IJMMS 26:10 (2001) 589–596
PII. S0161171201006123
http://ijmms.hindawi.com

ARITHMETIC PROGRESSIONS THAT CONSIST ONLY OF REDUCED RESIDUES

PAUL A. TANNER III

(Received 13 June 2000 and in revised form 25 February 2001)

Abstract. This paper contains an elementary derivation of formulas for multiplicative functions of m which exactly yield the following numbers: the number of distinct arithmetic progressions of w reduced residues modulo m; the number of the same with first term n; the number of the same with mean n; the number of the same with common difference n. With m and odd w fixed, the values of the first two of the last three functions are fixed and equal for all n relatively prime to m; other similar relations exist among these three functions.

2000 Mathematics Subject Classification. 11A07, 11A41.

1. Introduction. Consider this definition: in modulo m, where $(a_j)_{j=1}^{w}$ and $(b_j)_{j=1}^{w}$ are arithmetic progressions of w residues, $(a_j)_{j=1}^{w}$ and $(b_j)_{j=1}^{w}$ are distinct if and only if $a_j \not\equiv b_j$ for some j. (To illustrate, (1,2,3) and (−9,7,23) are not distinct in modulo 5.) What is the number of distinct arithmetic progressions of w reduced residues modulo m? For $w = 1$, there are $\phi(m)$ such progressions, where ϕ is the Euler phi function. For $m = 5$ and $w = 3$, there are 12 such progressions: $\{(1,2,3),(1,4,7),(1,6,11),(2,3,4),(2,4,6),(2,7,12),(3,6,9),(3,7,11),(3,8,13),(4,6,8),(4,8,12),(4,9,14)\}$. (In Section 2, it is explained how this set is representative of all distinct arithmetic progressions of 3 reduced residues modulo 5.) The answers to this and similar questions are the findings of this paper. Part of the derivation mentioned in the abstract proceeds similarly to a standard 4-step derivation [1, Theorems 6.2–6.5] of a formula for ϕ. (Theorems 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10, 3.11, 3.12, 3.14, 3.15, 3.16, and 3.17 encompass these 4 steps. This is the motivation for grouping these 16 theorems into 4 collections.) The definitions are grouped together at the beginning so that after surveying the definitions, the reader can study the main results, Theorems 3.14, 3.15, 3.16, 3.17, 3.18, 3.20, and Corollary 3.19. Theorems 3.15, 3.16, 3.17, 3.18, and 3.20 give the formulas delineated in the abstract (Theorem 3.20 derives from Theorem 3.18 which derives from the sequence of Theorems 3.1, 3.5, 3.9, and 3.14). Parts (i), (ii), and (iii) of the corollary identify when the functions of Theorems 3.15, 3.16, 3.17, and 3.18 yield the same value. When studying this corollary, a question to consider is how it relates to the distribution of the integers relatively prime to m. (Notice that in the example above with 12 members, the first terms initiate the same number of progressions, and that in the given instances in the definitions section (Section 2), all of the functions have the same value.)

2. Definitions. All variables are positive integers except z which is an integer, p is a prime. The residue class multiplication table modulo p is the $p\times p$ matrix whose xth column for $x\le p$ is the sequence $\{[jx]\}_{j=1}^{p}$ (use $[z]=[jx]$ for some nonnegative $z<p$). A w-string modulo p is a sequence of the form $\{[jx]\}_{j=1}^{w}$. The w-string matrix modulo p is the $w\times p$ matrix whose xth column for $x\le p$ is the w-string $\{[jx]\}_{j=1}^{w}$. (This matrix is just the first w rows of the residue class multiplication table modulo p. If $w>p$ then we cycle through this table until w rows are obtained.) $|X|$ is the order of finite set X. The introduction defines distinct arithmetic progressions of w residues modulo m. We define α as an arithmetic progression of w reduced residues modulo m.

$$\begin{aligned} H_{m,w}=\{(n,x)\mid n\le m, x\le m, (n+jx,m)=(m,n)=1,\\ j=1,2,3,\dots,v, w=v+1\}. \end{aligned} \tag{2.1}$$

For each $w>1$, we define a function ρ_w as $\rho_w(m)=|H_{m,w}|$. Define $\rho_1(m)=\phi(m)$. Note that $\rho_w(m)$ is the number of distinct α, since for any arithmetic progression of $w>1$ integers relatively prime to m, the first term and common difference respectively are congruent modulo m to some n and x such that $(n,x)\in H_{m,w}$.

$$\begin{aligned} F_{m,n,w}&=\{x\mid x\le m, (n+jx,m)=1, j=1,2,3,\dots,w\},\\ F^{+}_{m,n,w}&=\{z\mid z\equiv x(\operatorname{mod} m)\text{ for some }x\in F_{m,n,w}\}. \end{aligned} \tag{2.2}$$

For each n,w, we define a function $\upsilon_{n,w}$ as $\upsilon_{n,w}(m)=|F_{m,n,w}|$. For $w>1$, $\upsilon_{n,w}(m)$ is the number of distinct α such that n is less than the first term of each progression by its common difference. For instance, $\upsilon_{3,4}(7)=3$: $\{(6,9,12,15),(8,13,18,23),(10,17,24,31)\}$.

$$\begin{aligned} F^{O}_{m,n,w}&=\{x\mid x\le m, (n-jx,m)=(n+jx,m)=(m,n)=1, j=1,2,3,\dots,v, w=2v+1\},\\ F^{O+}_{m,n,w}&=\{z\mid z\equiv x(\operatorname{mod} m)\text{ for some }x\in F^{O}_{m,n,w}\}. \end{aligned} \tag{2.3}$$

For each odd $w>1$ and by letting $(m,n)=1$, we define a function $\upsilon^{O}_{n,w}$ as $\upsilon^{O}_{n,w}(m)=|F^{O}_{m,n,w}|$. We also define $\upsilon^{O}_{n,1}(m)=1$. For odd w, $\upsilon^{O}_{n,w}(m)$ is the number of distinct α with mean n. For instance, $\upsilon^{O}_{4,5}(7)=3$: $\{(2,3,4,5,6),(-8,-2,4,10,16),(-10,-3,4,11,18)\}$.

$$\begin{aligned} F^{E}_{m,n,w}&=\{x\mid x\le m, (n-(2j-1)x,m)=(n+(2j-1)x,m)=1, j=1,2,3,\dots,v, w=2v\},\\ F^{E+}_{m,n,w}&=\{z\mid z\equiv x(\operatorname{mod} m)\text{ for some }x\in F^{E}_{m,n,w}\}. \end{aligned} \tag{2.4}$$

For each n and even w, we define a function $\upsilon^{E}_{n,w}$ as $\upsilon^{E}_{n,w}(m)=|F^{E}_{m,n,w}|$. For even w, $\upsilon^{E}_{n,w}(m)$ is the number of distinct α with mean n. For instance, $\upsilon^{E}_{2,4}(7)=3$: $\{(-1,1,3,5),(-16,-4,8,20),(-19,-5,9,23)\}$.

$$\begin{aligned} G_{m,n,w}&=\{x\mid x\le m, (x+(j-1)n,m)=1, j=1,2,3,\dots,w\},\\ G^{+}_{m,n,w}&=\{z\mid z\equiv x(\operatorname{mod} m)\text{ for some }x\in G_{m,n,w}\}. \end{aligned} \tag{2.5}$$

Table 2.1

[1]	[2]	[3]	[4]	[5]	[6]	[0]
[2]	[4]	[6]	[1]	[3]	[5]	[0]
[3]	[6]	[2]	[5]	[1]	[4]	[0]
[4]	[1]	[5]	[2]	[6]	[3]	[0]
[5]	[3]	[1]	[6]	[4]	[2]	[0]
[6]	[5]	[4]	[3]	[2]	[1]	[0]
[0]	[0]	[0]	[0]	[0]	[0]	[0]

For each n,w, we define a function $\kappa_{n,w}$ as $\kappa_{n,w}(m) = |G_{m,n,w}|$. For $w > 1$, $\kappa_{n,w}(m)$ is the number of distinct α with common difference n. For instance, $\kappa_{5,4}(7) = 3$: $\{(1,6,11,16),(3,8,13,18),(5,10,15,20)\}$.

$$F^*_{m,n,w} = \{x \mid x \le m, (n+jx,m) = (m,n) = 1, j = 1,2,3,\dots,v, w = v+1\}. \qquad (2.6)$$

For each $w > 1$ and by letting $(m,n) = 1$, we define a function $\upsilon^*_{n,w}$ as $\upsilon^*_{n,w}(m) = |F^*_{m,n,w}|$. We define $\upsilon^*_{n,1}(m) = 1$. Note that $\upsilon^*_{n,w}(m)$ is the number of distinct α with first term n. For instance, $\upsilon^*_{1,5}(7) = 3$: $\{(1,2,3,4,5),(1,5,9,13,17),(1,8,15,22,29)\}$.

For the sets defined in this paragraph, we select any n,w. We have $\{p_i\}_{i=1}^k$ as the distinct prime factors of $m = \prod_{i=1}^k p_i^{l_i}$, $\{q_a\}_{a=1}^{q'}$ as those p_i such that $(n,p_i) \ne 1$ and $p_i > w$. We also have $\{r_b\}_{b=1}^{r'}$ as those p_i such that $(n,p_i) = 1$ and $p_i > w$ and $\{s_c\}_{c=1}^{s'}$ as those p_i such that $p_i \ge w$. We have $\{t_d\}_{d=1}^{t'}$ as those p_i such that $(n,p_i) \ne 1$.

The proofs of Theorems 3.1, 3.2, 3.3, and 3.4 give the above instances $\upsilon_{3,4}(7)$, $\upsilon^O_{4,5}(7)$, $\upsilon^E_{2,4}(7)$, and $\kappa_{5,4}(7)$ by use of an example matrix, the residue class multiplication table modulo 7 as shown in Table 2.1.

3. Discussion

Theorem 3.1. *For any n,w,*

(i) $\upsilon_{n,w}(p) = p-w$ *if* $(n,p) = 1$ *and* $p > w$;

(ii) $\upsilon_{n,w}(p) = 1$ *if* $(n,p) = 1$ *and* $p \le w$;

(iii) $\upsilon_{n,w}(p) = p-1$ *if* $(n,p) \ne 1$ *and* $p > w$;

(iv) $\upsilon_{n,w}(p) = 0$ *if* $(n,p) \ne 1$ *and* $p \le w$.

Proof. Let $j \le w$, $x \le p$. Consider the following properties of the w-string matrix modulo p. In the jth row, those x satisfying $[p-n] = [jx]$ are precisely those x for which $(jx+n,p) \ne 1$, and those x satisfying $[p-n] \ne [jx]$ are precisely those x for which $(jx+n,p) = 1$. Since each column's first term is some $[x]$, those columns not containing $[p-n]$ identify exactly those x for which $(jx+n,p) = 1$, $j = 1,2,3,\dots,w$. For instance, in the example matrix with $n = 3$ and $w = 4$, those 3 columns not containing $[4]$ as one of the first 4 entries identify exactly those x for which $(jx+3,7) = 1$, $j = 1,2,3,4$. Hence, in the considered $w \times p$ matrix, $\upsilon_{n,w}(p)$ is the number of columns not containing $[p-n]$. Therefore, delete the columns containing $[p-n]$ and thereby construct formulas for the 4 particular cases of $\upsilon_{n,w}(p)$ as follows. Let $(n,p) = 1$. If $p > w$, then w columns contain $[p-n]$, which implies the formula $p-w$. Since all entries in the pth column are $[0]$, if $p \le w$, then $p-1$ columns contain $[p-n]$, which implies the formula $p-(p-1)=1$. Let $(n,p)\neq 1$ (and thus $[0]=[p-n]$). If $p>w$, then 1 column contains $[0]$, which implies the formula $p-1$. Since all entries in the pth row are $[0]$, if $p\leq w$, then all p columns contain $[0]$, which implies the formula $p-p=0$. □

Theorem 3.2. *For any w with $w=2v+1$ let $(n,p)=1$. Then*
(i) $v^{O}_{n,w}(p)=p-w+1$ *if* $p\geq w$;
(ii) $v^{O}_{n,w}(p)=1$ *if* $p<w$.

Proof. Let $j\leq v$, $x\leq p$. Consider the following properties of the v-string matrix modulo p. In the jth row, those x satisfying $[n]=[jx]$ or $[p-n]=[jx]$ are precisely those x for which $(jx-n,p)\neq 1$ or $(jx+n,p)\neq 1$, and those x satisfying $[n]\neq[jx]$ and $[p-n]\neq[jx]$ are precisely those x for which $(jx-n,p)=(jx+n,p)=1$. Since each column's first term is some $[x]$, those columns not containing $[n]$ or $[p-n]$ identify exactly those x for which $(jx-n,p)=(jx+n,p)=1$, $j=1,2,3,\dots,v$. For instance, in the example matrix with $n=4$ and $w=5$, those 3 columns not containing $[4]$ or $[3]$ as one of the first 2 entries identify exactly those x for which $(jx-4,7)=(jx+4,7)=1$, $j=1,2$. Hence, in the considered $v\times p$ matrix, $v^{O}_{n,w}(p)$ is the number of columns not containing $[n]$ or $[p-n]$. Therefore, delete the columns containing $[n]$ or $[p-n]$ and thereby construct formulas for the 2 particular cases of $v^{O}_{n,w}(p)$ as follows: if $p\geq w$, then v columns contain $[n]$, v columns contain $[p-n]$, and no one column contains both $[n]$ and $[p-n]$ (since in each of the first $p-1$ columns in the residue class multiplication table modulo p, the index of one of these entries exceeds v). Therefore $2v=w-1$ columns contain $[n]$ or $[p-n]$ which implies the formula $p-(w-1)=p-w+1$. Since all entries in the pth column are $[0]$, if $p<w$, then $p-1$ columns contain $[n]$ or $[p-n]$ which implies the formula $p-(p-1)=1$. □

Theorem 3.3. *For any n,w with $w=2v$,*
(i) $v^{E}_{n,w}(p)=p-w$ *if* $(n,p)=1$ *and* $p>w$;
(ii) $v^{E}_{n,w}(p)=1$ *if* $p=2$ *or if* p *is odd and* $(n,p)=1$ *and* $p<w$;
(iii) $v^{E}_{n,w}(p)=p-1$ *if* $(n,p)\neq 1$ *and* $p>w$;
(iv) $v^{E}_{n,w}(p)=0$ *if* p *is odd and* $(n,p)\neq 1$ *and* $p<w$.

Proof. Let $j\leq v$, $x\leq p$. For the w-string matrix modulo p, to consider only the odd-indexed entries in the columns, we eliminate the even-indexed rows. Consider the following properties of the resulting $v\times p$ matrix whose xth column is the sequence $\{[(2j-1)x]\}_{j=1}^{v}$. In the jth row, those x satisfying $[n]=[(2j-1)x]$ or $[p-n]=[(2j-1)x]$ are precisely those x for which $((2j-1)x-n,p)\neq 1$ or $((2j-1)x+n,p)\neq 1$, and those x satisfying $[n]\neq[(2j-1)x]$ and $[p-n]\neq[(2j-1)x]$ are precisely those x for which $((2j-1)x-n,p)=((2j-1)x+n,p)=1$. Since each column's first term is some $[x]$, those columns not containing $[n]$ or $[p-n]$ identify exactly those x for which $((2j-1)x-n,p)=((2j-1)x+n,p)=1$, $j=1,2,3,\dots,v$. For instance, in the example matrix with $n=2$ and $w=4$, those 3 columns not containing $[2]$ or $[5]$ as one of the first 2 odd-indexed entries identify exactly those x for which $((2j-1)x-2,7)=((2j-1)x+2,7)=1$, $j=1,2$. Hence, in the obtained $v\times p$ matrix, $v^{E}_{n,w}(p)$ is the number of columns not containing $[n]$ or $[p-n]$. Therefore, we delete the columns containing $[n]$ or $[p-n]$ and thereby construct formulas for the 4 particular cases of $\upsilon_{n,w}^E(p)$ as follows: let $p \neq 2$. Let $(n,p) = 1$. If $p > w$, then v columns contain $[n]$, v columns contain $[p-n]$, and no one column contains both $[n]$ and $[p-n]$ (since in each of the first $p-1$ columns in the residue class multiplication table modulo p, these entries are not both odd-indexed). Therefore $2v = w$ columns contain $[n]$ or $[p-n]$, which implies the formula $p-w$. Since all entries in the pth column are $[0]$, if $p < w$, then $p-1$ columns contain $[n]$ or $[p-n]$, which implies the formula $p-(p-1) = 1$. Let $(n,p) \neq 1$ (and thus $[0] = [n] = [p-n]$). If $p > w$, then 1 column contains $[0]$, which implies the formula $p-1$. Since all entries in the pth row are $[0]$, if $p < w$, then all p columns contain $[0]$, which implies the formula $p-p = 0$. If $p = 2$, then 1 column contains $[n]$ or $[p-n]$ for all n,w. This implies the formula $p-(p-1) = 1$. $\square$

Theorem 3.4. *For any n,w,*
(i) $\kappa_{n,w}(p) = p-w$ *if* $(n,p) = 1$ *and* $p > w$;
(ii) $\kappa_{n,w}(p) = 0$ *if* $(n,p) = 1$ *and* $p \leq w$;
(iii) $\kappa_{n,w}(p) = p-1$ *if* $(n,p) \neq 1$.

Proof. Let $j \leq w$, $x \leq p$, $y < p$. In the residue class multiplication table modulo p, consider the following properties of the row whose factor is $[y] = [n]$ if $(n,p) = 1$ or the row whose factor is $[1]$ if $(n,p) \neq 1$. Those x satisfying $[p-(j-1)n] = [x]$ for some j are precisely those x for which $(x+(j-1)n,p) \neq 1$ for some j, and those x satisfying $[p-(j-1)n] \neq [x]$ for $j = 1,2,3,\dots,w$ are precisely those x for which $(x+(j-1)n,p) = 1$, $j = 1,2,3,\dots,w$. For instance, in the example matrix with $n = 5$ and $w = 4$, those 3 entries (the first 3) in the fifth row not equal to $[7-(j-1)5]$ for $j = 1,2,3,4$ identify exactly those x for which $(x+(j-1)5,7) = 1$, $j = 1,2,3,4$. Hence, in the considered row, $\kappa_{n,w}(p)$ is the number of entries $[x]$ not equal to $[p-(j-1)n]$ for $j = 1,2,3,\dots,w$. Therefore delete those $[x]$ equal to $[p-(j-1)n]$ for some j, and thereby construct formulas for the 3 particular cases of $\kappa_{n,w}(p)$ as follows: let $(n,p) = 1$ and consider the row whose factor is $[y] = [n]$. If $p > w$, then the last w entries are equal to $[p-(j-1)n]$ for some j, which implies the formula $p-w$. If $p \leq w$ then all p entries are equal to $[p-(j-1)n]$ for some j, which implies the formula $p-p = 0$. Let $(n,p) \neq 1$ and consider the row whose factor is $[1]$. Then for all w, 1 entry is equal to $[p-(j-1)n] = [0]$ for some j, which implies the formula $p-1$. $\square$

Theorem 3.5. *For any n,w,*
(i) $\upsilon_{n,w}(p^l) = (p-w)p^{l-1}$ *if* $(n,p) = 1$ *and* $p > w$;
(ii) $\upsilon_{n,w}(p^l) = p^{l-1}$ *if* $(n,p) = 1$ *and* $p \leq w$;
(iii) $\upsilon_{n,w}(p^l) = (p-1)p^{l-1}$ *if* $(n,p) \neq 1$ *and* $p > w$;
(iv) $\upsilon_{n,w}(p^l) = 0$ *if* $(n,p) \neq 1$ *and* $p \leq w$.

Proof. Let $j \leq w$. The function $\upsilon_{n,w}(p^l)$ is the number of $x \in \{1,2,3,\dots,p^l\}$ remaining after deleting those x where $jx+n \equiv 0 \pmod p$ for some j. As x increases through the positive integers not exceeding p^l in their natural order, $\{[jx]\}_{j=1}^{w}$ cycles through the w-string matrix modulo p. By Theorem 3.1, with each such cycle there are w or $p-1$ or 1 or p distinct x where $jx+n \equiv 0 \pmod p$ for some j. There are p^{l-1} such cycles and therefore the stated formulas for the 4 specific cases of $\upsilon_{n,w}(p^l)$

are immediate:

(i) $p^l - wp^{l-1} = (p-w)p^{l-1}$;

(ii) $p^l - (p-1)p^{l-1} = p^{l-1}$;

(iii) $p^l - p^{l-1} = (p-1)p^{l-1}$;

(iv) $p^l - pp^{l-1} = 0$. □

Theorem 3.6. *For any w with $w = 2v+1$ let $(n,p) = 1$. Then*

(i) $\upsilon^O_{n,w}(p^l) = (p-w+1)p^{l-1}$ *if* $p \geq w$;

(ii) $\upsilon^O_{n,w}(p^l) = p^{l-1}$ *if* $p < w$.

Proof. Let $j \leq v$. The function $\upsilon^O_{n,w}(p^l)$ is the number of $x \in \{1,2,3,\ldots,p^l\}$ remaining after deleting those x where for some j, $jx - n \equiv 0 \pmod p$ or $jx + n \equiv 0 \pmod p$. As x increases through the positive integers not exceeding p^l in their natural order, $\{[jx]\}_{j=1}^{v}$ cycles through the v-string matrix modulo p. By Theorem 3.2, with each such cycle there are $w-1$ or $p-1$ distinct x where for some j, $jx - n \equiv 0 \pmod p$ or $jx + n \equiv 0 \pmod p$. There are p^{l-1} such cycles and therefore the stated formulas for the 2 specific cases of $\upsilon^O_{n,w}(p^l)$ are immediate:

(i) $p^l - (w-1)p^{l-1} = (p-w+1)p^{l-1}$;

(ii) $p^l - (p-1)p^{l-1} = p^{l-1}$. □

Theorem 3.7. *For any n,w with $w = 2v$,*

(i) $\upsilon^E_{n,w}(p^l) = (p-w)p^{l-1}$ *if* $(n,p) = 1$ *and* $p > w$;

(ii) $\upsilon^E_{n,w}(p^l) = p^{l-1}$ *if* $p = 2$ *or if* p *is odd and* $(n,p) = 1$ *and* $p < w$;

(iii) $\upsilon^E_{n,w}(p^l) = (p-1)p^{l-1}$ *if* $(n,p) \neq 1$ *and* $p > w$;

(iv) $\upsilon^E_{n,w}(p^l) = 0$ *if* p *is odd and* $(n,p) \neq 1$ *and* $p < w$.

Proof. Let $j \leq v$. The function $\upsilon^E_{n,w}(p^l)$ is the number of $x \in \{1,2,3,\ldots,p^l\}$ remaining after deleting those x such that for some j, $(2j-1)x - n \equiv 0 \pmod p$ or $(2j-1)x + n \equiv 0 \pmod p$. As x increases through the positive integers not exceeding p^l in their natural order, $\{[(2j-1)x]\}_{j=1}^{v}$ cycles through the $v \times p$ matrix considered in the proof of Theorem 3.3. By Theorem 3.3, with each such cycle there are w or $p-1$ or 1 or p distinct x such that for some j, $(2j-1)x - n \equiv 0 \pmod p$ or $(2j-1)x + n \equiv 0 \pmod p$. There are p^{l-1} such cycles and therefore the stated formulas for the 4 specific cases of $\upsilon^E_{n,w}(p^l)$ are immediate:

(i) $p^l - wp^{l-1} = (p-w)p^{l-1}$;

(ii) $p^l - (p-1)p^{l-1} = p^{l-1}$;

(iii) $p^l - p^{l-1} = (p-1)p^{l-1}$;

(iv) $p^l - pp^{l-1} = 0$. □

Theorem 3.8. *For any n,w,*

(i) $\kappa_{n,w}(p^l) = (p-w)p^{l-1}$ *if* $(n,p) = 1$ *and* $p > w$;

(ii) $\kappa_{n,w}(p^l) = 0$ *if* $(n,p) = 1$ *and* $p \leq w$;

(iii) $\kappa_{n,w}(p^l) = (p-1)p^{l-1}$ *if* $(n,p) \neq 1$.

Proof. Let $j \leq w$. The function $\kappa_{n,w}(p^l)$ is the number of $x \in \{1,2,3,\ldots,p^l\}$ remaining after deleting those x such that $x + (j-1)n \equiv 0 \pmod p$ for some j. As x increases through the positive integers not exceeding p^l in their natural order, $[x]$ cycles through the multiplication table row considered in the proof of Theorem 3.4.

By Theorem 3.4, with each such cycle there are w or p or 1 distinct x such that $x+(j-1)n \equiv 0 \pmod p$ for some j. There are p^{l-1} such cycles; therefore, the stated formulas for the 3 specific cases of $\kappa_{n,w}(p^l)$ are immediate:

(i) $p^l - wp^{l-1} = (p-w)p^{l-1}$;
(ii) $p^l - pp^{l-1} = 0$;
(iii) $p^l - p^{l-1} = (p-1)p^{l-1}$. □

Theorem 3.9. *The function $\upsilon_{n,w}(m)$ is multiplicative.*

Proof. We select any n,w and let $(m_1,m_2)=1$. We consider $F^+_{m_1,n,w}$, $F^+_{m_2,n,w}$, and $F^+_{m_1m_2,n,w}$ and choose any residue class modulo m_1 containing integers in the complement of $F^+_{m_1,n,w}$. No integer in this residue class is in $F^+_{m_1m_2,n,w}$. There are $\upsilon_{n,w}(m_1)$ residue classes modulo m_1 containing the integers in $F^+_{m_1,n,w}$, and we choose any such residue class. Since $(m_1,m_2)=1$, the m_2 least positive integers in this class form a complete residue system modulo m_2 [1, Theorem 3.6]. There are $\upsilon_{n,w}(m_2)$ integers in this residue system that are in $F^+_{m_2,n,w}$ and thus in $F^+_{m_1m_2,n,w}$. Since taking these $\upsilon_{n,w}(m_2)$ least positive integers in each of these $\upsilon_{n,w}(m_1)$ residue classes modulo m_1 forms $F_{m_1m_2,n,w}$, $\upsilon_{n,w}(m_1m_2)=\upsilon_{n,w}(m_1)\upsilon_{n,w}(m_2)$. □

Theorem 3.10. *The function $\upsilon^O_{n,w}(m)$ is multiplicative.*

Theorem 3.11. *The function $\upsilon^E_{n,w}(m)$ is multiplicative.*

Theorem 3.12. *The function $\kappa_{n,w}(m)$ is multiplicative.*

Proof of Theorems 3.10, 3.11, and 3.12. Employing the relevant restrictions on the variables n,w, prove Theorems 3.10, 3.11, and 3.12 along lines identical to that of Theorem 3.9's proof by making the appropriate substitutions with respectively $F^O_{m,n,w}, F^{O^+}_{m,n,w}, \upsilon^O_{n,w}(m)$; $F^E_{m,n,w}, F^{E^+}_{m,n,w}, \upsilon^E_{n,w}(m)$; $G_{m,n,w}, G^+_{m,n,w}, \kappa_{n,w}(m)$. □

Remark 3.13. For the following, we recall the convention that empty products have value 1.

Theorem 3.14. *For any n,w,*

(i) $\upsilon_{n,w}(m)=\prod_{a=1}^{q'}(q_a-1)\prod_{b=1}^{r'}(r_b-w)\prod_{i=1}^{k}p_i^{l_i-1}$ *if for any i, $(n,p_i)=1$ or $p_i>w$;*
(ii) $\upsilon_{n,w}(m)=0$ *if for some i, $(n,p_i)\neq 1$ and $p_i \le w$.*

Proof. By Theorems 3.5 and 3.9, $\upsilon_{n,w}(m)=\prod_{i=1}^{k}\upsilon_{n,w}(p_i^{l_i})$. Accordingly, we apply the appropriate definitions on the prime factors of m to obtain the stated formulas: case (i) of Theorem 3.14 covers cases (i), (ii), and (iii) of Theorem 3.5, and case (ii) of Theorem 3.14 covers case (iv) of Theorem 3.5. □

Theorem 3.15. *For any odd $w>1$ let $(m,n)=1$. Then $\upsilon^O_{n,w}(m)=\prod_{c=1}^{s'}(s_c-w+1)\prod_{i=1}^{k}p_i^{l_i-1}$.*

Proof. By Theorems 3.6 and 3.10, $\upsilon^O_{n,w}(m)=\prod_{i=1}^{k}\upsilon^O_{n,w}(p_i^{l_i})$. Accordingly, we apply the appropriate definitions on the prime factors of m to obtain the stated formula which covers both cases of Theorem 3.6. □

Theorem 3.16. *For any n and even w,*

(i) $\upsilon^E_{n,w}(m)=\prod_{a=1}^{q'}(q_a-1)\prod_{b=1}^{r'}(r_b-w)\prod_{i=1}^{k}p_i^{l_i-1}$ *if for any* i, $p_i=2$ *or* $(n,p_i)=1$ *or* $p_i\geq w$;

(ii) $\upsilon^E_{n,w}(m)=0$ *if for some* i, p_i *is odd and* $(n,p_i)\neq 1$ *and* $p_i<w$.

Proof. By Theorems 3.7 and 3.11, $\upsilon^E_{n,w}(m)=\prod_{i=1}^{k}\upsilon^E_{n,w}(p_i^{l_i})$. Accordingly, we apply the appropriate definitions on the prime factors of m to obtain the stated formulas: case (i) of Theorem 3.16 covers cases (i), (ii), and (iii) of Theorem 3.7, and case (ii) of Theorem 3.16 covers case (iv) of Theorem 3.7. □

Theorem 3.17. *For any* n,w,

(i) $\kappa_{n,w}(m)=\prod_{d=1}^{t'}(t_d-1)\prod_{b=1}^{r'}(r_b-w)\prod_{i=1}^{k}p_i^{l_i-1}$ *if for any* i, $(n,p_i)\neq 1$ *or* $p_i>w$;

(ii) $\kappa_{n,w}(m)=0$ *if for some* i, $(n,p_i)=1$ *and* $p_i\leq w$.

Proof. By Theorems 3.8 and 3.12, $\kappa_{n,w}(m)=\prod_{i=1}^{k}\kappa_{n,w}(p_i^{l_i})$. Accordingly, we apply the appropriate definitions on the prime factors of m to obtain the stated formulas: case (i) of Theorem 3.17 covers cases (i) and (iii) of Theorem 3.8, and case (ii) of Theorem 3.17 covers case (ii) of Theorem 3.8. □

Theorem 3.18. *For any* $w>1$ *let* $(m,n)=1$. *Then* $\upsilon^*_{n,w}(m)=\prod_{c=1}^{s'}(s_c-w+1)\prod_{i=1}^{k}p_i^{l_i-1}$.

Proof. $F^*_{m,n,w}=F_{m,n,w-1}$; therefore, $\upsilon^*_{n,w}(m)=\upsilon_{n,w-1}(m)$. Therefore, we apply the appropriate definitions on the prime factors of m to modify the formula of Theorem 3.14(i) and thus obtain the formula of Theorem 3.18. □

Corollary 3.19. *For parts (i), (ii), and (iii), select any* w *and let* $(m,n)=(m,n')=1$.

(i) $\upsilon^*_{n,w}(m)=\upsilon^*_{n',w}(m)$.

(ii) *If* w *is even, then*

$$\upsilon^*_{n,w+1}(m)=\upsilon^*_{n',w+1}(m)=\upsilon^O_{n,w+1}(m)=\upsilon^O_{n',w+1}(m)=\upsilon^E_{n,w}(m)=\upsilon^E_{n',w}(m). \tag{3.1}$$

(iii) *If each prime factor of* m *is greater than* w, *then*

$$\upsilon^*_{n,w+1}(m)=\upsilon^*_{n',w+1}(m)=\kappa_{n,w}(m)=\kappa_{n',w}(m). \tag{3.2}$$

Theorem 3.20. *For any* $w>1$, $\rho_w(m)=\phi(m)\upsilon^*_{n,w}(m)$.

Proof. For $(n,x)\in H_{m,w}$, there are $\phi(m)$ instances of n, and by Corollary 3.19(i), $\upsilon^*_{n,w}(m)$ instances of x for each n. Therefore, $\phi(m)\upsilon^*_{n,w}(m)=|H_{m,w}|$. □

References

[1] K. H. Rosen, *Elementary Number Theory and its Applications*, 3rd ed., Addison-Wesley Publishing, Massachusetts, 1993. MR 93i:11002. Zbl 766.11001.

Paul A. Tanner III: Department of Mathematics, University of South Florida, 4202 E. Fowler Avenue, Tampa, FL 33620, USA

E-mail address: ptanneri@tarski.math.usf.edu