MATHEMATICS OF COMPUTATION
Volume 78, Number 266, April 2009, Pages 1193–1195
S 0025-5718(08)02090-5
Article electronically published on October 31, 2008

A NEW PRIME p FOR WHICH THE LEAST PRIMITIVE ROOT $(\mathrm{mod}\ p)$ AND THE LEAST PRIMITIVE ROOT $(\mathrm{mod}\ p^2)$ ARE NOT EQUAL

A. PASZKIEWICZ

Abstract. With the aid of a computer network we have performed a search for primes $p < 10^{12}$ and revealed a new prime $p = 6692367337$ for which its least primitive root $(\mathrm{mod}\ p)$ and its least primitive root $(\mathrm{mod}\ p^2)$ are not equal.

1. Introduction

Denote by $g(p)$ the least primitive root of a prime p and by $h(p)$ the least primitive root $(\mathrm{mod}\ p^2)$. Note that according to Jacobi, for an odd prime p, any primitive root $(\mathrm{mod}\ p^2)$ is also a primitive root $(\mathrm{mod}\ p^k)$ for each natural number k. Given a primitive root $(\mathrm{mod}\ p)$, it is quite easy to find a primitive root $(\mathrm{mod}\ p^k)$. This is due to an old theorem by V. A. Lebesque which states:

Theorem. *Let p be an odd prime. If g is a primitive root* $(\mathrm{mod}\ p)$ *and* $g \cdot g' \equiv 1 \pmod{p^k}$, $1 < g, g' < p$, *then either g or g' is a primitive root* $(\mathrm{mod}\ p^k)$ *for* $k = 1, 2, \ldots$.

Unfortunately, this theorem does not give the answer to which number g or g' is the primitive root $(\mathrm{mod}\ p^k)$. It has been shown by computation that in most small cases we have $g(p) = h(p)$. In 1971 E. L. Litver and G. E. Yudina [5] found that among primes below 1001321 there exists only one prime $p = 40487$, for which $g(p) \neq h(p)$. We have $g(p) = 5$ and $h(p) = 10$ for that p.

2. Method of approach and the new result

From elementary number theory we have the following simple criterion.

Criterion. *If g is a primitive root* $(\mathrm{mod}\ p)$, *then it is also a primitive root* $(\mathrm{mod}\ p^2)$ *if and only if* $g^{p-1} \not\equiv 1 \pmod{p^2}$.

The above criterion suggests a method for obtaining exceptional primes p for which $g(p) \neq h(p)$. It is sufficient to check for each prime p if $g(p)^{p-1} \equiv 1 \pmod{p^2}$.

We have divided all computations into two steps. In the first step we took advantage of a large earlier precomputed table consisting of primes less than 2^{32} and its least primitive roots. There is only one prime p in the interval $[2, 2^{32}]$ for which $g(p) \neq h(p)$, just the prime $p = 40487$, found by Litver and Yudina. All computations of this step were performed on one Pentium IV PC computer. In

Received by the editor November 15, 2004 and, in revised form, July 27, 2007.
2000 *Mathematics Subject Classification.* Primary 11Y16; Secondary 11A07, 11M26.
Key words and phrases. Prime generators, primitive roots.

the second step, we used about 20 Pentium PC computers at the Warsaw School of Information Technology under auspices of the Polish Academy of Sciences and performed computations for primes p up to 10^{12}. During all process of computation we exploited the fact stated by R. Crandall, K. Dilcher and C. Pomerance [2] that below $4 \cdot 10^{12}$ there exist only two primes $p = 1093$, found by W. Meissner [6] and $p = 3511$, found by N. Beeger [1], for which the congruence $2^{p-1} \equiv 1 \pmod{p^2}$ holds. These are called Wieferich primes. We check that for these two primes we have $g(p) = h(p)$. The search for Wieferich primes has been extended and the recent result for these primes was established by J. Knauer and J. Richstein [4], who checked all primes up to $1.25 \cdot 10^{15}$ and did not find any new Wieferich primes. All these arguments imply that there is no need to consider the least primitive root $g = 2$ in our study. By [8] this eliminates about 37.4% of primes $p \in [2, 10^{12}]$ for which we do not verify the condition of the above critetion.

Our calculations show that there is only one Litver–Yudina type prime $p = 6692367337$ in the interval $[2^{32}, 10^{12}]$. For this prime p we have $g(p) = 5$ and $h(p) = 7$.

In [3] all generalized Wieferich primes were found, with bases a between 100 and 1000, and $p < 10^{11}$. The smaller values of a are listed in [7]. It is worth mentioning that the prime $p = 6692367337$ is among these reported in [3]. It follows from [3], that for all $10^{12} < p < 10^{13}$ if $g(p) = 3$ or $g(p) = 5$, then $g(p) = h(p)$.

On the base of computational observations we can formulate the following conjecture and question.

Conjecture. *For most primes p, we have $g(p) = h(p)$.*

Question. Do there exist infinitely many primes p for which $g(p) \neq h(p)$?

Concerning the Conjecture and Question it should be pointed out that we do not know that there are infinitely many primes p with $g(p) = h(p)$. I believe that the answer is positive in both cases.

Acknowledgments

There are three people that I would like to express my gratitude to: Professor Zbigniew Nahorski, the Dean of Informatics Faculty at the Warsaw School of Information Technology under the auspices of the Polish Academy of Sciences for allowing the computational experiment in January 2003 during idle time of the school computer network. Next is Mr. Mariusz Kwas, a student of the Warsaw University of Technology, who has carefully written all software for distributed computing. I also thank Joshua Knauer for information about his investigation of Wieferich primes and for the unpublished version of the paper [4]. Thanks are also due to the anonymous referees for their valuable suggestions and especially for the very important reference [3].

References

[1] N. Beeger, *On a new case of the congruence* $2^{p-1} \equiv 1 \pmod{p^2}$. Messenger of Mathematics, 51 (1922), pp. 149–150.

[2] R. Crandall, K. Dilcher, C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp., 1997, 66, pp. 433-449. MR1372002 (97c:11004)

[3] W. Keller, J. Richstein, *Solutions of the congruence* $a^{p-1} \equiv 1 \pmod{p^r}$, Math. Comp., 2005, 74, pp. 927–936. MR2114655 (2005i:11004)

[4] J. Knauer, J. Richstein, *The continuing search for Wieferich primes*, Math. Comp., 2005, 74, pp. 1559–1563. MR2137018 (2006a:11006)

[5] E. L. Litver, G. E. Yudina, *Primitive roots for the first million primes and their powers* (Russian), in: *Matematiceskij analiz i ego prilozenija*, III Rostov 1971, pp. 106–109. MR0340159 (49:4915)

[6] W. Meissner, *Über die Teilbarkeit von* $2^p - 2$ *durch das Quadrat der Primzahl* $p = 1093$, Sitzungsberichte Preuss. Akad. Wiss. (1913), pp. 663–667.

[7] P. L. Montgomery, *New solutions of* $a^{p-1} \equiv 1 \pmod{p^2}$, Math. Comp. 61 (1993), 361–363. MR1182246 (94d:11003)

[8] A. Paszkiewicz, A. Schinzel, *Numerical calculation of the density of prime numbers with a given least primitive root*, Math. Comp., 2002, 71, pp. 1781–1797. MR1933055 (2003g:11109)

Warsaw University of Technology, Institute of Telecommunications, ul. Nowowiejska 15/19, 00-665 Warsaw, Poland

E-mail address: anpa@tele.pw.edu.pl