The distribution of totatives

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 clarify results due to Erdős and prove his conjecture by establishing a theorem on the ordering of residues.

1. Introduction

J. J. Sylvester called the numbers $a \le n$ 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

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

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

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

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 [5] proved that $A_k \ne B_k$ 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 [2], 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 $B_k \ne C_k$ if $k \ne p$ and $k \ne 2p$, with p odd.

The notation (1.2) was introduced by N. G. de Bruijn [1] in the review of [2]. The introduction of these sets A_k, B_k, C_k helps to clarify and summarise the above results. De Bruijn also pointed out that parts of the proof in [2] required rectifications which Erdős was to have supplied, and we give these necessary amendments in Section 2. In [2] Erdős also 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 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* (mod k) *and satisfying*

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

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

In Section 3 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.

2. Amendments to [2]

We first give the amendments to Erdős' proof of $B_k \neq C_k$ when k is neither a prime nor twice an odd prime. The more general argument given in the next section involves $\phi(n;k,\ell)$, and can be used for the proof, while the argument by Erdős makes use of $\phi(n;k,0)$ only. We shall write $\{\theta\}$ for the fractional part of the real number θ. First, Lehmer [3] already found that $21 \in C_4 \setminus B_4$, and it is easy to check that $35 \in C_8 \setminus B_8$.

We now set $k = ab$ where $a, b > 2$. Erdős wrote "It is not difficult to see that for such k there exist infinitely many primes p, q satisfying

$$p \equiv 1 \,(\mathrm{mod}\ a), \quad p \equiv 1 \,(\mathrm{mod}\ b), \quad pq \equiv -1 \,(\mathrm{mod}\ k), \qquad \Big\{\frac{p}{k}\Big\} > \frac{1}{2}, \quad \Big\{\frac{q}{k}\Big\} > \frac{1}{2}." \tag{2.1}$$

From what will be required in the following, it is clear that $p \equiv 1 \,(\mathrm{mod}\ b)$ here should be $q \equiv 1 \,(\mathrm{mod}\ b)$. More confusing is that the condition $pq \equiv -1 \,(\mathrm{mod}\ k)$ should be $pq \not\equiv -1 \ (\mathrm{mod}\ k)$ instead. We therefore replace (2.1) by

$$p \equiv 1 \,(\mathrm{mod}\ a), \quad q \equiv 1 \,(\mathrm{mod}\ b), \quad pq \not\equiv -1 \ (\mathrm{mod}\ k), \qquad \Big\{\frac{p}{k}\Big\} > \frac{1}{2}, \quad \Big\{\frac{q}{k}\Big\} > \frac{1}{2}. \tag{2.2}$$

Actually (2.2) does not always hold when $a = 3$. For if $q \equiv bt + 1 \,(\mathrm{mod}\ 3b)$, then the condition $\{q/3b\} > 1/2$ requires $t \equiv 2 \,(\mathrm{mod}\ 3)$, and hence $3|q$ when $b \equiv 1 \,(\mathrm{mod}\ 3)$. In fact, the proof of $B_{3b} \neq C_{3b}$, where $b > 2$, has to involves $\phi(n;k,\ell)$, and will be given in the next section.

Now let a, b be numbers not taking the values $1, 2, 3, 6$. We show that it is possible to choose ℓ so that $\frac{b}{2} \le \ell < b$ and $(\ell a + 1, b) = 1$, noting that a sufficient condition for the latter is that ℓa is divisible by each prime factor of b. If $d = (a, b) \ge 2$ then we choose $\ell = \big(d - 1\big)b/d$. Suppose now that $(a, b) = 1$. If b has a divisor $s^2 \ge 4$, then we choose $\ell = [\frac{1}{2}(s + 1)]b/s$. If b has a prime divisor $\rho \ge 5$ such that $\rho^2 \not| b$ then we set $\ell = (\rho + j)b/2\rho$ choosing $j = 1$ or 3. Observe that ρ cannot divide $\ell a + 1$ for both choices of j since otherwise it would divide their difference, namely b/ρ, which is not the case. Thus, for at least one of the choices, we have $(\ell a + 1, b) = 1$. Similarly, there are integers m such that $\frac{a}{2} \le m < a$ and $(mb + 1, a) = 1$. We may assume that $\ell a + mb + 2 \not\equiv 0 \ (\mathrm{mod}\ ab)$, since in general there are more than one choice for ℓ and m; if there are exceptional cases we can still deal with them using the general method in the next section. From Dirichlet's theorem for primes in arithmetic progressions there are infinitely many primes p and q such that $p \equiv \ell a + 1 \,(\mathrm{mod}\ ab)$ and $q \equiv mb + 1 \,(\mathrm{mod}\ ab)$, and such primes will now satisfy the conditions in (2.2). We also remark that in their study of sparsely totient numbers D. W. Masser and P. Shiu (Lemma 6 in [4]) gave a proof for the existence of primes p satisfying the more demanding condition of $\{k/p\} > 1 - k/p^2$. Anyway, we now set $n = pq$ and it is easy to check that $n \in C_k \setminus A_k$. A simple counting argument shows that

$$\phi(n;k,0) = \sum_{\substack{a \le n/k \\ (a,n)=1}} 1 = \Big[\frac{pq}{k}\Big] - \Big[\frac{p}{k}\Big] - \Big[\frac{q}{k}\Big] + \Big[\frac{1}{k}\Big] = \frac{\phi(n)}{k} + E, \tag{2.3}$$

where

$$E = -\Big\{\frac{pq}{k}\Big\} + \Big\{\frac{p}{k}\Big\} + \Big\{\frac{q}{k}\Big\} - \Big\{\frac{1}{k}\Big\}. \tag{2.4}$$

We already remarked that $n \in C_k$, so that E is an integer according to (2.3). Moreover, since $1 < \left\{\frac{p}{k}\right\} + \left\{\frac{q}{k}\right\} < 2$ by (2.2), it follows from (2.4) that $E = 1$, provided that $\left\{\frac{pq}{k}\right\} + \left\{\frac{1}{k}\right\} < 1$, which is the case since $pq \not\equiv -1 \pmod{k}$. Therefore $E = 1$, so that $n \notin B_k$ by (2.3) and (1.2).

The proof, apart from the case $k = 3b$ where $b > 2$, has been rectified.

3. 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

$$p, q \not\equiv 1 \pmod{k}. \tag{3.1}$$

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

$$pq + 1 \equiv p + q \pmod{k}. \tag{3.2}$$

By (1.1) and the counting argument for (2.3) and (2.4), in order to show that $pq \notin B_k$ it suffices to find an integer ℓ such that

$$\left\{\frac{\ell pq}{k}\right\} + \left\{\frac{\ell}{k}\right\} \neq \left\{\frac{\ell p}{k}\right\} + \left\{\frac{\ell q}{k}\right\}. \tag{3.3}$$

If $pq|k$ then we may simply set $\ell = k/pq$. We may therefore assume that $p\not|k$. 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 (3.2) 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

$$a(p + q) \equiv acm \equiv c \pmod{k}. \tag{3.4}$$

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 (3.1) and (3.4). By the theorem, there exists x such that

$$ax < cx < bx \pmod{k}. \tag{3.5}$$

At this point we recover the general case on multiplying through by d. We also have, by (3.2) and (3.4), $axpq + ax \equiv axp + axq \equiv cx \pmod{k}$. Letting $r(x)$ denote the least non-negative residue of $x \pmod{k}$ it now follows from (3.5) that

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

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

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

so that (3.3) is proved.

In particular, we take $k = 3b$, with $b > 2$. Let $p = 7$ and $q \equiv 1 \pmod b$, so that $\phi(pq) = 6(q-1)$ is a multiple of $k = 3b$, and hence $pq \in C_{3b}$. As before, we find that

$$\sum_{\substack{a \le \ell pq/k \\ (a,pq)=1}} 1 = \Big[\frac{\ell pq}{k}\Big] - \Big[\frac{\ell p}{k}\Big] - \Big[\frac{\ell q}{k}\Big] + \Big[\frac{\ell}{k}\Big] = \frac{\ell\phi(pq)}{k} + E,$$

where

$$E = \Big\{\frac{\ell p}{k}\Big\} + \Big\{\frac{\ell q}{k}\Big\} - \Big\{\frac{\ell pq}{k}\Big\} - \Big\{\frac{\ell}{k}\Big\}.$$

By (3.3) there exists $\ell < k$ such that $E \ne 0$, so that $pq \notin B_{3b}$, and hence $B_{3b} \ne C_{3b}$.

4. 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

$$\mathcal{A}(a) = \{r : 1 \le r < p,\ ra < r \pmod p\}. \tag{4.1}$$

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 $|\mathcal{A}(a)| = \frac12(p-1)$ 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

$$2 \le a < b \le \frac{p+1}{2}, \tag{4.2}$$

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

$$F(a,\chi) = \sum_{r \in \mathcal{A}(a)} \chi(r) \tag{4.3}$$

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

$$F(a,\chi) = W(\chi)\big\{1 + \bar\chi(a-1) - \bar\chi(a)\big\}, \tag{4.4}$$

where

$$W(\chi) = \frac1p \sum_{1 \le r < p} r\chi(r). \tag{4.5}$$

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

$$\begin{aligned} F(a,\chi) &= \sum_{1\le r<p} \chi(r) \sum_{0 \le s < r} \frac1p \sum_{0 \le h < p} e\Big(\frac{-h(s-ra)}{p}\Big) \\ &= \frac1p \sum_{1\le r<p} r\chi(r) + \frac1p \sum_{1\le h<p} \sum_{1\le r<p} \chi(r) e\Big(\frac{hra}{p}\Big) \sum_{0\le s<r} e\Big(\frac{-hs}{p}\Big) \\ &= W(\chi) + \frac1p \sum_{1\le h<p} \frac{1}{e(-h/p)-1} \sum_{1\le r<p} \chi(r) e\Big(\frac{hra}{p}\Big)\Big\{e\Big(\frac{-hr}{p}\Big) - 1\Big\}. \end{aligned}$$

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

$$\begin{aligned}
\sum_{1\le h<p}\frac{\bar\chi(h)}{e(-h/p)-1}&=-\lim_{\lambda\to1}\sum_{1\le h<p}\frac{\bar\chi(h)}{1-\lambda e(-h/p)}\\
&=-\lim_{\lambda\to1}\sum_{1\le h<p}\bar\chi(h)\sum_{m=0}^{\infty}\lambda^m e\Big(\frac{-mh}{p}\Big)\\
&=-\lim_{\lambda\to1}\sum_{1\le h<p}\bar\chi(h)\sum_{0\le m<p}\frac{\lambda^m e(-mh/p)}{1-\lambda^p}\\
&=\lim_{\lambda\to1}\sum_{1\le h<p}\bar\chi(h)\sum_{1\le m<p}\frac{m\lambda^{m-1}e(-mh/p)}{p\lambda^{p-1}}\quad\text{(l'Hôpital)}\\
&=\frac{1}{p}\sum_{1\le m<p}m\sum_{1\le h<p}\bar\chi(h)e(-mh/p)\\
&=\frac{1}{p}\sum_{1\le m<p}m\chi(m)\overline{G(\chi)}=W(\chi)\overline{G(\chi)},
\end{aligned}$$

and (4.4) now follows from $|G(\chi)|=\sqrt{p}$.

When χ is an odd character, that is $\chi(-1)=-1$, the sum (4.5) can be evaluated. Thus, from

$$\begin{aligned}
W(\chi)&=\sum_{1\le r<p}\Big(\frac{r}{p}-\frac12\Big)\chi(r)\\
&=-\sum_{1\le r<p}\sum_{m\in\mathbb{N}}\chi(r)\frac{\sin(2\pi mr/p)}{\pi m}\\
&=\frac{1}{2\pi}\sum_{m\in\mathbb{N}}\frac{\bar\chi(m)}{m}\sum_{1\le r<p}\chi(mr)\Big(e\big(\frac{mr}{p}\big)-e\big(\frac{-mr}{p}\big)\Big),
\end{aligned}$$

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

$$W(\chi)=\frac{i}{\pi}\sum_{m\in\mathbb{N}}\frac{\bar\chi(m)}{m}G(\chi)=\frac{i}{\pi}G(\chi)L(1,\bar\chi).\tag{4.6}$$

In particular, $W(\chi)\ne0$ for an odd character, and we may now consider the sum

$$\Delta(a,b)=\sum_{\chi}^{\star}\frac{|F(a,\chi)-F(b,\chi)|^2}{|W(\chi)|^2},\tag{4.7}$$

where $\star$ indicates that the sum is restricted to odd characters χ. From (4.4) we have

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

where

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

When a, b satisfy (4.2) we find that $S(a-1,a) = S(b-1,b) = S(a-1,b-1) = S(a-1,b) = 0$. Moreover, if $a \equiv \pm b \,(\mathrm{mod}\ p)$ then $a = \frac{1}{2}(p-1)$, $b = \frac{1}{2}(p+1)$, with $S(a,b) = -(p-1)$. Finally $S(a,b-1) \neq 0$ if and only if $a = b-1$, when its value is $p-1$. Therefore, for a, b satisfying (4.2),

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

In particular $\Delta(a,b) > 0$, so that, by (4.7), 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 (4.6), (4.7) 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 $c \not\equiv 0 \ (\mathrm{mod}\ k)$, we need to replace the definition of $\mathcal{A}(a)$ in (4.1) by $\mathcal{A}(a) = \{r : 1 \leq r < k, (r,k) = 1,\ ra < rc \ (\mathrm{mod}\ k)\}$. Then $\mathcal{A}(a) = \mathcal{A}(b)$ when $a + b \equiv c \,(\mathrm{mod}\ k)$, so that (4.2) 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] N. G. de Bruijn, Review of [2] in *Math. Reviews* 20 (1959), ♯3093.

[2] P. Erdős, "Some remarks on a paper of McCarthy", *Can. Math. Bull.* 1, 71–75 (1958).

[3] D. H. Lehmer, "The distribution of totatives," *Canad. J. of Math.* 7, 347–357 (1955).

[4] D. W. Masser and P. Shiu, "On sparsely totient numbers," *Pacific J. Math.* 121 , 407–426 (1986).

[5] P. J. McCarthy, "Note on the distribution of the totatives," *Amer. Math. Monthly*, 64, 585–586 (1957).

R. R. Hall
Department of Mathematics
York University
Heslington
York YO1 5DD
United Kingdom
Email: rrh1@york.ac.uk

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