Fixed points for discrete logarithms

Mariana Levin[1], Carl Pomerance[2], and and K. Soundararajan[3]

[1] Graduate Group in Science and Mathematics Education
University of California
Berkeley, CA 94720, USA
levin@berkeley.edu
[2] Department of Mathematics
Dartmouth College
Hanover, NH 03755, USA
carl.pomerance@dartmouth.edu
[3] Department of Mathematics
Stanford University
Stanford, CA 94305, USA
ksound@math.stanford.edu

Abstract. We establish a conjecture of Brizolis that for every prime $p > 3$ there is a primitive root g and an integer x in the interval $[1, p-1]$ with $\log_g x = x$. Here, $\log_g$ is the discrete logarithm function to the base g for the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$. Tools include a numerically explicit "smoothed" version of the Pólya–Vinogradov inequality for the sum of values of a Dirichlet character on an interval, a simple lower bound sieve, and an exhaustive search over small cases.

1 Introduction

If g is an element in a group G and $t \in \langle g \rangle$, there is some integer n with $g^n = t$. Finding a valid choice for n is known as the discrete logarithm problem. Note that if g has finite order m, then n is actually a residue class modulo m. We write

$$\log_g t = n \text{ (or } \log_g t \equiv n \pmod{m})$$

in analogy to usual logarithmic notation. Thus, the problem in the title of this paper does not seem to make good sense, since if $\log_g x = x$, then the first x is a member of the group $\langle g \rangle$ and the second x is either an integer or a residue class modulo m. However, sense is made of the equation through the traditional conflation of members of the ring $\mathbb{Z}/k\mathbb{Z}$ with least nonnegative members of residue classes.

The work for this paper was begun at Bell Laboratories in 2001 while the first author was a summer student working with the second author. A version of this work was presented as the 2003 Master's Thesis of the first author at U. C. Berkeley, see [3]. The second author was supported in part by NSF grant DMS-0703850. The third author was supported in part by NSF grant DMS-0500711.

In particular, suppose $G = (\mathbb{Z}/p\mathbb{Z})^\times$, where p is a prime number. This is known to be a cyclic group of order $p-1$. Suppose g is a cyclic generator of this group, known as a primitive root for p. A fixed point for the discrete logarithm modulo p to the base g is then an integer x in the interval $[1, p-1]$ such that $\log_g x = x$, that is, $g^x \equiv x \pmod{p}$. (Note that if x is not restricted to the interval $[1, p-1]$ it is easy to find fixed points. Namely, if x is a solution to the Chinese remainder problem $x \equiv 1 \pmod{p-1}$, $x \equiv g \pmod{p}$, then $g^x \equiv x \pmod{p}$.)

Brizolis (see Guy [6, Section F9]) made the conjecture that for every prime $p > 3$ there is a primitive root g and an integer x in $[1, p-1]$ with $\log_g x = x$, that is, $g^x \equiv x \pmod{p}$. In this paper we prove this conjecture in a somewhat stronger form. Brizolis had noticed that if there is a primitive root x for p with x in $[1, p-1]$ and $\gcd(x, p-1) = 1$, then with y the multiplicative inverse of x modulo $p-1$ and $g = x^y$, we would have that g is a primitive root for p as well, and

$$g^x \equiv x^{xy} \equiv x \pmod{p},$$

that is, there is a solution to the fixed point problem. We shall prove then the stronger result that for each prime $p > 3$ there is a primitive root x for p in $[1, p-1]$ that is coprime to $p-1$.

Several authors have shown that the Brizolis property holds for all sufficiently large primes p. In particular, Zhang [12] showed the strong conjecture holds for all sufficiently large primes p, but did not give an estimate of what "sufficiently large" is. Cobeli and Zaharescu [4] also showed that the strong conjecture holds for sufficiently large primes p, and gave the details that it holds for all $p > 10^{2070}$, but they indicated that their method would support a bound around 10^{50}.

Our method is similar to that of Zhang, who used the Pólya–Vinogradov inequality for character sums on an interval. Here we introduce a numerically explicit "smoothed" version of this inequality, see §2. In addition, we combine the traditional character-sum approach with a simple lower bound sieve. There is still some need for direct calculation for smaller values of p, which are easily handled by a short Mathematica program. In particular, we directly verified the strong conjecture for each prime $p < 1.25 \cdot 10^9$.

We mention the article by Holden and Moree [8], which considers some related problems. The total number of solutions to $g^x \equiv x \pmod{p}$ as p runs up to some high bound N, where either g is restricted to be a primitive root, and where it is not so restricted, is considered in Bourgain, Konyagin, and Shparlinski [2].

The smoothed version of the Pólya–Vinogradov inequality that we introduce in the next section is quite simple and the proof is routine, so it may be known to others. We have found it to be quite useful numerically; we hope it will find applications in "closing the gap" in other problems where character sums arise.

Some notation: $\omega(n)$ denotes the number of distinct prime divisors of n.

2 A "smoothed" Pólya–Vinogradov inequality

Let χ be a non-principal Dirichlet character to the modulus q. The Pólya–Vinogradov inequality (independently discovered by Pólya and Vinogradov in 1918) asserts that there is a universal constant c such that

$$\left| \sum_{M \le a \le M+N} \chi(a) \right| \le c\sqrt{q} \log q \tag{1}$$

for any choice of numbers M, N.

Let $N(p)$ denote the numer of primitive roots g for p with $g \in [1, p-1]$ and $\gcd(g, p-1) = 1$. Using (1) one can show (see Zhang [12] and Campbell [3]) that

$$N(p) = \frac{\varphi(p-1)^2}{p-1} + O(p^{1/2+\epsilon}),$$

for every fixed $\epsilon > 0$, and so $N(p) > 0$ for all sufficiently large p. The aim of this paper is to close the gap and find the complete set of primes p with $N(p) > 0$. Towards this end it would be useful to have a numerically explicit version of (1). In [3], the theorem of Bachman and Rachakonda [1] was used (plus a small unpublished improvement on a secondary term in their inequality due to the second author of the present paper). Recently, elaborating on the work in an early paper of Landau [10], plus an idea of Bateman as mentioned in Hildebrand [7], the second author in [11] proved a stronger numerically explicit version of (1). Using this simplifies the approach in [3]. However, we have found a way to simplify even further by using a "smoothed" version of (1). In this section we prove the following theorem.

Theorem 1. *Let χ be a primitive Dirichlet character to the modulus $q > 1$ and let M, N be real numbers with $0 < N \le q$. Then*

$$\left| \sum_{M \le a \le M+2N} \chi(a) \left(1 - \left| \frac{a-M}{N} - 1 \right| \right) \right| \le \sqrt{q} - \frac{N}{\sqrt{q}}.$$

Proof. We use Poisson summation, see [9, §4.3]. Let

$$H(t) = \max\{0, 1 - |t|\}.$$

We wish to estimate $|S|$, where

$$S := \sum_{a \in \mathbb{Z}} \chi(a) H\left(\frac{a-M}{N} - 1 \right).$$

Towards this end we use the identity

$$\chi(a) = \frac{1}{\tau(\bar{\chi})} \sum_{j=0}^{q-1} \bar{\chi}(j) e(aj/q),$$

where $\tau(\bar{\chi})$ is the Gauss sum for $\bar{\chi}$ and $e(x) := e^{2\pi i x}$. Thus,

$$S = \frac{1}{\tau(\bar{\chi})} \sum_{j=0}^{q-1} \bar{\chi}(j) \sum_{a \in \mathbb{Z}} e(aj/q) H\left(\frac{a-M}{N} - 1\right).$$

The Fourier transform of H is

$$\hat{H}(s) = \int_{-\infty}^{\infty} H(t) e(-st)\, dt = \frac{1-\cos 2\pi s}{2\pi^2 s^2} \text{ when } s \neq 0,\ \hat{H}(0) = 1,$$

which is nonnegative for s real. By a change of variables in the integral, we see that the Fourier transform of $e(jt/q)H((t-M)/N - 1)$ is

$$Ne\big(-(M+N)(s-j/q)\big)\hat{H}\big((s-j/q)N\big).$$

Hence, by Poisson summation, we have

$$S = \frac{N}{\tau(\bar{\chi})} \sum_{j=0}^{q-1} \bar{\chi}(j) \sum_{n \in \mathbb{Z}} e\big(-(M+N)(n-j/q)\big)\hat{H}\big((n-j/q)N\big).$$

Estimating trivially (that is, taking the absolute value of each term) and using $\hat{H}$ nonnegative and $\chi(0) = 0$, we have

$$|S| \leq \frac{N}{\sqrt{q}} \sum_{j=1}^{q-1} \sum_{n \in \mathbb{Z}} \hat{H}\big((n-j/q)N\big) = \frac{N}{\sqrt{q}} \sum_{k \in \mathbb{Z} \setminus q\mathbb{Z}} \hat{H}\left(\frac{kN}{q}\right).$$

Since $(N/q)\hat{H}(sN/q)$ is the Fourier transform of $H(qt/N)$, from the last calculation we have

$$\begin{aligned} |S| &\leq \sqrt{q} \sum_{k \in \mathbb{Z} \setminus q\mathbb{Z}} \frac{N}{q} \hat{H}\left(\frac{kN}{q}\right) \leq \sqrt{q}\left(-\frac{N}{q}\hat{H}(0) + \sum_{k \in \mathbb{Z}} \frac{N}{q}\hat{H}\left(\frac{kN}{q}\right)\right) \\ &= \sqrt{q}\left(-\frac{N}{q} + \sum_{l \in \mathbb{Z}} H\left(\frac{ql}{N}\right)\right) = -\frac{N}{\sqrt{q}} + \sqrt{q}H(0) = \sqrt{q} - \frac{N}{\sqrt{q}}, \end{aligned}$$

by another appeal to Poisson summation and the definition of H. This completes the proof of the theorem.

In our application we will need a version of Theorem 1 with the variable a satisfying a coprimality condition. We deduce such a result below.

Corollary 2 *Let k be a square-free integer and let χ be a primitive character to the modulus $q > 1$. For $0 < N \leq q$, we have*

$$\left| \sum_{\substack{0 \leq a \leq 2N \\ (a,k)=1}} \chi(a)\left(1 - \left|\frac{a}{N} - 1\right|\right) \right| \leq \begin{cases} 2^{\omega(k)}\sqrt{q} & \text{always} \\ 2^{\omega(k)-1}\sqrt{q} & \text{if } k \text{ is even.} \end{cases}$$

Proof. Since $\sum_{d|(k,a)} \mu(d)$ gives 1 if $(a,k) = 1$ and 0 otherwise, the sum in question equals

$$\sum_{d|k} \mu(d)\chi(d) \sum_{a \le 2N/d} \chi(a)\Big(1 - \Big|\frac{ad}{N} - 1\Big|\Big)$$

and using Theorem 1 this is bounded in size by $2^{\omega(k)}\sqrt{q}$ as desired. If (k,q) is even, then $\chi(d) = 0$ for even divisors d of k, so that we achieve the bound $2^{\omega(k)-1}\sqrt{q}$, again as desired. Suppose now that k is even and q is odd. For each odd divisor d of k, we group together the contribution from d and $2d$, and so we may write the sum in question as

$$\sum_{d|k/2} \mu(d)\chi(d) \sum_{\substack{a \le 2N/d \\ a \text{ odd}}} \chi(a)\Big(1 - \Big|\frac{ad}{N} - 1\Big|\Big).$$

We replace a in the inner sum by $q + a$, and since q is now odd, the condition that a is odd may be replaced with the condition that $q + a = 2b$ is even. Thus, the above sum becomes

$$\sum_{d|k/2} \mu(d)\chi(d)\chi(2) \sum_{q/2 \le b \le q/2 + N/d} \chi(b)\left(1 - \left|\frac{2d(b - q/2)}{N} - 1\right|\right),$$

and appealing again to Theorem 1 we obtain the Corollary in this case.

Though we will not need it for our proof, we record the following corollary of Theorem 1.

Corollary 3 *Let χ be a primitive Dirichlet character to the modulus $q > 1$ and let M, N be real numbers with $N > 0$. Then, with θ the fractional part of N/q,*

$$\left|\sum_{M \le a \le M+2N} \chi(a)\left(1 - \left|\frac{a - M}{N} - 1\right|\right)\right| \le \frac{q^{3/2}}{N}\theta(1-\theta).$$

3 A criterion for the Brizolis property

Let us write the largest square-free divisor of $p - 1$ as uv where u and v will be chosen later. We shall assume that u is even, and have in mind the situation that u is composed of the small prime factors of $p - 1$, and that v is composed of the large prime factors; we also allow for the possibility that $v = 1$. For the rest of the paper, the letter ℓ will denote a prime number.

Let $\mathcal{S}$ denote the set of primitive roots in $[1, p-1]$ that are coprime to $p-1$. Thus, an integer $g \in [1, p-1]$ is in $\mathcal{S}$ if and only if for each prime $\ell \mid p - 1$ we have both $\ell \nmid g$ and g is not an ℓ-th power (mod p). Let $\mathcal{S}_1$ denote the set of integers in $[1, p-1]$ that are coprime to u and which are not equal to an ℓ-th power (mod p) for any prime ℓ dividing u. Let $\mathcal{S}_2$ denote the set of integers in $\mathcal{S}_1$ which are divisible by some prime ℓ which divides v. Let $\mathcal{S}_3$ denote the set

of integers in $\mathcal{S}_1$ which equal an ℓ-th power (mod p) for some prime ℓ dividing v. Now $\mathcal{S} \subset \mathcal{S}_1$, and the elements in $\mathcal{S}_1$ that are not in $\mathcal{S}$ are precisely those that, for some prime $\ell \mid v$, are either divisible by ℓ or are an ℓ-th power (mod p). Thus, $\mathcal{S} = \mathcal{S}_1 \backslash (\mathcal{S}_2 \cup \mathcal{S}_3)$. We seek a positive lower bound for

$$N := \sum_{g \in \mathcal{S}} \Big(1 - \Big|\frac{2g}{p-1} - 1\Big|\Big),$$

since if $N > 0$, then $\mathcal{S} \neq \emptyset$. By our observation above we have

$$N \geq N_1 - N_2 - N_3,$$

where, for $j = 1, 2, 3$,

$$N_j = \sum_{g \in \mathcal{S}_j} \Big(1 - \Big|\frac{2g}{p-1} - 1\Big|\Big).$$

If d is a square-free divisor of $p-1$ and g is an integer in $[1, p-1]$, let $C_d(g)$ be 1 if g is a d-th power (mod p) and 0 otherwise. Thus,

$$\begin{aligned} C_d(g) &= \prod_{\ell \mid d} C_\ell(g) = \prod_{\ell \mid d} \frac{1}{\ell} \sum_{\chi^\ell = \chi_0} \chi(g) \\ &= \frac{1}{d} \prod_{\ell \mid d} \left(1 + \sum_{\chi \text{ of order } \ell} \chi(g)\right) = \frac{1}{d} \sum_{m \mid d} \sum_{\chi \text{ of order } m} \chi(g). \end{aligned}$$

Note that

$$\sum_{d \mid u} \mu(d) C_d(g)$$

is 1 if, for each $\ell \mid u$, g is *not* an ℓ-th power (mod p), and is 0 otherwise. By the above calculation, this expression is

$$\sum_{d \mid u} \frac{\mu(d)}{d} \sum_{m \mid d} \sum_{\chi \text{ of order } m} \chi(g) = \sum_{m \mid u} \sum_{\chi \text{ of order } m} \chi(g) \sum_{n \mid u/m} \frac{\mu(nm)}{nm}.$$

The inner sum here is $(\varphi(u)/u)\mu(m)/\varphi(m)$, so that

$$N_1 = \frac{\varphi(u)}{u} \sum_{\substack{1 \leq g \leq p-1 \\ (g,u)=1}} \Big(1 - \Big|\frac{2g}{p-1} - 1\Big|\Big) \sum_{m \mid u} \frac{\mu(m)}{\varphi(m)} \sum_{\chi \text{ of order } m} \chi(g). \tag{2}$$

Let $m \mid u$ with $m > 1$. Using Corollary 2, the terms above contribute an amount bounded in magnitude by

$$\frac{\varphi(u)}{u} 2^{\omega(u)-1} \sqrt{p},$$

so the total contribution over all $m \mid u$ with $m > 1$ has magnitude at most

$$\frac{\varphi(u)}{u}\left(2^{\omega(u)}-1\right)2^{\omega(u)-1}\sqrt{p}.$$

The sum over g in (2) with $m = 1$ (and so $\chi = \chi_0$) is

$$\frac{\varphi(u)}{u}\sum_{\substack{1\le g\le p-1\\(g,u)=1}}\left(1-\left|\frac{2g}{p-1}-1\right|\right)=\frac{\varphi(u)}{u}\sum_{d\mid u}\mu(d)\sum_{h\le (p-1)/d}\left(1-\left|\frac{2dh}{p-1}-1\right|\right).$$

The inner sum over h can be evaluated explicitly: it equals $(p-1)/(2d)$ if $(p-1)/d$ is even, and it equals $(p-1)/(2d) - d/(2(p-1))$ if $(p-1)/d$ is odd. It follows that the contribution when $m = 1$ is

$$\left(\frac{\varphi(u)}{u}\right)^2\frac{p-1}{2}-\frac{\varphi(u)}{u}\frac{1}{2(p-1)}\sum_{\substack{d\mid u\\(p-1)/d \text{ odd}}}d\mu(d)$$
$$\ge\left(\frac{\varphi(u)}{u}\right)^2\frac{p-1}{2}-\frac{\varphi(u)^2}{u(p-1)}\ge\left(\frac{\varphi(u)}{u}\right)^2\frac{p}{2}-\frac{\varphi(u)}{u}.$$

We conclude that

$$N_1\ge\left(\frac{\varphi(u)}{u}\right)^2\frac{p}{2}-\frac{\varphi(u)}{u}-\frac{\varphi(u)}{u}\left(2^{\omega(u)}-1\right)2^{\omega(u)-1}\sqrt{p}$$
$$>\left(\frac{\varphi(u)}{u}\right)^2\frac{p}{2}-\frac{\varphi(u)}{2u}4^{\omega(u)}\sqrt{p}.$$

Next we turn to N_2. Since an element in $\mathcal{S}_2$ must be divisible by some prime $\ell|v$ we have that

$$N_2\le\sum_{\ell\mid v}\sum_{\substack{h\le(p-1)/\ell\\(h,u)=1}}\left(1-\left|\frac{2h\ell}{p-1}-1\right|\right)\frac{\varphi(u)}{u}\sum_{m\mid u}\frac{\mu(m)}{\varphi(m)}\sum_{\chi \text{ of order } m}\chi(h\ell).$$

If $v = 1$, then $N_2 = 0$, so assume $v > 1$. The terms with $m > 1$ contribute, using Corollary 2, an amount bounded in size by

$$\frac{\varphi(u)}{u}\omega(v)\left(2^{\omega(u)}-1\right)2^{\omega(u)-1}\sqrt{p}.$$

The main term $m = 1$ above contributes (arguing as in our evaluation of the main term for N_1 above)

$$\frac{\varphi(u)}{u}\sum_{\ell\mid v}\sum_{\substack{h\le(p-1)/\ell\\(h,u)=1}}\left(1-\left|\frac{2h\ell}{p-1}-1\right|\right)\le\left(\frac{\varphi(u)}{u}\right)^2\sum_{\ell\mid v}\left(\frac{p-1}{2\ell}+\frac{\ell}{v}\right).$$

Since $\sum_{\ell|v}\ell \le v$, and using $v>1$, we conclude that

$$N_2 \le \left(\frac{\varphi(u)}{u}\right)^2 \frac{p-1}{2}\sum_{\ell|v}\frac{1}{\ell} + \left(\frac{\varphi(u)}{u}\right)^2 + \frac{\varphi(u)}{u}\omega(v)\left(2^{\omega(u)}-1\right)2^{\omega(u)-1}\sqrt{p}$$
$$\le \left(\frac{\varphi(u)}{u}\right)^2 \frac{p}{2}\sum_{\ell|v}\frac{1}{\ell} + \frac{\varphi(u)}{2u}4^{\omega(u)}\omega(v)\sqrt{p}.$$

Lastly we consider N_3. An element g of $\mathcal{S}_3$ must be an ℓ-th power for some prime $\ell|v$, and the indicator function for this condition is $\frac{1}{\ell}\sum_{\psi^\ell=\chi_0}\psi(g)$, as seen above. Therefore we have that N_3 is at most

$$\sum_{\ell|v}\sum_{\substack{g\le p-1\\(g,u)=1}}\Big(1-\Big|\frac{2g}{p-1}-1\Big|\Big)\Big(\frac{\varphi(u)}{u}\sum_{m|u}\frac{\mu(m)}{\varphi(m)}\sum_{\chi \text{ of order } m}\chi(g)\Big)\Big(\frac{1}{\ell}\sum_{\psi^\ell=\chi_0}\psi(g)\Big).$$

Appealing to Corollary 2 for the terms above with $\chi\psi\neq\chi_0$ we find that the contribution of such terms is bounded in magnitude by

$$\frac{\varphi(u)}{u}2^{2\omega(u)-1}\omega(v)\sqrt{p}.$$

The main term $\chi=\psi=\chi_0$ gives

$$\frac{\varphi(u)}{u}\sum_{\ell|v}\frac{1}{\ell}\sum_{\substack{g\le p-1\\(g,u)=1}}\Big(1-\Big|\frac{2g}{p-1}-1\Big|\Big) \le \frac{\varphi(u)}{u}\Big(\frac{\varphi(u)}{u}\frac{p-1}{2}+\frac{\varphi(u)}{p-1}\Big)\sum_{\ell|v}\frac{1}{\ell}$$
$$= \left(\frac{\varphi(u)}{u}\right)^2\left(\frac{p-1}{2}+\frac{1}{v}\right)\sum_{\ell|v}\frac{1}{\ell} \le \left(\frac{\varphi(u)}{u}\right)^2\frac{p}{2}\sum_{\ell|v}\frac{1}{\ell}.$$

Thus,

$$N_3 \le \left(\frac{\varphi(u)}{u}\right)^2\frac{p}{2}\sum_{\ell|v}\frac{1}{\ell}+\frac{\varphi(u)}{2u}4^{\omega(u)}\omega(v)\sqrt{p}.$$

Combining these bounds for N_1, N_2 and N_3 we obtain that

$$N \ge \left(\frac{\varphi(u)}{u}\right)^2\frac{p}{2}\Big(1-2\sum_{\ell|v}\frac{1}{\ell}\Big)-\frac{\varphi(u)}{2u}4^{\omega(u)}(1+2\omega(v))\sqrt{p}.$$

We may conclude as follows: The Brizolis property holds for the prime $p\ge 5$, if we may write the largest square-free divisor of $p-1$ as uv with u even, $\sum_{\ell|v}1/\ell<1/2$, and with

$$\sqrt{p} > \frac{4^{\omega(u)}u}{\varphi(u)}\cdot\frac{1+2\omega(v)}{1-2\sum_{\ell|v}1/\ell}. \tag{3}$$

4 Completing the proof

Our criterion (3) can be used in a straightforward way with $v = 1$ to get an upper bound for possible counterexamples to the Brizolis conjecture. Indeed, after a small calculation (using $4^{\omega(n)} < 1404 n^{1/3}$ and $n/\varphi(n) < 2 \log\log n$ for n larger than the product of the first eleven primes), it is seen that the Brizolis property holds for all $p > 10^{25}$. It is not pleasant to contemplate checking each prime to this point, so instead we use (3) with $v > 1$.

Suppose $\omega(p-1) = k \geq 10$, and take v to be the product of the six largest primes dividing $p-1$, and u to be the product of the other smaller primes. Since $\omega(p-1) \geq 10$, the primes dividing v are all at least 11, and we have that

$$1 - 2\sum_{\ell \mid v} \frac{1}{\ell} \geq 1 - 2\Big(\frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \frac{1}{19} + \frac{1}{23} + \frac{1}{29}\Big) > 0.28.$$

If p_j denotes the j-th prime, then $4^{\omega(u)} u/\varphi(u) \leq \prod_{j=1}^{k-6} (4p_j/(p_j - 1))$, and $p > p - 1 \geq \prod_{j=1}^{k} p_j$. So from our criterion (3), if we have

$$\prod_{j=1}^{k} \sqrt{p_j} \geq \frac{13}{0.28} \prod_{j=1}^{k-6} \frac{4p_j}{p_j - 1},$$

then the Brizolis property holds for all p with $\omega(p-1) = k$. We verified that the inequality above holds for $k = 10$. If k is increased by 1 then the LHS of our inequality is increased by a factor of at least $\sqrt{31} > 5$, but the RHS is increased only by a factor of at most $4 \times (11/10) = 4.4$. Thus, the inequality holds for all $k \geq 10$.

Suppose now that $k = \omega(p-1) \leq 9$. If $k \geq 4$, we take u to be the product of the four smallest primes dividing $p-1$, and otherwise, we take u to be the product of all the primes dividing $p-1$. Then v has at most 5 prime factors, and $1 - 2\sum_{\ell \mid v} 1/\ell \geq 1 - 2(1/11 + 1/13 + 1/17 + 1/19 + 1/23) \geq 0.35$. Further $\prod_{p \mid u} 4p/(p-1) \leq \prod_{j=1}^{4} 4p_j/(p_j - 1) = 1120$. Our criterion (3) shows that if

$$p \geq \Big(1120 \times \frac{11}{0.35}\Big)^2 = 1{,}239{,}040{,}000,$$

then p satisfies the Brizolis property.

Using the functions Prime[ ] and PrimitiveRoot[ ] in Mathematica, we were able to directly exhibit a primitive root g for each prime $3 < p < 1.25 \cdot 10^9$ with g in $[1, p-1]$ and coprime to $p-1$. Our program runs as follows. The function Prime[ ] allows us to sequentially step through the primes up to our bound. For each prime p returned by Prime[ ], we invoke PrimitiveRoot[p] to find the least positive primitive root r for p. We then sequentially check $r^{2k-1} \bmod p$ for $k = 1, 2, \ldots$ until we find a value coprime to $p-1$ with $2k-1$ also coprime to $p-1$. The exponent being coprime to $p-1$ guarantees that the power is a primitive root, and the residue being coprime to $p-1$ then guarantees that we

have found a member of $\mathcal{S}$. If no such primitive root exists, this algorithm would not terminate, but it did, thus verifying the Brizolis property for the given range.

There are various small speed-ups that one can use to augment the program. For example, if $r = 2$ is a primitive root and $p \equiv 1 \pmod 4$, then note that $p-2$ is a primitive root coprime to $p-1$, and so work with this prime p is complete. The augmented program ran in about 90 minutes on a Dell workstation.

This completes our proof of the Brizolis conjecture.

Acknowledgment. We thank Richard Crandall for some technical assistance with the Mathematica program and the referees for some helpful comments.

References

1. G. Bachman and L. Rachakonda, On a problem of Dobrowolski and Williams and the Pólya–Vinogradov inequality, *Ramanujan J.* **5** (2001), 65–71.
2. J. Bourgain, S. V. Konyagin, and I. E. Shparlinski, Product sets of rationals, multiplicative translates of subgroups in residue rings, and fixed points of the discrete logarithm, *Int. Math. Res. Notices* 2008, art. ID rnn090, 29 pp. (Corrigendum: ibid. 2009, no. 16, 3146–3147.)
3. M. E. Campbell, On fixed points for discrete logarithms, Master's Thesis, U. C. Berkeley Department of Mathematics, 2003.
4. C. Cobeli and A. Zaharescu, An exponential congruence with solutions in primitive roots, Rev. Romaine Math. Pures Appl. **44** (1999), 15–22.
5. R. Crandall and C. Pomerance, Prime numbers: a computational perspective, Second ed., Springer, New York, 2005.
6. R. K. Guy, Unsolved problems in number theory, Springer, New York–Berlin, 1984.
7. A. Hildebrand, On the constant in the Pólya–Vinogradov inequality, *Canad. Math. Bull.* **31** (1988), 347–352.
8. J. Holden and P. Moree, Some heuristics and results for small cycles of the discrete logarithm, Math. Comp. **75** (2006), 419–449.
9. H. Iwaniec and E. Kowalski, Analytic number theory, American Math. Soc., Providence, 2004.
10. E. Landau, Abschätzungen von Charaktersummen, Einheiten und Klassenzahlen, *Nachrichten Königl. Ges. Wiss. Göttingen* (1918), 79–97.
11. C. Pomerance, Remarks on the Pólya–Vinogradov inequality, submitted for publication, 2010.
12. W.-P. Zhang, On a problem of Brizolis. (Chinese. English, Chinese summary.) Pure Appl. Math. **11** (1995) suppl., 1–3.