# SIZE OF THE SET OF RESIDUES OF INTEGER POWERS OF FIXED EXPONENT 

RICHARD J. MATHAR


#### Abstract

The positive integers coprime to some integer $m$ generate the abelian group $(\mathbb{Z} / n \mathbb{Z})^{*}$ of multiplication modulo $m$. Admitting only integers of the form $n^{k}$ of a common fixed exponent $k$ defines a subgroup of this. We consider the order of this subgroup-which is divisor of Euler's multiplicative totient function $\varphi(m)$.

If the generating integers $n$ do not need to be coprime to $m$, semigroups of the integers of the format $n^{k}(\bmod m)$ are defined in an equivalent manner by multiplication modulo $m$. We show that the orders of these semigroups are multiplicative functions of $m$ for fixed exponent $k$, and derive linear recurrences and (conjectural) closed forms for the orders of these multiplicative functions if $m$ is a prime power.


## 1. Group of Multiplication Modulo m

1.1. Set of Totients. The number of integers coprime to some positive integer $m$ is counted by Euler's totient $\varphi(m)$ [9, A000010]:

Definition 1. (Euler's totient)

$$
\begin{equation*}
\varphi(m)=\#\{n:(n, m)=1,1 \leq n \leq m\} \tag{1}
\end{equation*}
$$

Definition 2. (.,.) denotes the greatest common divisor of the two arguments.
Theorem 1. [1, thm. 2.5] $\varphi$ is a multiplicative function of its argument.
1.2. Multiplicative Group with Totients. For some fixed modulus $m$, the elements of this set of totients $n_{i}$ with $\left(n_{i}, m\right)=1$ define an abelian group $(\mathbb{Z} / m \mathbb{Z})^{*}$ of multiplication modulo $m$ with the product rule

$$
\begin{equation*}
\left(n_{i} \quad \bmod m\right)\left(n_{j} \quad \bmod m\right)=\left(n_{i} n_{j}\right) \quad \bmod m \tag{2}
\end{equation*}
$$

1 is the unit element. The order of an element $n_{i}$ of this group is denoted by $\operatorname{ord}_{m}\left(n_{i}\right)$. From Euler's theorem of number theory [1, Thm. 5.17] (or the theory of groups of finite order $\varphi(m)$ ) it follows that the order is a divisor of $\varphi(m)$ [8, §3.2.2].

Example 1. The multiplication table of the group of multiplication modulo $m=10$ is Table 1 with $\operatorname{ord}_{10}(1)=1, \operatorname{ord}_{10}(3)=\operatorname{ord}_{10}(7)=4, \operatorname{ord}_{10}(9)=2$.

Example 2. The multiplication table of the group of multiplication modulo $m=20$ is Table 2 with $\operatorname{ord}_{20}(1)=1$, $\operatorname{ord}_{20}(3)=\operatorname{ord}_{20}(7)=\operatorname{ord}_{20}(13)=\operatorname{ord}_{20}(17)=4$, $\operatorname{ord}_{20}(9)=\operatorname{ord}_{20}(11)=\operatorname{ord}_{20}(19)=2$.

[^0]|  | 1 | 3 | 7 | 9 |
| :--- | :--- | :--- | :--- | :--- |
| 1 | 1 | 3 | 7 | 9 |
| 3 | 3 | 9 | 1 | 7 |
| 7 | 7 | 1 | 9 | 3 |
| 9 | 9 | 7 | 3 | 1 |

TABLE 1. Group of multiplication modulo 10 (Cayley table).

|  | 1 | 3 | 7 | 9 | 11 | 13 | 17 | 19 |
| ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: |
| 1 | 1 | 3 | 7 | 9 | 11 | 13 | 17 | 19 |
| 3 | 3 | 9 | 1 | 7 | 13 | 19 | 11 | 17 |
| 7 | 7 | 1 | 9 | 3 | 17 | 11 | 19 | 13 |
| 9 | 9 | 7 | 3 | 1 | 19 | 17 | 13 | 11 |
| 11 | 11 | 13 | 17 | 19 | 1 | 3 | 7 | 9 |
| 13 | 13 | 19 | 11 | 17 | 3 | 9 | 1 | 7 |
| 17 | 17 | 11 | 19 | 13 | 7 | 1 | 9 | 3 |
| 19 | 19 | 17 | 13 | 11 | 9 | 7 | 3 | 1 |

TABLE 2. Group of multiplication modulo 20 (Cayley table).

| $i \backslash k$ | 1 | 2 | 3 | 4 | $\ldots$ |  |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- |
| 1 | $n_{1}$ | $n_{1}^{2}$ | $\bmod m$ | $n_{1}^{3}$ | $\bmod m$ | $n_{1}^{4} \bmod m$ |
| 2 | $n_{2}$ | $n_{2}^{2} \bmod m$ | $n_{2}^{3} \bmod m$ | $n_{2}^{4} \bmod m$ | $\ldots$ |  |
| 3 | $n_{3}$ | $n_{3}^{2} \bmod m$ | $n_{3}^{3} \bmod m$ | $n_{3}^{4} \bmod m$ | $\ldots$ |  |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\ldots$ |  |
| $\varphi(m)$ | $n_{\varphi(m)}$ | $n_{\varphi(m)}^{2} \bmod m$ | $n_{\varphi(m)}^{3} \bmod m$ | $\ldots$ |  |  |

Table 3. Structure of the table of residues of $k$-th powers in the multiplicative group modulo $m$.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | $\ldots$ |
| ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | $\ldots$ |
| 2 | 4 | 3 | 1 | 2 | 4 | 3 | 1 | 2 | 4 | $\ldots$ |
| 3 | 4 | 2 | 1 | 3 | 4 | 2 | 1 | 3 | 4 | $\ldots$ |
| 4 | 1 | 4 | 1 | 4 | 1 | 4 | 1 | 4 | 1 | $\ldots$ |

Table 4. Table 3 for the modulus $m=5$.
1.3. Number of residues of $n_{i}^{k}(\bmod m)$. The powers of the elements $n_{i}$ of the group of multiplication modulo $m, n_{i}^{k}(\bmod m)$, can be arranged as in Table 3 . The table has $\varphi(m)$ rows labeled uniquely by the elements $n_{i}$, and columns labeled by the powers $k \geq 1$.

Example 3. The table of the $k$-powers of the elements of the multiplicative group modulo $m=5$ is shown in Table 4. The table of the $k$-powers of the elements of the multiplicative group modulo $m=10$ is shown in Table 5 .

Remark 1. As a result of the abelian structure, the sequences of integers in two rows of Table 3 which are inverses of each other (in the group) are given by inverting

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | $\ldots$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | $\ldots$ |
| 3 | 9 | 7 | 1 | 3 | 9 | 7 | 1 | 3 | 9 | $\ldots$ |
| 7 | 9 | 3 | 1 | 7 | 9 | 3 | 1 | 7 | 9 | $\ldots$ |
| 9 | 1 | 9 | 1 | 9 | 1 | 9 | 1 | 9 | 1 | $\ldots$ |

Table 5. Table 3 for the modulus $m=10$.
the left-right order or reading. This is equivalent to transversing the cycle graph of the group in the two opposite directions.
1.4. Group of residues of $n^{k} \bmod m$.

Theorem 2. The residues $n_{i}^{k}(\bmod m)$, the set of numbers in the $k$-th column of Table 3, are a subgroup $\left(\mathbb{Z} / n^{k} \mathbb{Z}\right)^{*}$ of the multiplicative group modulo $m$ :

$$
\begin{equation*}
\left(\mathbb{Z} / n^{k} \mathbb{Z}\right)^{*} \subset(\mathbb{Z} / n \mathbb{Z})^{*} \tag{3}
\end{equation*}
$$

Proof. For two elements $n_{i}^{k}(\bmod m)$ and $n_{j}^{k}(\bmod m)$ in the same column $k$ of the table, the product (defined with the multiplication in the group) is $\left(n_{i}^{k} \bmod m\right)\left(n_{j}^{k}\right.$ $\bmod m)=\left(n_{i} n_{j}\right)^{k} \bmod m$ according to (2). Because $n_{i} n_{j}$ is also an element in the group of multiplication modulo $m$, the $\left(n_{i} n_{j}\right)^{k} \bmod m$ is also somewhere in the $k$-th column (closure property [1, Thm. 6.4]). Furthermore the unit element of the group is in all columns of the table because $1^{k} \bmod m=1 \bmod m$.

The finite set of numbers in some fixed $k$-th column of Table 3 defines:
Definition 3. $N_{m}(k)$ is the number of distinct residues of the $k$-th powers of the elements in the multiplicative group modulo $m$, the order of $\left(\mathbb{Z} / n^{k} \mathbb{Z}\right)^{*}$.

$$
\begin{equation*}
N_{m}(k)=\#\left\{n^{k} \quad \bmod m:(n, m)=1 \wedge n \in \mathbb{Z}\right\}=\left|\left(\mathbb{Z} / n^{k} \mathbb{Z}\right)^{*}\right| \tag{4}
\end{equation*}
$$

A row in Table 3 is periodic with period length $\operatorname{ord}_{m}\left(n_{i}\right)$. The least common multiple (l.c.m.) of these orders of the rows, $\left[\operatorname{ord}_{m}\left(n_{1}\right), \operatorname{ord}_{m}\left(n_{2}\right), \ldots, \operatorname{ord}_{m}\left(n_{\varphi(m)}\right)\right]$, gives the period length of the entire table, and is known as Carmichael's $\lambda$-function [2, 6][9, A002322][5, Defn 2.20]. In consequence, $N_{m}(k)$ is a periodic function of $k$ with a period length given by $\lambda(m)$.

Example 4. In Table 5 the number of distinct elements in column $k$ are $N_{10}(1)=4$, $N_{10}(2)=2, N_{10}(3)=4, N_{10}(4)=1$, and periodic with $N_{10}(k+4)=N_{10}(k)$ thereafter. $\lambda(10)=4$.

Because the order of the subgroup in the $k$-th column of the table has been defined as $N_{m}(k)$, and because subgroup orders divide group orders by Lagrange's Theorem:

$$
\begin{equation*}
N_{m}(1)=\varphi(m) ; \quad N_{m}(k) \mid \varphi(m) \tag{5}
\end{equation*}
$$

If the exponent $k$ is composite with a proper divisor $d \mid k, 1<d<k$, one can "interrupt" the computation of the set of residues by computing first the residues $n^{d} \bmod m$, and then computing their $k / d$-th powers modulo $m$. Because in the latter step the number of residues cannot increase beyond the $N_{m}(k / d)$, we have:

$$
\begin{equation*}
N_{m}(k) \leq N_{m}(d), \quad d \mid k \tag{6}
\end{equation*}
$$

Even stronger, the residues $n^{k} \bmod m$ are a subgroup of the residues of $n^{d} \bmod m$ : The two subgroups of $\mathbb{Z} / m \mathbb{Z}$ share the unit element. Each $k$-th power can be written

| $k \backslash m$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | OEIS |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 1 | 1 | 1 | 2 | 2 | 4 | 2 | 6 | 4 | 6 | 4 | 10 | 4 | 12 | 6 | 8 | 8 | 16 | 6 | 18 | 8 | A000010 |
| 2 | 1 | 1 | 1 | 1 | 2 | 1 | 3 | 1 | 3 | 2 | 5 | 1 | 6 | 3 | 2 | 2 | 8 | 3 | 9 | 2 | A046073 |
| 3 | 1 | 1 | 2 | 2 | 4 | 2 | 2 | 4 | 2 | 4 | 10 | 4 | 4 | 2 | 8 | 8 | 16 | 2 | 6 | 8 | A087692 |
| 4 | 1 | 1 | 1 | 1 | 1 | 1 | 3 | 1 | 3 | 1 | 5 | 1 | 3 | 3 | 1 | 1 | 4 | 3 | 9 | 1 | A250207 |
| 5 | 1 | 1 | 2 | 2 | 4 | 2 | 6 | 4 | 6 | 4 | 2 | 4 | 12 | 6 | 8 | 8 | 16 | 6 | 18 | 8 | A293482 |
| 6 | 1 | 1 | 1 | 1 | 2 | 1 | 1 | 1 | 1 | 2 | 5 | 1 | 2 | 1 | 2 | 2 | 8 | 1 | 3 | 2 | A293483 |
| 7 | 1 | 1 | 2 | 2 | 4 | 2 | 6 | 4 | 6 | 4 | 10 | 4 | 12 | 6 | 8 | 8 | 16 | 6 | 18 | 8 | A293484 |
| 8 | 1 | 1 | 1 | 1 | 1 | 1 | 3 | 1 | 3 | 1 | 5 | 1 | 3 | 3 | 1 | 1 | 2 | 3 | 9 | 1 | A293485 |
| 9 | 1 | 1 | 2 | 2 | 4 | 2 | 2 | 4 | 2 | 4 | 10 | 4 | 4 | 2 | 8 | 8 | 16 | 2 | 2 | 8 |  |
| 10 | 1 | 1 | 1 | 1 | 2 | 1 | 3 | 1 | 3 | 2 | 1 | 1 | 6 | 3 | 2 | 2 | 8 | 3 | 9 | 2 |  |
| 11 | 1 | 1 | 2 | 2 | 4 | 2 | 6 | 4 | 6 | 4 | 10 | 4 | 12 | 6 | 8 | 8 | 16 | 6 | 18 | 8 |  |
| 12 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 5 | 1 | 1 | 1 | 1 | 1 | 4 | 1 | 3 | 1 |  |
| 13 | 1 | 1 | 2 | 2 | 4 | 2 | 6 | 4 | 6 | 4 | 10 | 4 | 12 | 6 | 8 | 8 | 16 | 6 | 18 | 8 |  |
| 14 |  | 1 | 1 | 1 | 2 | 1 | 3 | 1 | 3 | 2 | 5 | 1 | 6 | 3 | 2 | 2 | 8 | 3 | 9 | 2 |  |
|  | Table 6. Top corner of the table of $N_{m}(k)$, orders of the subgroups of the $k$-th powers of the elements of the multiplicative group modulo $m$, and their sequence numbers in the Online Encyclopedia of Integer Sequences [9]. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

as a $d$-th power, so $n \rightarrow n^{k / d}$ is a homomorphism between the two subgroups. Again by Lagrange's theorem

## Theorem 3.

$$
\begin{equation*}
N_{m}(k)\left|N_{m}(d), \quad d\right| k \tag{7}
\end{equation*}
$$

So far this characterizes the residue sets for fixed modulus $m$ and variable exponents $k$.
1.5. Multiplicative group order of $m$. For fixed $k$ and variable $m$, scanning Table 6 along rows, we find:

Theorem 4. For fixed exponent $k$ the orders $N_{m}(k)$ are multiplicative functions of $m$.

Proof. We need to show that for coprime $\left(m_{1}, m_{2}\right)$ the "size" (order of the set of elements) of column $k$ of two tables of the format of table 3 fulfills $N_{m_{1}}(k) N_{m_{2}}(k)=$ $N_{m_{1} m_{2}}(k)$. We do this by settling the numbers coprime to $m_{1}$ along rows and the numbers coprime to $m_{2}$ along columns of a two-dimensional $N_{m_{1}}(k) \times N_{m_{2}}(k)$ mapping array, and by showing that there is a 1-to-1 map of the products $m_{1} m_{2}$ to pairs of $m_{1}$ and $m_{2}$, which means, each $m_{1} m_{2}$ can be placed at exactly one entry of the array according to that map. If that association $m_{1} m_{2} \leftrightarrow m_{1}, m_{2}$ is indeed unique, the number of distinct elements in the group of order $N_{m_{1} m_{2}}(k)$ is obviously the product of the group orders $N_{m_{1}}(k)$ and $N_{m_{2}}(k)$, because in a rectangular array the number of entries is the product of the number of rows by the number of columns. The forward and backward maps are:
(1) Given an element $n_{1}^{k} \bmod m_{1}$ and an element $n_{2}^{k} \bmod m_{2}$ with $\left(n_{1}, m_{1}\right)=$ 1 and $\left(n_{2}, m_{2}\right)=1$, fixing rows and columns in the mapping table, the $n_{1}$ and $n_{2}$ are not necessarily unique in the multiplicative groups modulo
$m_{1}$ and modulo $m_{2}$. (See for example Table 5 where the 9 appears twice in column $k=2$.) Select one representative pair $n_{1}$ and $n_{2}$ and derive the unique solution $x$ of the generalized Chinese Remainder Theorem for coprime $\left(m_{1}, m_{2}\right)=1[4,7]$ :

$$
\begin{aligned}
x & \equiv n_{1} \quad\left(\bmod m_{1}\right) \\
x & \equiv n_{2} \quad\left(\bmod m_{2}\right)
\end{aligned}
$$

Note that $x=n_{1}+\alpha m_{1}$ and $x=n_{2}+\beta m_{2}$ imply that $x^{k} \equiv\left(n_{1}+\right.$ $\left.\alpha m_{1}\right)^{k} \equiv n_{1}^{k}\left(\bmod m_{1}\right)$ and $x^{k} \equiv\left(n_{2}+\beta m_{2}\right)^{k} \equiv n_{2}^{k}\left(\bmod m_{2}\right)$ by binomial expansion: although $n_{1}$ and $n_{2}$ may not be unique representatives, the algorithm finds a unique $x$ which has a unique power $x^{k}$-with the fitting exponent-to be put as $n_{12}=x^{k}\left(\bmod m_{1} m_{2}\right)$ into the mapping table.
(2) Each element $n_{12}^{k}$ in the residue set of $k$-powers modulo $m_{1} m_{2}$ is mapped uniquely onto a pair of residues modulo $m_{1}$ and modulo $m_{2}$ as follows: because $n_{12}$ is coprime to $m_{1} m_{2}$ by definition, it is individually coprime to $m_{1}$ and to $m_{2}$, so $n_{12}^{k}$ appears in the row of $n_{12}^{k} \bmod m_{1}$ and in the column of $n_{12}^{k} \bmod m_{2}$.
Finally note that the assembly of the elements in the table with the Chinese Remainder Theorem followed by the disassociation into row and column indices leads to the same row and columns that we started with. In summary, the mapping table is full and all its entries are unique.

Theorem 4 reduces the computation of $N_{m}(k)$ to the cases where $m=p^{e}$ are powers of primes, and to finding the integer ratios implied by Theorem 3. For the quartic and octic characters Finch derived the orders of the kernel of the groups [3]. Dividing the group order $\varphi\left(p^{e}\right)=(p-1) p^{e-1}$ through these orders yields

## Theorem 5.

$$
\begin{gather*}
N_{2^{e}}(4)= \begin{cases}1, & e \leq 3 \\
2^{e-4}, & e \geq 4\end{cases}  \tag{8}\\
N_{p^{e}}(4)=\left\{\begin{array}{lll}
\frac{p-1}{2} p^{e-1}, & p \equiv 3 & (\bmod 4), e \geq 1 \\
\frac{p-1}{4} p^{e-1}, & p \equiv 1 & (\bmod 4), e \geq 1
\end{array}\right. \tag{9}
\end{gather*}
$$

Theorem 6.

$$
\begin{gather*}
N_{2^{e}}(8)= \begin{cases}1, & e \leq 5 ; \\
2^{e-5}, & e \geq 5\end{cases}  \tag{10}\\
N_{p^{e}}(8)= \begin{cases}\frac{p-1}{2} p^{e-1}, & p \equiv\{3,7\}(\bmod 8), e \geq 1 ; \\
\frac{p-1}{4} p^{e-1}, & p \equiv 5(\bmod 8), e \geq 1 ; \\
\frac{p-1}{8} p^{e-1}, & p \equiv 1(\bmod 8), e \geq 1 .\end{cases} \tag{11}
\end{gather*}
$$

Based on a numerical search for linear recurrences and ordinary generating functions $\sum_{e \geq 0} N_{p^{e}}(k) x^{e}$ we arrive at the following analysis for small $k$ :

Conjecture 1. For $k=5$

$$
N_{5^{e}}(5)= \begin{cases}1, & e<1  \tag{12}\\ 4, & e=1 \\ 4 \times 5^{e-2}, & e>1\end{cases}
$$



Conjecture 2. If $k=6$

$$
\begin{align*}
& N_{2^{e}}(6)= \begin{cases}1, & e \leq 3 \\
2^{e-3}, & e \geq 3\end{cases}  \tag{13}\\
& N_{3^{e}}(6)= \begin{cases}1, & e \leq 2 \\
3^{e-2}, & e \geq 2\end{cases} \tag{14}
\end{align*}
$$

Conjecture 3. If $k=7$

$$
N_{7^{e}}(7)= \begin{cases}1, & e<1  \tag{15}\\ 6, & e=1 \\ 6 \times 7^{e-2}, & e \geq 2\end{cases}
$$

Conjecture 4. If $k=9$

$$
N_{3^{e}}(9)= \begin{cases}1, & e=0  \tag{16}\\ 2, & 1 \leq e \leq 3 \\ 2 \times 3^{e-3}, & e \geq 3\end{cases}
$$

If the bases are coprime to the exponents:
Conjecture 5. If $(p, k)=1$,

$$
N_{p^{e}}(k)=\left\{\begin{array}{rll}
\frac{p-1}{k} p^{e-1}, & p \equiv 1 & (\bmod k)  \tag{17}\\
\frac{p-1}{(p-1, k)} p^{e-1}, & p \not \equiv 1 & (\bmod k)
\end{array} .\right.
$$

## 2. Number of $k$-Th powers modulo $m$

2.1. Sets of $k$-th powers modulo $m$. The previous section considered powers of bases coprime to $m$. In this section we consider the sets of powers of any numbers modulo $m$, totients or non-totients. A table of the $k$-th powers modulo $m$ is defined by inserting lines to Table 3 handling all $0 \leq n<m$ leading to Table 7 .

Example 5. The extension of Table 5 by rows including numbers $(n, m) \neq 1$ is shown in Table 8.

The group property of Section 1.3 is lost, which means for example that the unit element of multiplication modulo $m$, the 1 , may be missing in some of the rows of Table 7. These elements do not have inverses. The $m \times m$ table for multiplications modulo $m$ creates only a semigroup.

For the same reason that led to Equ. (6) we have:

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 4 | 8 | 6 | 2 | 4 | 8 | 6 | 2 | 4 | 8 | 6 | 2 | 4 | 8 | 6 | 2 | 4 | 8 | 6 |
| 3 | 9 | 7 | 1 | 3 | 9 | 7 | 1 | 3 | 9 | 7 | 1 | 3 | 9 | 7 | 1 | 3 | 9 | 7 | 1 |
| 4 | 6 | 4 | 6 | 4 | 6 | 4 | 6 | 4 | 6 | 4 | 6 | 4 | 6 | 4 | 6 | 4 | 6 | 4 | 6 |
| 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 7 | 9 | 3 | 1 | 7 | 9 | 3 | 1 | 7 | 9 | 3 | 1 | 7 | 9 | 3 | 1 | 7 | 9 | 3 | 1 |
| 8 | 4 | 2 | 6 | 8 | 4 | 2 | 6 | 8 | 4 | 2 | 6 | 8 | 4 | 2 | 6 | 8 | 4 | 2 | 6 |
| 9 | 1 | 9 | 1 | 9 | 1 | 9 | 1 | 9 | 1 | 9 | 1 | 9 | 1 | 9 | 1 | 9 | 1 | 9 | 1 |

Table 8. Example of Table 7 for modulus $m=10$.

## Theorem 7.

$$
\begin{equation*}
R_{m}(k) \leq R_{m}(d), \quad d \mid k \tag{18}
\end{equation*}
$$

2.2. Periodicity with respect to the exponent. There still is a periodicity of $n^{k} \bmod m$ along each row of Table 7 -which generalizes the group orders of Section 1.3. Let $x$ be the period length associated with $n$. Here is a constructive proof of its existence. First there are cases where $n \mid m$.

$$
\begin{equation*}
n^{k+x} \equiv n^{k} \quad(\bmod m) \rightsquigarrow n^{k}\left(n^{x}-1\right) \equiv 0 \quad(\bmod m) \tag{19}
\end{equation*}
$$

Let $d$ be the greatest divisor of $m$ which is divisible through all prime factors of $n$. By removing all powers of primes for all primes which $m$ and $n$ have in common, $d=\prod_{p|n, p| m} p^{\nu_{p}(m)}$ and $(n, m / d)=1$. For example $d=9$ if $m=9$ and $n=6$.

Definition 4. $\nu_{a}(m)$ denotes the greatest exponent such that the power of a divides $m: a^{\nu_{a}(m)} \| m$.

The period length $x$ is found by dividing the previous equation through $d$ :

$$
\begin{equation*}
\frac{n^{j}}{d} n^{k-j}\left(n^{x}-1\right) \equiv 0 \quad\left(\bmod \frac{m}{d}\right) \tag{20}
\end{equation*}
$$

The exponent $j$ is the smallest exponent such that $n^{j} / d$ is integer. To be valid for general exponents $k$ we require

$$
\begin{equation*}
n^{x}-1 \equiv 0 \quad\left(\bmod \frac{m}{d}\right) \rightsquigarrow n^{x} \equiv 1 \quad\left(\bmod \frac{m}{d}\right) \tag{21}
\end{equation*}
$$

$n$ and $m / d$ are coprime. $x=\operatorname{ord}_{m / d}(n)$ is well defined, and equals the order of $n$ in the multiplicative group modulo $m / d$. If $m / d=1$, set $x=1$. At that step, the exponent $k$ must be sufficiently large to support this integer division, $k-j \geq 0$, which means, the periodicity may step in after some set of transient $k$.

Example 6. Column $m=16$ in Table 9 starts with 3 transient terms and is $\lambda(16)=4$-periodic: $16,4,10, \overline{2,9,3,9}$.

The reduction for cases $(n, m)>1$ has removed prime powers from $m$; these $x$ are divisors of those derived from the cases $(n, m)=1$ (because the Carmichael function is essentially equal to $\varphi$ and this is multiplicative). Eventually the least common multiple of these $x$ is again Carmichael's $\lambda$-function, so inclusion of the $n$

| $k \backslash m$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | OEIS |
| ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | A000027 |
| 2 | 1 | 2 | 2 | 2 | 3 | 4 | 4 | 3 | 4 | 6 | 6 | 4 | 7 | 8 | 6 | 4 | 9 | 8 | 10 | 6 | A000224 |
| 3 | 1 | 2 | 3 | 3 | 5 | 6 | 3 | 5 | 3 | 10 | 11 | 9 | 5 | 6 | 15 | 10 | 17 | 6 | 7 | 15 | A046530 |
| 4 | 1 | 2 | 2 | 2 | 2 | 4 | 4 | 2 | 4 | 4 | 6 | 4 | 4 | 8 | 4 | 2 | 5 | 8 | 10 | 4 | A052273 |
| 5 | 1 | 2 | 3 | 3 | 5 | 6 | 7 | 5 | 7 | 10 | 3 | 9 | 13 | 14 | 15 | 9 | 17 | 14 | 19 | 15 | A052274 |
| 6 | 1 | 2 | 2 | 2 | 3 | 4 | 2 | 2 | 2 | 6 | 6 | 4 | 3 | 4 | 6 | 3 | 9 | 4 | 4 | 6 | A052275 |
| 7 | 1 | 2 | 3 | 3 | 5 | 6 | 7 | 5 | 7 | 10 | 11 | 9 | 13 | 14 | 15 | 9 | 17 | 14 | 19 | 15 | A085310 |
| 8 | 1 | 2 | 2 | 2 | 2 | 4 | 4 | 2 | 4 | 4 | 6 | 4 | 4 | 8 | 4 | 2 | 3 | 8 | 10 | 4 | A085311 |
| 9 | 1 | 2 | 3 | 3 | 5 | 6 | 3 | 5 | 3 | 10 | 11 | 9 | 5 | 6 | 15 | 9 | 17 | 6 | 3 | 15 | A085312 |
| 10 | 1 | 2 | 2 | 2 | 3 | 4 | 4 | 2 | 4 | 6 | 2 | 4 | 7 | 8 | 6 | 3 | 9 | 8 | 10 | 6 | A085313 |
| 11 | 1 | 2 | 3 | 3 | 5 | 6 | 7 | 5 | 7 | 10 | 11 | 9 | 13 | 14 | 15 | 9 | 17 | 14 | 19 | 15 | A228849 |
| 12 | 1 | 2 | 2 | 2 | 2 | 4 | 2 | 2 | 2 | 4 | 6 | 4 | 2 | 4 | 4 | 2 | 5 | 4 | 4 | 4 |  |
| 13 | 1 | 2 | 3 | 3 | 5 | 6 | 7 | 5 | 7 | 10 | 11 | 9 | 13 | 14 | 15 | 9 | 17 | 14 | 19 | 15 |  |
| 14 | 1 | 2 | 2 | 2 | 3 | 4 | 4 | 2 | 4 | 6 | 6 | 4 | 7 | 8 | 6 | 3 | 9 | 8 | 10 | 6 |  |
| 15 | 1 | 2 | 3 | 3 | 5 | 6 | 3 | 5 | 3 | 10 | 3 | 9 | 5 | 6 | 15 | 9 | 17 | 6 | 7 | 15 |  |
| 16 | 1 | 2 | 2 | 2 | 2 | 4 | 4 | 2 | 4 | 4 | 6 | 4 | 4 | 8 | 4 | 2 | 2 | 8 | 10 | 4 |  |
| 17 | 1 | 2 | 3 | 3 | 5 | 6 | 7 | 5 | 7 | 10 | 11 | 9 | 13 | 14 | 15 | 9 | 17 | 14 | 19 | 15 |  |

Table 9. Top corner of the table of $R_{m}(k)$, size of the set of the
$k$-th powers of integers modulo $m$.
that are not coprime to $m$ does not change the periodicity of the number of residues as a function of $k$.
2.3. Cardinality of the Set of $k$-th Power Residues. Similar to Definition 3, dropping the requirement of co-primality, we count how many different integers appear in a column of Table 7:
Definition 5. $R_{m}(k)$ is the number of distinct residues of the $k$-th powers of the integers modulo $m$.

$$
\begin{equation*}
R_{m}(k)=\#\left\{n^{k} \quad \bmod m: n \in \mathbb{Z}\right\} \tag{22}
\end{equation*}
$$

The array of the $R_{m}(k)$ is illustrated in Table 9 for small $m$ and $k$. The periodicity of the residues evaluated in Section 2.2 for the individual $n$ induces that, for fixed $m, R_{m}(k)$ is a periodic function of $k$ with a period length defined by the l.c.m. of the period lengths $x$ for the individual $n$.

Remark 2. As long as the $n^{k}$ are smaller than the modulus, all of them are counted by $R_{m}(k)$, so we have the simple bounds

$$
\begin{equation*}
1+\lfloor\sqrt[k]{m-1}\rfloor \leq R_{m}(k) \leq m \tag{23}
\end{equation*}
$$

The following theorem was claimed in the Online Encylopedia of Integer Sequences [9] for all sequences cited in Table 9 without proof; the observation deemed to be interesting enough to write up this manuscript:

Theorem 8. For fixed exponent $k$, the cardinality $R_{m}(k)$ of the set of residues is a multiplicative function of $m$.

The proof is essentially the same as the proof for Theorem 4.
Since $R_{m}(k)$ is multiplicative, the evaluation is reduced to derive $R_{m}(k)$ for prime powers $m=p^{e}$.

| $k \backslash e$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 2 | 1 | 3 | 6 | 10 | 15 | 21 | 28 | 36 |
| 3 | 1 | 4 | 10 | 20 | 35 | 56 | 84 | 120 |
| 4 | 1 | 5 | 15 | 35 | 70 | 126 | 210 | 330 |
| 5 | 1 | 6 | 21 | 56 | 126 | 252 | 462 | 792 |
| 6 | 1 | 7 | 28 | 84 | 210 | 462 | 924 | 1716 |
| 7 | 1 | 8 | 36 | 120 | 330 | 792 | 1716 | 3432 |
| 8 | 1 | 9 | 45 | 165 | 495 | 1287 | 3003 | 6435 |
| 9 | 1 | 10 | 55 | 220 | 715 | 2002 | 5005 | 11440 |
| 10 | 1 | 11 | 66 | 286 | 1001 | 3003 | 8008 | 19448 |

Table 10. The number of weak compositions of $k$ into $e$ parts, $\binom{k+e-1}{e-1}$, a tilted version of Pascal's triangle [9, A007318].
2.4. Inheritance Structure in Prime Power Bases. We can rephrase the problem of "folding" the $n^{k}$ into the interval $\left[0, p^{e}\right)$ as representing $n^{k}$ for $0 \leq n \leq m$ in the basis $p$ :

$$
\begin{equation*}
n=\sum_{j=0}^{e} \alpha_{j, n^{k}, p} p^{j}, \quad 0<\alpha_{j, n^{k}, p}<p \tag{24}
\end{equation*}
$$

The power has the multinomial expansion

$$
\begin{align*}
& (25) \quad n^{k}=\left[\sum_{j \geq 0} \alpha_{j, n^{k}, p} p^{j}\right]^{k}  \tag{25}\\
& =\sum_{\substack{k_{0}+k_{1}+\ldots k_{e-1}=k \\
k_{j} \geq 0}} \frac{k!}{k_{0}!k_{1}!k_{2}!\cdots k_{e-1}!} \alpha_{k_{0}, n^{k}, p}^{k_{0}}\left(\alpha_{k_{1}, n^{k}, p} p\right)^{k_{1}}\left(\alpha_{k_{2}, n^{k}, p} p^{2}\right)^{k_{2}} \cdots\left(\alpha_{k_{e-1}, n^{k}, p} p^{e-1}\right)^{k_{e-1}}
\end{align*}
$$

Each term of the sum on the right hand side has a structure defined by a weak composition (composition into non-negative parts) of $k$ into $e$ parts, $k \equiv \sum_{j=0}^{e-1} k_{j}$. The number of weak compositions of $k$ in $e$ parts defines Table 10.

Example 7. For $k=3$ and $e=4$ the structure of the right hand side contains 20 weak compositions of $3 ; 16$ of them are:

| $\backslash j$ | 0 | 1 | 2 | 3 |
| :--- | :--- | :--- | :--- | :--- |
|  | 3 | 0 | 0 | 0 |
|  | 2 | 1 | 0 | 0 |
|  | 2 | 0 | 1 | 0 |
|  | 2 | 0 | 0 | 1 |
| 1 | 2 | 0 | 0 |  |
| 1 | 1 | 1 | 0 |  |
| 1 | 0 | 2 | 0 |  |
| 1 | 0 | 1 | 1 |  |
| 1 | 0 | 0 | 2 |  |
| 0 | 3 | 0 | 0 |  |
| 0 | 2 | 1 | 0 |  |
| 0 | 2 | 0 | 1 |  |
| 0 | 1 | 2 | 0 |  |
| 0 | 1 | 1 | 1 |  |
| 0 | 1 | 0 | 2 |  |
| 0 | 0 | 3 | 0 |  |
| $\cdots$ |  |  |  |  |

Reducing $n^{k}$ modulo $p^{e}$ means that only terms where

$$
\begin{equation*}
\sum_{j=0}^{e-1} j k_{j}<e \tag{26}
\end{equation*}
$$

(the first moment of the row sums of the structure is less than e) contribute.
Example 8. If the constraint (26) is imposed to Example 7, only the following 7 of the 20 structures remain:

| $\backslash j$ | 0 | 1 | 2 | 3 | $\sum_{j} j k_{j}$ |
| :--- | :--- | :--- | :--- | :--- | ---: |
|  | 3 | 0 | 0 | 0 | 0 |
|  | 2 | 1 | 0 | 0 | 1 |
|  | 2 | 0 | 1 | 0 | 2 |
|  | 2 | 0 | 0 | 1 | 3 |
|  | 1 | 2 | 0 | 0 | 2 |
| 1 | 1 | 1 | 0 | 3 |  |
|  | 0 | 3 | 0 | 0 | 3 |

This reduces the number of contributing structures to those in Table 11. The ordinary generating function of row $k$ in this table is

$$
\begin{equation*}
\frac{x}{(1-x)^{2} \prod_{j=1}^{k}\left(1-x^{j}\right)} . \tag{27}
\end{equation*}
$$

So row $k$ is obtained from row $k-1$ by convolution with an "aerated" sequence with generating function

$$
\begin{equation*}
\frac{1}{1-x^{k}}=\sum_{i \geq 0} x^{i k} \tag{28}
\end{equation*}
$$

A combinatorial interpretation of that convolution is: a weak composition for $(k, e)$ is constructed by (i) adding a 1 to the left-most part of a weak composition for $(k-1, e)$, or (ii) by adding a 1 to the left-most part of a weak composition of ( $k-1, e-k$ ), and inserting a leading zero and $k-1$ trailing zeros, (iii) by adding

| $k \backslash e$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | OEIS |
| ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | A000012 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | A 000027 |
| 2 | 1 | 2 | 4 | 6 | 9 | 12 | 16 | 20 | 25 | 30 | 36 | 42 | A 087811 |
| 3 | 1 | 2 | 4 | 7 | 11 | 16 | 23 | 31 | 41 | 53 | 67 | 83 | A 000601 |
| 4 | 1 | 2 | 4 | 7 | 12 | 18 | 27 | 38 | 53 | 71 | 94 | 121 | A 002621 |
| 5 | 1 | 2 | 4 | 7 | 12 | 19 | 29 | 42 | 60 | 83 | 113 | 150 | A 002622 |
| 6 | 1 | 2 | 4 | 7 | 12 | 19 | 30 | 44 | 64 | 90 | 125 | 169 | A 288341 |
| 7 | 1 | 2 | 4 | 7 | 12 | 19 | 30 | 45 | 66 | 94 | 132 | 181 | A 288342 |
| 8 | 1 | 2 | 4 | 7 | 12 | 19 | 30 | 45 | 67 | 96 | 136 | 188 | A 288343 |
| 9 | 1 | 2 | 4 | 7 | 12 | 19 | 30 | 45 | 67 | 97 | 138 | 192 | A 288344 |
| 10 | 1 | 2 | 4 | 7 | 12 | 19 | 30 | 45 | 67 | 97 | 139 | 194 | A 288345 |

Table 11. Top corner of the number of weak compositions of $k$ into $e$ parts under the restriction (26) [9, A092905].
a 1 to the left-most part of a weak composition of $(k-1, e-2 k)$ and padding this with $2 k$ zeros ( 2 leading, $2 k-2$ trailing), and so on.
2.5. Conjectured Terms for Prime Power Moduli. By numerical experimentation with large set of different primes $p$ and exponents $e$ we arrive at the following set of conjectures.

Conjecture 6. $R_{p^{e}}(k)$ obeys a linear recurrence with constant coefficients:

$$
\begin{equation*}
R_{p^{e}}(k)=p R_{p^{e-1}}(k)+R_{p^{e-k}}(k)-p R_{p^{e-k-1}}(k), \quad e-k \geq 1 \tag{29}
\end{equation*}
$$

Conjecture 7. If the modulus $p^{e}$ and the exponent $k$ are coprime, so $(p, k)=1$,

$$
\begin{equation*}
R_{p^{e}}(k)=1+\left\lfloor\frac{\frac{p-1}{(p-1, k)} p^{e+k-1}}{p^{k}-1}\right\rfloor, \quad(p, k)=1, \quad e \geq 0 \tag{30}
\end{equation*}
$$

This leaves the cases where $(p, k)>1$. If $p=k$ we summarize experience based on $p \leq 7$ by:

Conjecture 8. For $p=k$,

$$
R_{p^{e}}(p)=\left\{\begin{array}{lll}
1+\left\lfloor\frac{(p-1) p^{e+k-2}}{p^{p}-1}\right\rfloor, & e \not \equiv 1 & (\bmod p)  \tag{31}\\
p+\left\lfloor\frac{(p-1) p^{e+k-2}}{p^{p}-1}\right\rfloor, & e \equiv 1 & (\bmod p)
\end{array}, k=p, e \geq 0\right.
$$

Conjectural equations for composite $k \leq 12,(p, k)>1$, are gathered in Equations (32)-(40).

$$
R_{2^{e}}(4)=\left\{\begin{array}{ll}
1+\left\lfloor\frac{p^{e}}{p^{k}-1}\right\rfloor & e \equiv 0 \quad(\bmod 4)  \tag{32}\\
2+\left\lfloor\frac{p^{e}}{p^{k}-1}\right\rfloor & e \equiv\{1,2,3\} \quad(\bmod 4)
\end{array} \quad, k=4, \quad p=2, e \geq 0\right.
$$

$$
R_{2^{e}}(6)=\left\{\begin{array}{ll}
1+\left\lfloor\frac{p^{e+k-3}}{p^{k}-1}\right\rfloor, & e+3 \equiv\{0,1,2,3\} \quad(\bmod 6)  \tag{33}\\
2+\left\lfloor\frac{p^{+k-3}}{p^{k}-1}\right\rfloor, & e+3 \equiv\{4,5\} \quad(\bmod 6)
\end{array}, \quad k=6, \quad p=2\right.
$$

$$
R_{3^{e}}(6)=\left\{\begin{array}{ll}
1+\left\lfloor\frac{p^{e+k-2}}{p^{k}-1}\right\rfloor, & e+4 \equiv\{0,1,2,3,4\} \quad(\bmod 6)  \tag{34}\\
2+\left\lfloor\frac{p^{e+k-2}}{p^{k}-1}\right\rfloor, & e+4 \equiv 5 \quad(\bmod 6)
\end{array} \quad k=6, \quad p=3 .\right.
$$

$$
R_{2^{e}}(8)=\left\{\begin{array}{ll}
1+\left\lfloor\frac{p^{e+3}}{p^{k}-1}\right\rfloor, & e+3 \equiv\{0,1,2,3\}  \tag{35}\\
(\bmod 8) \\
2+\left\lfloor\frac{p^{e+3}}{p^{k}-1}\right\rfloor, & e+3 \equiv\{4,5,6,7\} \\
(\bmod 8)
\end{array} \quad, \quad k=8, \quad p=2\right.
$$

$$
R_{3^{e}}(9)=\left\{\begin{array}{ll}
1+\left\lfloor\frac{2 p^{e+6}}{p^{k}-1}\right\rfloor, & e+6 \equiv\{0,1,2, \ldots, 6\} \quad(\bmod 9)  \tag{36}\\
3+\left\lfloor\frac{2 p^{e+6}}{p^{k}-1}\right\rfloor, & e+6 \equiv\{7,8\} \quad(\bmod 9)
\end{array}, \quad k=9, \quad p=3 .\right.
$$

$R_{2^{e}}(10)=\left\{\begin{array}{lll}1+\left\lfloor\frac{p^{e+7}}{p^{k}-1}\right\rfloor, & e+7 \equiv\{0,1,2,3, \ldots, 7\} & (\bmod 10) \\ 2+\left\lfloor\frac{p^{e+7}}{p^{k}-1}\right\rfloor, & e+7 \equiv\{8,9\} & (\bmod 10)\end{array} \quad, \quad k=10, \quad p=2\right.$.
$R_{5^{e}}(10)=\left\{\begin{array}{lll}1+\left\lfloor\frac{2 p^{e+8}}{p^{k}-1}\right\rfloor, & e+8 \equiv\{0,1,2, \ldots, 8\} & (\bmod 10) \\ 3+\left\lfloor\frac{2 p^{e+8}}{p^{k}-1}\right\rfloor, & e+8 \equiv 9 \quad(\bmod 10)\end{array}, \quad k=10, \quad p=5\right.$.
$R_{2^{e}}(12)=\left\{\begin{array}{ll}1+\left\lfloor\frac{p^{e+8}}{p^{k}-1}\right\rfloor, & e+8 \equiv\{0,1,2, \ldots, 8\} \quad(\bmod 12) \\ 2+\left\lfloor\frac{p^{e+8}}{p^{k}-1}\right\rfloor, & e+8 \equiv\{9,10,11\} \quad(\bmod 12)\end{array}, \quad k=12, \quad p=2\right.$.
$R_{3^{e}}(12)=\left\{\begin{array}{ll}1+\left\lfloor\frac{p}{}^{e+10}\right. \\ p^{k}-1 \\ & e+10 \equiv\{0,1,2, \ldots, 10\} \quad(\bmod 12) \\ 2+\left\lfloor\frac{p^{e+10}}{p^{k}-1}\right\rfloor, & e+10 \equiv 11 \quad(\bmod 12)\end{array} \quad k=12, \quad p=3\right.$.
In all these cases the factor in the numerator of the floor-functions appears to be $\frac{p-1}{(p-1, k)}$, the same as in (30).

## References

1. Tom M. Apostol, Introduction to analytic number theory, Undergraduate Texts in Mathematics, Springer, 1976. MR 0434929
2. R. D. Carmichael, On composite numbers $p$ which satisfy the fermat congrues $a^{p-1} \equiv 1$ modp, Am. Math. Monthly 19 (1912), no. 2, 22-27.
3. Steven Finch, Quartic and octic characters modulo n, arXiv:0907.4893 (2016).
4. Aviezri S. Fraenkel, New proof of the general chinese remainder theorem, Proc. Amer. Math. Soc. 14 (1963), no. 5, 790-791. MR 0154841
5. Michal Křížek, Florian Luca, and Lawrence Somer, 17 lectures on fermat numbers, CMS Books in Mathematics, vol. 9th, Springer, New York, 2001. MR 1866957
6. Romeo Meštrović, Generalizations of carmichael numbers i, arXiv:1305.1867 [math.NT] (2013).
7. Oystein Ore, The general chinese remainder theorem, Am. Math. Monthly 59 (1952), no. 6, 365-370. MR 0048481
8. József Sándor and B. Crstici, Handbook of number theory ii, Kluwer, 2004. MR 2119686
9. Neil J. A. Sloane, The On-Line Encyclopedia Of Integer Sequences, Notices Am. Math. Soc. 50 (2003), no. 8, 912-915, http://oeis.org/. MR 1992789
URL: http://www.mpia.de/~mathar
Max-Planck Institute of Astronomy, Königstuhl 17, 69117 Heidelberg, Germany

[^0]:    Date: November 10, 2017.
    2010 Mathematics Subject Classification. Primary 05C30; Secondary 05C20, 05C75.
    Key words and phrases. Graph Enumeration, Combinatorics.

