On Consecutive kth Power Residues, II

ADOLF HILDEBRAND

1. Introduction

Brauer [1] proved that for any positive integers k and l and every sufficiently large prime p there exists a positive integer r such that the numbers $r, r+1, \ldots, r+l-1$ are all kth power residues modulo p. Let $r(k,l,p)$ be the least such integer and define

$$\Lambda(k,l) = \limsup_{p\to\infty} r(k,l,p).$$

The function $\Lambda(k,l)$ has been studied by a number of authors. For example, it is known ([4], [8]) that $\Lambda(k,l)=\infty$ for $l\geq 4$ and all $k\geq 2$ and for $l=3$ and all even values of k. On the other hand, using machine computation it was shown that $\Lambda(k,2)$ is finite for every $k\leq 7$, and it has been conjectured [2] that the same is true for $k>7$ (see [7] for further references). In [7] we proved this conjecture for the case when k is a prime number. Here we shall prove the conjecture in full.

THEOREM 1. *$\Lambda(k,2)<\infty$ for all positive integers k.*

Stated differently, the assertion of the theorem is that, given a positive integer k, there exists a constant $c_0(k)$ such that for every sufficiently large prime p there exists a pair $(r, r+1)$ of consecutive kth power residues modulo p satisfying $1\leq r\leq c_0(k)$.

As in [7], we shall deduce Theorem 1 from a slightly more general result concerning completely multiplicative functions whose values are kth roots of unity. Let F_k denote the set of all such functions; that is,

$$F_k = \{f: \mathbf{N}\to\mathbf{C}: f^k\equiv 1, f(nm)=f(n)f(m)\ (n,m\in\mathbf{N})\}.$$

THEOREM 2. *Let k be a positive integer. There exists a constant $c_0(k)$ such that for any function $f\in F_k$ there exists a positive integer $n\leq c_0(k)$ with $f(n)=f(n+1)=1$.*

The deduction of Theorem 1 from Theorem 2 is easy and will be given at the end of this section. The proof of Theorem 2 is based on the same ideas as

Received March 28, 1990.
The author was supported by an NSF grant.
Michigan Math. J. 38 (1991).

that of the corresponding result in [7], but is considerably more involved. As in [7], a key role is played by so-called "special" sets of integers, that is, sets $S=\{n_1<\cdots<n_r\}$ of positive integers satisfying $n_j-n_i \mid (n_i, n_j)$ for all $i<j$. Such sets were first considered by Heath-Brown [5]. Their significance lies in the fact that for any two distinct elements n_i and n_j of such a set the numbers $n_i/(n_i, n_j)$ and $n_j/(n_i, n_j)$ are consecutive integers. In order to prove the assertion of Theorem 2, it therefore suffices to show that, given a function $f \in F_k$, there exists a special set $S=\{n_1<\cdots<n_r\}$ with $r \geq 2$, $n_r \leq c_0(k)$, and

$$f(n_i/(n_i, n_j))=1 \quad (i \neq j). \tag{1.1}$$

The main difficulty we will have to overcome is to ensure condition (1.1). This requires the use of a variety of combinatorial and number-theoretic tools, such as the pigeonhole principle, Ramsey's theorem, elementary sieve estimates, and estimates for multiplicative arithmetic functions.

DEDUCTION OF THEOREM 1. We first note that it suffices to consider kth power residues modulo primes $p \equiv 1 \bmod k$, for the set of kth power residues modulo a prime p is equal to the set of dth power residues modulo p with $d=(k, p-1)$. Let now p be a prime with $p \equiv 1 \bmod k$, g a primitive root modulo p, and define a function f by $f(n)=\exp(2\pi i \nu/k)$ if $(n, p)=1$ and $g^\nu \equiv n \bmod p$, and $f(p^m n)=f(n)$ if $(n, p)=1$ and $m \geq 1$. It is easy to see that f is well defined, belongs to F_k, and satisfies, for $(n, p)=1$, $f(n)=1$ if and only if n is a kth power residue modulo p. Theorem 2 therefore implies that for all primes $p>c_0(k)+1$ there exists a pair of kth power residues $(n, n+1)$ with $n \leq c_0(k)$. Hence $\Lambda(k, 2) \leq c_0(k)$, which proves Theorem 1.

2. Preliminaries

We begin with an elementary sieve result.

LEMMA 1. *Let $f(n)=\prod_{i=1}^{k}(a_i n+b_i)$ be a product of linear polynomials with integer coefficients satisfying*

$$a_i \neq 0, \quad (a_i, b_i)=1 \quad (i=1, \ldots, k), \tag{2.1}$$

and let $\mathcal{P}$ be a set of primes satisfying

$$\sum_{p \in \mathcal{P}} \frac{1}{p} \leq c \tag{2.2}$$

for some constant $c>0$, and

$$p \in \mathcal{P} \Rightarrow p>k. \tag{2.3}$$

Then there exists a positive integer $n \leq c_1$ such that $p \nmid f(n)$ for all $p \in \mathcal{P}$. Here c_1 is a constant depending on the constant c in (2.2) and the coefficients of f, but not on the set $\mathcal{P}$.

Proof. Define the sifting functions

$$S(x)=\#\{n\le x:(f(n),\mathcal{P})=1\},$$

$$S(x,z)=\#\{n\le x:(f(n),\mathcal{P}(z))=1\},$$

where $\mathcal{P}(z)=\mathcal{P}\cap[2,z)$ and $(n,\mathcal{P})=1$ means that $p\nmid n$ for all $p\in\mathcal{P}$. We must show that $S(x)>0$ holds for some value $x\ge 1$ bounded in terms of f and c.

For any $x\ge z\ge 2$ we have

$$S(x)\ge S(x,z)-\sum_{\substack{z\le p\\ p\in\mathcal{P}}} N_p(x), \tag{2.4}$$

with

$$N_p(x)=\#\{n\le x:p\mid f(n)\}.$$

Now note that if $p\mid f(n)$ then $p\mid a_in+b_i$, and hence $p\le|a_i|n+|b_i|$, for some i. Thus, setting $A=\max_i(|a_i|+|b_i|)$, we have $N_p(x)=0$ for $p>Ax$, and

$$N_p(x)\le\sum_{i=1}^{k}\#\{n\le x:p\mid a_in+b_i\}\le k\left(\frac{x}{p}+1\right)\le k(A+1)\frac{x}{p}$$

for $p\le Ax$, in view of the hypothesis (2.1). The last term in (2.4) is therefore bounded by

$$\sum_{\substack{z\le p\\ p\in\mathcal{P}}} N_p(x)\le k(A+1)x\sum_{\substack{z\le p\le Ax\\ p\in\mathcal{P}}}\frac{1}{p}. \tag{2.5}$$

Furthermore, a straightforward application of the sieve of Eratosthenes gives

$$S(x,z)=\prod_{\substack{p<z\\ p\in\mathcal{P}}}\left(1-\frac{\rho(p)}{p}\right)x+O((1+k)^z), \tag{2.6}$$

where $\rho(p)$ denotes the number of pairwise incongruent solutions to $f(n)\equiv 0 \bmod p$. By (2.1) and (2.3) we have $\rho(p)\le k<p$ for all $p\in\mathcal{P}$, whence, by (2.2),

$$\prod_{\substack{p\le z\\ p\in\mathcal{P}}}\left(1-\frac{\rho(p)}{p}\right)\ge\exp\left\{-\sum_{\substack{p\le z\\ p\in\mathcal{P}}}\frac{k}{p}+O_k(1)\right\}\ge\delta_1$$

for some positive constant $\delta_1=\delta_1(k,c)$. Thus, if we suppose that z is sufficiently large in terms of c and k and take $x=(1+k)^{2z}$, then (2.6) implies that

$$S(x,z)\ge\frac{\delta_1}{2}x. \tag{2.7}$$

Inserting (2.7) and (2.5) into (2.4), we obtain the desired bound $S(x)>0$, provided that

$$\sum_{\substack{z\le p\le Ax\\ p\in\mathcal{P}}}\frac{1}{p}\le\frac{\delta_1}{3k(A+1)}$$

holds with $x=(1+k)^{2z}$. In view of (2.2), we can ensure this last condition by choosing z suitably, but bounded in terms of c and k. This completes the proof of Lemma 1. □

We next derive an auxiliary result concerning the behavior of certain classes of multiplicative functions on arithmetic progressions. Given a Dirichlet character χ modulo q and a (possibly empty) set of primes of $\mathcal{P}$, we set

$$F_k(x, \chi, \mathcal{P}) = \{f: \mathbf{N} \to \mathbf{C}: f(p)^k = \chi(p)\ (p \le x, p \nmid q, p \notin \mathcal{P})\}.$$

LEMMA 2. *Let k, q, and q_1 be positive integers with $q \mid q_1$, and let c be a positive constant. There exist positive constants $c_2 = c_2(k, q_1, c)$ and $\delta_2 = \delta_2(k, c)$ with the following property. Let $x \ge c_2$, χ be a character modulo q, and $\mathcal{P}$ a set of primes satisfying* (2.2). *Given any function $f \in F_k(x, \chi, \mathcal{P})$, we then have either*

$$\sum_{\substack{n \le x,\ (n, \mathcal{P}) = 1 \\ n \equiv 1 \bmod q_1 \\ f(n) = \omega}} \frac{1}{n} \ge \frac{\delta_2}{q_1} \log x \tag{2.8}$$

for every kth root of unity ω, or $f \in F_{k_1}(x, \chi_1, \mathcal{P}_1)$ for some k_1 $(1 \le k_1 < k)$, a character χ_1 modulo q_1, and a set of primes $\mathcal{P}_1$ satisfying

$$\sum_{p \in \mathcal{P}_1} \frac{1}{p} \le c_2. \tag{2.9}$$

Proof. The proof follows largely that of Lemma 3 in [7]. We fix a function $f \in F_k(x, \chi, \mathcal{P})$ and suppose (as we may) that x is sufficiently large in terms of k, q_1, and c, and that $f(p) = 0$ for $p > x$.

Let ω be a kth root of unity, and consider the Dirichlet series

$$F(\sigma) = \sum_{n \ge 1}{}' \frac{1}{n^\sigma},$$

where $\sum'$ denotes summation over positive integers n satisfying the conditions

$$n \equiv 1 \bmod q_1, \quad f(n) = \omega, \quad p \mid n \Rightarrow p \le x, \ p \notin \mathcal{P}.$$

We first reduce the bound (2.8) to a bound for $F(\sigma)$.

For any $\sigma > 1$ we have

$$\begin{aligned} \sum_{n \le x}{}' \frac{1}{n} &\ge F(\sigma) - \sum_{\substack{n > x \\ n \equiv 1 \bmod q_1}} \frac{1}{n^\sigma} \\ &\ge F(\sigma) - \frac{1}{q_1^\sigma} \sum_{n \ge x/q_1 - 1} \frac{1}{n^\sigma} \\ &\ge F(\sigma) - \frac{1}{q_1^\sigma} \int_{x/q_1 - 2}^{\infty} \frac{du}{u^\sigma} \ge F(\sigma) - \frac{x^{(1-\sigma)/2}}{q_1^\sigma (\sigma - 1)}, \end{aligned}$$

provided that $x \ge 4q_1^2$, as we may assume. Taking

$$\sigma = 1 + \frac{1}{\delta \log x} \tag{2.10}$$

with a suitable constant $\delta = \delta(k, c)$, $0 < \delta \le 1$, to be specified later, we obtain

$$\sum_{n \le x}{}' \frac{1}{n} \ge F(\sigma) - \frac{\delta_2}{q_1} \log x$$

with

$$\delta_2 = \delta e^{-1/(2\delta)}. \tag{2.11}$$

Thus, (2.8) holds if

$$F(\sigma) \ge \frac{2\delta_2}{q_1} \log x. \tag{2.12}$$

We shall show that this last estimate indeed holds if the second alternative of the lemma fails.

By the assumptions $f \in F_k(x, \chi, \mathcal{P})$, $q \mid q_1$, and $f(p) = 0$ for $p > x$, we have that $f(n)$, and hence $f(n)\bar{\omega}$, is a kth root of unity for every n satisfying $n \equiv 1 \bmod q_1$ and $p \nmid n$ for $p > x$ or $p \in \mathcal{P}$. We therefore have

$$\sum_{l=0}^{k-1} (f(n)\bar{\omega})^l = \begin{cases} k & \text{if } f(n) = \omega, \\ 0 & \text{otherwise,} \end{cases}$$

for each such n. Using this relation and the orthogonality relation for Dirichlet characters, we obtain

$$\begin{aligned} F(\sigma) &= \frac{1}{k} \sum_{l=0}^{k-1} \bar{\omega}^l \sum_{\substack{n \ge 1 \\ p \mid n \Rightarrow p \le x,\ p \notin \mathcal{P} \\ n \equiv 1 \bmod q_1}} \frac{f(n)^l}{n^\sigma} \\ &= \frac{1}{k\phi(q_1)} \sum_{l=0}^{k-1} \bar{\omega}^l \sum_{\psi \bmod q_1} F_{l,\psi}(\sigma) \end{aligned} \tag{2.13}$$

with

$$F_{l,\psi}(\sigma) = \sum_{\substack{n \ge 1 \\ p \mid n \Rightarrow p \le x,\ p \notin \mathcal{P}}} \frac{f(n)^l \psi(n)}{n^\sigma},$$

where ϕ denotes the Euler phi function and ψ runs over all characters modulo q_1.

The contribution to (2.13) from F_{0,ψ_0}, where ψ_0 is the principal character modulo q_1, is

$$\begin{aligned} \frac{1}{k\phi(q_1)} F_{0,\psi_0}(\sigma) &= \frac{1}{k\phi(q_1)} \prod_{\substack{p \le x \\ p \notin \mathcal{P} \\ p \nmid q_1}} \left(1 - \frac{1}{p^\sigma}\right)^{-1} \\ &\ge \frac{1}{k\phi(q_1)} \zeta(\sigma) \prod_{p > x} \left(1 - \frac{1}{p^\sigma}\right) \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p^\sigma}\right) \prod_{p \mid q_1} \left(1 - \frac{1}{p^\sigma}\right) \\ &\gg \frac{1}{kq_1} \zeta(\sigma) \exp\left\{ - \sum_{p > x} \frac{1}{p^\sigma} - \sum_{p \in \mathcal{P}} \frac{1}{p} \right\} \\ &\gg \frac{e^{-c}}{kq_1(\sigma - 1)} = \frac{\delta e^{-c}}{kq_1} \log x = \frac{\delta_2 e^{1/(2\delta) - c}}{kq_1} \log x \end{aligned}$$

by (2.2), (2.10), (2.11), the bound $\zeta(\sigma-1) \gg 1/(\sigma-1)$, and the estimate $\sum_{p>x} p^{-\sigma} \ll 1$ for $\sigma \geq 1+1/\log x$, which follows by partial summation from Chebycheff's prime number estimate. The implied constants here are absolute. Thus, by choosing $\delta = \delta(k, c)$ small enough, we obtain

$$\frac{1}{k\phi(q_1)} F_{0,\psi_0}(\sigma) \geq \frac{3\delta_2}{q_1} \log x,$$

and (2.12) will follow, provided

$$|F_{l,\psi}(\sigma)| \leq \frac{\delta_2}{q_1} \log x \tag{2.14}$$

holds whenever $l \neq 0$ or $\psi \neq \psi_0$.

We now fix a pair $(l, \psi) \neq (0, \psi_0)$ and show that either (2.14) holds for this pair or the second alternative of the lemma is satisfied with a sufficiently large constant $c_2 = c_2(k, q_1, c)$. Since f is a completely multiplicative function, we have the Euler product representation

$$F_{l,\psi}(\sigma) = \prod_{\substack{p \leq x \\ p \notin \mathcal{P} \\ p \nmid q_1}} \left(1 - \frac{f(p)^l \psi(p)}{p^\sigma}\right)^{-1},$$

which yields the bound

$$|F_{l,\chi}(\sigma)| \ll \exp\left\{ \sum_{\substack{p \leq x \\ p \notin \mathcal{P},\, p \nmid q_1}} \frac{\Re f(p)^l \psi(p)}{p^\sigma} \right\}.$$

Now note that, by the definition of the class $F_k(x, \chi, \mathcal{P})$, $f(p)$ and $\psi(p)$ (and therefore also $f(p)^l \psi(p)$) are $(k\phi(q_1))$th roots of unity for each prime $p \leq x$ with $p \notin \mathcal{P}$ and $p \nmid q_1$. It follows that for each such prime we have either $f(p)^l = \bar{\psi}(p)$ or $\Re f(p)^l \psi(p) \leq 1 - 1/(k\phi(q_1))^2$. Hence

$$\sum_{\substack{p \leq x \\ p \notin \mathcal{P},\, p \nmid q_1}} \frac{\Re f(p)^l \psi(p)}{p^\sigma} \leq \sum_{p \leq x} \frac{1}{p^\sigma} - \frac{1}{(k\phi(q_1))^2} \sum_{p \in \mathcal{P}_{l,\bar{\psi}}} \frac{1}{p^\sigma},$$

where

$$\mathcal{P}_{l,\bar{\psi}} = \{p \leq x : f(p)^l \neq \bar{\psi}(p)\}.$$

Now, if

$$\sum_{p \in \mathcal{P}_{l,\bar{\psi}}} \frac{1}{p} > c_2 \tag{2.15}$$

with a sufficiently large constant $c_2 = c_2(k, q_1, c)$, then the above estimates together with the elementary prime number estimate,

$$\sum_{p \leq x} \frac{1}{p^\sigma} \leq \sum_{p \leq x} \frac{1}{p} = \log\log x + O(1),$$

imply (2.12). Suppose therefore that (2.15) fails for some pair $(l, \psi) \neq (0, \psi_0)$. In the case when $l = 0$ and $\psi \neq \psi_0$ we have

$$\sum_{p\in\mathcal{P}_{0,\bar{\psi}}}\frac{1}{p}=\sum_{\substack{p\le x\\ \bar{\psi}(p)\neq 1}}\frac{1}{p}\ge\sum_{\substack{p\le x\\ p\equiv a \bmod q_1}}\frac{1}{p}$$

for some a, $(a,q)=1$, which, by Dirichlet's theorem for primes in arithmetic progressions, yields (2.15) if x is sufficiently large in terms of q_1. Thus, (2.15) can only fail if $1\le l\le k-1$, and in this case we have $f\in F_{k_1}(x,\chi_1,\mathcal{P}_1)$ with $k_1=l$, $\chi_1=\bar{\psi}$, and a set of primes $\mathcal{P}_1=\mathcal{P}_{l,\bar{\psi}}$ satisfying (2.9). Hence the second alternative of the lemma is satisfied, and the proof of the lemma is complete. □

3. Construction of Special Sets

Recall that a special set is a set $S=\{n_1<n_2<\cdots<n_r\}$ of positive integers satisfying

$$n_j-n_i\,|\,(n_j,n_i)\quad(1\le i<j\le r). \tag{3.1}$$

This condition is obviously equivalent to

$$n_j-n_i=(n_j,n_i)\quad(1\le i<j\le r). \tag{3.1}'$$

The existence of such sets for arbitrarily large values of r was first proved by Heath-Brown [5]. Recently, Heath-Brown [6] proved a quantitative form of this result, showing that for any $r\ge 2$ there exists a special set with $\log n_r\ll r^3\log r$.

In this section we shall construct special sets satisfying certain congruence conditions.

LEMMA 3. *Let k, q, r, and t be positive integers, and let c be a positive constant. There exist constants $p_0=p_0(r,t)$ and $c_3=c_3(k,q,r,t,c)$ with the following property. Let $\mathcal{P}$ be a set of primes satisfying*

$$\sum_{p\in\mathcal{P}}\frac{1}{p}\le c \tag{3.2}$$

and

$$p\in\mathcal{P}\Rightarrow p>p_0, \tag{3.3}$$

and let $C_1,\dots,C_t$ be a decomposition of **N** *into t disjoint sets. Then there exists a special set $S=\{n_1<\cdots<n_r\}$ with $n_r\le c_3$ such that each n_i is of the form*

$$n_i=q^{\alpha_i}m_i,\quad(m_i,q)=1 \tag{3.4}$$

with

$$\alpha_i\equiv 0 \bmod k, \tag{3.5}$$

$$m_i\equiv(m_i,m_j) \bmod q\quad(j\neq i), \tag{3.6}$$

$$(m_i, \mathcal{P}) = 1, \tag{3.7}$$

and, for suitable fixed indices $s, s' \le t$,

$$n_i \in C_s \quad \textit{for all } i, \tag{3.8}$$

$$(n_i, n_j) \in C_{s'} \quad \textit{for all } i \ne j. \tag{3.9}$$

Proof. Fix k, q, c and a set of primes $\mathcal{P}$ satisfying (3.2) and (3.3) with a constant p_0 to be specified later. We shall first prove by induction on r that if $p_0 \ge r+1$ in (3.3) then there exists a special set $S = \{n_1 < \cdots < n_r\}$ satisfying (3.4), (3.5), (3.7), and

$$m_i \equiv 1 \bmod q \tag{3.10}$$

for all i, and whose elements are bounded in terms of k, q, r, and c. The argument here is in part inspired by Heath-Brown [6].

In the case $r = 1$ we can take the set $S = \{n_1\} = \{1\}$ which trivially has the desired properties. Now let $r \ge 1$ and assume there exists a special set $S = \{n_1 < \cdots < n_r\}$ whose elements are bounded in terms of k, q, r and c, and which satisfies (3.4), (3.5), (3.7), and (3.10). Set

$$P = q^k \prod_{i=1}^{r} n_i \quad \text{and} \quad P_i = \frac{P}{n_i},$$

so that, by (3.4),

$$P = q^{k+\alpha_1+\cdots+\alpha_r} \prod_{i=1}^{r} m_i, \tag{3.11}$$

and consider the sets

$$S(t) = \{n_i(t) : 0 \le i \le r\},$$

where

$$n_0(t) = tP, \qquad n_i(t) = n_i + tP = (1 + tP_i)n_i. \tag{3.12}$$

Each of these sets has $r+1$ elements. We shall show that for each $t \ge 1$ with $t \equiv 1 \bmod q$, $S(t)$ satisfies (3.1), (3.4), (3.5), and (3.10), and that there exists at least one such t, bounded in terms of the parameters k, q, r, and c of the lemma, so that $S(t)$ also satisfies (3.7). This will complete the induction step.

To prove (3.1), note first that for $1 \le i < j \le r$, $n_j(t) - n_i(t) = n_j - n_i$, which divides (n_i, n_j) and hence also divides $(n_i(t), n_j(t))$, since the set S satisfies (3.1) and $n_i \mid n_i(t)$ by (3.12). Moreover, for $i = 0$ and $1 \le j \le r$ we have $n_j(t) - n_0(t) = n_j$ by (3.12), which again divides $n_0(t), n_j(t)$, and hence also $(n_0(t), n_j(t))$. Thus (3.1) holds for the elements of $S(t)$ for each $t \ge 1$.

Next, from (3.4), (3.11), and (3.12) we see that

$$n_i(t) = q^{\alpha_i(t)} m_i(t)$$

with

$$\alpha_0(t) = k + \sum_{i=1}^{r} \alpha_i, \quad \alpha_i(t) = \alpha_i \quad (1 \le i \le r),$$

$$m_0(t) = t\prod_{i=1}^{r} m_i, \quad m_i(t) = (1+tP_i)m_i \quad (1 \le i \le r), \tag{3.13}$$

provided $(t, q) = 1$. Here we have used the fact that q divides P and each P_i. Since, by the induction hypothesis, (3.5) and (3.10) hold for α_i and m_i, it follows that these conditions hold for $\alpha_i(t)$ and $m_i(t)$ as well if $t \equiv 1 \bmod q$.

We now show that, for some t with $t \equiv 1 \bmod q$, $S(t)$ also satisfies (3.7). From (3.13) and the induction hypothesis we see that this is the case if $t \equiv 1 \bmod q$ and none of the factors t and $1+tP_i$ $(i = 1, \ldots, r)$ is divisible by a prime $p \in \mathcal{P}$, that is, if $t = 1+nq$ for some integer $n \ge 0$ and $(f(n), \mathcal{P}) = 1$, where

$$f(n) = (1+qn)\prod_{i=1}^{r}(1+(1+qn)P_i) = (1+qn)\prod_{i=1}^{r}((1+P_i)+qP_in).$$

To prove that $(f(n), \mathcal{P}) = 1$ for some n, we apply Lemma 1. The hypotheses (2.1), (2.2), and (2.3) of that lemma are satisfied for the polynomial $f(n)$, in view of the assumptions (3.2) and (3.3) (assuming that $p_0 \ge r+1$), and since $(1+P_i, qP_i) = (1+P_i, q) = 1$ for each i. Hence there exists a positive integer n with $(f(n), \mathcal{P}) = 1$, which is bounded in terms of c and the coefficients of f, and therefore, by the induction hypothesis, bounded in terms of the parameters k, q, r, and c. This completes the proof of (3.7).

It remains to show that the conditions (3.6), (3.8), and (3.9) can also be achieved. We shall do this by showing that suitable subsets of the special sets constructed above will have these properties.

Replacing q by $2q$, if necessary, we may assume for the proof of (3.6) that $2 \mid q$. We fix a special set S satisfying (3.4), (3.5), (3.7), and (3.10). We first note that for any fixed $\alpha \ge 0$ at most one element $n_i \in S$ can have $\alpha_i = \alpha$. Indeed, if this were not the case, then (by our assumption $2 \mid q$) two such elements would be exactly divisible by 2^α but congruent to each other modulo $2^{\alpha+1}$, which is impossible in view of the condition (3.1). Thus the exponents α_i in (3.4) are pairwise distinct. Furthermore, by taking a suitable subset, increasing the constants p_0 and c_3 as functions of r if necessary, and using a well-known result of Erdös and Szekeres [3] that any sequence of integers of length n^2+1 contains a monotone subsequence of length $n+1$, we may assume that the exponents α_i are either increasing or decreasing with i.

With these assumptions we can now embark on the proof of (3.6). Suppose first that the α_i are increasing. Then, by (3.1)′ and (3.4), we have for $i < j$ that

$$\begin{aligned}(m_i, m_j) &= q^{-\alpha_i}(q^{\alpha_i}m_i, q^{\alpha_j}m_j) = q^{-\alpha_i}(n_i, n_j)\\ &= q^{-\alpha_i}(n_j - n_i) = q^{\alpha_j-\alpha_i}m_j - m_i\end{aligned} \tag{3.14}$$

with $\alpha_j - \alpha_i > 0$. Hence $(m_i, m_j) \equiv -m_i \bmod q$ for all $i < j$, and in view of (3.10) it follows that

$$(m_i, m_j) \equiv -1 \bmod q \quad (i \ne j). \tag{3.15}$$

Similarly, in case the α_i are decreasing, we obtain

$$(m_i, m_j) \equiv 1 \bmod q \quad (i \neq j).$$

The last relation, in conjunction with (3.10), immediately yields (3.6). In case (3.15) holds, we consider instead of S the sets

$$S'(t) = \{n_i'(t) : 1 \le i \le r\}, \quad n_i' = tP - n_{r+1-i} \quad (1 \le i \le r),$$

where P is defined as in (3.11). Arguing as above, we see that, with a suitable choice of t such that $t \equiv 1 \bmod q$, the set $S'(t)$ satisfies the conditions (3.1), (3.4), (3.5), and (3.7) of Lemma 3. Defining $m_i'(t)$ in the same way as m_i with respect to $n_i'(t)$, we have

$$m_i'(t) \equiv -m_i \equiv -1 \bmod q \tag{3.10}'$$

for all i, and obtain as in (3.14) that $(m_i'(t), m_j'(t)) \equiv m_i'(t) \bmod q$ for $i < j$, and hence

$$(m_i'(t), m_j'(t)) \equiv -1 \bmod q \quad (i \neq j). \tag{3.15}'$$

From (3.10)′ and (3.15)′ it follows that (3.6) holds for the set $S'(t)$.

Finally, we note that the conditions (3.8) and (3.9) can be achieved by taking a suitable subset of a special set satisfying the remaining conditions of the lemma with a sufficiently large cardinality and increasing the constants p_0 and c_3 as functions of r and t. In the case of (3.8) this follows from the pigeonhole principle, and in the case of (3.9) an application of Ramsey's theorem gives the desired result (cf. Lemma 2 in [7]).

The proof of Lemma 3 is now complete. □

4. Proof of Theorem 2

Our proof will involve an iteration argument, the main step of which is contained in the following lemma.

LEMMA 4. *Let k and q be positive integers, and let c be a positive constant. There exists a constant $c_4 = c_4(k, q, c)$ with the following property. Let $x \ge c_4$ and $f \in F_k \cap F_{k_0}(x, \chi, \mathcal{P})$, where $1 \le k_0 \le k$, χ is a character modulo q, and $\mathcal{P}$ is a set of primes satisfying* (3.2). *Then we have either*

$$f(n) = f(n+1) = 1 \tag{4.1}$$

for some positive integer $n \le x$, or there exist positive integers $k_1 < k_0$ and $q_1 \le c_4$, a character χ_1 modulo q_1, and a set of primes $\mathcal{P}_1$ satisfying

$$\sum_{p \in \mathcal{P}_1} \frac{1}{p} \le c_4, \tag{4.2}$$

such that $f \in F_k \cap F_{k_1}(x, \chi_1, \mathcal{P}_1)$.

Proof of Lemma 4. Given $f \in F_k \cap F_{k_0}(x, \chi, \mathcal{P})$ as in the lemma, set $r = [(2/\delta_2(k_0, c)) + 2]$, where δ_2 is the constant of Lemma 2, so that $r \ge 2$ and

$r\delta_2(k_0, c) \geq 2$. We shall apply Lemma 3 with this value of r and the decomposition of $\mathbf{N}$ into the k sets

$$C_h = \{n \in \mathbf{N}: f(n) = e^{2\pi ih/k}\} \quad (h = 0, \ldots, k-1).$$

By assumption, the set $\mathcal{P}$ satisfies (3.2). The condition (3.3) is not necessarily satisfied, but if we set $q' = q\prod_{p \leq p_0} p$ and $\mathcal{P}' = \{p \in \mathcal{P}: p > p_0\}$, where $p_0 = p_0(r, k)$ is defined as in Lemma 3, and denote by χ' the character modulo q' equivalent to χ, then we have $f \in F_k \cap F_{k_0}(x, \chi', \mathcal{P}')$ (since $F_{k_0}(x, \chi, \mathcal{P}) \subset F_{k_0}(x, \chi', \mathcal{P}')$), and the hypotheses (3.2) and (3.3) of Lemma 3 are now satisfied with $\mathcal{P}'$ and q' in place of $\mathcal{P}$ and q, respectively. (Note that for the success of this argument it is essential that the constant p_0 of Lemma 3 be independent of q.) Without loss of generality we may therefore assume that the set $\mathcal{P}$ already satisfies both (3.2) and (3.3). If x is sufficiently large in terms of k, q, and c, we can then apply Lemma 3 and obtain a special set $\{n_1 < \cdots < n_r\}$ with $n_r \leq c_3(k, q, r, k, c) \leq x$ which satisfies (3.4)–(3.9).

By (3.8), (3.9), and the definition of the sets C_h, we have

$$f\left(\frac{n_i}{(n_i, n_j)}\right) = \frac{f(n_i)}{f((n_i, n_j))} = \omega \quad (i \neq j) \tag{4.3}$$

for some fixed kth root of unity ω. Moreover, (3.4)–(3.7) and the hypothesis $f \in F_k \cap F_{k_0}(x, \chi, \mathcal{P})$ imply that

$$\begin{aligned} f\left(\frac{n_i}{(n_i, n_j)}\right)^{k_0} &= f(q^{(\alpha_i - \min(\alpha_i, \alpha_j))/k})^{kk_0} f\left(\frac{m_i}{(m_i, m_j)}\right)^{k_0} \\ &= f\left(\frac{m_i}{(m_i, m_j)}\right)^{k_0} = \chi\left(\frac{m_i}{(m_i, m_j)}\right) = \chi(1) = 1 \quad (i \neq j). \end{aligned}$$

Hence ω is in fact a k_0th root of unity.

Now let

$$P = q\prod_{i=1}^{r} n_i, \quad P_i = \frac{P}{n_i},$$

and consider the integers

$$n_i(t) = n_i + tP = (1 + tP_i)n_i \quad (1 \leq i \leq r).$$

Note that, by (3.1)′,

$$\begin{aligned} (n_i(t), n_j(t)) &= (n_i + tP, n_j + tP) = (n_i + tP, n_j - n_i) = (n_i + tP, (n_i, n_j)) \\ &= (n_i, n_j) = n_j - n_i = n_j(t) - n_i(t) \quad (i < j), \end{aligned}$$

so that $n_i(t)/(n_i(t), n_j(t))$ and $n_j(t)/(n_i(t), n_j(t))$ are consecutive integers for any fixed $t \geq 0$ and $i < j$. Moreover, by (4.3) we have

$$f\left(\frac{n_i(t)}{(n_i(t), n_j(t))}\right) = f\left(\frac{n_i}{(n_i, n_j)}\right) f(1 + tP_i) = \omega f(1 + tP_i) \quad (i \neq j). \tag{4.4}$$

Thus, in order to prove (4.1), it suffices to show that there exists an integer t, bounded in terms of k, q, and c, such that

(4.5) $$f(1+tP_i)=\bar{\omega}$$

holds for at least two indices i.

If $\omega=1$ then (4.5) holds for $t=0$ and all $i\le r$, and since $r\ge 2$, (4.1) follows. We may therefore assume that $\omega\ne 1$. Let $N(t)$ denote the number of indices $i\le r$ satisfying (4.5). Then

$$\sum_{1\le t\le x}\frac{N(t)}{t}\ge\sum_{i=1}^{r}P_i\sum_{\substack{n\le x,\,(n,\mathcal{P})=1\\ n\equiv 1 \bmod P_i\\ f(n)=\bar{\omega}}}\frac{1}{n},$$

where the term $n=1$ does not contribute to the last sum, since $f(1)=1\ne\bar{\omega}$ by the above assumption. By Lemma 2 and the choice of r, the right-hand side of this expression is greater than or equal to $r\delta_2(k_0,c)\log x\ge 2\log x$ if $x\ge\max_i c_2(k_0,P_i,c)$, unless $f\in F_{k_1}(x,\chi_1,\mathcal{P})$ for some k_1 $(1\le k_1<k_0)$, a character χ_1 modulo some P_i, and a set of primes $\mathcal{P}_1$ satisfying (2.9), and hence (4.2) for $c_4\ge\max_i c_2(k_0,P_i,c)$, where c_2 and δ_2 are the constants in Lemma 2. We conclude that if c_4 is sufficiently large in terms of k, q, and c, and if $x\ge c_4$, then either the second alternative of the lemma holds or $N(t)\ge 2$ for some $t\le x^{2/3}$. In the latter case it follows, by (4.4) and the definition of $N(t)$, that (4.1) holds with $n=n_i(1+tP_i)/(n_i,n_j)\le x$ for some $i<j$. This proves the lemma. □

Proof of Theorem 2. Set

$$c_4^*(k,c)=\max\{c_4(k',q',c'):k'\le k,\,q'\le c,\,c'\le c\}$$

and

$$F_k^*(x,c)=\bigcup F_{k_1}(x,\chi,\mathcal{P}),$$

where the union is taken over all positive integers $k_1\le k$, all characters χ to moduli $\le c$, and all sets of primes $\mathcal{P}$ satisfying (3.2). Lemma 4 implies that if $x\ge c_4^*(k,c)$ and $f\in F_k\cap F_{k_0}^*(x,c)$ for some $k_0\le k$, then either f satisfies (4.1) for some $n\le x$ or $f\in F_k\cap F_{k_0-1}^*(x,c_4^*(k,c))$. Now let $f\in F_k$ be given. Then trivially $f\in F_k^*(x,1)$ for all $x\ge 1$, and defining constants $c_0^{(l)}=c_0^{(l)}(k)$ $(l=0,1,\dots)$ by

$$c_0^{(0)}=1,\quad c_0^{(l)}=\max\{c_0^{(l-1)},c_4^*(k,c_0^{(l-1)})\}\quad(l\ge 1),$$

we see inductively that for each l with $1\le l\le k$ either (4.1) holds for some $n\le c_0^{(k)}$ or $f\in F_{k-l}^*(c_0^{(k)},c_0^{(l)})$. For $l=k$ the second alternative is impossible, because $F_0^*(x,c)=\emptyset$. Hence (4.1) necessarily holds for some $n\le c_0^{(k)}$. This proves the assertion of Theorem 2 with $c_0(k)=c_0^{(k)}(k)$. □

Added in proof: The statement of Theorem 2 is actually equivalent to that of Theorem 1 under some additional conditions on f; see Mills [9].

References

1. A. Brauer, *Über Sequenzen von Potenzresten,* S. B. Akad. Wiss. Berlin Kl. Math. Phys. Tech. (1928), 9–16.

2. P. Chowla and S. Chowla, *On k*th *power residues,* J. Number Theory 10 (1978), 351–353.
3. P. Erdös and G. Szekeres, *A combinatorial problem in geometry,* Compositio Math. 2 (1935), 463–470.
4. R. L. Graham, *On quadruples of consecutive k*th *power residues,* Proc. Amer. Math. Soc. (N.S.) 15 (1964), 196–197.
5. D. R. Heath-Brown, *The divisor function at consecutive integers,* Mathematika 31 (1984), 141–149.
6. ———, *Consecutive almost-primes,* J. Indian Math. Soc. 52 (1987), 39–49.
7. A. Hildebrand, *On consecutive k*th *power residues,* Monatsh. Math. 102 (1986), 103–114.
8. D. H. Lehmer and E. Lehmer, *On runs of residues,* Proc. Amer. Math. Soc. 13 (1962), 102–106.
9. W. H. Mills, *Bounded consecutive residues and related problems,* Proc. Sympos. Pure Math., 8, pp. 170–174, Amer. Math. Soc., Providence, R.I., 1965.

Department of Mathematics
University of Illinois
Urbana, IL 61801