

1145-VL-1378

Shahriyar Roshan Zamir* (rosha013@d.umn.edu). *Subgroups of Groups of Units Modulo n* . Preliminary report.

The set of all positive integers less than n and relatively prime to n with multiplication mod n is a group denoted $U(n)$. These groups are useful in algebra, number theory and computer science. We are interested in subgroups of $U(n)$. As part of their 1980's paper titled *factoring groups of integers modulo n* Gallian and Rusin determined the structure of $U(n)$ and $U_s(n)$ for $n = st$ where $\gcd(s, t) = 1$ and $U_s(n) = \{x \in U(n) \mid x \pmod{s} = 1\}$. Inspired by their work and some exercises in Gallian's *Contemporary Abstract Algebra* we identified new families of subgroups of $U(n)$. For a subgroup H of $U(n)$ and an integer k we define:

$$U_{k,H}(n) = \{x \in U(n) \mid x \pmod{k} \in H\}.$$

We give a complete classification of these subgroups and their factor groups for the special cases of $H = \{1\}$ and $H = \{1, -1\}$. We also define $U^{(k)}(n) = \{x \in U(n) \mid x^k = e\}$ and $U(n)^{(k)} = \{x^k \mid x \in U(n)\}$. Our results completely classify the latter subgroups and their factor groups.

(Received September 21, 2018)