Euler's work on four square identity and related properties regarding prime numbers and partitioning into squares

Aarush Garg

August 2023

1 Introduction

This paper discusses the development of Lagrange's four square theorem as well as Euler's importance towards influencing this through the four square identity and related theorems. The paper also includes the extension of Euler's work into modern day usage and identities in matrices in real life. In this paper, the works of modern mathematicians' extension of Euler's and Lagrange's work are discussed, with reference to papers [Eul08], [LG18], [Leh48], [PF09]

2 Euler's four square identity

Theorem 1. *This is one of the key identities that Lagrange used in proving the four square theorem. The theorem is as follows:*

$$XY = (a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2), X, Y \in Z.$$

Proof. The proof begins as follows. First, the values of α and β are assigned.

$$\alpha = a_1 + a_2 i + a_3 j + a_4 k$$

$$\beta = b_1 + b_2 i + b_3 j + b_4 k.$$

He then uses the quaternion conjugate of this pair of quaternions. A quaternion is essentially a 4 dimensional vector as written above, with a constant term, and i, j, k vector directions. The quaternion conjugate of α and β are α^* and β^* respectively where they follow the general rule of conjugates. Thus we have

$$\alpha^* = a_1 - a_2 i - a_3 j - a_4 k$$

$$\beta^* = b_1 - b_2 i - b_3 j - b_4 k$$

Using the definition of conjugates, the computation of $\alpha\alpha^*$ and $\beta\beta^*$ is $a_1^2+a_2^2+a_3^2+a_4^2$ and $b_1^2+b_2^2+b_3^2+b_4^2$ respectively.

Let's assign $\alpha\alpha^*$ and $\beta\beta^*$ to X and Y respectively. Thus we get:

$$XY = \alpha\alpha^*\beta\beta^*$$

Due to the associative property of quaternions, as 4 dimensional vectors, the following equation is derived

$$XY = \alpha\beta(\alpha\beta)^*$$

Using the substitution $\gamma = \alpha\beta$, gives: $XY = \gamma\gamma*$

$$\gamma = (a_1 + \langle a_2, a_3, a_4\rangle)(b_1 + \langle b_2, b_3, b_4\rangle)$$

Using Hamilton product, the following can be observed:

$$\begin{aligned}\gamma = (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4) + (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)i+\\ (a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)j + (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)k\end{aligned}$$

$$\begin{aligned}\gamma^* = (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4) - (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)i-\\ (a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)j - (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)k\end{aligned}$$

Thus, since $XY = \gamma\gamma^*$, the equation below follows:

$$\begin{aligned}XY = (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4)^2 + (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)^2+\\ (a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)^2 + (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)^2\end{aligned}$$

Thus the equation below has been proved:

$$\begin{aligned}(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4)^2\\ +(a_1b_2+a_2b_1+a_3b_4-a_4b_3)^2+(a_1b_3-a_2b_4+a_3b_1+a_4b_2)^2+(a_1b_4+a_2b_3-a_3b_2+a_4b_1)^2\end{aligned}$$

□

3 Extension of Euler's four square identity to Lagrange's four square theorem

Lagrange's four square theorem proves that any positive integer can be written as the sum of four square numbers. This can be done building upon Euler's identity. First Lagrange explored the fact that all prime numbers can be written as the sum of four squares. This was done by using the pigeonhole theorem and modular arithmetic as follows:

3.1 Case 1: Proof for Composite numbers

It starts as follows:

Theorem 2. $mp = a^2 + b^2 + c^2 + d^2$

Proof. Since p is odd, $\frac{p-1}{2}$ is an integer, and there are $\frac{p+1}{2}$ integers between 0 and $\frac{p-1}{2}$ inclusive.
Choose any arbitrary number f_p from this range and let's say $f_p^2 \equiv r_p \pmod{p}$

For sake of contradiction assume: that for two distinct integers a_i and a_j in the range 0 to ($\frac{p-1}{2}$, their square has the same remainder r_p when divided by p.

We get:

$$a_i^2 - a_j^2 = (q_i - q_j)p$$

This means p is a divisor of $(a_i - a_j)(a_i + a_j)$
By Euclid's lemma for prime factors, $p|(a_i - a_j)$ or $p|(a_i + a_j)$. But since a_i and a_j are both less than $\frac{p-1}{2}$, $a_i + a_j$ is at max $p - 1$ and thus it can not be divisible by p, thus giving us a contradiction. Hence the above is impossible.
$\forall r_i, s_i = p - (r_i + 1)$
Thus we have $\frac{p+1}{2}$ positive distinct integers s_i such that $0 < s_i < p - 1$

But some r_i and s_i must be the same using pigeonhole principle, as there are $\frac{p+1}{2}$ of r_i and $\frac{p+1}{2}$ of s_i, thus giving p+1 possible values of r_i and s_i all of which are in the range $0 < r_i < p - 1$ and $0 < s_i < p - 1$, thus at least $\lceil \frac{n+1}{n-1} \rceil = 2$ of them have to be the same.
So let's choose the case where r = s

By construction we have $0 < a, b < \frac{p-1}{2}$

$$a^2 = q_1 p + r$$
$$b^2 = q_2 p + r'$$
$$s = p - (r' + 1)$$

Adding these together gives

$$a^2 + b^2 + s = q_1 p + r + q_2 p + p - 1$$

But since r=s, we get for a particular r and s,

$$a^2 + b^2 = q_1 p + q_2 p + p - 1$$

$$a^2 + b^2 + 1 = p(q_1 + q_2) = p(m), m = q_1 + q_2, m \in Z$$

Thus $mp = a^2 + b^2 + 1^2 + 0^2$ and is the sum of four squares

This satisfies only when m is not equal to 1, i.e all composite numbers. Thus we must now prove the case for prime numbers to complete the proof.

□

3.2 Case 2: Proof for Prime numbers

Since we have established that all composite numbers of form mp, where m is not equal to 1, are the sum of 4 squares all that is left to do is prove that primes are the sum of four squares.

From the previous part, we have the following equation:

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

Theorem 3. *Let's assume for sake of contradiction that m is an even number. In this case we have:*

$$\frac{m}{2}p = (\frac{x_1 + x_2}{2})^2 + (\frac{x_1 - x_2}{2})^2 + (\frac{x_3 + x_4}{2})^2 + (\frac{x_3 - x_4}{2})^2$$

Proof. As we know that the parity of a number and its square are the same, this means that there must be an even number of numbers x_1 through x_4 that must have even parity (i.e 0,2 or 4 of them must be even). When either all of them are even (4 even) or all of them are odd (0 even), then the pairs $x_1 + x_2$, $x_1 - x_2$, $x_3 + x_4$, $x_3 - x_4$, are all even and thus the sum must be even. In the case where 2 are even and 2 are odd, if the pairs are such that x_1 and x_2 are of same parity and x_3 and x_4 are of same parity, then once again we end up with a desired result. But if they are not, then the problem arises that $\frac{mp}{2}$ is not even, as all numbers are of form $\frac{2k+1}{4}, k \in Z$. This does not work, as mp is not an integer in this case. Thus, since we want $\frac{mp}{2}$ even for contradiction, the only cases which are allowed are listed above. But the contradiction follows that $m > \frac{m}{2}$ and thus m is not the smallest number, such that mp can be written as sum of four squares.

Thus, by contradiction m must be odd. Now let's assume once again for sake of contradiction that is $m > 1$.

Once again, we have:

$$\frac{m}{2}p = (\frac{x_1 + x_2}{2})^2 + (\frac{x_1 - x_2}{2})^2 + (\frac{x_3 + x_4}{2})^2 + (\frac{x_3 - x_4}{2})^2$$

Divide each x_i by m, to obtain a remainder r_i, such that $0 <= r_i <= m-1$. Thus we define y_i as follows:

$$y_i = r_i : 0 <= r_i <= \frac{m-1}{2}$$

$$y_i = r_i - m : \frac{m+1}{2} <= r_i <= m - 1$$

Thus, we get $x_i = q_i m + y_i$, where $\frac{-m-1}{2} <= y_i <= \frac{m-1}{2}$. Thus we have $y_i = x_i - q_i m$.

$y_1^2 + y_2^2 + y_3^2 + y_4^2 = x_1^2 + x_2^2 + x_3^2 + x_4^2 - 2m(x_1q_1 + x_2q_2 + x_3q_3 + x_4q_4) + m^2(q_1^2 + q_2^2 + q_3^2 + q_4^2) = mn$

,where $n \in Z$.

Thus assume for contradiction n = 0: but this means that all y's are zero and x's are divisible by m, but that means $m|p$, but this is impossible, as $1 < m < p$. Thus n is not equal to zero.

Thus we get the following equation:

$$mn = y_1^2 + y_2^2 + y_3^2 + y_4^2 < 4(\frac{m}{2})^2 = m^2$$

Using the equation for mp, and mn, we get:

$$m^2np = (y_1^2 + y_2^2 + y_3^2 + y_4^2)(x_1^2 + x_2^2 + x_3^2 + x_4^2)$$

Using Euler's four square identity, we get:

$$\begin{aligned} m^2np = {} & (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 - x_3y_4 + x_4y_3)^2 \\ & + (x_1y_3 + x_2y_4 - x_3y_1 - x_4y_2)^2 + (x_1y_4 - x_2y_3 + x_3y_2 - x_4y_1)^2. \end{aligned}$$

Each of these numbers are all multiples of m, as can be seen by some manipulation using the definition of q_i. Thus we get:

$$m^2np = (mz_3)^2 + (mz_3)^2 + (mz_3)^2 + (mz_3)^2$$

Thus we get the following when dividing by m^2

$$np = z_1^2 + z_2^2 + z_3^2 + z_4^2$$

, where $1 <= n < m$, but this contradict the minimality of m, as n satisfies the equation as well. Thus we must have m = 1, and p can be expressed as the sum of 4 squares. □

4 Prime numbers and four squares

Lagrange goes on to further prove that if 2 sums of 2 squares: (i.e $p^2 + q^2$ and $r^2 + s^2$ share a common factor, δ, which is not a divisor of any of the individual squares, then δ, $\frac{p^2+q^2}{\delta}$, and $\frac{r^2+s^2}{\delta}$ can also be written as sum of four squares.

Theorem 4. *The proposition thus follows that if $p^2 + q^2 + r^2 + s^2 = ab$, then a and b themselves can be written as the sum of four squares.*

Euler shows the proof in the paper:

He splits into two cases:
1. Case where $p^2 + q^2$ and $r^2 + s^2$ have a common factor δ
2. Case where $p^2 + q^2$ and $r^2 + s^2$ do not have a common factor

4.1 Defining example

An example of this case is to take $p = 2, q = 4$ and $r = 6, q = 8$.

$p^2 + q^2 = 20$
$r^2 + s^2 = 80$
In this case we have a common factor $\delta = 20$.

$$AB = \frac{p^2 + q^2}{\delta} + \frac{r^2 + s^2}{\delta}$$

In this case, since we know that all numbers can be written as the sum of four squares, this means that we must have 80/20 and 20/20 written as the sum of four squares.
$4 = 2^2 + 0^2 + 0^2 + 0^2$
$1 = 1^2 + 0^2 + 0^2 + 0^2$

As seen above by the motivating example, and Lagrange's lemma, we can now write this as follows:

4.2 Manipulation of Lagrange's four square theorem

$ac = P^2 + Q^2 + R^2 + S^2$, where $c = b\delta$, and GCD $(P, Q, R, S) = 1$, as δ is the largest factor.

Let's say $P^2 + Q^2 = t$, $R^2 + S^2 = u$. Then $act = t^2 + tu$.

$$act = t^2 + (PR + QS)^2 + (PS + QR)^2 = t^2 + x^2 + y^2$$

Since we have a factor of t on L.H.S, we must have a factor of c and t on each of the terms on R.H.S. Thus we can express $x = \alpha t + \gamma c$ and $y = \beta t + \delta c$.

This results in the expression as below for act.

$$act = t^2(1 + \alpha^2 + \beta^2) + 2ct(\alpha\gamma + \beta\delta) + c^2(\gamma^2 + \delta^2)$$

We must thus have $t^2(1 + \alpha^2 + \beta^2) = cx$. Thus let's assume that $c\alpha' = (1 + \alpha^2 + \beta^2)$.

Then we get the following equation:

$$at = a't^2 + 2t(\alpha\gamma + \beta\delta) + c(\gamma^2 + \delta^2)$$

Thus we get multiplying by a':

$$aa't = (a't)^2 + 2a't(\alpha\gamma + \beta\delta) + a'c(\gamma^2 + \delta^2)$$

Replacing $a'c = 1 + \alpha^2 + \beta^2$ gives us:

$$aa't = (a't)^2 + 2a't(\alpha\gamma + \beta\delta) + (\alpha^2 + \beta^2)(\gamma^2 + \delta^2) + \gamma^2 + \delta^2$$

$$aa't = (a't + \alpha\gamma + \beta\delta)^2 + (\beta\gamma - \alpha\delta)^2 + \gamma^2 + \delta^2$$

Dividing by t, we get the following, where $\frac{\gamma^2+\delta^2}{t} = (r')^2 + (s')^2$ and $\frac{(a't+\alpha\gamma+\beta\delta)^2+(\beta\gamma-\alpha\delta)^2}{t} = (p')^2 + (q')^2$

Thus we get $aa' = p'^2 + q'^2 + r'^2 + s'^2$

5 Proof of Theorem 1 about sum of 2 squares and divisor

Theorem 5. *If a number N is a divisor of a sum of two squares P^2+Q^2 which are prime to each other, then that number N will itself be a sum of two squares.*

Euler approaches this through the following lens, as seen in [Eul08]:
Let us choose 2 arbitrary numbers P and Q. Upon inspection, we see that the number N, is such that it can itself be expressed as the sums of two squares, $a^2 + b^2$, however, we note that neither root can be greater than $N/2$.

We take $P = fN \pm p$ and $Q = gN \pm q$

$$P^2 + Q^2 = N^2(f^2 + g^2) + 2N(\pm fp \pm gq) + p^2 + q^2$$

Since we know that N is a divisor of $P^2 + Q^2$, this means that $p^2 + q^2 = Nn$, for some positive integer n.

Using the fact that $p < N/2$ and $q < N/2$,then $n < N/2$. One can then substitute values for p and q, as we did before for P and Q. Thus we get, the following:

$$p = a + \alpha n$$
$$q = b + \beta n$$

Using this substitution, we get:

$$Nn = (a + \alpha n)^2 + (b + \beta n)^2$$
$$Nn = a^2 + b^2 + n^2(\alpha^2 + \beta^2) + 2n(a\alpha + b\beta)$$

Using Diophantus and Fermat's theorem on sum of two square we get

$$Nn = a^2 + b^2 + n^2(\alpha^2 + \beta^2) + 2nA$$

and since we know that N is an integer, we get $a^2 + b^2 = nn'$.

Thus we have the following equation when substituting and dividing by n:

$$N = n' + 2A + n(\alpha^2 + \beta^2)$$

Finally multiplying by n', we get the following equation using the lemma by Fermat:

$$Nn' = n'^2 + 2n'A + A^2 + B^2 = (n' + A)^2 + B^2$$

Thus we have proved that if a number N is a divisor of a sum of two squares, then it is a sum of 2 squares itself. An example of this is taking N as 5, and $P^2 + Q^2 = 25$. $N = 1^2 + 2^2$.

This has therefore helped us to come to a more important realisation: every multiple of a number which cannot be expressed as the sum of 2 square numbers (i.e 3) cannot be the sum of 2 squares. Linking to Euler's previous work on which numbers can be expressed as the sum of 2 squares, this is quite interesting. We see that prime numbers of form $4n+3$ cannot be written as the sum of two squares, whereas prime numbers of form $4n+1$ can be written as sum of two squares. From Euler's proof, we see that numbers of form $k(4n+3)$, where $4n+3$ is prime cannot be the sum of two squares.

6 Proof of Theorem 2 regarding prime numbers and squares

Theorem 6. *Given any prime number N, not only four squares but even in fact three squares can be exhibited in infinitely many ways whose sum is divisible by this number N, but no single one can be divided by it.*

Proof. We see that all numbers x are of form $x \equiv a \pmod{N}$, where a is an integer between 0 and $N-1$. Thus $x = \lambda n + a$.

We also notice that the squares of these numbers can be represented in the forms of $\lambda n + b$, where b is a square of an integer between 0 and $(N-1)/2$. These are called forms of first class.

If b exceeds n itself, then we have forms of second class represented by $\lambda n + c$, where c is the residue when divided by n.

Product of two numbers in the first class gives us numbers of form: $\lambda n + b_1 b_2$

Product of two numbers one the first class and one in the second class gives us numbers of form: $\lambda n + b_1 c_1$, which is another number in the second class.

Product of two numbers in the second class gives us numbers of form: $\lambda n + c_1 c_2$, which is a number in the first class.

If sum of three squares were not to be divisible by N, then any two squares would also have sum not be a multiple of N, otherwise we can just add 0, and get the desired result. This means that numbers of for, $\lambda N + a$ and $\lambda N - a$,

cannot be in the same class. This means that without loss of generality, we can assume the numbers in second class are of form $\lambda N - a$, such that $c_1, c_2, ...$ are comprised of -1, -4, -9, -16, -25, ...

Let f be any number of the form class, so that a square of the form $\lambda N + f$ is given; if squares of the form $\lambda + 1$ are added to this, $\lambda N + f + 1$ will be a sum of two squares. Now if a square of the form $\lambda N - f - 1$ were given, we would obtain a sum of square squares that was divisible by N; since this is false, the form $\lambda N - f - 1$ will not be in the first class and will this be contained in the latter. However, since the numbers -1 and $-f - 1$ are there, it is necessary that their product $f + 1$ occurs in the first class. It can be shown in a similar way that the numbers $f + 2$, $f + 3$, $f + 4$ also exist in the first class, and taking $f = 1$, gives $\lambda N + 1$, $\lambda N + 2$, ... all exist in the first class, whilst -1, $-\lambda N - 1$, $-\lambda N - 2$, ... all exist in the second class.

Thus using the above lemmas of multiplication of two numbers in first class and second class, we see that the sum of three squares or four squares have many forms in the first and second class. □

7 Partitioning numbers into squares

Similar to Ramanujan and Euler's method of calculating partitions of numbers, there is an analogous partition of numbers into squares, Jacobi theorised the following, see [Leh48]:

Theorem 7. *The number of representations of n as the sum of 4 squares*

$$R_4(n) = 8(2 + -1^n)(\sigma_0(n))$$

where $\sigma_0(n)$ is the sum of odd divisors of n.

7.1 Defining Example

$R_4(98) = 8(2 + 1)(1 + 7 + 49) = 1368$, but we know that $P_4(n) = 7$, namely as listed below:

$$98 = 0^2 + 0^2 + 7^2 + 7^2$$
$$98 = 0^2 + 1^2 + 4^2 + 9^2$$
$$98 = 2^2 + 2^2 + 3^2 + 9^2$$
$$98 = 0^2 + 3^2 + 5^2 + 8^2$$
$$98 = 2^2 + 3^2 + 6^2 + 7^2$$
$$98 = 1^2 + 5^2 + 6^2 + 6^2$$
$$98 = 3^2 + 3^2 + 4^2 + 8^2$$

7.2 Explanation behind the discrepancy shown in the example

This discrepancy is due to the difference in terms of the description of representations and partitions of numbers. Understanding the relationship between these numbers can be put down to the fact that there are 11 different types of ways a number can be the sum of at most 4 squares, and using these types, they are assigned a value. Essentially, this can be explained as follows:

$I : a^2+b^2+c^2+d^2$, has 384 representations due to the fact that $a^2 = (-a)^2$, and order does matter in a representation, thus we can use simple combinatorics to see that a can be any of 8 values, b can be any of 6 values, c can be any of 4 values, and d can be any of 2 values.

Similarly, we can identify that the number of representation of a different type can be determined by the combinatorics of arranging them. Using this, we can get that the 7 partitions have 1368 representations.

As of date, there is still no sure way to calculate the number of partitions of a number into 4 squares, but there are ways of calculating approximations for numbers of special formats.

7.3 Approximations of partitions in specific cases

For example, we clearly see that $\frac{R_4(n)}{384} <= P_4(n) <= \frac{R_4(n)}{8}$, because the maximum number of representations for any type of partition is 384, and the minimum number of representations for any partition is 8.

Since we don't know a formula for $\sigma_0(n)$, for even numbers $n = 2k$, we can only say that for $n = 2k + 1$, $\sigma(n) = \sigma_0(n)$, and thus we get the following equation:

$$\sigma(2k+1) >= P_4(2k+1) >= \frac{\sigma(2k+1)}{48}$$

Further work has been done in this field to approximate partitions of numbers into 3 squares and 4 squaes and as in the next part we will see the importance of this in modern applications of cryptography.

8 Application of Lagrange's four square theorem and Euler's four square identity into cryptography

This paper [PF09] discusses the importance of Euler's and Lagrange's work to modern aspects of cryptography. Thus, in this section the discussion regards the algorithm used and the importance of these formula and proofs on reducing computation for users decrypting. We see that the Lagrange four square theorem as well as the Euler four square identity are used in cryptography, as a trapdoor in the initialization of RSA prime numbers. A trapdoor of an RSA algorithm is a secret door which requires significantly less computation for the user to know how to decrypt a message once given the particular algorithm. Since we want to factorise n into prime factors p and q, we use Lagrange's four square theorem, we have:

$$p = x_1^2 + x_2^2 + x_3^2 + x_4^2$$
$$q = y_1^2 + y_2^2 + y_3^2 + y_4^2$$
$$n = a^2 + b^2 + c^2 + d^2$$

Thus we have:

$$a^2 + b^2 + c^2 + d^2 = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2)$$

Using Euler's four square identity, we get the following values for a, b, c, d:

$$a = x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4$$
$$b = x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3$$
$$c = x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2$$
$$d = x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1$$

Using this a base is set to determine the bounds or maximum values of x_1, x_2 and y_1.

We also use the approximation of number of partitions of a number into 3 squares to find the approximate number of tries required for decrypting a password, given the Lagrange four square theorem backdoor. Assuming we have $0 <= y_1 <= 100$, then using the formula for partitions p is approximated as $p - 100^2$, and thus we only need to try $200\pi\sqrt{p}$ representations compared to without knowing, if number of prime numbers less than n is denoted by $p(n)$ we would need to try $2^{p(n)}$.

9 Summary

Euler's work on the partitioning of numbers into four squares as well as other ways of partitioning numbers into the sums of squares has been very influential in

mathematics, especially in some fields of cryptography. These interesting proofs have led researchers to extend this to exploring 4D vectors and the geometric analogies of square numbers by finding the magnitude of these vectors and their relation to the Lagrange four square theorem, as can be seen here [LG18]

References

[Leh48] Derrick H Lehmer. "On the partition of numbers into squares". In: *The American Mathematical Monthly* 55.8 (1948), pp. 476–481.

[Eul08] Leonhard Euler. "New demonstrations about the resolution of numbers into squares". In: *arXiv preprint arXiv:0806.0104* (2008).

[PF09] Constantinos Patsakis and Evangellos Fountas. "Creating RSA trapdoors using lagrange four square theorem". In: *2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. IEEE. 2009, pp. 779–782.

[LG18] Jesús Lacalle and Laura N Gatti. "Extended Lagrange's four-square theorem". In: *Electronic Notes in Discrete Mathematics* 68 (2018), pp. 209–214.