The Liouville–Heath-Brown–Zagier Proof of the Two Squares Theorem and generalizations

Christian Elsholtz

July 9, 2002

Abstract

HEATH-BROWN [6] suggested a short proof of the two squares theorem, thereby simplifying ideas of LIOUVILLE. ZAGIER [15] suggested a particularly neat form of this, a "One sentence proof". It consists of two suitable involutions on the finite set of the solutions of $p = x^2 + 4yz$ in positive integers. A parity argument ensures the existence of a solution with $y = z$. The proof can be stated in one sentence since elementary calculations (namely to check that the mappings are well defined and are indeed involutory) can be left to the reader. The proof remained somewhat mysterious, since it is not obvious, where these mappings come from. In this paper we reveal this mystery and systematically explore similar proofs that can be given for related problems. We show that the very same method proves results on $p = x^2 + 2y^2$ (see also Jackson [7]), $p = x^2 - 2y^2$, $p = 3x^2 + 4y^2$, and $p = 3x^2 - 4y^2$.

1 Introduction

It is well known that suitable maps on suitably defined sets are a very powerful tool. A nice example was given by MCKAY [8], who gave a very short proof of CAUCHY's theorem in group theory. To find the suitable set and define the map is the key of the proof. Another example is the proof of the two squares theorem, as proved by HEATH-BROWN [6], and ZAGIER [15]. According to AIGNER and ZIEGLER [1] this is the "book"-proof.
A predecessor of such proofs is the work of LIOUVILLE. The reader may consult accounts of LIOUVILLE's work in the books of DICKSON [4], BACHMANN [2], USPENSKY & HEASLET [12], or NATHANSON [9], but will surely appreciate the simplifications due to HEATH-BROWN and ZAGIER.

[1]Parts of these results were found in 1990, other parts in 95/96, when a preliminary version of this paper was written up. The resulys were presented at the Number Theory Seminar at the University of Stuttgart, Spring 1998, at the occasion of T. Wooley's visit to Stuttgart. The present version was updated, after having seen a recent paper by Jackson who found some of these results.

The HEATH-BROWN-ZAGIER proof is based on two involutions. One of these is easy, and gives in the end the desired representation as sums of two squares. The other one is mysterious but allows to count easily the number of solutions modulo 2.
Very recently, JACKSON [7] gave a variant of this method adapted to the case $p = x^2 + 2y^2$ for primes $p \equiv 3 \bmod 8$. The second involution however is even more mysterious.
It is the purpose of this paper to explain how such mysterious involutions can be constructed and to perform a systematic search for further proofs of this type. We shall prove by this method:

Theorem 1. *Let p denote a prime.*

a) For $p = 8k + 3$ there is a solution of $p = x^2 + 2y^2$ in positive integers.

b) For $p = 8k + 7$ there is a solution of $p = x^2 - 2y^2$ in positive integers.

c) For $p = 8k + 5$ there is a representation as $p = x^2 + y^2$. (A new proof!)

Theorem 2. *Let p denote a prime.*

a) For $p = 12k + 7$ there is a solution of $p = 3x^2 + 4y^2$ in positive integers.

b) For $p = 12k + 11$ there is a solution of $p = 3x^2 - 4y^2$ in positive integers.

We hope that these notes will inspire teachers for projects in a course on linear algebra, computer algebra or automatic proof systems. At the end of some sections we will sketch some ideas for further exploration.
I would like to thank Prof. ARTMANN (Technische Universität Darmstadt). In his course on first year linear algebra he challenged me to reveal the secret behind the one sentence proof. I would also like to thank Prof. HEATH-BROWN for some remarks on this subject and for providing a copy of the original version of his proof.

2 The two squares theorem

2.1 Zagier's proof

Here is the famous one-sentence-proof for primes $p = 4k + 1$.
"The involution on the finite set $S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$ defined by

$$(x, y, z) \mapsto \begin{cases} (x + 2z, z, y - x - z) & \text{if } x < y - z \\ (2y - x, y, x - y + z) & \text{if } y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{if } x > 2y \end{cases}$$

has exactly one fixed point, so $|S|$ is odd and the involution defined by $(x, y, z) \to (x, z, y)$ also has a fixed point."
For the ease of the reader we would like to add that solutions with $x < y - z$ are mapped to solutions with $x > 2y$ and the other way around. Solutions with $y - z < x < 2y$ are mapped to solutions with the very same property. Thus fixed points are to be found amongst those solutions with $y - z < x < 2y$. Here it can easily be shown, since p is prime, that the only fixed point is $(1, 1, (p - 1)/4)$. Similarly, there are no solutions with $y - z = x$ or $x = 2y$, since p is a prime.
To verify these claims it is convenient to rewrite this proof with the matrices

$$A = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 0 & 1 \\ -1 & 1 & -1 \end{pmatrix}, B = \begin{pmatrix} -1 & 2 & 0 \\ 0 & 1 & 0 \\ 1 & -1 & 1 \end{pmatrix}, C = \begin{pmatrix} 1 & -2 & 0 \\ 1 & -1 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

2.2 Heath-Brown's proof

Heath-Brown's original version appeared in a hardly accessible student's magazine. Since it was slightly different, we describe his proof briefly.
Let us define

$$X_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad X_2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad X_3 = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & 0 \\ 0 & 2 & -1 \end{pmatrix}.$$

Define the sets

$$S = \{(x, y, z) \in \mathbb{Z}^3 : p = 4xy + z^2\},$$

$$T = \{(x, y, z) \in S : z > 0\}, \quad U = \{(x, y, z) \in S : x + z > y\}.$$

One can check that $X_1^2 = X_2^2 = X_3^2 = I$. Moreover, X_1 maps S to itself, X_2 maps T to itself, and X_3 maps U to itself. One also verifies that $|T| = |X_1 T|$ and $|U| = |X_1 U|$. Since S is the disjoint union of T and $X_1 T$ it follows that $|S| = |T| + |X_1 T| = 2|T|$ and similarly $|S| = 2|U|$. This implies $|T| = |U|$. Since the map X_3 acting on U has exactly one orbit of length 1 (for $y = z = 1$), and since all other orbits have length two, we find that $|U|$ must be odd. So, $|T|$ is also odd, and the action of X_2 on T must have an orbit of length 1 (i.e. a fixed point with $x = y$), giving $p = 4x^2 + z^2$.

2.3 How can we construct these mappings?

When analyzing this proof one observes that it is possible to *construct* the "complicated" involution by means of some fairly easy assumptions on that mapping, (see also [5]). These assumptions ensure that the final mapping would be as easy as possible.
If we look for a mapping that

I) is linear, so that we can write $B = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$, with integer entries which are independent of k,

II) maps the solutions (in positive integers) of $p = 4k+1 = x^2 + 4yz$ onto such solutions,

III) has the easiest solution, namely $(1, 1, k)$ as its only fixed point,

then we are uniquely led to $B = \begin{pmatrix} -1 & 2 & 0 \\ 0 & 1 & 0 \\ 1 & -1 & 1 \end{pmatrix}$.
This can be seen as follows: Property (III) gives

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ k \end{pmatrix} \stackrel{!}{=} \begin{pmatrix} 1 \\ 1 \\ k \end{pmatrix}.$$

In particular $a + b + ck = 1$. But since this shall be independent of k, we have that

$$\begin{aligned} a + b + ck = 1 \quad &\Rightarrow c = 0, \quad a + b = 1 \\ d + e + fk = 1 \quad &\Rightarrow f = 0, \quad d + e = 1 \\ g + h + ik = k \quad &\Rightarrow i = 1, \quad g + h = 0. \end{aligned}$$

Property (II) gives

$$(x')^2 + 4y'z' = (ax + by + cz)^2 + 4(dx + ey + fz)(gx + hy + iz) \stackrel{!}{=} x^2 + 4yz.$$

Hence, a comparison of the coefficients shows that

$$\begin{array}{ll} x^2 & a^2 + 4dg = 1 \\ xy & 2ab + 4(dh + eg) = 0 \\ \vdots & \qquad\qquad \vdots \\ yz & \text{with } c = f = 0 : ei = 1 \quad \Rightarrow e = 1, \Rightarrow d = 0. \end{array}$$

Now $a^2 + 4dg = 1$ is simplified to $a^2 = 1$. Suppose that $a = 1$. Then $b = 0$ and from $2ab + 4(dh + eg) = 0$ we get $g = 0$ and finally $h = 0$. Then, the matrix would be the identity matrix I. This is not what we want, since this map shall have only one fixed point.

Thus, $a = -1$, and so $b = 2, g = 1$, and finally $h = -1$. So, we have found the matrix B.
Surprisingly, we did not even need that our map shall be an involution but we can readily check that $B^2 = I$.
This only works for $-x + 2y > 0$ and $x - y + z > 0$. For the other cases one apparently needs a different matrix. Let us see how we can manipulate B to yield a corresponding row condition $x - 2y > 0$. We look for a matrix X which turns the row conditions of B into $(1, -2, 0)$ and $(1, -1, 1)$. The matrix $X = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ would do the job, but then again, we need a new idea to cover the cases $-x + y - z > 0$.

There is another possibility, namely to consider the matrix $X = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.
The advantage of this matrix is that the matrices $A = BX$ and $C = XB$ cover all cases. Let $A = BX = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 0 & 1 \\ -1 & 1 & -1 \end{pmatrix}$ and $C = XB = \begin{pmatrix} 1 & -2 & 0 \\ 1 & -1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$. We see that the row conditions perfectly fit to each other and induce a partition of all solutions.
We can also find these matrices A and C by choosing small primes ($p = 13, 17, 29$) and observing that here the sets of solutions with $-x + 2y < 0$ or $x - y + z < 0$ only have one or two elements. For $p = 13$, we find that $(1, 3, 1)$ must be mapped to $(3, 1, 1)$ and vice versa. For $p = 17$, we find that $(1, 4, 1)$ must be mapped to $(3, 1, 2)$ and vice versa. For $p = 29$ there are two possibilities. One excludes by the partially known mapping that $(1, 7, 1)$ is mapped to $(5, 1, 1)$ and finds that $(1, 7, 1)$ is mapped to $(3, 1, 5)$.
Even though we did not know about the partition of S we have found the map $\alpha : S \to S$ with

$$\alpha = \begin{cases} \alpha_1 & \text{decribed by matrix A, if } -x + y - z > 0 \\ \alpha_2 & \text{described by matrix B, if } -x + 2y > 0 \text{ and } x - y + z > 0 \\ \alpha_3 & \text{decribed by matrix C, if } x - 2y > 0 \text{ and } x - y + z > 0. \end{cases}$$

This is precisely the mapping given by Zagier. Of course, α as a whole is not a linear map, so that property (I) is not strictly satisfied. We obtain in this way the easiest involution, α, with the required property, namely that we know the set of fixed points.
Zagier's second mapping, β (say), with $\beta : S \to S$ and $(x, y, z) \mapsto (x, z, y)$ corresponds to the matrix

$$Y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

2.4 Ideas for further explorations

Hinweis an den Gutachter:

2.4.1 Geometric interpretation

Interprete the surface $p = x^2 + 4yz$ as a hyperboloid. Use a computer to plot the surface $41 = x^2 + 4yz$ and the integer solutions. Draw the curves $-x + 2y = 0, x - y + z = 0, x = y$, and $y = z$ into the diagram. Study which solutions (i.e. points) are paired together, i.e. $((x, y, z), \alpha(x, y, z))$ and $((x, y, z), \beta(x, y, z))$.

2.4.2 Another map

Given such a mapping, one can construct an even more involved involution. For $p = 4k+1 > 5$ consider the mapping $\alpha\beta\alpha\beta\alpha$. This shall consist of all 27 matrices. (In fact, only 15 of these are distinct.) Here the only fixed point is $(3, 1, k - 2)$.

2.4.3 Making the proof constructive

In his paper ZAGIER mentioned the proof only shows the existence of the solution. Combining the two involutions α and β, we can give a constructive proof. Starting with the only fixed point of α, and iterating β, α... we must arrive at a period.

$$(1,1,k) \xrightarrow{\beta} (1,k,1) \xrightarrow{\alpha} (3,1,k-2) \xrightarrow{\beta} \cdots \xrightarrow{\beta} (3,1,k-2) \xrightarrow{\alpha} (1,k,1) \xrightarrow{\beta} (1,1,k).$$

Since the maps are bijective, there is no pre-period. So, we eventually come back to $(1, 1, k)$ with β. The number of elements in the period is even. By symmetry, there must be another fixed point in the middle of the cycle. Since there is only one fixed point of α, this iteration constructs a fixed point of β, that is a solution of $p = x^2 + 4y^2$.

Applying this algorithm to a composite integer $n = 4k + 1$ which is not a square the very same argument shows that any cycle containing $(1, 1, k)$ must also contain another fixed point. Since n is no longer prime we may well come to another fixed point of α which corresponds to a factorization of n. Let us concentrate on products of two distinct primes $n = p_1p_2$ with $p_1 \equiv p_2 \equiv 3 \bmod 4$. Here β does not have fixed points, since otherwise $n = x^2 + 4y^2 \equiv 0 \bmod p_1$ which is impossible. Hence, in this case the iteration $\beta, \alpha, \beta \ldots$ must eventually come to a fixed point of α which corresponds to $x = y$, i.e. a factorization of n (example: $p = 33$). For more details see [10]. The algorithm in this form is very slow. SHIU describes how one can accelerate this algorithm. It turns out to have an interpretation in the theory of continued fractions.

2.4.4 The mapping generates a finite group

It is interesting to look at the following properties of the matrices A, B, C, X.

$$B^2 = I,\ A^3 = C^3 = -I,\ A^6 = C^6 = I,$$
$$A = C^{-1},\ AB = (BX)B = B(XB) = BC = BA^5.$$

This shows that the 12 matrices $A, A^2, \ldots, A^6 = I, BA, \ldots, BA^6 = B$ are a model of the dihedral group D_6. The 15 matrices mentioned in section 2.4.2, however, generate an infinite group of matrices. This infinite group has a subgroup isomorphic to D_6. Furthermore, starting with the powers of $T = AYAYA = \begin{pmatrix} 1 & 0 & 6 \\ 0 & 0 & 1 \\ -3 & 1 & -9 \end{pmatrix}$, one can generate an infinite series of matrices, where the last entries in the last rows of $-T, T^2, -T^3, \cdots$, namely $(9, 64, 221, 3025, \cdots)$, are squares of the Fibonacci numbers.

3 How to construct new mappings

One can ask for similar involutions α for $p = x^2 + ayz$. For example it is well known that for a prime p the following holds

$$p \equiv 1, 3 \bmod 8 \Leftrightarrow p = x^2 + 2y^2.$$

It would be nice to have an easy proof of this theorem by the idea of the Liouville—Heath-Brown—Zagier proof.

Generalizing the approach of section 2.3 one can prove that the matrix $B = \begin{pmatrix} -1 & 2\frac{m}{n} & 0 \\ 0 & 1 & 0 \\ 4\frac{sm}{tn} & -4\frac{sm^2}{tn^2} & 1 \end{pmatrix}$ maps solutions of $p = sx^2 + tyz$ to such solutions and has the single fixed point (m, n, k'). Here m, n, s, and t are fixed positive integers. So $k' = \dfrac{p - sm^2}{tn}$. We note that again $B^2 = I$. Unfortunately, in the general case the boundaries induced by the rows, namely $-x + 2\frac{m}{n} > 0$ and $4\frac{sm}{tn}x - 4\frac{sm^2}{tn^2}y + z > 0$, do not induce such a balanced three-partition of the set of solutions.

However, it is possible to construct mappings for $p = x^2 + 2y^2$ and $p = 3x^2 + 4y^2$ consisting of even more matrices. As before, these matrices are generated by B and X.

Note, even though the occurring matrices will be more complicated, the idea of the proof is still the same. The justification of the properties of the map α can -in principle- be left to an automatic system since it requires elementary calculations only.

As before, we try, if $A = BX$ can be useful. As above we use $X = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.

At this point, we do not worry about the boundaries or a partition of the set of all solutions.

Geometrically, we can expect that $|\det A| = 1$, since we should not map bijectively a large region to a small one and vice versa.

Consider the eigenvalues of

$$\begin{aligned} A = BX &= \begin{pmatrix} -1 & 2\frac{m}{n} & 0 \\ 0 & 1 & 0 \\ 4\frac{sm}{tn} & -4\frac{sm^2}{tn^2} & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 2\frac{m}{n} \\ 0 & 0 & 1 \\ -4\frac{sm}{tn} & 1 & -4\frac{sm^2}{tn^2} \end{pmatrix} = \begin{pmatrix} 1 & 0 & a \\ 0 & 0 & 1 \\ -c & 1 & -d \end{pmatrix}, \text{ say.} \end{aligned}$$

Noting that $ac = 2d$ we find

$$\begin{aligned} 0 &= (1-\lambda)(0-\lambda)(-d-\lambda) - (1-\lambda) - (-c)(0-\lambda)a \\ &= (\lambda+1)(\lambda^2 + (d-2)\lambda + 1). \end{aligned}$$

We find that $\lambda_1 = -1$ and $\lambda_{2,3} = -\frac{d-2}{2} \pm \sqrt{\left(\frac{d-2}{2}\right)^2 - 1}$.

Since $|\det A| = |\lambda_1| = 1$ and $|\lambda_2| = |\lambda_3|$, we find that necessarily $|\lambda_2| = |\lambda_3| = 1$. This is a good property. Of course, we hope to end up with a matrix A that satisfies $A^k = I$ for some $k \in \mathbb{N}$. Otherwise we might find a map consisting of infinitely many parts. The fact that $|\lambda_i| = 1$ gives us hope that A generates a mapping with finitely many parts only.
Here d shall be an integer. This is only possible for $d = 0, 1, 2, 3, 4$. If $d \geq 5$ or $d \leq -1$, then $\lambda_{2,3} \in \mathbb{R}$ will be irrational.
Recall that $d = \dfrac{4sm^2}{tn^2}$. Since we want to represent primes with $p = sx^2 + tyz = sm^2 + tnz$ we may assume that $\gcd(sm, tn) = 1$. We shall systematically consider all cases.

3.1 $d = 0$

For $d = 0$ we have $sm = 0$, so that $p = tnz$. This case is of no interest.

3.2 $d = 1$

Here $d = \dfrac{4sm^2}{tn^2} = 1$, and $(s,t) = (s,n) = (t,m) = (m,n) = 1$. Hence there are two possibilities:

- $s = m = n = 1$, $t = 4$. This is precisely Zagier's case.
- $s = m = t = 1$, $n = 2$.

  In $p = x^2 + yz$ the solution with $p = x^2 + y^2 = y^2 + x^2$ is counted twice. In order to make the original argument work we need to break the symmetry. This can be done by assuming y and z to be even.

  The involution α is generated by

$$B = \begin{pmatrix} -1 & 1 & 0 \\ 0 & 1 & 0 \\ 2 & -1 & 1 \end{pmatrix},$$

$A = BX$, and $C = A^{-1}$.

This gives the following variant of the proof of the two squares theorem: The involution on the finite set $S = \{(x, y, z) \in \mathbb{N} \times 2\mathbb{N} \times 2\mathbb{N} : x^2 + yz = p\}$ defined by

$$(x, y, z) \mapsto \begin{cases} (x + z, z, -2x + y - z) & \text{if } 2x + z < y \\ (-x + y, y, 2x - y + z) & \text{if } x < y < 2x + z \\ (x - y, 2x - y + z, y) & \text{if } y < x \end{cases}$$

has exactly one fixed point, so $|S|$ is odd and the involution defined by $(x, y, z) \to (x, z, y)$ also has a fixed point.

3.3 $d = 2$

3.3.1 The case $p = x^2 + 2yz$

Here we consider the case $d = \dfrac{4sm^2}{tn^2} = 2$. We necessarily have that $s = m = n = 1$, $t = 2$.
Empirically one observes that the number of fixed points varies with the residue classes modulo 8:
a) primes $p \equiv 3 \bmod 8$ induce 1 fixed point,
b) primes $p \equiv 7 \bmod 8$ induce 2 fixed points,
c) primes $p \equiv 5 \bmod 8$ induce 2 fixed points, and
d) primes $p \equiv 1 \bmod 8$ induce 3 fixed points.

Case a) was also proved and case d) was also observed but not proven by Jackson. We shall prove a), b) and c) which corresponds to our Theorem 1 a,b,c). Unfortunately we do not see either a convenient way to prove d) without appealing to the theory of quadratic forms.
Let $S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 2yz = p\}$. The one sentence proof is as before with the following map $\alpha : S \to S$.

$$\alpha = \begin{cases} A = BX & = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 0 & 1 \\ -2 & 1 & -2 \end{pmatrix} \text{ if } -2x + y - 2z > 0 \\ E = -XA^2 & = \begin{pmatrix} -3 & 2 & -2 \\ -2 & 2 & -1 \\ 2 & -1 & 2 \end{pmatrix} \begin{cases} \text{if } -3x + 2y - 2z > 0 \\ \text{and } 2x - y + 2z > 0 \\ \text{(then } -2x + 2y - z > 0 \text{ is implied.)} \end{cases} \\ D = -A^2 & = \begin{pmatrix} 3 & -2 & 2 \\ 2 & -1 & 2 \\ -2 & 2 & -1 \end{pmatrix} \begin{cases} \text{if } 3x - 2y + 2z > 0 \\ \text{and } -2x + 2y - z > 0 \\ \text{(then } 2x - y + 2z > 0 \text{ is implied.)} \end{cases} \\ B = XA^3 & = \begin{pmatrix} -1 & 2 & 0 \\ 0 & 1 & 0 \\ 2 & -2 & 1 \end{pmatrix} \text{ if } -x + 2y > 0 \text{ and } 2x - 2y + z > 0 \\ C = A^{-1} = A^3 = XB & = \begin{pmatrix} 1 & -2 & 0 \\ 2 & -2 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{array}{l} \text{if } x - 2y > 0, \\ (2x - 2y + z > 0 \text{ follows trivially.)} \end{array} \end{cases}$$

Note that this map makes use of all matrices of the form $(-1)^{j+1}A^j, (j = 1, \cdots, 3)$, and $(-1)^{j+1}XA^j, (j = 2, j = 3)$. Note that also $A^4 = I$. The matrix XA is of no use, since this contains an impossible row condition $-x - 2z > 0$. The map is equivalent to Jackson's map:

$$(x, y, z) \mapsto \begin{cases} (x - 2y, z + 2x - 2y, y) & \text{if} & & y < & \frac{x}{2} \\ (2y - x, y, 2x - 2y + z) & \text{if } \frac{x}{2} & < & y < & x + \frac{z}{2} \\ (3x - 2y + 2z, 2x - y + 2z, -2x + 2y - z) & \text{if } x + \frac{z}{2} & < & y < & \frac{3}{2}x + z \\ (-3x + 2y - 2z, -2x + 2y - z, 2x - y + 2z) & \text{if } \frac{3}{2}x + z & < & y < & 2x + 2z \\ (x + 2z, z, -2x + y - 2z) & \text{if } 2x + 2z & < & y. & \end{cases}$$

Let us call the subsets of S that correspond to the matrices A, B, C, D, E by $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}, \mathcal{E}$. For a complete proof we have to show that

1. $\alpha : S \to S$, i.e. α maps (x, y, z) with $p = x^2 + 2yz$ to (x', y', z') with $p = x'^2 + 2y'z'$,
2. $\alpha^2 = id$,
3. the boundaries $(x - 2y = 0, 2x - 2y + z = 0$ etc.) are never attained,
4. the sets $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}, \mathcal{E}$ induce a partition of the set of all solutions,
5. there is only one fixed point.

3.3.2 Proof of theorem 1

1. Since all parts of the mapping α are generated by $-I, X$ and B, it suffices to prove the first property for $-I, X$ and B. It is obvious for $-I$ and X. For B we have:

$$(x')^2 + 2y'z' = (-x + 2y)^2 + 2(y)(2x - 2y + z) = x^2 + 2yz.$$

2. Note that A maps the region $\mathcal{A}$ to the region $\mathcal{C}$. Because of $C = A^{-1}$ the region $\mathcal{C}$ is mapped to the region $\mathcal{A}$. The first assertion follows from $x' - 2y' = (x+2z) - 2z > 0$ and $2x' - 2y' + z' = 2(x+2z) - 2z + (-2x+y-2z) = y > 0$. For the second assertion we need that $-2x' + y' - 2z' > 0$ with $x' = x - 2y, y = 2x - 2y + z, z' = y$ and so $-2x' + y' - 2z' = z > 0$. Note that $B^2 = D^2 = E^2 = I$. So the matrix B maps the set $\mathcal{B}$ onto $\mathcal{B}$. The same holds for $D : \mathcal{D} \to \mathcal{D}$ and $E : \mathcal{E} \to \mathcal{E}$.

3. Suppose the boundaries are attained. This will lead to a contradiction.

   (a) For the boundaries in the first row, namely $x - 2y = 0, -x + 2y = 0, 3x - 2y + 2z = 0, -3x + 2y - 2z = 0$, it would follow that x is even. This contradicts $p = x^2 + 2yz$, since p is odd.

   (b) $-2x + y - 2z = 0$: $p = x^2 + 2yz = x^2 + 2(2x + 2z)z = (x + 2z)^2$. This contradicts the primality of p.

   (c) $2x - 2y + z = 0$: $p = x^2 + 2yz = x^2 + 2y(2y - 2x) = (x - 2y)^2$, contradicting the primality of p.

   (d) $2x - y + 2z = 0$: See (b).

   (e) $-2x + 2y - z = 0$: See (c).

4. It follows easily from the boundaries in JACKSON's map that α induces a partition of S.

5. We now look for the fixed points of α. Here we distinguish between the various cases depending on the residue class modulo 8. We see that A and C cannot have fixed points, since the set $\mathcal{A}$ is mapped onto $\mathcal{C}$ and the other way around.

   Suppose that (x, y, z) is a fixed point of B, then

$$B \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -x + 2y \\ y \\ 2x - 2y + z \end{pmatrix} \stackrel{!}{=} \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

   Hence $x = y$. Because of $p = x^2 + 2yz$ this is only possible for $x = y = 1$. Hence B has precisely one fixed point.

   For the matrix D we find that

$$D \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 3x - 2y + 2z \\ 2x - y + 2z \\ -2x + 2y - z \end{pmatrix} \stackrel{!}{=} \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

Hence $y = x+z$, and therefore, $p = x^2+2yz = x^2+2(x+z)z = (x+z)^2+z^2$. Similarly,

$$E\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -3x+2y-2z \\ -2x+2y-z \\ 2x-y+2z \end{pmatrix} \stackrel{!}{=} \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

Hence $y = 2x + z$, which implies that $p = x^2 + 2yz = x^2 + 2(2x + z)z = (x + 2z)^2 - 2z^2$.

If $p \equiv 3 \bmod 8$, there is no fixed point coming from D and E. To see this recall that squares modulo 8 only take the values $0, 1, 4$. So, $|S|$ is odd. As before, the involution β must have an odd number of fixed points. Hence there is at least one fixed point with $y = z$, leading to the solution of $p = 8k + 3 = x^2 + 2y^2$.

The same consideration of the values of squares modulo 8 shows:

If $p \equiv 7 \bmod 8$, we have again the trivial fixed point of B. There cannot be a fixed point from D. Since there cannot be a representation $p = x^2 + 2y^2$, we see that there must be a fixed point coming from E. So, $p \equiv 7 \bmod 8$ can be written as $p = x^2 - 2y^2$. This proves theorem 1b).

If $p \equiv 5 \bmod 8$, there cannot be a fixed point of E. Since $p = x^2 + 2y^2$ is impossible, there must be a fixed point of D, hence p has a representation of the form $x^2 + y^2$. This gives a new proof for one half of the two squares theorem.

If $p \equiv 1 \bmod 8$, we have a fixed point of B and (by the two squares theorem) of D. In order to prove the existence of the representation $p = x^2 + 2y^2$ it is enough to prove that there is (precisely) one fixed point of E. I do not see how to prove this with the methods of this paper.

3.3.3 The group of the matrices

One easily verifies the following identities. $A = BX, A^2 = -D = BXBX = XBXB, D = D^{-1}, E = E^{-1} = -BXB$. This shows that the matrices

$$I, B, X, BX, XB, XBX, BXB, BXBX,$$

$$-I, -B, -X, -BX, -XB, -XBX, -BXB, -BXBX$$

form a multiplicative group with 16 elements.

3.4 $d = 3$

3.4.1 The case $p = 3x^2 + 4y^2$

Here we deal with the case $d = \dfrac{4sm^2}{tn^2} = 3$. We have again two sub-cases.

- $s = 3$, $m = n = 1$, $t = 4$.

- $s = 3$, $m = t = 1$, $n = 2$, with even y and z.

As above in the case $d = 1$, both of these sub-cases are equivalent. We will thus concentrate on the first case.
The form $p = 3x^2 + 4yz$ represents only primes $p \equiv 3 \bmod 4$, hence we consider $p = 12k + 7$ and $p = 12k + 11$. We will proceed as in the case $d = 2$.
The general form of our matrix B is now

$$B = \begin{pmatrix} -1 & 2 & 0 \\ 0 & 1 & 0 \\ 3 & -3 & 1 \end{pmatrix}, A = BX = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 0 & 1 \\ -3 & 1 & -3 \end{pmatrix}.$$

In view of $A^6 = I$ we consider the 9 matrices

$$(-1)^{j+1} A^j, (j = 1, \cdots, 5) \text{ and } (-1)^{j+1} X A^j, (j = 2, \cdots, 5).$$

(As before, the matrix XA is useless, because of the row condition $-x - 2z > 0$.)

$$-A^2 = \begin{pmatrix} 5 & -2 & 4 \\ 3 & -1 & 3 \\ -6 & 3 & -4 \end{pmatrix}, A^3 = \begin{pmatrix} 7 & -4 & 4 \\ 6 & -3 & 4 \\ -6 & 4 & -3 \end{pmatrix}, -A^4 = \begin{pmatrix} 5 & -4 & 2 \\ 6 & -4 & 3 \\ -3 & 3 & -1 \end{pmatrix},$$

$$A^5 = A^{-1} = XB = \begin{pmatrix} 1 & -2 & 0 \\ 3 & -3 & 1 \\ 0 & 1 & 0 \end{pmatrix}, D = -XA^2 = \begin{pmatrix} -5 & 2 & -4 \\ -6 & 3 & -4 \\ 3 & -1 & 3 \end{pmatrix},$$

$$E = XA^3 = \begin{pmatrix} -7 & 4 & -4 \\ -6 & 4 & -3 \\ 6 & -3 & 4 \end{pmatrix}, F = -XA^4 = \begin{pmatrix} -5 & 4 & -2 \\ -3 & 3 & -1 \\ 6 & -4 & 3 \end{pmatrix}, B = XA^5.$$

The corresponding boundaries are induced by the matrices themselves: for example the matrix $\begin{pmatrix} -5 & 4 & -2 \\ -3 & 3 & -1 \\ 6 & -4 & 3 \end{pmatrix}$ corresponds to $-5x+4y-2z > 0$, $-3x+3y-z > 0, 6x - 4y + 3z > 0$.
Hence the map α is:

$$(x,y,z) \to \begin{cases} (x-2y, 3x-3y+z, y) & \text{if } \quad y < \frac{x}{2} \\ (-x+2y, y, 3x-3y+z) & \text{if } \frac{x}{2} < y < x + \frac{z}{3} \\ (5x-4y+2z, 6x-4y+3z, -3x+3y-z) & \text{if } x + \frac{z}{3} < y < \frac{5}{4}x + \frac{z}{2} \\ (-5x+4y-2z, -3x+3y-z, 6x-4y+3z) & \text{if } \frac{5}{4}x + \frac{z}{2} < y < \frac{3}{2}x + \frac{3}{4}z \\ (7x-4y+4z, 6x-3y+4z, -6x+4y-3z) & \text{if } \frac{3}{2}x + \frac{3}{4}z < y < \frac{7}{4}x + z \\ (-7x+4y-4z, -6x+4y-3z, 6x-3y+4z) & \text{if } \frac{7}{4}x + z < y < 2x + \frac{4}{3}z \\ (5x-2y+4z, 3x-y+3z, -6x+3y-4z) & \text{if } 2x + \frac{4}{3}z < y < \frac{5}{2}x + 2z \\ (-5x+2y-4z, -6x+3y-4z, 3x-y+3z) & \text{if } \frac{5}{2}x + 2z < y < 3x + 3z \\ (x+2z, z, -3x+y-3z) & \text{if } 3x + 3z < y. \end{cases}$$

In order to prove theorem 2, we shall show: For primes $p \equiv 7 \bmod 12$ there is one fixed point of α. For primes $p \equiv 11 \bmod 12$ there are two fixed points of α.

3.4.2 Proof of theorem 2

Suppose that the boundaries are attained. This will lead to a contradiction. Note that for odd primes $p = 3x^2 + 4yz$ the value of x is odd. This excludes the boundaries $-x+2y = 0$, $5x-2y+4z = 0$, $5x-4y+2z = 0$ and $7x-4y+4z = 0$. Since $p = 3x^2 + 4yz$ is prime ($p > 3$), we can deduce that y and z are not divisible by 3. This excludes the boundaries $3x - 3y + z = 0$, $3x - y + 3z = 0$, $6x - 4y + 3z = 0$, and $6x - 3y + 4z = 0$.
Now let us look at the fixed points: The mappings $A, -A^2, -A^4, A^5$ cannot have any fixed points, (since A maps the region A onto the region A^5 etc.). The matrices B, A^3, D, E, F are involutions. So we have to check their fixed points.

- As before, B has precisely one fixed point: $(1, 1, k' = \frac{p-3}{4})$.
- For A^3 the fixed point condition $A^3 \begin{pmatrix} x \\ y \\ z \end{pmatrix} \overset{!}{=} \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ simplifies to: $3x - 2y + 2z = 0$. This is a contradiction since x is odd.
- Similarly, for D, we need to look at $3x-y+2z = 0$. Consider the equation $p = 3x^2 + 4yz = 3x^2 + 12xz + 8z^2 = 3(x + 2z)^2 - 4z^2$ modulo 3. With $z^2 \equiv 0, 1 \bmod 3$ and for $p \equiv 7 \bmod 12$, we find that $1 = 2z^2 \bmod 3$, a contradiction.
- For E, the fixed point condition is $2x-y+z = 0$. We look at $p = 3x^2+4yz = 3x^2 + 8xz + 4z^2 = 4(x + z)^2 - x^2 = (3x + 2z)(x + 2z)$, contradicting the primality of p.
- Finally, for F we have to look at $3x - 2y + z = 0$, and plug this into our ternary form $p = 3x^2 + 4yz = 3x^2 - 12xy + 8y^2 = 3(x - 2y)^2 - 4y^2$. Again, we consider this modulo 3: For $p = 12k + 7$ and with $2y^2 = 1 \bmod 3$ we see that there cannot be a fixed point.

We find that for $p = 12k + 7$ there is only the trivial fixed point of B, namely $(1, 1, (p - 3)/4)$. By the standard argument p can be written as $p = 3x^2 + 4y^2$. Since $p = 12k + 11$ cannot be written as $p = 3x^2 + 4y^2$, there must be a fixed point of D or F. Any such fixed point induces a representation of the type $p = 3x^2 - 4y^2$, (see the analysis of these cases above).
This proves theorem 2.

3.5 $d = 4$

$d = \dfrac{4sm^2}{tn^2} = 4$. Here necessarily $s = t = m = n = 1$, and therefore

$$B = \begin{pmatrix} -1 & 2 & 0 \\ 0 & 1 & 0 \\ 4 & -4 & 1 \end{pmatrix}.$$

This matrix generates an infinite partition. Since in the case $s = t = 1$ we do not expect anything new, we do not pursue this case further.

4 On infinite but incomplete mappings

One can also consider corresponding mappings induced by B and X for other values of d. We cannot expect that the number of required matrices will be finite. Here we give an example of a mapping which consists of infinitely many regions (and matrices) but which is in the present form still incomplete. It may be possible to complement this mapping by some symmetry arguments.
Consider $p = 3x^2 + 2yz = 24k + 5$. Generate the matrices with

$$B = \begin{pmatrix} -1 & 2 & 0 \\ 0 & 1 & 0 \\ 6 & -6 & 1 \end{pmatrix}.$$

Take

$$A = BX \text{ and } C = A^{-1} = XB.$$

$$A = BX, -A^2, A^3, -A^4, A^5 \text{ etc.}$$

$$C = XB, -C^2, C^3, -C^4, \text{ etc.}$$

$$B, -BC, BC^2, -BC^3, BC^4 \text{ etc.}$$

$$-XA^2, XA^3, -XA^4 \text{ etc.}$$

(Note: $-X$ and XA are again omitted.) For the matrix A we never have that $A^k = I$. This can easily be seen by looking at the eigenvalues of A, namely $-1, -2-\sqrt{3}, -2+\sqrt{3}$.
Taking infinitely many of these matrices, we see: The region of each matrix becomes smaller and smaller.
For the powers of $-A$ the row conditions come arbitrarily close to:

$$(3+\sqrt{3})x - y + (2+\sqrt{3})z > 0$$

and

$$-(3+\sqrt{3})x + y - (2+\sqrt{3})z > 0.$$

There are similar row conditions for the other series of matrices. The series

$$C = XB, -C^2, C^3, -C^4, \text{ etc.}$$

corresponds to

$$B, -BC, BC^2, -BC^3, BC^4 \text{ etc.}$$

in that respect that the row conditions of the first and third row are the same and the condition of the first row is reversed. Similarly, the two series

$$A = BX, -A^2, A^3, -A^4, A^5 \text{ etc.}$$

and

$$-XA^2, XA^3, -XA^4 \text{ etc.}$$

have associated boundaries. This latter series tends to a row condition of

$$(3+\sqrt{3})x - (2+\sqrt{3})y + z > 0$$

and

$$-(3+\sqrt{3})x + (2+\sqrt{3})y - z > 0.$$

Unfortunately the two boundaries

$$(3+\sqrt{3})x - y + (2+\sqrt{3})z > 0$$

and

$$(3+\sqrt{3})x - (2+\sqrt{3})y + z > 0$$

do not correspond. Hence there is a gap in between the regions of these series. It may be possible to fill this gap by some more series of matrices. But so far I do not know how to do this. Possibly, we only have to find one new matrix that generates all the other matrices. Possibly, a simple change of two coordinates suffices.

Looking at the conditions $ax - by + cz > 0$ and $ax - cy + bz > 0$, we see how incidental the above described mappings are.

In ZAGIER's case we have $a = b = c$. So there are no problems at all. In the case $p = x^2 + 2yz$ we had $2x - y + 2z$. Here $a = c$ so we still do not clearly see, what the condition in the general case is.

In the case $p = 3x^2 + 4yz$ we had $6x - 3y + 4z$ and $6x - 4y + 3z$. Here, we see the importance of the matrices $A^3 = BXBXBX$ and $XA^3 = XBXBXBX$ with both rows, $6, -3, 4$ and $-6, 4, -3$. These matrices are the "turning point", reversing the y and z coordinate. We have a complete cycle: $(-3, 1, -3) \Rightarrow (3, -1, 3) \Rightarrow (-6, 3, -4) \Rightarrow (6, -3, 4) \Rightarrow (-6, 4, -3) \Rightarrow (6, -4, 3) \Rightarrow (-3, 3, -1) \Rightarrow (3, -3, 1)$.

These matrices can be discovered by a sub-matrix (omit the first row and column) of the form $\begin{pmatrix} a & -b \\ -b & a \end{pmatrix}$.

In the incomplete mapping above there are no such "turning points".

References

[1] Aigner, M., Ziegler, G.M., Proofs from THE BOOK, Springer, Berlin Heidelberg, 1998.

[2] Bachmann, P., Niedere Zahlentheorie, reprint by Chelsea Publishing Co., New York, 1968.

[3] Barbeau, E. J., Polynomials. Corrected reprint of the original. Problem Books in Mathematics. Springer-Verlag, New York, 1995.

[4] Dickson, L. E., History of the theory of numbers, reprint by Chelsea Publishing Co., New York, 1966

[5] Elsholtz, C., Primzahlen der Form $4k + 1$ sind Summe zweier Quadrate, Mathematiklehren, no. 62, February 1994, pp. 58–61.

[6] Heath-Brown, D.R., Fermat's two squares theorem, Invariant (Journal of the Undergraduate Society of students of Mathematics at Oxford University), 1984, 3–5.

[7] Jackson, T., A Short Proof That Every Prime $p = 3(\mod 8)$ is of the Form $x^2 + 2y^2$, Amer. Math. Monthly, 107 (2000) p. 447.

[8] McKay, James H., Another proof of Cauchy's group theorem. Amer. Math. Monthly, 66 (1959), 119.

[9] Nathanson, M.B., Elementary methods in number theory. Graduate Texts in Mathematics, 195. Springer-Verlag, New York, 2000.

[10] Shiu, P., Involutions associated with sums of two squares., Publ. Inst. Math. (Beograd) (N.S.) 59(73) (1996), 18–30.

[11] Tikhomirov, V., Quantum, May/June 1994, pp. 5–7.

[12] Uspensky, J. V.; Heaslet, M. A. Elementary Number Theory. McGraw-Hill Book Company, New York, 1939.

[13] Varouchas, I., Une démonstration élémentaire du théorème des deux carrés, I.R.E.M. Bull, 6 (1984), 31-39.

[14] Williams, K.S., Heath-Brown's elementary proof of the Girard-Fermat theorem, Carleton Coordinates, (1985), 4-5.

[15] Zagier, D., A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares, Amer. Math. Monthly, 97 (1990), 144.

Christian Elsholtz
Institut für Mathematik
Technical University Clausthal
Erzstrasse 1
D-38678 Clausthal-Zellerfeld
Germany
(elsholtz@math.tu-clausthal.de)