SUMS OF SQUARES

WUSHI GOLDRING

1. Introduction

Here are some opening big questions to think about:

Question 1. *Which positive integers are sums of two squares?*

Question 2. *Which positive integers are sums of three squares?*

Question 3. *Which positive integers are sums of four squares?*

People started thinking seriously about these questions and answered them in the 17th and 18th centuries. The first question, involving two squares, was studied by Pierre de Fermat. You may have heard of him in connection with "Fermat's Last Theorem", which states that when $n \geq 3$, the equation $x^n + y^n = z^n$ has no solutions with x, y, z all positive integers. This last statement was proved in the 1990's by Andrew Wiles. I mention this also so that you see that Fermat's work has kept people busy to this day.

Back to sums of squares. Let's start computing a little.

Question 4. *Of the numbers from* 1 *to* 10*, which are sums of* 2 *squares?* 3 *squares?* 4 *squares? (We count* 0 *as a square,* $0 = 0^2$*)*

From this little experiment, it seems like more numbers are sums of 3 squares than 2 squares, and more numbers are sums of 4 squares than 3 squares. It turns out this is indeed true. Up to 10, we could not find a number which is not a sum of 4 squares.

Question 5. *Is there a positive integer that is not a sum of four squares?*

Think about it, it's not easy to answer!

W. G. Department of Mathematics, Washington University in St. Louis, One Brookings Drive, St. Louis, MO 63130, USA
E-mail address: wushijig@gmail.com.
Date: March 10, 2016.

2. Primes and prime factorization

A positive integer $n > 1$ is *prime* if the only positive integers that are factors of n are 1 and n itself. For example, 17 is prime, but 15 is not, because $15 = 3 \cdot 5$. Primes are the building blocks of all positive integers. Every positive integer can be written in a unique way as a product of primes (up to reordering the factors); this is called prime factorization.

Problem 6. *Find the prime factorization of the following numbers:* 105, 61, 75, 192.

Most questions about numbers can be reduced to asking the same question only about prime numbers. So if we have a question about numbers, we might try first to study it for prime numbers, and then build up from there by using prime factorization. Let's apply these general comments to Question 1 about sums of 2 squares.

3. Primes that are sums of 2 squares

We want to find out which primes are sums of 2 squares.

Problem 7. *Below is a list of the primes up to* 100. *Find the ones that are sums of 2 squares. Here are the primes:*

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$$

Question 8. *Can you make a conjecture based on what you found looking up to* 100*?*

4. Modular arithmetic

What makes one prime different from another? Here is one simple way to split off primes into three groups: Start with an odd prime number p. Divide it by 4. You get a remainder. What are the possible remainders? At first, you know the remainder is between 0 and 3, inclusive. But since p is odd, the remainder must be odd, so 0 and 2 are excluded. Therefore the remainder must be either 1 or 3. So we can group primes into (i) those that have remainder 1 when divided by 4, (ii) those that have remainder 3 when divided by 4, and (iii) the unique even prime: 2.

The study we performed of looking at remainders after dividing by a fixed number (in our case the number 4) is called modular arithmetic. In our case we looked at primes "modulo 4". We could equally take the primes and see what remainders we get when we divide by 5. This will be called looking at the primes "modulo 5". When we divide by 5, the primes split off into 5 groups (instead of the 3 groups that we had for division by 4).

Problem 9. *Here again is the list of primes up to 100:*

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

Determine which admit remainder 1 *when divided by* 4 *and which admit remainder* 3 *when divided by* 4. *Compare your answer with your answer to Problem 7 and then reconsider Question 8. Has your answer changed?*

Theorem 10 (Fermat-Euler)**.** *The primes which are sums of* 2 *squares are precisely the prime* 2 *and those odd primes that admit remainder* 1 *when divided by* 4*.*

I can't prove this theorem for you today. For those of you who go on to study some number theory, you can find a nice proof in [Sam70, V.6]. You can prove the negative half of this theorem:

Problem 11. *Show that if* n *is a positive integer whose remainder when divided by* 4 *is* 3*, then* n *is not a sum of* 2 *squares (it makes no difference whether you assume* n *is prime or not in this problem).*

On the other hand, for the positive direction of the theorem, the assumption that the number is prime is crucial:

Problem 12. *Give an example of a number whose remainder when divided by* 4 *is equal to* 1*, and which is not a sum of* 2 *squares.*

For now, if we accept this theorem, it leads us to some natural questions:

Question 13. *Are there infinitely many primes which are sums of* 2 *squares? Are there infinitely many primes that are not sums of* 2 *squares*

The second part is easier:

Problem 14. *Give an argument why there are infinitely many primes whose remainder modulo* 4 *is equal to* 3

The other part is a bit trickier.

Problem 15 (This is a hard one, can one of you do it?)**.** *Give an argument why there are infinitely many primes whose remainder modulo* 4 *is equal to* 1*.*

5. Sums of 2 squares: Building up from primes

The main tool for exhibiting numbers that are not prime as sums of 2 squares is the following "product property":

Question 16. *Suppose we know that* $n = x^2 + y^2$ *and* $m = z^2 + w^2$. *Can you express the product* nm *as a sum of* 2 *squares? Here are some examples to try first: Given that* $17 = 4^2 + 1^2$ *and* $5 = 2^2 + 1^2$, *how can you write* $85 = 5 \cdot 17$ *as a sum of* 2 *squares? Given that* $41 = 4^2 + 5^2$ *and* $29 = 5^2 + 2^2$, *how can you write* $1189 = 41 \cdot 29$ *as a sum of* 2 *squares?*

Hint: Try making up "combinations" out of the x, y, z, w.

Here is a somewhat related question:

Question 17. *What is the smallest number that is a sum of* 2 *squares in* 2 *different ways? For example,* 205 *is a sum of* 2 *squares in* 2 *different ways, because* $205 = 14^2 + 3^2 = 13^2 + 6^2$, *but it is not the smallest example. If this is too easy for you, what is the smallest number that is a sum of* 2 *squares in* 4 *different ways?*

Question 18. *Can you now conjecture exactly which numbers are sums of* 2 *squares?*

Theorem 19 (Fermat-Euler)**.** *A positive integer n is a sum of 2 squares if and only if, when we factor it into primes, each prime which is 3 modulo 4 appears with an even exponent.*

Problem 20. *Using the theorem, determine whether each of*

$$41 \cdot 67^3 \cdot 97,$$

$$53 \cdot 103^2 \cdot 2^5 \cdot 29^8$$

and

$$1001$$

are sums of two squares.

6. Sums of 4 squares

Theorem 21 (Lagrange)**.** *Every positive integer is a sum of* 4 *squares.*

This theorem is again too hard for us to prove right now, but you may be able to check the following ingredient:

Problem 22. *Suppose n and m are sums of* 4 *squares. Without assuming the theorem, show that the product nm is also a sum of* 4 *squares. (Hint: The idea is the same as for two squares, the computation is just more involved)*

Given the problem, you see that in order to prove the theorem, it is enough to prove that every prime is a sum of 4 squares. Again, if you go on to study number theory, you can find a proof of this in [Sam70, V.7]

7. Sums of 3 squares

Sums of 3 squares is by far the hardest of the three initial problems! Nevertheless, there are some important observations that you can make:

Problem 23. *Show that, if n is a sum of 3 squares and n is divisible by 4, then $n/4$ is also a sum of 3 squares.*

Hint: Write $n = x^2 + y^2 + z^2$ and now try to make 3 numbers x_1, y_1 and z_1 out of x, y, z such that $n/4 = x_1^2 + y_1^2 + z_1^2$.

Problem 24. *Suppose that when you divide n by 8 the remainder is 7. Show that n is not a sum of 3 squares.*

Theorem 25 (Gauss)**.** *The positive integers which are not sums of* 3 *squares are precisely those that can be written as* $4^e(8n+7)$ *for some non-negative integers* e *and* n*.*

You have already seen that 7 is not a sum of 3 squares; 7 is the case $e = n = 0$. You can check that 15 and 28 are also not a sum of 3 squares; these are the cases $(e = 0, n = 1)$ and $(e = 1, n = 0)$.

To see a proof of this last theorem requires a more in-depth study of number theory. My favorite reference is [Ser73, Appendix to Chapter IV].

8. Where to go from here: Sums of Cubes?

Since we have discussed sums of squares, you might wonder about sums of cubes. This leads questions that are much more difficult, some of which are still open problems. This is suggestive of the general situation in math: Linear equations are easy, quadratic equations are doable, and cubic equations are a complete mystery...

References

[Sam70] P. Samuel, *Algebraic theory of numbers*, Hermann, 1970.

[Ser73] J.-P. Serre, *A course in arithmetic*, Graduate Texts in Math., vol. 7, Springer-Verlag, 1973.