RESOLUTION OF MATHAR'S CONJECTURES ON COUNTING POWER RESIDUES

Samer Seraj
Existsforall Academy, Mississauga, Ontario. Canada
samer_seraj@outlook.com

Received: 11/11/22, Accepted: 8/12/23, Published: 8/25/23

Abstract

Given that every integer is taken to the power of a fixed integer exponent $k \geq 2$ and then these powers are reduced modulo a fixed integer $n \geq 2$, denote the set of resulting distinct remainders by $R_k(n)$. In 2017, based on numerical evidence, Richard Mathar posted a document and comments on the OEIS with a list of conjectures that addressed the determination of the cardinalities of such sets in various special cases. By modifying our recently published formula that counts $R_k(n)$ in essentially closed form, we prove all of Mathar's conjectures.

1. General Formulas

Definition 1. Let $n \geq 2$, $k \geq 2$, and a be integers. Then a is a k^{th} *power residue modulo* n if there exists an integer x such that

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

We denote the set of k^{th} power residue classes by $R_k(n)$.

It is a classic result that the counting function $|R_k(n)|$ is multiplicative in n if k is fixed; a proof is given in [5]. As such, it suffices to have a formula for $|R_k(p^m)|$ for primes p and positive integers m. We published a formula for this as follows.

Definition 2. Let ϵ be the *parity function*, which is defined, for integers t, as

$$\epsilon(t) = \begin{cases} 0 & \text{if } 2 \mid t \\ 1 & \text{if } 2 \nmid t \end{cases}.$$

Definition 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, $\nu_2(80) = 4$.

DOI: 10.5281/zenodo.8283150

Theorem 1 ([5]). *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

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

where $\dfrac{p^k}{p^{\beta+1}} \cdot \dfrac{p^m - p^\gamma}{p^k - 1}$ in the first line is necessarily an integer, so it can be absorbed into the ceiling function as shown in the second line. The formula correctly yields p^m in the $k = 1$ case as well.

Our proof of Theorem 1 in [5] is a generalization of Stangl's methods in [6], in conjunction with certain classical results. Another paper that addresses the determination of $|R_k(p^m)|$ is by Maxim Korolev [3], who cites Ji Chungang [1]. Both authors left their formulas as unclosed series and spread across several cases. Our contribution was to close the sums using p-adic valuation and unify the disparate cases by observing their overall similar structure.

The main new result of the current paper is the following modified formula.

Theorem 2. *Let $p, m, k, r, \alpha, \beta, \gamma$ be as defined in Theorem 1. Then*

$$|R_k(p^m)| = \begin{cases} \left\lfloor \frac{\alpha \cdot p^{m+k-\beta-1}}{p^k - 1} \right\rfloor + 1 & \text{if } \gamma \geq \beta + 1 \\ \left\lfloor \frac{\alpha \cdot p^{m+k-\beta-1}}{p^k - 1} \right\rfloor + \alpha + 1 & \text{if } \gamma \leq \beta \end{cases}.$$

Note that, unlike Theorem 1, this formula only works for $k \geq 2$, as it does not yield p^m for $k = 1$.

Proof. Suppose $\gamma \geq \beta + 1$. By Theorem 1,

$$\begin{aligned} |R_k(p^m)| - 1 &= \alpha \cdot \left(p^{k-\beta-1} \cdot \frac{p^m - p^\gamma}{p^k - 1} + p^{\gamma-\beta-1} \right) \\ &= \alpha \cdot \frac{p^{m+k-\beta-1} - p^{\gamma-\beta-1}}{p^k - 1} \\ &= \frac{\alpha \cdot p^{m+k-\beta-1}}{p^k - 1} - \frac{\alpha \cdot p^{\gamma-\beta-1}}{p^k - 1}. \end{aligned}$$

This is equal to the left side $|R_k(p^m)| - 1$, which is an integer. In general, we have the following equivalences:

$$c - d = \lfloor c \rfloor \iff c - 1 < c - d \leq c \iff 0 \leq d < 1,$$

where we have used a characterization of the floor function from [2, p. 69]. Indeed, using $\gamma \leq k$ and $\beta \geq 0$, we find that

$$0 \leq \frac{\alpha \cdot p^{\gamma-\beta-1}}{p^k - 1} = \frac{(p-1) \cdot p^{\gamma-\beta-1}}{(k, p-1)(p^k-1)} \leq \frac{(p-1) \cdot p^{k-1}}{p^k - 1} = \frac{p^k - p^{k-1}}{p^k - 1} \leq 1.$$

On the far right, equality holds if and only if $k = 1$, which is excluded.

In the other case, suppose $\gamma \leq \beta$. Then

$$\begin{aligned} |R_k(p^m)| - 1 &= \alpha \cdot \left(p^{k-\beta-1} \cdot \frac{p^m - p^\gamma}{p^k - 1} + 1 \right) \\ &= \alpha \cdot \frac{p^{m+k-\beta-1} - p^{\gamma+k-\beta-1}}{p^k - 1} + \alpha \\ &= \frac{\alpha \cdot p^{m+k-\beta-1}}{p^k - 1} - \frac{\alpha \cdot p^{\gamma+k-\beta-1}}{p^k - 1} + \alpha. \end{aligned}$$

Following the earlier logic, we use $\gamma \leq \beta$ to prove that

$$0 \leq \frac{\alpha \cdot p^{\gamma+k-\beta-1}}{p^k - 1} = \frac{(p-1) \cdot p^{\gamma+k-\beta-1}}{(k, p-1)(p^k-1)} \leq \frac{(p-1) \cdot p^{k-1}}{p^k - 1} = \frac{p^k - p^{k-1}}{p^k - 1} \leq 1.$$

Once again, equality on the far right does not hold due to $k \geq 2$, so we have the desired strict upper bound of 1. □

2. Mathar's Conjectures

In 2017, based on numerical verification, R. J. Mathar posted on the OEIS numerous conjectures regarding counting power residues [4]. All of them may be resolved using the results in the present paper (note that his notation slightly differs from our chosen one).

- Conjectures 1-5 are simple consequences of the classical formulas for counting the number of k^{th} power residues modulo n that are coprime to n, so we will not comment on them. The necessarily formulas were given a full exposition in [5].

- Conjecture 6 is a recurrence relation for any prime p that may be rewritten as

  $$|R_k(p^m)| - |R_k(p^{m-k})| = p \cdot \left(|R_k(p^{m-1})| - |R_k(p^{m-1-k})| \right).$$

  This is a direct result of applying Theorem 1 to all four terms and simplifying.

- Conjecture 7 says that, if p^m and k are coprime with any prime p (meaning $p \nmid k$), then
$$|R_k(p^m)| = \left\lfloor \frac{p-1}{(k,p-1)} \cdot \frac{p^{m+k-1}}{p^k-1} \right\rfloor + 1.$$
Here, $\beta = 0$ (because at least one of p or k must be odd, by their coprimality) and $1 \leq \gamma \leq k$, so $\beta + 1 \leq \gamma$. Thus, the conjecture is a consequence of the first case of Theorem 2.

- Conjecture 8 says that, taking $k = p$, we get
$$|R_p(p^m)| = \begin{cases} \left\lfloor \frac{(p-1)\cdot p^{m+p-2}}{p^p-1} \right\rfloor + 1 & \text{if } m \not\equiv 1 \pmod{p} \\ \left\lfloor \frac{(p-1)\cdot p^{m+p-2}}{p^p-1} \right\rfloor + p & \text{if } m \equiv 1 \pmod{p} \end{cases}.$$
This is actually not true for $p = 2$, but it does work for odd primes p (the omission of this restriction is likely a typographical error by Mathar). The expressions are easy to get from Theorem 2. The conditions come from the fact that $\beta = 1$, so the condition $\gamma \leq \beta$ is equivalent to $\gamma = 1$ since $\gamma \geq 1$, and $\gamma = 1$ if and only if $m \equiv 1 \pmod{p}$.

- Nine more conjectural equations are given as equations 32-40, all of which may be proven using Theorem 2 for specific k and specific p; we have independently checked the details. These compute $|R_k(p^m)|$ for
$$(k,p) = (4,2), (6,2), (6,3), (8,2), (9,3), (10,2), (10,5), (12,2), (12,3).$$

- Several sequences in the OEIS list $\{|R_k(n)|\}_{n=1}^{\infty}$ for fixed k: squares are in A000224, cubes in A046530, fourth powers in A052273, fifth powers in A052274, sixth powers in A052275, seventh powers in A085310, eighth powers in A085311, ninth powers in A085312, tenth powers in A085313, eleventh powers in A085314, and twelfth powers in A228849. There, Mathar conjectured formulas for fourth powers
$$|R_4(2^m)| = \begin{cases} \left\lfloor \frac{2^m}{2^4-1} \right\rfloor + 1 & \text{if } 4 \mid m \\ \left\lfloor \frac{2^m}{2^4-1} \right\rfloor + 2 & \text{if } 4 \nmid m \end{cases},$$
$$|R_4(p^m)| = \left\lfloor \frac{p-1}{(4,p-1)} \cdot \frac{p^{m+3}}{p^4-1} \right\rfloor + 1, \text{ odd primes } p,$$

and fifth powers

$$|R_5(5^m)| = \begin{cases} \left\lfloor \frac{(5-1)\cdot 5^{m+3}}{5^5-1} \right\rfloor + 1 & \text{if } m \not\equiv 1 \pmod 5, \\ \left\lfloor \frac{(5-1)\cdot 5^{m+3}}{5^5-1} \right\rfloor + 5 & \text{if } m \equiv 1 \pmod 5 \end{cases},$$

$$|R_5(p^m)| = \left\lfloor \frac{p-1}{(5,p-1)} \cdot \frac{p^{m+4}}{p^5-1} \right\rfloor + 1, \text{ primes } p \neq 5.$$

These are direct consequences of Theorem 2.

Theorem 1 and Theorem 2 are undoubtedly rich with other special cases that can be computed, optimized for software implementation, and otherwise analyzed.

References

[1] J. Chungang, The number of kth power residues modulo m, *J. Nanjing Norm. Univ. Nat. Sci. Ed.* **24(1)** (2001), 1-2.

[2] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics: A Foundation for Computer Science* (Second edition), Addison-Wesley Publishing Company, Inc., Boston, 1994.

[3] M. A. Korolev, On the average number of power residues modulo a composite number, *Izv. Math.* **74(6)** (2010), 1225-1254.

[4] R. J. Mathar, Size of the set of residues of integer powers of fixed exponent, *OEIS* (2017). https://oeis.org/A293482/a293482.pdf

[5] S. Seraj, Counting general power residues, *Not. Numb. Th. Discr. Math.* **28(4)** (2022), 730-743. DOI: 10.7546/nntdm.2022.28.4.730-743

[6] W. D. Stangl, Counting squares in $\mathbb{Z}_n$, *Math. Mag.* **69(4)** (1996), 285–289.