

ON THE REPRESENTATION OF NATURAL NUMBERS AS SUMS OF FOUR SQUARES

Titu Andreescu
Marian Tetiva

1. Introduction. The main character of the story told in this paper is one of the first truly spectacular results in modern number theory, namely *Lagrange's four-square theorem*. Such as many number theoretic results, this great theorem has a very simple statement, but a not-so-simple proof (actually, nowadays, many not-so-simple proofs).

Theorem 1. (*Lagrange's four-square theorem*) Any natural number (nonnegative integer) can be expressed as the sum of the squares of four natural numbers.

Thus we have $0 = 0^2 + 0^2 + 0^2 + 0^2$, $1 = 1^2 + 0^2 + 0^2 + 0^2$, $2 = 1^2 + 1^2 + 0^2 + 0^2$, $3 = 1^2 + 1^2 + 1^2 + 0^2$, $4 = 1^2 + 1^2 + 1^2 + 1^2$, $20 = 4^2 + 2^2 + 0^2 + 0^2$, $77 = 8^2 + 3^2 + 2^2 + 0^2$, and so on. In general, the representation of a natural number as a sum four squares is not unique, for instance we also have $77 = 6^2 + 6^2 + 2^2 + 1^2$ (not to speak of the possibilities to change the order of summands).

Bachet formulated the theorem in his translation from 1621 of Diophantus's book *Arithmetica* (note that the validity of the result has been observed by Diophantus himself in particular cases), and the first proof came from Lagrange in 1770. Numerous proofs, generalizations, and related results appeared later on. In this paper we intend to show two of these proofs: the classical proof of Lagrange (in a modern form), and another one in which the pigeonhole principle plays a very important role, being used not less than four times. In both proofs the following identity of Euler will be used.

Lema 2. (*Euler's four-square identity*) For any numbers $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4$ the equality

$$\begin{aligned} & (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = \\ &= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 + \\ &+ (x_1y_3 - x_2y_4 - x_3y_1 + x_4y_2)^2 + (x_1y_4 + x_2y_3 - x_3y_2 - x_4y_1)^2 \end{aligned}$$

holds.

Proof. We leave the proof mostly to the reader, as it only relies on straightforward algebraic computations. By using the well-known identity

$$(x + y + z + t)^2 = x^2 + y^2 + z^2 + t^2 + 2xy + 2xz + 2xt + 2yt + 2yz + 2zt$$

for each parenthesis from the right-hand side, after cancellations we will remain only with the sixteen terms of the form $x_i^2y_j^2$, with $i, j \in \{1, 2, 3, 4\}$, and then a pretty obvious factorization will yield the product from the left-hand side. (We do not discuss here the fact that this identity basically represents the multiplicative property of the norm of the quaternions, or that it holds for any elements $x_1, \dots, x_4, y_1, \dots, y_4$ from a commutative ring—with the same proof by direct computations.) Clearly, Euler's four-square identity shows that the product of two sums of four squares of natural numbers is also a sum of the squares of four natural numbers (we do not forget that $x^2 = |x|^2$ for any real number x), which easily extends, by induction, to the fact that a product of any number of sums of four squares is also a sum of four squares. Consequently, because 0 and 1 are evidently sums of four squares, and any natural number greater than 1 is a product of primes (by the fundamental theorem of arithmetic), theorem 1 would be demonstrated if we proved the following result (which can be considered the very core of Lagrange's four-square theorem).

Theorem 3. Any prime can be represented as the sum of the squares of four natural numbers.

For instance, knowing the representations $7 = 2^2 + 1^2 + 1^2 + 1^2$ and $11 = 3^2 + 1^2 + 1^2 + 0^2$, we get (via Euler's four-square identity) the representation as a sum of four squares of the product $77 = 7 \cdot 11$, namely we have

$$77 = 7 \cdot 11 = (2^2 + 1^2 + 1^2 + 1^2)(3^2 + 1^2 + 1^2 + 0^2) = 8^2 + 2^2 + 0^2 + 3^2.$$

Thus we further focus on proving (in two ways) that any prime can be written as a sum of four squares.

2. First proof of theorem 3. Since $2 = 1^2 + 1^2 + 0^2 + 0^2$ is, clearly, expressible as a sum of four squares it is enough to show that any odd prime p can be written as a sum of four squares (actually this is the statement for which we provide two proofs). We start with a helping result.

Lemma 4. Let p be an odd prime. Then a positive multiple of p that can be represented as a sum of four squares exists. Moreover, we can find such a multiple np with $1 \leq n < p$.

Proof. We first notice that the numbers j^2 , with j running through the set $\left\{0, 1, \dots, \frac{p-1}{2}\right\}$ yield different remainders when divided by p . Indeed, if we could find $j_1, j_2 \in \left\{0, 1, \dots, \frac{p-1}{2}\right\}$ such that $j_1^2 \equiv j_2^2 \pmod{p}$, then p would divide $j_1^2 - j_2^2 = (j_1 - j_2)(j_1 + j_2)$, hence p would divide one of the factors $j_1 - j_2, j_1 + j_2$. If p divided $j_1 - j_2$, since

$$|j_1 - j_2| \leq \frac{p-1}{2} - \left(-\frac{p-1}{2}\right) = p-1,$$

it would necessarily follow that $j_1 - j_2 = 0$, that is, $j_1 = j_2$. Also, since

$$0 \leq j_1 + j_2 \leq \frac{p-1}{2} + \frac{p-1}{2} = p-1,$$

if p divided $j_1 + j_2$, the only possibility would be that $j_1 = j_2 = 0$. Thus the assumption that j_1^2 and j_2^2 give the same remainder when divided by p leads, anyway, to $j_1 = j_2$, consequently all the remainders when divided by p of the numbers from the set

$$A = \left\{j^2 : j = 0, 1, \dots, \frac{p-1}{2}\right\}$$

are distinct. Similarly, the remainders of the numbers from the set

$$B = \left\{-k^2 - 1 : k = 0, 1, \dots, \frac{p-1}{2}\right\}$$

when divided by p are distinct. Since there are only p possible remainders at division by p , and there are $p+1$ numbers in the union $A \cup B$, by the pigeonhole principle we infer that necessarily one number from A and one number from B have equal remainders when divided by p . Thus, there exist $j, k \in \left\{0, 1, \dots, \frac{p-1}{2}\right\}$ such that j^2 and $-k^2 - 1$ produce equal remainders when divided by p , which shows that $j^2 + k^2 + 1$ is divisible by p , meaning that p has positive multiple (namely $j^2 + k^2 + 1$) which is representable as the sum of four squares (one of the squares being 0). The particular form $j^2 + k^2 + 1$ of this multiple of p is important, as we will see, in the second proof. For now, it only matters that this multiple is positive, and moreover, it is important that for the positive integer n having the property that $np = j^2 + k^2 + 1$ we also have

$$np = j^2 + k^2 + 1 \leq 2 \left(\frac{p-1}{2}\right)^2 + 1 < (p-1)(p+1) + 1 = p^2,$$

therefore we have $1 \leq n < p$. It is now time for the first proof.

The first proof of theorem 3. We saw that we only need to show that an odd prime p can be written as a sum of four squares. By the previous lemma, there exist positive multiples np of p that are representable as sums of four squares, and such that $1 \leq n < p$. Let mp be the smallest such positive multiple of p , which is a sum of four squares. Clearly, we also have $1 \leq m < p$, and if $m = 1$ the proof is done, so we can assume further that $1 < m < p$. We intend to show further that (when $m > 1$) another such multiple m_1p of p exists, with $1 \leq m_1 < m < p$ —which will contradict the minimality of m (so $m = 1$ is the only possibility for the smallest m , finishing the proof).

To this purpose assume first that $mp = a_1^2 + a_2^2 + a_3^2 + a_4^2$ for some natural numbers a_1, a_2, a_3, a_4 , and $1 < m < p$ also a natural number. If m is even we immediately see that we cannot have three odd numbers and one even number, nor can we have three even numbers and one odd number among a_1, a_2, a_3, a_4 (since in both of these cases $a_1^2 + a_2^2 + a_3^2 + a_4^2$ is odd), therefore either a_1, a_2, a_3, a_4 have all the same parity, or among them there are two even and two odd numbers. In any of these situations, among a_1, a_2, a_3, a_4 there exist two numbers of the same parity, and the two others also have the same parity (not necessarily the same as the parity of the first two). Due to symmetry, there is no loss of generality if we assume that a_1, a_2 have the same parity, and a_3, a_4 also have the same parity (not necessarily the same as the parity of a_1, a_2). We then get that

$$\frac{m}{2}p = \left(\frac{a_1 + a_2}{2}\right)^2 + \left(\frac{a_1 - a_2}{2}\right)^2 + \left(\frac{a_3 + a_4}{2}\right)^2 + \left(\frac{a_3 - a_4}{2}\right)^2$$

is the sum of the squares of four natural numbers, so we found $m_1 = \frac{m}{2}$ for which m_1p is a sum of four squares, and $1 \leq m_1 < m$, and thus the case of even m is solved.

From now on we consider $m > 1$ and odd. One variant of the division theorem ensures that there exist integers b_1, b_2, b_3, b_4 such that

$$b_i \equiv a_i \pmod{m} \quad \text{and} \quad |b_i| \leq \frac{m-1}{2}$$

for any $i \in \{1, 2, 3, 4\}$. We then have

$$b_1^2 + b_2^2 + b_3^2 + b_4^2 \equiv a_1^2 + a_2^2 + a_3^2 + a_4^2 = mp \equiv 0 \pmod{m},$$

therefore $b_1^2 + b_2^2 + b_3^2 + b_4^2$ is a multiple of m . Say, for instance, that $b_1^2 + b_2^2 + b_3^2 + b_4^2 = m_1m$ for some natural number m_1 . This m_1 cannot be 0, otherwise we would have $b_1^2 + b_2^2 + b_3^2 + b_4^2 = 0$, hence $b_1 = b_2 = b_3 = b_4 = 0$. But this would imply $a_i \equiv 0 \pmod{m}$ for all $i \in \{1, 2, 3, 4\}$, meaning that $mp = a_1^2 + a_2^2 + a_3^2 + a_4^2$ would be divisible by m^2 , that is, p would be divisible by m , which is impossible for $1 < m < p$ —and the contradiction thus obtained shows that $m_1 \geq 1$. We also have

$$m_1m = b_1^2 + b_2^2 + b_3^2 + b_4^2 \leq 4 \left(\frac{m-1}{2}\right)^2 = (m-1)^2 < m^2,$$

and we thus obtain $1 \leq m_1 < m$.

On the other hand, according to lemma 2, we have

$$m^2m_1p = (a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = c_1^2 + c_2^2 + c_3^2 + c_4^2,$$

where

$$\begin{aligned} c_1 &= a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4, & c_2 &= a_1b_2 - a_2b_1 + a_3b_4 - a_4b_3, \\ c_3 &= a_1b_3 - a_2b_4 - a_3b_1 + a_4b_2, & c_4 &= a_1b_4 + a_2b_3 - a_3b_2 - a_4b_1. \end{aligned}$$

By using the congruences $b_i \equiv a_i \pmod{m}$ (for $i = 1, 2, 3, 4$) we get

$$c_1 \equiv a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 0 \pmod{m},$$

$$c_2 \equiv a_1a_2 - a_2a_1 + a_3a_4 - a_4a_3 = 0 \pmod{m},$$

$$c_3 \equiv a_1a_3 - a_2a_4 - a_3a_1 + a_4a_2 = 0 \pmod{m}$$

and

$$c_4 \equiv a_1a_4 + a_2a_3 - a_3a_2 - a_4a_1 = 0 \pmod{m},$$

and hence c_1, c_2, c_3, c_4 are all divisible by m . Then the equality $m^2m_1p = c_1^2 + c_2^2 + c_3^2 + c_4^2$ written as

$$m_1p = \left(\frac{c_1}{m}\right)^2 + \left(\frac{c_2}{m}\right)^2 + \left(\frac{c_3}{m}\right)^2 + \left(\frac{c_4}{m}\right)^2$$

shows that m_1p is a multiple of p with $1 \leq m_1 < m$, and which can be written as the sum of the squares of four natural numbers, which solves the case of odd m too, thus completing the proof.

The reasoning can also be formulated as follows. We do not necessarily start with *the smallest* positive multiple of p that can be expressed as a sum of four squares, but rather with an arbitrary such multiple. Anyway, if $1 < m < p$, we find another multiple m_1p of p which is a sum of four squares, and for which $1 \leq m_1 < m$ (the minimality of m is not used in the above proof). If $m_1 = 1$, then the proof is done; otherwise we analogously find some $1 \leq m_2 < m_1$ such that m_2p is the sum of four squares, and so on. We thus get a strictly decreasing sequence $m = m_0 > m_1 > m_2 > \dots$ of positive integers for which each m_jp is a sum of four squares, and m_{j+1} can be found whenever $m_j > 1$. Nevertheless, a sequence of positive integers cannot decrease indefinitely, therefore some j must exist for which we have $m_j = 1$, meaning that p is a sum of four squares, as we intended to prove. This is a classical example of applying Fermat's *method of infinite descent*, in both of the above variants.

Example 5. Let $p = 19$. The numbers from the set $A = \{j^2 : j = 0, 1, \dots, 9\}$ yield, when divided by 19 the remainders 0, 1, 4, 9, 16, 6, 17, 11, 7, 5 respectively. Also, the numbers from $B = \{-k^2 - 1 : k = 0, 1, \dots, 9\}$ produce, when divided by 19, the remainders 18, 17, 14, 9, 2, 12, 1, 7, 11, 13 respectively. (Note that A and B are the sets from the proof of lemma 4.) We immediately see that 3^2 and $-3^2 - 1$ have the same remainder (namely 9) when divided by 19, meaning that $3^2 + 3^2 + 1$ is a multiple of 19, which actually gives the representation of 19 as a sum of two squares: $19 = 3^2 + 3^2 + 1^2 + 0^2$.

Assume now (for the sake of the example) that we start with the observation that 7^2 and $-8^2 - 1$ yield the same remainder when divided by 19 (namely the remainder 11), which tells us that $8^2 + 7^2 + 1$ is divisible by 19. Indeed, we see that $8^2 + 7^2 + 1 = 6 \cdot 19$ hence, as 6 is even, we infer the equality $3 \cdot 19 = 4^2 + 4^2 + 4^2 + 3^2$, where (with the notations from the proof above) $m = 3$ is now odd and we have $a_1 = a_2 = a_3 = 4$, $a_4 = 3$. Reducing modulo 3 (to remainders from the set $\{-1, 0, 1\}$, although here this is not important, since there is no remainder of 2, or, equivalently, -1) we find $b_1 = b_2 = b_3 = 1$, $b_4 = 0$, and $m_1 = 1$, that is, we find the equality $1 \cdot 3 = 1^2 + 1^2 + 1^2 + 0^2$. We can calculate now $c_1 = 12 = 3 \cdot 4$, $c_2 = -3 = 3 \cdot (-1)$, $c_3 = 3 = 3 \cdot 1$, $c_4 = -3 = 3 \cdot (-1)$, therefore we get the equality

$$3^2 \cdot 19 = (4^2 + 4^2 + 4^2 + 3^2)(1^2 + 1^2 + 1^2 + 0^2) = 3^2 \cdot 4^2 + 3^2 \cdot 1^2 + 3^2 \cdot 1^2 + 3^2 \cdot 1^2,$$

equivalent to the representation $19 = 4^2 + 1^2 + 1^2 + 1^2$.

We still note that we can arrive to the same result by reducing modulo 6 the a_i s from the equality $6 \cdot 19 = 8^2 + 7^2 + 1^2$ (considering thus that $m = 6$, even though it is even, and $a_1 = 8$, $a_2 = 7$, $a_3 = 1$, $a_4 = 0$) in order to get $b_1 = 2$, $b_2 = b_3 = 1$, $b_4 = 0$, and $m_1 = 1$, that is, the equality $1 \cdot 6 = 2^2 + 1^2 + 1^2 + 0^2$. Then we find $c_1 = 24 = 6 \cdot 4$, $c_2 = c_3 = c_4 = 6 = 6 \cdot 1$, and hence we get

$$6^2 \cdot 19 = 6^2 \cdot 4^2 + 6^2 \cdot 1^2 + 6^2 \cdot 1^2 + 6^2 \cdot 1^2,$$

giving the same representation of 19 as a sum of four squares.

Exercise 6. We invite the reader to proceed similarly with $p = 29$, that is to find an m_1 smaller than m starting (in turn) from the equalities $13^2 + 2^2 + 1 = 6 \cdot 29$ ($m = 6$) and

$9 \cdot 29 = 14^2 + 8^2 + 1$ ($m = 9$) by following the algorithm from the proof. The final goal is, of course, to find a representation of 29 as a sum of squares.

3. Four times the pigeonhole principle: the second proof of theorem 3. We intend thus to show once more that an odd prime p can be written as the sum of the squares of four natural numbers. We will again rely on lemma 4, where we first used the pigeonhole principle. We will use it again in the proof of the following helping result.

Lemma 7. Let a and b be two integers. Then integers x, y, w, z exist such that they are not all equal to 0, they have absolute values less than $\sqrt{p}$, and they verify the simultaneous congruences

$$x \equiv aw + bz \pmod{p} \quad \text{and} \quad y \equiv bw - az \pmod{p}.$$

Proof. Consider the pairs of numbers of the form $(k - am - bn, l - bm + an)$, where k, l, m, n independently run through the set $\{0, 1, \dots, \lfloor \sqrt{p} \rfloor\}$ ($\lfloor t \rfloor$ being the integral part of the real number t). Their number is $(\lfloor \sqrt{p} \rfloor + 1)^4$, so (since $(\lfloor \sqrt{p} \rfloor + 1)^4 > (\sqrt{p})^4 = p^2$) there are more such pairs than the pairs of remainders at division by p . The pigeonhole principle (as we said) applies and ensures that we can find two pairs $(k_1 - am_1 - bn_1, l_1 - bm_1 + an_1)$ and $(k_2 - am_2 - bn_2, l_2 - bm_2 + an_2)$ for which both congruences

$$k_1 - am_1 - bn_1 \equiv k_2 - am_2 - bn_2 \pmod{p}$$

and

$$l_1 - bm_1 + an_1 \equiv l_2 - bm_2 + an_2 \pmod{p}$$

hold. It is clear now that the numbers $x = k_1 - k_2$, $y = l_1 - l_2$, $w = m_1 - m_2$, and $z = n_1 - n_2$ are integers, not all equal to 0 (as the quadruples (k_1, l_1, m_1, n_1) and (k_2, l_2, m_2, n_2) are distinct), their absolute values are $\leq \lfloor \sqrt{p} \rfloor < \sqrt{p}$, and they verify the desired congruences

$$x \equiv aw + bz \pmod{p} \quad \text{and} \quad y \equiv bw - az \pmod{p}.$$

The second proof of theorem 3. By lemma 4, the natural numbers a and b do exist such that $a^2 + b^2 + 1 \equiv 0 \pmod{p}$. According to lemma 7, for these a and b , there exist integers x, y, w, z , not all equal to 0, having absolute values lesser than $\sqrt{p}$, and for which we have

$$x \equiv aw + bz \pmod{p} \quad \text{and} \quad y \equiv bw - az \pmod{p}.$$

Consequently

$$x^2 + y^2 \equiv (aw + bz)^2 + (bw - az)^2 = (a^2 + b^2)(w^2 + z^2) \equiv -(w^2 + z^2) \pmod{p}$$

(because $a^2 + b^2 \equiv -1 \pmod{p}$). Thus $x^2 + y^2 + w^2 + z^2 \equiv 0 \pmod{p}$, thus $x^2 + y^2 + w^2 + z^2$ is a positive multiple of p , which is obviously a sum of four squares, and is lesser than $4p$, since

$$x^2 + y^2 + w^2 + z^2 < 4(\sqrt{p})^2 = 4p.$$

In other words, we just showed that one of the numbers $p, 2p, 3p$ is a sum of four squares. If p is a sum of four squares, there is nothing else to prove, so we remain with two cases.

Consider first that $2p$ is the sum of four squares, say $2p = x^2 + y^2 + w^2 + z^2$ (we keep this notation, hoping that no confusion is possible). Then (the pigeonhole principle again) at least two among x, y, w, z have the same parity. Without loss of generality we may assume that x and y have the same parity, hence (since $x^2 + y^2 + w^2 + z^2 = 2p$ is even) w and z also have both the same parity (not necessarily the same as the parity of x and y). But then we have

$$p = \frac{x^2 + y^2 + w^2 + z^2}{2} = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{w+z}{2}\right)^2 + \left(\frac{w-z}{2}\right)^2,$$

meaning that p is a sum of four squares, as desired. (We recognize here, in a slightly different form, the argument from the first proof in the case when an even multiple of p is expressible as a sum of four squares.)

Finally, let $3p = x^2 + y^2 + w^2 + z^2$ be a sum of four squares (again, we do not change the notation anymore). As we know, any square u^2 leaves when divided by 3 a remainder of 0 or 1 (according to whether u is, or is not divisible by 3), hence (the pigeonhole principle for the fourth time) at least two of the four squares x^2, y^2, z^2, w^2 yield the same remainder when divided by 3. Because $x^2 + y^2 + w^2 + z^2$ is divisible by 3, if two of the four squares give remainder 0 when divided by 3, then it is clear that all of the four squares must give remainder 0 when divided by 3 (and hence in this subcase all of x, y, w, z are divisible by 3), while if two of the four square give remainder 1 when divided by 3, then one of the other two leaves remainder 1 when divided by 3, and the other is divisible by 3.

In the first subcase it follows that $3p = x^2 + y^2 + w^2 + z^2$ is divisible by 9, which implies that p is divisible by 3, that is (being a prime) p is actually equal to 3. Since $3 = 1^2 + 1^2 + 1^2 + 0^2$ is a sum of four squares, this first subcase is solved.

In the second subcase we can assume (without loss of generality) that x^2 is divisible by 3 (thus x itself is divisible by 3), while y^2, w^2, z^2 give remainder 1 when divided by 3, meaning that each of y, w, z is congruent either to 1, or to -1 modulo 3. We can actually consider that any of y, w, z is congruent to 1 modulo 3 (since if, for example, $y \equiv -1 \pmod{3}$, then we can replace y with $-y \equiv 1 \pmod{3}$). Thus we can assume that $x \equiv 0 \pmod{3}$ and $y \equiv w \equiv z \equiv 1 \pmod{3}$. But then p can be written as a sum of four squares in the form

$$p = \left(\frac{y + w + z}{3}\right)^2 + \left(\frac{x + y - w}{3}\right)^2 + \left(\frac{x + w - z}{3}\right)^2 + \left(\frac{x + z - y}{3}\right)^2,$$

where all fractions are integers due to the above congruences, and if one of these fractions is negative, we can replace it with its opposite (additive inverse) in order to make it a natural number. The proof is now complete.

Of course, the last two applications of the pigeonhole principle can be avoided, by simply examining the sum of four squares modulo 2, and modulo 3 respectively, but using the principle makes this examination more elegant. On the other hand, we really need the pigeonhole principle in the proofs of lemmas 4 and 7, and its well-known importance in the whole mathematics is once more underlined by this second proof of Lagrange's four-square theorem.

4. Last but not (at all) least. We only remind in this closing paragraph a few related results among which the two-squares theorem (stated by Fermat, and first proved by Euler) and Legendre's three-square theorem are most prominent.

Theorem 8. (*Euler-Fermat two-square theorem*) A natural number N can be expressed as the sum of the squares of two natural numbers if and only if $N = 0$, or $N = 1$, or $N > 1$ and any prime factor of the form $4k + 3$ from the prime factorization of N appears in this factorization with an even exponent.

For instance, $80 = 2^4 \cdot 5$, or $180 = 2^2 \cdot 3^2 \cdot 5$ can be represented as sums of two squares (as the exponents of the primes of the form $4k + 3$ in their factorizations are even; and, indeed, we have $80 = 8^2 + 4^2$, and $180 = 12^2 + 6^2$), while numbers such as 7, $21 = 3 \cdot 7$, $35 = 5 \cdot 7$, or $440 = 2^3 \cdot 5 \cdot 11$ are not sums of two squares.

Theorem 9. (*Legendre's three-square theorem*) A natural number N can be represented as the sum of the squares of three natural numbers if and only if N is not of the form $4^l(8m + 7)$ for some natural numbers l and m .

Thus the first natural numbers that can be written as sums of three squares are $0 = 0^2 + 0^2 + 0^2$, $1 = 1^2 + 0^2 + 0^2$, $2 = 1^2 + 1^2 + 0^2$, $3 = 1^2 + 1^2 + 1^2$, $4 = 2^2 + 0^2 + 0^2$, $5 = 2^2 + 1^2 + 0^2$, $6 = 2^2 + 1^2 + 1^2$, while the first that cannot be thus written is 7. Then 8, 9, 10, 11, 12, 13, 14 are all sums of three squares (see how), but 15 is not, and so on. We do not intend to deal with these results in here, although the first one can be proved in an elementary manner (which doesn't

mean simple). Instead, such an elementary proof for Legendre's theorem does not exist for now and it will never exist, probably, unless we change the meaning of the word "elementary". We included its statement in our paper due to its remarkable beauty, and in order to invite the interested reader to prove Lagrange's four-square theorem by using it. It can also be used to prove another beautiful result about the representation of natural numbers as sums of certain type of numbers which is akin to the four-squares theorem, both of them being instances of the polygonal number theorem stating that any natural number is the sum of at most n polygonal numbers of order n (or n -gonal numbers). The polygonal number theorem was also formulated by Fermat, and it was completely proved only in 1813 by Cauchy.

Exercise 10. Prove Lagrange's four-square theorem by using Legendre's three-square theorem.

Exercise 11. Prove (also by relying on Legendre's theorem) Euler's "Eureka" theorem, namely prove that any natural number can be expressed as the sum of (at most) three triangular numbers.

On the day he succeeded in proving this result, Euler wrote in his diary: "Eureka! Num= $\Delta + \Delta + \Delta$." Any of the Δ s from his note represents, of course, a triangular number. We remind that the triangular numbers are those of the form

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}, \quad k \in \mathbb{N},$$

and thus their sequence starts 0, 1, 3, 6, 10, 15, 21, etc. For example, we have $23 = 21 + 1 + 1$, and $99 = 78 + 21 + 0$.

We end our paper with a somehow more complicated exercise, whose proof also uses Legendre's three-square theorem. The interested reader can find its proof in [1].

Exercise 12. Show that the positive integers that can *not* be written as sums of four *strictly positive* squares are: 1, 3, 5, 9, 11, 17, 29, 41, and those having one of the forms $2 \cdot 4^n$, $6 \cdot 4^n$, or $14 \cdot 4^n$ for some natural number n . In other words, these are the numbers in whose representation as a sum of four squares at least one $0 (= 0^2)$ must occur.

References

1. J. H. Conway: *The Sensual Quadratic Form*, Mathematical Association of America, 1997
2. W. Sierpinski: *Elementary Theory of Numbers*, North Holland, 1988
3. https://en.wikipedia.org/wiki/Lagrange%27s_four-square_theorem