Quantum Simulation of the Factorization Problem

Jose Luis Rosales* and Vicente Martin†
Center for Computational Simulation, ETS Ingenieros Informáticos, Universidad Politécnica de Madrid, Campus Montegancedo, E28660 Madrid, Spain

(Received 1 December 2015; revised manuscript received 20 July 2016; published 10 November 2016)

Feynman's prescription for a quantum simulator was to find a Hamitonian for a system that could serve as a computer. The Pólya-Hilbert conjecture proposed the demonstration of Riemann's hypothesis through the spectral decomposition of Hermitian operators. Here we study the problem of decomposing a number into its prime factors, $N = xy$, using such a simulator. First, we derive the Hamiltonian of the physical system that simulates a new arithmetic function formulated for the factorization problem that represents the energy of the computer. This function rests alone on the primes below $\sqrt{N}$. We exactly solve the spectrum of the quantum system without resorting to any external *ad hoc* conditions, also showing that it obtains, for $x \ll \sqrt{N}$, a prediction of the prime counting function that is almost identical to Riemann's $R(x)$ function. It has no counterpart in analytic number theory, and its derivation is a consequence of the quantum theory of the simulator alone.

DOI: 10.1103/PhysRevLett.117.200502

The computational complexity assumption [1] to find the prime factors of a large number N is the basis for the security of the ubiquitous RSA, a cornerstone of the public key cryptosystems so widely used in our digital society. However, despite the many mathematical and computational advances, the classical complexity of the factorization problem is still unknown. Fortunately, the best classical algorithms known scale worse than polynomially in the number of bits of N: by now, the building blocks of the cyberinfrastructure still resist.

Nonetheless, in the quantum world, factoring is an easy problem that requires only polynomial resources using Shor's algorithm [2]. This amazing result raises new questions about the relationship between quantum mechanics and number theory and, more generally, with physics, a connection dating back to Pólya and Hilbert [3,4], who laid a program to prove Riemann's hypothesis through the spectrum of physical operators. However, the physical realization of Shor's algorithm is still limited to proof-of-concept demonstrations, far away from factoring numbers of the size used in real-world cryptosystems.

An alternative would be to build the solutions in Hilbert space of a quantum simulator performing factorization, instead of going through the route of a gate-based, fully programmable, quantum computer. The key idea following the pioneering suggestions of Feynman [5] is to translate factoring arithmetics into the physics of a device whose superposition of states mimics the problem: i.e., a factoring (analog) computer. The states of the simulator would be the solutions of some Hermitian operator depending only on the number that we want to factorize. Moreover, by simply using the computer over different values of N, a quantum factoring simulator must be capable of accessing the statistics of the prime numbers. Thus, it might provide insight into fundamental problems in number theory following the Pólya-Hilbert program. Here we propose a new approach to the factorization problem based on the physics of a bounded Hamiltonian that corresponds to a new arithmetic function defined for this problem. The values of this new function should correspond, in the quantum theory, to eigenvalues of the simulator. To the best of our knowledge, this is the first example of a quantum system whose spectrum supports the Pólya-Hilbert conjecture.

First, to bind the Hamiltonian, we need a problem definition leading to a finite Hilbert space. For this we define a factorization ensemble for a given N [6]. Suppose that we want to factorize N. A simple trial division algorithm will require us to inspect all the primes x less than or equal to $\sqrt{N}$; i.e., a total of $\pi(\sqrt{N})$ trials will be required. The factorization ensemble of N is defined as the set of all pairs of primes that when multiplied give numbers N_k with the property $\pi(\sqrt{N_k}) = j$, where $j = \pi(\sqrt{N})$.

The solution to the factorization problem consists then in finding the appropriate pair in the factorization ensemble that we will denote as $\mathcal{F}(j)$.

Then, to build a bridge between number theory and quantum mechanics, we redefine the factorization problem introducing a single-valued arithmetic function computed for a pair of primes (x_k, y_k) in the ensemble of N. After, we transform this function into a Hamiltonian mapping the arithmetics of factorization to the physics of a classical system; finally, we obtain the quantum observable (operator) corresponding to the energies of the classical counterpart. Thus, obtaining the factor of N is equivalent to measuring the energy of this simulator.

The cardinality of the factorization ensemble is, thus, important, since, given this interpretation, it is the

dimension of the Hilbert space associated with the observable. It can be derived [6] as a corollary of theorem 437 in [7] for the special case of the product of two primes,

$$|\mathcal{F}(j)| \simeq \sqrt{N}(\log\log\sqrt{N} + o(1)) \sim \sum_{x_k=2}^{\sqrt{N}} \frac{\sqrt{N}}{x_k}, \quad (1)$$

where the sum is taken over the primes. Moreover, given these estimates, one would expect $\sqrt{N}/x_k$ as the number of possible different coprimes y_k per each x_k. The new arithmetic function that represents the Hamiltonian of the system should be symmetric in the factors of N and also include an explicit dependence on j.

A simple function with these properties for $N_k = x_k y_k \in \mathcal{F}(j)$ is

$$E(x_k, y_k) = \frac{\pi(x_k)\pi(y_k)}{j^2}, \quad (2)$$

where $\pi(x)$ is the prime counting function. Note that knowing an exact rational value of E, there necessarily exists a single solution of the equation $E = \pi(x)\pi(N/x)/j^2$ in the ensemble. Obviously, $E = E(x)$. Moreover, the behavior of $E(x)$, similar to $\pi(x)$, has two components: a regular plus a oscillatory one [6],

$$E(x) = 1 + \epsilon(N, x),$$

where $\epsilon(N, x) = u(N, x)^2 + \epsilon_{fl}(N, x)$.

Here, $\epsilon_{fl}(N, x)$, the oscillating function, depends on the zeros of Riemann's ζ [9], while u is a regular function that can be approximated for $N \gg 1$ as

$$u(N, x) = \gamma \log(\sqrt{N}/x), \quad (3)$$

where $\gamma = j/\sqrt{N} \sim 1/\log(\sqrt{N})$.

Let us introduce now two new arithmetic functions:

$$p = \frac{\pi(y) - \pi(x)}{2j}, \qquad q = \frac{\pi(y) + \pi(x)}{2j}. \quad (4)$$

Of course, these are related to E, because after Euclid's factorization theorem there exist a single free parameter for the problem of factoring N (the factor x or, as we have reformulated here, the value E)

$$-p^2 + q^2 = E, \quad (5)$$

which has the form of the energy of the classical inverted harmonic oscillator whose trajectories can be parametrized as $q = E^{1/2}\cosh(t)$. From this point of view, along with the computation of E from Eq. (5), we might also consider variations in p and q due entirely to changes in t at constant E. For large N, t can be considered a quasicontinuum parameter, and it has indeed the meaning of the time variable in Hamilton's equations (i.e., E is an adiabatic invariant of the variation),

$$\delta p = -\partial_q H \delta t, \qquad \delta q = \partial_p H \delta t, \quad (6)$$

H being the Hamiltonian on the canonical coordinates p and q,

$$H(p, q) = \frac{1}{2}(-p^2 + q^2). \quad (7)$$

Moreover, $p = \partial_q S(q)$, in terms of Hamilton's principal function (the action) $S(q)$ obtaining the Hamilton-Jacobi equation

$$H(\partial_q S(q), q) = E/2. \quad (8)$$

Equation (8) is relevant because q must be bounded in $\mathcal{F}(j)$, and, therefore, its solutions are confined trajectories in parametric space,

$$\sqrt{E} \le q \le \frac{\pi(N/x_m) + \pi(x_m)}{2j} = q_m \quad (9)$$

for some x_m in $\mathcal{F}(j)$.

Now, the Hamilton-Jacobi constraint for $S(q)$ and quantum transformation theory allow us to obtain the momentum operator acting on the wave functional $\psi_E(q)$ for the q numbers $p \to -i\partial_q$; the Hamiltonian constraint in Eq. (5) becoming a Hermitian operator in our coordinates acting on ψ. It is interesting to note that the same Hamiltonian has been used previously, although through a different canonical transformation, in the study of the distribution of Riemann's zeros [10].

Hence, Eq. (5) transforms into

$$\psi_E(q)'' + q^2\psi_E(q) = E\psi_E(q), \quad (10)$$

our coordinate space satisfies $E^{1/2} \le q \le q_m$, and our quantum conditions should be

$$\psi_E(E^{1/2}) = 0, \qquad \psi_E(q_m(N)) = 0. \quad (11)$$

The Schrödinger Eq. (10) and the Sturm-Liouville conditions in Eq. (11) define the eigenvalue problem leading to the quantization of E. It is important to note here that we do not have to impose any *ad hoc* constraints to the wave function in order to reach the limits required for quantization. Now, a coordinate transformation $\rho = q^2$ and $\psi_E = R_E(\rho)\rho^{3/4}$ gives

$$R_E'' + \frac{2}{\rho}R_E' - \frac{l(l+1)}{\rho^2}R_E + 2\mu\left(r^2 - \frac{z^2}{\rho}\right)R_E = 0, \quad (12)$$

where $l=-1/4$, $\mu=1/2$, $r=1/2$, and $z^2=E/4$ transforms our equation in the tridimensional Schrödinger equation for the Coulomb scattering of two identical charged particles in their center of mass.

The general solution of Eq. (12) is

$$R_E(\rho)=\rho^{-1/4}\Re\{e^{-i\rho/2}[U(\alpha(E),3/2,i\rho) + D_0F(\alpha(E),3/2,i\rho)]\}. \quad (13)$$

$F(a,b,c)$ and $U(a,b,c)$ are the confluent hypergeometric functions, $\alpha(E)=-i(E/4)+\frac{3}{4}$, and D_0 is a function of E obtained from $R_E(E)=0$. After Eq. (11), the solution exists if and only if the energy E is real and exactly satisfies the quantum condition [6]:

$$\Re\left\{\frac{F(\alpha,3/2,i\rho_m)U(\alpha,3/2,iE)}{F(\alpha,3/2,iE)U(\alpha,3/2,i\rho_m)}\right\}=1. \quad (14)$$

Note that inverting Eq. (14) provides an algorithm to get $x|N$ from E, the eigenvalue corresponding to the quantum stationary state of the simulator.

The hypothesis of the existence of the quantum simulator will be true if and only if the spectrum of the simulator provides the statistics of the prime numbers.

The problem requires the theory of scattering of nuclear charged particles [11]. Asymptotically, for $\rho\gg 1$, Eq. (12) gives

$$R_E\sim 1/\rho\sin\left(\rho/2-\frac{E}{4}\log\rho+\delta_C+\frac{7\pi}{8}+\delta_0\right). \quad (15)$$

Here, $\delta_C=\arg\Gamma(\alpha)$ is a shift in the distorted Coulomb wave for the asymptote, and δ_0 is obtained from the asymptotic formulas of $U(\alpha,3/2,i\rho)$ and $F(\alpha,3/2,i\rho)$ as

$$D_0e^{3\pi E/8}\cot\delta_0\to 1. \quad (16)$$

Recall now that in the ensemble, E attains its maximum at $\pi(3)=2$,

$$\max E=2\frac{\pi(N/3)}{j^2}\sim 1/3\gamma^{-1}=o(\log\sqrt{N}). \quad (17)$$

It means that for small prime factor candidates $x|N$, the values of $e^{3E\pi/8}$ in Eq. (16) are $O(\sqrt{N})$ when we expand E in a series near $\frac{1}{3}\log\sqrt{N}$. This gets [6]

$$\delta_0=A\sqrt{N}\log E-h+\frac{\pi}{2},$$

where A and h depend only on N.

From the asymptote in Eq. (15), the second quantum condition at $\rho_m=q_m^2$ imposes $R_E(\rho_m)=0$. Therefore,

$$\delta_C+\delta_0+\rho_m/2-E/4\log\rho_m+\frac{7\pi}{8}=n\pi, \quad (18)$$

where n is an integer number. Redefine $n=\lfloor\rho_m/(2\pi)\rfloor-k$, for some integer k, $1\le k\le|\mathcal{F}(j)|$ (the convention taken that large k's map the region $E\gg 1$). When $N\gg 1$, the leading term in Eq. (18) is precisely δ_0, and it yields to

$$-A\frac{\sqrt{N}}{\pi}\log E+o(1/E^2)\to\left(k-\frac{h-\pi/2}{\pi}\right). \quad (19)$$

Now we have $E(\max k)=\max E$. Using Eq. (1) with $\max k=|\mathcal{F}(j)|$ gets

$$A\to-\pi,\qquad h=O(\sqrt{N}),$$

and $\delta_0\to-\pi\sqrt{N}\log E+O(\sqrt{N})$; $h(N)$ contributes to the wave function as a global phase and can be fixed with a new redefinition of n as previously done.

Thus, from Eq. (19) one obtains the solution $E(k)$ for $k\sim O(|\mathcal{F}(j)|)$, i.e., small prime factor candidates

$$E\to C\gamma^{-\kappa}, \quad (20)$$

where, for convenience, we defined the variable $\kappa\equiv k/|\mathcal{F}(j)|$, and C is a parameter depending on N.

It is possible to obtain better insight into the meaning of Eq. (20) by transforming its dependence on the variable κ on another in $u(N,x)$. This is possible because there is only one pair of coprimes in $\mathcal{F}(j)$ such that $N=xy$, implying a relation $\kappa\to x$. To explore this, we can use a simple interpolating polynomial of degree 2 in two known primes, say, $x=2$ and $x=3$, using the statistics of the primes in $\mathcal{F}(j)$:

$$u(N,x)\simeq\alpha_1(N)\kappa-\alpha_2(N)\kappa^2. \quad (21)$$

Equation (21) also satisfies that $u(N,\sqrt{N})=0$ at $\kappa=0$, forcing the constant term to be zero. The result for $\mathcal{F}(304)$ is shown in Fig. 1.

This solution valid for any N can also be used as a theoretical test of the quantum simulator. Let us check explicitly that the statistics of the states corresponds to that of the primes. Simply inverting Eq. (21) we get [6]

$$E(x)\to C\gamma^{-\kappa(x)}. \quad (22)$$

Now, directly from Eq. (2) and recalling that asymptotically $\pi(N/x)\to j/(1+u)(\sqrt{N}/x)$, we finally obtain [6] for $x\ll\sqrt{N}$,

$$\pi(x|N)\to\gamma x(1+u)E(x) \quad (23)$$

for x a prime candidate to factor N. This can be interpreted as a parametric family of curves enveloping $\pi(x)$. Thus, we

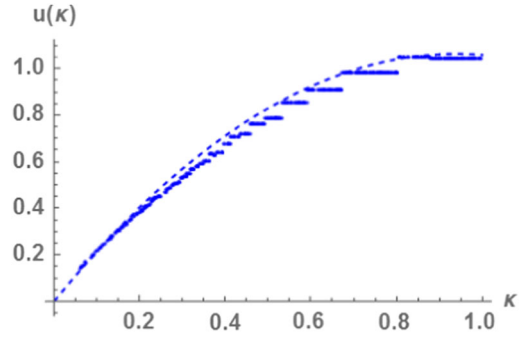

FIG. 1. The function u is represented versus $\kappa = k/\mathcal{F}$ for x in the factorization ensemble with $j = 304$. The dashed line is the Lagrange polynomial in $x = 2$ and $x = 3$ ($u = 2.26\kappa - 1.20\kappa^2$), although other pairs work the same. Remarkably, the number of divisor candidates in $\mathcal{F}(j)$ for $x = 2$, $x = 3$, etc., satisfies empirically the statistics predicted from our asymptotic estimates in Eq. (1).

can determine the constant C by simply matching some known value of $\pi(x)$ to the asymptote above.

Further proof of the exactness of the results obtained here is to show that the expression of $\pi(x|N)$ in Eq. (23) actually does not depend on N, as can be deduced classically from the universality of the primes and that for $N \to \infty$ every prime should be in $\mathcal{F}(j)$. We have experimentally tested this in many cases. This is a necessary condition but comes as a striking verification, since all the results arise from a purely quantum theory.

As seen in Fig. 2, Eq. (23) (for $x \ll \sqrt{N}$) is tantamount to the best possible approximation given by the Riemann function. The result fully confirms the consistency of the quantum solution.

Equation (21) is just an element required for the calculations; it was obtained specifically to match, using the simplest possible polynomial, the function $u(N, x)$ in terms of the statistics of the primes in $\mathcal{F}(j)$. Note that $\kappa(x)$ must exist—independent of our approximations—and, according to the distribution of prime factor candidates in the ensemble, should be a stepwise function.

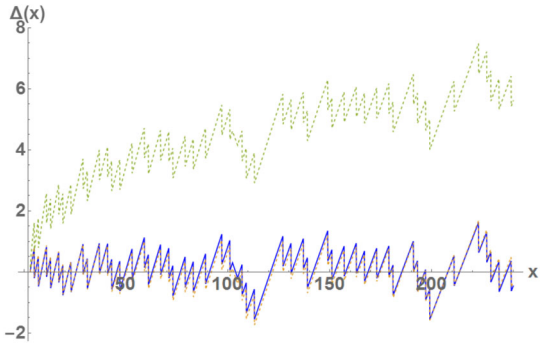

FIG. 2. The functions $\Delta(x) = \pi(x|N) - \pi(x)$ calculated here (blue), $R(x) - \pi(x)$ (dashed orange), and $Li(x) - \pi(x)$ (dashed green) for x in the factorization ensemble with $j = 3155$. Note how $\pi(x|N)$ fits perfectly to the best analytical approximation given by $R(x)$ for $x \ll \sqrt{N}$.

To summarize, we introduced new concepts and arithmetic functions that could play a significant role in the quantum factorization problem. The factorization ensemble is the main one: it allows us to bind the Hamiltonian of a quantum factoring simulator. Then, we reformulated the factorization problem to that of finding a new parameter of the problem: the arithmetic function E; it corresponds to the energy eigenvalues of the simulator. We showed that the spectrum of the simulator gives in the semiclassical quantization regime—large k, i.e., $x \ll \sqrt{N}$—the statistics of the primes. The compelling exactitude of this prediction justifies that both the simulator and the new algorithm of factorization outlined, which inverts the quantum conditions [Eq. (14)] for the coprime factor $x = f(E)$, will work. The next step will be to find out a suitable physical system described by this Hamiltonian, to which the boundary conditions can be applied. The spectrum of the system will provide the E values that, through the inverse of the quantum conditions found in this paper, will finally give the factors.

As a final remark, this work supports indirectly the Pólya-Hilbert program [3] to prove Riemann's hypothesis: the spectrum of the imaginary part of the zeros of $\zeta(\sigma)$ should be eigenvalues of a Hermitian operator. This being true, it will imply, according to Riemann, the statistics of the primes $\pi(x)$. Here we evaluated $E(x)$—an eigenvalue of a Hermitian operator—obtaining an approximation to $\pi(x)$ for the primes in $\mathcal{F}(j)$. It suggests that, perhaps, the truth of Riemann's hypothesis could be found with the help of the functions and the approach introduced in this work, particularly—let us speculate with the physics of the hypothesis [4]—if the contributions of $\delta_C(E)$, for $E \sim 1$ to the spectrum of the energies of the simulator were correlated with those obtained for the arithmetic function E computed from the zeros of $\zeta(\sigma)$ on the critical line.

This work has been partially supported by the project Quantum Information Technologies Madrid (QUITEMAD +), Comunidad de Madrid, Project No. S2013/ICE-2801 and by project CVQuCo, Ministerio de Economía y Competitividad, Spain, Project No. TEC2015-70406-R. MINECO/FEDER UE. We thank to J. Martínez-Mateo for suggestions and to F. A. G. Lahoz for pointing us to Ref. [7].

*Jose.Rosales@fi.upm.es
†Vicente@fi.upm.es

[1] R. Crandall and C. Pomerance, *Prime Numbers: A Computational Perspective* (Springer, New York, 2001), ISBN 0-387-94777-9.
[2] P. W. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, edited by

S. Goldwasser (IEEE Computer Society Press, Los Alamitos, 1994), p. 124.

[3] H. L. Montgomery, Analytic number theory, in *Proceedings of the Symposium on Pure Mathematics, St. Louis Univ., St. Louis, Mo., 1972* (American Mathematical Society, Providence, R.I., 1973), Vol. XXIV, pp. 181–193.

[4] D. Schumayer and D. A. W. Hutchinson, Physics of the Riemann hypothesis, Rev. Mod. Phys. **83**, 307 (2011).

[5] R. Feymann, Simulating Physics with Computers, Int. J. Theor. Phys. **21**, 467 (1982).

[6] See the Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.117.200502, which includes Refs. [7–9], for detailed derivations and further examples.

[7] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th ed. (Oxford University Press, New York, 1960), Chap. XXII, p. 368ff. Theorem 437 (for $k = 2$).

[8] A. E. Ingham, *The Distribution of Prime Numbers*, Cambridge Tract No. 30 (Cambridge University Press, Cambridge, England, 1932).

[9] H. Riesel and G. Göhl, Some calculations related to Riemann's prime number formula, Math. Comput. **112**, 969 (1970).

[10] M. V. Berry and J. P. Keating, The Riemann zeros and eigenvalue asymptotics, SIAM Rev. **41**, 236 (1999).

[11] See, e.g., L. D. Landau and E. M. Lifshitz, *Quantum Mechanics* (Pergamon Press, New York, 1965), Vol. 3.