# L-functions and Elliptic Curves 

Nuno Freitas

Universität Bayreuth
January 2014

## Motivation

Let $m(P)$ denote the logarithmic Mahler measure of a polynomial $P \in \mathbb{C}\left[x^{ \pm 1}, y^{ \pm 1}\right]$.

## Motivation

Let $m(P)$ denote the logarithmic Mahler measure of a polynomial $P \in \mathbb{C}\left[x^{ \pm 1}, y^{ \pm 1}\right]$.

- In 1981, Smyth proved the following formula:

$$
m(1+x+y)=L^{\prime}\left(\chi_{-3},-1\right)
$$

where $\chi_{-3}$ is the Dirichlet character associated to the quadratic field $\mathbb{Q}(\sqrt{-3})$.

## Motivation

Let $m(P)$ denote the logarithmic Mahler measure of a polynomial $P \in \mathbb{C}\left[x^{ \pm 1}, y^{ \pm 1}\right]$.

- In 1981, Smyth proved the following formula:

$$
m(1+x+y)=L^{\prime}(\chi-3,-1)
$$

where $\chi_{-3}$ is the Dirichlet character associated to the quadratic field $\mathbb{Q}(\sqrt{-3})$.

- In 1997, Deninger conjectured the following formula

$$
m\left(x+\frac{1}{x}+y+\frac{1}{y}+1\right)=L^{\prime}(E, 0)
$$

where $E$ is the elliptic curve that is the projective closure of the polynomial in the left hand side.

## Motivation

Let $m(P)$ denote the logarithmic Mahler measure of a polynomial $P \in \mathbb{C}\left[x^{ \pm 1}, y^{ \pm 1}\right]$.

- In 1981, Smyth proved the following formula:

$$
m(1+x+y)=L^{\prime}(\chi-3,-1)
$$

where $\chi_{-3}$ is the Dirichlet character associated to the quadratic field $\mathbb{Q}(\sqrt{-3})$.

- In 1997, Deninger conjectured the following formula

$$
m\left(x+\frac{1}{x}+y+\frac{1}{y}+1\right)=L^{\prime}(E, 0)
$$

where $E$ is the elliptic curve that is the projective closure of the polynomial in the left hand side.
Our goal: Sketch the basic ideas that allow to make sense of the right hand side of these formulas.

## The Riemann Zeta function

The $L$-functions are constructed on the model of the Riemann Zeta function $\zeta(s)$, so let us recall properties of this function.

## The Riemann Zeta function

The $L$-functions are constructed on the model of the Riemann Zeta function $\zeta(s)$, so let us recall properties of this function.
The Riemann Zeta function $\zeta(s)$ is defined on $\mathbb{C}$, for $\operatorname{Re}(s)>1$, by the formula

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

## The Riemann Zeta function

The $L$-functions are constructed on the model of the Riemann Zeta function $\zeta(s)$, so let us recall properties of this function.
The Riemann Zeta function $\zeta(s)$ is defined on $\mathbb{C}$, for $\operatorname{Re}(s)>1$, by the formula

$$
\zeta(s)=\sum_{n \geq 1} \frac{1}{n^{s}}
$$

Euler showed that

$$
\zeta(s)=\prod_{p} \frac{1}{1-p^{-s}} .
$$

## The Riemann Zeta function

The $L$-functions are constructed on the model of the Riemann Zeta function $\zeta(s)$, so let us recall properties of this function.

The Riemann Zeta function $\zeta(s)$ is defined on $\mathbb{C}$, for $\operatorname{Re}(s)>1$, by the formula

$$
\zeta(s)=\sum_{n \geq 1} \frac{1}{n^{s}}
$$

Euler showed that

$$
\zeta(s)=\prod_{p} \frac{1}{1-p^{-s}}
$$

In particular, Euler's equality provides an alternative proof of the existence of infinitely many prime numbers.

## The Riemann Zeta function

Theorem (Riemann)
The Riemann Zeta function $\zeta(s)$ can be analytical continued to a meromorphic function of the complex plane. Its only pole is at $s=1$, and its residue is 1 .
Moreover, the function $\Lambda$ defined by

$$
\Lambda(s):=\pi^{-s / 2} \Gamma(s / 2) \zeta(s)
$$

satisfies the functional equation

$$
\Lambda(s)=\Lambda(1-s)
$$

## The Gamma function

The function $\Gamma$ in the previous theorem is defined by

$$
\Gamma(s):=\int_{0}^{\infty} e^{-t} t^{s-1} d t
$$

## The Gamma function

The function $\Gamma$ in the previous theorem is defined by

$$
\Gamma(s):=\int_{0}^{\infty} e^{-t} t^{s-1} d t
$$

It admits a meromorphic continuation to all $\mathbb{C}$ and satisfies the functional equation

$$
\Gamma(s+1)=s \Gamma(s)
$$

## The Gamma function

The function $\Gamma$ in the previous theorem is defined by

$$
\Gamma(s):=\int_{0}^{\infty} e^{-t} t^{s-1} d t
$$

It admits a meromorphic continuation to all $\mathbb{C}$ and satisfies the functional equation

$$
\Gamma(s+1)=s \Gamma(s) .
$$

The function $\Gamma(s / 2)$ has simple poles at the negative even integers.

## The Gamma function

The function $\Gamma$ in the previous theorem is defined by

$$
\Gamma(s):=\int_{0}^{\infty} e^{-t} t^{s-1} d t
$$

It admits a meromorphic continuation to all $\mathbb{C}$ and satisfies the functional equation

$$
\Gamma(s+1)=s \Gamma(s) .
$$

The function $\Gamma(s / 2)$ has simple poles at the negative even integers. To compensate these poles we have $\zeta(-2 n)=0$. These are called the trivial zeros of $\zeta(s)$.

## The Gamma function

The function $\Gamma$ in the previous theorem is defined by

$$
\Gamma(s):=\int_{0}^{\infty} e^{-t} t^{s-1} d t
$$

It admits a meromorphic continuation to all $\mathbb{C}$ and satisfies the functional equation

$$
\Gamma(s+1)=s \Gamma(s) .
$$

The function $\Gamma(s / 2)$ has simple poles at the negative even integers. To compensate these poles we have $\zeta(-2 n)=0$. These are called the trivial zeros of $\zeta(s)$.
Conjecture (Riemann Hypothesis)
All the non-trivial zeros of $\zeta(s)$ satisfy $\operatorname{Re}(s)=1 / 2$.

## Analytic L-functions

Definition
A Dirichlet series is a formal series of the form

$$
F(s)=\sum_{n=1}^{\infty} \frac{a_{n}}{n^{s}}, \quad \text { where } a_{n} \in \mathbb{C} .
$$

## Analytic L-functions

Definition
A Dirichlet series is a formal series of the form

$$
F(s)=\sum_{n=1}^{\infty} \frac{a_{n}}{n^{s}}, \quad \text { where } a_{n} \in \mathbb{C}
$$

We call an Euler product to a product of the form

$$
F(s)=\prod_{p} L_{p}(s)
$$

The factors $L_{p}(s)$ are called the local Euler factors.

## Analytic L-functions

Definition
A Dirichlet series is a formal series of the form

$$
F(s)=\sum_{n=1}^{\infty} \frac{a_{n}}{n^{s}}, \quad \text { where } a_{n} \in \mathbb{C}
$$

We call an Euler product to a product of the form

$$
F(s)=\prod_{p} L_{p}(s)
$$

The factors $L_{p}(s)$ are called the local Euler factors.
An analytic L-function is a Dirichlet series that has an Euler product and satisfies a certain type of functional equation.

## Dirichlet characters

A function $\chi: \mathbb{Z} \rightarrow \mathbb{C}$ is called a Dirichlet character modulo $N$ if there is a group homomorphism $\tilde{\chi}:(\mathbb{Z} / N \mathbb{Z})^{*} \rightarrow \mathbb{C}^{*}$ such that

$$
\chi(x)=\tilde{\chi}(x(\bmod N)) \quad \text { if } \quad(x, N)=1
$$

## Dirichlet characters

A function $\chi: \mathbb{Z} \rightarrow \mathbb{C}$ is called a Dirichlet character modulo $N$ if there is a group homomorphism $\tilde{\chi}:(\mathbb{Z} / N \mathbb{Z})^{*} \rightarrow \mathbb{C}^{*}$ such that

$$
\chi(x)=\tilde{\chi}(x(\bmod N)) \quad \text { if } \quad(x, N)=1
$$

and

$$
\chi(x)=0 \quad \text { if }(x, N) \neq 1
$$

## Dirichlet characters

A function $\chi: \mathbb{Z} \rightarrow \mathbb{C}$ is called a Dirichlet character modulo $N$ if there is a group homomorphism $\tilde{\chi}:(\mathbb{Z} / N \mathbb{Z})^{*} \rightarrow \mathbb{C}^{*}$ such that

$$
\chi(x)=\tilde{\chi}(x(\bmod N)) \quad \text { if } \quad(x, N)=1
$$

and

$$
\chi(x)=0 \quad \text { if }(x, N) \neq 1
$$

Moreover, we say that $\chi$ is primitive if there is no strict divisor $M \mid N$ and a character $\tilde{\chi}_{0}:(\mathbb{Z} / M \mathbb{Z})^{*} \rightarrow \mathbb{C}^{*}$ such that

$$
\chi(x)=\tilde{\chi}_{0}(x(\bmod M)) \quad \text { if } \quad(x, M)=1
$$

## Dirichlet characters

A function $\chi: \mathbb{Z} \rightarrow \mathbb{C}$ is called a Dirichlet character modulo $N$ if there is a group homomorphism $\tilde{\chi}:(\mathbb{Z} / N \mathbb{Z})^{*} \rightarrow \mathbb{C}^{*}$ such that

$$
\chi(x)=\tilde{\chi}(x(\bmod N)) \quad \text { if } \quad(x, N)=1
$$

and

$$
\chi(x)=0 \quad \text { if }(x, N) \neq 1
$$

Moreover, we say that $\chi$ is primitive if there is no strict divisor $M \mid N$ and a character $\tilde{\chi}_{0}:(\mathbb{Z} / M \mathbb{Z})^{*} \rightarrow \mathbb{C}^{*}$ such that

$$
\chi(x)=\tilde{\chi}_{0}(x(\bmod M)) \quad \text { if } \quad(x, M)=1
$$

In particular, if $N=p$ is a prime every non-trivial character modulo $N$ is primitive.

## Dirichlet characters

A function $\chi: \mathbb{Z} \rightarrow \mathbb{C}$ is called a Dirichlet character modulo $N$ if there is a group homomorphism $\tilde{\chi}:(\mathbb{Z} / N \mathbb{Z})^{*} \rightarrow \mathbb{C}^{*}$ such that

$$
\chi(x)=\tilde{\chi}(x(\bmod N)) \quad \text { if } \quad(x, N)=1
$$

and

$$
\chi(x)=0 \quad \text { if }(x, N) \neq 1
$$

Moreover, we say that $\chi$ is primitive if there is no strict divisor $M \mid N$ and a character $\tilde{\chi}_{0}:(\mathbb{Z} / M \mathbb{Z})^{*} \rightarrow \mathbb{C}^{*}$ such that

$$
\chi(x)=\tilde{\chi}_{0}(x(\bmod M)) \quad \text { if } \quad(x, M)=1
$$

In particular, if $N=p$ is a prime every non-trivial character modulo $N$ is primitive. Moreover, any Dirichlet character is induced from a unique primitive character $\tilde{\chi}_{0}$ as above. We call $M$ its conductor.

## Dirichlet L-functions

Definition
We associate to a Dirichlet character $\chi$ an L-function given by

$$
L(\chi, s)=\sum_{n \geq 1} \frac{\chi(n)}{n^{s}}
$$

## Dirichlet L-functions

Definition
We associate to a Dirichlet character $\chi$ an L-function given by

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

## Dirichlet L-functions

## Definition

We associate to a Dirichlet character $\chi$ an L-function given by

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

For example,

$$
L(\chi-3, s)=\sum_{n=1}^{\infty}\left(\frac{n}{3}\right) \frac{1}{n^{s}}=1-\frac{1}{2^{s}}+\frac{1}{4^{s}}-\frac{1}{5^{s}}+\ldots
$$

where the sign is given by the symbol

$$
\left(\frac{n}{3}\right)= \begin{cases}1 & \text { if } n \text { is a square } \bmod 3 \\ -1 & \text { if } n \text { is not a square } \bmod 3 \\ 0 & \text { if } 3 \mid n\end{cases}
$$

## Dirichlet L-functions

Let $\chi$ be a Dirichlet character. We say that $\chi$ is even if $\chi(-1)=1$; we say that $\chi$ is odd if $\chi(-1)=-1$.

## Dirichlet L-functions

Let $\chi$ be a Dirichlet character. We say that $\chi$ is even if $\chi(-1)=1$; we say that $\chi$ is odd if $\chi(-1)=-1$.

Define also, if $\chi$ is even,

$$
\Lambda(\chi, s):=\pi^{-s / 2} \Gamma(s / 2) L(\chi, s)
$$

or, if $\chi$ is odd,

$$
\Lambda(\chi, s):=\pi^{-(s+1) / 2} \Gamma((s+1) / 2) L(\chi, s)
$$

## Dirichlet L-functions

Theorem
Let $\chi$ be a primitive Dirichlet character of conductor $N \neq 1$. Then, $L(\chi, s)$ has an extension to $\mathbb{C}$ as an entire function and satisfies the functional equation

$$
\Lambda(\chi, s)=\epsilon(\chi) N^{1 / 2-s} \wedge(\bar{\chi}, 1-s)
$$

where

$$
\epsilon(\chi)= \begin{cases}\frac{\tau(\chi)}{\sqrt{N}} & \text { if } \chi \text { is even } \\ -i \frac{\tau(\chi)}{\sqrt{N}} & \text { if } \chi \text { is odd }\end{cases}
$$

and

$$
\tau(\chi)=\sum_{x(\bmod N)} \chi(x) e^{2 i \pi x / N}
$$

## Elliptic Curves

Definition
An elliptic curve over a field $k$ is a non-singular projective plane curve given by an affine model of the form

$$
E: y^{2}+a_{1} x y+a_{3} y=x^{3}+a_{2} x^{2}+a_{4} x+a_{6}
$$

where all $a_{i} \in k$. Write $O=(0: 1: 0)$ for the point at infinity.

## Elliptic Curves

Definition
An elliptic curve over a field $k$ is a non-singular projective plane curve given by an affine model of the form

$$
E: y^{2}+a_{1} x y+a_{3} y=x^{3}+a_{2} x^{2}+a_{4} x+a_{6}
$$

where all $a_{i} \in k$. Write $O=(0: 1: 0)$ for the point at infinity. The change of variables fixing $O$ are of the form

$$
x=u^{2} x^{\prime}+r \quad y=u^{3} y^{\prime}+u^{2} s x^{\prime}+t
$$

where $u, r, s, t \in \bar{k}, u \neq 0$.

## Elliptic Curves

## Definition

An elliptic curve over a field $k$ is a non-singular projective plane curve given by an affine model of the form

$$
E: y^{2}+a_{1} x y+a_{3} y=x^{3}+a_{2} x^{2}+a_{4} x+a_{6}
$$

where all $a_{i} \in k$. Write $O=(0: 1: 0)$ for the point at infinity. The change of variables fixing $O$ are of the form

$$
x=u^{2} x^{\prime}+r \quad y=u^{3} y^{\prime}+u^{2} s x^{\prime}+t
$$

where $u, r, s, t \in \bar{k}, u \neq 0$. If $\operatorname{char}(k) \neq 2,3$, after a change of variables, $E$ can be writen as

$$
y^{2}=x^{3}+A x+B, \quad A, B \in k, \quad \Delta(E)=4 A^{3}+27 B^{2} .
$$

If $\Delta(E) \neq 0$ then $E$ is nonsingular.

## Example

Consider the curve

$$
E: y^{2}=x^{3}-2 x+1
$$

having attached quantities

$$
\Delta=2^{4} \cdot 5 \neq 0, \quad j=2^{11} \cdot 3^{3} \cdot 5^{-1}
$$

## Another example

Consider the set defined by

$$
x+\frac{1}{x}+y+\frac{1}{y}+1=0
$$

## Another example

Consider the set defined by

$$
x+\frac{1}{x}+y+\frac{1}{y}+1=0
$$

Multiplication by $x y$ followed by homogenization gives

$$
x^{2} y+y z^{2}+y^{2} x+x z^{2}+x y z=0
$$

## Another example

Consider the set defined by

$$
x+\frac{1}{x}+y+\frac{1}{y}+1=0
$$

Multiplication by $x y$ followed by homogenization gives

$$
x^{2} y+y z^{2}+y^{2} x+x z^{2}+x y z=0
$$

Applying the isomorphism $(x, y, z) \mapsto(y, x-y, z-x)$ yelds

$$
x^{3}-2 x^{2} z+x y z-y^{2} z+x z^{2}=0
$$

## Another example

Consider the set defined by

$$
x+\frac{1}{x}+y+\frac{1}{y}+1=0
$$

Multiplication by $x y$ followed by homogenization gives

$$
x^{2} y+y z^{2}+y^{2} x+x z^{2}+x y z=0
$$

Applying the isomorphism $(x, y, z) \mapsto(y, x-y, z-x)$ yelds

$$
x^{3}-2 x^{2} z+x y z-y^{2} z+x z^{2}=0
$$

After setting $z=1$ and rearranging we get the elliptic curve with conductor 15 given by

$$
y^{2}-x y=x^{3}-2 x^{2}+x
$$

## Theorem

Let $E / k$ be an elliptic curve. There is an abelian group structure on the set of points $E(\bar{k})$.

$P+Q+R=0$

$P+Q+Q=0$

$P+Q+0=0$

$P+P+0=0$

## Theorem

Let $E / k$ be an elliptic curve. There is an abelian group structure on the set of points $E(\bar{k})$.

$P+Q+R=0$

$P+Q+Q=0$

$P+Q+0=0$

$P+P+0=0$

Theorem (Mordell-Weil)
Let $E / k$ be an elliptic curve over a number field $k$. The group $E(k)$ is finitely generated.

## Example

Consider the curve

$$
E: y^{2}=x^{3}-2 x+1
$$

having attached quantities

$$
\Delta=2^{4} \cdot 5 \neq 0, \quad j=2^{11} \cdot 3^{3} \cdot 5^{-1}
$$

## Example

Consider the curve

$$
E: y^{2}=x^{3}-2 x+1
$$

having attached quantities

$$
\Delta=2^{4} \cdot 5 \neq 0, \quad j=2^{11} \cdot 3^{3} \cdot 5^{-1}
$$

Its rational torsion points are

$$
E(\mathbb{Q})_{\text {Tor }}=\{O,(0:-1: 1),(0: 1: 1),(1: 0: 1)\}
$$

and they form a cyclic group of order 4.

## Reduction modulo $p$

Let $E / \mathbb{Q}$ be an elliptic curve. There exists a model $E / \mathbb{Z}$ such that $|\Delta(E)|$ is minimal. For such a model and a prime $p$, we set $\tilde{a}_{i}=a_{i}$ $(\bmod p)$ and consider the reduced curve over $\mathbb{F}_{p}$

$$
\tilde{E}: \quad y^{2}+\tilde{a}_{1} x y+\tilde{a}_{3} y=x^{3}+\tilde{a}_{2} x^{2}+\tilde{a}_{4} x+\tilde{a}_{6} .
$$

## Reduction modulo $p$

Let $E / \mathbb{Q}$ be an elliptic curve. There exists a model $E / \mathbb{Z}$ such that $|\Delta(E)|$ is minimal. For such a model and a prime $p$, we set $\tilde{a}_{i}=a_{i}$ $(\bmod p)$ and consider the reduced curve over $\mathbb{F}_{p}$

$$
\tilde{E}: \quad y^{2}+\tilde{a}_{1} x y+\tilde{a}_{3} y=x^{3}+\tilde{a}_{2} x^{2}+\tilde{a}_{4} x+\tilde{a}_{6} .
$$

It can be seen that $\tilde{E}$ has at most one singular point.

## Reduction modulo $p$

Let $E / \mathbb{Q}$ be an elliptic curve. There exists a model $E / \mathbb{Z}$ such that $|\Delta(E)|$ is minimal. For such a model and a prime $p$, we set $\tilde{a}_{i}=a_{i}$ $(\bmod p)$ and consider the reduced curve over $\mathbb{F}_{p}$

$$
\tilde{E}: \quad y^{2}+\tilde{a}_{1} x y+\tilde{a}_{3} y=x^{3}+\tilde{a}_{2} x^{2}+\tilde{a}_{4} x+\tilde{a}_{6} .
$$

It can be seen that $\tilde{E}$ has at most one singular point.
Definition (type of reduction)
Let $p$ be a prime. We say that $E$

- has good reduction at $p$ if $\tilde{E}$ is an elliptic curve.


## Reduction modulo $p$

Let $E / \mathbb{Q}$ be an elliptic curve. There exists a model $E / \mathbb{Z}$ such that $|\Delta(E)|$ is minimal. For such a model and a prime $p$, we set $\tilde{a}_{i}=a_{i}$ $(\bmod p)$ and consider the reduced curve over $\mathbb{F}_{p}$

$$
\tilde{E}: \quad y^{2}+\tilde{a}_{1} x y+\tilde{a}_{3} y=x^{3}+\tilde{a}_{2} x^{2}+\tilde{a}_{4} x+\tilde{a}_{6} .
$$

It can be seen that $\tilde{E}$ has at most one singular point.
Definition (type of reduction)
Let $p$ be a prime. We say that $E$

- has good reduction at $p$ if $\tilde{E}$ is an elliptic curve.
- has bad multiplicative reduction at $p$ if $\tilde{E}$ admits a double point with two distinct tangents.


## Reduction modulo $p$

Let $E / \mathbb{Q}$ be an elliptic curve. There exists a model $E / \mathbb{Z}$ such that $|\Delta(E)|$ is minimal. For such a model and a prime $p$, we set $\tilde{a}_{i}=a_{i}$ $(\bmod p)$ and consider the reduced curve over $\mathbb{F}_{p}$

$$
\tilde{E}: \quad y^{2}+\tilde{a}_{1} x y+\tilde{a}_{3} y=x^{3}+\tilde{a}_{2} x^{2}+\tilde{a}_{4} x+\tilde{a}_{6} .
$$

It can be seen that $\tilde{E}$ has at most one singular point.
Definition (type of reduction)
Let $p$ be a prime. We say that $E$

- has good reduction at $p$ if $\tilde{E}$ is an elliptic curve.
- has bad multiplicative reduction at $p$ if $\tilde{E}$ admits a double point with two distinct tangents. We say it is split or non-split if the tangents are defined over $\mathbb{F}_{p}$ or $\mathbb{F}_{p^{2}}$, respectively.


## Reduction modulo $p$

Let $E / \mathbb{Q}$ be an elliptic curve. There exists a model $E / \mathbb{Z}$ such that $|\Delta(E)|$ is minimal. For such a model and a prime $p$, we set $\tilde{a}_{i}=a_{i}$ $(\bmod p)$ and consider the reduced curve over $\mathbb{F}_{p}$

$$
\tilde{E}: \quad y^{2}+\tilde{a}_{1} x y+\tilde{a}_{3} y=x^{3}+\tilde{a}_{2} x^{2}+\tilde{a}_{4} x+\tilde{a}_{6} .
$$

It can be seen that $\tilde{E}$ has at most one singular point.
Definition (type of reduction)
Let $p$ be a prime. We say that $E$

- has good reduction at $p$ if $\tilde{E}$ is an elliptic curve.
- has bad multiplicative reduction at $p$ if $\tilde{E}$ admits a double point with two distinct tangents. We say it is split or non-split if the tangents are defined over $\mathbb{F}_{p}$ or $\mathbb{F}_{p^{2}}$, respectively.
- has bad additive reduction at $p$ if $\tilde{E}$ admits a double point with only one tangent.


## The Conductor of an elliptic curve.

## Definition

The conductor $N_{E}$ of an elliptic curve $E / \mathbb{Q}$ is an integer. It is computed by Tate's algorithm, and is of the form

$$
N_{E}=\prod_{p} p^{f_{p}}
$$

where the exponents $f_{p}$ satisfy

$$
f_{p}=\left\{\begin{array}{l}
0 \\
1 \\
2 \\
2+\delta_{p}, 0 \leq \delta_{p} \leq 6
\end{array}\right.
$$

if $E$ has good reduction at $p$,
if $E$ has bad multiplicative reduction at $p$,
if $E$ has bad additive reduction at $p \geq 5$,
if $E$ has bad additive reduction at $p=2,3$.
In particular, $N_{E} \mid \Delta(E)$ for the discriminant associated with any model of $E$.

## Example

Consider the curve

$$
E: y^{2}=x^{3}-2 x+1, \quad \text { which is a minimal model }
$$

having attached quantities

$$
\Delta=2^{4} \cdot 5, \quad j=2^{11} \cdot 3^{3} \cdot 5^{-1}
$$

## Example

Consider the curve

$$
E: y^{2}=x^{3}-2 x+1, \quad \text { which is a minimal model }
$$

having attached quantities

$$
\Delta=2^{4} \cdot 5, \quad j=2^{11} \cdot 3^{3} \cdot 5^{-1}
$$

The reduction type at $p=5$ is bad split multiplicative reduction and at $p=2$ is bad additive reduction. Furthermore,

$$
N_{E}=2^{3} \cdot 5=40
$$

## Example

Consider the curve

$$
E: y^{2}=x^{3}-2 x+1, \quad \text { which is a minimal model }
$$

having attached quantities

$$
\Delta=2^{4} \cdot 5, \quad j=2^{11} \cdot 3^{3} \cdot 5^{-1}
$$

The reduction type at $p=5$ is bad split multiplicative reduction and at $p=2$ is bad additive reduction. Furthermore,

$$
N_{E}=2^{3} \cdot 5=40
$$

Its rational torsion points are

$$
E(\mathbb{Q})_{\text {Tor }}=\{O,(0:-1: 1),(0: 1: 1),(1: 0: 1)\} \cong(\mathbb{Z} / 4 \mathbb{Z})
$$

## Artin Zeta Function

Let $E / \mathbb{F}_{p}$ be an elliptic curve given by

$$
y^{2}+a_{1} x y+a_{3} y-x^{3}+a_{2} x^{2}+a_{4} x+a_{6}=0
$$

## Artin Zeta Function

Let $E / \mathbb{F}_{p}$ be an elliptic curve given by

$$
y^{2}+a_{1} x y+a_{3} y-x^{3}+a_{2} x^{2}+a_{4} x+a_{6}=0
$$

Consider the associated Dedekind domain

$$
A=\mathbb{F}_{p}[X, Y] /(E)
$$

## Artin Zeta Function

Let $E / \mathbb{F}_{p}$ be an elliptic curve given by

$$
y^{2}+a_{1} x y+a_{3} y-x^{3}+a_{2} x^{2}+a_{4} x+a_{6}=0
$$

Consider the associated Dedekind domain

$$
A=\mathbb{F}_{p}[X, Y] /(E)
$$

For a non-zero ideal $\mathcal{I}$ of $A$ we define its norm

$$
N(\mathcal{I})=\#(A / \mathcal{I})
$$

## Artin Zeta Function

Let $E / \mathbb{F}_{p}$ be an elliptic curve given by

$$
y^{2}+a_{1} x y+a_{3} y-x^{3}+a_{2} x^{2}+a_{4} x+a_{6}=0
$$

Consider the associated Dedekind domain

$$
A=\mathbb{F}_{p}[X, Y] /(E)
$$

For a non-zero ideal $\mathcal{I}$ of $A$ we define its norm

$$
N(\mathcal{I})=\#(A / \mathcal{I})
$$

The Zeta function associated to $A$ is

$$
\zeta_{A}(s)=\sum_{\mathcal{I} \neq 0} \frac{1}{N(\mathcal{I})^{s}}
$$

## Artin Zeta Function

Let $E / \mathbb{F}_{p}$ be an elliptic curve given by

$$
y^{2}+a_{1} x y+a_{3} y-x^{3}+a_{2} x^{2}+a_{4} x+a_{6}=0
$$

Consider the associated Dedekind domain

$$
A=\mathbb{F}_{p}[X, Y] /(E)
$$

For a non-zero ideal $\mathcal{I}$ of $A$ we define its norm

$$
N(\mathcal{I})=\#(A / \mathcal{I})
$$

The Zeta function associated to $A$ is

$$
\zeta_{A}(s)=\sum_{\mathcal{I} \neq 0} \frac{1}{N(\mathcal{I})^{s}}=\prod_{\mathcal{P}} \frac{1}{1-N(\mathcal{P})^{-s}}
$$

## Artin Zeta Function

Let $E / \mathbb{F}_{p}$ be an elliptic curve given by

$$
y^{2}+a_{1} x y+a_{3} y-x^{3}+a_{2} x^{2}+a_{4} x+a_{6}=0
$$

Consider the associated Dedekind domain

$$
A=\mathbb{F}_{p}[X, Y] /(E)
$$

For a non-zero ideal $\mathcal{I}$ of $A$ we define its norm

$$
N(\mathcal{I})=\#(A / \mathcal{I})
$$

The Zeta function associated to $A$ is

$$
\zeta_{A}(s)=\sum_{\mathcal{I} \neq 0} \frac{1}{N(\mathcal{I})^{s}}=\prod_{\mathcal{P}} \frac{1}{1-N(\mathcal{P})^{-s}}
$$

Definition
For $s \in \mathbb{C}$ such that $\operatorname{Re}(s)>1$, we set

$$
\zeta_{E}(s)=\frac{1}{1-p^{-s}} \zeta_{A}(s)
$$

## Artin Zeta Function

Theorem (Artin)
Let $E / \mathbb{F}_{p}$ be an elliptic curve and set

$$
a_{E}:=p+1-\# E\left(\mathbb{F}_{p}\right)
$$

## Artin Zeta Function

Theorem (Artin)
Let $E / \mathbb{F}_{p}$ be an elliptic curve and set

$$
a_{E}:=p+1-\# E\left(\mathbb{F}_{p}\right)
$$

Then,

$$
\zeta_{E}(s)=\frac{1-a_{E} \cdot p^{-s}+p \cdot p^{-2 s}}{\left(1-p^{-s}\right)\left(1-p \cdot p^{-s}\right)}
$$

and

$$
\zeta_{E}(s)=\zeta_{E}(1-s)
$$

## The Hasse-Weil L-function of $E / \mathbb{Q}$

Let $E / \mathbb{Q}$ be an elliptic curve. For a prime $p$ of good reduction, let $\tilde{E}$ be the reduction of $E \bmod p$, and set

$$
L_{p}(s)=\left(1-a_{\tilde{E}} \cdot p^{-s}+p \cdot p^{-2 s}\right)^{-1} .
$$

## The Hasse-Weil L-function of $E / \mathbb{Q}$

Let $E / \mathbb{Q}$ be an elliptic curve. For a prime $p$ of good reduction, let $\tilde{E}$ be the reduction of $E \bmod p$, and set

$$
L_{p}(s)=\left(1-a_{\tilde{E}} \cdot p^{-s}+p \cdot p^{-2 s}\right)^{-1}
$$

Define also Euler factors for primes $p$ of bad reduction by

$$
L_{p}(s)= \begin{cases}\left(1-p^{-s}\right)^{-1} & \text { if } E \text { has bad split multiplicative reduction at } \\ \left(1+p^{-s}\right)^{-1} & \text { if } E \text { has bad non-split mult. reduction at } p \\ 1 & \text { if } E \text { has bad additive reduction at } p\end{cases}
$$

## The Hasse-Weil L-function of $E / \mathbb{Q}$

Let $E / \mathbb{Q}$ be an elliptic curve. For a prime $p$ of good reduction, let $\tilde{E}$ be the reduction of $E \bmod p$, and set

$$
L_{p}(s)=\left(1-a_{\tilde{E}} \cdot p^{-s}+p \cdot p^{-2 s}\right)^{-1}
$$

Define also Euler factors for primes $p$ of bad reduction by
$L_{p}(s)= \begin{cases}\left(1-p^{-s}\right)^{-1} & \text { if } E \text { has bad split multiplicative reduction at } \\ \left(1+p^{-s}\right)^{-1} & \text { if } \mathrm{E} \text { has bad non-split mult. reduction at } p, \\ 1 & \text { if } \mathrm{E} \text { has bad additive reduction at } p .\end{cases}$

## Definition

The L-function of $E$ is defined by

$$
L(E, s)=\prod_{p} L_{p}(s)
$$

## A really brief incursion into modular cuspforms

- A modular form is a function on the upper-half plane that satisfies certain transformation and holomorphy conditions.


## A really brief incursion into modular cuspforms

- A modular form is a function on the upper-half plane that satisfies certain transformation and holomorphy conditions.
- Let $N \geq 1$ be an integer. Define

$$
\Gamma_{0}(N)=\left\{\left[\begin{array}{ll}
a & b \\
c & d
\end{array}\right] \in \mathrm{SL}_{2}(\mathbb{Z}):\left[\begin{array}{ll}
a & b \\
c & d
\end{array}\right] \equiv\left[\begin{array}{ll}
* & * \\
0 & *
\end{array}\right] \quad(\bmod N)\right\}
$$

- In particular, a cuspform $f$ for $\Gamma_{0}(N)$ (of weight 2) admits a Fourier expansion

$$
f(\tau)=\sum_{n=1}^{\infty} a_{n}(f) q^{n / N}, \quad a_{n}(f) \in \mathbb{C}, \quad q=e^{2 \pi i \tau}
$$

## A really brief incursion into modular cuspforms

- A modular form is a function on the upper-half plane that satisfies certain transformation and holomorphy conditions.
- Let $N \geq 1$ be an integer. Define

$$
\Gamma_{0}(N)=\left\{\left[\begin{array}{ll}
a & b \\
c & d
\end{array}\right] \in \mathrm{SL}_{2}(\mathbb{Z}):\left[\begin{array}{ll}
a & b \\
c & d
\end{array}\right] \equiv\left[\begin{array}{ll}
* & * \\
0 & *
\end{array}\right] \quad(\bmod N)\right\}
$$

- In particular, a cuspform $f$ for $\Gamma_{0}(N)$ (of weight 2) admits a Fourier expansion

$$
f(\tau)=\sum_{n=1}^{\infty} a_{n}(f) q^{n / N}, \quad a_{n}(f) \in \mathbb{C}, \quad q=e^{2 \pi i \tau}
$$

- There is a family of Hecke operators $\left\{T_{n}\right\}_{n \geq 1}$ acting on the $\mathbb{C}$-vector space of cuspforms for $\Gamma_{0}(N)$ of weight 2.
- To a cuspform that is an eigenvector of all $T_{n}$ we call an eigenform. Furthermore, we assume they are normalized such that $a_{1}(f)=1$.


## The $L$-function of an eigenform

## Definition

The L-function attached to an eigenform for $\Gamma_{0}(N)$ is defined by

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

Theorem
Let $f$ be an eigenform for $\Gamma_{0}(N)$ of weight 2. The function $L(f, s)$ has an entire continuation to $\mathbb{C}$. Moreover, the function

$$
\Lambda_{f}(s):=\left(\frac{\sqrt{N}}{2 \pi}\right)^{-s} \Gamma(s) L(f, s)
$$

satisfies the functional equation

$$
\Lambda_{f}(s)=w \Lambda_{f}(2-s)
$$

where $w= \pm 1$.

## Modularity and the L-function of $E / \mathbb{Q}$

Theorem (Wiles, Breuil-Conrad-Diamond-Taylor)
Let $E / \mathbb{Q}$ be an elliptic curve of conductor $N_{E}$. There is an eigenform $f$ for $\Gamma_{0}\left(N_{E}\right)$ (of weight 2) such that

$$
L(E, s)=L(f, s) .
$$

## Modularity and the $L$-function of $E / \mathbb{Q}$

Theorem (Wiles, Breuil-Conrad-Diamond-Taylor)
Let $E / \mathbb{Q}$ be an elliptic curve of conductor $N_{E}$. There is an eigenform $f$ for $\Gamma_{0}\left(N_{E}\right)$ (of weight 2) such that

$$
L(E, s)=L(f, s) .
$$

## Corollary

Let $E / \mathbb{Q}$ be an elliptic curve of conductor $N_{E}$. Define the function

$$
\Lambda_{E}(s):=\left(\frac{\sqrt{N_{E}}}{2 \pi}\right)^{-s} \Gamma(s) L(E, s) .
$$

The function $L(E, s)$ has an entire continuation to $\mathbb{C}$ and $\Lambda_{E}(s)$ satisfies

$$
\Lambda_{E}(s)=w \Lambda_{E}(2-s),
$$

where $w= \pm 1$.

## Example

Consider the curve

$$
E: y^{2}=x^{3}-2 x+1, \quad \Delta=2^{4} \cdot 5 \neq 0, \quad j=2^{11} \cdot 3^{3} \cdot 5^{-1}
$$

It has conductor $N_{E}=2^{3} \cdot 5=40$.

## Example

Consider the curve

$$
E: y^{2}=x^{3}-2 x+1, \quad \Delta=2^{4} \cdot 5 \neq 0, \quad j=2^{11} \cdot 3^{3} \cdot 5^{-1}
$$

It has conductor $N_{E}=2^{3} \cdot 5=40$. The cuspform of weight 2 for $\Gamma_{0}(40)$ corresponding to $E$ by modularity is

$$
f:=q+q^{5}-4 q^{7}-3 q^{9}+O\left(q^{10}\right)
$$

## Example

Consider the curve

$$
E: y^{2}=x^{3}-2 x+1, \quad \Delta=2^{4} \cdot 5 \neq 0, \quad j=2^{11} \cdot 3^{3} \cdot 5^{-1}
$$

It has conductor $N_{E}=2^{3} \cdot 5=40$. The cuspform of weight 2 for $\Gamma_{0}(40)$ corresponding to $E$ by modularity is

$$
f:=q+q^{5}-4 q^{7}-3 q^{9}+O\left(q^{10}\right)
$$

The rational torsion points are

$$
E(\mathbb{Q})_{\text {Tor }}=\{O,(0:-1: 1),(0: 1: 1),(1: 0: 1)\} \cong(\mathbb{Z} / 4 \mathbb{Z})
$$

## The BSD conjecture

Theorem (Mordell-Weil)
Let $E / \mathbb{Q}$ be an elliptic curve. Then the group $E(\mathbb{Q})$ is finitely generated. More precisely,

$$
E(\mathbb{Q}) \cong E(\mathbb{Q})_{T o r} \oplus \mathbb{Z}^{r_{E}}
$$

## The BSD conjecture

Theorem (Mordell-Weil)
Let $E / \mathbb{Q}$ be an elliptic curve. Then the group $E(\mathbb{Q})$ is finitely generated. More precisely,

$$
E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text {Tor }} \oplus \mathbb{Z}^{r_{E}}
$$

Conjecture (Birch-Swinnerton-Dyer)
The rank $r_{E}$ of the Mordell-Weil group of an elliptic $E / \mathbb{Q}$ is equal to the order of the zero of $L(E, s)$ at $s=1$.

## Example

Consider the curve

$$
E: y^{2}=x^{3}-2 x+1, \quad \Delta=2^{4} \cdot 5 \neq 0, \quad j=2^{11} \cdot 3^{3} \cdot 5^{-1}
$$

It has conductor $N_{E}=2^{3} \cdot 5=40$. The cuspform of weight 2 for
$\Gamma_{0}(40)$ corresponding to $E$ by modularity is

$$
f:=q+q^{5}-4 q^{7}-3 q^{9}+O\left(q^{10}\right)
$$

The rational torsion points are

$$
E(\mathbb{Q})_{\text {Tor }}=\{O,(0:-1: 1),(0: 1: 1),(1: 0: 1)\} \cong(\mathbb{Z} / 4 \mathbb{Z})
$$

## Example

Consider the curve

$$
E: y^{2}=x^{3}-2 x+1, \quad \Delta=2^{4} \cdot 5 \neq 0, \quad j=2^{11} \cdot 3^{3} \cdot 5^{-1}
$$

It has conductor $N_{E}=2^{3} \cdot 5=40$. The cuspform of weight 2 for $\Gamma_{0}(40)$ corresponding to $E$ by modularity is

$$
f:=q+q^{5}-4 q^{7}-3 q^{9}+O\left(q^{10}\right)
$$

The rational torsion points are

$$
E(\mathbb{Q})_{\text {Tor }}=\{O,(0:-1: 1),(0: 1: 1),(1: 0: 1)\} \cong(\mathbb{Z} / 4 \mathbb{Z})
$$

Moreover, the rank $r_{E}=0$ since the function $L(E, s)$ satisfies

$$
L(E, 1)=0.742206236711
$$

Thus $E(\mathbb{Q}) \cong(\mathbb{Z} / 4 \mathbb{Z})$.

## Counting Points on Varieties

Let $V / \mathbb{F}_{q}$ be a projective variety, given by the set of zeros

$$
f_{1}\left(x_{0}, \ldots, x_{N}\right)=\cdots=f_{m}\left(x_{0}, \ldots, x_{N}\right)=0
$$

of a collection of homogeneous polynomials. The number of points in $V\left(\mathbb{F}_{q^{n}}\right)$ is encoded in the zeta function
Definition
The Zeta function of $V / \mathbb{F}_{q}$ is the power series

$$
Z\left(V / \mathbb{F}_{q} ; T\right):=\exp \left(\sum_{n \geq 1} \# V\left(\mathbb{F}_{q^{n}}\right) \frac{T^{n}}{n}\right)
$$

## The Zeta function of the Projective space

Let $N \geq 1$ and $V=\mathbb{P}^{N}$. A point in $V\left(\mathbb{F}_{q^{n}}\right)$ is given by homogeneous coordinates ( $x_{0}: . .: x_{N}$ ) with $x_{i}$ not all zero. Two choices of coordinates give the same point if they differ by multiplication of a non-zero element in $\mathbb{F}_{q^{n}}$. Hence,

$$
\begin{gathered}
\# V\left(\mathbb{F}_{q^{n}}\right)=\frac{q^{n(N+1)}-1}{q^{n}-1}=\sum_{i=0}^{N} q^{n i} \quad \text { so } \\
\log Z\left(V / \mathbb{F}_{q} ; T\right)=\sum_{n=0}^{\infty}\left(\sum_{i=0}^{N} q^{n i}\right) \frac{T^{n}}{n}=\sum_{i=0}^{N}-\log \left(1-q^{i} T\right)
\end{gathered}
$$

Thus,

$$
Z\left(\mathbb{P}^{N} / \mathbb{F}_{q} ; T\right)=\frac{1}{(1-T)(1-q T) \ldots\left(1-q^{N} T\right)}
$$

## The Zeta function of $E / \mathbb{F}_{p}$

Theorem
Let $E / \mathbb{F}_{p}$ be an elliptic curve and define

$$
a_{E}=p+1-\# E\left(\mathbb{F}_{p}\right)
$$

Then,

$$
Z\left(E / \mathbb{F}_{p} ; T\right)=\frac{1-a_{E} T+p T^{2}}{(1-T)(1-p T)}
$$

Moreover,

$$
1-a_{E} T+p T^{2}=(1-\alpha)(1-\beta) \quad \text { with } \quad|\alpha|=|\beta|=\sqrt{p}
$$

## The Zeta function of $E / \mathbb{F}_{p}$

Theorem
Let $E / \mathbb{F}_{p}$ be an elliptic curve and define

$$
a_{E}=p+1-\# E\left(\mathbb{F}_{p}\right)
$$

Then,

$$
Z\left(E / \mathbb{F}_{p} ; T\right)=\frac{1-a_{E} T+p T^{2}}{(1-T)(1-p T)}
$$

Moreover,

$$
1-a_{E} T+p T^{2}=(1-\alpha)(1-\beta) \quad \text { with } \quad|\alpha|=|\beta|=\sqrt{p}
$$

Note that by setting $T=p^{-s}$ we obtain the equality

$$
Z\left(E / \mathbb{F}_{p} ; p^{-s}\right)=\zeta_{E}(s)
$$

## Example

Consider the curve $E: y^{2}=x^{3}-2 x+1$ which has bad additive reduction at 2.
Let $p=2$. Its $\bmod p$ reduction is given by

$$
\tilde{E}_{2}:(y-1)^{2}=x^{3}
$$

and satisfies $\# \tilde{E}_{2}\left(\mathbb{F}_{2^{n}}\right)=2^{n}+1$. Hence,

$$
\begin{aligned}
\log Z\left(\tilde{E}_{2} / \mathbb{F}_{2^{n}} ; T\right) & =\sum_{n=1}^{\infty} \frac{2^{n}+1}{n} T^{n} \\
& =\log \left(\frac{1}{1-2 T}\right)+\log \left(\frac{1}{1-T}\right)
\end{aligned}
$$

Thus,

$$
Z\left(\tilde{E}_{2} / \mathbb{F}_{2^{n}} ; T\right)=\frac{1}{(1-2 T)(1-T)}
$$

## Bibliography

- C.J. Smyth, On measures of polynomials in several variables, Bull. Austral. Math. Soc. 23 (1981), 49-63;
- C. Deninger, Deligne periods of mixed motives, K-theory and the entropy of certain $\mathbb{Z}^{n}$-actions, J. Amer. Math. Soc. 10:2 (1997), 259-281;
- J.H. Silverman, The Arithmetic of Elliptic Curves, GTM 106, Springer, 1986;
- F. Diamond and J. Shurman, A First Course on Modular Forms, GTM 228, Springer, 2005;

