Canad. Math. Bull. Vol. **48** (2), 2005 pp. 211–220

The Distribution of Totatives

Jam Germain

Abstract. The integers coprime to n are called the *totatives* of n. D. H. Lehmer and Paul Erdős were interested in understanding when the number of totatives between in/k and $(i+1)n/k$ are $1/k$th of the total number of totatives up to n. They provided criteria in various cases. Here we give an "if and only if" criterion which allows us to recover most of the previous results in this literature and to go beyond, as well to reformulate the problem in terms of combinatorial group theory. Our criterion is that the above holds if and only if for every odd character $\chi \pmod{\kappa}$ (where $\kappa := k/\gcd(k, n/\prod_{p|n} p)$) there exists a prime $p = p_\chi$ dividing n for which $\chi(p) = 1$.

1 Introduction

The integers coprime to n are called the *totatives* of n. D. H. Lehmer [4] was interested in understanding when

$$(1)_{n,k} \qquad \phi(n; l/k) = (l/k)\phi(n) \quad \text{for all integers } l \text{ in the range } 0 \le l \le k-1,$$

where

$$\phi(n; t) := \sum_{\substack{m \le tn \\ (m,n)=1}} 1.$$

If (1) holds then $\phi(n)/k = \phi(n; 1/k) \in \mathbb{Z}$ so k divides $\phi(n)$. Considerable effort has gone into determining when this is a sufficient condition as well as necessary (see [1–5]).

Here we shall obtain necessary and sufficient conditions for (1) to hold in terms of (a subset of) the prime factors of n.

Theorem 1.1 *Let $g = \gcd(k, n/\prod_{p|n} p)$. Then (1) holds if and only if for every character $\chi \pmod{k/g}$ with $\chi(-1) = -1$ there exists a prime $p = p_\chi$ dividing n for which $\chi(p) = 1$.*

We simplify our workings in section 2 by showing that it suffices to consider pairs n, k with n squarefree and $(n, k) = 1$. In section 3 we introduce characters and deduce our result from the fact that $L(1, \chi) \neq 0$ for all odd characters $\chi \pmod{k}$; in other words, this result depends on the fact that the product of these is non-zero, that is, that $h_1(k) \neq 0$, where $h_1(k)$ is the "first factor" of class number $h(k)$ of the cyclotomic field $\mathbb{Q}(\zeta_k)$; defined as the ratio $h_1(k) := h(k)/h_2(k)$ where $h_2(k)$ is the class number of $\mathbb{Q}(\zeta_k + \zeta_k^{-1})$, the maximal real subfield of $\mathbb{Q}(\zeta_k)$.

Received by the editors June17, 2003.
AMS subject classification: Primary: 11A05; secondary 11A07, 11A25, 20C99.

Carmichael's λ-function, $\lambda(n)$ is defined as the maximal order of an element in $(\mathbb{Z}/n\mathbb{Z})^*$. Thus $\lambda(n) = \text{lcm}[\lambda(p^a) : p^a|n]$, where $\lambda(p^a) = \phi(p^a)$ if p is odd or $p^a = 2$ or 4, and $\lambda(2^a) = 2^{a-2}$ for $a \geq 3$. Theorem 1.1 allows us to improve the condition "k divides $\phi(n)$".

Corollary 1.2 *If $(1)_{n,k}$ holds where $(k, 2n) = 1$ then k divides $\lambda(n)$.*

If n is prime then Theorem 1.1 requires $\chi(n) = 1$ for all odd $\chi \pmod k$; that is $n \equiv 1 \pmod k$. We have proved the well-known result [4]:

Corollary 1.3 *If $n = p$ is prime then $(1)_{p,k}$ holds if and only if $p \equiv 1 \pmod k$.*

Erdős [1] considered the case of $n = pq$ where p, q are distinct odd primes; Hall and Shiu [3] proved Erdős's conjecture that if $(1)_{pq,k}$ holds then either $p \equiv 1 \pmod k$, or $q \equiv 1 \pmod k$, or $pq \equiv -1 \pmod k$. In fact it is possible to give an exact criterion :

Corollary 1.4 *Let p and q be distinct odd primes. Then $(1)_{pq,k}$ holds if and only if $p \equiv 1 \pmod k$, or $q \equiv 1 \pmod k$, or $p^2 \equiv 1 \pmod k$ and $q \equiv -p \pmod k$.*

This is proved in section 4.

Define (n, k) to be a "primitive solution" if $(1)_{n,k}$ holds, $(n, k) = 1$, n is a squarefree and if $(1)_{N,K}$ holds where $N|n$ and $k|K$, then $n = N$ and $k = K$. We will see in section 2 that all solutions are easily derived from the primitive ones. Thus Corollary 1.4 may be rephrased as follows:

Corollary 1.4′ *If (pq, k) is a primitive solution, then $p^2 \equiv 1 \pmod k$ and $q \equiv -p \pmod k$.*

In section 5 we look at the problem where (n, k) is a primitive solution and n has at least three prime factors. This is rather more complicated. We prove the following result:

Corollary 1.5 *If (pqr, k) is a primitive solution with k odd, then either $pqr \equiv 1 \pmod k$ with $p^2 \equiv q^2 \equiv r^2 \equiv 1 \pmod k$ and $(p - 1, q - 1, r - 1, k) = 1$; or we can write $k = lm$ with $(l, m) = 1$ where $p \equiv qr \equiv -1 \pmod l$ and $r \equiv -q \pmod l$, and $p \equiv 1 \pmod m$, $q^2 \equiv r^2 \equiv -1 \pmod m$ and $r \equiv \pm q \pmod m$.*

In the solutions so far the orders of p, q and r mod k have all been 1, 2 or 4. As n is allowed more prime divisors these orders may increase, as well as the set of possibilities, making this all very complicated. We give an example with odd orders in section 6, and formulate a combinatorial group theory version of our problem.

https://doi.org/10.4153/CMB-2005-019-9 Published online by Cambridge University Press

2 Some Elementary Observations

We start by noting that

$$\phi(n,t) = \sum_{m\le tn}\sum_{\substack{d|m\\ d|n}}\mu(d) = \sum_{d|n}\mu(d)\sum_{\substack{m\le tn\\ d|m}}1$$
$$= \sum_{d|n}\mu(d)\Big[\frac{tn}{d}\Big],$$

whereas $t\phi(n) = \sum_{d|n}\mu(d)tn/d$. Therefore,

$$\phi(n,t) - t\phi(n) = -\sum_{d|n}\mu(d)\Big\{\frac{tn}{d}\Big\} \tag{2.1}$$

where $\{u\} = u - [u]$. Thus $(1)_{n,k}$ is equivalent to

$$\sum_{d|n}\mu(d)\Big\{\frac{ln}{kd}\Big\} = 0 \tag{2.2}_{n,k,l}$$

for all integers l. We shall use the formula (2.2) to simplify the question, so we can work only with pairs n, k that are coprime, with n squarefree. Then (2.2) becomes, for $1 \le l \le k-1$,

$$\sum_{d|n}\mu(d)\Psi\Big(\frac{ln}{kd}\Big) = 0. \tag{2.3}_{n,k,l}$$

where

$$\Psi(z) = \begin{cases} 0 & \text{if } z \text{ is an integer,}\\ z - 1/2 & \text{otherwise.}\end{cases}$$

Proposition 2.1

(a) *If* $g = (k, n/\prod_{p|n}p)$ *then* $(1)_{n,k}$ *holds if and only if* $(1)_{n/g,k/g}$ *holds.*
(b) *If prime* p *does not divide* k *then* $(1)_{p^2n,k}$ *holds if and only if* $(1)_{pn,k}$ *holds.*
(c) *If* $(1)_{n,k}$ *holds then* $(1)_{mn,k}$ *holds*
(d) *If* $(1)_{n,k}$ *holds then* $(1)_{n,h}$ *holds for any integer* h *dividing* k.
(e) *If* p *divides* n *and* k, *but* p^2 *does not divide* n, *and* $(1)_{n,k}$ *holds then* $(1)_{n/p,k}$ *holds.*

As a consequence of Proposition 2.1 (a), (b), (e) we may determine all pairs n, k for which $(1)_{n,k}$ holds, simply by examining pairs with $\gcd(n,k) = 1$ and n squarefree. By Proposition 2.1 (c), (d) if (n,k) is a primitive solution then $(1)_{N,K}$ holds whenever $n|N$ and $K|k$.

https://doi.org/10.4153/CMB-2005-019-9 Published online by Cambridge University Press

Proof (a) If $p|n$ then $p|(n/g)$ so $\{d|n : \mu(d) \neq 0\} = \{d|(n/g) : \mu(d) \neq 0\}$. Therefore

$$\sum_{d|n} \mu(d)\Big\{\frac{ln}{kd}\Big\} = \sum_{d|(n/g)} \mu(d)\Big\{\frac{l(n/g)}{(k/g)d}\Big\}$$

so $(2.2)_{n,k,l}$ holds for all l if and only if $(2.2)_{n/g,k/g,l}$ holds for all l.

(b) Now $\{d|pn : \mu(d) \neq 0\} = \{d|p^2n : \mu(d) \neq 0\}$, so that

$$\sum_{d|p^2n} \mu(d)\Big\{\frac{l}{k}\frac{(p^2n)}{d}\Big\} = \sum_{d|pn} \mu(d)\Big\{\frac{pl}{k}\frac{(pn)}{d}\Big\} = \sum_{d|pn} \mu(d)\Big\{\frac{i}{k}\frac{pn}{d}\Big\}$$

where $i \equiv pl \pmod{k}$, since $(p,k) = 1$. Thus $(2.2)_{p^2n,k,l}$ holds for all l if and only if $(2.2)_{pn,k,i}$ holds for all i.

(c) Let $M = \prod_{p|m, p\not|n} p$ so that

$$\{d|mn : \mu(d) \neq 0\} = \{Dg : D|n \text{ and } g|M \text{ with } \mu(D) \neq 0 \text{ and } \mu(g) \neq 0\}.$$

Thus

$$\sum_{d|nm} \mu(d)\Big\{\frac{lnm}{kd}\Big\} = \sum_{g|M} \mu(g)\Big(\sum_{D|n} \mu(D)\Big\{\frac{l(m/g)}{k}\frac{n}{D}\Big\}\Big).$$

Now, by hypothesis $(2.2)_{n,k,l(m/g)}$ holds for each $g|M$ (which divides m), so the right side is 0, so $(2.2)_{nm,k,l}$ holds.

(d) By hypothesis $(2.2)_{n,k,l}$ holds for $l = i(k/h)$ for each i. But this is simply $(2.2)_{n,h,i}$ and so $(1)_{n,h}$ holds.

(e) Write $n = pm$ where $p \not| m$ so

$$\{d|n : \mu(d) \neq 0\} = \{d|m : \mu(d) \neq 0\} \cup \{pd : d|m \text{ and } \mu(d) \neq 0\}.$$

Therefore, by $(2.2)_{n,k,l,}$

$$\begin{aligned} 0 &= \sum_{d|m} \mu(d)\Big\{\frac{l}{k}\frac{(pm)}{d}\Big\} + \sum_{d|m} \mu(dp)\Big\{\frac{l}{k}\frac{pm}{pd}\Big\} \\ &= \sum_{d|m} \mu(d)\Big\{\frac{l}{k/p}\frac{m}{d}\Big\} - \sum_{d|m} \mu(d)\Big\{\frac{l}{k}\frac{m}{d}\Big\}. \end{aligned} \tag{2.4}$$

Now for a given j, $0 \leq j \leq k/p - 1$ consider the set of values $l = j + ik/p$, $0 \leq i \leq p - 1$.

https://doi.org/10.4153/CMB-2005-019-9 Published online by Cambridge University Press

Then

$$\left\{\frac{l}{k}\frac{m}{d}\right\} = \left\{\frac{j}{k}\frac{m}{d} + i\frac{m}{pd}\right\}.$$

Since $p \not| m$, so $p \not| m/d$, so this set of values is

$$\frac{1}{p}\left\{\frac{pmj}{kd}\right\} + \frac{h}{p} \quad \text{for } 0 \le h \le p-1.$$

Therefore taking these values in (2.3) and summing,

$$\begin{aligned} p\sum_{d|m}\mu(d)\left\{\frac{j}{k/p}\frac{m}{d}\right\} &= \sum_{i=0}^{p-1}\sum_{d|m}\mu(d)\left\{\frac{(j+ik/p)}{k}\frac{m}{d}\right\} \\ &= \sum_{d|m}\mu(d)\left(\sum_{h=0}^{p-1}\frac{1}{p}\left\{\frac{pmj}{kd}\right\} + \frac{h}{p}\right) \\ &= \sum_{d|m}\mu(d)\left\{\frac{j}{k/p}\frac{m}{d}\right\}, \end{aligned}$$

and thus this equals 0. That is $(2.2)_{n/p,k/p,j}$ holds for each j, and thus $(2.2)_{n/p,k,j,}$ holds for each j by (2.4). ∎

3 The Main Idea

Let χ be a character $\pmod k$ with $\chi(-1) = -1$. Assume that $(n,k) = 1$, and n is squarefree. Then

$$\begin{aligned} (3.1)\qquad \sum_{\substack{j=1\\(j,k)=1}}^{k}\overline{\chi}(j)\left(\sum_{d|n}\mu(d)\Psi\left(\frac{jn}{kd}\right)\right) &= \sum_{d|n}\mu(d)\chi(n/d)\sum_{\substack{j=1\\(j,k)=1}}^{k}\overline{\chi}(jn/d)\Psi\left(\frac{jn}{dk}\right) \\ &= \sum_{d|n}\mu(d)\chi(n/d)\sum_{\substack{i=1\\(i,k)=1}}^{k}\overline{\chi}(i)\Psi\left(\frac{i}{k}\right) \end{aligned}$$

taking $i \equiv jn/d \pmod k$, and thus i runs over a reduced residue system (mod k).

By [6, Proposition 4.1, Theorem 4.2] and the functional equation (see [6, p. 35]), it is known that if χ is an odd primitive character (mod q) then

$$\frac{1}{q}\sum_{i=1}^{q}\chi(i)i = \frac{q}{i\pi\tau(\chi)}L(1,\chi)$$

where $\tau(\chi)$ is the Gauss sum associated with χ and $L(s,\chi)$ the Dirichlet L-function.

https://doi.org/10.4153/CMB-2005-019-9 Published online by Cambridge University Press

Now, for principal character χ_0 modulo prime p,

$$\begin{aligned}\frac{1}{pq}\sum_{j=1}^{pq}(\overline{\chi\chi_0})(j)j &= \frac{1}{pq}\Bigg(\sum_{j=1}^{pq}\overline{\chi}(j)j - \sum_{\substack{j=1\\ p\mid j}}^{pq}\overline{\chi}(j)j\Bigg)\\ &= \frac{1}{pq}\Bigg(\sum_{m=0}^{p-1}\sum_{i=1}^{q}\overline{\chi}(mq+i)(mq+i) - \sum_{i=1}^{q}\overline{\chi}(pi)pi\Bigg)\\ &= \frac{1}{pq}\Bigg(q\sum_{m=0}^{p-1}m\sum_{i=1}^{q}\overline{\chi}(i) + p\sum_{i=1}^{q}\overline{\chi}(i)i - p\overline{\chi}(p)\sum_{i=1}^{q}\overline{\chi}(i)i\Bigg)\\ &= \frac{1-\overline{\chi}(p)}{q}\sum_{i=1}^{q}\overline{\chi}(i)i.\end{aligned}$$

Therefore if σ is a primitive odd character (mod m), where m divides k, which induces a character χ (mod k), then

$$\begin{aligned}\sum_{\substack{i=1\\ (i,k)=1}}^{k}\overline{\chi}(i)\Psi\Big(\frac{i}{k}\Big) &= \prod_{p\mid k}(1-\overline{\sigma}(p))\sum_{i=1}^{m}\overline{\sigma}(i)\Psi\Big(\frac{i}{m}\Big)\\ &= \frac{m}{i\pi\tau(\sigma)}\prod_{p\mid k}\big(1-\overline{\sigma}(p)\big)L(1,\sigma).\end{aligned}$$

Since n is squarefree we also have

$$\sum_{d\mid n}\mu(d)\chi(n/d) = \prod_{p\mid n}(\chi(p)-1) = \chi(n)\prod_{p\mid n}\big(1-\overline{\sigma}(p)\big)$$

as $(n,k)=1$. Therefore, by (3.1), if χ is induced by σ (mod m) then

$$\sum_{j=1}^{k}\overline{\chi}(j)\Bigg(\sum_{d\mid n}\mu(d)\Psi\Big(\frac{jn}{kd}\Big)\Bigg) = \frac{m\sigma(n)}{i\pi\tau(\sigma)}\prod_{p\mid kn}\big(1-\overline{\sigma}(p)\big)L(1,\sigma). \tag{3.2}$$

We may invert this as follows: if $(l,k)=1$ then

$$\sum_{d\mid n}\mu(d)\Psi\Big(\frac{ln}{kd}\Big) = \frac{1}{\phi(k)}\sum_{m\mid k}\sum_{\substack{\sigma \,(\mathrm{mod}\, m)\\ \sigma \text{ primitive}\\ \sigma(-1)=-1}}\frac{m\sigma(ln)}{i\pi\tau(\sigma)}\prod_{p\mid kn}\big(1-\overline{\sigma}(p)\big)L(1,\sigma). \tag{3.3}$$

From (3.2) and (3.3) we then deduce, since $\sigma(ln)L(1,\sigma)\neq 0$, the following:

https://doi.org/10.4153/CMB-2005-019-9 Published online by Cambridge University Press

Proposition 3.1 *If $(n,k)=1$ and n is squarefree then*

$$\sum_{d|n}\mu(d)\Psi\Big(\frac{ln}{kd}\Big)=0 \quad \textit{for all } l,\ 1\le l\le k \textit{ with } (l,k)=1$$

if and only if for each m dividing k and for every odd primitive character σ (mod m), there exists a prime p dividing kn for which

$$\sigma(p)=1.$$

Corollary 3.2 *If $(n,k)=1$ and n is squarefree then*

$$\sum_{d|n}\mu(d)\Psi\Big(\frac{ln}{kd}\Big)=0 \quad \textit{for all integers } l,$$

if and only if for every odd character χ (mod k), there exists a prime p dividing n for which $\chi(p)=1$.

Proof Since $(2.2)_{n,k,l}$ is the same as $(2.2)_{n,k/g,l/g}$ where $g=\gcd(k,l)$, thus $(2.2)_{n,k,l}$ holds for all l if and only if $(2.2)_{n,K,L}$ holds for every K dividing k and every integer L with $(L,k)=1$. By Proposition 3.1, this is equivalent to stating that for every m dividing K, for every odd primitive character σ (mod m) we have prime p dividing Kn for which $\sigma(p)=1$. Taking $K=m$ we see we must have such a prime p dividing mn. Thus p divides n; else if p divides m then $\sigma(p)=0$. Therefore $(p,k)=1$, so if χ (mod k) is induced by σ, then $\chi(p)=\sigma(p)=1$. ∎

Proof of Theorem 1.1 By Proposition 2.1(a) and (b) it suffices to prove this assuming n is squarefree (since $p|n$ if and only $p|(n/g)$, by definition). Let $N=n/(k,n)$. Then $(1)_{n,k}$ holds if and only if $(1)_{N,k}$ holds by Proposition 2.1(e) and (c). Note that $(N,k)=1$ and N is squarefree. By Corollary 3.2, we have that $(1)_{N,k}$ holds if and only if for each odd character χ (mod k) there exists a prime p dividing N for which $\chi(p)=1$. Now if prime q divides n but not N then q divides k, so $\chi(q)=0$. The result follows. ∎

4 Corollaries

Two Proofs of Corollary 1.4 (i) We may assume $p\not\equiv 1 \pmod k$ and $q\not\equiv 1 \pmod k$. After the result of Hall and Shiu [3]we may assume $pq\equiv -1 \pmod k$, so that $pq+1\equiv 0 \pmod k$ and so, for $1\le l\le k-1$,

$$\Big\{\frac{lpq}{k}\Big\}+\Big\{\frac{l}{k}\Big\}=1.$$

If $(1)_{pq,k}$ holds then $(2.2)_{pq,k,1}$ gives that

$$\Big\{\frac{p}{k}\Big\}+\Big\{\frac{q}{k}\Big\}=\Big\{\frac{pq}{k}\Big\}+\Big\{\frac{1}{k}\Big\}=1$$

https://doi.org/10.4153/CMB-2005-019-9 Published online by Cambridge University Press

and so $p+q \equiv 0 \pmod{k}$. On the other hand if $p+q \equiv 0 \pmod{k}$ then

$$\left\{\frac{lp}{k}\right\} + \left\{\frac{lq}{k}\right\} = 1$$

for $1 \leq l \leq k-1$, so $(2.2)_{pq,k,l}$ holds. Thus our criterion is $pq \equiv -1 \pmod{k}$ and $p+q \equiv 0 \pmod{k}$. This implies $p^2 \equiv p(-q) \equiv 1 \pmod{k}$; and if this holds then $p(p+q) = p^2 + pq \equiv 1 + (-1) \equiv 0 \pmod{k}$ so $p+q \equiv 0 \pmod{k}$ as $(p,k) = 1$.

(ii) In Theorem 1.1 we must have $g = 1$ as n is squarefree, so (1) holds if and only if for every odd $\chi \pmod{k}$ either $\chi(p) = 1$ or $\chi(q) = 1$. Now, either $\chi(p) = 1$ for all such χ (so $p \equiv 1 \pmod{k}$), or similarly $q \equiv 1 \pmod{k}$, or there exists odd characters χ_p,χ_q with $\chi_p(p) \neq 1$ (so $\chi_p(q) = 1$) and $\chi_q(q) \neq 1$ (so $\chi_q(p) = 1$). But $\chi_p^2\chi_q$ is an odd character and $(\chi_p^2\chi_q)(q) = \chi_q(q) \neq 1$, so $1 = (\chi_p^2\chi_q)(p) = \chi_p^2(p)$, and thus $\chi_p(p) = -1$. Similarly $\chi_q(q) = -1$. There is no odd χ such that $\chi(p) = \chi(q) = 1$, else $(\chi\chi_p\chi_q)(-1) = -1$ but $(\chi\chi_p\chi_q)(p) = \chi_p(p) \neq 1$ and $(\chi\chi_p\chi_q)(q) = \chi_q(q) \neq 1$. Therefore $\chi(p^2) = \chi(-pq) = 1$ for all odd χ, implying the result. ∎

Proof of Corollary 1.2 Suppose q^e divides k but not q^{e+1}, where $e \geq 1$. By hypothesis $q > 2$. Let χ be a character of maximal order $\pmod{q^e}$ so χ is odd. By Theorem 1.1, there exists prime p dividing n with $\chi(p) = 1$ so $p \equiv 1 \pmod{q^e}$. Therefore q^e divides $\lambda(n)$ and the result follows. ∎

5 Classifying When n Has a Fixed Number of Prime Factors

Suppose (n,k) is a primitive solution with k odd and $n = p_1 \cdots p_r$ where $p_1, \ldots, p_r$ are distinct primes. For each character $\chi \pmod{k}$ define

$$v_\chi = \big(\chi(p_1), \chi(p_2), \ldots, \chi(p_r)\big).$$

Let $G = \{v_\chi : \chi \text{ a character } \pmod{k}\}$ and $H = \{v_\chi \in G : \chi(-1) = -1\}$; we consider the elements of those sets without multiplicity. For each prime power $Q = q^e || k$, let χ_Q be a primitive character mod Q of order $\phi(Q)$, so that $v_{\chi_Q} \in H \subseteq G$. Note that $\chi_Q(p_i) = 1$ if and only if $p_i \equiv 1 \mod Q$. Let $R = \{v_{\chi_Q} : Q = q^e || k\}$. We have

$$R \subseteq H \quad \text{and} \quad G = \langle R \rangle,$$

where multiplication of vectors is defined componentwise, that is if $u = vw$ then $u_i = v_i w_i$ for each i where u_i is the ith component of u. Note that $(1,1,\ldots,1) \notin R$ since (n,k) is primitive. By the conditions in Theorem 1.1, and since (n,k) is primitive, we have

(i) For all $w \in H$, there exists i, $1 \leq i \leq r$ with $w_i = 1$;
(ii) For all i, $1 \leq i \leq r$ there exists $w \in H$, with $w_i = 1$, but $w_j \neq 1$ when $j \neq i$.

Thus our problem can be made "abstract" as follows: for each integer $r \geq 2$ we wish to find all groups G of r-dimensional vectors, whose entries are roots of unity, such that

https://doi.org/10.4153/CMB-2005-019-9 Published online by Cambridge University Press

- There exists $H \subseteq G$ where either $H = G$ or there exists a subgroup G^+ of G of index 2 with $H = G \backslash G^+$.
- G is generated by a subset R of H, where $1 \notin R$
- Properties (i) and (ii) hold.

6 Examples When n Has a Fixed Number of Prime Factors

$r = 2$: By (ii) there exists $w_1, w_2 \in H$ of the form $w_1 = (1, \alpha), w_2 = (\beta, 1)$ with $\alpha, \beta \neq 1$. Now $(\beta, \alpha^2) = w_2 w_1^2 \in H$, so $\alpha^2 = 1$ by (i), and thus $\alpha = -1$. Similarly $\beta = -1$. But then $R = H = \{(1, -1), (-1, 1)\}$. This is a reworking of the second proof of Corollary 1.4′ given above.

$r = 3$: By (ii) there exists $w_1, w_2, w_3 \in H$ with $w_{i,i} = 1$ and $w_{i,j} \neq 1$ for $j \neq i$. Now $w_1 w_2 w_3 \in H$ so $w_{1,i} w_{2,i} w_{3,i} = 1$ for some i, by (i). Re-arranging the ordinates if necessary we may assume this is true for $i = 3$, so $w_{1,3} = \gamma$ and $w_{2,3} = \overline{\gamma}$ for some $\gamma \neq 1$. But then $w_1^2 w_2 = (w_{2,1}, w_{1,2}^2, \gamma) \in H$ so $w_{1,2}^2 = 1$ by (i), and thus $w_{1,2} = -1$. Similarly $w_{2,1} = -1$, so our three vectors look like $w_1 = (1, -1, \gamma), w_2 = (-1, 1, \overline{\gamma})$ and $w_3 = (\alpha, \beta, 1)$ for some $\alpha, \beta, \gamma \neq 1$. Now $(\alpha, \beta, \gamma^2) = w_1^2 w_3 \in H$ so $\gamma^2 = 1$ by (i) and thus $\gamma = -1$. Also $(\alpha^2, -\beta^2, -1) = w_1 w_3^2, (-\alpha^2, \beta^2, -1) = w_2 w_3^2 \in H$, so $\alpha^2 = \beta^2 = 1$ or -1 by (i). Thus $w_1 = (1, -1, -1), w_2 = (-1, 1, -1)$, and there are several candidates for w_3, namely $u_1 = (-1, -1, 1), u_2 = (i, i, 1), u_3 = (i, -i, 1)$, where $i^2 = -1$. Now each of $w_2 u_2^3 u_3$, $w_2 u_1 u_2$ and $w_2 u_1 u_3$ fail (i), so no two u_i's belong to H. We claim that $H = \{w_1, w_2, u_1, (1, 1, 1)\}$ or $\{w_1, w_2, u_2, \overline{u}_2\}$ or $\{w_1, w_2, u_3, \overline{u}_3\}$, for if H contains any other elements we may reason as follows. If $(1, 1, 1) \in H$ then $u_1 = w_1 w_2 (1, 1, 1) \in H$. H cannot contain another vector $u = (1, \alpha, \beta)$, as may be seen by considering $u w_1 w_2, u^2 w_2, u^2 w_3, u w_2 w_3$, and $u w_1 w_3 \in H$ in turn; similarly H cannot contain another vector $(\alpha, 1, \beta)$. If H contains another vector $u = (\alpha, \beta, 1)$ then as above $\alpha^2 = \beta^2 = 1$ so $u = -w_1$, or $-w_2$. Then $u(-u) w_3$ or $u w_2 w_3$ or $w_1 u w_3 \in H$ contradicts (i). Thus $R \subseteq \{u_1, w_1, w_2\}$ with $|R| \geq 2$, or $R = R_1 \cup R_2$ with $R_1 \subseteq \{w_1 w_2\}, R_2 \subseteq \{u_j, \overline{u}_j\}$ for $j = 2$ or 3 and $|R_1|, |R_2| \geq 1$. This proves Corollary 1.5.

$|G|$ odd : Let $G = H$ be generated by

$$R = \{u = (1, w, w, w), v = (w, 1, w, w^2)\} \quad \text{where } w = e^{2i\pi/3}.$$

This can be achieved with $n = 29 \times 79 \times 107 \times 191, k = 91$.

It is not hard to determine whether (n, k) is a primitive solution to $(1)_{n,k}$: First check that $(n, k) = 1$ and that k is squarefree. Next, for each prime q dividing n, verify that $(1)_{n/q,k}$ is false. Now for each prime p dividing $\phi(n)/k$, verify that $(1)_{n,pk}$ is false. For example, $(29 \times 79 \times 107 \times 191, 91)$ is thus proved to be primitive.

It remains an open question in combinatorial group theory to determine all of the possibilities for G, H, R for a given r. Other than a laborious case-by-case analysis we see no way to achieve a better understanding.

References

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

https://doi.org/10.4153/CMB-2005-019-9 Published online by Cambridge University Press

[2] P. Erdős *Remarks and corrections to my paper "Some remarks on a paper of McCarthy".* Canad. Math. Bull. **3**(1960), 127–129.
[3] R. R. Hall and P. Shiu *The distribution of totatives.* Canad. Math. Bull. **45**(2002), 109–114.
[4] D. H. Lehmer *The distribution of totatives.* Canad. J. Math. **7**(1955), 347–357.
[5] P. J. McCarthy *Note on the distribution of the totatives.* Amer. Math. Monthly **64**(1957), 585–586.
[6] L. C. Washington *Introduction to cyclotomic fields.* Graduate Texts in Mathematics 83, Springer-Verlag, New York, 1982.

Département de Mathématiques et statistique
Université de Montréal
CP 6128 succ. Centre-Ville
Montréal, QC
H3C 3J7
e-mail: germain@dms.umontreal.ca