Numbers that are Sums of Squares in Several Ways

David J.C. MacKay
mackay@mrao.cam.ac.uk

Sanjoy Mahajan
sanjoy@mrao.cam.ac.uk

December 10, 2001

Which number comes next?

50
65
85
125
130
145
170
185
200
205

Hint: it's related to Hardy's taxi, number 1729.

When Hardy, visiting the brilliant mathematician Ramanujan, remarked that he had taken taxi number 1729, "rather a dull number", Ramanujan immediately responded "On the contrary, it is the smallest number that can be expressed as the sum of two cubes in two different ways".

$$1729 = 1^3 + 12^3 = 9^3 + 10^3 \tag{1}$$

We were curious to understand how Ramanujan was able not only to spot that 1729 is a sum of two cubes in two ways – not difficult for someone who knows all the numbers as friends – but also to know that 1729 is the *smallest* number having this property. We therefore decided to study the analogous problem for squares:

> What is the smallest integer that can be expressed as the sum of two squares in two different ways?

We haven't figured out Ramanujan's insight, but we encountered some fun ideas along the way.

1 Numbers that are the sum of two squares in several ways

After a little hunting by hand for examples of numbers that are the sum of two squares in several ways, we found a simple way to construct them systematically. If the number n satisfies

$$n = a^2 + b^2 = c^2 + d^2 \tag{2}$$

then

$$a^2 - c^2 = d^2 - b^2 \tag{3}$$

so

$$(a + c)(a - c) = (d + b)(d - b). \tag{4}$$

So to make an n that satisfies $n = a^2 + b^2 = c^2 + d^2$, all we need to do is find four numbers w, x, y, and z satisfying

$$wx = yz \tag{5}$$

then use them to define a, b, c, and d as follows:

$$\begin{array}{ccccc} \overbrace{w}^{} & \overbrace{x}^{} & = & \overbrace{y}^{} & \overbrace{z}^{} \\ \overbrace{(a+c)} & \overbrace{(a-c)} & = & \overbrace{(d+b)} & \overbrace{(d-b)}, \end{array} \tag{6}$$

that is,

$$a = \frac{w+x}{2},\ c = \frac{w-x}{2},\ d = \frac{y+z}{2},\ b = \frac{y-z}{2}. \tag{7}$$

As long as all these numbers are non-zero integers, we have a solution of $n = a^2 + b^2 = c^2 + d^2$.

In summary, we can find solutions by picking a w and an x satisfying

- at least one of w and x is composite (*i.e.*, not a prime number);
- w and x are both odd or both even;

then by factoring and recomposing, we obtain y and z, which must be both odd or both even.

We applied this recipe and found

$$\begin{array}{rcrcrcr} 50 &=& 1^2 &+& 7^2 &=& 5^2 + 5^2 \\ 65 &=& 1^2 &+& 8^2 &=& 4^2 + 7^2 \\ 85 &=& 2^2 &+& 9^2 &=& 6^2 + 7^2 \\ 125 &=& 2^2 &+& 11^2 &=& 5^2 + 10^2 \\ 130 &=& 3^2 &+& 11^2 &=& 7^2 + 9^2 \\ 145 &=& 1^2 &+& 12^2 &=& 8^2 + 9^2 \end{array} \tag{8}$$

At this point, we became curious:

> Are all numbers that are expressible as the sum of two squares in several ways multiples of five?

The next two numbers confirmed this pattern.

$$\begin{array}{rcrcrcr} 170 &=& 1^2 &+& 13^2 &=& 7^2 + 11^2 \\ 185 &=& 4^2 &+& 13^2 &=& 8^2 + 11^2 \end{array} \tag{9}$$

We therefore attempted to prove or disprove this conjecture.

2 All $n = a^2 + b^2 = c^2 + d^2$ are zero modulo 5?

A probabilistic argument for feeling pretty convinced about this conjecture might be spelt out as follows. A square, a^2, either leaves 1, 4, or 0, when divided by five.

$a \bmod 5$	$a^2 \bmod 5$
1	1
2	4
3	4
4	1
0	0

(10)

If we add two random squares, a^2 and b^2, the probability that their sum is divisible by 5 is

$$9/25. \tag{11}$$

[We can see this by checking all 25 cases as shown below, which shows $a^2 + b^2 \bmod 5$. Nine cases are zero.]

		$a \bmod 5$				
		1	2	3	4	0
	1	2	0	0	2	1
	2	0	3	3	0	4
$b \bmod 5$	3	0	3	3	0	4
	4	2	0	0	2	1
	0	1	4	4	1	0

(12)

So now let us compare the two hypotheses

$\mathcal{H}_1$: numbers n that are sums of squares in several ways are multiples of 5.

$\mathcal{H}_0$: numbers n that are sums of squares in several ways are made from squares a^2 and b^2 that are 'random'.

We haven't really defined $\mathcal{H}_0$ very precisely, but the idea is that $\mathcal{H}_0$ expects the number n to be a multiple of 5 with probability 9/25.

Now, we observe the first 8 numbers n and find that they are all multiples of 5. The evidence these data 'D' give in favour of $\mathcal{H}_1$ is a likelihood ratio of

$$\frac{P(D|\mathcal{H}_1)}{P(D|\mathcal{H}_0)} = \frac{1^8}{(9/25)^8} \simeq \frac{3500}{1}. \tag{13}$$

However, it could be that there is something special about the first few n, the smallest ones; maybe our null hypothesis is too naive.

3 Resolution of the modulo 5 question

We hunted for a proof of $\mathcal{H}_1$ or for a counterexample by assuming the existence of numbers w, x, y, and z such that n was equal to 1 modulo 5 (for example, $n = 101$). We found that $n \bmod 5$ could equal 1 if $(a+d)$ or $(a-d)$ was a multiple of 25. This led us to find the following counterexamples:

$$\begin{aligned} 3161 &= 5^2 + 56^2 = 35^2 + 44^2 \\ 481 &= 9^2 + 20^2 = 15^2 + 16^2 \end{aligned} \tag{14}$$

Evidently there *is* something atypical about the smallest n that satisfy $n = a^2 + b^2 = c^2 + d^2$. We confirmed this by finding the first 40,000 solutions by computer and plotting the fraction that are divisible by 5, as a function of how many solutions n we found (figure 1). Evidently, even when we reach n as big as 100,000, we still have not reached 'large n': the fraction divisible by 5 is still changing.

Finally, the answer to the puzzle posed on page 1. The next number is 221:

$$221 = 5^2 + 14^2 = 10^2 + 11^2 \tag{15}$$

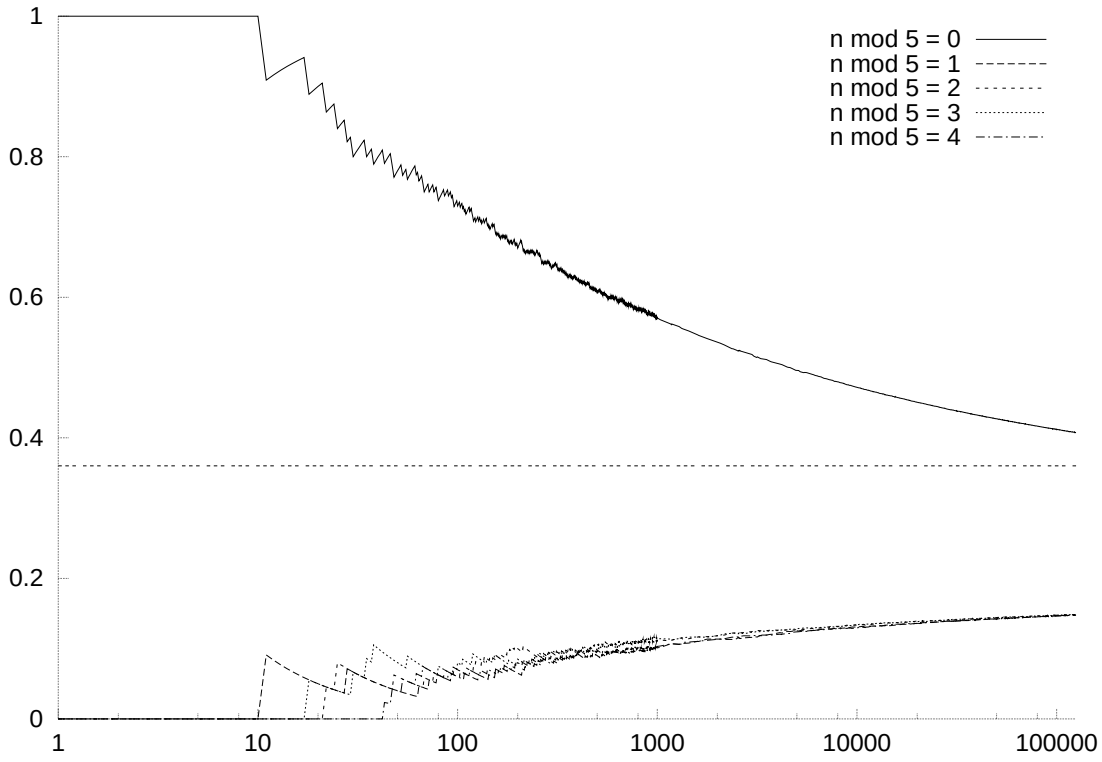

Figure 1: Fraction of integers n satisfying $n = a^2 + b^2 = c^2 + d^2$ that are equal to 0, 1, 2, 3, and 4, modulo 5, as a function of the rank of n. The 10,000th integer on the list is 92485. The marked asymptote is 9/25.

Here is the list of the first 24 solutions.

$$
\begin{array}{rcrcrcrcrcl}
50 &=& 1^2 &+& 7^2 &=& 5^2 &+& 5^2 & & \\
65 &=& 1^2 &+& 8^2 &=& 4^2 &+& 7^2 & & \\
85 &=& 2^2 &+& 9^2 &=& 6^2 &+& 7^2 & & \\
125 &=& 2^2 &+& 11^2 &=& 5^2 &+& 10^2 & & \\
130 &=& 3^2 &+& 11^2 &=& 7^2 &+& 9^2 & & \\
145 &=& 1^2 &+& 12^2 &=& 8^2 &+& 9^2 & & \\
170 &=& 1^2 &+& 13^2 &=& 7^2 &+& 11^2 & & \\
185 &=& 4^2 &+& 13^2 &=& 8^2 &+& 11^2 & & \\
200 &=& 2^2 &+& 14^2 &=& 10^2 &+& 10^2 & & \\
205 &=& 3^2 &+& 14^2 &=& 6^2 &+& 13^2 & & \\
221 &=& 5^2 &+& 14^2 &=& 10^2 &+& 11^2 & & \\
250 &=& 5^2 &+& 15^2 &=& 9^2 &+& 13^2 & & \\
260 &=& 2^2 &+& 16^2 &=& 8^2 &+& 14^2 & & \\
265 &=& 3^2 &+& 16^2 &=& 11^2 &+& 12^2 & & \\
290 &=& 1^2 &+& 17^2 &=& 11^2 &+& 13^2 & & \\
305 &=& 4^2 &+& 17^2 &=& 7^2 &+& 16^2 & & \\
325 &=& 1^2 &+& 18^2 &=& 6^2 &+& 17^2 &=& 10^2 + 15^2 \\
338 &=& 7^2 &+& 17^2 &=& 13^2 &+& 13^2 & & \\
340 &=& 4^2 &+& 18^2 &=& 12^2 &+& 14^2 & & \\
365 &=& 2^2 &+& 19^2 &=& 13^2 &+& 14^2 & & \\
370 &=& 3^2 &+& 19^2 &=& 9^2 &+& 17^2 & & \\
377 &=& 4^2 &+& 19^2 &=& 11^2 &+& 16^2 & & \\
410 &=& 7^2 &+& 19^2 &=& 11^2 &+& 17^2 & & \\
425 &=& 5^2 &+& 20^2 &=& 8^2 &+& 19^2 &=& 13^2 + 16^2
\end{array}
$$

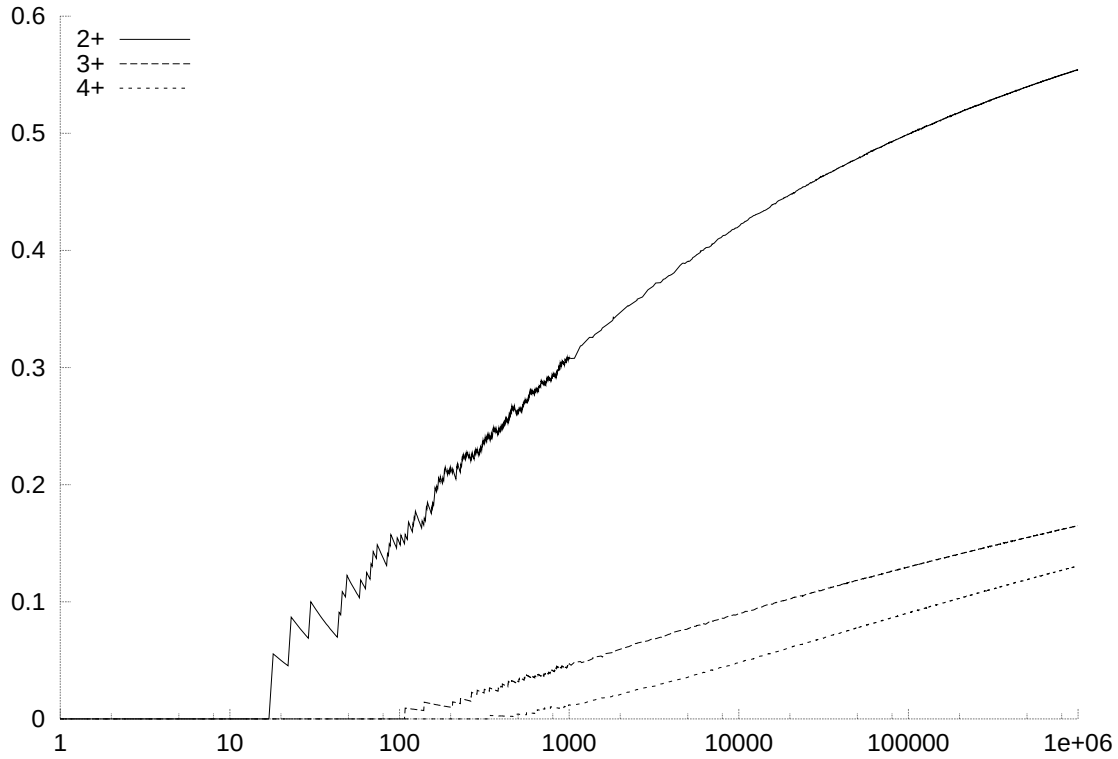

Figure 2: Fraction of integers m satisfying $m = a^2 + b^2$ that can be so written in at least 2, at least 3, and at least 4 ways. The horizontal axis is the number of such integers considered. The 1,000,082nd integer that is a sum of two squares is 4,917,497.

4 Coda

Our naive theory seems to be working surprisingly well. At large n, the probability that n is a multiple of 5 seems to tend to 9/25, the same as the probability that a random sum of two squares is a multiple of 5. Why? We think the reason is that at sufficiently large n, *all* sums of two squares can be written in several ways. So there is nothing special about n compared with ordinary sums of two squares, and the 'randomly chosen sum of squares' argument is accurate.

This observation motivates a new puzzle for future Ramanujans:

> what is the largest integer m that can *only* be expressed as the sum of two squares in *one* way?

From figure 2 we suspect that this largest integer will be rather greater than one billion.