Primes and hypotheses !

Professor Wazir Hasan Abdi Memorial Talk
CUSAT, October 7, 2006

B.Sury

Stat-Math Unit
Indian Statistical Institute
Bangalore, India
sury@isibang.ac.in

The great mathematician-physicist Henri Poincaré wrote a book on 'Science and Hypothesis'. There, he discusses the process of discovery in science. In this talk, let us take his cue and try to describe the process and history of discoveries/inventions in the theory of prime numbers which is based on coming up with hypotheses. The focus is on the Riemann Hypothesis which still stands out among all such hypotheses. When we trace our path through classical prime number theory, and try to see how the subject has evolved, we find ourselves led inevitably to the so-called Langlands Program, a sort of 'grand unification' theory in mathematics. The Riemann Hypothesis and ideas associated with it seem to light up the path of this discovery.
In 1748, Leonhard Euler wrote down the fundamental theorem of arithmetic as an analytic statement. The so-called Euler product

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p\ prime} (1 - p^{-s})^{-1}$$

valid for all real $r > 1$ is just a rephrasing on the fundamental theorem that every natural number > 1 is a unique product of prime powers. This proves the infinitude of primes in an analytic and quantitative manner since the series on the left diverges at $s = 1$. Needless to say the distribution of prime numbers, being a fundamental problem, fascinated the top mathematicians of each generation. The great Carl Friedrich Gauss - conjectured the so-called 'Prime Number Theorem' in 1794, at the ripe old age of 17 (!) Roughly speaking, this is the assertion that the function $\pi(x)$ measuring the number of primes upto a given x behaves like the function $Li(x) := \int_1^x \frac{dt}{log\ t}$. More precisely, $\frac{\pi(x) log\ x}{x} \to 1$ as $x \to \infty$. Equivalently, the n-th prime p_n satisfies $\frac{p_n}{n\ log(n)} \to 1$ as $n \to \infty$. It is amusing to compare Gauss's interest with 'FLT' (Fermat's last theorem) - he is said to have remarked that the problem doesn't interest him as he can come up with many similar questions on Diophantine equations which cannot be answered and that there was nothing particularly special about FLT ! Although the infinitude of primes was known from Euclid's time, the infinitude of primes in every arithmetic progression of the form $an+b$ with $(a, b) = 1$ was proved only in 1837 by Lejeune Dirichlet. Unlike Euclid's proof which is a variation of the fundamental theorem of arithmetic and can be (and is being) taught in schools, Dirichlet's proof requires much more sophisticated, *analytic* techniques. One might say that Euler's basic, but deep, observation on Euler product expansion was the key behind Dirichlet's perspective. Dirichlet would need to consider (approximately a) more series similar to Euler's series $\sum_{n=1}^{\infty} \frac{1}{n^s}$. During 1848-50, the Russian mathematician Chebychev proved the beautiful fact that there are certain constants $a, b > 0$ such that

$$a \frac{x}{log\ x} \leq \pi(x) \leq b \frac{x}{log\ x}$$

for large x. However, it is Bernhard Riemann's 1859 memoir which turned around prime number theory, introducing novel techniques and giving birth

to the subject of analytic number theory. Riemann lived less than 40 years (September 17, 1826 - July 20, 1866) and wrote, but one, paper on number theory ! Earlier, when Riemann was submitted a Doctoral Dissertation in 1851, Gauss remarked that Riemann had 'Gloriously fertile originality'. Riemann developed what is now known as Riemannian geometry and was the indispensable theory and language used by Einstein for formulating his theory of relativity. Coming back to Riemann's paper in number theory, the key difference between earlier workers and Riemann's paper was the he considered the series $\sum_{n=1}^{\infty} \frac{1}{n^s}$ as a function of a complex (!) variable s which varies over the right half-plane $Re(s) > 1$. This is now called the Riemann zeta function. Riemann proved two basic properties (meromorphic continuation and functional equation to be recalled below). The key point of viewing the zeta function as a function of a complex variable s allowed Riemann to prove an 'explicit formula' connecting the complex zeroes of the zeta function and the set of prime numbers ! Riemann also made 5 conjectures, 4 of which were solved in the next 40 years. The one-unproved conjecture is the so-called Riemann Hypothesis, a 'Problem of the Millennium' for which there is a million-dollar prize now.

Riemann's memoir

The Riemann zeta function $\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$ for $Re(s) > 1$ satisfies :
(I) Meromorphic continuation :
$\zeta(s)$ can be defined for all $s \in \mathbf{C}$ as a holomorphic function except for the single point $s = 1$ where it has a simple pole with residue 1;
The key function Riemann uses for this is Jacobi's theta function $\theta(x) = \sum_{n=-\infty}^{\infty} e^{-n^2 \pi x}$ *which has the transformation property* $\theta(1/x) = \sqrt{x}\theta(x)$ *which is also a harbinger of the connection of* $\zeta(s)$ *with modular forms to be discussed later.*
(II) Functional equation :
The continued function (again denoted $\zeta(s)$) satisfies

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \pi^{-(1-s)/2}\Gamma((1-s)/2)\zeta(1-s).$$

Here $\Gamma(s)$ is the Gamma function defined by

$$\Gamma(s) = \int_0^{\infty} x^{s-1}e^{-x}dx$$

for $x > 0$.
It ought to be mentioned that the appearance of the Gamma function here was not properly understood until the appearance of John Tate's thesis as late as 1950. From Tate's work, it becomes clear that the Gamma factor is the correct term corresponding to the the archimedean place (or 'the infinite prime') of $\mathbf{Q}$.

The functional equation tells us that the values of *zeta* at s and at $1 - s$ are related. As the Gamma function has poles at all negative integers, the zeta function has zeroes at all $-2n$ for natural numbers n. Also, from the simple

pole of $\zeta(s)$ at $s=1$ and of $\Gamma(s/2)$ at $s=0$, we obtain $\zeta(0)=-1/2$. Sometimes, this is stated in fancy language (by abusing notation) as

$$1+1+1+\cdots\cdots=-\frac{1}{2} \quad !$$

Similarly, the value $\zeta(-1)=-\frac{1}{12}$ gives :

$$1+2+3+\cdots\cdots=-\frac{1}{12} \quad !$$

As a matter of fact, one has

$$\zeta(-n)=(-1)^n\frac{B_{n+1}}{n+1}$$

where B_r are the Bernoulli numbers ! Note that $B_{odd>1}=0$ which is related to $\zeta(-even<0)=0$.
Looking at the symmetry in the functional equation, it may be tempting to muse whether all the zeroes of $\zeta(s)$ are on the line of symmetry $Re(s)=1/2$ but this, in itself may be too simplistic, as there are series with similar symmetry whose zeroes are not on the line of symmetry; so this symmetry by itself is not sufficient reason to conjecture the Riemann hypothesis (to be discussed below). However, these other series do not possess Euler products; so, this still does not rule out the possibility that the symmetry may be the property which prompted Riemann to formulate the Riemann hypothesis.

Riemann's five conjectures in his 8-page paper were :
(i) $\zeta(s)$ has infinitely many zeroes in $0\leq Re(s)\leq 1$.
(ii) The number of zeroes of $\zeta(s)$ in a rectangle of the form $0\leq Re(s)\leq 1$, $0\leq Im(s)\leq T$ equals $\frac{T}{2\pi}log\frac{T}{2\pi}-\frac{T}{2\pi}+O(log\ T)$ as $T\to\infty$, where the notation $f(T)=O(g(T))$ means $\frac{f(T)}{g(T)}$ is bounded by a constant independent of T.
(iii) The function

$$\xi(s)=s(s-1)\pi^{-s/2}\Gamma(s/2)\zeta(s)$$

has an infinite product expansion of the form $e^{A+Bs}\prod_\rho(1-\frac{s}{\rho}e^{s/\rho})$ for some constants A,B where the product runs over the zeroes of $\zeta(s)$ in the infinite strip $0\leq Re(s)\leq 1$.
(iv) If $\Lambda(n)$ is the von Mangoldt arithmetical function defined to be $log\ p$ if n is a power of a single prime p and zero otherwise, and if $\psi(x)=\sum_{n\leq x}\Lambda(n)$, then

$$\psi(x)=x-\sum_\rho\frac{x^\rho}{\rho}-\frac{\zeta'}{\zeta}(0)-\frac{log(1-x^{-2})}{2}.$$

The value $\frac{\zeta'}{\zeta}(0)$ can be seen to be $log(2\pi)$ on using the functional equation. Note that the sum over the zeroes is to be interpreted as $lim_{T\to\infty}\sum_{|\rho|\leq T}\frac{x^\rho}{\rho}$ and is not absolutely convergent.

(v) (**Riemann hypothesis**) All the zeroes of $\zeta(s)$ in the so-called critical strip $0 \leq Re(s) \leq 1$ lie on the vertical line $Re(s) = \frac{1}{2}$.

The conjectures (i),(ii), and (iv) were proved in 1895 by von Mangoldt and (iii) was proved by Hadamard in 1893. Until date, (v) is open. Notice that (iv) gives an explicit relation between prime numbers and *zeroes* of $\zeta(s)$! In fact, in 1893, Hadamard and de la vallé Poussin independently proved that

$$\zeta(s) \neq 0 \ \ \forall \ \ Re(s) = 1.$$

This non-vanishing on the vertical line implies immediately that the ratio $\frac{\psi(x)}{x} \to 1$ as $x \to \infty$. This is just another rephrasing of the Prime number theorem ! Indeed, looking at (iv), we see that $|x^{\rho}| = x^{Re(\rho)}$ and, therefore, the prime number theorem ($\psi(x) \sim x$) is equivalent to the assertion $Re(\rho) < 1$.
Incidentally, the key to the proof of the non-vanishing of the Riemann zeta function on the line $Re(s) = 1$ is the elementary fact $3 + 4Cos(\theta) + Cos(2\theta) \geq 0$.
Another rephrasing is the assertion $\frac{\theta(x)}{x} \to 1$ as $x \to \infty$, where the Chebychev function $\theta(x) = \sum_{p \leq x} log\ p$. The above statements are quite easy to see using a very simple elementary idea known as Abel's partial summation formula which states :
For any arithmetic function $a(n)$, consider the partial sums $A(x) = \sum_{n \leq x} a(n)$ (and $A(x) = 0$ if $x < 1$). For any C^1-function f on (y, x) where $0 < y$, one has

$$\sum_{y < n \leq x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt.$$

For instance, taking $f(x) = log\ x$ in the partial summation formula, one can deduce

$$\theta(x) = \pi(x) log\ x - \int_2^x \frac{\pi(t)}{t} dt.$$

One can also use $0 \leq \psi(x) = \sum_{m \leq log_2 x} \theta(x^{1/m})$ to obtain

$$\frac{\psi(x)}{x} - \frac{\theta(x)}{x} \to 0$$

as $x \to \infty$.
It is not difficult to see that the RH itself is equivalent to the assertion :

$$\pi(x) = \int_2^x \frac{dt}{log\ t} + O(x^{1/2} log\ x)$$

where $\pi(x)$ counts the number of primes upto x.
An important technique used in analytic number theory to estimate the sum $\sum_{n \leq x} a_n$ for a given $f(s) = \sum_n \frac{a_n}{n^s}$ is the Perron formula (for any $c > 0$) :
$\frac{1}{2\pi i} \int_{Re(s)=c} \frac{x^s}{s} ds = 0, 1/2$ or 1, according as to whether $0 < x < 1, x = 1$ or

$x > 1$.
Then, for a suitably chosen $c > 0$, we would have

$$\frac{1}{2\pi i}\int_{Re(s)=c} f(s)x^s/sds = \sum_{n\leq x} a_n.$$

This is used for the logarithmic derivative of $\zeta(s)$ to obtain the prime number theorem in the form $\psi(x) \sim x$. Note $\frac{\zeta'(s)}{\zeta(s)} = \sum_n \frac{\Lambda(n)}{n^s}$ from the Euler product formula.
Actually, The fact that $\zeta(s) \neq 0$ for $Re(s) > 1$ (which is not obvious from the series expression but becomes clear from the absolute convergence of the Euler product expression) is said to be the key analytical information used in Deligne's first proof of the analogue of the Riemann Hypothesis for varieties over finite fields (mentioned below). We will discuss the place of the RH in contemporary mathematics as well as point out results which provide evidence for it to be true. On the way, we will encounter many classes of so-called L-functions of which the Riemann zeta function is a prototype and also mention other hypotheses which imply or are implied by RH. Before proceeding towards that, we just mention that a rather simple aspect already makes the RH as the main open problem in prime number theory - if RH were to fail, it would create havoc in the distribution of prime numbers. David Hilbert had some interesting views on the RH. Comparing the problem of transcendence of e^π, Fermat's last theorem and the Riemann Hypothesis, Hilbert felt that RH would be proved in a few years, Fermat would take quite a few years but that the transcendence result would not be proved for several hundred years. The opposite situation seems to have prevailed ! In fact, Hilbert seems to have expressed conflicting views on RH. Once he said that if he were to wake up after a sleep of a thousand years, the first question he would ask is whether the RH has been solved ! G.H.Hardy grew to be very fond of the RH. Once, while beginning a risky journey, he wrote to Harald Bohr that he had solved the RH although he had not done so !
It is not difficult to show that the RH gives

$$\frac{Li(x) - \pi(x)}{\sqrt{x}log(x)} \simeq 1 + 2\sum_\gamma \frac{Sin(\gamma log(x)}{\gamma}$$

where the sum is over all positive real γ such that $\frac{1}{2} + i\gamma$ is a zero of $\zeta(s)$. Therefore, as the right side is a sum of periodic functions, sometimes people express the RH as saying that 'the primes have music in them'!

Lindelöf hypothesis and Mertens conjecture
A consequence of the RH is the Lindelöf hypothesis :

$$\zeta(\frac{1}{2} + it) = O(t^\epsilon)$$

as $t \to \infty$. This is still open.
Let $\mu(n)$ denote the Mobius function defined for $n > 1$ as $(-1)^r$ if n is a square-free product of r prime numbers, and 0 if n is not square-free. One takes

$\mu(1) = 1$. Note that formally, one has

$$\zeta(s) \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = 1.$$

Landau proved that the prime number theorem is equivalent to the assertion $\frac{1}{x} \sum_{n \leq x} \mu(n) \to 0$ as $x \to \infty$. It is also easy to show that the RH is equivalent to the assertion :

$$\sum_{n \leq x} \mu(n) = O(x^{1/2+\epsilon}).$$

Indeed, clearly the RH implies this assertion. Conversely, assuming this assertion, partial summation gives us that $\sum_n \frac{\mu(n)}{n^s}$ converges for all s for which $Re(s) > 1/2$. Thus, $\frac{1}{\zeta(s)} = \sum_n \frac{\mu(n)}{n^s}$ has no poles in this half-plane; this is the RH.
It is conceivable that it may be easier to work with the function on the left hand side above by some combinatorial method rather than working with $\pi(x)$. Actually, most random sequences of $+1$'s and -1's give a sum upto x which is bounded by $x^{1/2+\epsilon}$ and the Möbius function appears to be fairly random; thus, this is some probabilistic evidence for the RH to hold.
Mertens conjectured the stronger :

$$|\sum_{n \leq x} \mu(n)| \leq \sqrt{x}$$

for $x > 1$. This was proved to be false by Odlyzko & te Riele in 1985. It should be noted that in the nice book 'Introduction to Analytic Number Theory' by Tom Apostol (available in an Indian edition) this has not been pointed out - indeed, it is asserted on page 91 that Mertens's conjecture is neither proved nor disproved.
It is unknown (although expected to be false) whether the assertion

$$\sum_{n \leq x} \mu(n) = O(x^{1/2})$$

which is stronger than the RH holds.

Turan's theorem
Paul Turan showed the interesting result that if, for every N, the finite sum $\sum_{n=1}^{N} \frac{1}{n^s}$ is non-zero for all $Re(s) > 1$, then the RH follows.

However, this approach towards solving the RH was doomed to failure as well : Montgomery proved that Turan's hypothesis does not hold; indeed, for each large N, the finite series $\sum_{n=1}^{N} \frac{1}{n^s}$ has a zero in $Re(s) > 1$! A somewhat careful analysis of Turan's proof reveals that positivity of a certain function was used. In the following discussion, such a positivity condition makes it possible to obtain an equivalent rephrasing of the RH.

Weil's explicit formula and the RH

Let $\rho = \frac{1}{2} + i\gamma$ vary over the zeroes of $\zeta(s)$; here γ is complex, and the RH implies that γ is real. Consider any analytic function $h(z)$ on $|Im(z)| \leq \frac{1}{2} + \delta$ satisfying

$$h(-z) = h(z), |h(z)| \leq A(1 + |z|)^{-2-\delta}$$

for some $A, \delta > 0$.

Suppose g is the Fourier transform of h; that is, $g(u) = \frac{1}{2\pi} \int_{\mathbf{R}} h(z) e^{-izu} dz$. André Weil proved the so-called *explicit formula*

$$\sum_{\gamma} h(\gamma) = \frac{1}{2\pi} \int_{-\infty}^{\infty} h(z) \frac{\Gamma'}{\Gamma} (\frac{1}{4} + \frac{iz}{2}) dz + 2h(\frac{i}{2}) - g(0) log\ \pi - 2 \sum_{n=1}^{\infty} \frac{\Lambda(n)}{\sqrt{n}} g(log\ n).$$

In other words, *the set of prime numbers and the nontrivial zeroes of $\zeta(s)$ are in duality ! As Weil observed, the Riemann Hypothesis is true if and only if $\sum_{\gamma} h(\gamma) > 0$ for all h of the form $h(z) = h_0(z)\overline{h_0(\bar{z})}$.*

Other equivalent hypotheses to RH

(i) Hardy & Littlewood proved for the first time in 1918 that infinitely many zeroes of $\zeta(s)$ lie on the critical line $Re(s) = 1/2$. They also showed that the RH holds good if and only if $\sum_{n=1}^{\infty} \frac{(-1)^n x^n}{n!\zeta(2n+1)} = O(x^{-1/4})$.

(ii) In 1977, Redheffer showed that the truth of the RH is equivalent to the assertion that for each $\epsilon > 0$, there exists $c(\epsilon) > 0$ so that $|detA_n| < c(\epsilon) n^{1/2+\epsilon}$, where A_n is the $n \times n$ matrix whose (i, j)-th entry is 1 if either $j = 1$ or $i|j$ and zero otherwise.

(iii) Recently, in 2002, Jeffrey Lagarias proves that RH is equivalent to the assertion

$$\sigma(n) \leq H_n + e^{H_n} log(H_n)$$

where $\sigma(n) = \sum_{d|n} d, H_n = \sum_{i=1}^{n} \frac{1}{i}$.

(iv) Functional-analytic approaches seem quite promising in view of Weil's positivity condition. Nyman, and later Baez-Duarte have versions of the RH. The latter's results were rephrased by Bhaskar Bagchi to yield the following avataar of the RH.

Look at the inner product space $\mathcal{H}$ consisting of all sequences $a := \{a_n\}$ of complex numbers which satisfy $\sum_{n=1}^{\infty} \frac{|a_n|^2}{n(n+1)} < \infty$. Here, we take

$$< a, b >= \sum_{n=1}^{\infty} \frac{a_n \overline{b_n}}{n(n+1)}.$$

All bounded sequences are in $\mathcal{H}$. For $k = 1, 2, 3 \cdots$ consider the special elements $a(k) \in \mathcal{H}$ given by $a(k)_n = \{\frac{n}{k}\}$, the fractional part of $\frac{n}{k}$. Then, the RH is equivalent to either of the following statements :

(a) *The constant sequence $1, 1, 1, \cdots$ is in the closure of the space spanned by*

the $a(k)$'s; $k = 1, 2, \cdots$.
(b) *The set of finite linear combinations of the $a(k)$'s is dense in $\mathcal{H}$.*

Evidence towards RH - zeta functions of curves over finite fields

There may be said to be three types of evidence to believe in the possible truth of RH. One is, of course, deep analytic methods which show that at least 40 per cent of the zeroes of the nontrivial zeroes lie on the critical line. The other is indirect evidence by virtue of statements which are nontrivial consequences of the RH and are either believable for other reasons or have been shown to be true by other means. The Generalized Riemann Hypothesis (which we will mention later) implies things like : (i) Miller's primality test, (ii) Artin's primitive roots conjecture, (iii) knowledge of rate of equidistribution in case of geodesic motion on an arithmetic hyperbolic surface (this is a central topic in quantum chaos). The third, and perhaps the most compelling sort of evidence comes from the proof of RH (yes proof!) for analogues of the Riemann zeta function. Let us talk about this third type of evidence. Just as the Riemann zeta function is an Euler product involving all the prime numbers, there is an analogous zeta function for finite fields which involves its irreducible monic polynomials. In fact, a definition of the zeta function of an algebraic curve over a finite field was given by Emil Artin in his 1924 thesis. He also proved the analogue of the RH for some 40 curves. In 1934, Helmut Hasse established that the analogue of RH holds for the class of zeta functions associated to elliptic curves (nonsingular cubic curves $y^2 = f(x)$) over finite fields. Andre Weil proved the RH for *all* nonsingular curves over finite fields in 1948 by deep methods from algebraic geometry. A simpler proof by Andrei Stepanov in 1969 was further simplified by Enrico Bombieri in 1972 using the Riemann-Roch theorem to a 5-page proof ! As a matter of fact, Weil can be thought of as the creator of the subject now known as arithmetic geometry. In 1949, Weil defined a zeta function for any algebraic variety over a finite field and made several conjectures (which came to be known as the Weil conjectures). One of these conjectures is an analogue of the RH. Actually, Weil proved all these conjectures (not just the RH analogue) in the special case of nonsingular algebraic curves. It is perhaps amazing that the prototype already occurs in the work of Gauss ! The Last entry in his famous mathematical diary is a special case of Weil's RH :
Let $p \equiv 1$ mod 4 be a prime. Then, the number of solutions of the congruence $x^2 + y^2 + x^2y^2 \equiv 1$ mod p equals $p - 1 - 2a$, where $p = a^2 + b^2$ and $a + ib \equiv 1$ mod $2(1 + i)$.
It required tremendous progress in algebraic geometry before Pierre Deligne proved the Weil conjectures in general in 1973. Deligne's journey takes him through the theory of modular forms and a beautiful conjecture due to Ramanujan turns out to be the analogue of the RH ! Before that, in 1950, Atle Selberg defined another kind of analogue of the zeta function which counts the lengths of closed geodesics in Riemannian manifolds. In a remarkable tour-de-force, Selberg developed a so-called trace formula involving eigenvalues of

Laplacian and deduced the analogue of the RH for his zeta function ! The trace formula resembles Weil's explicit formula above. Selberg had received a Fields medal for his elementary (that is not involving complex analysis) proof of the prime number theorem. His work on the trace formula was perhaps worthy of another Fields medal !

Let C be a nonsingular projective curve over a finite field $\mathbf{F}_q$ where $q = p^e$ and p is a prime. One considers the formal finite sums of the form $D = \sum a_i P_i$ where a_i are integers (of any sign) and the points P_i in C are defined over some finite extensions of $\mathbf{F}_q$ where $Frob_q(D) = D$. This is called the group $Div(C)$ of divisors of C. One calls a divisor $D = \sum a_i P_i$ effective (and writes $D > 0$) if $a_i \geq 0$ for all i. The *prime divisors* are those which are not expressible as a sum of effective divisors. Denoting the homomorphism $\sum a_i P_i \to \sum a_i$ by 'deg', Artin-Hasse-Schmidt's definition of the zeta function of C is :

$$\zeta(C, s) := \sum_{D>0} (q^{deg(D)})^{-s} = \prod_P (1 - q^{deg(P)})^{-s}.$$

This satisfies the functional equation

$$q^{(g-1)s}\zeta(C, s) = q^{(g-1)(1-s)}\zeta(C, 1 - s)$$

where g is the genus of C.
The Riemann-Roch theorem implies that $\zeta(C, s)$ is a rational function of q^{-s}; write $\zeta(C, s) = Z(C, t)$ where $t = q^{-s}$ and Z is a rational function of t.
The RH is the statement that all zeroes of $\zeta(C, s)$ lie on $Re(s) = \frac{1}{2}$; this is equivalent to the assertion that the numerator polynomial of Z has all zeroes of absolute value $q^{-1/2}$. This is easy to verify for $g = 0$. For $g = 1$, one has the case of elliptic curves and it is Hasse's theorem.
In the Weil conjectures for general algebraic varieties X, the RH corresponds to the statement that the zeroes and poles of the corresponding rational function have absolute values $q^{\pm d/2}$ for some integer d. In fact, the roots (even in Hasse's theorem for elliptic curves) are viewed as eigenvalues of the Frobenius automorphism of $\mathbf{F}_q$ acting on the cohomology of the variety X.

Dedekind zeta functions

For an algebraic number field K (example $K = \{a + ib : a, b \in \mathbf{Q}\}$), with its ring of integers $\mathcal{O}$ (in the above example, it is the ring $\mathbf{Z}[i]$ of Gaussian integers), the 'fundamental theorem of arithmetic' in $\mathbf{Z}$ generalizes to an analogue which asserts that ideals in $\mathcal{O}$ are uniquely products of prime ideals. Moreover, every non-zero ideal I has finite index in $\mathcal{O}$, which is denoted by $N(I)$. Thus, one has the Dedekind zeta function

$$\zeta_K(s) = \sum_{I \neq 0} N(I)^{-s} = \prod_P (1 - N(P)^{-s})^{-1}.$$

The series and the product are absolutely convergent for $Re(s) > 1$. Note that $\zeta_{\mathbf{Q}} = \zeta$ and the Dedekind zeta function of K carries the same information on

distribution of prime ideals in $\mathcal{O}$ as does the Riemann zeta function about prime numbers.
The residue of the Riemann zeta function at $s = 1$ is 1 and does not contain any information. However, the corresponding residue for $\zeta_K(s)$ carries subtle information on K like its class number etc. In fact, we have :
Analytic continuation of $\zeta_K(s)$ *:*
$\zeta_K(s)$ admits a meromorphic continuation to $Re(s) > 1-1/d$ and is holomorphic except for a simple pole at $s = 1$ with residue given by 'the analytic class number formula' :

$$lim_{s\to 1^+}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}h(K)Reg(K)}{|\mu(K)|\sqrt{|disc(K)|}}.$$

There is also a functional equation of the form $\Lambda(s) = \Lambda(1-s)$ which gives in particular the location of the 'trivial zeroes' of $\zeta_K(s)$. For example, it turns out that $\zeta_K(-n) = 0$ for all non-negative integers n if $K \not\subset \mathbf{R}$. Finally, there is the :
Extended Riemann hypothesis :
All the 'nontrivial' zeroes of $\zeta_K(s)$ *lie on* $Re(s) = \frac{1}{2}$.

Dirichlet L-functions

The Riemann zeta function can be thought of as one of a class of the Dirichlet L-functions. Dirichlet proved the infinitude of primes in progressions several years before Riemann's work and, so, he looked at all his series in terms of convergence etc. but not in terms of analytic continuation. Suppose we wish to investigate the prime distribution in residue classes modulo q for some natural number q. Dirichlet considered the finite, abelian group $\mathbf{Z}_q^*$ of invertible residue classes mod q and the dual (in the sense of harmonic analysis) group of homomorphisms from this group to $\mathbf{C}^*$. Defining any such homomorphism to be zero on non-invertible residue classes and extending it to the whole of $\mathbf{Z}$ so as to be periodic mod q, one has the notion of Dirichlet characters mod q. For any such Dirichlet character χ mod q, one has a Dirichlet L-function

$$L(s,\chi) = \sum_{n=1}^{\infty}\frac{\chi(n)}{n^s} = \prod_{p\ prime}(1-\frac{\chi(p)}{p^s})^{-1}.$$

The Euler product expression is valid from the complete multiplicativity property of χ. For example, if $q = 4$, the group has two elements and the nontrivial character is the map which takes the value $(\frac{-1}{p})$ - the Legendre symbol - at any odd prime p. Note that $\zeta(s)$ is essentially $L(s,\chi)$ for the trivial character $\chi \equiv 1$. Look at any $a \geq 1$ which is relatively prime to q. Using the Schur's orthogonality property for characters shows :

$$\sum\{\frac{1}{p} : p \leq x, p \equiv a\ mod\ q\} = \frac{1}{\phi(q)}\sum_{p\leq x}\frac{1}{p} + \frac{1}{\phi(q)}\sum_{\chi\neq 1}\bar{\chi}(a)\sum_{p\leq x}\frac{\chi(p)}{p}.$$

Therefore, the assertion that

$$L(1,\chi) \neq 0 \ \ \forall \ \ \chi \neq 1$$

is equivalent to Dirichlet's theorem that :

$$\sum \{\frac{1}{p} : p \leq x, p \equiv a \ mod \ q\} = \frac{1}{\phi(q)} log \ log \ x + O(1).$$

Here, we have used the relation proved easily by Euler :

$$\sum_{p \leq x} \frac{1}{p} = log \ log \ x + O(1).$$

Note that in the case of $q = 4$, the nontrivial character χ satisfies

$$L(1,\chi) = 1 - \frac{1}{3} + \frac{1}{5} - \cdots = \frac{\pi}{4}.$$

Thus, asympotically, half the number of primes upto x are in each of the two classes 1 mod 4 and 3 mod 4.

Generalized Riemann hypothesis :
All the 'nontrivial' zeroes of $L(s,\chi)$ lie on $Re(s) = \frac{1}{2}$ for any Dirichlet character χ.

In some very interesting works, an explicit connection of the RH with the so-called Gauss class number problem was uncovered by Deuring, Hecke and Heilbronn. The number $h(d)$ of equivalence classes of binary quadratic forms of discriminant $d < 0$ is also the class number of the imaginary quadratic field $\mathbf{Q}(\sqrt{d})$. Gauss conjectured that $h(d) \to \infty$ as $-d \to \infty$. If χ_d is the Dirichlet character $p \mapsto (\frac{d}{p})$ on primes, then Dirichlet's class number formula gives (for $d < -4$),

$$h(d) = \frac{\sqrt{-d} L(1,\chi_d)}{\pi}.$$

Hecke showed that the analogue of the RH for $L(s,\chi_d)$ implies $h(d) \to \infty$. Deuring proved that if the usual RH were false, then one would have $h(d) > 1$ for large $-d$. This was generalized by Heilbronn who showed that if the RH were to be false for any Dirichlet L-function $L(s,\chi)$, then $h(d) \to \infty$. In this manner, Gauss's conjecture was proved !
To indicate a relationship of $\zeta_K(s)$ with Dirichlet L-functions, consider a nontrivial primitive Dirichlet character χ and look at the quadratic field $K = \mathbf{Q}(\sqrt{\pm q})$ where the sign is the value $\chi(-1)$. Then, one has :

$$\zeta_K(s) = \zeta(s) L(s,\chi).$$

At least, some readers may be surprised to know that this statement contains in it the quadratic reciprocity law of Gauss ! A point to be noted is that the right

hand side is defined essentially in terms of $\mathbf{Q}$*. As a matter of fact, whenever* K *is a Galois extension of* $\mathbf{Q}$ *whose Galois group is abelian, the famous theorem of Kronecker-Weber asserting that* K *is contained in a field of the form* $\mathbf{Q}(e^{2i\pi/m})$ *is equivalent to writing* $\zeta_K(s)$ *as a product of* $L(s,\chi)$ *for certain Dirichlet characters* χ*'s and of* $\zeta(s)$*. Whenever we have a decomposition of some Dedekind zeta function* $\zeta_K(s)$ *as a product of terms like the above involving only information from* $\mathbf{Q}$*, this gives a description of 'the primes which split in* K*'. This is valid when* L *is an abelian extension field of an algebraic number field* K *(with the RHS involving data from* K*) and is known as an 'Artin's reciprocity law' or 'abelian class field theory'. A conjectural form of this idea started with Emil Artin and led to the famous conjectures of Langlands.*

It should be mentioned that there are several concrete applications of this point of view (of viewing the distribution of ideals in $\mathcal{O}$ of norm less than some x in terms of $\zeta_K(s)$). For example, one has :

$$|\{I : N(I) \leq x\}| = (Res_{s=1}\zeta_K(s))x + O(x^{1-1/d})$$

as $x \to \infty$, where d is the degree of K over $\mathbf{Q}$. As a concrete instance, the analytic properties of $\zeta_K(s)$ for $K = \mathbf{Q}(i)$ implies :

$$\sum_{n \leq x} r_2(n) = \pi x + O(\sqrt{x})$$

as $x \to \infty$, where $r_2(n)$ is the number of ways of writing n as a sum of two squares of integers.

We end this section by merely mentioning two interesting things. The first is that analogous to (and generalizing) Dirichlet characters, there are - associated to a number field K - the so-called Hecke characters defined on the ray class groups of K.

The second is that there is a conjecture of Dedekind (which is still open) asserting that when $L \supset K$ are number fields, then the quotient $\frac{\zeta_L(s)}{\zeta_K(s)}$ extends to an entire function of s.

L-function of elliptic curves

Let E be an elliptic curve defined over $\mathbf{Q}$; this means that it is defined by an equation of the form $y^2 = x^3 + ax + b$ with $a, b \in \mathbf{Z}$, such that the roots of the cubic $x^3 + ax + b$ are distinct. There is a group law on the points of E which can be described explicitly. For any odd prime number p which does not divide $4a^3 + 27b^2$ (the discriminant of the cubic here), the equation reduces mod p to give an elliptic curve over the finite field $\mathbf{F}_p$. The number $a_p = p + 1 - |E(\mathbf{F}_p)|$ measures the deficiency in the number of points of the curve from the projective line. The famous thesis of Hasse in 1934 where he proves the Weil conjectures for elliptic curves, proves in particular the bound

$$|a_p| \leq 2\sqrt{p}.$$

This was conjectured by Emil Artin and is the RH here ! To indicate how, let us consider the Frobenius map $Frob_p$ at p. Then, the points of $E(\mathbf{F}_p)$ are those of E fixed by $Frob_p$. Therefore,

$$|E(\mathbf{F}_p)| = |Ker(Frob_p - 1)| = 1 - (\lambda + \lambda') + p$$

where λ, λ' are the roots of the characteristic polynomial.
Even when the prime p is one of the finitely many of bad reduction - those for which the equation defining E does not reduce mod p to give a nonsingular curve (that is, does not have distinct roots) - the nonsingular points form a group and one defines $a_p = p + 1 - |E_{ns}(\mathbf{F}_p)|$. These numbers are encoded in the L-function of E which is defined as

$$L(s, E) = \prod_{p|N_E} (1 - \frac{a_p}{p^s})^{-1} \prod_{p \not| N_E} (1 - \frac{a_p}{p^s} + \frac{1}{p^{2s-1}})^{-1}$$

where N_E, the conductor of E which we do not define precisely here, is divisible by only the bad primes. One can similarly define the L-function of an elliptic curve defined over a number field K. The analogue of the Hasse inequality is

$$|a_v| \leq 2\sqrt{N(v)}$$

where $N(v)$ is the norm of the prime ideal v. Writing $a_v = 2\sqrt{N(v)}Cos(\theta_v)$, there is a conjecture due to Sato & Tate which predicts how the angles θ_v are distributed as v varies. When E has CM (complex multiplication) - which means that there are group endomorphisms of E other than 'raising to an integral power' - Hecke already showed that uniform distribution theorem of Hermann Weyl holds good for the angles in the interval $[0, \pi]$. On the other hand, when E does not have CM, such a uniform distribution theorem does not hold good for the angles with respect to the usual Lebesgue measure but Sato-Tate conjecture predicts that it does hold good with respect to the measure $\frac{2}{\pi}Sin^2(\theta)d\theta$.
A strengthened form of the Sato-Tate conjecture due to Akiyama & Tanigawa predicts :
the number of prime ideals v with norms at the most x and $\theta_v \in (\alpha, \beta)$ is asymptotic (as $x \to \infty$) to $(\frac{2}{\pi}\int_\alpha^\beta Sin^2(\theta)d\theta)\pi_K(x)$ with an error term $O(x^{1/2+\epsilon})$.
This conjecture implies the truth of RH for all the L-functions :

$$L_n(s) = \prod_{p \not| N_E} \prod_{j=0}^{n} (1 - \frac{e^{i(n-2j)\theta_p}}{p^s})^{-1}.$$

These latter L-functions come from modular forms which we discuss now.

L-functions of modular forms

Consider a positive integer N and a Dirichlet character χ mod N. We look at the vector space $S_k(\Gamma_0(N), \chi)$ of cusp forms of type (k, χ). Any element f here satisfies the transformation formula

$$f(\frac{az+b}{cz+d}) = \chi(d)(cz+d)^k f(z)$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, and is a holomorphic function on the upper half-plane as well as on all the cusps. In particular, any such f satisfies $f(z+1) = f(z)$ and thus, at $i\infty$, it has a Fourier expansion $f(z) = \sum_{n=1}^{\infty} a_n q^n$ where $q = e^{2i\pi z}$. One defines the L-function of f as

$$L(s, f) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Using the theory of the so-called Hecke operators, Hecke proved that for any $f \in S_k(\Gamma_0(N))$, the L-function $L(s, f)$ extends to an entire function and satisfies a functional equation with a symmetry $s \leftrightarrow k - s$. He also proved that the L-function has an Euler product

$$L(s, f) = \prod_{p|N} (1 - \frac{a_p}{p^s})^{-1} \prod_{p \not| N} (1 - \frac{a_p}{p^s} + \frac{\chi(p)}{p^{2s+1-k}})^{-1}$$

which converges for $Re(s) > (k+2)/2$, if and only if, f is a (normalized) common eigenform for all the Hecke operators.

Ramanujan-Petersson and Selberg conjectures

In its simplest form, this is the conjecture that the Fourier coefficients $a_n(f)$ of a normalized Hecke eigenform of weight k for $SL_2(\mathbf{Z})$ satisfies $|a_p(f)| \leq 2p^{\frac{k-1}{2}}$ for every prime p. Hecke's work shows that the Fourier coefficients $a_n(f)$ are just the eigenvalues for the Hecke operators T_n. This conjecture is therefore an analogue of the RH, and was proved by Deligne in the work on Weil conjectures alluded to earlier. The analogue of the Ramanujan-Petersson conjecture for Maass forms (that is, forms where the holomorphy assumption is dropped) is the assertion that $a_n(f) = O(n^\epsilon)$ for each $\epsilon > 0$. This is still open. Later, we will mention a much more general version of the conjecture. In a seemingly unrelated work, Selberg made a conjecture. If a Maass form $f(z)$ for $\Gamma_0(N)$ - viewed as a function of two real variables x, y - is an eigenfunction for the non-Euclidean Laplacian $\Delta = -y^2(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2})$, Selberg conjectured that the corresponding non-zero eigenvalues λ ($\lambda = 0$ corresponds to a holomorphic form) satisfy $\lambda > \frac{1}{4}$. Selberg proved this for $SL_2(\mathbf{Z})$ and, in the case of general N, he proved the weaker lower bound $\frac{3}{16}$. The general conjecture is still open. The adelic formalism of Satake shows that the Ramanujan-Petersson conjecture and the Selberg conjecture are two sides of the same coin - the latter may be thought of as an archimedean analogue of the former. Both conjectures could be unified as an adelic formulation of the Ramanujan-Petersson conjecture which will be discussed below.

Eichler-Shimura correspondence and Taniyama-Shimura-Weil conjecture

If $f \in S_2(\Gamma_0(N))$, it is clear that the differential form $f(z)dz$ is invariant under $\Gamma_0(N)$. Then, for any fixed point z_0 on the upper half-plane, the integral $\int_{z_0}^{z} f(z)dz$ is independent of the path joining z_0 to z. Thus, for any $\gamma \in \Gamma_0(N)$, there is a well-defined function

$$\gamma \mapsto \Phi_f(\gamma) = \int_{z_0}^{\gamma(z_0)} f(z)dz.$$

It is also easy to see that this function does not depend on the choice of z_0.
Theorem (Eichler-Shimura) :
When f is a normalized newform with integer coefficients, the set $\{\Phi_f(\gamma)\}$ as γ varies, forms a lattice Λ_f in $\mathbf{C}$. There is an elliptic curve E_f defined over $\mathbf{Q}$ which becomes isomorphic to the complex torus $\mathbf{C}/\Lambda_f$ over $\mathbf{C}$. Moreover $L(s, E_f) = L(s, f)$.
The converse result that every elliptic curve E over $\mathbf{Q}$ comes from a modular form of weight 2 for $\Gamma_0(N_E)$ as above was conjectured by Taniyama-Shimura-Weil and is now a famous theorem of Taylor and Wiles for square-free N and of Breuil, Conrad, Diamond & Taylor for other N.

Weil's converse theorem

This is the basic method used to prove any of the theorems that underlies the Langlands philosophy. The latter roughly is the idea that all sorts of L-functions arising 'geometrically' are L-functions of certain modular forms. The results of Weil we are talking about is :
Weil's converse theorem :
Let $\{a_n\}$ be a sequence of complex numbers such that $a_n = O(n^c)$ for some constant $c > 0$. Fix a natural number N, an even natural number k and a sign ϵ. Assume :
(i) $\Lambda(s) = N^{s/2}(2\pi)^{-s}\Gamma(s)\sum_n \frac{a_n}{n^s}$ is an entire function which is bounded in vertical strips,
(ii) $\Lambda(s) = \epsilon(-1)^{k/2}\Lambda(k-s)$,
(iii) for each $(m, N) = 1$, and every primitive character χ,

$$\Lambda_\chi(s) = (m^2N)^{s/2}(2\pi)^{-s}\Gamma(s)\sum_n \frac{a_n\chi(n)}{n^s}$$

is entire and bounded in vertical strips,
(iv) $\Lambda_\chi(s) = \epsilon(-1)^{k/2}\chi(-N)\frac{T(\chi)}{T(\bar{\chi})}\Lambda_{\bar{\chi}}(k-s)$,
where $T(\chi) = \sum_{l(mod\ m)} \chi(l)e^{2i\pi l/m}$ and
(v) $\sum \frac{a_n}{n^s}$ converges absolutely at $s = k - \delta$ for some $\delta > 0$.
Then, $f(z) = \sum a_n e^{2i\pi nz}$ is a cusp form in $S_k(\Gamma_0(N))$.

Artin L-functions

Now, we introduce one of the most interesting L-functions. Let L/K be a Galois extension of number fields with Gal $(L/K) = G$, say. For a prime ideal P of

$\mathcal{O}_K$, write

$$P\mathcal{O}_L = (P_1 P_2 \cdots P_g)^e$$

with P_i prime ideals. Consider the decomposition groups

$$D_{P_i} = \{\sigma \in G : \sigma(P_i) = P_i\}.$$

They are all conjugate. Also, there is a surjective natural homomorphism to the Galois group of the residue field extension

$$D_{P_i} \to Gal(\frac{\mathcal{O}_L/P_i}{\mathcal{O}_K/P})$$

whose kernel is the inertia group I_{P_i}. The inertia groups are trivial if P is unramified in L (that is, if $e = 1$) - something which happens for all but finitely many prime ideals P. As the Galois group of an extension of finite fields is cyclic with a distinguished generator, the Frobenius automorphism, there is a conjugacy class σ_P in G corresponding to any unramified prime ideal P. This is also called the Frobenius conjugacy class or the Artin symbol of P.
Whenever one has a finite-dimensional complex representation of G, say, $\rho : G \to GL(V)$, Artin attached an L-function defined by

$$L(s, \rho; L/K) = \prod_P det(1 - \rho(\sigma_P)N(P)^{-s}|V^{I_P})^{-1}$$

where V^{I_P}, the subspace fixed by I_P is acted on by the conjugacy class σ_P. Artin showed that these L-functions have nice properties like invariance under the induction of representations. He also posed :
Artin's Conjecture :
$L(s, \rho; L/K)$ extends to an entire function when the character of ρ does not contain the trivial character.
Thus, essentially the pole of a Dedekind zeta function ought to come from that of the Riemann zeta function. Artin's conjecture is still open although it has been proved in a few cases. A consequence of Artin's reciprocity law is the statement (weaker than Artin's conjecture) that these L-functions extend to meromorphic functions for any s.

Automorphic L-functions and Langlands program

The whole point of view ever since Artin defined his L-functions shifted to viewing everything in the powerful language of representation theory. Classical modular forms for subgroups of $SL_2(\mathbf{Z})$ started to be viewed as representations of $SL_2(\mathbf{R})$. More generally, representations of adele groups (to be defined below) surfaced as the principal objects of study. We have already alluded to the fact that Ramanujan-Petersson conjecture and Selberg conjecture could be unified in the adelic framework. In fact, we also mentioned in passing that Tate's thesis afforded the first understanding of why the Gamma factors appeared in the functional equation for the Riemann zeta function. Let us describe the adelic

setting briefly now.
A basic understanding now is that to do number theory (to 'know' $\mathbf{Q}$) or any algebraic number field K is to look at all possible notions of distance on K. For example, the usual notion of distance on $\mathbf{Q}$ as a subset of $\mathbf{R}$ keeps the number theory of $\mathbf{Q}$ hidden. If p is a prime number, there is a 'p-adic distance' defined as $|x-y|_p = p^{-ord_p(x-y)}$, where $ord_p(p^t a/b) = t$ for any non-zero rational number $p^t a/b$ where a, b are indivisible by p. One takes $\mathrm{Ord}_p(0) = \infty$ and $|0|_p = 0$. So, a number which is divisible by a high power of p is close to zero in this distance ! Our usual intuition based on the geometry of Euclidean spaces takes a beating here - for instance, every triangle is isoceles, every point inside a disc is its center etc. ! This is because the p-adic distance has the property that it is nonarchimedean (that is, $|x-y|_p \leq max(|x-z|_p, |z-y|_p)$ for any x, y, z); in particular, $|nx| = |x|$ for all natural numbers n. So, given x, y with $|x|_p < |y|_p$, one cannot choose n such that $|nx|_p$ is bigger than $|y|_p$. Ostrowski showed that the possible distinct notions of distance on $\mathbf{Q}$ are the usual archimedean one coming from $\mathbf{R}$ and the p-adic ones for primes p. Also, just as $\mathbf{R}$ is constructed from $\mathbf{Q}$ by a process of completion with respect to the usual distance, there are p-adic completions of $\mathbf{Q}$ to which the notion of p-adic distance extends. These are fields called the p-adic numbers $\mathbf{Q}_p$. They are locally compact like $\mathbf{R}$ is. But, they are different (much nicer !) from $\mathbf{R}$ in many ways. The nonarchimedeanness shows, for example, that a series in $\mathbf{Q}_p$ converges if and only if the terms converge to 0. Unlike $\mathbf{R}$, there is a subring of $\mathbf{Q}_p$ is called the p-adic integers which form a compact subset. Akin to viewing real numbers as decimals, one may think of $\mathbf{Q}_p$ as consisting formally of series of the form $\sum_{n=-r}^{\infty} a_n p^n$ where r is an integer and the 'digits' a_n's are between 0 and $p-1$. While adding and multiplying such numbers, one adds them and multiplies as if they were formal series but one has to rewrite the expressions so that the resulting expression has digits between 0 and $p-1$. The p-adic integers $\mathbf{Z}_p$ can be thought of as those series which have no terms of negative degree. Note that $\mathbf{Q}_p = \bigcup_{n \geq 1} p^n \mathbf{Z}_p$. The p-adic integers is also the closure of $\mathbf{Z}$ in $\mathbf{Q}_p$ for the p-adic completion.
More generally, for any number field K (with ring of integers $\mathcal{O}$), one has the P-adic completion for each prime ideal of $\mathcal{O}$. The point is that every ideal is uniquely a product of prime ideals even if a similar unique decomposition does not hold good for elements of $\mathcal{O}$. These P-adic topologies are nonarchimedean and are all mutually inequivalent. There are also $[K : \mathbf{Q}]$ archimedean distance functions on K extending the usual one on $\mathbf{Q}$ although some of them may be equivalent. The inequivalent ones are called places of K. It is in this regard that Tate's thesis tells us that the Gamma factors in the functional equation for $\zeta_K(s)$ are 'Euler factors' corresponding to the archimedean places of K. If v is a place of K, the completion K_v is a locally compact field - it is $\mathbf{R}$ or $\mathbf{C}$ when v is archimedean and a finite extension field of $\mathbf{Q}_p$ when v corresponds to a prime ideal P and $P \cap \mathbf{Z} = p\mathbf{Z}$. The closure of $\mathcal{O}$ in K_v is a compact subring $\mathcal{O}_{\sqsubseteq}$ when v is nonarchimedean. The best way to study K is to introduce the adele ring $\mathbf{A}_K$ of K which is a certain locally compact ring. The adele ring of K is defined as the set of all tuples $(x_v)_v$ with $x_v \in K_v$ where all but finitely many of the x_v are in $\mathcal{O}_v$. Note that for any $x \in K$, the 'diagonal embedding' $(x, x, \cdots)$ is

in $\mathbf{A}_K$. To define the topology on adeles, consider any finite set S of places of K containing all the archimedean ones. The product ring $\prod_{v\in S} K_v \times \prod_{v\notin S} \mathcal{O}_v$ is locally compact as S is finite. As S varies, these products form a basis of neighbourhoods of zero for a unique topology on $\mathbf{A}_K$ for which it is locally compact. The addition and multiplication on $\mathbf{A}_K$ are continuous functions for the adelic topology. The diagonal embedding $x \mapsto (x, x, \cdots,)$ maps K as a discrete subgroup of $\mathbf{A}_K$.
A natural way to arrive at the adeles is via harmonic analysis. For example, if the abelian group $\mathbf{Q}$ *is regarded with discrete topology, then the compact abelian group which is dual to it (its group of continuous characters) can be computed from first principles. It turns out to be the quotient group* $\mathbf{A}_{\mathbf{Q}}/\mathbf{Q}$. *Here* $\mathbf{Q}$ *is viewed via its diagonal embedding. The situation is a generalization of the duality between* $\mathbf{Z}$ *and* $\mathbf{R}/\mathbf{Z}$.
More generally, when we have a matrix group like $GL_n(K)$ (or more generally an algebraic subgroup $G \subset GL_n$ defined over K), one can naturally consider the groups $G(K_v)$ and $G(\mathcal{O}_v)$ for all places v of K. The groups $GL_n(K_v)$ are locally compact and although $GL_n(\mathcal{O}_v)$ is not compact, it is compact modulo the scalar matrices. In particular, one has the 'adelic group' $G(\mathbf{A}_K)$ which has a basis of neighbourhoods of the identity given by $\prod_{v\in S} G(K_v) \times \prod_{v\notin S} G(\mathcal{O}_v)$ as S varies over finite sets of places containing all the archimedean places of K. The diagonal embedding of $G(K)$ in $G(\mathbf{A}_K)$ embeds it as a discrete subgroup. Unlike $\mathbf{A}_K/K$ which is compact, the quotient space $GL_n(\mathbf{A}_K)/GL_n(K)$ (not a group) is not compact; it does not even have finite 'measure' for a Haar measure of the adele group. However, the finiteness of measure holds modulo the group $Z = \{diag(t, t, \cdots, t) \in GL_n(\mathbf{A}_K)\}$ of scalar matrices in $GL_n(\mathbf{A}_K)$.

Therefore, for a Grossencharacter ω (a character of the group $GL_1(\mathbf{A}_K)/GL_1(K)$), it makes sense to consider the following Hilbert space consisting of measurable functions on the quotient space $GL_n(\mathbf{A}_K)/GL_n(K)$ with certain properties which remind us of transformation properties of modular forms. This is the Hilbert space $L^2(GL_n(\mathbf{A}_K)/GL_n(K), \omega)$ of those measurable functions ϕ which satisfy :
(i) $\phi(zg) = \omega(z)\phi(g), z \in Z$,
(ii) $\int_{GL_n(\mathbf{A}_K)/Z.GL_n(K)} |\phi(g)|^2 dg < \infty$.

The subspace $L^2_0(GL_n(\mathbf{A}_K)/GL_n(K), \omega)$ of cusp forms is defined by the additional conditions corresponding to any parabolic subgroup. The latter are conjugates in GL_n of 'ladder' groups of the form $P_{n_1,\cdots,n_r} = \{ \begin{pmatrix} g_1 & \cdots & \cdots & \\ 0 & g_2 & \cdots & \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & g_r \end{pmatrix} \}$ where g_i is an $n_i \times n_i$ invertible matrix. The standard parabolic $P_{n_1,\cdots,n_r}$ is a

semidirect product of its unipotent radical $U = \{ \begin{pmatrix} I_{n_1} & \cdots & \cdots & \\ 0 & I_{n_2} & \cdots & \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & I_{n_r} \end{pmatrix} \}$ and $GL_{n_1} \times \cdots \times GL_{n_r}$. Any parabolic subgroup P has a similar semidirect product decomposition $P = M \propto U$. The parabolic subgroups are characterized by the condition that they are closed subgroups such that $GL_n(\mathbf{C})/P(\mathbf{C})$ is compact. The additional 'cuspidality' condition for a parabolic subgroup P is

$$\int_{U_P(\mathbf{A}_K)/U_P(K)} \phi(ug)du = 0 \ \ \forall \ \ g \in GL_n(\mathbf{A}_K).$$

The adele group acts as unitary operators by right multiplication on the Hilbert space $L^2(GL_n(\mathbf{A}_K)/GL_n(K), \omega)$. It leaves the space of cusp forms invariant. By definition, a subquotient of this representation is called *an automorphic representation* of $GL_n(\mathbf{A}_K)$. Moreover, a subrepresentation of the representation on cusp forms is said to be a *cuspidal automorphic representation.* One further notion is that of an *admissible* representation of the adele group - this is one which can contain any irreducible representation of a maximal compact subgroup of the adele group only finitely many times. It is a theorem of D.Flath which tells us that any irreducible, admissible representation of the adele group is a 'restricted' tensor product of unique irreducible representations of $GL_n(K_v)$. Further, for an admissible automorphic representation $\pi = \otimes_v \pi_v$, the representation π_v belongs to a special class known as the unramified principal series for all but finitely many v. An unramified principal series representation π_v is one whose restriction to $GL_n(\mathcal{O}_v)$ contains the trivial representation; a certain isomorphism theorem due to Satake shows that corresponding to π_v, there is a conjugacy class in $GL_n(\mathbf{C})$ of a diagonal matrix of the form

$$A_v = diag(N(v)^{-z_1}, \cdots, N(v)^{-z_n})$$

for some n-tuple $(z_1, \cdots, z_n) \in \mathbf{C}^n$.
Corresponding to an admissible, automorphic representation $\pi = \otimes_v \pi_v$, Langlands defined an L-function. If S is the finite set of places outside of which π_v is unramified principal series, define for $v \notin S$,

$$L(s, \pi_v) = det(1 - A_v N(v)^{-s})^{-1}.$$

If $L_S(s, \pi) := \prod_{v \notin S} L(s, \pi_v)$, then Langlands proved that this product has a meromorphic extension to the whole complex plane. Defining $L(s, \pi_v)$ for $v \in S$ in a suitable manner, it also follows that $L(s, \pi) = \prod_v L(s, \pi_v)$ has meromorphic continuation, and a functional equation. If π is cuspidal also, then Godement & Jacquet showed that $L(s, \pi)$ is an entire function unless $n = 1$ and $\pi = |.|^t$ for some $t \in \mathbf{C}$.
Ramanujan-Petersson conjecture :
If π is cuspidal automorphic, then the eigenvalues of A_v have absolute value 1 for all v. Equivalently, for such a π, the matrix coefficients of π_v, for each

prime p, belongs to $L^{2+\epsilon}(GL_n(\mathbf{Q}_p)/Z(\mathbf{Q}_p))$ *for any* $\epsilon > 0$.
Note that Selberg conjecture can be interpreted as asserting that π_∞ is a tempered representation of $GL_n(\mathbf{R})$.

Langlands Reciprocity conjecture :
Let L/K *be a Galois extension of number fields and let* G *be the Galois group. Let* (ρ, V) *be an* n*-dimensional complex representation of* G*. Then, there is a cuspidal automorphic representation* π *of* $GL_n(\mathbf{A}_K)$ *such that* $L(s, \rho; L/K) = L(s, \pi)$.

This is just Artin's reciprocity law (a theorem!) when ρ is 1-dimensional. There are also other conjectures of Langlands which imply that the automorphic L-functions multiplicatively generate all the L-functions like the Dedekind zeta functions, Hasse-Weil zeta functions etc. One has :
Grand Riemann Hypothesis
All the zeroes of $L(s, \pi)$ *for a cuspidal automorphic representation* π*, lie on* $Re(s) = 1/2$.
The Grand Riemann Hypothesis has several concrete number-theoretic consequences. For instance, it implies the Artin primitive root conjecture which asserts that any non-square $a \neq -1$ is a primitive root for infinitely many primes.

Selberg's Program

For what general L-functions can the RH be formulated meaningfully ? The final section discusses this and it is a program started by Selberg. One defines the *Selberg class* $\mathcal{S}$ consisting of those complex functions $F(s)$ which satisfy the following hypotheses :
(i) $F(s) = 1 + \sum_{n \geq 2} \frac{a_n}{n^s}$ for $Re(s) > 1$.
(ii) $F(s)$ has a meromorphic continuation to the whole complex plane and there is some m so that $(s-1)^m F(s)$ is holomorphic of finite order.
(iii) There are positive real Q, α and complex r_i with $Re(r_i) > 0$ and a complex number w of absolute value 1 such that the function

$$\Phi(s) := Q^s F(s) \prod_{i=1}^{d} \Gamma(\alpha_i s + r_i)$$

satisfies the functional equation

$$\Phi(s) = w\overline{\Phi(1 - \bar{s})}.$$

(iv) $F(s) = \prod_p exp(\sum_{k=1}^{\infty} b_{p^k} p^{-ks})$ with $b_{p^k} = O(p^{k\theta})$ for some $\theta < 1/2$.
(v) (**Ramanujan/Riemann Hypothesis**) For any $\epsilon > 0$, one has $a_n = O(n^\epsilon)$.

It is an expectation that the class of funcions satisfying the first 4 axioms automatically satisfy the fifth. If this turns out to be true, then we would have a characterization of all Dirichlet series for which the Riemann Hypothesis holds

good.
All the familiar L-functions studied so far are in the Selberg class or are conjectured to be so. Any function in the Selberg class can be factorized into 'primitive' functions - this is a theorem due to Selberg, Conrey and Ghosh. Selberg predicted a certain type of orthonormal system in $\mathcal{S}$; this has consequences like the uniqueness of the factorization into primitives !

Selberg's Conjecture :
For any primitive function $F \in \mathcal{S}$, one has

$$\sum_{p \leq x} \frac{|a_p(F)|^2}{p} = log\ log\ x + O(1).$$

For primitive functions $F \neq G \in \mathcal{S}$, one has

$$\sum_{p \leq x} \frac{a_p(F)\overline{a_p(G)}}{p} = O(1).$$

Artin's conjecture on the entirety of the Artin L-functions is a consequence of the Selberg conjectures. There are quite a few results in operator theory and noncommutative geometry related to the theme of Riemann Hypothesis that we have not touched upon but that is inevitable as must be with a fundamental theme as this. In conclusion, one might say that the Riemann Hypothesis really is not an isolated problem whose solution is an end in itself but a beacon which shines its light on all of mathematics, generating new and beautiful byproducts.