Year: 2019 | **Vol.: 94** | **Fasc.: 1-2**

Title: Pseudo-random subsets constructed by using Fermat quotients

Author(s): Huaning Liu and Guotuo Zhang

Let p be a prime, and let n be an arbitrary integer with $(n, p) = 1$. The Fermat quotient $q_p(n)$ is defined as the unique integer with

$$q_p(n) \equiv \frac{n^{p-1} - 1}{p} \pmod{p}, \qquad 0 \le q_p(n) \le p - 1.$$

We also define $q_p(kp) = 0$ for $k \in \mathbb{Z}$. In this paper, we study the pseudo-randomness of subsets constructed by Fermat quotients, by using the estimates for exponential sums and character sums with Fermat quotients.

Address:
Huaning Liu
School of Mathematics
Northwest University
Xi'an 710127, Shaanxi
P. R. China

Address:
Guotuo Zhang
School of Mathematics
Northwest University
Xi'an 710127, Shaanxi
P. R. China