Journal of Integer Sequences, Vol. 26 (2023),
Article 23.8.1

Counting Integers Representable as Sums of k-th Powers Modulo n

Fabián Arias
Departamento de Matemáticas
Universidad del Atlántico
Barranquilla, 081007
Colombia
farias374@hotmail.com

Jerson Borja and Samuel Anaya
Departamento de Matemáticas y Estadística
Universidad de Córdoba
Montería, 230002
Colombia
jersonborjas@correo.unicordoba.edu.co
samuelanayai@correo.unicordoba.edu.co

Abstract

Given a polynomial $f(x_1, x_2, \ldots, x_t)$ in t variables with integer coefficients and a positive integer n, we define $\alpha(n)$ as the number of integers $0 \leq a < n$ such that the congruence $f(x_1, x_2, \ldots, x_t) \equiv a \pmod{n}$ is solvable.

We improve some known results for computing $\alpha(p^n)$, where p is prime and $n \geq 1$, for polynomials of the form $c_1 x_1^k + c_2 x_2^k + \cdots + c_t x_t^k$. We apply these results to calculate $\alpha(p^n)$ for polynomials of the form $x^k \pm y^k$ and to study the modular Waring problem.

1 Introduction

Additive number theory focuses on estimating the size of sumsets or characterizing the elements that can be expressed as sums of elements from a given set. One of the earliest problems in this context concerns the characterization of integers that can be expressed as sums of squares. Fermat's theorem states that an odd prime number p can be written as a sum of two squares if and only if p is of the form $4k+1$. Euler characterized the integers that can be represented as a sum of two squares. The Gauss-Legendre theorem gives a criterion for an integer n to be represented as a sum of three squares. Finally, Lagrange's theorem asserts that every nonnegative integer can be expressed as the sum of four squares. These results completely solve the problem of representing integers as sums of squares.

A natural question that arises when we consider a polynomial $f(x_1, \dots, x_t)$ with integer coefficients is to characterize the integers that can be expressed in the form $f(k_1, \dots, k_t)$, where $k_1, \dots, k_t$ are integers. We know the answer to this question for certain polynomials, such as $x^2 + y^2$, $x^2 + y^2 + z^2$, and $x^2 + y^2 + z^2 + w^2$.

Another well known problem in additive number theory is the Waring problem. It states that for every positive integer k, there exists a positive integer t such that every nonnegative integer can be written as a sum of t k-th powers. The Waring-Hilbert theorem establishes the existence of t for every k. The minimum value of such t is denoted by $g(k)$. For instance, $g(2) = 4$, $g(3) = 9$, $g(4) = 15$.

It is interesting to consider modular versions of the above problems. Specifically, let $f(x_1, \dots, x_t)$ be a polynomial with integer coefficients, $n \in \mathbb{Z}^+$, and let A_n be the set of all elements $a \in \{0, 1, \dots, n-1\}$ such that the congruence $f(x_1, x_2, \dots, x_t) \equiv a \pmod{n}$ has a solution. Let $\alpha(n)$ denote the size of A_n. In these terms, we consider the following questions:

1. Determine $\alpha(n)$ in terms of n.

2. Characterize all n such that $\alpha(n) = n$.

Harrington, Jones, and Lamarche [5] characterized the integers in $\mathbb{Z}_n$ that can be expressed as a sum of two nonzero squares in $\mathbb{Z}_n$, and they also determined the integers n such that $\alpha(n) = n$, for the function α associated with $x^2 + y^2$. Broughan [4] provided explicit calculations of $\alpha(n)$ for the polynomial x^3+y^3. Arias, Borja, and Rubio [3] found explicit formulas for $\alpha(n)$ in terms of the prime decomposition of n for the polynomials x^2+y^2, x^2-y^2, and $x^2 + y^2 + z^2$.

In this work, we study the aforementioned problems for polynomials of the form $c_1x_1^k + \cdots + c_tx_t^k$. We focus our attention on polynomials of the form x^k+y^k and x^k-y^k. In Section 2, we give slightly improvements of some results by Arias et al. [3] about polynomials of the form $c_1x_1^k + \cdots + c_tx_t^k$. One of these results is Proposition 4, which provides a method to compute $\alpha(p^n)$ for such polynomials. Then we apply these results to the computation of $\alpha(p^n)$ for polynomials of the form $x^k + y^k$ and $x^k - y^k$.

Finally, we consider the modular version of the Waring problem. It consists in determining the minimum positive integer $\gamma(k, n)$ such that every element in $\mathbb{Z}_n$ can be expressed as a sum of $\gamma(k, n)$ k-th powers in $\mathbb{Z}_n$. Small [8] showed a method to solve the modular Waring problem. Waring problem for diagonal forms has been treated recently, for instance by Alnaser and Cochrane [2]. We apply our techniques to compute $\alpha(p^n)$ for polynomials of the form $x_1^k + x_2^k + \cdots + x_t^k$, for $t \leq \gamma(k, n)$, and to determine the value $\max_n \gamma(k, n)$ for small values of k.

2 General results

We will follow the notation of [3]. For a prime p and $n \geq 1$ we define sets

$$A_{p^n} = \{a \in \{0, 1, \ldots, p^n - 1\} : f(x_1, \ldots, x_t) \equiv a \pmod{p^n} \text{ is solvable}\},$$

and

$$A_{p^n}(p^{n-1}) = \{a + jp^{n-1} : a \in A_{p^{n-1}}, 0 \leq j < p\}.$$

The inclusion $A_{p^n} \subseteq A_{p^n}(p^{n-1})$ holds and we set $N_{p^n} = A_{p^n}(p^{n-1}) \setminus A_{p^n}$.

We say that a nonnegative integer e is an *exponent of p in $f(x_1, \ldots, x_t)$,* if whenever p^e divides an integer of the form $f(m_1, \ldots, m_t)$, then the quotient $f(m_1, \ldots, m_t)/p^e$ is also of the form $f(q_1, \ldots, q_t)$, for some integers $q_1, \ldots, q_t$.

Now we show some results related to the function α associated with a polynomial of the form $f(x_1, x_2, \ldots, x_t) = c_1x_1^k + c_2x_2^k + \cdots + c_tx_t^k$, where $c_1, \ldots, c_t$ are integers and $k \geq 1$.

Proposition 1. *Let p be a prime number that does not divide $c_1, c_2, \ldots, c_t$, and let s be the highest nonnegative integer such that p^s divides k. Let $a \in A_{p^n}$ and suppose that the congruence*

$$c_1x_1^k + c_2x_2^k + \cdots + c_tx_t^k \equiv a \pmod{p^n}$$

has a solution, where at least one of the x_i's is not divisible by p. If at least one of the following conditions holds:

1. *p is odd and $n \geq s + 1$, or*

2. *$p = 2$ and $n \geq \min(s + 2, 2s + 1)$,*

then $a + jp^n \in A_{p^{n+1}}$, for all $0 \leq j < p$. Moreover, for all $0 \leq j < p$, the congruence

$$c_1x_1^k + c_2x_2^k + \cdots + c_tx_t^k \equiv a + jp^n \pmod{p^{n+1}}$$

has a solution, where at least one of the x_i's is not divisible by p.

Proof. The proof of this proposition, in the case $s \geq 1$, is similar to that of [1, Lemma 1]. In the case $s = 0$, the result follows from [3, Lemma 2.6]. □

Remark 2. Assume $n_0 \geq s + 1$, if p is an odd prime, or $n_0 \geq \min(s + 2, 2s + 1)$, if $p = 2$. If $a \in A_{p^{n_0}}$, then there are integers $m_1, \ldots, m_t$ such that $c_1m_1^k + \cdots + c_tm_t^k \equiv a \pmod{p^{n_0}}$. If $p \nmid a$, then at least one of the m_i's is not divisible by p. Thus, from Proposition 1 we conclude that $a + jp^{n_0} \in A_{p^{n_0+1}}$ for all $0 \leq j < p$. Hence, the only elements that might not belong to $A_{p^{n_0+1}}$ are those of the form $a+jp^{n_0}$, where $p \mid a$ and $0 \le j < p$. Therefore, under the assumption that the congruence

$$c_1x_1^k + c_2x_2^k + \cdots + c_tx_t^k \equiv a \pmod{p^{n_0}}$$

has a solution, where some x_i is not divisible by p, for every $a \in A_{p^{n_0}}$ such that $p \mid a$, then we get $A_{p^{n_0+1}} = \{a + jp^{n_0} : a \in A_{p^{n_0}}, 0 \le j < p\}$. So $\alpha(p^{n_0+1}) = p\alpha(p^{n_0})$, and an induction argument shows that $\alpha(p^n) = p^{n-n_0}\alpha(p^{n_0})$, for all $n \ge n_0$. We can now formulate the following result.

Proposition 3. *Let p be a prime number that does not divide $c_1, c_2, \ldots, c_t$, let s be the highest nonnegative integer such that p^s divides k, and n_0 be a positive integer. Assume that $n_0 \ge s+1$, if p is an odd prime, or $n_0 \ge \min(s+2, 2s+1)$, if $p = 2$. Suppose that for every $a \in A_{p^{n_0}}$ such that $p \mid a$, the congruence*

$$c_1x_1^k + c_2x_2^k + \cdots + c_tx_t^k \equiv a \pmod{p^{n_0}}$$

has a solution, where some x_i is not divisible by p. Then $\alpha(p^n) = p^{n-n_0}\alpha(p^{n_0})$ for all $n \ge n_0$.

Proposition 4. *Let p be a prime number that does not divide $c_1, c_2, \ldots, c_t$, and let s be the highest nonnegative integer such that p^s divides k. If p is odd, assume that the congruence*

$$c_1x_1^k + c_2x_2^k + \cdots + c_tx_t^k \equiv 0 \pmod{p^{s+1}}$$

has a solution, where some x_i is not divisible by p. Then $\alpha(p^n) = p^{n-s-1}\alpha(p^{s+1})$ for all $n \ge s+1$. If $p = 2$ and $k \ne 2$, define $\beta = \min(s+2, 2s+1)$ and assume that the congruence

$$c_1x_1^k + c_2x_2^k + \cdots + c_tx_t^k \equiv 0 \pmod{2^{\beta}}$$

has a solution, where some x_i is not divisible by 2. Then $\alpha(2^n) = 2^{n-\beta}\alpha(2^{\beta})$ for all $n \ge \beta$.

Proof. Assume p is an odd prime number. Write $k = p^s k_0$, where $p \nmid k_0$ and $s \ge 0$. Given $a \in A_{p^{s+1}}$, let us consider the congruence

$$c_1x_1^k + c_2x_2^k + \cdots + c_tx_t^k \equiv 0 \pmod{p^{s+1}}. \tag{1}$$

By hypothesis, if $a = 0$, then (1) has a solution where, some x_i is not divisible by p. The same conclusion is true, if $p \nmid a$.

Now assume $p \mid a$ and $a \ne 0$. Since $a \in A_{p^{s+1}}$, there are integers $m_1, \ldots, m_t, w$ such that $c_1m_1^k + c_2m_2^k + \cdots + c_tm_t^k = a + wp^{s+1}$. We want to prove that some m_i is not divisible by p. On the contrary, if all m_i's are divisible by p, then there exist integers $n_1, n_2, \ldots, n_t$ such that $m_i = pn_i$, for all $i \in \{1, \ldots, t\}$. Therefore, $p^k(c_1n_1^k + c_2n_2^k + \cdots + c_tn_t^k) = a + wp^{s+1}$, which shows that p^{s+1} divides a, since $k \ge s+1$. It follows that $a = 0$, which is a contradiction.

We have proved that for every $a \in A_{p^{s+1}}$, the congruence (1) has a solution, where at least one x_i is not divisible by p. By Proposition 3, we have $\alpha(p^n) = p^{n-s-1}\alpha(p^{s+1})$, for all $n \ge s+1$.

The proof for the case $p = 2$ is similar. □

Corollary 5. *Let p be a prime number that does not divide $k, c_1, c_2, \ldots, c_t$. If the congruence*

$$c_1x_1^k + c_2x_2^k + \cdots + c_tx_t^k \equiv 0 \pmod{p}$$

has a nontrivial solution, then $\alpha(p^n) = p^{n-1}\alpha(p)$, for all $n \geq 1$.

The hypothesis of Corollary 5 holds when $c_1 + c_2 + \cdots + c_t$ is divisible by p. Clearly, this occurs for a difference of k-th powers $x^k - y^k$.

Recall that N_{p^n} is the set of all elements of the form $a + jp^{n-1}$, $a \in \{0, 1, \ldots, p^{n-1} - 1\}$, $0 \leq j < p$ such that the congruence $c_1x_1^k + c_2x_2^k + \cdots + c_tx_t^k \equiv a \pmod{p^{n-1}}$ is solvable, but the congruence $c_1x_1^k + c_2x_2^k + \cdots + c_tx_t^k \equiv a + jp^{n-1} \pmod{p^n}$ is not solvable.

Proposition 6. *Let p be a prime number that does not divide $c_1, c_2, \ldots, c_t$, and s be the highest nonnegative integer such that p^s divides k. Then*

$$N_{p^r} \subseteq \{jp^{r-1} : 0 < j < p\},$$

for $s + 2 \leq r \leq k$, and

$$N_{p^{k+1}} \subseteq \{jp^k : j \notin A_p,\ 0 < j < p\}.$$

Moreover, if some exponent of p in $c_1x_1^k + c_2x_2^k + \cdots + c_tx_t^k$ divides k, then

$$N_{p^{k+1}} = \{jp^k : j \notin A_p,\ 0 < j < p\}.$$

Proof. Assume $s + 2 \leq r \leq k + 1$. Let us show that $a + jp^{r-1} \in A_{p^r}$, for all $a \in A_{p^{r-1}}$ with $a \neq 0$ and $0 \leq j < p$. Indeed, if $a \in A_{p^{r-1}}$ and $a \neq 0$, then there exist integers $m_1, \ldots, m_t$ such that

$$c_1m_1^k + c_2m_2^k + \cdots + c_tm_t^k \equiv a \pmod{p^{r-1}}.$$

If p divides all the m_i's, then p^{r-1} divides a because $s + 1 \leq r - 1 \leq k$. Since $0 \leq a < p^{r-1}$, it follows that $a = 0$, which is a contradiction. So, at least one m_i is not divisible by p. By Proposition 1, we have $a + jp^{r-1} \in A_{p^r}$, for all $0 \leq j < p$. Therefore, every element in N_{p^r} has the form jp^{r-1}, where $0 \leq j < p$. Since $0 \notin N_{p^r}$, we have $N_{p^r} \subseteq \{jp^{r-1} : 0 < j < p\}$.

Now, if $r = k + 1$ and $j \in A_p$, where $0 < j < p$, then there are integers $m_1, \ldots, m_t$ such that

$$c_1m_1^k + c_2m_2^k + \cdots + c_tm_t^k \equiv j \pmod{p},$$

from which

$$c_1(pm_1)^k + c_2(pm_2)^k + \cdots + c_t(pm_t)^k \equiv jp^k \pmod{p^{k+1}}.$$

This implies that $jp^k \in A_{p^{k+1}}$. Consequently, $N_{p^{k+1}} \subseteq \{jp^k : j \notin A_p, 0 < j < p\}$.

Finally, we assume that some exponent of p in $c_1x_1^k + c_2x_2^k + \cdots + c_tx_t^k$ divides k. If $jp^k \in A_{p^k}$, then $c_1m_1^k + c_2m_2^k + \cdots + c_tm_t^k \equiv jp^k \pmod{p^{k+1}}$ for some integers $m_1, m_2, \ldots, m_t$. Since $(c_1m_1^k + c_2m_2^k + \cdots + c_tm_t^k)/p^k = c_1q_1^k + c_2q_2^k + \cdots + c_tq_t^k$ for some integers $q_1, q_2, \ldots, q_t$, we obtain the congruence $c_1q_1^k + c_2q_2^k + \cdots + c_tq_t^k \equiv j \pmod{p}$, which shows that $j \in A_p$. Thus, $N_{p^{k+1}} = \{jp^k : j \notin A_p,\ 0 < j < p\}$. □

The following two results can be found in [3].

Proposition 7. *Let p be a prime and $k \geq 1$. Suppose that some exponent e of p in the polynomial $c_1x_1^k + \cdots + c_tx_t^k$ divides k. Then*

$$\alpha(p^n) = p\alpha(p^{n-1}) - |N_{p^r}|,$$

for all $n > 1$ such that $n \equiv r \pmod{k}$.

Proposition 8. *Let p be a prime and k be a positive integer. Suppose that some exponent e of p in the polynomial $c_1x_1^k + \cdots + c_tx_t^k$ divides k, and p does not divide $c_1, \ldots, c_t$. Let n be a positive integer. Then*

(*i*) *If $n \equiv 1 \pmod{k}$, then*

$$\alpha(p^n) = p^{n-1}\alpha(p) - \frac{p^{n-1}-1}{p^k-1}\sum_{j=2}^{k+1}|N_{p^j}|p^{k-j+1};$$

(*ii*) *If $n \equiv r \pmod{k}$, where $2 \leq r \leq k$, then*

$$\alpha(p^n) = p^{n-1}\alpha(p) - \frac{p^{n-1}-p^{r-1}}{p^k-1}\sum_{j=2}^{k+1}|N_{p^j}|p^{k-j+1} - \sum_{j=2}^{r}|N_{p^j}|p^{r-j}.$$

3 Some results from additive number theory

The following results from additive number theory can be consulted in [7].

Theorem 9 (Cauchy-Davenport)**.** *Let p be a prime number, and let A and B be nonempty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then*

$$|A+B| \geq \min(p, |A|+|B|-1).$$

By an induction argument, we see that if $B_1, B_2, \ldots, B_h$ are nonempty subsets of $\mathbb{Z}/p\mathbb{Z}$, then

$$|B_1 + B_2 + \cdots + B_h| \geq \min\left(p, \sum_{i=1}^{h}|B_i| - h + 1\right).$$

The following theorem gives us conditions to get equality in the Cauchy-Davenport theorem.

Theorem 10 (Vosper)**.** *Let p be a prime number, and let A and B be nonempty subsets of the group $G = \mathbb{Z}/p\mathbb{Z}$ such that $A + B \neq G$. Then*

$$|A+B| = |A| + |B| - 1$$

if and only if at least one of the following three conditions holds:

(i) $\min(|A|,|B|)=1$,

(ii) $|A+B|=p-1$ *and* $B=\overline{c-A}$ *(the complement of* $c-A$*), where* $\{c\}=G\setminus(A+B)$,

(iii) A *and* B *are arithmetic progressions with the same common difference.*

Proposition 11. *Let* $p>3$ *be a prime number, and let* $p\equiv 1 \pmod{k}$*, where* $1<k<(p-1)/2$*. If* $B_k=\left\{x^k : x\in\mathbb{Z}/p\mathbb{Z}\right\}$*, then* B_k *is not an arithmetic progression in* $\mathbb{Z}/p\mathbb{Z}$*.*

Following the terminology of Nathanson [7, Section 2.6], the polynomial $f(x_1,\ldots,x_t)=c_1x_1^k+\cdots+c_tx_t^k$ with coefficients in the finite field $\mathbb{Z}/p\mathbb{Z}$ is called a *diagonal form* of degree k. The *range* of f is the set

$$\mathrm{R}(f)=\{f(x_1,\ldots,x_t) : x_1,\ldots,x_t\in\mathbb{Z}/p\mathbb{Z}\}\,.$$

Note that $|\mathrm{R}(f)|=\alpha(p)$, where α is the function associated with $c_1x_1^k+\cdots+c_tx_t^k$.

Theorem 12. *Let* $p>3$ *be a prime number, and let* k *be a positive integer such that*

$$1<\gcd(p-1,k)<\frac{p-1}{2}.$$

Let $c_1,c_2,\ldots,c_t$ *be nonzero elements of the field* $\mathbb{Z}/p\mathbb{Z}$*, and let* $f(x_1,\ldots,x_t)=c_1x_1^k+\cdots+c_tx_t^k$*. Then*

$$|\mathrm{R}(f)|\geq\min\left(p,\frac{(2t-1)(p-1)}{\gcd(p-1,k)}+1\right).$$

The following theorem is an application of the above results.

Theorem 13. *Let* p *be a prime number and* $c_1,\ldots,c_t$ *be integers numbers not divisible by* p*. Assume that* $1<\gcd(k,p-1)<(p-1)/2$ *and* $t>(k+2)/2$*. Then the congruence*

$$c_1x_1^k+\cdots+c_tx_t^k\equiv 0 \pmod{p}$$

has a nontrivial solution.

Proof. Let $A=\{c_1x_1^k+\cdots+c_tx_t^k \pmod{p} : x_1,\ldots,x_t\in\mathbb{Z}, p\nmid x_1\}$ and $d=\gcd(p-1,k)$. It is easy to check that

$$A=\{c_1x_1^d+\cdots+c_tx_t^d \pmod{p} : x_1,\ldots,x_t\in\mathbb{Z}, p\nmid x_1\}.$$

We want to show that $0\in A$. Assume that $0\notin A$. Let $B=\{c_1x_1^d \pmod{p} : x_1\in\mathbb{Z}, p\nmid x_1\}$ and $C=\{c_2x_2^d+\cdots+c_tx_t^d \pmod{p} : x_2,\ldots,x_t\in\mathbb{Z}\}$. Thus, $A=B+C$. It is clear that $|B|=(p-1)/d$ and it follows from Theorem 12 that $|C|\geq\min\left(p,\frac{(2t-3)(p-1)}{d}+1\right)$. Now, from the Cauchy-Davenport theorem, we obtain

$$|A|=|B+C|\geq\min(p,|B|+|C|-1)=\min\left(p,\frac{(2t-2)(p-1)}{d}\right).$$

Note that $|A|<p$. If we assume that $|A|=\frac{(2t-2)(p-1)}{d}$, then by Vosper's theorem we have three cases:

1. $|B| = 1$ or $|C| = 1$. This is impossible because $(p-1)/d > 1$.

2. $|B+C| = p-1$. This implies that $p-1 = (2t-2)(p-1)/d$, so $t = (d+2)/2$. Now, since $d \leq k$, we obtain that $t \leq (k+2)/2$, which contradicts the hypothesis.

3. B and C are arithmetic progressions with the same common difference. This is impossible by Proposition 11.

We conclude that

$$|A| > \frac{(2t-2)(p-1)}{d}.$$

Now the set A is a disjoint union of sets of the form $\left\{cx^d \pmod{p} : x \in \mathbb{Z}, p \nmid x\right\}$, where $p \nmid c$, see [7, Lemma 2.9]. Therefore, we have $|A| \equiv 0 \pmod{(p-1)/d}$. If follows that

$$|A| \geq \frac{(2t-2)(p-1)}{d} + \frac{p-1}{d} = \frac{(2t-1)(p-1)}{d}.$$

Since $|A| < p$, we have $\frac{(2t-1)(p-1)}{d} < p$. Hence, $t \leq (k+1)/2$, which contradicts the hypothesis. This finishes the proof. □

4 Polynomials of the form $x^k + y^k$

In this section, α is the function associated with a polynomial of the form $x^k + y^k$. We want to determine explicit formulas for $\alpha(p^n)$, where p is prime and $n \geq 1$. Since the cases $k = 2$ and $k = 3$ were solved by Arias et al. [3], and Broughan [4], respectively, we will focus on $k \geq 4$.

4.1 General results on the computation of $\alpha(p^n)$

We start with $p = 2$. The following proposition will help us to find $\alpha(2^n)$, when k is even.

Proposition 14. *Let k be an even positive integer. Then k is an exponent of the prime number $p = 2$ in the polynomial $x^k + y^k$.*

Proof. Assume 2^k divides an integer of the form $x^k + y^k$. Clearly, x and y have the same parity. If x and y are even, then $x = 2x_0$ and $y = 2y_0$, for some integers x_0 and y_0. So, we have $x^k + y^k = 2^k(x_0^k + y_0^k)$, which implies that $(x^k + y^k)/2^k = x_0^k + y_0^k$. Now, if x and y are odd, then $x = 2x_0 + 1$ and $y = 2y_0 + 1$, for some integers x_0 and y_0. Using the binomial theorem, we find that $x^k = 4x_1 + 1$ and $y^k = 4y_1 + 1$, for some positive integers x_1 and y_1. Therefore, $x^k + y^k = 4(x_1 + y_1) + 2$, which is not divisible by 2^k. We conclude that k is an exponent of the prime 2 in the polynomial $x^k + y^k$. □

Now we consider the case where the prime p is odd. It is easy to check the following result.

Lemma 15. *Let p be an odd prime number and d be a positive divisor of $p-1$. Then $p \equiv 1 \pmod{2d}$ or $p \equiv d+1 \pmod{2d}$.*

Proposition 16. *Let p be an odd prime, $d = \gcd(p-1, k)$, and assume that $p \equiv d + 1 \pmod{2d}$. Then k is an exponent of p in the polynomial $x^k + y^k$.*

Proof. Suppose that p^k divides $a^k + b^k$, where a and b are integer. For the proof, it is sufficient to show that p divides a and b. Assume that p does not divide a. Then there exists an integer c such that $ca \equiv 1 \pmod{p}$. Since $a^k + b^k \equiv 0 \pmod{p}$, it follows that

$$1 + (cb)^k \equiv (ca)^k + (cb)^k \equiv c^k(a^k + b^k) \equiv 0 \pmod{p}.$$

Therefore, the congruence $z^k \equiv -1 \pmod{p}$ has a solution, which implies $(-1)^{\frac{p-1}{d}} \equiv 1 \pmod{p}$, so $\frac{p-1}{d}$ is even. This contradicts the hypothesis that $\frac{p-1}{d}$ is odd. Thus, we conclude that p divides a. Similarly, p divides b.

We conclude that $(a^k + b^k)/p^k = (a/p)^k + (b/p)^k$ is a sum of two k-th powers. This ends the proof. □

Proposition 17. *Suppose p is an odd prime, p^s is the highest power of p that divides k, and let $d = \gcd(p-1, k)$. If $p \equiv d + 1 \pmod{2d}$, then $N_{p^r} = \{jp^{r-1} : 0 < j < p\}$, for $s + 2 \le r \le k$ and $N_{p^{k+1}} = \{jp^k : 0 < j < p, j \notin A_p\}$.*

Proof. By Proposition 6, it only remains to prove that $\{jp^{r-1} : 0 < j < p\} \subseteq N_{p^r}$ for $s+2 \le r \le k$. Let us suppose that there exists $0 < j_0 < p$ such that $j_0 p^{r-1} \notin N_{p^r}$, that is, there are integers x, y such that, $x^k + y^k \equiv j_0 p^{r-1} \pmod{p^r}$. Since $r - 1 \ge 1$, we have p divides $x^k + y^k$, so p divides both x and y. Thus, from the congruence $x^k + y^k \equiv j_0 p^{r-1} \pmod{p^r}$ and the fact that $r \le k$, it follows that p^r divides $j_0 p^{r-1}$, so p divides j_0, which is a contradiction. □

In the following theorem, we find recursive formulas for computing $\alpha(p^n)$.

Theorem 18. *Let p be an odd prime, $d = \gcd(p-1, k)$, and s be the highest nonnegative integer such that p^s divides k.*

1. *If k is even, $s = 0$ and $p \equiv 1 \pmod{2d}$, then $\alpha(p^n) = p^{n-1}\alpha(p)$, for all $n \ge 1$.*
2. *If k is even and $p \equiv d + 1 \pmod{2d}$, then $\alpha(p^n) = p\alpha(p^{n-1}) + \alpha(p) - p$, for all $n \equiv 1 \pmod{k}$.*
3. *If k is even and $p \equiv d+1 \pmod{2d}$, then $\alpha(p^n) = p\alpha(p^{n-1}) - p + 1$, for all $n \equiv r \pmod{k}$, where $s + 2 \le r \le k$.*
4. *If k is odd and $s = 0$, then $\alpha(p^n) = p^{n-1}\alpha(p)$, for all $n \ge s + 1$.*

Proof. We first assume that k is even, $s = 0$ and $p \equiv 1 \pmod{2d}$. Then $\frac{p-1}{d}$ is even, so $(-1)^{\frac{p-1}{d}} \equiv 1 \pmod{p}$. It follows that the congruence $x^k \equiv -1 \pmod{p}$ is solvable, which implies that $x^k + y^k \equiv 0 \pmod{p}$ has a nontrivial solution. Therefore, from Corollary 5, it follows that $\alpha(p^n) = p^{n-1}\alpha(p)$, for all $n \geq 1$.

Statements 2 and 3 follow from Propositions 7 and 17.

Finally, we prove statement 4. If k is odd, then $d = \gcd(p-1, k)$ is odd, so $p \equiv 1 \pmod{2d}$. The rest of the proof is the same as the proof of statement 1. □

Corollary 19. *Let p be an odd prime that does not divide k, where k is even, and let $d = \gcd(p-1, k)$. If $n \equiv r \pmod{k}$, where $1 \leq r \leq k$, then*

$$\alpha(p^n) = \begin{cases} (\alpha(p) - 1)\dfrac{p^{n+k-1} - p^{r-1}}{p^k - 1} + 1, & \text{if } p \equiv d + 1 \pmod{2d}; \\ p^{n-1}\alpha(p), & \text{if } p \equiv 1 \pmod{2d}. \end{cases}$$

4.2 Calculation of $\alpha(p)$

We have already formulas that express $\alpha(p^n)$ in terms of $\alpha(p)$, for an odd prime p. To compute $\alpha(p)$, we will use the following result of Joly [6].

Proposition 20. *Let K be a finite field with q elements, d_i be positive integers and $b, a_i \in K$, for $i = 1, 2, \ldots, t$. If $N(b, t)$ is the number of solutions of the diagonal equation given by $a_1x_1^{d_1} + a_2x_2^{d_2} + \cdots + a_tx_t^{d_t} = b$ in K^t, then*

$$|N(b, t) - q^{t-1}| \leq Aq^{\frac{t-1}{2}},$$

where $A = (\delta_1 - 1)\cdots(\delta_t - 1)$, and $\delta_i = \gcd(q - 1, d_i)$, for $i = 1, 2, \ldots, t$.

A direct application of Proposition 20 is the following.

Corollary 21. *Let p be a prime, $b, c_i \in \mathbb{Z}/p\mathbb{Z}$ for $i = 1, 2, \ldots, t$, and k be a positive integer. If $N(b, t)$ is the number of solutions in $(\mathbb{Z}/p\mathbb{Z})^t$ of the diagonal equation $c_1x_1^k + c_2x_2^k + \cdots + c_tx_t^k = b$, then*

$$|N(b, t) - p^{t-1}| \leq (k - 1)^t p^{\frac{t-1}{2}}.$$

Moreover, if $p > (k - 1)^{\frac{2t}{t-1}}$, then $\alpha(p) = p$.

Proof. The first part is a direct consequence of Proposition 20. For the second part, if $K = \mathbb{Z}/p\mathbb{Z}$, $d_i = k$, for $i = 1, 2, \ldots, t$ and $\delta_i = \gcd(k, p - 1)$, then $\delta_i \leq k$ and $N(b, t) - p^{t-1} \geq -(k - 1)^t p^{\frac{t-1}{2}}$, which implies that $N(b, t) \geq p^{t-1} - (k - 1)^t p^{\frac{t-1}{2}}$. The hypothesis that $p > (k - 1)^{\frac{2t}{t-1}}$ yields $N(b, t) > 0$. Hence, for $p > (k - 1)^{\frac{2t}{t-1}}$, the diagonal equation $c_1x_1^k + c_2x_2^k + \cdots + c_tx_t^k = b$ has a solution, for all $b \in \mathbb{Z}/p\mathbb{Z}$. It follows that $\alpha(p) = p$. □

As an example, for polynomials of the form $c_1x^k + c_2y^k$, we obtain $\alpha(p) = p$, for every prime $p > (k - 1)^4$.

5 The polynomial $x^k - y^k$ with k even

Throughout this section, let p be a prime and s be the highest nonnegative integer such that p^s divides k, where k is even. For the polynomial $x^k - y^k$, we can apply Proposition 4 (take $x = y = 1$), to obtain the following formula:

$$\alpha(p^n) = \begin{cases} 2^{n-s-2}\alpha(2^{s+2}), & \text{if } p = 2 \text{ and } n \geq s+2; \\ p^{n-s-1}\alpha(p^{s+1}), & \text{if } p \text{ is odd and } n \geq s+1. \end{cases} \tag{2}$$

We show the explicit calculation of $\alpha(2^n)$, for all n. Let α_0 be the function associated with the polynomial $x^{2^s} - y^{2^s}$.

Lemma 22. *For $1 \leq n \leq s+2$, the congruence $x^{2^s} - y^{2^s} \equiv a \pmod{2^n}$ has a solution if and only if $a = 0, 1, 2^n - 1$. Then $\alpha_0(2^n) = 3$ for $2 \leq n \leq s+2$.*

Proof. Let $2 \leq n \leq s+2$. If $a \in \{0, 1, 2, \ldots, 2^n - 1\}$, then the congruence $x^{2^s} \equiv a \pmod{2^n}$ is solvable only for $a = 0$ and $a = 1$. Thus, the congruence $x^{2^s} - y^{2^s} \equiv a \pmod{2^n}$ has solution only for $a = 0, 1, -1$. Since $-1 \equiv 2^n - 1 \pmod{2^n}$, we obtain the desired result. □

Theorem 23. *Let α be the function associated with the polynomial $x^k - y^k$. If $k = 2^s m$, where $s \geq 1$ and m is odd, then*

$$\alpha(2^n) = \begin{cases} 2, & \text{if } n = 1; \\ 3, & \text{if } 1 < n \leq s+2; \\ 3 \cdot 2^{n-s-2}, & \text{if } n > s+2. \end{cases}$$

Proof. If the congruence $x^{2^s m} - y^{2^s m} \equiv a \pmod{2^n}$ is solvable, then the congruence $x^{2^s} - y^{2^s} \equiv a \pmod{2^n}$ is also solvable. Thus, $\alpha(2^n) \leq \alpha_0(2^n)$, for $2 \leq n \leq s+2$. Since $0, 1, 2^n - 1 \in A_{2^n}$ (for the polynomial $x^k - y^k$), we obtain $\alpha(2^n) = 3$ for $2 \leq n \leq s+2$. For $n > s+2$, it follows from (2) that $\alpha(2^n) = 2^{n-s-2}\alpha(2^{s+2}) = 3 \cdot 2^{n-s-2}$. □

6 Applications to particular polynomials

In this section, we will apply our results to find explicit formulas for $\alpha(p^n)$, where α is the function associated with the following polynomials: $x^4 + y^4$, $x^4 - y^4$, $x^5 + y^5$ and $x^6 + y^6$.

Theorem 24. *Let α be the function associated with the polynomial x^4+y^4. Then*

$$\alpha(p^n)=\begin{cases}\frac{4}{15}(2^{n-1}-2^{r-1})+3, & \textit{if } p=2,\ n\equiv r \pmod 4),\ \textit{where } r=2,3,4;\\ \frac{4}{15}(2^{n-1}-1)+2, & \textit{if } p=2 \textit{ and } n\equiv 1 \pmod 4);\\ p^n, & \textit{if } p\equiv 1 \pmod 8),\ p\neq 17,\ n\geq 1;\\ 13\cdot 17^{n-1}, & \textit{if } p=17,\ n\geq 1;\\ (p-1)\dfrac{p^{n+3}-p^{r-1}}{p^4-1}+1, & \textit{if } p\not\equiv 1 \pmod 8),\ p\neq 5,13,29,\ n\equiv r \pmod 4),\\ & \textit{where } 1\leq r\leq 4;\\ \frac{1}{312}(5^{n+3}-5^{r-1})+1, & \textit{if } p=5,\ n\equiv r \pmod 4),\ \textit{where } 1\leq r\leq 4;\\ \frac{1}{3173}(13^{n+3}-13^{r-1})+1, & \textit{if } p=13,\ n\equiv r \pmod 4),\ \textit{where } 1\leq r\leq 4;\\ \frac{1}{33680}(29^{n+3}-29^{r-1})+1, & \textit{if } p=29,\ n\equiv r \pmod 4),\ \textit{where } 1\leq r\leq 4.\end{cases}$$

Proof. For $p=2$, direct calculations show that $|N_{2^2}|=1$, $|N_{2^3}|=|N_{2^4}|=3$, and $|N_{2^5}|=0$. Then from Proposition 8, we obtain the given formulas for $\alpha(2^n)$.

Now, from Corollary 21, it follows that $\alpha(p)=p$, for all $p>81$. For primes $p<81$, we have $\alpha(5)=3$, $\alpha(13)=10$, $\alpha(17)=13$, $\alpha(29)=22$, and $\alpha(p)=p$, for $31\leq p<81$.

Odd primes divide into 4 types depending on their residue upon division by 8. Observe that only those primes of the form $8m+1$ satisfy $p\equiv 1 \pmod{2d}$, where $d=\gcd(p-1,4)$. The rest of the proof follows from Theorem 18 and Corollary 19. □

Theorem 25. *If α is the function associated with the polynomial x^5+y^5, p is prime and $n\geq 1$, then*

$$\alpha(p^n)=\begin{cases}5, & \textit{if } p=5 \textit{ and } n=1;\\ 13\cdot 5^{n-2}, & \textit{if } p=5 \textit{ and } n\geq 2;\\ 5\cdot 11^{n-1}, & \textit{if } p=11;\\ 19\cdot 31^{n-1}, & \textit{if } p=31;\\ 33\cdot 41^{n-1}, & \textit{if } p=41;\\ 49\cdot 61^{n-1}, & \textit{if } p=61;\\ p^n, & \textit{if } p\neq 5,11,31,41,61.\end{cases}$$

Proof. It follows, from Corollary 21 and direct computations, that $\alpha(p)=p$ for all $p\neq 11,31,41,61$, and $\alpha(11)=5, \alpha(31)=19, \alpha(41)=33$, $\alpha(61)=49$. Now we apply part 4 of Theorem 18 to obtain $\alpha(p^n)=p^{n-1}\alpha(p)$, for all odd primes $p\neq 5$, and $n\geq 1$. This gives us the desired formulas for $\alpha(p^n)$, for all primes $p\neq 2,5$.

On the other hand, it is clear that the congruence $x^5+y^5\equiv 0 \pmod{5^2}$ has a nontrivial solution. From Proposition 4, it follows that $\alpha(5^n)=5^{n-2}\alpha(5^2)$, for all $n\geq 2$. An easy computation shows that $\alpha(5)=5$ and $\alpha(5^2)=13$.

Finally, we apply Proposition 4 to obtain $\alpha(2^n)=2^{n-1}\alpha(2)=2^n$. □

The following proposition shows us formulas for $\alpha(2^n)$ and $\alpha(3^n)$, where α is the function associated with x^6+y^6. These formulas are obtained by using the fact that 6 is an exponent of $p=2$ and $p=3$ in x^6+y^6 by Propositions 14 and 16. Then we finish the proof by applying Proposition 8.

Proposition 26. *Let α be the function associated with the polynomial x^6+y^6. Then $\alpha(2^n) = \frac{1}{63}(16 \cdot 2^n + \beta_i)$ and $\alpha(3^n) = \frac{1}{364}(81 \cdot 3^n + \gamma_i)$, where $n \equiv i \pmod 6$, $i = 0, 1, 2, 3, 4, 5$, and the values β_i and γ_i are shown in Table 1.*

i	β_i	γ_i
0	47	283
1	94	849
2	125	363
3	61	361
4	59	355
5	55	337

Table 1: The values β_i and γ_i.

Before computing $\alpha(p^n)$ for primes $p > 3$ and $n \geq 1$, we compute $\alpha(p)$. By Corollary 21 and direct computations, we obtain the following result.

Proposition 27. *Let α be the function associated with the polynomial x^6+y^6. Then $\alpha(p) = p$ for all primes p, where $p \notin \{7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 109, 139, 223\}$.*

For $p \in \{7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 109, 139, 223\}$, Table 2 shows the values $\alpha(p)$.

p	7	13	19	31	37	43	61	67	73	79	109	139	223
$\alpha(p)$	3	5	10	16	19	29	51	56	61	66	91	116	186

Table 2: The values $\alpha(p)$.

The following proposition shows us a formula for computing $\alpha(p^n)$ in terms of $\alpha(p)$, where $p > 3$ is prime. This result is a direct application of Corollary 19.

Proposition 28. *Let $p > 3$ be a prime, and α be the function associated with the polynomial $x^6 + y^6$. If $n \equiv r \pmod 6$, where $1 \leq r \leq 6$, then*

$$\alpha(p^n) = \begin{cases} \big(\alpha(p) - 1\big)\dfrac{p^{n+5} - p^{r-1}}{p^6 - 1} + 1, & \text{if } p \equiv 3 \pmod 4; \\ p^{n-1}\alpha(p), & \text{if } p \equiv 1 \pmod 4. \end{cases}$$

The following result shows a formula for $\alpha(p^n)$, where α is the function associated with $x^4 - y^4$. To obtain this formula, we apply Equation (2), Corollary 21, Theorem 23, and direct computations.

Theorem 29. *Let α be the function associated with the polynomial $x^4 - y^4$. If p is a prime and $n \geq 1$, then*

$$\alpha(p^n) = \begin{cases} 2, & \text{if } p = 2,\ n = 1; \\ 3, & \text{if } p = 2,\ n = 2, 3; \\ 3 \cdot 2^{n-4}, & \text{if } p = 2,\ n \geq 4; \\ 3 \cdot 5^{n-1}, & \text{if } p = 5; \\ 13 \cdot 17^{n-1}, & \text{if } p = 17; \\ p^n, & \text{if } p \text{ is odd, } p \neq 5, 17. \end{cases}$$

7 Application to the modular Waring problem

Let $\alpha_{k,t}$ be the function associated with the polynomial $x_1^k + \cdots + x_t^k$. Given $n \in \mathbb{Z}^+$, we define $\gamma(k, n)$ to be the least positive integer t such that $\alpha_{k,t}(n) = n$, and $\gamma(k)$ to be the least positive integer t such that $\alpha_{k,t}(n) = n$, for all $n \in \mathbb{Z}^+$. For every k, the integer $\gamma(k)$ exists by the Hilbert-Waring theorem. We clearly have

$$\gamma(k) = \max_{n \in \mathbb{Z}^+} \gamma(k, n).$$

Moreover, since $\alpha_{k,t}$ is multiplicative,

$$\gamma(k) = \max_{p,n} \gamma(k, p^n),$$

where p runs over all primes and $n \geq 1$. The computation of $\gamma(k, n)$ is called the *modular Waring problem.*

We are interested in comparing $\gamma(k)$ and $g(k)$, where $g(k)$ is the least positive integer t such that every positive integer can be expressed as a sum of at most t k-th powers (see sequence A002804 in the *On-Line Encyclopedia of Integer Sequences*).

The following three results, concerning the functions $\alpha_{2,j}$, for $j \in \{1, 2, 3\}$, can be inferred from [3]:

i) $\alpha_{2,1}(n) = n$ if and only if $n = 1$ or $n = 2$,

ii) $\alpha_{2,2}(n) = n$ if and only if $4 \nmid n$ and n is not divisible by the square of any prime $p \equiv 3 \pmod 4$,

iii) $\alpha_{2,3}(n) = n$ if and only if 8 does not divide n.

Lagrange four-square theorem implies that $\alpha_{2,4}(n) = n$, for all n. Hence,

$$\gamma(2, n) = \begin{cases} 1, & \text{if } n = 1, 2; \\ 2, & \text{if } n \neq 1, 2;\ 4 \nmid n \text{ and } p^2 \nmid n \text{ for all primes } p \equiv 3 \pmod 4; \\ 3, & \text{if } 4 \mid n \text{ and } 8 \nmid n; \\ 4, & \text{if } 8 \mid n. \end{cases}$$

It follows that $\gamma(2) = 4$.

Now let us consider the modular Waring problem for cubic powers. Let $\alpha_{3,t}$ be the function associated with $x_1^3 + \cdots + x_t^3$. Broughan [4] proved that

$$\alpha_{3,2}(n) = \begin{cases} n, & \text{if } 7 \nmid n \text{ and } 9 \nmid n; \\ \frac{5}{7}n, & \text{if } 7 \mid n \text{ and } 9 \nmid n; \\ \frac{5}{9}n, & \text{if } 7 \nmid n \text{ and } 9 \mid n; \\ \frac{25}{63}n, & \text{if } 7 \mid n \text{ and } 9 \mid n. \end{cases}$$

Proposition 30. *Let p be a prime and n be a positive integer. Then*

$$\alpha_{3,3}(p^n) = \begin{cases} 3, & \textit{if } p = 3 \textit{ and } n = 1; \\ 7 \cdot 3^{n-2}, & \textit{if } p = 3 \textit{ and } n \geq 2; \\ p^n, & \textit{if } p \neq 3. \end{cases}$$

Proof. The triple $(1, -1, 0)$ is a nontrivial solution of the congruence $x^3 + y^3 + z^3 \equiv 0 \pmod{p}$. It follows, from Corollary 5, that if $p \neq 3$, then $\alpha_{3,3}(p^n) = p^{n-1}\alpha_{3,3}(p)$, for all n. Note that $\gcd(3, p-1) = 1$ or 3. If $\gcd(3, p-1) = 1$, then there are $p-1$ cubic residues modulo p, so $\alpha_{3,3}(p) = p$. On the other hand, if $\gcd(3, p-1) = 3$ and $p \geq 11$, then, from Theorem 12 we have

$$\alpha_{3,3}(p) \geq \min\left(p, \frac{(2 \cdot 3 - 1)(p-1)}{3}\right) = p.$$

Therefore, $\alpha_{3,3}(p) = p$. We conclude that $\alpha_{3,3}(p^n) = p^n$, for all $p \neq 3, 7$, $n \geq 1$. When $p = 7$, we see that $\alpha_{3,3}(7) = 7$, so $\alpha_{3,3}(7^n) = 7^n$, for all $n \geq 1$.

Finally, from Proposition 4, it follows that

$$\alpha_{3,3}(3^n) = 3^{n-2}\alpha(3^2),$$

for all $n \geq 3$, and it is easily seen that $\alpha_{3,3}(3) = 3$ and $\alpha_{3,3}(9) = 7$. This finishes the proof. □

The formula in the above proposition can be simplified as follows:

$$\alpha_{3,3}(n) = \begin{cases} n, & \text{if } 9 \nmid n \text{ ;} \\ \frac{7}{9}n, & \text{if } 9 \mid n. \end{cases}$$

It is not difficult to see that $\alpha_{3,4}(n) = n$, for all $n \in \mathbb{Z}^+$, which implies that $\gamma(3) = 4$.

Proposition 31. *Let t be a positive integer, $1 \leq t \leq 15$. If 16 divides an integer of the form $x_1^4 + x_2^4 + \cdots + x_t^4$, then x_i is even for all i. Consequently, 4 is an exponent of $p = 2$ in the polynomial $x_1^4 + x_2^4 + \cdots + x_t^4$.*

Proof. We proceed by induction on t. The result is clear for $t = 1$. Let us assume that if 16 divides a sum of the form $x_1^4 + x_2^4 + \cdots + x_t^4$, where $1 \leq t < 15$, then all x_i's are even.

Suppose that 16 divides a sum of the form $x_1^4 + x_2^4 + \cdots + x_{t+1}^4$. If all the x_i's are odd, then $x_i^4 \equiv 1 \pmod{16}$ for all i, so 16 divides $t + 1$, which is absurd. Thus, we can assume that x_{t+1} is even. It follows that 16 divides $x_1^4 + x_2^4 + \cdots + x_t^4$, and the induction hypothesis implies that all the x_i's are even. □

With our techniques and the use of a computer program, it is not difficult to deduce the following result.

Proposition 32. *Let t be an integer, $3 \leq t \leq 15$, and $\alpha_{4,t}$ be the function associated with the polynomial $x_1^4 + x_2^4 + \cdots + x_t^4$. Then*

$$\alpha_{4,t}(2^n) = \begin{cases} \frac{1}{15}(t \cdot 2^n - 2t + 30), & \text{if } n \equiv 1 \pmod{4} \text{ and } 3 \leq t \leq 15; \\ \frac{1}{15}(t \cdot 2^n - 4t + 60), & \text{if } n \equiv 2 \pmod{4} \text{ and } 3 \leq t \leq 15; \\ \frac{1}{15}(t \cdot 2^n + 7t + 15), & \text{if } n \equiv 3 \pmod{4} \text{ and } 3 \leq t \leq 7; \\ \frac{1}{15}(t \cdot 2^n - 8t + 120), & \text{if } n \equiv 3 \pmod{4} \text{ and } 8 \leq t \leq 15; \\ \frac{1}{15}(t \cdot 2^n - t + 15), & \text{if } n \equiv 4 \pmod{4} \text{ and } 3 \leq t \leq 15. \end{cases}$$

Furthermore, if p is an odd prime and $t \geq 5$, then $\alpha_{4,t}(p^n) = p^n$, for all $n \geq 5$.

In particular, when $t = 15$ in Proposition 32, we obtain $\alpha_{4,t}(2^n) = 2^n$, for all $n \geq 1$. Thus, we see that $\gamma(4) = 15$.

With the use of a computer program, we can compute $\gamma(k)$ for small values of k. In Table 3, we compare $\gamma(k)$ and $g(k)$, for $2 \leq k \leq 9$.

k	$g(k)$	$\gamma(k)$
2	4	4
3	9	4
4	19	15
5	37	5
6	73	9
7	143	5
8	279	32
9	548	13

Table 3: Comparison of $g(k)$ and $\gamma(k)$, $2 \leq k \leq 9$.

8 Acknowledgments

The authors thank the referee and editor for all the suggestions that helped to improve this paper.

References

[1] A. Alnaser and T. Cochrane, Waring's number mod m, *J. Number Theory* **128** (2008), 2582–2590.

[2] A. Alnaser, T. Cochrane, M. Ostergaard, and C. Spencer, Waring numbers for diagonal congruences, *Rocky Mountain J. Math.* **50** (2020), 825–838.

[3] F. Arias, J. Borja, and L. Rubio, Counting integers representable as images of polynomials modulo n, *J. Integer Sequences* **22** (2019), Article 19.6.7.

[4] K. Broughan, Characterizing the sum of two cubes, *J. Integer Sequences* **6** (2003), Article 03.4.6.

[5] J. Harrington, L. Jones, and A. Lamarche, Representing integers as the sum of two squares in the ring $\mathbb{Z}_n$, *J. Integer Sequences* **17** (2014), Article 14.7.4.

[6] J. Joly, Equations et variétés algébriques sur un corps fini, *Enseign. Math.* **19** (1973), 1–117.

[7] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer, 1996.

[8] C. Small, Waring's problem mod n, *Amer. Math. Monthly* **84** (1977), 12–25.

2020 *Mathematics Subject Classifications*: Primary 11A07; Secondary 11B13, 11B83, 11P05.
Keywords: polynomial congruence, modular Waring problem, additive number theory.

(Concerned with sequence A002804)

Received April 19 2023; revised versions received April 24 2023; May 16 2023; August 24 2023. Published in *Journal of Integer Sequences*, August 28 2023.

Return to Journal of Integer Sequences home page.