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.

We note that in case both G and R are commutative, as they will be in our applications of the lemma, we have $\epsilon(x, y) = \epsilon(y, x)$ and we may write (4) as

$$\epsilon(x, y)T(z) + \epsilon(z, xy) = \epsilon(y, z)T(x) + \epsilon(x, yz). \tag{7}$$

To begin with we shall consider the case where $T(x)$ is a mapping of the residues modulo n, which are prime to n, into themselves, where n is not necessarily prime. In this case we have the following theorem.

THEOREM 1. *If* (1) $\|T(xy) - T(x)T(y)\|_n < k$, (2) $k < \min_{p|n} p$, *and* (3) $T(x)$ *takes on more than* $8k^2$ *distinct values, then*

$$T(xy) \equiv T(x)T(y) \pmod{n}. \tag{8}$$

PROOF. Suppose that, for some two integers x_1, x_2, (8) does not hold, so that

$$T(x_1x_2) \equiv T(x_1)T(x_2) + \epsilon(x_1, x_2) \pmod{n}$$

where

$$\|\epsilon(x_1, x_2)\|_n < k \tag{9}$$

and $\epsilon(x_1, x_2) \not\equiv 0 \pmod{n}$.

We now apply the lemma to the case where G is the group of residues mod n which are prime to n, and R all residues. We get for any integer y,

$$\epsilon(x_1, x_2)T(y) + \epsilon(y, x_1x_2) \equiv \epsilon(x_2, y)T(x_1) + \epsilon(x_1, x_2y) \tag{10}$$

where from hypothesis (1) we have $\|\epsilon(y, x_1x_2)\|_n < k$, $\|\epsilon(x_2, y\|_n < k$, and $\|\epsilon(x_1, x_2y)\|_n < k$. From the hypothesis $k < \min_{p|n} p$ so that by (9) we see that $(\epsilon(x_1, x_2), n) = 1$. Thus having fixed x_1, x_2, $\epsilon(x_1, x_2)$ is fixed, and (10) determines the value of $T(y)$ uniquely, modulo n. Clearly then $T(y)$ could take on at most $8k^2$ distinct values, whence the theorem.

For the special case where $n = p^\alpha$, the power of an odd prime we get the following theorem.

THEOREM 2. *If* (1) $\|T(xy) - T(x)T(y)\|_{p^\alpha} < k$, (2) $k < p$, *and* (3) $T(x)$ *takes on more than* $8k^2$ *distinct values,*

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

PROOF. From Theorem 1 we see that $T(xy) \equiv T(x)T(y) \pmod{p^\alpha}$. Then if ρ is a primitive root mod p^α we have

$$T(x) \equiv T(\rho^{\mu}) \equiv \{T(\rho)\}^{\mu} \equiv \rho^{\alpha\mu} \equiv x^{\alpha} \pmod{p^{\alpha}}.$$

COROLLARY. *If* $\|T(xy) - T(x)T(y)\|_p < k$ *and* $T(x)$ *takes on more than* $8k^2$ *distinct values, then* $T(x) \equiv x^{a} \pmod{p}$.

If we now restrict our attention to the case of a prime modulus we see that the above discussion covers those cases for which $N =$ the number of distinct values in the value domain is such that $N < k^{1/2}$ or $N > 8k^2$. The question then arises as to what can be said for $k^{1/2} < N \leqq 8k^2$. In this direction we have:

THEOREM 3. *If* $N > 8k$, *and* $\|T(xy) - T(x)T(y)\|_p < k$, *then, for* $p > 8k^2$, N *divides* $p-1$.

PROOF. (a) We first note that $T(1) = 1$. For we have for any x

$$T(x)(1 - T(1)) = \epsilon(1, x), \qquad \|\epsilon(1, x)\|_p < k,$$

so that if $T(1) \neq 1$, $T(x)$ could take on at most $2k$ values.

(b) If $N > 8k^2$ we have already proved above that $T(x) \equiv x^{a} \pmod{p}$ and it follows in this case that $N \mid (p-1)$.

(c) It remains only to consider the case $8k < M \leqq 8k^2$. Since $N \leqq 8k^2$ there must be a value c such that $T(x) = c$ for more than $(p-1)/N$ different x. Let $z_1, \cdots, z_{\Delta}$, $\Delta \geqq (p-1)/N$, be the numbers such that $T(z_i) = c$, $i = 1, \cdots, \Delta$. Then for p sufficiently large (for example, $p > 8k^2$) $\Delta > 1$, and we have from (7), for $i \neq j$,

$$\epsilon(x, y)T(z_i) + \epsilon(z_i, xy) \equiv \epsilon(x, z_i)T(y) + \epsilon(y, z_i x), \tag{11}$$

$$\epsilon(x, y)T(z_j) + \epsilon(z_j, xy) \equiv \epsilon(x, z_j)T(y) + \epsilon(y, z_j x). \tag{12}$$

Subtracting (11) and (12) gives for *all* x, y, i, j,

$$\begin{aligned} \epsilon(z_i, xy) - \epsilon(z_j, xy) \equiv T(y)\{\epsilon(x, z_i) - \epsilon(x, z_j)\} \\ + \epsilon(y, z_i x) - \epsilon(y, z_j x). \end{aligned} \tag{13}$$

If for *some* x, i, j, $\epsilon(x, z_i) \not\equiv \epsilon(x, z_j)$, (13) implies that $T(y)$ has a value domain of not more than $8k$ values, which contradicts the hypothesis. Hence for all x; $i, j = 1, \cdots, \Delta$,

$$\epsilon(x, z_i) = \epsilon(x, z_j). \tag{14}$$

This gives $T(xz_i) - T(x)T(z_i) = T(xz_j) - T(x)T(z_j)$ or

$$T(xz_i) = T(xz_j). \tag{15}$$

Replacing x by xz_i^{-1} in (15) we get for all $x, i, j = 1, \cdots, \Delta$,

$$T(x) = T(xz_i^{-1}z_j). \tag{16}$$

From (16) we see that $Z=\{z_1^{-1}z_1, z_1^{-1}z_2, \cdots, z_1^{-1}z_\Delta\}$ are Δ distinct numbers such that

$$T(z_1^{-1}z_i) = 1.$$

Then if $\alpha_1, \cdots, \alpha_N$ are the N distinct values in the value domain and $x_1, \cdots, x_N$ are such that $T(x_i)=\alpha_i$, $i=1, \cdots, N$, we see from (16) that

$$T(x_iZ) = T(x_i) = \alpha_i, \qquad i = 1, \cdots, N.$$

Hence at least Δ numbers map into each α_i, and we have $p-1 \geqq \Delta N \geqq p-1$. Thus $p-1=N\Delta$ and $N \mid (p-1)$.

COROLLARY 1. *If $N>8k$, $p>8k^2$, and $\|T(xy)-T(x)T(y)\|_p<k$, then the set Z of those numbers which map into 1 is a subgroup of order $(p-1)/N$ of the group of residues prime to p, and all the elements of a given coset map into the same number.*

PROOF. To prove that Z is a group we need only show that it is closed. Both this and the remainder of the corollary is clear from (16) and Theorem 2.

COROLLARY 2. *If $N>8k$, $p>8k^2$, $\|T(xy)-T(x)T(y)\|_p<k$, and $p-1$ has no divisors which lie in the interval $(8k, 8k^2)$, then $T(x)\equiv x^a \pmod p$.*

COROLLARY 3. *If $\|T(xy)-T(x)T(y)\|_p<k$, $k>0$, $p>8k^2$ and, for some primitive root ρ, $T(\rho)=1$ then $N \leqq 8k$.*

PROOF. If $N>8k$ then the subgroup Z contains ρ and hence Z is the whole group. But this means $N=1>8k$ which is impossible.

PRINCETON UNIVERSITY