QM
QUAESTIONES MATHEMATICAE
JOURNAL OF THE SOUTH AFRICAN MATHEMATICAL SOCIETY
47(7) 2024

Taylor & Francis
Taylor & Francis Group

Quaestiones Mathematicae

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/tqma20

Sophie Germain prime *p* and the permutation of product of first *p* cycles

M. Makeshwari, V.P. Ramesh & R. Thangadurai

To cite this article: M. Makeshwari, V.P. Ramesh & R. Thangadurai (31 Jul 2024): Sophie Germain prime *p* and the permutation of product of first *p* cycles, Quaestiones Mathematicae, DOI: 10.2989/16073606.2024.2374787

To link to this article: https://doi.org/10.2989/16073606.2024.2374787

Published online: 31 Jul 2024.

Quaestiones Mathematicae 2024: 1–6.

https://doi.org/10.2989/16073606.2024.2374787

This is the final version of the article that is published ahead of the print and online issue

SOPHIE GERMAIN PRIME p AND THE PERMUTATION OF PRODUCT OF FIRST p CYCLES

M. Makeshwari
Department of Mathematics, Central University of Tamil Nadu, Thiruvarur - 610005, Tamil Nadu, India.
E-Mail makheswarim@gmail.com

V.P. Ramesh*
Department of Mathematics, Central University of Tamil Nadu, Thiruvarur - 610005, Tamil Nadu, India.
E-Mail vpramesh@gmail.com

R. Thangadurai
Harish-Chandra Research Institute, A CI of Homi Bhabha National Institute, Chhatnag Road, Jhunsi, Prayagraj 211019, India.
E-Mail thanga@hri.res.in

Abstract. For a natural number n, the permutation $(n!)$ is defined as the left-to-right product of the first n cycles, namely, $(n!) = \prod_{k=0}^{n-1}(1, 2, \ldots, (n-k))$ (see [1]). In this article, we prove that for any natural number n, 2 is a primitive root of $2n+1$ if and only if $2n+1 = p^k$ for some odd prime number p and for some natural number k such that the permutation $(n!)$ has exactly k orbits. We also prove that a prime number p is a Sophie Germain prime if and only if the permutation $(p!)$ has at most two orbits.

Mathematics Subject Classification (2020): Primary: 20B30; Secondary: 11A41.
Key words: Primitive root, Sophie Germain prime, permutation, orbits of permutation.

1. Introduction. A prime number p is called *a Sophie Germain prime* [2] if $2p+1$ is also a prime number. It is well-known that Fermat's last theorem is true for such a prime exponent. However, it is still unknown on the infinitude of such prime numbers. For any natural number $n > 1$, an integer a which is coprime to n is called *a primitive root of* n (see for instance, [2]) if the order of a modulo n is $\phi(n)$, the Euler totient function.

On a set of symbols A and a permutation σ on A, it is easy to see that a relation $\sim$ on A defined as $i \sim j$ for any $i, j \in A$, if there exists $k \in \mathbb{Z}$ such that $\sigma^k(i) = j$ is an equivalence relation. The equivalence classes of this equivalence

*Corresponding author.

relation are called *orbits of* σ (refer [3]). It is easy to see that, the orbits of the identity permutation of A are the singleton subsets of A and hence the identity permutation has $|A|$ orbits. Now, a permutation σ is said to be *transitive* if σ has exactly one orbit.

In 1969, for any natural number n, Aulicino and Goldfeld in [1] defined a permutation $(n!)$ as $(n!) = \prod_{k=0}^{n-1}(1, 2, \ldots, (n-k))$ and they proved that *the permutation* $(n!)$ *is transitive if and only if* $2n+1$ *is a prime number with* 2 *as a primitive root of* $2n+1$. Here, it is to be noted that the product of permutations is in left-to-right order.

In this article, we present an extension of the result of Aulicino and Goldfeld by considering $2n+1$ to be prime power and the permutation $(n!)$ having more than one orbit, which provides an equivalent condition for 2 being a primitive root of $2n+1$. More precisely, we prove

THEOREM 1.1. *Let* n *be any natural number. Then* 2 *is a primitive root of* $2n+1$ *if and only if* $2n+1 = p^k$ *for some odd prime number* p *and for some natural number* k *such that the permutation* $(n!)$ *has exactly* k *orbits.*

And, we prove a relation connecting a Sophie Germain prime p with the permutation $(p!)$ as follows.

THEOREM 1.2. *Let* p *be a prime number. Then* p *is a Sophie Germain prime if and only if the permutation* $(p!)$ *has at most two orbits.*

We also prove the following result connecting natural number n, the permutation $(n!)$ and the order of 2 modulo $2n+1$.

THEOREM 1.3. *Let* n *be a natural number such that* $2n+1$ *is prime. Then* $(n!)$ *has* k *orbits if and only if the order of* 2 *modulo* $2n+1$ *is* $\frac{\phi(2n+1)}{k}$.

2. Preliminaries.

In this section, we first recall some notations from [1]. For any natural number n, the permutation $P(2n+1)$ is defined as

$$P(2n+1) = \prod_{k=1}^{n}(1, 3, 5, \ldots, (2n+1-2k)).$$

We recall a result proved by Aulicino and Goldfeld in [1] as follows.

PROPOSITION 2.1. (Aulicino and Goldfeld [1]) *Let* $m \geq 3$ *be any odd integer and let* j *be any odd integer such that* $1 \leq j \leq m-2$.

(1) *The permutations* $(\frac{m-1}{2}!)$ *and* $P(m)$ *have the same number of orbits.*

(2) *If the image of* j *in the permutation* $P(m)$ *is denoted by* $A_m(j)$, *then,*

$$A_m(j) = \frac{j+m}{(j+m, 2^m)}.$$

(3) *Let* $O_m(j) = \{A_m^0(j), A_m^1(j), \ldots, A_m^{r-1}(j)\}$ *be the orbit of* j *in* $P(m)$*, where* $A_m^0(j) = A_m^r(j) = j$ *and* $A_m^{k+1}(j) = A_m(A_m^k(j))$*. Let*

$$S_m(j) = \left\{A_m^0(j), \frac{A_m^0(j)+m}{2}, \ldots, \frac{A_m^0(j)+m}{2^{s_1}}; A_m^1(j), \ldots, \frac{A_m^1(j)+m}{2^{s_2}};\right.$$

$$\left. \ldots A_m^{r-1}(j), \ldots, \frac{A_m^{r-1}(j)+m}{2^{s_r}}\right\}$$

be the set derived from $O_m(j)$ *where* $2^{s_k+1} = (2^m, A_m^{k-1}(j)+m)$*. Then* $S_m(1)$ *is a subgroup of* $(\mathbb{Z}/m\mathbb{Z})^*$ *generated by* 2*.*

We observe the following.

LEMMA 2.1. *Let* $m \geq 3$ *be any odd integer and* $j \in (\mathbb{Z}/m\mathbb{Z})^*$ *be any odd integer. Then* $A_m(j) \in (\mathbb{Z}/m\mathbb{Z})^*$*.*

Proof. Suppose there exists an odd element j of $(\mathbb{Z}/m\mathbb{Z})^*$ such that $A_m(j) \notin (\mathbb{Z}/m\mathbb{Z})^*$. Then

$$\begin{aligned} \left(\frac{j+m}{(j+m,2^m)}, m\right) &\neq 1, \text{ since } A_m(j) = \frac{j+m}{(j+m,2^m)} \\ \implies (j+m,m) &\neq 1, \end{aligned}$$

which is a contradiction to $j \in (\mathbb{Z}/m\mathbb{Z})^*$. Therefore, $A_m(j) \in (\mathbb{Z}/m\mathbb{Z})^*$. □

We recall the following results which are needed in the proof of Theorem 1.2.

THEOREM 2.1. (Theorem 1.1 in [5]) *Let* $p > 2$ *be a prime number such that* $2p+1$ *is a prime or prime power. Then* 2 *is a primitive root of* $2p+1$ *if and only if* $p \equiv 1 \pmod 4$.

LEMMA 2.2. (Lemma 1.2 in [5]) *Let* p *be an odd prime number such that* $2p+1 = q^k$ *for some prime* q *and* $k \geq 2$*. Then* $q = 3$*,* k *is a prime and* $p \equiv 1 \pmod 4$.

LEMMA 2.3. (Corollary 1.6 in [5]) *Let* p *be an odd prime number. Then the permutation* $(p!)$ *is transitive if and only if* $2p+1$ *is a prime number and* $p \equiv 1 \pmod 4$.

LEMMA 2.4. (Lemma 1 in [4]) *Let* m *be odd and* $1 \leq j \leq m-2$ *be also odd. Then* $S_m(j) = \{(2^k j) \pmod m \mid 1 \leq k \leq \ell\}$ *where* ℓ *is the order of* 2 *modulo* $\frac{m}{(j,m)}$*.*

3. Proof of Theorem 1.1. Let n be any natural number such that 2 is a primitive root of $2n+1$. Then, by Gauss's theorem, we conclude that $2n+1 = p^k$ for some odd prime number p and $k \in \mathbb{N}$.

In order to prove the permutation $(n!)$ has k orbits, we shall show that the orbits of $P(2n+1)$ precisely are

$$O_{2n+1}(1), O_{2n+1}(p), \ldots, O_{2n+1}(p^{k-1}).$$

Now, since 2 is a primitive root of $2n+1$, by the definitions of $O_{p^k}(1)$ and $S_{p^k}(1)$, we have $O_{p^k}(1)$ is the set of all odd integers residues in $S_{p^k}(1)$ and $S_{p^k}(1) = \{2^\ell \pmod{p^k} \mid 1 \leq \ell \leq p^{k-1}(p-1)\} = (\mathbb{Z}/p^k\mathbb{Z})^*$.

If $k=1$, then $S_p(1) = (\mathbb{Z}/p\mathbb{Z})^*$ and hence $O_p(1)$ is the only orbit of $P(2n+1)$. Therefore, the permutation $(n!)$ has only one orbit in this case. Now, we can assume that $k > 1$.

In this case, $p \notin S_{p^k}(1)$, since $p \notin (\mathbb{Z}/p^k\mathbb{Z})^*$. Then note that $S_{p^k}(p) = \{2^\ell p \pmod{p^k} \mid \ell \in \mathbb{N}\}$. If $2^{\ell_1}p \equiv 2^{\ell_2}p \pmod{p^k}$ for some $\ell_1, \ell_2 \in \mathbb{N}$, then $2^{\ell_1} \equiv 2^{\ell_2} \pmod{p^{k-1}}$ which implies that $\ell_1 \equiv \ell_2 \pmod{ord_{p^{k-1}}(2)}$. Since 2 is a primitive root of p^k (and hence modulo p^{k-1}), we conclude that $\mid S_{p^k}(p) \mid = p^{k-2}(p-1)$. Thus, if $k=2$, then, it is easy to see that $S_{p^2}(1) \cup S_{p^2}(p) = \{1, 2, \ldots, p^2-1\}$ and hence $O_{p^2}(1)$ and $O_{p^2}(p)$ are the only two orbits of $P(2n+1)$.

Now, assume that $k > 2$. Now note that $p^2 \notin S_{p^k}(p)$. For otherwise, if $p^2 \in S_{p^k}(p)$, then $p^2 \equiv 2^\ell p \pmod{p^k}$ for some $1 \leq \ell \leq p^{k-2}(p-1)$ which implies that $p \equiv 2^\ell \pmod{p^{k-1}}$, a contradiction. Since $S_{p^k}(p^2) = \{2^\ell p^2 \pmod{p^k} \mid \ell \in \mathbb{N}\}$, in a similar way, we can conclude that $\mid S_{p^k}(p^2) \mid = p^{k-3}(p-1)$.

By repeating this procedure, we get $S_{p^k}(p^i) = \{2^\ell p^i \pmod{p^k} \mid \ell \in \mathbb{N}\}$ and $\mid S_{p^k}(p^i) \mid = p^{k-i-1}(p-1)$ for all $i \leq k-1$. Since $\mid S_{p^k}(1) \mid + \mid S_{p^k}(p) \mid + \cdots + \mid S_{p^k}(p^{k-1}) \mid = p^k - 1$, we get $\displaystyle\bigcup_{a=0}^{k-1} S_{p^k}(p^a) = \{1, 2, 3, \ldots, p^k-1\}$.

Note that if $1 \leq j < p^k$ is any odd integer, then $j \in O_{p^k}(p^i)$ for some $0 \leq i \leq k-1$. Hence, $O_{p^k}(1), O_{p^k}(p), \ldots, O_{p^k}(p^{k-1})$ are the k orbits of $P(2n+1)$ which implies that $(n!)$ has k orbits.

Conversely, suppose 2 is not a primitive root of $2n+1$. Therefore, $(\mathbb{Z}/(2n+1)\mathbb{Z})^* \neq \langle 2 \rangle$. Then observe that there exists an odd integer g such that $g \in (\mathbb{Z}/(2n+1)\mathbb{Z})^* \backslash \langle 2 \rangle$. Suppose that any element $g \in (\mathbb{Z}/(2n+1)\mathbb{Z})^* \backslash \langle 2 \rangle$ is an even integer. Then $\dfrac{g}{(g, 2^{\phi(2n+1)})}$ is odd and hence we get $\dfrac{g}{(g, 2^{\phi(2n+1)})} \in \langle 2 \rangle$, a contradiction as $g \notin \langle 2 \rangle$. Then, by Lemma 2.1, it follows that $O_{p^k}(g) \subset (\mathbb{Z}/(2n+1)\mathbb{Z})^*$. Therefore, we get $O_{p^k}(1), O_{p^k}(g), O_{p^k}(p), \ldots, O_{p^k}(p^{k-1})$ are disjoint orbits of $P(2n+1)$, which is a contradiction to $(n!)$ has k orbits. □

4. Proof of Theorem 1.2. Suppose p is a Sophie Germain prime. We prove that $(p!)$ has at most 2 orbits. When $p=2$, we clearly see that the permutation $(2!) = (1\ 2)$ has only one orbit. Hence we can assume that p is an odd prime. If $p \equiv 1 \pmod 4$, then by Lemma 2.3, we can conclude that the permutation $(p!)$ has single orbit. Thus, we can assume that $p \equiv 3 \pmod 4$.

In this case, it is enough to prove that $O_{2p+1}(1)$ and $O_{2p+1}(p)$ are the only two orbits of $P(2p+1)$. Since $p \equiv 3 \pmod 4$, by Theorem 2.1, we conclude that 2 is not a primitive root of $2p+1$. Since $2p+1$ is also a prime number, we conclude that the order of 2 modulo $2p+1$ is p. Thus, $S_{2p+1}(1) = \{2^i \pmod{2p+1} \mid 1 \le i \le p\}$.

If $p \in S_{2p+1}(1)$, then $p \equiv 2^i \pmod{2p+1}$ for some $1 < i < p$ and hence we get

$$p^p \equiv (2^i)^p = (2^p)^i \equiv 1 \pmod{2p+1}$$

as the order of 2 is p modulo $2p+1$. Therefore, we get $(-1)^p \equiv (2p)^p \equiv 1 \pmod{2p+1}$, a contradiction to $p \equiv 3 \pmod 4$. Therefore, we conclude that $p \notin S_{2p+1}(1)$. Then by the definition of $S_{2p+1}(p)$, we can get $S_{2p+1}(p) = \{2^i p \pmod{2p+1} \mid 1 \le i \le p\}$. Since $S_{2p+1}(1) \cap S_{2p+1}(p) = \emptyset$ and $\mid S_{2p+1}(1) \mid + \mid S_{2p+1}(p) \mid = 2p$, we get $S_{2p+1}(1) \cup S_{2p+1}(p) = (\mathbb{Z}/(2p+1)\mathbb{Z})^*$. Therefore, if j is any odd integer satisfying $1 \le j \le 2p-1$, then we see that either $j \in O_{2p+1}(1)$ or $j \in O_{2p+1}(p)$. Thus, $O_{2p+1}(1)$ and $O_{2p+1}(p)$ are the two orbits of $P(2p+1)$ and hence $(p!)$ has two orbits.

Conversely, suppose p is a prime number such that $2p+1$ is not a prime number. Hence p must be an odd prime such that $p \ge 7$. We consider the following two cases.

Case 1. $2p+1 = p_1 p_2 \ell$, where p_1, p_2 are two distinct odd prime factors of $2p+1$ and ℓ is an odd positive integer.

In order to get a contradiction, we shall prove that $P(2p+1)$ has at least three orbits comprising, $O_{2p+1}(1)$, $O_{2p+1}(p_1)$ and $O_{2p+1}(p_2)$.

By Lemma 2.1, since $O_{2p+1}(1)$ contains only the odd integers of $(\mathbb{Z}/(2p+1)\mathbb{Z})^*$ and p_1 and p_2 are odd prime divisors of $2p+1$, we conclude that $p_1, p_2 \notin O_{2p+1}(1)$. Now, to finish the proof, we shall prove that $p_2 \notin O_{2p+1}(p_1)$.

Let j be any odd positive integer such that j is not a multiple of p_2 and $jp_1 < 2p+1$. Then we see that

$$A_{2p+1}(jp_1) = \frac{jp_1 + p_1 p_2 \ell}{(jp_1 + p_1 p_2 \ell, 2^{p_1 p_2 \ell})} = \frac{j + p_2 \ell}{(jp_1 + p_1 p_2 \ell, 2^{p_1 p_2 \ell})} p_1.$$

Therefore, we conclude that every element of the orbit $O_{2p+1}(p_1)$ is a multiple of p_1 and hence $p_2 \notin O_{2p+1}(p_1)$. Thus, $P(2p+1)$ has at least three orbits, namely, $O_{2p+1}(1), O_{2p+1}(p_1)$ and $O_{2p+1}(p_2)$, a contradiction to $(p!)$ has at most two orbits.

Case 2. $2p+1 = q^k$, for some odd prime q and a positive integer $k > 1$.

By Lemma 2.2, we must have $q = 3$ and k is a prime. Further, since $\frac{3^2-1}{2} = 4$ is not a prime number, we can assume that $k \ge 3$. In this case, to get a contradiction, we shall prove that $O_{2p+1}(1), O_{2p+1}(3)$ and $O_{2p+1}(9)$ are disjoint orbits of $P(2p+1)$.

Similar to the previous case, it is easy to see that $3, 9 \notin O_{2p+1}(1)$ and we prove that $9 \notin O_{2p+1}(3)$.

If j is any odd positive integer such that it is not a multiple of 3 and $3j < 2p+1$, then by the computation

$$A_{2p+1}(3j) = \frac{3j + 3^k}{(3j + 3^k, 2^{3^k})} = \frac{j + 3^{k-1}}{(3j + 3^k, 2^{3^k})} 3,$$

we see that the elements of the orbit $O_{2p+1}(3)$ are multiples of 3 which are not divisible by 9 and hence $9 \notin O_{2p+1}(3)$. Thus, $O_{2p+1}(1), O_{2p+1}(3)$, and $O_{2p+1}(9)$ are disjoint orbits of $P(2p+1)$, a contradiction. Therefore, $2p+1$ must be a prime number. This proves the theorem. □

5. Proof of Theorem 1.3. Let n be any natural number such that $2n+1$ is prime. We shall prove that $P(2n+1)$ has k orbits if and only if the order of 2 modulo $2n+1$ is $\frac{\phi(2n+1)}{k}$.

Let $1 \leq j \leq 2n-1$ be odd, by Lemma 2.4, it follows that $S_{2n+1}(j) = \{(2^k j) \pmod{2n+1} \mid 1 \leq k \leq ord_{2n+1}(2)\}$ and are cosets of $S_{2n+1}(1) = \langle 2 \rangle$ in $(\mathbb{Z}/(2n+1)\mathbb{Z})^*$. Now, by definitions of $O_{2n+1}(j)$ and $S_{2n+1}(j)$, we have $O_{2n+1}(j)$ is the set all odd integers residues in $S_{2n+1}(j)$.

Therefore, the number of orbits of $P(2n+1)$ is equal to the number of cosets of $\langle 2 \rangle$ in $(\mathbb{Z}/(2n+1)\mathbb{Z})^*$ which is equal to $\frac{\phi(2n+1)}{ord_{2n+1}(2)}$. Hence, $P(2n+1)$ has k orbits if and only if the order of 2 modulo $2n+1$ is $\frac{\phi(2n+1)}{k}$. □

REFERENCES

1. D.J. AULICINO AND M. GOLDFELD, A New Relation Between Primitive Roots and Permutations, *Amer. Math. Monthly* **76**(6) (1969), 664–666.
2. D.M. BURTON, *Elementary Number Theory,* McGraw-Hill, New York, 2012.
3. J.B. FRALEIGH, *A First Course in Abstract Algebra,* Pearson, Harlow, Essex, 2002.
4. V.P. RAMESH, M. MAKESHWARI, AND S. SINHA, Connecting primitive roots and permutations, *Indian J. Pure Appl. Math.* **55** (2024), 513–516.
5. V.P. RAMESH, R. THANGADURAI, M. MAKESHWARI, AND S. SINHA, A necessary and sufficient condition for 2 to be a primitive root of $2p+1$, *Math. Student, Indian Math. Soc.* **89**(3–4) (2020), 171–176.

Received 19 December, 2023 and in revised form 30 May, 2024.