In this talk we will take some old geometric problems as cues to discuss various recent number-theoretic results and questions, mainly (but not only) related to the theory of elliptic curves. Many results will not be proven, as this is intended to be more of an expository talk. Nonetheless, we will mention examples and recent advances.

1 The congruent number problem

It all starts from the following quite simple question: can a (squarefree) natural number $n$ be the area of a right-angled triangle with rational sides?

**Definition 1.** We say that $n$ is a congruent number if there exists rational numbers $X, Y, Z \in \mathbb{Q}$ such that

$$X^2 + Y^2 = Z^2, \quad XY = 2n.$$ 

Amazingly, this question is still an open problem, in the following sense: there is no known algorithm to determine if a given squarefree integer $n$ is a congruent number.

**Example 1.** 5 is a congruent number: the rational right-angled triangle has sides $\frac{3}{2}, \frac{20}{3}$ and $\frac{41}{6}$. Similarly, 17 is a congruent number (sides $\frac{225}{30}, \frac{272}{30}, \frac{353}{30}$).

Notice that $n$ is a congruent number if and only if there exists a 3-terms arithmetic progression of rational squares $\alpha^2, \beta^2, \gamma^2$ with difference $n$. In fact, given the triangle of sides $X, Y, Z$ we set

$$\alpha = \frac{Y - X}{2}, \quad \beta = \frac{Z}{2}, \quad \gamma = \frac{Y + X}{2},$$

and the inverse transformation will give $X, Y, Z$ in terms of $\alpha, \beta, \gamma$. This gives an equivalent formulation of our problem.

**Example 2.** 1 is not a congruent number: this is a nontrivial result due to Fermat. Notice that with a little manipulation this implies that there are no rational solutions to $a^4 + b^4 = 1$, which may have prompted Fermat to conjecture his famous Last Theorem.

Now let’s give a few results about prime congruent numbers:

**Theorem 1** (Genocchi 1874, Razar 1974). A prime $p$ with $p \equiv 3 \mod 8$ is not congruent. If $p$ is a prime with $p \equiv 5 \mod 8$ then $2p$ is not congruent.
Theorem 2 (Heegner 1952, Bitch-Stephens 1975, Monsky 1990). A prime $p$ with $p \equiv 5 \mod 8$ or $p \equiv 7 \mod 8$ is congruent. If $p$ is a prime with $p \equiv 3 \mod 4$ then $2p$ is congruent.

This settles the cases for $p$ and $2p$, except when $p \equiv 1 \mod 8$.

We also have infinitude results:

Theorem 3 (various 1985-2012). For any positive integer $k$, there are infinitely many congruent numbers $n$ with exactly $k$ odd prime factors.

It is now time to introduce a more number-theoretic object to deal with:

Definition 2. An elliptic curve $E$ is a smooth, projective algebraic curve of genus one, on which there is a specified point $O$.

In fact, any elliptic curve can be written as a plane algebraic curve defined by an equation of the form

$$y^2 = x^3 + ax + b$$

with $a, b$ in some coefficient field satisfying the nonzero discriminant condition

$$\Delta = -16(4a^3 + 27b^2) \neq 0.$$  

What’s really astonishing about elliptic curves is that

Theorem 4. Consider the elliptic curve $E \subset \mathbb{P}^2$. Then there is an abelian group law on $E$. Moreover, if the equation defining $E$ has coefficients in a field $K$, then $E(K)$ is a subgroup of $E$ according to this group rule.

[It’d be nice to have a picture here]

The most natural field of definition of an elliptic curve for us number-theorists is $\mathbb{Q}$, or a number field $K$. In both cases, we have the following important theorem

Theorem 5 (Mordell-Weil). Suppose $E$ is defined over a number field $K$. Then $E(K)$ is a finitely generated abelian group.

Then, by the structure theorem for abelian groups, one has that

$$E(K) \cong \mathbb{Z}^r \oplus E(K)_{\text{tors}}$$

where $r$ is the rank of the group $E(K)$ and $E(K)_{\text{tors}}$ its torsion subgroup.

Remark. In the case $K = \mathbb{Q}$, the theorem was proved by Mordell alone in 1922.

Theorem 6 (Mazur, 1978). The torsion subgroup has one of the following forms:

$$\mathbb{Z}/n\mathbb{Z} \text{ for } 1 \leq n \leq 12$$

or

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \text{ for } n \in \{2, 4, 6, 8\}.$$  

Theorem 7 (Siegel). The set of integral points of an elliptic curve $E$ defined over $\mathbb{Q}$, i.e. the set of points $(x, y) \in \mathbb{Z}^2$ which belongs to the elliptic curve, is a finite set.

We mention the following important results which will be used later.
Theorem 8. Let $E$ be an elliptic curve defined over $\mathbb{Z}$, and $p$ a prime not dividing the discriminant $\Delta$ of $E$. Then $E$ has good reduction modulo $p$, which means that $E(\mathbb{F}_p)$ is still an elliptic curve. Moreover, we have an injection of the $p$-torsion into the $\mathbb{F}_p$-points:

$$E(\mathbb{Q})[p] \hookrightarrow E(\mathbb{F}_p).$$

Example 3. The previous theorem is a basic tool in the computation of torsion subgroups of elliptic curves. Consider for instance $E; y^2 = x^3 + x$. By the geometric picture, it is clear that $(0, 0)$ is the only 2-torsion point, so the torsion subgroup contains $\{\infty, (0, 0)\}$.

Now the discriminant is $\Delta = -64$, so for any odd prime $p$, we have $E(\mathbb{Q})[p] \hookrightarrow E(\mathbb{F}_p)$. By manually solving the diophantine equations on finite fields, we calculate

$$E(\mathbb{F}_3) = \{\infty, (0, 0), (2, 1), (2, 2)\} \cong \mathbb{Z}/4\mathbb{Z}$$

and

$$E(\mathbb{F}_5) = \{\infty, (0, 0), (2, 0), (3, 0)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

but as the torsion subgroup should embed in both, we get

$$E(\mathbb{Q})_{tors} = \mathbb{Z}/2\mathbb{Z} = \{\infty, (0, 0)\}.$$

Let’s come back to our original congruent number problem. We introduced elliptic curves because of the following useful characterization. Define

$$C_n := \{y^2 = x^3 - n^2x\}.$$

Theorem 9. Let $n$ be a squarefree positive integer. TFAE

1. $n$ is a congruent number;
2. $C_n$ has a rational point $(x, y)$ with $y \neq 0$;
3. $C_n$ has infinitely many rational points;
4. the Mordell-Weil group $C_n(\mathbb{Q})$ has rank $r \geq 1$.

Proof. (1) $\Rightarrow$ (2) Suppose $n$ is a congruent number, so there’s a right-angled triangle with sides $X, Y, Z$ such that $X^2 + Y^2 = Z^2$ and $XY = 2n$. The point we want is

$$x = \left(\frac{Z}{2}\right)^2, \quad y = \frac{Z(X-Y)(X+Y)}{8}.$$

(2) $\Rightarrow$ (3) We rely on theorem 8. For any prime $p$ not dividing $2n$ we have

$$C_n(\mathbb{Q})[p] \hookrightarrow C_n(\mathbb{F}_p)$$

and as the group on the right has order $p+1$ for all primes $p \equiv 3(\text{mod}4)$, we obtain that the only torsion is 2-torsion, which means that every torsion point has $y = 0$ if we write explicitly the composition law. Hence a rational point with nonzero $y$ means that the rank is at least 1, which in particular proves (3). (3) $\Rightarrow$ (4) is the Mordell theorem. (4) $\Rightarrow$ (1). Given a rational point $(x, y)$ with $y \neq 0$, take the triangle with sides

$$X = \left\lfloor \frac{(x+n)(y-n)}{y} \right\rfloor, \quad Y = 2n \left\lfloor \frac{x}{y} \right\rfloor, \quad Z = \left\lfloor \frac{x^2+n^2}{y} \right\rfloor.$$
So the question now is: how do we calculate the rank of an elliptic curve? Or at least, how do we show that this rank is at least one? Not surprisingly (given the above theorem), this is also an open problem. There are partial results about ranks of special families of elliptic curves, and techniques that work for some particular families, but no general result.

**Theorem 10** (Nagell, 1929). For $n = p$ a prime number congruent to $3 \mod 8$, the rank is zero. The same method works for $1, 2$ and all $n = 2p$ for $p \equiv 5 \mod 8$.

In general, most partial results about congruent numbers come exactly from estimating the rank of $C_n$.

**Example 4.** Nemenzo calculated all $n < 42553$ for which $C_n(\mathbb{Q})$ is infinite, so we know all the congruent numbers up to this bound. Elkies verified that for all natural numbers $n < 10^6$ that are congruent to $5, 6, 7 \mod 8$, the group $C_n(\mathbb{Q})$ has positive rank.

Now let’s try to develop a more general method. We can attach to $C_n$ the following analytic object, called the $L$-function (or $L$-series) for $C_n$ over $\mathbb{Q}$:

$$L(C_n, s) := \prod_{(p, 2n) = 1} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1}$$

where

$$a_p = p + 1 - |C_n(\mathbb{F}_p)|,$$

when we denote by $|C_n(\mathbb{F}_p)|$ the number of ‘solutions’ of $C_n$ modulo $p$ (i.e. points of $C_n$ in $\mathbb{F}_p$).

**Proposition 11.** This $L$-series is a complex function converging absolutely, uniformly for $\Re s > \frac{3}{2}$.

But in fact we have stronger results!

**Theorem 12.** $L(C_n, s)$ has an analytic continuation to an entire function on the whole complex plane. Moreover, it satisfies the following functional equation: define

$$\Lambda(s) = \left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma(s) L(C_n, s)$$

where $N$ equals $32n^2$ if $n$ is odd, and $16n^2$ if $n$ is even. Then

$$\Lambda(s) = \pm \Lambda(2 - s)$$

with the following sign condition

+ if $n \equiv 1, 2, 3 \mod 8$  
  - if $n \equiv 5, 6, 7 \mod 8$.

We finally get to one of the most intriguing questions of modern number theory.

**Conjecture 1** (Birch, Swinnerton-Dyer, 1965, weak form). The expansion of $L(E, s)$ near $s = 1$ has the form

$$L(E, s) = c(s - 1)^r + \text{higher order terms}$$

with $c \neq 0$ and $r$ the rank of the elliptic curve.

In particular, $L(E, 1) \neq 0$ if and only if $E(\mathbb{Q})$ is finite.
Remark. This conjecture is amazing! We relate an algebro-geometric property of the elliptic curve, the 'size' of the group of its rational points, to the analytic property of an object defined just by looking at 'modulo p' points.

This is the very celebrated BSD conjecture. It is still open, and one of the Millenium problems worth a million dollars.

**Theorem 13** (Many). The conjecture holds for an elliptic curve $E$ defined over $\mathbb{Q}$ if $L(E, s)$ vanishes of order at most 1 near $s = 1$.

**Theorem 14** (Many). A positive proportion of elliptic curves defined over $\mathbb{Q}$ have analytic rank 0 and hence satisfies the BSD conjecture.

The big fact is that the BSD conjecture solves a huge part of our congruent number problem!

**Theorem 15.** Assuming BSD, $n$ is congruent if $n \equiv 5, 6, 7 \mod 8$.

**Proof.** The functional equation above tells us that the order of vanishing of $L(C_n, s)$ at $s = 1$ is odd in that case. Hence $r$ is odd, thus at least 1. $\square$

This method does not solve the problem in every case, but we have a full resolution (conditional on the BSD conjecture) using the following theorem.

**Theorem 16** (Tunnell, 1983). Let $n$ be a squarefree positive integer, and define

\[
A_n = |\{(x, y, z) \in \mathbb{Z}^3 | n = 2x^2 + y^2 + 32z^2\}|
\]

\[
B_n = |\{(x, y, z) \in \mathbb{Z}^3 | n = 2x^2 + y^2 + 8z^2\}|
\]

\[
C_n = |\{(x, y, z) \in \mathbb{Z}^3 | n = 8x^2 + 2y^2 + 64z^2\}|
\]

\[
D_n = |\{(x, y, z) \in \mathbb{Z}^3 | n = 8x^2 + 2y^2 + 16z^2\}|
\]

Suppose $n$ is a congruent number. If $n$ is odd, then $2A_n = B_n$, while if $n$ is even, then $2C_n = D_n$. Vice versa, if BSD holds for $C_n$, then these conditions are sufficient to determine whether $n$ is a congruent number.

**Remark.** This is quite useful, as we can do a brute-force search for solutions of the quadratic forms in the range $[0, \sqrt{n}]^3$.

## 2 Generalization of the congruent number problem

We can parametrize the previous problem to get a more generic question, for example by relaxing the condition of our triangle being right-angled:

**Definition 3** ($t$-congruent number problem). Let $t \in \mathbb{Q}$ be positive. An integer $n$ is called a $t$-congruent number if there exist rational numbers $a, b, c$ such that

\[
a^2 = b^2 + c^2 - 2bc \frac{t^2 - 1}{t^2 + 1}, \quad 2n = bc \frac{2t}{t^2 + 1}.
\]

This is equivalent to the following geometric formulation: denoting by $\theta$ the angle between the sides measuring $b$ and $c$, we have

\[
\sin \theta = \frac{2t}{t^2 + 1}, \quad \cos \theta = \frac{t^2 - 1}{t^2 + 1}.
\]
Clearly the case \( t = 1 \) corresponds to the classical congruent number problem.

**Proposition 17.** Let \( t > 0 \) be rational and \( n \in \mathbb{N} \). TFAE

1. \( n \) is a \( t \)-congruent number;
2. Either both \( \frac{n}{t} \) and \( t^2 + 1 \) are perfect rational squares, or the elliptic curve

\[
C_{n,t} : y^2 = x \left( x - \frac{n}{t} \right) (x + nt)
\]

has a rational point \((x, y)\) with nonzero \( y \).

**Proof.** Suppose \( n \) is a \( t \)-congruent number, for a triangle with rational sides \( a, b, c \). Then take

\[
(x, y) = \left( \frac{a^2}{4}, \frac{ab^2 - ac^2}{8} \right)
\]

which turns out to be a rational point on \( C_{n,t}(\mathbb{Q}) \). Either \( y \neq 0 \) or \( b = c \). The latter case implies (check!) that

\[
\frac{n}{t} = \left( \frac{a}{2} \right)^2, \quad t^2 + 1 = \left( \frac{2b}{a} \right)^2.
\]

Vice versa, suppose first that \( \frac{n}{t} \) and \( t^2 + 1 \) are perfect rational squares. Then taking

\[
a = 2\sqrt{\frac{n}{t}}, \quad b = c = \sqrt{\frac{n(t^2 + 1)}{t}}
\]

give a triangle which makes \( n \) a \( t \)-congruent number. Otherwise, if \((x, y)\) is a rational point with \( y \neq 0 \), take

\[
a = \left| \frac{x^2 + n^2}{y} \right|, \quad b = \left| \frac{(x + nt)(x - \frac{n}{t})}{y} \right|, \quad c = n \left| \frac{\frac{1}{t} + t}{y} \right|
\]

and again this choice makes \( n \) a \( t \)-congruent number. \( \square \)

**Example 5.** Let \( n = 12, \ t = \frac{4}{3} \). One checks that

\[
C_{12,\frac{4}{3}}(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}
\]

and two generators are \((0, 0)\) and \((-6, 30)\). This latter point, plugged into the formulas above, give us the triangle with sides 5, 5, 6 and area \( n = 12 \).

**Remark.** Notice that, contrary to the previous situation, here we have a torsion point giving us a congruent number! So we may have \( C_{n,t} \) of rank zero but such that \( n \) is a \( t \)-congruent number.

**References**

