Quantum Chaos and the Spectrum of Factoring

Jose Luis Rosales,* Samira Briongos, and Vicente Martín

The factorization ensemble is a set to which integer factorable numbers \( N' = x'y' \), having the same trivial factorization complexity, belong. Hence, the Rivest-Shamir-Adleman (RSA) cryptographic moduli pertain to this set. A function \( E(x', y') \) can be defined therein which will be associated to the energy of a system of ions in a Penning trap. This is the quantum factoring simulator hypothesis connecting quantum mechanics with number theory. Here, a possible setup of the simulator from the magnetron energies of a Coulomb crystal in a cylindrical trap is described. Then, quantum mechanically, these energies may have only discrete values. To test the validity of the simulator hypothesis, evidence of this kind of discreteness from the statistics of the \( E(x', y') \)s of a large random sample of RSA moduli is reported; indeed, their unfolded distance probability distribution fits to a Gaussian Unitary Ensemble, exactly as required if they actually correspond to the quantum energy levels spacing of a magnetically confined system that exhibits chaos. The confirmation of these predictions is consistent with the quantum simulator hypothesis and, thereby, it points to the existence of a liaison between quantum mechanics and number theory.

1. Introduction

Arithmetic and quantum mechanics share captivating similarities. For example, there is a typical probability distribution to measure some fixed distance between two prime numbers, similarly, as is the case with quantum physics, where there are different intensities for the observation of the transition between any two distant energy levels of the atom. Even more visual examples exist, for instance, Raman barcodes emerging from nonlinear media quantum optics spectroscopy, are the counterpart of number theoretical congruence classes, being on the grounds of optical readable code technologies. Thus, even though no confirmed connection between those two sciences exists to date, given the relevance of number theory in cybersecurity, discovering a possible deep connection between them will be of crucial interest. In order to emphasize this point recall that the celebrated Rivest–Shamir–Adleman code (RSA) has been broadly used to cipher credit card signatures and transactions on the internet. Since the usefulness of this code for cryptography is based on the (classical) mathematical intractability of the prime factorization problem for very large integers \( N = xy \), given that the expected outputs of the quantum theory would be the probabilities for a given prime to be a probable factor of \( N \), if a true connection between quantum mechanics and number theory does really exist, such a theory would eventually lead to debilitate the strength of the RSA code.

Analytical number theory was indeed born to life, historically, trying to improve a very related concern to the factorization problem known as the Prime Number Theorem, that is, the estimation for the distribution of the prime numbers below a given quantity \( x \),

\[
\pi(x) = \sum_{\text{prime} \leq x} 1
\]  

As a matter of fact, Riemann has given a successful formula for this arithmetic function (refs. [1] and [2]), a formula that is related with the primes through the complex zeta function defined as

\[
\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} (1 - p^{-s})^{-1}
\]

Even though, Riemann states in his demonstration a conjecture for the zeroes of \( \zeta(s) \) that must still be proved. Recall that the zeta function is well defined and analytic throughout the complex plane with the exception of a simple pole at \( s = 1 \) and it can be shown that \( \zeta(s) = 0 \) if \( s \) is a negative, even integer. Otherwise \( \zeta(s) \neq 0 \) outside the critical strip \( 0 < \Re(s) < 1 \). The hypothesis states that all additional zeroes of \( \zeta(s) \) must be on the line \( \Re(s) = 1/2 \).

This historical remark will help us to clarify the point of this article. The reason is that our physical insights are very related to the existence of a surprising approach to the proof of the hypothesis that suggests a glaring idea about a possible liaison between quantum mechanics and number theory. These early thoughts emerged from Hilbert’s and, independently, Pólya’s suggestion (see ref. [3]) that the Riemann hypothesis will become trivially true if some Hermitian operator can be found such that its eigenvalues are the imaginary part of the zeroes of \( \zeta(s) \). As a matter of fact, Pólya’s hypothetical Hermitian operator could be assimilated to the Hamiltonian of some physical system and, on these regards, the truth of Riemann’s hypothesis implies that quantized energies exist that are the imaginary part of the zeroes

Dr. J. L. Rosales, Prof. V. Martín
Center for Computational Simulation (Madrid)
DLSII ETS Ingenieros Informáticos
Universidad Politécnica de Madrid
Campus Montegancedo, Madrid E-28660, Spain
E-mail: jose.rosales@fi.upm.es

Dr. S. Briongos
Integrated System Laboratory ETSI Telecommunicaciones
Universidad Politécnica de Madrid
Avenida Complutense 30, Madrid E-28040, Spain

DOI: 10.1002/qute.202000086
of $\zeta(s)$. There is also numerical evidence that the statistical behavior of these complex zeroes is related to the eigenvalues of large random Hermitian matrices (refs. [4] and [5]), an intriguing fact that also shares the statistics of the energy levels of magnetic quantum systems with anti-unitary symmetry breaking, that is, a Gaussian unitary ensemble (a remarkable example of this is the Aharonov–Bohm billiard—see refs. [6, 7]).

The most comprehensive program to implement these ideas, relating pure number theoretical conjectures with physics, was by Berry and Keating (ref. [8]—see also refs. [9] and [10]). Nevertheless, these authors did not succeed to find a true bound Hamiltonian from which quantum discreteness would eventually emerge to cope with the, also discrete, Riemann zeros. In spite of this, since, modulus the truth of the hypothesis, the zeroes would univocally determine the distribution of the primes, if the connection suggested by Hilbert and Pólya is correct, then, there must also exist a quantum system whose energies universally give the primes themselves, and, since the primes are defined from Euclid’s unique factorization theorem, such a quantum system should determine a new and universal distribution of the possible prime factors of a number $N = xy$, product of two primes—clearly a finite and bound set because the possible lower factor will satisfy the simple constraint $x \leq \sqrt{N}$. The number theoretical energy function has to be multiplicative with the primes $x, y$, and, given that the relevant quantity is the amount of primes not larger than $x$, that is, the function $\pi(x)$, it has been conjectured earlier by Rosales and Martín in ref. [11], that the analogous to the energy of the physical counterpart of the factorization problem should read as

$$E[x, N/x] = \pi(\sqrt{N})^{-1} \pi(x)\pi(N/x)$$

As a matter of fact, this arithmetic function may be considered, with the appropriate choice of canonical variables, as the Hamiltonian of a inverse harmonic oscillator of some physical system with confined trajectories.

On the other hand, in the center of mass of every two ions in a Penning trap, the Hamiltonian of the magnetron degree of freedom coincides, in the practice, for large orbits, with the inverse harmonic oscillator prescription in number theory and, wherefore, Rosales and Martín in ref. [12] suggested to model the factorization problem on these physical grounds. Here we will generalize this model upon adding a time periodic electric quadrupolar perturbation. It is an important modification to the autonomous model, the inverse harmonic oscillator Hamiltonian will generalize this model upon adding a time periodic electric perturbation. It is an important modification to the autonomous model, the inverse harmonic oscillator Hamiltonian will be determined from the Hamiltonian of the magnetron degree of freedom, a consequence of the instability of the magnetron degree of freedom, is demonstrated. In the non-autonomous model, the inverse harmonic oscillator Hamiltonian becomes those corresponding to the time average of a periodically perturbed Hamiltonian. Special emphasis and details are given to the analysis of the experimental setup for the technologically achievable parameters of the actual quantum factoring simulator. Section 5, given some factorable $N$, the probability distribution of the arithmetic function $E(x, N/x)$ is computed (for the probable prime factors not larger than $\sqrt{N}$). This distribution comes to be discrete, as predicted from the spectrum of the measurable quantum simulator energies. Given this discreteness, an inversion algorithm from this spectrum is equivalent to a factorization algorithm with polynomial complexity, that is, only requires resources scaling as a function of $\ln N$. Also in this section, we demonstrate that a Gaussian unitary ensemble probability distribution fits to the number theoretical computations for the unfolded level spacing of the function $E$. This fact, indeed, represents a falsifiability test of the hypothesis of the quantum simulator of factoring. Our conclusions are summarized in Section 6. Finally, the proof of the dynamic confinement of a Coulomb lattice having magnetron instabilities, in the presence of a non-autonomous Penning trap, is found in the appendix.

2. Hamiltonian Formulation of Factoring

There are many composed integers $N^*$, such that $\pi(\sqrt{N^*}) = \pi(\sqrt{N}) \equiv j$. It is convenient then to define the factorization
ensemble \( \mathbf{F}(j) \) as the set of primes, say \( x_k, y_l \), whose products give numbers \( N_{jl} \) with this property:

\[
\mathbf{F}(j) = \{ x_k, y_l \text{ primes } | N_{jl} = x_k y_l \}, \text{ with } j = \pi[\sqrt{N_{jl}}] \tag{4}
\]

The cardinal of this set is the amount of the different number theoretical energies \( E[x, y] \) in the ensemble

\[
P(N) = \#[\mathbf{F}(j)] \sim \sqrt{N} (\ln \sqrt{N} + B)
\]

where \( B \) is Meissel–Mertens constant (see ref. [11]). Since this quantity is larger than the trivial algorithm complexity of factoring, \( E \) is approximately degenerate, that is, many \( N \in \mathbf{F}(j) \) have almost the same energy. This prediction was previously confirmed in ref. [12].

Asymptotically, the prime number theorem states that \( \pi[x] \sim x/\ln x \), writing \( h = \sqrt{N} \), we get

\[
E \sim 1 + \left( \frac{\ln(x/h)}{\ln h} \right)^2 \tag{6}
\]

Let us now compute the probability \( P_p \) for the energy function defined in the factorization ensemble. First, if for each of the primes \( x_k \in \mathbf{F}(j) \), the probability of being a factor of a given \( N \) is given by a function \( P_p(x) \), one has

\[
1 = \sum_{p \text{ prime}} P_p(\pi(x)) = \int_2^h P_p(x) D\pi(x) \tag{7}
\]

where one uses a Lebesgue measure integration and the sum is taken over the primes less than or equal to \( h \). The Lebesgue integral runs over all the real numbers and, in order to compute it, we can take the approximation from the prime number theorem formulated for the density of the primes, that is, \( D\pi(x) \approx dx/\ln x \). It gives \( P_p(x) = \ln x/h \). Moreover, since per each factorization there is univocally a single \( E \) function, we infer the existence of the new Lebesgue measure \( \text{DE} = |\partial_p E| \frac{d\pi(x)/dx}{h} \), that is

\[
\int_2^h P_p(x) D\pi(x) = \int_1^{\ln h} P_p(x) \text{DE} \tag{8}
\]

to such a degree one asymptotically obtains, using Equation (6),

\[
P_p \sim \frac{1}{2} \left( \frac{\ln h}{2} \right)^2 \tag{9}
\]

Recall also that, number theoretically, there are two positive independent arithmetic functions, depending on \( \pi[x], \pi[y] \) and \( j \), that can be built, namely

\[
p[x, y] = \frac{1}{2} (\pi[y] - \pi[x]) / j \quad q[x, y] = \frac{1}{2} (\pi[x] + \pi[y]) / j \tag{10}
\]

that suggests to write

\[
H(p, q) = \frac{1}{2} (p^2 - q^2) \tag{11}
\]

which can be evaluated for every pair of primes \( (x, y) \in \mathbf{F}(j) \), that is

\[
H(p, q) = -E/2 \tag{12}
\]

with \( E = \pi[x] \pi[y] / j^2 \). Trivial solutions are

\[
q = \sqrt{E} \cosh(t + t_0), \quad p = \sqrt{E} \sinh(t + t_0) \tag{13}
\]

where \( t \) should be considered as a quasi-continuous "time coordinate" and \( t_0 \) is a constant depending on \( E \). Then, neglecting \( \delta E/\delta t \), that is, for \( x = O(h) \), we get

\[
\dot{q}(t) = p(t) \equiv -\partial_q H, \quad \dot{p}(t) = q(t) \equiv -\partial_p H \tag{14}
\]

which means that, asymptotically, for large \( N \), the arithmetic function \( H(p, q) \) behaves exactly as expected for the Hamiltonian of a negative energy inverse harmonic oscillator. Now, in order for the physical analogy to be fully consistent, the actual system that simulates the solutions of the factorization problem should be confined, that is, it has a bound set of possible classical trajectories in the phase space. Let us now describe how a bound for the primes in \( \mathbf{F}(j) \) can be computationally built. Given the finiteness of the ensemble, there will always exist a minimum bound \( x_k \) for the lower factor of any \( N_{kl} = x_k y_l \in \mathbf{F}(j) \). Specifically, let us define a "gauge parameter" \( g \) and the integer \( k \) as follows

\[
x_k(k) = \lfloor h^{2/3} (\ln h)^{g} - k \ln h \rfloor \tag{15}
\]

thus, \( g = O(1) \) because \( x_k(k) \ll h \). Here, the integer \( k \) indicates that the limit must be taken for the prime numbers that, according to the prime number theorem, are separated from each other by a unit of distance of the order of \( \ln x_k \sim \ln h \), on average. For the arithmetic function \( q \) it imposes

\[
q \leq q_p(x_k, N/x_k) \tag{16}
\]

which asymptotically scales as a function of the gauge \( g \) and the integer \( k \),

\[
q_p(k) \sim 2/3 k (\ln h)^{-2g} h^{-1/3} + h^{1/3} (\ln h)^{-g} \tag{17}
\]

### 3. Stationary Quantum States

We proceed now to establish the physical counterpart of the factorization problem on the grounds of the Hamiltonian formulation described in the preceding section. The full experimental situation will be described in the following section, nonetheless, in order to understand how the actual physics is, let us summarize first the properties of a confined system of ions in a Penning trap which is characterized by some fundamental rotation frequency \( \omega \), the unit of mass \( m \) and the charge \( e \) of the ion. Radial and axial confinement are driven by means of a static electric field and an axially oriented constant magnetic field. In the center of mass coordinate system the electric and magnetic forces are balanced when the charged particles lay on exactly opposite radial positions near the center of symmetry of the trap, that is, in the electrostatic saddle point region. In this equilibrium state (see appendix) the time average magnetron degree of freedom
Hamiltonian becomes that of the factorization problem, that is, an inverse harmonic oscillator with negative energies. Classically, the balance of magnetic and electric forces is unstable for each of the ion pairs in their center of mass coordinate system but, recall that, in the quantum realm, there is no instability because we should extend the state coordinates of each particle to include its spin coordinate \( s \). The initial state of the system is then a tensor product of entangled-parity preserved states of every pair of indistinguishable particles

\[
\Psi[\{q_1^{(1)}\}, \{q_2^{(2)}\}; \{s_1\}, \{s_2\}, 0] = \prod_i \{\psi(q_1^{(1)}; s_1), \psi(q_2^{(2)}; s_2) \pm \psi(q_2^{(2)}; s_2), \psi(q_1^{(1)}; s_1)\} \tag{18}
\]

where the product is extended to every particle pair and the + or − sign corresponds to whether the ions are either bosons or fermions. Then \( q_i = |q_i^{(1)}| = |q_i^{(2)}| \), the relative distance between each pair, becomes a c-number of the individual state of each entangled pair. In what follows we will consider that the full state of the system consists of the tensor factorization in Equation (18).

The system's initial state is described only in terms of the relative distance between the ions and the parity entangled spin state \( \chi(s_1; s_2) = \psi(s_1; s_2)\psi(s_2; s_1) \pm \psi(s_2; s_1), \psi(s_1; s_2) \) of each of the interacting pairs, that is

\[
\Psi_{F|0|}[\{q_i\}; \{s_i\}, 0] = \prod_i \chi(s_i; s_i) \sum_{kl} \left\{ \sum_g a_{kl}^g \phi_k^g(q_i) \right\} \tag{19}
\]

where \( \phi_k^g(q) \) are the eigenfunctions of the Hamiltonian of the magneton degree of freedom of each pair in the trap (which may depend on the boundary conditions, denoted here by the gauge parameter \( g \)). On the other hand, \( F(N) = \|F|0\| \) maps the cardinality of the factorization ensemble with that from the Hilbert space of the physical system.

With this picture in mind, there will be a probability \( |a_{kl}|^2 \) to measure the magneton energy eigenvalue, \( F_{kl} \), say, proportional to the arithmetic function \( F[x_k, y_i] \). This corresponds to the factorization of the number \( N_{kl} = x_k y_i \in F|0\). At time \( t = 0 \), the quantum state of the system is exactly solved once we determine the complex amplitudes \( a_{kl} \).

In order to get the quantum theory an additional theoretical abstraction is required: we declare that the canonical arithmetic functions \( p \) and \( q \) are quantum operators acting on the state of the confined physical system.

Let us now land into physics from number theory upon proposing dimensionally measurable canonical coordinates from the known arithmetic functions:

\[
p = \hat{p} \sqrt{\hbar \omega_0 m}, \quad q = r \sqrt{\hbar \omega_0 / \hbar} \quad \text{and} \quad E = -2\hbar \omega_0
\]

the system then satisfies the energy constraint

\[
\frac{\hbar^2}{2m} - \frac{m \phi_k^g(r^2)}{2} = \hbar \omega_0
\]

This means that for the confined system, there is a Hamiltonian whose eigenvalues \( E_{kl} \) label the allowed physical states that the quantum factoring algorithm operates with. If the system corresponds to some confined set of particles, say, the state at \( t = 0 \) would be \( \Psi_{F|0|}[q_i, 0] \) with the appropriate boundary conditions, for example, \( \Psi_{F|0|}[q_i, 0] = 0 \), where \( q_i \) represents the size of the box where the system is confined. The full state wave function is written as a series of all its quantum states labeled by \( \{kl\} \), or

\[
\Psi_{F|0|}[\{q_i\}; t] = \prod_i \chi(q_i; q_i) \sum_{kl} \left\{ \sum_g a_{kl}^g e^{-iE_{kl}/\hbar} \phi_k^g(q_i) \right\}
\]

The simulator is programmed with the number \( N \) depending on the values of the wave function on the boundary. The spectrum of frequencies depending on \( q_k \) is the Fourier transform of the autocorrelation function

\[
\text{Spec}(\omega; N) = \frac{1}{2\pi} \int_{-\infty}^{\infty} d\omega \int_{-\infty}^{\infty} dq \psi_{F|0|}[\{q_i\}; 0]^{*} \psi_{F|0|}[\{q_i\}; t]
\]

As usual, the only possible output of the simulator should be its allowed frequencies \( E_{kl} / \hbar \) with probability \( |a_{kl}|^2 \) which are the expected outputs of the quantum algorithm of factoring. Boundary conditions for \( \psi(q_i, 0) \), for the radial wave function of each entangled spin state, read

\[
\psi(q_i, 0) = \frac{1}{\sqrt{q_k}} \quad \text{if} \quad \sqrt{E} \leq q_i \leq q_k(k),
\]

\[
\psi(q_i, 0) = 0 \quad \text{otherwise}
\]

The full Hamiltonian of the confined system of particles is \( H[p_j, \{q_i\}] = \sum p_j^2 - q_i^2 \). The transit to quantum mechanics comes from the usual substitution \( p_j \rightarrow -i\partial_j \), which leads to the Schrödinger equation of the simulator of factoring (hereafter, to simplify notation, we will drop the particle index \( j \))

\[
\partial_j^2 \phi(q) + q_j^2 \phi(q) = \hbar E \phi(q)
\]

with the proposed boundary conditions for \( \phi(q) \). It leads univocally to the spectrum of energies. To solve this problem, let us develop the solution in the semiclassical regime. This method, as a difference with the exact one, given in ref. [12], provides a physical meaning for the number theoretical—rather arbitrarily introduced—gauge parameter \( g \). The WKB wave functions are

\[
\phi_k^g(q) \sim p^{-1/2} \sin \left\{ \int pdq + \theta_k^g(q) \right\}, \quad \sqrt{E} \leq q \leq q_k(k)
\]

where \( \theta_k^g \) is global a phase depending on the gauge \( g \). Far from the turning point at \( q = \sqrt{E} \), we take the approximation \( p \approx 0 \), obtaining

\[
\phi_k^g(q) \sim (q^2 - E)^{-1/4} \sin \left\{ q^2/2 - E/2 \ln \frac{q}{q_k(k)} + \theta_k^g \right\}
\]
The condition \( \phi_i^l(q_g(k)) = 0 \) leads to \( \delta_i^l = \pi l - q_g(k)^2/2 \) (for \( l \in \mathbb{Z} \)) while the second condition \( \phi_i^l(\sqrt{E}) = 0 \) can be satisfied if and only if \( E \) is the solution of

\[
2\pi l - E \ln \frac{\sqrt{E}}{q_g(k)} - q_g(k)^2 + E = 0
\]

(28)

Now one develops \( E \rightarrow 1 + \varepsilon + O(\varepsilon^2) \), a method that is only possible when \( 2\pi l \sim q_g(k)^2 \) implying that the gauge \( g \) is indeed a function of the mode \( l \), that is, Equation (17) taken into account,

\[
g(l) \sim 1 + \frac{1}{\ln[(\ln h^2/2)^2]} \left[ 1 - 2\pi l/Q^2 \right]
\]

(29)

where \( Q^2 = h^{3/2}/(\ln h)^{-1} \). Finally, feeding these expressions into Equation (28) yields to the spectrum of energies

\[
E_{kl} \simeq 1 + \frac{4k}{3(\ln h)^{10}\ln q_g(k)}
\]

(30)

that coincides with the solution obtained in ref. [12]. Equation (30) should be compared with Equation (6).

In the semiclassical approximation the probability of the \( k, l \) state becomes, for \( q_g(k) \approx h^{1/3}(\ln h)^{-1/3} \),

\[
|a_{kl}|^2 \sim |\phi_{k,l}(0)|^2 \rightarrow k^{-1/2}
\]

(31)

and Equation (9) was taken into account; then, up to an arbitrary phase \( \chi_l \),

\[
a_{kl} \rightarrow k^{-1/4} \exp \{-i\chi_l\}
\]

(32)

which is an important genuine quantum result: there exists a discrete universal spectrum of energies for the factorization ensemble of any number \( N \), a result that is indeed independently of its bit size. Moreover, the result is consistent with the scalability of the quantum simulator, because these Fourier amplitudes do not depend on the initial configuration where the number \( N \) has been encoded, as it should be. This feature demonstrates the consistency and the validity of the quantum factoring simulator model. Moreover, given that the energy is degenerate, depending on the allowed gauges in the \( k \) labeled state, there could be in general many lines, labeled by the quantum number \( l \), for the same state.

4. Experimentally Realizable Quantum Factoring Simulator

As shown in ref. [12], for a confined system of two ions in a Penning trap the Hamiltonian of the magnetron degree of freedom can be approximated by that of an inverse harmonic oscillator in radial coordinates. Then, for two particles (classically) on their respective equilibrium positions, their quantized energy levels become negative. The system can therefore be considered as a good approximation of the quantized factorization problem. This approach was based entirely on the grounds of a straightforward correspondence between the arithmetic function \( g \) and the ions center of mass system relative distance. Even though the situation could be correct for a few number of ions, it will become clearly inexact when the number of particle pairs increases.

In order to cope with the extension of this model for a very large number of ions, the applicable theory is that of a Coulomb lattice confined in a Penning–Malmberg trap. The situation is summarized in Figure 1. This is due to the fact that long term confinement requires the trap to have cylindrical symmetry. This is due to the confinement theorem (see ref. [13] for the classical picture). Let the common angular velocity of the ions be \( \omega \). In the trap, axial confinement is achieved in the saddle point equilibrium region of a static electric field, while the radial confinement is obtained owing to the presence of a axial magnetic field. In the same magnetron orbit plane, there exists a rapid cyclotron oscillation of frequency \( \Omega = eB/m \). If the total number of ions in the trap is \( T \), owing to the cylindrical symmetry of the problem the canonical angular momentum of the system is conserved. In cylindrical coordinates \((z, r, \theta)\)

\[
L = \sum_{j=1}^{T} \left[ m v_\theta(r_j) + eA_\theta(r_j) r_j \right]
\]

(33)

where \( v_\theta(r) = \omega r \) is the angular component of the ion velocity and the quantity \( eA_\theta(r) \) is the vector potential part. For a uniform axial magnetic field \( A_\theta(r) = Br/2 \) and therefore,

\[
L = \left( m \omega + \frac{eB}{2} \right) \sum_{j=1}^{T} r_j^2
\]

(34)

Figure 1. Penning trap with cylindrical electrodes and a perturbed periodic quadrupolar electric stroboscopic field. By means of Doppler cooling techniques, a laser beam may reduce the temperature of the ion cloud to less than 5 mK.
implying that $\sum_i r_i^2 = \text{constant}$. This condition is a dynamical constraint on the allowed radial positions of the ions; the mean square radius of the system is now a conserved quantity which obviously means dynamical confinement. As shown in the appendix, in order for the ions magnetron orbits to obtain a common angular velocity a rotating periodic quadrupolar electric field perturbation of a frequency almost coincident with that of the magnetron motion should be applied.

The ions in the confined cloud become cooled by means of a laser beam pulse (Doppler cooling). The implementation of these techniques, it will be shown below, will become very important in order to develop a true experimentally realisable quantum simulator.

On the other hand, the system is in thermal equilibrium. This implies that the electrostatic potential harmonic degree of freedom of frequency $\omega_2$ can be considered as thermal with temperature

$$k_B T = 1/2m\omega_2^2 \langle z^2 \rangle$$

(35)

In this case, the electrostatic equilibrium distance between the ions, analogous to the Debye shielding length would be

$$\lambda_0 = \sqrt{k_B T e/n e^2}$$

(36)

where $n$ is the ions number density of the confined Coulomb lattice. It can be shown (see ref. [13]) that the condition for no density fluctuation is

$$n = 2\pi e/m \langle \omega_2 \rangle / (\Omega - \omega)$$

(37)

Recall that if the additional condition $\omega_2 \to 2\pi / (\Omega - \omega)$ is satisfied (see the appendix), the density becomes $n \to e/m \omega_2^2$, and, since $\omega_2 \leq \Omega / \sqrt{2}$, there would be maximum density, which is Brillouin’s limit. In that case, using Equations (35), (36), and (37), we obtain $\lambda_0 = \langle z^2 \rangle / \sqrt{2}$, that is, the equilibrium distance of between the ions does not exceed the expected thermal minimum. This can be physically interpreted in the sense that the lattice average motion is approximately restricted to the magnetron orbit plane. In the saddle point region, where the particles become confined, there is an effective repulsive inverted harmonic oscillator potential, that is, denoting $\omega_2^2 = \kappa/m$, $U(\rho) = -1/2 \kappa \rho^2$. In the center of mass system, the energy constraint becomes

$$\hat{H}(\rho, \phi) \equiv \frac{1}{2} \left\{ \frac{\hat{\rho}^2}{m} - \kappa \rho^2 \right\} = \hat{E}$$

(38)

The Penning trap axial frequency is $\omega_z = \sqrt{2 \pi} \lambda_0$.

As said, a realizable model of the quantum simulator can be devised when the number of particles pairs increases. In that case, the system should be considered as a Coulomb lattice. Confinement is experimentally achieved through the presence of a stroboscopically driven periodic electric quadrupolar field perturbation of strength $\lambda$ with a frequency $\omega_2 \to \omega$. In these practical situations, a more convenient configuration of the Penning trap will be cylindric and the effective equilibrium of the electric and magnetic forces are achieved when the quadrupolar field frequency $\omega_2$ is very close to that of the Penning trap magnetron degree of freedom. If the total number of particles in the confined Coulomb lattice is $I$, the time dependant Hamiltonian becomes

$$\mathbf{H}_I(\rho \phi) = \sum_{i=1}^{I} \epsilon \mathbf{H} (\hat{\rho}_i, \hat{\phi}_i) + \lambda \mathbf{r}_i^2 \cos 2\omega_i t$$

(39)

In general, an exact solution of this problem cannot be obtained and the trajectories are known to be chaotic. Therefore, in the quantum theory only the average time problem makes sense. Indeed, in the center of mass coordinate system, according to Feynman–Hellmann theorem, its time average Hamiltonian should be that of the inverse harmonic oscillator presented here (see ref. [15]).

$$\int_{-\pi/2 \omega}^{\pi/2 \omega} d\omega \langle \mathbf{H}_I (\hat{\rho}, \hat{\phi}) | \mathbf{H}_I (\hat{\rho}, \hat{\phi}) \rangle \rightarrow \mathbf{E}$$

(40)

where $\mathbf{E} = (I/2) \mathbf{E} + L_\omega$, is Floquet’s quasi-energy and $L = \partial L / \partial \mathbf{E}$ is the conserved angular momentum. Along these lines, the Coulomb lattice rotates with the stroboscopic frequency $\omega$ and the energy of every parity preserved entangled ion pair is defined as a time average

$$\langle \hat{E}(\rho \phi) \rangle \rightarrow \left\langle \frac{\hat{p}^2}{2m} - \frac{\kappa \rho^2}{4} \right\rangle$$

(41)

Therefore, since $L$ is also a constant of motion, the time average Hamiltonian of the confined Coulomb lattice model, with the stroboscopic forced rotating wall, becomes now an exact experimental proposal for the Hamiltonian formulation of the factorization problem.

Moreover, as shown in the appendix, exact dynamical equilibrium can be achieved upon fine tuning the parameters of the rotating wall frequency and intensity. In this case one obtains, analogously to the quantum Feynman–Hellmann Equation (40), not only an average Hamiltonian but, in addition, a new collective radial breathing vibrational mode with period $\pi / \omega$: the exact classical stable degree requires (in the simplest case approximation, i.e., $\omega_2 \ll \Omega$) for the intensity of the rotating wall potential that

$$\lambda \rightarrow 1/2 + \epsilon$$

(42)

and $\epsilon \ll 1$. In that configuration the radial modes are Mathieu’s resonances of the system, which, indeed, might correspond to some special cases of those observed by Affolter, Driscoll and Anderegg in Penning trap confined Mg++ ions experiments in ref. [16], where the observed phenomenon was said to correspond to a characteristitc radial breathing degree of freedom for the periodically perturbed (collective) Coulomb lattice trajectories.

Let us now return to our physical model. We need to discover how the number of confined ions $(I)$ scales with the cardinal of the factorization ensemble, $\mathcal{F}(N)$. Recall that the magnetic flux of the system must be quantized. This determines the Landau levels of the system

$$\mathcal{F}(N) \frac{\hbar}{2e} \equiv \sum_{i=1}^{I} B \pi r_i^2 = I B \pi \frac{1}{2} \left\{ \sum_{i=1}^{I} r_i^2 \right\}/I$$

(43)
replacing the conserved quantity \( \langle R^2 \rangle = (\sum_{i=1}^{N} r_i^2)/I \), and considering that every two ions follow the same magnetron orbit, we obtain the maximum dynamical radius condition

\[
\frac{I}{2} B \langle R^2 \rangle = F(N) \frac{\hbar}{2e} \tag{44}
\]

On the other hand, taking into account Equation (37), we get

\[
n = \frac{I}{(V)} = \frac{e_0}{m} B^2 (\omega_z/\Omega)^2 \tag{45}
\]

and, the volume \( V \) of the confined Coulomb lattice is given by \( V = 4\pi/3 (R^2 z) \approx 4\pi/3 \sqrt{2} \lambda_0 (R^2) \). Now, taking into account Equations (44), (45), and (36), one directly obtains

\[
I = \left( \frac{2\omega_z}{3z^2 a \Omega} F(N) \mu(T) \right)^{1/2} \tag{46}
\]

where \( \mu(T) = \sqrt{k_B T/mc^2} \ll 1 \) is a function of the temperature of the ions in the Coulomb lattice, \( a \approx 1/137.036 \) is the fine structure constant and \( z \) is the number of charges of the ions. On the other hand, the quadratic average radius of the confinement ellipsoid becomes

\[
\langle R^2 \rangle^{1/2} = \sqrt{\frac{\hbar}{m \omega_z} \left( \frac{3z^2 a \omega_z F(N)}{\Omega \mu(T)} \right)^{1/4}} \tag{47}
\]

A typical experimental setup is in ref. [14] of Kriesel et al., where Coulomb crystals produced in a cylindrical Penning–Malmberg trap with \( \approx 20000 \) laser-cooled beryllium ions \((^9\text{Be})\) has been reported. In these circumstances the ion cloud reaches a density of about \( n \approx 10^{10} \text{cm}^{-3} \) with an axial trapping field of \( B \approx 4.465 \text{ Tesla} \) and an electrostatic potential of \( V_0 = 1000 \) Volts. The radius of the cloud is then of the order of \( R \approx 2 \text{ mm} \). The applied rotating wall frequency is about the same than the corresponding magnetron frequency, that is, \( \omega_z/2\pi \approx 42.5 \text{ kHz} \). The temperature is reduced, using laser cooling techniques, to less than 5 mK. Now, to confirm that our formulas Equations (47) and (46) make sense, notice that a confined cloud of \( R \approx 2.8 \text{ mm} \), with \( T = 1 \text{ mK} \), say, is obtained for a number of \( I \approx 1000 \) confined ions (i.e., 500 entangled pairs). Such a experimental device will correspond to the quantum factoring simulator of numbers \( N = xy \) such that \( \pi(\sqrt{N}) \approx 2.6 \times 10^{12} \). A remark is in order: even though the number of entangled pairs scales with the square root of the cardinality of the factorization ensemble, it is also proportional to a very small non-dimensional quantity \( \sqrt{\mu(T)} \approx 5.7 \times 10^{-3} \) for \( T \approx 1 \text{ mK} \), which allows for a technologically achievable trap. Moreover, the radius of the cloud only scales as \( N^{1/8} \) which allows for a physically realisable experimental device even for huge numbers, that is, using Equations (5) and (46)

\[
\sqrt{N(T)} \sim \Lambda(T)/\ln \Lambda(T) \tag{48}
\]

and \( \Lambda(T) = 3T^2 \Omega/(2z^2 a \omega_z \mu(T)) \) is a numerical constant of the trap that could reach very large values for low ions temperatures or large axial magnetic fields. The spectrum of factoring is a universal function computed for the histogram of measurable values of the energies

\[
4 \left( \tilde{E}_i/(2\hbar \omega) - 1 \right) / \ln^4 \sqrt{N(T)} \tag{49}
\]

Here we have taken into account that radial breathing modes have twice the frequency from the magnetron degree of freedom. Then, given this experimental setup, if we are able to measure, with enough precision, the (axial and radial modes) emission or absorption spectra of the cloud, it will also determine the approximate mathematical constraints enumerated in the following section. This will permit to obtain the factors at least in some special cases. Recall that this experimental program will become possible only if very precise techniques to reduce the temperature of the cloud are developed.

Recall that since at zero temperature the system oscillations and energies become purely quantum mechanical, and that, formally, \( N(T) \rightarrow \infty \) in that limit, every prime should be a solution of the simulator. This also means that, since the limit of exact zero temperature is physically unattainable, the boundlessness of the primes might be considered as a corollary of the simulator, which is also a test of the consistency and exactness of the Penning trap model independently of the number of confined ions \( I \).

Recall that, in the semiclassical theory, every quantum number should be assigned to every classically periodic degree of freedom. Therefore, in quantum simulator model, the integer \( I \), which arises precisely from the wave function conditions at the actual maximum and minimum turning points of the radial coordinate, must necessarily correspond to the classical radial breathing modes.

5. The Spectrum of Factoring

A practical model of the factorization ensemble is the set of all products of two primes with the same number of bits, \( n - 1 < \log_2 x' < n \) say. It represents an extension to the actual factorization ensemble that, recall, refers to a single \( \pi(\sqrt{N}) \).

\[
F(n) = \bigcup_{i=a}^{x[2^{[n/2]}-1]} F(i) \tag{50}
\]

As a result, within the extended factorization ensemble are the \( n \)-bits public moduli keys used in the RSA cryptography system. The histogram of the function \( E[x',y'] \) for a sample of these keys should fit to a universal discrete distribution of probabilities. From the scalability of the spectrum to any size of the number \( N = xy \) we are allowed to calculate \( F(n) \) with arbitrary \( n \), for example, \( n = 120 \). Hence, a sample of 150 000 factorable \( N \in F(120) \) RSA keys has been generated using OpenSSL. In order to perform a numerical experiment, we generated 150 000 values of \( E[x,y] \), using the aforementioned OpenSSL keys. The Gaussian kernel distribution histogram of the factorization function is shown in Figure 2 which effectively displays the existence of a discrete set of favored values. Many \( E \) became apparently avoided while other are statistically amplified. The histogram represents the spectrum of factoring, confirming the expectations of the quantum theory for a system that classically exhibits chaos,
Figure 2. Best fit Gaussian Kernel distribution calculated for the histogram of the factorization function. 

To get here some the required tools and number theoretical methods. Detailed techniques will be given elsewhere; however, let us advance here some the required tools and number theoretical methods. To get \( x = X[E_{ij}, N] \) recall that, owing to Euclid’s unique factorization theorem, for some known \( N \), the unique solution of the implicit constraint

\[
E_{ij} - E[N, x] = 0 
\]

must be found.

We now define the function

\[
\zeta(x) = 1 - \sum_{\zeta(x) = 0}^{T} \frac{R(x^n)}{R(x)}
\]

where \( R(x) \) is Riemann’s approximation to \( \pi(x) = \lim_{T \to \infty} \zeta_T(x) R(x) \). Then, up to some truncation order \( T \) in the series of \( \zeta_T(x) \), a probable factor of \( N \), having probability \( |a_{ij}|^2 \), can be obtained if \( x_0 \) exists that minimizes the constraints

\[
(E_{ij} - E_T[x_0, N/x])^2 \approx 0
\]

where the notation \( E_T[x, N/x] \) means that the replacements \( \pi(x) \to \zeta_T(x) R(x) \) etc., were used. Then \( x = \lim_{T \to \infty} x_0 \).

Notice that the function \( \zeta(x) \), owing to its definition as a series depending on the Riemann’s zeros, suffers from large and rapid oscillations and, therefore, the constraints have many possible solutions. In the end, the solutions of Equation (55) give numerical approximations to the actual probable factors of \( N \) (with the given spectral probability \( |a_{ij}|^2 \)). Yet, the exact factor \( x \) can still be found. One requires to feed \( x_0 \) into Coppersmith’s algorithm that computes an integer solution of a set of polynomial constraints of the kind

\[
P_k[z^4(x - [x_0])] = 0 \mod N
\]

which for the formally independent variable \( z = x - [x_0] < 2h^{1/4} \), and \( k \in N \), form a set of problems that can be formally assimilated to that of finding the minimum reduced basis of a large lattice. Using the celebrated polynomial time LLL lattice basis reduction algorithm, the factor, \( x = [x_0] + z \), will be obtained with resources only scaling as \( \ln N \) (see refs. [18] and [19]).

Provided with these techniques, let us theoretically estimate the best case factorization algorithm complexity coming from the existence of the spectrum of some \( n \) bits size number \( N \approx 2^n \), which, recall, is an scalable universal function of the function \( k \approx (\ln^4 h(E - 1)) \). Note first that there are

\[
\#(F[j]/j \sim (\log_2 N)^{3} \log_2 \log_2 N
\]

constraints. Their solutions provide all the possible approximations to the factors of \( N \). On the other hand, if \( T \) becomes indefinitely large, the distance \( |x - x_0| \) will necessarily be small, that is, certainly not larger than \( x^{1/4} \), say, which is the condition required for the applicability of Coppersmith’s algorithm. In that case, the factor \( x \) will be obtained in just \( \log_2 N \) additional steps for every approximate solution of the constraints. This determines that the inversion algorithm obtains the factor \( x \) in

\[
\Gamma(N) \sim (\log_2 N)^{3} \log_2 \log_2 N
\]

steps, which exactly coincides with the prescribed quantum factoring algorithm complexity of Shor in ref. [22] for a quantum gate computer, as it should be. Notwithstanding with this encouraging result, recall that the best case corresponds to the exact summation of all the zeroes of \( \zeta(s) \) the series

\[
\zeta(x) = \lim_{T \to \infty} \zeta_T(x)
\]
that is, the Riemann hypothesis must be true. In all practical purposes, though, the complexity achievable with a classical computer that implements the inversion algorithm will strongly depend on the truncation order \( T \).

### 5.2. Level Spacings Probability Distribution

As said in the introduction, the classical trajectories of the dynamically confined system will be chaotic. As a matter of fact, owing to the Von Neumann–Wigner theorem (ref. [20]), the probability that two energy curves (depending on the strength \( \lambda \)) cross each other is extremely low, a phenomenon called level’s repulsion. Considering that, in the Coulomb lattice, there are classical phase space trajectories having nearly the same semiclassical states, one should conclude that only the statistical distribution of the quantized energies can be studied. This may correspond in number theory, we conjecture, to the fact that the value of the particular gauge \( g(0) \) remains unknown. Hence, if two close—orbital—quantum numbers, say \( l \) and \( l' \), can be assigned to the same energy state corresponding to two nearly equally large radial breathing motions, one would expect that

\[
\Delta E_{li} = E_{li} - E_{li} = s_i \omega
\]

where \( s \) is a random variable of non zero average. Thereby, the quantum state can be described instead by the spectral statistic of the level spacing \( \varphi(s) \). This procedure is, by construction, convenient for numerical studies.

The action of the Hamiltonian on the state vector of such a chaotic or unpredictable system can be replaced by the action of random matrices (see refs. [20, 21] and [22]). Therefore, level repulsion and randomness should become essential features of the energy distribution of the factoring simulator. Note that the presence of a magnetic field imposes that the system has no time reversal invariance, which means that the matrices should have a complex Hermitian representation (see the net examples in ref. [7]). If the hypothesis of the simulator is correct, then, the expected distribution of the (unfolded, i.e., measured over the average) level spacing of the factorization function \( E \), in the ensemble of \( n \)-bits RSA moduli, should be that of the Gaussian unitary ensemble which is given by the expression

\[
\varphi(s) = \frac{32}{\pi} s^2 \exp \left( -\frac{4}{\pi} s^2 \right)
\]

We have tested the validity of these physical ideas with numerical simulations regarding the distribution of the primes in \( F(n) \). To do our analysis, we computed \( E[x_i, y_j] \) for 500 000 OpenSSL \( n \)-bits RSA factorable moduli of the usual form \( N_{ai} = x_i y_j \in F(n) \). Just for the sake of cross testing the results with the available table of primes in Mathematica, we took \( n = 80 \). Thereon, recalling the quantum predicted energy function in Equation (30), we define the \( k \)-index function

\[
k(x_i, y_j) = \frac{1}{4} \{ E[x_i, y_j] - 1 \} \{ \ln[2^{n/2}] \}^s
\]

and we have taken into account that \( \ln h \approx \ln[2^{n/2}] \) should be a good approximation. This arithmetic function is always \( O(1) \) for any \( n \)-bit RSA moduli and, according to the prediction of the quantum simulator, it should exhibit an universal probability density \( |a_{hj}|^2 \sim k^{-1/2} \) independently of the number of bits to which the extended factorization ensemble pertains. Now, in order to calculate the unfolded level spacing, for the randomly selected 500 000 samples in the extended factorization ensemble, we must, first, order \( \{ k(x_i, y_j) \} \) from lowest to highest values to obtain an ordered set

\[
\{ k_i \}_\text{sampled} \rightarrow \{ k_i \}_\text{ordered}
\]

Moreover, in order to avoid any possible bias in the definition of the closest energy level, we computed the differences of almost consecutive values of the array of the ordered \( k \)-index function at the running \( i \)th labeled position

\[
\Delta k_i(\ell) = \frac{1}{\ell} (k_{i+\ell/2} - k_{i-\ell/2})
\]

with the index \( 1 \leq \ell \leq 6 \) taken as a random variable, that is, \( \ell = O(1) \), which is the only prescribed condition. This numerical procedure makes sense inasmuch as we are trying to erase any kind of probabilistic bias originated from the external program (in view of the fact that the pairs \( (x_i, y_j) \) of the sample OpenSSL generated primes were also randomly generated). Therefore one proceeds to compute the average level spacing. It requires to take into consideration values in the array well beyond the actual level spacing that we are calculating at the position labeled by the index \( i \). Numerically, we take some large \( L \gg \text{Max}[\ell] \) and define

\[
\langle \Delta k_i \rangle_L \equiv \frac{1}{L} \{ k_{i+\ell/2} - k_{i-\ell/2} \}
\]

In the numerical experiment \( L = 1000 \) is taken (because it is much lower than the actual size of the sample, but is much larger than that considered for the nearby levels). The unfolded level spacing of the quantum index function at the running ordered position \( i \) is then the random variable

\[
\sigma_i(\ell) = \frac{\Delta k_i(\ell)}{\langle \Delta k_i \rangle_L}
\]

whose normalized histogram is shown in Figure 3. It fits exactly to the Gaussian unitary ensemble statistics, a result that is perfectly consistent with the expected level repulsion of the quantum simulator with its associated number theoretical function \( E \). The figure shows, for the primes in the extended factorization ensemble of 80 bits RSA moduli, \( F(80) \), the histogram of the unfolded differences of the arithmetic function \( \{ E[x_i, N_i/x_i] \} \) calculated for a sample of 500 000 moduli in this set. These primes were generated by the Unix standard cybersecurity package OpenSSL. In the quantum factoring simulator model, those values should be associated to the level spacing of the quantum factoring simulator energies with the prescribed level repulsion. This supports, by evidence, the predictions anticipated from the quantum theory on regards to the distribution of the primes in the extended factorization ensemble.
6. Conclusions

The hypothesis of the quantum simulation of the factorization problem connects quantum mechanics and number theory. This is very analogous to Hilbert and Pólya conjecture to prove the Riemann’s hypothesis related to the existence of a Hamiltonian system whose energy eigenvalues are the imaginary part of the non trivial Riemann’s zeroes. The quantum simulator approach extends this connection to the primes. The Hamiltonian formulation of the problem is that of an inverse harmonic oscillator of a confined system with negative energies. It is for this reason that a realisable experimental setup, that actually, as required, exactly implements this Hamiltonian, has been given and analyzed in this work. We expect that, using the available technology for Penning–Malmberg traps, the probability distribution for the prime factors of large composed numbers \( N \) can be obtained. Extending the concept of the factorization ensemble to cope with numerically computable RSA cryptographic moduli \( N = \phi \) that is, to actual standard cryptograpic factorable \( n \)-bits numbers, we have observed that the proposed “energy factorization function” statistical distribution is fully consistent with the predictions of the quantum model (since \( E(x, y) \) correctly exhibits a discrete spectrum of probabilities). The asymptotic probability predicted dependence was also observed. This can be explained in the context of the quantum simulator model, but has no explanation whatsoever in the classical realm. To such a degree, then, the evidence provided here discovers an essential (i.e., quantum theoretical unavoidable) vulnerability of the RSA cryptographic system. On these regards, we have developed an alternative and independent deduction of the polynomial time complexity of the quantum factorization problem. This result, that comes from pure quantum simulation primitives, Equation (58), requires the universality of the spectrum of the quantum simulator energies as well as the truth of the Riemann hypothesis.

Finally, in this work, a crucial additional statistical test can be designed: if the exposed quantum theory of factoring is correct, that is, if the factorization function \( E \) corresponds to the actual energy of a magnetically confined set of charged particles, as suggested in ref. [12] and, more explicitly described here, for the case of a very special kind of stroboscopically perturbed Coulomb lattice system, the probability distribution of the level spacing of the factorization function must be that of the Gaussian unitary ensemble and no other. This last test has also been numerically confirmed, a fact that affirmatively points out toward the existence of a profound connection between quantum mechanics and number theory (since we have been able to confirm predictions that physics alone imposes on the distribution of the primes).

Appendix: Dynamic Confinement in Penning Traps

Let us find the stable solution for the motion of two (ideally identically charged) clusters of ions in a Penning trap with a rotating wall. Radial symmetry is also taken into account. The case of many pairs of clusters to form a Coulomb lattice is straightforward using this symmetry.

In the Penning trap, the motion is decomposed into separated radial and axial ones. The system of particles in the trap is restricted to follow a harmonic oscillation in the \( z \)-axis and a planar \( (x, y) \) motion. For the \( x, y \) plane of motion of two identical charges at \( x_1 = -x_2 = x \) and \( y_1 = -y_2 = y \), of total mass \( M = 2m \), the Lagrangian is given in terms of the electrostatic quadrupole and the magnetic field frequencies of the trap

\[
\mathbf{L}_\omega = \frac{1}{2} M (\dot{x}^2 + \dot{y}^2) + \omega_1^2 \frac{1}{4} M (x^2 + y^2) + \mathbf{e}_1 \cdot \mathbf{A}(x, y) + \mathbf{e}_2 \cdot \mathbf{A}(-x, -y) - \frac{e^2}{2 \sqrt{x^2 + y^2}} - \frac{M}{2} \omega^2 (x^2 - y^2) \lambda \cos(2\omega t) + M \omega^2 xy \lambda \sin(2\omega t) \tag{67}
\]

Here \( \mathbf{A}(x, y) = -B_l/2i + B_x/2j \) is the vector potential in the Johnson–Lippman gauge and \( \mathbf{v}_1 = \dot{x} i + \dot{y} j \), \( \mathbf{v}_2 = -\mathbf{v}_1 \). A periodic rotating quadrupolar electric potential wall was added. This term is required for the adiabatic stability of the ions in the trap (see ref. [25]). The relative intensity of the rotating wall \( \lambda \) will be determined from dynamic equilibrium considerations of the confined ensemble of ions in the trap. Hence, close to dynamic equilibrium, statistically, the ions should occupy positions in the trap satisfying approximately, for their polar radius \( x^2 + y^2 \approx a^2 \), in terms of some constant distance to the center \( a \), that will be determined below using the dynamic equilibrium conditions. Moreover, one can write, denoting \( \phi = \sqrt{x^2 + y^2} \),

\[
\frac{1}{\phi} = \frac{1}{4\phi} \left( \frac{\phi^2}{a^2} + 3 \right) + \ldots \tag{68}
\]

Then, for each of every two approximately identical charged density clumps near their equilibrium position, that is, disregarding higher order terms, obtains the approximate quadratic Lagrangian

\[
\mathbf{L}_\omega = -\frac{1}{2} m (\dot{x}^2 + \dot{y}^2) + \frac{m}{2} \omega_1^2 (x^2 + y^2) \left( \frac{\omega_1^2}{2} + \frac{\beta}{\omega_1^2} \right) + \frac{m}{2} \Omega (x\dot{y} - y\dot{x}) - \frac{1}{2} m \omega^2 (x^2 - y^2) \lambda \cos(2\omega t) + m \omega^2 xy \lambda \sin(2\omega t) \tag{69}
\]

where \( \Omega = eB/m \) and \( \beta = e^2/4 \). In the rotating frame, all the quadratic centrifugal terms have been included into the definition of an arbitrary Lagrange multiplier which does not
contribute to the dynamics. We now define $\delta \omega^2 = \omega^2 + 2\beta/(ma^4)$. Let also use a new coordinate frame $(\xi, \zeta)$ defined by a rotation of angle $\delta \omega t$. In this case, the rotating wall quadrupole perturbation becomes

\[-ma_0^2/2(x^2 - y^2) \lambda \cos(2\omega_0 t) + ma_0^2(xy) \lambda \sin(2\omega_0 t)\]

\[-ma_0^2/2(\xi^2 - \zeta^2) \lambda\]  

\[\text{(70)}\]

which leads us to obtain the Euler–Lagrange equations (we follow almost exactly ref. [16]),

\[
\ddot{\xi} - (\Omega - 2\omega_0)\dot{\xi} + \{\omega_0(\Omega - \omega_0) - (\delta \omega^2 / 2 - \lambda \omega_0^2)\}\xi = 0
\]

\[
\ddot{\zeta} + (\Omega - 2\omega_0)\dot{\zeta} + \{\omega_0(\Omega - \omega_0) - (\delta \omega^2 / 2 + \lambda \omega_0^2)\}\zeta = 0
\]  

\[\text{(71)}\]

Their solutions are

\[\dot{\zeta} = A_x \cos(\chi_x t) + A_x \cos(\chi_x t)\]

\[\dot{\lambda} = \lambda_x \sin(\chi_x t) + c_A \lambda_x \sin(\chi_x t)\]  

\[\text{(72)}\]

where $A_x$ are constants. The frequencies $\chi_x$ and the constants $c_x$ are given by

\[\chi_x = \frac{1}{2} \left\{ \Omega^2 - 2 \delta \omega^2 + (\Omega - 2\omega_0)^2 \right\} \pm \sqrt{4\delta \omega^2 \lambda^2 + (\Omega^2 - 2\delta \omega^2)(\Omega - 2\omega_0)^2}\]

\[\text{(73)}\]

\[c_x = \frac{\chi_x^2 - \lambda_x(\Omega - \omega_x)}{\chi_x(\Omega - 2\omega_0)}\]  

\[\text{(74)}\]

The system of equations in Equation (71) is satisfied for each ion in the trap. Recall that, owing to the symmetry of the problem, any pair of statistically identical charged density clumps in a Coulomb lattice, will also obtain the same solutions at the corresponding equilibrium positions. In general, the motion of this system is unstable in three dimensions. The more stable configurations should be those with the charged density clumps oscillating in the $x - y$ plane. As shown in ref. [26], it is consistent with the rotating quadrupolar frequency stroboscopic election

\[\omega_x \rightarrow \omega_x, \ \delta \omega^2 \rightarrow 2(\Omega - \omega_x)\omega_x\]  

\[\text{(75)}\]

where $\omega_x$ is the trap magnetron frequency. We will simplify the formulas introducing the trap angle

\[\sin \Theta = \sqrt{2\omega_x / \Omega}\]  

\[\text{(76)}\]

In terms of the angle $\Theta$ the magnetron frequency is simply $\omega_x = \Omega \sin^2 \Theta / 2$ while the cyclotron frequency becomes $\omega_\lambda = \Omega \cos^2 \Theta / 2$. Interestingly, in the limit of a thin disk of ions, the equilibrium radius $a$ must be

\[a = \left( \frac{\beta / m}{\omega_\lambda \omega_\lambda - \omega_\lambda^2 / 2} \right)^{1/2}\]  

\[\text{(77)}\]

Which can take any limit, that is, it remains undetermined by the perturbed Penning trap model. On the other hand, whenever Equation (75) are satisfied, the terms depending on $\chi_x$ in Equation (73) become irrelevant since, in this case

\[\chi_x \rightarrow 0, \ \chi_x \rightarrow \omega_x - \omega_\lambda = \Omega \cos \Theta\]  

\[\text{(78)}\]

which leads to select $A_x = 0$. Moreover, a rotation of angle $\chi_x$ leads to the ion center of mass coordinate frame $(x_{\chi_x}(t), y_{\chi_x}(t))$. In this system, when the trap angle $\Theta \ll \pi / 2$, the positions $y_{\chi_x}(t), z \rightarrow 0$ and every two ions lay in opposed positions at a distance $x_{\chi_x}(t) = x_{\chi_x}(t) = 2a$, while the cyclotron motion remains as a rapid oscillation around those adiabatically quasi-stable positions.

**Mathieu resonances.** Given that the quadratic Lagrangian Equation (69) uses only the first two terms in the series of the nonlinear interaction potential energy, when the trap angle $\Theta \ll \pi / 2$, the positions should only be stable during a very short period of time of the order of $1 / \chi_x \sim 1 / \omega_x$. To cope with this difficulty, one should, in general, consider a new dynamic degree of freedom: the polar radial coordinate $a$. Consequently, one should replace the constant $a$ by a function of time $\rho(t)$, which, indeed, ought to evolve adiabatically in a period of the order of $1 / \omega_x \gg 1 / \chi_x$. Therefore, for each of the individual charges the effective Lagrangian for this new dynamic degree of freedom becomes

\[L_{\omega_x}(\rho, \dot{\rho}) = \frac{1}{2} m \dot{\rho}^2 + \frac{1}{4} m \dot{\rho}^2 \rho^2 - \frac{1}{2} m \dot{\rho}^2 \dot{\rho} \cos(2\omega_0 t)\]  

\[\text{(79)}\]

and the effective time periodic Hamiltonian becomes

\[H_{\omega_x}(\rho, \dot{\rho}, t) = \frac{\dot{\rho}^2}{2m} - \frac{1}{4} m \dot{\rho}^2 \rho^2 + \frac{1}{2} m \dot{\rho}^2 \dot{\rho} \cos(2\omega_0 t)\]  

\[\text{(80)}\]

The two ions rotate with an angular frequency $\omega_\lambda$. $\rho(t)$ is the solution of the Mathieu equation,

\[
\frac{d^2 \rho}{d\tau^2} + \theta - 2\phi \cos 2\tau \rho = 0
\]  

\[\text{(81)}\]

In Equation (81), $\tau = \omega_x t, \theta = \cot^2 \frac{\omega_x}{2}, \phi = \lambda \theta$. The solutions are written in terms of the oscillatory Mathieu cosine functions

\[\phi(t) = aC_{(-\theta, -\phi, r)} C_{(-\theta, -\phi, 0)}\]  

\[\text{(82)}\]

Nonetheless, there would only be periodic solution stable within a very narrow parametric region $\phi(t)$ (see ref. [27] for reviewing the entire parametric map); these have $\pi$ period for the variable $r$. When $\Theta \rightarrow 0$, the first order parametric stability constraint is

\[\phi(\theta) \sim \theta / 2 + o(\sqrt{\theta})\]  

or, simply

\[\lambda \rightarrow 1 / 2\]  

\[\text{(83)}\]

This largely oscillatory behavior corresponds to a radial breathing collective motion of the Coulomb lattice, that is, a new degree of freedom. Finally, if Equation (83) is satisfied, the Euler–Lagrange equation, Equation (81), reads

\[
\frac{d^2 \rho}{d\tau^2} - \theta \rho [2 \sin^2 \tau + o(1 / \sqrt{\theta})] = 0
\]  

\[\text{(85)}\]
Since the solutions of Equation (85) are necessarily periodic, in
order to physically understand the motion of the ion in the Pen-
ing trap, an average of the periodic term will be now obtained
(assuming that \( \langle 2 \sin^2 \tau \rangle = 1 \) during many loops of its orbit). The
average motion is identical to that of an inverted harmonic oscil-
lator for \( \langle \phi(\tau) \rangle \). The orbits should be restricted between a maxi-
mum and a minimum \( \phi(\tau) \).

\[
\frac{d^2}{d\tau^2} \phi - \frac{d\phi}{d\tau} = 0 \quad (86)
\]

In that limit, the Lagrangian becomes

\[
L \rightarrow \left\langle \frac{1}{2} m \dot{\phi}^2 + \frac{m \omega^2 \phi^2}{4} \right\rangle \quad (87)
\]

and average Hamiltonian reads

\[
H_0 \rightarrow \left\langle \frac{\hat{p}^2}{2m} - m \frac{\omega^2 \phi^2}{4} \right\rangle \quad (88)
\]

which coincides with the postulated Hamiltonian of the factor-
ization function.

Acknowledgements

This work has been partially supported by the UPM-NETBLUE SOLU-
CIONES INFORMATICAS S.L. contract number P180021289 and the
Spanish Ministry of Economy and Competitiveness under contract RTC-
2016-5434-8.

Conflict of Interest

The authors declare no conflict of interest.

Keywords
quantum chaos, quantum simulation, trapped ions

Received: August 16, 2020
Revised: December 6, 2020
Published online: January 22, 2021

[1] H. M. Edwards, Riemann’s Zeta Function, Dover, New York 2001.
[2] B. Riemann, Über die Anzahl der Primzahlen unter einer gegebenen
Größe, Gesammelte Werke, Teubner, Leipzig 1892.
[3] H. L. Montgomery, in Proc. of the Symposium on Pure Mathematics,
Vol. XXIV, American Mathematical Society, Providence 1973, pp. 181–
193.
[4] A. M. Odlyzko, Math. Comput. 1987, 48, 273.
[5] A. M. Odlyzko, Primes, Quantum Chaos and Computers, National Re-
search Council, Washington DC 1990, pp. 35–46.
[6] M. V. Berry, Proc. R. Soc. Lond. A: Math. Phys. Sci. 1987, 8, 183.
[7] M. V. Berry, M. Robnik, J. Phys. A: Math. Gen. 1986, 19, 649.
[8] M. V. Berry, J. P. Keating, SIAM Rev. 1999, 41, 236.
[9] D. Schumayer, D. A. W. Hutchinson, Rev. Mod. Phys. 2011, 83, 307.
[10] G. Sierra, P. K. Townsend, Phys. Rev. Lett. 2008, 101, 110201.
[11] J. L. Rosales, V. Martin, Phys. Rev. Lett. 2016, 117, 200502.
[12] J. L. Rosales, V. Martin, Phys. Rev. A 2018, 97, 032325.
[13] T. O’Neil, Phys. Scr. T 1995, 59, 341.
[14] J. M. Kriesel, J. J. Bollinger, T. B. Mitchell, L. B. King, D. H. E. Dubin,
Phys. Rev. Lett. 2002, 88, 125003.
[15] H. Sambe, Phys. Rev. A 1973, 7, 2203.
[16] M. Affolter, C. F. Driscoll, F. Anderegg, J. Am. Soc. Mass Spectrom.
2014, 26, 330.
[17] D. Coppersmith, J. Crypt. 1997, 10, 233.
[18] A. K. Lenstra, H. W. Lenstra, Jr, L. Lovász, Math. Ann. 1982, 261, 515.
[19] P. W. Shor, SIAM Rev. 1999, 41, 303.
[20] J. von Neumann, J. Wigner, Phys. Zeit. 1929, 30, 467.
[21] F. J. Dyson, J. Math. Phys. 1962, 3, 140.
[22] T. Hasegawa, M. J. Jensen, J. J. Bollinger, Phys. Rev. A 2005, 71,
023406.
[23] D. H. E. Dubin, T. M. O’Neil, Rev. Mod. Phys. 1999, 71, 87.
[24] L. Meirovitch, Methods of Analytical Mechanics, Dover Books, New
York 2003, pp. 282–288.