entropy

MDPI

Article

Spectral Signatures of Prime Factorization

Giuseppe Mussardo [1,2,*] and Andrea Trombettoni [2,3]

[1] SISSA, Via Bonomea 265, 34136 Trieste, Italy
[2] INFN Sezione di Trieste, Via Valerio 2, 34127 Trieste, Italy
[3] Department of Physics, University of Trieste, Strada Costiera 11, 34151 Trieste, Italy
* Correspondence: mussardo@sissa.it

Abstract

We present a protocol for integer factorization for all integers N below a certain cut-off $\Lambda = 2^d$, grounded in the theory of quantum measurement. In this framework, the factorization of an integer $N \leq \Lambda$ is achieved in a number of steps equal to the total number I of primes present in its factorization; explicitly, the procedure consists of a sequence of I quantum measurements. The method requires a single-purpose quantum device designed to perform measurements of an observable with a prescribed spectrum. Crucially, the construction of this device involves solving, once and for all, a set of approximately 2^d differential equations, independently of the specific integer to be factorized. We argue that the initialization task of this device can be efficiently implemented on a quantum computer in d steps, thereby decoupling the computational cost of device preparation from the factorization process itself.

Keywords: prime factorization; quantum mechanics; projective measurements

1. Introduction

The aim of this manuscript is not to present a patent-style proposal for a new device intended to outperform existing, highly optimized classical algorithms for integer factorization (or to enable a practical attack on RSA-2048). Instead, our goal here is simply conceptual and theoretical: to show that quantum mechanics offers a natural and elegant framework in which problems arising in a field as distant from quantum theory as number theory can be formulated and, potentially, solved in an optimal way. The emphasis on the conceptual nature of the idea, rather than on its practical or engineering implementation, is unequivocal. Indeed, any attempt to address infinite families of instances (as the infinite set of integers) necessarily encounters a fundamental mismatch between physics and mathematics: physical systems are unavoidably subject to cutoffs and finite resources, whereas mathematics imposes no such limitations. Consequently, even if a given physical setup were capable of factoring a 100-digit integer, it would always remain true that it does not yet handle a 1000-digit integer, and so on without end. For instance, in what follows, the proposed protocol is endowed with a natural cutoff, defined by an integer $\Lambda = 2^d$, which must be specified *ab initio* and determines the range of integers that the device is capable of factorizing.

It is worth observing that analogous considerations apply to the well-known Shor algorithm [1,2] for integer factorization. From a practical standpoint, extending its implementation to cryptographically relevant instances such as RSA-2048 would entail the use of quantum error correction at the scale of millions of physical qubits, together with stringent requirements on the mitigation of decoherence-induced errors. Accordingly, to date, experimental validations of the Shor algorithm have been confined to the factorization of comparatively small integers: the factorization of the number $15 = 3 \times 5$, for instance, was

Received: 17 February 2026
Revised: 9 March 2026
Accepted: 21 March 2026
Published: 23 March 2026

done using 7 qubits with an NMR implementation of a quantum computer [3]. Similar demonstrations were performed using photonic [4,5] and solid-state qubits [6], while in 2012, with the n qubits control register replaced by a single qubit recycled n times, it was achieved the factorization of the integer $21 = 3 \times 7$ [7]. Despite their simplicity, it goes without saying that these examples nevertheless provide a *proof of principle* realization of the algorithm.

Therefore, with the same spirit and the same awareness of the crucial role played by physical constraints in the implementation of a mathematical algorithm such as Shor's, we present below an alternative different route for integer factorization, based on an algorithm which exploits another genuine quantum property: projective quantum measurements [8–10]. As it is well known from quantum mechanics axioms, if a physical system is in a normalised state $|\psi\rangle$, a measurement of an observable $\hat{O}$ will yield one eigenvalue α of its spectrum with probability $|\langle\psi \mid \alpha\rangle|^2$, where $|\alpha\rangle$ is the normalised eigenfunction corresponding to the eigenvalue α

$$\hat{O}\,|\alpha\rangle \;=\; \alpha\,|\alpha\rangle\,. \tag{1}$$

As a result of the measurement, the system state will change from $|\psi\rangle$ to $|\alpha\rangle$ (for a recent discussion on quantum meaurement, see [11]). For problems related to number theory, interesting spectra to consider are: (a) the natural numbers, corresponding to the Hamiltonian of an harmonic oscillator [9,10]; (b) the primes [12,13]; and (c) the logarithm of the primes [14–19]. Employing such spectra, one may translate number theory problems in quantum physical settings. As an example of this general philosophy, in this paper we show that with a suitable choice of the operator $\hat{O}$ is possible to determine the prime factors of an integer number N less than a given cut-off Λ by making a finite set of quantum measurements.

The organization of this article is as follows. After providing a brief overview of classical algorithms for primality testing and integer factorization, we present a quantum algorithm addressing the factorization problem. For expository convenience, the algorithm is initially formulated within the well-established framework of Schrödinger Hamiltonians, wherein the potential terms effectively act as a data repository for integers and prime numbers. Other implementations are, in principle, equally admissible; accordingly, as discussed in the Appendices, we also consider a digital realization of the algorithm. The computational costs of Shor's and our algorithm are thoroughly discussed in the last part of the paper.

2. Classical Primality Tests and Factorization Algorithms

The fundamental theorem of arithmetic states that every natural number N greater than 1 is either a prime number p_k or can be represented as a product of prime numbers

$$N = p_{a_1}^{\alpha_1} p_{a_2}^{\alpha_2} \dots p_{a_k}^{\alpha_k}\;, \tag{2}$$

where $p_{a_1} < p_{a_2} \cdots < p_{a_k}$ are k ordered primes and $\alpha_i \geq 1$ their multiplicity. Hence, prime numbers may be regarded as the atoms of arithmetic but, in contrast with the finitely many chemical elements, the number of primes is instead infinite, as shown by a classic argument by Euclid dated more than 2000 years ago. The appearance of prime numbers along the integer sequence is completely unpredictable. However, their coarse graining properties, and in particular how many prime numbers there are below any real number x, are aspects which can be controlled with remarkable precision. In other words, while there is no known simple function $f(n)$ which gives the n-th prime number p_n (and the actual determination of prime numbers can only be done by means of the familiar Eratosthenes's sieve [20–24]), we have instead perfect knowledge of the inverse function $\pi(x)$ which counts the number of primes below the real number x [20–31]. Such a function was exactly determined by

Riemann (see, for instance [30]): it has a staircase behaviour (since it jumps by 1 each time x crosses a prime), but becomes smoother and smoother for increasing values of x, and its asymptotic behaviour is constrained by the "Prime Number Theorem" [25] stating that $\lim_{x\to\infty} \frac{\pi(x)\ln x}{x} = 1$. Notice that $p_n = \pi^{-1}(n)$. Hence, inverting at the lowest order the function $\pi(x)$, one gets the following scaling law for the n-th prime number: $p_n \simeq n \log n$.

Let us first discuss the primality test. How can one tell whether an integer N is prime? What if the number has hundreds or thousands of digits? This question may seem abstract or irrelevant, but primality tests are performed every time to make online transactions secure. Given an integer N, determine whether or not N is a prime number constitutes a primality test. The naive way to check the primality of an integer N is to divide it by any prime number between 2 and $\sqrt{N}$. Assuming we express the number N in binary basis, if N is of order 2^d, the number of operations $\mathcal{D}$ of this naive primality algorithm scales exponentially with the number of digits, i.e., $\mathcal{D} \sim 2^{d/2}$. Many different algorithms have been proposed, both deterministic or probabilistic nature (see, for instance [32]), to reduce the complexity of the primality test. The final answer was given in 2002 [33] in terms of a deterministic protocol (the AKS test) whose complexity scales as [33] $\mathcal{D}_{AKS} \sim (\log N)^{7.5}$.

Let us now imagine that the primality test outputs that N is not a prime. Then, looking at (2), how do we determine the prime factors $p_{a_1} \dots p_{a_k}$ of the integer N? This is the question addressed by any factorisation algorithm. Let N be a number of n-bit digits: currently there is no classical factorization algorithm whose complexity scales $\mathcal{D} \sim \mathcal{O}(n^\alpha)$ for some constant α. Although neither the existence nor non-existence of such algorithms has been proved, it is generally believed that they do not exist and hence that the problem is not in the class of Polynomial Time Algorithms. If so, then the problem is clearly in class NP, although it is not certain whether it is or is not in the class of NP-complete problems [34–36]. The best classical algorithm known is the so-called general number field sieve (GNFS) [35] whose complexity for a number N scales as $\exp(\ln N)^{1/3}$.

3. The Factorization Algorithm by Quantum Measurements

In the following we discuss how to devise a very efficient algorithm for factorizing integers N less than a given cut-off $\Lambda = 2^d$ using quantum mechanical measurements in a way that the number of steps is finite and does not scale with the n digits of N. For the implementation of the protocol, it is essential to specify *ab initio* the cutoff Λ and to have an a-priori knowledge of all prime numbers $p_n \leq \Lambda$.In our presentation, the operator $\hat{O}$ is the guise of the familiar Hamiltonian $\hat{H}$, but the reader is of course free to substitute the operator $\hat{H}$ with any other hermitian operator with the appropriate spectra. Let us assume that the Hamiltonian $\hat{H}$ is made up of two Hamiltonians $\hat{H}_1$ and $\hat{H}_2$ which commute to each other:

$$\hat{H} = \hat{H}_1 + \hat{H}_2\,, \qquad [\hat{H}_1, \hat{H}_2] = 0\ . \tag{3}$$

We choose $\hat{H}_1$ to have Λ eigenvalues given by the logarithms of the primes, where $\Lambda = 2^d$ is a fixed cut-off

$$E_n^{(1)} = \log p_n\,; \quad n = 1, 2, 3, \cdots 2^d\,. \tag{4}$$

The corresponding eigenfunctions will be denoted as $|\log p_n\rangle$.

On the other hand, the second term $\hat{H}_2$ in the Hamiltonian $\hat{H}$ is chosen to have the eigenvalues given by the logarithms of the integers, up to the same cut-off Λ, i.e.,

$$E_m^{(2)} = \log m\,; \quad m = 1, 2, 3, \dots 2^d\,. \tag{5}$$

The corresponding eigenvectors will be denoted as $|\log m\rangle$. As discussed below, these Hamiltonians H_1 and H_2 could in principle be realised in a laboratory by means of spatial

light laser modulators, as it was recently done for a Hamiltonian which had the prime numbers as quantum spectrum [13].

The generic eigenfunctions of $\hat{H}$ are then given by

$$|\log p_n\rangle\,|\log m\rangle\,, \tag{6}$$

which correspond to the eigenvalues $E_{n,m} \equiv \log p_n + \log m$.

The factorization problem of a natural number N consists of finding the primes entering its decomposition (2). In order to do so, our protocol consists of the following steps.

1. Take initially the logarithm of the number N to be factorized, promote it to be an eigenvalue of the Hamiltonian $\hat{H}$ and prepare the initial state, hereafter denoted as $|\log N\rangle$, which has this energy.
2. For an integer N—as the one given in Equation(2)—made of k distinct primes, the corresponding energy level of $\hat{H}$ is k-fold degenerate, i.e., the degeneracy of the level depends *only* on the number of distinct primes present in N and not on their multiplicities. Indeed, $\log N$ can be written in the following k different ways

$$\begin{aligned}
\log N &= \log p_1 + \log\left(p_1^{a_1-1} p_2^{a_2} ... p_{k-1}^{a_{k-1}} p_k^{a_k}\right) \equiv \\
&\equiv \log p_1 + \log \tilde{N}_1 \\
\log N &= \log p_2 + \log\left(p_1^{a_1} p_2^{a_2-1} .. p_{k-1}^{a_{k-1}} p_k^{a_k}\right) \equiv \\
&\equiv \log p_2 + \log \tilde{N}_2 \\
&\dots \\
\log N &= \log p_k + \log\left(p_1^{a_1} p_2^{a_2} ... p_{k-1}^{a_{k-1}} p_k^{a_k-1}\right) \equiv \\
&\equiv \log p_k + \log \tilde{N}_k
\end{aligned}$$

   where $\tilde{N}_a \equiv N/p_a$ is the integer obtained dividing the original number N by one of its prime factor p_a.
3. Hence, the generic state of the k-th degenerate manifold with energy $\log N$ (as before, here simply denoted as $|\log N\rangle$) admits the expansion

$$|\log N\rangle \;=\; \sum_{a=1}^{k} c_a |\log p_a\rangle |\log N_a\rangle\,, \tag{7}$$

   with $\sum_{a=1}^{k} |c_a|^2 = 1$. For a generic state, we can assume that all coefficients of this expansion are different from zero. Their values are actually not essential for the running of the algorithm, so one may assume to be randomly distributed, as would occur in the case of a random initial state preparation.
4. After the state (7) is prepared, measure $\hat{H}_1$. With all coefficients c_a different from zero, the output will be the logarithm of one of the primes present in N, say $\log p_b$, with probability $|c_b|^2$.
5. Once the result of this measurement is known, divide the original number N by the prime p_b identified by the output of the $\hat{H}_1$ measurement. In this way, one obtains the lower integer $\tilde{N}_b = N/p_b$. Then, start over, taking $\tilde{N}_b$ as the integer to be factorized. The procedure will halt after a number of iterations l equal to the total number of primes present in N, i.e.,

$$I \;=\; \sum_{l=1}^{k} \alpha_l \;. \tag{8}$$

Notice that the number of quantum measurements can be made equal to the number of distinct factors substituting the previous point 5 with this new one.

6. Once the result of this measurement is known, divide the original number N by the prime p_b identified by the output of the $\hat{H}_1$ measurement. In this way one obtains the lower integer N/p_b. Use a classical computer to continue to divide for p_b till the obtained number is not longer divisible for p_b. In this way, one obtains the multiplicity α_b associated to the factor p_b. Then, start the procedure again, taking $\tilde{N}_b = N/p_b^{\alpha_b}$ as the integer to be factorized.

Three significant remarks are in order:

- A primality test can be immediately implemented by performing a single quantum measurement of $\hat{H}_1$ on the initial state $|\log N\rangle$. If the system collapses (remains) in itself, N is a prime.
- If the multiplicity of the last factor, say p_k, to be factorized is 1, then the last operation with the measurement of $\hat{H}_1$ actually amounts to apply the identity operator. If the multiplicity is different from 1, i.e., $\alpha_k > 1$, then α_k subsequent quantum measurements of $\hat{H}_1$ will produce each time with probability 1 the same eigenstate $|\log p_k\rangle$.
- The successful implementation of the algorithm is guaranteed independently of the $\hat{H}_1$ outputs obtained at the various stages of the algorithm. It is an *all roads lead to Rome* procedure. As shown in Figure 1, there are possible branches resulting from successive measurements of $\hat{H}_1$. Imagine, for instance, that we want to factorize the number $N = 231$, whose prime decomposition is given by $N = 3 \times 7 \times 11$. As a result of the first measurement, we could have one of three possible outputs: $\log 3$, $\log 7$ or $\log 11$.
    1. If the first output is $\log 3$, the next integer to be factorized is $\tilde{N}_3 = 77$ and the next measurement of H_1 starting from the (log) of this number can give, as output, either $\log 7$ or $\log 11$. Once this last measurement is made, the next number is uniquely determined, thus, arriving to the complete factorization of the number $N = 231$. It is easy to see that the same conclusion will be reached if there is a different initial output.
    2. If the first output is $\log 7$, the next integer to be factorized is $\tilde{N}_7 = 33$ and the next measurement of H_1 starting from the (log) of this number, can give, as output, either $\log 3$ or $\log 11$. Once this last measurement is made, the next number is uniquely determined, thus arriving to the complete factorization of the number $N = 231$.
    3. If the first output is $\log 11$, the next integer to be factorized is $\tilde{N}_{11} = 21$ and the next measurement of H_1 starting from the (log) of this number can give, as output, either $\log 3$ or $\log 7$. Once this last measurement is made, the next number is uniquely determined, thus, arriving at the complete factorization of the number $N = 231$.

The key feature of this algorithm is the projective quantum measurements of hermitian operators, such as the Hamiltonians we have employed. This leads to an algorithm with the least possible number of operations, equal to k, relative to the factorization of an integer made of k primes, see below for a discussion of this point.

Given that quantum mechanics is based on linear algebra while the mathematical problem relative to factorization involves products, Hamiltonians with logarithm of the primes as spectrum are very natural to study and have been also used before [15–18]. In more detail, a thermally isolated non-interacting Bose gas loaded in a one-dimensional potential with logarithmic energy eigenvalues was discussed in [15], where asymptotic formulas for factorising products of different primes were provided. Time-dependent perturbation in (possibly multiple copies of) a potential having logarithms of the primes as eigenvalues was instead proposed in [16–18], where the number N to be factorized is encoded in the frequency of a sinusoidally modulated interaction acting on the ground-

state of the potential. In this approach, if the integer is a product of k primes, one needs to prepare an ensemble of k identical systems each with an energy spectrum given by the logarithm of the primes [18]. Recently, a paper discussed the possible use of a Hamiltonian having as eigenvalues the logarithm of the primes for search algorithm [37].

Our approach differs from the one discussed in [18] for two key features: first, the presence of $\hat{H}_2$ in our Hamiltonian and, secondly, the use of quantum measurements. Employing our Hamiltonian, made of a piece relative to the logarithm *and* another one relative to the logarithm of the integers, it is possible to factorize an integer N without knowing a-priori the number k of distinct primes (and their multicplicities) this number N is made of. Concerning the quantum measurement of $\hat{H}_1$, one could use the von Neumann scheme [38], which consists of setting up a coupling with a test particle of the form $\hat{p}\,\hat{O}$, where $\hat{p}$ is the momentum operator of the test particle and $\hat{O}$ the operator to be measured. As a matter of fact, the explicit implementation of the von Neumann measurement scheme constitutes a problem of intrinsic interest, warranting a separate and detailed investigation, which will be presented in forthcoming work [39]. For the purposes of the present analysis, it is sufficient to assume that the operator $\hat{H}_1$ is measurable, as is the case for any quantum observable.

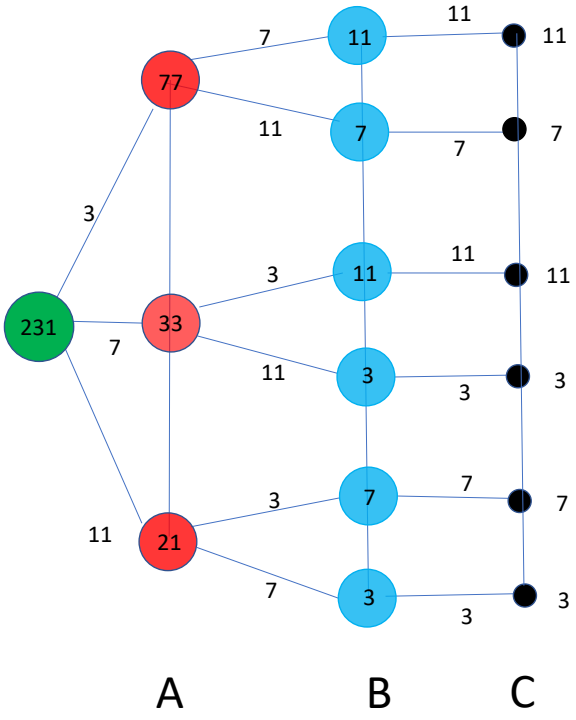

Figure 1. The graph associated with the various quantum measurements of $\hat{H}_1$ which pin down the different prime factors of N. In the example shown in the figure, the number to factorize is $N = 231 = 3 \times 7 \times 11$. For simplicity, along the links of the graph, we indicate the primes (rather than their logarithm) which are the outputs of the three stages A, B, C measurements of $\hat{H}_1$. One gets a complete factorisation independently of the path associated with the chain of $\hat{H}_1$ measurements.

4. Quantum Potentials

Let us now discuss a possible implementation of the algorithm described in the previous section. Essentially, we require a convenient database of natural numbers and prime numbers below a given cutoff Λ. One possible approach is to encode these numbers as spectra of Schrödinger Hamiltonians. This is similar to what has been done recently [13] for a quantum potential of the primes. Hence, we will deal with Hamiltonians of a particle of mass m of the form $\hat{H} = p^2/2m + V(x)$ with their eigenvalues determined by the Schrödinger equation $\hat{H}\psi_n = e_n\psi_n$.

A potential $\mathcal{V}_N(x)$ entering a Schrödinger Hamiltonian with a finite and assigned number of eigenvalues $\{e_0, e_1, ..., e_M\}$ can be constructed using methods of Supersymmetric Quantum Mechanics (SQM) [40–42]. The protocol is as follows:

1. First of all, we subtract from all the eigenvalues e_n the highest one e_N, so that the new set of numbers $\{\tilde{E}_n\}$
$$\tilde{E}_k \;=\; e_{N-k} - e_N, \quad k = 0, 1, \ldots, N, \tag{9}$$
will be considered as the new spectrum. The $\tilde{E}_k$'s are of course the (negative) gaps computed from the *highest* eigenvalue e_N. Notice that, consistently, they are enumerated starting from the top to the bottom, so $\tilde{E}_0 = 0$, $\tilde{E}_1$ is the first gap, $\tilde{E}_2$ the second gap, and so on. A potential $\mathcal{V}(x)$ where its only eigenvalue is $\tilde{E}_0 = 0$ is of course $\mathcal{V}_0(x) = 0$. This potential is used as input for the Riccati equation for the super-potential $W_1(x)$
$$W_1'(x) - W_1^2(x) + \mathcal{V}_0(x) \;=\; \tilde{E}_1 \tag{10}$$
with boundary condition $W_1(0) = 0$.
2. Once such a function $W(x)$ has been obtained, one can construct another potential $\mathcal{V}_1(x)$ as
$$\mathcal{V}_1(x) \;=\; 2\tilde{E}_1 + 2W_1^2(x) - \mathcal{V}_0(x) \;. \tag{11}$$
This potential is then substituted into Equation (10) (i.e., $\mathcal{V}_1(x) \to \mathcal{V}_0(x)$, substituting also $\tilde{E}_1 \to \tilde{E}_2$), so that one has a differential equation for another super-potential $W_2(x)$
$$W_2'(x) - W_2^2(x) + \mathcal{V}_1(x) \;=\; \tilde{E}_2 \;, \tag{12}$$
3. Proceeding iteratively in this way, one has a recursive sequence of differential equations
$$\begin{aligned} &W_k'(x) - W_k^2(x) + \mathcal{V}_k(x) \;=\; \tilde{E}_k \;, \\ &\mathcal{V}_k(x) = 2\tilde{E}_k + 2W_k^2(x) - \mathcal{V}_{k-1}(x) \end{aligned} \tag{13}$$
with all of them being solved with the boundary condition $W_k(0) = 0$, which ensures that the final potential $\mathcal{V}(x) = \mathcal{V}_N(x)$ is an even function. This recursive system is continued until all the gaps have been taken into account. Hence, solving (in general numerically) the differential equations of Equation (13), one arrives to the Hamiltonian which has *exactly* the spectrum $\{e_n\}$
$$H \;=\; -\frac{d^2}{dx^2} + \mathcal{V}_N(x) + e_N \;, \tag{14}$$

These are indeed the theoretical steps which lead to the potential $V_N(x)$ with *exactly* the first M prime numbers [13,42] or the logarithm of the first M primes [14].

To conclude the implementation of our algorithm, let us then define the potentials $V_1(x)$ and $V_2(y)$ entering the two Schrödinger Hamiltonians $\hat{H}_1$ and $\hat{H}_2$ of the previous section (it is worth recalling that both potentials $V_1(x)$ and $V_2(y)$ can be also constructed in a semi-classical approximation [12] for *all* primes and integers.)
$$\hat{H}_1(x) \;=\; \frac{p_x^2}{2m} + V_1(x), \quad \hat{H}_2(y) \;=\; \frac{p_y^2}{2m} + V_2(y), \tag{15}$$
where p_x and p_y are the x and y components of its momentum, and such $\hat{H}_1$ ($\hat{H}_2$) has as eigenvalues the logarithm of the first 2^d primes (respectively, the logarithm of the first 2^d integers). The plot of $V_1(x)$ and $V_2(y)$ in a specific case is shown in Figure 2. Incidentally, if the Goldbach conjecture were true, taking the same Hamiltonian $\hat{H}_1$ in both the x and y

direction, i.e., $\mathcal{H} = \hat{H}_1(x) + \hat{H}_1(y)$, the spectrum of $\mathcal{H}$ would be given by the logarithms of *all* even numbers.

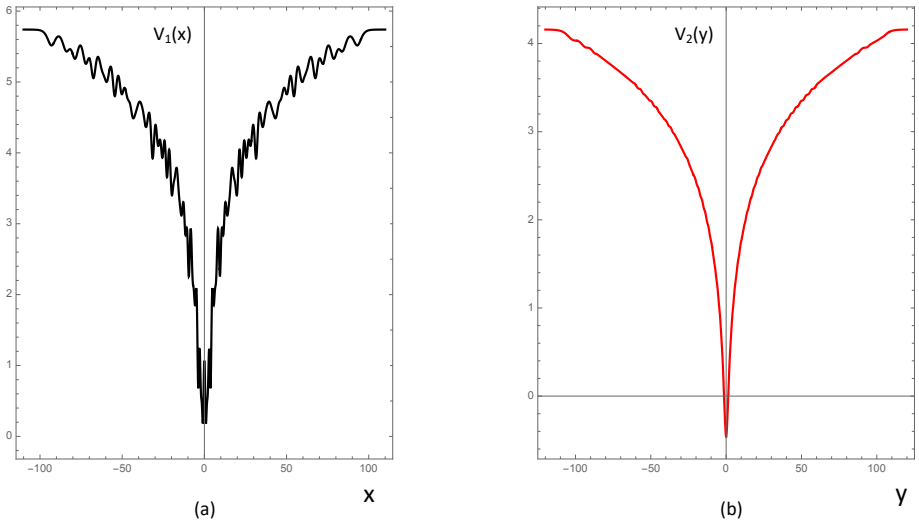

Figure 2. Plots of the potentials $V_1(x)$ (**a**) and $V_2(y)$ (**b**) relative to $\Lambda = 64 = 2^5$ energy levels given respectively by the logarithm of the primes, $\log p_k$, and the logarithm of the integers, $\log m$.

5. Discussion and Conclusions

Once we have the two Hamiltonians $\hat{H}_1$ and $\hat{H}_2$, we can build up the Hamiltonian $\hat{H} = \hat{H}_1 + \hat{H}_2$ and proceed to factorize the integers N below the cut-off Λ through a sequence of k measurements of $\hat{H}_1$, where k is the number of different prime factors the number N is made of. As an example, if N is a product of three primes, only three quantum measurements are needed.

One can show that k is clearly the lower bound of operations which are needed to factorize an integer, independently from quantum mechanics. Indeed, suppose that the integer N has the form (2) and that one is given the information that $p_1, \cdots, p_k$ are its factors. To verify it, one would divide by one of them, say p_1, and continue by it till it is possible ($\alpha_1 + 1$ divisions), and so on, for a total of $\sum_{i=1}^{k} \alpha_i + k$ divisions. If one is also provided the information about the multiplicities, then only k divisions are needed. In the latter case, the last division is trivial.

The procedure proposed here saturates such lower bounds. Indeed, from the first quantum measurement one gets one of the factors, and then divides N (e.g., using a classical computer) by the latter till the obtained number is no longer divisible. Iterating this way one needs k quantum measurements (the last, k-th, being equal to the identity) and $\sum_{i=1}^{k} \alpha_i$ divisions on the classical computer. One sees that the factorization based on quantum measurements saturates the lower bound, whether the multiplicities are given or they are not.

Underlying this procedure, however, is the nontrivial problem of constructing a data repository for integers and prime numbers below a prescribed cutoff $\Lambda = 2^d$. If this information is encoded in the potentials of two Schrödinger Hamiltonians, the task amounts to solving a system of Λ coupled Riccati equations. This issue is more appropriately regarded as a hardware-level rather than a software-level problem, in the sense that it must be addressed once and for all in order to enable access to the factorization of all integers $N \leq \Lambda$. A noteworthy observation is that the computational complexity of this construction scales as $\log \Lambda = d$, as argued in [43]. Indeed, it was discussed in [43] that a system of M, possibly non-linear, differential equations of the form

$$\frac{d\vec{W}}{dx} + \mathbf{f}(W) \cdot \vec{W} = \vec{b}\,, \tag{16}$$

where $\mathbf{f}$ is a $M \times M$ matrix and $\vec{b}$ is a constant vector, can be solved on a quantum computer in $\log M$ number of steps. Namely, there is an exponential speed up which turns our problem to adjust an exponential number 2^d of eigenvalues in each of the Hamiltonians H_1 and H_2 in terms of only d computational steps.

$$f_{ab} = \begin{cases} 0 & , \quad a > b \\ -W_a & , \quad a = b \\ (-1)^a 2W_b & , \quad a < b \end{cases} \tag{17}$$

and

$$b_k = \tilde{E}_k + 2\sum_{i=1}^{k-1}(-1)^i \tilde{E}_{k-i}\,. \tag{18}$$

Hence the exponential growth of complexity of our procedure which arises at its hardware level can be cured using an ordinary quantum computer.

In summary, the factorization procedure proposed in this paper for all integers N less than a given cut-off $\Lambda = 2^d$ consists in two distinct parts: (i) the implementation of an integer and prime data repository which consists in solving 2^d differential equations, a task which an universal quantum computer can solve in d number of steps, i.e., in. polynomial time; (ii) a series of k quantum measurements, where k is the number of different primes entering the prime decomposition of the integer N.

Author Contributions: The authors contribute equally to the content of the article. Conceptualization, G.M. and A.T.; Methodology, G.M. and A.T.; Validation, G.M. and A.T.; Formal analysis, G.M. and A.T.; Writing—original draft, G.M. and A.T.; Writing—review and editing, G.M. and A.T.; Funding acquisition, G.M. and A.T. All authors have read and agreed to the published version of the manuscript.

Funding: We acknowledge financial support from PNRR M4C2I1.3 PE 00000023 NQSTI Grant, Spoke A2, funded by NextGenerationEU. G.M. also acknowledges PR03 Quantum Pathfinder while A.T. also acknowledges the MIT-FVG Seed Fund Collaboration Grant "Non-Equilibrium Thermodynamics of Dissipative Quantum Systems".

Data Availability Statement: The original contributions presented in this study are included in the article material. Further inquiries can be directed to the corresponding author

Acknowledgments: We thank D. Bernard, M. Berry, J. L. Cardy, D. Cassettari, A. Schwimmer and A. Smerzi for useful discussions and correspondence. G.M. acknowledges the Indian Institute of Technology of Chennai (India) while A.T. acknowledges MIT for kind hospitality during the writing of the final part of the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Shor, P.W. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*; Goldwasser, S., Ed.; IEEE Computer Society: Los Alamitos, CA, USA, 1994; pp. 124–134.
2. Shor, P.W. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A* **1995**, *52*, R2493. [CrossRef] [PubMed]
3. Vandersypen, L.M.K.; Steffen, M.; Breyta, G.; Yannoni, C.S.; Sherwood, M.H.; Chuang, I.L. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature* **2001**, *414*, 883–887. [CrossRef] [PubMed]
4. Lu, C.Y.; Browne, D.E.; Yang, T.; Pan, J.W. Demonstration of a Compiled Version of Shor's Quantum Factoring Algorithm Using Photonic Qubits. *Phys. Rev. Lett.* **2007**, *99*, 250504. [CrossRef]
5. Lanyon, B.P.; Weinhold, T.J.; Langford, N.K.; Barbieri, M.; James, D.F.V.; Gilchrist, A.; White, A.G. Experimental Demonstration of a Compiled Version of Shor's Algorithm with Quantum Entanglement. *Phys. Rev. Lett.* **2007**, *99*, 250505. [CrossRef] [PubMed]
6. Lucero, E.; Barends, R.; Chen, Y.; Kelly, J.; Mariantoni, M.; Megrant, A.; O'Malley, P.; Sank, D.; Vainsencher, A.; Wenner, J.; et al. Computing prime factors with a Josephson phase qubit quantum processor. *Nat. Phys.* **2012**, *8*, 719. [CrossRef]
7. Martín-López, E.; Laing, A.; Lawson, T.; Alvarez, R.; Zhou, X.Q.; O'Brien, J.L. Experimental realization of Shor's quantum factoring algorithm using qubit recycling. *Nat. Photonics* **2012**, *6*, 773–776. [CrossRef]

8. Peres, A. *Quantum Theory: Concepts and Methods*; Kluwer Academic Publishers: Dordrecht, The Netherlands, 1993.
9. Shankar, R. *Principles of Quantum Mechanics*, 2nd ed.; Plenum Press: New York, NY, USA, 1994.
10. Sakurai, J.J.; Napolitano, J. *Modern Quantum Mechanics*, 3rd ed.; Cambridge University Press: Cambridge, UK, 2020.
11. Allahverdyan1, A.E.; Balian, R.; Nieuwenhuizen, T.M. Teaching ideal quantum measurement, from dynamics to interpretation. *Comptes Rendus. Phys.* **2024**, *25*, 251–287. [CrossRef]
12. Mussardo, G. The quantum mechanical potential for the prime numbers. *arXiv* **1997**, arXiv:cond-mat/9712010. [CrossRef]
13. Cassettari, D.; Mussardo, G.; Trombettoni, A. Holographic realization of the prime number quantum potential. *PNAS Nexus* **2022**, *2*, pgac279. [CrossRef]
14. Mack, R.; Dahl, J.P.; Moya-Cessa, H.; Strunz, W.T.; Walser, R.; Schleich, W.P. Riemann ζ function from wave-packet dynamics. *Phys. Rev. A* **2010**, *82*, 032119. [CrossRef]
15. Weiss, C.; Page, S.; Holthaus, M. Factorising numbers with a Bose-Einstein condensate. *Phys. A* **2004**, *341*, 586–596 [CrossRef]
16. Gleisberg, F.; Mack, R.; Vogel, K.; Schleich, W.P. Factorization with a logarithmic energy spectrum. *New J. Phys.* **2013**, *15*, 023037. [CrossRef]
17. Gleisberg, F.; Volpp, M.; Schleich, W.P. Factorization with a logarithmic energy spectrum of a two-dimensional potential. *Phys. Lett. A* **2015**, *379*, 2556–2560 [CrossRef]
18. Gleisberg, F.; Pumpo, F.D.; Wolff, G.; Schleich, W.P. Factorization with a logarithmic energy spectrum of a quantum system. *J. Phys. At. Mol. Opt. Phys.* **2018**, *51*, 035009. [CrossRef]
19. Mussardo, G.; Trombettoni, A.; Zhang, Z. Prime Suspects in a Quantum Ladder. *Phys. Rev. Lett.* **2020**, *125*, 240603. [CrossRef]
20. Ribenboim, P. *The New Book of Prime Number Records*; Springer: Berlin/Heidelberg, Germany; New York, NY, USA, 1996.
21. Schroeder, M.R. *Number Theory in Science and Communication*; Springer: Berlin/Heidelberg, Germany, 1990.
22. Zagier, D. The first 50 million prime numbers. *Math. Intell.* **1977**, *1*, 7–19. [CrossRef]
23. Granville, A.; Martin, G. Prime Number Races. *Am. Math. Mon.* **2006**, *113*, 1–33. [CrossRef]
24. Rose, H.E. *A Course in Number Theory*; Oxford Science Publications: Oxford, UK, 1994.
25. Hardy, G.H.; Wright, E.M. *An Introduction to the Theory of Numbers*; Oxford University Press: Oxford, UK, 1979.
26. Apostol, T.M. *Introduction to Analytic Number Theory*, 5th ed.; Springer: New York, NY, USA, 1998.
27. Tao, T. Structure and randomness in the prime numbers. In *An Invitation to Mathematics*; Schleicher, D., Lackmann, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2011.
28. Ore, O. *Number Theory and Its History*; McGraw-Hill: New York, NY, USA, 1948.
29. Riemann, B. Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse. *Monatsberichte Königlichen Preuss. Akad. Wiss. Berlin* **1859**, *2*, 671–680.
30. Edwards, H.M. *Riemann Zeta Function*; Academic Press: New York, NY, USA, 1974.
31. Borwein, P.; Choi, S.; Rooney, B.; Weirathmueller, A. *The Riemann Hypothesis: A Resource for the Afficionado and Virtuoso Alike*; Springer: New York, NY, USA, 2007.
32. Rempe-Gillen, L.; Waldecker, R. *Primality Testing for Beginners*; American Mathematical Society: Providence, RI, USA, 2014.
33. Agrawal, M.; Kayal, N.; Saxena, N. Primes is in P. *Ann. Math.* **2004**, *160*, 781–793. [CrossRef]
34. Lenstra, A.K. Integer factoring. In *Encyclopedia of Cryptography and Security*; van Tilborg, H.C.A., Jajodia, S., Eds.; Springer: Boston, MA, USA, 2011; p. 611.
35. Crandall, R.; Pomerance, C. *Prime Numbers: A Computational Perspective*, 1st ed.; Springer: New York, NY, USA, 2001.
36. Wagstaff, S.S. The Joy of Factoring. In *Student Mathematical Library*; American Mathematical Society: Providence, RI, USA, 2013; Volume 68.
37. Allahverdyan, A.E.; Petrosyan, D. Dissipative search of an unstructured database. *Phys. Rev. A* **2022**, *105*, 032447 [CrossRef]
38. von Neumann, J. *Mathematical Foundations of Quantum Mechanics*; Princeton University Press: Princeton, NJ, USA, 1955.
39. Mussardo, G.; Trombettoni, A. INFN Sezione di Trieste, Via Valerio 2, Trieste, Italy. 2026; *manuscript in preparation*.
40. Cooper, F.; Khare, A.; Sukhatme, U. Supersymmetry and Quantum Mechanics. *Phys. Rep.* **1995**, *251*, 267–385. [CrossRef]
41. Ramani, A.; Grammaticos, B.; Caurier, E. Fractal potentials from energy levels. *Phys. Rev. E* **1995**, *51*, 6323–6331. [CrossRef]
42. van Zyl, B.P.; Hutchinson, D.A. Riemann zeros, prime numbers, and fractal potentials. *Phys. Rev. E* **2003**, *67*, 066211. [CrossRef]
43. Lloyd, S.; Palma, G.D.; Gokler, C.; Kiani, B.; Liu, Z.; Marvian, M.; Tennie, F.; Palmer, T. Quantum algorithm for nonlinear differential equations. *arXiv* **2020**, arXiv:2011.06571. [CrossRef]