The j-function, the golden ratio, and rigid meromorphic cocycles

Henri Darmon, McGill University

CNTA XV, July 2018

Reminiscences of CNTA 0

- The 1987 CNTA in Quebec City was an exciting one for me personally, and also for number theory;

Reminiscences of CNTA 0

• The 1987 CNTA in Quebec City was an exciting one for me personally, and also for number theory;

• Karl Rubin had just exhibited the first examples of elliptic curves (with CM) with finite Shafarevich-Tate groups, building on ideas of Thaine;

Reminiscences of CNTA 0

• The 1987 CNTA in Quebec City was an exciting one for me personally, and also for number theory;

• Karl Rubin had just exhibited the first examples of elliptic curves (with CM) with finite Shafarevich-Tate groups, building on ideas of Thaine;

• I was just about to start graduate school, and these lectures made a strong impression on me;

Reminiscences of CNTA 0

• The 1987 CNTA in Quebec City was an exciting one for me personally, and also for number theory;

• Karl Rubin had just exhibited the first examples of elliptic curves (with CM) with finite Shafarevich-Tate groups, building on ideas of Thaine;

• I was just about to start graduate school, and these lectures made a strong impression on me;

• It was at CNTA 0 that I really met for the first time many future colleagues: Claude, Jean-Marie, Damien, Hershy, Ram and Kumar Murty...

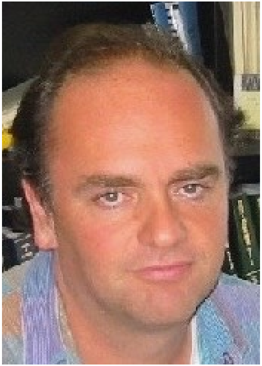
Andrew Granville

- Andrew Granville was also present at the meeting, having just finished writing his PhD under Paulo Ribenboim;

Andrew Granville

- Andrew Granville was also present at the meeting, having just finished writing his PhD under Paulo Ribenboim;

Andrew at CNTA 0



Andrew Today

The j-function, the golden ratio, and rigid meromorphic cocycles

Henri Darmon, McGill University

CNTA, July 2018

This is joint work with Jan Vonk

The modular function j

The modular function $j(z)$ is the unique holomorphic function on $\mathcal{H} := \{z \in \mathbb{C},\ \mathrm{Im}(z) > 0\}$,

The modular function j

The modular function $j(z)$ is the unique holomorphic function on $\mathcal{H} := \{z \in \mathbb{C},\ \mathrm{Im}(z) > 0\}$, satisfying

$$j(z+1) = j(z), \qquad j(-1/z) = j(z),$$

The modular function j

The modular function $j(z)$ is the unique holomorphic function on $\mathcal{H} := \{z \in \mathbb{C},\ \mathrm{Im}(z) > 0\}$, satisfying

$$j(z+1) = j(z), \qquad j(-1/z) = j(z),$$

$$j(q) = \frac{1}{q} + 744 + 196884q + \cdots \qquad \text{with } q = e^{2\pi i z}.$$

The modular function j

The modular function $j(z)$ is the unique holomorphic function on $\mathcal{H} := \{z \in \mathbb{C},\ \mathrm{Im}(z) > 0\}$, satisfying

$$j(z+1) = j(z), \qquad j(-1/z) = j(z),$$

$$j(q) = \frac{1}{q} + 744 + 196884q + \cdots \qquad \text{with } q = e^{2\pi i z}.$$

This function crops up in many parts of mathematics:

The modular function j

The modular function $j(z)$ is the unique holomorphic function on $\mathcal{H} := \{z \in \mathbb{C},\ \mathrm{Im}(z) > 0\}$, satisfying

$$j(z+1) = j(z), \qquad j(-1/z) = j(z),$$

$$j(q) = \frac{1}{q} + 744 + 196884q + \cdots \qquad \text{with } q = e^{2\pi i z}.$$

This function crops up in many parts of mathematics: complex analysis (proof of the uniformisation theorem),

The modular function j

The modular function $j(z)$ is the unique holomorphic function on $\mathcal{H} := \{z \in \mathbb{C},\ \mathrm{Im}(z) > 0\}$, satisfying

$$j(z+1) = j(z), \qquad j(-1/z) = j(z),$$

$$j(q) = \frac{1}{q} + 744 + 196884q + \cdots \qquad \text{with } q = e^{2\pi i z}.$$

This function crops up in many parts of mathematics: complex analysis (proof of the uniformisation theorem), elliptic curves and number theory,

The modular function j

The modular function $j(z)$ is the unique holomorphic function on $\mathcal{H} := \{z \in \mathbb{C},\ \mathrm{Im}(z) > 0\}$, satisfying

$$j(z+1) = j(z), \qquad j(-1/z) = j(z),$$

$$j(q) = \frac{1}{q} + 744 + 196884q + \cdots \qquad \text{with } q = e^{2\pi i z}.$$

This function crops up in many parts of mathematics: complex analysis (proof of the uniformisation theorem), elliptic curves and number theory, finite group theory (monstrous moonshine),

The modular function j

The modular function $j(z)$ is the unique holomorphic function on $\mathcal{H} := \{z \in \mathbb{C},\ \mathrm{Im}(z) > 0\}$, satisfying

$$j(z+1) = j(z), \qquad j(-1/z) = j(z),$$

$$j(q) = \frac{1}{q} + 744 + 196884q + \cdots \qquad \text{with } q = e^{2\pi i z}.$$

This function crops up in many parts of mathematics: complex analysis (proof of the uniformisation theorem), elliptic curves and number theory, finite group theory (monstrous moonshine), etc.

Special values, or singular moduli

A *singular modulus* is a special value of j at a quadratic imaginary argument (CM point) in $\mathcal{H}$.

Special values, or singular moduli

A *singular modulus* is a special value of j at a quadratic imaginary argument (CM point) in $\mathcal{H}$.

The *theory of complex multiplication* asserts that these values are *algebraic integers*, and enjoy many remarkable properties.

Special values, or singular moduli

A *singular modulus* is a special value of j at a quadratic imaginary argument (CM point) in $\mathcal{H}$.

The *theory of complex multiplication* asserts that these values are *algebraic integers*, and enjoy many remarkable properties.

Examples:

$j(i) = 1728$; $\quad j\left(\frac{1+\sqrt{-3}}{2}\right) = 0$; $\quad j\left(\frac{1+\sqrt{-7}}{2}\right) = -3375$.

Special values, or singular moduli

A *singular modulus* is a special value of j at a quadratic imaginary argument (CM point) in $\mathcal{H}$.

The *theory of complex multiplication* asserts that these values are *algebraic integers*, and enjoy many remarkable properties.

Examples:

$j(i) = 1728; \qquad j\left(\frac{1+\sqrt{-3}}{2}\right) = 0; \qquad j\left(\frac{1+\sqrt{-7}}{2}\right) = -3375.$

$j\left(\frac{1+\sqrt{-23}}{2}\right) = w,$ where

Special values, or singular moduli

A *singular modulus* is a special value of j at a quadratic imaginary argument (CM point) in $\mathcal{H}$.

The *theory of complex multiplication* asserts that these values are *algebraic integers*, and enjoy many remarkable properties.

Examples:

$$j(i) = 1728; \qquad j\left(\frac{1+\sqrt{-3}}{2}\right) = 0; \qquad j\left(\frac{1+\sqrt{-7}}{2}\right) = -3375.$$

$$j\left(\frac{1+\sqrt{-23}}{2}\right) = w, \qquad \text{where}$$

$$w^3 + 3491750w^2 - 5151296875w + 12771880859375 = 0.$$

Special values, or singular moduli

A *singular modulus* is a special value of j at a quadratic imaginary argument (CM point) in $\mathcal{H}$.

The *theory of complex multiplication* asserts that these values are *algebraic integers*, and enjoy many remarkable properties.

Examples:

$j(i) = 1728$; $\quad j\left(\frac{1+\sqrt{-3}}{2}\right) = 0$; $\quad j\left(\frac{1+\sqrt{-7}}{2}\right) = -3375$.

$j\left(\frac{1+\sqrt{-23}}{2}\right) = w$, where

$$w^3 + 3491750w^2 - 5151296875w + 12771880859375 = 0.$$

It generates an interesting cubic extension of $\mathbb{Q}(\sqrt{-23})$.

Gauss composition and class groups

For τ quadratic, there is a unique primitive integral binary quadratic form $F(x, y) = Ax^2 + Bxy + Cy^2$ satisfying $A > 0$ and $F(\tau, 1) = 0$.

Gauss composition and class groups

For τ quadratic, there is a unique primitive integral binary quadratic form $F(x, y) = Ax^2 + Bxy + Cy^2$ satisfying $A > 0$ and $F(\tau, 1) = 0$.

$D := B^2 - 4AC$ is called the *discriminant* of τ.

Gauss composition and class groups

For τ quadratic, there is a unique primitive integral binary quadratic form $F(x, y) = Ax^2 + Bxy + Cy^2$ satisfying $A > 0$ and $F(\tau, 1) = 0$.

$D := B^2 - 4AC$ is called the *discriminant* of τ.

The set of $\mathbf{SL}_2(\mathbb{Z})$-equivalence classes of primitive integral binary quadratic forms of discriminant D forms a group under Gauss's composition law, denoted G_D: the *class group* of discriminant D.

Gauss composition and class groups

For τ quadratic, there is a unique primitive integral binary quadratic form $F(x, y) = Ax^2 + Bxy + Cy^2$ satisfying $A > 0$ and $F(\tau, 1) = 0$.

$D := B^2 - 4AC$ is called the *discriminant* of τ.

The set of $\mathbf{SL}_2(\mathbb{Z})$-equivalence classes of primitive integral binary quadratic forms of discriminant D forms a group under Gauss's composition law, denoted G_D: the *class group* of discriminant D.

Class groups have been intensely studied since the time of Gauss, and are fundamental objects in number theory.

Abelian extensions and Kronecker's theorem

The class group G_D measures the failure of the principle of unique factorisation in the ring of integers of $K = \mathbb{Q}(\sqrt{D})$,

Abelian extensions and Kronecker's theorem

The class group G_D measures the failure of the principle of unique factorisation in the ring of integers of $K = \mathbb{Q}(\sqrt{D})$, and also arises in the study of abelian extensions of K:

Abelian extensions and Kronecker's theorem

The class group G_D measures the failure of the principle of unique factorisation in the ring of integers of $K = \mathbb{Q}(\sqrt{D})$, and also arises in the study of abelian extensions of K:

If D is a fundamental discriminant, the group G_D is *canonically identified* with $\mathrm{Gal}(H_D/K)$, where H_D is the *Hilbert class field* associated to D.

Abelian extensions and Kronecker's theorem

The class group G_D measures the failure of the principle of unique factorisation in the ring of integers of $K = \mathbb{Q}(\sqrt{D})$, and also arises in the study of abelian extensions of K:

If D is a fundamental discriminant, the group G_D is *canonically identified* with $\mathrm{Gal}(H_D/K)$, where H_D is the *Hilbert class field* associated to D.

Theorem (Kronecker)

For quadratic $\tau \in \mathcal{H}$ of fundamental discriminant $D < 0$, the singular modulus $j(\tau)$ is an algebraic integer in H_D, and generates this field.

Differences of singular moduli and their factorisations

Gross, Zagier (1984). For all τ_1, τ_2 quadratic imaginary,

Differences of singular moduli and their factorisations

Gross, Zagier (1984). For all τ_1, τ_2 quadratic imaginary, the quantity

$$J(\tau_1, \tau_2) \quad := \quad j(\tau_1) - j(\tau_2)$$

is a *smooth* algebraic integer with an explicit factorisation.

Differences of singular moduli and their factorisations

Gross, Zagier (1984). For all τ_1, τ_2 quadratic imaginary, the quantity

$$J(\tau_1, \tau_2) \quad := \quad j(\tau_1) - j(\tau_2)$$

is a *smooth* algebraic integer with an explicit factorisation.

The norm of $J(\tau_1, \tau_2)$ to $\mathbb{Z}$ is divisible only by (large powers of) small primes.

Differences of singular moduli and their factorisations

Gross, Zagier (1984). For all τ_1, τ_2 quadratic imaginary, the quantity

$$J(\tau_1, \tau_2) \quad := \quad j(\tau_1) - j(\tau_2)$$

is a *smooth* algebraic integer with an explicit factorisation.

The norm of $J(\tau_1, \tau_2)$ to $\mathbb{Z}$ is divisible only by (large powers of) small primes.

The equation

$$J(\tau_1, \tau_2) + J(\tau_2, \tau_3) = J(\tau_1, \tau_3)$$

Differences of singular moduli and their factorisations

Gross, Zagier (1984). For all τ_1, τ_2 quadratic imaginary, the quantity

$$J(\tau_1, \tau_2) \quad := \quad j(\tau_1) - j(\tau_2)$$

is a *smooth* algebraic integer with an explicit factorisation.

The norm of $J(\tau_1, \tau_2)$ to $\mathbb{Z}$ is divisible only by (large powers of) small primes.

The equation

$$J(\tau_1, \tau_2) + J(\tau_2, \tau_3) = J(\tau_1, \tau_3)$$

expresses a "powerful" number as a sum of two "powerful" numbers.

An example

$D = -4$ and -163 have class number one,

An example

$D = -4$ and -163 have class number one, and,

$$j(i) = 1728 = 2^6 \cdot 3^3,$$

An example

$D = -4$ and -163 have class number one, and,

$$j(i) = 1728 = 2^6 \cdot 3^3, \qquad j\left(\frac{1+\sqrt{-163}}{2}\right) = -2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3,$$

An example

$D = -4$ and -163 have class number one, and,

$$j(i) = 1728 = 2^6 \cdot 3^3, \qquad j\left(\tfrac{1+\sqrt{-163}}{2}\right) = -2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3,$$

$$J\left(\frac{1+\sqrt{-163}}{2}, i\right) = -2^6 \cdot 3^6 \cdot 7^2 \cdot 11^2 \cdot 19^2 \cdot 127^2 \cdot 163,$$

An example

$D = -4$ and -163 have class number one, and,

$$j(i) = 1728 = 2^6 \cdot 3^3, \qquad j\left(\frac{1+\sqrt{-163}}{2}\right) = -2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3,$$

$$J\left(\frac{1+\sqrt{-163}}{2}, i\right) = -2^6 \cdot 3^6 \cdot 7^2 \cdot 11^2 \cdot 19^2 \cdot 127^2 \cdot 163,$$

$$2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3 + 2^6 3^3 = 2^6 \cdot 3^6 \cdot 7^2 \cdot 11^2 \cdot 19^2 \cdot 127^2 \cdot 163,$$

An example

$D = -4$ and -163 have class number one, and,

$$j(i) = 1728 = 2^6 \cdot 3^3, \qquad j\left(\tfrac{1+\sqrt{-163}}{2}\right) = -2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3,$$

$$J\left(\frac{1+\sqrt{-163}}{2}, i\right) = -2^6 \cdot 3^6 \cdot 7^2 \cdot 11^2 \cdot 19^2 \cdot 127^2 \cdot 163,$$

$$2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3 + 2^6 3^3 = 2^6 \cdot 3^6 \cdot 7^2 \cdot 11^2 \cdot 19^2 \cdot 127^2 \cdot 163,$$

$$2^{12} \cdot 5^3 \cdot 23^3 \cdot 29^3 + 1 = 3^3 \cdot 7^2 \cdot 11^2 \cdot 19^2 \cdot 127^2 \cdot 163.$$

An example

$D = -4$ and -163 have class number one, and,

$$j(i) = 1728 = 2^6 \cdot 3^3, \qquad j\left(\tfrac{1+\sqrt{-163}}{2}\right) = -2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3,$$

$$J\left(\frac{1+\sqrt{-163}}{2}, i\right) = -2^6 \cdot 3^6 \cdot 7^2 \cdot 11^2 \cdot 19^2 \cdot 127^2 \cdot 163,$$

$$2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3 + 2^6 3^3 = 2^6 \cdot 3^6 \cdot 7^2 \cdot 11^2 \cdot 19^2 \cdot 127^2 \cdot 163,$$

$$2^{12} \cdot 5^3 \cdot 23^3 \cdot 29^3 + 1 = 3^3 \cdot 7^2 \cdot 11^2 \cdot 19^2 \cdot 127^2 \cdot 163.$$

Similar examples arise from any $J(\tau_1, \tau_2)$ for which $j(\tau_1)$ and $j(\tau_2)$ are integers.

The abc conjecture

The abc conjecture predicts that there can not be “too many” such instances.

The abc conjecture

The abc conjecture predicts that there can not be "too many" such instances.

Why doesn't complex multiplication contradict the abc conjecture?

The Gauss class number problem

Theorem (Gauss; Heilbronn; Baker, Heegner, Stark)

There are finitely many $D < 0$ with for which $G_D = \{1\}$, namely

$$-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43 - 67, -163.$$

The Gauss class number problem

Theorem (Gauss; Heilbronn; Baker, Heegner, Stark)

There are finitely many $D < 0$ with for which $G_D = \{1\}$, namely

$$-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43 - 67, -163.$$

Hence there are finitely many *quadratic imaginary τ for which $j(\tau) \in \mathbb{Z}$.*

The Gauss class number problem

Theorem (Gauss; Heilbronn; Baker, Heegner, Stark)

There are finitely many $D < 0$ with for which $G_D = \{1\}$, namely

$$-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43 - 67, -163.$$

Hence there are finitely many *quadratic imaginary τ for which $j(\tau) \in \mathbb{Z}$.*

The abc conjecture is saved!

The Gauss class number problem

Theorem (Gauss; Heilbronn; Baker, Heegner, Stark)

There are finitely many $D < 0$ with for which $G_D = \{1\}$, namely

$$-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43 - 67, -163.$$

Hence there are finitely many *quadratic imaginary τ for which $j(\tau) \in \mathbb{Z}$.*

The abc conjecture is saved!

Granville, Stark (2000): A strong form of the abc conjecture implies the non-existence of Siegel zeroes for L-functions attached to odd Dirichlet characters.

How to disprove the abc conjecture ;-)

Real quadratic discriminants *behave differently* from negative ones.

How to disprove the abc conjecture ;-)

Real quadratic discriminants *behave differently* from negative ones.

Conjecture (Gauss)

There are infinitely many $D > 0$ for which $G_D = \{1\}$.

How to disprove the abc conjecture ;-)

Real quadratic discriminants *behave differently* from negative ones.

Conjecture (Gauss)

There are infinitely many $D > 0$ *for which* $G_D = \{1\}$.

Empirically, it seems like the majority of prime $D > 0$–somewhat over $3/4$– have this "class number one" property.

How to disprove the abc conjecture ;-)

Real quadratic discriminants *behave differently* from negative ones.

Conjecture (Gauss)

There are infinitely many $D > 0$ for which $G_D = \{1\}$.

Empirically, it seems like the majority of prime $D > 0$–somewhat over $3/4$– have this "class number one" property.

One might disprove the abc conjecture by *extending* the definition of $J(\tau_1, \tau_2)$ so that it can be evaluated at real quadratic, and not just imaginary quadratic, arguments!

The motivating question

Let $\varphi := \left(\frac{1+\sqrt{5}}{2}\right)$ be the golden ratio.

The motivating question

Let $\varphi := \left(\frac{1+\sqrt{5}}{2}\right)$ be the golden ratio.

Question. What is $j(\varphi)$....?

The motivating question

Let $\varphi := \left(\frac{1+\sqrt{5}}{2}\right)$ be the golden ratio.

Question. What is $j(\varphi)$....?

Answer.

The motivating question

Let $\varphi := \left(\frac{1+\sqrt{5}}{2}\right)$ be the golden ratio.

Question. What is $j(\varphi)$....?

Answer. It depends on p.

The motivating question

Let $\varphi := \left(\frac{1+\sqrt{5}}{2}\right)$ be the golden ratio.

Question. What is $j(\varphi)$....?

Answer. It depends on p.

Here, p is a prime congruent to 2 or 3 modulo 5.

The motivating question

Let $\varphi := \left(\frac{1+\sqrt{5}}{2}\right)$ be the golden ratio.

Question. What is $j(\varphi)$....?

Answer. It depends on p.

Here, p is a prime congruent to 2 or 3 modulo 5.

The rest of the talk will try to explain this cryptic answer.

p-adic methods

Imaginary and real quadratic fields differ in that their usual completions are isomorphic to $\mathbb{C}$ and $\mathbb{R}$ respectively.

p-adic methods

Imaginary and real quadratic fields differ in that their usual completions are isomorphic to $\mathbb{C}$ and $\mathbb{R}$ respectively.

After fixing a prime p, one can consider the p-adic distance, whereby two rational numbers are decreed to be close if their difference is divisible by a high power of p.

p-adic methods

Imaginary and real quadratic fields differ in that their usual completions are isomorphic to $\mathbb{C}$ and $\mathbb{R}$ respectively.

After fixing a prime p, one can consider the p-adic distance, whereby two rational numbers are decreed to be close if their difference is divisible by a high power of p.

The completion of $\mathbb{Q}$ with respect to this new metric is called the field $\mathbb{Q}_p$ of p-adic numbers.

p-adic methods

Imaginary and real quadratic fields differ in that their usual completions are isomorphic to $\mathbb{C}$ and $\mathbb{R}$ respectively.

After fixing a prime p, one can consider the p-adic distance, whereby two rational numbers are decreed to be close if their difference is divisible by a high power of p.

The completion of $\mathbb{Q}$ with respect to this new metric is called the field $\mathbb{Q}_p$ of p-adic numbers.

The field $\mathbb{Q}_p$ plays the role of $\mathbb{R}$, while the counterpart of $\mathbb{C}$ is

$$\mathbb{C}_p := \widehat{\bar{\mathbb{Q}}}_p.$$

Drinfeld's p-adic upper-half plane

Likewise, the complex upper half plane $\mathcal{H}$ with its action of $\mathbf{SL}_2(\mathbb{R})$ by Möbius transformations, admits a good p-adic analogue.

Drinfeld's p-adic upper-half plane

Likewise, the complex upper half plane $\mathcal{H}$ with its action of $\mathbf{SL}_2(\mathbb{R})$ by Möbius transformations, admits a good p-adic analogue.

Drinfeld. The p-adic analytic space $\mathcal{H}_p := \mathbb{P}_1(\mathbb{C}_p) - \mathbb{P}_1(\mathbb{Q}_p)$ is called the p-adic upper half-plane.

Drinfeld's p-adic upper-half plane

Likewise, the complex upper half plane $\mathcal{H}$ with its action of $\mathbf{SL}_2(\mathbb{R})$ by Möbius transformations, admits a good p-adic analogue.

Drinfeld. The p-adic analytic space $\mathcal{H}_p := \mathbb{P}_1(\mathbb{C}_p) - \mathbb{P}_1(\mathbb{Q}_p)$ is called the p-adic upper half-plane. It is analogous to the union

$$\mathcal{H}^+ \cup \mathcal{H}^- = \mathbb{P}_1(\mathbb{C}) - \mathbb{P}_1(\mathbb{R})$$

of two copies of the Poincaré upper half plane.

Drinfeld's p-adic upper-half plane

Likewise, the complex upper half plane $\mathcal{H}$ with its action of $\mathbf{SL}_2(\mathbb{R})$ by Möbius transformations, admits a good p-adic analogue.

Drinfeld. The p-adic analytic space $\mathcal{H}_p := \mathbb{P}_1(\mathbb{C}_p) - \mathbb{P}_1(\mathbb{Q}_p)$ is called the p-adic upper half-plane. It is analogous to the union

$$\mathcal{H}^+ \cup \mathcal{H}^- = \mathbb{P}_1(\mathbb{C}) - \mathbb{P}_1(\mathbb{R})$$

of two copies of the Poincaré upper half plane.

Tate, Mumford: a *rigid analytic function* on $\mathcal{H}_p$ is a $\mathbb{C}_p$-valued function whose restriction to every good ("affinoid") subset S is a uniform limit of rational functions having poles outside of S.

Drinfeld's p-adic upper-half plane

Likewise, the complex upper half plane $\mathcal{H}$ with its action of $\mathbf{SL}_2(\mathbb{R})$ by Möbius transformations, admits a good p-adic analogue.

Drinfeld. The p-adic analytic space $\mathcal{H}_p := \mathbb{P}_1(\mathbb{C}_p) - \mathbb{P}_1(\mathbb{Q}_p)$ is called the p-adic upper half-plane. It is analogous to the union

$$\mathcal{H}^+ \cup \mathcal{H}^- = \mathbb{P}_1(\mathbb{C}) - \mathbb{P}_1(\mathbb{R})$$

of two copies of the Poincaré upper half plane.

Tate, Mumford: a *rigid analytic function* on $\mathcal{H}_p$ is a $\mathbb{C}_p$-valued function whose restriction to every good ("affinoid") subset S is a uniform limit of rational functions having poles outside of S.

This is the proper generalisation of holomorphic functions on $\mathcal{H}$.

RM points

Unlike its complex counterpart, $\mathcal{H}_p$ contains plenty of real quadratic arguments.

RM points

Unlike its complex counterpart, $\mathcal{H}_p$ contains plenty of real quadratic arguments.

E.g., the golden ratio belongs to $\mathcal{H}_2$, $\mathcal{H}_3$, $\mathcal{H}_5$, $\mathcal{H}_7$, $\mathcal{H}_{13}$ . . .,

RM points

Unlike its complex counterpart, $\mathcal{H}_p$ contains plenty of real quadratic arguments.

E.g., the golden ratio belongs to $\mathcal{H}_2$, $\mathcal{H}_3$, $\mathcal{H}_5$, $\mathcal{H}_7$, $\mathcal{H}_{13}$ ..., (but not to $\mathcal{H}_{11}$, $\mathcal{H}_{19}$, ...).

RM points

Unlike its complex counterpart, $\mathcal{H}_p$ contains plenty of real quadratic arguments.

E.g., the golden ratio belongs to $\mathcal{H}_2$, $\mathcal{H}_3$, $\mathcal{H}_5$, $\mathcal{H}_7$, $\mathcal{H}_{13}$ ..., (but not to $\mathcal{H}_{11}$, $\mathcal{H}_{19}$, ...).

Definition

A point on $\tau \in \mathcal{H}_p$ is called a *real multiplication (RM) point* if it belongs to $\mathcal{H}_p \cap K$ for some real quadratic field K.

RM points

Unlike its complex counterpart, $\mathcal{H}_p$ contains plenty of real quadratic arguments.

E.g., the golden ratio belongs to $\mathcal{H}_2$, $\mathcal{H}_3$, $\mathcal{H}_5$, $\mathcal{H}_7$, $\mathcal{H}_{13}$ ..., (but not to $\mathcal{H}_{11}$, $\mathcal{H}_{19}$, ...).

Definition

A point on $\tau \in \mathcal{H}_p$ is called a *real multiplication (RM) point* if it belongs to $\mathcal{H}_p \cap K$ for some real quadratic field K.

Goal: Define a "convincing" p-adic avatar of j which can be meaningfully *evaluated* at RM points, leading to singular moduli for real quadratic $\tau \in \mathcal{H}_p$.

Rigid meromorphic functions on $\mathcal{H}_p$

Question: What is this p-adic analogue of the j-function?

Rigid meromorphic functions on $\mathcal{H}_p$

Question: What is this p-adic analogue of the j-function?

Classical setting: $j(z)$ is an $\mathbf{SL}_2(\mathbb{Z})$-invariant meromorphic function on $\mathcal{H}$.

Rigid meromorphic functions on $\mathcal{H}_p$

Question: What is this p-adic analogue of the j-function?

Classical setting: $j(z)$ is an $\mathbf{SL}_2(\mathbb{Z})$-invariant meromorphic function on $\mathcal{H}$.

The p-adic setting: A *rigid meromorphic function* is a ratio of rigid analytic functions.

Rigid meromorphic functions on $\mathcal{H}_p$

Question: What is this p-adic analogue of the j-function?

Classical setting: $j(z)$ is an $\mathbf{SL}_2(\mathbb{Z})$-invariant meromorphic function on $\mathcal{H}$.

The p-adic setting: A *rigid meromorphic function* is a ratio of rigid analytic functions.

Let $\mathcal{M} :=$ the ring of rigid meromorphic functions on $\mathcal{H}_p$.

$\mathbf{SL}_2(\mathbb{Z})$-invariant functions

First futile attempt: Study rigid meromorphic functions that are invariant under $\mathbf{SL}_2(\mathbb{Z}) \subset \mathbf{SL}_2(\mathbb{Q}_p)$.

$\mathbf{SL}_2(\mathbb{Z})$-invariant functions

First futile attempt: Study rigid meromorphic functions that are invariant under $\mathbf{SL}_2(\mathbb{Z}) \subset \mathbf{SL}_2(\mathbb{Q}_p)$.

This is a futile, because: The actions of $\mathbf{SL}_2(\mathbb{Z})$ on $\mathcal{H}_p$ is not discrete in the p-adic topology.

$\mathbf{SL}_2(\mathbb{Z})$-invariant functions

First futile attempt: Study rigid meromorphic functions that are invariant under $\mathbf{SL}_2(\mathbb{Z}) \subset \mathbf{SL}_2(\mathbb{Q}_p)$.

This is a futile, because: The actions of $\mathbf{SL}_2(\mathbb{Z})$ on $\mathcal{H}_p$ is not discrete in the p-adic topology. The subgroup of translations $z \mapsto z + n$, with $n \in \mathbb{Z}$, already has non-discrete orbits!

$\mathbf{SL}_2(\mathbb{Z})$-invariant functions

First futile attempt: Study rigid meromorphic functions that are invariant under $\mathbf{SL}_2(\mathbb{Z}) \subset \mathbf{SL}_2(\mathbb{Q}_p)$.

This is a futile, because: The actions of $\mathbf{SL}_2(\mathbb{Z})$ on $\mathcal{H}_p$ is not discrete in the p-adic topology. The subgroup of translations $z \mapsto z + n$, with $n \in \mathbb{Z}$, already has non-discrete orbits!

There are no non-constant $\mathbf{SL}_2(\mathbb{Z})$-invariant elements in $\mathcal{M}$:

$\mathbf{SL}_2(\mathbb{Z})$-invariant functions

First futile attempt: Study rigid meromorphic functions that are invariant under $\mathbf{SL}_2(\mathbb{Z}) \subset \mathbf{SL}_2(\mathbb{Q}_p)$.

This is a futile, because: The actions of $\mathbf{SL}_2(\mathbb{Z})$ on $\mathcal{H}_p$ is not discrete in the p-adic topology. The subgroup of translations $z \mapsto z + n$, with $n \in \mathbb{Z}$, already has non-discrete orbits!

There are no non-constant $\mathbf{SL}_2(\mathbb{Z})$-invariant elements in $\mathcal{M}$:

$$H^0(\mathbf{SL}_2(\mathbb{Z}), \mathcal{M}) = \mathbb{C}_p.$$

The p-modular group

In fact, it turns out to be profitable to consider functions that have good transformation properties under an *even larger* subgroup of $\mathbf{SL}_2(\mathbb{Q}_p)$:

The p-modular group

In fact, it turns out to be profitable to consider functions that have good transformation properties under an *even larger* subgroup of $\mathbf{SL}_2(\mathbb{Q}_p)$: the p-modular group

$$\Gamma := \mathbf{SL}_2(\mathbb{Z}[1/p]).$$

The p-modular group

In fact, it turns out to be profitable to consider functions that have good transformation properties under an *even larger* subgroup of $\mathbf{SL}_2(\mathbb{Q}_p)$: the p-modular group

$$\Gamma := \mathbf{SL}_2(\mathbb{Z}[1/p]).$$

This does nothing to alleviate the problems of the previous slide:

$$H^0(\Gamma, \mathcal{M}) = \mathbb{C}_p.$$

Rigid meromorphic modular cocycles

Let $\mathcal{M}^\times$ be the *multiplicative group* of non-zero elements of $\mathcal{M}$.

Rigid meromorphic modular cocycles

Let $\mathcal{M}^\times$ be the *multiplicative group* of non-zero elements of $\mathcal{M}$.

Key idea: Since $H^0(\Gamma, \mathcal{M}^\times) = \mathbb{C}_p^\times$ is uninteresting, consider its higher cohomology!

Rigid meromorphic modular cocycles

Let $\mathcal{M}^\times$ be the *multiplicative group* of non-zero elements of $\mathcal{M}$.

Key idea: Since $H^0(\Gamma, \mathcal{M}^\times) = \mathbb{C}_p^\times$ is uninteresting, consider its higher cohomology!

Definition

A *rigid meromorphic cocycle* is a class in $H^1(\Gamma, \mathcal{M}^\times)$

Rigid meromorphic modular cocycles

Let $\mathcal{M}^\times$ be the *multiplicative group* of non-zero elements of $\mathcal{M}$.

Key idea: Since $H^0(\Gamma, \mathcal{M}^\times) = \mathbb{C}_p^\times$ is uninteresting, consider its higher cohomology!

Definition

A *rigid meromorphic cocycle* is a class in $H^1(\Gamma, \mathcal{M}^\times)$ whose restriction to the parabolic subgroups of Γ is $\mathbb{C}_p^\times$-valued.

Rigid meromorphic modular cocycles

Let $\mathcal{M}^\times$ be the *multiplicative group* of non-zero elements of $\mathcal{M}$.

Key idea: Since $H^0(\Gamma, \mathcal{M}^\times) = \mathbb{C}_p^\times$ is uninteresting, consider its higher cohomology!

Definition

A *rigid meromorphic cocycle* is a class in $H^1(\Gamma, \mathcal{M}^\times)$ whose restriction to the parabolic subgroups of Γ is $\mathbb{C}_p^\times$-valued.

$H^1_f(\Gamma, \mathcal{M}^\times) :=$ the group of rigid meromorphic cocycles.

Rigid meromorphic modular cocycles

Let $\mathcal{M}^\times$ be the *multiplicative group* of non-zero elements of $\mathcal{M}$.

Key idea: Since $H^0(\Gamma, \mathcal{M}^\times) = \mathbb{C}_p^\times$ is uninteresting, consider its higher cohomology!

Definition

A *rigid meromorphic cocycle* is a class in $H^1(\Gamma, \mathcal{M}^\times)$ whose restriction to the parabolic subgroups of Γ is $\mathbb{C}_p^\times$-valued.

$H^1_f(\Gamma, \mathcal{M}^\times) :=$ the group of rigid meromorphic cocycles.

$$J(\gamma_1\gamma_2)(z) = J(\gamma_1)(z) \times J(\gamma_2)(\gamma_1^{-1}z).$$

Rigid meromorphic modular cocycles

Let $\mathcal{M}^\times$ be the *multiplicative group* of non-zero elements of $\mathcal{M}$.

Key idea: Since $H^0(\Gamma, \mathcal{M}^\times) = \mathbb{C}_p^\times$ is uninteresting, consider its higher cohomology!

Definition

A *rigid meromorphic cocycle* is a class in $H^1(\Gamma, \mathcal{M}^\times)$ whose restriction to the parabolic subgroups of Γ is $\mathbb{C}_p^\times$-valued.

$H^1_f(\Gamma, \mathcal{M}^\times) :=$ the group of rigid meromorphic cocycles.

$$J(\gamma_1\gamma_2)(z) = J(\gamma_1)(z) \times J(\gamma_2)(\gamma_1^{-1}z).$$

Thesis: rigid meromorphic cocycles play the role of meromorphic modular functions in extending CM theory to real quadratic fields.

Evaluating a modular cocycle at an RM point

Evaluating a modular cocycle at an RM point

An element $\tau \in \mathcal{H}_p$ is an RM point if and only if

$$\mathrm{Stab}_\Gamma(\tau) = \langle \pm\gamma_\tau \rangle$$

is an infinite group of rank one.

Evaluating a modular cocycle at an RM point

An element $\tau \in \mathcal{H}_p$ is an RM point if and only if

$$\mathrm{Stab}_{\Gamma}(\tau) = \langle \pm\gamma_\tau \rangle$$

is an infinite group of rank one.

Definition

If $J \in H^1(\Gamma, \mathcal{M}^\times)$ is a rigid meromorphic cocycle, and $\tau \in \mathcal{H}_p$ is an RM point, then the *value* of J at τ is

$$J[\tau] := J(\gamma_\tau)(\tau) \in \mathbb{C}_p \cup \{\infty\}.$$

Evaluating a modular cocycle at an RM point

An element $\tau \in \mathcal{H}_p$ is an RM point if and only if

$$\mathrm{Stab}_{\Gamma}(\tau) = \langle \pm\gamma_\tau \rangle$$

is an infinite group of rank one.

Definition

If $J \in H^1(\Gamma, \mathcal{M}^\times)$ is a rigid meromorphic cocycle, and $\tau \in \mathcal{H}_p$ is an RM point, then the *value* of J at τ is

$$J[\tau] := J(\gamma_\tau)(\tau) \in \mathbb{C}_p \cup \{\infty\}.$$

The quantity $J[\tau]$ is a well-defined numerical invariant,

Evaluating a modular cocycle at an RM point

An element $\tau \in \mathcal{H}_p$ is an RM point if and only if

$$\mathrm{Stab}_\Gamma(\tau) = \langle \pm\gamma_\tau \rangle$$

is an infinite group of rank one.

Definition

If $J \in H^1(\Gamma, \mathcal{M}^\times)$ is a rigid meromorphic cocycle, and $\tau \in \mathcal{H}_p$ is an RM point, then the *value* of J at τ is

$$J[\tau] := J(\gamma_\tau)(\tau) \in \mathbb{C}_p \cup \{\infty\}.$$

The quantity $J[\tau]$ is a well-defined numerical invariant, independent of the cocycle representing the class of J,

Evaluating a modular cocycle at an RM point

An element $\tau \in \mathcal{H}_p$ is an RM point if and only if

$$\mathrm{Stab}_\Gamma(\tau) = \langle \pm\gamma_\tau \rangle$$

is an infinite group of rank one.

Definition

If $J \in H^1(\Gamma, \mathcal{M}^\times)$ is a rigid meromorphic cocycle, and $\tau \in \mathcal{H}_p$ is an RM point, then the *value* of J at τ is

$$J[\tau] := J(\gamma_\tau)(\tau) \in \mathbb{C}_p \cup \{\infty\}.$$

The quantity $J[\tau]$ is a well-defined numerical invariant, independent of the cocycle representing the class of J, and

$$J[\gamma\tau] = J[\tau], \qquad \text{for all } \gamma \in \Gamma.$$

Explicit rigid meromorphic cocycles

For any $\tau \in \mathcal{H}_p$, the orbit $\Gamma\tau$ is dense in $\mathcal{H}_p$.

Explicit rigid meromorphic cocycles

For any $\tau \in \mathcal{H}_p$, the orbit $\Gamma\tau$ is dense in $\mathcal{H}_p$.

Suppose that τ is an RM point in $\mathcal{H}_p$.

Explicit rigid meromorphic cocycles

For any $\tau \in \mathcal{H}_p$, the orbit $\Gamma\tau$ is dense in $\mathcal{H}_p$.

Suppose that τ is an RM point in $\mathcal{H}_p$.

The set $\Sigma_\tau := \{w \in \Gamma\tau \text{ such that } ww' < 0\}$ is discrete.

Explicit rigid meromorphic cocycles

For any $\tau \in \mathcal{H}_p$, the orbit $\Gamma\tau$ is dense in $\mathcal{H}_p$.

Suppose that τ is an RM point in $\mathcal{H}_p$.

The set $\Sigma_\tau := \{w \in \Gamma\tau \text{ such that } ww' < 0\}$ is discrete.

Theorem (Jan Vonk, D)

For each real quadratic $\tau \in \mathcal{H}_p$, there is a unique $J_\tau \in H^1(\Gamma, \mathcal{M}^\times/\mathbb{C}_p^\times)$ for which

Explicit rigid meromorphic cocycles

For any $\tau \in \mathcal{H}_p$, the orbit $\Gamma\tau$ is dense in $\mathcal{H}_p$.

Suppose that τ is an RM point in $\mathcal{H}_p$.

The set $\Sigma_\tau := \{w \in \Gamma\tau \text{ such that } ww' < 0\}$ is discrete.

Theorem (Jan Vonk, D)

For each real quadratic $\tau \in \mathcal{H}_p$, there is a unique $J_\tau \in H^1(\Gamma, \mathcal{M}^\times/\mathbb{C}_p^\times)$ for which

$$J_\tau(S)(z) \sim \prod_{w \in \Sigma_\tau} (z - w)^{\mathrm{sgn}(w)}, \qquad S := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

The classification theorem

If $\Delta = \sum_i n_i[\tau_i] \in \mathrm{Div}(\Gamma\backslash\mathcal{H}_p)$, write

$$J_\Delta := \prod_i J_{\tau_i}^{n_i}.$$

The classification theorem

If $\Delta = \sum_i n_i[\tau_i] \in \mathrm{Div}(\Gamma\backslash\mathcal{H}_p)$, write

$$J_\Delta := \prod_i J_{\tau_i}^{n_i}.$$

A hint that rigid meromorphic cocycles are intimately tied to the arithmetic of real quadratic fields is given by the following classification theorem:

The classification theorem

If $\Delta = \sum_i n_i[\tau_i] \in \mathrm{Div}(\Gamma\backslash\mathcal{H}_p)$, write

$$J_\Delta := \prod_i J_{\tau_i}^{n_i}.$$

A hint that rigid meromorphic cocycles are intimately tied to the arithmetic of real quadratic fields is given by the following classification theorem:

Theorem (Vonk, D)

If $J \in H^1(\Gamma, \mathcal{M}^\times)$, then there exists

- *A divisor $\Delta \in \mathrm{Div}(\Gamma\backslash\mathcal{H}_p^{\mathrm{RM}})$;*

The classification theorem

If $\Delta = \sum_i n_i[\tau_i] \in \mathrm{Div}(\Gamma\backslash\mathcal{H}_p)$, write

$$J_\Delta := \prod_i J_{\tau_i}^{n_i}.$$

A hint that rigid meromorphic cocycles are intimately tied to the arithmetic of real quadratic fields is given by the following classification theorem:

Theorem (Vonk, D)

If $J \in H^1(\Gamma, \mathcal{M}^\times)$, then there exists

- *A divisor $\Delta \in \mathrm{Div}(\Gamma\backslash\mathcal{H}_p^{\mathrm{RM}})$;*
- *An analytic cocycle $J_0 \in H^1(\Gamma, \mathcal{A}^\times/\mathbb{C}_p^\times)$;*

The classification theorem

If $\Delta = \sum_i n_i[\tau_i] \in \mathrm{Div}(\Gamma \backslash \mathcal{H}_p)$, write

$$J_\Delta := \prod_i J_{\tau_i}^{n_i}.$$

A hint that rigid meromorphic cocycles are intimately tied to the arithmetic of real quadratic fields is given by the following classification theorem:

Theorem (Vonk, D)

If $J \in H^1(\Gamma, \mathcal{M}^\times)$, then there exists

- *A divisor $\Delta \in \mathrm{Div}(\Gamma \backslash \mathcal{H}_p^{\mathrm{RM}})$;*
- *An analytic cocycle $J_0 \in H^1(\Gamma, \mathcal{A}^\times / \mathbb{C}_p^\times)$;*

such that $J = J_\Delta \times J_0 \pmod{\mathbb{C}_p^\times}$.

The classification theorem

If $\Delta = \sum_i n_i[\tau_i] \in \mathrm{Div}(\Gamma\backslash\mathcal{H}_p)$, write

$$J_\Delta := \prod_i J_{\tau_i}^{n_i}.$$

A hint that rigid meromorphic cocycles are intimately tied to the arithmetic of real quadratic fields is given by the following classification theorem:

Theorem (Vonk, D)

If $J \in H^1(\Gamma, \mathcal{M}^\times)$, then there exists
- *A divisor $\Delta \in \mathrm{Div}(\Gamma\backslash\mathcal{H}_p^{\mathrm{RM}})$;*
- *An analytic cocycle $J_0 \in H^1(\Gamma, \mathcal{A}^\times/\mathbb{C}_p^\times)$;*

such that $J = J_\Delta \times J_0 \pmod{\mathbb{C}_p^\times}$.
Δ determines J completely.

The classification theorem

If $\Delta = \sum_i n_i[\tau_i] \in \mathrm{Div}(\Gamma\backslash\mathcal{H}_p)$, write

$$J_\Delta := \prod_i J_{\tau_i}^{n_i}.$$

A hint that rigid meromorphic cocycles are intimately tied to the arithmetic of real quadratic fields is given by the following classification theorem:

Theorem (Vonk, D)

If $J \in H^1(\Gamma, \mathcal{M}^\times)$, then there exists
- *A divisor $\Delta \in \mathrm{Div}(\Gamma\backslash\mathcal{H}_p^{\mathrm{RM}})$;*
- *An analytic cocycle $J_0 \in H^1(\Gamma, \mathcal{A}^\times/\mathbb{C}_p^\times)$;*

such that $J = J_\Delta \times J_0 \pmod{\mathbb{C}_p^\times}$.
Δ determines J completely. (It is called the divisor *of J).*

Fields of definition

The previous discussion allows us to associate to an arbitrary $J \in H^1_f(\Gamma, \mathcal{M}^\times)$ a *field of definition*.

Fields of definition

The previous discussion allows us to associate to an arbitrary $J \in H^1_f(\Gamma, \mathcal{M}^\times)$ a *field of definition*.

Definition

The *field of definition of J*, denoted H_J, is the compositum of H_D as D ranges over the discriminants of all the RM points in the support of the divisor of J.

The main conjecture of real multiplication

The main assertion of complex multiplication:

The main conjecture of real multiplication

The main assertion of complex multiplication:

Theorem (Kronecker, ...)

Let J be a meromorphic modular function on $\mathbf{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ with fourier coefficients in a field H_J.

The main conjecture of real multiplication

The main assertion of complex multiplication:

Theorem (Kronecker, ...)

Let J be a meromorphic modular function on $\mathbf{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ with fourier coefficients in a field H_J. For all imaginary quadratic $\tau \in \mathcal{H}$ of discriminant D, the value $J(\tau)$ belongs to the compositum of H_J and H_D.

The main conjecture of real multiplication

The main assertion of complex multiplication:

Theorem (Kronecker, ...)

Let J be a meromorphic modular function on $\mathbf{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ with fourier coefficients in a field H_J. For all imaginary quadratic $\tau \in \mathcal{H}$ of discriminant D, the value $J(\tau)$ belongs to the compositum of H_J and H_D.

Conjecture (Jan Vonk, D)

Let J be a rigid meromorphic cocycle, and let H_J denote its field of definition.

The main conjecture of real multiplication

The main assertion of complex multiplication:

Theorem (Kronecker, ...)

Let J be a meromorphic modular function on $\mathbf{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ with fourier coefficients in a field H_J. For all imaginary quadratic $\tau \in \mathcal{H}$ of discriminant D, the value $J(\tau)$ belongs to the compositum of H_J and H_D.

Conjecture (Jan Vonk, D)

Let J be a rigid meromorphic cocycle, and let H_J denote its field of definition. For all real quadratic $\tau \in \mathcal{H}_p$ of discriminant D, the value $J[\tau]$ belongs to the compositum of H_J and H_D.

Monstrous primes and principal divisors

Definition

A prime p is said to be monstrous if it satisfies the following equivalent conditions:

Monstrous primes and principal divisors

Definition

A prime p is said to be monstrous if it satisfies the following equivalent conditions:

- $p = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59$ or 71.

Monstrous primes and principal divisors

Definition

A prime p is said to be monstrous if it satisfies the following equivalent conditions:

- $p = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59$ or 71.
- p divides the cardinality of the monster sporadic simple group;

Monstrous primes and principal divisors

Definition

A prime p is said to be monstrous if it satisfies the following equivalent conditions:

- $p = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59$ or 71.
- p divides the cardinality of the monster sporadic simple group;
- the quotient $X_0(p)/w_p$ has genus zero.

Monstrous primes and principal divisors

Definition

A prime p is said to be monstrous if it satisfies the following equivalent conditions:

- $p = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59$ or 71.
- p divides the cardinality of the monster sporadic simple group;
- the quotient $X_0(p)/w_p$ has genus zero.

Proposition

If p is a monstrous prime and τ is any RM point on $\mathcal{H}_p$, then $(\tau) - (p\tau)$ is a principal divisor.

A cocycle attached to the golden ratio

Recall that $\varphi = \frac{-1+\sqrt{5}}{2}$ is the golden ratio.

A cocycle attached to the golden ratio

Recall that $\varphi = \frac{-1+\sqrt{5}}{2}$ is the golden ratio.

If $p = 2, 3, 5, 7, 13, 17, 23$, or 47 is a monstrous prime which is $\neq \pm 1 \pmod 5$, the divisor $(\varphi) - (p\varphi)$ is principal.

A cocycle attached to the golden ratio

Recall that $\varphi = \frac{-1+\sqrt{5}}{2}$ is the golden ratio.

If $p = 2, 3, 5, 7, 13, 17, 23$, or 47 is a monstrous prime which is $\neq \pm 1 \pmod 5$, the divisor $(\varphi) - (p\varphi)$ is principal. Let J_φ^+ be the associated rigid meromorphic cocycle.

A cocycle attached to the golden ratio

Recall that $\varphi = \frac{-1+\sqrt{5}}{2}$ is the golden ratio.

If $p = 2, 3, 5, 7, 13, 17, 23$, or 47 is a monstrous prime which is $\neq \pm 1 \pmod 5$, the divisor $(\varphi) - (p\varphi)$ is principal. Let J_φ^+ be the associated rigid meromorphic cocycle.

The RM point $\tau = \sqrt{223}$ of discriminant 223 has class number 6, and $J_\varphi^+[\sqrt{223}]$ appears to satisfy:

A cocycle attached to the golden ratio

Recall that $\varphi = \frac{-1+\sqrt{5}}{2}$ is the golden ratio.

If $p = 2, 3, 5, 7, 13, 17, 23,$ or 47 is a monstrous prime which is $\neq \pm 1 \pmod{5}$, the divisor $(\varphi) - (p\varphi)$ is principal. Let J_φ^+ be the associated rigid meromorphic cocycle.

The RM point $\tau = \sqrt{223}$ of discriminant 223 has class number 6, and $J_\varphi^+[\sqrt{223}]$ appears to satisfy:

$$p = 7. \quad 282525425x^6 + 27867770x^5 + 414793887x^4 - 128906260x^3 + 414793887x^2 + 27867770x + 282525425,$$

A cocycle attached to the golden ratio

Recall that $\varphi = \frac{-1+\sqrt{5}}{2}$ is the golden ratio.

If $p = 2, 3, 5, 7, 13, 17, 23$, or 47 is a monstrous prime which is $\neq \pm 1 \pmod 5$, the divisor $(\varphi) - (p\varphi)$ is principal. Let J_φ^+ be the associated rigid meromorphic cocycle.

The RM point $\tau = \sqrt{223}$ of discriminant 223 has class number 6, and $J_\varphi^+[\sqrt{223}]$ appears to satisfy:

$$p = 7. \quad 282525425x^6 + 27867770x^5 + 414793887x^4 - 128906260x^3 + 414793887x^2 + 27867770x + 282525425,$$

$$p = 13. \quad 464800x^6 + 1275520x^5 + 1614802x^4 + 1596283x^3 + 1614802x^2 + 1275520x + 464800,$$

A cocycle attached to the golden ratio

Recall that $\varphi = \frac{-1+\sqrt{5}}{2}$ is the golden ratio.

If $p = 2, 3, 5, 7, 13, 17, 23$, or 47 is a monstrous prime which is $\neq \pm 1 \pmod 5$, the divisor $(\varphi) - (p\varphi)$ is principal. Let J_φ^+ be the associated rigid meromorphic cocycle.

The RM point $\tau = \sqrt{223}$ of discriminant 223 has class number 6, and $J_\varphi^+[\sqrt{223}]$ appears to satisfy:

$$p = 7. \quad 282525425x^6 + 27867770x^5 + 414793887x^4 - 128906260x^3 + 414793887x^2 + 27867770x + 282525425,$$

$$p = 13. \quad 464800x^6 + 1275520x^5 + 1614802x^4 + 1596283x^3 + 1614802x^2 + 1275520x + 464800,$$

$$p = 47. \quad 4x^6 + 4x^5 + x^4 - 2x^3 + x^2 + 4x + 4.$$

Differences of RM singular moduli

If $p = 2, 3, 5, 7$, or 13, then any $\tau \in \mathcal{H}_p^{\mathrm{RM}}$ is principal.

Differences of RM singular moduli

If $p = 2, 3, 5, 7$, or 13, then any $\tau \in \mathcal{H}_p^{\mathrm{RM}}$ is principal.

Definition: The quantity $J_p(\tau_1, \tau_2) := J_{\tau_1}[\tau_2]$ is called the *p-adic intersection number* of τ_1 and τ_2.

Differences of RM singular moduli

If $p = 2, 3, 5, 7$, or 13, then any $\tau \in \mathcal{H}_p^{\mathrm{RM}}$ is principal.

Definition: The quantity $J_p(\tau_1, \tau_2) := J_{\tau_1}[\tau_2]$ is called the *p-adic intersection number* of τ_1 and τ_2.

Conjecture (Jan Vonk, D)

The quantity $J_p(\tau_1, \tau_2)$ belongs to the compositum $H_1 H_2$ of the ring class fields of $K_1 = \mathbb{Q}(\tau_1)$ and $K_2 = \mathbb{Q}(\tau_2)$ attached to τ_1 and τ_2 respectively,

Differences of RM singular moduli

If $p = 2, 3, 5, 7$, or 13, then any $\tau \in \mathcal{H}_p^{\mathrm{RM}}$ is principal.

Definition: The quantity $J_p(\tau_1, \tau_2) := J_{\tau_1}[\tau_2]$ is called the *p-adic intersection number* of τ_1 and τ_2.

Conjecture (Jan Vonk, D)

The quantity $J_p(\tau_1, \tau_2)$ belongs to the compositum $H_1 H_2$ of the ring class fields of $K_1 = \mathbb{Q}(\tau_1)$ and $K_2 = \mathbb{Q}(\tau_2)$ attached to τ_1 and τ_2 respectively, and behaves in all important respects just like the classical

$$J_\infty(\tau_1, \tau_2) := J(\tau_1, \tau_2) = j(\tau_1) - j(\tau_2)$$

of Gross-Zagier.

Gross-Zagier factorisations

Let τ_1 and $\tau_2 \in \mathcal{H}$ be CM points with (negative) discriminants D_1 and D_2, and let $\mathcal{O}_{D_1}$ and $\mathcal{O}_{D_2}$ be the associated quadratic orders.

Gross-Zagier factorisations

Let τ_1 and $\tau_2 \in \mathcal{H}$ be CM points with (negative) discriminants D_1 and D_2, and let $\mathcal{O}_{D_1}$ and $\mathcal{O}_{D_2}$ be the associated quadratic orders.

For each prime q that is non-split in $\mathbb{Q}(\tau_1)$ and $\mathbb{Q}(\tau_2)$, Gross and Zagier define an explicit "purely algebraic" quantity $e_{q\infty}(\tau_1, \tau_2)$ in terms of the embeddings of $\mathcal{O}_{D_1}$ and $\mathcal{O}_{D_2}$ into the **definite** quaternion algebra $B_{q\infty}$ ramified at q and ∞.

Gross-Zagier factorisations

Let τ_1 and $\tau_2 \in \mathcal{H}$ be CM points with (negative) discriminants D_1 and D_2, and let $\mathcal{O}_{D_1}$ and $\mathcal{O}_{D_2}$ be the associated quadratic orders.

For each prime q that is non-split in $\mathbb{Q}(\tau_1)$ and $\mathbb{Q}(\tau_2)$, Gross and Zagier define an explicit "purely algebraic" quantity $e_{q\infty}(\tau_1, \tau_2)$ in terms of the embeddings of $\mathcal{O}_{D_1}$ and $\mathcal{O}_{D_2}$ into the **definite** quaternion algebra $B_{q\infty}$ ramified at q and ∞.

Conjecture (Gross-Zagier)

If q is split in either $\mathbb{Q}(\tau_1)$ or $\mathbb{Q}(\tau_2)$, then $\operatorname{ord}_q J_\infty(\tau_1, \tau_2) = 0$.

Gross-Zagier factorisations

Let τ_1 and $\tau_2 \in \mathcal{H}$ be CM points with (negative) discriminants D_1 and D_2, and let $\mathcal{O}_{D_1}$ and $\mathcal{O}_{D_2}$ be the associated quadratic orders.

For each prime q that is non-split in $\mathbb{Q}(\tau_1)$ and $\mathbb{Q}(\tau_2)$, Gross and Zagier define an explicit "purely algebraic" quantity $e_{q\infty}(\tau_1, \tau_2)$ in terms of the embeddings of $\mathcal{O}_{D_1}$ and $\mathcal{O}_{D_2}$ into the **definite** quaternion algebra $B_{q\infty}$ ramified at q and ∞.

Conjecture (Gross-Zagier)

If q is split in either $\mathbb{Q}(\tau_1)$ or $\mathbb{Q}(\tau_2)$, then $\operatorname{ord}_q J_\infty(\tau_1, \tau_2) = 0$. Otherwise,

$$\operatorname{ord}_q J_\infty(\tau_1, \tau_2) = e_{q\infty}(\tau_1, \tau_2).$$

Factorisations of real quadratic singular moduli

For $\tau_1, \tau_2 \in \mathcal{H}_p^{\mathrm{RM}}$, one can likewise define an arithmetic quantity $e_{qp}(\tau_1, \tau_2)$ involving the **indefinite** quaternion algebra B_{qp} ramified at q and p.

Factorisations of real quadratic singular moduli

For $\tau_1, \tau_2 \in \mathcal{H}_p^{\mathrm{RM}}$, one can likewise define an arithmetic quantity $e_{qp}(\tau_1, \tau_2)$ involving the **indefinite** quaternion algebra B_{qp} ramified at q and p.

The group $\Gamma_{pq} = (\mathcal{O}_{B_{qp}})_1^\times \subset \mathbf{SL}_2(\mathbb{R})$ acts discretely and co-compactly on $\mathcal{H}$;

Factorisations of real quadratic singular moduli

For $\tau_1, \tau_2 \in \mathcal{H}_p^{\mathrm{RM}}$, one can likewise define an arithmetic quantity $e_{qp}(\tau_1, \tau_2)$ involving the **indefinite** quaternion algebra B_{qp} ramified at q and p.

The group $\Gamma_{pq} = (\mathcal{O}_{B_{qp}})_1^\times \subset \mathbf{SL}_2(\mathbb{R})$ acts discretely and co-compactly on $\mathcal{H}$;

The Riemann surface $\Gamma_{pq} \backslash \mathcal{H}$ is called the *Shimura curve* X_{qp} attached to the pair (p, q).

Factorisations of real quadratic singular moduli

For $\tau_1, \tau_2 \in \mathcal{H}_p^{\mathrm{RM}}$, one can likewise define an arithmetic quantity $e_{qp}(\tau_1, \tau_2)$ involving the **indefinite** quaternion algebra B_{qp} ramified at q and p.

The group $\Gamma_{pq} = (\mathcal{O}_{B_{qp}})_1^\times \subset \mathbf{SL}_2(\mathbb{R})$ acts discretely and co-compactly on $\mathcal{H}$;

The Riemann surface $\Gamma_{pq} \backslash \mathcal{H}$ is called the *Shimura curve* X_{qp} attached to the pair (p, q).

To τ_1 and τ_2 are associated hyperbolic geodesics γ_1 and γ_2 on X_{qp}.

Factorisations of real quadratic singular moduli

For $\tau_1, \tau_2 \in \mathcal{H}_p^{\mathrm{RM}}$, one can likewise define an arithmetic quantity $e_{qp}(\tau_1, \tau_2)$ involving the **indefinite** quaternion algebra B_{qp} ramified at q and p.

The group $\Gamma_{pq} = (\mathcal{O}_{B_{qp}})_1^\times \subset \mathbf{SL}_2(\mathbb{R})$ acts discretely and co-compactly on $\mathcal{H}$;

The Riemann surface $\Gamma_{pq} \backslash \mathcal{H}$ is called the *Shimura curve* X_{qp} attached to the pair (p, q).

To τ_1 and τ_2 are associated hyperbolic geodesics γ_1 and γ_2 on X_{qp}.

$e_{qp}(\tau_1, \tau_2) :=$ weighted intersection of γ_1 and γ_2 on X_{qp}.

A Gross-Zagier-style factorisation

Let $\tau_1 \in \mathcal{H}_p^{D_1}$ and $\tau_2 \in \mathcal{H}_p^{D_2}$.

A Gross-Zagier-style factorisation

Let $\tau_1 \in \mathcal{H}_p^{D_1}$ and $\tau_2 \in \mathcal{H}_p^{D_2}$.

Conjecture (Jan Vonk, D)

Let q be a prime.

A Gross-Zagier-style factorisation

Let $\tau_1 \in \mathcal{H}_p^{D_1}$ and $\tau_2 \in \mathcal{H}_p^{D_2}$.

Conjecture (Jan Vonk, D)

Let q be a prime. If q is split in either $\mathbb{Q}(\tau_1)$ or $\mathbb{Q}(\tau_2)$, then $\mathrm{ord}_q J_p(\tau_1, \tau_2) = 0$.

A Gross-Zagier-style factorisation

Let $\tau_1 \in \mathcal{H}_p^{D_1}$ and $\tau_2 \in \mathcal{H}_p^{D_2}$.

Conjecture (Jan Vonk, D)

Let q be a prime. If q is split in either $\mathbb{Q}(\tau_1)$ or $\mathbb{Q}(\tau_2)$, then $\operatorname{ord}_q J_p(\tau_1, \tau_2) = 0$. *Otherwise,*

$$\operatorname{ord}_q J_p(\tau_1, \tau_2) = e_{qp}(\tau_1, \tau_2).$$

An example

James Rickards has developed and implemented efficient algorithms for computing the q-weighted topological intersection numbers $e_{qp}(\tau_1, \tau_2)$ of real quadratic geodesics on the Shimura curve X_{qp}.

An example: $D_1 = 13$, $D_2 = 285 = 3 \cdot 5 \cdot 19$, $p = 2$

An example: $D_1 = 13$, $D_2 = 285 = 3 \cdot 5 \cdot 19$, $p = 2$

$J_2(\tau_1, \tau_2)$ satisfies (to 800 digits of 2-adic precision)

An example: $D_1 = 13$, $D_2 = 285 = 3 \cdot 5 \cdot 19$, $p = 2$

$J_2(\tau_1, \tau_2)$ satisfies (to 800 digits of 2-adic precision)

$$7736097284175893694750297399823 9x^4 + 14018107043889083172131413509980 3x^3$$

$$+20989561954979125519941348989929 2x^2 + 14018107043889083172131413509980 3x$$

$$+77360972841758936947502973998239,$$

An example: $D_1 = 13$, $D_2 = 285 = 3 \cdot 5 \cdot 19$, $p = 2$

$J_2(\tau_1, \tau_2)$ satisfies (to 800 digits of 2-adic precision)

$$7736097284175893694750297399823 9x^4 + 14018107043889083172131413509980 3x^3$$

$$+20989561954979125519941348989929 2x^2 + 14018107043889083172131413509980 3x$$

$$+7736097284175893694750297399823 9,$$

James Rickards: The topological intersection $e_{q2}(\tau_1, \tau_2)$ is zero except for the primes q in the following table:

q	7	19	31	73	109	151	163	397	457	463
$e_{q2}(\tau_1, \tau_2)$	7	2	2	1	2	2	1	1	1	1

An example: $D_1 = 13$, $D_2 = 285 = 3 \cdot 5 \cdot 19$, $p = 2$

$J_2(\tau_1, \tau_2)$ satisfies (to 800 digits of 2-adic precision)

$$773609728417589369475029739982239x^4 + 140181070438890831721314135099803x^3$$
$$+209895619549791255199413489899292x^2 + 140181070438890831721314135099803x$$
$$+773609728417589369475029739982239,$$

James Rickards: The topological intersection $e_{q2}(\tau_1, \tau_2)$ is zero except for the primes q in the following table:

q	7	19	31	73	109	151	163	397	457	463
$e_{q2}(\tau_1, \tau_2)$	7	2	2	1	2	2	1	1	1	1

Jan Vonk, D: $773609728417589369475029739982239 =$

An example: $D_1 = 13$, $D_2 = 285 = 3 \cdot 5 \cdot 19$, $p = 2$

$J_2(\tau_1, \tau_2)$ satisfies (to 800 digits of 2-adic precision)

$$7736097284175893694750297399823 9x^4 + 14018107043889083172131413509980 3x^3$$

$$+20989561954979125519941348989929 2x^2 + 14018107043889083172131413509980 3x \cdot$$

$$+7736097284175893694750297399823 9,$$

James Rickards: The topological intersection $e_{q2}(\tau_1, \tau_2)$ is zero except for the primes q in the following table:

q	7	19	31	73	109	151	163	397	457	463
$e_{q2}(\tau_1, \tau_2)$	7	2	2	1	2	2	1	1	1	1

Jan Vonk, D: $77360972841758936947502973998239 =$

$$7^7 \cdot 19^2 \cdot 31^2 \cdot 73 \cdot 109^2 \cdot 151^2 \cdot 163 \cdot 397 \cdot 457 \cdot 463,$$

Conclusion

We have described a convincing *conjectural* extension of the theory of complex multiplication, and of differences of singular moduli, to real quadratic fields.

Conclusion

We have described a convincing *conjectural* extension of the theory of complex multiplication, and of differences of singular moduli, to real quadratic fields.

Whither the abc conjecture?

Some key difference with the classical setting

Meromorphic functions form a ring: they can be added and multiplied.

Some key difference with the classical setting

Meromorphic functions form a ring: they can be added and multiplied. Rigid meromorphic cocycles can only be multiplied!

Some key difference with the classical setting

Meromorphic functions form a ring: they can be added and multiplied. Rigid meromorphic cocycles can only be multiplied!

The (trivial) identity

$$J_\infty(\tau_1, \tau_2) + J_\infty(\tau_2, \tau_3) = J_\infty(\tau_1, \tau_2)$$

has no counterpart for $J_p(\tau_1, \tau_2)$.

Some key difference with the classical setting

Meromorphic functions form a ring: they can be added and multiplied. Rigid meromorphic cocycles can only be multiplied!

The (trivial) identity

$$J_\infty(\tau_1, \tau_2) + J_\infty(\tau_2, \tau_3) = J_\infty(\tau_1, \tau_2)$$

has no counterpart for $J_p(\tau_1, \tau_2)$.

The abc conjecture is saved!

Some key difference with the classical setting

Meromorphic functions form a ring: they can be added and multiplied. Rigid meromorphic cocycles can only be multiplied!

The (trivial) identity

$$J_\infty(\tau_1, \tau_2) + J_\infty(\tau_2, \tau_3) = J_\infty(\tau_1, \tau_2)$$

has no counterpart for $J_p(\tau_1, \tau_2)$.

The abc conjecture is saved!

Likewise there seem to be no applications to Siegel zeroes for even Dirichlet characters, à la Granville-Stark.

Theoretical evidence

The evidence for this theory so far is largely experimental, but there has been some recent progress on the theoretical front.

Theoretical evidence

The evidence for this theory so far is largely experimental, but there has been some recent progress on the theoretical front.

Definition

The *cuspidal value* of a rigid meromorphic cocycle J is the quantity

$$J[\infty] := J(\gamma_\infty), \qquad \text{where} \quad \gamma_\infty(\infty) = \infty.$$

Theoretical evidence

The evidence for this theory so far is largely experimental, but there has been some recent progress on the theoretical front.

Definition

The *cuspidal value* of a rigid meromorphic cocycle J is the quantity

$$J[\infty] := J(\gamma_\infty), \qquad \text{where} \quad \gamma_\infty(\infty) = \infty.$$

Theorem (Vonk, D)

$J[\infty]$ is algebraic. More precisely, a power of it belongs to $H_J^\times$.

Theoretical evidence

The evidence for this theory so far is largely experimental, but there has been some recent progress on the theoretical front.

Definition

The *cuspidal value* of a rigid meromorphic cocycle J is the quantity

$$J[\infty] := J(\gamma_\infty), \qquad \text{where} \quad \gamma_\infty(\infty) = \infty.$$

Theorem (Vonk, D)

$J[\infty]$ is algebraic. More precisely, a power of it belongs to $H_J^\times$.

The proof rests on a remarkable recent work of Samit Dasgupta and Mahesh Kakde, building on the proof of the "rank one p-adic Gross-Stark conjecture" by Dasgupta-Darmon-Pollack (2006).

Thank you for your attention.