Tatra Mt. Math. Publ. **20** (2000), 59–63

**TATRA MOUNTAINS**
*Mathematical Publications*

# AUTOMORPHS AND INVOLUTIONS

TERENCE JACKSON

ABSTRACT. This paper shows that when the quadratic form $ax^2 + byz$ has enough automorphs of finite order they can often be used to construct involutions of certain interesting finite sets. The existing direct proofs about the representation of primes as sums of squares are then shown to correspond to simple families of automorphs.

This paper is concerned with some recent short proofs (see [1], [2] and [3]) of classical results about the representation of primes by quadratic forms. I aim to show that there is a uniform approach which not only illuminates these proofs but may also enable us to find all such proofs, or show that there are no more.

Before Lagrange and Gauss developed the general theory of quadratic forms, Fermat and Euler had already found several interesting results about the representation of primes by individual binary quadratic forms such as $x^2 + y^2$, $x^2 + 2y^2$ and $x^2 + 3y^2$. These typically say that primes in certain congruence classes can all be represented by a given form for integer values of the variables. The first such theorem they proved was the beautiful result that each prime congruent to 1 modulo 4 is a sum of two squares. This had already been observed by Girard [4] in 1625, but Fermat [5] in 1640 was the first to indicate that he had a proof — by his method of descent, and over a hundred years later Euler [6] was the first to give a complete proof. Many proofs of this fact have been published in the intervening 250 years since Euler, but most of them rely on knowledge of some background material such as continued fractions or quadratic residues. Then in 1984 Heath-Brown [7] gave a new proof which he described in terms of group actions on sets. This inspired Zagier [1] to give the following one-paragraph proof which can be understood with hardly any background at all.

The involution on the finite set

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

2000 Mathematics Subject Classification: 11E25.
Keywords: automorphs, involutions.

defined by

$$(x,y,z) \mapsto \begin{cases} (x-2y,\ x-y+z,\ y) & \text{if } x > 2y\,, \\ (2y-x,\ y,\ x-y+z) & \text{if } y-z < x < 2y\,, \\ (x+2z,\ z,\ y-x-z) & \text{if } x < y-z \end{cases} \tag{1}$$

has exactly one fixed point, namely $\left(1,1,\frac{p-1}{4}\right)$. This means that $|S|$ is odd and so the involution $(x,y,z) \mapsto (x,z,y)$ must have a fixed point.

The essential ingredients of this proof were already present in Heath-Brown's paper, but he used three sets instead of one. Notice that each of the individual transformations $(x,y,z) \mapsto (x-2y, x-y+z, y)$, $(x,y,z) \mapsto (2y-x, y, x-y+z)$ and $(x,y,z) \mapsto (x+2z, z, y-x-z)$ is an *automorph* of the ternary form $x^2+4yz$ in the sense that they each leave it unchanged.

The corresponding theorem for $x^2+2y^2$ is that each prime congruent to 1 or 3 modulo 8 is of the form $x^2+2y^2$ and by looking at automorphs of the form $x^2+2yz$ I constructed the following short proof [2] which gives the result for primes congruent to 3 modulo 8.

Let $p$ be an odd prime and consider the finite, non-empty set $S=\{(x,y,z)\in \mathbb{N}^3 : x^2+2yz=p\}$. Define a map from $S$ to itself as follows:

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

It is elementary, though a little tedious, to check that this is a well-defined map from $S$ to $S$ which is actually an involution. Further, when we impose the restriction $p \equiv 3 \pmod 8$, there is only one fixed point, namely $\left(1,1,\frac{p-1}{2}\right)$ which occurs in the second branch of the involution. This means that in this case $|S|$ is odd, so again the involution $(x,y,z) \mapsto (x,z,y)$ must have a fixed point giving the result. When $p \equiv 1 \pmod 8$, there are also fixed points in the third and fourth branches, but to know that they exist we have to know that we can solve $p=(x+z)^2+z^2$ in the case of the third branch and $p=(x+2z)^2-2z^2$ in the fourth. So we no longer can argue independently of any background knowledge.

In order to phrase these proofs in the language of automorphs we first observe that we can express any quadratic form $\sum_{i\leqslant j} a_{ij}x_ix_j$ as a matrix product $\frac{1}{2}\boldsymbol{x}'A\boldsymbol{x}$ where $A$ is a symmetric matrix formed from the coefficients and $\boldsymbol{x}$ is the column vector of variables. The $\frac{1}{2}$ is only there because I use non-Gaussian notation but in this problem it makes no difference. An automorph of the form is then a matrix $\mathcal{U}$ such that

$$\mathcal{U}'A\mathcal{U} = A\,, \tag{3}$$

where I denote the transpose of $\mathcal{U}$ by $\mathcal{U}'$. This property means that the form is unaltered by the change of variables $\mathbf{x} \mapsto \mathcal{U}\mathbf{x}$.

For example the ternary form $x^2 + 4yz$ has non-Gaussian coefficient matrix $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 4 \\ 0 & 4 & 0 \end{pmatrix}$ and has the automorphs

$$\mathcal{R}_1 = \begin{pmatrix} 1 & -2 & 0 \\ 1 & -1 & 1 \\ 0 & 1 & 0 \end{pmatrix} \qquad \text{and} \qquad \mathcal{T} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

These are both of finite order since $\mathcal{R}_1^6 = \mathcal{T}^2 = \mathcal{I}$. Also $(\mathcal{T}\mathcal{R}_1)^2 = \mathcal{I}$. So the transformation (1) can be written as

$$\mathbf{x} \mapsto \begin{cases} \mathcal{R}_1\mathbf{x} & \text{if } x > 2y\,, \\ \mathcal{T}\mathcal{R}_1\mathbf{x} & \text{if } y - z < x < 2y\,, \\ \mathcal{R}_1^5\mathbf{x} & \text{if } x < y - z\,. \end{cases} \tag{4}$$

It is now clearer why this is an involution, since when the transformation is applied twice, the second branch is followed by itself and it is of order 2, and the first and third branches follow each other and they are inverses.

Similarly the ternary form $x^2 + 2yz$ has the automorphs

$$\mathcal{R}_2 = \begin{pmatrix} 1 & -2 & 0 \\ 2 & -2 & 1 \\ 0 & 1 & 0 \end{pmatrix} \qquad \text{and} \qquad \mathcal{T} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

and $\mathcal{R}_2^4 = \mathcal{T}^2 = (\mathcal{T}\mathcal{R}_2)^2 = (\mathcal{T}\mathcal{R}_2^2)^2 = \mathcal{I}$. So the involution (2) can be written as

$$\mathbf{x} \mapsto \begin{cases} \mathcal{R}_2\mathbf{x} & \text{if } y < x/2\,, \\ \mathcal{T}\mathcal{R}_2\mathbf{x} & \text{if } x/2 < y < x + z/2\,, \\ -\mathcal{R}_2^2\mathbf{x} & \text{if } x + z/2 < y < \frac{3}{2}x + z\,, \\ -\mathcal{T}\mathcal{R}_2^2\mathbf{x} & \text{if } \frac{3}{2}x + z < y < 2x + 2z\,, \\ \mathcal{R}_2^3\mathbf{x} & \text{if } y > 2x + 2z\,, \end{cases} \tag{5}$$

and again the middle branches are of order 2 and the first and last are inverses.

In [8] Watson gives a general way to construct automorphs of any form. However in the above examples the important automorphs come from the fact that for any natural number $n$ the form $nx^2 + 4yz$ has the automorphs

$$\mathcal{R}_n = \begin{pmatrix} 1 & -2 & 0 \\ n & -n & 1 \\ 0 & 1 & 0 \end{pmatrix} \qquad \text{and} \qquad \mathcal{T} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}. \tag{6}$$

Here $(\mathcal{T}\mathcal{R}_n)^2 = \mathcal{T}^2 = \mathcal{I}$ for every $n$ and $\mathcal{R}_n$ has order 6, 4, 6 for $n = 1, 2, 3$, respectively. The fact that $\mathcal{R}_3$ has finite order suggests that $\mathcal{T}$ and powers of $\mathcal{R}_3$

might very likely produce an involution on the set $\{(x,y,z)\in\mathbb{N}^3\colon\ 3x^2+4yz=p\}$. They do and it is given by

$$\mathbf{x}\mapsto\begin{cases}\mathcal{R}_3\mathbf{x} & \text{if } y<x/2\,,\\ \mathcal{T}\mathcal{R}_3\mathbf{x} & \text{if } x/2<y<x+z/3\,,\\ -\mathcal{R}_3^2\mathbf{x} & \text{if } x+z/3<y<\frac{5}{4}x+\frac{1}{2}z\,,\\ -\mathcal{T}\mathcal{R}_3^2\mathbf{x} & \text{if } \frac{5}{4}x+\frac{1}{2}z<y<\frac{3}{2}x+\frac{3}{4}z\,,\\ \mathcal{R}_3^3\mathbf{x} & \text{if } \frac{3}{2}x+\frac{3}{4}z<y<\frac{7}{4}x+z\,,\\ \mathcal{T}\mathcal{R}_3^3\mathbf{x} & \text{if } \frac{7}{4}x+z<y<2x+\frac{4}{3}z\,,\\ -\mathcal{R}_3^4\mathbf{x} & \text{if } 2x+\frac{4}{3}z<y<\frac{5}{2}x+2z\,,\\ -\mathcal{T}\mathcal{R}_3^4\mathbf{x} & \text{if } \frac{5}{2}x+2z<y<3x+3z\,,\\ \mathcal{R}_3^5\mathbf{x} & \text{if } y>3x+3z\,.\end{cases}\tag{7}$$

This is an involution because each branch is followed by its inverse when the whole transformation is applied twice. What is more remarkable is that if we restrict $p$ to be congruent to 7 modulo 12, the transformation turns out to have just one fixed point, namely $\left(1,1,\frac{p-3}{4}\right)$ which occurs in the second branch. So when $p\equiv 7 \pmod{12}$ we get a short[1] proof that $p$ is of the form $3x^2+(2y)^2$. See also [3].

Attila Pethö pointed out in conversation in Liptovský Ján that for $n\ge 4$ the eigenvalues of $\mathcal{R}_n$ are not all roots of unity, so it has infinite order; and he asked whether there are any other suitable matrices of finite order which could be viewed as automorphs of a ternary form and might lead to similar involutions. There are, but not many lead to short proofs. Using the matrix $\mathcal{T}$ above together with one other automorph in each case it is possible to construct involutions for the set $\{(x,y,z)\in\mathbb{N}^3 : ax^2+byz=p\}$ for $(a,b)=(1,1)$, $(1,2)$, $(1,3)$, $(1,4)$, $(1,8)$, $(1,12)$, $(2,1)$, $(3,1)$ and $(3,4)$. It would be interesting to know if involutions can be constructed in a similar way for any other such sets. I have discussed above the short proofs arising from the cases $(1,2)$, $(1,4)$ and $(3,4)$. There is also another short proof of the result about primes congruent to 3 modulo 8 coming from the case $(2,1)$ (see [3]). However there does not seem to be a direct proof of the result that primes congruent to 1 modulo 8 are of the form $x^2+2y^2$. Although that is frustrating, it is not surprising that there should only be a few of these direct proofs, since we should not expect them to work when there is more than one equivalence class of forms in the same genus.

[1] perhaps direct would be more accurate!

## REFERENCES

[1] 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.

[2] JACKSON, T.: *A short proof that every prime* $p \equiv 3 \pmod 8$ *is of the form* $x^2 + 2y^2$, Amer. Math. Monthly **107** (2000), 447.

[3] JACKSON, T.: *Direct proofs of some of Euler's results.* in: Proceedings of the Turku Number Theory Symposium in memory of Kustaa Inkeri, de Gruyter, Berlin, 2001, 163–166.

[4] GIRARD, A.: L'arith de Simon Stevin ... annotations par A. Girard, Leide, 1625, 622; *cited in* L. E. Dickson, History of the Theory of Numbers, vol. 2, p. 227, Carnegie Institute, 1919.

[5] de FERMAT, P.: letter to Mersenne, 25 December 1640 and letter to Carcavi, 14 August 1659; *cited in* L. E. Dickson, History of the Theory of Numbers, vol. 2, p. 228, Carnegie Institute, 1919.

[6] EULER, L.: letter to Goldbach, 12 April 1749; *cited in* L. E. Dickson, History of the Theory of Numbers, vol. 2, p. 231, Carnegie Institute, 1919.

[7] HEATH-BROWN, D. R.: *Fermat's two-squares theorem*, Invariant (1984), 3–5.

[8] WATSON, G. L.: *Integral Quadratic Forms*, Cambridge University Press, Cambridge, 1960.

Received October 21, 1999

*Department of Mathematics*
*University of York*
*Heslington, York*
*YO10 5DD*
*GREAT BRITAIN*
*E-mail*: thj1@york.ac.uk