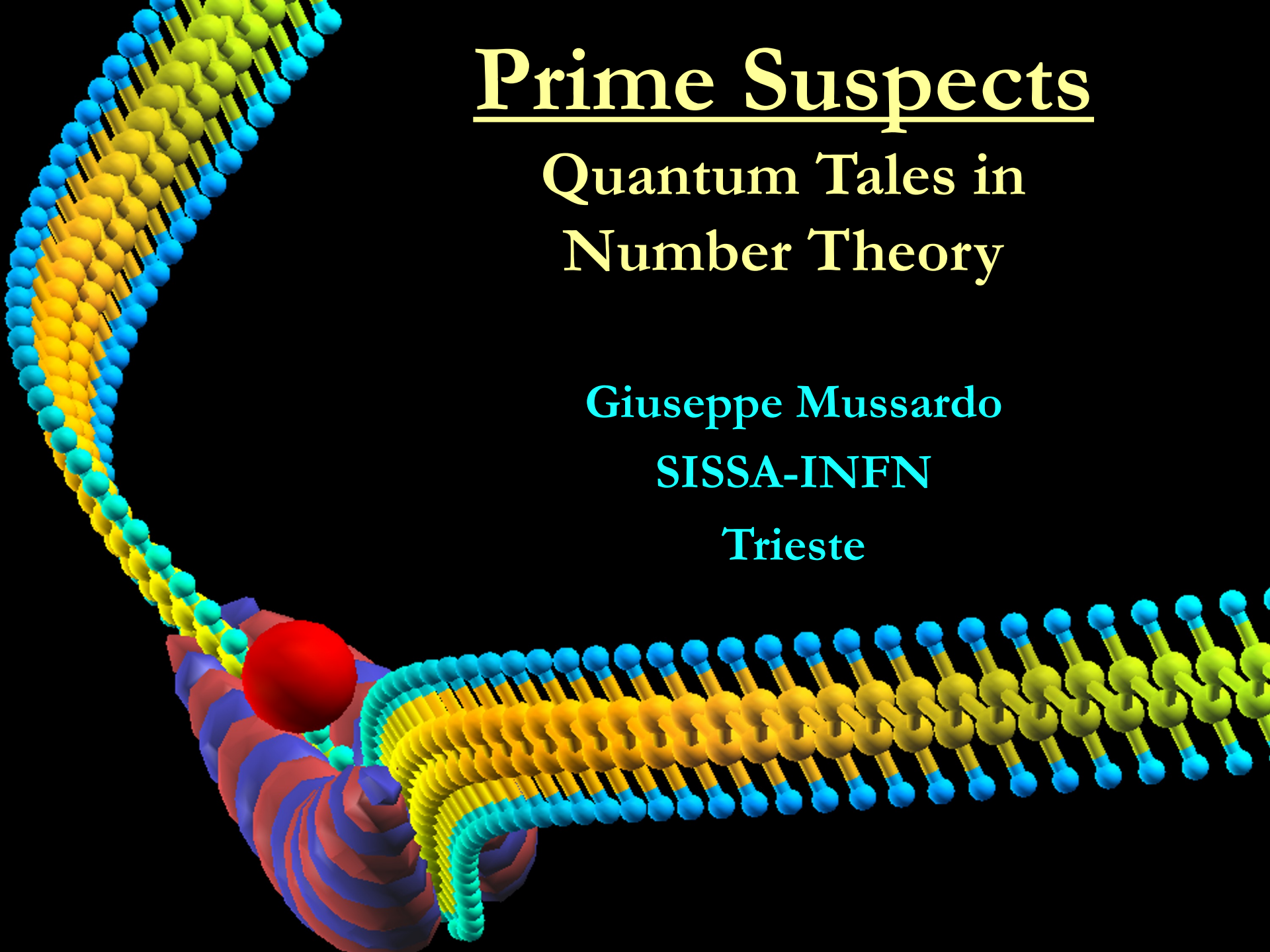


Prime Suspects

Quantum Tales in Number Theory

Giuseppe Mussardo
SISSA-INFN
Trieste

Magic of Many (Real and Imaginary) Paths

Nuclear Physics B280 [FS 18] (1987) 445–465
North-Holland, Amsterdam

MODULAR INVARIANT PARTITION FUNCTIONS IN TWO DIMENSIONS

A. CAPPELLI*, C. ITZYKSON and J.-B. ZUBER

Service de Physique Théorique, CEN-Saclay, 91191 Gif-sur-Yvette Cedex, France

Received 3 September 1986

We present a systematic study of modular invariance of partition functions, relevant both for two-dimensional minimal conformal invariant theories and for string propagation on a SU(2) group manifold. We conjecture that all solutions are labelled by simply laced Lie algebras.

1. Introduction

The minimal two-dimensional conformal invariant field theories [1] carry a set of representations of two Virasoro algebras of common central charge

$$c = 1 - \frac{6(p-p')^2}{pp'}, \tag{1.1}$$

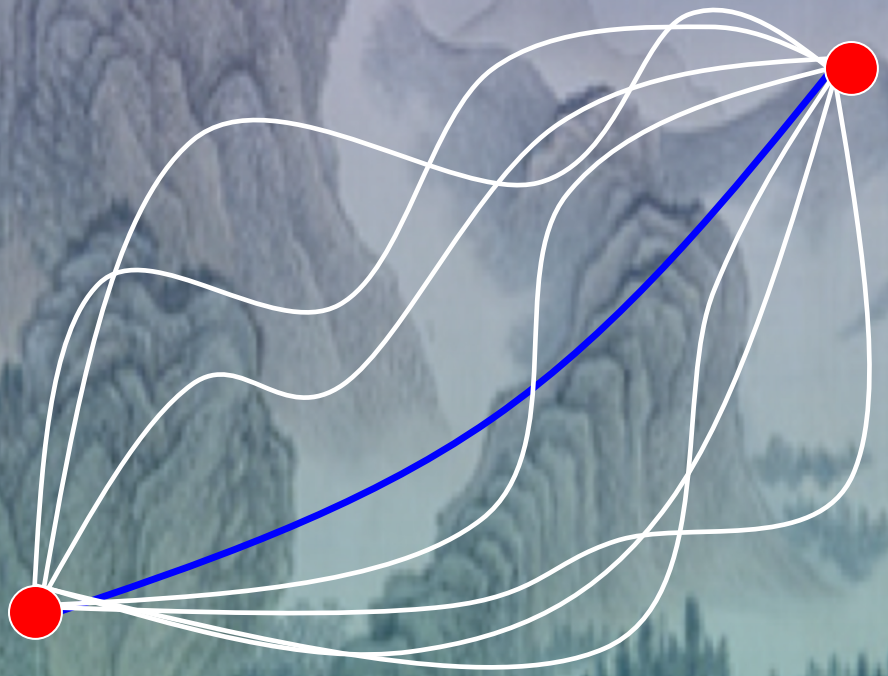
with (p, p') a pair of coprime positive integers. Belavin, Polyakov and Zamolodchikov have shown that it is consistent to retain only a finite number of primary fields $\phi_{h,\bar{h}}$, of conformal dimensions h and $\bar{h}$ chosen among the Kac values [2]

$$h_{rs} = \frac{(rp-sp')^2 - (p-p')^2}{4pp'} = h_{p'-r,p-s}, \tag{1.2a}$$

with

$$1 \leqslant r \leqslant p'-1, \qquad 1 \leqslant s \leqslant p-1. \tag{1.2b}$$

Paths of life



IL DECAMERON

Di Messer

Giovanni Boccacci

Cittadino Fiorentino.

Ricorretto in Roma, et Emendato secondo l'ordine del Sacro Conc. di Trento,

Et riscontrato in Firenze con Testi Antichi & alla sua vera lezione ridotto da' Deputati di loro Alt. Ser.

Nuovamente Stampato.

IN FIORENZA
Nella Stamperia de i Giunti
MDLXXIII.

ridiano, sotto deiquale a pricipio ne la lor prima reuolutione dentro al concauo de la sfera del fuoco, habbiamo veduto, che s'erano partiti, E di qui saleno al cielo Empireo, che p esser im mobile, e mouer il tutto, in qsto mācano di circolar moto, ma con le due militie del cielo, rimangon a contemplar la diuina essentia, in che consiste il sōmo de la felicita, e gloria del Para diso. Resta a veder il tempo, ch'essi cōsumarō in salir, e circuir p li gradi di quello, che leggier cosa è ad intēdere, essendo sta- to, come habbiamo veduto in vna reuolution del cielo, cioè, dal suo violente moto, che fa da oriente in occidente, e torna in oriente quasi sempre in vn di naturale, o vogliamo dire in xxiiij. hore, de lequali habbiamo veduto hauerne cōsumate xij. ne le prime otto reuolutioni in due quarte del cielo, cioè, da mezzo l'altro, fino a mezzo il nostro hemisferio, toccandone hore sei p ogni quarta, Le altre xij. in due altre reuolutioni, ne le due altre quarte, cioè, da mezzo 'l nostro fin a mezzo l'altro hemisferio dōde prima s'erano partiti, e l'una quarta nel nostro e ne l'ottaua sfera dal cerchio meridiano fin a l'orizonte occi- dētale, L'altra ne l'altro hemisferio, e ne la sfera nona da l'ori- zonte occidētale, che a quelli di la e orientale, ad esso cerchio

meridiano, e fu da l'un otto del sole a l'altro, Onde nel primo Canto, douendo leuarsi da terra, e cominciar a salire, e partendo de la foce, dōde allhora nel'altro hemisferio surgeua il sole dice, Fatto hauea di la mane, e di qua sera Tal foce quasi, e tutto era là biāco. Quello hemisferio, e l'altra parte nera, &c. Ma che 'l salire fosse, come di sopra habbiamo detto, in istante, e quasi senza interuallio d'alcun tempo, Questo lo dimostra in piu luoghi, come nel primo cāto del salir a la sfera del fuoco in persona di Beat. Tu non se in terra, si come tu credi, Ma fol gore fuggendo 'l primo sito, Non corse, come tu, che ad esso ri- di. E nel secondo canto, del suo salir dal concauo del fuoco a quel de la luna, Beatrice in suso, & io in lei guardaua, E forse in tanto, in quanto vn quadrel posa, E uola, e da la noce si disciaua, Giūto mi vidi, &c. Nel quinto canto, del suo salir dal concauo de la luna a quel di Mercurio, E si come saetta, che nel segno Percote, pria che sia la corda queta, Cosi corremmo nel secondo regno, Ma piu chiaramente nel xxij. canto del sa- lir dal cōcauo di Saturno a quel de l'ottaua sfera, Tu nō hauresti in tanto tratto, e messo Nel fuoco 'l dito, in quant'io vidi 'l segno, Che segue 'l Tauro, e fui dentro da esso.

DELLA COMEDIA DI DANTE ALIGIERI PRIMO CANTO DELLA TERZA CANTICA, DETTA PARADISO.

ARGOMENTO.

TRATTA il poeta in questo primo Canto come egli asce- se verso il primo cielo, & essendogli nati alcuni dubbij, gli furono dichiarati da Beatrice.

LA GLORIA di colui, che tutto moue,
Per l'vniuerso penetra, & risplende
In vna parte piu, & meno altroue.
Nel ciel, che piu de la sua luce prende,
Fu io; & vidi cose, che ridire
Nè sa, nè puo, qual di la su discende;
Perche appressando se al suo disire
Nostro intelletto si profonda tanto,
Che retro la memoria non puo ire.
Veramente quant'io del regno santo
Ne la mia mente potei far thesoro,
Sarà hora materia del mio canto.

ALLEGORIA.

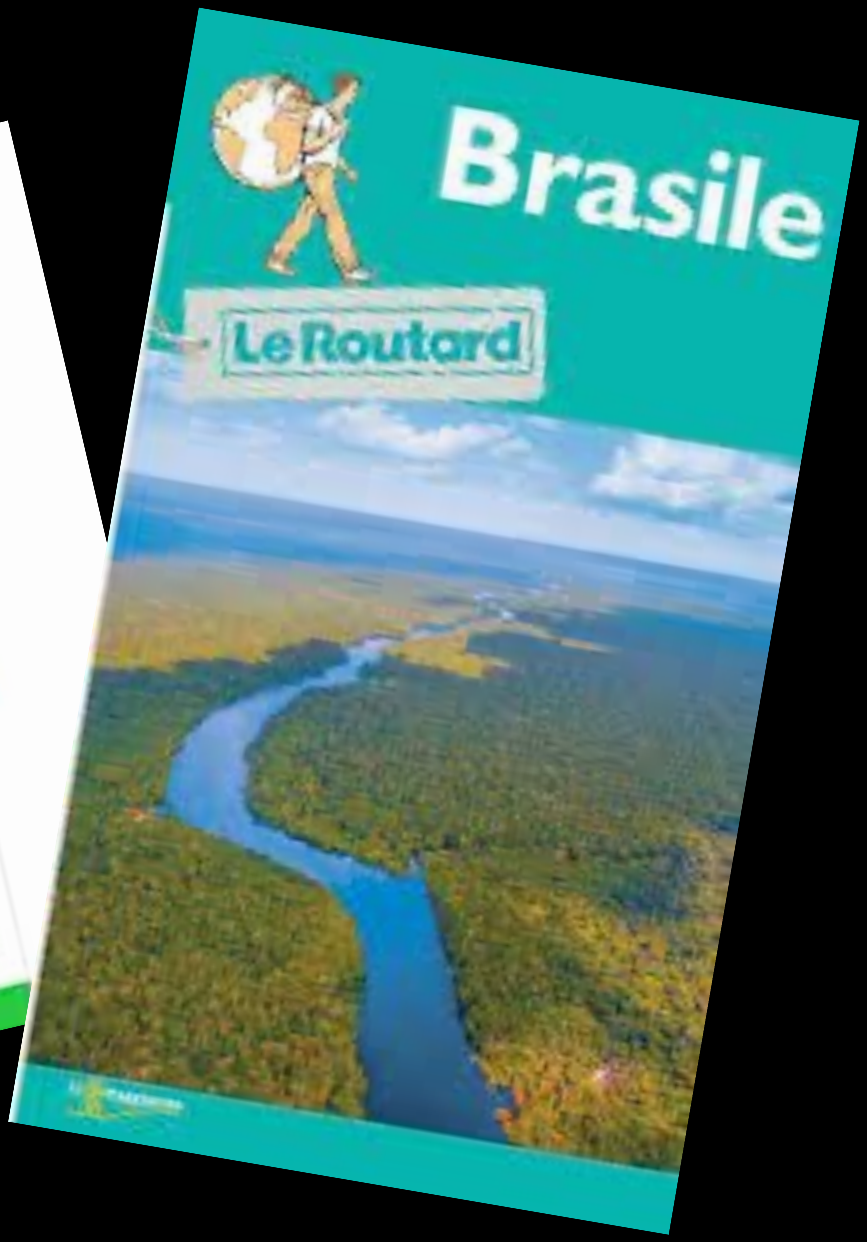
SANS. PER lo accrescimento del- la luce, che si mostrò a gli occhi di Dante, si dinota la ec- cellenza della theologia, laqual di tanto vince le dottrine hu- mane, quanto ella illuminan- doci nella vera cognition di Dio, è stromento di farci perue nire alla beatitudine.

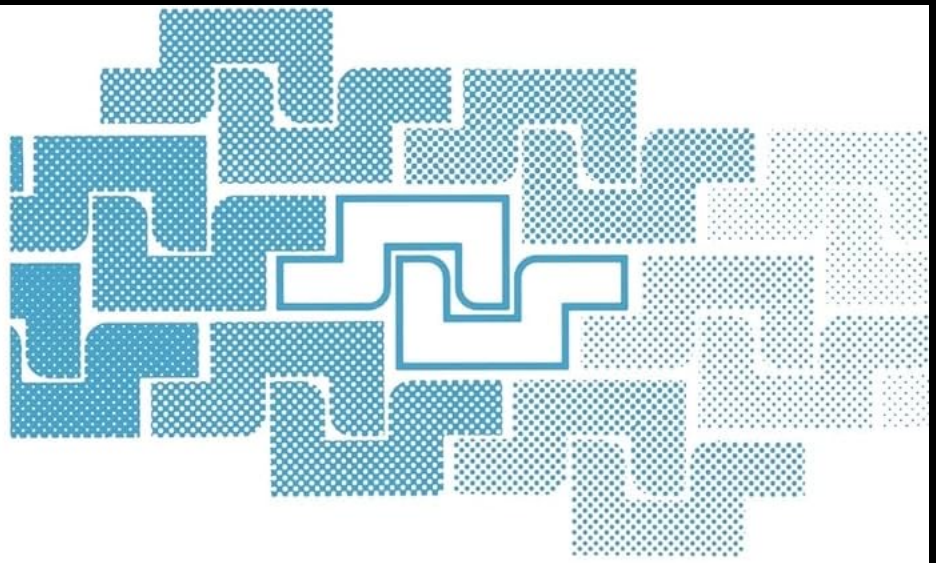
LAND. PERCHE, come habbiamo dimo stro nella prima Cantica, tutti i poeti heroici diui dono l'opera in tre parti. In propositione, inuocatione, & narratione, questi quattro ter- narij contengono la proposi- tione, nella quale brieuemen- te la materia di tutta l'opera è trattar del superno regno, non secondo sua natura, perche questo trascēde il nostro intelletto, ma quāto puote comprēder la sua mēte, & cōpreso mādare alla memoria. Et perche la propositione, & inocatione sono in luo- go di proemio, osserua qui quello, che è proprio del proemio: delquale qual sia l'officio, pche assai apertamēte dimostrammo nel principio dell'Inferno, nō m'affaticherò in descriuere quali sieno le parti di quello, ma dichiarerò come al presente il poe- ta l'osserua. Catta attentione dimostrando d'hauer a dir co- sa si alta che tutte l'altre gli sono lungamente, & senza com- paratione inferiori: perche non è comparatione dall'infini- to al finito, cioè, da Dio alle creature. Catta beneuolentia dalla persona sua, dimostrando, che la fatica sua nello scri- uere ha ad essere molto vtile a gli altri. Catta docilità, per- che brieuemente dimostra quello, di che per tutta la Can- tica tratterà, cioè, del regno eterno. LA Gloria. Benche fama, & gloria a molti paiano quasi quel medesimo, nondimeno fa- ma è notitia molto frequente d'alcuna cosa: gloria è notitia chiara d'alcuna cosa con loda. Adunque la fama puo esser di co sa, che nè splendore, nè laude alcuna seco adduce: ma la gloria

non puo esser senza quelle, On de è diffinita da Cicerone nel- le Tusculane. Gloria est con- sentiens laus bonorum, incor- rupta vox bene iudicantium de excellenti virtute. Di que- sto seguita, che ogni gloria sia fama, ma non ogni fama glo- ria. LA gloria, la gloriosa ope- ra, & è l'opera di Dio l'vniuer so. Di colui, che tutto moue, cioè, di Dio, & è color rhetori co, detto circuitione, che è quā do quello, che si puo dir in vna parola, si dice in piu. Tutto mo ue, onde Boetio, Stabilisq; mo nens das cuncta moueri. Solo adunque egli è stabile, questo cosi proua Tomaso Aquinate. ogni cosa che è mossa, cōuien che sia mossa da altri, come è il sole, la luna, & gli altri: on- de accioche non habbiamo a proceder in infinito, è necessario porre vn motore immobile. Iddio adunque immobile muoue & tanto significa Che tutto muoue, quanto Iddio, percioche egli essēdo stabile, & imobile, è primo motore: egli muoue gli angeli, & gli Angeli i cieli, & i cieli cō le lor reuolutioni indu- cono giu nel mōdo diuersi effetti. Adunque Iddio è primo mo- tore, & prima cagione di tutte le cagioni. Il pche diremo la glo ria di Dio penetra per l'vniuerso, cioè, trapassa p tutte le crea- ture, questa, & p potentia potè, & per sapiētia seppe, & p som- ma bōtà, & amore volle produr pfettissima creatura, & dicēdo vniuerso, intēdiamo il tutto, ilqual è di diuerse spetie: pche alcu na cosa ha solo l'essere, cōe la pietra, alcuna l'essere, e 'l viuere, cōe l'herbe, & gli alberi, alcuna arroge a' primi due il sēture, co me sono certi calcinegli, alcuna ha l'essere, il viuere, & il sēture & imaginare, come sono i bruti, alcuna alle quattro dette potē tie arroge il discorso della ragione, come sono gli huomini, ma piu nobil creatura è qlla, che ha l'esser formale, e l'itelletto, co- me è l'angelo, ma i breue possiamo, secōdo i filosofi diuider q- sto vniuerso i tre specie, pcioche ciò che è, o è pura forma, cōe è Dio, angeli, & aia humana. Ma Dio è forma delle formi, o è


RUFFINO
RISERVA DUCALE
Chianti Classico
Riserva
SPACCIO
DI VINI
E
LIQUORI


Mosca
le Guide
routard


Brasile
Le Routard



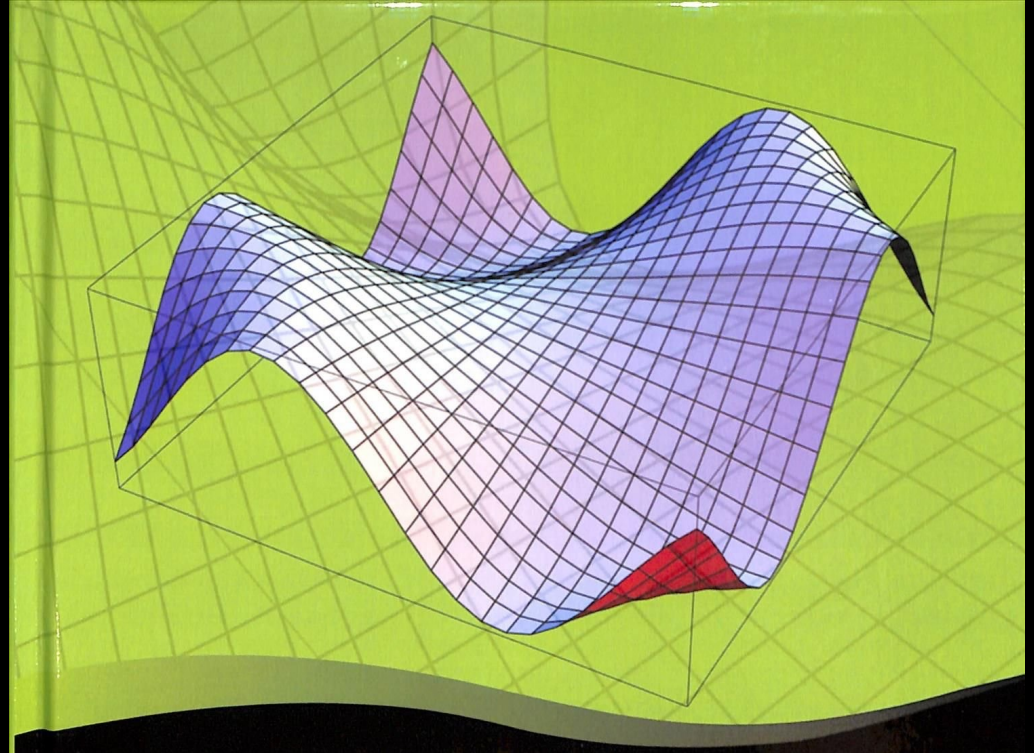
Statistical Field Theories

Edited by

Andrea Cappelli and Giuseppe Mussardo

NATO Science Series

II. Mathematics, Physics and Chemistry – Vol. 73



Statistical Field Theory

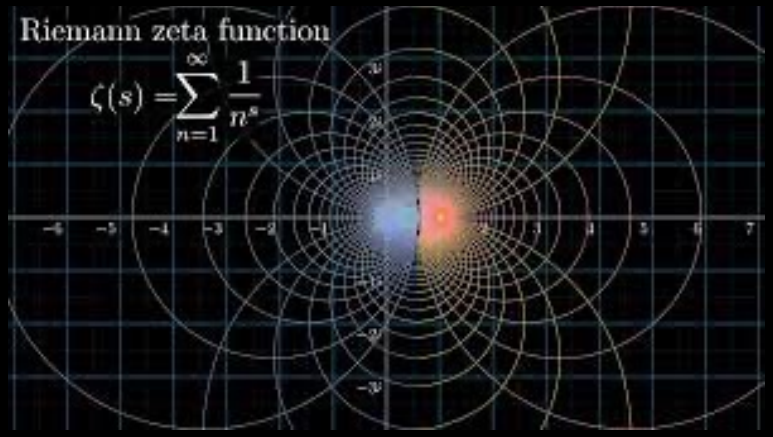
An Introduction to Exactly Solved Models in Statistical Physics

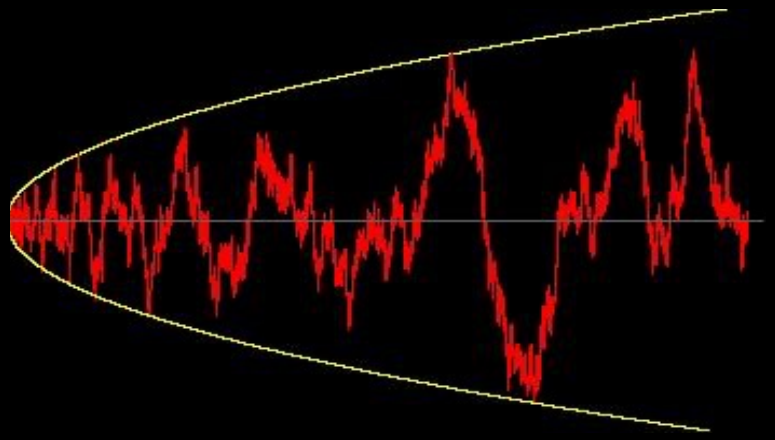
Second Edition

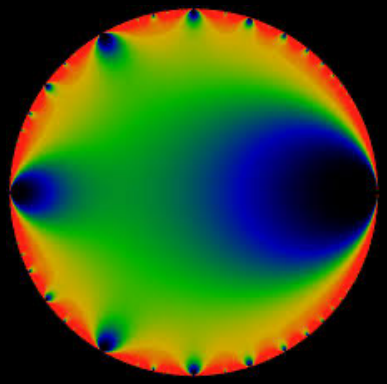
Giuseppe Mussardo

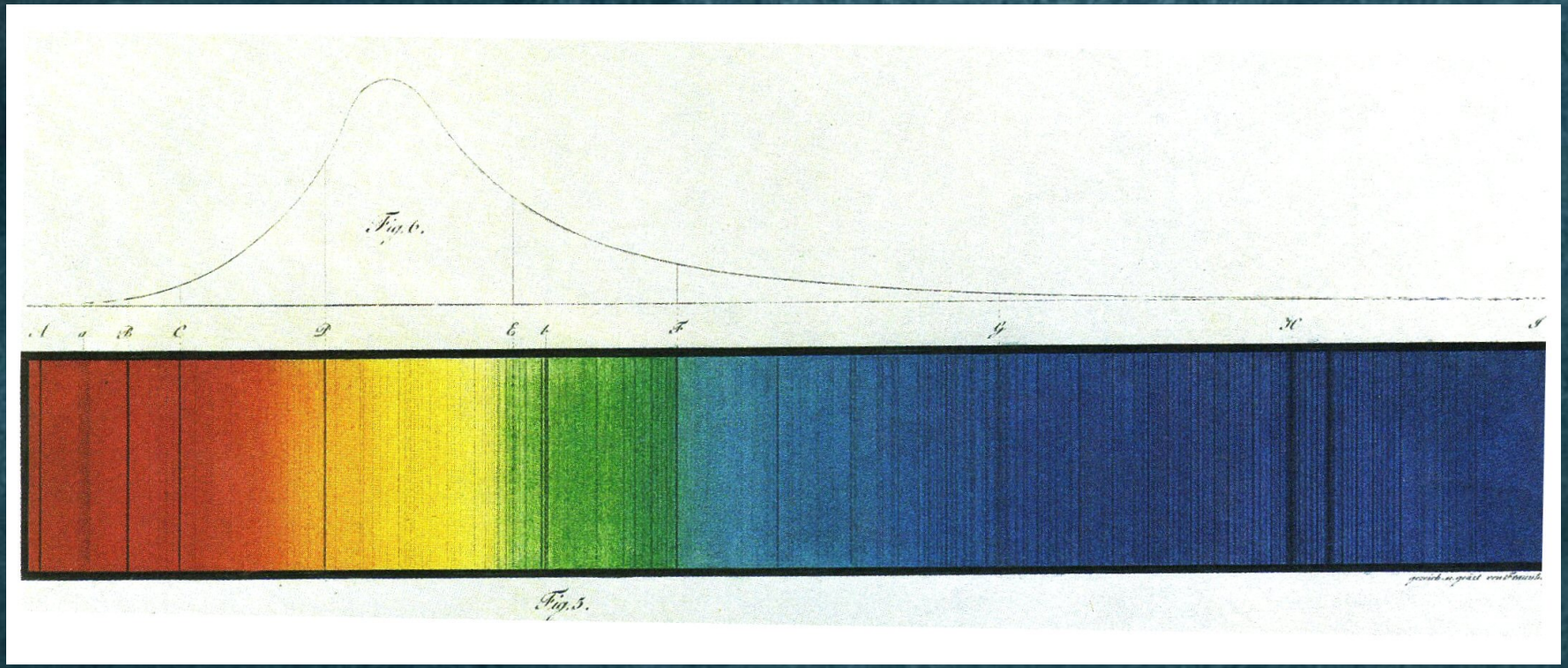
OXFORD GRADUATE TEXTS

There is an increasing interest for the profound and engaging links recently discovered between Number Theory and Physics









$$\nu_{n,m} = E_n - E_m$$

Natural questions

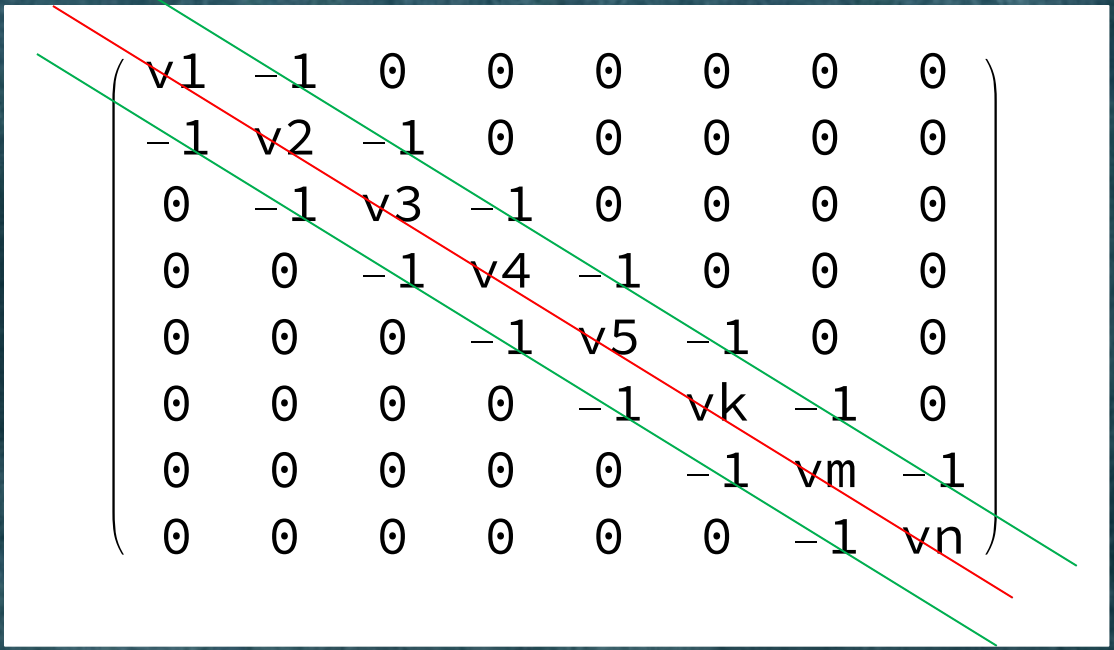
- Given an arithmetic sequence $\{S_n\}$, does exist a quantum mechanics system which has this sequence as a spectrum?

- Is the Hamiltonian of such a system unique?

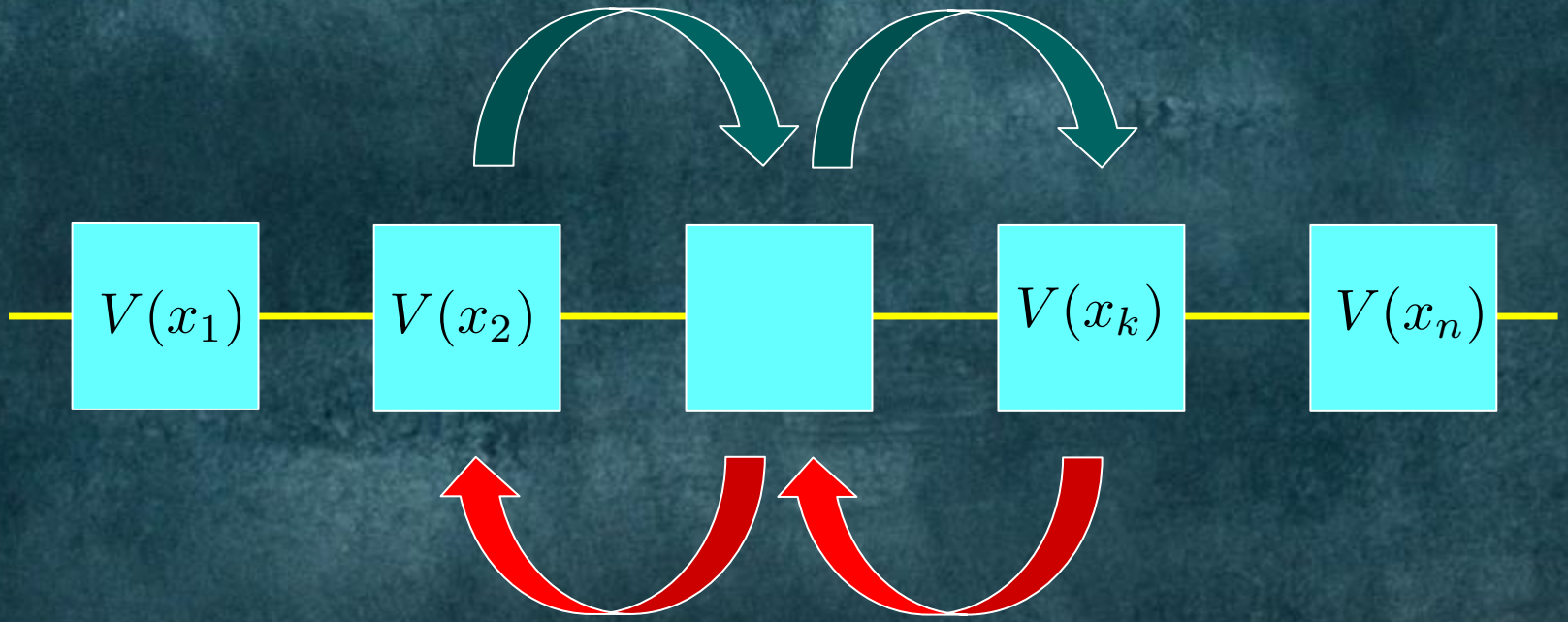
Our attention is on one-dimensional and one-body Hamiltonians of the form

$$H = \frac{p^2}{2m} + V(x)$$

Equivalently, on tridiagonal Hamiltonians of the form

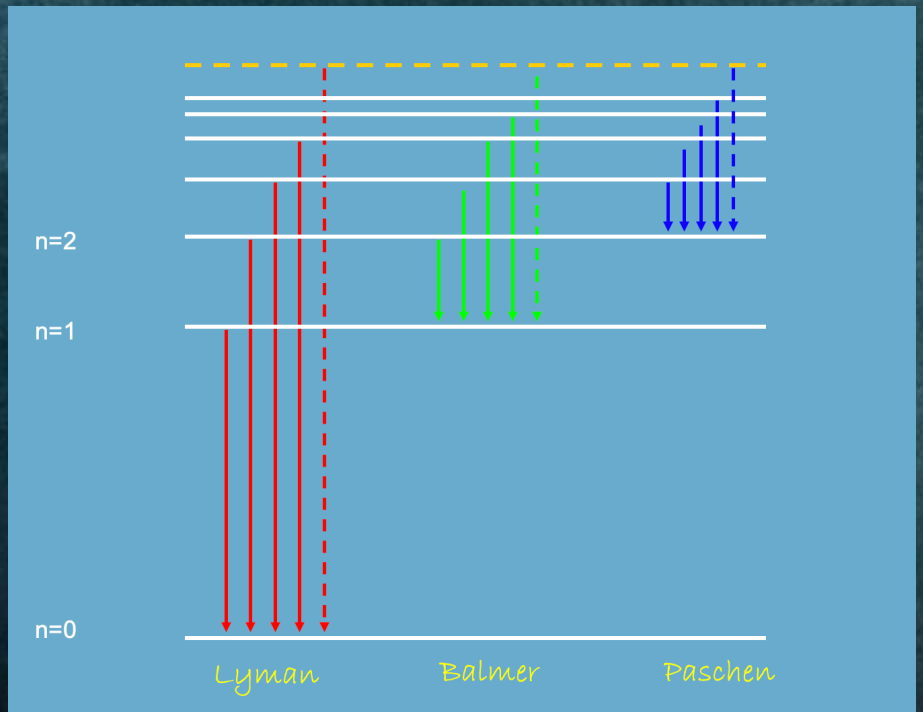


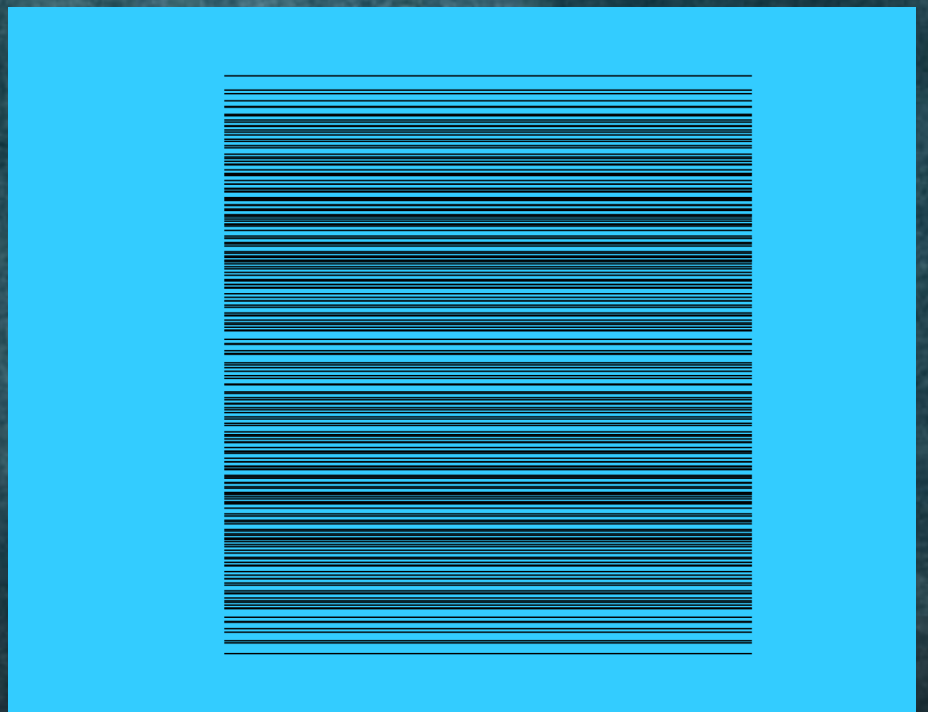
Equivalently, on tridiagonal Hamiltonians of the form



Why one-body Hamiltonians?

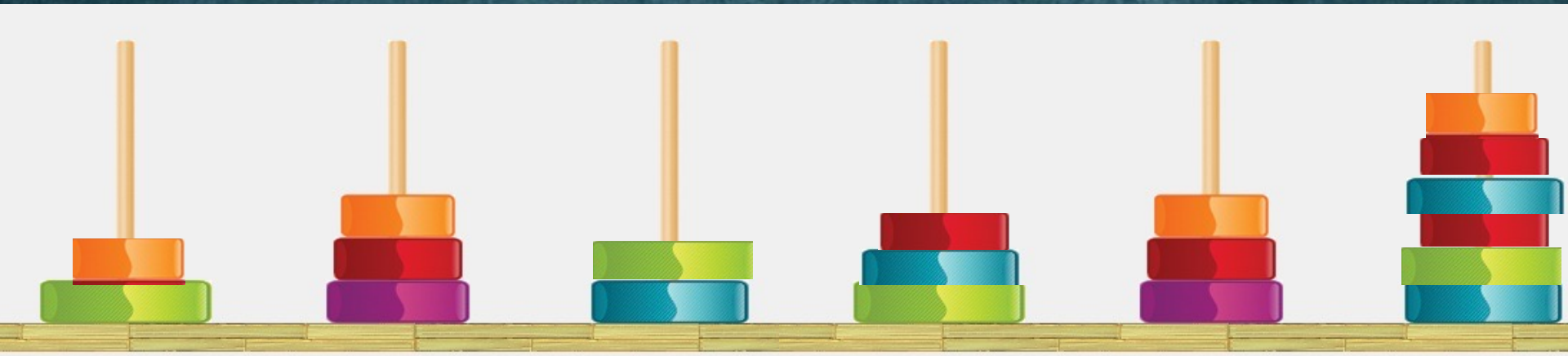
- These Hamiltonians possess discrete spectrum
- Many-body Hamiltonians on the other hands, have dense spectrum





But, we can use nevertheless many-body Hamiltonians to encode interesting number sequences!

- Instead of using energy levels, use wave functions!



$$n_i = \{S_n\}$$

Prime Suspects in a Quantum Ladder

Giuseppe Mussardo,[1,*] Andrea Trombettoni,[2,1] and Zhao Zhang[3,4]
[1]SISSA and INFN, Sezione di Trieste, via Beirut 2/4, I-34151 Trieste, Italy
[2]Department of Physics, University of Trieste, Strada Costiera 11, I-34151 Trieste, Italy
[3]Tsung-Dao Lee Institute, Shanghai Jiao Tong University, Shanghai 200240, China
[4]Nordita, KTH Royal Institute of Technology and Stockholm University, Roslagstullsbacken 23, SE-106 91 Stockholm, Sweden

(Received 10 May 2020; accepted 6 November 2020; published 9 December 2020)

In this Letter we set up a suggestive number theory interpretation of a quantum ladder system made of $\mathcal{N}$ coupled chains of spin 1/2. Using the hard-core boson representation and a leg-Hamiltonian made of a magnetic field and a hopping term, we can associate to the spins σ_a the prime numbers p_a so that the chains become quantum registers for square-free integers. The rung Hamiltonian involves permutation terms between next-neighbor chains and a coprime repulsive interaction. The system has various phases; in particular, there is one whose ground state is a coherent superposition of the first $\mathcal{N}$ prime numbers. We also discuss the realization of such a model in terms of an open quantum system with a dissipative Lindblad dynamics.

DOI: 10.1103/PhysRevLett.125.240603

Introduction.—The aim of this Letter is to point out some interesting connections between quantum many-body systems and number theory, in particular, prime numbers. Prime numbers are the building blocks of arithmetics and, arguably, one of the pillars of the entire mathematics [1,2]. Their nature has two fascinating but opposite features [3]: If their appearance in the sequence of natural numbers is rather unpredictable, their coarse-graining properties [e.g., their total number $\pi(x)$ less than x] can be captured instead rather efficiently by simple statistical considerations [4–8]. In particular, the scaling of the kth prime is particularly plain:

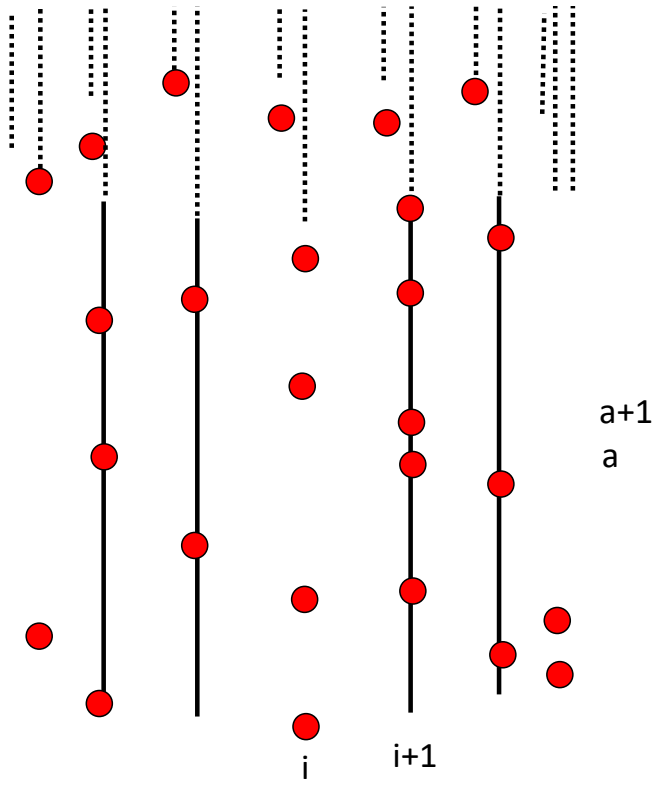
$$p_k \simeq k \log k. \tag{1}$$

Equally fascinating is the connection between prime numbers and quantum mechanics: Prime numbers, for instance, were the main concern of Shor's algorithm, one of the first quantum computing algorithms [9]. Moreover, the scaling behavior (1) permits one to show the existence of a single-particle one-dimensional quantum mechanical potential $V(x)$ with eigenvalues given just by the prime numbers and, therefore, permits one to address the primality test of a natural number in terms of a quantum scattering [10]. Such a potential $V(x)$ can be determined either semiclassically [10] or exactly, using in this case methods of supersymmetric quantum mechanics [11,12]. In experimental setups of cold atom systems, $V(x)$ could be realized using a holographic trap [13].

Turning now our attention to quantum many-body systems, for the dense nature of their spectra it is obviously impossible to have energy levels given by prime numbers, but we can have instead many-body ground state wave functions expressed in terms of prime numbers. This is what we are going to present below, where we consider a quantum ladder system with a suggestive number theoretic interpretation. We will see that such a system has a rich spectrum of ground states and, in particular, there is one whose wave function is given in terms of a highly coherent superposition of prime number occupations. To the best of our knowledge, this is the first time where a ground state of this type has been constructed.

Quantum ladder systems, made of coupled one-dimensional chains, have attracted considerable interest in recent years as truly interpolating between one- and two-dimensional systems [14–20]. In our case, we have $\mathcal{N}$ coupled half-infinite chains of spins 1/2 subjected to a magnetic field and a hopping term. As discussed below, properly tuning these two interactions, we can put in correspondence the spins with the prime numbers and reformulate the spin-spin rung interaction in terms of coprimality conditions (two integers are coprime if they do not share common factors other than 1).

Degrees of freedom.—As it is well known, spin 1/2 can be described by hard-core bosons: The mapping between the Pauli matrices σ_a and the hard-core annihilation and creation operators f and $f^\dagger$ [$f^2 = (f^\dagger)^2 = 0$] is provided by $\sigma_z = f^\dagger f - 1/2$; $\sigma_+ = f^\dagger$; $\sigma_- = f$ [21]. Hence, instead of the spins, we can equivalently take as degrees of freedom the hard-core boson operators $f_i(a)$ and $f_i^\dagger(a)$, where the index i refers to the ith chain ($i = 1, 2, \ldots, \mathcal{N}$), while $a = 1, 2, \ldots$ to the vertical position along the half-infinite chain (see Fig. 1). Since $[f_i(a)]^2 = [f_i^\dagger(a)]^2 = 0$, the occupation number of each vertical site in the ladder can take only values $\{0, 1\}$. Let $|\mathrm{vac}\rangle$ be the vacuum state, i.e.,



Natural questions

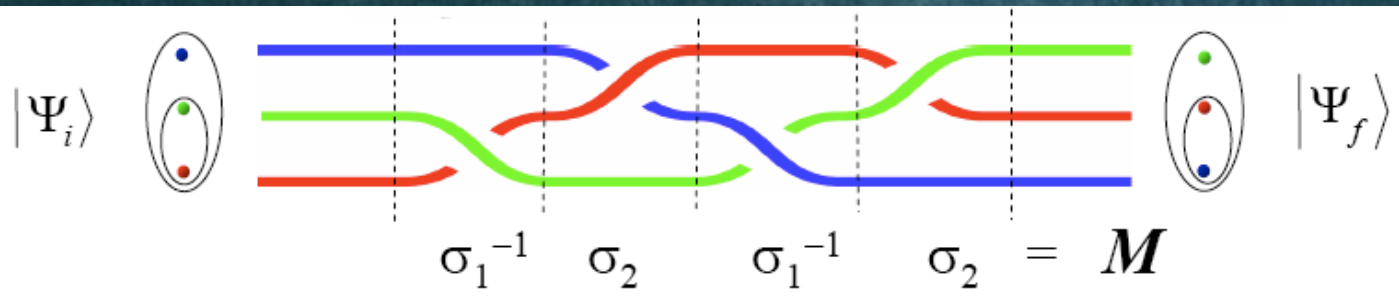
- Given an arithmetic sequence $\{S_n\}$, does exist a quantum mechanics system which has this sequence as a spectrum?

- Is the Hamiltonian of such a system unique?

Fibonacci numbers

$$F_{n+2} = F_{n+1} + F_n$$

$\{F_n\}$ =1, 1, 2, 3, 5, 8, 13, 21, 34, 55,…



$$|\Psi_f\rangle = M^{-1} |\Psi_i\rangle$$

Fibonacci numbers

$$F_{n+2} = F_{n+1} + F_n$$

$\{F_n\}$ =1, 1, 2, 3, 5, 8, 13, 21, 34, 55,…

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$$

$$F_{n+2} = F_{n+1} + F_n$$

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n$$

Fibonacci numbers

$$F_{n+2} = F_{n+1} + F_n$$

$\{F_n\}$ =1, 1, 2, 3, 5, 8, 13, 21, 34, 55,…

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$$

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$$

- Unfortunately, it does not exist a quantum system which has the Fibonacci numbers as spectrum…

- The reason is that their sequence grows too fast

- Similarly, it does not exist a quantum Schroedinger Hamiltonian with a spectrum given, for instance, by the Mersenne numbers or the perfect numbers

$$M_n = 2^n - 1$$

$$P_n = 2^{n-1} M_n$$

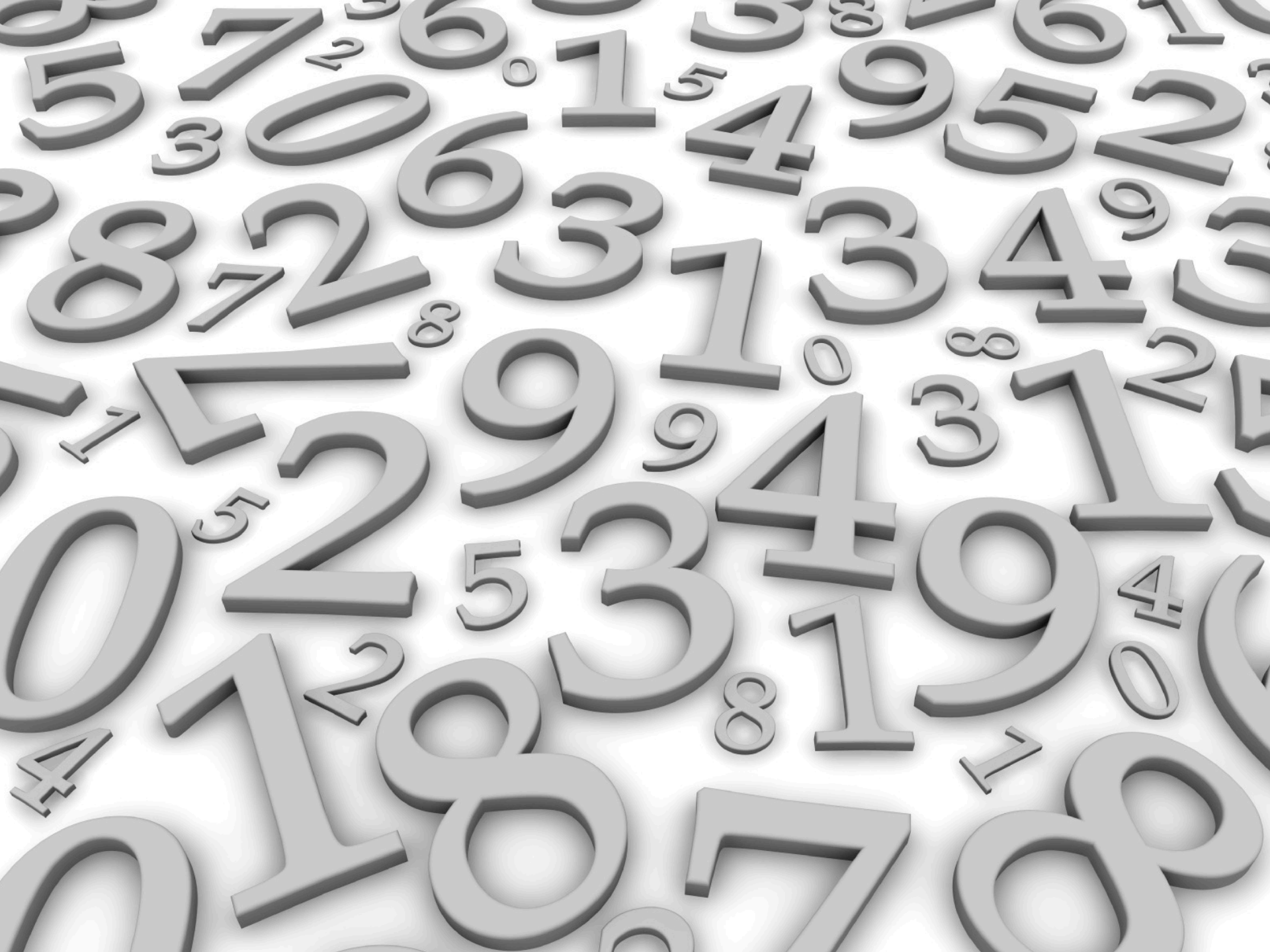
Bound on the growth of eigenvalues

- For a one-dimensional Hamiltonian of the form

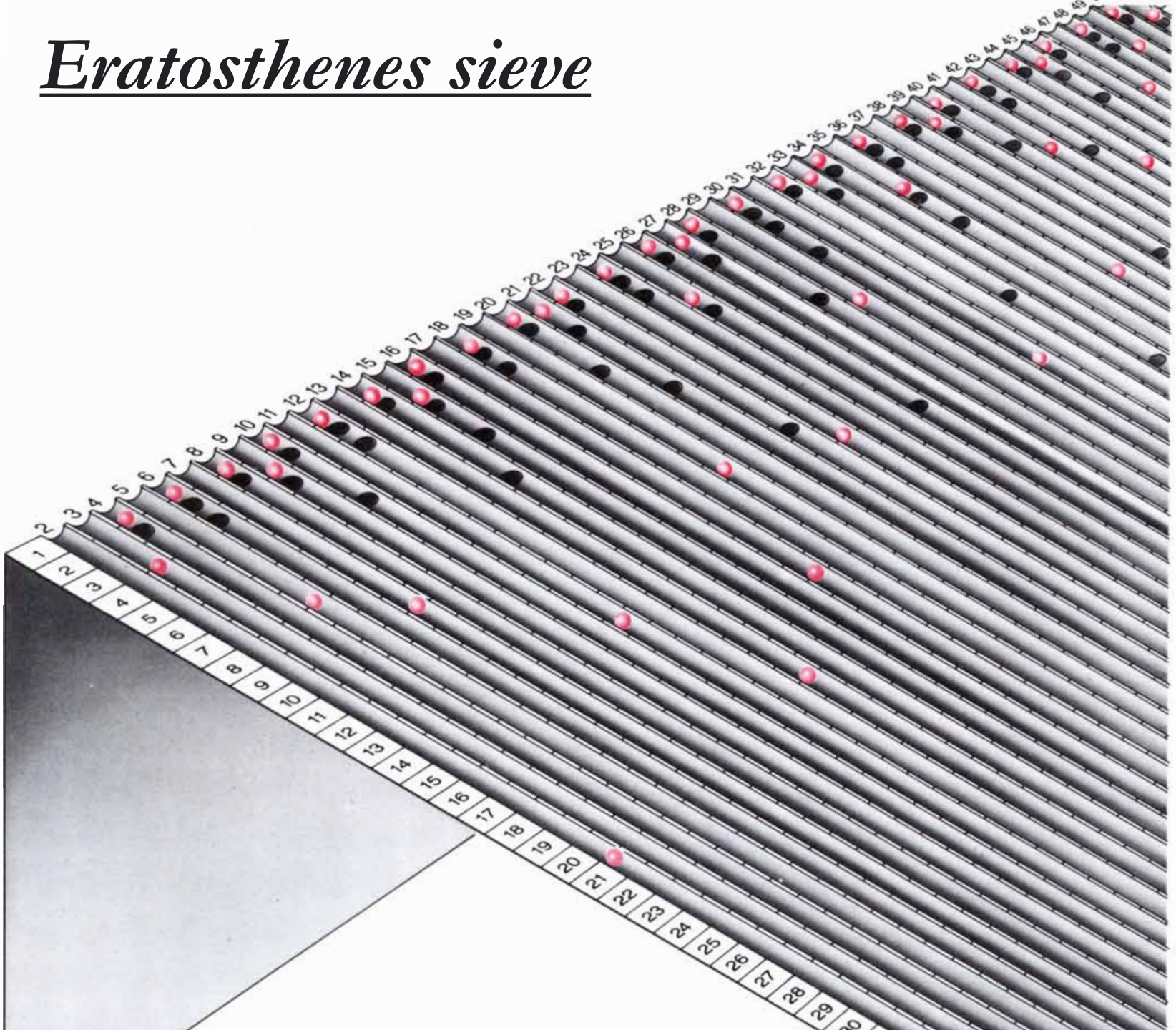
$$H = \frac{p^2}{2m} + V(x)$$

the sequence of energy eigenvalues must satisfy

$$E_n \leq n^2$$



Eratosthenes sieve



It does not exist a close formula for the n-th prime number

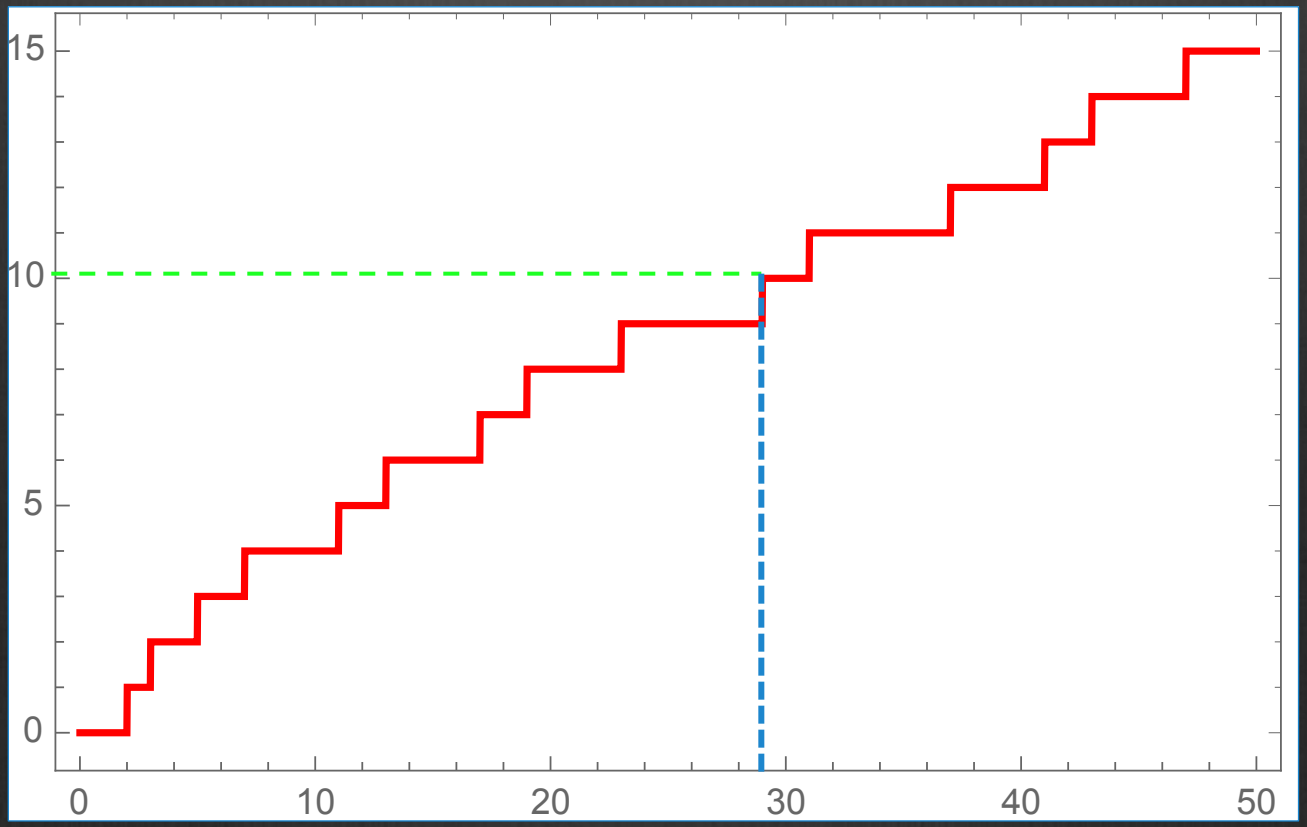
However their scaling law is captured by this simple formula

$$p_n \simeq n \log n$$

Hence, there must exist a quantum Hamiltonian that has the primes as eigenvalues!

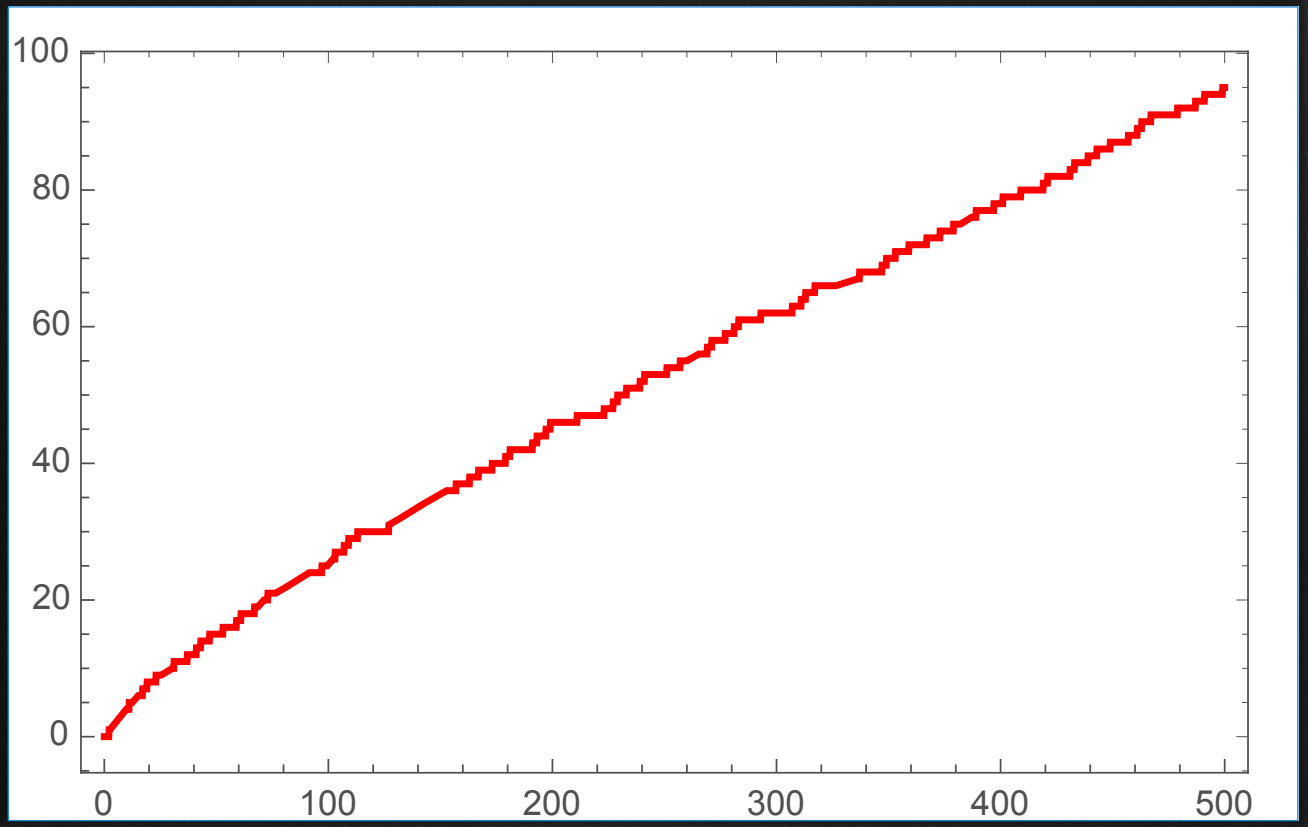
Counting the Primes

$\pi(x)$: gives the number of primes less or equal to x



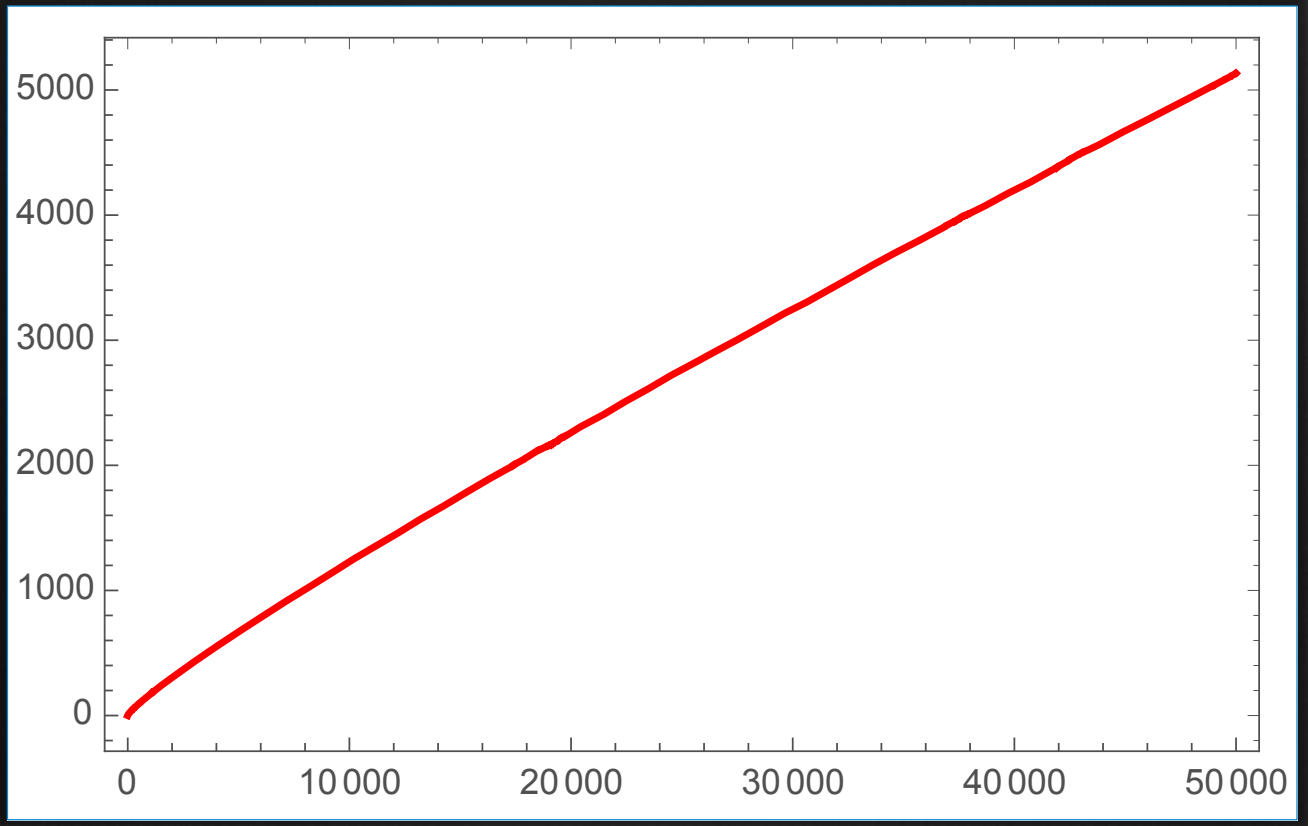
Counting the Primes

$\pi(x)$: gives the number of primes less or equal to x



Counting the Primes

$\pi(x)$: gives the number of primes less or equal to x



Prime Number Theorem: Riemann

$$\pi(x) \simeq R(x)$$

$$R(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} Li(x^{1/n})$$

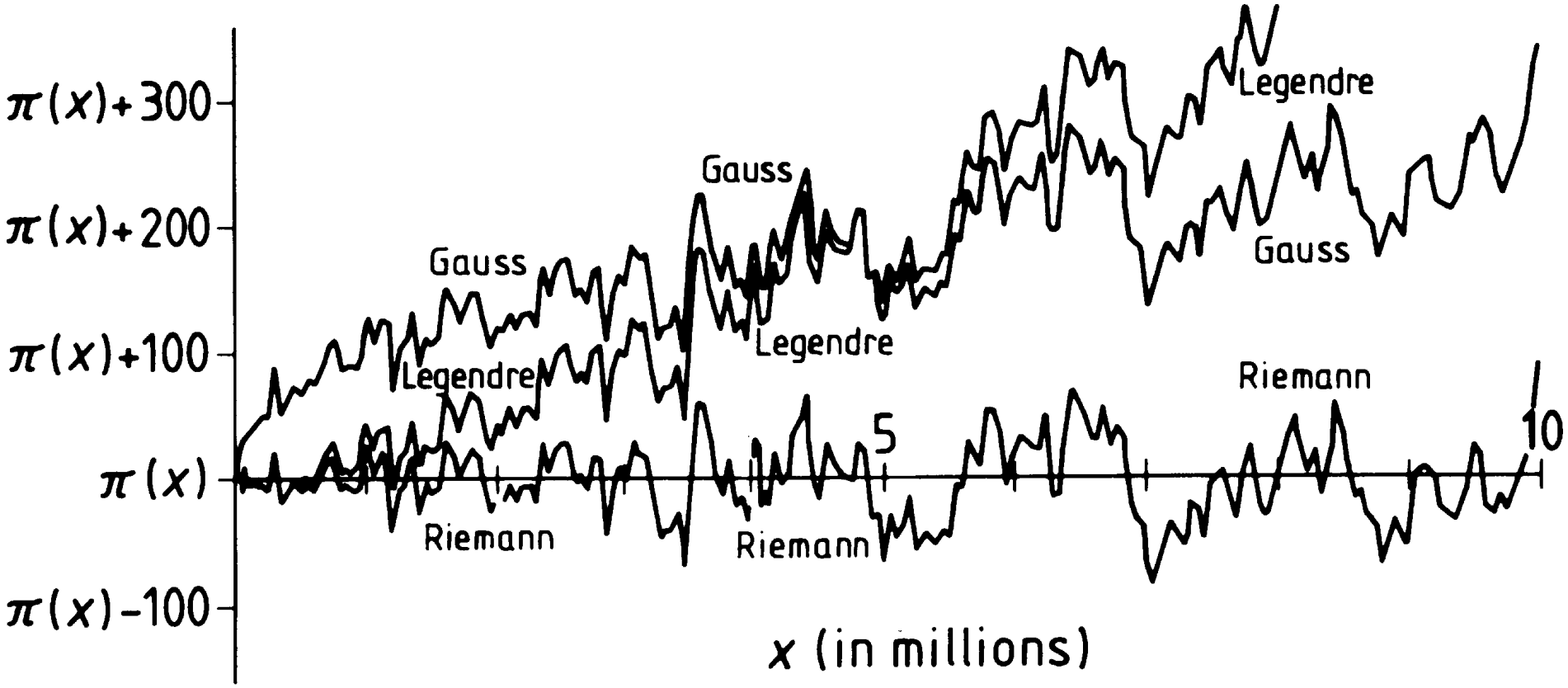
$$Li(t) \equiv \int_1^t \frac{ds}{\log s}$$

Prime Number Theorem: Riemann

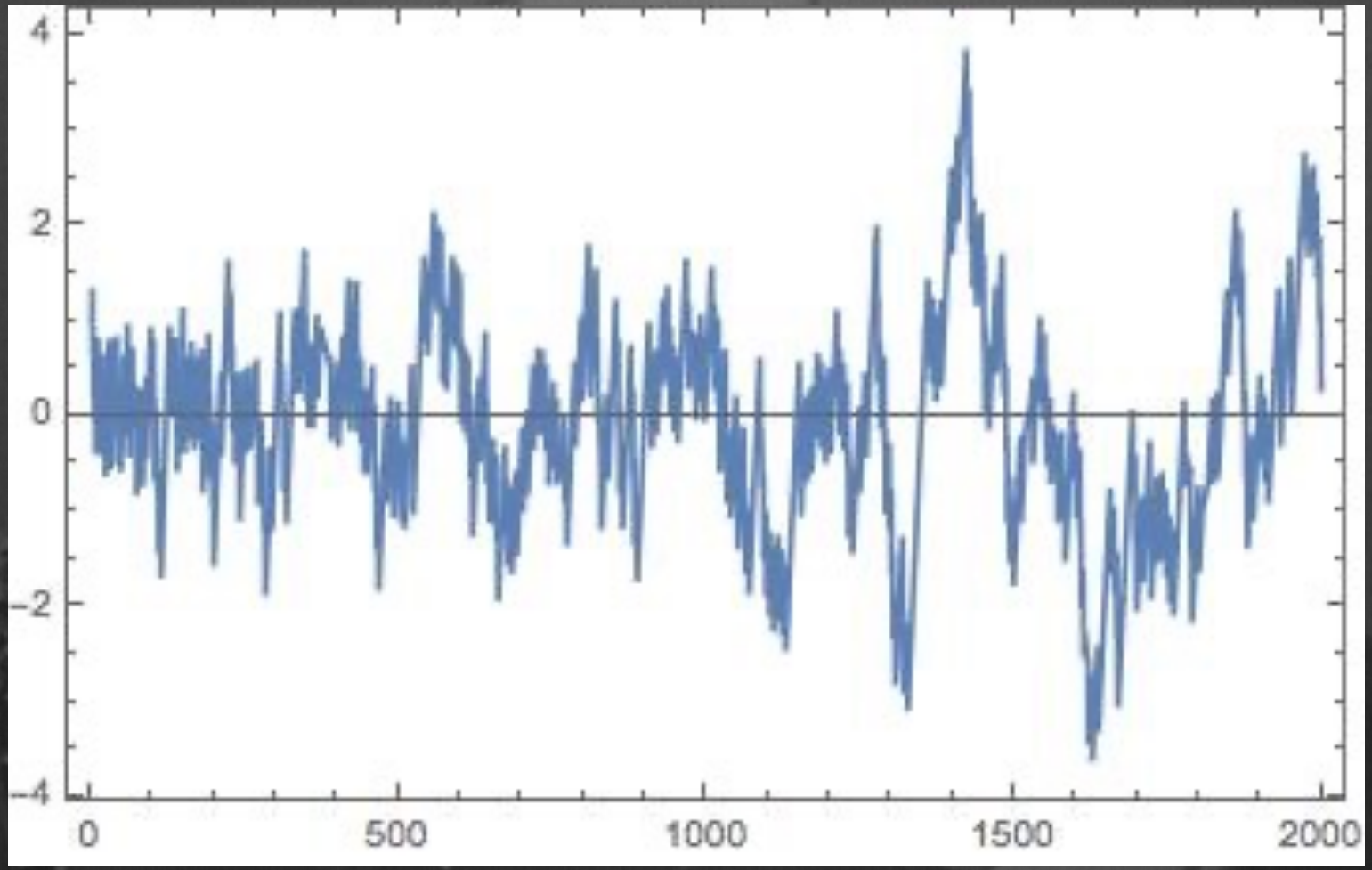
$$\pi(x) \simeq R(x)$$

$$R(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} Li(x^{1/n})$$

$$\mu(n) = \begin{cases} 1 & \text{if n is squarefree with an even number of prime factors} \\ -1 & \text{if n is squarefeee with an odd number of prime factors} \\ 0 & \text{if n has a squared prime factor} \end{cases}$$


π(x)+300
π(x)+200
π(x)+100
π(x)
π(x)−100
Gauss
Legendre
Riemann
Gauss
Legendre
Riemann
Legendre
Gauss
Riemann
5
10
x (in millions)

“The music of the primes”



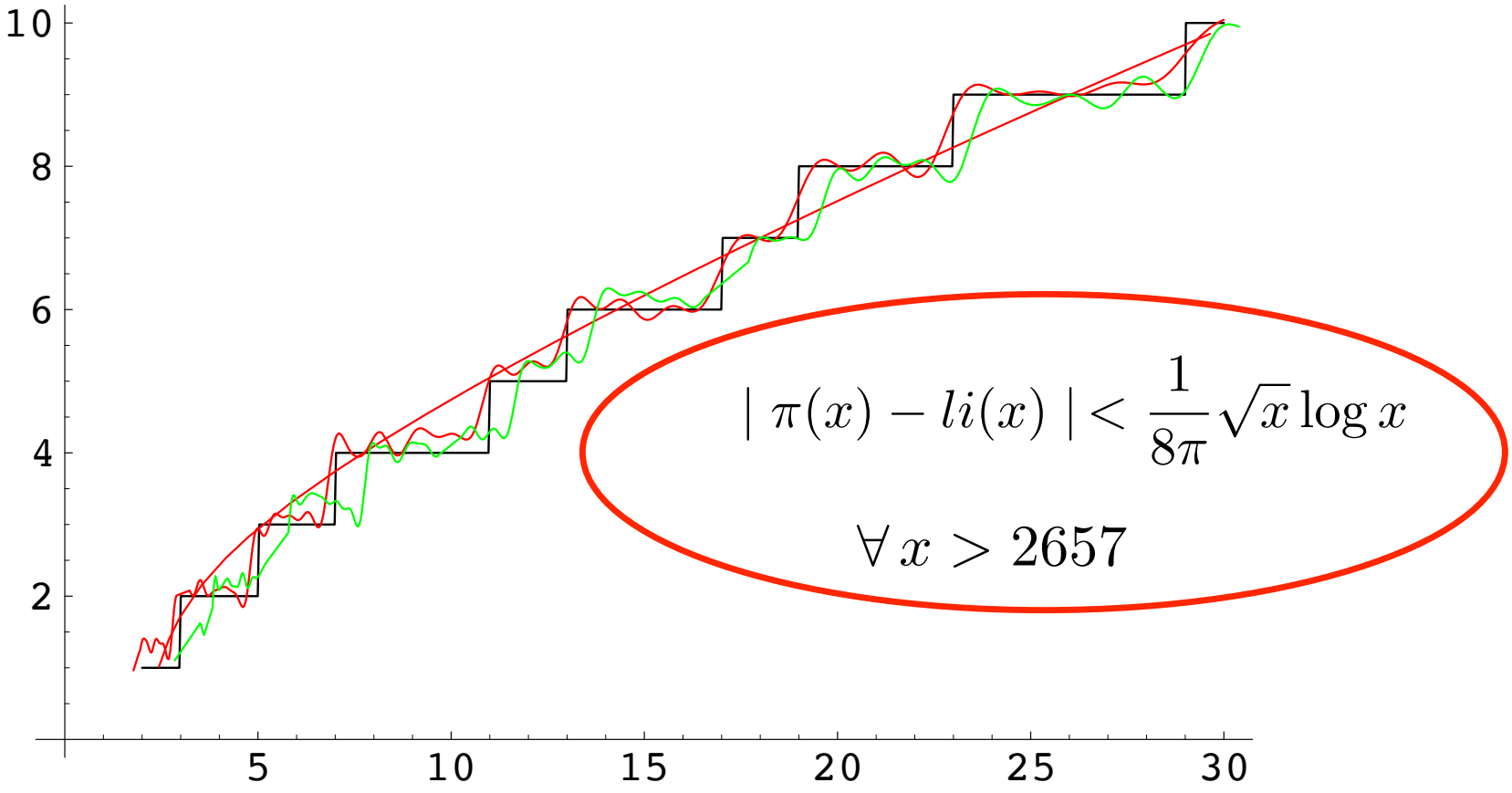
Prime Number Theorem: Riemann

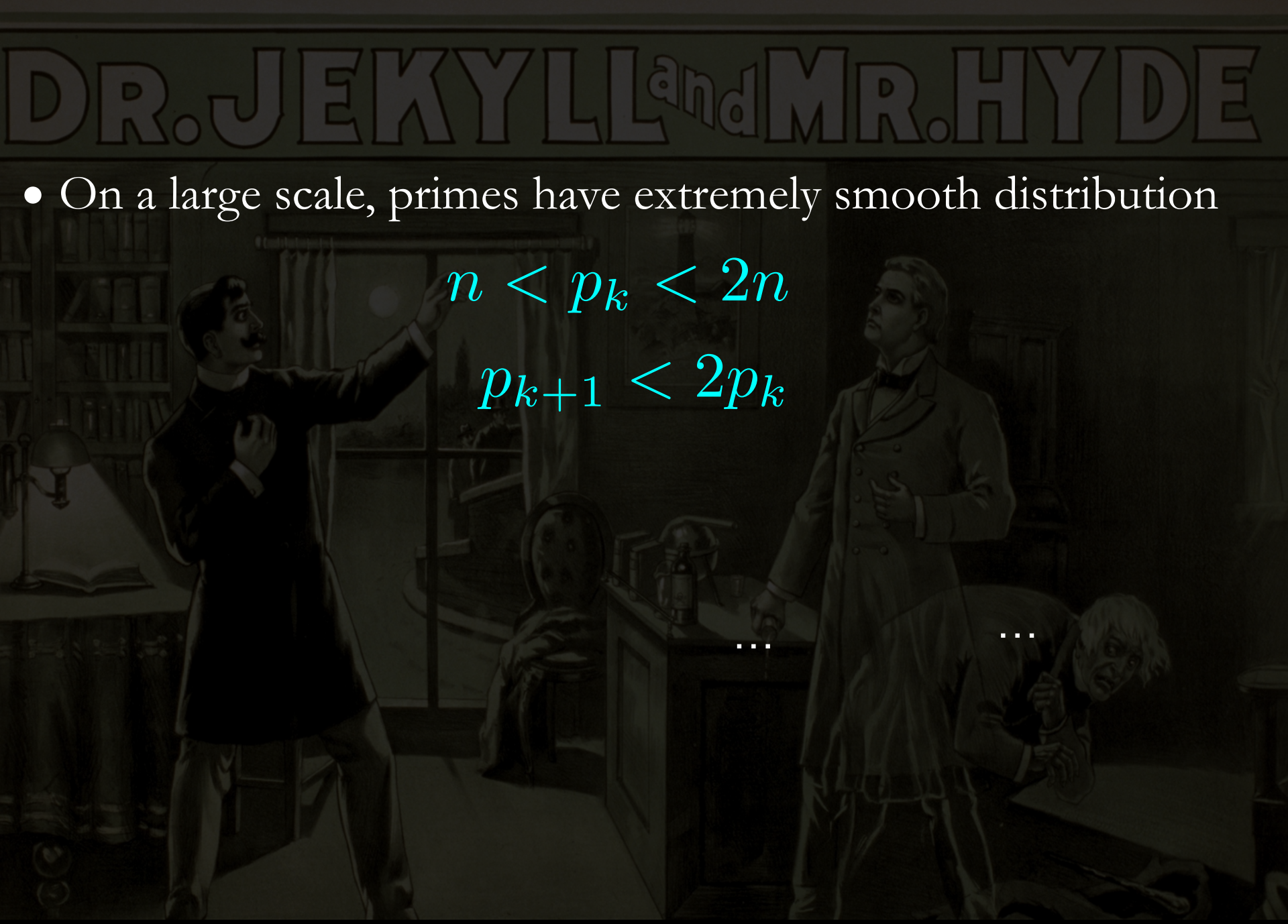
$$R(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} Li(x^{1/n})$$

$$\pi(x) = R(x) - \sum_{\rho} R(x^{\rho})$$

ϱ: non-trivial zeros of the ζ(z) Riemann function in the critical strip

Climbing the staircase





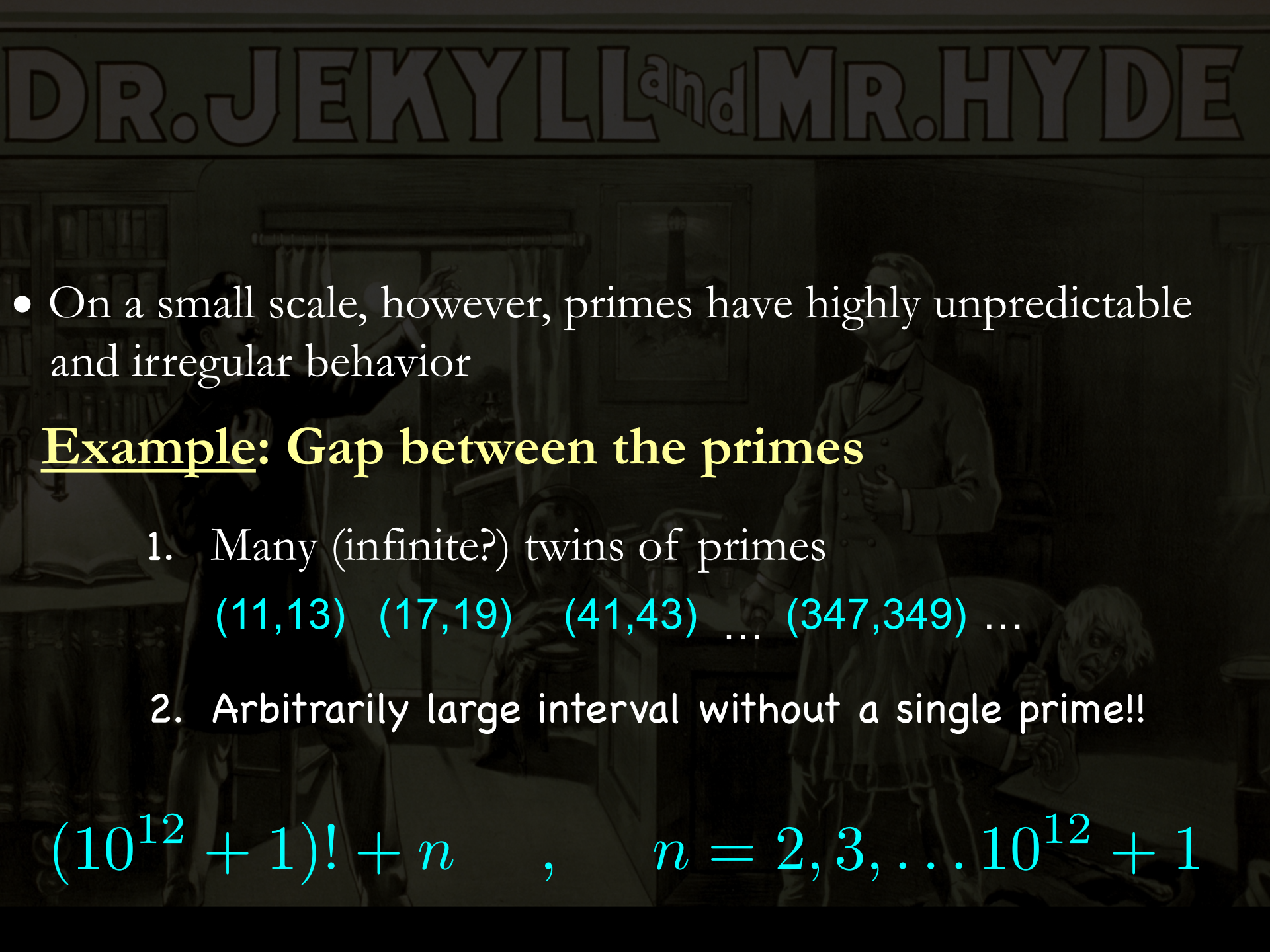
- On a large scale, primes have extremely smooth distribution

$$n < p_k < 2n$$

$$p_{k+1} < 2p_k$$

…

…



- On a small scale, however, primes have highly unpredictable and irregular behavior

Example: Gap between the primes

1. Many (infinite?) twins of primes

   (11,13) (17,19) (41,43) … (347,349) …

2. Arbitrarily large interval without a single prime!!

$$(10^{12}+1)!+n \quad , \quad n = 2, 3, \ldots 10^{12}+1$$

Inverse problems

Given an admissible sequence of numbers S_n,

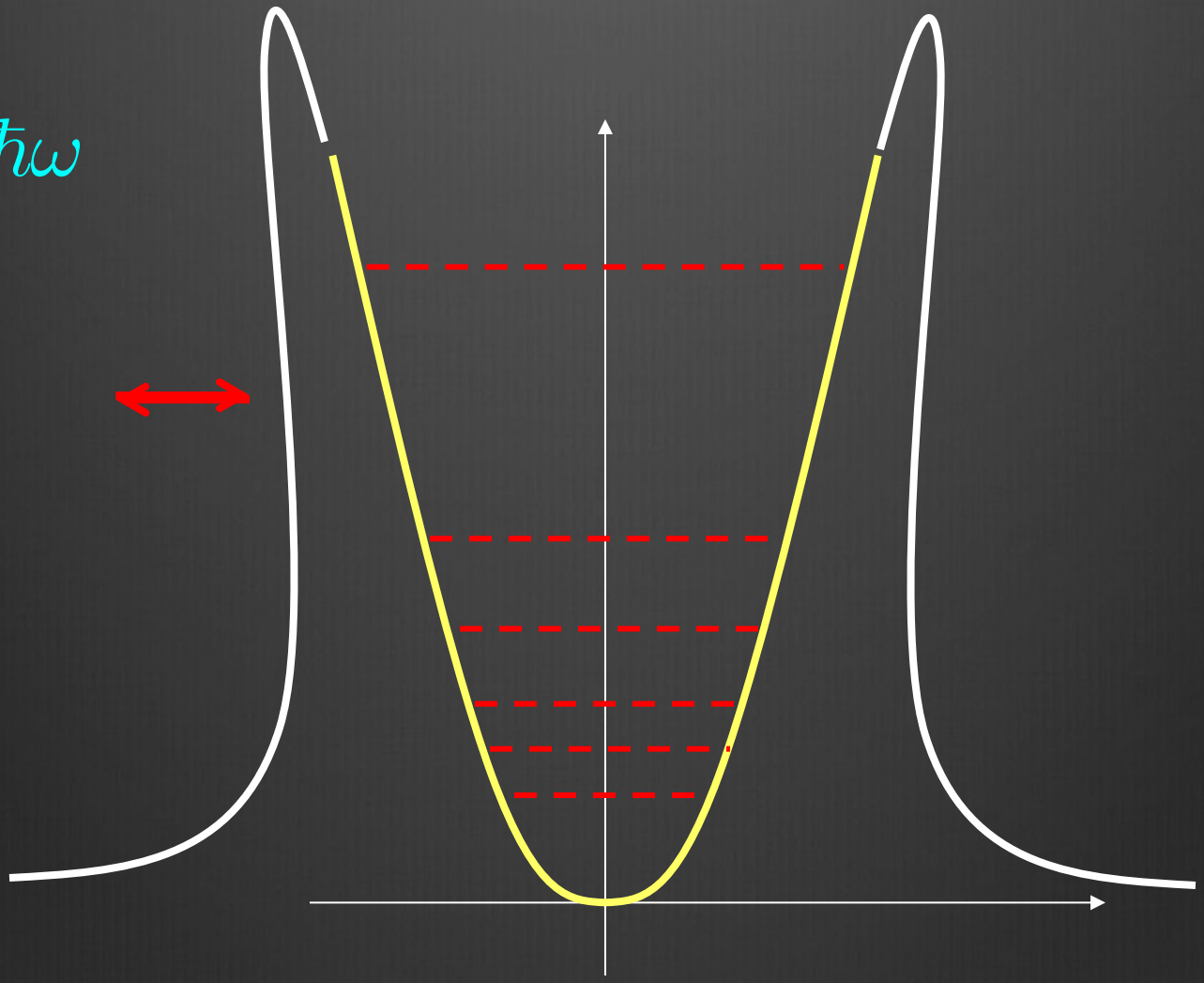
how to find the potential V(x) ?

- Semi-classical method
- Dressing method (solitonic equations)

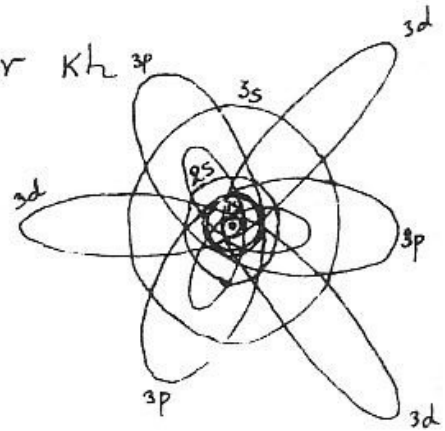
Quantum experiment

Primality test

$E = N\hbar\omega$



$$\int_{\varphi=0}^{\varphi=2\pi} p_\varphi \, d\varphi = jh \int_{\varphi=0}^{\varphi=2\pi} p_r \, dr \quad Kh$$



$$E_{j,K} = -\frac{2\pi^2 m_e e^2 Z^2}{h^2} \frac{1}{(j+K)^2}$$

$$j + K = n$$

$$E_n = -\frac{2\pi^2 m_e e^2 Z^2}{h^2} \frac{1}{n^2} \qquad h\nu_{m,n} = E_n - E_m$$

Semi-classical potential

$$\oint p(x)\,dx = \oint \sqrt{E - V(x)}\,dx = n\,\hbar$$

This formula can be inverted, i.e.once the energy levels E_n are assigned, we can find the potential V(x) !

Semi-classical potential

GM, (1995)

$$x(V) = \frac{\hbar}{\sqrt{2m}} \int_{E_0}^{V} \frac{dE}{\omega(E)\sqrt{V-E}} \ ,$$

$$E_n \to p_n \qquad\qquad p_n = \pi^{-1}(n)$$

$$\omega(p) = \frac{dp_n}{dn} = \frac{1}{\frac{dn}{dp_n}}$$

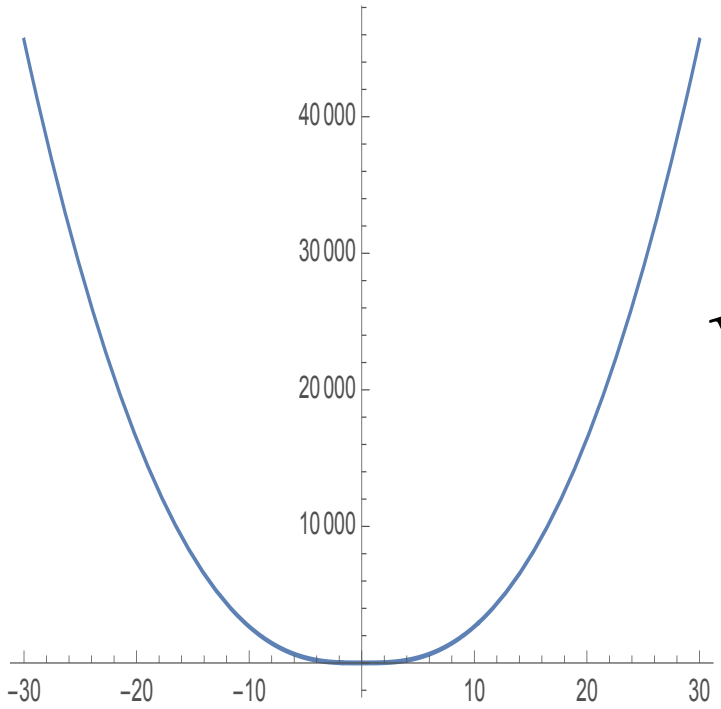
Semi-classical potential

GM, (1995)

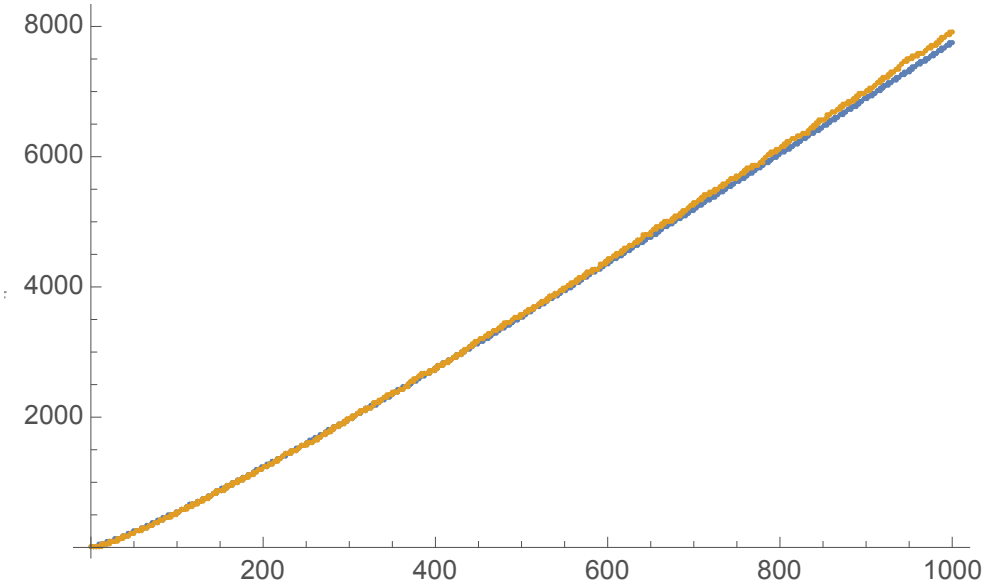
$$x(V) = \frac{\hbar}{\sqrt{2m}} \int_{E_0}^{V} \frac{dE}{\omega(E)\sqrt{V-E}} ,$$

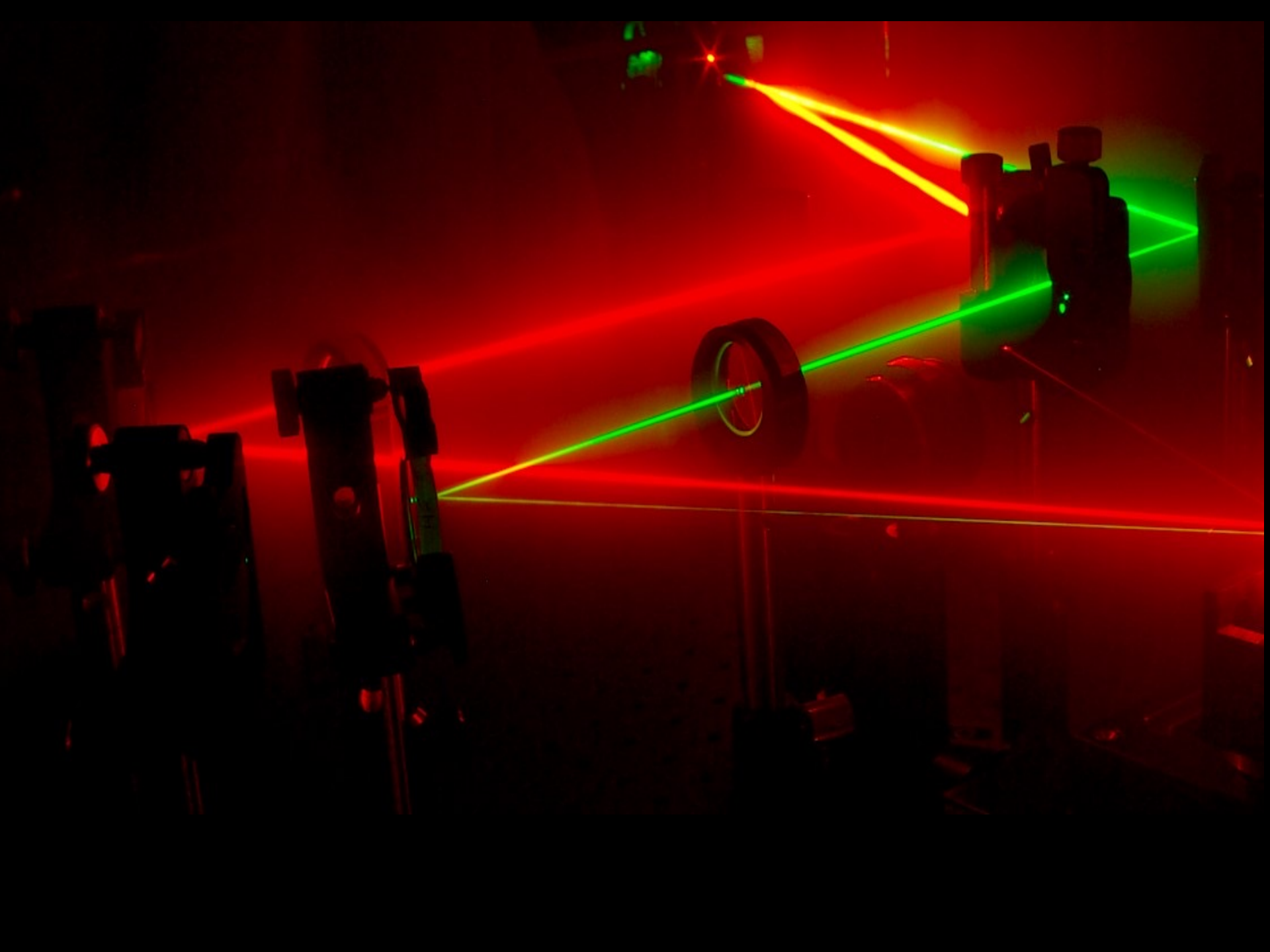
For prime numbers…

$$\omega^{-1}(E) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} \frac{\mathcal{E}^{\frac{1-n}{n}}}{\ln \mathcal{E}}$$



$$V(x) \simeq x^2 \log x$$



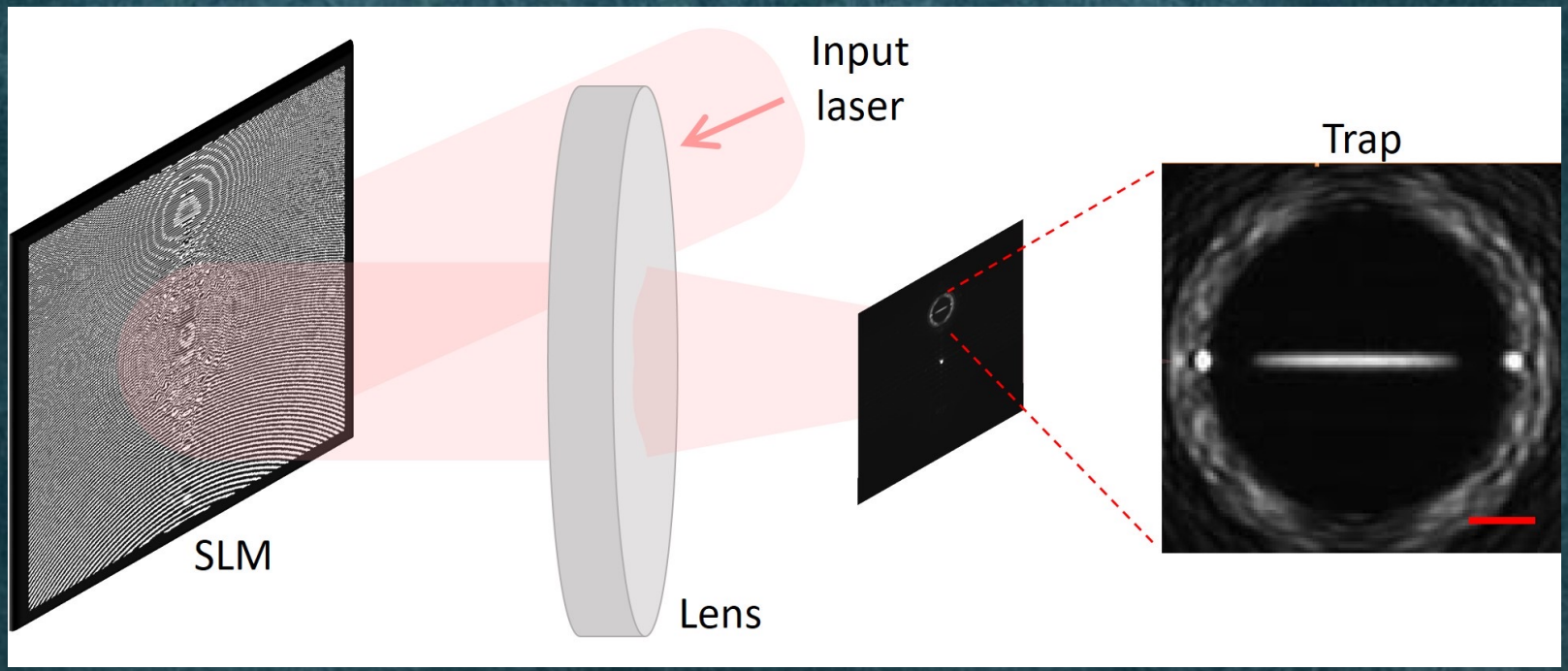


PNAS nexus

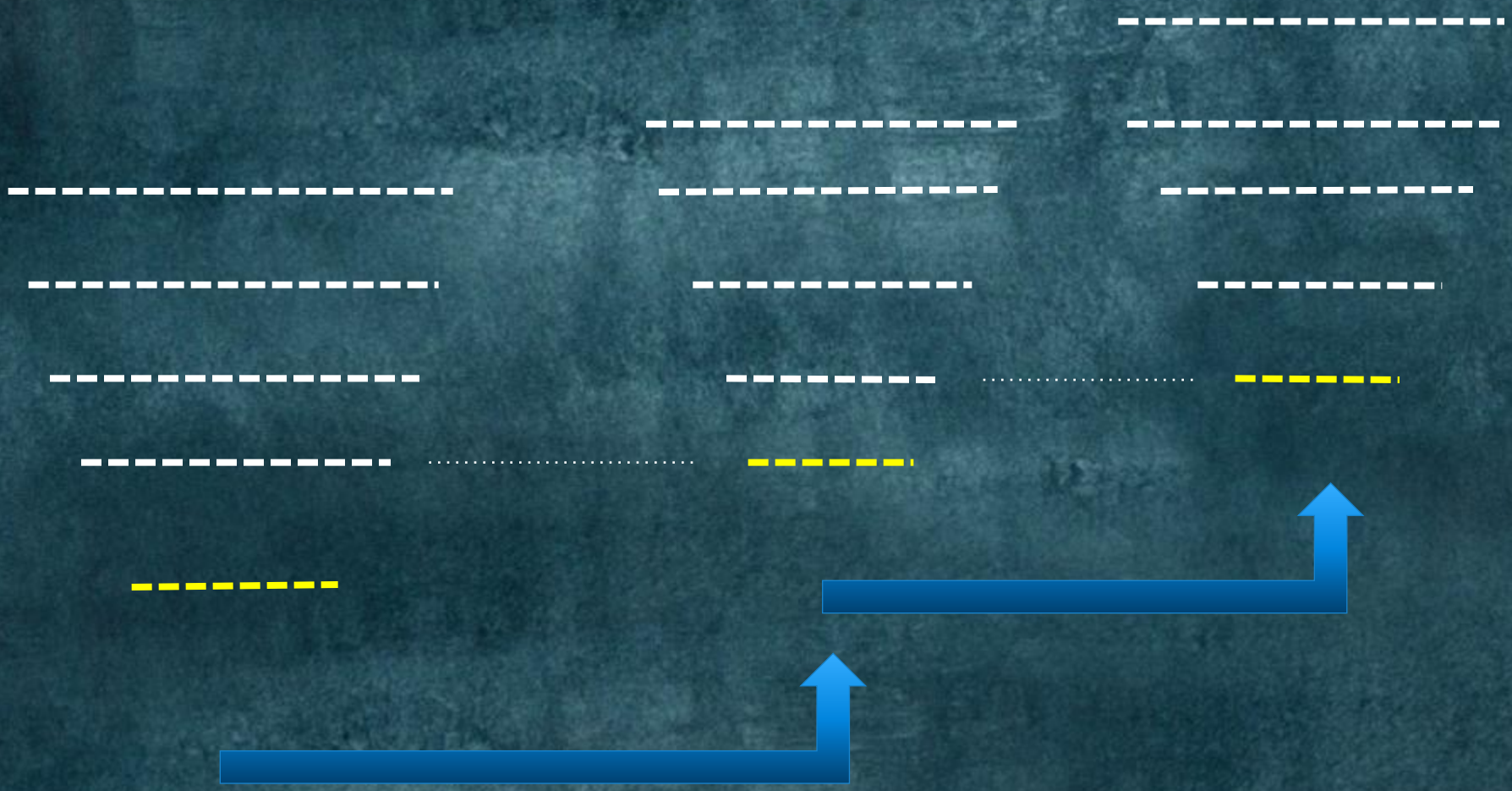
PNAS Nexus, 2022, **2**, 1–9
https://doi.org/10.1093/pnasnexus/pgac279
Advance access publication date: 12 December 2022
Research Report

Holographic realization of the prime number quantum potential

Donatella Cassettari [a,*], Giuseppe Mussardo [b] and Andrea Trombettoni [b,c]



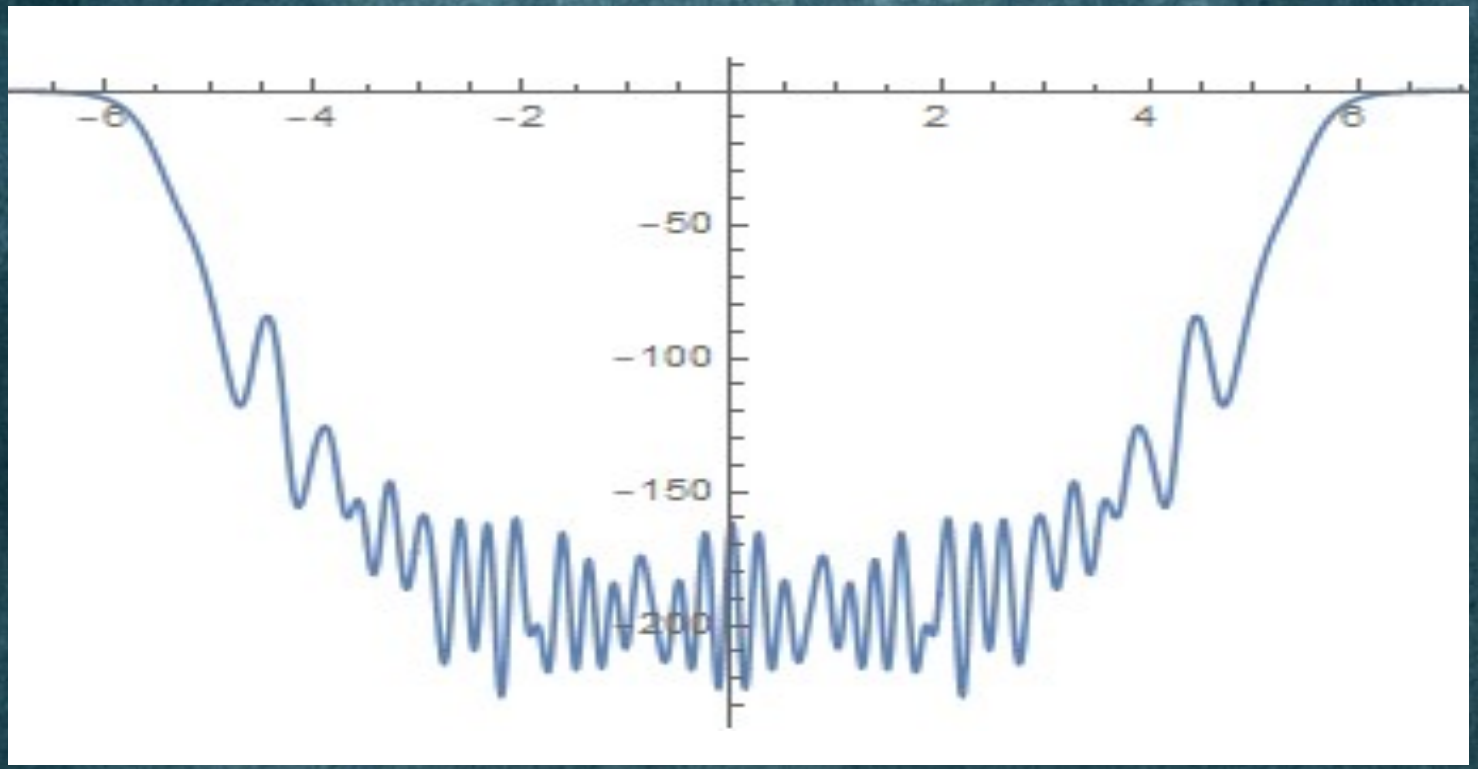
SUSY Quantum Mechanics



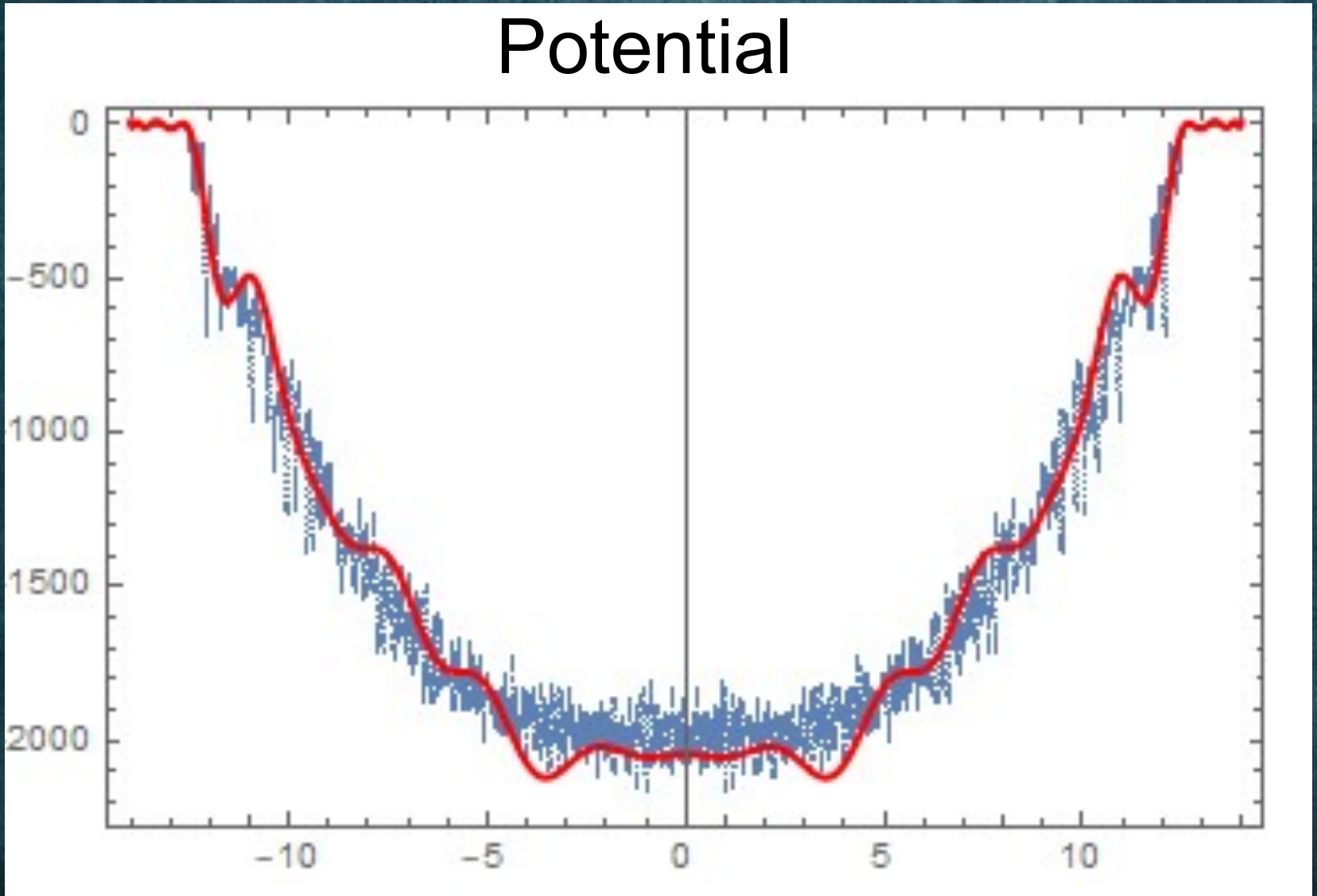
$$V_1(x) \to V_2(x) \to V_3(x) \to \cdots$$

$$E = \{E_1, E_2, E_3, \ldots, E_n\}$$

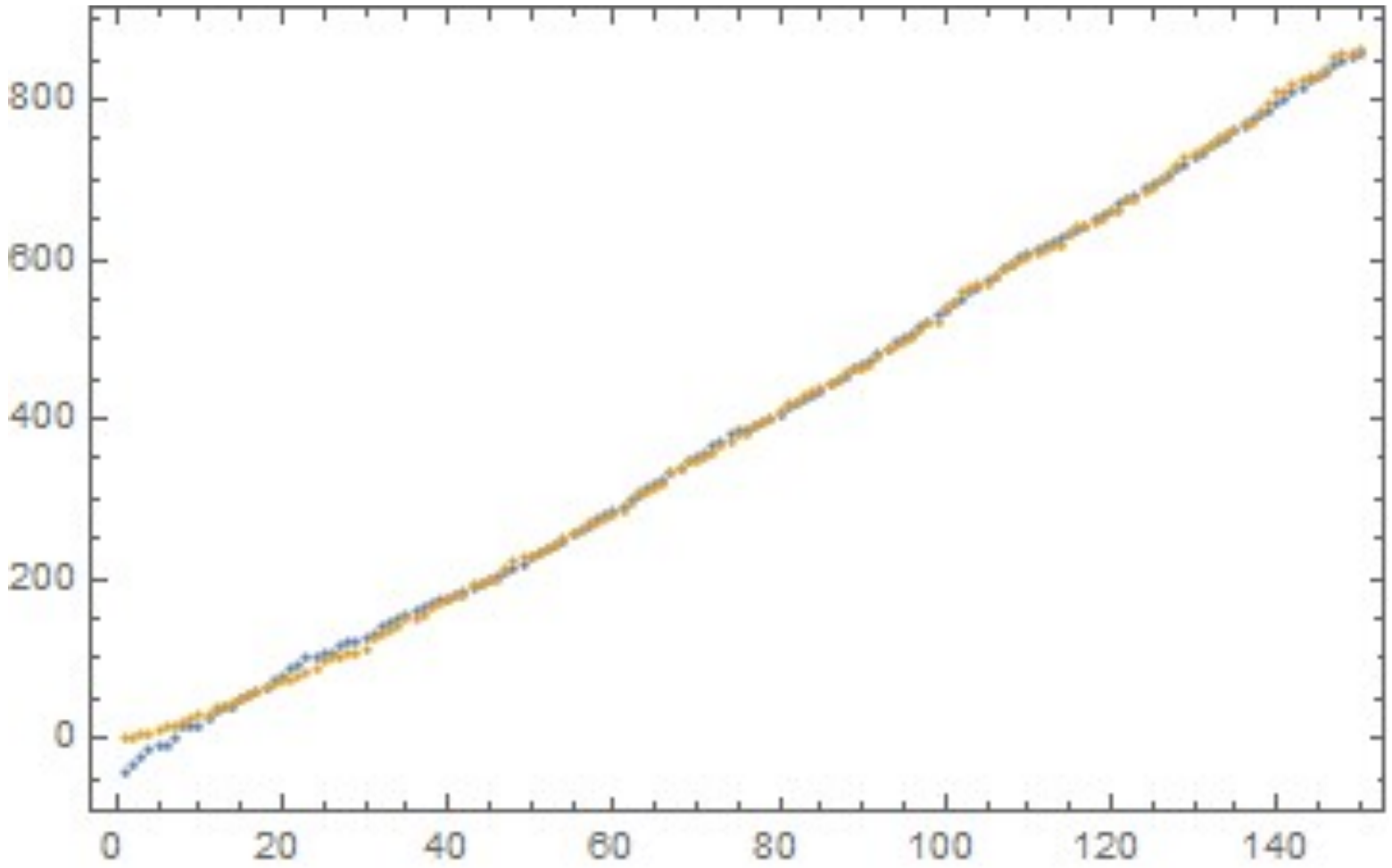
Quantum potential relative to the first 45 primes



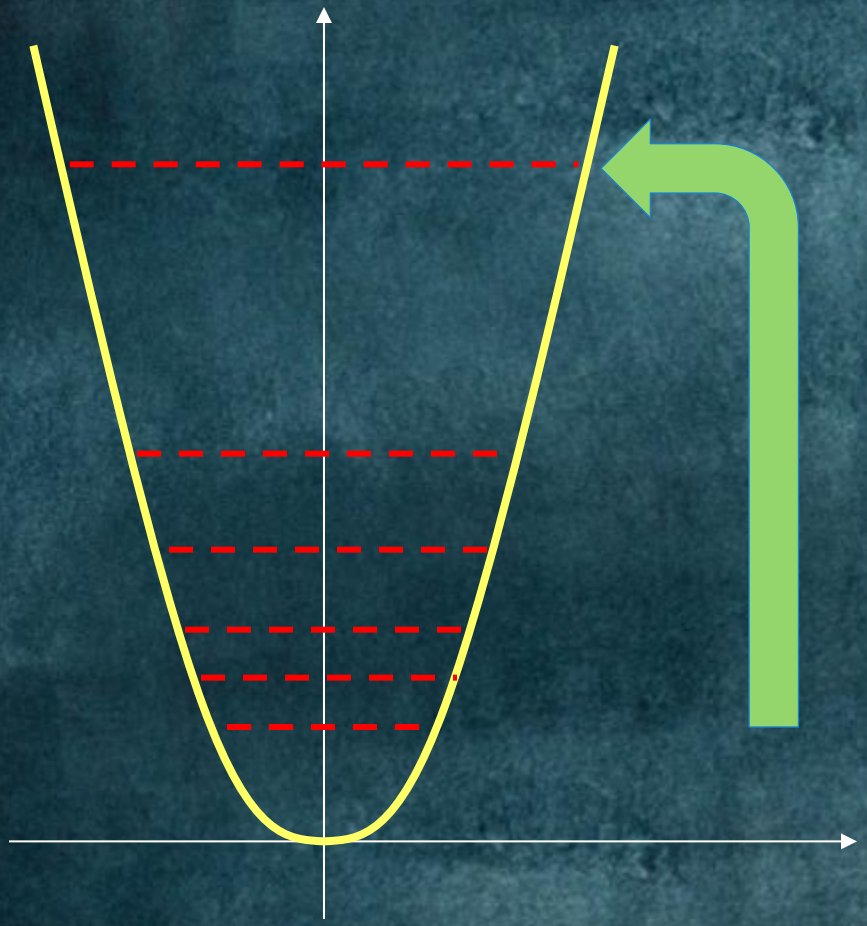
Quantum potential relative to the first 150 primes approximated by the first 35 Chebychev polys



n=35



Parametric resonance

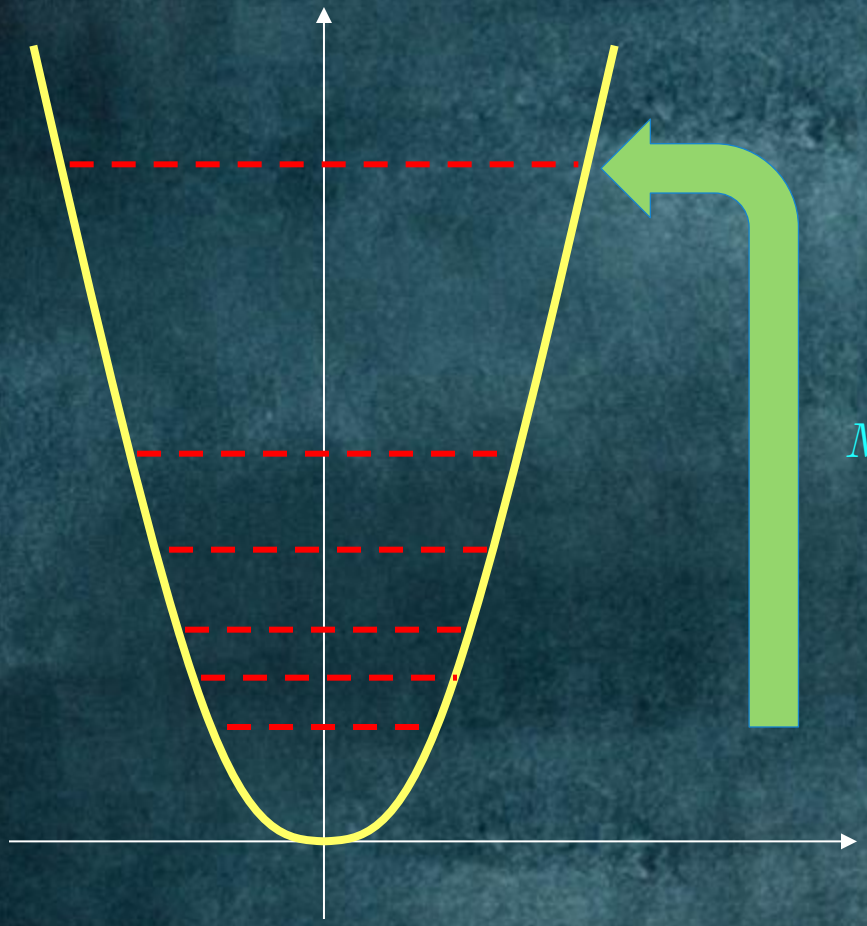


$$H \to H + W(x)\cos\omega t$$

$$W_I = e^{iHt/\hbar}\, W\, e^{-iHt/\hbar}$$

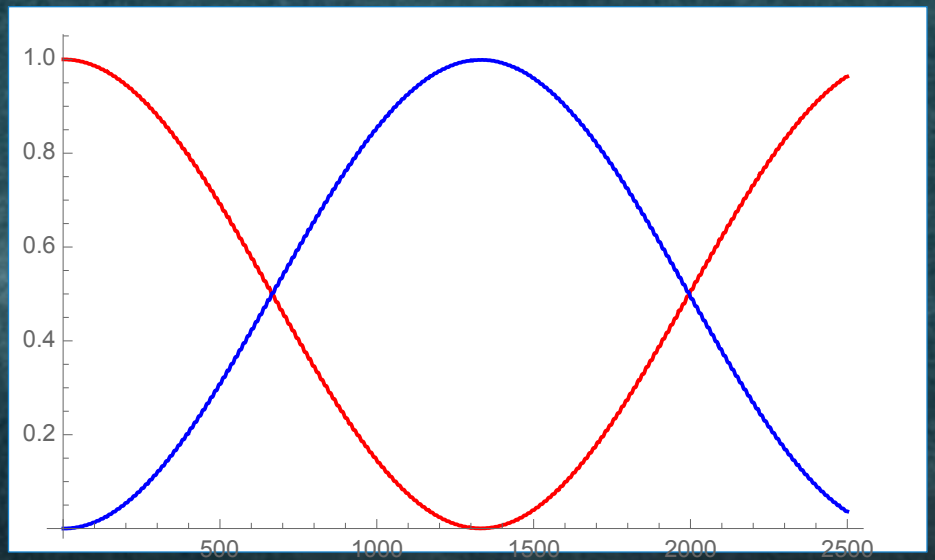
$$|\alpha; t\rangle_i = \sum_n c_n(t)\,|n\rangle$$

Parametric resonance



$$\dot{c}_k = -i \left(M(t) \right)_{km} c_m$$

$$M(t) = \begin{pmatrix} W_{11} & W_{12}\, e^{i\omega_{12}t} & \cdots \\ W_{21}\, e^{i\omega_{21}t} & W_{22} & \cdots \\ & & W_{33} \quad \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}$$



New perspectives on a series of problems…

- Lucky numbers
- Goldbach conjecture
- Factorization
- ….

Integer Factorization

(GM, Trombettoni)

Integer Factorization by Quantum Measurements

G. Mussardo[1,2] and A. Trombettoni[3,2]

[1]*SISSA, Via Bonomea 265, I-34136 Trieste, Italy.*
[2]*INFN, Sezione di Trieste, Via Valerio 2, I-34127 Trieste, Italy*
[3]*Dipartimento di Fisica, Universitá di Trieste, Strada Costiera 11, I-34151 Trieste, Italy*

Quantum algorithms are at the heart of the ongoing efforts to use quantum mechanics to solve computational problems unsolvable on ordinary classical computers[1–3]. Their common feature is the use of genuine quantum properties such as entanglement and superposition of states[4]. Among the known quantum algorithms, a special role is played by the Shor algorithm[5,6], i.e. a polynomial-time quantum algorithm for integer factorization, with far reaching potential applications in several fields, such as cryptography[7]. For an integer N of the order of 2^n, i.e. with n digits, the Shor algorithm permits its factorization in (order of) n steps. This results in an exponential gain in computational efficiency with respect to the best known classical algorithms. Here we present a different algorithm for integer factorization based on another genuine quantum property: quantum measurement[8–10]. In this new scheme, the factorization of the integer N is achieved in a number of steps equal to the number of its prime factors, referred to as k– e.g., if N is the product of two primes, two quantum measurements are enough, regardless of the number of digits n of the number N. Since k is the lower bound to the number of operations one can do to factorize a general integer, then one sees that a quantum mechanical setup can saturate such a bound. Once established this, we discuss how the algorithm can physically be ran. We argue that one needs a single-purpose device where quantum measurements of an observable with assigned spectrum can be performed. The preparation from scratch of this device requires the solution, once for all and not for each factorization operation, of $\sim 2^n$ differential equations, a task that with a quantum computer can be accomplished in n steps.

Introduction. Recent progress in the implementation of quantum devices has led to the experimental demonstration of some instances of quantum advantage. This happens when a specific computational problem may be solved faster and more efficiently on quantum processors rather than a classical computer[13]. To achieve this goal the quantum processor must have an architecture made at least of several tens of qubits and long enough decoherence times.

A notable example, from a historical and conceptual point of view, of a clear quantum advantage is provided by the Shor algorithm[5,6]. This algorithm indicates how to solve efficiently on a quantum computer the long-standing problem of finding the prime factors of an integer number N. Assuming that such a number N is of order 2^n, the Shor algorithm exploits in an ingenious way the implementation of the discrete Fourier transform on n qubits. To date, its validity has been shown with the factorization of a small numbers (the present computational bottleneck being the quantum modular exponentiation). The factorization of the number, $15 = 3 \times 5$, was done using 7 qubits with an NMR implementation of a quantum computer[14]. Similar demonstrations were performed using photonic[15,16] and solid-state qubits[17], 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 $21 = 3 \times 7$[18]. Despite their simplicity, these examples nevertheless provide a *proof of principle* realization of the algorithm.

In this paper we present a different route for integer factorization, based on an algorithm which exploits another genuine quantum property: projective quantum measurement[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 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[11,12]; and (c) the logarithm of the primes[40–45]. 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 by making a finite set of quantum measurements.

Integer Factorization

(GM, Trombettoni)

Given an integer N, find its unique prime factorization

$$N = p_1^{\alpha_1} \, p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

Integer Factorization

(GM, Trombettoni)

(Quantum) Degeneracy

$$\log N = \log p_1 + \log \hat{N}_1$$
$$= \log p_2 + \log \hat{N}_2$$
$$\vdots$$
$$= \log p_k + \log \hat{N}_k$$

k times

$$\log \hat{N}_j = \log \left(p_1^{\alpha_1} \cdots p_j^{\alpha_j - 1} \cdots p_k^{\alpha_k} \right)$$

Quantum Hamiltonians

$$H = H_1 + H_2$$

$$H_1 = \frac{1}{2}p_x^2 + V(x) \qquad E_n^{(1)} = \{\log p_k\}$$

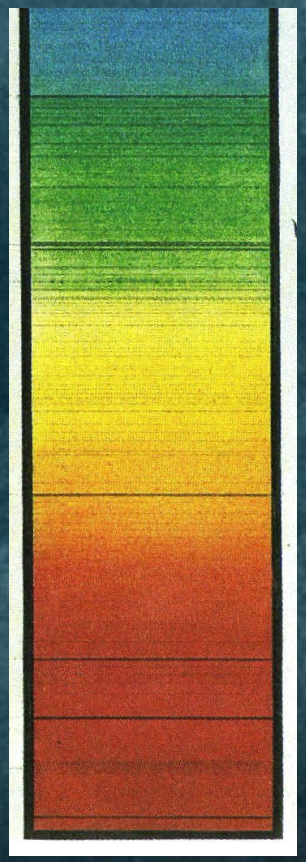
$$H_2 = \frac{1}{2}p_y^2 + W(x) \qquad E_n^{(2)} = \{\log N\}$$

$$E_n = E_n^{(1)} + E_n^{(2)}$$

Quantum Hamiltonians

$$H = H_1 + H_2$$

$$E_n = E_n^{(1)} + E_n^{(2)}$$



d(n) = # of distinct prime factors of the integer number n

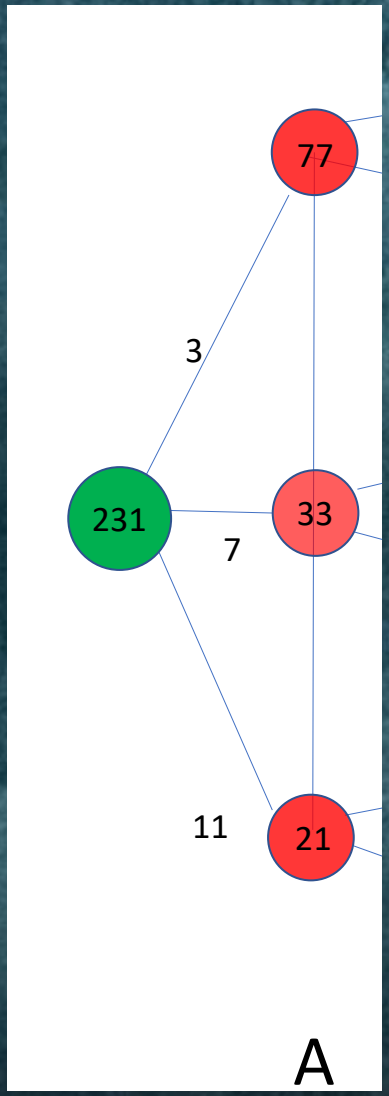
Initial state

$$|\Psi\rangle = |\log N\rangle = \sum_{n=1}^{k} c_n |\log p_n\rangle \, |\log \hat{N}_n\rangle$$

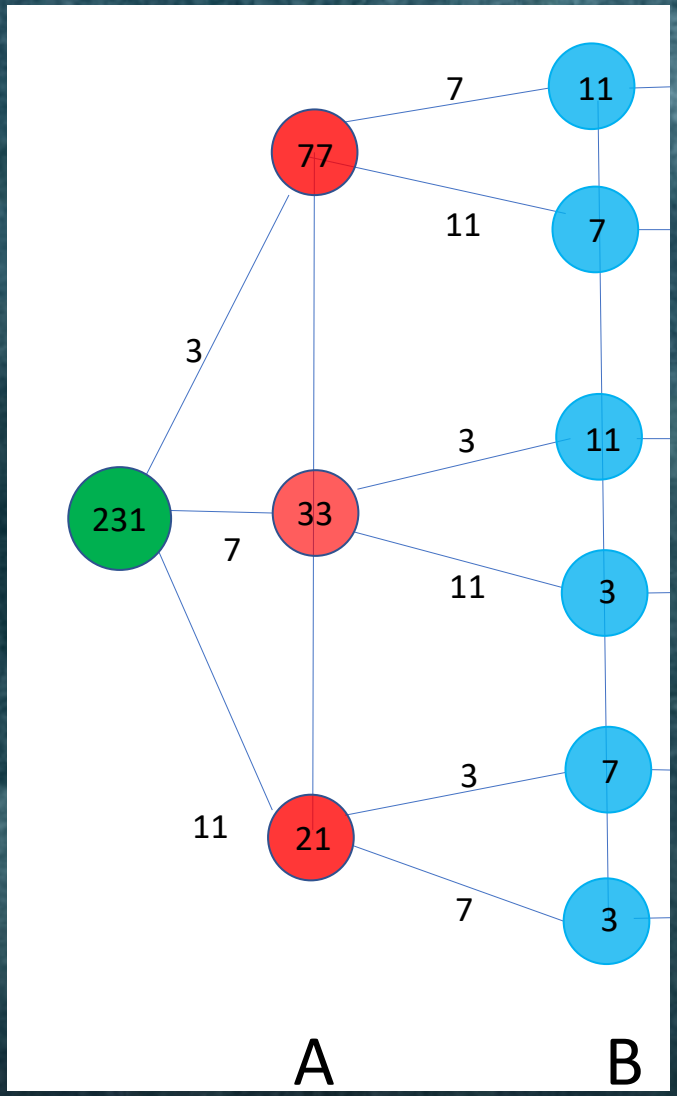
where the coefficients may also be regarded as random

It is however crucial that all of them are different from 0

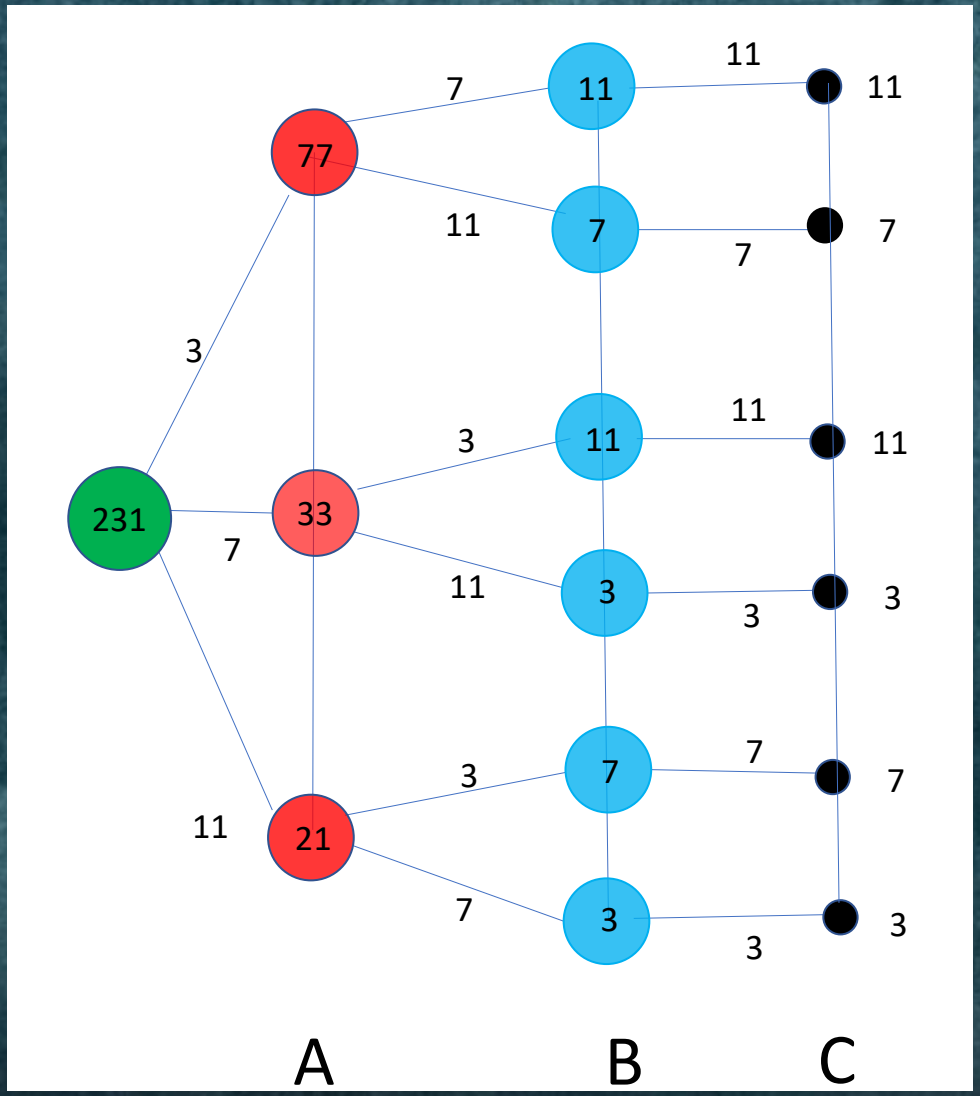
Branching tree paths



Branching tree paths



Branching tree paths



Conclusions

- Interesting interplays between Number Theory & Physics
- Proof of principle: it is possible to realize in lab quantum mechanics potentials which encode interesting arithmetic sequences
- These realizations transform genuine mathematical questions into quantum experiments
- These quantum abacuses provide an alternative way to implement quantum algorithms