PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 59 (73), 1996, 18–30

INVOLUTIONS ASSOCIATED WITH SUMS OF TWO SQUARES

P. Shiu

Communicated by Aleksandar Ivić

Abstract. In 1984 D. R. Heath-Brown constructed two involutions from which a new and simple proof of Fermat's theorem on the decomposition of a prime $p \equiv 1 \pmod 4$ as a sum of two squares was derived. An algorithm based on the composition of the two involutions is constructed for the decomposition of p, and the method can also be used for the factorisations of suitable composite numbers. The process corresponds to the continued fraction expansion of a reduced quadratic irrational related to $\sqrt{p}$, and the period of the composite map is the sum of the relevant partial quotients.

1. Introduction

For a positive integer $n \equiv 1 \pmod 4$, not a perfect square, we let

$$S = S(n) = \{(x, y, z) : x, y, z \in \mathbb{N},\, x^2 + 4yz = n\}. \tag{1.1}$$

There is a natural involution on S, namely $b : S \to S$ given by $b(x, y, z) = (x, z, y)$. We call the fixed-points of this involution the b-points on S. These are points of the form (x, y, y), and they correspond to the decomposition $n = x^2 + (2y)^2$ as a sum of two squares. There are, of course, numbers $n \equiv 1 \pmod 4$ for which such a decomposition is impossible, and so there will be no b-point on such $S(n)$. However, if the cardinal $|S|$ of the set S is an *odd* number, then there must be at least one b-point. This is because, for any involution on any finite set, the number of fixed-points of the involution must have the same parity as that of the cardinal of the set.

Observe that the positive integer x corresponding to the vector $\mathbf{v} = (x, y, z) \in S$ is necessarily odd, and that $x \neq |y - z|$ because n is not a square. In 1984

AMS Subject Classification (1991): Primary 11A51; Secondary 11A55, 11Y05

Key Words and Phrases: Fermat's two square theorem, involutions, periods factorisation, continued fractions

D. R. Heath-Brown [**2**] gave a beautiful new proof of Fermat's two squares theorem by constructing the following involution h on S:

$$h(x,y,z) = \begin{cases} (x+2z, \quad z \quad , y-x-z) & \text{if} \quad x < y-z, \\ (2y-x, \quad y \quad , x-y+z) & \text{if} \quad y-z < x < 2y, \\ (x-2y, x-y+z, \quad y \quad) & \text{if} \quad 2y < x. \end{cases} \tag{1.2}$$

As we shall see in Section 4, it is rather easy to check that h is indeed an involution on S. The fixed-points of h, which we shall call the h-points on S, are now of the form (x,x,z), and they correspond to the factorisation $n = x(x+4z)$. There is always at least one h-point; for if we write $n = 4k+1$, then $(1,1,k)$ is an h-point. Indeed, Heath-Brown's argument is that if n is prime, then $(1,1,k)$ is the only h-point, and therefore $|S|$ is odd. When combined with the earlier observation on the possible b-points on S, the argument now gives what D. Zagier [**7**] described as a "one-sentence proof" of Fermat's theorem, which states that every prime $p \equiv 1 \pmod 4$ is a sum of two squares. It is interesting that the uniqueness part of the theorem does not follow immediately from the argument. Indeed, as it stands at the moment, the proof is a purely existence one in the sense that it has not yet led to a construction of the b-point on S.

Actually very much more can be said on Heath-Brown's proof by considering the map $f = b \circ h$ on the set S. This composite map f possesses considerably enhanced power which we exploit to extend the basic method on the use of two involutions. When n is a prime, the b-point can now be constructed by an interesting algorithm corresponding to the development of the continued fraction expansion for a certain reduced quadratic irrational, and in particular the period of the composite map is the sum of the relevant partial quotients.

2. The Partitioning of S into Orbits

We first establish a result which is applicable to a general finite set S on which two arbitrary involutions b and h have been defined. Let f^0 be the identity map, $f = b \circ h$ and $f^{m+1} = f \circ f^m$ for $m = 0, 1, 2, \ldots$. It will be convenient to omit the $\circ$ in the formation of the composition of maps in the following. For any $\mathbf{v} \in S$, we consider the sequence $\big(\mathbf{v}, f(\mathbf{v}), f^2(\mathbf{v}), \ldots\big)$. Since there are finitely many points in S, and the map f is a bijection on S, it is clear that this sequence is purely periodic in the sense that there is a positive integer L such that $f^L(\mathbf{v}) = \mathbf{v}$. The least such L is the period of an *orbit* on S, namely the points

$$\mathbf{v}_m = f^{m-1}(\mathbf{v}), \qquad m = 1, 2, \ldots, L. \tag{2.1}$$

Being in the same orbit is obviously an equivalence relation, and the set S is now partitioned into orbits whose periods have the sum $|S|$.

We call the b-points and the h-points the special points of different types, and an orbit is called special or ordinary according to whether it contains special points or not. If an orbit has period 1, then the point concerned is a fixed point of the composite map f. This fixed point may or may not be a special point, so that there are special and ordinary orbits with period 1. In fact the point in such a special orbit must be a special point of both types, while the point $\mathbf{v}$ in such an ordinary orbit must satisfy $b(\mathbf{v}) = h(\mathbf{v}) \neq \mathbf{v}$, and in this case $b(\mathbf{v})$ forms a distinct ordinary orbit with period 1. Our main result here is that a special orbit with period $L > 1$ contains exactly two special points, which are of the same type if and only if L is even. This can be proved by the introduction of $g = hb$, the inverse of f. The inverse of f^m is then given by $g^m = h(bh \cdots bh)b = hf^{m-1}b = bf^m b = hf^m h$, and we remark that $f^i(\mathbf{v}) = g^j(\mathbf{v})$, $i + j \equiv 0 \pmod{L}$ for any point $\mathbf{v}$ in an orbit with period L.

THEOREM 1. *Let $\mathbf{v}_1$ be a special point, and set $\theta = 0$ or 1 according to whether $\mathbf{v}_1$ is a b-point or an h-point. Suppose that the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_L$ in* (2.1) *form an orbit with period $L > 1$. Then*

$$\begin{aligned} \mathbf{v}_i = h(\mathbf{v}_j) &\quad \textit{if and only if} \quad i + j \equiv \theta + 1 \pmod{L}, \\ \mathbf{v}_i = b(\mathbf{v}_j) &\quad \textit{if and only if} \quad i + j \equiv \theta + 2 \pmod{L}. \end{aligned}$$

Furthermore, if $t = [(L+\theta)/2]$, then $\mathbf{v}_{t+1}$ is a special point of the same type to, or different type from, $\mathbf{v}_1$ according to whether L is even or odd, and $\mathbf{v}_1, \mathbf{v}_{t+1}$ are the only two special points on the orbit.

Proof. We consider the case when $\mathbf{v}_1$ is a b-point, so that $\theta = 0$. Let i, j be positive integers satisfying $i + j = L + 1$. Then, by (2.1), $\mathbf{v}_j = f^{j-1}(\mathbf{v}_1) = f^{L-i}(\mathbf{v}_1) = g^i(\mathbf{v}_1)$ so that, on using $b(\mathbf{v}_1) = \mathbf{v}_1$, we have $h(\mathbf{v}_j) = hg^i(\mathbf{v}_1) = f^{i-1}b(\mathbf{v}_1) = f^{i-1}(\mathbf{v}_1) = \mathbf{v}_i$. Similarly, if $i + j = L + 2$, then $\mathbf{v}_j = g^{i-1}(\mathbf{v}_1)$, and we find that $b(\mathbf{v}_j) = \mathbf{v}_i$. Since b and h are injective it is clear that the conditions on i, j are also necessary.

When $i = j = t + 1$ we have $i + j = 2t + 2$, which is congruent to2 (mod 2)t and also congruent to 1 (mod $2t + 1$). Therefore $\mathbf{v}_{t+1}$ is a b-point or an h-point depending on whether $L = 2t$ or $2t + 1$, and it is clear that there are no special points besides $\mathbf{v}_1$ and $\mathbf{v}_{t+1}$.

The case when $\mathbf{v}_1$ is an h-point is similar, and the theorem is proved. □

The argument above shows that if $\mathbf{v}$ is any point on S such that $b(\mathbf{v}) = f^m(\mathbf{v})$ for some m, and if $t = [m/2]$, then $f^t(\mathbf{v})$ is a b-point or an h-point according to whether m is even or odd. It follows that if $\mathbf{v}_1, \ldots, \mathbf{v}_L$ form an ordinary orbit, then $b(\mathbf{v}_1), \ldots, b(\mathbf{v}_L)$ form a distinct ordinary orbit, and we may describe these two orbits as a "conjugate pair", so that the number of ordinary orbits having a given period must be even.

3. The Special Points on $S(n)$

We now return to our problem on the set $S = S(n)$ in (1.1) together with the involution b and the involution h defined in (1.2). We already mentioned that the b-points correspond to the decompositions of $n = 4k + 1$ as sums of two squares, while the h-points are associated with the factorisations of n. By the *principal orbit* we mean the special orbit containing the h-point $(1,1,k)$, and we shall write $L(n)$ for its period. Thus, given a prime $p = 4k+1$, we know by Theorem 1 that the principal orbit must contain a b-point, since $(1,1,k)$ is the only h-point on $S(p)$. The period $L(p)$ is odd, and if we start with $\mathbf{v}_1 = (1,1,k)$ and successively compute $\mathbf{v}_{m+1} = f(\mathbf{v}_m)$, then we shall arrive at the b-point $\mathbf{v}_{t+1} = (x,y,y)$ where $t = (L(p)+1)/2$. Similarly, if $n = 4k+1$ is not a sum of two squares, say a product of two distinct primes $p \equiv 3 \pmod 4$, so that there is no b-point on $S(n)$, then the principal orbit now has an even period $L(n)$, and tracing out the orbit will lead to the other h-point $\mathbf{v}_{t+1} = f^t(\mathbf{v}_1) = (x,x,z)$, where $t = L(n)/2$ and $n = x(x+4z)$ is a non-trivial factorisation of n.

Although the method is now constructive, the accompanying algorithm is extremely clumsy in that we need to compute half of the points on the principal orbit in order to locate the remaining special point. The amount of computation can be substantially reduced by a modification of the method whereby we need only compute a subset of the points which we call *nodes* on an orbit. We shall describe the modification in the next two sections, where we also derive a formula for $L(n)$ as a by-product.

If $L(n) = |S(n)|$, then the principal orbit is the only orbit on $S(n)$, and n must be either a prime $p \equiv 1 \pmod 4$, or a product of two distinct primes $p \equiv 3 \pmod 4$, depending on whether $L(n)$ is odd or even. However, there are primes such as $p = 229$ for which $S(p)$ possesses ordinary orbits besides the principal orbit. It will therefore be appropriate to make some remarks on $|S(n)|$ and also on the numbers of special points. From (1.1) we find that, corresponding to each fixed odd $x < \sqrt{n}$, the solutions to $4yz = n - x^2$ form the vectors $(x,y,z) \in S$. Therefore $|S(n)|$ is the value of $\sum d\big((n-x^2)/4\big)$, where $d(u)$ counts the divisors of u, and x runs over the odd numbers less than $\sqrt{n}$ in the sum. Since each $u > 1$ has at least two divisors, it follows that if we write $m = [(1+\sqrt{n}\,)/2]$, the number of odd numbers less than $\sqrt{n}$, then $|S(n)| \geq 2m-1$, the largest odd number less than $\sqrt{n}$. Indeed, for fixed x, the equation $x^2 + 4yz = n$ always has the trivial solutions with $y = 1$ or $z = 1$, and, as we shall see, the vectors corresponding to these solutions are in the principal orbit, so that

$$|S(n)| \geq L(n) \geq 2m-1,$$

and in fact $L(n) = 2m-1$ when and only when $n = (2m-1)^2 + 4$. However $|S(n)| = 2m-1$ can only happen for those $n = (2m-1)^2+4$ with the additional property that $(n-x^2)/4$ is a prime for each odd $x < 2m-1$. This happens, for example, when $n = 5, 13, 29, 53, 173$ and 293. Thus, when $n = 293$ and $x = 1,3,5,7,9,11,13,15$, the values for $(n-x^2)/4$ are the primes 73, 71, 67, 61, 53, 43, 31, 17. It seems likely that $|S(n)| \gg \sqrt{n}\log n$ as $n \to \infty$, which implies that there are only finitely many such numbers n.

The number of h-points in $S(n)$ is the number of solutions to the equation $n = x(x+4z)$, namely the number of divisors x of n satisfying $x < \sqrt{n}$. Since n is not a square, the number concerned is precisely $d(n)/2$. Similarly, the number of b-points in $S(n)$ is $r(n)/8$ where $r(n)$ is the usual arithmetic function which counts the representations of n as a sum of two squares of integers, positive or negative, and taking account of the ordering of the squares. Since $n \equiv 1 \pmod 4$, the total number of prime divisors $p \equiv 3 \pmod 4$ of n must be even. Let $d_1(n)$ and $d_3(n)$ count the divisors x of n satisfying $x \equiv 1 \pmod 4$ and $x \equiv 3 \pmod 4$ respectively. Then $d(n) = d_1(n) + d_3(n)$, and it is well known that $r(n)/4 = d_1(n) - d_3(n)$. It follows that $d_1(n)$ is the total number of special points on $S(n)$, while $d_3(n)$ represents the excess number of h-points over the b-points. In particular, if $d_3(n) = 0$, that is if n is not divisible by a prime $p \equiv 3 \pmod 4$, then there are $d(n)$ special points on $S(n)$ with exactly half for each of the two types. On the other hand, if $d_3(n) = d_1(n)$, which happens when and only when the prime factorisation of n possesses an exact odd power of a prime $p \equiv 3 \pmod 4$, then all the $d_1(n)$ special points on $S(n)$ are h-points.

4. Factorisation of f^M and the Nodes on $S(n)$

For a more efficient method to locate the special points on the principal orbit we need to design a scheme whereby, given any point $\mathbf{v} \in S$ and any integer M, the point $f^M(\mathbf{v})$ can be obtained without having to compute $f^m(\mathbf{v})$ for every $m \leq M$. Since $f = bh$, we first examine the maps h and b, and we observe that the defining equations for these involutions are linear in the coordinates of the vector concerned. However, we also note that the set of equations to be used for h is not fixed, but is dependent on the coordinates of the vector $\mathbf{v}$ to which the involution h is to apply. It is natural to apply the machinery of linear algebra and use matrices of order 3 to represent maps on $S(n)$. From (1.2) there are three matrices

$$H_1 = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 0 & 1 \\ -1 & 1 & -1 \end{pmatrix}, \qquad H_2 = \begin{pmatrix} -1 & 2 & 0 \\ 0 & 1 & 0 \\ 1 & -1 & 1 \end{pmatrix}, \qquad H_3 = \begin{pmatrix} 1 & -2 & 0 \\ 1 & -1 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

for the involution h. Let $\mathbf{v} = (x, y, z)$ and $\mathbf{v}' = h(\mathbf{v}) = (x', y', z')$, and we allow such row vectors to be considered as column vectors when they appear in an equation involving matrices, so that we may write $\mathbf{v}' = H_i\mathbf{v}$. Now the choice of the value for i depends on the values of the coodinates x, y and z, namely $i = 1, 2, 3$ corresponding to the conditions

$$\text{(i)} \quad x < y - z, \qquad \text{(ii)} \quad y - z < x < 2y, \qquad \text{(iii)} \quad 2y < x$$

respectively, as given in (1.2). We remark that, on eliminating z from $n = x^2 + 4yz$, we may rewrite these three conditions as (i) $2y - x > \sqrt{n}$, (ii) $0 < 2y - x < \sqrt{n}$, (iii) $2y - x < 0$. That h is an involution can be established from the following observation. Suppose that condition (i) holds for a certain vector $\mathbf{v}$. Then, after an application of H_1, the image vector $\mathbf{v}'$ now satisfies condition (iii). Similarly the image of any vector under H_3 will always satisfy condition (i), whereas if condition (ii) holds for a vector, then it also holds for its image vector under H_2.

But $H_2^2 = H_1 H_3 = I$, the identity matrix, so that h is indeed an involution. We now write

$$J = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \qquad H = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

so that B is the matrix for the involution b, and that

$$J^2 = B^2 = H^2 = I, \qquad J = HB = BH, \qquad H = H_3 H_2 = H_2 H_1.$$

It will be misleading to describe J and H as matrices representing involutions since they do not represent maps from $S(n)$ into itself, because, under such maps, the image of the first coordinate for a vector on $S(n)$ is negative. Nevertheless we can use these matrices in various useful ways.

The matrices representing the map f are given by $F_i = BH_i$, with the previously stated accompanying conditions for the appropriate value for i. We need only concentrate on one of them since they are related via the matrix H. In fact we have $F_1 = BH_1 = B(H_2 H_2)H_1 = (BH_2)H$ and $F_3 = BH_3 = (JH)(HH_2) = JH_2 = H(BH_2)$, so that

$$F_1 = F_2 H, \qquad \text{and} \qquad F_3 = HF_2,$$

and we remark that $F_1^m F_2 = F_2 F_3^m$.

Returning to the computation of $f^M(\mathbf{v})$, we now consider the matrix Φ which represents the map f^M applied to $\mathbf{v}$. Again this matrix Φ will depend not only on M but also on $\mathbf{v}$, and in fact

$$\Phi = F_{i_M} \cdots F_{i_1}, \tag{4.1}$$

where F_{i_m} is the matrix for f applied to the point $f^{m-1}(\mathbf{v})$. The crux of the matter is that although this matrix Φ can be rather complicated we can always factorise it into matrices of the form

$$\phi_m = \begin{pmatrix} -1 & 2m & 0 \\ m & -m^2 & 1 \\ 0 & 1 & 0 \end{pmatrix}. \tag{4.2}$$

We shall see that, with an appropriate definition for a node, each ϕ_m represents the map f^m applied to a node, and the image of $\mathbf{v}$ under f^M can then be obtained by tracing out only the nodes "between" $\mathbf{v}$ and $f^M(\mathbf{v})$. Actually $\phi_m = HF_3^m = F_1^m H$, so that $F_2 = \phi_1$. In fact, for $\lambda, \mu \geq 0$ and $m = \lambda + 1 + \mu$, we have

$$\begin{aligned} \phi_m F_3^{-\mu} F_2^{-1} F_1^{-\lambda} &= HF_3^{m-\mu} F_2^{-1} F_1^{-\lambda} = HF_3^{1+\lambda} F_2^{-1} F_1^{-\lambda} \\ &= HF_3^{\lambda} HF_1^{-\lambda} = F_1^{\lambda} HHF_1^{-\lambda} = I, \end{aligned}$$

so that

$$F_1^\lambda F_2 F_3^\mu = \phi_m \qquad \text{when} \qquad \lambda + 1 + \mu = m. \tag{4.3}$$

It is important to observe that the combination F_1F_3 never occurs in (4.1). This is because, under the condition (iii), namely $x > 2y$ for the application of F_3, we have $f(x,y,z) = (x-2y, y, x-y+z)$, and now the condition (i) for F_1 becomes $x - 2y < y - (x - y + z)$, that is $2x < 4y - z$ which contradicts $x > 2y$, so that the image of a vector under F_3 can only be mapped via another F_3 or F_2. We may now group the matrices in (4.1) in blocks of the form $F_1^\lambda F_2 F_3^\mu$ and apply (4.3) to simplify the matrix representation of Φ. For example, we have

$$F_1F_2F_3^9F_2^2F_1^8F_2F_3^7F_1F_2F_3 = (F_1F_2F_3^9)F_2^2(F_1^8F_2F_3^7)(F_1F_2F_3) = \phi_{11}\phi_1^2\phi_{16}\phi_3,$$

where the number of terms F_i involved is equal to the sum of the suffices m for the terms ϕ_m, and we remark that the number of such terms required is the number of times i takes the value 2. For a general Φ in (4.1), there are numbers $m_1, \dots, m_s$ such that $m_1 + \cdots + m_s = M$ and

$$\Phi = H^\alpha \phi_{m_s} \cdots \phi_{m_1} H^\beta, \tag{4.4}$$

where $\alpha = 1$ if and only if $i_M = 3$, and $\beta = 1$ if and only if $i_1 = 1$, and that the value for s is the number of times i_m takes the value 2 in the original formula for Φ in (4.1).

In order to determine the values m_i for the factorisation of Φ in (4.4) we now define a *node* to be a vector $\mathbf{v}$ with the property that $\mathbf{v}$ does *not* satisfy condition (i), and that $g(\mathbf{v})$ does *not* satisfy condition (iii). Another way of describing a node is that it is the image of a vector under the map f^m where m is taken as large as possible, subject to the condition that the matrix for f^m has the form F_1^m or ϕ_m. In fact, if the vector concerned satisfies condition (i), then we use F_1^m, otherwise we use ϕ_m, and the maximal property of m ensures that condition (i) will not hold at a node. The value for m can be determined as follows. Suppose that $\mathbf{v} = (x,y,z)$ does not satisfy condition (i), so that the matrix ϕ_m is applicable. From (4.2) we find that $x \mapsto -x + 2my$, so that we need to have $0 < -x + 2my < \sqrt{n}$, if we wish to stay within $S(n)$. It is worth remarking that the second inequality here can also be obtained by requiring that the image of y should be positive. We may therefore choose any m in the range $1 \le m < (x + \sqrt{n})/2y$. However, for the application of ϕ_m as given by (4.2), there is also the condition (4.3) which implies $m > \mu$. Thus, if $\mathbf{v}$ satisfies condition (iii) initially and that the image vector $f^m(\mathbf{v})$ does not satisfy condition (i), so that the matrix concerned is F_3^m, then we need to apply $H\phi_m$ intead of just ϕ_m in order to stay on $S(n)$. In any case, in order to reach a node we need to set

$$m = \left[\frac{x + \sqrt{n}}{2y}\right]. \tag{4.5}$$

If the vector $\mathbf{v}$ satisfies the condition (i) initially, so that we need to apply F_1^m, then we write $F_1^m = \phi_m H$ and apply the same formula for m, except that we use the coordinates of the image vector under H instead.

By the *successor node* to the node $\mathbf{v}$ we mean the node $\mathbf{v}' = f^m(\mathbf{v})$ where f^m has the matrix ϕ_m, and we say that $\mathbf{v}'$ has *order* m. Thus, in order to obtain $f^M(\mathbf{v})$ more efficiently, we first compute the node corresponding to $\mathbf{v}$, and then proceed from node to successor node until we reach $f^M(\mathbf{v})$ with Φ in (4.4), finishing with $H\phi_m$ if necessary. Note that there is always exactly one vector satisfying the condition (ii) between any two successive nodes, inclusive of the successor node.

The inverse of the matrix ϕ_m in (4.2) is given by $\gamma_m = B\phi_m B$, and so the inverse of Φ in (4.4) has the form

$$\Gamma = \Phi^{-1} = H^\beta \gamma_{m_1} \cdots \gamma_{m_s} H^\alpha = H^\beta B \phi_{m_1} \cdots \phi_{m_s} B H^\alpha .$$

The following lemma is important for our results in the next section.

Lemma 1. *Let* $\mathbf{v}$ *be a node whose successor node* $\mathbf{v}'$ *has order* m. *Then* $b(\mathbf{v}')$ *and* $b(\mathbf{v})$ *are also successive nodes, and* $b(\mathbf{v})$ *has order* m.

Proof. We first prove that the image of a node $\mathbf{v}$ under b is a node. Recall that if a vector satisfies condition (i), then its image under h must satisfy condition (iii). Since h is an involution, this means that if a vector does not satisfy condition (iii), then its image under h does not satisfy condition (i). By hypothesis, $g(\mathbf{v})$ does not satisfy condition (iii), so that $h\big(g(\mathbf{v})\big) = b(\mathbf{v})$ does not satisfy condition (i). We also have $g\big(b(\mathbf{v})\big) = h(\mathbf{v})$, and by a similar argument, this vector cannot satisfy condition (iii) because $\mathbf{v}$ does not satisfy condition (i). Therefore $b(\mathbf{v})$, and also $b(\mathbf{v}')$, are nodes, and we have

$$b(\mathbf{v}) = bg^m(\mathbf{v}') = b(bf^m b)(\mathbf{v}') = f^m\big(b(\mathbf{v}')\big).$$

It remains to show that the matrix for f^m at the node $b(\mathbf{v}')$ is of the form ϕ_m. But we know that the matrix for g^m at $\mathbf{v}'$ is γ_m, so that the required matrix for f^m at $b(\mathbf{v}')$ must have the form $B\gamma_m B = \phi_m$. □

5. Computing a Sub-orbit and the Special Points

We can now determine the period of an orbit associated with a given point on $S(n)$ by computing only the nodes on this orbit. For a given point $\mathbf{v} = (x, y, z)$ we first check that condition (i) does not hold. If the condition does hold, then we replace $\mathbf{v}$ by $H\mathbf{v}$. We then set $m = [(x + \sqrt{n})/2y]$ in accordance with (4.5), and proceed to calculate the first node $\mathbf{v}_1 = (x_1, y_1, z_1) = f^m(\mathbf{v})$. The matrix for f^m is now given by ϕ_m in (4.2), so that

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} = \begin{pmatrix} -1 & 2m & 0 \\ m & -m^2 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2my - x \\ mx - m^2 y + z \\ y \end{pmatrix}.$$

We then successively calculate m_i and $\mathbf{v}_{i+1} = (x_{i+1}, y_{i+1}, z_{i+1})$ for $i = 1, 2, \ldots$ from

$$m_i = \left[\frac{x_i + \sqrt{n}}{2y_i}\right] \qquad \text{and} \qquad \begin{pmatrix} x_{i+1} \\ y_{i+1} \\ z_{i+1} \end{pmatrix} = \begin{pmatrix} -1 & 2m_i & 0 \\ m_i & -m_i^2 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_i \\ y_i \\ z_i \end{pmatrix}. \tag{5.1}$$

According to (4.5), this generates a sequence of nodes $\mathbf{v}_i = (x_i, y_i, z_i)$ given by $\mathbf{v}_{i+1} = f^{m_i}(\mathbf{v}_i)$, with the associated sequence of orders $(m_1, m_2, \dots)$, where m_i is the order of $\mathbf{v}_{i+1}$. Since the mapping from node to successor node is injective, these sequences must be purely periodic so that there exists a positive integer s such that $m_{s+1} = m_1$, and $\mathbf{v}_{s+1} = \mathbf{v}_1$. The least such s is the period for the sub-orbit of nodes $\mathbf{v}_1, \dots, \mathbf{v}_s$, while the period for the orbit itself is $m_1 + \cdots + m_s$.

The case concerning the special orbits is particularly interesting. For example, we may take the h-point $\mathbf{v} = (1, 1, k)$, where $n = 4k+1$, for the determination of $L(n)$, the period of the principal orbit. In general, let $a < \sqrt{n}$ be a divisor of $n \equiv 1 \pmod 4$, and write $n = a(a+4k')$, so that $\mathbf{v} = (a, a, k')$ is an h-point on $S(n)$. Let $\mathbf{v}_1, \dots, \mathbf{v}_s$ be the nodes generated by the algorithm (5.1), with $\mathbf{v}_1$ being the node associated with $\mathbf{v}$. We find that $m_1, \dots, m_{s-1}$ are symmetrical, that is $m_i = m_j$ for $i+j = s$, and that $m_s = x_1 = 2m-1$. There is a central term for the symmetrical part when and only when $s = 2t$ is even, and in this case the central term m_t is odd. Since m_s is also odd, it follows that s and $m_1 + \cdots + m_s$ always have the same parity. The nodes $\mathbf{v}_i$ also exhibit symmetry in the form of $\mathbf{v}_i = b(\mathbf{v}_j)$ for $i + j = s+1$. It therefore suffices to compute only half of the sub-orbit, but we will need a criterion on which to specify the stage when half of the nodes have been computed. The initial point $\mathbf{v} = (a, a, k')$ is not a node because $m_s > m$, and since the main purpose of the method is the determination of the special point distinct from the initial h-point on the special orbit, we may also need to know whether this special point will actually be a node. It turns out that if $s = 2t+1$ is odd, so that the required special point is a b-point, then this point is a node, and in fact it is given by $\mathbf{v}_{t+1}$. On the other hand, if $s = 2t$ is even, so that the required special point is also an h-point, then this point may or may not be a node. In fact the required h-point is given by $f^{\mu}(\mathbf{v}_t)$, where $\mu = (m_t - 1)/2$, so that it is a node if and only if the central term $m_t = 1$. These claimed properties for the special orbits associated with the algorithm (5.1) are now given in the following theorem.

Theorem 2. *Let $a < \sqrt{n}$ be a divisor of $n \equiv 1 \pmod 4$, and write $n = a(a+4k')$, so that $\mathbf{v} = (a, a, k')$ is an h-point on $S(n)$. Set $\mathbf{v}_1 = f^m(\mathbf{v})$, where $m = [(a+\sqrt{n})/2a]$, and define $m_1, m_2, \dots$ and $\mathbf{v}_2, \mathbf{v}_3, \dots$ by the algorithm* (5.1). *Then there exists a least positive integer s such that $m_{s+1} = m_1$ and $\mathbf{v}_{s+1} = \mathbf{v}_1$, so that the sequences (m_i) and $(\mathbf{v}_i)$ are purely periodic with period s. The orbit containing $\mathbf{v}$ has period $m_1 + \cdots + m_s$, and the vectors $\mathbf{v}_1, \dots, \mathbf{v}_s$ are all the nodes on this orbit. Also, $m_i = m_j$ for $i + j = s$ and $m_s = 2m-1$, and $\mathbf{v}_i = b(\mathbf{v}_j)$ for $i + j = s+1$. Moreover, the two periods $m_1 + \cdots + m_s$ and s have the same parity. Furthermore, let t be the least positive integer with the property that the two successive nodes $\mathbf{v}_t$ and $\mathbf{v}_{t+1}$ have either the first or the second coordinates repeating. Then we have the following:*

(1) (i) *If both the coordinates repeat, then $s = 1$, and $n = a^2\big((2m-1)^2 + 4\big)$.*

(2) (ii) *If only the first coordinates repeat, then $s = 2t$, and the value of m_t is odd. Furthermore, if $\mu = (m_t - 1)/2$, then $f^{\mu}(\mathbf{v}_t)$ is an h-point, which is a node if and only if $m_t = 1$.*

(3) (iii) *If only the second coordinates repeat, then $s = 2t+1$, and $\mathbf{v}_{t+1}$ is a b-point.*

Proof. The first part of the theorem has already been established. We proceed to establish the property of symmetry by first proving that $\mathbf{v}_s = b(\mathbf{v}_1)$ and $m_s = 2m-1$. The vector $b(\mathbf{v}_1) = (2ma-a, a, ma - m^2a + k')$ is also a node according to Lemma 1, and it is easy to check that the matrix for f^{2m-1} at $b(\mathbf{v}_1)$ has the form ϕ_{2m-1} which maps $b(\mathbf{v}_1)$ back to $\mathbf{v}_1$. In fact $f^{m-1}\big(b(\mathbf{v}_1)\big) = \mathbf{v} = (a, a, k')$, and the matrix here is F_3^{m-1}, while the matrix for $f^m(\mathbf{v}) = \mathbf{v}_1$ is given by $F_1^{m-1}F_2$, so that the matrix for $f^{2m-1}\big(b(\mathbf{v}_1)\big) = \mathbf{v}_1$ is given by $F_1^{m-1}F_2F_3^{m-1} = \phi_{2m-1}$ according to (4.3). This shows that $\mathbf{v}_1$ is the successor node to $b(\mathbf{v}_1)$, and its order is $2m-1$. In other words, $\mathbf{v}_s = b(\mathbf{v}_1)$ and $m_s = 2m-1$.

Next, $\mathbf{v}_2$ is the successor node to $\mathbf{v}_1$ with order m_1, and the images of $\mathbf{v}_1$ and $\mathbf{v}_2$ under b must also be a pair of successive nodes with the corresponding order according to Lemma 1. Since we already proved that $b(\mathbf{v}_1) = \mathbf{v}_s$, we must have $b(\mathbf{v}_2) = \mathbf{v}_{s-1}$, and that the order of $\mathbf{v}_s$ is m_1, which means that $m_{s-1} = m_1$. An inductive argument now shows that $b(\mathbf{v}_i) = \mathbf{v}_j$ when $i + j = s + 1$ and that $m_i = m_j$ when $i + j = s$. We remark that conversely if $\mathbf{v}_i = b(\mathbf{v}_j)$, then $i + j = s + 1$. This follows from the fact that b is injective.

Since m_s is odd, that $m_1 + \cdots + m_s$ and s have the same parity will follow if we can show that the central term of the symmetric part $m_1, \ldots, m_{s-1}$ is always odd, if this central term exists at all. Suppose then that there is a central term m_t, so that $s = 2t$ and $\mathbf{v}_t = b(\mathbf{v}_{t+1})$, which gives $y_{t+1} = z_t$. But, by (5.1), $y_{t+1} = m_t x_t - m_t^2 y_t + z_t$, so that $x_t = m_t y_t$, and since x_t is odd it follows that m_t must be odd.

We now consider case (i) of the last part of the theorem. Since $x_t^2 + 4y_t z_t = n = x_{t+1}^2 + 4y_{t+1}z_{t+1}$, it follows that if $x_t = x_{t+1}$ and $y_t = y_{t+1}$ then $z_t = z_{t+1}$, and hence $\mathbf{v}_t = \mathbf{v}_{t+1}$ which implies $s = 1$. Furthermore, the period of the orbit is $m_1 = 2m-1$, so that the first node $\mathbf{v}_1$ is already the b-point according to Theorem 1. Since $z_1 = a$, we must have $y_1 = a$, so that $n = a^2\big((2m-1)^2 + 4\big)$.

For case (ii), in which $x_t = x_{t+1}$ only, we consider the three equation for x_{t+1}, y_{t+1}, z_{t+1} in (5.1). The first equation is $x_{t+1} = 2m_t y_t - x_t$ which now gives $x_t = m_t y_t$. The second equation then yields $y_{t+1} = m_t x_t - m_t^2 y_t + z_t = z_t$, while the third equation is $z_{t+1} = y_t$. Therefore $\mathbf{v}_t = b(\mathbf{v}_{t+1})$, and so $2t + 1 = s + 1$, giving $s = 2t$. We already proved that m_t is odd, and we now write $2\mu = m_t - 1$. Then the vector $f^\mu(\mathbf{v}_t)$ is given by

$$H\phi_\mu \begin{pmatrix} x_t \\ y_t \\ z_t \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 2\mu y_t - x_t \\ \mu^2 y_t - \mu x_t + z_t \\ y_t \end{pmatrix} = \begin{pmatrix} x_t - 2\mu y_t \\ y_t \\ \mu^2 y_t - \mu x_t + z_t \end{pmatrix}.$$

But $x_t - 2\mu y_t = m_t y_t - (m_t - 1)y_t = y_t$, so that $f^\mu(\mathbf{v}_t)$ is an h-point.

Finally, for case (iii) in which $y_t = y_{t+1}$ only, we deduce at once that $\mathbf{v}_{t+1}$ is a b-point because $z_{t+1} = y_t = y_{t+1}$. Thus $\mathbf{v}_{t+1} = b(\mathbf{v}_{t+1})$, so that $2(t+1) = s + 1$, giving $s = 2t + 1$.

The proof of the theorem is complete. $\square$

We illustrate the theorem by examining the three principal orbits corresponding to $n = 1277, 879397$ and 69529.

Example 1. Let $n = 1277$. For the principal orbit we take $\mathbf{v} = (1, 1, 319)$ as the entry point, which then gives $m = 18$ and also the first node $\mathbf{v}_1 = (35, 13, 1)$. We then calculate the sequence of nodes $\mathbf{v}_i$ generated by (5.1), and it turns out that $\mathbf{v}_{10} = \mathbf{v}_1$, so that $s = 9$. In fact $m_i = 2, 1, 2, 1, 1, 2, 1, 2, 35$ for $i = 1, 2, 3, 4, 5, 6, 7, 8, 9$ respectively, and the corresponding column vectors $\mathbf{v}_i$ are:

$$\begin{pmatrix} 35 \\ 13 \\ 1 \end{pmatrix}, \begin{pmatrix} 17 \\ 19 \\ 13 \end{pmatrix}, \begin{pmatrix} 21 \\ 11 \\ 19 \end{pmatrix}, \begin{pmatrix} 23 \\ 17 \\ 11 \end{pmatrix}, \begin{pmatrix} 11 \\ 17 \\ 17 \end{pmatrix}, \begin{pmatrix} 23 \\ 11 \\ 17 \end{pmatrix}, \begin{pmatrix} 21 \\ 19 \\ 11 \end{pmatrix}, \begin{pmatrix} 17 \\ 13 \\ 19 \end{pmatrix}, \begin{pmatrix} 35 \\ 1 \\ 13 \end{pmatrix}.$$

The entry h-point $\mathbf{v}$ is not a node, while the remaining special point is the b-point $\mathbf{v}_5$, which corresponds to the decomposition $n = 11^2 + 34^2$. Observe that $y_4 = y_5$, besides the symmetry of $m_i = m_j$ for $i + j = 9$, and $\mathbf{v}_i = b(\mathbf{v}_j)$ for $i + j = 10$. The period of the principal orbit is $L(1277) = m_1 + \cdots + m_9 = 47$, and since $|S(1277)| = 47$, there is no other orbit, so that 1277 must be a prime.

Example 2. Let $n = 879397$. Here we find that $L(n) = 4138$ and $s = 412$. Since the period is even there is another h-point on the principal orbit besides the entry point. There is a central term for m_i, namely $m_t = 1$ where $t = 206$. The required h-point is a node, and is given by $\mathbf{v}_t = (863, 863, 39)$. Since this is an h-point, we must have $\mathbf{v}_{t+1} = f(\mathbf{v}_t) = b(\mathbf{v}_t) = (863, 39, 863)$, and in fact $\mathbf{v}_i = b(\mathbf{v}_j)$ when $i + j = s + 1$. We note that $x_t = x_{t+1}$ in this case.

Example 3. Let $n = 69529$. We find that $L(n) = 2590$ and $s = 384$. The central term concerned is $m_t = 11$, where $t = 192$, and the required h-point is therefore not a node. In fact $\mathbf{v}_t = (253, 23, 60)$ and $\mathbf{v}_{t+1} = f^{11}(\mathbf{v}_t) = b(\mathbf{v}_t) = (253, 60, 23)$, and we note that $x_t = x_{t+1}$. The required h-point can be obtained by calculating $f^5(\mathbf{v}_t)$ using the matrix $H\phi_5$ for the map f^5. In fact

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} -1 & 10 & 0 \\ 5 & -25 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 253 \\ 23 \\ 60 \end{pmatrix} = \begin{pmatrix} 23 \\ 23 \\ 750 \end{pmatrix}.$$

6. Relationship to Quadratic Irrationals

The algorithm (5.1) can be identified with the integer arithmetic algorithm for the computation of the partial quotients of the continued fraction expansion of a certain quadratic irrational involving $\sqrt{n}$. Indeed, if we set $m = [(1 + \sqrt{n})/2]$, $x = 2m - 1$, $y = (n - x^2)/4$, so that x is the greatest odd integer less than $\sqrt{n}$ and hence y is a positive integer, then the quadratic irrational concerned is

$$\theta = \frac{x + \sqrt{n}}{2y}. \tag{6.1}$$

The well known integer arithmetic algorithm (see, for example, O. Perron [**5**]) for the delivery of the partial quotients of the continued fraction expansion for $\sqrt{n}$ itself can be extended easily for this number θ. Let $x_1 = x$, $y_1 = y$ and $y_0 = 1$. Then, for $i = 1, 2\ldots$, we define

$$m_i = \left[\frac{x_i + \sqrt{n}}{2y_i}\right], \qquad x_{i+1} = 2m_i y_i - x_i, \qquad y_{i+1} = m_i x_i - m_i^2 y_i + y_{i-1}, \quad (6.2)$$

in order to give the partial quotients m_i so that $\theta = [m_1, m_2, \ldots]$. On examining our algorithm (5.1), we find that $z_i = y_{i-1}$ and that the two equations for x_{i+1} and y_{i+1} in (5.1) are precisely the same as those in (6.2), so that the two algorithms deliver the same integers $m_1, m_2 \ldots$. We could have proved Theorem 2 using the known properties for the continued fraction expansions for quadratic irrationals. Instead our method can now be considered as a new proof of these properties. In any case we now have the following corollary to our Theorem 2.

COROLLARY. *The period of the principal orbit on $S(n)$ is the sum of the purely periodic partial quotients for the continued fraction expansion of the quadratic irrational θ in* (6.1).

Lagrange proved that the continued fraction expansion for a real number θ is eventually periodic if and only if θ is a quadratic irrational, and according to H. Davenport [**1**, p. 100], Galois was the first to prove that a necessary and sufficient condition for pure periodicity is that θ should be a *reduced* quadratic irrational, that is $\theta > 1$ and $-1 < \theta' < 0$, where θ' is the algebraic conjugate of θ. The number θ in (6.1) is indeed reduced, and in fact the process here is related to the reduction of quadratic forms with discriminant n. Davenport [**1**, p. 120] also mentioned that, when n is a prime $p \equiv 1 \pmod 4$, an algorithm for the construction of the b-point was given by Legendre back in 1808. Our algorithm here seems to be more revealing and more efficient than the Legendre algorithm which is based on the continued fraction expansion of $\sqrt{p}$ itself. For example, although the periods for θ and for $\sqrt{p}$ are of similar size, that for the former is more often the shorter. We also remark that a theorem of T. Muir (see, for example, Perron [**5**, p. 91]) gives a similar criterion concerning exactly when half of the period has been reached for the continued fraction expansion of $\sqrt{n}$. Our use of the involutions here gives a more transparent proof of this useful result.

When there are more than one b-points on $S(n)$ it does *not* follow that one of them must be on the principal orbit. For example, the two special points on the principal orbit corresponding to $205 = 5\times 41 = 3^2 + 14^2 = 13^2 + 6^2$ are the h-points $(1, 1, 41)$ and $(5, 5, 9)$, while the two b-points $(3, 7, 7)$ and $(13, 3, 3)$ lie in another special orbit, and so both these special orbits have even periods. Our notion of orbits here has given some insight to the well known parity problem concerning the period (of the periodic part) of the continued fraction expansion for $\sqrt{n}$. The problem is to classify those integers n for which the period concerned is odd, and it is directly related to the problem of whether the equation $X^2 - nY^2 = -1$ is soluble or not. Thus, according to Davenport [**1**, p. 111],

> "... The distinction between the cases when (this period) is odd or even raises problems to which no complete answer is known. No way of completely characterising the numbers n for which (the period) is odd has been found. ... A necessary condition for (the period) to be odd is that n is representable as a sum of two squares, but it is not sufficient."

The usual approach to the problem involves generalised residue symbols criteria, and some progress has been made by relating it to the structure of the 2-Sylow subgroup of a ring class group of $\mathbb{Q}(\sqrt{n})$. In particular, in a series of papers culminating in [**6**], L. Rédei used class-field theory to deduce a complete characterisation for an odd period in terms of a certain "conditional Artin symbol" (see also P. Morton [**4**]). More recently J. C. Lagarias [**3**] has studied the computational complexity of the parity problem.

Our approach here gives another "characterisation" for the period for $\sqrt{n}$ to be odd. We note that, although the two periods of the continued fraction expansions corresponding to the two numbers $\sqrt{n}$ and θ in (6.1) may be different nevertheless the two periods always have the same parity. Consequently we may say that the period for $\sqrt{n}$ is odd if and only if the principal orbit on $S(n)$ has a b-point. In other words the parity is odd when, and only when, n is not only representable as a sum of two squares, but also that this representation corresponds to a b-point on the principal orbit. Thus, although 205 is a sum of two squares, nevertheless the period for $\sqrt{205}$ is even because neither of the b-points corresponding to the decomposition of 205 as a sum of two squares appears on the principal orbit.

The parity of $L(n)$ is the same as that for the number of nodes on the principal orbit, that is the number of vectors satisfying the condition (ii). The problem can therefore be investigated by analysing the inequality $y - z < x < 2y$, and the method introduced in the paper has given some useful machinery for the purpose. Unfortunately, at the moment, we do not even have an explicit criterion to determine whether a given vector lies on the principal orbit or not.

References

1. H. Davenport, *The Higher Arithmetic*, Hutchinson's University Library, London, 1952.
2. D. R. Heath-Brown, *Fermat's two-squares theorem,* Invariant (1984), 3–5.
3. J. C. Lagarias, *On the computational complexity of determining the solvability or unsolvability of the equation* $X^2 - DY^2 = -1$, Trans. Amer. Math. Soc. **260** (1980), 485–508.
4. P. Morton, *On Rédei's theory of the Pell equation,* J. Reine Angnew. Math. **307/8** (1979), 373–398.
5. O. Perron, *Die Lehre von den Kettenbrüchen,* Stuttgart, 1954.
6. L. Rédei, *Die 2-Ringklassengruppe des Quadratischen Zahlkörpers und die theorie der Pellschen Gleichung,* Acta Math. Acad. Sci. Hungar. **4**(1953), 31–87.
7. D. Zagier, *A one-sentence proof that every prime* $p \equiv 1 \pmod 4$ *is a sum of two squares,* Amer. Math. Monthly **97** (1990), 144.

Department of Mathematical Sciences, Loughborough University, Leicestershire LE11 3TU, United Kingdom

(Received 29 02 1995)