An Introduction to Special Values of L-Functions

Jay Daigle
jdaigle@caltech.edu
http://jaydaigle.net

California Institute of Technology

May 30, 2014


i can has
attenshun plz?

Finding Prime Numbers

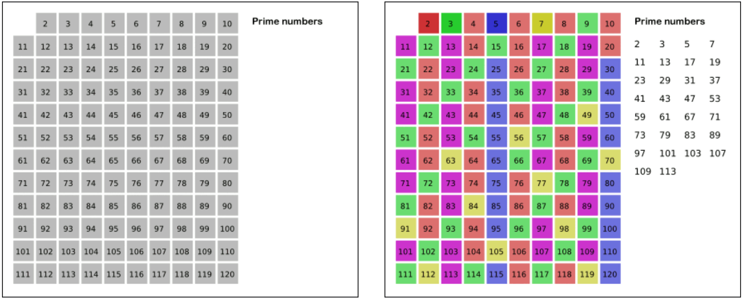


Figure : Sieve of Eratosthenes
Sebastian Koppehel / CC-BY-SA-3.0

Counting prime numbers between 10 and 100

- Every composite in $[10, 100]$ is divisible by a prime $p \leq 10$.
- $(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5})(1-\frac{1}{7}) = \frac{1\cdot 2\cdot 4\cdot 6}{2\cdot 3\cdot 5\cdot 7} = \frac{8}{35} \approx .23$
- $.23 \cdot 90 \approx 21$. Primes between 10 and 100:

$$11, 13, 17, 19, 23, 29, 31,$$
$$37, 41, 43, 47, 53, 59, 61,$$
$$67, 71, 73, 79, 83, 89, 97$$

There are twenty-one!

Prime Number Theorem

Let $\pi(x)$ be the number of prime numbers less than or equal to x. Then

$$\lim_{x\to+\infty} \frac{\pi(x)\ln(x)}{x} = 1.$$

Counting prime numbers

$$(1-\tfrac{1}{2})(1-\tfrac{1}{3})(1-\tfrac{1}{5})(1-\tfrac{1}{7})\ldots = \prod_{p \text{ prime}} \left(1-\frac{1}{p}\right)$$

$$\left(1-\frac{1}{p}\right)^{-1} = 1+\frac{1}{p}+\frac{1}{2p}+\ldots$$

$$\prod_{p \text{ prime}} \left(1-\frac{1}{p}\right)^{-1} = \prod_{p \text{ prime}} \left(1+\frac{1}{p}+\frac{1}{2p}+\ldots\right) \qquad = \sum_{n\geq 1} \frac{1}{n}$$

This is the harmonic series, which doesn't converge (and order matters!).

The Riemann zeta series

- Idea (from calculus): We can look at behavior of functions near bad points.

Definition

The Riemann zeta function is the function of one complex variable

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}$$

- Converges absolutely for $\mathrm{Re}(s) > 1$.
- Want to study behavior near $s = 1$.

Meromorphic continuations

Definition: Meromorphic Continuation

- A function $f : \mathbb{C} \to \mathbb{C}$ is meromorphic if it can be represented as the ratio of two power series:

$$f(z) = \frac{\sum_{n \geq 0} a_n (z - z_0)^n}{\sum_{n \geq 0} b_n (z - z_0)^n}$$

- If $g : U \to \mathbb{C}$ is a meromorphic function, and $f : \mathbb{C} \to \mathbb{C}$ is a meromorphic function with $f(u) = g(u)$ for all $u \in U$, we say f is the (unique!) meromorphic continuation of g.

The functional equation and the Riemann zeta function

We observe:

The functional equation

$$\zeta(s) = 2^s \pi^{s-1} \sin(\pi s/2) \left(\int_0^{+\infty} x^{-s} e^{-x} dx \right) \zeta(1-s).$$

Theorem

- The Riemann zeta series has a meromorphic contiuation to the complex plane, with a single pole at $s = 1$.
- $\lim_{s \to 1} (s-1)\zeta(s) = 1$.

The Riemann Zeta Function

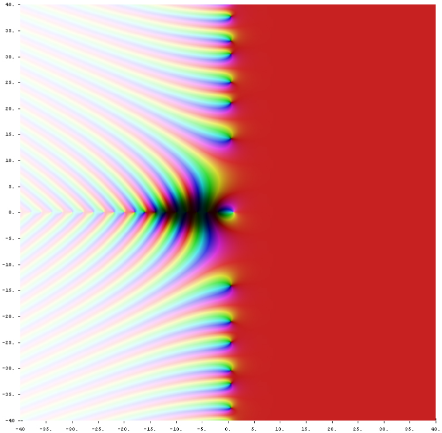


Figure : Values in black are close to 0
Hue gives the complex argument, with red being totally real

Special Values of the Riemann Zeta Function

- The prime number theorem is true if and only if $\zeta(s) \neq 0$ for all $\mathrm{Re}(s) = 1$.
- $\zeta(-n) = -\frac{B_{n+1}}{n+1}$.
- $\zeta(-2n) = 0$ for every $n \in \mathbb{N}$ ("trivial zeros").

Fun fact

$$-\frac{1}{12} = \zeta(-1) = \sum_{n \geq 0} \frac{1}{n^{-1}} = 1 + 2 + 3 + 4 + \dots$$

Zeroes of the Riemann Zeta Function

Zeroes of ζ control how far primes are from where we “expect” them.

Riemann zeros control:

- The error term in the prime number theorem.
- The growth of the Möbius function and other counting functions.
- The size of prime gaps.

The Riemann Hypothesis

What do we know?

- If $\zeta(s) = 0$ then either $s = -2n$, or $0 < \mathrm{Re}(s) < 1$ ("critical strip").
- Zeroes are symmetric about the "critical line" $\mathrm{Re}(s) = \frac{1}{2}$.
- The function $\zeta(\frac{1}{2} + it)$ is zero for infinitely many $t \in \mathbb{R}$ (Hardy 1914).

Riemann Hypothesis (Riemann 1859)

If $\zeta(s) = 0$ then either $s = -2n$, or s is on the critical line $\mathrm{Re}(s) = \frac{1}{2}$.

Fermat's "Last Theorem"

Theorem (Wiles 1994)

Suppose $x^n + y^n = z^n$ for integers x, y, z. Then $n \leq 2, x = 0$ or $y = 0$.

Cauchy, Lamé 1847

- $z^n = x^n + y^n = (x+y)(x+\zeta_n y)(x+\zeta_n^2 y)\dots(x+\zeta_n^{n-1} y)$
- These products are all relatively prime and divide z^n, and so by unique factorization are all nth powers.
- "Infinite descent": use this solution to generate a smaller solution.

Kummer 1844

$$(1+\zeta_{23}^2+\zeta_{23}^4+\zeta_{23}^5+\zeta_{23}^6+\zeta_{23}^{10}+\zeta_{23}^{11})(1+\zeta_{23}+\zeta_{23}^5+\zeta_{23}^6+\zeta_{23}^7+\zeta_{23}^9+\zeta_{23}^{11})$$
$$=2(\zeta_{23}^5+\zeta_{23}^7+\zeta_{23}^9+\zeta_{23}^{10}+3\zeta_{23}^{11}+\zeta_{23}^{12}+\zeta_{23}^{13}+\zeta_{23}^{15}+\zeta_{23}^{16}+\zeta_{23}^{17})$$


damn anti-gravity cat
always disproving ma theorem
ICANHASCHEEZBURGER.COM

Fields and Field Extensions

- A field: you can do addition, multiplication, and division.
- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Q}_p$, $\mathbb{Q}(t)$.

Definition

- If F and K are fields with $F \subset K$ then K is a field extension of F.
- K is a vector field over F and we write $[K : F] = \dim_F(K)$ for the degree of the extension.
- A number field is a finite extension of $\mathbb{Q}$. All number fields embed into $\mathbb{C}$.

- $\mathbb{C} = \mathbb{R}(i)$.
- $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}, i)$
- $\mathbb{Q}(e^{2\pi i/n}) = \mathbb{Q}(\zeta_n)$
- $\mathbb{Q}(\sqrt{D} : D \in \mathbb{Z})$

Algebraic Extensions

Definition

- We say that $\alpha \in K$ is algebraic over F if there's a polynomial $f \in F[x]$ with $f(\alpha) = 0$.
- K/F is an algebraic extension if every $\alpha \in K$ is algebraic over F.

Normal Basis Theorem

- Every number field is algebraic over $\mathbb{Q}$.
- If F is a number field then $F = \mathbb{Q}(\alpha)$ for some $\alpha \in F$.

Algebraic Integers

Definition

- Let K be a number field, and let $\alpha \in K$. We say α is an algebraic integer if $f(\alpha) = 0$ for some $f \in \mathbb{Z}[x]$.
- The ring of integers $\mathcal{O}_K$ is the set of all algebraic integers in K.

$\mathbb{Q}$	$\mathbb{Z}$
$\mathbb{Q}(i)$	$\mathbb{Z}[i]$
$\mathbb{Q}(\zeta_n)$	$\mathbb{Z}[\zeta_n]$
$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$

Factorization

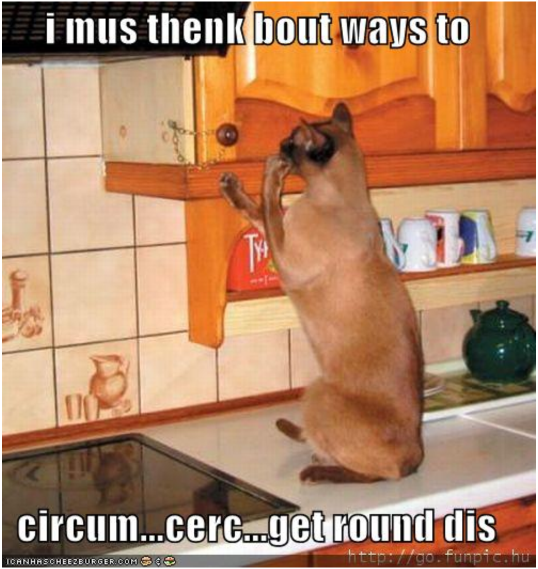
Fundamental Theorem of Arithmetic

Every integer factors uniquely up to order and sign as a product of prime numbers.

- $6 = 2 \cdot 3 = 3 \cdot 2 = -3 \cdot -2$

What about in number fields?

- Unique factorization in $\mathbb{Z}[i], \mathbb{Z}[\sqrt{-2}], \mathbb{Z}[\zeta_{19}]$
- $6 = \left(1 - \sqrt{-5}\right)\left(1 + \sqrt{-5}\right) \in \mathbb{Z}[\sqrt{-5}]$.
- $(1+\zeta_{23}^2+\zeta_{23}^4+\zeta_{23}^5+\zeta_{23}^6+\zeta_{23}^{10}+\zeta_{23}^{11})(1+\zeta_{23}+\zeta_{23}^5+\zeta_{23}^6+\zeta_{23}^7+\zeta_{23}^9+\zeta_{23}^{11})$
  $= 2(\zeta_{23}^5+\zeta_{23}^7+\zeta_{23}^9+\zeta_{23}^{10}+3\zeta_{23}^{11}+\zeta_{23}^{12}+\zeta_{23}^{13}+\zeta_{23}^{15}+\zeta_{23}^{16}+\zeta_{23}^{17}) \in \mathbb{Z}[\zeta_{23}]$


i mus thenk bout ways to
circum...cerc...get round dis
ICANHASCHEEZBURGER.COM
http://go.funpic.hu

Prime Ideals and Unique Factorization

Definition

- Ideal: if a or $b \in I$ then $ab \in I$.
- Prime ideal: If $ab \in I$ then $a \in I$ or $b \in I$.

Unique Factorization Theorem

Every ideal factors uniquely as a product of prime ideals.

Ideal Classes

Principal Ideals

An ideal is principal if it's generated by one element.
e.g. $(2), (3), (2-\sqrt{-5}+i)$. $(0), (1)$.
Not principal: $(2, 1+\sqrt{-17}), (2, 1+\sqrt{-29}), (2, \sqrt{-6})$.

Definition

We say two ideals $\mathfrak{p}, \mathfrak{q} \subset K$ are equivalent if there are $a, b \in K$ such that $(a)\mathfrak{p} = (b)\mathfrak{q}$.
An equivalence class of ideals is called an ideal class. The (finite) group of ideal classes is the class group of K, and its size h_K is the class number.

Ideal Norms

$$\prod_{\mathfrak{p} \subset \mathcal{O}_K} \frac{1}{1 - \mathfrak{p}^{-s}} \qquad ??$$

- It's unclear what it means to divide by an ideal.
- Number fields don't embed in $\mathbb{C}$ canonically.

Definition

The index of $\mathfrak{p}$ is $\|\mathfrak{p}\| = \mathcal{O}_K/\mathfrak{p}$. Equivalently, $N(\mathfrak{p}) = \mathbb{Z} \cap \prod_{\sigma \in G} \sigma(\mathfrak{p})$.

The Dedekind Zeta Function

Definition

The Dedekind zeta function for K is

$$\zeta_K(s) = \prod_{\mathfrak{p} \subset \mathcal{O}_F} \frac{1}{1 - \|\mathfrak{p}\|^{-s}} = \sum_{I \subset \mathcal{O}_F} \|I\|^{-s} = \sum_{n \geq 1} \frac{j_n}{n^s}.$$

- $\zeta_K(-2n) = 0$.
- $\zeta_K(-n) = 0$ unless K is totally real. Otherwise $\zeta_K(-n) \in \mathbb{Q}$.
- Generalized Riemann Hypothesis: All nontrivial zeros in the critical strip $0 < \mathrm{Re}(s) < 1$ are on the critical line $\mathrm{Re}(s) = \frac{1}{2}$.

The Best Proof Technique of All Time

Gauss's Class Number Conjecture

- Gauss (1798) conjectured that as the discriminant D of an imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ approaches $-\infty$, the class number $h(D) \to +\infty$.
- Hecke 1918: If the GRH is true, then the conjecture holds.
- Heilbronn 1932: If the GRH is false, then the conjecture holds.

The Analytic Class Number Formula

Class Number Formula

$$\lim_{s \to 1}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h_K \operatorname{Reg}_K}{w_K \cdot \sqrt{|D_K|}}.$$

Do we need all that information? Sadly, yes. Bosma and Smit (2002) found pairs of fields with different class numbers but the same zeta function.

The Rank Formula

- A finitely generated abelian group has a finite set of generators.
- Isomorphic to $\mathbb{Z}^r \oplus \bigoplus \mathbb{Z}/n\mathbb{Z}$.
- The rank is the integer r.

Rank Formula

The group of units of $\mathcal{O}_F$ is a finitely generated abelian group.

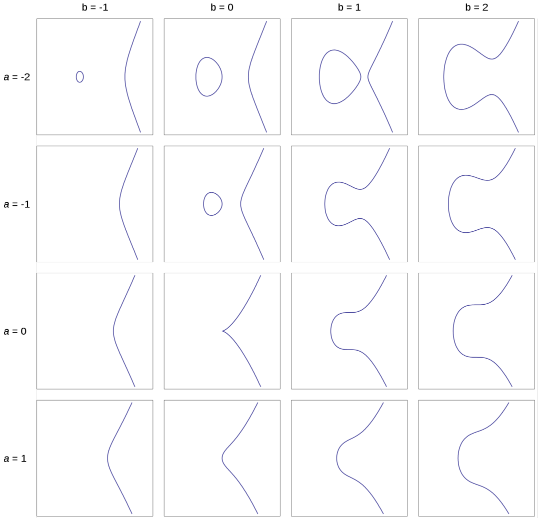
$$\lim_{s\to 0} s^{-r}\zeta_K(s) = -\frac{h_K \operatorname{Reg}_K}{w(K)}.$$

Elliptic Curves

- A smooth genus 1 curve with a rational point
- $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$
- $y^2 = x^3 + ax + b$

Key Question

How many rational points are there?



Group Law on Elliptic Curves

The rational points on an elliptic curve form an abelian group.

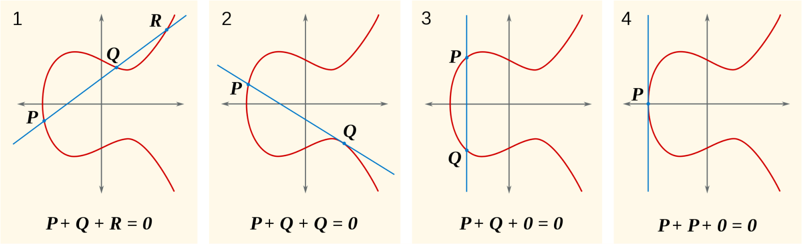


Figure : The group law on elliptic curves
Emmanuel Boutet / CC-BY-SA-3.0

Elliptic Curves over Finite Fields

- Let $E : y^2 = x^3 + ax + b$ for $a, b \in \mathbb{F}_q$.
- $E(\mathbb{F}_q)$ is finite.
- $E(\mathbb{F}_q)$ is either cyclic or the product of two cyclic groups.

Theorem (Hasse 1933)

$|\#E(\mathbb{F}_1) - (q+1)| < 2\sqrt{q}$.

Elliptic Curves over a number field

- Weak Mordell-Weil Theorem: $E(K)/mE(K)$ is finite for any $m > 1$.
- Mordell-Weil Theorem: $E(K)$ is a finitely generated abelian group.
- Merel: For each K there are only finitely many possible torsion subgroups for $E(K)$.
- Conjecture: Rank is unbounded.

Fact (Elkies 2009)

The curve

$$y^2 + xy + y$$
$$= x^3 - x^2 + 31368015812338065133318565292206590792820353345x$$
$$+ 302038802698566087335643188429543498624522041683874493555186$$

has rank 19.

Elliptic Curves over $\mathbb{Q}$

- Mazur: The torsion component of $E(\mathbb{Q})$ can only be $\mathbb{Z}/N\mathbb{Z}$ for $N = 1, 2, \ldots, 10, 12$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ for $N = 1, 2, 3, 4$.
- Still expect rank to be unbounded.
- However, we expect 50% of curves to be rank 0 and 50% to be rank 1. (100% doesn't mean all of an infinite set)

The Hasse-Weil L-function

Definition

- E has good reduction at p if E/p is an elliptic curve.
- If E has good reduction at p, set $a_p = p + 1 - \#(E/p)(\mathbb{F}_p)$, and $L_p(E, s) = 1 - a_p p^{-s} + p^{1-2s}$.
- $L(E, s) = \prod_p L_p(s, E)^{-1}$.

Facts

- Easy fact: $L(E, s)$ converges absolutely for $\mathrm{Re}(s) > 3/2$.
- Very, very hard fact: $L(E, s)$ has a meromorphic continuation to the complex plane (Breuil-Conrad-Diamond-Taylor 2001) .

Birch and Swinnerton-Dyer Conjecture

Conjecture (Birch and Swinnerton-Dyer 1965)

- Rank conjecture: $\operatorname{rk} E(\mathbb{Q}) = \operatorname{ord}_{s=1} L(E,s)$
- Formula:

$$\lim_{s \to 1} (s-1)^r L(E,s) = \Omega_E \frac{\operatorname{Reg}(e) \cdot |\text{Ш}(E)|}{|E(\mathbb{Q})|_{tors}} \prod_{\ell} c_\ell$$

- Tate: “This remarkable conjecture relates the behaviour of a function L, at a point where it is not at present known to be defined, to the order of a group Ш, which is not known to be finite.”

What do we know?

"Old" results

- Gross-Zagier (1986): A modular elliptic curve with analytic rank 1 has rank at least one.
- Kolyvagin (1989): A modular elliptic curve with analytic rank 0 has rank 0, and a modular curve with analytic rank 1 has rank 1.
- Breuil et al (2001): All rational elliptic curves are modular.

This year (Bhargava, Shankar, Skinner, Urban, Zhang)

- Average rank is $\leq .885$
- At least 83.75% have rank 0 or 1
- At least 66.48% satisfy BSD.


OMG
I KNEW IT!!!
ICANHASCHEEZBURGER.COM

Bonus: Fermat's Last Theorem

- Frey 1982: If $a^n + b^n = c^n$ then $y^2 = x(x - a^n)(x + b^n)$ is an elliptic curve.
- Serre 1985, Ribet 1986: This curve is semistable and not modular.
- Wiles 1995: All semistable elliptic curves over $\mathbb{Q}$ are modular.
- Breuil-Conrad-Diamond-Taylor 2001: All elliptic curves over $\mathbb{Q}$ are modular.

Generalizations of L-functions

- Dirichlet L-series $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ for Dirichlet characters $\chi : \mathbb{Z} \to \mathbb{C}$.
- Artin L-functions, from a linear representation of a Galois group.
- Hecke L-functions attached to modular forms or Hecke characters
- p-adic L-functions, from p-adic interpolation or from Galois modules
- Hasse-Weil L-functions for algebraic varieties
- L-functions from automorphic representations
- Conjecture: these are all basically the same.

L-functions on motives

If X is a smooth projective variety and i, j are integers, a motive $M = h^i(X)(j)$ is essentially X together with cohomological data about X. To every motive we can associate:

- A representation $M_l = H^i_{et}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_l)(j)$
- A polynomial $P_p(T) = \det(1 - Fr_p^{-1} \cdot T | M_l^{I_p}) \in \mathbb{Q}_l[T]$, conjectured to be independent of l.
- An L function $L(M, s) = \prod_p P_p(p^{-s})^{-1}$ analytic for $\mathrm{Re}(s) \gg 0$.
- We conjecture that $L(M, s)$ can be meromorphically continued to $s = 0$,and study the Taylor expansion

$$L(M, s) = L^*(M, s)s^{r(M)} + \dots$$

The Tamagawa number conjecture on Tate motives