Analytic number theory for probabilists

E. Kowalski

ETH Zürich

27 October 2008

Je crois que je l'ai su tout de suite : je partirais sur le Zéta, ce serait mon navire Argo, celui qui me conduirait à la travers la mer jusqu'au lieu dont j'avais rêvé, à Rodrigues, pour ma quête d'un trésor sans fin.

J.M.G Le Clézio, "Le chercheur d'or".

I think I knew it immediately: I would sail on the Zeta, it would be my own Argo, the one that would bring me across the sea to the place I had dreamed of, to Rodrigues, for my quest of a treasure without bounds.

J.M.G Le Clézio, "The prospector".

Outline

This is an introduction for the probabilist audience and other non-specialists. As such, it is probably heretical for the true analytic number theorists.

Outline

This is an introduction for the probabilist audience and other non-specialists. As such, it is probably heretical for the true analytic number theorists.

1. Probabilistic interpretations of common patterns in analytic number theory;
2. Introducing L-functions;
3. Introducing modular forms;
4. Introducing elliptic curves.

Elements of analytic number theory

Analytic number theory is often concerning with understanding some properties of (arithmetical) objects in a statistic sense, and this can frequently be understood in probabilistic terms. These typically involve asymptotic considerations that can be seen as analogues of limits of random variables.

Elements of analytic number theory

Analytic number theory is often concerning with understanding some properties of (arithmetical) objects in a statistic sense, and this can frequently be understood in probabilistic terms. These typically involve asymptotic considerations that can be seen as analogues of limits of random variables.

Example (Counting primes)

The function

$$\pi(X) = |\{n \leq X \mid n \text{ is prime}\}|$$

counts primes up to X. The Prime Number Theorem states

$$\pi(X) \sim \frac{X}{\log X} \text{ as } X \to +\infty,$$

which is often summarized as saying the the probability of an integer $n \simeq X$ being prime is about $1/\log X$.

Primes in progressions

Example (Primes in progressions)

Let $q \geq 1$ be an integer, and a a non-zero integer; let

$$\pi(X; q, a) = |\{p \leq X \mid p \equiv a \pmod{q}\}|.$$

Primes in progressions

Example (Primes in progressions)

Let $q \geq 1$ be an integer, and a a non-zero integer; let

$$\pi(X; q, a) = |\{p \leq X \mid p \equiv a \pmod{q}\}|.$$

Consider reduction modulo q:

$$\mathbf{Z} \xrightarrow{\rho_q} \mathbf{Z}/q\mathbf{Z}.$$

Dirichlet's Theorem, in quantitative form, states that if $(a, q) = 1$, we have

$$\pi(X; q, a) \sim \frac{1}{\varphi(q)} \pi(X), \text{ as } X \to +\infty.$$

Primes in progressions

Example (Primes in progressions)

Let $q \geq 1$ be an integer, and a a non-zero integer; let

$$\pi(X; q, a) = |\{p \leq X \mid p \equiv a \pmod q\}|.$$

Consider reduction modulo q:

$$\mathbf{Z} \xrightarrow{\rho_q} \mathbf{Z}/q\mathbf{Z}.$$

Dirichlet's Theorem, in quantitative form, states that if $(a, q) = 1$, we have

$$\pi(X; q, a) \sim \frac{1}{\varphi(q)} \pi(X), \text{ as } X \to +\infty.$$

In other words: the image under ρ_q of the normalized counting measure on $\{p \leq X\}$ converges in law, as $X \to +\infty$, to the normalized counting measure on $(\mathbf{Z}/q\mathbf{Z})^\times$.

(cont.)

In fact, one can show (Siegel-Walfisz Theorem) that the convergence above is uniform for $q \leq (\log X)^A$, for any constant $A > 0$.

(cont.)

In fact, one can show (Siegel-Walfisz Theorem) that the convergence above is uniform for $q \leq (\log X)^A$, for any constant $A > 0$.
Extending this uniformity is an outstanding problem and is directly linked to the *Generalized Riemann Hypothesis*, which is equivalent with the statement

$$\pi(X; q, a) = \frac{1}{\varphi(q)} \int_2^X \frac{dt}{\log t} + O(\sqrt{X}(\log qX)^2)$$

for $X \geq 2$ and $(a, q) = 1$.

Fairly typical setting(s)

(1) A collection of (often) finite sets Ω_X with counting measure (or another probability measure), depending on a parameter $X \to +\infty$;

Fairly typical setting(s)

(1) A collection of (often) finite sets Ω_X with counting measure (or another probability measure), depending on a parameter $X \to +\infty$;
(2) Invariants ("random variables") defined on Ω_X, for which we wish to understand the distribution;

Fairly typical setting(s)

(1) A collection of (often) finite sets Ω_X with counting measure (or another probability measure), depending on a parameter $X \to +\infty$;
(2) Invariants ("random variables") defined on Ω_X, for which we wish to understand the distribution;
(3) Both Ω_X and the invariants have some *arithmetic* significance...

Fairly typical setting(s)

(1) A collection of (often) finite sets Ω_X with counting measure (or another probability measure), depending on a parameter $X \to +\infty$;
(2) Invariants ("random variables") defined on Ω_X, for which we wish to understand the distribution;
(3) Both Ω_X and the invariants have some *arithmetic* significance...
(3.1) ... which may be revealed by the possibility of local-global considerations: reduction modulo primes give "local" information

$$\Omega_X \xrightarrow{\rho_p} Y_p$$

and one tries to leverage this local information over all primes...

Fairly typical setting(s)

(1) A collection of (often) finite sets Ω_X with counting measure (or another probability measure), depending on a parameter $X \to +\infty$;
(2) Invariants ("random variables") defined on Ω_X, for which we wish to understand the distribution;
(3) Both Ω_X and the invariants have some *arithmetic* significance...
(3.1) ... which may be revealed by the possibility of local-global considerations: reduction modulo primes give "local" information

$$\Omega_X \xrightarrow{\rho_p} Y_p$$

and one tries to leverage this local information over all primes...
(3.2) ... using very often the fact that ρ_p is well-distributed for a fixed p as $X \to +\infty$, uniformly in p,...

Fairly typical setting(s)

(1) A collection of (often) finite sets Ω_X with counting measure (or another probability measure), depending on a parameter $X \to +\infty$;
(2) Invariants ("random variables") defined on Ω_X, for which we wish to understand the distribution;
(3) Both Ω_X and the invariants have some *arithmetic* significance...
(3.1) ... which may be revealed by the possibility of local-global considerations: reduction modulo primes give "local" information

$$\Omega_X \xrightarrow{\rho_p} Y_p$$

and one tries to leverage this local information over all primes...
(3.2) ... using very often the fact that ρ_p is well-distributed for a fixed p as $X \to +\infty$, uniformly in p,...
(3.3) ... and "nearly" independent for p in a suitable range ("level of distribution" in sieve theory).

Example 1

1. $\Omega_X = \{n \leq X\}$, with counting measure;

Example 1

1. $\Omega_X = \{n \leq X\}$, with counting measure;
2. ρ_p is reduction modulo p;

Example 1

1. $\Omega_X = \{n \leq X\}$, with counting measure;
2. ρ_p is reduction modulo p;
3. Equidistribution modulo p:

$$\begin{aligned}\mathbf{P}_X(n \equiv a \pmod p) &= \frac{1}{|\Omega_X|}|\{n \leq X \mid n \equiv a \pmod p\}| \\ &= \frac{1}{p} + O(X^{-1}) \to \frac{1}{p} \text{ as } X \to +\infty;\end{aligned}$$

Example 1

1. $\Omega_X = \{n \leq X\}$, with counting measure;
2. ρ_p is reduction modulo p;
3. Equidistribution modulo p:

$$\begin{aligned}\mathbf{P}_X(n \equiv a \pmod{p}) &= \frac{1}{|\Omega_X|}|\{n \leq X \mid n \equiv a \pmod{p}\}| \\ &= \frac{1}{p} + O(X^{-1}) \to \frac{1}{p} \text{ as } X \to +\infty;\end{aligned}$$

4. ρ_{p_1}, ρ_{p_2} are "independent" on $\mathbf{Z}$: Chinese Remainder Theorem;

Example 1

1. $\Omega_X = \{n \leq X\}$, with counting measure;
2. ρ_p is reduction modulo p;
3. Equidistribution modulo p:

$$\mathbf{P}_X(n \equiv a \pmod{p}) = \frac{1}{|\Omega_X|}|\{n \leq X \mid n \equiv a \pmod{p}\}|$$
$$= \frac{1}{p} + O(X^{-1}) \to \frac{1}{p} \text{ as } X \to +\infty;$$

4. ρ_{p_1}, ρ_{p_2} are "independent" on $\mathbf{Z}$: Chinese Remainder Theorem;
5. *Approximate* independence by combining the last two facts.

Example 2 (Erdös-Kác Theorem)

Define "random variables"

$$\omega_X : \begin{cases} \Omega_X \to \mathbf{N} \\ n \mapsto \omega(n) = \text{number of distinct primes } p \mid n. \end{cases}$$

Example 2 (Erdös-Kác Theorem)

Define "random variables"

$$\omega_X : \begin{cases} \Omega_X \to \mathbf{N} \\ n \mapsto \omega(n) = \text{number of distinct primes } p \mid n. \end{cases}$$

Theorem (Erdös-Kác)

As $X \to +\infty$, we have

$$\mathbf{P}_X\Big(\frac{\omega_X - \log\log X}{\sqrt{\log\log X}}\Big) \to \frac{1}{\sqrt{2\pi}} \int_\alpha^\beta e^{-t^2/2} dt.$$

Example 2 (Erdös-Kác Theorem)

Define "random variables"

$$\omega_X \ : \begin{cases} \Omega_X \to \mathbf{N} \\ n \mapsto \omega(n) = \text{number of distinct primes } p \mid n. \end{cases}$$

Theorem (Erdös-Kác)

As $X \to +\infty$, we have

$$\mathbf{P}_X\Big(\frac{\omega_X - \log\log X}{\sqrt{\log\log X}}\Big) \to \frac{1}{\sqrt{2\pi}} \int_\alpha^\beta e^{-t^2/2} dt.$$

Same limit as for sums of random variables $\sum_{p \leq X} B_p$, where (B_p) are independent Bernoulli random variables with $\mathbf{P}(B_p = 1) = p^{-1}$, but *mod-Poisson convergence* can distinguish the two.

Example 3 (Gaps between primes)

With the same Ω_X, consider random variables

$$\begin{aligned} G_{X,c}(n) &= \pi(n + c \log n) - \pi(n) \\ &= (\text{number of primes between } n \text{ and } n + c \log n). \end{aligned}$$

Example 3 (Gaps between primes)

With the same Ω_X, consider random variables

$$\begin{aligned} G_{X,c}(n) &= \pi(n + c\log n) - \pi(n) \\ &= (\text{number of primes between } n \text{ and } n + c\log n). \end{aligned}$$

Conjecture

For any fixed $c > 0$, we have:

$$G_{X,c} \xrightarrow{law} Poisson(c)$$

as $X \to +\infty$.

Example 3 (Gaps between primes)

With the same Ω_X, consider random variables

$$\begin{aligned} G_{X,c}(n) &= \pi(n + c\log n) - \pi(n) \\ &= (\text{number of primes between } n \text{ and } n + c\log n). \end{aligned}$$

Conjecture

For any fixed $c > 0$, we have:

$$G_{X,c} \xrightarrow{law} \mathit{Poisson}(c)$$

as $X \to +\infty$.

Strong heuristic evidence from sieve methods and Hardy-Littlewood conjecture (Gallagher). Extends to gaps between twin primes, etc.

L-functions

L-functions were invented by Dirichlet and generalized by many people (Hecke, Maass, Langlands in particular) as the "right" tools of harmonic analysis to detect many arithmetic conditions, such as:

1. Arithmetic progressions: $n \equiv a \pmod q$ (*Dirichlet L-functions*);
2. Determinant relations: $ax - by = h$ (*automorphic L-functions* of degree 2).

L-functions

L-functions were invented by Dirichlet and generalized by many people (Hecke, Maass, Langlands in particular) as the "right" tools of harmonic analysis to detect many arithmetic conditions, such as:

1. Arithmetic progressions: $n \equiv a \pmod q$ (*Dirichlet L-functions*);
2. Determinant relations: $ax - by = h$ (*automorphic L-functions* of degree 2).

They are holomorphic functions with, *among other properties*, an Euler product ("local-global") expression:

$$L(s) = \sum_{n \geq 1} \lambda(n) n^{-s} = \prod_p L_p(p^{-s})^{-1}$$

where $L_p \in \mathbf{C}[X]$ with $L_p(0) = 1$.

(cont.)

Example

The Riemann zeta function is

$$\zeta(s) = \sum_{n \geq 1} n^{-s} = \prod_{p} (1 - p^{-s})^{-1}.$$

(cont.)

Example

The Riemann zeta function is

$$\zeta(s) = \sum_{n \geq 1} n^{-s} = \prod_p (1 - p^{-s})^{-1}.$$

It is meromorphic on $\mathbf{C}$ with a single pole with residue 1 at $s = 1$, and satisfies a *functional equation*

$$\Lambda(s) = \Lambda(1 - s), \quad \text{where} \quad \Lambda(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s).$$

Functional equation

These other properties extend to other L-functions, with a more general functional equation:

$$\Lambda(L,s) = e^{i\theta(L)} q(L)^{1/2-s} \Lambda(\bar{L}, 1-s), \quad \Lambda(L,s) = \gamma(L,s)L(s),$$

where $q(L) \geq 1$ is the *conductor* of $L(s)$, $e^{i\theta(L)}$ is the *sign/argument* of the functional equation, $\gamma(L,s)$ is the gamma/archimedean factor and

$$\bar{L}(s) = \sum_{n\geq 1} \overline{\lambda(n)} n^{-s}.$$

Zeros of L-functions

The logarithmic derivatives of L-functions may be used to control the distribution of *primes*. Thus the location of their zeros is extremely important as they give singularities of L'/L.

Zeros of L-functions

The logarithmic derivatives of L-functions may be used to control the distribution of *primes*. Thus the location of their zeros is extremely important as they give singularities of L'/L.
This can be seen in the *explicit formula*:

$$\sum_{p \le X} \log p = X - \sum_{\rho} \frac{X^{\rho}}{\rho} + (\text{small term})$$

where ρ runs over the zeros of $\zeta(s) = 0$ with $0 < \mathrm{Re}(\rho) < 1$.

Zeros of L-functions

The logarithmic derivatives of L-functions may be used to control the distribution of *primes*. Thus the location of their zeros is extremely important as they give singularities of L'/L.
This can be seen in the *explicit formula*:

$$\sum_{p \le X} \log p = X - \sum_{\rho} \frac{X^{\rho}}{\rho} + (\text{small term})$$

where ρ runs over the zeros of $\zeta(s) = 0$ with $0 < \mathrm{Re}(\rho) < 1$.
The *Riemann Hypothesis* states that $\mathrm{Re}(\rho) = 1/2$ for all those zeros. It follows that

$$\pi(X) = \int_2^X \frac{dt}{\log t} + O(\sqrt{X}(\log X)^2).$$

Example: smallest quadratic non-residue

For a prime ℓ, define

$$\begin{aligned} q(\ell) &= \min\{q \geq 1 \mid q \text{ is not a square modulo } \ell\} \\ &= \min\left\{q \geq 1 \mid \left(\frac{q}{\ell}\right) = -1\right\}. \end{aligned}$$

Example: smallest quadratic non-residue

For a prime ℓ, define

$$\begin{aligned} q(\ell) &= \min\{q \geq 1 \mid q \text{ is not a square modulo } \ell\} \\ &= \min\{q \geq 1 \mid \left(\frac{q}{\ell}\right) = -1\}. \end{aligned}$$

To show $q(p) < A$ one can try to prove that

$$S_\ell(A) = \sum_{q \leq A} \left(\frac{q}{\ell}\right) < A.$$

(cont.)

By Mellin inversion (harmonic analysis), we have

$$S_\ell(A) \simeq \frac{1}{2i\pi} \int_{2-i\infty}^{2+i\infty} \left(\sum_{n \geq 1} \binom{n}{\ell} n^{-s} \right) A^s \frac{ds}{s} = \frac{1}{2i\pi} \int_{2-i\infty}^{2+i\infty} L_\ell(s) A^s \frac{ds}{s}.$$

(cont.)

By Mellin inversion (harmonic analysis), we have

$$S_\ell(A) \simeq \frac{1}{2i\pi} \int_{2-i\infty}^{2+i\infty} \Big(\sum_{n \geq 1} \Big(\frac{n}{\ell}\Big) n^{-s} \Big) A^s \frac{ds}{s} = \frac{1}{2i\pi} \int_{2-i\infty}^{2+i\infty} L_\ell(s) A^s \frac{ds}{s}.$$

The function $L_\ell(s)$ is a *Dirichlet L-function* which is entire. Integrating over $\mathrm{Re}(s) = 1/2$, one can get

$$S_\ell(A) \leq C\ell^{1/4} A^{1/2} < A, \quad \text{if } A > C^2\sqrt{\ell},$$

and hence $q(\ell) \leq C^2 \ell^{1/2}$.

(cont.)

By Mellin inversion (harmonic analysis), we have

$$S_\ell(A) \simeq \frac{1}{2i\pi}\int_{2-i\infty}^{2+i\infty}\Big(\sum_{n\geq 1}\Big(\frac{n}{\ell}\Big)n^{-s}\Big)A^s\frac{ds}{s} = \frac{1}{2i\pi}\int_{2-i\infty}^{2+i\infty}L_\ell(s)A^s\frac{ds}{s}.$$

The function $L_\ell(s)$ is a *Dirichlet L-function* which is entire.
Integrating over $\mathrm{Re}(s) = 1/2$, one can get

$$S_\ell(A) \leq C\ell^{1/4}A^{1/2} < A, \quad \text{if } A > C^2\sqrt{\ell},$$

and hence $q(\ell) \leq C^2\ell^{1/2}$.
Improving this requires great ingenuity and quickly runs into issues related to the Lindelöf and Generalized Riemann Hypothesis.

Modular forms

A *cusp form* of weight k and level N is an holomorphic function

$$f : \mathbf{H} = \{z \in \mathbf{C} \mid \mathrm{Im}(z) > 0\} \to \mathbf{C}$$

Modular forms

A *cusp form* of weight k and level N is an holomorphic function

$$f\ :\ \mathbf{H} = \{z \in \mathbf{C} \mid \operatorname{Im}(z) > 0\} \to \mathbf{C}$$

such that

$$f\Big(\frac{az+b}{cNz+d}\Big) = (cNz+d)^k f(z), \qquad \text{if } a,b,c,d \in \mathbf{Z},\ ad-bcN = 1,$$

$$\int_0^1 \int_1^{+\infty} |f(z)|^2 y^k \frac{dxdy}{y^2} < +\infty.$$

Modular forms

A *cusp form* of weight k and level N is an holomorphic function

$$f \; : \; \mathbf{H} = \{z \in \mathbf{C} \mid \operatorname{Im}(z) > 0\} \to \mathbf{C}$$

such that

$$f\left(\frac{az+b}{cNz+d}\right) = (cNz+d)^k f(z), \qquad \text{if } a,b,c,d \in \mathbf{Z},\ ad - bcN = 1,$$
$$\int_0^1 \int_1^{+\infty} |f(z)|^2 y^k \frac{dxdy}{y^2} < +\infty.$$

Example

The *Ramanujan function*, with $N = 1$ and $k = 12$:

$$\Delta(z) = e^{2i\pi z} \prod_{n \geq 1} (1 - e^{2i\pi nz})^{24}.$$

L-functions of modular forms

Certain ("primitive") cusp forms (including Δ) lead to L-functions

$$L(f,s) = \sum_{n\geq 1} \lambda_f(n) n^{-s}$$
$$= \prod_{p\nmid N} (1 - \lambda_f(p)p^{-s} + p^{-2s})^{-1} \prod_{p\mid N} (1 - \lambda_p(p)p^{-s})^{-1},$$

with $\lambda_f(n)$ characterizing f through the Fourier expansion

$$f(z) = \sum_{n\geq 1} \lambda_f(n) n^{(k-1)/2} \exp(2i\pi nz).$$

L-functions of modular forms

Certain ("primitive") cusp forms (including Δ) lead to L-functions

$$\begin{aligned} L(f,s) &= \sum_{n\geq 1} \lambda_f(n) n^{-s} \\ &= \prod_{p\nmid N} (1-\lambda_f(p)p^{-s}+p^{-2s})^{-1} \prod_{p\mid N} (1-\lambda_p(p)p^{-s})^{-1}, \end{aligned}$$

with $\lambda_f(n)$ characterizing f through the Fourier expansion

$$f(z) = \sum_{n\geq 1} \lambda_f(n) n^{(k-1)/2} \exp(2i\pi nz).$$

Those have conductor N and gamma factor

$$\gamma(s) = \pi^{-s}\Gamma(s+\tfrac{k-1}{2}).$$

Families of L-functions

There are only finitely many "primitive" cusp forms of given weight and level.

Families of L-functions

There are only finitely many "primitive" cusp forms of given weight and level. One can see them probabilistically:

1. $\Omega_{k,N} = \{\text{primitive } f \text{ of weight } k \text{ and level } N\}$;

Families of L-functions

There are only finitely many "primitive" cusp forms of given weight and level. One can see them probabilistically:

1. $\Omega_{k,N} = \{\text{primitive } f \text{ of weight } k \text{ and level } N\}$;
2. Counting measure or "harmonic" measure (easier analytically);

Families of L-functions

There are only finitely many "primitive" cusp forms of given weight and level. One can see them probabilistically:

1. $\Omega_{k,N} = \{\text{primitive } f \text{ of weight } k \text{ and level } N\}$;
2. Counting measure or "harmonic" measure (easier analytically);
3. Local factors $\rho_p : f \mapsto \lambda_f(p)$;

Families of L-functions

There are only finitely many "primitive" cusp forms of given weight and level. One can see them probabilistically:

1. $\Omega_{k,N} = \{\text{primitive } f \text{ of weight } k \text{ and level } N\}$;
2. Counting measure or "harmonic" measure (easier analytically);
3. Local factors $\rho_p : f \mapsto \lambda_f(p)$;
4. Approximate independence: trace formula or Petersson formula;

Families of L-functions

There are only finitely many "primitive" cusp forms of given weight and level. One can see them probabilistically:

1. $\Omega_{k,N} = \{\text{primitive } f \text{ of weight } k \text{ and level } N\}$;
2. Counting measure or "harmonic" measure (easier analytically);
3. Local factors $\rho_p : f \mapsto \lambda_f(p)$;
4. Approximate independence: trace formula or Petersson formula;
5. Local equidistribution: *with harmonic measure*, if $\lambda_f(p) = 2\cos\theta_f(p)$, we have

$$(f \mapsto \theta_f(p)) \xrightarrow{law} \mu_{ST} = \frac{2}{\pi}\sin^2\theta d\theta \text{ on } [0,\pi].$$

Families of L-functions

There are only finitely many "primitive" cusp forms of given weight and level. One can see them probabilistically:

1. $\Omega_{k,N} = \{\text{primitive } f \text{ of weight } k \text{ and level } N\}$;
2. Counting measure or "harmonic" measure (easier analytically);
3. Local factors $\rho_p : f \mapsto \lambda_f(p)$;
4. Approximate independence: trace formula or Petersson formula;
5. Local equidistribution: *with harmonic measure*, if $\lambda_f(p) = 2\cos\theta_f(p)$, we have

$$(f \mapsto \theta_f(p)) \xrightarrow{law} \mu_{ST} = \frac{2}{\pi}\sin^2\theta d\theta \text{ on } [0,\pi].$$

6. Interesting random variable: $L(f, \frac{1}{2})$.

Elliptic curves

Equations of the type

$$y^2 = x^3 + Ax + B$$

where the parameters $A, B \in \mathbf{Z}$ are such that the right-hand side has no double-root in $\mathbf{C}$.

Elliptic curves

Equations of the type

$$y^2 = x^3 + Ax + B$$

where the parameters A, $B \in \mathbf{Z}$ are such that the right-hand side has no double-root in $\mathbf{C}$.

Question. Are there infinitely many rational solutions?

Elliptic curves

Equations of the type

$$y^2 = x^3 + Ax + B$$

where the parameters $A,\ B \in \mathbf{Z}$ are such that the right-hand side has no double-root in $\mathbf{C}$.

Question. Are there infinitely many rational solutions?

One may want to study this for a family:

1. $\Omega_X = \{(A, B) \mid |A|^3, |B|^2 \leq X\}$;
2. ρ_p associates the number of solutions modulo p, or even the equation modulo p;

Elliptic curve L-functions

It happens to be possible to package the local information in an L-function

$$L(E,s)\text{''} = \text{''} \prod_p (1 - a_p p^{-s} + p^{-2s})^{-1}$$

where, for all p with finitely many exceptions, we have

$$|\{(x,y) \in (\mathbf{Z}/p\mathbf{Z})^2 \mid y^2 \equiv x^3 + Ax + B\}| = p - p^{1/2} a_p.$$

Elliptic curve L-functions

It happens to be possible to package the local information in an L-function

$$L(E,s)\text{''} = \text{''} \prod_p (1 - a_p p^{-s} + p^{-2s})^{-1}$$

where, for all p with finitely many exceptions, we have

$$|\{(x,y) \in (\mathbf{Z}/p\mathbf{Z})^2 \mid y^2 \equiv x^3 + Ax + B\}| = p - p^{1/2} a_p.$$

Taylor–Wiles (and Breuil, Conrad, Diamond, Taylor) proved that this L-function is indeed the L-function of a cusp form of weight 2 and some level N (dividing the discriminant of $X^3 + AX + B$).

Birch–Swinnerton-Dyer conjecture, “baby” version

Conjecture

There exist infinitely many rational solutions $(x, y) \in \mathbf{Q}^2$ *to* $y^2 = x^3 + Ax + B$ *if and only if*

$$L(E, 1/2) = 0.$$

Birch–Swinnerton-Dyer conjecture, “baby” version

Conjecture

There exist infinitely many rational solutions $(x, y) \in \mathbf{Q}^2$ *to* $y^2 = x^3 + Ax + B$ *if and only if*

$$L(E, 1/2) = 0.$$

A much more precise version relates the leading term of

$$L(E, s) = c_r(s - 1/2)^r + c_{r-1}(s - 1/2)^{r-1} + \cdots$$

to many deep arithmetic invariants of the elliptic curve.