CYCLOTOMIC EQUATIONS AND SQUARE PROPERTIES IN RINGS

BENJAMIN FINE

Department of Mathematics
University of California Santa Barbara
Santa Barbara, California 93106
and
Department of Mathematics
Fairfield University
Fairfield, Connecticut 06430

(Received May 5, 1985)

ABSTRACT. If \( R \) is a ring, the structure of the projective special linear group \( \text{PSL}_2(R) \) is used to investigate the existence of sum of square properties holding in \( R \). Rings which satisfy Fermat's two-square theorem are called \textit{sum of squares rings} and have been studied previously. The present study considers a related property called \textit{square property one}. It is shown that this holds in an infinite class of rings which includes the integers, polynomial rings over many fields and \( \mathbb{Z}_p \) where \( p \) is a prime such that \(-3\) is not a square mod \( p \). Finally, it is shown that the class of sum of squares rings and the class satisfying square property one are non-coincident.

KEY WORDS AND PHRASES. Fermat's Two-Square Theorem, PSL_2(R), Trace Class, Sum of Squares Ring, Modular Group, Free Product of Groups

1980 MATHEMATICS SUBJECT CLASSIFICATION CODE 10C30, 10C01, 13F99, 20G99

1. INTRODUCTION

Fermat's classical two-square theorem gives the relationship between those integers \( n \) which are sums of two squares and those integers \( n \) for which the cyclotomic equation \( x^2 + 1 = 0 \) can be solved modulo \( n \). Specifically \(-1\) is a quadratic residue mod \( n \) if and only if \( n \) is expressible as the sum of two relatively prime squares. In [1] a proof of this was given which involved the group theoretical structure of the modular group - \( \text{PSL}_2(\mathbb{Z}) \). Fermat's theorem is then, in a sense, independent of number theory in that the structure of \( \text{PSL}_2(\mathbb{Z}) \) can be deduced by purely analytic (Fuchsian group) methods. (Lehner [7]) This idea was used by Fine [3] to show that Fermat's result holds in an infinite class of rings. Such rings were termed \textit{sum of squares rings}. In this note we first use a technique similar to [3] to investigate the structure of those integers \( n \) for which the cyclotomic equation \( x^2 + x + 1 = 0 \) has solutions mod \( n \). A square result similar to Fermat's theorem is obtained. It is then shown that this square property holds in infinitely many sum of squares rings but that
the two square properties are independent. Finally, some questions that were raised in \cite{3} are answered. Before beginning, we note that the technique of \cite{3} has been extended by Kern-Isberner and Rosenberger \cite{4} to consider those integers which can be expressed in the form \( n = x^2 + dy^2 \) where \( d \) is a fixed positive integer. In a different direction, the general situation for which the equation \( x^2 + dx + 1 = 0 \) has solutions \( \mod n \) was considered by Fine in \cite{5}. A collection of square results was obtained.

2. We first prove the following theorem concerning the integers \( \mathbb{Z} \).

**Theorem 1:** The equations \( x^2 + x + 1 = 0 \) and \( x^2 - x + 1 = 0 \) have solutions \( \mod n \) if and only if there exist relatively prime integers \( a \) and \( b \) with

\[
   n = a^2 + b^2 + ab
\]

**Proof:** Consider the modular group \( M = \text{PSL}_2(\mathbb{Z}) \) consisting of linear fractional transformations

\[
   z' = \frac{az + b}{cz + d} \quad \text{with} \quad a, b, c, d \text{ integers and } ad - bc = 1.
\]

It is well known (Lehner \cite{2}, Newman \cite{6}) that \( M = \mathbb{Z}_2 \ast \mathbb{Z}_3 \), that is group theoretically \( M \) is a free product of a cyclic group of order 2 and a cyclic group of order 3.

If \( A \) is the map \( z' = -i/z \) and \( B \) is the map \( z' = -i/z + 1 \) then \( M \) has the presentation \( \langle A, B; A^2 = B^3 = 1 \rangle \). \cite{6}. Since in a free product any element of finite order must be conjugate to an element of finite order in one of the factors \cite{7} it follows that any element of order 3 in \( M \) must be conjugate to either \( B; z' = -1/z + 1 \) or to \( B^{-1}; z' = (-z + 1)/z \).

If \( U: z' = (az + b)/(cz + d) \) is an element of \( M \) then conjugating \( B \) and \( B^{-1} \) by \( U \) we obtain

\[
   U^{-1}BU: z' = \frac{(dz - b)(-1)(az + b)}{-cz + a} \quad \text{or} \quad \frac{(dz - b)(-1)(az + b)}{-cz + a}
\]

\[
   = \frac{(ab + d^2 + bd)}{-a^2 + c^2 + ac}z - (bc + ab + cd)
\]

or

\[
   U^{-1}BU: z' = \frac{(dz - b)(-1)(az + b)}{-cz + a} \quad \text{or} \quad \frac{(dz - b)(-1)(az + b)}{-cz + a}
\]

\[
   = \frac{(ad + ab + cd)}{-a^2 + c^2 + ac}z - (bc + ab + cd)
\]

where multiplication is done via matrix multiplication

\[
   \begin{pmatrix}
   d & a \\
   -c & a
   \end{pmatrix}
   \begin{pmatrix}
   0 & -1 \\
   1 & 1
   \end{pmatrix}
   \begin{pmatrix}
   a & b \\
   c & d
   \end{pmatrix}
   \quad \text{or} \quad
   \begin{pmatrix}
   d & a \\
   -c & a
   \end{pmatrix}
   \begin{pmatrix}
   -1 & -1 \\
   -1 & 0
   \end{pmatrix}
   \begin{pmatrix}
   a & b \\
   c & d
   \end{pmatrix}
\]

Therefore, any element of \( M \) of order 3 must have form (2.1) or (2.2).

Now let \( a > 0, n \in \mathbb{Z} \). Suppose the equation \( x^2 + x + 1 = 0 \) has a solution \( \mod n \). Then there exists integers \( m \) and \( k \) with

\[
   m^2 + m + 1 = nk
\]
Therefore, the linear fractional transformation

\[ z' = \frac{-mz + n}{kz + (m+1)} \]  

(2.3).

has determinant +1 and is thus in \( M \). Further it has trace +1. Elements of \( M \) with trace 1 have order 3, \([6]\) so the map in (2.3) has order 3. Therefore, this map must have either form (2.1) or form (2.2). Thus, \( n = b^2 + d^2 + bd \) for some \( b, d \in \mathbb{Z} \). Further, since \( U: z' = (az+b)/(cz+d) \) has determinant 1, \( ad-bc = 1 \) and so \( b \) and \( d \) are relatively prime.

Conversely, suppose \( n = b^2 + d^2 + bd \) with \( (b, d) = 1 \). Since \( b \) and \( d \) are relatively prime, there exist integers \( a, c \) with \( ad-bc = 1 \). Then there exists a map \( U: z' = (az+b)/(cz+d) \) in \( M \). Conjugating the map \( B^{-1} \) by this \( U \) give us form (2) - that is

\[ z' = \frac{(ad+cd+ab)z + (b^2+d^2+bd)}{-(a^2+c^2+ac)z-(bc+ab+cd)} \]

since \( n = b^2 + d^2 + bd \). Since conjugation preserves determinants, we have \( -m^2 - m - nk = 1 \) or \( m^2 + m + 1 = n, k \). Therefore, \( x^2 + x + 1 = 0 \) has a solution modulo \( n \). In an identical manner, by dealing with traces of -1 we get the result concerning the equation \( x^2 - x + 1 = 0 \) mod \( n \).

By quadratic formula, \( x^2 + x + 1 = 0 \) and \( x^2 - x + 1 = 0 \) have solutions mod \( p \) (where \( p \) is an odd prime) if and only if \(-3\) is a square mod \( p \). Thus as a corollary we have

**COROLLARY:** If \( p \) is an odd prime then \(-3\) is a quadratic residue mod \( p \) if and only if \( p = a^2 + b^2 + ab \) for some relatively prime integers \( a, b \).

The structure of the modular group can be used to effectively classify all the trace classes. This was done in \([5]\). From this is obtained that for each \( d > 0 \) there exist finitely many quadratic forms (depending on \( d \)) such that \( x^2 + dx + 1 = 0 \) has solutions mod \( n \) if and only if \( n \) is represented by one of these forms. Further, there exists an effective procedure to write down each of these forms for each \( d \). In this paper we take a different tract and consider those rings for which theorem 1 is valid.

3. Recall from \([3]\) that a **sum of squares ring** is a commutative ring \( R \) with an identity (not a field) with \(-1\) not a square in \( R \) which satisfies the following two square properties:

**SS1:** If \( r \in R \) and \(-1\) is a quadratic residue mod \( (r) \) then \( r = \pm (u^2 + v^2) \)

**SS2:** If \( r = u^2 + v^2 \) with \((u, v) = 1\) then \(-1\) is a quadratic residue mod \( (r) \)

For **SS2** a \( CD \) ring was not required \(- (u, v) = 1 \) indicating only that \( u \) and \( v \) have no common divisors. In \([3]\) it was shown that there are infinitely many sum of squares rings. Specifically, the following classes of rings were proven to be sum of squares rings.
1) $\mathbb{Z}_p$ where $p$ is a prime, $p \equiv 3 \mod 4$ and $n > 1$

2) The polynomial rings $F[x]$ where $F$ is a field with $-1$ not a square in $F$ and where $\text{PSL}_2(F)$ has only one conjugacy class in trace zero. In particular

a) $\mathbb{Z}_p[x]$ where $p$ is a prime congruent to $3 \mod 4$

b) $K[x]$ where $K$ is an ordered field permitting square roots of all positive elements. Examples here are $\mathbb{R}[x]$ and $A[x]$ where $A$ is the subfield of algebraic numbers.

3) General Euclidean domains $D$ with trivial units, of characteristic $\neq 2$ and with a subadditive norm function satisfying $0 \neq N(b) \leq N(a)$ implies $N(a+kb) < N(a)$ for some $k \in D$. (The integers $\mathbb{Z}$ provide an example of this last type of ring.)

We now consider rings which satisfy the results of Theorem 1. We say that a commutative ring with an identity (not a field) satisfies square property one abbreviated $\text{SPI}$ if the ring $R$ satisfies

\begin{equation}
\text{SPIa: If } r \in R \text{ and } x^2 + x + 1 = 0 \text{ has solutions mod } (r) \text{ then } r = \pm (u^2 + v^2 + uv)
\end{equation}

for some ring elements $u, v$.

\begin{equation}
\text{SPIb: If } r = \pm (u^2 + v^2 + uv) \text{ for some } u, v \in R \text{ with } (u, v) = 1 \text{ then } x^2 + x + 1 = 0 \text{ has solutions mod } (r).
\end{equation}

As in the case of sume of squares ring $(u, v) = 1$ indicates that $u$ and $v$ have no common divisors. A GCD ring is not required. We obtain:

**THEOREM 2:** The following classes of rings all satisfy square property one.

a) $\mathbb{Z}_p$ where $p \not\equiv 1 \mod 4$

b) $F[x]$ where $F$ is a field of characteristic $\neq 2$, with $-3$ not a square in $F$ and every matrix of trace 1 in $\text{PSL}_2(F)$ is conjugate within $\text{PSL}_2(F)$ to either $^{-1}_{1 0}$ or $^{-1}_{1 0}$

c) Euclidean domains $D$ of char $\neq 2$ with trivial units and a sub-additive norm function satisfying $0 \neq N(b) \leq N(a)$ implies $N(a+kb) < N(a)$ for some $k \in D$.

**PROOF:** All of the above rings have the property that the GCD of two elements is expressible as a linear combination of these elements. Thus if $(u, v) = 1$ there exist $a, b$ with $au + bv = 1$. Employing the identical formal method as in the second part of the proof of Theorem 1, it is seen that these rings all satisfy $\text{SPIb}$.

Since each of these rings has only trivial idempotents, the center of their special linear groups $\text{SL}_2(k)$ is $1$ - with $I$ the identity matrix. Thus $\text{PSL}_2(R) = \text{SL}_2(R)/Z$ for any of the above rings. It follows that any element of $\text{PSL}_2(R)$ can be considered as $I$ or $-I$ a matrix in $\text{SL}_2(R)$. Modeled on the first part of Theorem 1, it is seen that these rings will satisfy $\text{SPIa}$ if every matrix of trace 1 is conjugate within $\text{PSL}_2(R)$ either to $^{-1}_{1 0}$ or $^{-1}_{1 0}$. We will show in turn that this is true for each of the above classes.

a) If $-3$ is not a square in $\mathbb{Z}_p$ then $-3$ is not a square in $\mathbb{Z}_p$ for all $n > 1$. Therefore, there exists no solutions to $x^2 + x + 1 = 0$ in $\mathbb{Z}_p$. Since $n > 1$, $\mathbb{Z}_p$ is not a field. By a result of D. L. McQuillan [8] if $\text{A}\text{PSL}_2(\mathbb{Z}_p)$ and $\text{tr}(A) = 1$ then $A$
is conjugate to \( \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \). Thus, \( \mathbb{Z}_p \) satisfies square property one.

b) If \( F \) is a field with char \( F \neq 2 \) and \(-3\) not a square to \( F \), we show that every matrix of trace 1 in \( \text{PSL}_2(\mathbb{F}[x]) \), every matrix of trace one is conjugate to either
\[
\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},
\]
the result follows as above.

Suppose \( T \in \text{PSL}_2(\mathbb{F}[x]) \) with \( T = \begin{pmatrix} -f & g \\ h & f+1 \end{pmatrix} \). Let \( S \) be the set of all conjugates of \( T \) in \( \text{PSL}_2(\mathbb{F}[x]) \) and suppose \( V \in S \) with \( V = \begin{pmatrix} -u & v \\ w & u+1 \end{pmatrix} \) and with the degree of \( u \) minimal among all the conjugates of \( T \). If \( v = 0 \) or \( w = 0 \) then \(-u(u+1) = 1\). Then \( u^2 + u + 1 = 0 \) has a solution in \( F \) (\( u \) must be in \( F \) since the only units in \( \mathbb{F}[x] \) are in \( F \)) contradicting \(-3\) not being a square in \( F \). Therefore, \( v \neq 0 \) and \( w \neq 0 \). If \( u \in F \) then since
\[
-u^2 - u = -(wv) + 1,
\]
it follows that \( \deg v + \deg v = 2 \deg u \), and thus \( v \) and \( w \) are also in \( F \).

Assume \( \deg u \geq 1 \). Since \( \deg v + \deg w = 2 \deg u \) then \( \deg v \leq \deg u \) or \( \deg w \leq \deg u \).

The division algorithm a polynomial \( q \) can be determined so that \( \det (u + qv) < \deg u \).

Conjugating the matrix \( V \) by \( \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} \) gives a matrix \( \begin{pmatrix} u+qv & * \\ w & v+1 \end{pmatrix} \). This matrix is in \( S \) being a conjugate of \( V \). But this contradicts the minimality of \( \deg u \) among the elements of \( S \) since \( \deg (u+qv) < \deg u \). Therefore \( \deg u < 1 \) and so \( u \in F \). From the argument given before then \( v \) and \( w \) must also be in \( F \) and thus \( V \in \text{PSL}_2(F) \). Therefore, every matrix in \( \text{PSL}_2(\mathbb{F}[x]) \) of trace one in \( \text{PSL}_2(F) \).

c) Finally in a Euclidean domain the stated conditions on the subadditive norm functions are exactly what is necessary to allow the proof of theorem 1 to go through.

As a corollary, we obtain

COROLLARY 2:

1) If \(-3\) is not a square mod \( p \), then \( \mathbb{Z}[x] \) satisfies square property one.

2) If \( F \) is an ordered field where every positive element has a square root, then \( \mathbb{F}[x] \) satisfies square property one. In particular if \( R \) is the real field and \( A \) the subfield of algebraic numbers when both \( R[x] \) and \( A[x] \) satisfy square property one.

The proofs of the two statements in the corollary consist in showing that over these fields the conjugacy conditions on matrices of trace one hold. In fact, over these fields every matrix of trace one is conjugate to \( \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \), [3] [8].

3. Each of the rings discussed in the previous section, except for the conditions on primes, are sum of squares rings. There are trivial examples of sum of squares rings which do not satisfy square property one - for example \( \mathbb{Z}_3[x] \) which is a sum of squares ring but does not satisfy square property one since \(-3\) is a square in \( \mathbb{Z}_3 \). In this section, we give a non-trivial example of a ring which satisfies square property one but which is not a sum of squares ring. The example will lead us to pose a question about sum of squares rings.

Let \( I_2 \) denote the ring of integers in the quadratic imaginary number field \( \mathbb{Q} \sqrt{-2} \). Then we get
THEOREM 3: $I_2$ satisfies square property one but is not a sum of squares ring.

PROOF: An integral basis for $I_2$ is $(1, i\sqrt{2})$, so then this ring can be considered as $\mathbb{Z}[i\sqrt{2}]$. Neither $x^2 + 1 = 0$ nor $x^2 + x + 1 = 0$ have solutions in $I_2$. Further $I_2$ is Euclidean [9], so that both SS2 and SPlb hold in $I_2$. We now show that SPla holds in $I_2$ but that SS1 does not.

From Fine [9], it is known that the projective special linear group over $I_2$, $\text{PSL}_2(I_2)$, is an HNN extension (see [9] for terminology) of a base $K_2$ which is in an free product with amalgamation. The structure of this base group can be described as

$$K_2 = (\mathbb{Z}_2 \times \mathbb{Z}_2) \ast \mathbb{A}_4.$$ 

That is, $K_2$ is the free product of a Klein 4-group $\mathbb{Z}_2 \times \mathbb{Z}_2$ with the alternating group on 4 symbols $\mathbb{A}_4$ amalgamated over a subgroup $H$ which is cyclic of order 2.

The linear fractional transformation $M: z' \to \frac{-1}{z + 1}$ which represents the matrix

$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$

is in the factor $\mathbb{A}_4$. This has order 3 and in $\mathbb{A}_4$ every element of order 3 must be conjugate to this or its inverse.

In an HNN extension, every element of finite order must be conjugate to an element of finite order in the base group. Further, in a free product with amalgamation elements of finite order are conjugate to elements of finite order in the factors. Now suppose $T = \pm \begin{pmatrix} a & b \\ c & -a+1 \end{pmatrix}$ is an element of $\text{PSL}_2(I_2)$ of trace $\pm 1$. Elements of trace $\pm 1$ have order 3 in the base $K_2$. Since $K_2$ is a free product with amalgamation, $T$ in turn must be conjugate to an element of order 3 in one of the factors of $K_2$. Since $\mathbb{Z}_2 \times \mathbb{Z}_2$ has no elements of order 3, $T$ then must be conjugate to an element of order 3 in $\mathbb{A}_4$. Thus $T$ must be conjugate to either $M$ or $M^{-1}$. From this, as in the proofs of theorem 1 and 2, it follows that SPlb holds in $I_2$.

We show, however, that SS2 does not hold in $I_2$. Consider $v = 1 + i\sqrt{2}$. Then $v^2 + 1 = -1 + 2i\sqrt{2} + 1 = 2i\sqrt{2}$. Therefore $-1$ is a quadratic residue mod $(i\sqrt{2})$ is a sum of two squares. If $u^2 + v^2 = \pm i\sqrt{2}$ with $u = a + ib\sqrt{2}$, $v = A + iB\sqrt{2}$, then $a^2 + A^2 - 2(b^2 + B^2) + 2(ab + AB)\sqrt{2} + 1 = \pm 1$ or $2(ab + AB) = \pm 1$ which is impossible.

What led to this example was that $\text{PSL}_2(I_2)$ has several conjugacy classes in trace zero. In [3] it was shown that certain conditions on the conjugacy classes in $\text{PSL}_2(R)$ for $R$ a ring implied that $R$ was a sum of squares ring. Combining these, we ask the following question.

QUESTION: If $R$ is a sum of squares ring, must $\text{PSL}_2(R)$ have only one conjugacy class in trace zero?

4. In [3] the following two questions were posed.

1) If $R$ is both an integral domain and a sum of squares ring must it be a UFD?
2) Is \( \mathbb{Z}[x] \) - the polynomial ring over the integers - a sum of squares ring?

Both turn out to be false. The following elegant example showing that 1) is false is due to R. Keith Dennis [10]. As a first step, he needs the following lemma whose proof is straightforward.

**Lem**: The direct limit of a directed system of sum of squares rings is again a sum of squares ring.

Now suppose that for each positive integer \( n \), \( A_n \) is the ring of \( p \)-adic integers with the \( 2^n \)-th root of \( p \) adjoined. Let \( A \) be the direct limit of the system \( A_n \). If \( p \equiv 3 \mod 4 \) each \( A_n \) will be a sum of squares ring and therefore \( A \) will be a sum of squares ring. However, \( A \) will not be a UFD since there are no primes in \( A \).

Showing that \( \mathbb{Z}[x] \) is not a sum of squares ring is rather direct and was pointed out first by E. Mendola (among others). Consider \( p(x) = x^2 + 4 \). This is a sum of two relatively prime squares in \( \mathbb{Z}[x] \). Suppose \(-1\) was a quadratic residue mod \( (p(x)) \) so that

\[
(g(x))^2 + 1 = p(x) \cdot f(x)
\]

Evaluating at zero gives \((g(0))^2 + 1 = 4 \cdot f(0)\). Since these are integral polynomials, this would make \(-1\) a quadratic residue mod 4 which is false.

**References**

4. KERN-ISBERNER, G. AND ROSENBERGER, G. "A note on Numbers of the Form \( n = x^2 + Ny^2 \) to appear.
5. FINE, B. "Trace Classes and Quadratic Forms in the Modular Group" - to appear.
10. DENNIS, R. K. - correspondence.
Submit your manuscripts at http://www.hindawi.com