ON THE CONGRUENCE $x^x \equiv x \pmod{n}$

James Hammer
Department of Mathematics, Cedar Crest College, Pennsylvania
jmhammer@cedarcrest.edu

Joshua Harrington
Department of Mathematics, Cedar Crest College, Pennsylvania
Joshua.Harrington@cedarcrest.edu

Lenny Jones
Department of Mathematics, Shippensburg University, Pennsylvania
lkjone@ship.edu

Received: 1/3/16, Revised: 8/4/16, Accepted: 10/22/16, Published: 11/11/16

Abstract

Solutions to the congruence $x^x \equiv x \pmod{p}$, where p is a prime and $1 \leq x \leq p-1$, have been investigated by several authors. Although Kurlberg, Luca and Shparlinski have recently shown that a solution exists with $x \neq 1$ for almost all primes, there do exist primes for which the only solution is $x = 1$, and they conjectured that the set of such primes is infinite. In this article, we investigate the nature of the solutions to this congruence when the prime modulus is replaced with a composite number. Among the results presented, we show that, unlike the situation when the modulus is a prime, there is always a solution with $x \neq 1$. In addition, we prove several results concerning the structure of these solutions, with special attention given to the algebraic structure. In particular, we show that there exist infinitely many composite numbers n for which the set of all solutions to $x^x \equiv x \pmod{n}$, with $1 \leq x \leq n-1$, is a subgroup of the group of units modulo n.

1. Introduction

Although investigations into the type and number of residues of x^x modulo a prime [4, 5, 9, 1, 2, 7, 6, 3] appeared as early as 1966, such questions have recently become a topic of growing interest. This resurgence is most likely due in part to the connections of the map $x \mapsto x^x \pmod{p}$ with dynamical systems and cryptography. In fact, an explanation of these connections is given in [7] where the authors also

show that for almost all primes p, there exists some x with $2 \leq x \leq p-1$ such that

$$x^x \equiv x \pmod{p}. \tag{1}$$

Indeed, there do exist primes for which the only solution to (1) is the *trivial solution*, $x = 1$, and the authors in [7] conjectured that the set of such primes is infinite.

In this article, we are primarily concerned with the solutions to (1) when the prime p is replaced with a composite integer n. For a fixed positive integer n, we let $\mathcal{S}_n$ denote the set of all solutions x to

$$x^x \equiv x \pmod{n}, \tag{2}$$

with $1 \leq x \leq n-1$. Not surprisingly, we see that the composite situation is quite different in many respects from the situation when n is a prime. For example, we show that for any composite integer n, there exists $x \in \mathcal{S}_n$ with $x \geq 2$. Such a solution will be called a *nontrivial solution*.

We also investigate the nature of the elements of $\mathcal{S}_n$, including the algebraic structure. In particular, we show that $\mathcal{S}_n$ contains a nontrivial subgroup of U_n, the multiplicative group of units modulo n, when no prime divides n exactly to the first power. Additionally, we show that $\mathcal{S}_n$ itself is a subgroup of U_n in infinitely many, but somewhat rare, situations.

2. Preliminaries

Definition 1. Let $n > 1$ be an integer, and let x be a positive integer with $\gcd(x, n) = 1$. We define $\mathrm{ord}_n(x)$ be the order of x in U_n.

Definition 2. Let k be a positive integer, and let p be a prime. We define $\nu_p(k)$ to be the exponent on the largest power of p that divides k.

The following result is due to Kummer [8].

Proposition 1. *Let p be a prime. Let b and k be positive integers. Then*

$$\nu_p\left(\binom{p^m}{k}\right) = m - \nu_p(k).$$

Definition 3. We define the *Legendre symbol modulo a prime p* as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo the prime } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo the prime } p \\ 0 & \text{if } a \equiv 0 \pmod{p}. \end{cases}$$

3. Lifting the Upper Bound Restriction on Solutions to (2)

In this section, we investigate the situation when solutions x to (2) are not required to have $x \leq n-1$.

Lemma 1. *Let $n \geq 2$ and $k \geq 2$ be integers. If x is a solution to (2), then x^k is a solution to (2).*

Proof. Since x is a solution to (2), we have

$$\left(x^k\right)^{x^k} \equiv x^{kx^k} \equiv (x^x)^{kx^{k-1}} \equiv x^{kx^{k-1}} \equiv \cdots \equiv x^k \pmod{n}. \qquad \square$$

Note that if $x \in \mathcal{S}_n$ and $k \geq 2$ is an integer, then it could be that $x^k > n-1$. Thus, if $x^k \equiv m \pmod{n}$, where $1 \leq m \leq n-1$, then it could be that $m \notin \mathcal{S}_n$. For example, let $n = 7$. Then $x = 4 \in \mathcal{S}_n$, so that $x = 4^2$ is a solution to (2) by Lemma 1. However, $4^2 \equiv 2 \pmod{7}$ and $x = 2 \notin \mathcal{S}_n$. Nevertheless, under certain conditions, given m with $1 \leq m \leq n-1$, we can show that there exists some integer $x \equiv m \pmod{n}$ that satisfies (2). We first need the following lemma.

Lemma 2. *If n is a square-free positive integer, then for any positive integer k, $m^{k\phi(n)+1} \equiv m \pmod{n}$ for any integer m.*

Proof. If $\gcd(m,n) = 1$, then the result follows from Euler's generalization of Fermat's Little Theorem. Since n is square-free, we can write $n = p_1 p_2 \cdots p_t$, where each p_i is a distinct prime. Without loss of generality, suppose that $\gcd(m,n) = p_1 p_2 \cdots p_r$ for some $r \geq 1$, and $\gcd(m, p_i) = 1$ for all i, with $r < i \leq t$. Then, by Fermat's Little Theorem,

$$m^{k\phi(n)} = m^{k(p_1-1)(p_2-1)\cdots(p_t-1)} \equiv 1 \pmod{p_i},$$

for each i with $r < i \leq t$. Thus, if $1 \leq i \leq r$, then p_i divides m and if $r < i \leq t$, then p_i divides $m^{k\phi(n)} - 1$. Hence,

$$m^{k\phi(n)+1} - m = m(m^{k\phi(n)} - 1) \equiv 0 \pmod{n}.$$

$\square$

Theorem 4. *Suppose that $n \geq 4$ is composite. Then, for every integer m with $0 \leq m \leq n-1$, there exists a positive integer x, such that $x \equiv m \pmod{n}$ and x is a solution to (2) if and only if $\gcd(n, \phi(n)) = 1$.*

Proof. First suppose that $\gcd(n, \phi(n)) = 1$. Then there exist positive integers u and v such that

$$u\phi(n) - vn = 1.$$

Thus, for any positive integer m, we have that

$$u(m-1)\phi(n)+1 = m + v(m-1)n.$$

Choosing $x = m+v(m-1)n$ ensures that x is a positive integer and $x \equiv m \pmod{n}$. Since $\gcd(n, \phi(n)) = 1$, n must be square-free. Hence, we have by Lemma 2 that

$$x^x \equiv m^{m+v(m-1)n} \equiv m^{u(m-1)\phi(n)+1} \equiv m \equiv x \pmod{n}.$$

Next, suppose that $\gcd(n, \phi(n)) \neq 1$. If n is not square-free, then there exists a prime p such that $n \equiv 0 \pmod{p^2}$. Let $m = n/p$. Then $m^t \equiv 0 \pmod{n}$ for all $t > 1$. Thus, there is no $x \equiv m \pmod{n}$ satisfying (1.2).

Now suppose that n is square-free. Since $\gcd(n, \phi(n)) \neq 1$, there exist distinct primes p and q such that

$$n \equiv 0 \pmod{pq} \quad \text{and} \quad p \equiv 1 \pmod{q}. \tag{3}$$

Notice then that there exists some integer z such that $\mathrm{ord}_p(z) = q$. Thus, using the Chinese Remainder Theorem, there exists an integer a relatively prime to n satisfying

$$a \equiv z \pmod{p} \qquad \text{and} \qquad a \equiv 1 \pmod{q}. \tag{4}$$

Suppose that

$$\left(\frac{n+aq}{q}\right)^{\frac{n+aq}{q}+nt} \equiv \frac{n+aq}{q} \pmod{n}$$

for some integer t. Since $\gcd(a, n) = 1$, we know from (3) that

$$\frac{n+aq}{q} \equiv a \not\equiv 0 \pmod{p}.$$

Also, from (4), we see that $\mathrm{ord}_p(a) = q$, Thus, from (3) and (4), it follows that

$$1 \equiv \left(\frac{n+aq}{q}\right)^{\frac{n+aq}{q}+nt-1} \equiv a^{n/q+a+nt-1} \equiv a^{n/q+a-1} \equiv a^{n/q} \not\equiv 1 \pmod{p}.$$

Hence, there is no integer $x \equiv \frac{n+aq}{q} \pmod{n}$ such that $x^x \equiv x \pmod{n}$. □

We get the following immediate corollary of Theorem 4 in the special case of when n is prime.

Corollary 1. *Let $n = p$ be a prime. For every integer m with $0 \leq m \leq p-1$, there exists a positive integer x such that $x \equiv m \pmod{p}$ and x is a solution to (2).*

4. Nontrivial Solutions in $\mathcal{S}_n$

As mentioned in Section 1, the authors of [7] show that for almost all primes p, there exists a nontrivial solution $x \in \mathcal{S}_p$. Their proof uses Galois theory of Kummer extensions, along with some analytic techniques. One ponders if a weaker, but still interesting, result can be established using only elementary methods. For example, can it be shown in an elementary manner that there exist infinitely many primes p for which there exists a nontrivial solution to (1)? We answer this question in the affirmative in the following proposition.

Proposition 2. *Let $p \equiv \pm 1 \pmod 8$. Then $(p+1)/2 \in \mathcal{S}_p$.*

Proof. Since $p \equiv \pm 1 \pmod 8$, then $\left(\frac{2}{p}\right) = 1$. Thus, by Euler's criterion, we have that $2^{(p-1)/2} \equiv 1 \pmod p$, which can be rewritten as

$$\left(\frac{1}{2}\right)^{(p+1)/2} \equiv \frac{1}{2}.$$

Since $(p+1)/2 \equiv 1/2 \pmod p$, the proposition follows. □

We turn now to the situation when n is composite. Our main result here is that, unlike the case when n is a prime, $\mathcal{S}_n$ always contains a nontrivial solution in this situation. We first need a definition.

Definition 5. Let $n \geq 4$ be composite. We define

$$\lambda := \phi(n) + 1.$$

Lemma 3. *Let $n \geq 4$ be a composite number and let $d = \gcd(\lambda, n)$. Then*

$$d^{\phi(n)} \equiv 1 \pmod{n/d}.$$

Proof. The lemma is clearly true if $d = 1$, so suppose that $d > 1$ and let p be a prime such that $d \equiv 0 \pmod p$. Then $n \equiv 0 \pmod p$. If $n \equiv 0 \pmod{p^2}$, then $\phi(n) \equiv 0 \pmod p$, which is impossible since $\lambda \equiv 0 \pmod p$. Hence, d is square-free and $\gcd(d, n/d) = 1$. Thus,

$$d^{\phi(n/d)} \equiv 1 \pmod{n/d}. \tag{5}$$

Since $n \equiv 0 \pmod{n/d}$, we have that $\phi(n) \equiv 0 \pmod{\phi(n/d)}$, and the lemma follows from (5). □

We now prove the main result of this section.

Theorem 6. *Let n be a composite number. Then there exists a nontrivial $x \in \mathcal{S}_n$.*

Proof. First note that $2 < \lambda < n-1$ since n is composite. Let $d = \gcd(\lambda, n)$. Since

$$\gcd\left(\frac{\lambda}{d}, \frac{n}{d}\right) = 1,$$

we have that

$$\left(\frac{\lambda}{d}\right)^{\phi(n/d)} \equiv 1 \pmod{n/d}.$$

Thus,

$$\left(\frac{\lambda}{d}\right)^{\phi(n)} \equiv 1 \pmod{n/d}, \tag{6}$$

since $\phi(n) \equiv 0 \pmod{\phi(n/d)}$. Then, multiplying both sides of the congruence in (6) by λ/d, and using Lemma 3, it follows that

$$\begin{aligned}\frac{\lambda}{d} &\equiv \left(\frac{\lambda}{d}\right)^{\lambda} \pmod{n/d} \\ &\equiv \frac{\lambda^{\lambda}}{d^{\lambda}} \pmod{n/d} \\ &\equiv \frac{\lambda^{\lambda}}{d} \pmod{n/d}.\end{aligned}$$

Therefore,

$$\lambda^{\lambda} \equiv \lambda \pmod{n},$$

and the theorem is established with $x = \lambda$. □

5. The Structure of $\mathcal{S}_n$

In this section, we delve further into the nature of the elements of $\mathcal{S}_n$. In particular, we are interested in the algebraic structure of $\mathcal{S}_n$.

Proposition 3. *Let $n \geq 2$ be an integer. Then $\mathcal{S}_n$ contains all nonzero squares modulo n if and only if $n \in \{6, 12, 18, 36\}$.*

Proof. The proposition can be checked computationally for $n \leq 64$. For $n \geq 64$, $4^4 \not\equiv 4 \pmod{n}$. Thus, $4 \notin \mathcal{S}_n$ for any $n \geq 64$. □

Theorem 7. *Let $n \geq 2$ be an integer, and let $\omega(n)$ be the number of distinct prime divisors of n. Then there exists a nontrivial $x \in \mathcal{S}_n$, such that $\gcd(x, n) > 1$, if and only if $\omega(n) \geq 2$. Moreover, if $\omega(n) \geq 2$, then there are at least $2^{\omega(n)} - 2$ such solutions.*

Proof. Suppose first that $\omega(n) = 1$ and let $n = p^a$, for some prime p and integer $a \geq 1$. Clearly, if $a = 1$, then no element $x \in \mathcal{S}_n$ exists with $\gcd(x, n) > 1$. So assume that $a \geq 2$ and let x be such an element of $\mathcal{S}_n$. Since $x^x \equiv x \pmod{p^a}$ and $x \not\equiv 0 \pmod{p^a}$, it follows that $x^{x-1} \equiv 1 \pmod{p}$, which is impossible since $x \equiv 0 \pmod{p}$.

Now suppose that $\omega(n) \geq 2$, and let $n = \prod_{i=1}^{\omega(n)} p_i^{a_i}$ be the product of n into distinct prime powers. Let

$$\mathcal{P} = \left\{ p_1^{a_1}, p_2^{a_2}, \ldots, p_{\omega(n)}^{a_{\omega(n)}} \right\},$$

and let $\mathcal{T}$ be any nonempty proper subset of $\mathcal{P}$. Let T be the product of all elements of $\mathcal{T}$, and let Q be the product of all elements of $\mathcal{P} \setminus \mathcal{T}$. Then there exists b, with $1 \leq b < Q$, such that

$$bT \equiv 1 \pmod{Q}.$$

Thus

$$(bT)^{bT-1} \equiv 1 \pmod{Q},$$

so that

$$bT^{bT} = bT\,(bT)^{bT-1} \equiv bT \pmod{QT} = bT \pmod{n}.$$

Hence, $x = bT \in \mathcal{S}_n$, since $2 \leq x \leq QT - 1 = n - 1$. Since there are $2^{\omega(n)} - 2$ such subsets $\mathcal{T}$ of $\mathcal{P}$, and the values bT are distinct modulo n for each of the subsets $\mathcal{T}$, the result follows. □

The following is immediate from Theorem 7.

Corollary 2. *Let n be such that $\omega(n) \geq 2$. Then $\mathcal{S}_n$ is not a subgroup of U_n.*

The following theorem establishes the fact that $\mathcal{S}_n$ contains a nontrivial subgroup of U_n when $n \equiv 0 \pmod{p^2}$ for every prime p with $n \equiv 0 \pmod{p}$.

Theorem 8. *Let $n \geq 4$ be a composite integer, and let $n = \prod_{i=1}^{k} p_i^{a_i}$ be the factorization of n into distinct prime powers. Let $\kappa = \prod_{i=1}^{k} p_i$. Let λ be as in Definition 5, and let*

$$L := \left\{ \lambda^j \pmod{n} \,\middle|\, j \geq 1 \right\}.$$

If $a_i \geq 2$ for all i, then $\lambda \in U_n$, and L is a subgroup of U_n, with $\kappa \equiv 0 \pmod{|L|}$, that is completely contained in $\mathcal{S}_n$.

Proof. Since $a_i \geq 2$ for all i, it follows that $\gcd(\lambda, n) = 1$. Therefore, $\lambda \in U_n$, and hence L is a subgroup of U_n. Note that $\lambda \not\equiv 1 \pmod{n}$. Since $\phi(n) \equiv 0 \pmod{p^{a_i - 1}}$ for all i, we conclude that $\lambda^\kappa \equiv 1 \pmod{n}$. Thus, $|L|$ is a divisor of κ by Lagrange's theorem.

We know from Theorem 6 and Lemma 1 that λ^e is a solution to (2) for each e with $1 \leq e \leq |L|$. That is, we have

$$(\lambda^e)^{\lambda^e} \equiv \lambda^e \pmod{n}. \tag{7}$$

Suppose that $m \equiv \lambda^e \pmod{n}$. Since $n \equiv 0 \pmod{\kappa}$ and $\kappa \equiv 0 \pmod{|L|}$, we deduce that $m \equiv \lambda^e \pmod{|L|}$. Thus, $\lambda^e = m + z\,|L|$ for some $z \in \mathbb{Z}$. Hence, since $(\lambda^e)^{|L|} \equiv 1 \pmod{n}$, it follows from (7) that

$$m \equiv \lambda^e \equiv (\lambda^e)^{\lambda^e} \equiv (\lambda^e)^{m+z|L|} \equiv (\lambda^e)^m \left((\lambda^e)^{|L|}\right)^z \equiv (\lambda^e)^m \equiv m^m \pmod{n}.$$

Thus, m is a solution to (2) and $L \subseteq \mathcal{S}_n$, which completes the proof. □

A natural question to ask is whether the order of L in Theorem 8 can be determined precisely. In general, this seems to be a difficult question. However, the answer is immediate in a special case, which is the focus of the next section.

5.1. A Special Case: $n = p^a$

In this section, our main focus is on the special case of when $n = p^a$, for some prime p and integer a. Unless stated otherwise, we assume throughout this section that $a \geq 2$. We begin with the statement of an immediate corollary to Theorem 8 for this special case.

Corollary 3. *Let $k = 1$ in the statement of Theorem 8. Then $|L| = p$.*

The next theorem gives a situation where certain solutions to (2) can be ruled out, but first we give a simple lemma.

Lemma 4. *Let $a \geq 1$ be an integer. Then $\mathcal{S}_{p^a} \subseteq U_{p^a}$.*

Proof. Let $x \in \mathcal{S}_n$. Then $x\left(x^{x-1} - 1\right) \equiv 0 \pmod{p^a}$ and $x \not\equiv 0 \pmod{p^a}$. Thus, $x^{x-1} \equiv 1 \pmod{p}$. Hence, $x \not\equiv 0 \pmod{p}$, and therefore $x \in U_{p^a}$. □

Theorem 9. *Let $a \geq 1$ be an integer, and let p be an odd prime. If $x \in \mathcal{S}_{p^a}$, then x is not a primitive root modulo p^a.*

Proof. We proceed by way of contradiction. Let $x \in \mathcal{S}_{p^a}$. Then $x^{x-1} \equiv 1 \pmod{p^a}$ as in the proof of Lemma 4, and if x is a primitive root, we deduce that

$$x - 1 \equiv 0 \pmod{\phi(p^a)},$$

with $2 \leq x \leq p^a - 2$. Hence,

$$k(p^a - p^{a-1}) = k\phi\left(p^a\right) = x - 1 \leq p^a - 3 < p^a,$$

for some integer $k \geq 1$. Thus, $k = 1$ and $x = p^a - p^{a-1} + 1$, so that $a \geq 2$. Therefore, using the binomial theorem, it follows that

$$x^{2p} \equiv \left(p^{a-1} - 1\right)^{2p} \equiv 1 \pmod{p^a}.$$

We conclude that

$$2p \equiv 0 \pmod{p^a - p^{a-1}},$$

since the order of x modulo p^a is $p^a - p^{a-1}$. Consequently, $p^a - p^{a-1} \leq 2p$, or equivalently, $p^{a-2}(p-1) \leq 2$, which is impossible unless $p = 3$ and $a = 2$. In this case, we see that $x = 7$ is indeed a solution to (2) when $n = 9$. However, the order of 7 modulo 9 is 3, so that 7 is not a primitive root modulo 9. □

Remark 10. The proof of Theorem 9 can be modified to show that the result is also true for $n = 2p^a$, where p is an odd prime and $a \geq 1$ is an integer..

Theorem 9 gives us a natural upper bound on $|\mathcal{S}_{p^a}|$ when p is an odd prime and $a \geq 1$ is an integer.

Corollary 4. *Let p be an odd prime. Then*

$$|\mathcal{S}_{p^a}| \leq \begin{cases} p - 1 - \phi(p-1) & \text{if } a = 1 \\ p^{a-2}(p-1)\left(p - \phi(p-1)\right) & \text{if } a \geq 2, \end{cases}$$

where ϕ is Euler's totient function.

Proof. Since $|U_{p^a}| = \phi(p^a)$, and the number of primitive roots is $\phi(\phi(p^a))$, we have from Lemma 4 and Theorem 9 that

$$|\mathcal{S}_{p^a}| \leq \phi(p^a) - \phi(\phi(p^a)),$$

and the corollary follows. □

Remark 11. It has been shown in [1] that

$$|\mathcal{S}_p \setminus \{1\}| \leq p^{1/3 + o(1)},$$

and a slightly stronger result can be deduced from the work in [3]. Also, numerical evidence suggests that when $a \geq 2$, the bound in Corollary 4 is quite weak. (See Theorem 19 later in this paper.)

We now investigate further the algebraic structure of $\mathcal{S}_{p^a}$.

Lemma 5. *Let p be an odd prime, and let $x = p^b z + 1$, where b and z are integers, with $1 \leq b \leq a - 1$ and $z \not\equiv 0 \pmod{p}$. Then $\operatorname{ord}_{p^a}(x) = p^{a-b}$.*

Proof. Let m be a positive integer. Using the binomial theorem, we see that

$$x^{p^m} = \left(p^b z + 1\right)^{p^m} = 1 + \sum_{k=0}^{p^m-1} T_k,$$

where

$$T_k = \binom{p^m}{k} \left(p^b z\right)^{p^m-k}.$$

By Proposition 1, we conclude that

$$\nu_p\left(T_k\right) = \begin{cases} bp^m & \text{if } k = 0 \\ m - \nu_p(k) + bp^m - bk & \text{if } k \geq 1. \end{cases}$$

Since

$$m \leq 2^m - 1 \leq p^m - 1 \leq b\left(p^m - 1\right),$$

we have that

$$m + b \leq bp^m \leq m + b\left(p^m - 1\right). \tag{8}$$

Note that $\nu_p\left(T_k\right)$ is a nonincreasing function of k on the interval $[1, p^m - 1]$. Thus, from (8), it follows that

$$\min_{k\in[0,p^m-1]} \nu_p\left(T_k\right) = m + b \quad \text{and} \quad \max_{k\in[0,p^m-1]} \nu_p\left(T_k\right) = m + b\left(p^m - 1\right),$$

which occur at $k = p^m - 1$ and $k = 1$, respectively. Therefore, $x^{p^m} \equiv 1 \pmod{p^a}$ if and only if $m \geq a - b$, and consequently $\mathrm{ord}_{p^a}(x) = p^{a-b}$. □

Definition 12. Define

$$\alpha := \begin{cases} p^{a/2} + 1 & \text{if } a \equiv 0 \pmod 2 \\ p^{(a+1)/2} + 1 & \text{if } a \equiv 1 \pmod 2. \end{cases}$$

Noting that $\alpha \in U_{p^a}$, we define A to be the subgroup of U_{p^a} generated by α.

Theorem 13. *Let α and A be as in Definition 12. Then*

$$|A| = \begin{cases} p^{a/2} & \text{if } a \equiv 0 \pmod 2 \\ p^{(a-1)/2} & \text{if } a \equiv 1 \pmod 2 \end{cases}$$

and $A \subseteq \mathcal{S}_{p^a}$.

Proof. We provide details only in the case $a \equiv 0 \pmod 2$ since the proof when $a \equiv 1 \pmod 2$ is similar. From Lemma 5 with $b = a/2$, we have that $\mathrm{ord}_{p^a}(\alpha) = p^{a/2}$. Hence, $|A| = p^{a/2}$.

Using the binomial theorem, it is easy to see that

$$\alpha^{\alpha} \equiv \left(p^{a/2}+1\right)^{p^{a/2}+1} \equiv p^{a/2}+1 \equiv \alpha \pmod{p^a},$$

so that $\alpha \in \mathcal{S}_{p^a}$. Now let k be an integer with $2 \leq k < p^{a/2}$. Since $\alpha \in \mathcal{S}_{p^a}$, we know from Lemma 1 that

$$\left(\alpha^k\right)^{\alpha^k} \equiv \alpha^k \pmod{p^a}.$$

Suppose that $\alpha^k \equiv m \pmod{p^a}$, where $1 \leq m < p^a$. Then $\alpha^k \equiv m \pmod{p^{a/2}}$, and so we can write $\alpha^k = p^{a/2}z+m$ for some integer z. Therefore, since $\mathrm{ord}_{p^a}(\alpha) = p^{a/2}$, it follows that

$$m \equiv \alpha^k \equiv \left(\alpha^k\right)^{\alpha^k} \equiv \left(\alpha^{p^{a/2}z+m}\right)^k \equiv \left(\alpha^{p^{a/2}}\right)^{kz} \alpha^{km} \equiv \left(\alpha^k\right)^m \equiv m^m \pmod{p^a}.$$

Hence, $A \subseteq \mathcal{S}_{p^a}$. □

The following simple lemma will be helpful in our investigation.

Lemma 6. *Let A be the group defined in Definition 12. Then*

$$A = \begin{cases} \left\{p^{a/2}z+1 \,\middle|\, z = 0,1,\ldots,p^{a/2}-1\right\} & \text{if } a \equiv 0 \pmod 2 \\ \left\{p^{(a+1)/2}z+1 \,\middle|\, z = 0,1,\ldots,p^{(a-1)/2}-1\right\} & \text{if } a \equiv 1 \pmod 2. \end{cases}$$

Proof. Use the binomial theorem to expand powers of α modulo p^a, where α is as defined in Definition 12. □

Corollary 5. *For $n = p^a$, let L be as defined in Theorem 8. Then $L \subseteq A$.*

Proof. If $a \equiv 0 \pmod 2$, then

$$\lambda = \phi\left(p^a\right)+1 = p^{a-1}(p-1)+1 = p^{a/2}\left(p^{a/2-1}(p-1)\right)+1 \in A,$$

since $p^{a/2-1}(p-1) \leq p^{a/2}-1$. The proof is similar when $a \equiv 1 \pmod 2$. □

Theorem 14. *If $x \in \mathcal{S}_{p^a}$, then*

$$p \equiv 1 \pmod{\mathrm{ord}_{p^a}(x)} \quad \text{or} \quad \mathrm{ord}_{p^a}(x) = p^c \quad \text{with} \quad 0 \leq c \leq a/2. \tag{9}$$

Proof. Note that the theorem is clearly true for $x = 1 \in \mathcal{S}_{p^a}$. So, let $x \in \mathcal{S}_{p^a}$, with $x \neq 1$. Suppose first that $p \geq 3$. We know from Lemma 4 that $x \in U_{p^a}$. Thus, we can write

$$\mathrm{ord}_{p^a}(x) = p^s t,$$

for some nonnegative integer s and positive integer t, with $0 \leq s \leq a-1$ and $p \equiv 1 \pmod{t}$, so that $t \not\equiv 0 \pmod{p}$. Since $x \equiv 1 \pmod{\operatorname{ord}_{p^a}(x)}$, we have that

$$x = p^b tz + 1,$$

for some nonnegative integer b and positive integer z, with $s \leq b \leq a-1$ and $z \not\equiv 0 \pmod{p}$. If $b = 0$, then $s = 0$ and the first congruence in (9) holds. If $b > 0$, then, by Lemma 5, we deduce that $\operatorname{ord}_{p^a}(x) = p^{a-b}$, so that $t = 1$ and $x = p^b z + 1$. Since $\gcd(z, p) = 1$, we have that

$$\operatorname{ord}_{p^a}(x^z) = p^{a-b} \tag{10}$$

as well. Also, since $x \in \mathcal{S}_n$, we see that

$$(x^z)^{p^b} = x^{x-1} \equiv 1 \pmod{p^a}. \tag{11}$$

Thus, from (10) and (11), we conclude that $a - b \leq b$, or equivalently, $-b \leq -a/2$, which implies that

$$c := a - b \leq a - a/2 = a/2,$$

and the proof is complete when $p \geq 3$.

Now suppose that $p = 2$. By inspection, it is easy to verify that the theorem is true for $a = 2$. Suppose then that $a \geq 3$. In this situation, we have that

$$\{1, 3, 5, \ldots, 2^a - 1\} = U_{2^a} \simeq \mathbb{Z}_2 \times \mathbb{Z}_{2^{a-2}}, \tag{12}$$

and therefore $\operatorname{ord}_{2^a}(x) = 2^c$, where $0 < c \leq a-2$. We give details only in the case $a \equiv 0 \pmod{2}$ since the other case is similar. We must show that, in fact, $c \leq a/2$. Assume, by way of contradiction, that $c \geq (a+2)/2$. Then, since $x \equiv 1 \pmod{\operatorname{ord}_{2^a}(x)}$, we can write $x = 2^{(a+2)/2} z + 1$, for some positive integer z. However, using the binomial theorem, we see that

$$\left(2^{(a+2)/2} z + 1\right)^{2^{a/2}} \equiv 1 \pmod{2^a},$$

which contradicts the assumption that $c \geq (a+2)/2$, and the proof is complete. □

Theorem 14 tells us that the set $\mathcal{S}_{p^a}$ can be partitioned into two subsets: the set of elements in $\mathcal{S}_{p^a}$ whose orders are powers of p (which is simply the group A), and the set $\mathcal{R}$ of elements in $\mathcal{S}_{p^a}$ whose orders are divisors $d > 1$ of $p-1$, when $p \geq 3$, and whose orders are 2, when $p = 2$. We observe that $\mathcal{R}$ is sometimes empty, so that $\mathcal{S}_{p^a} = A$. For example, it is easy to show that $\mathcal{S}_{p^a} = A$ when $n = 5$ and $a = 2$. However, if $p = 5$ and $a = 3$, then $x = 57 \in \mathcal{R}$. Thus, we are motivated to make the following definition.

Definition 15. Let A be the subgroup defined in Definition 12. We define a *rogue element modulo* p^a (or simply a *rogue*, if the context is clear) to be any element $x \in \mathcal{R} := \mathcal{S}_{p^a} \setminus A$.

The next theorem classifies all rogue elements in the special case when $p = 2$.

Theorem 16. *Let $n = 2^a$. Then*

$$\mathcal{R} = \begin{cases} \emptyset & \text{if } a = 2 \\ \left\{2^{a-1} - 1, 2^a - 1\right\} & \text{if } a > 2 \end{cases}$$

Proof. We give details only in the case of $a \equiv 0 \pmod 2$ since the other case is similar. By Lemma 6, we have

$$A = \left\{ 2^{a/2} z + 1 \;\middle|\; z = 0, 1, \ldots, 2^{a/2} - 1 \right\}. \tag{13}$$

It is easy to see that $\mathcal{R}$ is empty when $a = 2$. Suppose then that $a \geq 4$. We show first that $\left\{2^{a-1} - 1, 2^a - 1\right\} \subseteq \mathcal{R}$. Using the binomial theorem, we have that

$$\left(2^{a-1} - 1\right)^{2^{a-1}-1} \equiv 2^{a-1} - 1 \pmod{2^a},$$

so that $2^{a-1} - 1 \in \mathcal{S}_n$. Suppose that $2^{a-1} - 1 \in A$. Then

$$2^{a/2} z + 1 \equiv 2^{a-1} - 1 \pmod{2^a},$$

for some $z \in \{0, 1, \ldots, 2^{a/2} - 1\}$. Consequently,

$$2^{(a+2)/2} z + 2 \equiv -2 \pmod{2^a},$$

from which it follows that

$$2^{(a-2)/2} z + 1 \equiv 0 \pmod{2^{a-2}},$$

which is impossible since $a \geq 4$. Hence, $2^{a-1} - 1$ is a rogue.

Note that

$$(2^a - 1)^{2^a - 1} \equiv (-1)^{2^a - 1} \equiv -1 \equiv 2^a - 1 \pmod{2^a},$$

and so $2^a - 1 \in \mathcal{S}_{2^a}$. An argument identical to the one used to show that $2^{a-1} - 1 \notin A$ shows that $2^a - 1 \notin A$. Hence, $2^a - 1$ is a rogue.

Now let $x \in \mathcal{R}$. Note that $x \neq 1$. Hence, by Theorem 14, $\mathrm{ord}_{2^a}(x) = 2^c$, for some c with $2 \leq c \leq a/2$. From (12), we see that U_{2^a} contains exactly 2^c elements of order 2^c for each such c, and exactly 2^{c-1} of these elements are elements of A. These elements of A are precisely the elements $y \in U_{2^a}$ such that $y \equiv 1 \pmod{2^c}$. In other words, A contains all elements in $\mathcal{S}_{2^a}$ of order 2^c, for each such value of c. We deduce that any rogue elements must be elements in U_{2^a} of order 2, of which there are three: $2^{a-1} - 1$, $2^{a-1} + 1$ and $2^a - 1$. Since $2^{(a-2)/2} < 2^{a/2} - 1$, we have from (13) that

$$2^{a-1} + 1 = 2^{a/2} \left(2^{(a-2)/2}\right) + 1 \in A.$$

(Alternatively, $2^{a-1} + 1 \equiv 1 \pmod{2^c}$, so that $2^{a-1} + 1 \in A$.) Therefore, it follows that $x \in \left\{2^{a-1} - 1, 2^a - 1\right\}$. □

The next theorem, which is an immediate corollary of Theorem 14, provides necessary and sufficient conditions for an element in U_{p^a} to be a rogue element when $p^a \geq 9$.

Theorem 17. *Let p be an odd prime, and let $x \in U_{p^a}$, with $x \neq 1$. Then*

$$x \in \mathcal{R} \text{ if and only if } x - 1 \equiv p - 1 \equiv 0 \pmod{\operatorname{ord}_{p^a}(x)}.$$

Proof. Since $x \in U_{p^a}$, it follows that $x \in \mathcal{S}_{p^a}$ if and only if $x-1 \equiv 0 \pmod{\operatorname{ord}_{p^a}(x)}$. If $x \in \mathcal{S}_{p^a}$, it follows from Theorem 14 that $x \in \mathcal{R}$ if and only if $p - 1 \equiv 0 \pmod{\operatorname{ord}_{p^a}(x)}$. □

Example 18. Let $p = 7$ and $a = 3$. Then

$$\mathcal{S}_n = \{1, 19, 50, 99, 148, 197, 246, 295, 325\},$$

$$A = L = \{1, 50, 99, 148, 197, 246, 295\} \quad \text{and} \quad \mathcal{R} = \{19, 325\}.$$

The following corollary establishes the existence of infinitely many situations when $\mathcal{S}_{p^a} = A$.

Corollary 6. *Let $p = 3$ and $a \geq 2$. Then $\mathcal{R} = \emptyset$, so that $\mathcal{S}_{3^a} = A$.*

Proof. Let $x \in \mathcal{R}$. Since $x \notin A$, then $\operatorname{ord}_{3^a}(x) = 2$ by Theorem 17. But an easy check reveals that $x = 3^a - 1$, the only element of order 2 in U_{3^a}, does not satisfy (2). Hence, $\mathcal{R}$ is empty. □

With the exception of the rogue elements, we have shown that the algebraic structure of $\mathcal{S}_n$ when $n = p^a$, with $a \geq 2$, is quite nice. Although Theorem 17 gives necessary and sufficient conditions for the existence of these rogue elements when $p \geq 3$, the conditions are not particularly useful in providing an efficient algorithm for determining them.

We end this section with the following theorem.

Theorem 19. *Let p be a prime and let $a \geq 2$ be an integer. Then*

$$|\mathcal{S}_{p^a}| \leq \begin{cases} p^{a/2} + p & \text{if } a \equiv 0 \pmod 2 \\ p^{(a-1)/2} + p & \text{if } a \equiv 1 \pmod 2. \end{cases}$$

Proof. By Theorem 14, we have that

$$\mathcal{S}_{p^a} = A \cup \mathcal{R},$$

where A is the group as defined in Definition 12, and $\mathcal{R}$ is the set of rogue elements. When p is odd, the elements in $\mathcal{R}$ have orders that are divisors of $p - 1$. Hence, $|\mathcal{R}| \leq p - 1$ in that case. When $p = 2$, we have by Theorem 16 that $|\mathcal{R}| \leq 2$. Since $A \cap \mathcal{R} = \emptyset$, the theorem follows from Theorem 13. □

Remark 20. Theorem 19 improves the bound given in Corollary 4 except when $p = 3$ and $a = 2$.

5.2. One Last General Theorem

In this section we prove a theorem that gives sufficient conditions, from the structure of $\mathcal{S}_n$, for the primality of n.

Theorem 21. *Let $n \geq 2$ be an integer. If no $x \in \mathcal{S}_n$ exists with $19n/27 \leq x \leq n-1$, then n is prime.*

Proof. We prove the contrapositive by assuming that n is composite and considering the following three cases:

1. $n \equiv 0 \pmod 2$, with $n \geq 4$
2. $n = 3^a$, for some integer $a \geq 2$
3. n is not contained in the previous two cases.

First suppose that $n \equiv 0 \pmod 2$, with $n \geq 4$, and let $x = n - 1$. Then, since $n - 1$ is odd,

$$x^x \equiv (n-1)^{n-1} \equiv (-1)^{n-1} \equiv -1 \equiv n - 1 \equiv x \pmod n,$$

so that $x \in \mathcal{S}_n$. Since $n \geq 4 \geq 27/8$, it follows that $x = n - 1 \geq 19n/27$.

Now suppose that $n = 3^a$, for some integer $a \geq 2$, where $a \equiv 0 \pmod 2$. Let

$$x = n - \left(3^{a/2} - 1\right) = 3^a - 3^{a/2} + 1 = 3^{a/2}\left(3^{a/2} - 1\right) + 1.$$

Then $x \in \mathcal{S}_{3^a}$ by Theorem 13 and Lemma 6, and it is straightforward to show that $x \geq 19n/27$. In the situation when $a \equiv 1 \pmod 2$, we let $x = 3^a - 3^{(a+1)/2} + 1$ and the proof is similar.

Finally, suppose that n is in Case 3., and let $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ be the factorization of n into distinct prime powers, where $p_1 < p_2 < \cdots < p_k$. Let

$$x = n - p_k^{\alpha_k - 1} \prod_{i=1}^{k-1} p_i^{\alpha_i} + 1 = \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right) \prod_{i=1}^{k-1} p_i^{\alpha_i} + 1, \tag{14}$$

so that

$$x^{x-1} - 1 = \left(\left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right) \prod_{i=1}^{k-1} p_i^{\alpha_i} + 1\right)^{\left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right) \prod_{i=1}^{k-1} p_i^{\alpha_i}} - 1, \tag{15}$$

where $\prod_{i=1}^{k-1} p_i^{\alpha_i} = 1$ if $k = 1$. If $\alpha_k \geq 2$, then we see from (15) that

$$x^{x-1} - 1 \equiv 0 \pmod{p_i^{\alpha_i}} \tag{16}$$

for all i, and hence $x^x \equiv x \pmod{n}$ by the Chinese Remainder Theorem. If $\alpha_k = 1$, then (16) holds for all i with $1 \leq i \leq k-1$. If

$$\prod_{i=1}^{k-1} p_i^{\alpha_i} - 1 \equiv 0 \pmod{p_k},$$

then $x \equiv 0 \pmod{p_k}$, and so $x^x \equiv x \pmod{n}$ by the Chinese Remainder Theorem. If

$$\prod_{i=1}^{k-1} p_i^{\alpha_i} - 1 \not\equiv 0 \pmod{p_k},$$

then $x^{x-1} \equiv 1 \pmod{p_k}$ by Fermat's Little Theorem, and thus $x^x \equiv x \pmod{n}$, again by the Chinese Remainder Theorem. Therefore, for any value of n in this third case, we have that $x \in \mathcal{S}_n$.

We show now that $19n/27 \leq x \leq n-1$. From the fact that n is not contained in the first two cases, we deduce that $p_k \geq 5$. Then, using (14), we have that

$$n - x = p_k^{\alpha_k - 1} \prod_{i=1}^{k-1} p_i^{\alpha_i} - 1 \geq \begin{cases} 2 & \text{if } \alpha_k = 1 \\ 4 & \text{if } \alpha_k > 1. \end{cases}$$

Hence, $x < n - 1$. Since

$$p_k \geq 5 > \frac{27}{8},$$

it follows (with some algebra) that

$$p_k - 1 > \frac{19 p_k}{27}.$$

Therefore, again using (14), it follows that

$$x - 1 = p^{\alpha_k - 1} (p_k - 1) \prod_{i=1}^{k-1} p_i^{\alpha_i} > \frac{19n}{27},$$

and the proof is complete. □

Remark 22. The value of x used in Case 3. of the proof of Theorem 21 also satisfies $x \in \mathcal{S}_n$ in Case 1. and Case 2. However, in those two cases, that value of x does not always satisfy the lower bound constraint.

We observe that the largest element in $\mathcal{S}_n$ when $n = 3^3$ is $x = 19$ so that $x = 19n/27$ for this particular value of n. In other words, the lower bound of $19n/27$ in Theorem 21 is, in some sense, the best possible. We also note that Theorem 6 is an immediate corollary of Theorem 21. Additionally, the converse of Theorem 21 is false, and we conjecture that there are infinitely many counterexamples. The

smallest is $p = 17$, where $13 \in \mathcal{S}_{17}$ since $13^{13} \equiv 13 \pmod{17}$, but $13 > (19 \cdot 17)/27$. However, we also conjecture that there are infinitely many primes for which the converse of Theorem 21 is true.

Acknowledgements The authors thank the referee for the many suggestions that improved the paper.

References

[1] A. Balog, K. Broughan and I. Shparlinski, On the number of solutions of exponential congruences, *Acta Arith.* **148** (2011), no. 1, 93–103.

[2] A. Balog, K. Broughan and I. Shparlinski, Sum-products estimates with several sets and applications, *Integers* **12** (2012), no. 5, 895–906.

[3] J. Cilleruelo and M. Garaev, On the congruence $x^x \equiv \lambda \pmod{p}$, *arXiv:1503.02730v1 [math.NT].*

[4] R. Crocker, On a new problem in number theory, *Amer. Math. Monthly* **73** (1966), 355–357.

[5] R. Crocker, On residues of n^n, *Amer. Math. Monthly* **76** (1969), 1028–1029.

[6] J. Holden and P. Moree, Some heuristics and results for small cycles of the descrete logarithm, *Math. Comp.* **75** (2006), 419–449.

[7] P. Kurlberg, F. Luca and I. Shparlinski On the fixed points of the map $x \mapsto x^x$ modulo a prime, *Math. Res. Lett.* **22** (2015), no. 1, 141–168.

[8] E. E. Kummer,Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, *Journal fur die reine und angewandte Mathematik* **44** (1852), 93–146.

[9] L. Somer, The residues of n^n modulo p, *The Fibonacci Quart* **19** (1981), 110–117.