Internat. J. Math. & Math. Sci.
Vol. 9 No. 1 (1986) 89-95

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 $PSL_2(R)$ is used to investigate the existence of sum of square properties holding in R. Rings which satisfy Fermat's two-square theorem are called sum of squares rings and have been studied previously. The present study considers a related property called 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 $Z_p n$ where p is a prime such that -3 is not a square mod p. Finally, it is shown that the class of sume of squares rings and the class satisfying square property one are non-coincidental.

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 - $PSL_2(Z)$. Fermat's theorem is then, in a sense, independent of number theory in that the structure of $PSL_2(Z)$ can be deduced by purely analytic (Fuchsian group) methods. (Lehner [2]) This idea was used by Fine [3] to show that Fermat's result holds in an infinite class of rings. Such rings were termed 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 [3] are answered. Before beginning, we note that the technique of [3] has been extended by Kern-Isberner and Rosenberger [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 [5]. A collection of square results was obtained.

2. We first prove the following theorem concerning the integers Z.

THEOREM 1: The equations $x^2 + x + 1 = 0$ and $x^2 - x + 1 = 0$ have solutions modulo 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 $M = PSL_2(Z)$ consisting of linear fractional transformations

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

It is well know (Lehner [2], Newman [6]) that $M = Z_2 * Z_3$ - 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 $z' = -1/z$ and B is the map $z' = -1/z+1$ then M has the presentation $\langle A, B: A^2 = B^3 = 1 \rangle$ [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 [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

$$U^{-1}BU: z' = \left(\frac{dz-b}{-cz+a}\right)\left(\frac{-1}{z+1}\right)\left(\frac{az+b}{cz+d}\right)$$

$$= \frac{(ab+cd+bc)z + (b^2 + d^2 + bd)}{-(a^2 + c^2 + ac)z - (bc + ab + cd)} \qquad (2.1)$$

or

$$U^{-1}BU: z' = \left(\frac{dz-b}{-cz+a}\right)\left(\frac{-z-1}{z}\right)\left(\frac{az+b}{cz+d}\right)$$

$$= \frac{(ad+ab+cd)z + (b^2 + d^2 + bd)}{-(a^2 + c^2 + ac)z - (bc + ab + cd)} \qquad (2.2)$$

where multiplication is done via matrix multiplication -

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

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

Now let $a > 0$, $n \in Z$. Suppose the equation $x^2 + x + 1 = 0$ has a solution modulo n. Then there exists integers m and k with

$$m^2 + m + 1 = nk$$

Therefore, the linear fractional transformation

$$z' = \frac{-mz + n}{kz + (m+1)} \qquad (2.3),$$

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, dε 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

$$z' = \frac{(ad+cd+ab)z + (b^2+d^2+bd)}{-(a^2+c^2+ac)z - (bc+ab+cd)} = \frac{-mz + n}{kz+(m+1)}$$

since $n = b^2 + d^2 + bd$. Since conjugation preserves determinants, we have $-m^2 - m - nk = 1$ or $m^2 + m + 1 = n_1 k$. 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 $x^2 - x + 1 = 0 \bmod n$.

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 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 rε 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 GCD 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) $Z_p n$ where p is a prime, $p \equiv 3 \bmod 4$ and $n > 1$

2) The polynomial rings F[x] where F is a field with -1 not a square in F and where $PSL_2(F)$ has only one conjugacy class in trace zero. In particular

a) $Z_p[x]$ 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 $\mathbb{R}$ is the real field and A 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 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 SP1 if the ring R satisfies

SP1a: If $r \in R$ and $x^2 + x + 1 = 0$ has solutions mod (r) then $r = \pm (u^2 + v^2 + uv)$ for some ring elements u, v.

SP1b: If $r = \pm(u^2 + v^2 + uv)$ for some $u, v \in R$ with (u, v) = 1 then $x^2 + x + 1 = 0$ has solutions mod (r).

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) $Z_p n$ where $n>1$ and p is a prime such that -3 is not a square mod p

b) F[x] where F is a field of characteristic $\neq 2$, with -3 not a square in F and every matric of trace 1 in $PSL_2(F)$ is conjugate within $PSL_2(F)$ to either $\pm\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ or $\pm\begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}$

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 idential formal method as in the second part of the proof of Theorem 1, it is seen that these rings all satisfy SP1b.

Since each of these rings has only trivial idempotents, the center of their special linear groups $SL_2(R)$ is $\pm$ I - with I the identity matrix. Thus $PSL_2(R) = SL_2(R)/\pm I$ for any of the above rings. It follows that any element of $PSL_2(R)$ can be considered as + or - a matrix in $SL_2(R)$. Modeled on the first part of Theorem 1, it is seen that these rings will satisfy SP1a if every matrix of trace 1 is conjugate within $PSL_2(R)$ either to $\pm\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ or $\pm\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$. We will show in turn that this is true for each of the above classes.

a) If -3 is not a square in Z_p then -3 is not a square in $Z_p n$ for all $n > 1$. Therefore, there exists no solutions to $x^2 + x + 1 = 0$ in $Z_p n$. Since $n > 1$, $Z_p n$ is not a field. By a result of D. L. McQuillan [8] if $A \in PSL_2(Z_p n)$ and tr(A) = 1 then A

is conjugate to $\pm \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$. Thus, $Z_p n$ 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 $PSL_2(F[\chi])$every matrix of trace one is conjugate to either $\pm \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ or $\pm \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ the result follows as above.

Suppose $T \in PSL_2(F[x])$ with $T = \pm \begin{pmatrix} -f & g \\ h & f+1 \end{pmatrix}$. Let S be the set of all conjugates of T in $PSL_2F[x])$ and suppose $V \in S$ with $V = \pm \begin{pmatrix} -u & v \\ w & v+1 \end{pmatrix}$ 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 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 $-u^2 - u = -(vw) + 1$, it follows that deg v + deg w = 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. By 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 $\pm \begin{pmatrix} u+qv & * \\ * & * \end{pmatrix}$. 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 $V \in PSL_2(F)$. Therefore, every matrix in $PSL_2(F[x])$ of trace one in $PSL_2(F)$.

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

As a corollary, we obtain

COROLLARY 2:

1) If -3 is not a square mod p, then $Z_p[x]$ satisfies square property one.

2) If F is an ordered field where every positive element has a square root, then 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 $\pm \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$, [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 $Z_3[x]$ which is a sum of squares ring but does not satisfy square property one since -3 is a square in 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 $Q\sqrt{-2}$. 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 $Z[i\sqrt{2}]$. 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 SP1a holds in I_2 but that SS1 does not.

From Fine [9], it is known that the projective special linear group over I_2-$PSL_2(I_2)$ - is an HNN extension (see [9] for terminology) of a base K_2 which is in turn a free product with amalgamation. The structure of this base group can be described as

$$K_2 = (Z_2 \times Z_2)*_H A_4.$$

That is K_2 is the free product of a Klein 4-group $Z_2 \times Z_2$ with the alternating group on 4 symbols A_4 amalgamated over a subgroup H which is cyclic of order 2.

The linear fractional transformation M: $z' = -1/z+1$ which represents the matrix $\pm \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ is in the factor A_4. This has order 3 and in 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 $PSL_2(I_2)$ of trace ± 1. Elements of trace ± 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 $Z^2 \times Z^2$ has no elements of order 3, T then must be conjugate to an element of order 3 in A_4. Tus T must be conjugate to either M or M^{-1}. From this, as in the proofs of theorem 1 and 2, it follows that SP1b 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 not a sum of two squares. If $u^2+v^2 = \pm i\sqrt{2}$ with $u = a+ib\sqrt{2}$, $v = A + iB\sqrt{2}$. with a, b, A, B $\in$ Z then

$$a^2+A^2-2(b^2+B^2) + 2(ab + AB)\sqrt{2}\, i = \pm i\sqrt{2}$$

or

$$2(ab + AB) = \pm 1$$

which is impossible.

What led to this example was that $PSL_2(I_2)$ has several conjugacy classes in trace zero. In [3] it was shown that certain conditions on the conjugacy classes in $PSL_2(R)$ 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 $PSL_2(R)$ have only one conjgacy 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 $Z[x]$ - 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.

LEMMA: 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-the root of p adjoined. Let A be the direct limit of the system A_n. If $p \equiv 3 \bmod 4$ 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 $Z[x]$ is not a sum of squares ring is rather direct and was pointed out first by E. Mendoza (among others). Consider $p(x) = x^2 + 4$. This is a sum of two relatively prime squares in $Z[x]$. 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

1. FINE, B. "A Note on the Two Square Theorem" - Can. Math. Bull. Vol. 20, (1), 1977, 93-95.
2. LEHNER, J. "Discontinuous Groups and Automorphic Functions" - Math. Surveys, No. VIII, AMS, Providence, RI (1964).
3. FINE, B. "Sum of Squares Rings" - Can. J. Math., Vol. XXIX, No. 1977, 155-161.
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.
6. NEWMAN, M. "Integral Matrices" - Academic Press, New York, 1972.
7. MAGNUS, W., KARRASS, A. and SOLITAR, D. "Combinatorial Group Theory" - Wiley Interscience, New York, 1966.
8. MCQUILLAN, D. L. "Classification of Normal Congruence Subgroups of the Modular Group" - Amer. J. Math. 87, 1965.
9. FINE, B. "The HNN and Generalized Free Product Structure of Certain Linear Groups" - Bull. Amer. Math. Soc. Vol. 81, No. 2, 1975, 413-416.
10. DENNIS, R. K. - correspondence.