Canad. Math. Bull. Vol. **20** (1), 1977

A NOTE ON THE TWO-SQUARE THEOREM

BY
BENJAMIN FINE

One of the nicest theorems of elementary number theory is the two-square theorem of Fermat.

THEOREM. *A prime p is expressible as the sum of* 2 *squares if and only if* -1 *is a quadratic residue* mod p.

This can be proven in several ways [2], *and is readily extended to general integers n, with the proviso that if $n=u^2+v^2$, then we must have $(u, v)=1$, for* -1 *to be a quadratic residue* mod n.

In this note we give a new proof of the theorem. This proof involves the structure of the modular group $M=PSL_2(Z)$ which is group theoretically a free product. This proof is interesting for several reasons; first, it is essentially independent of number theory, secondly, it proves the result for general integers quickly and directly, and finally the technique of the proof can be used in considering the sum of square properties in more general rings than the integers. Rings which satisfy the two-square theorem (in its general form as given below) are called *sum of squares rings* and were investigated in [1]. As a general principle if the 2×2 special linear group over a ring is group theoretically decomposable as a free product or amalgamated free product then the ring satisfies some sum of squares properties (see [1]).

THEOREM. *A positive integer n is the sum of* 2 *squares if* -1 *is a quadratic residue* mod n. *Conversely if $n=u^2+v^2$ with $(u, v)=1$ then* -1 *is a quadratic residue* mod n.

Proof. Consider the modular group $M\cong PSL_2(Z)$ consisting of linear fractional transformations $z'=(az+b)/(cz+d)$ where a, b, c, d are integers with $ad-bc=1$. It is well known [3], [4] that M is a free product of a cyclic group of order 2 and a cyclic group of order 3 ($M\cong Z_2 * Z_3$). Further, this is proven independently of number theory by methods of discontinuous groups [3], [4]. Therefore in M as a group, every element of order 2 is conjugate [4]. Now the map $T=(z'=-1/z)$ has order 2 and is in M so every element of order 2 must be conjugate to T. Let $U=(z'=(az+b)/(cz+d)$ be in M. Conjugating T by U

Received by the editors Sept 14, 1976.

https://doi.org/10.4153/CMB-1977-015-2 Published online by Cambridge University Press

we get

$$(1)\qquad UTU^{-1}=\left(\frac{az+b}{cz+d}\right)\left(\frac{-1}{z}\right)\left(\frac{dz-b}{-cz+a}\right)=\frac{-(ac+bd)z+(a^2+b^2)}{-(c^2+d^2)z+(ac+bd)}$$

where the multiplication is done via matrix multiplication;

$$\begin{pmatrix} ab \\ cd \end{pmatrix}\begin{pmatrix} 01 \\ -10 \end{pmatrix}\begin{pmatrix} d-b \\ -ca \end{pmatrix}$$

Therefore every element of order 2 in M must have form (1).

Now let $n>0$, $n\in Z$. Say -1 is a quadratic residue mod n. Then there is an l, $k\in Z$ with $l^2+1=kn$. Therefore, the transformation

$$(2)\qquad z'=\frac{lz+n}{-kz-l}$$

has integral entries and determinant $+1$, and thus is in M. Further, it has trace 0. Elements of M with trace 0 have order 2 [4], and so this transformation has order 2 and is conjugate to T. Therefore (2) has form (1) so $n=a^2+b^2$ for some a, $b\in Z$.

Conversely say $n=a^2+b^2$, with a, $b\in Z$, and $(a,b)=1$. Since $(a,b)=1$ there exist c, $d\in Z$ such that $ad-bc=1$.

Therefore the

$$(3)\qquad \text{map } z'=\frac{az+b}{cz+d}$$

is in M.

Conjugating $T=(z'=-1/z)$ by (3) gives the map

$$z'=\frac{(ac+bd)z+(a^2+b^2)}{-(c^2+d^2)z+(ac+bd)}=\frac{\alpha z+n}{mz-\alpha}$$

since $a^2+b^2=n$. Since conjugation preserves determinants $-\alpha^2-mn=1$ or $\alpha^2+1=-mn$.

Therefore -1 is a quadratic residue mod n. Q.E.D.

References

1. Benjamin Fine, *Sum of Squares Rings* (to appear Canadian Journal of Mathematics).
2. G. H. Hardy and E. M. Wright, *Introduction to the Theory of Numbers* Clarendon Press.
3. Joseph Lehner, *Discontinuous Groups and Automorphic Functions* Math. Surveys No. **VIII** Amer. Math. Soc. (1964).
4. Morris Newman, *Integral Matrices* Academic Press (1972).

Department of Mathematics
Fairfield University
Fairfield, Connecticut 06430

https://doi.org/10.4153/CMB-1977-015-2 Published online by Cambridge University Press