AIMS Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 10(11): 27513–27518.
DOI: 10.3934/math.20251209
Received: 15 July 2025
Revised: 04 November 2025
Accepted: 13 November 2025
Published: 25 November 2025

Research article

On Brizolis' a problem related to primitive roots modulo a prime p

Wenpeng Zhang* **and Xiaoling Xu**

School of Data Science and Engineering, Institute of Mathematical Modeling and Intelligent Computing, Xi'an Innovation College of Yan'an University, Xi'an, Shaanxi, China

* **Correspondence:** Email: wpzhang@nwu.edu.cn.

Abstract: The main purpose of this paper is to use very simple elementary and analytic methods to study a problem related to the primitive root modulo p asked by Brizolis and prove a more general and stronger conclusion.

Keywords: primitive root; elementary and analytic methods; Brizolis' problem and its generalization
Mathematics Subject Classification: 11A07, 11L40

1. Introduction

Let p be an odd prime. For any integer g with $(g, p) = 1$, we call g as a primitive root modulo p, if $g^k \not\equiv 1 \pmod p$ for all $1 \leq k \leq p-2$. For example, if $p = 5$, then $g = 2$ is a primitive root modulo 5; If $p = 7$, then $g = 3$ is a primitive root modulo 7. It is known that for any odd prime p, there are $\varphi(p-1)$ primitive roots in the reduced residue system modulo p, where $\varphi(n)$ is the Euler's totient function. Here, $\varphi(n)$ is defined to be the number of positive integers not exceeding n that are relatively prime to n. About the various properties of a primitive root modulo p, one can find them in many elementary number theory books, such as [1–4]. In [5], Brizolis asked if for any prime $p > 3$ there exists a primitive root g of p and a positive integer $x < p$ such that $x \equiv g^x \bmod p$. If so, can g also be chosen so that $(g, p-1) = 1$?

Regarding this problem, W. P. Zhang [6] proved a qualitative conclusion for the first time. That is, for any prime p large enough, there exists a primitive root g modulo p and a positive integer x such that the congruence $x \equiv g^x \bmod p$.

Based on the idea of W. P. Zhang in [6], M. Levin, C. Pomerance, and K. Soundararajan in [7] solved this problem completely.

In this paper, we use the elementary method to prove a more general conclusion. Namely, we have the following:

Theorem 1. Let p be a large enough prime number. Then, for any fixed positive integer k and distinct primitive roots $1 < g_1,\ g_2, \ldots,\ g_k < p-1$ modulo p with $(g_1 g_2 \cdots g_k, p-1) = 1$, there exist primitive roots $q_1, \ldots, q_k$ modulo p such that for each $i \in \{1, \ldots, k\}$ we have

$$g_i \equiv q_i^{g_i} \pmod{p}.$$

Let us note that when p is large enough, there exists a primitive root g modulo p such that $(g, p-1) = 1$. There is an asymptotic formula for the number $N(p)$ of primitive roots modulo p that satisfy such a condition. That is,

$$\lim_{p\to+\infty} \frac{p \cdot N(p)}{\varphi^2(p-1)} = 1.$$

Therefore, for any positive integer k, when prime p is large enough, there exist k distinct primitive roots $1 < g_1,\ g_2,\ \cdots,\ g_k < p-1$ modulo p such that $(g_1 g_2 \cdots g_k, p-1) = 1$.

Corollary 1. There exist two primitive roots $1 \le g,\ g_1 \le p-1$ modulo p such that $(gg_1, p-1) = 1$ when $p \ge 3600163$.

2. Two auxiliary lemmas

To illustrate the existence of some special primitive roots modulo p, we need the following two simple lemmas.

Lemma 1. Let p be a prime and a be an integer with $(a, p) = 1$. Then we have the identity

$$\frac{\varphi(p-1)}{p-1} \sum_{d|p-1} \frac{\mu(d)}{\varphi(d)} \sum_{\substack{\chi \\ \mathrm{ord}(\chi)=d}} \chi(a) = \begin{cases} 1, & \text{if } a \text{ is a primitive root modulo } p, \\ 0, & \text{otherwise} \end{cases}$$

where μ is the Möbius function, and χ runs over Dirichlet characters modulo p.

Proof. See Proposition 2.2 in [4]. □

Lemma 2. Let p be a prime, and $N(p)$ denote the number of all primitive roots g modulo p in the set $\{1, 2, \ldots, p-1\}$ with $(g, p-1) = 1$. Then we have the estimate

$$N(p) > \frac{\varphi^2(p-1)}{p-1} - \frac{\varphi(p-1)}{p-1} \cdot 4^{\omega(p-1)} \cdot \sqrt{p} \cdot \ln p,$$

where $\omega(n)$ denotes the number of distinct prime factors of n.

Proof. For any positive integer n, we have

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & if\, n = 1, \\ 0 & if\, n > 1. \end{cases}$$

By Lemma 1 we have

$$N(p) = \sum_{\substack{a=1 \\ (a,p-1)=1}}^{p-1} \frac{\varphi(p-1)}{p-1} \sum_{d|p-1} \frac{\mu(d)}{\varphi(d)} \sum_{\substack{\chi \\ \mathrm{ord}\chi=d}} \chi(a)$$

$$
\begin{aligned}
&= \frac{\varphi(p-1)}{p-1} \sum_{d|p-1} \frac{\mu(d)}{\varphi(d)} \sideset{}{'}\sum_{k=1}^{d} \sum_{\substack{a=1 \\ (a,p-1)=1}}^{p-1} \chi_{k,d}(a) \\
&= \frac{\varphi(p-1)}{p-1} \sum_{d|p-1} \frac{\mu(d)}{\varphi(d)} \sideset{}{'}\sum_{k=1}^{d} \sum_{a=1}^{p-1} \sum_{r|(a,p-1)} \mu(r)\chi_{k,d}(a) \\
&= \frac{\varphi(p-1)}{p-1} \sum_{d|p-1} \frac{\mu(d)}{\varphi(d)} \sideset{}{'}\sum_{k=1}^{d} \sum_{r|p-1} \mu(r) \sum_{a=1}^{\frac{p-1}{r}} \chi_{k,d}(ar) \\
&= \frac{\varphi(p-1)}{p-1} \sum_{d|p-1} \frac{\mu(d)}{\varphi(d)} \sideset{}{'}\sum_{k=1}^{d} \sum_{r|p-1} \mu(r)\chi_{k,d}(r) \sum_{a=1}^{\frac{p-1}{r}} \chi_{k,d}(a) \\
&= \frac{\varphi^2(p-1)}{p-1} + \frac{\varphi(p-1)}{p-1} \sum_{\substack{d|p-1 \\ d>1}} \frac{\mu(d)}{\varphi(d)} \sideset{}{'}\sum_{k=1}^{d} \sum_{r|p-1} \mu(r)\chi_{k,d}(r) \sum_{a=1}^{\frac{p-1}{r}} \chi_{k,d}(a), \qquad (2.1)
\end{aligned}
$$

where $\sum{}'^{d}_{k=1}$ denotes the sum of all values k that satisfy $(k,d) = 1$, $\chi_{k,d}$ denote a d-order character modulo p.

For any non-principal character χ modulo p, from Pólya's inequality (see [1]) we have the estimate

$$
\left| \sum_{a=1}^{\frac{p-1}{r}} \chi(a) \right| \le \sqrt{p} \cdot \ln p, \qquad (2.2)
$$

where r is a positive integer with $r \mid p-1$.

Note that

$$
\sum_{d|p-1} |\mu(d)| = 2^{\omega(p-1)}.
$$

From (2.1) and (2.2) we have the estimate

$$
\begin{aligned}
N(p) &\ge \frac{\varphi^2(p-1)}{p-1} - \frac{\varphi(p-1)}{p-1} \sum_{\substack{d|p-1 \\ d>1}} \frac{|\mu(d)|}{\varphi(d)} \sideset{}{'}\sum_{k=1}^{d} \sum_{r|p-1} |\mu(r)| \cdot \sqrt{p} \cdot \ln p \\
&= \frac{\varphi^2(p-1)}{p-1} - \frac{\varphi(p-1)}{p-1} \sum_{\substack{d|p-1 \\ d>1}} |\mu(d)| \cdot \sum_{r|p-1} |\mu(r)| \cdot \sqrt{p} \cdot \ln p \\
&> \frac{\varphi^2(p-1)}{p-1} - \frac{\varphi(p-1)}{p-1} \left(\sum_{d|p-1} |\mu(d)| \right)^2 \cdot \sqrt{p} \cdot \ln p \\
&= \frac{\varphi^2(p-1)}{p-1} - \frac{\varphi(p-1)}{p-1} \cdot 4^{\omega(p-1)} \cdot \sqrt{p} \cdot \ln p.
\end{aligned}
$$

This proves Lemma 2. □

3. Proof of the main result

In this section, we provide direct proofs of Theorem 1 and Corollary 1.

Proof of Theorem 1. Let p be a prime large enough. Then for any fixed positive integer k, from Lemma 2 we know that there exists k distinct primitive roots g_i modulo p with $(g_i, p-1) = 1$, $i = 0, 1, 2, \cdots, k$.

Fix a primitive root g modulo p. We know that there is a positive integer $y_i \leq p-1$ such that $g_i \equiv g^{y_i} \pmod{p}$. Since g_i is a primitive root modulo p, we have $(y_i, p-1) = 1$. Solve the following congruence for x_i.

$$x_i \cdot y_i \equiv g_i \pmod{p-1}. \tag{3.1}$$

Let $\overline{x}_i$ be such that $\overline{x}_i \cdot x_i \equiv 1 \pmod{p-1}$ and $q_i \equiv g^{\overline{x}_i} \pmod{p}$ for each $1 \leq i \leq k$. Since $(\overline{x}_i, p-1) = 1$, so $q_i \equiv g^{\overline{x}_i} \pmod{p}$, there exist primitive roots $q_1, \ldots, q_k$ modulo p. Now, from (3.1) we have

$$g_i \equiv g^{y_i} \equiv \left(g^{x_i \cdot \overline{x}_i}\right)^{y_i} \equiv \left(g^{\overline{x}_i}\right)^{y_i \cdot x_i} \equiv q_i^{g_i} \pmod{p}.$$

Hence, there exist k primitive roots $1 < q_1,\ q_2,\ \cdots,\ q_k < p-1$ such that the following congruence holds.

$$g_i \equiv q_i^{g_i} \pmod{p},\ i = 1,\ 2,\ \ldots,\ k.$$

This completes the proof of our theorem. □

Example 1. Let $p = 13$ and $i = 1$. Fix $g = 2$. Given $g_1 = 7$, we consider the congruence $7 \equiv 2^{y_1} \pmod{13}$. We get $y_1 = 11$. Solve $x_i \cdot y_i \equiv g_i \pmod{p-1}$.

$$11x_1 \equiv 7 \pmod{12} \implies x_1 \equiv 5 \pmod{12}.$$

Then, we construct $q_1 = g^{\overline{x}_i} \equiv 2^5 \equiv 6 \pmod{13}$. Finally $q_1^{g_1} = 6^7 \equiv 7 \pmod{13}$. Thus, we have $g_i \equiv q_i^{g_i} \pmod{p}$.

Proof of Corollary 1. Indeed, note that for any integer $n \geq 3$ we have (see [8])

$$\varphi(n) > \frac{\ln 2}{2} \cdot \frac{n}{\ln n}, \tag{3.2}$$

and (see [9,10])

$$\omega(n) \leq 1.3841 \cdot \frac{\ln n}{\ln \ln n}. \tag{3.3}$$

Using (3.2), (3.3), and Lemma 2, one can calculate that if $p \geq 3600163$, then $N(p) \geq 2$. That is, there exist two primitive roots $1 \leq g,\ g_1 \leq p-1$ modulo p such that $(gg_1, p-1) = 1$ when $p \geq 3600163$. □

4. Conclusions

The main purpose of this paper is to study a problem from [5] posed by Brizolis. We proved a more general and stronger result than the affirmative answer to the mentioned problem. Namely, for any sufficiently large prime p, fixed positive integer k and k distinct primitive roots $1 < g_1, g_2, \ldots, g_k < p-1$ modulo p with $(g_1, g_2, \ldots, g_k, 1) = 1$, there exist k distinct primitive roots $1 < q_1, q_2, \cdots, q_k < p-1$ modulo p such that

$$g_i \equiv q_i^{g_i} \pmod{p}, i = 1, 2, \cdots, k.$$

We believe that the research method in this paper can be used as a reference for further research on similar problems.

Author contributions

All authors have equally contributed to this work. All authors read and approved the final manuscript.

Acknowledgments

This work is supported by the N. S. F. (11771351) of China.

Conflict of interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

1. T. M. Apostol, *Introduction to analytic number theory,* Springer-Verlag, New York, 1976. https://doi.org/10.1007/978-1-4757-5579-4
2. R. Ayoub, *An introduction to the analytic theory of numbers,* American Mathematical Society, Providence, 1963, 295.
3. K. Ireland, M. Rosen, *A classical introduction to modern number theory,* Springer-Verlag, New York, 1982.
4. W. Narkiewicz, *Classical problems in number theory,* Polish Scientifc Publishers, WARSZAWA, 1986.
5. R. K. Guy, *Unsolved problems in number theory,* Springer-Vlerlag, Berlin, 1994, 244. https://doi.org/10.1007/978-0-387-26677-0
6. W. P. Zhang, On a problem of Brizolis, *Pure Appl. Math.*, **11** (1995), 1–3.
7. M. Levin, C. Pomerance, K. Soundararajan, *Fixed points for discrete logarithms,* ANTS-IX 2010, LNCS, **6197** (2010), 6–15. https://doi.org/10.1007/978-3-642-14518-6-5
8. H. Hatalová, T. Šalát, Remarks on two results in elementary theory of numbers, *Acta Fac. Rer. Natur Univ. Comenian. Math.*, **20** (1969), 113–117.

9. G. Robin, Estimation de la fonction de Tchebychef θ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n, *Acta Arith.*, **42** (1983), 367–389. http://eudml.org/doc/205883

10. G. Robin, Sur la différence $Li(\theta(x)) - \pi(x)$, *Annales Fac. Sci. Toulouse*, **6** (1984), 257–268.

AIMS Press