 643.

[5] Brune M., Hagley E., Dreyer J., Maitre X., Maali A., Wunderlich C., Raimond J. M. and Haroche S., *Phys. Rev. Lett.* , **77** (1996) 4887.

[6] Almeida M. P., de Melo F., Hor-Meyll M., Salles A., Walborn S. P., Ribeiro P. H. S. and Davidovich L., *Science* , **316** (2007) 579.

[7] Gleyzes S., Kuhr S., Guerlin C., Bernu J., Deleglise S., Busk Hoff U., Brune M., Raimond J.-M. and Haroche S., *Nature* , **446** (2007) 297.

[8] Merkel W., Crasser O., Haug F., Lutz E., Mack H., Freyberger M., Schleich W. P., Sh. Averbukh I., Bienert M., Girard B., Maier H. and Paulus G. G., *Int. J. Mod. Phys. B* , **20** (2006) 1893.

[9] Merkel W., Sh. Averbukh I., Girard B., Paulus G. G. and Schleich W. P., *Fortschr. Phys.* , **54** (2006) 856.

[10] Mehring M., Mueller K., Sh. Averbukh I., Merkel W. and Schleich W. P., *Phys. Rev. Lett.* , **98** (2007) 120502.

[11] Mahesh T. S., Rajendran N., Peng X. and Suter D., *Phys. Rev. A* , **75** (2007) 062303.

[12] Gilowski M., Wendrich T., Muller T., Jentsch C., Ertmer W., Rasel E. M. and Schleich W. P., *Phys. Rev. Lett.* , **100** (2008) 030201.

[13] Bigourd D., Chatel B., Girard B. and Schleich W. P., *Phys. Rev. Lett.* , **100** (2008) 030202.

[14] Zubairy M. S., *Science* , **316** (2007) 554.

[15] Maier H. and Schleich W. P., *Prime numbers 101: A primer on Number Theory* (Wiley-VCH, New-York) 2007.

[16] Štefaňák M., Merkel W., Schleich W. P., Haase D. and Maier H., *New J. Phys.* , **9** (2007) 370.

[17] Monmayrant A. and Chatel B., *Rev. Sci. Instr.* , **75** (2004) 2668.

[18] Stefanak M., Haase D., Merkel W., Zubairy M. S. and Schleich W. P., *in preparation* , (2007) .
[19] Suter D., *Communication to 37th winter colloquium on Physics of Quantum Electronics* , (2008) .
[20] Merkel W., Schleich W. P., Sh. Averbukh I. and Girard B., *in preparation* , (2008) .