There are at most finitely many singular moduli that are S-units

Sebastián Herrero
(joint with Ricardo Menares and Juan Rivera-Letelier)

International Seminar on Automorphic Forms, May 2021

Notation

$$\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$$

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

Notation

$$\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$$

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

$j : \mathbb{H} \to \mathbb{C}$ modular function with

$$j(z) = q^{-1} + 744 + \sum_{n=1}^{\infty} c_n q^n, \quad \text{where } q := e^{2\pi i z}.$$

Notation

$$\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$$

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

$j : \mathbb{H} \to \mathbb{C}$ modular function with

$$j(z) = q^{-1} + 744 + \sum_{n=1}^{\infty} c_n q^n, \quad \text{where } q := e^{2\pi i z}.$$

Facts:

1. j is a Hauptmodul for Γ.
2. $j(z)$ is the j-invariant of the elliptic curve $E_z \simeq \mathbb{C}/(\mathbb{Z} + z\mathbb{Z})$.

CM points and singular moduli

z in $\mathbb{H}$ is a CM point if $\mathbb{Q}(z)$ is quadratic (imaginary) over $\mathbb{Q}$.

CM points and singular moduli

z in $\mathbb{H}$ is a CM point if $\mathbb{Q}(z)$ is quadratic (imaginary) over $\mathbb{Q}$.

Theorem (CM theory)

If z is CM then $j(z)$ is an algebraic integer. Moreover, $\mathbb{Q}(z, j(z))$ is an abelian unramified extension of $\mathbb{Q}(z)$.

CM points and singular moduli

z in $\mathbb{H}$ is a CM point if $\mathbb{Q}(z)$ is quadratic (imaginary) over $\mathbb{Q}$.

Theorem (CM theory)

If z is CM then $j(z)$ is an algebraic integer. Moreover, $\mathbb{Q}(z, j(z))$ is an abelian unramified extension of $\mathbb{Q}(z)$.

If z is CM, we call $j(z)$ a singular modulus (following Kronecker).

A question of Masser

Are there *only finitely many* singular moduli that are algebraic units?

A question of Masser

Are there *only finitely many* singular moduli that are algebraic units?

Motivation: In

An effective "Theorem of André" for CM-points on a plane curve (2013)

Bilu, Masser and Zannier proved that there are no pairs (j_1, j_2) of singular moduli on $X_1 \cdot X_2 = 1$.

Habegger's theorem

Habegger's theorem

In

Singular moduli that are algebraic units (2015)

Habegger proved the there are at most finitely many singular moduli that are algebraic units.

Habegger's theorem

In

Singular moduli that are algebraic units (2015)

Habegger proved the there are at most finitely many singular moduli that are algebraic units.

Habegger's proof does not give a numerical bound for the number of singular moduli that are algebraic units.

Habegger's theorem

In

Singular moduli that are algebraic units (2015)

Habegger proved the there are at most finitely many singular moduli that are algebraic units.

Habegger's proof does not give a numerical bound for the number of singular moduli that are algebraic units.

Natural question: Is there any such *singular unit*?

Refinements

Refinements

1. In

   No singular modulus is a unit (2018)

   Bilu, Habegger and Kühne proved that there are no *singular units*.

Refinements

1. In

   No singular modulus is a unit (2018)

   Bilu, Habegger and Kühne proved that there are no *singular units*.

2. Let $\Phi_m(X, Y)$ denote the m-th modular polynomial ($m \geq 1$ integer). In

   Singular units and isogenies between CM *elliptic curves* (2019)

   Y. Li proved that $\Phi_m(j_1, j_2)$ is never an algebraic unit for j_1, j_2 singular moduli.

Differences of singular moduli

Habegger's work (2015) implies the following result: given an algebraic integer α there are at most finitely many singular moduli j such that $j - \alpha$ is an algebraic unit.

Differences of singular moduli

Habegger's work (2015) implies the following result: given an algebraic integer α there are at most finitely many singular moduli j such that $j - \alpha$ is an algebraic unit.

Example: If $\alpha = 1$ then

$$j\left(\frac{1+i\sqrt{3}}{2}\right) - \alpha = 0 - 1 = -1$$

is an algebraic unit.

Differences of singular moduli

Habegger's work (2015) implies the following result: given an algebraic integer α there are at most finitely many singular moduli j such that $j - \alpha$ is an algebraic unit.

Example: If $\alpha = 1$ then

$$j\left(\frac{1 + i\sqrt{3}}{2}\right) - \alpha = 0 - 1 = -1$$

is an algebraic unit.

In the case $\alpha = j_2$ is a singular modulus we have, by Y. Li's theorem with $m = 1$, that $j_1 - j_2$ is never an algebraic unit.

Fact: Differences of singular moduli are very special.

More on CM points

For z CM, define

$$D = \mathrm{Disc}(z) = \text{discriminant of min. poly. of } z \text{ over } \mathbb{Z}.$$

More on CM points

For z CM, define

$$D = \mathrm{Disc}(z) = \text{discriminant of min. poly. of } z \text{ over } \mathbb{Z}.$$

Then z is of the form

$$\frac{-b + \sqrt{D}}{2a}$$

with $a, b, c \in \mathbb{Z}$ coprime, $a > 0$, $D = b^2 - 4ac < 0$.

More on CM points

For z CM, define

$$D = \mathrm{Disc}(z) = \text{discriminant of min. poly. of } z \text{ over } \mathbb{Z}.$$

Then z is of the form

$$\frac{-b+\sqrt{D}}{2a}$$

with $a, b, c \in \mathbb{Z}$ coprime, $a > 0$, $D = b^2 - 4ac < 0$.
Γ acts on the set CM_D of CM points of discriminant D and we define

$$\Lambda_D = \Gamma \backslash \mathrm{CM}_D.$$

More on CM points

For z CM, define

$$D = \mathrm{Disc}(z) = \text{discriminant of min. poly. of } z \text{ over } \mathbb{Z}.$$

Then z is of the form

$$\frac{-b+\sqrt{D}}{2a}$$

with $a, b, c \in \mathbb{Z}$ coprime, $a > 0$, $D = b^2 - 4ac < 0$.
Γ acts on the set CM_D of CM points of discriminant D and we define

$$\Lambda_D = \Gamma \backslash \mathrm{CM}_D.$$

Theorem (CM theory)

Λ_D is finite of cardinality $h(D)$ (class number) and $j(\Lambda_D)$ is a full Galois orbit.

Norms of differences

Given α in $\overline{\mathbb{Q}}$ define

$$\mathrm{Nm}(\alpha) = \prod_{\sigma:\mathbb{Q}(\alpha)\hookrightarrow\overline{\mathbb{Q}}} \sigma(\alpha).$$

Norms of differences

Given α in $\overline{\mathbb{Q}}$ define

$$\mathrm{Nm}(\alpha) = \prod_{\sigma:\mathbb{Q}(\alpha)\hookrightarrow\overline{\mathbb{Q}}} \sigma(\alpha).$$

Then $j_1 - j_2$ is an algebraic unit if and only if $\mathrm{Nm}(j_1 - j_2) = \pm 1$.

Norms of differences

Given α in $\overline{\mathbb{Q}}$ define
$$\mathrm{Nm}(\alpha) = \prod_{\sigma:\mathbb{Q}(\alpha)\hookrightarrow\overline{\mathbb{Q}}} \sigma(\alpha).$$

Then $j_1 - j_2$ is an algebraic unit if and only if $\mathrm{Nm}(j_1 - j_2) = \pm 1$.

In

On singular moduli (1985)

Gross and Zagier gave an *arithmetic formula* for $\mathrm{Nm}(j_1 - j_2)$ under certain hypotheses.

Norms of differences

Given α in $\overline{\mathbb{Q}}$ define

$$\mathrm{Nm}(\alpha) = \prod_{\sigma:\mathbb{Q}(\alpha)\hookrightarrow\overline{\mathbb{Q}}} \sigma(\alpha).$$

Then $j_1 - j_2$ is an algebraic unit if and only if $\mathrm{Nm}(j_1 - j_2) = \pm 1$.

In

On singular moduli (1985)

Gross and Zagier gave an *arithmetic formula* for $\mathrm{Nm}(j_1 - j_2)$ under certain hypotheses.
It is not clear how to use Gross and Zagier's formula (or extensions of it) to prove *directly* that $j_1 - j_2$ is never an algebraic unit.

Singular S-units

Fix S a finite set of prime numbers.

Singular S-units

Fix S a finite set of prime numbers.

An algebraic integer is an S-unit if no primes outside S divide $\mathrm{Nm}(\alpha)$.

Singular S-units

Fix S a finite set of prime numbers.

An algebraic integer is an S-unit if no primes outside S divide $\mathrm{Nm}(\alpha)$.

Theorem (H–Menares–Rivera-Letelier, 2021)

There are at most finitely many singular moduli that are S-units.

Singular S-units

Fix S a finite set of prime numbers.

An algebraic integer is an S-unit if no primes outside S divide $\mathrm{Nm}(\alpha)$.

Theorem (H–Menares–Rivera-Letelier, 2021)

There are at most finitely many singular moduli that are S-units.

By Bilu, Habegger and Kühne, or by Y. Li, every singular modulus is an S-unit for some finite set S.

Numerics: A. Sutherland's table[1]

D	$\prod_{z\in\Lambda_D} j(z)$	D	$\prod_{z\in\Lambda_D} j(z)$	D	$\prod_{z\in\Lambda_D} j(z)$
-3	0	-32	$2^6 5^6 23^3$	-63	$-3^6 5^{12} 17^3 41^3 47^3$
-4	$2^6 3^3$	-35	$-2^{30} 5^3$	-64	$-2^3 3^6 23^3 47^3$
-7	$-3^3 5^3$	-36	$-2^{12} 3^3 11^3 23^3$	-67	$-2^{15} 3^3 5^3 11^3$
-8	$2^6 5^3$	-39	$3^{15} 17^3 23^3 29^3$	-68	$-2^{24} 5^{12} 17^3 47^3$
-11	-2^{15}	-40	$2^{12} 3^6 5^3 29^3$	-71	$-11^9 17^6 23^3 41^3 47^3 53^3$
-12	$2^4 3^3 5^3$	-43	$-2^{18} 3^3 5^3$	-72	$2^{12} 5^6 29^3 53^3$
-15	$-3^6 5^3 11^3$	-44	$2^{12} 11^3 17^3 29^3$	-75	$2^{30} 3^6 5^1 11^3$
-16	$2^3 3^3 11^3$	-47	$-5^{15} 11^6 23^3 29^3$	-76	$2^{12} 3^9 41^3 53^3$
-19	$-2^{15} 3^3$	-48	$2^4 3^9 5^6 11^3$	-79	$-3^{15} 17^3 29^3 47^3 53^3 59^3$
-20	$-2^{12} 5^3 11^3$	-51	$2^{33} 3^6$	-80	$2^{12} 5^6 11^3 17^6 59^3$
-23	$-5^9 11^3 17^3$	-52	$-2^{12} 3^6 5^6 23^3$	-83	$-2^{48} 5^9$
-24	$2^{12} 3^6 17^3$	-55	$-3^{12} 5^6 11^3 29^3 41^3$	-84	$-2^{24} 3^{15} 47^3 59^3$
-27	$-2^{15} 3^1 5^3$	-56	$2^{24} 11^6 17^3 41^3$	-87	$3^{18} 5^{18} 23^3 53^3 59^3$
-28	$3^3 5^3 17^3$	-59	$-2^{48} 11^3$	-88	$2^{12} 3^6 5^6 17^3 41^3$
-31	$-3^9 11^3 17^3 23^3$	-60	$3^6 5^3 29^3 41^3$	-91	$-2^{30} 3^6 17^3$

[1] https://math.mit.edu/ drew/NormsOfSingularModuli2000.pdf

Question

Question

It seems like $j\left(\frac{1+\sqrt{-11}}{2}\right) = -2^{15}$ is the only singular modulus that is an S-unit for S a singleton. Is this the case?

Question

It seems like $j\left(\frac{1+\sqrt{-11}}{2}\right) = -2^{15}$ is the only singular modulus that is an S-unit for S a singleton. Is this the case?

A. Sutherland checked this *conjecture* for discriminants D in $]-10^5, -3]$ (private communication).

Difference of singular moduli

Difference of singular moduli

Fix S a finite set of prime numbers.

Difference of singular moduli

Fix S a finite set of prime numbers.

Theorem (H–Menares–Rivera-Letelier, 2021)

Given a singular modulus j_2, there are at most finitely many singular moduli j_1 such that $j_1 - j_2$ is an S-unit.

Difference of singular moduli

Fix S a finite set of prime numbers.

Theorem (H–Menares–Rivera-Letelier, 2021)

Given a singular modulus j_2, there are at most finitely many singular moduli j_1 such that $j_1 - j_2$ is an S-unit.

We use Habegger's original strategy together with the new ingredient that for every prime number p, singular moduli are p-adically disperse.

Habegger's strategy (for singular units)

Habegger's strategy (for singular units)

Habegger considered the absolute logarithmic Weil height

$$h(a) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} d_v \log \max\{1, |a|_v\}$$

for a in K a number field, where

- M_K is the set of places of K,
- $|\cdot|_v$ is a representative absolute value extending $|\cdot|_p$ with p prime or ∞ (the usual field norms on $\mathbb{Q}$),
- $d_v = [K_v : \mathbb{Q}_p]$.

Habegger's strategy (for singular units)

Habegger considered the absolute logarithmic Weil height

$$h(a) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} d_v \log \max\{1, |a|_v\}$$

for a in K a number field, where

- M_K is the set of places of K,
- $|\cdot|_v$ is a representative absolute value extending $|\cdot|_p$ with p prime or ∞ (the usual field norms on $\mathbb{Q}$),
- $d_v = [K_v : \mathbb{Q}_p]$.

First ingredient: For j a singular modulus of discriminant D we have

$$h(j) \geq A \log|D| + B,$$

with A, B absolute constants, $A > 0$.
This follows from results of Colmez (1989), and Nakkajima and Taguchi (1991).

Second ingredient: A density estimate for the number of singular moduli around 0. Given $\varepsilon > 0$ find $r > 0$ small such that

$$\frac{1}{h(D)} \left(j(\Lambda_D) \cap B(0, r) \right) \leq \varepsilon \text{ for } D \to -\infty.$$

This follows from the following equidistribution theorem for CM points.

Second ingredient: A density estimate for the number of singular moduli around 0. Given $\varepsilon > 0$ find $r > 0$ small such that

$$\frac{1}{h(D)}\left(j(\Lambda_D) \cap B(0,r)\right) \leq \varepsilon \text{ for } D \to -\infty.$$

This follows from the following equidistribution theorem for CM points.

Theorem (Duke (1988) + Clozel and Ullmo (2004))

When $D \to -\infty$ we have

$$\frac{1}{h(D)} \sum_{z \in \Lambda_D} \delta_z \to \frac{3}{\pi} \frac{dxdy}{y^2}$$

weakly on $\Gamma \backslash \mathbb{H}$.

Second ingredient: A density estimate for the number of singular moduli around 0. Given $\varepsilon > 0$ find $r > 0$ small such that

$$\frac{1}{h(D)} \left(j(\Lambda_D) \cap B(0,r) \right) \leq \varepsilon \text{ for } D \to -\infty.$$

This follows from the following equidistribution theorem for CM points.

Theorem (Duke (1988) + Clozel and Ullmo (2004))

When $D \to -\infty$ we have

$$\frac{1}{h(D)} \sum_{z \in \Lambda_D} \delta_z \to \frac{3}{\pi} \frac{dxdy}{y^2}$$

weakly on $\Gamma \backslash \mathbb{H}$.

This step is not effective.

Third ingredient: An estimate for the Archimedean distance between a singular modulus and 0. For j a nonzero singular modulus of discriminant D we have

$$-\log|j| \leq c_\infty \log|D|,$$

with $c_\infty > 0$ absolute constant.

Third ingredient: An estimate for the Archimedean distance between a singular modulus and 0. For j a nonzero singular modulus of discriminant D we have

$$-\log|j| \le c_\infty \log|D|,$$

with $c_\infty > 0$ absolute constant.

In the "$(j-\alpha)$ version" of Habegger's theorem (α algebraic integer) one needs David and Hirata-Kohno's deep lower bound for linear forms on $n = 2$ elliptic logarithms (2009).

Putting everything together

Putting everything together

If j is a singular unit of discriminant D, then

$$\begin{aligned} A\log|D| + B &\leq h(j) \\ &= \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K} d_v \log\max\{1, |a|_v\} \\ &= \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K^\infty} d_v \log\max\{1, |a|_v\} \\ &= -\frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K^\infty, |a|_v<1} d_v \log|a|_v, \end{aligned}$$

by the product formula.

Putting everything together

If j is a singular unit of discriminant D, then

$$\begin{aligned} A \log|D| + B &\leq h(j) \\ &= \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} d_v \log \max\{1, |a|_v\} \\ &= \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K^\infty} d_v \log \max\{1, |a|_v\} \\ &= -\frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K^\infty, |a|_v < 1} d_v \log |a|_v, \end{aligned}$$

by the product formula.For $\varepsilon > 0$ convenient we get

$$-\frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K^\infty, |a|_v < 1} d_v \log |a|_v \leq A_\varepsilon \log|D| + B_\varepsilon$$

with $A_\varepsilon < A$.

Putting everything together

If j is a singular unit of discriminant D, then

$$\begin{array}{rcl} A\log|D| + B & \leq & h(j) \\ & = & \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K} d_v \log\max\{1,|a|_v\} \\ & = & \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K^\infty} d_v \log\max\{1,|a|_v\} \\ & = & -\frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K^\infty,|a|_v<1} d_v \log|a|_v, \end{array}$$

by the product formula.For $\varepsilon > 0$ convenient we get

$$-\frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K^\infty,|a|_v<1} d_v \log|a|_v \leq A_\varepsilon \log|D| + B_\varepsilon$$

with $A_\varepsilon < A$.Hence $|D|$ is bounded and the result follows.

Our proof (for singular S-units)

Our proof (for singular S-units)

We use Habegger's strategy. For p prime, fix an extension of $|\cdot|_p$ to $\overline{\mathbb{Q}}$.

First ingredient: For j a singular modulus of discriminant D we have

$$h(j) \geq A \log |D| + B,$$

with A, B absolute constants, $A > 0$.

Our proof (for singular S-units)

We use Habegger's strategy. For p prime, fix an extension of $|\cdot|_p$ to $\overline{\mathbb{Q}}$.

First ingredient: For j a singular modulus of discriminant D we have

$$h(j) \geq A \log |D| + B,$$

with A, B absolute constants, $A > 0$.

Second ingredient: A p-adic density estimate for the number of singular moduli around 0. Given $\varepsilon > 0$ find $r > 0$ small such that

$$\frac{1}{h(D)} (j(\Lambda_D) \cap B_p(0, r)) \leq \varepsilon \text{ for } D \to -\infty.$$

Our proof (for singular S-units)

We use Habegger's strategy. For p prime, fix an extension of $|\cdot|_p$ to $\overline{\mathbb{Q}}$.

First ingredient: For j a singular modulus of discriminant D we have

$$h(j) \geq A \log |D| + B,$$

with A, B absolute constants, $A > 0$.

Second ingredient: A p-adic density estimate for the number of singular moduli around 0. Given $\varepsilon > 0$ find $r > 0$ small such that

$$\frac{1}{h(D)} \left(j(\Lambda_D) \cap B_p(0, r) \right) \leq \varepsilon \text{ for } D \to -\infty.$$

Third ingredient: An estimate for the p-adic distance between a singular modulus and 0. For j a nonzero singular modulus of discriminant D we have

$$-\log |j|_p \leq c_p \log |D|,$$

with $c_p > 0$ absolute constant.

Putting everything together

Putting everything together

If j is a singular unit of discriminant D, then

$$\begin{array}{rcl} A\log|D|+B & \leq & h(j) \\ & = & \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K} d_v \log\max\{1,|a|_v\} \\ & = & \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K^\infty\cup M_K^S} d_v \log\max\{1,|a|_v\} \\ & = & -\frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K^\infty\cup M_K^S, |a|_v<1} d_v \log|a|_v, \end{array}$$

by the product formula.

Putting everything together

If j is a singular unit of discriminant D, then

$$\begin{aligned} A\log|D| + B &\leq h(j) \\ &= \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K} d_v \log\max\{1,|a|_v\} \\ &= \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K^\infty\cup M_K^S} d_v \log\max\{1,|a|_v\} \\ &= -\frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K^\infty\cup M_K^S, |a|_v<1} d_v \log|a|_v, \end{aligned}$$

by the product formula. For $\varepsilon > 0$ convenient we get

$$-\frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K^\infty\cup M_K^S, |a|_v<1} d_v \log|a|_v \leq A_{\varepsilon,S}\log|D| + B_{\varepsilon,S}$$

with $A_{\varepsilon,S} < A$.

Putting everything together

If j is a singular unit of discriminant D, then

$$\begin{aligned} A\log|D|+B &\leq h(j) \\ &= \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K} d_v \log\max\{1,|a|_v\} \\ &= \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K^\infty\cup M_K^S} d_v \log\max\{1,|a|_v\} \\ &= -\frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K^\infty\cup M_K^S,|a|_v<1} d_v \log|a|_v, \end{aligned}$$

by the product formula. For $\varepsilon > 0$ convenient we get

$$-\frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K^\infty\cup M_K^S,|a|_v<1} d_v \log|a|_v \leq A_{\varepsilon,S}\log|D| + B_{\varepsilon,S}$$

with $A_{\varepsilon,S} < A$. Hence $|D|$ is bounded and the result follows.

Singular moduli are p-adically disperse

Singular moduli are p-adically disperse

Theorem (H–Menares–Rivera-Letelier, 2021)

Given $\varepsilon > 0$ *there exists* $r > 0$ *small such that*

$$\frac{1}{h(D)}\left(j(\Lambda_D) \cap B_p(0, r)\right) \leq \varepsilon \text{ for } D \to -\infty.$$

Singular moduli are p-adically disperse

Theorem (H–Menares–Rivera-Letelier, 2021)

Given $\varepsilon > 0$ there exists $r > 0$ small such that

$$\frac{1}{h(D)}\left(j(\Lambda_D) \cap B_p(0, r)\right) \leq \varepsilon \text{ for } D \to -\infty.$$

This follows from our identification of all limit measures of CM points in the p-adic setting.

p-adic distribution of CM points

p-adic distribution of CM points

For simplicity, restrict to $D < 0$ fundamental discriminant.

We have $j(\Lambda_D) \subset \overline{\mathbb{Q}} \subset \mathbb{C}_p \subset \mathbb{A}^1_{\mathrm{Berk}}$.

p-adic distribution of CM points

For simplicity, restrict to $D < 0$ fundamental discriminant.

We have $j(\Lambda_D) \subset \overline{\mathbb{Q}} \subset \mathbb{C}_p \subset \mathbb{A}^1_{\mathrm{Berk}}$.

$\mathbb{A}^1_{\mathrm{Berk}}$ can be defined as the set of multiplicative semi-norms on $\mathbb{C}_p[X]$ extending $|\cdot|_p$ on $\mathbb{C}_p$, with a suitable topology (locally compact, arc-connected),

p-adic distribution of CM points

For simplicity, restrict to $D < 0$ fundamental discriminant.

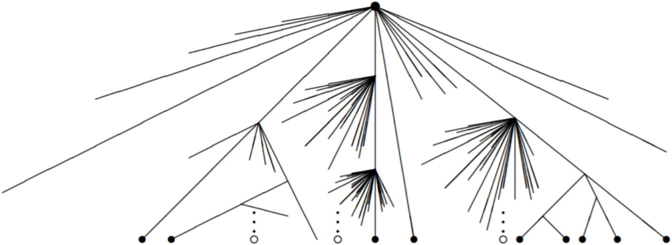
We have $j(\Lambda_D) \subset \overline{\mathbb{Q}} \subset \mathbb{C}_p \subset \mathbb{A}^1_{\mathrm{Berk}}$.

$\mathbb{A}^1_{\mathrm{Berk}}$ can be defined as the set of multiplicative semi-norms on $\mathbb{C}_p[X]$ extending $|\cdot|_p$ on $\mathbb{C}_p$, with a suitable topology (locally compact, arc-connected),and

$$\mathbb{C}_p \hookrightarrow \mathbb{A}^1_{\mathrm{Berk}}, \qquad z \mapsto \iota(z)$$

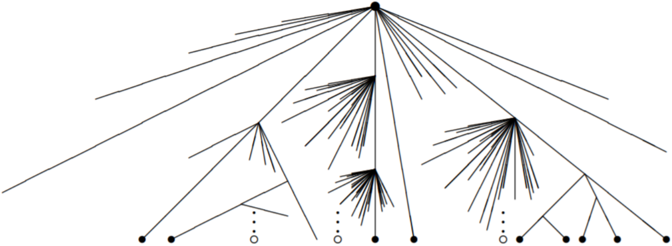
is defined by $\iota(z)(f) = |f(z)|_p$ for f in $\mathbb{C}_p[X]$.
$\mathbb{C}_p$ is dense in $\mathbb{A}^1_{\mathrm{Berk}}$.

Above the unit disc in $\mathbb{C}_p$ we have the following picture[2]



[2] Illustration of Joe Silverman

Above the unit disc in $\mathbb{C}_p$ we have the following picture[2]



At the top we have the Gauss point ζ defined by

$$\zeta(a_0 + a_1 X + \ldots + a_n X^n) = \max\{|a_0|_p, |a_1|_p, \ldots, |a_n|_p\}.$$

[2] Illustration of Joe Silverman

Convergence towards the Gauss point

Convergence towards the Gauss point

Theorem (H–Menares–Rivera-Letelier, 2020)

1. *For fundamental discriminants $D < 0$ with $\left(\frac{D}{p}\right) = 1$ we have*

$$\frac{1}{h(D)} \sum_{z \in \Lambda_D} \delta_{j(z)} \to \delta_\zeta$$

weakly on $\mathbb{A}^1_{\mathrm{Berk}}$.

2. *This is not the case for fundamental discriminants $D < 0$ with $\left(\frac{D}{p}\right) \neq 1$.*

The case $\left(\frac{D}{p}\right) \neq 1$

The case $\left(\frac{D}{p}\right) \neq 1$

Let $\mathcal{O}_D$ denote the ring of integers of $\mathbb{Q}(\sqrt{D})$. Then

$$\Lambda_D = \{E \text{ ell. curve over } \overline{\mathbb{Q}} \text{ with } \mathrm{End}(E) \simeq \mathcal{O}_D\} \subset Y(\overline{\mathbb{Q}})$$

where $Y(\overline{\mathbb{Q}})$ is the (open) moduli space of elliptic curves over $\overline{\mathbb{Q}}$.

The case $\left(\frac{D}{p}\right) \neq 1$

Let $\mathcal{O}_D$ denote the ring of integers of $\mathbb{Q}(\sqrt{D})$. Then

$$\Lambda_D = \{E \text{ ell. curve over } \overline{\mathbb{Q}} \text{ with } \mathrm{End}(E) \simeq \mathcal{O}_D\} \subset Y(\overline{\mathbb{Q}})$$

where $Y(\overline{\mathbb{Q}})$ is the (open) moduli space of elliptic curves over $\overline{\mathbb{Q}}$.

Let $\mathfrak{D}$ be the p-adic discriminant of the ring of integers $\mathcal{O}_{\mathfrak{D}}$ of $\mathbb{Q}_p(\sqrt{D})$.

The case $\left(\frac{D}{p}\right) \neq 1$

Let $\mathcal{O}_D$ denote the ring of integers of $\mathbb{Q}(\sqrt{D})$. Then

$$\Lambda_D = \{E \text{ ell. curve over } \overline{\mathbb{Q}} \text{ with } \operatorname{End}(E) \simeq \mathcal{O}_D\} \subset Y(\overline{\mathbb{Q}})$$

where $Y(\overline{\mathbb{Q}})$ is the (open) moduli space of elliptic curves over $\overline{\mathbb{Q}}$.

Let $\mathfrak{D}$ be the p-adic discriminant of the ring of integers $\mathcal{O}_{\mathfrak{D}}$ of $\mathbb{Q}_p(\sqrt{D})$.Then $D \in \mathfrak{D}$, $\mathcal{O}_D \subset \mathcal{O}_{\mathfrak{D}}$ and

$$\Lambda_D \subset \Lambda_{\mathfrak{D}} = \{E \text{ ell. curve over } \overline{\mathbb{Q}}_p \text{ with } \operatorname{End}(\widehat{E}) \simeq \mathcal{O}_{\mathfrak{D}}\} \subset Y(\overline{\mathbb{Q}}_p)$$

where $\widehat{E}$ is the *formal group* of E.

The case $\left(\frac{D}{p}\right) \neq 1$

The case $\left(\frac{D}{p}\right) \neq 1$

Every (fundamental) discriminant $D < 0$ with $\left(\frac{D}{p}\right) \neq 1$ belongs to some p-adic (fundamental) discriminant $\mathfrak{D}$.

The case $\left(\frac{D}{p}\right) \neq 1$

Every (fundamental) discriminant $D < 0$ with $\left(\frac{D}{p}\right) \neq 1$ belongs to some p-adic (fundamental) discriminant $\mathfrak{D}$.

Theorem (H–Menares–Rivera-Letelier, 2021)

For a p-adic discriminant $\mathfrak{D}$ the set $\Lambda_{\mathfrak{D}}$ is compact and there exists a (unique) Borel probability measure $\nu_{\mathfrak{D}}$ with support $\Lambda_{\mathfrak{D}}$ such that for fundamental discriminants $D < 0$ with $D \in \mathfrak{D}$ we have

$$\frac{1}{h(D)} \sum_{z \in \Lambda_D} \delta_{j(z)} \to \nu_{\mathfrak{D}}$$

weakly on $Y(\overline{\mathbb{Q}}_p)$.

The case $\left(\frac{D}{p}\right) \neq 1$

Every (fundamental) discriminant $D < 0$ with $\left(\frac{D}{p}\right) \neq 1$ belongs to some p-adic (fundamental) discriminant $\mathfrak{D}$.

Theorem (H–Menares–Rivera-Letelier, 2021)

For a p-adic discriminant $\mathfrak{D}$ the set $\Lambda_{\mathfrak{D}}$ is compact and there exists a (unique) Borel probability measure $\nu_{\mathfrak{D}}$ with support $\Lambda_{\mathfrak{D}}$ such that for fundamental discriminants $D < 0$ with $D \in \mathfrak{D}$ we have

$$\frac{1}{h(D)} \sum_{z \in \Lambda_D} \delta_{j(z)} \to \nu_{\mathfrak{D}}$$

weakly on $Y(\overline{\mathbb{Q}}_p)$.

There are 3 (for $p > 2$) or 7 (for $p = 2$) p-adic fundamental discriminants.

Singular moduli are p-adically disperse

Singular moduli are p-adically disperse

Theorem (H–Menares–Rivera-Letelier, 2021)

None of the limit measures of CM *poins in the p-adic topology has an atom in* $\mathbb{C}_p$.

Singular moduli are p-adically disperse

Theorem (H–Menares–Rivera-Letelier, 2021)

None of the limit measures of CM *poins in the p-adic topology has an atom in* $\mathbb{C}_p$.

This implies our second ingredient.

Singular moduli are p-adically disperse

Theorem (H–Menares–Rivera-Letelier, 2021)

None of the limit measures of CM *poins in the p-adic topology has an atom in* $\mathbb{C}_p$.

This implies our second ingredient.

Theorem (H–Menares–Rivera-Letelier, 2021)

Given $\varepsilon > 0$ *there exists* $r > 0$ *small such that*

$$\frac{1}{h(D)} \left(j(\Lambda_D) \cap B_p(0, r) \right) \leq \varepsilon \text{ for } D \to -\infty.$$

Singular moduli are p-adically disperse

Theorem (H–Menares–Rivera-Letelier, 2021)

None of the limit measures of CM *poins in the p-adic topology has an atom in* $\mathbb{C}_p$.

This implies our second ingredient.

Theorem (H–Menares–Rivera-Letelier, 2021)

Given $\varepsilon > 0$ *there exists* $r > 0$ *small such that*

$$\frac{1}{h(D)} \left(j(\Lambda_D) \cap B_p(0, r) \right) \leq \varepsilon \text{ for } D \to -\infty.$$

The last ingredient

The last ingredient

Theorem (H–Menares–Rivera-Letelier, 2021)

For j a nonzero singular modulus of discriminant D we have

$$-\log|j|_p \leq c_p \log|D|,$$

with $c_p > 0$ absolute constant.

The last ingredient

Theorem (H–Menares–Rivera-Letelier, 2021)

For j a nonzero singular modulus of discriminant D we have

$$-\log|j|_p \leq c_p \log|D|,$$

with $c_p > 0$ absolute constant.

The proof uses ideas of F. Charles (2018) and results of Gross (1986): deformation theory of elliptic curves, formal groups/modules, and canonical/quasi-canonical liftings.

The last ingredient

Theorem (H–Menares–Rivera-Letelier, 2021)

For j a nonzero singular modulus of discriminant D we have

$$-\log |j|_p \leq c_p \log |D|,$$

with $c_p > 0$ absolute constant.

The proof uses ideas of F. Charles (2018) and results of Gross (1986): deformation theory of elliptic curves, formal groups/modules, and canonical/quasi-canonical liftings.

With the three main ingredients, we get the result!

The last ingredient

Theorem (H–Menares–Rivera-Letelier, 2021)

For j a nonzero singular modulus of discriminant D we have

$$-\log |j|_p \leq c_p \log |D|,$$

with $c_p > 0$ absolute constant.

The proof uses ideas of F. Charles (2018) and results of Gross (1986): deformation theory of elliptic curves, formal groups/modules, and canonical/quasi-canonical liftings.

With the three main ingredients, we get the result!
The strategy is essentially the same for differences of singular moduli that are S-units.

Final comments

Final comments

In

On singular moduli that are S-units (2020)

F. Campagna shows that $S_0 = \{p \text{ prime }, p \equiv 1 \bmod 3\}$ every singular S-unit is a singular unit, hence there are none.

Final comments

In

On singular moduli that are S-units (2020)

F. Campagna shows that $S_0 = \{p \text{ prime }, p \equiv 1 \bmod 3\}$ every singular S-unit is a singular unit, hence there are none.

We can use Campagna's result to extend ours to certain classes of infinite sets S of prime numbers (larger than S_0).

Other modular functions

[3] (private communication)

Other modular functions

Habegger asked us[3]: What about the λ-invariants? These are Hauptmoduln for $\Gamma(2)$.

[3] (private communication)

Other modular functions

Habegger asked us[3]: What about the λ-invariants? These are Hauptmoduln for $\Gamma(2)$.

General question: What about more general Hauptmoduln?

[3](private communication)

Other modular functions

Habegger asked us[3]: What about the λ-invariants? These are Hauptmoduln for $\Gamma(2)$.

General question: What about more general Hauptmoduln?

The method seems to extend without major difficulties to the case of differences of singular moduli that are S-units for any Hauptmodul of a genus zero subgroup of $\mathrm{GL}_2^+(\mathbb{Q})$ that is algebraically related to the j-function.

[3] (private communication)

Examples

Examples

1. The λ-invariants: there are six of them, they satisfy

$$2^8(1-\lambda+\lambda^2)^3 - j\lambda^2(1-\lambda)^2 = 0.$$

Examples

1. The λ-invariants: there are six of them, they satisfy

$$2^8(1-\lambda+\lambda^2)^3 - j\lambda^2(1-\lambda)^2 = 0.$$

In

The lambda invariant at CM *points* (2018)

Yang, Yin and Yu chose a particular lambda invariant λ_0 and proved that $\lambda_0(z)$ is an algebraic unit for infinitely many CM points z.

Examples

1. The λ-invariants: there are six of them, they satisfy

$$2^8(1-\lambda+\lambda^2)^3 - j\lambda^2(1-\lambda)^2 = 0.$$

   In

   The lambda invariant at CM *points* (2018)

   Yang, Yin and Yu chose a particular lambda invariant λ_0 and proved that $\lambda_0(z)$ is an algebraic unit for infinitely many CM points z.

2. Weber functions $\mathbf{f}, \mathbf{f}_1, \mathbf{f}_2$ are roots of

$$(X^{24} \pm 16)^3 - X^{24} j = 0.$$

Examples

1. The λ-invariants: there are six of them, they satisfy

$$2^8(1-\lambda+\lambda^2)^3 - j\lambda^2(1-\lambda)^2 = 0.$$

In

The lambda invariant at CM *points* (2018)

Yang, Yin and Yu chose a particular lambda invariant λ_0 and proved that $\lambda_0(z)$ is an algebraic unit for infinitely many CM points z.

2. Weber functions $\mathbf{f}, \mathbf{f}_1, \mathbf{f}_2$ are roots of

$$(X^{24} \pm 16)^3 - X^{24} j = 0.$$

Weber's computations show that infinitely many singular moduli for these functions are algebraic units.

Examples

1. The λ-invariants: there are six of them, they satisfy

$$2^8(1-\lambda+\lambda^2)^3 - j\lambda^2(1-\lambda)^2 = 0.$$

In

The lambda invariant at CM *points* (2018)

Yang, Yin and Yu chose a particular lambda invariant λ_0 and proved that $\lambda_0(z)$ is an algebraic unit for infinitely many CM points z.

2. Weber functions $\mathbf{f}, \mathbf{f}_1, \mathbf{f}_2$ are roots of

$$(X^{24} \pm 16)^3 - X^{24} j = 0.$$

Weber's computations show that infinitely many singular moduli for these functions are algebraic units.

Note that 0 is not a singular modulus for any of these functions.

Fin

¡Muchas gracias!