Tracing the history of a theorem

Lagrange's Four Squares Theorem

feature

From conjecture to proof

Why are theorems discussed in class restricted to those in the syllabus? Do we fear that students would be intimidated by equations and long proofs? In this article the author traces the development of a famous theorem and its proof. Read the article not just for the theorem but also to pick up tips on how to use numerical examples to understand algebraic equations, how to use historical details to move from conjecture to proof, and how to provide students with sufficient scaffolding to enable them to prove the theorem for themselves.

Anuradha S. Garge

Number theory is a branch of mathematics in which we study the integers and rational numbers (e.g., prime numbers; squares; cubes) and concepts derived from them. It is a field with a long past and a rich history, and it has been strongly influenced by the work of mathematical giants like Gauss, Legendre, Lagrange, Fermat, Euler, Ramanujan, etc. This article presents the story of a theorem in number theory which is very easy to state, but it took mathematicians one and a half centuries to write its full proof! It is named after Joseph Louis Lagrange, the French mathematician who gave the first complete proof in 1770.

It is common for a theorem to appear initially in the form of a 'conjecture' which may be simply an intelligent guess concerning the properties of some mathematical object; for example, we have the *Four Colour Conjecture* which went unproven for over a century before it became a theorem. Such conjectures are usually

easy to verify for small instances of the problem. But as the size of the problem gets larger, verification becomes steadily more difficult. So one needs a proof which does not depend on case-by-case analysis. It can be an uphill task to produce such a proof.

The theorem proved by Lagrange concerns a conjecture made by Bachet, a French mathematician, about natural numbers written as sums of squares. Not every natural number is a square. Can every natural number be written as a sum of *two* squares, like $5 = 2^2 + 1^2$? No, we cannot write 3 this way (check!). Can every natural number be written as a sum of *three* squares, like $3 = 1^2 + 1^2 + 1^2$ and $11 = 3^2 + 1^2 + 1^2$? Many numbers can be written this way, but some cannot; e.g., 7. But we can write 7 as a sum of *four* squares: $7 = 2^2 + 1^2 + 1^2 + 1^2$. Can every natural number be written as a sum of four squares? Amazingly, the answer is **Yes**; we never need more than four squares! For example, we have $2011 = 35^2 + 28^2 + 1^2 + 1^2$, and $2012 = 44^2 + 6^2 + 6^2 + 2^2$.

Note that writing a natural number as a sum of squares is not difficult; 1 is our friend! But we are interested in finding the *least* number such that every natural number can be written as a sum of at most that many squares. Experimentation suggests that we never need more than four squares, and this is what the amazing theorem of Lagrange asserts: *Every natural number, however large, can be written as a sum of at most four squares*. (Yes, even big numbers like one lakh (10^5) or one crore (10^7) can be written this way; see if you can find the expressions for these numbers! Experimenting further, try to guess which numbers require three squares and no less, and which numbers require four squares and no less.)

In the century before Lagrange, another brilliant French mathematician had worked on this problem: Pierre de Fermat (1601–1665). He classified those natural numbers which could be expressed as sums of two squares and which are not squares themselves. The final part of the proof was completed by Lagrange in 1770. This article describes how Bachet's conjecture turned into a theorem, and gives a (very) brief idea of Lagrange's proof.


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.
AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANORVM.
LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

Fig. 1 *Arithmetica* by Diophantus; source: [6]

Bachet's conjecture

The origins of the conjecture lie in the work of Diophantus, a third century AD mathematician from Alexandria (Egypt), who was the first to introduce notation in algebra. He wrote a book called ARITHMETICA (see Figure 1) which had a collection of problems based on what are now called *Diophantine equations*. These equations differed from one another only marginally, but a new trick had to be used to solve each one.
A significant feature of the problems is their focus on *solutions which are rational numbers*. Here is an example; it shows the level of sophistication of the problems: Diophantus asks for an expression for 13 as the sum of two rational squares each exceeding 6, and gives the following as an answer:

$$13 = \frac{66049}{10201} + \frac{66564}{10201} = \left(\frac{257}{101}\right)^2 + \left(\frac{258}{101}\right)^2.$$

Diophantus was able to solve the equations by making clever substitutions so he had to deal with simpler equations. The sophistication of his approach justifies the title he is sometimes given, 'Father of Modern Algebra'.

In 1621, Bachet (Claude Gaspard Bachet de Méziriac, to give him his full name), a French mathematician, linguist and poet, translated ARITHMETICA from Greek into Latin. While doing so, he was led to claim (or perhaps to affirm the claim made by Diophantus) that every natural number can be written as a sum of at most four

Fig. 2 Claude Gaspard Bachet de Méziriac (1581–1638); source: [7]

Fig. 3 Pierre de Fermat (1601–1665); source: [8]

squares. This therefore came to be called **Bachet's conjecture**.

Fermat's contribution: the two squares theorem

Fermat was a lawyer by profession, but made numerous important contributions to mathematics, in fields such as probability theory, coordinate geometry, maxima-minima, optics and number theory. He often stated theorems without giving proofs. He studied Bachet's translation of Diophantus and worked on its problems. One of his remarkable claims, made in the margin of one of Bachet's books, was that the equation $a^n + b^n = c^n$ has no solutions in positive integers $a,\ b,\ c,\ n$ if $n > 2$. (See [1] for a review of the book [5] by Simon Singh which gives an account of this story.) An important result that Fermat found — which he *did* prove — had to do with natural numbers which can be written as sums of two squares. He had discovered a result now known as *Fermat's two squares theorem*.

The theorem says that *an odd prime p can be expressed as a sum of two squares if and only if it leaves remainder* 1 *when divided by* 4. For example: the primes 5, 13 and 17 can be written as sums of two squares, but 7, 11 and 19 need more than two squares. (Please check.) This observation had been made earlier (by Albert Girard, in 1632), but Fermat was the first to prove it. He announced the theorem in a letter to Marin Mersenne dated 25 December 1640, and for this reason it is sometimes called *Fermat's Christmas Theorem*.

Every natural number can be factored into a product of primes (in a unique way; this is the statement of the *Fundamental Theorem of Arithmetic*). Suppose that every prime in the factorization of a natural number N is a sum of two squares. Is N itself then a sum of two squares? The answer is yes, and this may be shown by using an interesting identity known as the *Brahmagupta identity* (see [10]) which states that for any natural number n,

$$\begin{aligned}(a^2 + nb^2)(c^2 + nd^2) \\ &= (ac - nbd)^2 + n(ad + bc)^2 \\ &= (ac + nbd)^2 + n(ad - bc)^2.\end{aligned}$$

The special case $n = 1$, which was known to Diophantus, states the following:

$$\begin{aligned}(a^2 + b^2)(c^2 + d^2) &= (ac - bd)^2 + (ad + bc)^2 \\ &= (ac + bd)^2 + (ad - bc)^2.\end{aligned}$$

It shows that a product of two numbers which are sums of two squares is itself a sum of two squares. For example, let $a = 2, b = 1, c = 3, d = 2$. Then from the relations

$$5 = 2^2 + 1^2, \quad 13 = 3^2 + 2^2$$

we find, by substitution, two different ways of writing $5 \times 13 = 65$ as a sum of two squares:

$$65 = 8^2 + 1^2 = 4^2 + 7^2.$$

Fermat's two squares theorem allows us to find an equivalent description of the natural numbers

that are sums of two squares. Let N be any natural number. Write N as k^2m where m is not divisible by any square number greater than 1. (Thus, k^2 is the largest square divisor of N.) *Then N is a sum of two squares if and only if every prime divisor of m leaves remainder* 1 *when divided by* 4. We illustrate this with two examples.

- Consider $N = 240 = 4^2 \times 3 \times 5$, for which $k^2 = 4^2$ and $m = 3 \times 5$. The presence of the '3' shows that this number cannot be written as a sum of two squares.
- Consider $N = 765 = 3^2 \times 5 \times 17$, for which $k^2 = 3^2$ and $m = 5 \times 17$. The primes which divide m (namely, 5 and 17) leave remainder 1 under division by 4. And indeed we have two such representations: $765 = 27^2 + 6^2 = 21^2 + 18^2$.

Lagrange's proof

It was Joseph Louis Lagrange (1736–1813), a brilliant Italian-born French mathematician and astronomer, who first proved the four squares theorem. Lagrange contributed not only to mathematics but also physics, specially classical mechanics. He served as the director of the Prussian Academy of Sciences for twenty years and won prizes for solving problems in astronomy posed by the French Academy of Sciences. A lunar crater is named after him, and his name appears amongst 72 names inscribed on the Eiffel tower! (See [3] and [9].)

We now mention the main steps in the proof of Lagrange's theorem. Ambitious students may want to complete the proof on their own, using the lemmas. Crucial to the proof is in an amazing identity for sums of four squares which is much like the Brahmagupta identity for sums of two squares. It was discovered by Euler and is called the *four squares identity*. It is easy to verify, but discovering it must have been quite an achievement! We state it as a lemma and leave its verification to you.

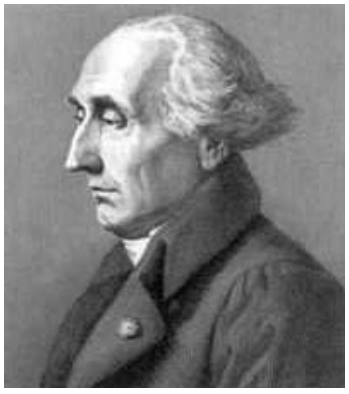

Fig. 4 Joseph Louis Lagrange (1736–1813); source: [9]

Lemma 1. For any numbers a, b, c, d and p, q, r, s we have:

$$\begin{aligned}(a^2+b^2+c^2+d^2)(p^2+q^2+r^2+s^2) &= (a\,p-b\,q-c\,r-d\,s)^2 \\ &\quad + (a\,q+b\,p+c\,s-d\,r)^2 \\ &\quad + (a\,r+c\,p+d\,q-b\,s)^2 \\ &\quad + (a\,s+d\,p+b\,r-c\,q)^2.\end{aligned}$$

The lemma tells us that the product of two numbers which are expressible as sums of at most four squares is itself expressible as a sum of at most four squares. Here is an instance of the identity: $31 = 5^2 + 2^2 + 1^2 + 1^2$, with $(a, b, c, d) = (5, 2, 1, 1)$; $71 = 7^2 + 3^2 + 3^2 + 2^2$, with $(p, q, r, s) = (7, 3, 3, 2)$; $31 \times 71 = 2201$; and $2201 = 24^2 + 28^2 + 21^2 + 20^2$.

Since every natural number can be written as a product of primes, Lemma 1 implies that if you can express each prime number as a sum of at most four squares, then you can express every natural number as a sum of at most four squares. As 2 is a sum of two squares, it only remains to prove that every odd prime p is a sum of at most four squares. This can be done by using the following sequence of lemmas:

Lemma 2. If n is even and is a sum of at most two squares, then so is $n/2$.

Lemma 3. If n is even and is a sum of at most four squares, then so is $n/2$.

Lemma 4. If p is an odd prime, then there exist integers a and b and an integer k, $0 < k < p$, such that $a^2 + b^2 + 1 = k\,p$.

Lemma 5. If p is an odd prime and there exists an integer $k_1 > 1$ such that $k_1 p$ is a sum of four squares, then there exists an integer $k_2 < k_1$ such that $k_2 p$ is a sum of four squares.

Of these, Lemmas 2 and 3 are not difficult to prove. (*Hint.* Simplify the expression $\left(\frac{1}{2}(x+y)\right)^2 + \left(\frac{1}{2}(x-y)\right)^2$.) Lemma 4 is proved using ideas from combinatorics (specifically, a principle called the 'pigeon hole principle'). Lemma 5 is the key step; it is called a *descent* step, as it allows us to 'descend' from a higher multiple of p to a lower multiple, and ultimately to p itself. The proofs of Lemmas 4 and 5 are fairly challenging.

Closing remarks

Lagrange's theorem led naturally to questions about writing the natural numbers as sums of fourth, fifth and higher powers; and this in turn led to a problem now known as *Waring's problem*, whose full story, spanning more than three centuries, involves many well known mathematicians including two from India: S S Pillai and R Balasubramanian.

In the computer algebra package *Mathematica* one can just type a command to get all decompositions of a natural number as a sum of squares or higher powers: the command PowersRepresentations[n, k, p] gives all representations of n as a sum of k non-negative p-th powers. A challenging exercise is to write this program and to get to know the powerful theorems that lie beneath it. The following theorem proved by Legendre (1752–1833) turns out to be handy: *A natural number is a sum of three squares if and only if it is not of the form* $4^k(8m+7)$.

Acknowledgements

I thank the editors for giving me an opportunity to write in *AtRiA*. Without Wikipedia, this article would not have got its colour!

References

[1] *At Right Angles*, A resource for school mathematics, Volume 1, Number 1, June 2012.
[2] Burton, David M. *Elementary Number Theory*. 2nd edition. W C Brown Publishers, Dubuque, IA, 1989.
[3] Bell, E. T. *Men of Mathematics*, New York, Simon and Schuster, 1965.
[4] Ore, O. *Number Theory and its History*, Dover, 1948.
[5] Singh, S. *Fermat's Last Theorem*, Harper Collins Paperback, 2002.
[6] http://en.wikipedia.org/wiki/Diophantus
[7] http://en.wikipedia.org/wiki/Claude_Gaspard_ Bachet_de_Méziriac
[8] http://en.wikipedia.org/wiki/Pierre_de_Fermat
[9] http://en.wikipedia.org/wiki/Joseph_Louis_ Lagrange
[10] http://en.wikipedia.org/wiki/Brahmagupta-Fibonacci_identity

ANURADHA S. GARGE did her Ph.D. from Pune University in 2008, on a problem related to the Waring problem. Currently she is Assistant Professor at the Centre for Excellence in Basic Sciences, Mumbai. She works in classical algebraic K-theory and commutative algebra. She also has an interest in Indian classical music. She may be contacted at anuradha@cbs.ac.in.