Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
2022, Volume 28, Number 4, 730–743
DOI: 10.7546/nntdm.2022.28.4.730-743

Counting general power residues

Samer Seraj

Existsforall Academy
Mississauga, Ontario, Canada
e-mail: samer_seraj@outlook.com

Received: 9 April 2022 **Revised:** 4 November 2022
Accepted: 4 November 2022 **Online First:** 7 November 2022

Abstract: Suppose every integer is taken to the power of a fixed integer exponent $k \geq 2$ and the remainders of these powers upon division by a fixed integer $n \geq 2$ are found. It is natural to ask how many distinct remainders are produced. By building on the work of Stangl, who published the $k = 2$ case in *Mathematics Magazine* in 1996, we find essentially closed formulas that allow for the computation of this number for any k. Along the way, we provide an exposition of classical results on the multiplicativity of this counting function and results on the number of remainders that are coprime to the modulus n.
Keywords: Modular arithmetic, Power residues, Primitive roots, Geometric series, Arithmetic functions.
2020 Mathematics Subject Classification: 11A15, 11A07, 11A25.

1 Introduction

Definition 1.1. *Let $n \geq 2$ and $k \geq 2$ and a be integers. Then a is said to be a k-th power residue modulo n if there exists an integer x such that*

$$x^k \equiv a \pmod{n}.$$

If a is coprime to n and satisfies the congruence, then we will call a a reduced k-th power residue modulo n. Modulo n:

1. *The set of k-th power residue classes is denoted by $R_k(n)$.*
2. *The set of reduced k-th power residue classes is denoted by $S_k(n)$.*
3. *The set of k-th power residue classes that are not reduced, meaning $R_k(n)$ excluding $S_k(n)$, is denoted by $T_k(n)$.*

These sets are well-defined: if a lives in one of these sets, then its entire congruence class modulo n lives there too. For ease of notation and language, we might speak of a particular integer, instead of its congruence class, being in $R_k(n)$ or $S_k(n)$ or $T_k(n)$.

Definition 1.2. *An arithmetic function is a function whose domain is the positive integers $\mathbb{Z}_+$ and whose codomain is the complex numbers $\mathbb{C}$. An arithmetic function f is said to be multiplicative if, for any inputs a, b such that $\gcd(a, b) = 1$, it holds that $f(ab) = f(a)f(b)$.*

The classic result that $|R_k(n)|$ and $|S_k(n)|$ are multiplicative arithmetic functions, in the variable n for fixed k, allows one to reduce their computation to the case where n is a prime power p^m. The formula for $|S_k(p^m)|$ for odd primes p and the formula for $|S_k(2^m)|$ are well-known results. In 1996, Walter Stangl [4] published formulas in *Mathematics Magazine* that allowed for the computation of $|R_2(n)|$. We will prove formulas that allow for the computation of $|R_k(n)|$ for any integer $k \geq 2$, and we will state the aforementioned classical results, along with proofs in cases where we were unable to find reputable references.

Definition 1.3. *Given a positive integer n and a prime p, the p-adic valuation of n is the exponent of the highest power of p that divides n. It is denoted by $\nu_p(n)$. For example, $\nu_2(40) = 3$.*

Definition 1.4. *Let ϵ be the parity function. So for integers t, $\epsilon(t) = \begin{cases} 0 & \text{if } 2 \mid t \\ 1 & \text{if } 2 \nmid t \end{cases}$.*

Definition 1.5. *For each real number x, let $\lceil x \rceil$ denote the ceiling function of x, which is the least integer greater than or equal to x.*

Definition 1.6. *The greatest common divisor of two integers a and b, at least one of which is non-zero, is the largest integer that divides both a and b. It is denoted by $\gcd(a, b)$ or (a, b), the latter of which is not to be confused with coordinates.*

The general formula is the following:

Theorem 1.1. *Let p be a prime, and $k \geq 2$ and $m \geq 1$ be integers. Let r be the remainder of m upon division by k. Let*

$$\alpha = \frac{p-1}{(k, p-1)},$$
$$\beta = (\nu_p(k) + 1)(1 - \epsilon(k))(1 - \epsilon(p)) + \nu_p(k)\epsilon(p),$$
$$\gamma = \begin{cases} k & \text{if } k \mid m \\ r & \text{if } k \nmid m \end{cases}.$$

Then

$$|R_k(p^m)| = \alpha \cdot \left(\frac{p^k}{p^{\beta+1}} \cdot \frac{p^m - p^\gamma}{p^k - 1} + \left\lceil \frac{p^\gamma}{p^{\beta+1}} \right\rceil \right) + 1$$
$$= \alpha \cdot \left\lceil \frac{1}{p^{\beta+1}} \cdot \frac{p^{m+k} - p^\gamma}{p^k - 1} \right\rceil + 1,$$

(Note that the $\dfrac{p^k}{p^{\beta+1}} \cdot \dfrac{p^m - p^\gamma}{p^k - 1}$ term is necessarily an integer, so it can be absorbed into the ceiling term $\left\lceil \dfrac{p^\gamma}{p^{\beta+1}} \right\rceil$ as shown.)

A special case is that, if $m = 1$ and $k \geq 2$ and p is an odd prime such that $p \nmid k$, then

$$|R_k(p)| = \frac{p-1}{(k, p-1)} + 1.$$

For example, there are exactly three cubes modulo 7, namely $0, 1,$ and 6, and there are exactly four eighth powers modulo 7, namely $0, 1, 2,$ and 4.

Our calculations are based on straightforward, albeit technical, extensions of Stangl's methods on various cases which may be brought together as above. We have not seen this unified formula stated elsewhere in the literature.

2 Preliminary results for all moduli

We will need the following result, a sort of Chinese remainder theorem (CRT) for power residues, to reduce the formulas for $|R_k(n)|$ and $|S_k(n)|$ to the case that n is a prime power. We could not find a textbook reference for the result, but it is certainly known.

Lemma 2.1. *Let $t \geq 2$ and $k \geq 2$ be integers, n_1 and n_2 be coprime positive integers. Then there exist bijections*

$$r_k : R_k(n_1) \times R_k(n_2) \to R_k(n_1 n_1),$$
$$s_k : S_k(n_1) \times S_k(n_2) \to S_k(n_1 n_2).$$

This proves that the arithmetic cardinality functions $|R_k(n)|$ and $|S_k(n)|$ are multiplicative in n when k is fixed.

Proof. Let a_1 and a_2 be any integers. The Chinese remainder theorem asserts the existence of an integer a that simultaneously satisfies the congruences

$$a \equiv a_1 \pmod{n_1},$$
$$a \equiv a_2 \pmod{n_2}$$

and that all solutions are given by those integers that are congruent to a modulo $n_1 n_2$. Let $k \geq 2$ be an integer. We will first prove that both $a_1 \in R_k(n_1)$ and $a_2 \in R_k(n_2)$ if and only if $a \in R_k(n_1 n_2)$. We will then deduce that both $a_1 \in S_k(n_1)$ and $a_2 \in S_k(n_2)$ if and only if $a \in S_k(n_1 n_2)$.

In one direction, it is clear that if a is a k-th power modulo $n_1 n_2$, then it is a k-th power modulo both n_1 and n_2 because $n_1, n_2 \mid n_1 n_2$. So we turn our attention to the other direction. Let a be the common CRT solution to the system of congruences, where a is unique up to congruence modulo $n_1 n_2$. We want a to be a k-th power residue modulo $n_1 n_2$, assuming that there exists an integers b_1 and b_2 such that

$$b_1^k \equiv a_1 \pmod{n_1},$$
$$b_2^k \equiv a_2 \pmod{n_2}.$$

We apply CRT again to get an integer b such that

$$b \equiv b_1 \pmod{n_1},$$
$$b \equiv b_2 \pmod{n_2},$$

where b is unique up to congruence modulo $n_1 n_2$. Then we find that

$$b^k \equiv b_1^k \equiv a_1 \equiv a \pmod{n_1},$$
$$b^k \equiv b_2^k \equiv a_2 \equiv a \pmod{n_2},$$

which proves that

$$b^k \equiv a \pmod{n_1 n_2}$$

because n_1 and n_2 are coprime. Therefore, the common solution a is a k-th power modulo $n_1 n_2$, as is every integer in its residue class modulo $n_1 n_2$.

This result can be restricted to reduced k-th power residues as follows. By the Euclidean algorithm, $(a, n_i) = (a_i, n_i)$ for each $i = 1, 2$. The multiplicativity of the two-entry $\gcd$ function with one entry fixed yields

$$(a_1, n_1)(a_2, n_2) = (a, n_1)(a, n_2) = (a, n_1 n_2).$$

Therefore, $(a, n_1 n_2) = 1$ if and only if $(a_1, n_1) = 1$ and $(a_2, n_2) = 1$.

To find the desired bijections, we use the maps that are the restrictions of the CRT map to k-th power residues or their reduced variants. The earlier part of this proof shows that these are indeed maps with the domains and ranges given by

$$r_k : R_k(n_1) \times R_k(n_2) \to R_k(n_1 n_2),$$
$$s_k : S_k(n_1) \times S_k(n_2) \to S_k(n_1 n_2).$$

So we just need to prove bijectivity. Since the mapping

$$(a_1, a_2) \mapsto a,$$

where a is the common solution to the two congruences, has a being unique modulo $n_1 n_2$, we find that r_k and its restriction s_k are injective. For surjectivity, note that every integer in $R_k(n_1 n_2)$ is a k-th power residue modulo n_1 and n_2, so those k-th powers to which it reduces then maps to it. The restricted map s_k is also surjective because we proved that $(a, n_1 n_2) = 1$ if and only if $(a_1, n_1) = 1$ and $(a_2, n_2) = 1$. Therefore, r_k and s_k are bijective. By the multiplication principle from combinatorics,

$$|R_k(n_1)| \cdot |R_k(n_2)| = |R_k(n_1 n_2)|,$$
$$|S_k(n_1)| \cdot |S_k(n_2)| = |S_k(n_1 n_2)|,$$

so $|R_k(n)|$ and $|S_k(n)|$ are multiplicative functions in the variable n for fixed k. □

The following result is the key recursion that, in conjunction with classical computations of $|S_k(n)|$, will allow us to find $|R_k(n)|$.

Lemma 2.2. *If p is any prime and $m > k \geq 2$ are integers, then*

$$|T_k(p^m)| = |R_k(p^{m-k})|.$$

Proof. We will produce a bijection from $R_k(p^{m-k})$ to $T_k(p^m)$. Choose a least representative b from a class in $R_k(p^{m-k})$ so that $0 \leq b < p^{m-k}$. Then there exists an integer c such that

$$\begin{aligned} c^k &\equiv b \pmod{p^{m-k}} \\ (cp)^k &\equiv bp^k \pmod{p^m}. \end{aligned}$$

Moreover,

$$0 \leq b < p^{m-k} \implies 0 \leq bp^k < p^m.$$

So $b \mapsto bp^k$ is a well-defined map from least representatives in $R_k(p^{m-k})$ to least representatives in $T_k(p^m)$, since bp^k is not coprime to p^m. We will show that this map is bijective.

For injectivity, suppose some least representatives b_1, b_2 modulo p^{m-k} get mapped to the same element. Then

$$\begin{aligned} b_1 p^k &\equiv b_2 p^k \pmod{p^m} \\ b_1 &\equiv b_2 \pmod{p^{m-k}}, \end{aligned}$$

which leads to $b_1 = b_2$ as integers because they are least non-negative residues modulo p^{m-k}. This establishes injectivity.

For surjectivity, suppose $y \in T_k(p^m)$ is a least residue. Then there exist integers x and z such that

$$\begin{aligned} x^k &\equiv y \pmod{p^m} \\ x^k &= y + p^m z. \end{aligned}$$

Since $\gcd(y, p^m) > 1$, we know that $p \mid y$. Then $p \mid x^k$, leading to $p^k \mid x^k$. Since $m > k$, we find that $p^k \mid x^k - p^m z = y$. So let b be the integer such that $bp^k = y$. Then

$$0 \leq bp^k < p^m \implies 0 \leq b < p^{m-k}$$

tells us that b is a least residue in $R_k(p^{m-k})$ that maps to the least residue $y \in T_k(p^m)$. □

As a result,

$$\begin{aligned} |R_k(p^m)| &= |S_k(p^m)| + |T_k(p^m)| \\ &= |S_k(p^m)| + |R_k(p^{m-k})|. \end{aligned}$$

Lemma 2.3. *If p is any prime, $k \geq 2$ is an integer, and m is an integer such that $0 < m \leq k$, then $T_k(p^m)$ consists of only the residue class of 0. Thus, $|T_k(p^m)| = 1$.*

Proof. Suppose $y \in T_k(p^m)$. Then there exist integers x and z such that

$$x^k \equiv y \pmod{p^m}$$
$$x^k = y + p^m z.$$

As in the preceding proof, it holds that

$$\gcd(y, p^m) > 1 \implies p \mid y \implies p \mid x^k \implies p^k \mid x^k.$$

Since the premise is that $0 < m \leq k$, we find that

$$y \equiv x^k \equiv 0 \pmod{p^m}.$$

So the only residue class in $T_k(p^m)$ is the class of 0. Thus, $|T_k(p^m)| = 1$. □

Combining the last two results yields the following formulas that will be the crux of our computations, as they reduce finding the more complicated $|R_k(n)|$ to finding the well-understood $|S_k(n)|$. We will need the preceding lemma at the end of each recursive calculation in Lemma 2.4.

Lemma 2.4. *Let p be any prime. If m and k are integers such that $1 \leq m \leq k$ and $k \geq 2$, then*

$$|R_k(p^m)| = |S_k(p^m)| + 1.$$

Now let $m > k \geq 2$ be integers. If $k \mid m$, then

$$|R_k(p^m)| = |S_k(p^m)| + |S_k(p^{m-k})| + \cdots + |S_k(p^{2k})| + |S_k(p^k)| + 1.$$

If $k \nmid m$, let r be the remainder upon Euclidean division of m by k. That is, $m = qk + r$ for some quotient q and remainder r such that $0 < r < k$. Then

$$|R_k(p^m)| = |S_k(p^m)| + |S_k(p^{m-k})| + \cdots + |S_k(p^{r+k})| + |S_k(p^r)| + 1.$$

As a final general note, we will need an unusual variant of the formula for a finite geometric series, as written below.

Lemma 2.5. *Let $z \neq 1$ be a real number and α, β, γ be integers such that $\gamma = \alpha - q\beta$ for some non-negative integer q. Then*

$$z^\alpha + z^{\alpha-\beta} + z^{\alpha-2\beta} + \cdots + z^\gamma = \frac{z^{\alpha+\beta} - z^\gamma}{z^\beta - 1}.$$

Proof. This is simply a geometric series. □

3 Prime power moduli with primitive roots

Now we turn to computing $|R_k(p^m)|$ where p^m is a prime power that has a primitive root. We will need the following results from [3, p. 104]:

Lemma 3.1. *Let $n \geq 2$ be an integer. Then there exists a primitive root modulo n if and only if $n = 2, 4, p^m$, or $2p^m$ where p is an odd prime and m is a positive integer.*

We will be focused on using the fact that a primitive root exists modulo $n = 2, 4$ and p^m. The case $n = 2p^m$ will not concern us because it is not a prime power.

Lemma 3.2 (Generalized Euler's criterion)**.** *Let $n \geq 2$ be an integer such that there exists a primitive root modulo n. Let a be an integer coprime to n, and $k \geq 2$ be an integer. Then the congruence*

$$x^k \equiv a \pmod{n}$$

has a solution x, meaning a is a reduced k-th power residue modulo n, if and only if

$$a^\ell \equiv 1 \pmod{n},$$

where $\ell = \dfrac{\varphi(n)}{(k, \varphi(n))}$. Here, φ is Euler's totient function.

These results allow us to derive the following classical formula. The main cases of Lemma 3.3 appear in [5, p. 113], but the $n = 2, 4$ cases are excluded, so we have provided a quick separate proof here.

Lemma 3.3. *Let $n \geq 2$ be an integer such that there exists a primitive root modulo n. Let $k \geq 2$ be an integer. Then*

$$|S_k(n)| = \frac{\varphi(n)}{(k, \varphi(n))}.$$

Proof. We are seeking the number of reduced k-th powers modulo n. Let $\ell = \frac{\varphi(n)}{(k,\varphi(n))}$. For $\gcd(a, n) = 1$, from Lemma 3.2, a is such a residue if and only if $a^\ell \equiv 1 \pmod{n}$. Note that $a^\ell \equiv 1 \pmod{n}$ if and only if $\mathrm{ord}_n(a) \mid \ell$, where $\mathrm{ord}_n(a)$ is the least positive exponent that sends a to 1. By a result on cyclic groups [2, pp. 57-58], if d is a divisor of $\varphi(n)$, then the number of distinct elements of order d is $\varphi(d)$ (this works as long as n has a primitive root). By the fact that the arithmetic summation function of φ is the identity function, we sum $\varphi(d)$ over all positive divisors d of ℓ (ℓ is a divisor of $\varphi(n)$, and thus so are all divisors d of ℓ) to get

$$|S_k(n)| = \sum_{d \mid \ell} \varphi(d) = \ell = \frac{\varphi(n)}{(k, \varphi(n))}. \qquad \square$$

Lemma 3.4. *Let p be an odd prime, and $m \geq 1$ and $k \geq 2$ be integers. If $m \geq k$, then*

$$|S_k(p^m)| = \frac{p-1}{(k, p-1)} \cdot \frac{1}{p^{\nu_p(k)+1}} \cdot p^m.$$

Proof. By Lemma 3.3, we know that

$$\begin{aligned} |S_k(p^m)| &= \frac{\varphi(p^m)}{(k, \varphi(p^m))} = \frac{p^{m-1}(p-1)}{(k, p^{m-1}(p-1))} \\ &= \frac{p^{m-1}(p-1)}{(k, p^{m-1})(k, p-1)} = \frac{p-1}{(k, p-1)} \cdot \frac{1}{(k, p^{m-1})} \cdot p^{m-1}. \end{aligned}$$

So it suffices to prove that $m - 1 \geq \nu_p(k)$, as that would allow us to evaluate (k, p^{m-1}) to be $p^{\nu_p(k)}$. For any positive integer k,

$$2^{k-1} \geq k \implies p^{k-1} \geq 2^{k-1} \geq k \geq p^{\nu_p(k)},$$
$$m \geq k \implies m-1 \geq k-1 \geq \nu_p(k).$$

The fact that $2^{k-1} \geq k$ can be proven by induction on $k \geq 1$. Moreover, $k \geq p^{\nu_p(k)}$ holds because the right side is a divisor of the left side. □

We are now ready for the first theorems pertaining to the casework on $|R_k(n)|$.

Theorem 3.1. *Let p be an odd prime and m and k be integers such that $k \geq 2$ and $k \geq m \geq 1$, or let $p = 2$ with $m = 1$ or $m = 2$ and $k \geq 2$. Then*

$$|R_k(p^m)| = \frac{p-1}{(k, p-1)} \cdot \left\lceil \frac{1}{p^{\nu_p(k)+1}} \cdot p^m \right\rceil + 1.$$

Proof. Since $k \geq m \geq 1$, applying Lemma 2.4 and Lemma 3.3 tells us that

$$\begin{aligned} |R_k(p^m)| &= |S_k(p^m)| + 1 \\ &= \frac{p-1}{(k, p-1)} \cdot \frac{p^{m-1}}{(k, p^{m-1})} + 1 = \frac{p-1}{(k, p-1)} \cdot \left\lceil p^{m-\nu_p(k)-1} \right\rceil + 1, \end{aligned}$$

which is equivalent to what we want. □

Corollary 3.1. *Let $k \geq 2$ be an integer. It holds that*

$$|R_k(2)| = |S_k(2)| + 1 = 2,$$
$$|R_k(2^2)| = |S_k(2^2)| + 1 = \begin{cases} 2 & \text{if } 2 \mid k \\ 3 & \text{if } 2 \nmid k \end{cases}.$$

Theorem 3.2. *Let p be an odd prime, and m and k be integers such that $m > k \geq 2$ and $k \mid m$. Then*

$$|R_k(p^m)| = \frac{p-1}{(k, p-1)} \cdot \frac{1}{p^{\nu_p(k)+1}} \cdot \frac{p^{m+k} - p^k}{p^k - 1} + 1.$$

Proof. By Lemma 2.4, Lemma 3.4, and Lemma 2.5,

$$\begin{aligned} |R_k(p^m)| &= |S_k(p^m)| + |S_k(p^{m-k})| + |S_k(p^{m-2k})| + \cdots + |S_k(p^k)| + 1 \\ &= \frac{p-1}{(k, p-1)} \cdot \frac{1}{p^{\nu_p(k)+1}} \cdot (p^m + p^{m-k} + p^{m-2k} + \cdots + p^k) + 1 \\ &= \frac{p-1}{(k, p-1)} \cdot \frac{1}{p^{\nu_p(k)+1}} \cdot \frac{p^{m+k} - p^k}{p^k - 1} + 1, \end{aligned}$$

which is equal to the formula that we are seeking. □

Theorem 3.3. *Let p be an odd prime, and m and k be integers such that $m > k \geq 2$ and $k \nmid m$. Let the remainder upon Euclidean division of m by k be r. Then*

$$|R_k(p^m)| = \frac{p-1}{(k, p-1)} \cdot \left\lceil \frac{1}{p^{\nu_p(k)+1}} \cdot \frac{p^{m+k} - p^r}{p^k - 1} \right\rceil + 1.$$

Proof. By Lemma 2.4, Lemma 3.4, and Lemma 2.5,

$$\begin{aligned}
|R_k(p^m)| &= |S_k(p^m)| + |S_k(p^{m-k})| + \cdots + |S_k(p^{r+k})| + |S_k(p^r)| + 1 \\
&= \frac{p-1}{(k,p-1)} \cdot \frac{1}{p^{\nu_p(k)+1}} \cdot (p^m + p^{m-k} + \cdots + p^{r+k}) + \frac{\varphi(p^r)}{(k,\varphi(p^r))} + 1 \\
&= \frac{p-1}{(k,p-1)} \cdot \frac{1}{p^{\nu_p(k)+1}} \cdot \frac{p^{m+k} - p^{r+k}}{p^k - 1} + \frac{p-1}{(k,p-1)} \cdot \frac{p^{r-1}}{(k,p^{r-1})} + 1 \\
&= \frac{p-1}{(k,p-1)} \cdot \left(p^{k-\nu_p(k)-1} \cdot \frac{p^m - p^r}{p^k - 1} + \left\lceil p^{r-\nu_p(k)-1} \right\rceil \right) + 1.
\end{aligned}$$

Since $p^{k-\nu_p(k)-1} \cdot \dfrac{p^m - p^r}{p^k - 1}$ is an integer, we can absorb it into the ceiling function and simplify to get the desired formula. □

4 Prime power moduli without primitive roots

Definition 4.1. *For each positive integer n, we will use the symbol $[n]$ to denote the first n positive integers $\{1, 2, \ldots, n\}$.*

With the results complete for $n = 2, 4$, and odd prime powers p^m, we turn to computing $|R_k(2^m)|$ for $m \geq 3$. When the prime is 2, it will be possible to absorb the $m = 1, 2$ cases into the $m = 3$ case as will later be shown.

The structure of units modulo 2^m is understood well, as the following result from [3, p. 105] shows.

Lemma 4.1. *Let $m \geq 3$ be an integer. Then*

$$\operatorname{ord}_{2^m}(5) = 2^{m-2}.$$

Moreover, the set

$$X = \left\{ \pm 5^i : i \in [2^{m-2}] \right\}$$

of 2^{m-1} elements form a system of all reduced residues modulo 2^m. Finally, these representations are unique in the sense that, if a is odd, then there exist integers x, y such that

$$a \equiv (-1)^x \cdot 5^y \pmod{2^m}$$

where x is unique modulo 2 and y is unique modulo 2^{m-2}.

The following result from [1, p. 432] will be helpful.

Lemma 4.2. *Let a and $n \geq 2$ be coprime integers, and k be a positive integer. Then*

$$\operatorname{ord}_n(a^k) = \frac{\operatorname{ord}_n(a)}{(k, \operatorname{ord}_n(a))}.$$

We will also need the following result from [3, p. 108], where it is stated as a problem at the end of a section.

Lemma 4.3. *Let $k \geq 2$ and $n \geq 2$ be integers. The k-th power map modulo an integer n is bijective on the set of reduced residue classes modulo n if and only if $(k, \varphi(n)) = 1$.*

It is extremely likely that the following result is known, but we have been unable to find a textbook reference, so we have proven it here.

Lemma 4.4. *Let $k \geq 2$ and $m \geq 3$ be integers. Then*

$$|S_k(2^m)| = \begin{cases} \dfrac{2^{m-2}}{(k, 2^{m-2})} & \text{if } 2 \mid k \\ 2^{m-1} & \text{if } 2 \nmid k \end{cases}.$$

Proof. Let $k = 2^j b$ where b is an odd integer. If $j = 0$, then k is odd, making it coprime to 2^m. By Lemma 4.3, this means that all residue classes coprime to 2^m are in $S_k(2^m)$, so $|S_k(2^m)| = 2^{m-1}$. For the rest of the argument, assume that $j \geq 1$. The k-th power map takes each element of

$$X = \left\{\pm 5^i : i \in [2^{m-2}]\right\}$$

to the power of b, followed by taking the power of 2^j of each element. Again by the preceding result, the first map has no effect because it is simply a bijection on X. The application of the second map to X is what we have to carefully observe. Since $j \geq 1$, the exponent is even and so

$$S_k(2^m) = \left\{(5^i)^{2^j} \pmod{2^m} : i \in [2^{m-2}]\right\}.$$

Not every $(5^i)^{2^j}$ is necessarily distinct modulo 2^m so we have count the number of distinct elements. We exchange exponents to rewrite each term as $(5^{2^j})^i$ for $i \in [2^{m-2}]$. Since $\operatorname{ord}_{2^m}(5) = 2^{m-2}$, we get

$$(5^{2^j})^{2^{m-2}} \equiv (5^{2^{m-2}})^{2^j} \equiv 1^{2^j} \equiv 1 \pmod{2^m},$$

and higher powers of 5^{2^j} are repeats of lower powers. So all powers of 5^{2^j} are in $S_k(2^m)$, and every element of $S_k(2^m)$ is a power of 5^{2^j}. Since powers of an element cycle if the element is coprime to the modulus, the number of distinct elements of $S_k(2^m)$, is

$$|S_k(2^m)| = \operatorname{ord}_{2^m}(5^{2^j}) = \frac{\operatorname{ord}_{2^m}(5)}{(2^j, \operatorname{ord}_{2^m}(5))} = \frac{2^{m-2}}{(2^j, 2^{m-2})} = \frac{2^{m-2}}{(k, 2^{m-2})}. \qquad \square$$

Lemma 4.5. *Let $k \geq 2$ and $m \geq 1$ be integers. Then*

$$|S_k(2^m)| = \begin{cases} \left\lceil 2^{m-\nu_2(k)-2} \right\rceil & \text{if } 2 \mid k \\ 2^{m-1} & \text{if } 2 \nmid k \end{cases} = \left\lceil \frac{2^{m-1}}{2^{(\nu_2(k)+1)(1-\epsilon(k))}} \right\rceil.$$

Proof. In the $2 \mid k$ case,

$$\begin{aligned} |S_k(2)| &= 1 = \left\lceil 2^{1-\nu_2(k)-2} \right\rceil, \\ |S_k(2^2)| &= 1 = \left\lceil 2^{2-\nu_2(k)-2} \right\rceil, \\ |S_k(2^m)| &= \frac{2^{m-2}}{(k, 2^{m-2})} = \left\lceil 2^{m-\nu_2(k)-2} \right\rceil, \end{aligned}$$

where $m \geq 3$ in the third line and we used Lemma 4.4. In the $2 \nmid k$ case,

$$\begin{aligned} |S_k(2)| &= 1 = 2^0, \\ |S_k(2^2)| &= 2 = 2^1, \end{aligned}$$

so $m = 1, 2$ match the formula 2^{m-1} for $m \geq 3$ from Lemma 4.4. $\square$

Lemma 4.6. *Let $m \geq 3$ and $k \geq 2$ be integers. If $m > k$ and $2 \mid k$, then*

$$|S_k(2^m)| = \frac{1}{2^{\nu_2(k)+2}} \cdot 2^m.$$

Proof. By Lemma 4.4, we know that

$$|S_k(2^m)| = \frac{2^{m-2}}{(k, 2^{m-2})}.$$

So it suffices to prove that $m - 2 \geq \nu_2(k)$, as that would allow us to evaluate $(k, 2^{m-2})$ to be $2^{\nu_2(k)}$. Since

$$m > k \implies m - 1 \geq k \implies m - 2 \geq k - 1,$$

we find that

$$2^{k-1} \geq k \geq 2^{\nu_2(k)} \implies m - 2 \geq k - 1 \geq \nu_2(k).$$

This is very similar to the reasoning for Lemma 3.4. □

We are now ready to complete the casework on $|R_k(n)|$.

Theorem 4.1. *Let m and k be integers such that $k \geq 2$ and $k \geq m \geq 3$. Then*

$$|R_k(2^m)| = \left\lceil \frac{1}{2^{(\nu_2(k)+1)(1-\epsilon(k))+1}} \cdot 2^m \right\rceil + 1.$$

This works for $m = 1, 2$ as well, matching Corollary 3.1.

Proof. Lemma 2.4 and Lemma 4.5 tell us

$$|R_k(2^m)| = |S_k(2^m)| + 1 = \left\lceil \frac{2^{m-1}}{2^{(\nu_2(k)+1)(1-\epsilon(k))}} \right\rceil + 1.$$

□

Theorem 4.2. *Let m and k be integers such that $m > k \geq 2$ and $k \mid m$. Then*

$$|R_k(2^m)| = \left\lceil \frac{1}{2^{(\nu_2(k)+1)(1-\epsilon(k))+1}} \cdot \frac{2^{m+k} - 2^k}{2^k - 1} \right\rceil + 1.$$

Proof. By Lemmas 2.4, 4.6, 2.5, and 4.5, if $2 \mid k$, then

$$\begin{aligned}
|R_k(2^m)| &= |S_k(2^m)| + |S_k(2^{m-k})| + \cdots + |S_k(2^{2k})| + |S_k(2^k)| + 1 \\
&= \frac{1}{2^{\nu_2(k)+2}} \cdot (2^m + 2^{m-k} + 2^{m-2k} + \cdots + 2^{2k}) + |S_k(2^k)| + 1 \\
&= \frac{1}{2^{\nu_2(k)+2}} \cdot \frac{2^{m+k} - 2^{2k}}{2^k - 1} + \left\lceil 2^{k-\nu_2(k)-2} \right\rceil + 1 \\
&= 2^{k-\nu_2(k)-2} \cdot \frac{2^m - 2^k}{2^k - 1} + \left\lceil 2^{k-\nu_2(k)-2} \right\rceil + 1.
\end{aligned}$$

Since $2^{k-\nu_2(k)-2} \cdot \dfrac{2^m - 2^k}{2^k - 1}$ is an integer, we can absorb it into the ceiling function and simplify to get

$$|R_k(2^m)| = \left\lceil 2^{k-\nu_2(k)-2} \cdot \frac{2^m - 1}{2^k - 1} \right\rceil + 1.$$

For the $2 \nmid k$ case, we compute

$$\begin{aligned}|R_k(2^m)| &= |S_k(2^m)| + |S_k(2^{m-k})| + |S_k(2^{m-2k})| + \cdots + |S_k(2^k)| + 1 \\ &= \frac{1}{2} \cdot (2^m + 2^{m-k} + 2^{m-2k} + \cdots + 2^k) + 1 \\ &= \frac{1}{2} \cdot \frac{2^{m+k} - 2^k}{2^k - 1} + 1.\end{aligned}$$

The two formulas are special cases into which the stated formula breaks. □

Theorem 4.3. *Let m and k be integers such that $m > k \geq 2$ and $k \nmid m$. Let the remainder upon Euclidean division of m by k be r. Then*

$$|R_k(2^m)| = \left\lceil \frac{1}{2^{(\nu_2(k)+1)(1-\epsilon(k))+1}} \cdot \frac{2^{m+k} - 2^r}{2^k - 1} \right\rceil + 1.$$

Proof. By Lemma 2.4, Lemma 4.6, and Lemma 2.5, if $2 \mid k$, then

$$\begin{aligned}|R_k(2^m)| &= |S_k(2^m)| + |S_k(2^{m-k})| + \cdots + |S_k(2^{r+k})| + |S_k(2^r)| + 1 \\ &= \frac{1}{2^{\nu_2(k)+2}} \cdot (2^m + 2^{m-k} + 2^{m-2k} + \cdots + 2^{r+k}) + |S_k(2^r)| + 1 \\ &= \frac{1}{2^{\nu_2(k)+2}} \cdot \frac{2^{m+k} - 2^{r+k}}{2^k - 1} + \left\lceil 2^{r-\nu_2(k)-2} \right\rceil + 1 \\ &= 2^{k-\nu_2(k)-2} \cdot \frac{2^m - 2^r}{2^k - 1} + \left\lceil 2^{r-\nu_2(k)-2} \right\rceil + 1.\end{aligned}$$

Since $2^{k-\nu_2(k)-2} \cdot \dfrac{2^m - 2^r}{2^k - 1}$ is an integer, we can absorb it into the ceiling function and simplify to derive

$$|R_k(2^m)| = \left\lceil \frac{1}{2^{\nu_2(k)+2}} \cdot \frac{2^{m+k} - 2^r}{2^k - 1} \right\rceil + 1.$$

For the $2 \nmid k$ case, we find that

$$\begin{aligned}|R_k(2^m)| &= |S_k(2^m)| + |S_k(2^{m-k})| + |S_k(2^{m-2k})| + \cdots + |S_k(2^r)| + 1 \\ &= \frac{1}{2} \cdot (2^m + 2^{m-k} + 2^{m-2k} + \cdots + 2^r) + 1 \\ &= \frac{1}{2} \cdot \frac{2^{m+k} - 2^r}{2^k - 1} + 1.\end{aligned}$$

The two cases can be unified as stated. □

5 Conclusion

The various cases for odd primes p and $p = 2$ may be unified to produce Theorem 1.1. As the reader might expect, substituting $k = 2$ into our formulas yields those of Stangl; we have checked this. In addition, we ran tests on a computer program to ensure that the number of k-th power residues counted by the program matched those predicted by Theorem 1.1.

$$
\begin{aligned}
p \text{ odd}, k \geq m: &\quad |R_8(3^4)| = 28, \\
p \text{ odd}, m > k, k \mid m: &\quad |R_6(3^{12})| = 59131, \\
p \text{ odd}, m > k, k \nmid m: &\quad |R_5(3^{11})| = 118587, \\
p = 2, k \geq m \geq 3, 2 \mid k: &\quad |R_6(2^4)| = 3, \\
&\quad |R_8(2^6)| = 3, \\
p = 2, k \geq m \geq 3, 2 \nmid k: &\quad |R_7(2^5)| = 17, \\
&\quad |R_7(2^6)| = 33, \\
p = 2, m > k, m \geq 3, k \mid m, 2 \mid k: &\quad |R_4(2^{16})| = 4370, \\
&\quad |R_{12}(2^{24})| = 1048833, \\
p = 2, m > k, m \geq 3, k \mid m, 2 \nmid k: &\quad |R_5(2^{15})| = 16913, \\
&\quad |R_7(2^{21})| = 1056833, \\
p = 2, m > k, m \geq 3, k \nmid m, 2 \mid k: &\quad |R_4(2^9)| = 36, r = 1 \\
&\quad |R_4(2^{10})| = 70, r = 2 \\
&\quad |R_4(2^{11})| = 138, r = 3 \\
p = 2, m > k, m \geq 3, k \nmid m, 2 \nmid k: &\quad |R_5(2^{11})| = 1058, r = 1 \\
&\quad |R_5(2^{12})| = 2115, r = 2 \\
&\quad |R_5(2^{13})| = 4229, r = 3.
\end{aligned}
$$

Below is the Python program that was implemented:

```
def residue_counter(k,p,m):
    residueset = set()
    for x in range(0,p**m):
        residueset.add((x**k) % (p**m))
    return(len(residueset))
```

This program is very slow for large inputs. We have also implemented a program that uses our formulas instead and it is empirically much faster, assuming the prime factorization of n is known.

Aside from the natural and intrinsically interesting formulation of the problem tackled in this paper, it can be motivated in relation to other problems. In the context of modular power residues, there are several other worthy pursuits. One hope is that this "power-counting problem" will shed light on more difficult problems, which, in order of increasing difficulty, are to:

1. Given an integer a, determine whether it is a k-th power residue modulo n. We call this the "power-identification problem"; it is related to reciprocity laws in number theory.
2. Given an integer a, determine the number of residues x whose k-th powers are congruent to a modulo n. We call this the "root-counting problem."
3. Given an integer a, determine all (if any) residues x whose k-th powers are congruent to a modulo n. We call this the "root-taking problem."

The power-counting problem is also relevant to what we refer to as the "modular arithmetic contradiction trick" for polynomial Diophantine equations. This technique takes a multivariable polynomial equation with integer coefficients, and reduces it modulo some (miraculously chosen) modulus so that all of the (finitely many) substitutions of residues into the variables lead to contradictory (i.e., non-zero) computations. Therefore, this technique shows that there exist no integer solutions. Although this method is used widely both professionally and in math competitions, there is, to the best of our knowledge, no known method of coming up with the modulus n. However, an accepted heuristic is that, since we know the degrees of the univariate components of terms like x^k, we should pick a modulus that will minimize the number of k-th power residues or minimize the fraction of residues that are k-th power residues. The reasoning is that minimizing the amount of values that x^k can undertake lowers the "probability" of it being able to collide with other terms in order to produce the 0 residue class in the end. Although this reasoning is not airtight, in conjunction with a second heuristic - annihilate coefficients by choosing a modulus that is a factor of several coefficients - it is useful in practice. The power-counting problem might be helpful in reverse-engineering candidates for moduli when we are following the first heuristic, and we can further curate the list using the second heuristic (or vice versa).

The interested reader might wish to explore replacing x^k with univariate or multivariable polynomials, which would take us further along the path of intelligently choosing a modulus for this Diophantine contradiction trick.

Acknowledgements

The author would like to thank Dr. Arturo Magidin for providing advice pertaining to proving the classical Lemma 4.4 in the absence of reference material. The author also thanks Dr. Yuri Burda for being his first teacher in number theory. Finally, the author thanks the anonymous reviewers for their feedback.

References

[1] Andreescu, T., Dospinescu, G., & Mushkarov, O. (2017). *Number Theory: Concepts and Problems*. XYZ Press, Plano, Texas.

[2] Dummit, D. S., & Foote, R. M. (2004). *Abstract Algebra* (Third edition). John Wiley and Sons Inc., New York.

[3] Niven, I., Zuckerman, H. S., & Montgomery, H. L. (1991). *An Introducton to the Theory of Numbers* (Fifth edition). John Wiley and Sons Inc., New York.

[4] Stangl, W. D. (1996). Counting Squares in $\mathbb{Z}_n$. *Mathematics Magazine*, 69(4), 285–289.

[5] Vinogradov, I. M. (1954). *Elements of Number Theory* (Fifth edition). Dover Publications Inc., USA.