Title: Quantum computing and Zeta functions

Date: Dec 13, 2006 02:00 PM

URL: http://pirsa.org/06120001

Abstract: In this talk I describe a possible connection between quantum computing and Zeta functions of finite field equations that is inspired by the \'spectral approach\' to the Riemann conjecture. This time the assumption is that the zeros of such Zeta functions correspond to the eigenvalues of finite dimensional unitary operators of quantum mechanical systems. To model the desired quantum systems I use the notion of universal, efficient quantum computation. Using eigenvalue estimation, such quantum systems should be able to approximately count the number of solutions of the specific finite field equations with an accuracy that does not appear to be feasible classically. For certain equations (Fermat hypersurfaces) one can indeed model their Zeta functions with efficient quantum algorithms, which gives some evidence in favor of the proposal. In the case of equations that define elliptic curves, the corresponding unitary transformation is an SU(2) matrix. Hence for random elliptic curves one expects to see the kind of statistics predicted by random matrix theory. In the last part of the talk I discuss to which degree this expectation does indeed hold. Reference: arXiv:quant-ph/0405081

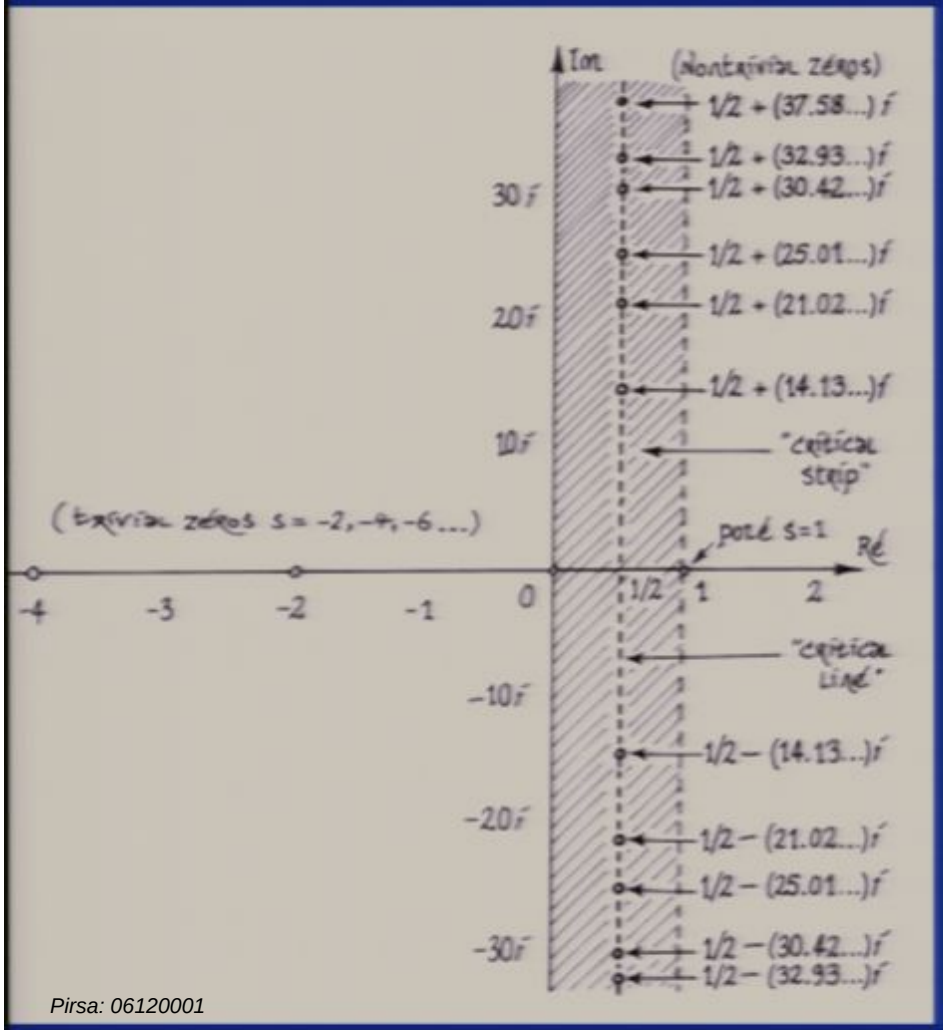
Quantum computing & Zeta functions

Wim van Dam
UC Santa Barbara

Perimeter Institute for Theoretical Physics
December 13, 2006

arXiv:quant-ph/0405081

Zeros of the Riemann ζ Function



Riemann's zeta function ζ(s) is the analytical continuation of the sum $1+1/2^s+1/3^s+1/4^s+\ldots$

"Analytical continuation": Think $1+z+z^2+z^3+\ldots = 1/(1-z)$ for all $z \in \mathbb{C}$.

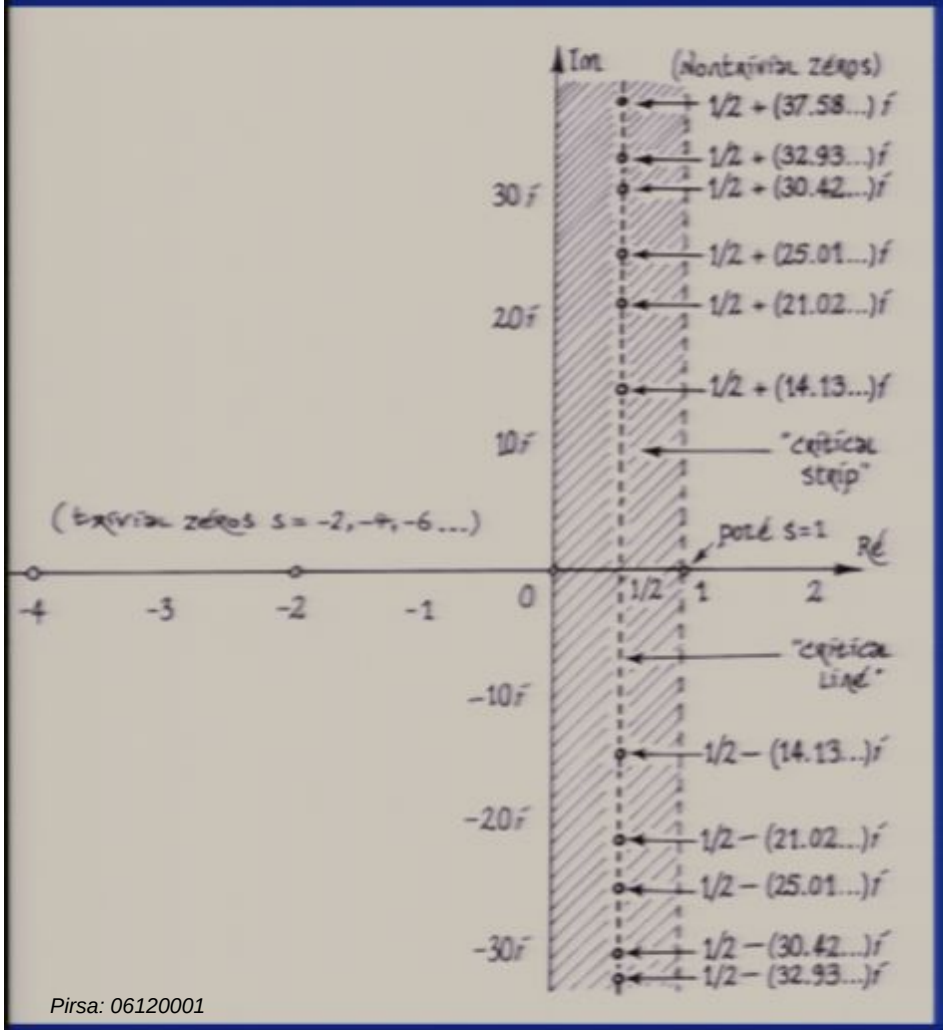
Riemann Hypothesis: All nontrivial zeros ζ(s)=0 lie on the line Re(s) = ½.

The Euler product

$$\zeta(s) = \sum_{n=1,2,3,\ldots} \frac{1}{n^s} = \prod_{p=2,3,5,7,\ldots} \frac{1}{1-p^{-s}}$$

shows the connection with primes.

Zeros of the Riemann ζ Function



Riemann's zeta function ζ(s) is the analytical continuation of the sum $1+1/2^s+1/3^s+1/4^s+\ldots$

"Analytical continuation": Think $1+z+z^2+z^3+\ldots = 1/(1-z)$ for all $z \in \mathbb{C}$.

Riemann Hypothesis: All nontrivial zeros ζ(s)=0 lie on the line Re(s) = ½.

The Euler product

$$\zeta(s) = \sum_{n=1,2,3,\ldots} \frac{1}{n^s} = \prod_{p=2,3,5,7,\ldots} \frac{1}{1-p^{-s}}$$

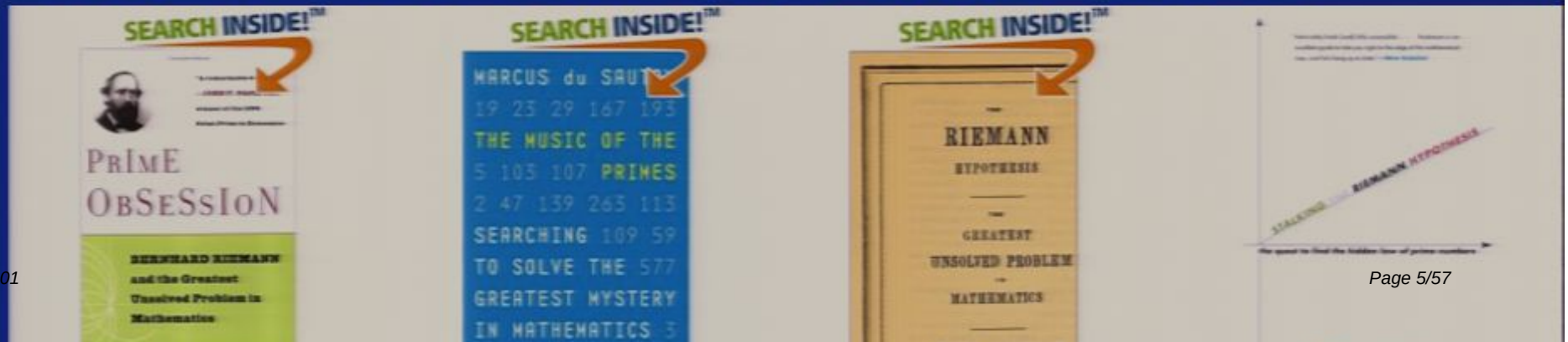
shows the connection with primes.

Trying to Prove the RH

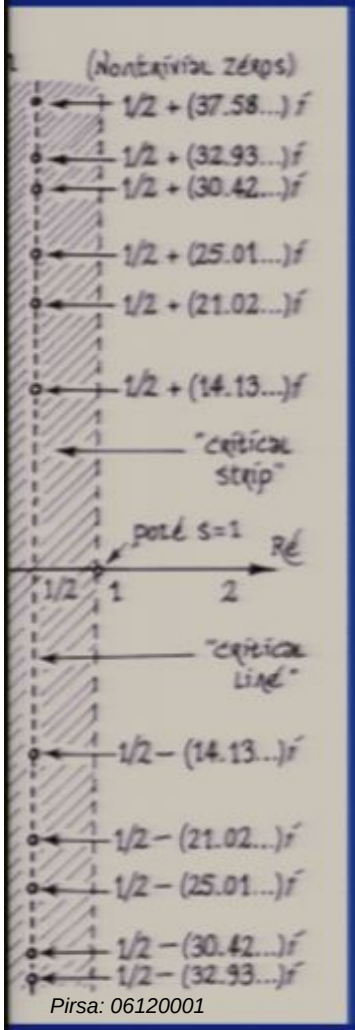
The RH is one of the 7 Millennium Problems of the Clay Mathematics Institute (1,000,000$ for a proof, 0$ for a disproof):

> *"… This has been checked for the first 1,500,000,000 solutions. A proof that it is true for every interesting solution would shed light on many of the mysteries surrounding the distribution of prime numbers."*

Four recent popular books describe the quest for a proof and the recent excitement about a "spectral approach" to the RH.

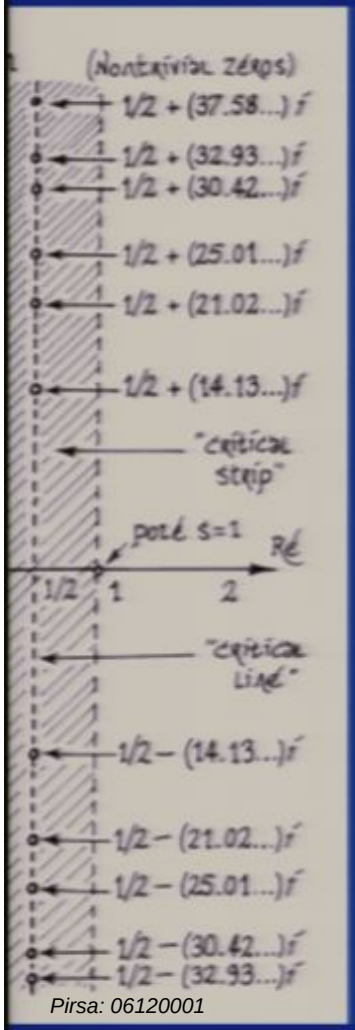


Zeta Zeros as Eigenvalues?



Let the n-th $\zeta(s)=0$ zero be $\frac{1}{2} + \gamma_n \cdot i$ and look at the normalized spacings between the γ_j defined by $\delta_n = (\gamma_{n+1} - \gamma_n) \cdot \log(\gamma_n/2\pi)/2\pi$.

Zeta Zeros as Eigenvalues?



Let the n-th $\zeta(s)=0$ zero be $\frac{1}{2} + \gamma_n \cdot i$ and look at the normalized spacings between the γ_j defined by $\delta_n = (\gamma_{n+1} - \gamma_n) \cdot \log(\gamma_n/2\pi)/2\pi$.

The Montgomery-Dyson law states that this δ-spacing has the same kind of eigenvalue repulsion that we see in GUE random Hermitian matrices (verified in great detail by Odlyzko).

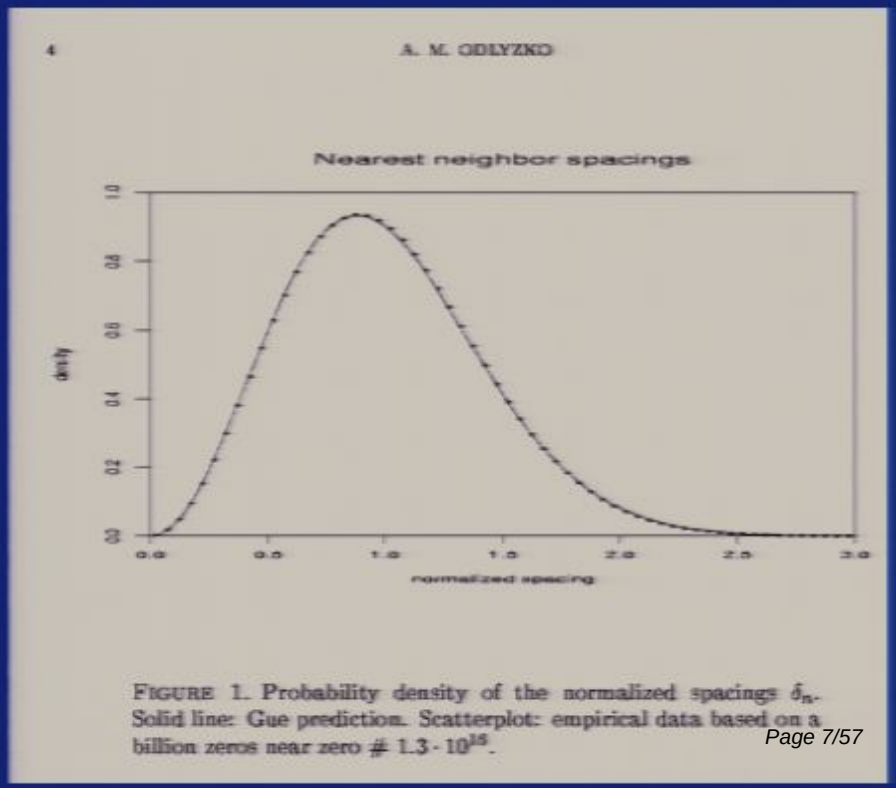
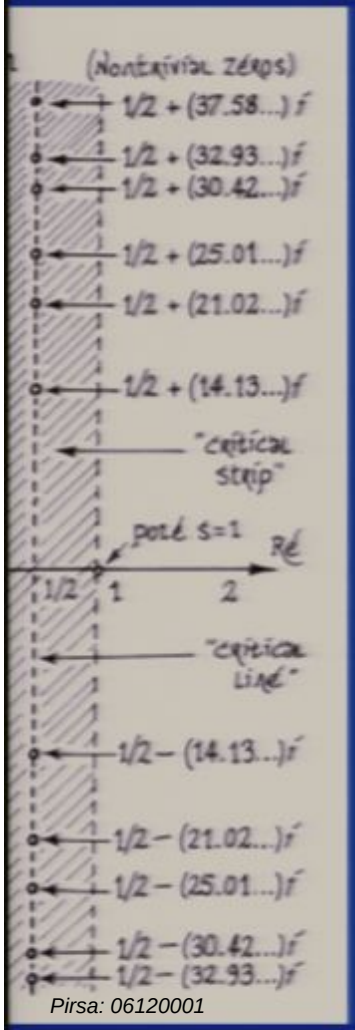


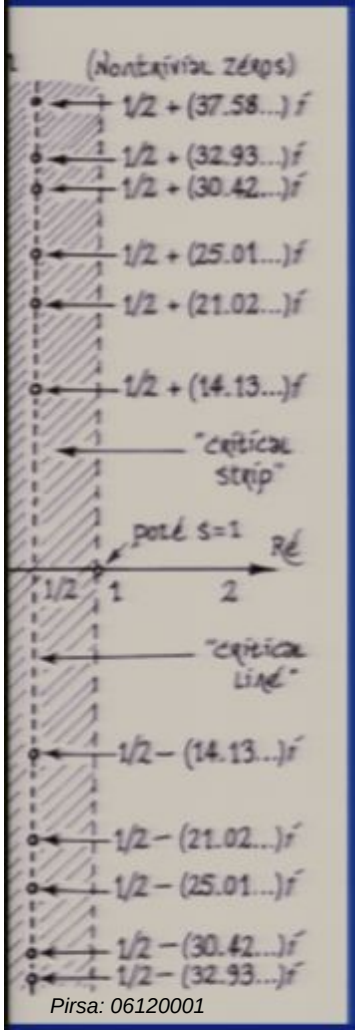
FIGURE 1. Probability density of the normalized spacings δ_n. Solid line: Gue prediction. Scatterplot: empirical data based on a billion zeros near zero # $1.3 \cdot 10^{15}$.

Zeta Zeros as Eigenvalues?



Let the n-th $\zeta(s)=0$ zero be $\frac{1}{2} + \gamma_n \cdot i$ and look at the normalized spacings between the γ_j defined by $\delta_n = (\gamma_{n+1} - \gamma_n) \cdot \log(\gamma_n/2\pi)/2\pi$.

Zeta Zeros as Eigenvalues?



Let the n-th $\zeta(s)=0$ zero be $\frac{1}{2} + \gamma_n \cdot i$ and look at the normalized spacings between the γ_j defined by $\delta_n = (\gamma_{n+1} - \gamma_n) \cdot \log(\gamma_n/2\pi)/2\pi$.

The Montgomery-Dyson law states that this δ-spacing has the same kind of eigenvalue repulsion that we see in GUE random Hermitian matrices (verified in great detail by Odlyzko).

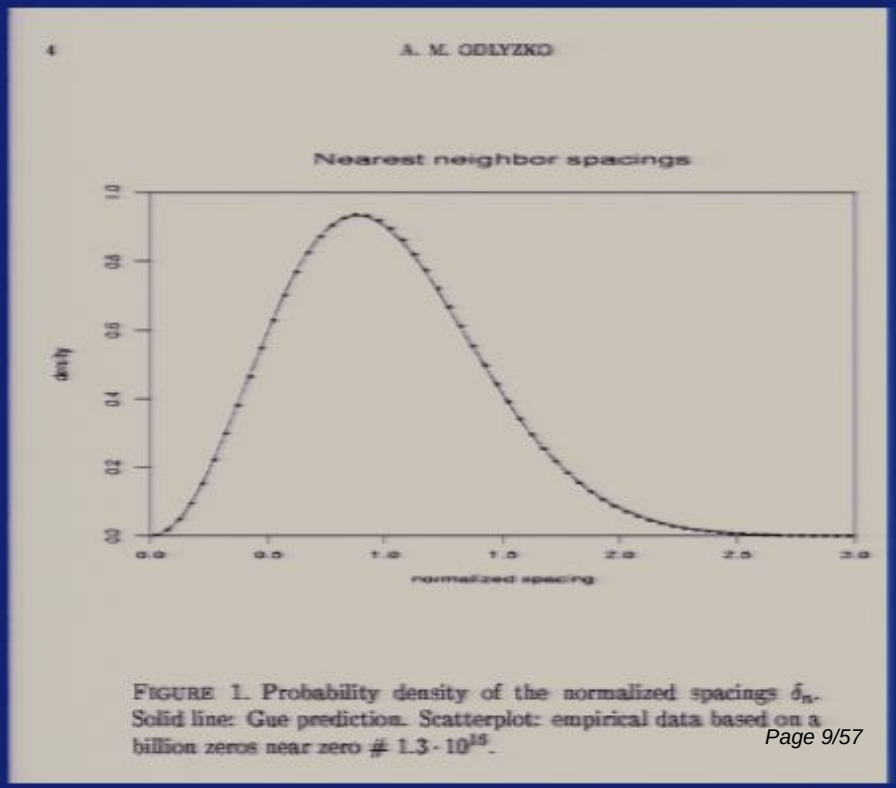


FIGURE 1. Probability density of the normalized spacings δ_n. Solid line: Gue prediction. Scatterplot: empirical data based on a billion zeros near zero # $1.3 \cdot 10^{15}$.

Spectral Approach to RH

The Hilbert-Pólya approach to the Riemann Hypothesis tries to view the γ_n values as the spectrum of (hopefully meaningful) Hermitian operator.

The random matrix statistics of the zeros suggests that it would have to correspond to a (pseudo)-random operator. Such operators occur naturally in the theory of chaotic quantum mechanical systems.

The hope is that we can use our physical intuition to make an educated/lucky guess of such an operator, thereby settling the Riemann Hypothesis.

More Than Just One ζ

The Riemann ζ-function deals with the ring of integers $\mathbb{Z}$*, its ideals* $n\mathbb{Z}$*, and prime ideals* $p\mathbb{Z}$*.*

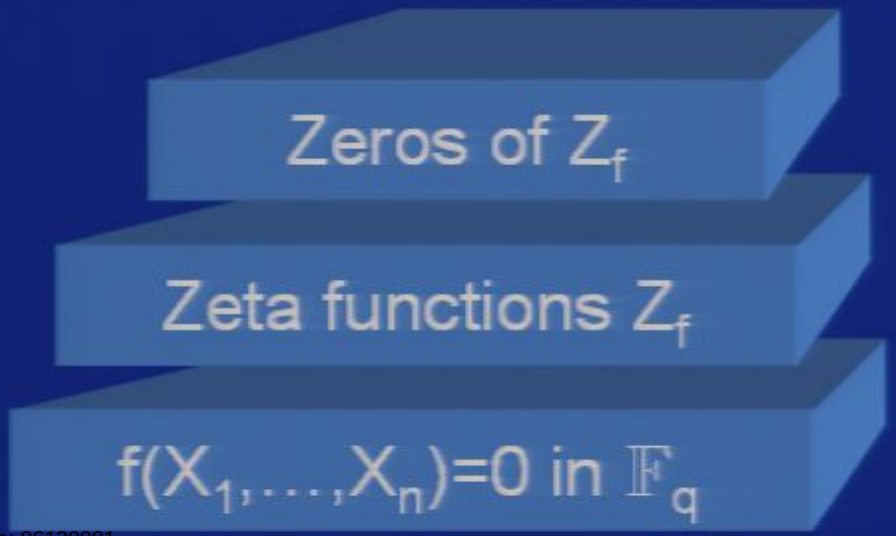
This idea can be generalized to other algebraic integer rings such as $\mathbb{Z}[\omega]$ and $\mathbb{Z}[\sqrt{-1}]$.

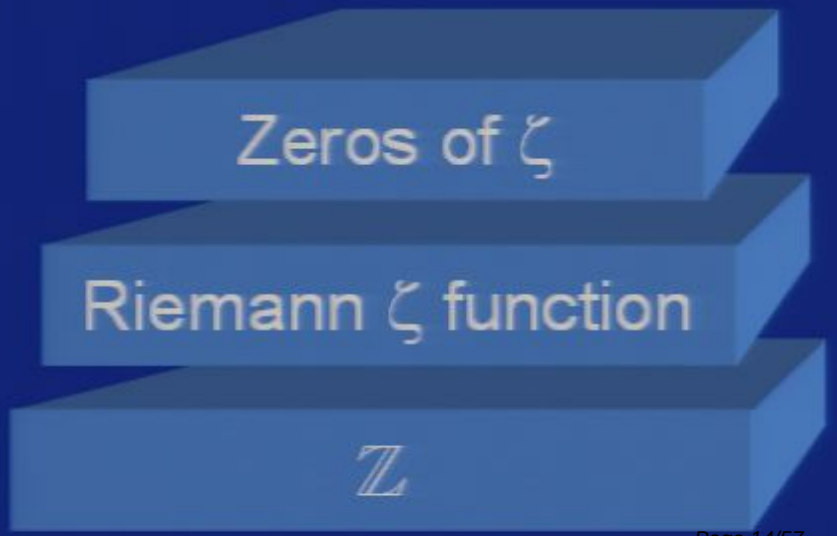
We can also look at the Zeta functions of rings $\mathbb{F}_p[X_1,\ldots,X_n]/(f_1,\ldots,f_r)$ *with* $f_j \in \mathbb{F}_p[X_1,\ldots,X_n]$ *some polynomial equations, thus defining an algebraic variety* $f_1(X) = \ldots = f_r(X) = 0$ *with* $X \in \mathbb{F}^n$.

Some Inspired Guessing

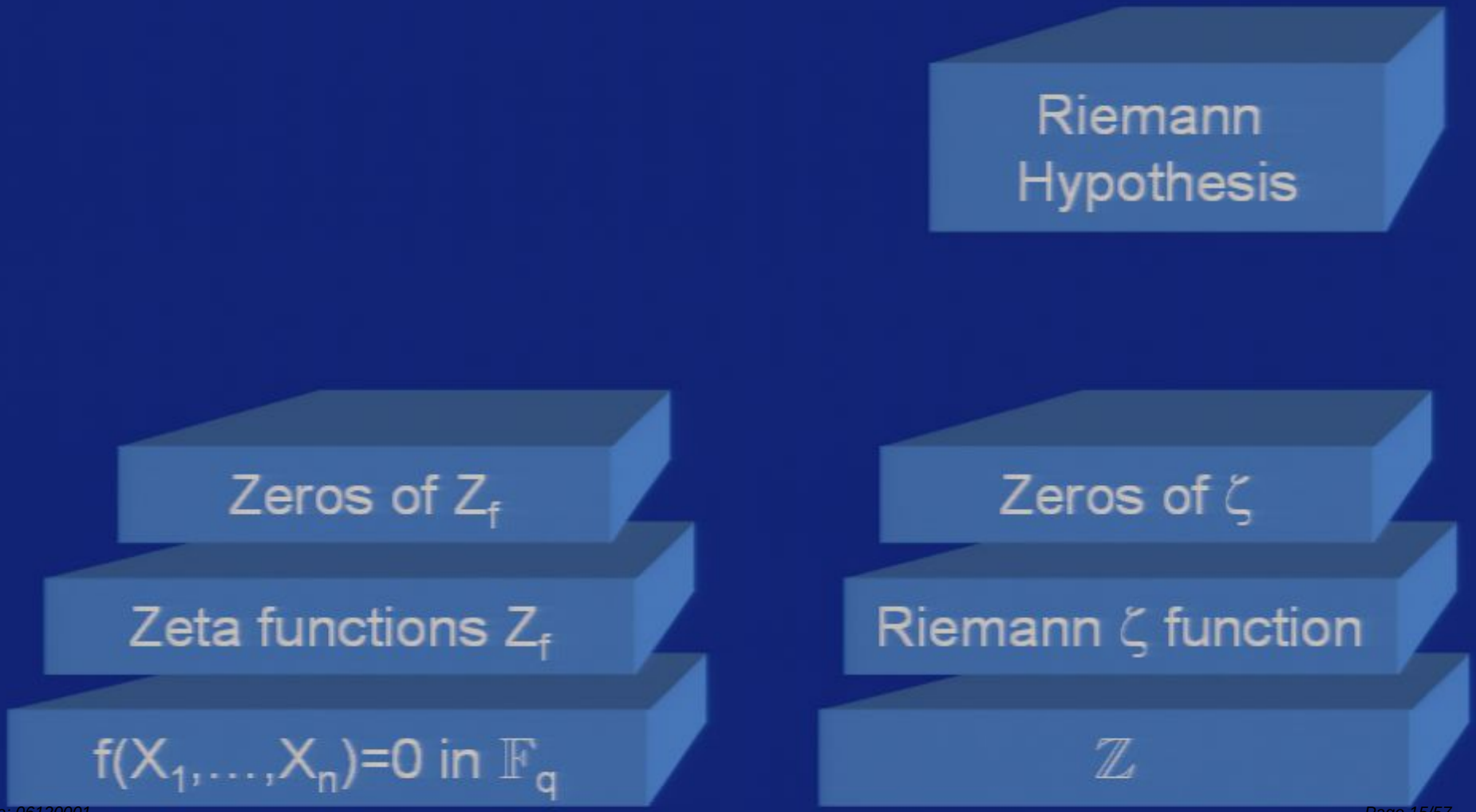
Some Inspired Guessing

Some Inspired Guessing

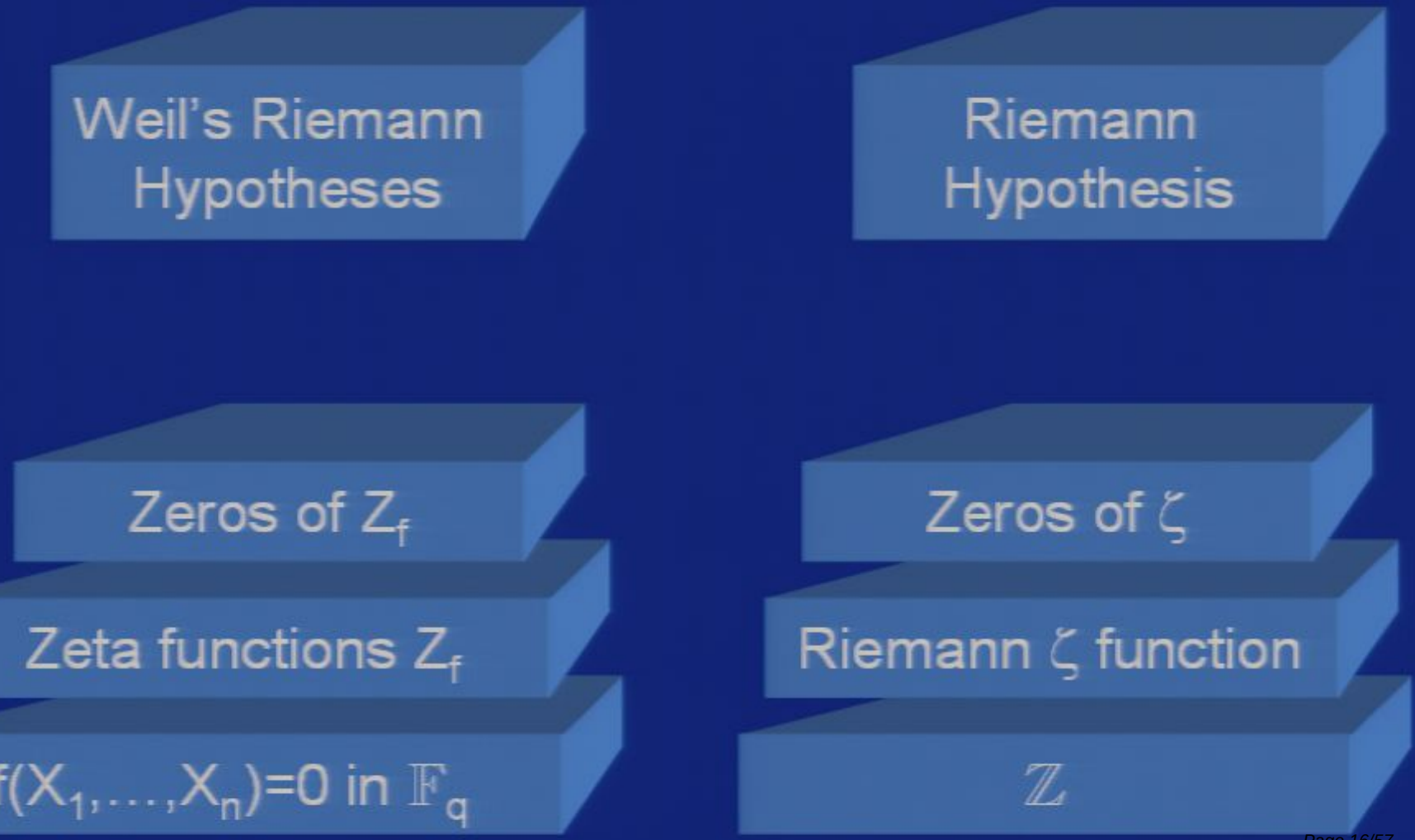




Some Inspired Guessing



Some Inspired Guessing



Some Inspired Guessing

Weil's Riemann Hypotheses

Proven in [Deligne'74]

Zeros of Z_f

Zeta functions Z_f

$f(X_1,\ldots,X_n)=0$ in $\mathbb{F}_q$

Riemann Hypothesis

Zeros of ζ

Riemann ζ function

$\mathbb{Z}$

Some Inspired Guessing

Weil's Riemann Hypotheses

Proven in [Deligne'74]

Zeros of Z_f

Zeta functions Z_f

$f(X_1,\ldots,X_n)=0$ in $\mathbb{F}_q$

Riemann Hypothesis

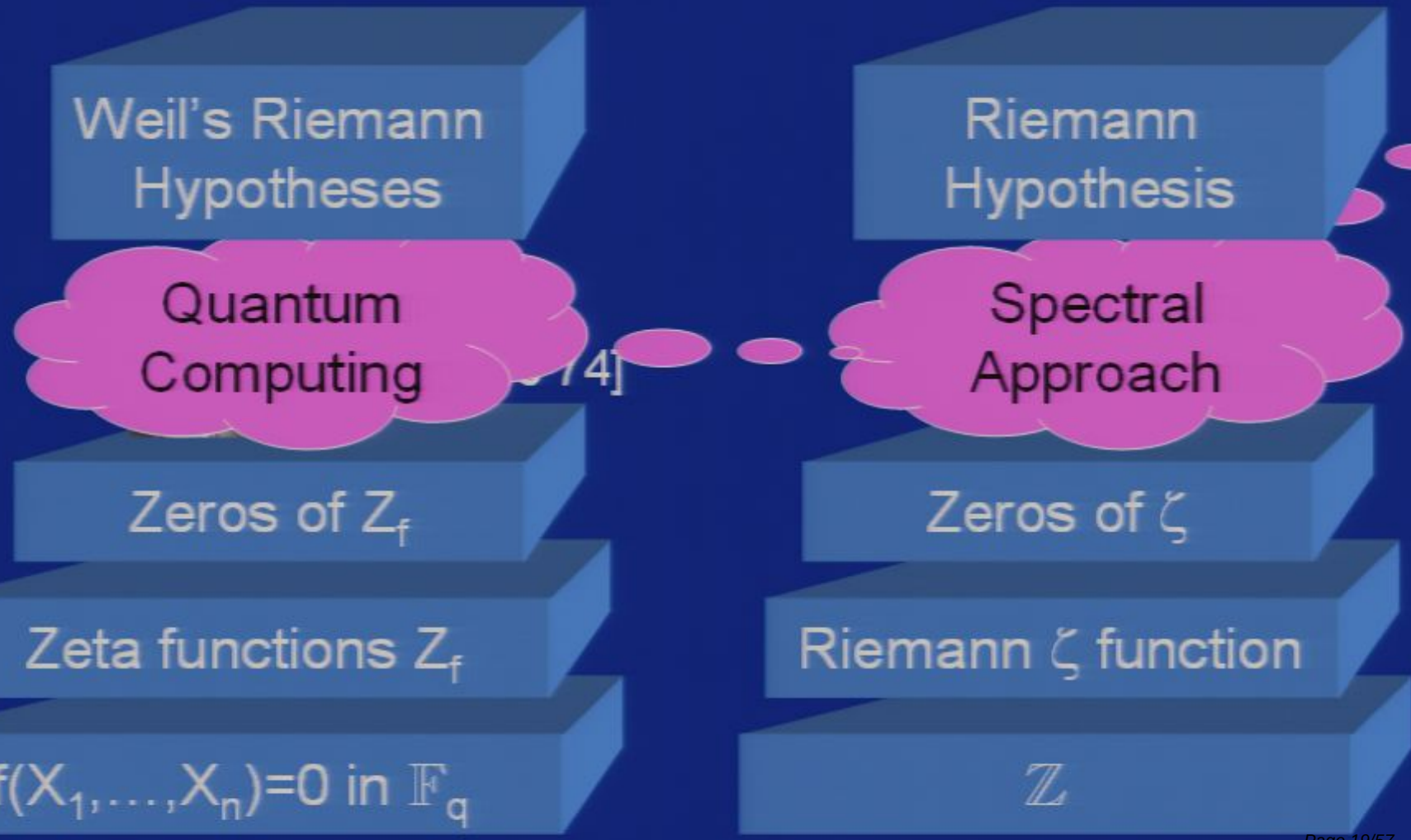
Spectral Approach

Zeros of ζ

Riemann ζ function

$\mathbb{Z}$

Some Inspired Guessing



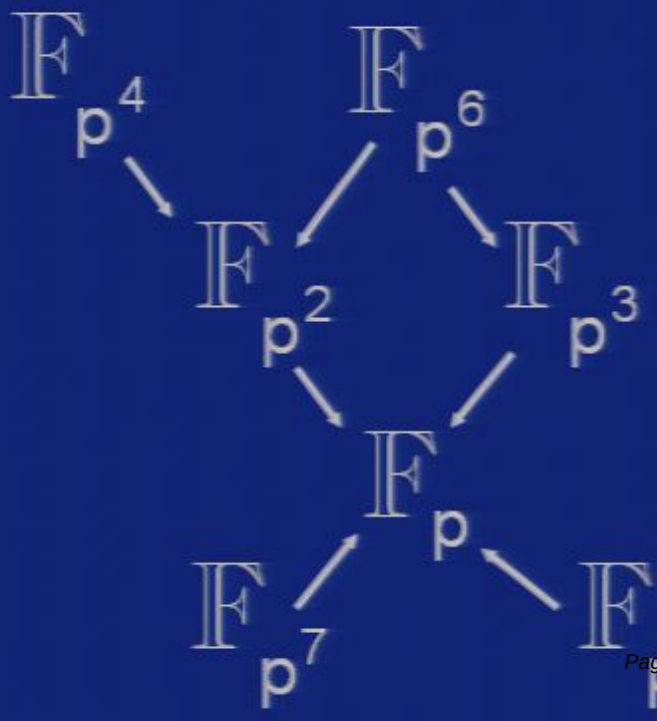
Zeta Functions and Quantum Computation

We want to establish a spectral interpretation of Zeta functions for finite field equations, using ideas from quantum computing.

The ultimate goal is find finite dimensional, efficient unitary transformations whose eigenvalues are the roots of such Z functions.

Curves over Finite Fields

We will be working over finite fields $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ and their extensions like $\mathbb{F}_2$, $\mathbb{F}_4$, $\mathbb{F}_8$, $\mathbb{F}_{16}$,... up to the *algebraic closure* of $\mathbb{F}_p$, which is denoted by $\overline{\mathbb{F}}_p$.

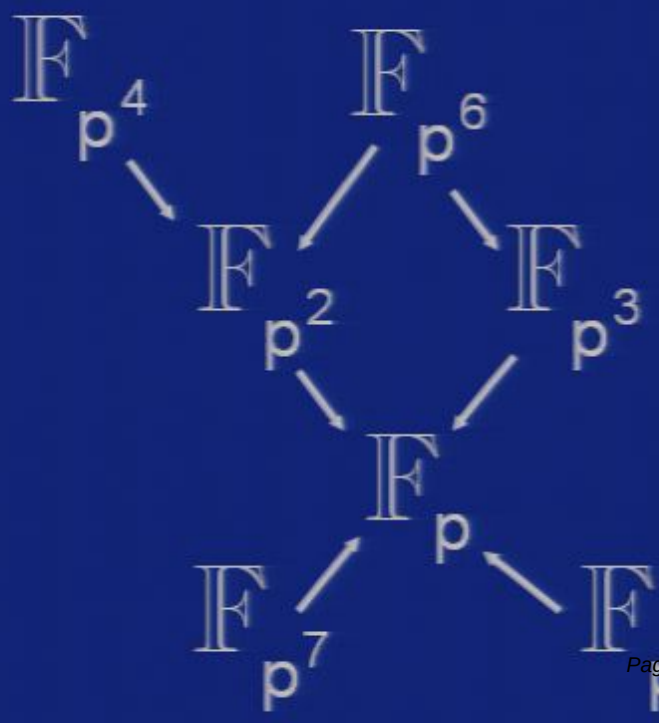


Curves over Finite Fields

We will be working over finite fields $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ and their extensions like $\mathbb{F}_2$, $\mathbb{F}_4$, $\mathbb{F}_8$, $\mathbb{F}_{16}$,... up to the *algebraic closure* of $\mathbb{F}_p$, which is denoted by $\overline{\mathbb{F}}_p$.

We want to count the solutions in the projective space $\mathbb{P}^n(\mathbb{F}_p)$ to a polynomial equation $0 = f \in \mathbb{F}_p[X_1,\ldots,X_n]$.

Special interest in curves $f \in \mathbb{F}_p[X,Y]$ in $\mathbb{P}^2(\mathbb{F}_p)$. When smooth et c., such curves have a genus g.



Zeta Function

Let $f \in \mathbb{F}_p[X_1,\ldots,X_n]$ be the polynomial and define the # of solutions to f=0 in degree-s extension of $\mathbb{F}_p$:

$$N_s = |\{x \in \mathbb{P}^n(\mathbb{F}_{p^s}) : f(x) = 0\}|$$

Zeta Function

Let $f \in \mathbb{F}_p[X_1,\ldots,X_n]$ be the polynomial and define the # of solutions to f=0 in degree-s extension of $\mathbb{F}_p$:

$$N_s = |\{x \in \mathbb{P}^n(\mathbb{F}_{p^s}) : f(x) = 0\}|$$

With $N_1, N_2, \ldots$ we define the Zeta function of f:

$$Z_f(T) = \exp\left(\sum_{s=1}^{\infty} \frac{N_s}{s} T^s\right)$$

which is a formal power series in T.

Of Note

Why this is a Zeta function is not trivial.

Things are easiest for curves $f(X,Y)=0$.

The theory works better if we work in the closed, projective space $\mathbb{P}^n$, *such that we also include the "points at infinity".*

Zeta Function

Let $f \in \mathbb{F}_p[X_1,\ldots,X_n]$ be the polynomial and define the # of solutions to f=0 in degree-s extension of $\mathbb{F}_p$:

$$N_s = |\{x \in \mathbb{P}^n(\mathbb{F}_{p^s}) : f(x) = 0\}|$$

With $N_1, N_2, \ldots$ we define the Zeta function of f:

$$Z_f(T) = \exp\left(\sum_{s=1}^{\infty} \frac{N_s}{s} T^s\right)$$

which is a formal power series in T.

Of Note

Why this is a Zeta function is not trivial.

Things are easiest for curves $f(X,Y)=0$.

The theory works better if we work in the closed, projective space $\mathbb{P}^n$, *such that we also include the "points at infinity".*

Zeta Function of Straight Line

For the line L defined by X+Y=0 in $\mathbb{P}^2(\mathbb{F}_p)$, we have $N_s=p^s+1$ for all s.

Zeta Function of Straight Line

For the line L defined by X+Y=0 in $\mathbb{P}^2(\mathbb{F}_p)$, we have $N_s=p^s+1$ for all s.

The Zeta function is thus:

$$Z_L(T) = \exp\left(\sum_{s=1}^{\infty}\frac{(1+p^s)}{s}T^s\right)$$

$$= \exp\left(\sum_{s=1}^{\infty}\frac{T^s}{s}\right)\exp\left(\sum_{s=1}^{\infty}\frac{(pT)^s}{s}\right)$$

$$= \frac{1}{(1-T)(1-pT)}$$

Trivial poles at T=1 and T=1/p and no zeros.

Z(T) of a Quartic Curve

Let $X^4+Y^4+1=0$ define a curve C in $\mathbb{P}^2$ over $\mathbb{F}_5$.
The Zeta function of this C turns out to be

$$Z_C(T) = \frac{(1-2T+5T^2)^3}{(1-T)(1-5T)}$$

Z(T) of a Quartic Curve

Let $X^4+Y^4+1=0$ define a curve C in $\mathbb{P}^2$ over $\mathbb{F}_5$.
The Zeta function of this C turns out to be

$$Z_C(T) = \frac{(1-2T+5T^2)^3}{(1-T)(1-5T)}$$

Again, trivial poles at T=1 and T=1/p=1/5.

Nontrivial roots at T=1/(1+2i) and T=1/(1–2i), both with norm $|T|=1/\sqrt{p}=1/\sqrt{5}$.

Number of solutions : $N_s = \underbrace{5}_{p}^{s} + 1^s - 3\underbrace{(1+2\sqrt{-1})}_{|\bullet|=\sqrt{p}}^{s} - 3\underbrace{(1-2\sqrt{-1})}_{|\bullet|=\sqrt{p}}^{s}.$

Two Qubic Curves over $\mathbb{F}_5$

$Y^2 + X^3 + 2X + 1 = 0$ has $N_1 = 7$ and $N_2 = 35,\ldots$

$$N_s = 5^s + 1^s - \underbrace{\left(-\tfrac{1}{2} + \tfrac{1}{2}\sqrt{-19}\right)^s}_{|\bullet| = \sqrt{p}} - \underbrace{\left(-\tfrac{1}{2} - \tfrac{1}{2}\sqrt{-19}\right)^s}_{|\bullet| = \sqrt{p}}$$

Two Qubic Curves over $\mathbb{F}_5$

$Y^2 + X^3 + 2X + 1 = 0$ has $N_1 = 7$ and $N_2 = 35,\ldots$

$$N_s = \underbrace{5^s + 1^s}_{\{p\}} - \underbrace{\left(-\tfrac{1}{2} + \tfrac{1}{2}\sqrt{-19}\right)^s}_{|\bullet| = \sqrt{p}} - \underbrace{\left(-\tfrac{1}{2} - \tfrac{1}{2}\sqrt{-19}\right)^s}_{|\bullet| = \sqrt{p}}$$

$Y^2 + X^3 + 2X + 2 = 0$ has $N_1 = 7$ and $N_2 = 25,\ldots$

$$N_s = \underbrace{5^s + 1^s}_{\{p\}} - \underbrace{(-1)^s}_{|\bullet| \neq \sqrt{p}}$$

The difference is explained by the fact that the first curve is smooth, while the second one is singular.

For *smooth* curves, N_s obeys Weil's Riemann hypothesis…

Weil's RH for Curves

Let f define a complete, nonsingular curve over $\mathbb{F}_p$, the Zeta function Z(T) of this C equals

$$Z_C(T) = \frac{P(T)}{(1-T)(1-pT)}$$

with $P(T) = (1-\alpha_1 T)(1-\alpha_2 T)\ldots(1-\alpha_{2g} T)$

Weil's Riemann Hypothesis says: $|\alpha_j| = \sqrt{p}$.

Furthermore, $\alpha_j^* = \alpha_{j+g}$ and g is the genus of C.

As a direct consequence:

Weil's RH for Curves

Let f define a complete, nonsingular curve over $\mathbb{F}_p$, the Zeta function Z(T) of this C equals

$$Z_C(T) = \frac{P(T)}{(1-T)(1-pT)}$$

with $P(T) = (1-\alpha_1 T)(1-\alpha_2 T)\ldots(1-\alpha_{2g} T)$

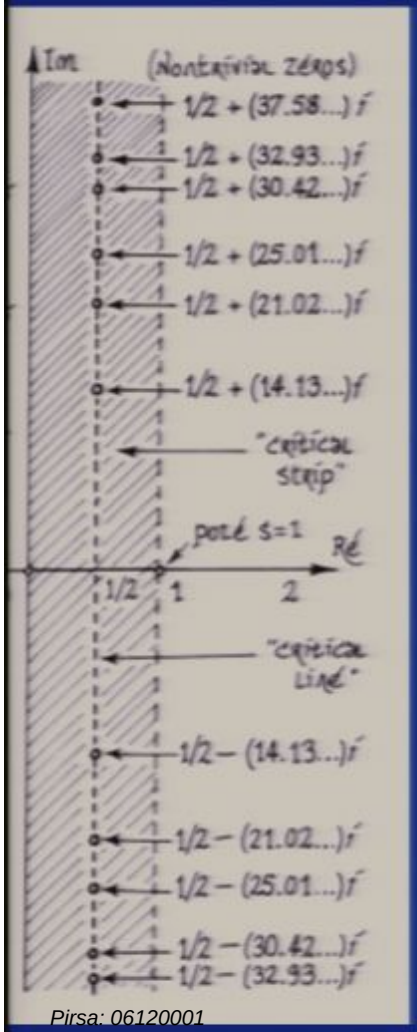
Weil's Riemann Hypothesis says: $|\alpha_j| = \sqrt{p}$.

Furthermore, $\alpha_j^* = \alpha_{j+g}$ and g is the genus of C.

As a direct consequence:

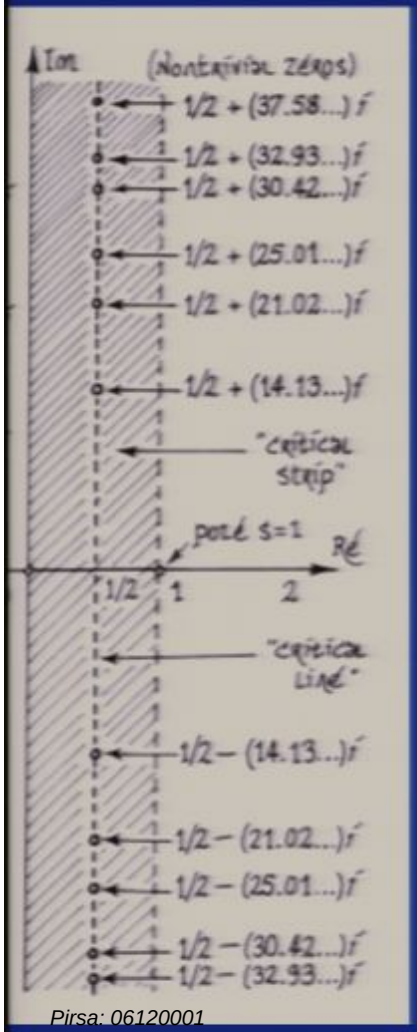
$$\#\text{ solutions} : N_s = p^s + 1 - \left(\underbrace{\alpha_1}_{|\bullet|=\sqrt{p}}{}^s + \underbrace{\alpha_2}_{|\bullet|=\sqrt{p}}{}^s + \cdots + \underbrace{\alpha_{2g}}_{|\bullet|=\sqrt{p}}{}^s \right).$$

Spectral Interpretation of Weil's Riemann Hypotheses



The roots of Riemann's zeta function ζ_R suggests an infinite dimensional Hamiltonian.

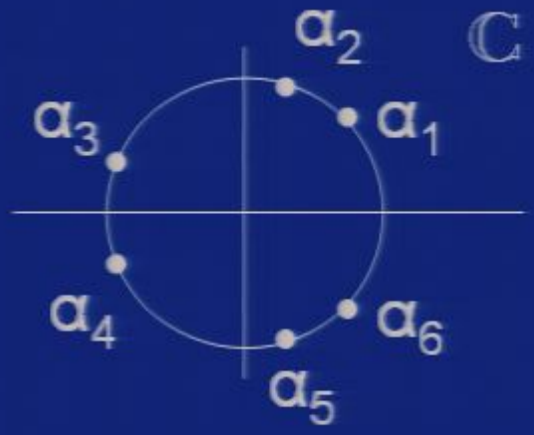
Spectral Interpretation of Weil's Riemann Hypotheses



The roots of Riemann's zeta function ζ_R suggests an infinite dimensional Hamiltonian.

The roots of the Zeta function Z_f suggest a finite dimensional *unitary* matrix.

For each equation f=0 we have 2g roots $\alpha_j = \sqrt{p} \cdot \exp(i\,\theta_j)$, giving a spectrum $\exp(i\,\theta_1), \ldots, \exp(i\,\theta_{2g})$.



Arguments in Favor of a Spectral Interpretation

Just as the $\zeta_{Riemann}$ zeros obey the kind of statistics of random Hermitian matrices, the zeros of these finite field equation Zeta functions (seem to) obey the statistics of random unitary matrices.

Arguments in Favor of a Spectral Interpretation

Just as the $\zeta_{Riemann}$ zeros obey the kind of statistics of random Hermitian matrices, the zeros of these finite field equation Zeta functions (seem to) obey the statistics of random unitary matrices.

[Sato-Tate] For a fixed elliptic curve the Zeta zeros over different $\mathbb{F}_p$ obey random SU(2) statistics.(?)

Arguments in Favor of a Spectral Interpretation

Just as the $\zeta_{Riemann}$ zeros obey the kind of statistics of random Hermitian matrices, the zeros of these finite field equation Zeta functions (seem to) obey the statistics of random unitary matrices.

[Sato-Tate] For a fixed elliptic curve the Zeta zeros over different $\mathbb{F}_p$ obey random SU(2) statistics.(?)

[Katz & Sarnak] For curves in the limit $g,p \to \infty$, the eigenvalues θ_j are distributed as if they are sampled from the random unitary matrices in USp(2g).

Zeta Functions and Quantum Computation

To distinguish between "arbitrary" unitary matrices and "quantum mechanical" unitary matrices, we use the quantum Turing thesis.

Conjecture: The spectra of Zeta functions of finite field equations can be reproduced by efficient (="natural") quantum circuits.

Arguments in Favor of a Spectral Interpretation

Just as the $\zeta_{Riemann}$ zeros obey the kind of statistics of random Hermitian matrices, the zeros of these finite field equation Zeta functions (seem to) obey the statistics of random unitary matrices.

[Sato-Tate] For a fixed elliptic curve the Zeta zeros over different $\mathbb{F}_p$ obey random SU(2) statistics.(?)

[Katz & Sarnak] For curves in the limit $g,p \to \infty$, the eigenvalues θ_j are distributed as if they are sampled from the random unitary matrices in USp(2g).

Zeta Functions and Quantum Computation

To distinguish between "arbitrary" unitary matrices and "quantum mechanical" unitary matrices, we use the quantum Turing thesis.

Conjecture: The spectra of Zeta functions of finite field equations can be reproduced by efficient (="natural") quantum circuits.

The Quantum Goal

Given a $\mathbb{F}_p$ function f where Z_f has 2g nontrivial roots construct a quantum circuit U_f with $\alpha_1/\sqrt{p},\ldots,\alpha_{2g}/\sqrt{p}$ as its eigenvalues and where the circuit has complexity polynomial in log p and log g:

such that the spectrum of U_f equals that of Z_f

The Quantum Goal

Given a $\mathbb{F}_p$ function f where Z_f has 2g nontrivial roots construct a quantum circuit U_f with $\alpha_1/\sqrt{p},\ldots,\alpha_{2g}/\sqrt{p}$ as its eigenvalues and where the circuit has complexity polynomial in log p and log g:

such that the spectrum of U_f equals that of Z_f

Note that we want the circuit to act on log 2g qubits. Compare this with the result described by [Kedlaya] where Z_f is calculated *exactly* using poly(g) qubits.

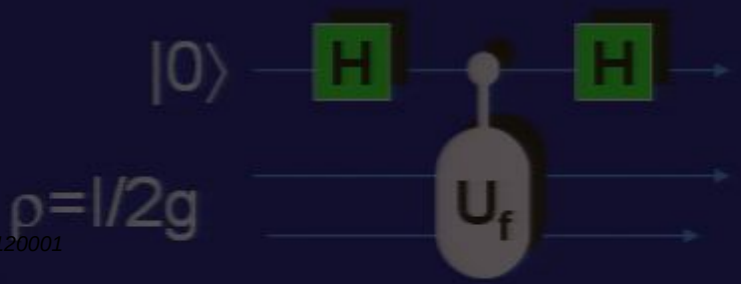
Quantum Zeta Algorithms

If we can design such circuits U_f, what good is it?

- It strengthens the connection between number theory and quantum mechanics (not just between number theory and random matrix theory).

- Using phase estimation we can discover information about the roots of $Z_f(T)$.

Especially the trace of U_f is easy to estimate:



This will allow us to approximately count the solutions X to f(X)=0.

Partial Quantum Results

$$0 = c_0 X_0^m + \ldots + c_n X_n^m$$

Done.

$$Y^2 = X^3 + D \text{ and } Y^2 = X^3 - Dx$$

Done.

Partial Quantum Results

$0 = c_0 X_0^m + \ldots + c_n X_n^m$ ✓ Done.

$Y^2 = X^3 + D$ and $Y^2 = X^3 - Dx$ ✓ Done.

- For these curves and hypersurfaces the Zeta zeroes are products of multiplicative characters χ and Gauß sums $g(\chi) = \Sigma_z e^{z \cdot 2\pi i/p} \chi(z)$.
- We know how to induce the $\chi(c)$ and $g(\chi)$ phases with efficient quantum algorithms (using discrete logarithms and quantum Fourier transforms).

Quantum Zeta Algorithms

If we can design such circuits U_f, what good is it?

- It strengthens the connection between number theory and quantum mechanics (not just between number theory and random matrix theory).

The Quantum Goal

Arguments in Favor of a Spectral Interpretation

Just as the $\zeta_{Riemann}$ zeros obey the kind of statistics of random Hermitian matrices, the zeros of these finite field equation Zeta functions (seem to) obey the statistics of random unitary matrices.

[Sato-Tate] For a fixed elliptic curve the Zeta zeros over different $\mathbb{F}_p$ obey random SU(2) statistics.(?)

[Katz & Sarnak] For curves in the limit $g,p \to \infty$, the eigenvalues θ_j are distributed as if they are sampled from the random unitary matrices in USp(2g).

Arguments in Favor of a Spectral Interpretation

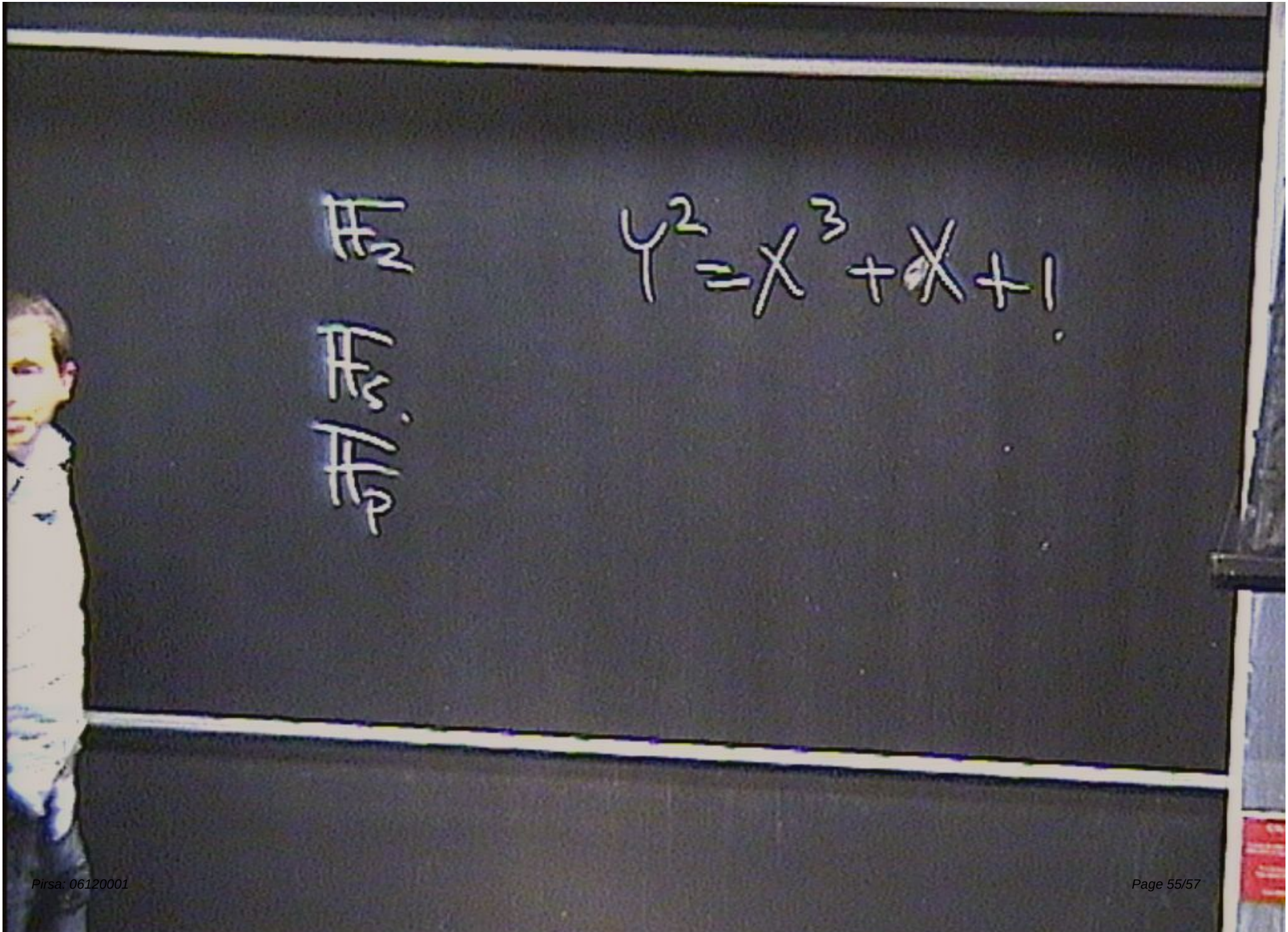
Just as the $\zeta_{Riemann}$ zeros obey the kind of statistics of random Hermitian matrices, the zeros of these finite field equation Zeta functions (seem to) obey the statistics of random unitary matrices.

[Sato-Tate] For a fixed elliptic curve the Zeta zeros over different $\mathbb{F}_p$ obey random SU(2) statistics.(?)

$\mathbb{F}_2$

$Y^2 = X^3 + X + 1$

$\mathbb{F}_2$ $\quad Y^2 = X^3 + X + 1$


$\mathbb{F}_2$
$\mathbb{F}_5$.
$\mathbb{F}_p$
$Y^2 = X^3 + aX + 1$.

Arguments in Favor of a Spectral Interpretation

Just as the $\zeta_{Riemann}$ zeros obey the kind of statistics of random Hermitian matrices, the zeros of these finite field equation Zeta functions (seem to) obey the statistics of random unitary matrices.

[Sato-Tate] For a fixed elliptic curve the Zeta zeros over different $\mathbb{F}_p$ obey random SU(2) statistics.(?)

[Katz & Sarnak] For curves in the limit $g,p \to \infty$, the eigenvalues θ_j are distributed as if they are sampled from the random unitary matrices in USp(2g).

Semiclassical Methods

For the Riemann zeta function Odlyzko and Berry looked at the deviations from the GUE statistics.

Using semi-classical methods for quantum chaotic systems, Berry managed to match the deviations in the 'number variance' with surprising accuracy:

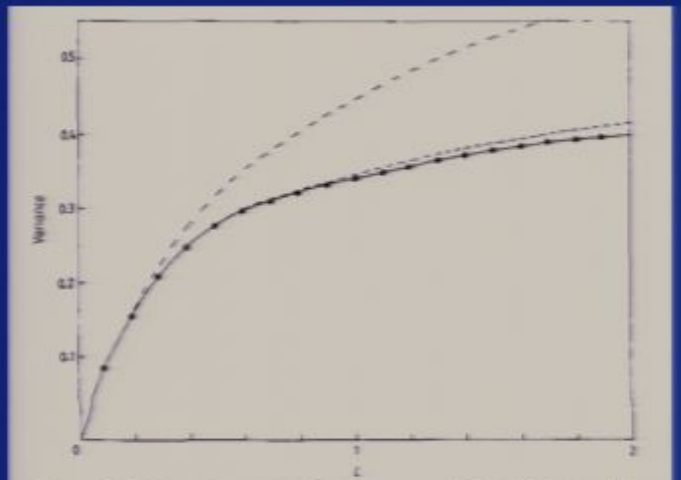


Figure 1. Number variance $V(L;x)$ of the Riemann zeros, for $0 \leq L \leq 2$ and $x = 10^{12}$. Dots: computed from the zeros by Odlyzko; full curve: semiclassical formula (19) with $\pi^* = \frac{1}{2}$; broken curve: number variance of the GUE; chain curve: number variance of the Gaussian orthogonal ensemble (GOE) of real symmetric random matrices.

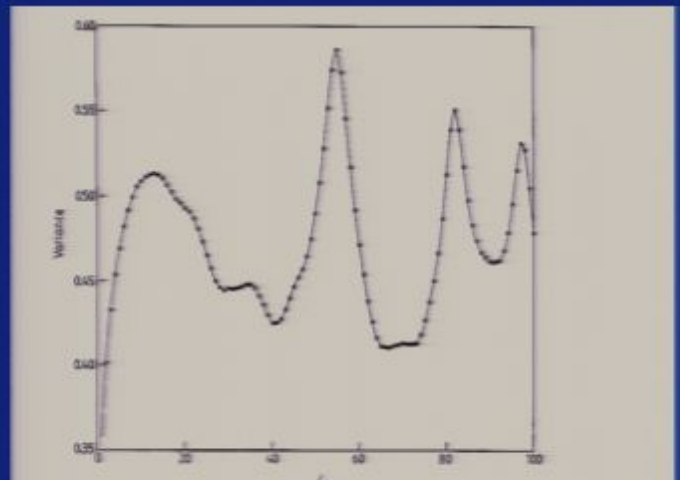


Figure 3. As figure 2 but for $0 \leq L \leq 100$ and with stars rather than dots for the variance computed from the zeros (GUE not shown).