Factorization with exponential sums

2008 J. Phys. A: Math. Theor. 41 304024

(http://iopscience.iop.org/1751-8121/41/30/304024)

J. Phys. A: Math. Theor. **41** (2008) 304024 (14pp) doi:10.1088/1751-8113/41/30/304024

Factorization with exponential sums

M Štefaňák[1,2], D Haase[3], W Merkel[2], M S Zubairy[4,5] and W P Schleich[2]

[1] Department of Physics, FJFI ČVUT v Praze, Břehová 7, 115 19 Praha 1—Staré Město, Czech Republic
[2] Institut für Quantenphysik, Universität Ulm, Albert-Einstein-Allee 11, D-89081 Ulm, Germany
[3] Institut für Reine Mathematik, Universität Ulm, Helmholtzstraße 18, D-89069 Ulm, Germany
[4] Department of Physics and Institute for Quantum Studies, Texas A&M University, College Station, TX 77843-4242, USA
[5] Texas A&M University at Qatar, Education City, PO Box 23874, Doha, Qatar

Received 4 December 2007, in final form 18 March 2008
Published 15 July 2008
Online at stacks.iop.org/JPhysA/41/304024

Abstract
We generalize the concept of factorization using truncated Gauss sums to exponential sums where the phase increases with the jth power of the summation index. For such sums the number of terms needed to suppress ghost factors of N scales as $\sqrt[2j]{N}$. Unfortunately, this advantageous scaling law is accompanied by a disadvantage: the gap between factors and non-factors decreases rapidly with increasing power j and as a consequence it gets more difficult to identify factors. This feature serves as our motivation to study sums with an exponential phase. Our numerical simulations indicate that in this case the scaling law is logarithmic and that we retain a significant gap between factors and non-factors.

PACS numbers: 02.10.De, 42.25.Hz

1. Introduction

Recently, several schemes for integer factorization [1–3] based on Gauss sums [4, 5] were proposed [6–13]. The resulting experiments rely on NMR [14–16], cold atoms [17] and ultra-short pulses [18, 19], and have successfully demonstrated the possibility of finding the prime factors of up to 17-digit numbers without applying paradigms of quantum computation used in the well-known Shor algorithm [20]. Indeed, Shor's algorithm solves a period finding problem using the translation invariance of the quantum Fourier transform and entanglement.

In contrast, factorization using Gauss sums consists of a feasible factor test based on a classical interference scheme. Indeed, constructive interference leads to a large signal for a factor of N. For non-factors destructive interference yields a small signal. This feature allows us to distinguish factors from non-factors. In the most elementary approach we have to perform this factor test for every number smaller than $\sqrt{N}$. As a consequence our method scales as $\sqrt{N}$ and is therefore exponential as shown in [14].

It is also instructive to consider the resources necessary to implement a Gauss sum. In all experiments performed so far the individual contributions to the Gauss sum are created by individual laser pulses. In [21], we have shown that the total number $\mathcal{R}$ of pulses needed to factor the number N is determined by the product

$$\mathcal{R} \sim M \cdot N^{\frac{1}{2}} \tag{1}$$

consisting of the number of terms M in the Gauss sum times the number of trials given by $N^{\frac{1}{2}}$. Hence, the scaling law between M and N determines the ultimate resources necessary to factor N.

In [21], we have shown that in order to achieve a significant contrast between factors and non-factors M has to be of the order of the fourth root of N. This condition leads us to the scaling law

$$\mathcal{R}_2 \sim N^{\frac{1}{4}} \cdot N^{\frac{1}{2}} = N^{\frac{3}{4}} \tag{2}$$

of pulses.

In the present study we extend our ideas of factorization with the help of Gauss sums by considering exponential sums. Here the phase is proportional to m^j where m is the summation index and j is an integer. We show that in such a case the truncation depends on the inverse of this function, i.e. $M \sim \sqrt[2j]{N}$ leading to

$$\mathcal{R}_j \sim N^{\frac{1}{2j}} \cdot N^{\frac{1}{2}} = N^{\frac{j+1}{2j}}. \tag{3}$$

Hence, we can save experimental resources by employing rapidly increasing phase functions. The extreme limit of an exponential sum where the phase varies exponentially with the summation index, i.e. m^m, should then be the optimal choice. We briefly address this case and demonstrate by a numerical analysis that the truncation parameter depends only logarithmically on the number to be factored providing us with the estimate

$$\mathcal{R}_{\text{exp}} \sim \log N \cdot N^{\frac{1}{2}} \tag{4}$$

of resources.

It is interesting to note that recently an experiment [16] based on NMR has used an exponential sum with $j = 5$ to factor a 17-digit number consisting of two prime factors of the same order. In this experiment π-pulses [22] drive a two-level atom. By choosing the phases of the pulses appropriately we can achieve [23] a situation in which the resulting polarization is determined by a truncated exponential sum with a particular choice of j. Moreover, even the extreme case of an exponential phase m^m can be realized in this way. First preliminary results from the Suter group exist [24].

Exponential sums play a central role in analytic number theory [25]. Here, they are defined over a set of coprime integers. In contrast, the exponential sums studied in the present paper are different from the classic exponential sums for two reasons: (i) in our sums the summation range extends over all integers including those having a common factor, and (ii) our sums are limited by a truncation parameter, and are normalized. The first condition allows us to distinguish uniquely between factors and non-factors. Our goal in the present paper is to investigate how this discrimination property survives the second modification, which is motivated by limited experimental resources.

Our paper is organized as follows: in section 2 we introduce exponential sums and show that they allow us to discriminate between factors and non-factors. In particular, we demonstrate by a numerical example that phases which increase as m^3 suppress ghost factors more effectively than Gauss sums which have phases proportional to m^2. This feature is our motivation to study the factorization properties of exponential sums.

In [21], we have shown that for truncated Gauss sums the influence of the truncation parameter M depends crucially on the choice of trial factors. We have identified four classes: (i) factors, which are not influenced by M, (ii) threshold trial factors, which are also independent of M, (iii) typical non-factors, which decay very quickly, and (iv) ghost factors, which decay slowly. In section 3 we perform a similar analysis for exponential sums.

In section 4 we confirm by an analytic argument the numerical calculations of section 2. We show that the number of terms which have to be summed in order to suppress the signal of all ghost factors depends on the $2j$th root of the number to be factored.

For all exponential sums except the Fourier sum there exist non-factors for which the signal cannot be suppressed below certain thresholds by further increasing the truncation parameter. The values of these thresholds are determined by the power j and can be close to the maximal signal of unity corresponding to a factor. In such a case we cannot achieve a sufficient contrast between the signals of factors and non-factors. We discuss the restrictions imposed by this fact on our factorization scheme in section 5.

Our analysis indicates that rapidly increasing phases suppress ghost factors most effectively. This feature suggests considering the extreme case with the phase m^m. We briefly address this case in section 6.

We summarize our results in the conclusions of section 7 and present an outlook.

2. Factorization with exponential sums

The landmark paper [26] by Heath–Brown and Patterson investigates the distribution of values of exponential sums defined by

$$g(c) = \sum_{\substack{d(\mathrm{mod}\ c)\\ \gcd(c,d)=1}} (d/c)_3 \cdot \mathrm{e}^{2\pi \mathrm{i}\frac{d}{c}}. \tag{5}$$

Here c and d are natural numbers, and $(d/c)_3$ is the cubic residue symbol [4].

However, for our purpose to factorize numbers we use truncated and normalized exponential sums of the type

$$\mathcal{A}_N^{(M,j)}(\ell) \equiv \frac{1}{M+1} \sum_{m=0}^{M} \exp\left[2\pi \mathrm{i} m^j \frac{N}{\ell}\right], \tag{6}$$

where the phases are determined by the integer power j. Here N is the number to be factored and ℓ is a trial factor which scans through all integers between 1 and $\lfloor\sqrt{N}\rfloor$. In the experiments performed so far the upper bound M in the sum is equal to the number of pulses applied.

We emphasize that in contrast to the sum in (5), the summation is no longer restricted to a set of coprime integers. In this way we obtain the unique discrimination property: $\left|\mathcal{A}_N^{(M,j)}(\ell)\right| = 1$ if l is a factor of N, and $\left|\mathcal{A}_N^{(M,j)}(\ell)\right| < 1$ otherwise.

In the case of $j = 1$ the exponential sum reduces to a Fourier sum. For $j = 2$ we find the truncated Gauss sum

$$\mathcal{A}_N^{(M)}(\ell) \equiv \mathcal{A}_N^{(M,2)}(\ell) = \frac{1}{M+1} \sum_{m=0}^{M} \exp\left[2\pi \mathrm{i} m^2 \frac{N}{\ell}\right]. \tag{7}$$

In the case of $j = 3$ the sum

$$\mathcal{A}_N^{(M,3)}(\ell) = \frac{1}{M+1} \sum_{m=0}^{M} \exp\left[2\pi \mathrm{i} m^3 \frac{N}{\ell}\right] \tag{8}$$

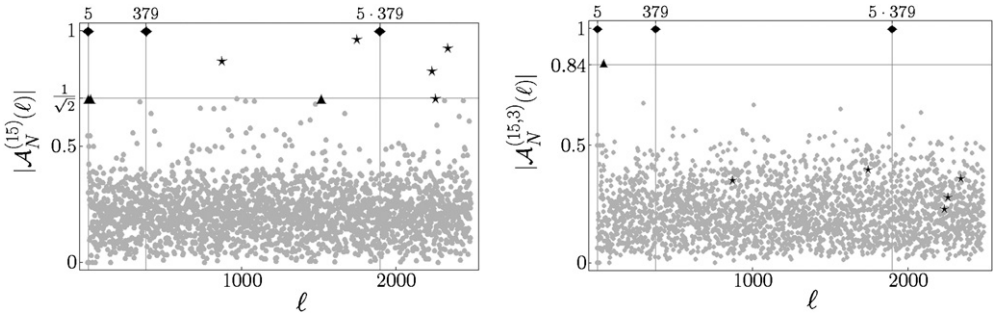

Figure 1. Factorization interference patterns of the number $N = 6172015 = 5 \cdot 379 \cdot 3257$ resulting from the Gauss sum (left) and the Kummer sum (right). Here we have chosen the truncation parameter $M \approx \ln N \approx 15$. The factors of N, depicted by black diamonds, correspond to the signal value of unity. For most of the non-factors, depicted by gray dots, the signal value is well suppressed. However, in the case of Gauss sum we note that for a few non-factors, depicted by stars, the signal is close to that of a factor. Since such arguments can be misinterpreted as factors of N we call them ghost factors. The presence of ghost factors in the factorization interference pattern indicates that the choice of the truncation parameter $M \approx \ln N$ is not sufficient for the Gauss sum. However, the cubic phases in the Kummer sum grow faster than the quadratic phases in the Gauss sum. As a result, the truncation parameter $M = 15$ is now sufficient to suppress all ghost factors. Moreover, some trial factors result in a threshold value of the signal depicted by black triangles which cannot be suppressed by further increasing the truncation parameter M. In the case of the Gauss sum the threshold is $1/\sqrt{2}$ whereas for the Kummer sum it has the value 0.844.

is the truncated version of a sum of the form (5) which carries the name *Kummer sum* after the mathematician Ernst Kummer (1810–1893).

The capability of the exponential sums, (6), to factor numbers stems from the fact that for an integer factor q of N with $N = q \cdot r$ all phases in $\mathcal{A}_N^{(M,j)}$ are integer multiples of 2π. Consequently, the terms add up constructively and yield $\mathcal{A}_N^{(M,j)}(q) = 1$. When ℓ is not a factor the phases oscillate with m and the signal $\left|\mathcal{A}_N^{(M,j)}(\ell)\right|$ takes on small values. In order to factor a number N we analyze $\left|\mathcal{A}_N^{(M,j)}(\ell)\right|$ for arguments ℓ out of the interval $[1, \sqrt{N}]$. We refer to the graphical representation of the signal data as *factorization interference pattern*.

In figure 1 we show the factorization interference patterns of the number $N = 6172\,015 = 5 \cdot 379 \cdot 3257$ resulting from the Gauss sum (left) and from the Kummer sum (right) for the choice of the truncation parameter $M = 15 \approx \ln N$. In both cases the factors of N lead to the maximal signal of unity depicted by black diamonds. In contrast for most of the non-factors the signal represented by gray dots is well suppressed. However, for the Gauss sum there appear some non-factors, the so-called *ghost factors*, where the signal indicated by black stars is still close to that of a factor. We recognize that the corresponding factorization pattern resulting from the Kummer sum does not display any ghost factors. The origin of this positive feature lies in the fact that the cubic phase of the Kummer sum shows a stronger increase than the quadratic variation of the Gauss sum.

3. Classification of trial factors

In the preceding section we have shown using numerical examples that the influence of the truncation parameter of the exponential sums depends crucially on the choice of the trial factors. In the present section we analyze this feature in more detail and identify four classes of trial factors.

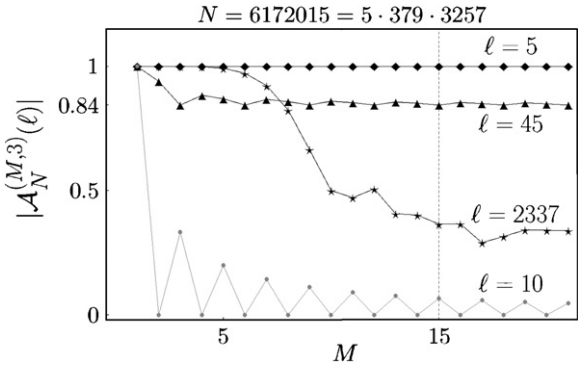

Figure 2. Four classes of trial factors ℓ illustrated by the dependence of the Kummer sum $|\mathcal{A}_N^{(M,3)}(\ell)|$ on the truncation parameter M. In order to compare with figure 1 where $M = 15$ as indicated by a vertical dashed line we have chosen again $N = 6172015 = 5 \cdot 379 \cdot 3257$. For factors of N, such as $\ell = 5$ depicted by black diamonds, the signal is constant and equal to unity. For typical non-factors, such as $\ell = 10$ depicted by gray dots, the signal is suppressed considerably already for small values of the truncation parameter M. However, for ghost factors, such as $\ell = 2337$ depicted by black stars, more terms in the sum (8) are needed to suppress the signal. Finally, for certain arguments, such as $\ell = 45$ depicted by black triangles, the signal levels at non-vanishing threshold and it is impossible to suppress it further by increasing the truncation parameter M.

For this purpose we start from the decomposition of the fraction N/ℓ into an integer k and the fractional part

$$\rho(N, \ell) = \frac{N}{\ell} - k \tag{9}$$

with $|\rho| \leqslant 1/2$. Indeed, the integer part contributes only as the multiplication by unity in (6) and we find

$$\mathcal{A}_N^{(M,j)}(\ell) = \mathcal{S}_j^{(M)}(\rho(N, \ell)) \tag{10}$$

where we have introduced the sum

$$\mathcal{S}_j^{(M)}(\rho) \equiv \frac{1}{M+1} \sum_{m=0}^{M} \exp(2\pi \mathrm{i} m^j \rho). \tag{11}$$

This elementary analysis allows us to identify four classes of the fractional part. Indeed, we find in complete analogy to the Gauss sums [21] : (i) for $\rho(N, \ell) = 0$ the trial factor ℓ is a factor of N, (ii) for $|\rho(N, \ell)| = t_j$ the trial factor ℓ results in a threshold value T_j of the exponential sum, where the values of t_j and T_j are determined by the power j, (iii) for $\rho(N, \ell)$ appropriately away from the origin the trial factor ℓ is a typical non-factor of N and (iv) for $\rho(N, \ell) \sim 0$ the trial factor ℓ is a ghost factor of N.

We illustrate the different dependences of representatives of these classes on the truncation parameter M in figure 2 using the example of the truncated Kummer sum (8). We find signals which are independent of M and equal to unity. They indicate factors. Moreover, we note a rapid suppression of the signal for a typical non-factor. However, for a ghost factor the signal is close to that of a factor and we have to include more terms in the sum (8) in order to suppress it. Moreover, we find that for certain trial factors ℓ the signal levels off at a non-zero threshold value and thus cannot be reduced at all.

4. Scaling law of the truncation parameter

In section 2 we have shown that the ghost factors spoil the discrimination of factors from non-factors. Fortunately, we can suppress the signal of a ghost factor by increasing the truncation parameter M. In this context the truncated Gauss sums were analyzed in [21] and it was shown that one needs $M \sim \sqrt[4]{N}$ terms in the sum in order to suppress the signal of all ghost factors considerably. We now derive the corresponding scaling law $M_j \sim \sqrt[2j]{N}$ of an exponential sum $\mathcal{A}_N^{(M,j)}$. In [21], the upper bound for the truncated Gauss sum (7) was obtained by approximating the Gauss sum by the Fresnel integral. We now perform a similar analysis for the exponential sums.

Since ghost factors result from small values of the fractional part $\rho \equiv N/\ell - k$ we replace the exponential sum by an integral, i.e.

$$\mathcal{A}_N^{(M,j)}(\ell) = \mathcal{S}_j^{(M)}(\rho) \approx \frac{1}{M} \int_0^M \mathrm{e}^{2\pi \mathrm{i} m^j \rho}\, \mathrm{d}m. \tag{12}$$

This approximation is justified by the van der Corput method [25] approximating sums by sums of shifted integrals.

With the help of the substitution $m^j \rho \equiv u^j$ and $\mathrm{d}m = \mathrm{d}u/\sqrt[j]{\rho}$ we find

$$\mathcal{A}_N^{(M,j)}(\ell) \approx F_j(M \cdot \sqrt[j]{\rho}) \tag{13}$$

where

$$F_j(x) \equiv \frac{1}{x} \int_0^x \mathrm{e}^{2\pi \mathrm{i} u^j}\, \mathrm{d}u\ . \tag{14}$$

This analysis brings out most clearly that for small fractional parts ρ the truncation parameters M and ρ appear in the exponential sum only as the product $M \cdot \sqrt[j]{\rho}$.

In order to suppress the absolute value $\left|\mathcal{A}_N^{(M,j)}(\ell)\right|$ below a given value ξ we have to choose the upper bound M according to

$$M \cdot \sqrt[j]{\rho} = \alpha \tag{15}$$

where α is the solution of the integral equation

$$|F_j(\alpha)| = \xi \tag{16}$$

which leads us to the relation

$$M = \alpha(\xi) \rho^{-\frac{1}{j}}. \tag{17}$$

This result shows that the smaller the fractional part $\rho(N, \ell)$ of the ghost factor ℓ the more terms are required. Since the largest trial factor is of the order of $\sqrt{N}$ the smallest attainable fractional part

$$\rho_{\min}(N) \sim \frac{1}{\sqrt{N}} \tag{18}$$

gives an upper bound

$$M_j \approx \alpha(\xi) \rho_{\min}^{-\frac{1}{j}} \approx \alpha(\xi)\, \sqrt[2j]{N} \tag{19}$$

on the truncation parameter M.

Hence, in order to suppress all ghost factors of N we require an order of $\sqrt[2j]{N}$ terms in the exponential sum $\mathcal{A}_N^{(M,j)}$. We point out that the scaling law (19) is inherent in the exponential sum since the change of ξ only modifies the pre-factor $\alpha(\xi)$.

In figure 3 we illustrate the behavior of $\left|\mathcal{A}_N^{(M,j)}(\ell)\right|$ for $N = 10^6 + 1$ and $\ell = 10^3$ resulting in the fractional part $\rho(N, \ell) = 10^{-3} \approx 1/\sqrt{N}$ as a function of the truncation parameter M.

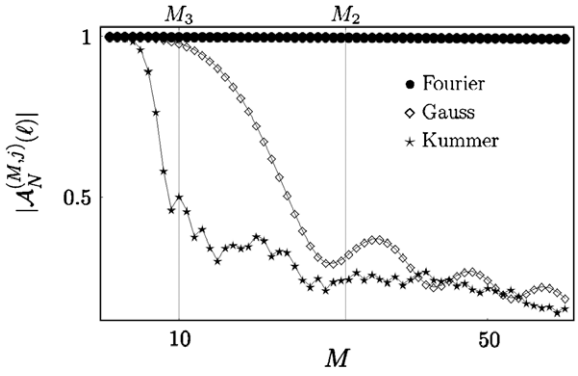

Figure 3. Decay of the signal $|\mathcal{A}_N^{(M,j)}(\ell)|$ for increasing truncation parameter M exemplified by the Fourier ($j = 1$), Gauss ($j = 2$) and Kummer ($j = 3$) sums. Here we have chosen $N = 10^6 + 1$ and $\ell = 10^3$ resulting in the fractional part $\rho(N, \ell) = 10^{-3} \approx 1/\sqrt{N}$. For the Fourier sum (black dots) we find an extremely slow decay of the signal. On the other hand, for the Gauss sum (diamonds) already $M_2 \sim \sqrt[4]{N} \approx 32$ terms are sufficient to suppress the signal considerably. This requirement is further reduced for the Kummer sum (stars) to $M_3 \sim \sqrt[6]{N} \approx 10$. We find that our numerical results are in good agreement with the analytical estimate (19).

We visualize the effect of the power j on the suppression of $\left|\mathcal{A}_N^{(M,j)}(\ell)\right|$ by presenting three different curves: (i) black dots correspond to the Fourier sum with linear phases, (ii) diamonds represent the Gauss sum, and finally (iii) stars result from the Kummer sum with cubic phases. We find that for the Fourier sum the suppression of the signal is extremely slow. Indeed, according to the estimate (19) we need $M_1 \sim \sqrt{N} \approx 10^3$ terms in order to suppress the signal considerably. On the other hand, for the Gauss sum already $M_2 \sim \sqrt[4]{N} \approx 32$ terms suffice to reduce the signal, in agreement with (19). Finally, for the Kummer sum the decay of the signal is even faster. We find that $M_3 \sim \sqrt[6]{N} \approx 10$ terms are sufficient to suppress the signal, in agreement with (19).

In order to verify the scaling law (19) for a broad range of N we have calculated numerically the truncation parameter M_j needed to suppress all ghost factors of N below the value ξ. We have chosen N randomly from the interval $[10^4, 10^{20}]$ and considered $\xi = 0.7$. In figure 4 we present the results for the Fourier sum (black dots), Gauss sum (open diamonds) and Kummer sum (stars). To unravel the scaling law we use a logarithmic scale for both N- and M-axes. The numerical results are in excellent agreement with the estimates (19) indicated by the dashed lines.

5. Threshold

An experiment must also take into account the limited measurement accuracy. Thus for the success of our factorization scheme we need a good contrast between the signals of factor and non-factors, i.e. we require that the signals of all non-factors be suppressed below the estimated measurement error. However, due to the existence of the thresholds discussed in section 3 this suppression might be impossible for certain powers j. In such a case we might misinterpret the signal arising from a non-factor as that of a factor. Hence, such exponential sums $\mathcal{A}_N^{(M,j)}$ are not suitable for integer factorization.

Relation (19) shows that the faster the phase grows the less terms in the exponential sum are needed in order to suppress the signal of a ghost factor argument ℓ. However, the

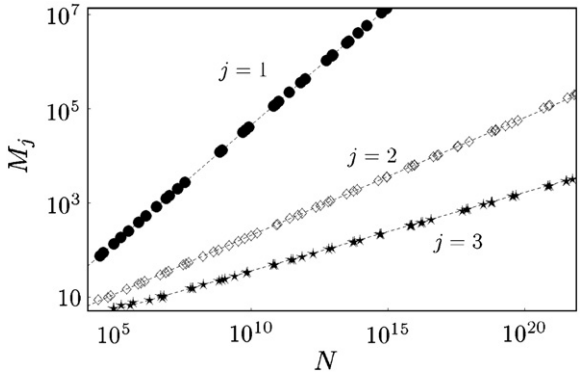

Figure 4. Number M_j of terms needed to suppress the signal of all ghost factors of N below the value 0.7 for the Fourier sum (black dots), Gauss sum (open diamonds) and Kummer sum (stars). To unravel the scaling of M_j with N we use a log–log scale. The dashed lines follow from the estimate $M_j \sim \sqrt[2j]{N}$ given by (19).

suppression of the signal might be impossible for all arguments ℓ, as we have seen already in figure 2. This feature is closely related to the power j determining the phase.

The absolute value $\left|\mathcal{A}_N^{(M,j)}(\ell)\right|$ depends on how many different roots of unity we find in the sum. These roots of unity are given by

$$\exp\left(2\pi \mathrm{i} m^j \frac{N}{\ell}\right) = \exp\left(2\pi \mathrm{i} m^j \rho(N,\ell)\right) = \exp\left(2\pi \mathrm{i} m^j \frac{p}{q}\right) \tag{20}$$

where p/q is the coprime rational representation of $\rho(N,\ell)$. This is equivalent to

$$m^j \frac{N}{\ell} q \equiv 0, 1, \ldots, q-1 \bmod q, \tag{21}$$

i.e. the terms in the exponential sum $\left|\mathcal{A}_N^{(M,j)}(\ell)\right|$ attain at most q different values.

For the Fourier sum we find all q different roots $\exp(2\pi \mathrm{i} m/q)$ with $m = 0, \ldots, q-1$ of unity. Moreover, since they are distributed symmetrically on the unit circle they cancel each other out. Hence, for the Fourier sum we can suppress the signal $\left|\mathcal{A}_N^{(M,1)}\right|$ of any non-factor ℓ below any given value by extending the summation range M.

However, for exponential sums $\mathcal{A}_N^{(M,j)}$ with powers $2 \leqslant j$ we are not guaranteed to find all different roots of unity. Moreover, since $j \neq 1$ the corresponding roots of unity $\exp(2\pi \mathrm{i} m^j p/q)$ are not necessarily distributed symmetrically on a unit circle. Hence, they do not cancel themselves completely. In such a case the signal $\left|\mathcal{A}_N^{(M,j)}(\ell)\right|$ has a non-zero limit as M tends to infinity. This limit value determines the threshold and depends on how many different roots of unity we find in the sum and their distribution on the unit circle. If we find only few different roots of unity which are moreover close to each other on the unit circle the signal $\left|\mathcal{A}_N^{(M,j)}(\ell)\right|$ attains values close to unity and cannot be suppressed further by increasing the truncation parameter M, even though ℓ does not correspond to a factor of N.

The fewest possible terms in the sum $\mathcal{A}_N^{(M,j)}$ for a non-factor ℓ occur if $j+1$ is the prime number q from the rational representation of $\rho(N,\ell)$. In such a case we find from the Euler's theorem (see e.g. chapter 3 in [27])

$$m^j \equiv \begin{cases} 1 & \text{if} \quad q \text{ is not a divisor of } m \\ 0 & \text{if} \quad q \text{ is a divisor of } m \end{cases} \tag{22}$$

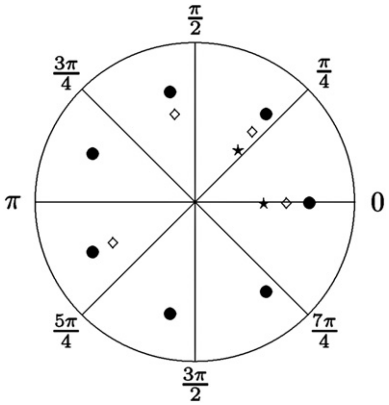

Figure 5. The roots of unity contained in the exponential sums $\mathcal{A}_N^{(M,j)}(\ell)$ exemplified by the Fourier sum ($j = 1$, black dots), the Gauss sum ($j = 2$, open diamonds) and a higher order exponential sum ($j = 6$, black stars). Here we have chosen $N = 99$ and $\ell = 7$ which lead to $\rho(N, \ell) = p/q = 1/7$. For the Fourier sum we find all seven different roots of unity. However, in the Gauss sum only four different roots of unity appear. This number is further reduced to just two different roots of unity in the higher order exponential sum with power $j = 6$.

so $m^j \cdot p$ is either congruent to p or 0 mod q. With the help of the periodicity $m^j \cdot p \equiv (m+q)^j \cdot p \bmod q$ and the relation (20) we obtain for $M+1$ being a multiple of q

$$\mathcal{A}_N^{(M,j)}(\ell) = \frac{1}{M+1} \sum_{m=0}^{M} \mathrm{e}^{2\pi \mathrm{i} m^j \frac{N}{\ell}} = \frac{1}{q} \sum_{m=0}^{q-1} \mathrm{e}^{2\pi \mathrm{i} m^j \frac{p}{q}} \tag{23}$$

$$= \frac{1}{q}(1 + (q-1)\,\mathrm{e}^{2\pi \mathrm{i} \frac{p}{q}}). \tag{24}$$

Hence we find for the absolute value squared

$$\left|\mathcal{A}_N^{(M,j)}(\ell)\right|^2 = \frac{1}{q^2}\left(\left(1 + (q-1)\cos\left(\frac{2\pi p}{q}\right)\right)^2 + (q-1)^2 \sin^2\left(\frac{2\pi p}{q}\right)\right). \tag{25}$$

Substituting $q = j + 1$ we find for $p = 1$ the threshold value of the sum $\mathcal{A}_N^{(M,j)}$

$$T_1(j) = \frac{1}{j+1}\sqrt{j^2 + 1 + 2j\cos\left(\frac{2\pi}{j+1}\right)}. \tag{26}$$

For $p > 1$ or for more than two different terms in the sum $\mathcal{A}_N^{(M,j)}$ the threshold will always be smaller.

To illustrate this we plot in figure 6 the behavior of the signal $\left|\mathcal{A}_N^{(M,6)}(\ell)\right|$ as a function of the truncation parameter M. Here we have chosen $N = 99$ and $\ell = 7$ resulting in $\rho(N, \ell) = p/q = 1/7$. Hence, $q = 7 = 1 \cdot 6 + 1$ and we find that the signal converges to the threshold value $T_1(6) \approx 0.953$.

More generally, for prime denominator $q = k \cdot j + 1$ the sum $\mathcal{A}_N^{(M,j)}$ contains at most $k+1$ different terms. For the case of $k = 2$ an analogous calculation results in the threshold value

$$T_2(j) = \frac{1}{2j+1}\left(1 + 2j\cos\left(\frac{2\pi}{2j+1}\right)\right). \tag{27}$$

Obviously, for large powers j the values of $T_{1,2}(j)$ are very close to 1.

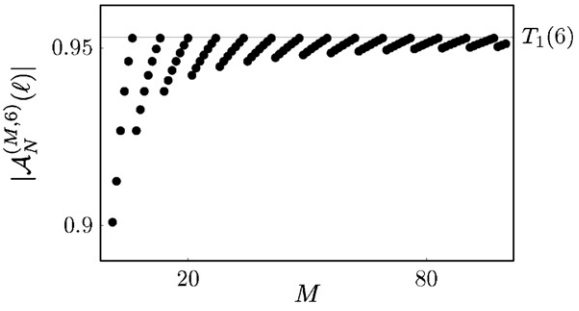

Figure 6. Emergence of the threshold for the exponential sum $\mathcal{A}_N^{(M,j)}$ with the power $j = 6$ for increasing truncation parameter M. We have chosen $N = 99$ and $\ell = 7$ resulting in $\rho(N, \ell) = p/q = 1/7$. The signal converges to the value of $T_1(6) \approx 0.953$ and cannot be suppressed by a further increase of M.

The above-derived results indicate that the exponential sums $\mathcal{A}_N^{(M,j)}$ with powers j larger than 2 can be used for integer factorization only when the experimental data are sufficiently precise. For the Fourier sum the signal for any non-factor can be suppressed below any given value. However, according to (19) we have to include number of terms of the order of the square-root of N to achieve this suppression. The quadratic Gauss sum of (7) provides a reasonable compromise between the number of terms needed and the non-factor discrimination. The gap between the signal of a factor and the greatest threshold is approximately 30% which should be sufficient for the experimental realization. The number of terms in the sum needed is according to [21] reduced to the fourth root of N.

6. Factorization with an exponential phase

One way to improve the scaling law might be offered by an exponential sum where the phase is not governed by a polynomial as in (6) but by an exponential function. This idea leads to the sum

$$\mathcal{E}_N^{(M)}(\ell) \equiv \frac{1}{M+1} \sum_{m=0}^{M} \exp\left[2\pi \mathrm{i} m^m \frac{N}{\ell}\right]. \tag{28}$$

We now present a numerical analysis which confirms a logarithmic scaling law. However, in contrast to sums involving a fixed exponent, we no longer have the tools of number theory at hand to prove perfect discrimination of factors from non-factors. Moreover, since the derivative of m^m grows faster than m^m itself, standard techniques to approximate these exponential sums by integrals cannot be applied. Nevertheless, we demonstrate that it is still possible to show that the sum actually discriminates factors from non-factors by methods of elementary number theory (see [27] for example).

6.1. Logarithmic scaling law

In section 4 we have found that the number of M_j terms needed to suppress all ghost factors for the exponential sum $\mathcal{A}_N^{(M,j)}$ scales like $M_j \sim \sqrt[2j]{N}$, i.e. M_j is determined by the inverse function of the phase evaluated at $\sqrt{N}$. This feature arises from the fact that the rising exponent prevents the function from accumulating values near unity for small arguments m, as we illustrate in figure 7. This result suggests that for the exponential sum $\mathcal{E}_N^{(M)}$ already a

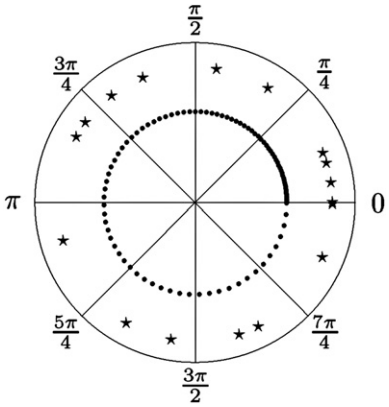

Figure 7. Distribution of the roots $e^{2\pi i m^2 p/q}$ (dots) and $e^{2\pi i m^m p/q}$ (stars) of unity for quadratic and exponential phases, respectively. Here we have chosen $p = 1$ and $q = 10^4$. Since the fraction p/q is small we observe an accumulation of the roots for small values of m in the case of the quadratic phase.

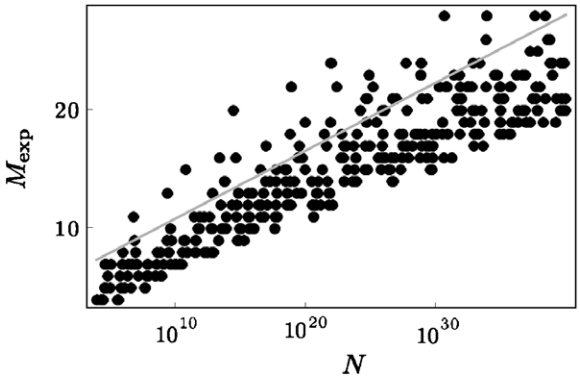

Figure 8. Number M_{exp} of terms needed to suppress the signal $|\mathcal{E}_N^{(M)}|$ of all non-factors of N below the value 0.7. To unravel the scaling of M we use a logarithmic scale for N. The gray line represents the estimate $M \sim \ln\sqrt{N}$. The plot indicates that already an order of $\ln\sqrt{N}$ terms in the exponential sum $\mathcal{E}_N^{(M)}$ is sufficient to find all factors of N.

logarithmic number of terms $M_{\mathrm{exp}} \sim \ln\sqrt{N}$ should be sufficient to eliminate all ghost factors. Moreover, our numerical analysis summarized in figure 8 indicates that the largest threshold for $\mathcal{E}_N^{(M)}$ occurs around the value 0.5. Hence, we can achieve perfect discrimination of factors from non-factors.

6.2. Discrimination property for variable exponents

The discrimination property of the exponential sums rests on the fact that only for integer values of l which are factors of N, the sum can take the value unity. There is a number theoretical argument supporting this fact, as long as the exponent j in the sum (6) is fixed. This feature comes from the distribution of the values $\exp\left(2\pi i m^j \frac{N}{\ell}\right)$ on the unit circle. For fixed j, it is impossible to hit the same point twice as m increases provided we use a truncation

parameter M below $\sqrt[2j]{N}$. However, for a variable power m^m that is an exponential phase, this non-recurrence property is not obvious. In this case we need to prove the discrimination property explicitly.

The value $\exp\left(2\pi \mathrm{i} m^m \frac{N}{\ell}\right)$ depends on the fractional part of $m^m \frac{N}{\ell}$ only. We hit the same point twice for different values m and n if and only if

$$m^m \frac{N}{\ell} - n^n \frac{N}{\ell} = k \tag{29}$$

where k is an integer.

As in (20) we make use of the coprime rational representation of $\rho(N, \ell) = p/q$ and find that the phase factor

$$\exp\left(2\pi \mathrm{i} m^m \frac{N}{\ell}\right) = \exp(2\pi \mathrm{i} m^m \rho(N, \ell)) = \exp\left(2\pi \mathrm{i} \frac{p m^m}{q}\right) \tag{30}$$

is a qth root of unity. In particular, it is the (pm^m)th one if we enumerate them counter-clockwise starting from the zeroth root $1 = \exp\left(2\pi \mathrm{i} \frac{0}{q}\right)$. Note that cth and dth roots coincide if and only if q is a divisor of $c - d$.

So the discrimination property depends on the fact that there are values c and d such that

$$q \text{ is not a divisor of } pc^c - pd^d \,. \tag{31}$$

The discrimination threshold does not only depend on the number of such pairs, but also on the position of the corresponding roots of unity. Opposite roots of unity eliminate themselves in the sum, so the worst case occurs if these roots accumulate on the same position.

We consider two cases: for large q, the first numbers in the sequence pm^m will be below q, so any pair chosen from the beginning of the sequence cannot fulfil the recurrence condition (29), so they correspond to pairwise distinct roots. As a consequence, the absolute value of the sum cannot assume the value unity.

For small q, we show that the pth root $\exp\left(2\pi \mathrm{i} \frac{p}{q}\right)$ and its conjugate $\exp\left(-2\pi \mathrm{i} \frac{p}{q}\right)$ appear in the sum, which leads to the elimination of their imaginary parts. According to Euler's theorem [27] there is an even m such that pm^m corresponds to the first root $\exp\left(2\pi \mathrm{i} \frac{1}{q}\right)$ and $j = m/2$ gives pj^j, which corresponds to the (-1)-root $\exp\left(-2\pi \mathrm{i} \frac{1}{q}\right) = \exp\left(2\pi \mathrm{i} \frac{q-1}{q}\right)$. The sum of this conjugate pair is a real number strictly below unity.

7. Conclusions and outlook

In the present study we have extended the idea of factorization with Gauss sums to exponential sums where the phase is governed by a power j of the summation index. These sums are also capable of non-factor discrimination in complete analogy to Gauss sums. However, the truncation parameter M_j needed to achieve a significant suppression of ghost factors of the number N scales like $M_j \sim \sqrt[2j]{N}$. Hence, we can save experimental resources by employing exponential sums with large powers j. On the other hand the gap between the signal of a factor and the greatest threshold value shrinks as j grows. Therefore, exponential sums with large values of j can be used for integer factorization only if the expected imperfections in the experiment are smaller than this gap.

Our technique to factor numbers takes advantage of the quasi-randomness of the phase factors of exponential sums. This feature makes exponential sums ideal for the use of pseudo-random number generators [28–30]. We look forward to exploring this realm of number theory.

We have also presented numerical simulations of factoring numbers using an exponential sum with exponentially increasing phases. Here the resources scale only logarithmically. Moreover, our results indicate that the gap survives.

Our results also show a connection to two recent experiments [16, 19] which factored a 13-digit and a 17-digit numbers using a Monte Carlo sampling technique of a complete Gauss sum. This method accepts a small fraction of ghost factors and achieves a logarithmic scaling very much in the spirit of the exponential phase.

It is interesting to compare and contrast these two approaches. Ghost factors arise from the addition of neighboring phase factors which only deviate slightly from each other. However, when many terms are added the phase factors are distributed homogeneously on the unit circle. The Monte Carlo technique does not add up consecutive terms but tries to collect those terms which almost cancel each other out. On the other hand, the exponential phase guarantees that neighboring phase factors deviate significantly from each other and no ghost factors can arise. This feature leads to the logarithmic scaling.

Needless to say, these schemes only rely on interference and thus our method for factoring numbers using exponential sums still scales exponentially. To improve this scaling law by involving entanglement is our next goal.

Acknowledgments

We thank J Kimble and A Winterhof for stimulating discussions and B Girard and D Suter for informing us about their experiments [16, 19] 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. M Š is grateful for a stipend from the European Community in the network CONQUEST and for the financial support by MSM 6840770039, MŠSMT LC 06002. Moreover, WPS would also like to thank the Alexander von Humboldt-Stiftung and the Max-Planck-Gesellschaft for receiving the Max-Planck-Forschungspreis. Work of M S Z is supported by the Alexander von Humboldt-Stiftung through the Alexander von Humboldt Research Award.

References

[1] Stenholm S and Suominen K-A 2005 *Quantum Approach to Informatics* (New York: Wiley)
[2] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[3] Schleich W P and Walther H 2007 *Elements of Quantum Information* (New York: Wiley-VCH)
[4] Davenport H 1980 *Multiplicative Number Theory* (New York: Springer)
[5] Maier H and Schleich W P 2008 *Prime Numbers 101: A Primer on Number Theory* (New York: Wiley-VCH)
[6] Clauser J F and Dowling J P 1996 *Phys. Rev.* A **53** 4587
[7] Harter W G 2001 *Phys. Rev.* A **64** 012312
[8] Harter W G 2001 *J. Mol. Spectrosc.* **210** 166
[9] Mack H, Bienert M, Haug F, Freyberger M and Schleich W P 2002 *Phys. Status Solidi* b **233** 408
[10] Mack H, Bienert M, Haug F, Straub F S, Freyberger M and Schleich W P 2002 *Experimental Quantum Computation* ed P Mataloni and F De Martini (Amsterdam: Elsevier)
[11] Merkel W *et al* 2006 *Int. J. Mod. Phys.* B **20** 1893
[12] Merkel W, Averbukh I Sh, Girard B, Paulus G G and Schleich W P 2006 *Fortschr. Phys.* **54** 856
[13] Merkel W, Averbukh I Sh, Girard B and Schleich W P 2007 *Elements of Quantum Information* ed Schleich W P and Walther H (New York: Wiley-VCH)
[14] Mehring M, Müller K, Averbukh I Sh, Merkel W and Schleich W P 2007 *Phys. Rev. Lett.* **98** 120502

[15] Mahesh T S, Rajendran N, Peng X and Suter D 2007 *Phys. Rev.* A **75** 062303
[16] Peng X and Suter D 2008 arXiv: 0803.3396
[17] Gilowski M, Wendrich T, Müller T, Jentsch Ch, Ertmer W, Rasel E M and Schleich W P 2008 *Phys. Rev. Lett.* **100** 030201
[18] Bigourd D, Chatel B, Schleich W P and Girard B 2008 *Phys. Rev. Lett.* **100** 030202
[19] Weber S, Chatel B and Girard B 2007 private communication
[20] Shor P 1994 *Proc. 35th Annual Symp. on Foundations of Computer Science* (New York: IEEE Computer Society)
[21] Štefaňák M, Merkel W, Schleich W P, Haase D and Maier H 2007 *New J. Phys.* **9** 370
[22] Sargent M, Scully M O and Lamb W E 1974 *Laser Physics* (Reading, MA: Addison-Wesley)
[23] Štefaňák M, Merkel W, Mehring M and Schleich W P 2008 *Contemporary Physics: Proc. Int. Symp. (Islamabad)* ed J Aslam, F Hussain and Riazuddin (Singapore: World Scientific)
[24] Suter D 2008 Private communication
[25] Iwaniec H and Kowalski E 2004 *Analytic Number Theory* (Providence, RI: American Mathematical Society)
[26] Heath-Brown D R and Patterson S J 1979 *J. Reine Angew. Math.* **310** 111
[27] Ireland K and Rosen M 1990 *A Classical Introduction to Modern Number Theory* (Heidelberg: Springer)
[28] Niederreiter H and Winterhof A 2008 *Finite Fields Th App* **14** 59
[29] Gutierrez J and Winterhof A 2007 *Finite Fields Th App* **14** 410
[30] Niederreiter H 1987 *Random Number Generation and Quasi-Monte Carlo Methods* (Philadelphia, PA: Society for Industrial Mathematics)