The Congruent Number Problem

Holly Green

University of Bristol

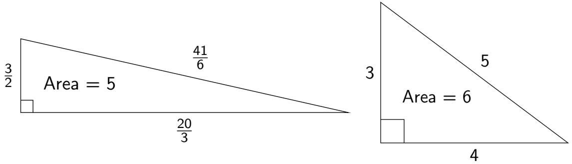
January 24th, 2024

The Congruent Number Problem

Which integers are the area of a right-angled triangle with sides of rational length?

$n \in \mathbb{N}$ is a *congruent number* if there exist $a, b, c \in \mathbb{Q}$ with

$$a^2 + b^2 = c^2 \quad \text{and} \quad \tfrac{1}{2}ab = n.$$



Let $n \in \mathbb{N}$ be square-free, $E_n : y^2 = x^3 - n^2 x$.

$$\left\{(a,b,c) \in \mathbb{Q}^3 \,\middle|\, a^2 + b^2 = c^2,\ \tfrac{1}{2}ab = n\right\} \overset{\text{1-to-1}}{\longleftrightarrow} \left\{(x,y) \in E_n(\mathbb{Q}) \,\middle|\, y \neq 0\right\}$$

$$(a,b,c) \longmapsto \big(nb/(c-a), 2n^2/(c-a)\big)$$

$$\big((x^2 - n^2)/y, 2nx/y, (x^2 + n^2)/y\big) \longleftarrow (x,y)$$

n is a congruent number $\iff \exists (x,y) \in E_n(\mathbb{Q}),\ y \neq 0 \iff \operatorname{rank}(E_n) \geq 1 \overset{\text{BSD}}{\iff} L(E_n, 1) = 0.$

⌂ → Elliptic curves → $\mathbb{Q}$ → 800 → d → 3

Citation · Feedback · Hide Menu

Elliptic curve with LMFDB label 800.d3 (Cremona label 800a1)

Introduction
Overview Random
Universe Knowledge

L-functions
Rational All

Modular forms
Classical Maass
Hilbert Bianchi

Varieties
Elliptic curves over $\mathbb{Q}$
Elliptic curves over $\mathbb{Q}(\alpha)$
Genus 2 curves over $\mathbb{Q}$
Higher genus families
Abelian varieties over $\mathbb{F}_q$

Fields

Minimal Weierstrass equation

Show commands: Magma / Oscar / PariGP / SageMath

$y^2 = x^3 - 25x$ (homogenize, simplify)

Mordell-Weil group structure

$\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

Infinite order Mordell-Weil generator and height

$P = (-4, 6)$
$\hat{h}(P) \approx 1.8994821725317955901072055096$

Torsion generators

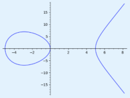
$(0,0)$, $(5,0)$

Integral points

$(-5,0)$, $(-4,\pm 6)$, $(0,0)$, $(5,0)$, $(45,\pm 300)$

Properties

Label	800.d3



Conductor	800
Discriminant	1000000
j-invariant	1728
CM	yes ($D = -4$)
Rank	1
Torsion structure	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

Related objects
Isogeny class 800.d
Minimal quadratic twist 32.a3

The Parity Conjecture

Let $E/\mathbb{Q}$ be an elliptic curve. Then

$$(-1)^{\mathrm{rank}(E)} = w(E).$$

When $E_n : y^2 = x^3 - n^2 x$,

$$w(E_n) = \begin{cases} +1 & n \equiv 1, 2 \text{ or } 3 \pmod 8, \\ -1 & n \equiv 5, 6 \text{ or } 7 \pmod 8. \end{cases}$$

Corollary

Assuming the Parity Conjecture, n is a congruent number whenever $n \equiv 5, 6$ or $7 \pmod 8$.

Unconditional results:

- primes $p \equiv 5, 7 \pmod 8$ are congruent numbers, (Heegner)
- primes $p \equiv 3 \pmod 8$ are not congruent numbers, (Nagell)
- $\geq 55.9\%$ of square-free $n \equiv 5, 6$ or $7 \pmod 8$ are congruent numbers. (Smith)

Thank you for listening!

Question

Is 52 a congruent number?