Arbitrary Precision Computation of Modular Functions

Caelen Feller

Supervised by Prof. Jan Manschot

June 27 2018

Goals of Project

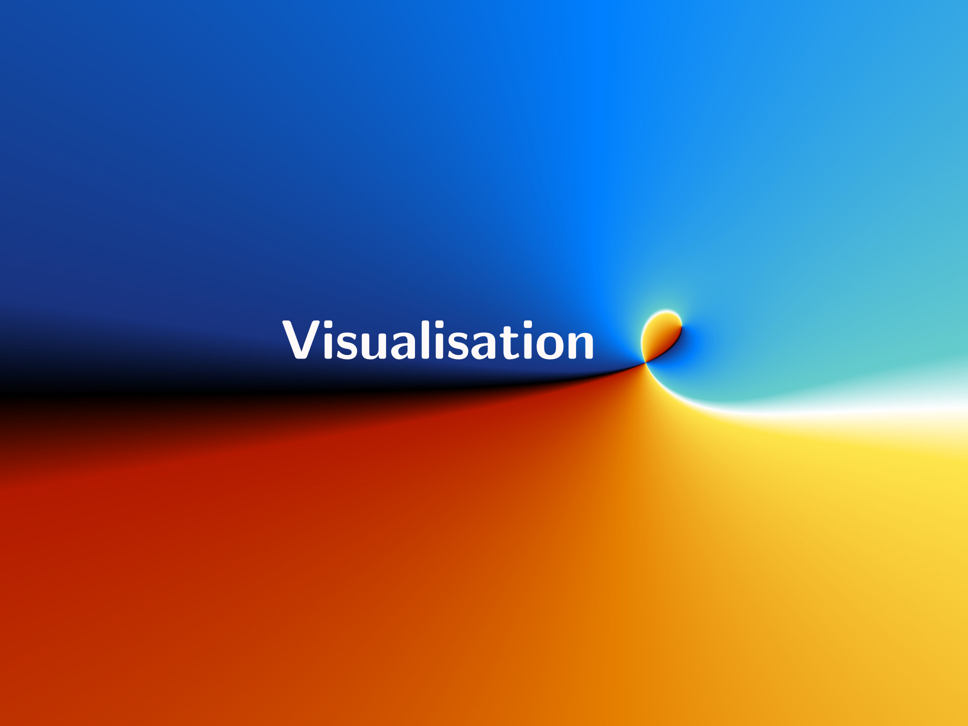
Software Library for

- Arbitrary precision computation
- Domain coloured plotting

Specifications

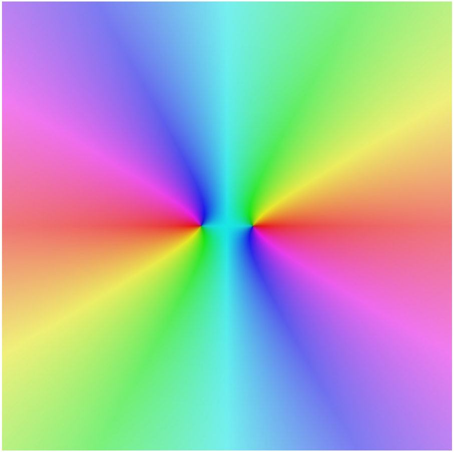
- Well documented
- Well tested
- Efficient
- Extensible

Visualisation



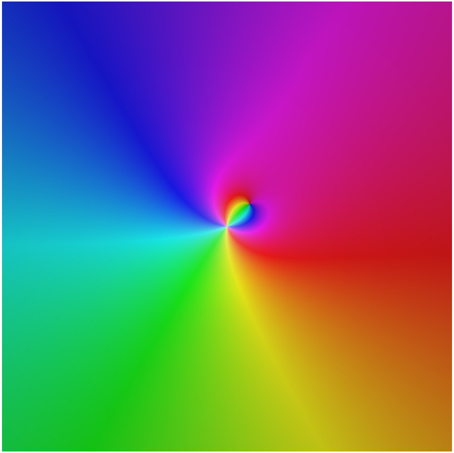
Domain Colouring - Examples 1

$f(z) = z$

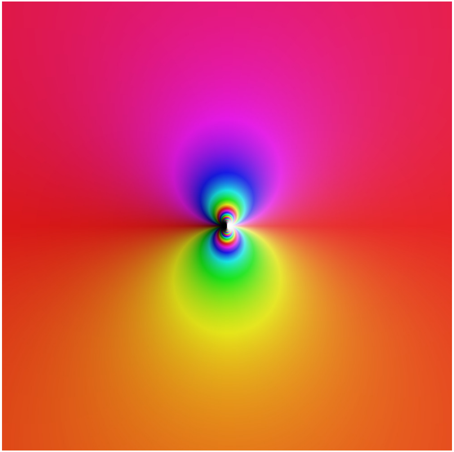


$f(z) = z^3 - 1$

Domain Colouring - Examples 2

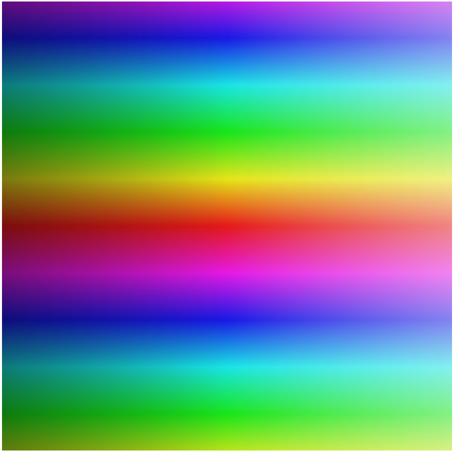


$f(z) = (z - 0.5(1+i))/z^2$

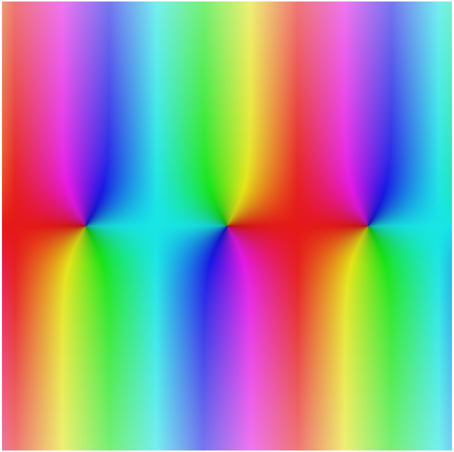


$f(z) = e^{1/z}$

Domain Colouring - Examples 3

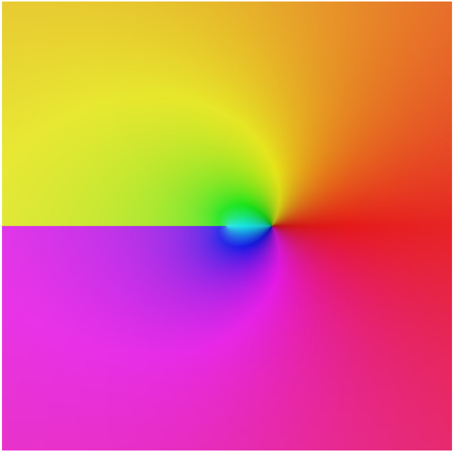


$f(z) = e^z$

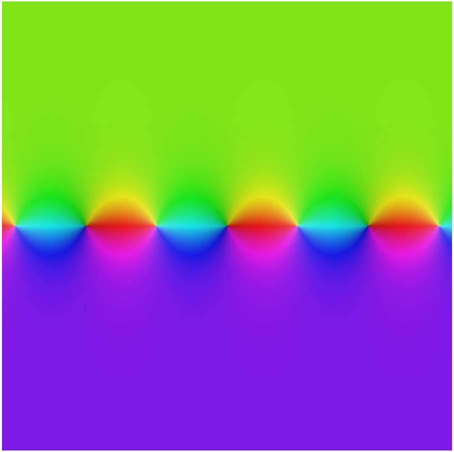


$f(z) = \sin(z)$

Domain Colouring - Examples 4



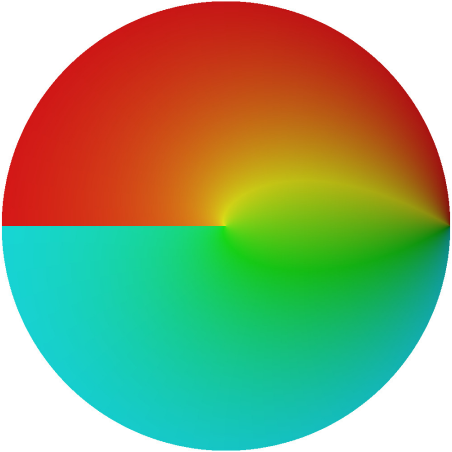
$f(z) = \log(z)$



$f(z) = \tan(z)$

Mapping $\mathbb{H}$ to Unit Disk

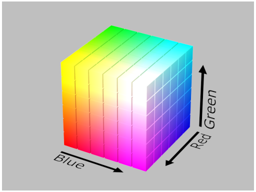
$\mathbb{H}$



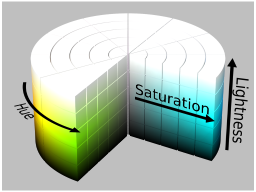
$f(z) = \frac{1}{i\pi}\log(z)$

Colour Space

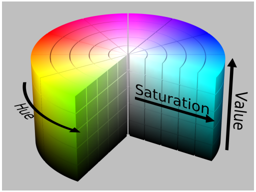
RGB Cube



HSL Cylinder



HSV Cylinder



Conversion from RGB to HSL/HSV

"Hexcone" model, standard feature in most environments.

Basic Colour Function

$$H = \frac{\arg(z)}{2\pi}$$

$$S = 1$$

$$L = 1 - 2^{-|z|}$$

$$L_{\text{alt}} = 1 - \frac{1}{1 + |z|^2}$$

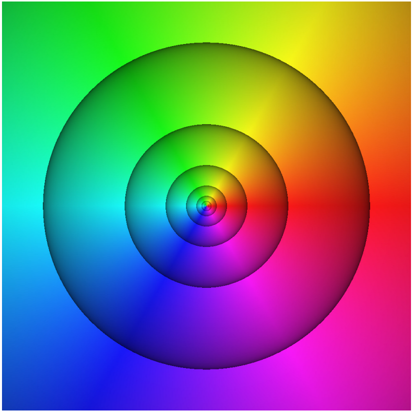
Identity

Colour Function - Contours

$$H = \frac{\arg(z)}{2\pi}$$

$$S = .9$$

$$V = \lceil \log_2(|z|) \rceil - \log_2(|z|)$$



Identity

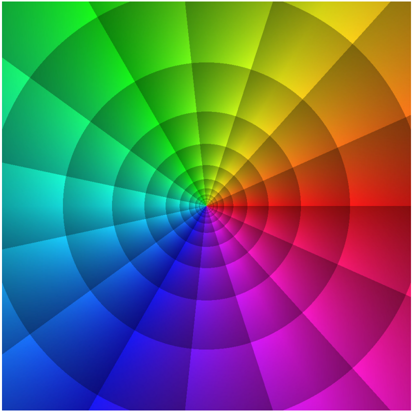
Colour Function - Conformality

$$H = \frac{\arg(z)}{2\pi}$$

$$S = .9$$

$$f(x) = (\lceil x \rceil - x)(M - m) + m$$

$$V = f(nH) \times f\left(\frac{n \log_2(|z|)}{2\pi}\right)$$



Brightness clamped to [m,M], n subdivisons of radial hue

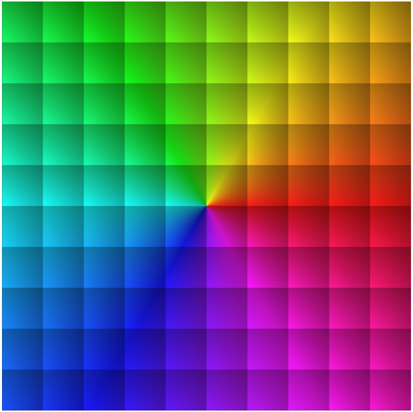
Colour Function - Transformation

$$H = \frac{\arg(z)}{2\pi}$$

$$S = .9$$

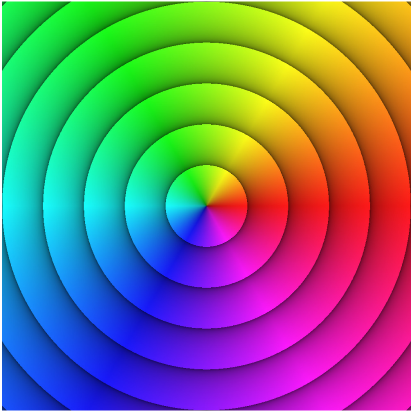
$$f(x) = (\lceil x \rceil - x)(M - m) + m$$

$$V = f(\Re(z)) \times f(\Im(z))$$



Brightness clamped to [m,M]

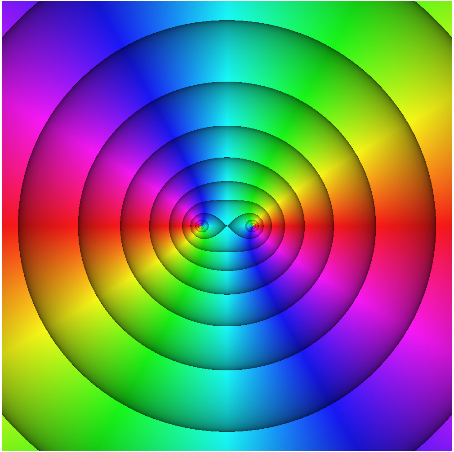
Other Colour Functions



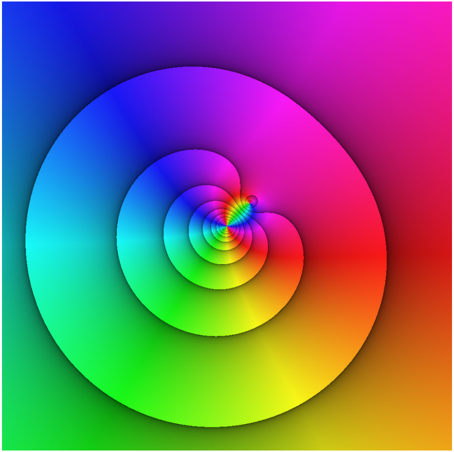
Radial without logarithm!

Qualitative Function

Colour Functions - Contour Examples

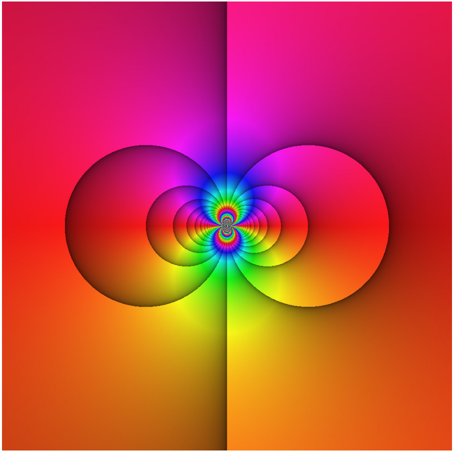


$f(z) = z^3 - 1$

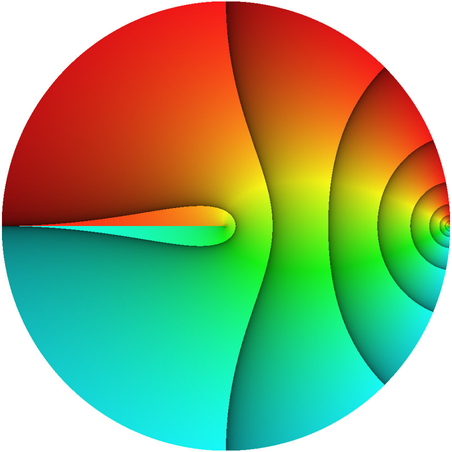


$f(z) = (z - 0.5(1 + i))/z^2$

Colour Functions - Contour Examples

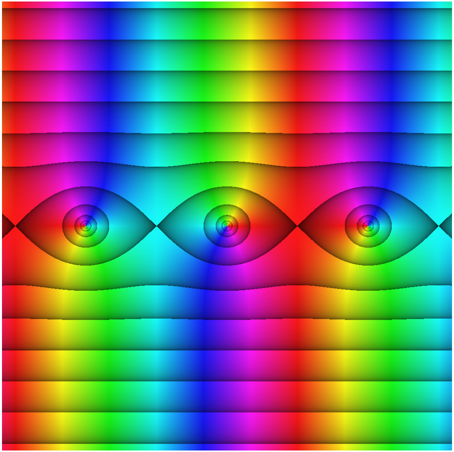


$f(z) = e^{1/z}$

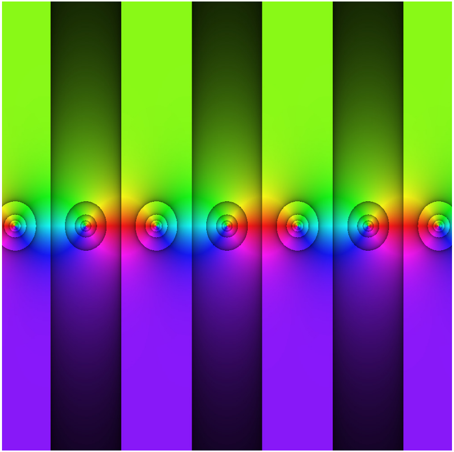


$f(z) = \frac{1}{i\pi} \log(z)$

Colour Functions - Contour Examples

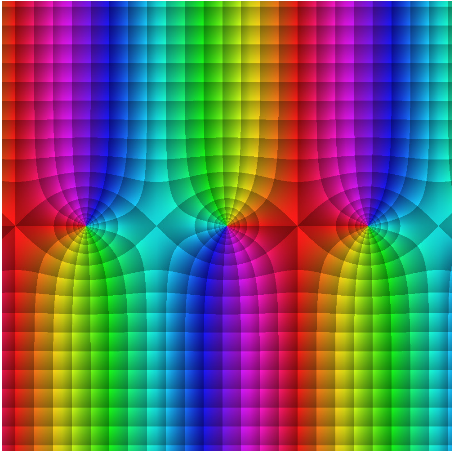


$f(z) = \sin(z)$

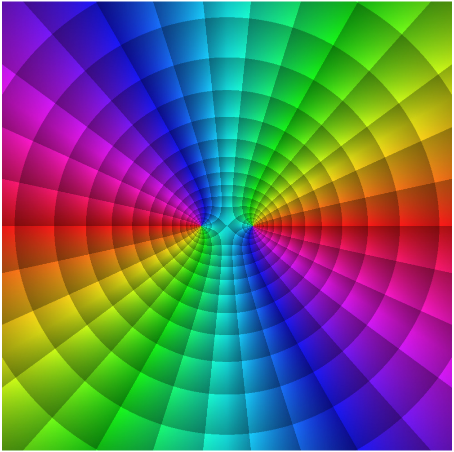


$f(z) = \tan(z)$

Colour Functions - Grid Examples

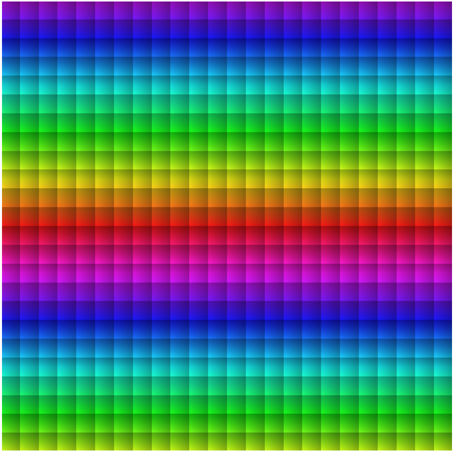


$f(z) = \sin(z)$

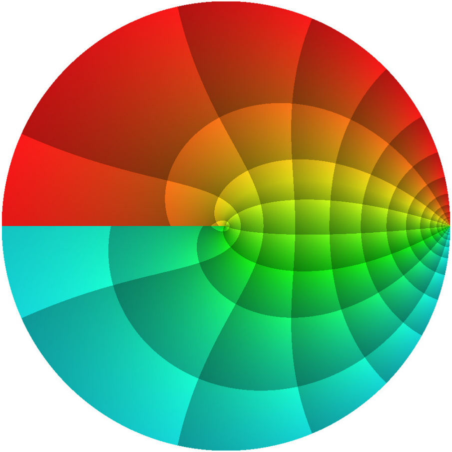


$f(z) = z^3 - 1$

Colour Functions - Conformal Examples

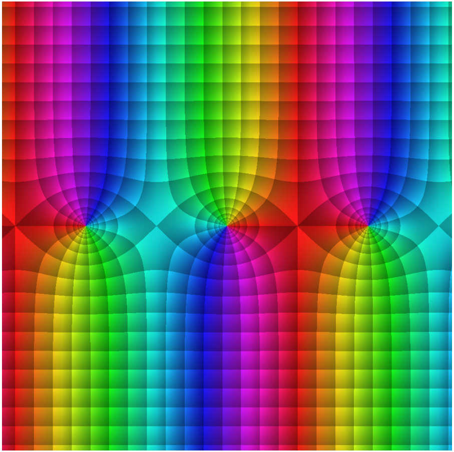


$f(z) = e^z$

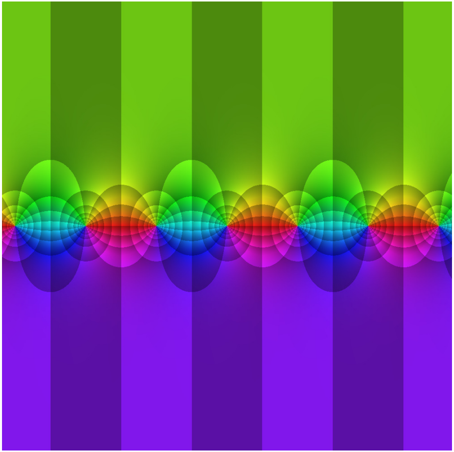


$f(z) = \frac{1}{i\pi} \log(z)$

Colour Functions - Conformal Examples

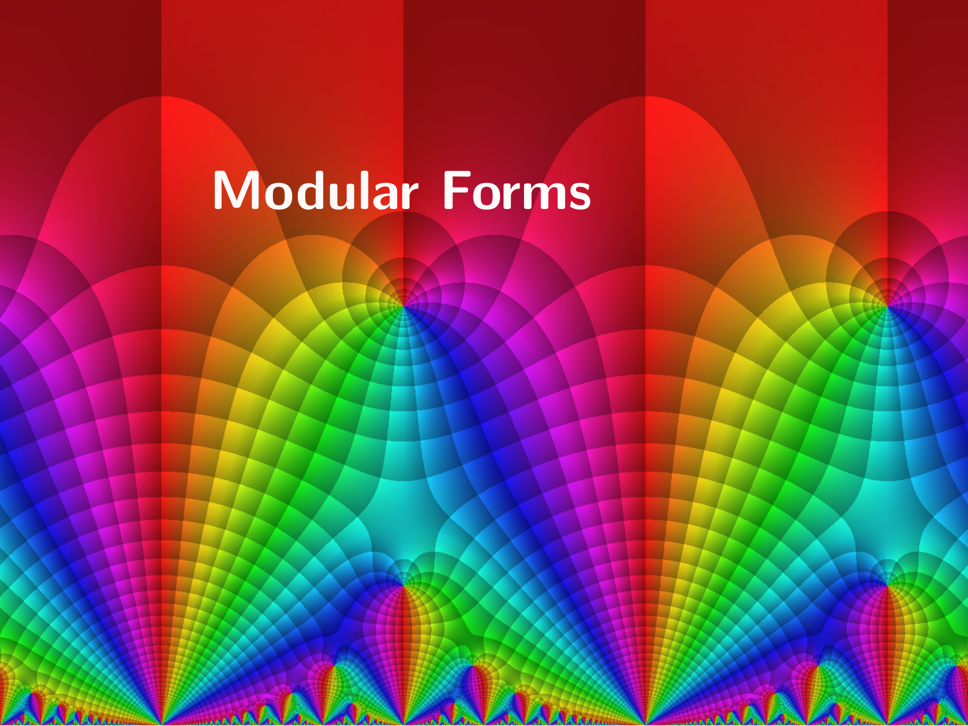


$f(z) = \sin(z)$



$f(z) = \tan(z)$

Modular Forms



Modular Group

Definition (Special Linear Group)

$$\mathsf{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$$

Generators

$$\mathsf{SL}_2(\mathbb{Z}) = \langle S, T \rangle\,, \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Definition (Group Action - Möbius Transformation)

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{za + b}{zc + d}, \quad z \in \hat{\mathbb{C}}$$

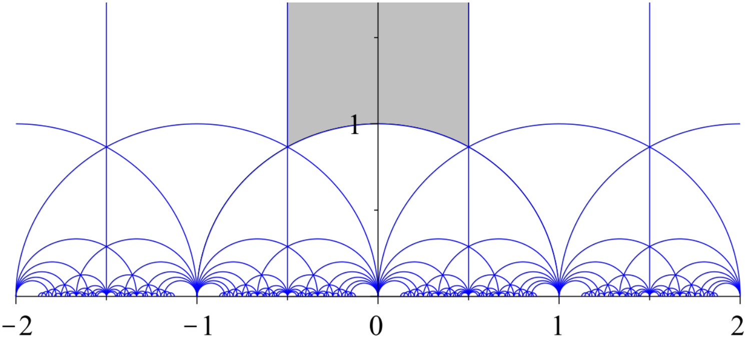
Fundamental Domains

Definition (Fundamental Domain)

A *fundamental domain* F for a subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is a closed subset of $\mathbb{H}$ such that:

1. Every $z \in \mathbb{H}$ is Γ-equivalent to a point in the closure of F.
2. No two distinct points in $\mathbb{H}$ are Γ-equivalent.

Fundamental Domains for $\mathrm{SL}_2(\mathbb{Z})$



Principle Fundamental Domain for $\mathrm{SL}_2(\mathbb{Z})$:

$$F = \{z \in \mathbb{H} | \; |\Re(z)| \leq 1/2, \; |z| \geq 1\}$$

Modular Transformation

Definition (Modular)

$f : \mathbb{H} \to \mathbb{C}$ transforms as a modular form of weight k if

$$f(\gamma \cdot \tau) = (c\tau + d)^k f(\tau) \quad \forall \tau \in \mathbb{H}, \gamma \in \mathsf{SL}_2(\mathbb{Z})$$

Remark

- As $\mathsf{SL}_2(\mathbb{Z}) = \langle S, T \rangle$ this is equivalent to
  - $f(\tau + 1) = f(\tau)$
  - $f(-1/\tau) = (\tau)^k f(\tau)$
- This means $f(\tau),\ \tau \in F$ completely determines our function.

Modular Forms

Definition (Modular Form of $\mathsf{SL}_2(\mathbb{Z})$)

A function $f : \mathbb{H} \to \mathbb{C}$ is a modular form, of weight k if

1. f transforms as a modular form of weight k
2. f is holomorphic on $\mathbb{H}$.
3. f is holomorphic at ∞

$M_k(\mathsf{SL}_2(\mathbb{Z}))$ is the space of modular forms of weight k.

Fourier Expansions

As $f(\tau+1) = f(\tau)$, can write $f = \sum_{n\in\mathbb{Z}} a_n q^n, \; q = e^{2\pi\tau i}$

f is *holomorphic at* ∞ iff $a_n = 0, \; \forall n < 0$

Eisenstein Series

Definition (Eisenstein Series of Weight k)

Let $k \geq 4, \ \tau \in \mathbb{H}$. We define the function

$$G_k(\tau) = \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq 0}} \frac{1}{(m\tau + n)^k}$$

Proposition

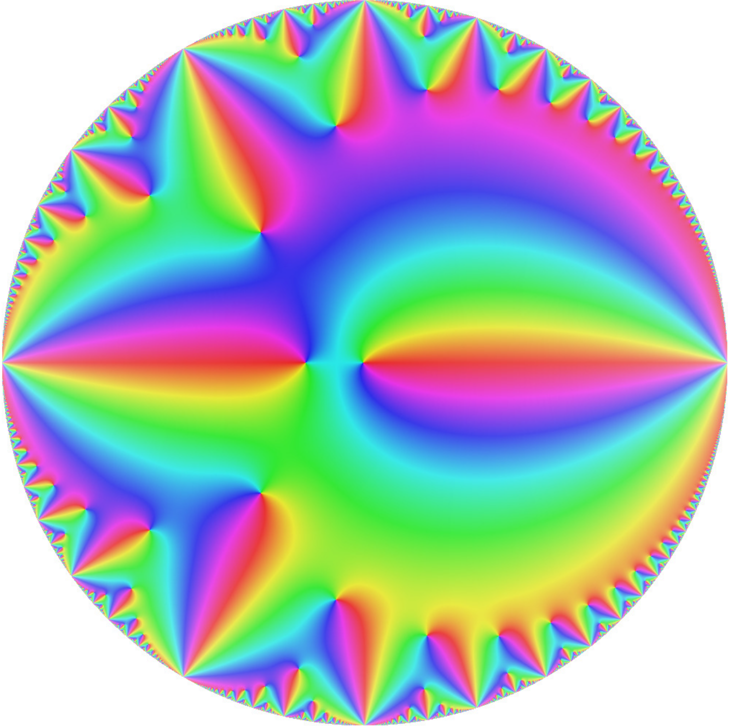
G_k is an non-zero modular form of weight k.

- $G_k(\tau + 1) = G_k(\tau)$
- $G_k(-1/\tau) = (\tau)^k G_k(\tau)$

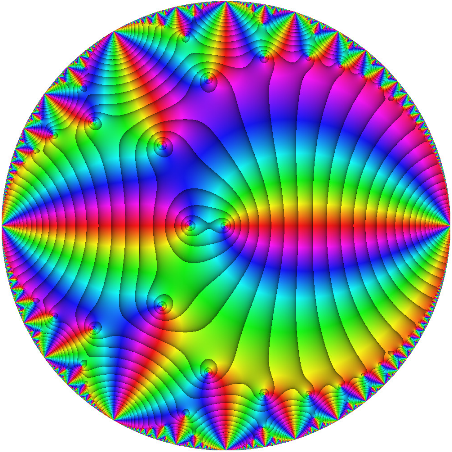
Let Λ be a lattice in $\mathbb{C}$.

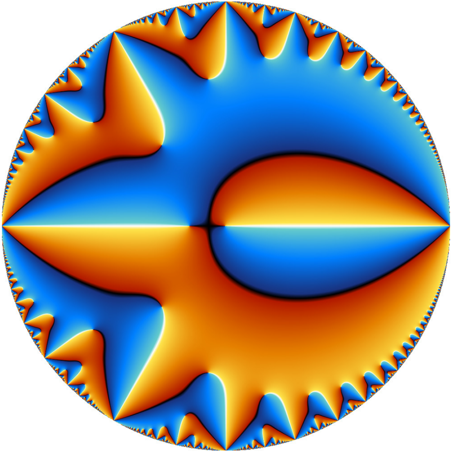
$$\sum_{0 \neq z \in \Lambda} \frac{1}{|z|^k}$$

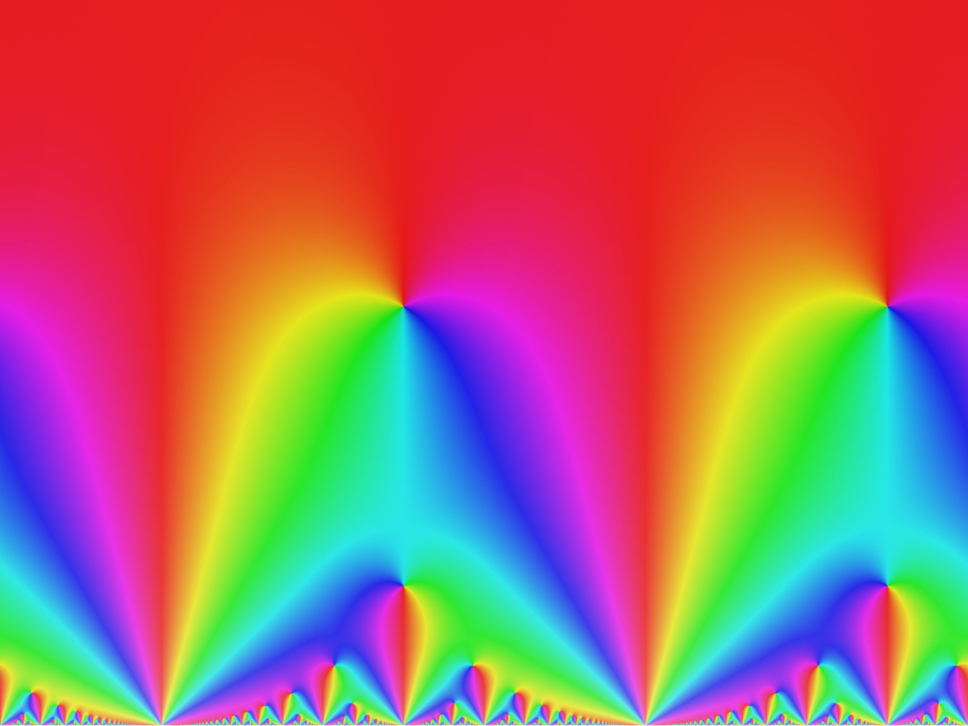
Is abs conv for $k > 2$

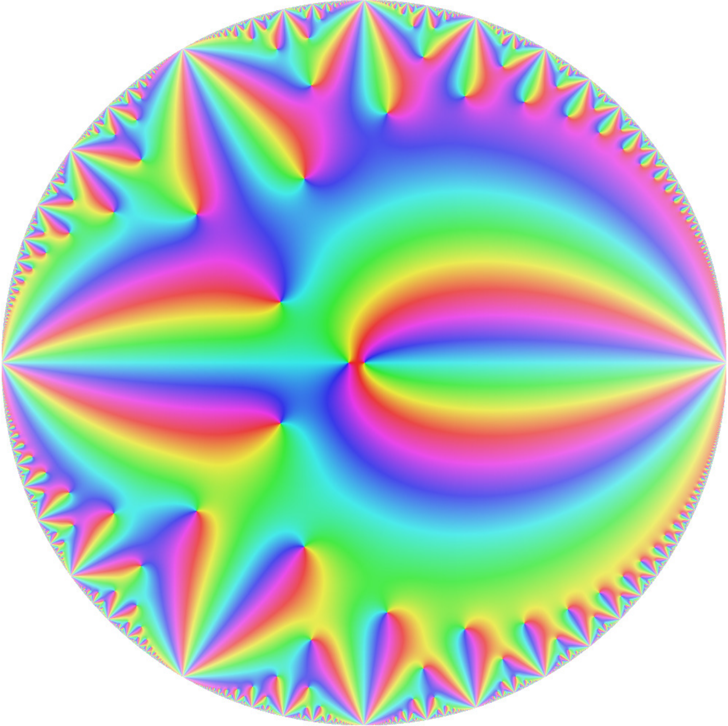


E_4 Graphs

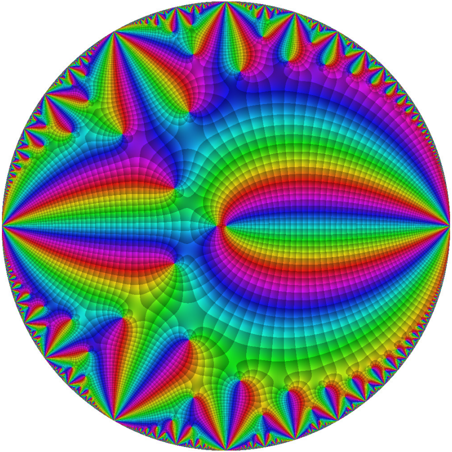


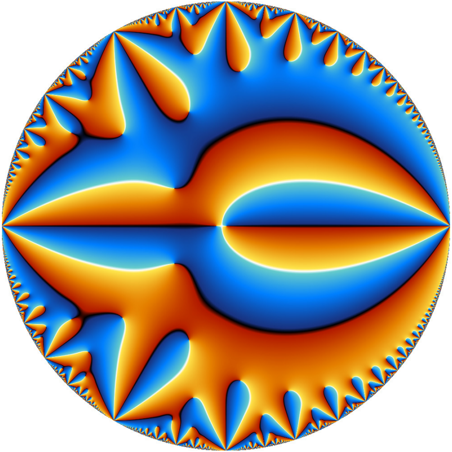


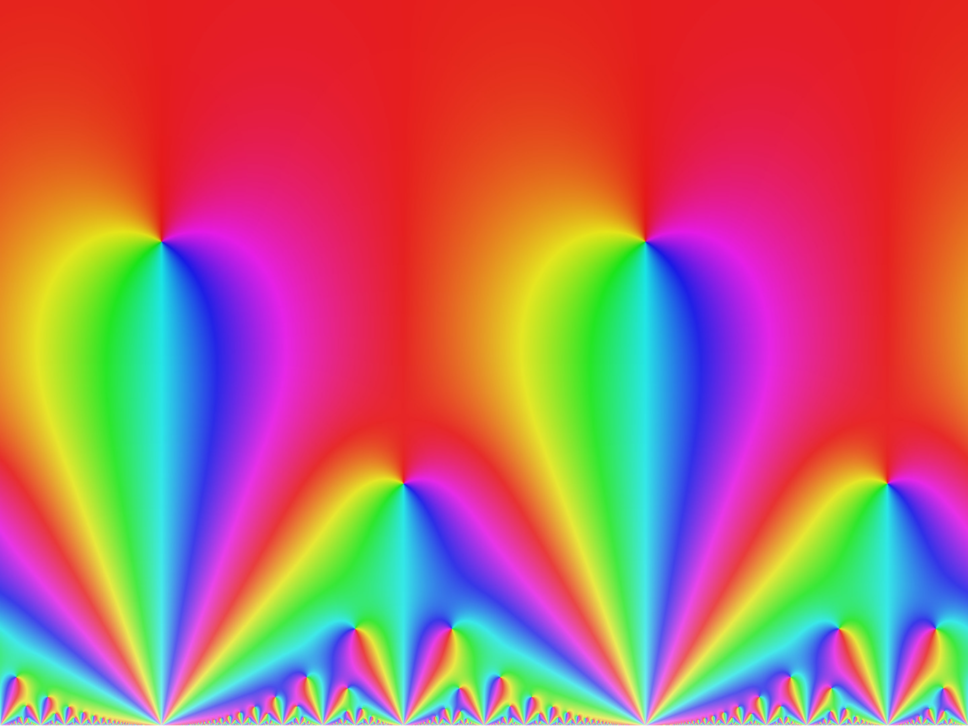


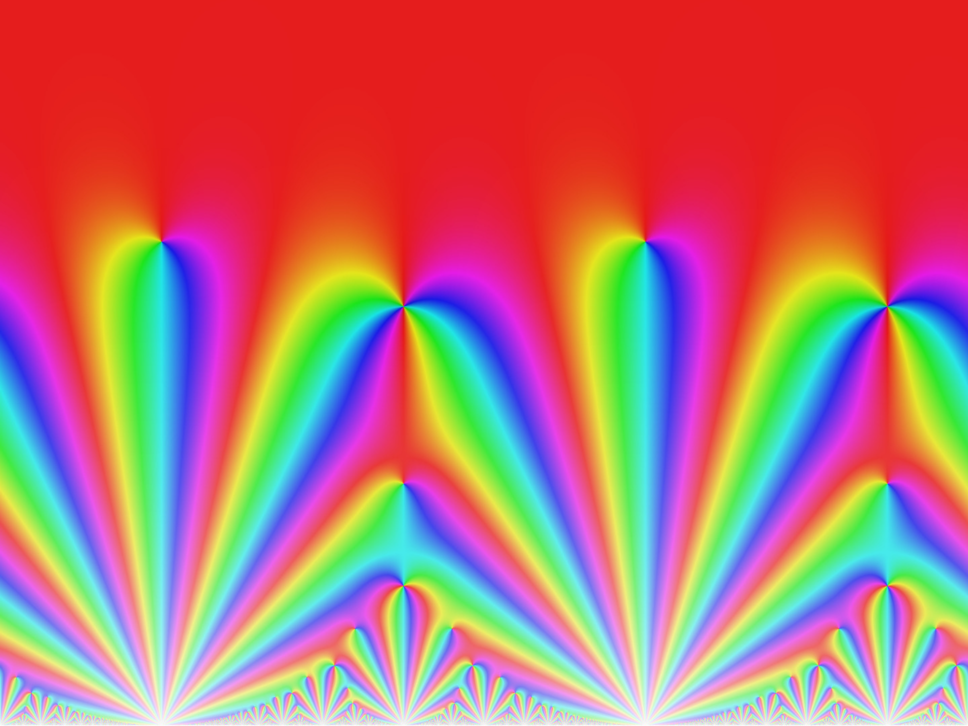


E_6 Graphs









Fourier Expansion

Proposition (Fourier Expansion for G_k)

$$G_k(\tau) = 2\zeta(k)\left(1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n\right)$$

Divisor Function

$$\sigma_t(n) = \sum_{d|n} d^t$$

Bernoulli Numbers

$$\frac{z}{e^z - 1} = \sum_{n\geq 0} B_k \frac{z^n}{n!}$$

Definition (Normalized Eisenstein Series)

$$E_k = \frac{1}{2\zeta(k)}G_k = 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n$$

(Can also normalise so q-coefficient is 1)

Cusp Forms - Δ

Definition (Cusp Form)

A modular form f is a *cusp form*$(S_k(\mathrm{SL}_2(\mathbb{Z})))$ if it vanishes at ∞. This is equivalent to having $a_0 = 0$ in the Fourier expansion.

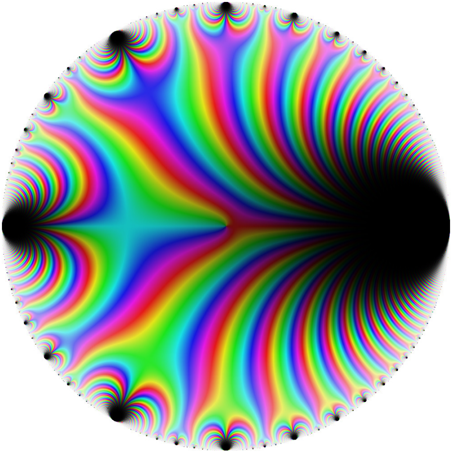
Definition (Modular Discriminant)

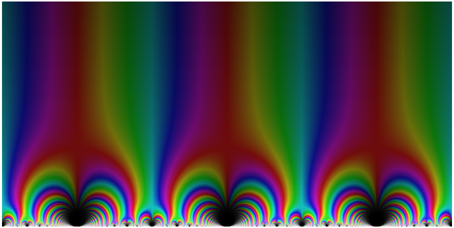
$$\Delta = (2\pi)^{12} \frac{E_4(z)^3 - E_6(z)^2}{1728}$$

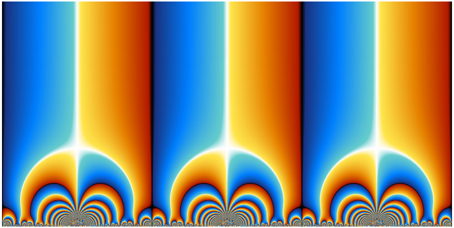
Properties

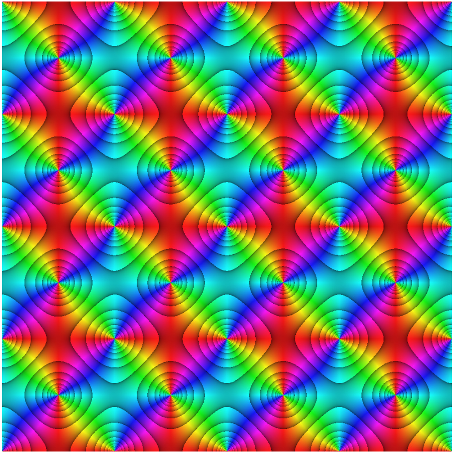
- Δ is a cusp form of weight 12, $\Delta \in S_{12}$
- Δ is the non-zero cusp form of lowest weight.

△ Graphs

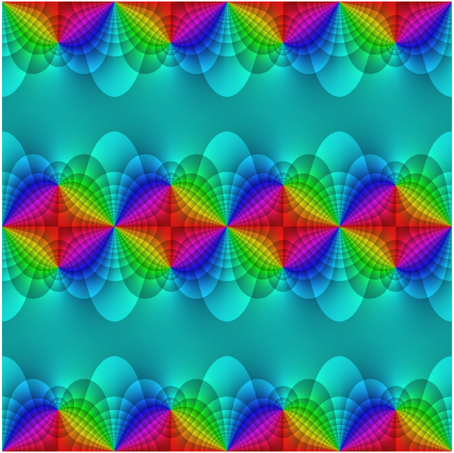








$\wp(\tau, 1 + 1i)$



$\wp(\tau, 1 + 4i)$

Modular Space Structure

Proposition

$M_k(\mathsf{SL}_2(\mathbb{Z})),\ S_k(\mathsf{SL}_2(\mathbb{Z}))$ are finite dim, complex vector spaces.

Valence/Structure Formula

For $f(z)$ non-zero, of weight k on $\mathsf{SL}_2(\mathbb{Z})$, then

$$\mathrm{ord}_\infty(f) + \frac{1}{2}\mathrm{ord}_i(f) + \frac{1}{3}\mathrm{ord}_\rho(f) \sum_{\substack{\omega \in F \\ \omega \neq i,p}} \mathrm{ord}_\omega(f) = \frac{k}{12}$$

Consequences

Any $f \in M_k(\mathsf{SL}_2(\mathbb{Z}))$ can be written in the form

$$f(z) = \sum_{4i+6j} c_{i,j} E_4(z)^i E_6(z)^j$$

Essentially giving us a basis for $M_k(\mathsf{SL}_2(\mathbb{Z}))$.

Modular Functions

Definition (Modular Function)

$f : \mathbb{H} \to \mathbb{C}$ is a modular function of weight k if

1. f transforms as a modular form of weight k
2. f is meromorphic on $\mathbb{H}$, may have a pole for $\tau \to i\infty \cup \mathbb{Q}$

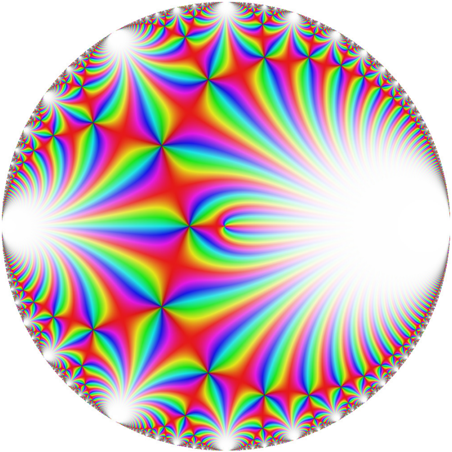
Definition (Klien J-Invariant - Weight 0 Modular Function)

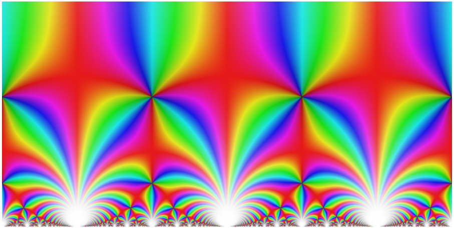
$$j(z) = 1728\frac{(60G_4(z))^3}{\Delta(z)} = 1728\frac{E_4(z)^3}{E_4(z)^3 - E_6(z)^2}$$

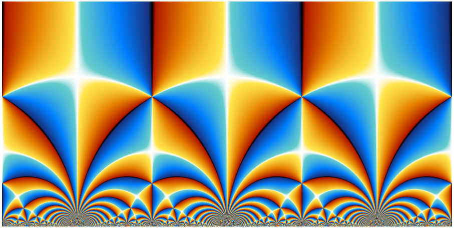
Proposition

- Modular functions of weight 0 are the rational functions of j.
- If a modular function has no poles on $\mathbb{H}$, and $\text{ord}_\infty(f) = r$, we can write f as a degree r polynomial in j.

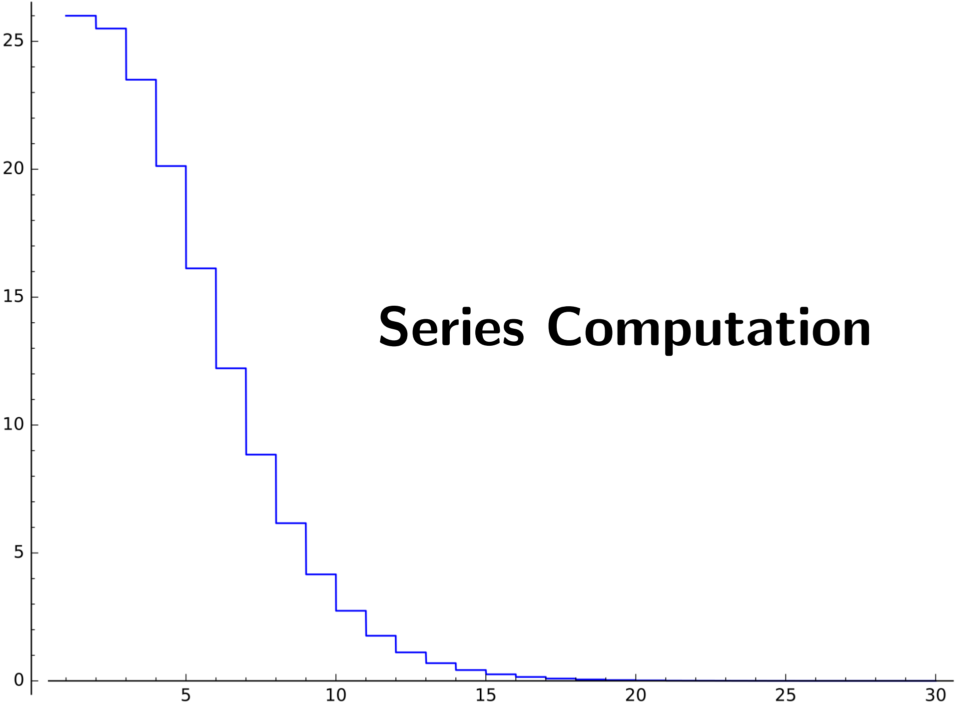
J Invariant Graphs







Series Computation



Error Bounding

Definition (Error Bound of Tail)

For convergent $\sum_{k=0}^{\infty} a_k$, $E(n,x) \geq \sum_{k=n}^{\infty} a_k$ is an n-bound.

Ideally, a bound will be easily solvable for a given precision.

Example (Some Bounds)

- $\sum_{k=0}^{n-1} \frac{(-1)^k x^{2k+1}}{(2k+1)!}$ is an n-bound for sine taylor series, as it is alternating and decreasing.
- $|\sum_{k=n}^{\infty} \frac{z^k}{k!}| \leq |\frac{1}{1-z^n}|$ is an n-bound for geometric overestimation of exponential taylor series - broadly applicable.

Often, a more accurate bound may not be worth the extra computation vs just computing more terms of the series.

Eisenstein Lambert N-Bound

Below, let $q = |q|$ for convenience. For E_4, this is an n-bound. This converges quickly on F, not so much as $q \to 1$

$$\frac{q^n}{(1-q)^2}\left(n^3 + \frac{3n^2 q}{1-q} + \frac{3nq(q+1)}{(1-q)^2} + \frac{q\left(q^2+4q+1\right)}{(1-q)^3}\right)$$

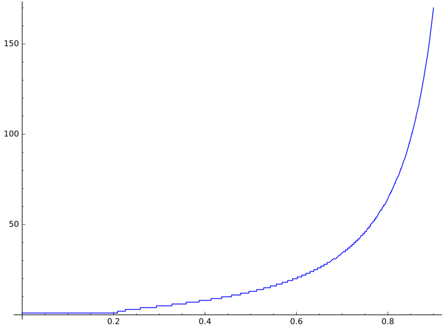
For E_6:

$$\frac{q^n}{(1-q)^2}\left(n^5 + \frac{5n^4 q}{1-q} + \frac{10n^3 q(q+1)}{(1-q)^2} + \frac{10n^2 q(q^2+4q+1)}{(1-q)^3} + \frac{5nq(q+1)(q^2+10q+1)}{(1-q)^4} + \frac{q^2(q^3+26q^2+66q+26)+q}{(1-q)^5}\right)$$

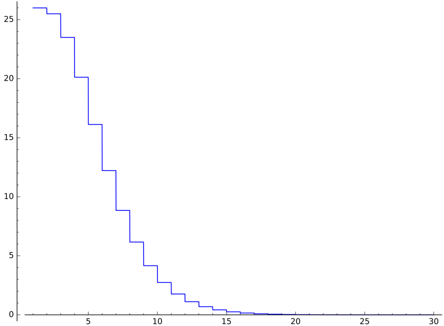
The n-bound for E_k is $\frac{q^n}{1-q}\sum_{i=0}^{\infty} q^i (n+i)^{k-1} = \frac{q^n}{1-q}\Phi(q, 1-k, n)$.

where Φ is the Lerch transcendent function, for which further expressions exist.

E_4 Error Graphs



n such that error less than 1



Error as n increases for $q = 0.5$

Horner's Method

Algorithm to evaluatate polynomials

$$f(q) = a_N q^N + \cdots + a_1 q + a_0$$
$$b_N = a_N$$
$$b_{N-1} = a_{N-1} + q b_N$$
$$\vdots$$
$$b_0 = a_0 + q b_1 = f(q).$$

Improvements

$\Theta(N^{1/2})$ expensive multiplications with BSGS algorithm.

(Paterson and Stockmeyer 1973)

Theta Functions

Definition (Jacobi Theta Constants)

$$\vartheta_0(\tau) = \sum_{n\in\mathbb{Z}} q^{n^2}$$

$$\vartheta_1(\tau) = \sum_{n\in\mathbb{Z}} (-1)^n q^{n^2}$$

$$\vartheta_2(\tau) = q^{\frac{1}{4}} \sum_{n\in\mathbb{Z}} q^{n(n+1)}$$

Transformation Rules for Theta Functions

$$\vartheta(-1/\tau) = \sqrt{\tau/i}\; \vartheta(\tau)$$

This follows from application of Poisson summation

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \mathcal{F}(f)(k)$$

Identities of the Theta Function

Eisenstein Identities

Due to the finite dimensionality of M_4, M_6, and the transformation rules for ϑ we have:

$$E_4 = \frac{1}{2}\left(\vartheta_0^8 + \vartheta_1^8 + \vartheta_2^8\right)$$

$$E_6 = \frac{1}{2}\left(-3\vartheta_2^8\left(\vartheta_0^4 + \vartheta_1^4\right) + \vartheta_0^{12} + \vartheta_1^{12}\right)$$

Consequences

ϑ-decompositions exist for:

- Modular forms of level one.
- Modular functions of weight 0.

J-Invariant, Discriminant

$$\Delta = (2\pi)^{12}\left(\frac{1}{2}\vartheta_0\vartheta_1\vartheta_2\right)^8$$

$$j = 32\frac{\left(\vartheta_0^8 + \vartheta_1^8 + \vartheta_2^8\right)^3}{\left(\vartheta_0\vartheta_1\vartheta_2\right)^8}$$

Computational Motivation

Why derive these Identities?

- ϑ q-series converges far more rapidly than E_k.
- Extensive optimisation - by Hart & Johansson 2018 (Used in Arb)

Sparse and Dense Exponent Sequences

Exponent sequence of $\sum_{n=0}^{N} c_n q^n$ is $E = (e_n)_{n=0}^{N}$ Take T where $e_N \leq T$, and $e_{N+1} \geq T$

- E is *dense* if $N \in \Omega(T)$
- E is *sparse* if $e_n \in \Theta(n^\alpha)$

Addition Sequences

Addition Sequences

A set $A \subset \mathbb{N}$ such that $1 \in A$, and $\forall c \in A_{\geq 1}\ \exists a, b \in A,\ a + b = c$.
For example, the Fibonacci sequence.

For any sequence of positive integers, we can construct an addition sequence by adding elements - "double and add" algorithm.

Short Addition Sequences for Theta

We can form addition sequences from the exponent sequences, allowing us to more easily group expensive multiplications of q.

Hart & Johansson found good addition sequences for the theta functions, and implemented them in Arb using a variation of BSGS.

Ball Arithmetic

Definition (Ball Function)

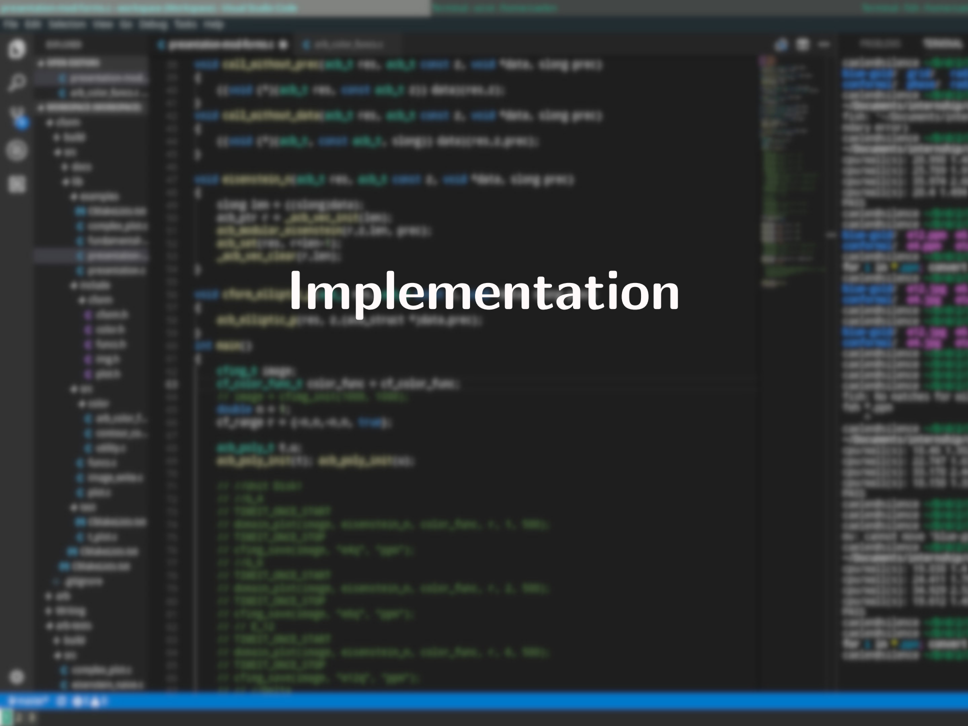
A ball implementation of $f : A \to B$ is $F : A \to B$ such that for $X \subset A$, $F(X) \subset B$ and $f(X) \subset F(X)$ - *inclusion principle*.

Benefits of Ball Arithmetic

- Guaranteed inclusion of value.
- Reduction of analysis of arithmetic error.
- Lazy infinities - crude bound when input exceeds precision.

Drawbacks of Ball Arithmetic

- Overestimation.
- Error precomputation.
- Algorithm convergence.



Implementation

Scientific Computing Environments

High Level Languages - Mathematica, Sage

- Interpreted, interactive scripting.
- Performance issues with scripting.
- Interfaces for native extension code.
- Sage: Flexibility due to Python, modular development.
- Mathematica: Commercial stability, monolithic.

Low Level Languages - C/C++

- Less intuitive, compiled, no unified mathematical framework.
- Low level control of types, memory, processing, optimised.
- Some excellent libraries for computer algebra make easier.
- Can be used as a black box for other languages.

C for Mathematics - ARB, FLINT, MPFR/GMP

GMP/MPFR

- Provides arbitrary size/precision integer/rational numbers.
- Arithmetic, with standard rounding behaviour.
- Extended in MPC, MPFI to complex numbers and interval arithmetic.

FLINT, ARB

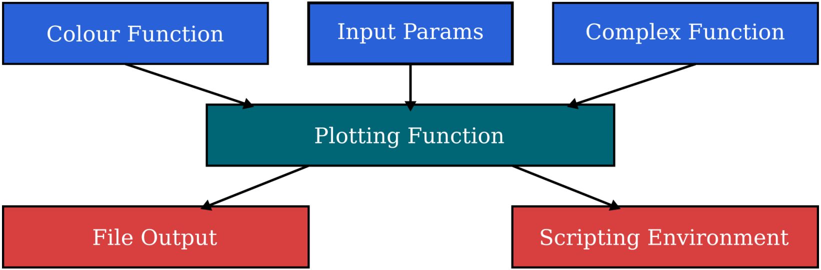
- Libraries specifically for number theory.
- FLINT handles and optimises GMP/MPFR for mathematics.
- FLINT also has linear algebra, polynomial/matrix support.
- ARB extends FLINT, ball arithmetic.
- ARB provides many useful functions, namely modern modular form implementations - addition sequence method.

C Form Library Structure

C Library Structure

- User interface - Header Files.
- Implementation - Compiled Binary Files.

C Form Library Interface



Algorithm Refinements

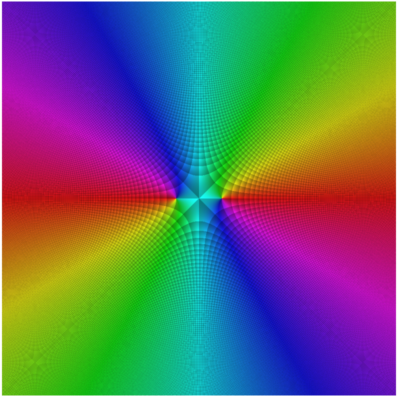
Improvements

- Convergence is faster on the fundamental domain.
- Can find $\gamma \in \mathsf{SL}_2(\mathbb{Z})$ taking any point to fundamental domain.
- All Eisenstein series are polynomials of E_4, E_6.
- Recursion and Caching.
- Parallelisation.

Precision

Series Length Prediction

- Estimate the precision needed for arithmetic, repeat.
- Output precision tested for fitness of purpose.
- Precomputed tables, predictions.
- Necessary error for plotting.



Generalisation

Congruence Subgroups

Standard Congruence Subgroups of $\mathrm{SL}_2(\mathbb{Z})$

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \bmod N \right\}$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \bmod N \right\}$$

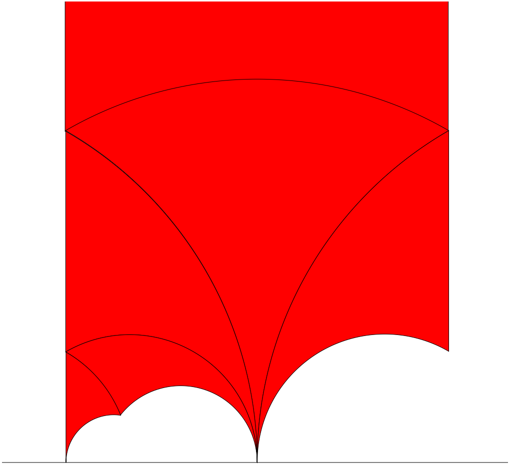
$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N \right\}$$

Definition (Congruence Subgroup of Level N)

A subgroup $G \subset \mathrm{SL}_2(\mathbb{Z})$ such that $\Gamma(N) \subset G$. The maximal N such that $\Gamma(N) \subset G$ is the level of G.

Fundamental Domains

$\Gamma_1(4)$



Eisenstein Series of level N

Definition (Eisenstein Series)

$$G_k^a(\tau) = G_k^{a \bmod N}(\tau) = \sum_{\substack{m \in \mathbb{Z}^2 \\ m \equiv a \bmod N}} \frac{1}{(m_1\tau + m_2)^k}$$

Definition (Dedekind Eta Function)

$$\eta(\tau) = q^{1/24} \prod^{\infty} n = 1(1 - q^n)$$

η Graphs