Congruent Numbers

Kent E. Morrison

Here are the first 10 congruent numbers along with the side lengths of the associated right triangles.

n	sides
5	3/2, 20/3, 41/6
6	3, 4, 5
7	24/5, 35/12, 337/60
13	780/323, 323/30, 106921/9690
14	8/3, 63/6, 65/6
15	15/2, 4, 17/2
20	3, 40/3, 41/3
21	7/2, 12, 25/2
22	33/35, 140/3, 4901/105
23	80155/20748, 41496/3485, 905141617/72306780

If n is congruent, then multiplying n by the square of a whole number gives another congruent number. For example, since 5 is congruent, it follows that $20 = 4 \cdot 5$ is congruent. The sides of the triangle are doubled and the area of the triangle is quadrupled. So, the search for congruent numbers focuses on those n which are not multiples of a square. These are called *square-free*.

Elliptic curves

All recent results about congruent number stem from the fact that n is a congruent number if and only if the elliptic curve $y^2 = x^3 - n^2x$ contains a rational point with $y \neq 0$, equivalently, a rational point of infinite order.

The first person to exploit this in a nontrivial way was Heegner, who developed the theory of what are now called Heegner points. In 1952 he proved that if $p \equiv 5 \mod 8$ or $p \equiv 7 \mod 8$ is prime, then p is a congruent number. This result is unconditional, while (as described below) most of the later results rely on the Birch and Swinnerton-Dyer Conjecture.

In general it is a hard problem to find points on an elliptic curve, even if you know that such a point exists. The issue is that it is difficult to tell in advance how large the numerator and denominator of the points might be. Heegner's method, which does explicitly produce a point of infinite order on the elliptic curve, cannot be adapted to handle the general case.

Tunnel's Criterion

In 1982 Jerrold Tunnell of Rutgers University made significant progress by connecting congruent numbers to elliptic curves, mathematical objects for which there is a well-understood theory. He showed that there is a formula for determining whether or not any positive number n is a congruent number, but the complete validity of his formula depends on the truth of one of the outstanding problems in mathematics known as the Birch and Swinnerton-Dyer Conjecture. In the 1960's Bryan Birch (Oxford University) Peter Swinnerton-Dyer (Cambrdige University) made a surprising conjecture about the algebraic structure of elliptic curves. The conjecture asserts the equivalence of two seemingly unrelated statements. In 1977 one direction of the implication was proved by J. Coates and A. Wiles, and all evidence points to the truth of the implication in the other direction.

Along with the Riemann Hypothesis the Birch and Swinnerton-Dyer Conjecture is one of the seven Millenium Prize Problems posed by the Clay Institute with a prize of one million dollars for the solution of each. For each positive square-free number n another number is computed by Tunnell's formula. If this number is not zero then n is not a congruent number, but if this computed number is zero then n is congruent as long as the BSD Conjecture is true. Tunnell's formula can even be computed by hand for small values of n, and it can be computed easily for larger values using a personal computer, but as the numbers get even larger the computations cannot be done with ordinary computers and the typical mathematical software available.

The Formula

Tunnell's Formula uses the following two power series in the variable q:

$$A(q) = \sum_{n=1}^{\infty} a_n q^n = q \prod_{n=1}^{\infty} (1-q^{8n})(1-q^{16n}) \left(1 + \sum_{n=1}^{\infty} 2q^{2n^2} \right)$$
$$B(q) = \sum_{n=1}^{\infty} b_n q^n = q \prod_{n=1}^{\infty} (1-q^{8n})(1-q^{16n}) \left(1 + \sum_{n=1}^{\infty} 2q^{4n^2} \right)$$

Let n be a positive integer that is square-free. If n is odd, compute a_n; if n is even, compute $b_{n/2}$. In either case, if the result is 0, then n is congruent, and if the result is not 0, then n is not congruent.

If the original number n is divisible by a square, then reduce it by factoring out all squares and use the resulting smaller number in place of n. For example, to determine whether 108 is congruent, we factor it as $108 = 2^2 \cdot 3^3$. Then we factor out $2^2 \cdot 3^2$, leaving just 3. Finally, we compute a_3. We will see below that $a_3 = 2$, and so 3 and 108 are not congruent numbers.

In order to compute the coefficients a_n for $n \leq 25$ we only need to multiply this much of $A(q)$:

$$q(1-q^8)(1-q^{16})(1-q^{16})(1+2q^2+2q^8+2q^{18})$$

because everything else contributes higher powers of q. After multiplying we see that

$$A(q) = q + 2q^3 + q^9 - 2q^{11} - 4q^{17} - 2q^{19} - 3q^{25} + \ldots$$

Thus, the odd values of n for which $a_n = 0$ are $n = 5, 7, 13, 15, 21, 23$. These are the odd congruent numbers less than 25. All of them are square-free.

For even numbers we need to look at the coefficients of $B(q)$. To check the even numbers up to 24 we need the factors in $B(q)$ that contribute terms of degree up to 12, which are

$$q(1-q^8)(1+2q^4).$$

Multiplying these we see that

$$B(q) = q + 2q^5 - q^9 - 2q^{13} + \ldots.$$

Thus, $b_{n/2} = 0$ for $n/2 = 2, 3, 4, 6, 7, 8, 10, 11, 12$, or for $n = 4, 6, 8, 12, 14, 16, 20, 22, 24$. Of these numbers only $6, 14, 22$ are square-free.

Combining the lists gives the square-free congruent numbers up to 25:

$$5, 6, 7, 13, 14, 15, 21, 22, 23.$$

The only other congruent number less than 25 is 20, but it is not square-free.