Canad. Math. Bull. Vol. **45** (1), 2002 pp. 109–114

The Distribution of Totatives

R. R. Hall and P. Shiu

Abstract. D. H. Lehmer initiated the study of the distribution of totatives, which are numbers coprime with a given integer. This led to various problems considered by P. Erdős, who made a conjecture on such distributions. We prove his conjecture by establishing a theorem on the ordering of residues.

1 Introduction

J. J. Sylvester called the numbers $a \leq n$ which are coprime with n the totatives of n. In order to study the distribution of these totatives, D. H. Lehmer [3] introduced the counting functions

$$\phi(n;k,\ell) = \sum_{\substack{n\ell/k<a\leq n(\ell+1)/k \\ (a,n)=1}} 1, \quad 0 \leq \ell < k. \tag{1.1}$$

In particular, $\phi(n;1,0) = \phi(n)$ is Euler's totient function. Define

$$\begin{aligned} A_k &= \{n : k^2 \mid n \text{ or there exists a prime } p \mid n \text{ with } p \equiv 1 \pmod{k}\}, \\ B_k &= \left\{ n : \phi(n;k,\ell) = \frac{\phi(n)}{k} \text{ for } 0 \leq \ell < k \right\}, \\ C_k &= \{n : k \mid \phi(n)\}. \end{aligned} \tag{1.2}$$

It is clear that A_k and B_k are subsets of C_k, and in fact Lehmer [3] proved that $A_k \subset B_k \subset C_k$. It is not difficult to show that $C_p \subset A_p$ for a prime p, so that $A_p = B_p = C_p$. P. J. McCarthy [4] proved that $A_k \neq B_k$ when k is not squarefree, and he asked if the result could be extended to all composite numbers k. This was done by P. Erdős [1], who proved that the set $B_k \setminus A_k$ is infinite for every composite k. Erdős also showed that $B_{2p} = C_{2p}$ for an odd prime p, and then proved that $B_k \neq C_k$ if $k \neq p$ and $k \neq 2p$, with p odd; see [2]. In [1] Erdős made the following

Conjecture *Let p, q be distinct odd primes such that $pq \notin A_k$ and $pq \not\equiv -1 \pmod{k}$. Then $pq \notin B_k$.*

The study of the distribution of totatives often involves the analysis of the condition under which the sum of two fractional parts of real numbers should exceed 1. In

Received by the editors March 23, 2000; revised December 4, 2000.
AMS subject classification: Primary: 11A05; secondary: 11A07, 11A25.
Keywords: Euler's function, totatives.

particular we found that the conjecture depends on an interesting inequality associated with residue classes. For a fixed modulus k, we write $x < y \pmod k$ to mean that the least non-negative residue congruent to x is less than that congruent to y.

Theorem *Let a, b, c be integers which are distinct $\pmod k$ and satisfying*

$$(ab, k) = 1, \quad c \not\equiv 0 \pmod k, \quad a + b \not\equiv c \pmod k. \tag{1.3}$$

Then there exists x such that $ax < cx < bx \pmod k$.

In the next section we show that the conjecture of Erdős follows from the theorem, the proof of which is given in the last section. We thank the diligent referee for his careful reading of the paper and for bringing our attention to [2].

2 Proof of the Conjecture

Let p, q be distinct odd primes such that $pq \not\equiv -1 \pmod k$. The condition that $pq \notin A_k$ amounts to

$$p, q \not\equiv 1 \pmod k. \tag{2.1}$$

We need to show that $pq \notin B_k$. Since $B_k \subset C_k$, we may assume that $pq \in C_k$, which then amounts to

$$pq + 1 \equiv p + q \pmod k. \tag{2.2}$$

By (1.1) and the counting argument given in [2], in order to show that $pq \notin B_k$ it suffices to find an integer ℓ such that

$$\left\{\frac{\ell pq}{k}\right\} + \left\{\frac{\ell}{k}\right\} \neq \left\{\frac{\ell p}{k}\right\} + \left\{\frac{\ell q}{k}\right\}. \tag{2.3}$$

If $pq \mid k$ then we may simply set $\ell = k/pq$. We may therefore assume that $p \nmid k$. We begin by letting $c = (p+q, k)$. Note that the condition $c \not\equiv 0 \pmod k$ in (1.3) follows from $c < k$, which holds because of (2.2) and the hypothesis $pq \not\equiv -1 \pmod k$. Write $p + q = cm$ where $(m, k/c) = 1$ and define a by $am \equiv 1 \pmod{k/c}$, so that $(a, k/c) = 1$ and

$$a(p + q) \equiv acm \equiv c \pmod k. \tag{2.4}$$

Now set $b = ap$. If $(a, c) = d > 1$ then the four numbers a, b, c, k are divisible by d, and we replace them by a/d, b/d, c/d, k/d, respectively in the following. We may now suppose that $(a, c) = 1$. Then $(ab, k) = 1$ and the remaining conditions in (1.3) for the theorem follows from (2.1) and (2.4). By the theorem, there exists x such that

$$ax < cx < bx \pmod k. \tag{2.5}$$

https://doi.org/10.4153/CMB-2002-012-1 Published online by Cambridge University Press

At this point we recover the general case on multiplying through by d. We also have, by (2.2) and (2.4), $axpq + ax \equiv axp + axq \equiv cx \pmod{k}$. Letting $r(x)$ denote the least non-negative residue of $x \pmod{k}$ it now follows from (2.5) that

$$r(axpq) + r(ax) = r(cx), \quad r(axp) + r(axq) = k + r(cx).$$

Writing $\ell = r(ax)$ we find that $r(\ell pq) + \ell < k \le r(\ell p) + r(\ell q)$, which is the same as

$$\left\{\frac{\ell pq}{k}\right\} + \left\{\frac{\ell}{k}\right\} < 1 \le \left\{\frac{\ell p}{k}\right\} + \left\{\frac{\ell q}{k}\right\},$$

so that (2.3) is proved.

3 Proof of the Theorem

Suppose first that $k = p$ is an odd prime, and that $c = 1$. For $2 \le a \le p-1$ we set

$$\mathcal{A}(a) = \{r : 1 \le r < p, ra < r \pmod{p}\}. \tag{3.1}$$

Since $ra < r \pmod{p}$ is equivalent to $(p-r)a > p - r \pmod{p}$ we find that $r \in \mathcal{A}(a)$ if and only if $p - r \notin \mathcal{A}(a)$, so that $|\mathcal{A}(a)| = \frac{1}{2}(p-1)$ and hence $|\mathcal{A}(a) \setminus \mathcal{A}(b)| = |\mathcal{A}(b) \setminus \mathcal{A}(a)|$. It is also easy to check that $\mathcal{A}(a) = \mathcal{A}(b)$ when $a + b \equiv 1 \pmod{p}$, since if for some j with $1 \le j < r$ we have $ra \equiv j$ then $rb \equiv r - j$. We proceed to show that if

$$2 \le a < b \le \frac{p+1}{2}, \tag{3.2}$$

then $\mathcal{A}(a) \ne \mathcal{A}(b)$, and the required result follows from the definition of $\mathcal{A}(a)$. The proof makes use of characters $\chi \pmod{p}$, Gauss sums and the fact that $L(1, \chi) \ne 0$.

Write

$$F(a, \chi) = \sum_{r \in \mathcal{A}(a)} \chi(r) \tag{3.3}$$

and we proceed to prove that $F(a, \chi) \ne F(b, \chi)$ for some character χ, which then implies $\mathcal{A}(a) \ne \mathcal{A}(b)$. We first establish the formula

$$F(a, \chi) = W(\chi)\{1 + \bar{\chi}(a-1) - \bar{\chi}(a)\}, \tag{3.4}$$

where

$$W(\chi) = \frac{1}{p} \sum_{1 \le r < p} r\chi(r). \tag{3.5}$$

https://doi.org/10.4153/CMB-2002-012-1 Published online by Cambridge University Press

The usual procedure of using an exponential sum to identify those $r \in \mathcal{A}(a)$ leads to the following

$$\begin{aligned} F(a,\chi) &= \sum_{1\le r<p} \chi(r) \sum_{0\le s<r} \frac{1}{p} \sum_{0\le h<p} e\Big(\frac{-h(s-ra)}{p}\Big) \\ &= \frac{1}{p} \sum_{1\le r<p} r\chi(r) + \frac{1}{p} \sum_{1\le h<p} \sum_{1\le r<p} \chi(r) e\Big(\frac{hra}{p}\Big) \sum_{0\le s<r} e\Big(\frac{-hs}{p}\Big) \\ &= W(\chi) + \frac{1}{p} \sum_{1\le h<p} \frac{1}{e(-h/p)-1} \sum_{1\le r<p} \chi(r) e\Big(\frac{hra}{p}\Big) \Big\{ e\Big(\frac{-hr}{p}\Big) - 1 \Big\}. \end{aligned}$$

Let

$$G(\chi, x) = \sum_{1\le r<p} \chi(r) e\Big(\frac{rx}{p}\Big),$$

so that $G(\chi, x) = \bar{\chi}(x) G(\chi)$, where $G(\chi) = G(\chi, 1)$, and hence

$$F(a,\chi) = W(\chi) + \frac{1}{p} G(\chi) \sum_{1\le h<p} \frac{\bar{\chi}(ha-h) - \bar{\chi}(ha)}{e(-h/p)-1}.$$

The sum here can be evaluated from

$$\begin{aligned} \sum_{1\le h<p} \frac{\bar{\chi}(h)}{e(-h/p)-1} &= -\lim_{\lambda\to 1} \sum_{1\le h<p} \frac{\bar{\chi}(h)}{1-\lambda e(-h/p)} \\ &= -\lim_{\lambda\to 1} \sum_{1\le h<p} \bar{\chi}(h) \sum_{m=0}^{\infty} \lambda^m e\Big(\frac{-mh}{p}\Big) \\ &= -\lim_{\lambda\to 1} \sum_{1\le h<p} \bar{\chi}(h) \sum_{0\le m<p} \frac{\lambda^m e(-mh/p)}{1-\lambda^p} \\ &= \lim_{\lambda\to 1} \sum_{1\le h<p} \bar{\chi}(h) \sum_{1\le m<p} \frac{m\lambda^{m-1} e(-mh/p)}{p\lambda^{p-1}} \quad \text{(l'Hôpital)} \\ &= \frac{1}{p} \sum_{1\le m<p} m \sum_{1\le h<p} \bar{\chi}(h) e(-mh/p) \\ &= \frac{1}{p} \sum_{1\le m<p} m\chi(m)\overline{G(\chi)} = W(\chi)\overline{G(\chi)}, \end{aligned}$$

and (3.4) now follows from $|G(\chi)| = \sqrt{p}$.

https://doi.org/10.4153/CMB-2002-012-1 Published online by Cambridge University Press

When χ is an odd character, that is $\chi(-1) = -1$, the sum (3.5) can be evaluated. Thus, from

$$\begin{aligned} W(\chi) &= \sum_{1\le r<p} \Big(\frac{r}{p} - \frac{1}{2}\Big)\chi(r) \\ &= -\sum_{1\le r<p}\sum_{m\in\mathbb{N}} \chi(r)\frac{\sin(2\pi mr/p)}{\pi m} \\ &= \frac{1}{2\pi}\sum_{m\in\mathbb{N}}\frac{\bar\chi(m)}{m}\sum_{1\le r<p}\chi(mr)\Big(e\Big(\frac{mr}{p}\Big) - e\Big(\frac{-mr}{p}\Big)\Big), \end{aligned}$$

and the fact that χ is odd, so that the terms $-e(-mr/p)$ just double up, we find that

$$W(\chi) = \frac{i}{\pi}\sum_{m\in\mathbb{N}}\frac{\bar\chi(m)}{m}G(\chi) = \frac{i}{\pi}G(\chi)L(1,\bar\chi). \tag{3.6}$$

In particular, $W(\chi) \ne 0$ for an odd character, and we may now consider the sum

$$\Delta(a,b) = \sum_{\chi}^{\star}\frac{|F(a,\chi) - F(b,\chi)|^2}{|W(\chi)|^2}, \tag{3.7}$$

where $\star$ indicates that the sum is restricted to odd characters χ. From (3.4) we have

$$\begin{aligned} \Delta(a,b) &= \sum_{\chi}^{\star}|\bar\chi(a-1) - \bar\chi(a) - \bar\chi(b-1) + \bar\chi(b)|^2 \\ &= 2(p-1) - S(a-1,a) - S(b-1,b) - S(a-1,b-1) - S(a,b) \\ &\quad + S(a,b-1) + S(a-1,b), \end{aligned}$$

where

$$S(x,y) = 2\,\mathrm{Re}\sum_{\chi}^{\star}\bar\chi(x)\chi(y) = \begin{cases} \pm(p-1) & \text{if } x \equiv \pm y \pmod p, \\ 0 & \text{otherwise.} \end{cases}$$

When a, b satisfy (3.2) we find that $S(a-1,a) = S(b-1,b) = S(a-1,b-1) = S(a-1,b) = 0$. Moreover, if $a \equiv \pm b \pmod p$ then $a = \frac{1}{2}(p-1)$, $b = \frac{1}{2}(p+1)$, with $S(a,b) = -(p-1)$. Finally $S(a,b-1) \ne 0$ if and only if $a = b-1$, when its value is $p-1$. Therefore, for a, b satisfying (3.2),

$$\Delta(a,b) = \begin{cases} 2(p-1) & \text{if } a < b-1, \\ 3(p-1) & \text{if } a = b-1 < \frac{1}{2}(p-1), \\ 4(p-1) & \text{if } a = b-1 = \frac{1}{2}(p-1). \end{cases}$$

https://doi.org/10.4153/CMB-2002-012-1 Published online by Cambridge University Press

In particular $\Delta(a,b) > 0$, so that, by (3.7), there exists a character χ such that $F(a,\chi) \neq F(b,\chi)$. Indeed, since $|L(1,\chi)| \gg_\epsilon 1/p^\epsilon$ for every $\epsilon > 0$, it now follows from (3.6), (3.7) and $\Delta(a,b) \geq 2(p-1)$ that

$$\sum_\chi{}^\star |F(a,\chi) - F(b,\chi)|^2 \gg_\epsilon p^{2-\epsilon}.$$

This implies

$$\frac{1}{p-1}\sum_\chi |F(a,\chi) - F(b,\chi)|^2 \gg_\epsilon p^{1-\epsilon},$$

that is $|\mathcal{A}(a) \setminus \mathcal{A}(b)| \gg_\epsilon p^{1-\epsilon}$ as $p \to \infty$.

For the general case, when k is composite and $c \not\equiv 0 \pmod k$, we need to replace the definition of $\mathcal{A}(a)$ in (3.1) by $\mathcal{A}(a) = \{r : 1 \leq r < k, (r,k) = 1, ra < rc \pmod k\}$. Then $\mathcal{A}(a) = \mathcal{A}(b)$ when $a + b \equiv c \pmod k$, so that (3.2) has to be adjusted accordingly. The argument then proceeds in the same way except that the occurrence of $p-1$ should be replaced by $\phi(k)$.

References

[1] P. Erdős, *Some remarks on a paper of McCarthy*. Canad. Math. Bull. **1**(1958), 71–75.
[2] ———, *Remarks and corrections to my paper 'Some remarks on a paper of McCarthy'*. Canad. Math. Bull. **3**(1960), 127–129.
[3] D. H. Lehmer, *The distribution of totatives*. Canad. J. Math. **7**(1955), 347–357.
[4] P. J. McCarthy, *Note on the distribution of the totatives*. Amer. Math. Monthly **64**(1957), 585–586.

Department of Mathematics
York University
Heslington
York YO1 5DD
United Kingdom
e-mail: rrh1@york.ac.uk

Department of Mathematical Sciences
Loughborough University
Loughborough
Leicestershire LE11 3TU
United Kingdom
e-mail: P.Shiu@lboro.ac.uk