Congruent numbers and local polynomials

Larry Rolen (joint work with Ehlen, Guerzhoy, and Kane)

Vanderbilt University

Joint Math Meetings, January 17, 2019

An ancient geometry problem

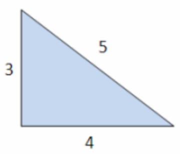
- A Pythagorean triple is an $(a, b, c) \in \mathbb{N}^3$ with $a^2 + b^2 = c^2$.

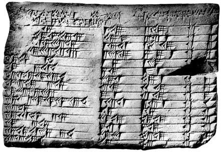
An ancient geometry problem

- A Pythagorean triple is an $(a, b, c) \in \mathbb{N}^3$ with $a^2 + b^2 = c^2$.
- Easy to find examples, like $(3, 4, 5)$, first tables in 1800 BC:

An ancient geometry problem

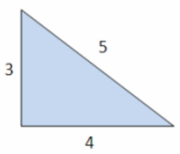
- A Pythagorean triple is an $(a, b, c) \in \mathbb{N}^3$ with $a^2 + b^2 = c^2$.
- Easy to find examples, like $(3, 4, 5)$, first tables in 1800 BC:

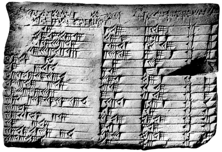




An ancient geometry problem

- A Pythagorean triple is an $(a, b, c) \in \mathbb{N}^3$ with $a^2 + b^2 = c^2$.
- Easy to find examples, like $(3, 4, 5)$, first tables in 1800 BC:

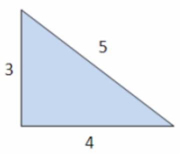


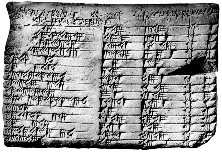


- Easy to parameterize **all** such triples: divide to get $(a/c)^2 + (b/c)^2 = 1$ on unit circle, line with rational slope:

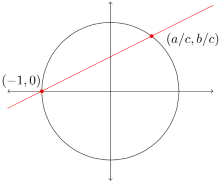
An ancient geometry problem

- A Pythagorean triple is an $(a, b, c) \in \mathbb{N}^3$ with $a^2 + b^2 = c^2$.
- Easy to find examples, like $(3, 4, 5)$, first tables in 1800 BC:





- Easy to parameterize **all** such triples: divide to get $(a/c)^2 + (b/c)^2 = 1$ on unit circle, line with rational slope:



A slight modification

- $n \in \mathbb{N}$ is congruent if some **rational** right tri. has area n.

A slight modification

- $n \in \mathbb{N}$ is congruent if some **rational** right tri. has area n.
- 6 is congruent as its the area of the $3 - 4 - 5$ triangle.

A slight modification

- $n \in \mathbb{N}$ is congruent if some **rational** right tri. has area n.
- 6 is congruent as its the area of the $3 - 4 - 5$ triangle.
- Question: Given $n \in \mathbb{N}$, how can we test if its congruent?

A slight modification

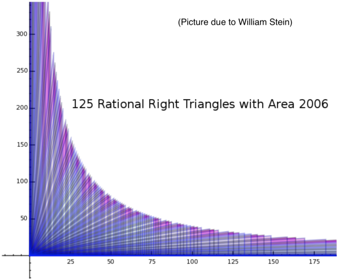
- $n \in \mathbb{N}$ is congruent if some **rational** right tri. has area n.
- 6 is congruent as its the area of the $3-4-5$ triangle.
- Question: Given $n \in \mathbb{N}$, how can we test if its congruent?
- A basic idea: Computer search through Pythagorean triples and their rescalings.

A slight modification

- $n \in \mathbb{N}$ is congruent if some **rational** right tri. has area n.
- 6 is congruent as its the area of the $3 - 4 - 5$ triangle.
- Question: Given $n \in \mathbb{N}$, how can we test if its congruent?
- A basic idea: Computer search through Pythagorean triples and their rescalings.
- Since $\mathbb{Q}$ is dense in $\mathbb{R}$, not a finite check.

A slight modification

- $n \in \mathbb{N}$ is congruent if some **rational** right tri. has area n.
- 6 is congruent as its the area of the $3-4-5$ triangle.
- Question: Given $n \in \mathbb{N}$, how can we test if its congruent?
- A basic idea: Computer search through Pythagorean triples and their rescalings.
- Since $\mathbb{Q}$ is dense in $\mathbb{R}$, not a finite check.



Examples

- Fermat famously proved by infinite descent (also known by Fibonacci) that 1 isn't congruent.

Examples

- Fermat famously proved by infinite descent (also known by Fibonacci) that 1 isn't congruent.
- First few (square-free) congruent numbers:
  $5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, 38, 39 \dots$

Examples

- Fermat famously proved by infinite descent (also known by Fibonacci) that 1 isn't congruent.
- First few (square-free) congruent numbers: $5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, 38, 39 \ldots$
- 157 is congruent.

Examples

- Fermat famously proved by infinite descent (also known by Fibonacci) that 1 isn't congruent.
- First few (square-free) congruent numbers: $5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, 38, 39 \ldots$
- 157 is congruent.
- Zagier: the "simplest" triangle showing this has hypotenuse: $\frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}$ (!!)

Connections to deeper theory

- There is a one-to-one correspondence:

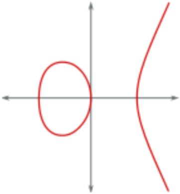
$$\{(a,b,c) : \frac{ab}{2} = n, a^2+b^2 = c^2\} \leftrightarrow \{(x,y) : y^2 = x^3-n^2x, y \neq 0\}.$$

Connections to deeper theory

- There is a one-to-one correspondence:

$$\{(a,b,c) : \frac{ab}{2} = n, a^2+b^2 = c^2\} \leftrightarrow \{(x,y) : y^2 = x^3 - n^2x, y \neq 0\}.$$

- So n is congruent iff there is a $\mathbb{Q}$-point on the **elliptic curve** E_n: $y^2 = x^3 - n^2x$ other than the 3 "easy" points on x-axis:

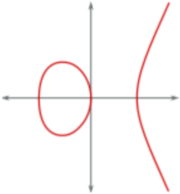


Connections to deeper theory

- There is a one-to-one correspondence:

$$\{(a,b,c) : \frac{ab}{2} = n, a^2+b^2 = c^2\} \leftrightarrow \{(x,y) : y^2 = x^3-n^2x, y \neq 0\}.$$

- So n is congruent iff there is a $\mathbb{Q}$-point on the **elliptic curve** E_n: $y^2 = x^3 - n^2x$ other than the 3 "easy" points on x-axis:



- Birch and Swinnerton-Dyer conjecture $\implies$ n is congruent if and only if the central L-value vanishes:

$$L(E,1) = 0.$$

An efficient criterion

- Tunnell gave a formula to check for congruent numbers.

An efficient criterion

- Tunnell gave a formula to check for congruent numbers.
- For example, assuming BSD, an odd number n is congruent iff

$$\begin{aligned}&\#\{(x,y,z)\in\mathbb{Z}^3 : x^2+2y^2+8z^2=n\}\\ =\ &2\cdot\#\{(x,y,z)\in\mathbb{Z}^3 : x^2+2y^2+32z^2=n\}.\end{aligned}$$

An efficient criterion

- Tunnell gave a formula to check for congruent numbers.
- For example, assuming BSD, an odd number n is congruent iff

$$\#\{(x,y,z)\in\mathbb{Z}^3 : x^2+2y^2+8z^2=n\}$$
$$=2\cdot\#\{(x,y,z)\in\mathbb{Z}^3 : x^2+2y^2+32z^2=n\}.$$

- Waldspurger, and later Kohnen and Zagier, related **families** of L-values like $L(E_n,1)$ to coefficients of **modular forms**.

An efficient criterion

- Tunnell gave a formula to check for congruent numbers.
- For example, assuming BSD, an odd number n is congruent iff

$$\begin{aligned} &\#\{(x,y,z) \in \mathbb{Z}^3 : x^2 + 2y^2 + 8z^2 = n\} \\ = 2\cdot&\#\{(x,y,z) \in \mathbb{Z}^3 : x^2 + 2y^2 + 32z^2 = n\}. \end{aligned}$$

- Waldspurger, and later Kohnen and Zagier, related **families** of L-values like $L(E_n, 1)$ to coefficients of **modular forms**.
- Other formulas for $L(E_n, 1)$ given by B-SD, for CM curves.

An efficient criterion

- Tunnell gave a formula to check for congruent numbers.
- For example, assuming BSD, an odd number n is congruent iff

$$\#\{(x,y,z)\in\mathbb{Z}^3 : x^2+2y^2+8z^2=n\}$$
$$=2\cdot\#\{(x,y,z)\in\mathbb{Z}^3 : x^2+2y^2+32z^2=n\}.$$

- Waldspurger, and later Kohnen and Zagier, related **families** of L-values like $L(E_n,1)$ to coefficients of **modular forms**.
- Other formulas for $L(E_n,1)$ given by B-SD, for CM curves.
- We will give alternate formulas which include some non-CM cases and have analogies with classical formulas.

Classical results of Dirichlet and Gauss

- For $\chi_d := \left(\frac{d}{\cdot}\right)$, the **Dirichlet L-series** is

$$L(\chi, s) := \sum_{n \geq 1} \chi(n) n^{-s} \quad (\mathrm{Re}(s) > 1).$$

Classical results of Dirichlet and Gauss

- For $\chi_d := \left(\frac{d}{\cdot}\right)$, the **Dirichlet L-series** is

$$L(\chi, s) := \sum_{n \geq 1} \chi(n) n^{-s} \quad (\mathrm{Re}(s) > 1).$$

- For example, the Leibniz formula is:

$$L(\chi_{-4}, 1) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} \cdots = \frac{\pi}{4}.$$

Classical results of Dirichlet and Gauss

- For $\chi_d := \left(\frac{d}{\cdot}\right)$, the **Dirichlet L-series** is

$$L(\chi, s) := \sum_{n \geq 1} \chi(n) n^{-s} \quad (\mathrm{Re}(s) > 1).$$

- For example, the Leibniz formula is:

$$L(\chi_{-4}, 1) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} \ldots = \frac{\pi}{4}.$$

- Dirichlet Class Number Formula: $L(\chi_d, 1) \doteq h(d)$, where $h(d)$ is the **class number** of $\mathbb{Q}(\sqrt{d})$.

Classical results of Dirichlet and Gauss

- For $\chi_d := \left(\frac{d}{\cdot}\right)$, the **Dirichlet L-series** is

$$L(\chi, s) := \sum_{n\geq 1} \chi(n) n^{-s} \quad (\mathrm{Re}(s) > 1).$$

- For example, the Leibniz formula is:

$$L(\chi_{-4}, 1) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} \cdots = \frac{\pi}{4}.$$

- Dirichlet Class Number Formula: $L(\chi_d, 1) \doteq h(d)$, where $h(d)$ is the **class number** of $\mathbb{Q}(\sqrt{d})$.
- Gauss gave formulas like for $d \equiv 3 \pmod 8$:

$$h(-d) = \sum_{x^2+y^2+z^2=d} 1.$$

Analogous results

Question

Are there similar eqns for other L-functions, e.g., for elliptic curves?

Analogous results

Question

Are there similar eqns for other L-functions, e.g., for elliptic curves?

Sample Theorem (Ehlen, Guerzhoy, Kane, R.)

Suppose that $D < 0$, $|D| \equiv 3 \pmod 8$, $3|D| \neq \square$. *Set*

$$\chi(a,b,c) := \begin{cases} \left(\frac{-3}{a}\right) & \text{if } 3 \nmid a, \\ \left(\frac{-3}{c}\right) & \text{if } 3 | a. \end{cases}$$

Analogous results

Question

Are there similar eqns for other L-functions, e.g., for elliptic curves?

Sample Theorem (Ehlen, Guerzhoy, Kane, R.)

Suppose that $D < 0$, $|D| \equiv 3 \pmod 8$, $3|D| \neq \Box$. *Set*

$$\chi(a,b,c) := \begin{cases} \left(\frac{-3}{a}\right) & \text{if } 3 \nmid a, \\ \left(\frac{-3}{c}\right) & \text{if } 3 | a. \end{cases}$$

Then, assuming BSD, $|D|$ *is congruent iff*

$$\sum_{\substack{b^2-4ac=-3D \\ c>0>a \\ 32|a}} \chi(a,b,c) = \sum_{\substack{b^2-4ac=-3D \\ a+3b+9c>0>a \\ 32|a}} \chi(a,b,c).$$

Example

- Is 11 congruent? Check quadratic forms of discriminant 33.

Example

- Is 11 congruent? Check quadratic forms of discriminant 33.
- No forms on LHS, one form $(-32, 17, -2)$ on RHS, so LHS$= 0$, RHS$= \left(\frac{-3}{-32}\right) = 1$. Thus, 11 is **not** congruent.

Example

- Is 11 congruent? Check quadratic forms of discriminant 33.
- No forms on LHS, one form $(-32, 17, -2)$ on RHS, so LHS$= 0$, RHS$= \left(\frac{-3}{-32}\right) = 1$. Thus, 11 is **not** congruent.
- New proof of classical result: All primes $p \equiv 3 \pmod 8$ are not congruent.

Example

- Is 11 congruent? Check quadratic forms of discriminant 33.
- No forms on LHS, one form $(-32, 17, -2)$ on RHS, so LHS$=0$, RHS$=\left(\frac{-3}{-32}\right)=1$. Thus, 11 is **not** congruent.
- New proof of classical result: All primes $p \equiv 3 \pmod 8$ are not congruent.
- The involution $b \mapsto -b$ shows that the LHS is even, so enough to show that the number of QFs on the RHS is always *odd*.

Example

- Is 11 congruent? Check quadratic forms of discriminant 33.
- No forms on LHS, one form $(-32, 17, -2)$ on RHS, so LHS$= 0$, RHS$= \left(\frac{-3}{-32}\right) = 1$. Thus, 11 is **not** congruent.
- New proof of classical result: All primes $p \equiv 3 \pmod 8$ are not congruent.
- The involution $b \mapsto -b$ shows that the LHS is even, so enough to show that the number of QFs on the RHS is always *odd*.
- This was proven by Genz.

Behind the proofs

- Special functions introduced by Zagier:

$$f_{k,D}(\tau) := \sum_{b^2-4ac=D} (a\tau^2 + b\tau + c)^{-k} \in S_{2k}.$$

Behind the proofs

- Special functions introduced by Zagier:

$$f_{k,D}(\tau) := \sum_{b^2-4ac=D} (a\tau^2 + b\tau + c)^{-k} \in S_{2k}.$$

- Kohnen's more general functions ($k = 1$: need "Hecke trick"):

$$f_{k,N,D,D_0}(\tau) := \sum_{b^2-4ac=DD_0, N|a} \chi_{D_0}(a,b,c)(a\tau^2+b\tau+c)^{-k} \in S_{2k}(N).$$

Behind the proofs

- Special functions introduced by Zagier:

$$f_{k,D}(\tau) := \sum_{b^2-4ac=D} (a\tau^2 + b\tau + c)^{-k} \in S_{2k}.$$

- Kohnen's more general functions ($k = 1$: need "Hecke trick"):

$$f_{k,N,D,D_0}(\tau) := \sum_{b^2-4ac=DD_0, N|a} \chi_{D_0}(a,b,c)(a\tau^2+b\tau+c)^{-k} \in S_{2k}(N).$$

- We also need **cycle integrals** of modular forms (C_Q is a semicircle determined by Q):

$$r_{k,N}(f; D_0, |D|) := \sum_{[a,b,c]\in\Gamma_0(N)\backslash\mathcal{Q}_{DD_0},\ N|a} \chi_{D_0}(a,b,c) \times \int_{C_Q} f(\tau)(a\tau^2 + b\tau + c)^{k-1} d\tau.$$

Connection to L-values

Theorem (Kohnen)

If $f \in S_{2k}(N)$, under some conditions:

$$\langle f, f_{k,N,D,D_0} \rangle \doteq r_{k,N,D,D_0}(f).$$

Connection to L-values

Theorem (Kohnen)

If $f \in S_{2k}(N)$, under some conditions:

$$\langle f, f_{k,N,D,D_0} \rangle \doteq r_{k,N,D,D_0}(f).$$

Theorem (Kohnen)

If $f \in S_{2k}(N)$, under some conditions:

$$L(f \otimes \chi_D, k) \cdot L(f \otimes \chi_{D_0}, k)\rangle \doteq |r_{k,N,D,D_0}(f)|^2.$$

Connection to L-values

Theorem (Kohnen)

If $f \in S_{2k}(N)$, under some conditions:

$$\langle f, f_{k,N,D,D_0} \rangle \doteq r_{k,N,D,D_0}(f).$$

Theorem (Kohnen)

If $f \in S_{2k}(N)$, under some conditions:

$$L(f \otimes \chi_D, k) \cdot L(f \otimes \chi_{D_0}, k)\rangle \doteq |r_{k,N,D,D_0}(f)|^2.$$

- Thus, if $L(f \otimes \chi_{D_0}, k) \neq 0$, then

$$L(f \otimes \chi_D, k) = 0 \iff \langle f, f_{k,N,D,D_0} \rangle = 0.$$

Where discontinuities arise

Definition

A locally harmonic Maass form is a function $f : \mathbb{H} \to \mathbb{C}$ which

Where discontinuities arise

Definition

A locally harmonic Maass form is a function $f : \mathbb{H} \to \mathbb{C}$ which

1. Transforms with modular symmetry.

Where discontinuities arise

Definition

A locally harmonic Maass form is a function $f : \mathbb{H} \to \mathbb{C}$ which

1. Transforms with modular symmetry.
2. Satisfies a special second-order differential equation (is an eigenfunction of a Laplacian).

Where discontinuities arise

Definition

A locally harmonic Maass form is a function $f : \mathbb{H} \to \mathbb{C}$ which

1. Transforms with modular symmetry.
2. Satisfies a special second-order differential equation (is an eigenfunction of a Laplacian).
3. Has possible jump discontinuities along geodesics like C_Q for quadratic forms Q.

Where discontinuities arise

Definition

A locally harmonic Maass form is a function $f : \mathbb{H} \to \mathbb{C}$ which

1. Transforms with modular symmetry.
2. Satisfies a special second-order differential equation (is an eigenfunction of a Laplacian).
3. Has possible jump discontinuities along geodesics like C_Q for quadratic forms Q.
4. Has polynomial growth at cusps.

Where discontinuities arise

Definition

A locally harmonic Maass form is a function $f : \mathbb{H} \to \mathbb{C}$ which

1. Transforms with modular symmetry.
2. Satisfies a special second-order differential equation (is an eigenfunction of a Laplacian).
3. Has possible jump discontinuities along geodesics like C_Q for quadratic forms Q.
4. Has polynomial growth at cusps.

- By Stokes' Theorem, to compute $\langle f, f_{k,N,D,D_0} \rangle$, take a "lift" under operator $\xi_{2-k} := 2i\,\mathrm{Im}(\tau)^{2-k}\overline{\frac{\partial}{\partial \overline{\tau}}}$.

Where discontinuities arise

Definition

A locally harmonic Maass form is a function $f : \mathbb{H} \to \mathbb{C}$ which

1. Transforms with modular symmetry.
2. Satisfies a special second-order differential equation (is an eigenfunction of a Laplacian).
3. Has possible jump discontinuities along geodesics like C_Q for quadratic forms Q.
4. Has polynomial growth at cusps.

- By Stokes' Theorem, to compute $\langle f, f_{k,N,D,D_0} \rangle$, take a "lift" under operator $\xi_{2-k} := 2i\,\mathrm{Im}(\tau)^{2-k} \overline{\frac{\partial}{\partial \overline{\tau}}}$.
- The "natural" lift has discontinuities from local polynomials.

Modular local polynomials

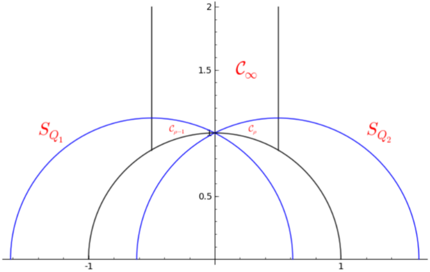
- Non-zero polynomials can't be modular forms.

Modular local polynomials

- Non-zero polynomials can't be modular forms.
- But **local polynomials** can be.

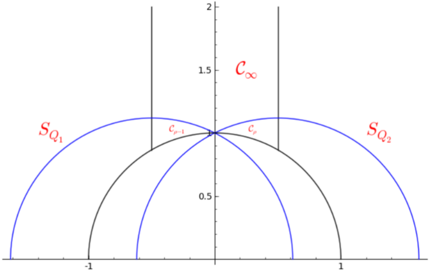
Modular local polynomials

- Non-zero polynomials can't be modular forms.
- But **local polynomials** can be.
- For example, in the "discriminant 5 case":



Modular local polynomials

- Non-zero polynomials can't be modular forms.
- But **local polynomials** can be.
- For example, in the "discriminant 5 case":



- The modular forms of weight -2 which are locally polynomial with "jumps" across the blue semicircles are ($\alpha, \beta \in \mathbb{C}$):

$$\begin{cases} \alpha & \text{if } \tau \in \mathcal{C}_\infty, \\ \beta\left(\tau^2 - \tau + 1\right) & \text{if } \tau \in \mathcal{C}_\rho, \\ \beta\left(\tau^2 + \tau + 1\right) & \text{if } \tau \in \mathcal{C}_{\rho-1}. \end{cases}$$

Thank You!

Thank you!