Eperson’s Conjecture on Sums of Three Squares:

Short Proof of an Improved Result

Werner Hürlimann

Swiss Mathematical Society, University of Fribourg
CH-1700 Fribourg, Switzerland

Abstract

For odd \( q > 1 \) there is at least one primitive representation of \( 3q^2 \) by sums of three non-zero squares. This result, which strengthens a conjecture of Eperson first proved by Hirschhorn, is derived very simply. An explicit formula for the exact number of distinct representations of \( 3q^2 \) by sums of three non-zero squares is also given. Examples illustrate these results.

Mathematics Subject Classification: 11E25, 11D45

Keywords: sum of squares; primitive representation; counting function

Eperson [3] conjectured and Hirschhorn [4] proved that for odd \( q > 1 \) the Diophantine equation

\[ q_1^2 + q_2^2 + q_3^2 = 3q^2 \]  

(1)

has besides the trivial solution \((q_1, q_2, q_3) = (q, q, q)\) at least another solution with \( q_i > 0, \; q_i \equiv \pm 1 \pmod{6} \). One observes that the trivial solution is not primitive, and that other such solutions exist. For example, if \( q = 9 \) then \((q_1, q_2, q_3) = (3, 3, 15)\) solves the equation (1). Therefore, one may strengthen Eperson’s original problem and ask for at least one primitive solution of (1) with \( \gcd(q_1, q_2, q_3) = 1 \). Theorem 1 shows very simply that this slightly improved result
remains true. Then, Theorem 2 determines the exact number of distinct representations of $3q^2$ by sums of three non-zero squares. Finally, some examples illustrate.

Some preliminary notations and results are required. Instead of (1) consider the representations of an arbitrary integer $n > 0$ by sums of three integer squares, that is the equation

$$x^2 + y^2 + z^2 = n.$$  \hfill (2)

The total number of primitive solutions of (2) counting zeros, permutations and sign changes, is denoted by $R_3(n)$. The number of distinct primitive integer solutions satisfying $0 < x \leq y \leq z$ is denoted by $R_3^d(n)$. The number of distinct primitive representations of $n$ by the binary quadratic forms $x^2 + y^2$ and $x^2 + 2y^2$ is denoted by $D_2(n)$ and $D_{(1,2)}(n)$ respectively. Taking into account possible zeros and equal entries, the distinct primitive solutions of (2) can take the 3 different forms $(x, y, z)$, $(x, y, y)$ and $(0, y, z)$, with distinct entries $x, y, z \neq 0$. For each form, one must determine the number of resulting representations counting permutations and sign changes, as well as the number of distinct primitive solutions generated by this form. The latter counting function is denoted by $D_3(n)$, where • stands for the quadratic form type of the corresponding Diophantine equation. For the form $(x, y, z)$ this counting function is denoted by $D_3(n)$. The binary quadratic forms $x^2 + 2y^2$ and $y^2 + z^2$, which correspond to the forms $(x, y, y)$ and $(0, y, z)$, define the counting functions denoted by $D_{(1,2)}(n)$ and $D_2(n)$ respectively. Table 1 summarizes the required information.

**Table 1:** Forms, Diophantine equations, representations and distinct solutions for the counting function $R_3(n)$

<table>
<thead>
<tr>
<th>form</th>
<th>Diophantine equation</th>
<th># of permutations</th>
<th># of sign changes</th>
<th>total # of representations</th>
<th># distinct solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(x, y, z)$</td>
<td>$x^2 + y^2 + z^2 = n$</td>
<td>6</td>
<td>8</td>
<td>48</td>
<td>$D_3(n)$</td>
</tr>
<tr>
<td>$(x, y, y)$</td>
<td>$x^2 + 2y^2 = n$</td>
<td>3</td>
<td>8</td>
<td>24</td>
<td>$D_{(1,2)}(n)$</td>
</tr>
<tr>
<td>$(0, y, z)$</td>
<td>$y^2 + z^2 = n$</td>
<td>6</td>
<td>4</td>
<td>24</td>
<td>$D_2(n)$</td>
</tr>
</tbody>
</table>

By definition of the first two forms in Table 1, one has the identity

$$D_3(n) + D_{(1,2)}(n) = R_3^d(n).$$  \hfill (3)
Furthermore, by definition of the counting function $R_3(n)$ one obtains from Table 1 the relationship
\[ 48D_3(n) + 24D_{(1,2)}(n) + 24D_2(n) = R_3(n). \] (4)

Next, solve (4) for $D_3(n)$ and insert into (3) to get the basic relationship
\[ 48R_3^d(n) = R_3(n) - 24D_2(n) + 24D_{(1,2)}(n). \] (5)

In the following, we specialize to $n=3q^2$ for odd $q>1$. Suppose the prime factorization of $q$ is given by $q = 3^6 \cdot \prod_{i=1}^{s} p_i^{r_i}$, $p_i \equiv \pm 1 \pmod{6}$. From Cooper and Hirschhorn [1], Theorem 2, equation (1.19), one borrows the formula
\[ R_3(3q^2) = R_3(3) \cdot q \cdot \prod_{i=1}^{s} \left(1 - \left(\frac{3}{p_i}\right) p_i^{-1}\right) = 8 \cdot 3^6 \cdot \prod_{i=1}^{s} p_i^{r_i-1} (p_i - \left(\frac{3}{p_i}\right)). \] (6)

One also needs the well-known result that $D_2(3q^2) = 0$ and the counting formula
\[ D_{(1,2)}(3q^2) = \begin{cases} 1, & s = 0, \\ \prod_{i=1}^{s} \left(1 + \left(\frac{3}{p_i}\right)\right), & s \geq 1. \end{cases} \] (7)

The first fact follows from [1], equation (1.6), and (7) is part of Cox [2], Lemma 3.25, p. 55.

**Theorem 1 (Improved Eperson-Hirschhorn Theorem)** For odd $q>1$ the number of distinct primitive representations of $3q^2$ by sums of three non-zero squares satisfies the inequality $R_3^d(3q^2) \geq 1$.

**Proof.** Consider the prime factorization $q = 3^6 \cdot \prod_{i=1}^{s} p_i^{r_i}$, $p_i \equiv \pm 1 \pmod{6}$. Two cases are possible. If $s = 0$, then one has necessarily $r_i \geq 1$ and $R_3(3q^2) = 8 \cdot 3^6 \geq 24$. Furthermore, one has $D_2(3q^2) = 0$ and $D_{(1,2)}(3 \cdot q^2) = 1$ by (7). Inserting into (5) one gets
\[ R_3^d(3q^2) = \frac{1}{48} R_3(3q^2) + \frac{1}{2} D_{(1,2)}(3 \cdot q^2) \geq \frac{1}{2} + \frac{1}{2} = 1. \]
If \( s \geq 1 \), then one has necessarily \( r_1 \geq 1 \). Since \( D_2(3q^2) = 0 \) and \( D_{(1,2)}(3q^2) \geq 0 \), one has \( R_3^d(3q^2) \geq \frac{1}{48} R_3(3q^2) \) by equation (5). Using this and (6) one obtains for arbitrary \( q > 1 \) that

\[
R_3^d(3q^2) \geq \frac{1}{48} R_3(3q^2) \geq \frac{1}{6} \left( p_1 - \left( \frac{2}{p_1} \right) \right).
\]

By assumption \( p_1 = 6k \pm 1 \), \( k \geq 1 \), and the Legendre symbol equals \( \left( \frac{2}{p_1} \right) = \pm 1 \) if \( p_1 = 6k \pm 1 \). Inserted into the preceding inequality, one concludes that \( R_3^d(3q^2) \geq \frac{1}{6} (6k \pm 1 \mp 1) = k \geq 1 \). ◊

**Theorem 2** For odd \( q = 3^6 \cdot \prod_{i=1}^{t} p_i^{s_i} > 1 \), \( p_i \equiv 6k_i \pm 1, k_i \geq 1 \), the number of distinct representations of \( 3q^2 \) by sums of three non-zero squares is given by

\[
R_3^d(3q^2) = \begin{cases} 
\frac{1}{2} \left( 3^{s_i-1} + 1 \right), & s = 0, \\
3^6 \cdot \prod_{i=1}^{t} k_i p_i^{s_i-1} + \frac{1}{6} \cdot \prod_{i=1}^{t} \left( 1 + \left( \frac{2}{p_i} \right) \right), & s \geq 1.
\end{cases}
\]  

(8)

**Proof.** Use that \( D_2(3q^2) = 0 \) and insert (6)-(7) into (5) to get the desired formula by noting that \( p_i - \left( \frac{2}{p_i} \right) = 6k_i \) if \( s \geq 1 \), as in the proof of Theorem 1. ◊

**Example 1:** The counting function \( R_3^d(3p^2) \) for primes \( p = 6k \pm 1, k \geq 1 \)

Formula (8) with \( s = 1, r_0 = 0, r_1 = 1, p_1 = p \), yields \( R_3^d(3p^2) = k + \frac{1}{6} \left( 1 + \left( \frac{2}{p} \right) \right) \).

The well-known values of the Legendre symbol implies the counting formula

\[
R_3^d(3p^2) = \begin{cases} 
k + 1, & p \equiv 1, 3 \pmod{8}, \\
k, & p \equiv 5, 7 \pmod{8}.
\end{cases}
\]  

(9)

The formula (9) can be viewed as a variant of Theorem 86 in Shanks [7] (see also Shanks [6], Hürlimann [5], Theorem 3.3), which states that \( R_3^d(p^2) = k \) for primes \( p = 8k \pm 1, 8k \pm 5 \).

**Example 2:** Completion of Eperson’s list of primitive representations

Eperson [3] illustrates his finding for the first odd \( 1 < q \leq 23 \), and lists some solutions of (1) without being exhaustive. Table 2 completes his calculations for the primitive representations.
Table 2: All primitive solutions of (1) for odd $1 < q \leq 23$.

<table>
<thead>
<tr>
<th>odd $q$</th>
<th>$3q^2$</th>
<th># primitive solutions</th>
<th>distinct primitive representations</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>27</td>
<td>1</td>
<td>(1,1,5)</td>
</tr>
<tr>
<td>5</td>
<td>75</td>
<td>1</td>
<td>(1,5,7)</td>
</tr>
<tr>
<td>7</td>
<td>147</td>
<td>1</td>
<td>(1,5,11)</td>
</tr>
<tr>
<td>9</td>
<td>243</td>
<td>2</td>
<td>(1,11,11), (5,7,13)</td>
</tr>
<tr>
<td>11</td>
<td>363</td>
<td>2</td>
<td>(1,1,19), (5,7,17), (5,13,13)</td>
</tr>
<tr>
<td>13</td>
<td>507</td>
<td>2</td>
<td>(5,11,19), (7,13,17)</td>
</tr>
<tr>
<td>15</td>
<td>675</td>
<td>2</td>
<td>(1,7,25), (5,11,23), (5,17,19)</td>
</tr>
<tr>
<td>17</td>
<td>867</td>
<td>2</td>
<td>(1,5,29), (7,17,23), (11,11,25), (13,13,23)</td>
</tr>
<tr>
<td>19</td>
<td>1063</td>
<td>2</td>
<td>(1,11,31), (5,23,23), (11,11,29), (13,17,25)</td>
</tr>
<tr>
<td>21</td>
<td>1323</td>
<td>2</td>
<td>(1,19,31), (13,23,25), (11,19,29)</td>
</tr>
<tr>
<td>23</td>
<td>1587</td>
<td>3</td>
<td>(1,19,35), (1,25,31), (7,13,37), (11,25,29)</td>
</tr>
</tbody>
</table>

References


Received: December 9, 2015; Published: January 14, 2016