THE DISTRIBUTION OF TOTATIVES

D. H. LEHMER

1. Introduction. This paper is concerned with the numbers which are relatively prime to a given positive integer

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$$

where the p's are the distinct prime factors of n. Since these numbers recur periodically with period n, it suffices to study the $\phi(n)$ numbers $\leqslant n$ and relatively prime to n. Here

$$\phi(n) = n(1 - p_1^{-1})(1 - p_2^{-1}) \dots (1 - p_t^{-1}) \tag{1}$$

is Euler's function. Following Sylvester, these $\phi(n)$ numbers are called the *totatives* of n. One may ask how these totatives are distributed among the integers $\leqslant n$. Specifically we may divide the interval from 0 to n into k equal subintervals and consider the number of totatives in each of these subintervals. It is natural to suppose that these intervals are of more than unit length so that we shall suppose that $n > k$ in what follows. The ambiguity of assigning an interval to a totative which occupies the common end point of two adjacent intervals does not arise. In fact if qn/k is a totative, n must divide k. But $n > k$. Hence we define, for each $q = 0, 1, \dots, k - 1$, the partial totient function $\phi(k, q, n)$ as the number of totatives τ for which

$$nq/k < \tau < n(q + 1)/k. \tag{2}$$

Alternatively, one may divide the unit circle into k equal arcs by the kth roots of unity and enquire about the number of *primitive* nth roots of unity in each such arc. It is clear that

$$\sum_{q=0}^{k-1} \phi(k, q, n) = \phi(1, 0, n) = \phi(n). \tag{3}$$

We shall be interested in the question of how uniformly the totatives are distributed and so we introduce the function

$$E(k, q, n) = \phi(n) - k\phi(k, q, n), \tag{4}$$

which may be described as the excess of the number of all totatives of n over the number there would be if the totatives were everywhere as dense as they are in the interval

$$nq/k \leqslant x \leqslant n(q + 1)/k. \tag{5}$$

The value of $E(k, q, n)$ is an integer, positive, negative, or zero. By (3) we have

$$\sum_{q=0}^{k-1} E(k, q, n) = 0. \tag{6}$$

Received November 5, 1954.

2. Uniform distribution. The vanishing of $E(k, q, n)$ is an indication of uniformly distributed totatives. For $E(k, q, n)$ to vanish even for one value of q it is necessary that $\phi(n)$ be divisible by k. That this condition is not sufficient is seen from the example of $n = 21$ and $k = 4$.

In this case $\phi(n) = 12$ is divisible by k but, as we shall see,

$$E(4, 0, 21) = E(4, 3, 21) = -4,$$
$$E(4, 1, 21) = E(4, 2, 21) = 4,$$

so that $E(4, q, 21)$ never vanishes.

If, for some k and n, the functions $E(k, q, n)$ vanish for all values of q, then we say that the totatives of n are uniformly distributed with respect to k, there being $\phi(n)/k$ totatives in each of the k intervals. For example, for every $n > 2$ the totatives are uniformly distributed with respect to $k = 2$. That is

$$E(2, 0, n) = E(2, 1, n) = 0 \qquad (n > 2).$$

This follows at once from the fact that if τ is a totative, so also is $n - \tau$. Similarly we have

THEOREM 1. *If $n > k$, $E(k, q, n) = E(k, k - q - 1, n)$ for all values of q.*

THEOREM 2. *If n is divisible by k^2 then the totatives of n are uniformly distributed with respect to k, that is,*

$$E(k, q, hk^2) = 0 \qquad (q = 0, 1, \ldots, k-1).$$

Proof. This follows at once if we consider the fact that all the totatives of $n = hk^2$ may be generated from those less than hk by adding successive multiples of hk. In fact the integers

$$\tau + qhk \qquad (q = 0, 1, \ldots, k - 1; 0 < \tau < hk)$$

are all totatives of $n = hk^2$ if τ is, and every totative of n is of this form.

3. Auxiliary numerical functions. We proceed to develop formulas for $E(k, q, n)$ in terms of simpler numerical functions. These functions are:

$\mu(n)$, Möbius' function;
$\lambda(n)$, Liouville's function;
$\theta(n)$, the number of square-free divisors of n.

All these functions, as well as $\phi(n)$, are multiplicative, that is, if f is any one of these functions, then

$$f(n) = \prod_{i=1}^{t} f(p_i^{\alpha_i}).$$

For prime power arguments we have:

$$\mu(p^\alpha) = \begin{cases} -1 & \text{if } \alpha = 1, \\ 0 & \text{if } \alpha > 1 \end{cases}$$
$$\lambda(p^\alpha) = (-1)^\alpha,$$
$$\theta(p^\alpha) = 2.$$

In particular,

$$\theta(n) = 2^t = \sum_{\delta | n,\ \mu(\delta) \neq 0} 1.$$

We conclude this list of well-known facts by quoting the following formulas:

$$\sum_{\delta | n} \mu(n/\delta) = 0,\ n > 1, \tag{7}$$

$$\sum_{\delta | n} \lambda(\delta)\, \mu(n/\delta) = \lambda(n)\, \theta(n), \tag{8}$$

where the sums, as indicated, range over all the divisors δ of n. The second of these is due to Liouville **(3)**.

In what follows we denote by $[x]$ the greatest integer $\leqslant x$.

THEOREM 3.

$$E(k, q, n) = \sum_{\delta | n} \left\{ \delta + k\left[\frac{q\delta}{k}\right] - k\left[\frac{(q+1)\delta}{k}\right] \right\} \mu(n/\delta).$$

Proof. By a theorem of Legendre **(1**, pp. 7–8**)** the number of totatives of n which do not exceed x is given by

$$\sum_{\delta | n} [x/\delta]\, \mu(\delta) = \sum_{\delta | n} [\delta x/n]\, \mu(n/\delta).$$

In particular,

$$\phi(n) = \sum_{\delta | n} \delta\, \mu(n/\delta) \tag{9}$$

and

$$\phi(k, q, n) = \sum_{\delta | n} \{[\delta(q+1)/k] - [\delta q/k]\}\, \mu(n/\delta). \tag{10}$$

The theorem now follows from (4).

For $q = 0$ we have the simple formula

$$E(k, 0, n) = \sum_{\delta | n} r_k(\delta)\, \mu(n/\delta), \tag{11}$$

where $r_k(\delta)$ is the least positive remainder, $\delta - k[\delta/k]$, on division of δ by k.

THEOREM 4. *If n is divisible by a prime p of the form $kx + 1$, then the totatives of n are uniformly distributed with respect to k, that is,*

$$E(k, q, n) = 0 \qquad (q = 0, 1, \ldots, k-1).$$

Proof. It suffices to show that in case

$$n = p^\alpha m, \quad p = kx + 1, \quad p \nmid m,$$

then $\phi(k, q, n)$ is not a function of q. Now

$$\phi(k, q, n) = \sum_{\delta | m} \mu(m/\delta)\, g(k, q, p^\alpha, \delta), \tag{12}$$

where

$$g(k, q, p^\alpha, \delta) = \sum_{v=0}^{\alpha} \left\{ \left[\frac{p^v\delta(q+1)}{k}\right] - \left[\frac{p^v\delta q}{k}\right] \right\} \mu(p^{\alpha - v}).$$

Since $\mu(p^\beta) = 0$ for $\beta > 1$, we have

$$g(k, q, p^\alpha, \delta) = \left[\frac{p^\alpha\delta(q+1)}{k}\right] - \left[\frac{p^\alpha\delta q}{k}\right] - \left[\frac{p^{\alpha-1}\delta(q+1)}{k}\right] + \left[\frac{p^{\alpha-1}\delta q}{k}\right].$$

Let $p^\alpha = kr + 1$, $p^{\alpha-1} = ks + 1$. Then:

$$\left[\frac{p^\alpha\delta q}{k}\right] = r\delta q + \left[\frac{\delta q}{k}\right],$$

$$\left[\frac{p^{\alpha-1}\delta q}{k}\right] = s\delta q + \left[\frac{\delta q}{k}\right],$$

$$\left[\frac{p^\alpha\delta(q+1)}{k}\right] = r\delta q + r\delta + \left[\frac{\delta(q+1)}{k}\right],$$

$$\left[\frac{p^{\alpha-1}\delta(q+1)}{k}\right] = s\delta q + s\delta + \left[\frac{\delta(q+1)}{k}\right].$$

Substituting, we find

$$g(k, q, p^\alpha, \delta) = (r - s)\delta = \delta\,\phi(p^\alpha)/k.$$

Since this is not a function of q, the theorem follows.

Incidentally we may substitute the value obtained for $g(k, q, p^\alpha, \delta)$ into (12) and get

$$\phi(k, q, n) = \sum_{\delta | m} \mu(m/\delta)\,\delta\,\frac{\phi(p^\alpha)}{k} = \phi(p^\alpha)\,\frac{\phi(m)}{k} = \frac{\phi(n)}{k},$$

as it should be.

We define n as an "exceptional number with respect to k" in case n is divisible either by k^2 or by a prime of the form $kx + 1$. Theorems 2 and 4 together state that if n is an exceptional number with respect to k, then the totatives are uniformly distributed with respect to k. We may confine our attention in what follows to non-exceptional numbers. Every number is exceptional with respect to 2. Hence we consider $k \geqslant 3$.

The cases $k = 3, 4, 6$, are sufficiently simple so that it is possible to give explicit formulas for $E(k, q, n)$. These we proceed to develop. Some of these were given by van der Corput and Kluyver **(4)**.

4. The case $k = 3$. By (6) and Theorem 1 we see that

$$E(3, 2, n) = E(3, 0, n), \qquad E(3, 1, n) = -2E(3, 0, n).$$

Hence it remains to find $E(3, 0, n)$.

THEOREM 5. *Let n be a non-exceptional number with respect to* 3, *then*

$$E(3, 0, n) = \begin{cases} -\frac{1}{4}\lambda(n)\,\theta(n), & 3 \mid n, \\ -\frac{1}{2}\lambda(n)\,\theta(n), & \text{otherwise.} \end{cases}$$

Proof. By (11) we have

$$E(3, 0, n) = \sum_{\delta | n} r_3(\delta)\,\mu(n/\delta). \tag{13}$$

Now let $n = 3^\alpha n_1$ where, since n is not exceptional and >3, n_1 is a non-empty product of primes of the form $3x - 1$ and $\alpha = 0$ or 1. If δ_1 be any divisor of n_1 then

$$\lambda(\delta_1) \equiv r_3(\delta_1) \pmod 3$$

and since $3 - 2r_3(\delta_1)$ takes on the values $+1$ or -1 and is congruent to $r_3(\delta_1)$ (mod 3), we have

$$\lambda(\delta_1) = 3 - 2r_3(\delta_1).$$

Hence, by (13),

$$\begin{aligned}-2E(3, 0, n) &= \sum_{\delta | n} (-2r_3(\delta))\, \mu(n/\delta) = \mu(3^\alpha) \sum_{\delta_1 | n_1} (-2r_3(\delta_1))\, \mu(n_1/\delta_1)\\ &= \mu(3^\alpha) \sum_{\delta_1 | n_1} (\lambda(\delta_1) - 3)\, \mu(n_1/\delta_1) = \mu(3^\alpha) \sum_{\delta_1 | n_1} \lambda(\delta_1)\, \mu(n_1/\delta_1)\\ &= \mu(3^\alpha)\, \lambda(n_1)\, \theta(n_1) = \lambda(n)\, \theta(n_1),\end{aligned}$$

by (8). Now

$$\theta(n_1) = \begin{cases} \frac{1}{2}\theta(n), & \text{if } 3 \mid n,\\ \theta(n), & \text{otherwise.}\end{cases}$$

From this the theorem follows.

It follows from the above that $E(3, q, n)$ vanishes only for exceptional numbers n and then vanishes for all q.

5. The case $k = 4$. By use of (6) and Theorem 1 we find

$$E(4, 1, n) = -E(4, 0, n), E(4, 2, n) = -E(4, 0, n), E(4, 3, n) = E(4, 0, n).$$

Hence it suffices to consider $E(4, 0, n)$.

THEOREM 6. *Let $n > 4$ be a non-exceptional number with respect to 4. Then*

$$E(4, 0, n) = \begin{cases} -\lambda(n)\, \theta(n), & \textit{if } n \textit{ is odd},\\ -\frac{1}{2}\lambda(n)\, \theta(n), & \textit{if } n \equiv 2 \pmod 4,\\ 0, & \textit{otherwise}.\end{cases}$$

Proof. Let $n = 2^\alpha n_1$ where n_1 is a product of primes of the form $4x - 1$. By (11)

$$E(4, 0, n) = \sum_{\delta | n} r_4(\delta)\, \mu(n/\delta).$$

Since $r_4(\delta)$ vanishes when δ is a multiple of 4 and is equal to 2 for other even δ, we may write, in view of (7)

$$E(4, 0, n) = \mu(2^\alpha) \sum_{\delta_1 | n_1} r_4(\delta_1)\, \mu(n_1/\delta_1).$$

Now, as in the proof of Theorem 5,

$$2 - r_4(\delta_1) = \lambda(\delta_1).$$

https://doi.org/10.4153/CJM-1955-038-5 Published online by Cambridge University Press

Hence, by (7) and (8),

$$\begin{aligned} E(4, 0, n) &= -\mu(2^\alpha)\sum_{\delta\mid n_1}(\lambda(\delta_1) - 2)\,\mu(n_1/\delta_1) \\ &= -\mu(2^\alpha)\,\lambda(n_1)\,\theta(n_1) \\ &= (-1)^{\alpha-1}\lambda(n)\,\mu(2^\alpha)\,\theta(n)\,2^{-\alpha}. \end{aligned}$$

Considering separately the cases $\alpha = 0$, $\alpha = 1$ and $\alpha > 1$, we have the results stated in the theorem.

6. The case $k = 6$. If we apply Theorem 1 we find

(14) $E(6, 5, n) = E(6, 0, n)$, $E(6, 4, n) = E(6, 1, n)$, $E(6, 3, n) = E(6, 2, n)$.

Since

(15) $$\phi(6, 0, n) + \phi(6, 1, n) = \phi(3, 0, n),$$

we have, by (4),

$$E(6, 0, n) + E(6, 1, n) = 2E(3, 0, n).$$

Hence by (6), (14), and (15), we have

$$E(6, 2, n) = -2E(3, 0, n),\ E(6, 1, n) = 2E(3, 0, n) - E(6, 0, n).$$

Thus it remains only to find $E(6, 0, n)$.

We have, as a special case of (11),

(16) $$E(6, 0, n) = \sum_{\delta\mid n} r_6(\delta)\,\mu(n/\delta).$$

Let us write $n = 2^\alpha 3^\beta m$ where m is prime to 6. We distinguish 5 cases.

Case I. $\alpha = 0, \beta = 0$. In this case the sum (16) extends over divisors δ which are prime to 6 so that

$$r_6(\delta) = 4r_3(\delta) - 3.$$

Since $n > 1$, we have

(17) $$E(6, 0, n) = 4\sum_{\delta\mid n} r_3(\delta)\,\mu(n/\delta) = 4E(3, 0, n).$$

Case II. $\alpha = 1, \beta = 0$. In this case we note that if h is even

(18) $$r_6(h) = 2r_3(\tfrac{1}{2}h).$$

Hence

$$\begin{aligned} E(6, 0, n) &= \sum_{\delta\mid\frac{1}{2}n}\{2r_3(\delta) - r_6(\delta)\}\,\mu(n/(2\delta)) \\ &= 2E(3, 0, \tfrac{1}{2}n) - E(6, 0, \tfrac{1}{2}n). \end{aligned}$$

Using case I we find

(19) $$E(6, 0, n) = -2E(3, 0, \tfrac{1}{2}n).$$

https://doi.org/10.4153/CJM-1955-038-5 Published online by Cambridge University Press

Case III. $\alpha \geqslant 2, \beta = 0$. In this case n/δ contains the factor 4 when δ is odd so that (16) has a contribution from only the even divisors δ. That is,

$$E(6, 0, n) = \sum_{\delta \mid \frac{1}{2}n} r_6(2\delta)\, \mu(n/(2\delta)) = 2E(3, 0, \tfrac{1}{2}n)$$

by (18).

Case IV. $\beta = 1$. Here we note that

$$r_6(3h) = 3r_2(h), \tag{20}$$

and write

$$\begin{aligned} E(6, 0, n) &= \sum_{\delta \mid \frac{1}{3}n} \{r_6(3\delta) - r_6(\delta)\}\, \mu(n/(3\delta)) \\ &= 3E(2, 0, \tfrac{1}{3}n) - E(6, 0, \tfrac{1}{3}n) \\ &= -\,E(6, 0, \tfrac{1}{3}n). \end{aligned}$$

Thus case IV reduces to one of the preceding cases.

Case V. $\beta \geqslant 2$. In this case n/δ contains the factor 9 when δ is not a multiple of 3, so that (16) becomes

$$E(6, 0, n) = \sum_{\delta \mid \frac{1}{3}n} r_6(3\delta)\, \mu(n/(3\delta)) = 3E(2, 0, \tfrac{1}{3}n) = 0,$$

in view of (20). Summing up the results of the 5 cases and applying Theorem 5 we have

THEOREM 7. *Let $n > 6$ be a non-exceptional number with respect to 6. Write $n = 2^\alpha 3^\beta n_1$ where n_1 is prime to 6. Then*

$$E(6, 0, n) = 2\mu^2(3^\beta)\, \frac{1 + 5\mu(2^\alpha)}{1 - 7\mu(2^\alpha)}\, \lambda(n)\, \theta(n_1).$$

We see that the non-zero values of $|E(6, q, n)|$ are powers of 2 as in the cases $k = 3, 4$.

7. Additional explicit formulas. Explicit formulas for $E(k, q, n)$ in case $\phi(k) > 2$ are in general lacking. We may remark, however, that

$$\begin{aligned} E(12, 2, n) &= 3E(4, 0, n) - 2E(6, 0, n) = E(12, 9, n) \\ E(12, 3, n) &= 4E(3, 0, n) - 3E(4, 0, n) = E(12, 8, n), \end{aligned}$$

so that $E(12, q, n)$ may be evaluated explicitly in the four cases $q = 2, 3, 8, 9$.

The case where n is a product of distinct primes of the form $kx - 1$ is however capable of treatment. In fact we have the following theorem.

THEOREM 8. *If n is the product of distinct primes of the form $kx - 1$ then:*

$$\begin{aligned} E(k, 0, n) &= E(k, k - 1, n) = \tfrac{1}{2}(2 - k)\, \mu(n)\, \theta(n) \\ E(k, 1, n) &= E(k, 2, n) = \ldots = E(k, k - 2, n) = \mu(n)\, \theta(n). \end{aligned}$$

https://doi.org/10.4153/CJM-1955-038-5 Published online by Cambridge University Press

Proof. Since every prime factor of n is of the form $kx - 1$, every divisor δ of n is of the form

$$\delta = m_\delta k + \mu(\delta), \tag{21}$$

where m_δ is an integer $\geqslant 0$.

If $q = 0$ then (9) gives

$$\begin{aligned} E(k, 0, n) &= \sum_{\delta | n} \mu(n/\delta)\left\{\delta - k\left[\frac{\delta}{k}\right]\right\} \\ &= \sum_{\delta | n} \mu(n/\delta)\{\delta - k(m_\delta + \tfrac{1}{2}(\mu(\delta) - 1))\} \\ &= \sum_{\delta | n} \mu(n/\delta)\{\mu(\delta) - \tfrac{1}{2}k\mu(\delta)\} \\ &= \mu(n)\,\theta(n)(1 - \tfrac{1}{2}k). \end{aligned}$$

By Theorem 1, $E(k, k-1, n) = E(k, 0, n)$. If now $0 < q < k - 1$, we may show that

$$\left[\frac{q\delta}{k}\right] - \left[\frac{(q+1)\delta}{k}\right]$$

is not a function of q as follows. By (21)

$$\left[\frac{q\delta}{k}\right] = \left[qm_\delta + \frac{q\mu(\delta)}{k}\right] = qm_\delta + \tfrac{1}{2}(\mu(\delta) - 1),$$

$$\left[\frac{(q+1)\delta}{k}\right] = \left[qm_\delta + m_\delta + \frac{(q+1)\,\mu(\delta)}{k}\right] = qm_\delta + m_\delta + \tfrac{1}{2}(\mu(\delta) - 1).$$

Hence

$$\left[\frac{(q+1)\delta}{k}\right] - \left[\frac{q\delta}{k}\right] = m_\delta$$

is not a function of q. Therefore by (9)

$$E(k, 1, n) = E(k, 2, n) = \ldots = E(k, k-2, n).$$

To find this common value we need only use the fact that the sum of all the E's is zero. Thus

$$(k-2)\,E(k, 1, n) + 2E(k, 0, n) = 0,$$

that is,

$$(k-2)\,E(k, 1, n) = 2(\tfrac{1}{2}k - 1)\,\mu(n)\,\theta(n)$$

or

$$E(k, 1, n) = \mu(n)\,\theta(n).$$

Thus the proof is complete.

The explicit values obtained above for $E(k, 0, n)$ show that for an infinity of k and n, $|E| \neq 0$ and for these values

$$E(k, 0, n) \neq o(\theta(n)),$$

as $\theta(n) \to \infty$. This contradicts a conjecture of Erdös. Vijayaraghavan **(5)** showed the invalidity of the conjecture by a different argument in 1951.

8. General estimates. On the other hand we give some general results which show that totatives are, after all, fairly evenly distributed. Thus the following theorem shows that any two ϕ's do not differ by as much as $\theta(n) = O(n^\epsilon)$ for any k.

THEOREM 9. $|\phi(k, q_1, n) - \phi(k, q_2, n)| \leqslant \theta(n)$.

Proof. Denote by $\{q_1, q_2\}$ the expression

$$[(q_1 + 1)\,\delta/k] - [q_1\,\delta/k] - [\delta/k] - [(q_2 + 1)\,\delta/k] + [q_2\,\delta/k] + [\delta/k].$$

For any real x, y the function

$$[x + y] - [x] - [y]$$

takes on the values 0 or 1. Hence $\{q_1, q_2\}$ takes on only 0, 1 or -1.

But by (10),

$$\phi(k, q_1, n) - \phi(k, q_2, n) = \sum_{\delta \mid n}{}' \mu(n/\delta)\{q_1, q_2\},$$

where the dash indicates that the summation extends over those divisors δ of n for which $\mu(n/\delta) \neq 0$. Hence

$$|\phi(k, q_1, n) - \phi(k, q_2, n)| \leqslant \sum_{\delta \mid n}{}' |\mu(n/\delta)|\,|\{q_1, q_2\}| \leqslant \sum_{\delta \mid n}{}' 1 = \theta(n).$$

As a consequence of Theorem 9 we have

THEOREM 10. *For every* q, $|E(k, q, n)| \leqslant (k - 1)\,\theta(n)$.

Proof.

$$|E(k, q, n)| = |\phi(n) - k\phi(k, q, n)| = \left|\sum_{q_1=0}^{k-1} \{\phi(k, q_1, n) - \phi(k, q, n)\}\right|$$
$$\leqslant \sum_{\substack{q_1=0 \\ q_1 \neq q}}^{k-1} |\phi(k, q_1, n) - \phi(k, q, n)| \leqslant (k - 1)\,\theta(n).$$

As a corollary we have

$$\frac{\phi(n) - (k - 1)\,\theta(n)}{k} < \phi(k, q, n) < \frac{\phi(n) + (k - 1)\,\theta(n)}{k},$$

uniformly in q. For $q = 0$ we have the stronger statement,

$$\frac{\phi(n)}{k} - \tfrac{1}{2}\,\theta(n) < \phi(k, 0, n) < \frac{\phi(n)}{k} + \tfrac{1}{2}\,\theta(n). \tag{22}$$

In fact, by (10),

$$\phi(k, 0, n) = \sum_{\delta \mid n} \mu(n/\delta)\left[\frac{\delta}{k}\right]$$
$$= \frac{1}{k}\sum_{\delta \mid n} \delta\mu(n/\delta) - \sum_{\delta \mid n} \mu(n/\delta)\left\{\frac{\delta}{k} - \left[\frac{\delta}{k}\right]\right\} = \frac{\phi(n)}{k} - S.$$

Now

$$|S| < \sum_{\substack{\delta | n \\ \mu(n/\delta)=1}} \mu(n/\delta) = \tfrac{1}{2}\,\theta(n).$$

From this (22) follows at once.

9. Applications. We conclude with a few remarks about an application of the foregoing results.

Let $Q_n(x)$ denote the irreducible polynomial whose roots are the $\phi(n)$ primitive nth roots of unity. That is

$$Q_n(x) = \prod_{\tau} (x - \exp(2\pi i\tau/n))$$

or

$$Q_n(x) = \prod_{\tau \leqslant \frac{1}{2}n} (x^2 - 2x\cos(2\pi\tau/n) + 1). \tag{23}$$

We suppose that $n > 6$ and $x > 0$ and ask for inequalities for $Q_n(x)$. Since the factors of (23) are monotone increasing functions of τ, inequalities are easily obtained by subdividing the range $0 \leqslant \tau < \frac{1}{2}n$ into (for example) the four intervals

$$0 \leqslant \tau < \tfrac{1}{6}n,\ \tfrac{1}{6}n \leqslant \tau < \tfrac{1}{4}n,\ \tfrac{1}{4}n \leqslant \tau < \tfrac{1}{3}n,\ \tfrac{1}{3}n \leqslant \tau < \tfrac{1}{2}n$$

and counting the number of totatives in these intervals. These numbers are respectively:

$$\begin{aligned}
A &= \phi(6, 0, n),\\
B &= \phi(4, 0, n) - \phi(6, 0, n),\\
C &= \phi(3, 0, n) - \phi(4, 0, n),\\
D &= \phi(6, 2, n) = \tfrac{1}{2}\phi(n) - \phi(3, 0, n).
\end{aligned}$$

Thus we obtain the following inequalities:

$$Q_n(x) > (x-1)^{2A}(x^2 - x + 1)^B(x^2+1)^C(x^2+x+1)^D, \tag{24}$$

$$Q_n(x) < (x^2 - x + 1)^A(x^2+1)^B(x^2+x+1)^C(x+1)^{2D}. \tag{25}$$

Estimates for $A, B, C, D,$ may be obtained from (22) and give

$$\begin{aligned}
\tfrac{1}{6}\phi(n) - \tfrac{1}{2}\theta(n) &\leqslant A \leqslant \tfrac{1}{6}\phi(n) + \tfrac{1}{2}\theta(n),\\
\tfrac{1}{12}\phi(n) - \theta(n) &\leqslant B \leqslant \tfrac{1}{12}\phi(n) + \theta(n),\\
\tfrac{1}{12}\phi(n) - \theta(n) &\leqslant C \leqslant \tfrac{1}{12}\phi(n) + \theta(n),\\
\tfrac{1}{6}\phi(n) - \tfrac{1}{2}\theta(n) &\leqslant D \leqslant \tfrac{1}{6}\phi(n) + \tfrac{1}{2}\theta(n).
\end{aligned}$$

Sharper inequalities, especially for certain types of n, can be obtained from (24) and (25) by applying Theorems 2, 4, 5, 6, and 7. Similar results may be written down for $x < 0$. Such results are useful in discussing the existence of "characteristic prime factors" of $a^n - b^n$, Lucas's functions and their generalizations **(2)**. Of course any such inequalities will not give the asymptotically correct result:

$$Q_n(x) = x^{\phi(n)}(1 - \mu(n)x^{-1} + O(x^{-2})) \qquad (x \to \infty).$$

Their utility lies in the direction of actual inequalities for a fixed value of x.

https://doi.org/10.4153/CJM-1955-038-5 Published online by Cambridge University Press

References

1. A. M. Legendre, *Essai sur la théorie des nombres* (2nd ed., Paris, 1808).

2. D. H. Lehmer, *On the converse of Fermat's theorem* II, Amer. Math. Monthly, *56* (1949), 304–306.

3. J. Liouville, *Sur quelques fonctions numériques*, J. de Math (2), *2* (1857), 244–248.

4. J. G. van der Corput and J. C. Kluyver, *Vraagstuk* CXCII, Wiskunde Opgaven, *11* (1912–14), 483–488.

5. T. Vijayaraghavan, *On a problem in elementary number theory*, J. Indian Math. Soc., *15* (1951), 51–56.

University of California

https://doi.org/10.4153/CJM-1955-038-5 Published online by Cambridge University Press