RIGHT TRIANGLES AND ELLIPTIC CURVES

KARL RUBIN

1. Introduction

In this lecture we would like to study, and answer as best we can, the following question.

Question. *Suppose we are given a natural number d. Is there a right triangle with three rational sides and area equal to d?*

We will write $\mathbf{Z}$ for the set of integers $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$, $\mathbf{Z}^+$ for the natural numbers (or positive integers) $\{1, 2, 3, \dots\}$, and $\mathbf{Q}$ for the set of rational numbers (fractions) $\{a/b : a, b \in \mathbf{Z}, b \neq 0\}$.

The Pythagorean Theorem says that a triangle with sides $a < b < c$ is a right triangle if and only if $a^2 + b^2 = c^2$. If it is a right triangle, then its area is $ab/2$. Thus we can rephrase our question as follows.

Question (restated)**.** *Suppose $d \in \mathbf{Z}^+$. Are there rational numbers $a, b, c > 0$ such that $a^2 + b^2 = c^2$ and $ab = 2d$?*

If the answer to this question is "yes", then d is called a *congruent number* (not to be confused with the notion of "congruence modulo an integer", which is different).

Table 1 gives some examples.

d	a	b	c
5	3/2	20/3	41/6
6	3	4	5
7	35/12	24/5	337/60

Table 1. Rational right triangles with area $5, 6, 7$

On the other hand, around 1640 Fermat proved that $d = 1$ is *not* a congruent number. That is, there is no right triangle with rational sides and area equal to 1. (Of course, this is true only because we insist that all three sides of the triangle are rational. The triangle with sides $1, 1, \sqrt{2}$ is a right triangle with area 1, but $\sqrt{2}$ is not a rational number.)

Note that to prove that a number d *is* congruent, one just has to produce the three rational numbers a, b, c. On the other hand, it is not at all obvious how to prove that a given d is *not* a congruent number.

Here is the best answer to our question that current mathematics can provide. It is easy to see that if d and t are natural numbers, than d is a congruent number if and only if dt^2 is a congruent number (just scale the right triangle by t). Thus it is

Partially supported by NSF grant DMS-9800881.

enough to answer our question for *squarefree* natural numbers d, those not divisible by a perfect square other than 1.

Theorem 1.1. *Suppose d is a squarefree natural number, and define*

$$a = \begin{cases} 1 & \text{if } d \text{ is odd} \\ 2 & \text{if } d \text{ is even,} \end{cases}$$
$$n = \#\{(x,y,z) \in \mathbf{Z}^3 : x^2 + 2ay^2 + 8z^2 = d/a\},$$
$$m = \#\{(x,y,z) \in \mathbf{Z}^3 : x^2 + 2ay^2 + 32z^2 = d/a\}.$$

If $n \neq 2m$, then d is not *a congruent number.*

Conjecture 1.2. *Suppose d is a squarefree natural number, and let a, n, and m be as in Theorem 1.1. If $n = 2m$, then d* is *a congruent number.*

(A *conjecture* is a statement which is believed to be true, but which nobody has been able to prove.)

Given d (not too large), it is easy to compute the integers n and m. Table 2 gives some examples. (Note that n and m are counting solutions (x,y,x) where x, y, and z are arbitrary integers, positive, negative, or zero). The last three columns

d	1	2	3	5	6	7	10	11	34	$8k$+5	$8k$+6	$8k$+7
n	2	2	4	0	0	0	4	12	8	0	0	0
m	2	2	4	0	0	0	4	2	4	0	0	0

TABLE 2. Some values of n and m in Theorem 1.1

of Table 2 reflect the fact that $x^2 + 2y^2$ can never leave a remainder of 5, or 7 when divided by 8, and $x^2 + 4y^2$ can never leave a remainder of 3 when divided by 8. Thus if d is 5, 6, or 7 more than a multiple of 8 then $n = m = 0$.

Exercise 1. Check the values of n and m in Table 2, and compute n and m for some other d.

It follows from Theorem 1.1 and Table 2 that 1, 2, 3, 10, and 11 are not congruent numbers. By Conjecture 1.2 and Table 2, then integer 34 and every integer which is 5, 6, or 7 more than a multiple of 8 *should be* congruent numbers. For $d = 5, 6$ or 7 we know this to be true, thanks to the examples in Table 1.

Exercise 2. Show that 34 is a congruent number by finding a rational right triangle of area 34.

Thanks to Theorem 1.1, it is now easy to show that d is *not* a congruent number. But it can be difficult to show that d *is* a congruent number, when Conjecture 1.2 predicts it to be. For example, Conjecture 1.2 predicts that $d = 157 = 19 \cdot 8 + 5$ is a congruent number, but the simplest rational right triangle with area 157 has sides

$$\frac{6803298487826435051217540}{411340519227716149383203}, \frac{411340519227716149383203}{21666555693714761309610},$$
$$\frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830},$$

(see [5], p. 5). Similarly $d = 1063 = 132 \cdot 8 + 7$ is a congruent number, but the simplest rational right triangle with area 1063 has shortest side a where the numerator of a has 104 digits and the denominator has 103 digits ([4][1]).

2. Translating the question

In the rest of this lecture we will explain where Theorem 1.1 and Conjecture 1.2 come from. The first step is to restate our question in a different form.

Exercise 3. Show that if a, b, c are the sides of a rational right triangle with area d, then

$$x = \frac{a-c}{b}, \quad y = \frac{2(a-c)}{b^2}$$

are nonzero rational numbers satisfying the equation $dy^2 = x^3 - x$.

Exercise 4. Conversely, if x and y are rational numbers satisfying the equation $dy^2 = x^3 - x$ and $y \neq 0$, then

$$\left|\frac{x^2-1}{y}\right|, \quad \left|\frac{2x}{y}\right|, \quad \left|\frac{x^2+1}{y}\right|$$

are the sides of a rational right triangle with area d.

Note that the equation

$$dy^2 = x^3 - x \tag{1}$$

has three solutions $(0,0)$, $(1,0)$, and $(-1,0)$ with $y = 0$. We will call these the *trivial* solutions, and we will call a solution of (1) *nontrivial* if $y \neq 0$. Combining the two exercises above gives the following reformulation of the definition of congruent number.

Proposition 2.1. *A squarefree natural number d is congruent if and only if the equation $dy^2 = x^3 - x$ has a nontrivial rational solution (x, y).*

3. Elliptic curves

Fix a squarefree natural number d. The equation

$$dy^2 = x^3 - x \tag{2}$$

defines an *elliptic curve*.[2] We will call this elliptic curve E_d, and by a rational point on E_d we will mean a pair of rational numbers (x, y) satisfying (2). For more about elliptic curves see [5], [6], [7]. We will continue our investigation of the congruent number problem by applying results from the general theory of elliptic curves. The most important of these is the following process for using two points on E_d to construct a third point.

Suppose that P and Q are two points on E_d.

- Draw the line through P and Q.

[1] There is an error in [4]; on page 130 the expression before the displayed value of X should read $X^2/1063$.

[2] One usually requires an elliptic curve to be a curve given by an equation $y^2 = x^3 + Ax + B$. Under the change of variables $(x, y) \mapsto (x/d, y/d^2)$ our elliptic curve is equivalent to $y^2 = x^3 - d^2x$.

- In general this line will intersect the curve E_d in three points (because the equation (2) has degree 3). Two of these points are P and Q; call the third point R. Since P and Q are rational points, R will be a rational point as well.

We also want to apply this construction when $P = Q$. In that case by "line through P and Q" we mean the tangent line to the curve E_d at P (the limiting line as Q approaches P on E_d).

Exercise 5. If $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ with $x_1 \neq x_2$, check that

$$R = \left(d\frac{(y_2 - y_1)^2}{(x_2 - x_1)^2} - x_1 - x_2, d\frac{(y_2 - y_1)^3}{(x_2 - x_1)^3} + \frac{x_1y_1 - x_2y_2 + 2(x_2y_1 - x_1y_2)}{x_2 - x_1} \right).$$

If $P = Q = (x, y)$, check that

$$R = \left(\frac{(x^2+1)^2}{4x(x^2-1)}, -\frac{x^6 - 5x^4 - 5x^2 + 1}{8d^3y^3} \right).$$

For example, if $P = (-1, 0)$ and $Q = (0, 0)$, then $R = (1, 0)$.

It is not obvious, but one can use this construction to prove the following theorem.

Theorem 3.1. *If the elliptic curve E_d has a nontrivial rational point (i.e., a rational point with $y \neq 0$), then it has infinitely many rational points.*

Figure 1 shows some of the rational points on E_6, which can be found by starting with $(-\frac{1}{2}, \frac{1}{4})$ and using the construction above.

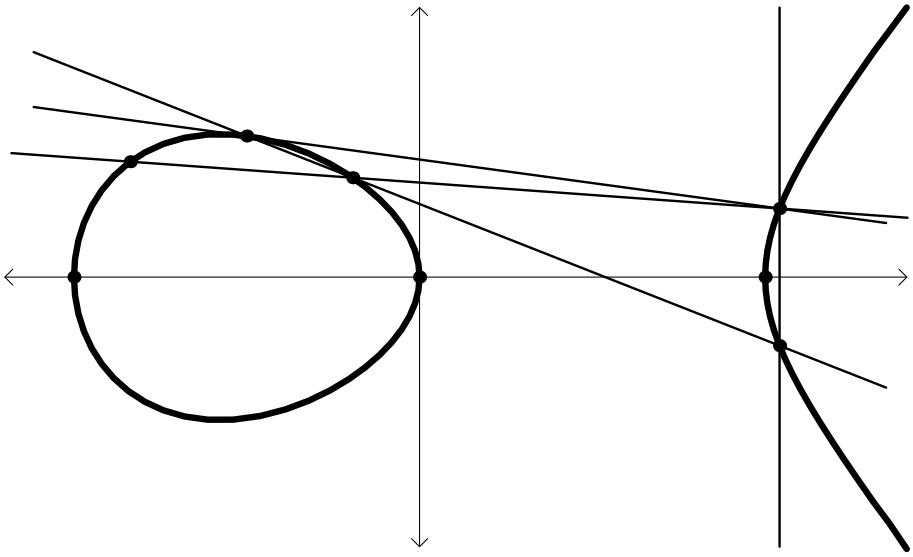

FIGURE 1. Some rational points on $6y^2 = x^3 - x$.

Using Exercise 4 and Proposition 2.1 this leads to the following corollaries.

Corollary 3.2. *If there is a rational right triangle with area d, then there are infinitely many rational right triangles with area d.*

Corollary 3.3. *A squarefree natural number d is congruent if and only if E_d has infinitely many rational points.*

Table 3 lists the shortest side of some rational right triangles with area 6. (If we call the short side a, then $b = 12/a$ and $c = \sqrt{a^2 + b^2}$ are the other two sides.) These were computed using the formulas of Exercises 4 and 5. Note the parabolic shape of the table.

$$3$$
$$\frac{7}{10}$$
$$\frac{3404}{1551}$$
$$\frac{2017680}{1437599}$$
$$\frac{3122541453}{2129555051}$$
$$\frac{43690772126393}{20528380655970}$$
$$\frac{3538478409041570404}{4644050785034096801}$$
$$\frac{12149807353008887088572640}{4156118808548967941769601}$$
$$\frac{562877367535365225251484084003}{909680258103070108113578792100 1}$$
$$\frac{9803605963104930848577505409137622406 00}{3184972098290942067271241688154609008 07}$$
$$\frac{1819157495197128710444993870521048471797359 8996}{2850984812127142751980727458173233067600976 0751}$$
$$\frac{2192913891960404693804016374075761895352212727 5858567818399}{9695960103990294331025984943841149560825669775138168420}$$
$$\frac{1076784912325042146290273662036091437066100455618812531478882273 47}{8030478905811822907573657897672805962703965798196446193362294285 1}$$
$$\frac{6386862753666818897897886697308412979750707771606181541981220408008859007160}{4176501831301593836542885342768698632287714214832228338980765292538706358393}$$

TABLE 3. The shortest side of some right triangles with area 6

4. Counting points modulo p

Thanks to Corollary 3.3, we can solve the congruent number problem if we can find a way to decide whether a given elliptic curve E_d has infinitely many rational points, or only the three trivial rational points $\{(-1,0),(0,0),(1,0)\}$. There is currently no known way to do this in general, but we will be able to make a good start and decide in many cases.

Instead of asking the difficult question "how often is $dy^2-(x^3-x)$ equal to zero?", we will ask, for each prime number p, "how often is $dy^2 - (x^3 - x)$ a multiple of p?" (of course when it is zero, it is a multiple of p for every p).

More precisely, for every prime number p define an integer

$$N_p(d) = \#\{(x,y) : 0 \le x, y < p, dy^2 - (x^3 - x) \text{ is a multiple of } p\} + 1.$$

For example, when $d = 1$ we have $N_5(1) = 8$ because the 7 points

$$\{(0,0),(1,0),(2,1),(2,4),(3,2),(3,3),(4,0)\}$$

all have the property that $dy^2 - (x^3 - x)$ is a multiple of 5, and no other pairs in the appropriate range have this property. Table 4 lists the values of $N_p(d)$ for some primes p, and certain d.

Exercise 6. Check some of the values in Table 4.

		p								
		5	7	11	13	17	19	1000003	1000033	1000037
	1	8	8	12	8	16	20	1000004	998208	998056
d	2	4	8	12	20	16	20	1000004	998208	1002020
	3	4	8	12	8	20	20	1000004	998208	1002020

TABLE 4. Some values of $N_p(d)$

Idea (Birch and Swinnerton-Dyer [1])**.** *Suppose d is a squarefree positive integer. The more rational points E_d has, the larger the $N_p(d)$ will be "on average", as p varies.*

To make sense of this, we need to measure the "average" size of the $N_p(d)$ as p varies. Birch and Swinnerton-Dyer first computed

$$\pi_d(X) = \prod_{p<X} \frac{N_p(d)}{p}.$$

Figure 2 shows the function $\pi_d(X)$ for $d = 1, 2, 3, 5, 6, 7$, with X plotted on a logarithmic scale. As the idea of Birch and Swinnerton-Dyer suggests, $\pi_d(X)$ is larger

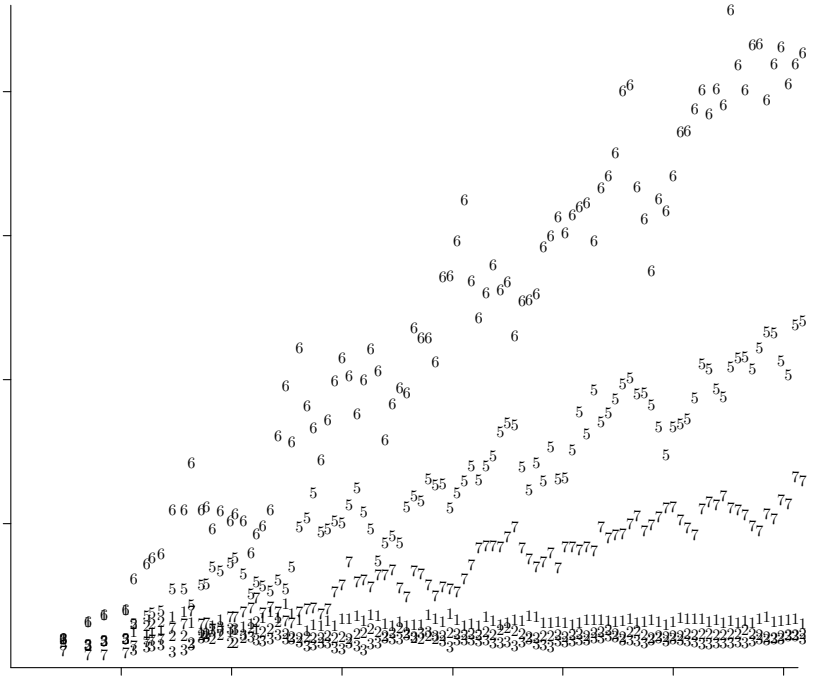

FIGURE 2. Plot of $\pi_d(X)$ as a function of X, for $d = 1, 2, 3, 5, 6, 7$.

for the three congruent numbers $d = 5, 6, 7$ than for the non-congruent numbers $d = 1, 2, 3$.

Birch and Swinnerton-Dyer observed that there is a better way to measure the average size of the $N_p(d)$. Hasse defined a function of a complex variable attached

to E_d, called the L-function of E_d, by

$$L(E_d, s) = \prod_{p \nmid 2d} (1 - (p + 1 - N_p(d))p^{-s} + p^{1-2s})^{-1}. \tag{3}$$

This infinite product converges if the real part $\mathrm{Re}(s)$ of the complex number s is bigger than $3/2$, and there is a natural way to extend the function $L(E_d, s)$ to all complex numbers s (called the analytic continuation: the only function defined by a convergent power series in s which agrees with $L(E_d, s)$ when $\mathrm{Re}(s) > 3/2$).

Note that *formally*, if we put $s = 1$ in the infinite product (3) we get $\prod_{p \nmid 2d} \frac{p}{N_p(d)}$, which is essentially the limit of the values $\pi_d(X)^{-1}$, if that limit exists. This doesn't *prove* a connection between $L(E_d, 1)$ and the $\pi_d(X)$, because the product (3) need not converge at $s = 1$, but it led Birch and Swinnerton-Dyer to the following conjecture.

Conjecture 4.1 (Birch and Swinnerton-Dyer)**.** *The elliptic curve E_d has infinitely many rational points if and only if $L(E_d, 1) = 0$.*

Equivalently (by Corollary 3.3), the Birch and Swinnerton-Dyer conjecture predicts that d is a congruent number if and only if $L(E_d, 1) = 0$.

Theorem 4.2 (Coates and Wiles [3])**.** *If E_d has infinitely many rational points, then $L(E_d, 1) = 0$.*

Unfortunately it is still an open problem to prove the converse (that if $L(E_d, 1) = 0$ then E_d has infinitely many rational points).

We next need a good way to evaluate $L(E_d, 1)$. This is provided by the following theorem.

Theorem 4.3 (Tunnell [8])**.** *If d is a squarefree positive integer, then*

$$L(E_d, 1) = \frac{(n - 2m)^2 a \Omega}{16\sqrt{d}}$$

where

$$\begin{aligned} &a = 1 \text{ if } d \text{ is odd, } a = 2 \text{ if } d \text{ is even,} \\ &n = \#\{(x, y, z) \in \mathbf{Z}^3 : x^2 + 2ay^2 + 8z^2 = d/a\}, \\ &m = \#\{(x, y, z) \in \mathbf{Z}^3 : x^2 + 2ay^2 + 32z^2 = d/a\}, \\ &\Omega = \int_1^\infty \frac{dx}{\sqrt{x^3 - x}} \approx 2.6220575542921198\ldots \end{aligned}$$

In particular

$$L(E_d, 1) = 0 \iff n = 2m.$$

Exercise 7. Show that Theorem 4.3, Theorem 4.2, and Corollary 3.3 together imply Theorem 1.1. Show that Theorem 4.3, Conjecture 4.1, and Corollary 3.3 together imply Conjecture 1.2.

References

[1] B. Birch, H. P. F. Swinnerton-Dyer, *Notes on elliptic curves. I*, J. Reine Angew. Math. **212** (1963), 7–25.

[2] ———, *Notes on elliptic curves. II*, J. Reine Angew. Math. **218** (1965), 79–108.

[3] J. Coates, A. Wiles, On the conjecture of Birch and Swinnerton-Dyer, *Inventiones math.* **39** (1977) 223–251.

[4] N. Elkies, Heegner point computations. In: Algorithmic Number Theory (ANTS-I) 1994, Adleman and Huang, eds., *Lect. notes in Comp. Sci.* **877** (1994) 122–133; see also `http://www.math.harvard.edu/~elkies/compnt.html`.
[5] N. Koblitz, Introduction to elliptic curves and modular forms, Graduate Texts in Mathematics **97**, Springer-Verlag, New York, 1993.
[6] J. H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Mathematics **106**, Springer-Verlag, New York, 1986.
[7] J. H. Silverman, J. Tate, Rational points on elliptic curves, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.
[8] J. B. Tunnell, *A classical Diophantine problem and modular forms of weight* 3/2, Invent. Math. **72** (1983), no. 2, 323–334.

Department of Mathematics, Stanford University, Stanford, CA 94305, USA
`http://www.math.stanford.edu/~rubin`
E-mail address: `rubin@math.stanford.edu`