# A PROPERTY OF FAREY SEQUENCES, WITH APPLICATIONS TO qTH POWER RESIDUES

PASQUALE PORCELLI AND GORDON PALL

THE Farey sequence of order $h - 1$ consists of the reduced rational fractions from 0 to 1 inclusive, with denominators less than $h$, and arranged in order of magnitude. Thus, if $h = 6$, the sequence is

$$0/1,\ 1/5,\ 1/4,\ 1/3,\ 2/5,\ 1/2,\ 3/5,\ 2/3,\ 3/4,\ 4/5,\ 1/1. \tag{1}$$

It is well known that for any two consecutive terms $r/s$ and $t/u$,

$$ts - ru = 1, \quad s + u \geqslant h. \tag{2}$$

The principal result of this note is the observation that, by means of a Farey sequence, there can be written a complete system of residues, modulo an integer $n$, this system being expressed by fractions of the form $a/u$, with $a$ and $u$ suitably bounded.

THEOREM 1. *The integers of the sequence* $1, 2, \ldots, n$ *are obtained in order, each integer exactly once, in the sequence of sequences associated in the following manner with the terms $t/u$ of a Farey sequence. With the term $t/u$ is associated the sequence (possibly, for small $n$, empty) of positive integers*

$$(nt + a)/u, \quad -n/(s + u) < a \leqslant n/(u + w), \tag{3}$$

*where $r/s$ and $v/w$ denote, respectively, the predecessor and successor of $t/u$ in the Farey sequence (non-positive or positive values $a$ being omitted if $t/u$ is* $0/1$ *or* $1/1$*, respectively), and $a$ runs over these integral values in the stated interval such that $(nt + a)/u$ is an integer.*

To illustrate the theorem and its later application, the sequences in the case $h = 6$ associated with the terms in (1) are

$$a\ (0 \leqslant a \leqslant n/6);\ (n + a)/5 \quad (-n/6 < a \leqslant n/9, a \equiv -n \bmod 5);$$
$$(n + a)/4 \quad (-n/9 < a \leqslant n/7, a \equiv -n \bmod 4); \ldots;$$
$$(2n + a)/5 \quad (-n/8 < a \leqslant n/7, a \equiv -2n \bmod 5); \ldots.$$

It will be noted that the sequences associated with different terms of the Farey sequence do not overlap, and between them exactly cover the interval 1 to $n$. Also, $|a|$ does not exceed $n/6$, and if $n$ is prime to all the denominators in (1), then the expression $a/u$ (where $1 \leqslant u \leqslant 5$ and $|a| \leqslant n/6$) gives every residue mod $n$, with possibly some overlapping.

The proof of the theorem depends on the simple observation that, if $r/s$ and $t/u$ are consecutive terms of the Farey sequence, then

$$\frac{rn + \dfrac{n}{s + u}}{s} = \frac{tn - \dfrac{n}{s + u}}{u}, \tag{4}$$

this reducing to $(2_1)$. It follows that the *real* numbers from 1 to $n$ are covered by allowing $a$ to assume all real values in the successive intervals in (3). The integers in this interval are therefore obtained by expressing the condition on $a$ for $(nt + a)/u$ to be an integer: namely, $a$ must be an integer congruent to $-nt$ mod $u$.

If $n$ is an odd prime $p$, and $p > 2h - 2$, then since $u + w < p$, equality cannot hold in the last part of (3). Thus, the sequence $1, 2, \ldots, p - 1$ is obtained by allowing $a$ to range over the integers not exceeding numerically the greatest integers in $n/(s + u)$ and $n/(u + w)$. Since $s + u \geqslant h$ and $u + w \geqslant h$, we have the following result.

THEOREM 2. *Let $p$ be an odd prime, $h$ be a positive integer, $p > 2h - 2$, $k = [p/h]$. The sequence $1, \ldots, p - 1$ is obtained, possibly with some overlapping, by giving $a$ the positive integer values from 1 to $k$ inclusive such that $(pt \pm a)/u$ are integers. Negative and positive values $\pm a$ are omitted if $t/u$ is 0/1 or 1/1 respectively.*

Since $1 \leqslant u < h$ and $1 \leqslant a \leqslant k$, the following is an immediate corollary.

THEOREM 3. *Let $p$ be an odd prime, $h$ and $q$ be positive integers, $p > 2h - 2$, $k = [p/h]$, and $D$ denote the residue modulo $p$ of the $q$th power of some integer prime to $p$. Then one of the numbers $Du^q$ $(u = 1, 2, \ldots, h - 1)$ is congruent to at least one of the numbers $(\pm 1)^q, (\pm 2)^q, \ldots, (\pm k)^q$ modulo $p$.*

It is interesting to notice that if $q = 2$ and $h = 2$, this reduces to the familiar proposition that the squares of $1, 2, \ldots, \frac{1}{2}(p - 1)$ constitute a complete system of quadratic residues mod $p$.

Theorem 3 permits a considerable reduction in the work of solving the congruence $x^q \equiv D \pmod{p}$, especially when $p$ is beyond the range of existing tables of indices. The single congruence can be replaced by a system in which $D$ is replaced in turn by $Du^q$ $(u = 1, 2, \ldots, h - 1)$ reduced mod $p$. If $D'$ denotes any one of these residues, the values $D' + yp$ need to be constructed only up to the limits $(\pm k)^q$, where $k = [p/h]$. The possible values $y$ can be restricted by the method of exclusion. Further restrictions on $y$ can be obtained from the property that the quantities (3) are integral, and by examining the Farey series for any given $h$, the limit $k$ can be replaced by possibly smaller limits $p/(s + u)$ or $p/(u + w)$ for each particular value of $u$. In the case $q = 2$, by taking $h$ approximately equal to $p^{\frac{1}{2}}$, the amount of work is reduced by a factor of the order of size of $\frac{1}{2}p^{\frac{1}{2}}$, and (as may be more important) the effective range of a table of squares (or $q$th powers) is greatly increased. Thus, by taking $h = [p^{\frac{1}{2}}]$, primes up to $10^8$ can be handled with a table of squares up to $10000^2$. Note, finally that the modulus need not be assumed to be a prime.

Thanks are due to the referee who pointed out an error in our earlier, different proof of Theorem 1, in which we overlooked the possibility that for some $n$'s, the sequence (3) may be vacuous.

*University of Texas and*
*Illinois Institute of Technology*