Congruent Numbers and Tunnell's theorem *

Manvendra Somvanshi (MS20126)

April 19, 2023

Contents

1 Congruent Numbers and the Problem

The congruent number problem is ancient problem in number theory. A congruent number is defined as follows.

Definition 1.1 An positive integer n is said to be a congruent number if there exists a right angle triangle with rational sides such that n is the area of that triangle.

The congruent number problem asks whether it is possible to devise a simple enough test to check if an integer is congruent. Here "simple enough" means that the congruency of the number can be determined in polynomial time. Using the concept of Pythagoras triplets it easy enough to generate right triangles. This technique can be used to generate all the congruent numbers as well. Let a, b be two integers. Then $x = a^2 - b^2, y = 2ab, z = a^2 + b^2$ satisfies the condition $x^2 + y^2 = z^2$. If g is the g.c.d. of a, b then $a = gc$ and $b = gd$ where $\gcd(c, d) = 1$. Let $x' = c^2 - d^2, y' = 2cd, z' = c^2 + d^2$. Then we can have

$$x = g^2x', \; y = g^2y', \; \& \; \; z = g^2z'.$$

Moreover when c, d are both not odd together then (x', y', z') are primitive Pythagoras triplets (i.e. they have no common divisor). Now consider the following result.

Proposition 1.2 An integer n is congruent if it's square free part is congruent.

Proof. Consider an integer $n = s^2m$, where m is square free. Then there exist $x, y, z \in \mathbb{Q}^*$ such that $z^2 = x^2 + y^2$ and $m = \frac{1}{2}xy$. Then the number $n = s^2m$ corresponds to the area of the triangle with sides sx, sy, sz. ∎

This result leads to the following definition of an equivalence relation on $\mathbb{Z}^+$: let $x \sim y$ if either $x = s^2y$ or $y = s^2x$ for some $s \in Z$. Let S be the $\mathbb{Z}^+/\sim$. S has an equivalence class for each square free integer. By the previous proposition it is enough to check congruence of elements in S. Returning back to the problem of generating congruent numbers: since the primitive Pythagoras triplets can generate any Pythagoras triplet with area of the respective triangles differing by factor of a square, it follows that looking at primitive Pythagoras triplets is enough. This discussion is summarised in the following theorem.

*All the source code used here has been uploaded on github.

THEOREM 1.3 For every congruent number n there exists integers a, b such that $\gcd(a,b) = 1$, a, b are both not odd, and $n \sim ab(a^2 - b^2)$.

Proof. For n there exists rationals x, y, z such that $n = \frac{1}{2}xy$ and $x^2 + y^2 = z^2$. Suppose that $x = p/q, y = r/s, z = t/u$ then $n' = \frac{1}{2}(prqs)u^2 = n(q^2s^2u^2)$ is the area of the triangle with integer sides psu, rqu, qst. By definition $n \sim n'$. Since primitive Pythagoras triplets generates Pythagoras triplets it follows that there is some Pythagoras triplet $x', y', z' \in \mathbb{Z}^+$ such that they are coprime. Since every primitive Pythagoras triplet can be written as $x' = a^2 - b^2, y' = 2ab, z' = a^2 + b^2$ where a, b are coprime and both are not odd, the conclusion follows. ∎

Using theorem 1.3 it follows that every primitive Pythagoras triplet generate the set of squarefree congruent numbers. I have written a program (discussed later) which will generate a list of congruent numbers. But note that it is not possible to know a specific congruent number would appear in this list.

PROPOSITION 1.5 An integer n is congruent if and only if there exists $a \in \mathbb{Q}^+$ such that $a, a \pm n$ are rational squares.

Proof. Suppose that n is congruent. Then there exists rational x, y, z such that $x^2 + y^2 = z^2$ and $n = \frac{1}{2}xy$. Thus it follows that

$$\begin{aligned} x^2 + y^2 \pm 4n &= z^2 \pm 4n \\ \implies (x \pm y)^2 &= z^2 \pm 4n \\ \implies \left(\frac{x \pm y}{2}\right)^2 &= \left(\frac{z}{2}\right)^2 \pm n \end{aligned} \tag{1.1}$$

Thus we get $a = (z/2)^2$. Conversly suppose that there is an a such that $a, a \pm n$ are a rational squares. Then let $x = \sqrt{a+n} - \sqrt{a-n}, y = \sqrt{a+n} + \sqrt{a-n}, z = 2\sqrt{a}$. Then we clearly have $x^2 + y^2 = z^2$ and $n = \frac{1}{2}xy$. ∎

THEOREM 1.6 (Fermat) 1 is not a congruent number.

Proof. Suppose that 1 is congruent. Then there exists an $a \in \mathbb{Q}^+$ such that $a \pm 1, a$ are rational squares. Suppose that $\sqrt{a} = \frac{u}{v}$ such that u, v are coprime. Then

$$a \pm 1 = \frac{u^2 \pm v^2}{v^2}$$

Multiplying these we get that

$$v^4(a^2 - 1) = u^4 - v^4.$$

Note that the LHS is a perfect integer square as well. Thus there exists an integral solution to the equation

$$X^4 - Y^4 = Z^2$$

This is a contradiction since the above equation has no solutions. ∎

COROLLARY 1.7 Perfect squares are not congruent.

Proof. Since the square free part of perfect squares is 1, it follows that n is not congruent. ∎

The above corollary has an interesting geometric interpretation as well. Given any right angle triangle with rational sides and area $n \in \mathbb{N}$ it is not possible to construct a square of rational side with area n.

2 Elliptic Curves and Tunnell's Theorem

Consider the eq. (1.1) in proposition 1.5. We can multiply the two equations together to obtain

$$\left(\frac{x^2 - y^2}{4}\right)^2 = \frac{z^4}{16} - n^2$$

Thus it follows that there exists a rational solution to the equation

$$v^2 = u^4 - n^2$$

where $v = (x^2 - y^2)/4, u = z/2$. Multiplying this equation by u^2 and setting $X = u^2$ and $Y = uv$ we get

$$Y^2 = X^3 - n^2 X \tag{2.1}$$

Thus given a right angle triangle which has rational sides and area n, there exists a point $(X, Y) \in \mathbb{Q}^2$ which lies on the curve given by eq. (2.1). An interesting question to ask at this point is whether every rational point on this curve corresponds to a right triangle with rational sides and area n? This is not true in general since the X coordinate must be a rational square (by the construction above). But a classification of such rational points on the curve eq. (2.1) is possible, as shown in the following theorem.

Theorem 2.1 Let (X, Y) be a rational point on the curve $Y^2 = X^3 - n^2 X$ such that

1) X is a rational square.
2) X has an even denominator.

Then there exists a right angle triangle with rational sides and area n.

Proof. Let $u = \sqrt{X}$ and $v = Y/u$. Then we get that

$$\begin{aligned} & v^2 u^2 = u^6 - n^2 u^2 \\ \implies & v^2 = u^4 - n^2 \\ \implies & v^2 + n^2 = x^2 \end{aligned}$$

Let $u = p/q$ where p, q are coprime. Then by assumption q is even. Since n is an integer it follows that v^2 and x^2 have the same denominator, i.e. q^4. Clearly $q^2 v, q^2 n, q^2 x$ is a primitive Pythagoras triplet. Thus there exists a, b coprime and $a + b$ odd, such that $q^2 v = a^2 - b^2, q^2 n = 2ab$, and $q^2 x = a^2 + b^2$. Then the right angle triangle with sides $x = 2a/q, y = 2b/q$, and $z = 2u$ has area n. ∎

Definition 2.2 Let K be some field with characteristic $\neq 2$ and let $f \in K[x]$ be a cubic polynomial with distinct roots in some extension K' of K. Then the set of solutions to the equation

$$E : \ y^2 = f(x),$$

where x, y are in K', are called the K' points of an elliptic curve. Represent this set by $E(K)$.

Till now we had been working with the elliptic curve $y^2 = x^3 - n^2x$ over the field $K = K' = \mathbb{Q}$. This is an elliptic curve because the roots of the polynomial $x^3 - n^3x$ are $0, \pm n$ (distinct in $\mathbb{Q}$). Thus the congruent number problem is very closely related to the study of elliptic curves.

Consider an elliptic curve $E(K)$ over some field K. Define an addition on $E(K)$ in the following way: consider 2 $K-$points P, Q, on the elliptic curve $E(K)$. Draw a line joining P, Q. This would intersect the curve at a third point R. Then define $P + Q = -R$, where $-R = (a, -b)$ if $R = (a, b)$. Let O be the (unique) point at infinity. This addition makes $E(K)$ an abelian group with identiy O. The inverse of a point is P is just $-P$.

Definition 2.3 If G is a group then the subgroup containing all finite order elements is called the torsion subgroup G_{tors} of G.

Theorem 2.4 (Mordell-Weil) If $E(\mathbb{Q})$ is a an elliptic curve then it is finitely generated and $E(\mathbb{Q}) \cong E(Q)_{\text{tors}} \times \mathbb{Z}^r$.

Here the number r is called the rank of the elliptic curve.

Conjecture 2.5 (Birch and Swinnerton-Dyer (BSD)) Let E be an elliptic curve and x be some integer, then

$$\prod_{p \mid x} \frac{\#E(\mathbb{F}_p)}{p} \sim C_E(\log(x))^{\text{rank}(E(\mathbb{Q}))}.$$

Now we can finally understand the statement of the amazing theorem proved by Tunnell regarding to classify congruent numbers.

Theorem 2.6 (Tunnell) Let n be a square free positive integer. Then define the following:

$$\begin{aligned}
a_n &= \#\{(x, y, z) \in \mathbb{Z}^3 \mid 2x^2 + y^2 + 8z^2 = n\} \\
b_n &= \#\{(x, y, z) \in \mathbb{Z}^3 \mid 2x^2 + y^2 + 32z^2 = n\} \\
a'_n &= \#\{(x, y, z) \in \mathbb{Z}^3 \mid 8x^2 + 2y^2 + 16z^2 = n\} \\
b'_n &= \#\{(x, y, z) \in \mathbb{Z}^3 \mid 8x^2 + 2y^2 + 64z^2 = n\}.
\end{aligned}$$

Then,

1) If n is an odd congruent number then $a_n = 2b_n$. If n is an even congruent number then $a'_n = 2b'_n$.
2) The converse of statement 1 is true if the BSD conjecture is assumed.

An immidiate corollary to Tunnell's theorem is the following.

Corollary 2.7 Let n be an integer. n is congruent if $n \equiv 5, 6, 7 \pmod 8$.

3 Computation of Congruent Numbers

There are three essentially three computations which I have done.

1) The first is brute force computation of congruent numbers using the Pythagoras triplet method discussed in theorem 1.3.

2) The second is generating the congruent numbers assuming that the BSD conjecture (and hence the converse in Tunnell's theorem) holds true.
3) The distribution of congruent numbers assuming the BSD conjecture.

3.1 Brute force Method

In this method I first generate pairs (a, b) such that $\gcd(a, b) = 1$ and $a + b$ is odd and for each pair the right angle triangle and its area is calculated and added to a list of dictionaries. This is done by the following snippet:

```
def generate_primitives(N):
    m = 1
    primitives = []
    while True:
        n=1
        while n<m:
            if m>n and m%2 != n%2 and GCD(m,n) ==1:
                primitives.append({"x": m**2-n**2, "y": 2*m*n, "z": m**2 + n**2, "area
    ": m*n*(m**2 - n**2)})
            n+=1
        if m == N:
            break
        m+=1
    return primitives
```

To generate the list of square free congruent numbers I add the "area" key in the dictionary to a set, after removing the square part from the integer.

```
    if method == "brute force":
        S = generate_primitives(N)
        cong_numbers = set()
        for d in S:
            cong_numbers.add(remove_square(d["area"]))
        cong_numbers = list(cong_numbers)
        cong_numbers.sort()
        return cong_numbers
```

This method gives the following output when $N = 40$.

```
[5, 6, 7, 14, 15, 21, 30, 34, 39, 41, 65, 70, 78, 110, 111, 138, 145, 154, 161, 165,
    174, 190, 210, 221, 231, 255, 286, 299, 310, 330, 357, 390, 429, 434, 462, 465,
    510, 517, 546, 561, 602, 609, 646, 651, 671, 741, 759, 798, 806, 957, 966, 1110,
    1113, 1122, 1131, 1155, 1190, 1254, 1295, 1311, 1326, 1330, 1365, 1406, 1419, 1443,
     1462, 1482, 1595, 1610, 1705, 1770, 1785, 1794, 1885, 1886, 1995, 2006, 2046,
    2139, 2310, 2470, 2485, 2530, 2701, 2706, 2730, 2990, 3102, 3135, 3255, 3458, 3534,
     3570, 3705, 3885, 3990, 4030, 4134, 4218, 4290, 4305, 4466, 4641, 4830, 4921,
    4935, 5394, 5510, 5610, 5865, 6006, 6090, 6251, 6270, 6279, 6355, 6486, 6545, 6555,
     6630, 6882, 7395, 7854, 8729, 8866, 8970, 9030, 9430, 9435, 9690, 10010, 10374,
    10385, 10614, 10626, 10730, 11310, 11571, 11914, 12369, 13195, 13566, 14070, 14835,
     15015, 15470, 15834, 15990, 16530, 16835, 17119, 17290, 17641, 17765, 18354,
    18870, 19006, 19866, 20670, 21390, 21855, 22010, 22134, 22386, 23970, 24486, 24510,
     25194, 25530, 25806, 26130, 26565, 26970, 27370, 28938, 29274, 29986, 30030,
    30810, 31746, 33915, 34510, 35409, 36146, 36890, 38409, 38766, 39270, 41055, 41181,
     41230, 42315, 43010, 43554, 43890, 45066, 46110, 47730, 49335, 50061, 51051,
    51330, 51414, 51794, 52026, 52170, 54834, 55510, 55614, 55965, 56730, 58695, 59334,
     60639, 63070, 66990, 68034, 70455, 71610, 72930, 73834, 74074, 75174, 75981,
    77330, 81510, 82110, 84630, 85470, 86955, 98670, 101010, 108570, 113505, 113646,
    113685, 114114, 116994, 118326, 124410, 128310, 136290, 140070, 158730, 162690,
    163590, 168630, 175890, 176046, 178710, 179265, 192270, 201201, 205530, 214890,
    218595, 220110, 222870, 227766, 229710, 235410, 243390, 249690, 255990, 257070,
    261870, 266910, 267954, 269610, 285090, 291270, 295926, 311610, 326370, 354354,
    412566, 436254, 445170, 483990, 490314, 510510, 513570, 520590, 568974, 570570,
    607614, 694830, 720390, 746130, 799710, 800394, 889746]
```

As evident this method is very inefficient to generate congruent numbers. For example the number 13, which is congruent, has not appeared in this list yet even after 40 trials.

3.2 Tunnell's method

In this method we assume that the BSD conjecture is true and use the converse of Tunnell's theorem to generate a list by checking if each integer below some N is congruent or not. This gives an exhaustive list congruent numbers below N. This is much better than the previous method which just gives us N congruent numbers.

```
    elif method == "tunnell":
        m = 1
        cong_numbers = set()
        while m <= N:
            n = remove_square(m)
            if n%8 == 5 or n%8 == 6 or n%8 == 7:
                cong_numbers.add(n)
            elif n%2 == 1:
                a = 0
                b = 0
                for x in range(-1*int(np.sqrt(n)), int(np.sqrt(n)) + 1):
                    for y in range(-1*int(np.sqrt(n)), int(np.sqrt(n)) + 1):
                        for z in range(-1*int(np.sqrt(n)), int(np.sqrt(n)) + 1):
                            if 2*x**2 + y**2 + 8*z**2 == n:
                                a+=1
                            if 2*x**2 + y**2 + 32*z**2 == n:
                                b+=1
                if a == 2*b:
                    cong_numbers.add(n)
            elif n%2 == 0:
                a = 0
                b = 0
                for x in range(-1*int(np.sqrt(n)), int(np.sqrt(n)) + 1):
                    for y in range(-1*int(np.sqrt(n)), int(np.sqrt(n)) + 1):
                        for z in range(-1*int(np.sqrt(n)), int(np.sqrt(n)) + 1):
                            if 8*x**2 +2*y**2 + 16*z**2 == n:
                                a+=1
                            if 8*x**2 + 2*y**2 + 64*z**2 == n:
                                b+=1
                if a == 2*b:
                    cong_numbers.add(n)
            m+=1
        cong_numbers = list(cong_numbers)
        return cong_numbers
```

Here are all the square free congruent numbers less than 1000:

```
[5, 6, 7, 13, 14, 15, 21, 22, 23, 29, 30, 31, 37, 38, 39, 46, 47, 53, 55, 61, 62, 69,
    70, 71, 77, 78, 79, 85, 86, 87, 93, 94, 95, 101, 102, 103, 109, 110, 111, 118, 119,
     127, 133, 134, 141, 142, 143, 149, 151, 157, 158, 159, 165, 166, 167, 173, 174,
    181, 182, 183, 190, 191, 197, 199, 205, 206, 213, 214, 215, 221, 222, 223, 229,
    230, 231, 237, 238, 239, 246, 247, 253, 254, 255, 262, 263, 269, 271, 277, 278,
    285, 286, 287, 293, 295, 301, 302, 303, 309, 310, 311, 317, 318, 319, 326, 327,
    334, 335, 341, 349, 357, 358, 359, 365, 366, 367, 373, 374, 381, 382, 383, 389,
    390, 391, 397, 398, 399, 406, 407, 413, 415, 421, 422, 429, 430, 431, 437, 438,
    439, 445, 446, 447, 453, 454, 455, 461, 462, 463, 469, 470, 471, 478, 479, 485,
    487, 493, 494, 501, 502, 503, 509, 510, 511, 517, 518, 519, 526, 527, 533, 534,
    535, 541, 542, 543, 551, 557, 559, 565, 566, 573, 574, 581, 582, 583, 589, 590,
    591, 597, 598, 599, 606, 607, 613, 614, 615, 622, 623, 629, 631, 638, 645, 646,
    647, 653, 654, 655, 661, 662, 663, 669, 670, 671, 677, 678, 679, 685, 687, 694,
    695, 701, 703, 709, 710, 717, 718, 719, 727, 733, 734, 741, 742, 743, 749, 751,
    757, 758, 759, 766, 767, 773, 781, 782, 789, 790, 791, 797, 798, 799, 805, 806,
    807, 813, 814, 815, 821, 822, 823, 829, 830, 831, 838, 839, 853, 854, 861, 862,
    863, 869, 870, 871, 877, 878, 879, 885, 886, 887, 893, 894, 895, 901, 902, 903,
    910, 911, 917, 919, 926, 933, 934, 935, 941, 942, 943, 949, 951, 957, 958, 959,
    965, 966, 967, 973, 974, 982, 983, 989, 991, 997, 998]
```

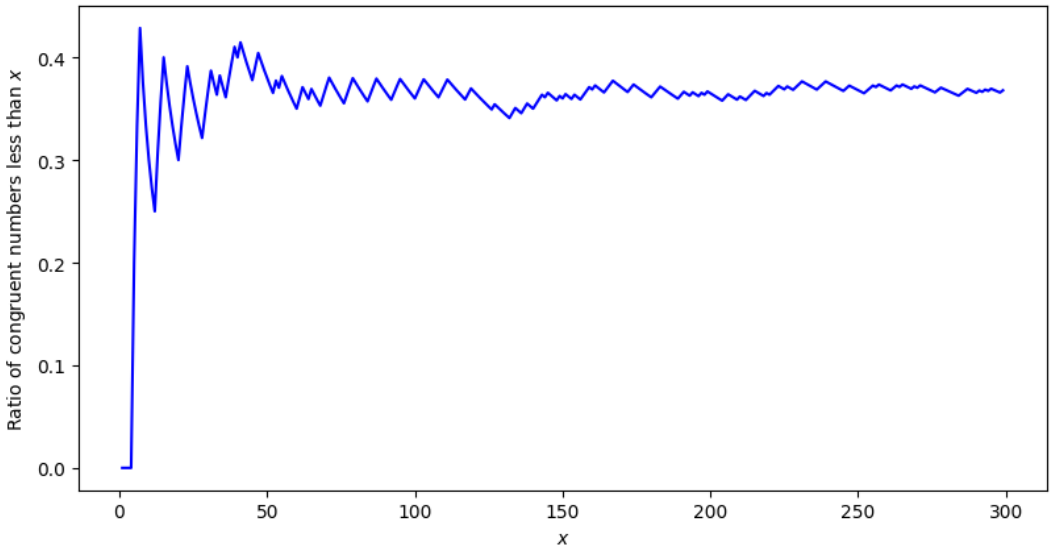

Figure 1: The distribution for $N = 500$. As observed here this ratio eventually becomes a constant with value of about 0.368.

3.3 Distribution of square free congruent numbers

I wrote a method that counts the number of square free congruent numbers less than N using Tunnell's method (assuming the BSD conjecture) and I have plotted their ratio against N.

```
def distribution(N):
    X = list(range(1, N))
    Y = []
    for x in X:
        cong_numbers = gen_congruent(x, "tunnell")
        Y.append(len(cong_numbers)/x)
    plt.plot(X, Y, "b-")
    plt.xlabel(r"$x$")
    plt.ylabel(r"Ratio of congruent numbers less than $x$")
    plt.show()
```

From the above figure one can also claim the following conjecture.

Conjecture 3.1 For large enough n the number of square free congruent numbers, $C(n)$, less than n can be approximated by

$$C(n) \sim \alpha n$$

where $\alpha \approx 0.368$.

This conjecture will be true given the assumption of the BSD conjecture.