Trinomials, Singular Moduli and Riffaut's Conjecture

Yuri Bilu
(joint work with Florian Luca, Amalia Pizarro-Madariaga)

Zykin memorial conference
June 19, 2020

My co-authors

Singular Moduli

A singular modulus is $j(E)$, where E is elliptic curve with CM.

$$E : y^2 = 4x^3 - g_2 x - g_3 \qquad j(E) = 1728\frac{g_2^3}{g_2^3 - 27g_3^2}.$$

Alternatively, a singular modulus is $j(\tau)$, where $\tau \in \mathbb{H}$ is a quadratic irrationality and $j : \mathbb{H} \to \mathbb{C}$ is the j-function

$$j(z) = q^{-1} + 744 + 196884q + 21493760q^2 + \ldots, \quad q = e^{2\pi iz}.$$

If $E = \mathbb{C}/\langle\tau, 1\rangle$ then $j(E) = j(\tau)$.

Discriminant of a singular modulus

The discriminant $\Delta = \Delta_x$ of a singular modulus $x = j(E) = j(\tau)$ is defined in two equivalent ways.

- the discriminant of the imaginary quadratic order $\mathrm{End}(E)$:

$$\mathrm{End}(E) = \mathbb{Z}\left[\frac{\Delta+\sqrt{\Delta}}{2}\right]$$

- the discriminant of the minimal polynomial $aT^2 - bT + c \in \mathbb{Z}[T]$ of τ:

$$\Delta = b^2 - 4ac, \qquad \tau = \frac{b+\sqrt{\Delta}}{2a}.$$

We have

$$\Delta < 0, \qquad \Delta \equiv 0, 1 \bmod 4,$$

and every Δ with these properties serves as the discriminant of some singular modulus.

Degree of a singular modulus

Fundamental facts

- A singular modulus of discriminant Δ is an algebraic integer of degree $h(\Delta)$, the class number of Δ.
- All singular moduli of discriminant Δ form a Galois orbit over $\mathbb{Q}$; in particular there are $h(\Delta)$ singular moduli of discriminant Δ.

In particular, there exist 13 singular moduli in $\mathbb{Q}$:

Δ	-3	-4	-7	-8	-11	-12	-16	-19	-27
x	0	1728	-3375	8000	-32768	54000	287496	-884736	-12288000

Δ	-28	-43	-67	-163
x	16581375	-884736000	-147197952000	-262537412640768000

Similarly, there are:

- 29 pairs of singular moduli of degree 2;
- 25 triples of singular moduli of degree 3;
- etc.

Riffaut's conjecture

Conjecture (A. Riffaut, 2019) A singular modulus of degree $h \geq 3$ cannot be a root of a trinomial with rational coefficients.

A trinomial is $X^m + AX^n + B$, where $m > n > 0$ and $B \neq 0$.

We do not formally assume $A \neq 0$, but for "trinomials" with $A = 0$ the conjecture is very easy.

Motivation: equations with singular moduli

Theorem (André, 1998) If $F(X, Y) \in \mathbb{C}[X, Y]$ is irreducible and not "special" then $F(x, y) = 0$ has at most finitely many solutions in singular moduli x, y.

Special polynomials

- $X - \alpha$, where α is a singular modulus
- $Y - \beta$, where β is a singular modulus
- $\Phi_N(X, Y)$ the modular polynomial of level N (the irreducible polynomial in $\mathbb{Z}[X, Y]$ satisfying $\Phi_N\big(j(z), j(Nz)\big) = 0$)

$$\Phi_1(X, Y) = X - Y$$

$$\begin{aligned}\Phi_2(X, Y) = {} & X^3 - X^2Y^2 + 1488X^2Y - 162000X^2 + 1488XY^2 \\ & + 40773375XY + 8748000000X + Y^3 - 162000Y^2 \\ & + 8748000000Y - 157464000000000\end{aligned}$$

$$\ldots \quad \ldots \quad \ldots$$

Motivation: equations with singular moduli

Theorem (André, 1998) If $F(X, Y) \in \mathbb{C}[X, Y]$ is irreducible and not "special" then $F(x, y) = 0$ has at most finitely many solutions in singular moduli x, y.

Proofs:

- André (1998): non-effective
- Edixhoven (1998): GRH
- Pila (2009): non-effective
- Kühne (2012), B., Masser, Zannier (2013): effective
- Kühne (2013): very effective

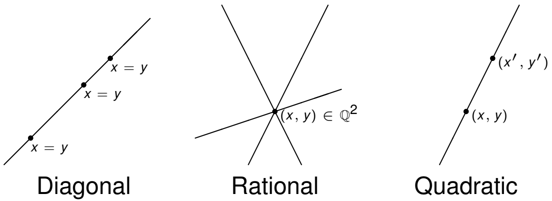
Linear equations

Kühne (2013): $x + y = 1$ has no solutions

Allombert, B., Pizarro-Madariaga (2015): $A, B, C \in \mathbb{Q}, \quad AB \neq 0$
$Ax + By = C$ has only "obvious" solutions:

- The "diagonal" case: any point with $x = y$ is a solution if $A + B = C = 0$;
- The "rational" case: $x, y \in \mathbb{Q}$
- The "quadratic case $\mathbb{Q}(x) = \mathbb{Q}(y)$ is of degree 2 over $\mathbb{Q}$

(No solutions of degree 3 or higher.)



Riffaut's work

Riffaut (and Luca), 2019: equation $Ax^m + By^n = C$,
where $A, B, C \in \mathbb{Q}$, $AB \neq 0$, $m, n \in \mathbb{Z}_{>0}$
has only "obvious" solutions

Riffaut's work

Riffaut (and Luca), 2019: equation $Ax^m + By^n = C$,
where $A, B, C \in \mathbb{Q}$, $\quad AB \neq 0$, $\quad m, n \in \mathbb{Z}_{>0}$
has only "obvious" solutions with $x \neq y$
("rational" case and "quadratic" case)

Riffaut's work

Riffaut (and Luca), 2019: equation $Ax^m + By^n = C$,
where $A, B, C \in \mathbb{Q}$, $\quad AB \neq 0$, $\quad m, n \in \mathbb{Z}_{>0}$
has only "obvious" solutions with $x \neq y$
("rational" case and "quadratic" case)

Riffaut's argument fails for $x = y$.

Riffaut's work

Riffaut (and Luca), 2019: equation $Ax^m + By^n = C$,
where $A, B, C \in \mathbb{Q}$, $\quad AB \neq 0$, $\quad m, n \in \mathbb{Z}_{>0}$
has only "obvious" solutions with $x \neq y$
("rational" case and "quadratic" case)

Riffaut's argument fails for $x = y$.

The case $x = y$ reduces to the following problem:
Determine singular moduli which are roots of trinomials

This is the case for singular moduli of degree $h = 1$ or $h = 2$.

Riffaut conjectured that there are no others.

> *much about trinomials is known, but this knowledge is still insufficient to rule out such a possibility*
>
> Riffaut (2019)

Our results

B., Luca, Pizarro-Madariaga arXiv:2003.06547 (March 2020)

Theorem 1: Assume GRH. Then a trinomial $/\mathbb{Q}$ cannot vanish at a singular modulus of degree $h \geq 3$. (GRH $\Rightarrow$ Riffaut's conjecture)

Our results

B., Luca, Pizarro-Madariaga arXiv:2003.06547 (March 2020)

Theorem 1: Assume GRH. Then a trinomial $/\mathbb{Q}$ cannot vanish at a singular modulus of degree $h \geq 3$. (GRH $\Rightarrow$ Riffaut's conjecture)

Call Δ trinomial discriminant if $h(\Delta) \geq 3$ and some singular modulus of discriminant Δ is a root of a trinomial $/\mathbb{Q}$. ($\Leftrightarrow$ All singular moduli of discriminant Δ are.)

Riffaut's conjecture: trinomial discriminants do not exist.

Our results

B., Luca, Pizarro-Madariaga arXiv:2003.06547 (March 2020)

Theorem 1: Assume GRH. Then a trinomial $/\mathbb{Q}$ cannot vanish at a singular modulus of degree $h \geq 3$. (GRH $\Rightarrow$ Riffaut's conjecture)

Call Δ trinomial discriminant if $h(\Delta) \geq 3$ and some singular modulus of discriminant Δ is a root of a trinomial $/\mathbb{Q}$. ($\Leftrightarrow$ All singular moduli of discriminant Δ are.)

Theorem 2: Every trinomial discriminant satisfies $|\Delta| > 10^{11}$.

Theorem 3: Every trinomial discriminant, with at most one exception, satisfies $|\Delta| < 10^{160}$. In particular, the set of trinomial discriminants is finite.

Theorem 4: A trinomial discriminant is of the form $-p$ or $-pq$, where p, q are (distinct) odd prime numbers.

Theorem 5: If $X^m + AX^n + B$ vanishes at a singular modulus of discriminant $> 10^{40}$ then $m - n \leq 2$.

Roots of trinomials

Proposition: Let $w, x, y \in \mathbb{C}$ be roots of $X^m + AX^n + B \in \mathbb{C}[X]$ with $|w| \geq |x| \geq |y|$. Then

$$0 \leq 1 - |y/x| \leq 4|x/w|^{m-n} \leq 4|x/w|$$

Informally: if $|w|$ is "much bigger" than $|x|$, $|y|$ then x and y have "almost the same" absolute value.

Proof We have

$$\begin{vmatrix} w^m & w^n & 1 \\ x^m & x^n & 1 \\ y^m & y^n & 1 \end{vmatrix} = 0.$$

Expanding the determinant, we obtain

$$\begin{aligned} |w|^m |x^n - y^n| &\leq |w|^n |x|^m + |w|^n |y|^m + |x|^m |y|^n + |x|^n |y|^m \\ &\leq 4|w|^n |x|^m. \end{aligned}$$

Dividing by $|w|^m |x|^n$, we obtain

$$|1 - (y/x)^n| \leq 4|x/z|^{m-n}.$$

But

$$|1 - (y/x)^n| \geq 1 - |y/x|^n \geq 1 - |y/x| \geq 0. \qquad \square$$

Gauss reduction theory

T_Δ the set of triples $(a, b, c) \in \mathbb{Z}^3$ such that

$$\Delta = b^2 - 4ac, \qquad \gcd(a, b, c) = 1,$$
$$\text{either} \quad -a < b \le a < c \quad \text{or} \quad 0 \le b \le a = c. \qquad (*)$$

Remark: $(*)$ is equivalent to "$\frac{b+\sqrt{\Delta}}{2a}$ belongs to the standard fundamental domain".

Gauss: there is a bijection

$$\begin{array}{ccc} T_\Delta & \leftrightarrow & \{\text{singular moduli of discriminant } \Delta\} \\ (a, b, c) & \mapsto & j\left(\dfrac{b+\sqrt{\Delta}}{2a}\right) \end{array}$$

In particular, $h(\Delta) = \# T_\Delta$.

Crucial: there is exactly one $(a, b, c) \in T_\Delta$ with $a = 1$:

$$\begin{array}{ll} (1, 1, (1-\Delta)/4) & \text{if } \Delta \equiv 1 \bmod 4 \\ (1, 0, -\Delta/4) & \text{if } \Delta \equiv 0 \bmod 4 \end{array}$$

We call the corresponding singular modulus dominant.

Size of singular moduli

- We have
$$j(z) = q^{-1} + 744 + 196884q + \ldots, \quad q = e^{2\pi iz}.$$
- If $\operatorname{Im} z \geq \varepsilon > 0$ then $j(z) = q^{-1} + O_\varepsilon(1)$.

Size of singular moduli

- We have

$$j(z) = q^{-1} + 744 + 196884q + \dots, \quad q = e^{2\pi iz}.$$

- If $\mathrm{Im}\, z \geq \varepsilon > 0$ then $|j(z)| = |q^{-1}| + O_\varepsilon(1)$.

Size of singular moduli

- We have

$$j(z) = q^{-1} + 744 + 196884q + \dots, \qquad q = e^{2\pi iz}.$$

- If $\mathrm{Im}\, z \geq \varepsilon > 0$ then $|j(z)| = |q^{-1}| + O_\varepsilon(1)$.
- If $(a, b, c) \in T_\Delta$ then $|b| \leq a \leq c$. We obtain

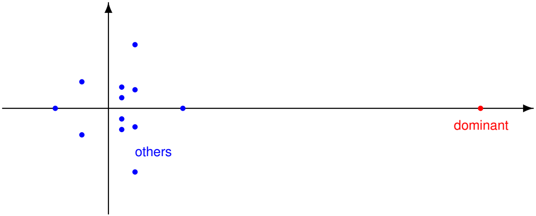
$$|\Delta| = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2; \qquad \boxed{a \leq |\Delta/3|^{1/2}};$$

In particular $\mathrm{Im}\left(\frac{b+\sqrt{\Delta}}{2a}\right) \geq \frac{\sqrt{3}}{2}$.

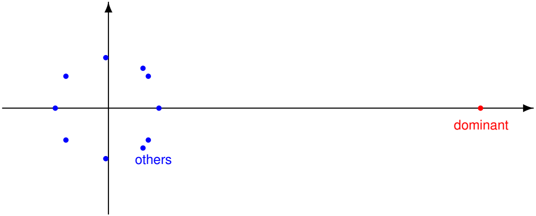
- Hence $x = j\left(\frac{b+\sqrt{\Delta}}{2a}\right)$ satisfies $\boxed{|x| = e^{\pi|\Delta|^{1/2}/a} + O(1).}$
- In particular:

$$\begin{aligned} |x| &= e^{\pi|\Delta|^{1/2}} + O(1) && \text{if } x \text{ is dominant,} \\ |x| &\leq e^{\pi|\Delta|^{1/2}/2} + O(1) && \text{if not.} \end{aligned}$$

Singular moduli on the complex plane



Arbitrary discriminant: one (dominant) very big ($\approx e^{\pi|\Delta|^{1/2}}$) and real, others much smaller ($\ll e^{\pi|\Delta|^{1/2}/2}$)



Trinomial discriminant: one (dominant) very big ($\approx e^{\pi|\Delta|^{1/2}}$) and real, others much smaller ($\leq |\Delta|^{0.8}$) and of almost the same absolute value

Suitable integers

Call a positive integer a suitable for the discriminant Δ if there exist $b, c \in \mathbb{Z}$ such that $(a, b, c) \in T_\Delta$.

Some properties:

- 1 is suitable for any discriminant.
- If a is suitable for Δ then $a \leq |\Delta/3|^{1/2}$.
- If $\Delta \equiv 0 \mod 4$ and $|\Delta| > 220$ then 2 or 4 or 8 is suitable for Δ.
- If p is a prime number such $(\Delta/p) = 1$ and $|\Delta| \geq 4p^2$ then p is suitable for Δ.
- In particular, 2 is suitable for Δ if $\Delta \equiv 1 \mod 8$ and $\Delta \neq -7$.
- Let a be an odd divisor of Δ satisfying $\gcd(a, \Delta/a) = 1$ and $|\Delta| \geq 3a^2$. Then a is suitable for Δ.

Suitable integers for trinomial discriminants

Proposition: Let Δ be a trinomial discriminant, $|\Delta| \geq 10^5$, and $a > 1$ suitable for Δ. Then $\boxed{a > 3|\Delta|^{1/2}/\log|\Delta|.}$

"Proof": Let a be the smallest suitable > 1. Let $a' > a$ be another suitable (it exists!), and x, x' corresponding singular moduli. Then $|x| \approx |x'|$. Recall that

$$|x| = e^{\pi|\Delta|^{1/2}/a} + O(1),$$
$$|x'| = e^{\pi|\Delta|^{1/2}/a'} + O(1) \leq e^{\pi|\Delta|^{1/2}/(a+1)} + O(1)$$

However, if a is small, then $e^{\pi|\Delta|^{1/2}/a}$ is "much bigger" than $e^{\pi|\Delta|^{1/2}/(a+1)}$. $\square$

A lower bound for trinomial discriminants

Theorem 2: Every trinomial discriminant satisfies $|\Delta| > 10^{11}$.

We prove this by running several PARI scripts.

- For Δ in the range $10^5 \le |\Delta| \le 10^{11}$ we use a sieving procedure to show that each such Δ admits a prime p with

$$(\Delta/p) = 1, \qquad p < 3|\Delta|^{1/2}/\log|\Delta|.$$

- For Δ with $|\Delta| \le 10^5$ and $h(\Delta) > 3$ we find singular moduli w, x, y of discriminant Δ such that $|w| \ge |x| \ge |y|$ but the inequality

$$1 - |y/x| \le 4|x/w|$$

  is not satisfied.
- The 25 discriminants with $h = 3$ require special treatment.

The total computational time was about 10 minutes on modern laptop. The bottleneck was not the processor time, but the memory: sieving requires dealing with big lists.

Structure of trinomial discriminants

Theorem 4: A trinomial discriminant is of the form $-p$ or $-pq$, where p, q are (distinct) odd prime numbers.

We prove this by showing that in all other cases there is a "small" suitable integer.

- **Step 1:** A trinomial discriminant cannot be even, because an even discriminant admits 2, 4 or 8 as a suitable integer.
- **Step 2:** A trinomial discriminant cannot have more than 2 distinct prime divisors.

  Write $\Delta = -p_1^{\nu_1} \cdots p_k^{\nu_k}$ with $k \geq 3$ and $p_1^{\nu_1} < \ldots < p_k^{\nu_k}$. Then $a = p_1^{\nu_1}$ is suitable and $a < |\Delta|^{1/3} < 3|\Delta|^{1/2}/\log|\Delta|$.
- **Step 3:** A trinomial discriminant is not a $-$square.

  Assume $\Delta = -\square$. One of the primes $5, 13, 17$ (call it q) does not divide Δ, and $(\Delta/q) = 1$.
- … … …

The conditional result

Theorem 1: Assume GRH. Then trinomial discriminants do not exist. In other words, GRH$\Rightarrow$Riffaut's conjecture

Let χ be a primitive real Dirichlet character $\bmod m$.

Lamzouri, Li, Soundararajan (2015): Assume GRH. Then there exists a prime p such that $\chi(p) = 1$ and

$$p \leq \max\left\{10^9, \left(\log m + \frac{5}{2}(\log\log m)^2 + 6\right)^2\right\}.$$

If Δ is a trinomial discriminant and $m = |\Delta|$ then $\chi = (\Delta/\cdot)$ is a primitive real character $\bmod m$. We obtain a contradiction if the rhs is smaller than $3m^{1/2}/\log m$, which is true for $m \geq 10^{21}$. However, we only know that $m > 10^{11}\ldots$

We slightly adapted their argument and obtained what we wanted: if Δ is trinomial, the previous statement holds with $\chi = (\Delta/\cdot)$ and $3m^{1/2}/\log m$ in the rhs.

The upper bound for all but one

Theorem 3: Every trinomial discriminant, with at most one exception, satisfies $|\Delta| < 10^{160}$. In particular, the set of trinomial discriminants is finite.

Let χ be a primitive real Dirichlet character $\bmod m$.

Linnik-Vinogradov (1966): there exists $p \ll_\varepsilon m^{1/4+\varepsilon}$ with $\chi(p) = 1$.

Good news: $m^{1/4+\varepsilon} < m^{1/2}/\log m$ for big m.
Bad news: the implied constant is not effective.

Two ingredients:

- Burgess estimate for short character sums (effective);
- Siegel's theorem $L(1,\chi) \gg_\varepsilon m^{-\varepsilon}$ (non-effective);

Replace Siegel by Tatuzawa: $L(1,\chi) \geq 0.655\varepsilon m^{-\varepsilon}$ for all m with at most one exception.

Result: with at most one exception, for each trinomial Δ satisfying $|\Delta| \geq 10^{160}$ there exists p such that $(\Delta/p) = 1$ and $p \leq 3|\Delta|^{1/2}/\log|\Delta|$.

The trinomial

Theorem 5: If $X^m + AX^n + B$ vanishes at a singular modulus of discriminant Δ satisfying $|\Delta| > 10^{40}$ then $m - n \leq 2$.

We will prove that $m - n \leq 4$.

- We have $h(\Delta) > 6$ (even > 100, by the work of Watkins). Since a trinomial has ≤ 4 real roots, there exist non-real singular moduli x, y of discriminant Δ such that $y \neq x, \bar{x}$.
- Set $z = x\bar{x} - y\bar{y} = |x|^2 - |y|^2$. It is a non-zero(!) real algebraic integer, satisfying $|z| \leq e^{-(m-n-0.01)\pi|\Delta|^{1/2}}$.
- The $\mathbb{Q}$-conjugates of z are of the form $x_1x_2 - y_1y_2$, where x_1, x_2, y_1, y_2 are distinct singular moduli of discriminant Δ.
- There are exactly 4 conjugates such that one of x_1, x_2, y_1, y_2 is dominant. Hence

$$|\mathcal{N}(z)| \leq e^{4.01\pi|\Delta|^{1/2} - (m-n-0.01)\pi|\Delta|^{1/2}}.$$

- But $|\mathcal{N}(z)| \geq 1$ because z is algebraic integer. Hence $m - n \leq 4.02$. □
- To prove $m - n \leq 2$ we use a p-adic argument to show that $|\mathcal{N}(z)| \geq e^{1.99\pi|\Delta|^{1/2}}$.

Thanks!