NOTE ON A PROBLEM IN NUMBER THEORY

HAROLD N. SHAPIRO

The problem which we shall consider originated from a conjecture of S. Ulam. For x, p, integers, p a prime, let $x \equiv a \pmod{p}$ where $-p/2 < a < p/2$; and define $\|x\|_p = |a|$. Then if $T(x)$ is a mapping of the nonzero residues modulo p into themselves, we consider the following "approximate multiplicative relation" modulo p,

$$\|T(xy) - T(x)T(y)\|_p < k \tag{1}$$

where k is a fixed integer. The problem is to ascertain simple conditions under which the only solutions to (1) are given by

$$T(x) \equiv x^a \pmod{p}. \tag{2}$$

Clearly, p must be larger than k in order that this be feasible. Also, if we give to $T(x)$ any arbitrary set of integral values between 0 and $k^{1/2}$ we may obtain mappings satisfying (1) but not (2). This then indicates in a sense that the value domain of $T(x)$ must not be too small in order that (2) follow from (1).

The results obtained in this note are derived essentially from the following very simple lemma.

LEMMA. *If for $T(x)$ a mapping of a semigroup G into a ring R we define*

$$\epsilon(x, y) = T(xy) - T(x)T(y), \tag{3}$$

then for any x, y, z of G,

$$\epsilon(x, y)T(z) + \epsilon(xy, z) = T(x)\epsilon(y, z) + \epsilon(x, yz). \tag{4}$$

PROOF. For any x, y, z of G we obtain from the associativity of multiplication:

$$\begin{aligned} T(xyz) &= T(xy)T(z) + \epsilon(xy, z) \\ &= T(x)T(y)T(z) + \epsilon(x, y)T(z) + \epsilon(xy, z) \end{aligned} \tag{5}$$

and

$$\begin{aligned} T(xyz) &= T(x)T(yz) + \epsilon(x, yz) \\ &= T(x)T(y)T(z) + T(x)\epsilon(y, z) + \epsilon(x, yz). \end{aligned} \tag{6}$$

Comparing (5) and (6) yields (4).

Received by the editors October 30, 1947, and, in revised form, November 10, 1947.