orders, including that few elements $\sigma \in S_n$ have orders comparable with the maximal asymptotic order, $g(n) \sim \exp(\sqrt{n \log n})$. They noted for example that there were $(n-1)!$ elements σ, consisting of a single cycle, having order n. They proved that the order of a "generic" element is much smaller than the maximum. Here we simply state two of their main results.

Theorem 10.43 *Given $\epsilon, \delta > 0$ and n sufficiently large, depending on ϵ and δ, we have, other than for at most $\delta n!$ permutations σ:*

$$e^{(1/2-\epsilon)\log^2 n} \le \operatorname{ord}(\sigma) \le e^{(1/2+\epsilon)\log^2 n}.$$

They indicated they could use the method they developed to show also that:

Theorem 10.44 *Provided $n \to \infty$ through integers such that $\omega(n) \to \infty$ we have for $\sigma \in S_n$*

$$\left|\log \operatorname{ord}(\sigma) - \frac{1}{2}\log^2 n\right| \le \omega(n) \log^{3/2} n$$

with at most $o(n!)$ exceptions.

10.11 Hilbert–Pólya Conjecture

To describe this conjecture and equivalence we first need some definitions. Let H be a complex Hilbert space and let Δ be a dense linear subspace and $T, \Delta \to H$ a linear transformation. Let

$$\Delta_* := \{x \in H : y \to \langle x, Ty\rangle \text{ is a continuous linear functional on all of } H\}.$$

By the Riesz representation theorem (Volume Two [32, Theorem J.1]), for each $x \in \Delta_*$ there is a unique $z \in H$ such that $\langle x, Ty\rangle = \langle z, y\rangle$ for all $y \in \Delta$. We define $T^*(x) = z$, and call the linear transformation T^* the **adjoint** of T. The map T is called **self-adjoint** if the domain of its adjoint transformation T^* is also Δ, so $\Delta_* = \Delta$, and on this domain we have $T = T^*$, so for all $f, g \in \Delta$ we have $\langle Tf, g\rangle = \langle f, Tg\rangle$. Thus T is symmetric, a weaker condition than being self-adjoint.

The Hilbert–Pólya conjecture, as formulated by Hugh Montgomery in 1973 [119] possibly for the first time, is that if we write each non-trivial zero of $\zeta(s)$ with positive imaginary part as $\frac{1}{2} + i\gamma_n$, then the numbers γ_n correspond to the eigenvalues of an unbounded self-adjoint operator T. This of course would force the γ_n to be real and solve RH.

Since (see Lorch [110, theorem 4-1]) a self-adjoint transformation defined on all of H is necessarily bounded, we must have $\Delta \ne H$.

It appears that the conjecture goes back to the very conception of RH. In considering what was left of Riemann's handwritten working paper collection in the Göttingen University library, John Keating found a note relating to the stability of a rotating fluid on the same page as notes on the zeros of $\zeta(s)$ (see du Sautoy [151, p. 286]). The condition for stability of the fluid subject to perturbation was that a set of eigenvalues should be on a straight line! An implicit connection between RH and something physical!

Andrew Odlyzko attempted, in the early 1980s while Pólya was still alive, to trace the formulation of the conjecture back to Pólya and Hilbert by corresponding with Pólya (see Volume Two [32, Chapter 5]). Pólya recalled answering a question of Landau as to whether or not there was a physical reason why RH should be true. Pólya's answer was that it would be the case if the nontrivial zeros of the function $\xi(s)$ were so connected with the physical problem that RH would be equivalent to all of the eigenvalues of that problem being real. Odlyzko was not able to find any reported statement by Hilbert, but the name of the conjecture is now well established by use.

While up to the time of writing Hilbert–Pólya has failed to provide a proof of RH, the conjecture has inspired a great deal of work and progress in the intersection of mathematics and physics. The main focus has been to design the Hilbert space H, domain Δ and transformation T. Macroscopic classical mechanical systems, quantum mechanical and quite a few others have been investigated, but no one seems to have come close to providing what is needed. Some believe asking for the transformation to be self-adjoint is too much, or that the structures should be constructed out of mathematics alone, i.e. starting with the integers. Sir Michael Berry and his co-workers have given quite precise specifications on what a successful structure might need to satisfy [11].

As part of this story of successful synergies between mathematics and physics, there is the well-known and often retold interaction between Hugh Montgomery and Freeman Dyson over tea in the Institute for Advanced Study, Princeton [151, p. 262]. This became related to the great body of work on random matrices, which was originally developed as a way to study, statistically, the energy levels of heavy nuclei, i.e. those with large numbers of neutrons and protons. The relationships with the results of computations of zeta zero imaginary parts, especially those carried out by Andrew Odlyzko [79, 130], have been startling.

Background reading might include Conrey [41], Katz and Sarnak [90] and Rudnick and Sarnak [147]. On the physics side, there is the survey preprint of Schumayer and Hutchinson [155].

One of the remarkable particular discoveries of random matrix theory has been very precise expressions for moments of distribution functions, providing corresponding conjectures for the moments of $\zeta(s)$. Here are the conjectured moments of John Keating and Nina Snaith [91] for $\zeta(s)$ for all $k \in \mathbb{N}$ and s on the critical line:

$$\frac{1}{T}\int_0^T |\zeta(\tfrac{1}{2}+it)|^{2k}\,dt \sim g_k a(k)\left(\log\tfrac{T}{2\pi}\right)^{k^2},$$

where

$$a(k) := \prod_p \left(1 - \frac{1}{p}\right)^{k^2} \sum_{m=0}^{\infty} \left(\frac{\Gamma(m+k)}{m!\Gamma(k)}\right)^2 \frac{1}{p^m}$$

and

$$g_1 = 1, \quad g_2 = 1/12, \quad g_3 = 42/9!, \quad g_4 = 2024/16!,$$

and if

$$G(n) := \prod_{i=0}^{n-2} i! \quad \Longrightarrow \quad g_k = \frac{G(k+1)^2}{G(2k+1)}.$$

Estimates for moments of zeta have been very significant, and have been so for a long time. For example Landau in his treatise of 1908 included the following theorem for the case $k = 1$ [51, section 9.7]: Given $\epsilon > 0$ and $\sigma_0 > \frac{1}{2}$ there is a T_0 such that for all $\sigma \geq \sigma_0$ and $T \geq T_0$ we have

$$\left| \frac{1}{T-1} \int_1^T |\zeta(\sigma + it)|^2 \, dt - \zeta(2\sigma) \right| < \epsilon.$$

This estimate was used by Bohr and Landau [51, section 9.6], together with Jensen's formula (Volume Two [32, Theorem B.5]), to show that the number of zeta zeros in any rectangle $R := [\delta, 1] \times [0, T]$ for any $\delta > \frac{1}{2}$ is bounded above by $K_\delta T$. Since the total number of zeta zeros $N(T)$ in $[0,1] \times [0,T]$ satisfies $N(T) \sim T/(2\pi) \log(T/(2\pi e))$, the proportion of roots in R divided by the total number up to T tends to zero as $T \to \infty$. This result is still one of the best pieces of analytic evidence for the truth of RH.

For more recent significant developments on the topic of estimates for moments and references, there is the article of Soundararajan [160].

Searching for a single self-adjoint transformation which would resolve RH could be asking too much. For example associating each zero with an individual transformation depending on the zero would give the same result. The work of Ross Barnett and the author leading to [21], consistent with random matrix theory, seems to indicate a relationship between rotations and zeta zeros, which has yet to be fully developed.

Theorem 10.45 (Hilbert–Pólya criterion) *The Riemann hypothesis is equivalent to the following property: for each critical zero ρ of $\zeta(s)$, when written in the form $\rho = \frac{1}{2} + i\eta$, there is a self-adjoint transformation T_ρ of a Hilbert space H_ρ such that η is an eigenvalue of T_ρ.*

Proof If RH is true let $H = \ell_2(\mathbb{N}, \mathbb{C})$ with Euclidean inner product, and for $n \in \mathbb{N}$ let $e_n := (0, 0, \ldots, 1, 0, \ldots)$ be the nth standard basis element. If $\rho_n = \frac{1}{2} + i\eta_n$

is the nth complex zero with positive imaginary part, define $T : \Delta \to H$ by setting $T(e_n) = \eta_n e_n$, so

$$T(x) = \sum_{n \in \mathbb{N}} \eta_n x_n e_n.$$

Let $\Delta := \{x \in H : \|T(x)\| < \infty\}$. Since the linear subspace generated by any finite subset of the (e_n) is in Δ, Δ is dense in H. Since by RH each η_n is real, T is self-adjoint. Setting $T_\rho = T$ completes the derivation. □

10.12 Epilogue

Looking back over the equivalences to RH described in Chapters 4 through 10, the reader might be surprised at their variety, but also at the few properties of $\zeta(s)$ which have been used to derive them: von Mangoldt's theorem, a simple zero-free region, both known for over 100 years, and a better critical zero line height H – but even deriving improvements to H often uses methods based on those dating back to Turing. The functional equation barely appears, neither does the lower bound for the proportion of zeros on the critical line, nor upper bounds for zeros possibly off the line.

In addition, the properties of primes that are used are slight and based on not much more than the prime number theorem – no quadratic reciprocity, no modular restrictions. It is some explicit estimates for arithmetic quantities which are used to derive the simple inequalities which have been shown to be equivalent to RH. Work on these estimates has thus been shown to be invaluable.

Another observation is that when RH fails, the failure has dramatic consequences. Just one off-critical-line zero will result in an infinite number of failures for an equivalent inequality.

One approach to resolving RH, begun as reported in Chapter 8, would be to further explore properties of potential counterexamples, or sets of counterexamples, i.e. integers which do not satisfy an equivalent inequality. Finding a set of restrictions which are inconsistent would be the goal. Another approach would be to work at weakening a given inequality and strengthening a related unconditional form, until they merge.

Bringing to bear on equivalences recent better understanding of prime properties, such as primes in progressions and infinite subsequences of primes with $p_{n+1} - p_n \leq K$ for some explicit (and small) value of K, as well as more classical properties, could also be fruitful. In this way it is properties of primes which could resolve RH, rather than the reverse!

In addition to the equivalences described here, there are a host of other equivalences which have been demonstrated. These are often fascinating and, on the face of it, it is difficult to detect any connection to RH. Many of these are described in Volume Two [32].