Factorization with Gauss sums: scaling properties of ghost factors

M Štefaňák\textsuperscript{1,2}, W Merkel\textsuperscript{2}, W P Schleich\textsuperscript{2}, D Haase\textsuperscript{3} and H Maier\textsuperscript{3}

\textsuperscript{1} Department of Physics, FJFI ČVUT v Praze, Břehová 7, 115 19 Praha
\textsuperscript{1} - Staré Město, Czech Republic
\textsuperscript{2} Institut für Quantenphysik, Universität Ulm, Albert-Einstein-Allee 11, D-89081 Ulm, Germany
\textsuperscript{3} Institut für Zahlentheorie und Wahrscheinlichkeitstheorie, Universität Ulm, Helmholtzstrasse 18, D-89069 Ulm, Germany

E-mail: martin.stefanak@uni-ulm.de

\textit{New Journal of Physics} 9 (2007) 370

Received 13 August 2007
Published 12 October 2007
Online at \url{http://www.njp.org/}
doi:10.1088/1367-2630/9/10/370

Abstract. Recent experiments have shown that truncated Gauss sums allow us to find the factors of an integer $N$. This method relies on the fact that for a factor the absolute value of the Gauss sum is unity. However, for every integer $N$ there exist integers which are not factors, but where the Gauss sum reaches a value which is arbitrarily close to unity. In order to distinguish such ghost factors from real factors we need to amplify this difference. We show that a proper choice of the truncation parameter of the Gauss sum suppresses the ghost factors below a threshold value. We derive the scaling law of the truncation parameter on the number to be factored. Moreover, we show that this scaling law is also necessary for the success of our factorization scheme, even if we relax the threshold or allow limited error tolerance.
1. **Introduction**

Gauss sums [1]–[3] play an important role in many phenomena of physics ranging from the Talbot effect of classical optics [4] via the curlicues emerging in the context of the semi-classical limit of quantum mechanics [5, 6], fractional revivals [7, 8] and quantum carpets [9] to Josephson junctions [10]. Moreover, they build a bridge to number theory, especially to the topic of factorization. Indeed, they can be viewed as a discrimination function of factors versus non-factors for a given natural number. The essential tool of this factorization scheme [11] is the periodicity of the Gauss sum.

Usually Gauss sums extend over some period which leads to the *complete Gauss sum*. However, recent experiments based on NMR [12, 13], cold atoms [14] and ultra-short pulses [15] have demonstrated the possibility of factoring numbers using *truncated Gauss sums* where the number of terms in the sum is much smaller than the period. Therefore, factorization with truncated Gauss sums offers enormous experimental advantages since the number of terms is limited by the decoherence time of the system. In the present paper, we address the dependence of the number of terms needed in order to factor a given number. In particular, we find an optimal number of terms which preserves the discrimination property and at the same time minimizes the number of terms in the sum.

In order to factor a number $N$ we analyze the *signal*, i.e. the absolute value of the Gauss sum, for integer arguments $\ell = 1, \ldots, \left\lfloor \sqrt{N} \right\rfloor$. We call the graphical representation of the signal data the *factorization interference pattern*. In order to gain information about the factors of $N$ we analyze the factorization interference pattern: whenever the argument $\ell$ corresponds to a factor of $N$ we observe the maximal signal value of unity. For most non-factor arguments this signal value is significantly below unity. However, for *ghost factors* we observe signal values close to unity even though these arguments do not correspond to an actual factor of $N$. Thus ghost factors spoil the discrimination of factors from non-factors in such a factorization interference pattern. Fortunately, ghost factors can be suppressed below a given threshold.
by extending the upper limit of the summation in the Gauss sum. This goal of completely suppressing all ghost factors provides us with an upper bound on the truncation parameter. This upper bound represents a sufficient condition for the success of our Gauss sum factorization scheme. The analysis of the number of ghost factors evaluated by the ghost factor counting function $g(N, M)$, which depends on the number to be factorized $N$ and the truncation parameter $M$, reveals that this upper bound on the truncation parameter is also a necessary condition for the success of our Gauss sum factorization scheme.

The paper is organized as follows: we first briefly review in section 2 the central idea of the factorization scheme based on the Gauss sums. In particular, we introduce complete and truncated Gauss sums and compare the resources necessary to factor a given number $N$. We find the first traces of ghost factors in the factorization interference pattern based on the truncated Gauss sum.

Since the truncation of the Gauss sum weakens the discrimination of the factors from non-factors, we dedicate section 3 to deriving a deeper understanding of this feature. We find four distinct classes of arguments $\ell$ which result in utterly different behaviors of the truncated Gauss sum. Rewriting the truncated Gauss sum in terms of the curlicue sum allows us to identify the class of problematic arguments—the ghost factors. Moreover, we identify a natural threshold which separates factors from non-factors. For a rigorous argument we refer to appendix A.

In section 4, we obtain an upper bound on the truncation parameter of the Gauss sum needed to suppress the signal of all ghost factors below the natural threshold. Ghost factors appear, whenever the ratio of the number to be factored and a trial factor is close to an integer. This fact allows us to replace the Gauss sum by an appropriate Fresnel integral. From this expression we find the scaling law $M \sim \sqrt[4]{N}$ for the truncation parameter $M$, which represents the sufficient condition for the success of our Gauss sum factorization scheme.

Finally, we analyze the ghost factor counting function in section 5 and show that the fourth-root law is also necessary for the success of our factorization scheme, even if we relax the threshold value or allow limited error tolerance. We conclude by presenting an outlook in section 6.

2. Factorization based on Gauss sums: appearance of ghost factors

To start our analysis we first consider the complete normalized quadratic Gauss sum

$$A_N^{(\ell-1)}(\ell) = \frac{1}{\ell} \sum_{m=0}^{\ell-1} \exp \left(2\pi i m^2 \frac{N}{\ell}\right),$$

which is frequently used in number theory. Here, $N$ is the integer to be factorized and the integer argument $\ell$ scans through all numbers from 1 to $\lfloor \sqrt{N} \rfloor$ for factors of $N$. If $\ell$ is a factor then all terms in the sum contribute with a value of unity and thus the resulting signal value $|A_N^{(\ell-1)}(\ell)|$ is one. However, for non-factor arguments the signal value is suppressed considerably as illustrated on the left in figure 1. Thus the absolute value of the Gauss sum allows one to discriminate factors from non-factors.

Factorization based on the complete Gauss sum (1) has several disadvantages. First of all, the limit of the sum depends on the trial factor $\ell$. Thus the number of terms in the sum increases
Figure 1. Influence of the truncation parameter $M$ of the incomplete Gauss sum $A_N^{(M)}(\ell)$ defined in (3) on the contrast of the factorization interference pattern for the example $N = 9624687 = 3 \times 919 \times 3491$. The left picture shows the corresponding pattern for the complete Gauss sum defined in (1) where $M = \ell - 1$. For the right picture we have truncated the Gauss sum after $M = \ln N = 16$ terms. At factors of $N$ indicated by vertical lines the Gauss sum assumes the value of unity marked by red dots. The complete Gauss sum enjoys an impressive contrast due to a suppressed signal value at all non-factors. However, the truncated Gauss sum with a relatively small number of terms also allows to discriminate factors from non-factors. However, we also observe several ghost factors marked by green dots.

with $\ell$ up to $\sqrt{N}$. Hence, to obtain a complete factorization interference pattern in total

$$\sum_{\ell=1}^{\sqrt{N}} \ell = \frac{1}{2} \sqrt{N}(\sqrt{N} - 1) \approx \frac{1}{2} N$$

(2)

terms have to be added.

In the recent experimental demonstrations [12]–[15] of our Gauss sum factorization scheme the number of terms in the sum translates directly into the number of pulses applied on to the system, or the number of interfering light fields. Due to decoherence it is favorable to use as few pulses as possible. Hence, the experiments employ a constant number $M$ of pulses for each argument $\ell$ to be tested. Thus the resulting signal is of the form of a truncated Gauss sum

$$A_N^{(M)}(\ell) = \frac{1}{M+1} \sum_{m=0}^{M} \exp \left( 2\pi i m^2 \frac{N}{\ell} \right),$$

(3)

rather than a complete Gauss sum of (1). Hence, we have to add

$$\sum_{i=1}^{\sqrt{N}} M = M \sqrt{N}$$

(4)

terms to obtain the factorization pattern with the truncated Gauss sum. With this fact in mind we now treat the number of terms in the Gauss sum as a resource for this factorization scheme.

The experiments impressively demonstrate that the truncated Gauss sums are also well suited to discriminate in the factorization interference pattern between factors and non-factors,
even though the summation range does not cover a full period. As a drawback we now find that
the signal value at non-factor arguments is not suppressed as well as in the case of the complete
Gauss sum.

In order to illustrate the effect of truncating the Gauss sum we compare in figure 1 the factorization interference patterns for the complete Gauss sum $A_N^{(\ell-1)}(\ell)$ (left) and for the truncated Gauss sum $A_N^{(M)}(\ell)$ (right). In a first guess we chose the truncation parameter $M = \ln N$ to depend logarithmically on the number to be factorized. It is remarkable that the small number $M = 16$ of terms in the truncated Gauss sum is sufficient to reveal the factors of a seven-digit number like $N = 9624687$. On the other hand we observe a number of data-points with signal values close to one (green dots), for example at the argument $\ell = 2555$. In an experiment such points might lead us to wrong conclusions in the interpretation of a factorization interference pattern. Thus, we call arguments $\ell$ resulting in such critical values of the signal ghost factors.

3. Classification of trial factors

The frequency of appearance of ghost factors is the central question of our study. Indeed, how
many terms in the truncated Gauss sum are needed in order to suppress the occurrence of
ghost factors. However, we first need to identify the class of arguments which results in ghost
factors.

Figure 1 already indicates that there are different classes of trial factors: (i) factors with
constant value of $|A_N^{(M)}(\ell)|$, (ii) typical non-factors at which already few terms $M$ are sufficient
to suppress the value of $|A_N^{(M)}(\ell)|$ considerably, (iii) ghost factors at which a larger summation
range is needed to suppress the value of $|A_N^{(M)}(\ell)|$, and (iv) threshold non-factors at which the
value of $|A_N^{(M)}(\ell)|$ cannot be suppressed by increasing $M$.

To illustrate this, we plot in figure 2 the truncated Gauss sum of (3) for $N = 9624687$
and various arguments $\ell$ characteristic for each one of the class (i)–(iv) as a function of the
truncation parameter $M$.

To which class of arguments (i)–(iv) the given $\ell$ belongs is determined by the relation
between the argument $\ell$ and the number we are factorizing $N$, namely on the value of the
fraction $2N/\ell$ which enters the Gauss sum (3). Indeed, for the number $N = 9624687$ and the
arguments $\ell$ used in figure 2 we find the following: (i) for a factor $\ell = 919$ the fraction $2N/\ell$ is
an even integer, (ii) for a typical non-factor $\ell = 14$ the fraction $2N/\ell$ is close to an odd integer,
(iii) for a ghost factor $\ell = 2555$ the fraction $2N/\ell$ is close to an even integer and (iv) for a
threshold non-factor $\ell = 12$ the fraction $2N/\ell$ is an even integer plus one-half.

Thus, we see that the class of $\ell$ is given by the fractional part of the fraction $2N/\ell$. Hence,
in order to bring out these classes most clearly, we represent the truncated Gauss sum (3) in
a different form. For any argument $\ell$ we decompose the fraction $2N/\ell$ into the closest even
integer $2k$ and the fractional part $\rho(N, \ell) = p/q$ with $|\rho| < 1$ and $p, q$ being coprime, i.e.

$$\rho(N, \ell) = \frac{2N}{\ell} - 2k. \quad (5)$$

Since $\exp(2\pi i m^2 \cdot k) = 1$ the Gauss sum (3) reads

$$A_N^{(M)}(\ell) = s_M(\rho(N, \ell)). \quad (6)$$
Figure 2. Emergence of four different classes of arguments $\ell$ of the truncated Gauss sum of (3) from its dependence on its truncation parameter $M$ for $N = 9624687 = 3 \times 919 \times 3491$. We show the signal value $|A_N^{(M)}(\ell)|$ for four arguments $\ell$ as a function of the truncation parameter $M$. For factors of $N$, such as $\ell = 919$ depicted by the black dots, the signal is constant and equal to unity. For typical non-factors, such as $\ell = 14$ depicted by the blue dots, the signal is suppressed considerably already for small values of the truncation parameter $M$. However, for ghost factors, such as $\ell = 2555$ depicted by the green dots, much more terms in the sum (3) are needed to suppress the signal. For arguments such as $\ell = 12$ depicted by the red dots, the signal levels off at a non-vanishing threshold determined by $1/\sqrt{2}$ and it is impossible to suppress it by further increasing the truncation parameter $M$.

where we have introduced the normalized curlicue function [5, 6]

$$s_M(\tau) \equiv \frac{1}{M + 1} \sum_{m=0}^{M} \exp \left( i\pi m^2 \tau \right),$$

which we consider for a real argument $\tau$ with $-1 \leq \tau \leq 1$.

The connection (6) between the truncated Gauss sum $A_N^{(M)}(\ell)$ defined in (3) and the normalized curlicue sum $s_M(\tau)$ for a given $N$ is established by the fractional part $\rho(N, \ell)$ of the fraction $2N/\ell$. Indeed, factors of $N$ correspond to $\rho = 0$. All other values of $\rho$ correspond to non-factors. In particular, ghost factors have $\rho$ values close to zero.

We depict the connection of $A_N^{(M)}(\ell)$ with $s_M(\tau)$ via $\rho(N, \ell)$ in figure 3 for the number to be factorized $N = 559 = 13 \times 43$ and the truncation parameter $M = 2$. The upper-left plot represents the master curve $|s_2(\tau)|$ (blue line) given by the absolute value of the normalized curlicue sum (7). The function $|s_M(\tau)|$ is even with respect to $\tau$, since

$$s_M(-\tau) = s_M^*(\tau).$$

Hence, it depends only on the absolute value of $\tau$.

Moreover, we note two characteristic domains of $|s_M(\tau)|$: (i) the function starts at unity for $\tau = 0$ and decays for increasing $\tau$. This central peak around $\tau = 0$ is the origin of the ghost factors. (ii) After this initial decay oscillations set in whose amplitudes seem to be bound.

New Journal of Physics 9 (2007) 370 (http://www.njp.org/)
Figure 3. Connection between the truncated Gauss sum $A_M(N, \ell)$ and the normalized curlicue sum $s_M(\tau)$ established by the fractional part $\rho(N, \ell)$ of the fraction $2N/\ell$. Here, the number $N$ to be factorized is $N = 559 = 13 \times 43$ with the truncation parameter $M = 2$. In the lower-left plot we assign to every value of $\ell$ the fractional part $\rho(N, \ell)$ defined by (5) for the number $N = 559$ as exemplified by $\ell = 20$ and the green dot. In the upper-left plot we show the master curve $|s_2(\tau)|$ indicated by the red curve and given by the absolute value of the normalized curlicue sum (7). This curve is an even function with respect to $\tau$ and attains the values above $1/\sqrt{2}$ only in the narrow peak located at $\tau = 0$. The factorization interference pattern for $N = 559$ shown in the upper-right corner follows from the dots in the upper-left plot in a two step process going through the master curve: from $\ell$ we find the fractional part $\rho(N, \ell)$ which determines through the master curve the signal value as indicated by the arrows.

Indeed, in appendix A we show that in the limit of large $M$ the absolute value of the normalized curlicue sum $|s_M(\tau)|$ evaluated at nonzero rational $\tau$ is bounded from above by $1/\sqrt{2}$.

The lower-left plot shows the distribution of the fractional parts $\rho(N, \ell)$ given by (5). The dots in the upper-left plot arise from the projection of the fractional parts (5) of the lower-left plot on to the master curve. Those data points represent the factorization interference pattern for $N = 559$, as depicted on the right.
4. Upper bound on the truncation by complete suppression of ghost factors

Ghost factors emerge from the central peak of the absolute value of the normalized curlicue function. Our goal is to suppress these ghost factors by increasing the truncation parameter $M$. For this purpose, we display in figure 4 the normalized curlicue sum (7) in the neighborhood of $\tau = 0$ in its dependence on $\tau$ and $M$. Indeed, we find a narrowing of the central peak with increasing $M$. In this way, we can suppress the ghost factors below a natural threshold.

As shown in appendix A for nonzero positive rational $\tau = p/q$ the absolute value of the normalized curlicue sum is asymptotically bounded from above by $1/\sqrt{2}$. Due to the connection (6) between the normalized curlicue sum $s_M(\tau)$ and the Gauss sum $A^{(M)}_N(\ell)$ it is natural to use this bound as a natural threshold between factors and non-factors. This observation allows us to define the ghost factor properly: ghost factors $\ell$ of a number $N$ arise when the fractional part $\rho(N, \ell)$ of $2N/\ell$ leads to a value of the normalized curlicue function $|s_M(\rho)|$ in the domain between $1/\sqrt{2}$ and unity.

We now determine the truncation parameter $M_0$ such that we can push the absolute value of the Gauss sum for all ghost factors below the natural threshold of $1/\sqrt{2}$. Ghost factors appear for small values of $\tau$. This fact allows us to replace the Gauss sum by an integral which leads us to an estimate for the truncation parameter $M_0$.

Indeed, with the substitution $u = \sqrt{2/\tau} m$ we can approximate the normalized curlicue function

$$s_M(\tau) \approx \frac{1}{M} \int_0^M du \ exp \left( i \pi m^2 \tau \right) = \frac{F \left( M \sqrt{2/\tau} \right)}{M \sqrt{2/\tau}}$$

with the Fresnel integral [16]

$$F(x) = \int_0^x du \ exp \left( i \frac{\pi}{2} u^2 \right)$$

New Journal of Physics 9 (2007) 370 (http://www.njp.org/)
Figure 5. Comparison between the exact discrete normalized curlicue sum (7) shown by black dots and its approximation (9) by the continuous Fresnel integral depicted by the red curve. We display the absolute value $|s_M(\tau)|$ as a function of the number $M$ of terms contributing to the curlicue sum (7) for $\tau = 10^{-3}$. The horizontal line marks the threshold $1/\sqrt{2}$ of the signal and the vertical line indicates the upper bound $M_0$ (14) required to suppress a ghost factor corresponding to $\tau = 10^{-3}$.

familiar from the diffraction from a wedge [17]. We note that in the continuous approximation the normalized curlicue function depends only on the product $M \times \sqrt{2\tau}$.

In figure 5, we compare the absolute value of the discrete curlicue sum $s_M(\tau)$ and the continuous Fresnel integral $F(M\sqrt{2\tau})/(M\sqrt{2\tau})$ at small value $\tau = 10^{-3}$. This approximation impressively models the results of the discrete curlicue sum.

We are now looking for the truncation parameter $M_0$ such that for a given fractional part $\tau$ the absolute value of the integral (9) is equal to $\frac{1}{\sqrt{2}}$. We denote $\alpha(\xi)$ to be the solution of the transcendental equation

$$|F(\alpha)| = \xi. \quad (11)$$

In particular, for the natural threshold $\xi = 1/\sqrt{2}$ defining the ghost factors we find the numerical value of $\alpha(\xi) \approx 1.318$. From the fact that $F$ depends only on the product of $M\sqrt{2\tau}$ it follows that

$$\alpha(\xi) = M_0\sqrt{2\tau}. \quad (12)$$

For the factorization of the number $N$ the argument $\ell$ is varied within the interval $[1, \sqrt{N}]$. Consequently, the minimal fractional part

$$\rho_{\text{min}}(N) \sim \frac{2}{\sqrt{N}}. \quad (13)$$

arises from the ratio $2N/\ell$ when the denominator takes on its maximum value $\ell = \sqrt{N}$.

Finally, we arrive at

$$M_0 \approx \frac{\alpha(\xi)}{\sqrt{2\rho_{\text{min}}(N)}} \approx \frac{\alpha(\xi)}{2} \sqrt{N}. \quad (14)$$

New Journal of Physics 9 (2007) 370 (http://www.njp.org/)
Hence, $M_0$ represents an upper bound for the number of terms in the truncated Gauss sum (3) required to push all non-factors below the threshold of $\xi$. In particular, we find that to suppress all ghost factors below the natural threshold $\xi = 1/\sqrt{2}$ we need $M_0 \approx 0.659 \sqrt{N}$ terms in the truncated Gauss sum. However, we point out that the power-law (14) arises from the fact that we use quadratic phases and will be unchanged by relaxing the threshold value $\xi$, as the change of this threshold will only change the prefactor $\alpha(\xi)$.

We conclude this section by noting that the scaling law rests on approximating the normalized curlicue sum by the Fresnel integral. In appendix B, we analyze the range of applicability of the Fresnel integral approximation (9) and find that our results lie within validity of the approximation.

5. Ghost factor counting function: inevitable scaling law

In the preceding section, we have derived a scaling law between the number $M$ of terms of the truncated Gauss sum to factor a given number $N$. This estimate is a sufficient condition for the success of the Gauss sum factorization scheme. In the present section, we show that it is also a necessary condition. In order to illustrate this feature we first choose logarithmic truncation $M = \ln N$ and show that at the end of our factorization scheme we will be left with too many candidate factors, most of them being a ghost factor. Moreover, we show that we cannot achieve a more favorable scaling than the fourth-root dependence, (14), even if we tolerate a limited number of ghost factors.

To answer these questions we introduce a ghost factor counting function

$$g(N, M) \equiv \# \left\{ \ell = 1, \ldots, \lfloor \sqrt{N} \rfloor \text{ with } \frac{1}{\sqrt{2}} < |A_N^{(M)}(\ell)| < 1 \right\},$$

which yields the number of data-points with critical values of the signal in the factorization interference pattern for a given $N$ and a chosen truncation $M$.

In order to study the behavior of the ghost factor counting function $g(N, M)$ on a broad range of numbers $N$ we show in figure 6 $g(N, M = \ln N)$ for 10,000 random numbers $N$ out of the interval $[1, 2 \times 10^{10}]$. Here, we choose the truncation parameter to depend logarithmically $M \approx \ln N$ on $N$. This result shows that the number of ghost factors $g(N, M)$ for $M \approx \ln N$ grows faster than the logarithm of $N$. Hence, the logarithmic truncation $M \approx \ln N$ is not sufficient for the success of our Gauss sum factorization scheme. We provide an explanation for the general trend observable in figure 6 in section 5.1 and discuss the deviations in section 5.2.

In evaluating the number of ghost factors we proceed in two steps. First, we make use of the connection (6) between the truncated Gauss sum $A_N^{(M)}(\ell)$ and the normalized curlicue sum $s_M(\tau)$. As already pointed out in section 3 the ghost factors appear only for $\tau$ values lying in the small interval $[-\tau_0, \tau_0]$ around zero. The Fresnel integral approximation from section 4 allows us to determine the fractional part $\tau_0$ where the normalized curlicue sum assumes the value $1/\sqrt{2}$. In the second step we relate the number of ghost factors $g(N, M)$ to $\tau_0$ by a density argument.

We determine $\tau_0$ with the help of the continuous approximation of the curlicue sum. From (12) we obtain

$$\tau_0 = \tau_0(M) \approx \frac{\alpha^2}{2M^2}$$

(16)
Figure 6. A logarithmic dependence of the truncation parameter $M$ on $N$ is not sufficient to suppress ghost factors. The ghost factor counting function $g(N, M)$ calculated for 10,000 random odd numbers $N$ out of the interval $[1, 2 \times 10^{10}]$ with $M = \ln N$ grows faster than the logarithm of $N$. The red line describes the general trend given by (19). We observe strong deviations, as exemplified by $N = 13,064,029,441$ highlighted by the circle and discussed in section 5.2.

and we thus arrive at the total width $2\tau_0 \approx \alpha^2/M^2$ of the interval of fractional parts resulting in signal values larger than $1/\sqrt{2}$.

We now relate the number of ghost factors $g(N, M)$ to the width of the interval $2\tau_0$ via the distribution of fractional parts $\tau$ for a given $N$. Firstly, we consider a uniform distribution. Here, we derive an analytical estimation for $g(N, M)$ which explains the general trend in figure 6. Secondly, we discuss the case of numbers $N$ where the distribution of fractional parts cannot be approximated as uniform. Finally, we analyze a trade-off between a smaller truncation parameter at the expense of more ghost factors. We show that this approach will not change the power-law (14).

5.1. Uniform distribution of fractional parts

Let us first for simplicity assume that the distribution of the fractional parts $\tau$ is uniform for a given number $N$. Here, the number of ghost factors $g(N, M)$ is directly proportional

$$ g(N, M) \approx \frac{2\tau_0}{\sqrt{N}}, \quad (17) $$

to the width $2\tau_0$ of the interval of the fractional parts which lead to ghost factors.

Recalling the dependence of $\tau_0$ on $M$ (16) we conclude that the number of ghost factors

$$ g(N, M) \approx \frac{1}{2} \left( \frac{\alpha}{M} \right)^2 \sqrt{N}, \quad (18) $$
depends via an inverse power-law on the truncation parameter $M$.

In figure 6, we already found indications that $g(N, M = \ln N)$ grows faster than the logarithm of $N$. Indeed, from (18) we obtain

$$ g(N, \ln N) \approx \frac{1}{2} \left( \frac{\alpha}{\ln N} \right)^2 \sqrt{N}, \quad (19) $$
which implies that \( g(N, \ln N) \) behaves like \( \sqrt{N} \). In figure 6, we display a fit according to (19). We find that this fit describes the general trend well over a large range of numbers \( N \). However, we also observe strong variations around this general trend. The deviations indicate that the distribution of fractional parts is not uniform for certain numbers \( N \). We analyze such numbers in section 5.2.

5.2. Non-uniform distribution of the fractional parts

In figure 6, we find that for certain numbers the actual number of ghost factors \( g(N, M) \) considerably deviates from our estimation (19). In the following we show that for such numbers the distribution of the fractional parts cannot be treated as uniform.

This unfavorable case occurs when \( N \) has only few divisors, but another number \( N' = N + k \) close to \( N \) has a lot of divisors (with \( |k| \ll N \)). For example for the number

\[
N = 13,064,029,441 = 2,164,7\times 603,503
\]

highlighted in figure 6 by the circle we find that

\[
N' = N - 1 = 2^8 \times 3 \times 5 \times 11 \times 17 \times 23 \times 113
\]

obviously has a lot of divisors.

Let us consider \( \ell' \) which is a divisor of \( N' = N + k \) but not of \( N \). It follows that if \( \ell' > 2k \) the fractional part of \( 2N/\ell' \) is equal to

\[
\rho(N, \ell') = -\frac{2k}{\ell'}
\]  

(22)

If we consider a plot of the fractional part \( \rho(N, \ell) \) of \( 2N/\ell \) as a function of \( \ell \) we will find that for divisors \( \ell' \) of \( N' \) the resulting fractional parts are aligned on the hyperbola (22) and are attracted to zero. Hence for \( N \) the distribution of fractional parts \( \rho(N, \ell) \) is not uniform.

In the factorization interference pattern of \( N \) data-points associated with arguments \( \ell' \) corresponding to divisors of \( N' \) will also be aligned to the curve

\[
\gamma^{(M)}_{k}(l) \equiv s_{M} \left( \frac{2k}{\ell'} \right).
\]  

(23)

As for large values of \( \ell' \) the associated fractional part \(-2k/\ell'\) tends to zero the resulting signal values \( |A_{N}^{(M)}(\ell')| \) approaches unity. Hence, the divisors of \( N' \) become ghost factors of \( N \).

We illustrate this fact in figure 7 where we plot the distribution of the fractional parts and the factorization interference pattern for two numbers: \( N' \) rich in factors and \( N = N' - 1 \) rich in ghost factors. To emphasize the region of fractional parts which lead to ghost factors we use the logarithmic scale. Here, we have chosen \( N' = 13,335,840 = 2^5 \times 3^5 \times 5 \times 7^3 \) which obviously has a lot of divisors, as depicted on the upper-left plot by the straight line of red points. In the factorization interference pattern shown on the right these divisors correspond to a straight line of signals equal to unity. However, the divisors of \( N' \) are non-factors of \( N = N' - 1 = 13,335,839 = 11 \times 479 \times 2531 \). Moreover, they are aligned on a hyperbola (22) and attracted to zero as shown in the lower-left plot where we can clearly identify the hyperbola of red points. Consequently, in the factorization interference pattern plotted on the right this hyperbola of arguments with small fractional parts (22) translates into the curve of ghost factors, as depicted on the right.
Figure 7. Emergence of ghost factors of $N$ from factors of $N'$. We display the distributions of the fractional parts (left column) and the factorization interference patterns (right column) for the numbers $N' = 13\,335\,840 = 2^5 \cdot 3^5 \cdot 5 \cdot 7^3$ which is rich in factors and $N = N' - 1 = 13\,335\,839 = 11 \times 479 \times 2531$ which is rich in ghost factors. To emphasize the region of fractional parts which lead to ghost factors we use a logarithmic scale for $|\rho|$ on the vertical axes. The number $N'$ has a lot of divisors, as depicted on the upper-left plot by the straight line of red points. In the factorization interference pattern shown on the right these divisors correspond to a straight line of signals equal to unity. However, the divisors of $N'$ are non-factors for $N = N' - 1$. Moreover, they are aligned on a hyperbola (22) and attracted to zero as shown in the lower-left plot where we can clearly identify the hyperbola of red points. Consequently, in the factorization interference pattern shown on the right this hyperbola translates into the curve of ghost factors.

5.3. Optimality of the fourth-root law

In section 4, we have derived the fourth-root law (14) as an upper bound on the truncation parameter. We will now show that it is also necessary for the success of our factorization scheme.

The analysis of $g(N, M)$ revealed that it behaves similarly to the inverse power in $M$ (18). The closer the distribution of the fractional parts for a given $N$ the better the estimation (18) fits the actual data.

In figure 8, we present the log–log plot of $g(N, M)$ as a function of the truncation parameter $M$ for three characteristic examples. First, for the number $N = 13\,335\,769$ which has the fractional parts $\rho(N, \ell)$ of $2N/\ell$ distributed almost uniformly we find that scaling
Figure 8. The number $g(N, M)$ of ghost factors expressed by the ghost factor counting function (6) as a function of the truncation parameter $M$ for three characteristic examples. We use a log–log plot to bring out the scaling of $g(N, M)$ with $M$. For the number $N = 13\,335\,769$ the scaling $g(N, M) \sim M^{-2}$ predicted by (18) with the help of the Fresnel integral is satisfied. In contrast for $N = 13\,335\,839$ which is rich in ghost factors we see a strong deviation. Finally, for $N = 13\,335\,840$ which is poor in ghost factors due to the fact it has many divisors the ghost factor counting function $g(N, M)$ decays even faster than the estimation (18) predicts.

$\sim M^{-2}$ predicted by (18) is obeyed. For $N = 13\,335\,839$ we find strong deviations for larger values of $M$ due to the fact that the actual distribution of fractional parts is not uniform. Finally, for $N = 13\,335\,840$ the ghost factor counting function $g(N, M)$ decays even faster than the estimation (18) predicts. Nevertheless, in all three cases the number of ghost factors drops down rapidly in the beginning.

The inverse power-law (18) suggests an alternative truncation of the Gauss sum when we tolerate a limited number of ghost factors, say $K$. Indeed, the power-law reduces the number of ghost factors considerably for small values of $M$. On the other hand, it has a long tail, which implies that we have to include many more terms in the Gauss sum in order to discriminate the last few ghost factors. However, this approach will not change the power law dependence of $M$, (14), as equation (18) yields that

$$M_K \approx \frac{\alpha}{\sqrt{2K}} \sqrt[4]{N}$$

(24)

terms are required to achieve this goal. Let us point out that this result holds if we can approximate the distribution of the fractional parts by uniform distribution. However, as we have seen in figure 8, if this simplification is not feasible such $M_K$ might be even greater. Therefore, we cannot achieve a better scaling on $N$ than $\sqrt[4]{N}$, even if we tolerate a limited number of ghost factors.

New Journal of Physics 9 (2007) 370 (http://www.njp.org/)
We conclude that the scaling \( M_0 \sim 4 \sqrt{N} \) of the upper limit of the Gauss sum \( A_N^{(M)} \) provides both sufficient and necessary condition for the success of our factorization scheme. Using \( M_0 \) terms in the Gauss sum we can suppress all ghost factors for any number \( N \). From the relation (4) we see that we need to add \( \sim \sqrt{N} \cdot \sqrt{N} = N^{3/4} \) terms for the success of the factorization scheme based on the truncated Gauss sum. In comparison with the value of \( \sim N \) of terms required for the complete Gauss sum (2) we have gained a factor of fourth-root. We emphasize that we cannot reduce the amount of resources further.

6. Conclusion

Motivated by the use of truncated Gauss sums in the context of factorization of numbers we have investigated the dependence on the upper limit of the summation. We have identified four distinct classes of candidate factors \( \ell \) with respect to the number to be factorized \( N \). In particular, with the help of the normalized curlicue sum we have found a simple criterion for the most problematic class of ghost factors. The natural threshold of the signal value of the Gauss sum which can be employed to discriminate factors from non-factors was identified. We have derived the scaling law \( M_0 \sim \sqrt{N} \) for the upper limit of the Gauss sum which guarantees that all ghost factors are suppressed, i.e. the signal values for all non-factors lie below the natural threshold. Unfortunately, we cannot achieve a more favorable scaling even if we change the threshold value or tolerate a limited amount of non-factors.

However, a generalization of Gauss sums to sums with phases of the form \( m^j \) with \( 2 < j \) might offer a way out of the fourth-root scaling law. Indeed, such a naive approach suggests the scaling law \( M_0 \sim \sqrt[2j]{N} \). For an exponential phase dependence \( m^m \) we would finally achieve a logarithmic scaling law. However, these new phases bring in new thresholds and a more detailed analysis is needed. However, the answer to these questions goes beyond the scope of the present paper.

Moreover, the analysis of the non-uniform distribution of the fractional parts provides us with a new perspective on the ghost factors. So far we have treated them as problematic trial factors which might spoil the identification of factors from the factorization interference pattern. However, the fact that the ghost factors of \( N \) are factors of numbers close to \( N \) offers an interesting possibility—by factorizing \( N \) we can find candidate factors of numbers close to \( N \). Indeed, as we have found in (23) the factors of \( N \pm k \) align on the curve \( \gamma_k^{(M)}(\ell) \) in the factorization interference pattern of \( N \). Hence, if we identify the data points lying on these curves we find candidate factors of \( N \pm k \). However, to take advantage of this positive aspect of ghost factors we need a very good resolution of the experimental signal data.

We illustrate this feature in figure 9 on the factorization interference pattern of \( N = 32\,183\,113 = 613 \times 52\,501 \). Here, we have chosen the truncation parameter according to \( M \approx \ln N \approx 17 \) which leads to an interference pattern with several ghost factors. However, we can clearly fit the ghost factors to curves \( \gamma_k^{(17)}(\ell) \) for \( k = 1, \ldots, 5 \). Hence, by factorizing \( N \) we also find candidate factors of \( N \pm k \) with \( k = 1, \ldots, 5 \).

Ghost factors are factors of neighboring numbers which make their way into the interference pattern through the curlicue sum. Since the curlicue sum is a continuous function of \( N/\ell \), factors of neighbors of \( N \) emerge like factors of \( N \). These two sentences summarize the central topic of the present paper and at the same time give a rather positive outlook. A detailed study of this idea is currently underway.
Figure 9. Factors of \( N \pm k \) obtained from the ghost factors of the factorization interference pattern of \( N = 32\,183\,113 = 613 \times 52\,501 \) with the truncation parameter \( M = 17 \approx \ln N \). Such a choice of \( M \) is clearly not sufficient to suppress all ghost factors. However, the remaining ghost factors can be fitted to the curves \( \gamma_k^{(17)}(\ell) \) for \( k = 1, \ldots, 5 \). Hence, we can identify candidate factors of numbers close to \( N \), in our case up to \( N \pm 5 \).

Acknowledgments

We thank H J Kimble and M S Zubairy for stimulating discussions and B Girard, E M Rasel and D Suter for informing us about their experiments prior to publication. All of us appreciate the stimulating atmosphere of the Ulm Graduate School Mathematical Analysis of Evolution, Information and Complexity under the leadership of W Arendt. WM and WPS acknowledge financial support from the Ministry of Science, Research and the Arts of Baden-Württemberg in the framework of the Center of Quantum Engineering. MŠ is grateful for a stipend from the European Community in the framework of CONQUEST. Moreover, WPS also would like to thank the Alexander von Humboldt Stiftung and the Max-Planck-Gesellschaft for the award of the Max-Planck-Forschungspreis.

Appendix A. Determination of threshold

In this appendix, we show that for nonzero positive rational \( \tau = p/q \) the absolute value of the normalized curlicue sum is asymptotically bound from above by \( 1/\sqrt{2} \). This property follows immediately from [5].

Indeed, as shown in [5] the asymptotic behavior of the curlicue sum depends on the product \( pq \). For \( pq \) being odd the absolute value of the normalized curlicue sum decays with increasing \( M \). For \( pq \) being even the limit of \( |s_M(\tau)| \) can be approximated by the finite product

\[
|s_M(\tau)| \approx (\tau_0 \cdot \tau_1 \cdots \tau_{\mu-1})^{1/2},
\]

where

\[
\tau_j = (1/\tau_{j-1}) \mod 1, \quad \text{if} \quad \tau_{j-1} \neq 0
\]
belongs to the \( j \)th step in the repeating curlicue pattern with \( \tau_0 = \tau \). The recursion terminates [5] at \( \tau_\mu = 0 \) which implies \( \tau_\mu-1 = 1/b \) where \( b \) is a natural number.

Since \( \tau_j < 1 \), we find the estimate

\[
|s_M(\tau)| \leq \sqrt{\tau_{\mu-1}} = 1/\sqrt{b}. \tag{A.3}
\]

The case \( b = 1 \) cannot be produced by the recursion formula since all \( \tau_j \) are strictly less than one. As a consequence the absolute value of the normalized curlicue sum \( |s_M(\tau)| \) is asymptotically bound from above by \( 1/\sqrt{2} \).

**Appendix B. Applicability of the Fresnel approximation**

In this appendix, we briefly discuss the range of applicability of the continuous approximation (9). The scaling law \( M_0 \sim \sqrt{N} \) connecting the number to be factored with the truncation parameter \( M_0 \) necessary to push all ghost factors below the threshold \( 1/\sqrt{2} \) relies on the approximation of the normalized curlicue function by the Fresnel integral. For large values of \( N \) the scaling law requires large values of \( M_0 \). However, for large \( M \) the continuous approximation might not hold any more.

Indeed, for the continuous approximation to hold true the phase difference

\[
\pi \left((m+1)^2 - m^2\right) \tau = \pi(2m+1)\tau \tag{B.1}
\]

of two successive terms in the sum (7) should at most be of the order of \( \pi \). Together with the fact that the maximal phase difference appears for \( m = M \) we arrive at the inequality

\[
\tau(2M+1) < 1. \tag{B.2}
\]

Indeed, this condition is violated for sufficiently large \( M \).

When we recall that for a given \( N \) the smallest fractional part is \( \tau_{\min} = 1/\sqrt{N} \) we arrive at the constraint

\[
M_c \approx \frac{1}{4}\sqrt{N} \tag{B.3}
\]
on the maximal value \( M_c \) of the truncation parameter for a given \( N \).

Thus \( M_c \sim \sqrt{N} \) provides an upper bound on the validity of the Fresnel approximation, (9). Since \( M_0 \sim \sqrt{N} \) the Fresnel approximation is valid.

**References**

[1] Davenport H 1980 *Multiplicative Number Theory* (New York: Springer)
[2] Maier H and Schleich W P 2007 *Prime Numbers 101: A Primer on Number Theory* (New York: Wiley-VCH) to be published
[3] Lang S 1970 *Algebraic Number Theory* (New York: Addison Wesley)
[4] Talbot H F 1836 *Phil. Mag.* 9 401
[5] Berry M V and Goldberg J 1988 *Nonlinearity* 1 1
[6] Berry M V 1988 *Physica* D 33 26
[7] Leichtle C, Averbukh I Sh and Schleich W P 1996 *Phys. Rev. Lett.* 77 3999
[8] Leichtle C, Averbukh I Sh and Schleich W P 1996 *Phys. Rev. A* 54 5299
[9] Berry M V, Marzoli I and Schleich W P 2001 *Phys. World* 14 39
[10] Oppenländer J, Häussler Ch and Schopohl N 2000 *Phys. Rev. B* 63 024511
[11] Merkel W, Averbukh I Sh, Girard B, Paulus G G and Schleich W P 2006 *Fortschr. Phys.* 54 856

*New Journal of Physics* 9 (2007) 370 (http://www.njp.org/)
[12] Mehring M, Müller K, Averbukh I Sh, Merkel W and Schleich W P 2007 Phys. Rev. Lett. 98 120502
[13] Mahesh T S, Rajendran N, Peng X and Suter D 2007 Phys. Rev. A 75 062303
[14] Gilowski M, Wendrich T, Müller T, Jentsch Ch, Ertmer W, Rasel E M and Schleich W P 2007 Phys. Rev. Lett. submitted (Preprint 0709.1424v1)
[15] Bigourd D, Chatel B, Girard B and Schleich W P 2007 Phys. Rev. Lett. submitted (Preprint 0709.1906v1)
[16] Abramowitz M and Stegun I A 1972 Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables (New York: Dover)
[17] Born M and Wolf E 1993 Principles of Optics (Oxford: Pergamon)