Journal of Integer Sequences, Vol. 22 (2019),
Article 19.6.7

Counting Integers Representable as Images of Polynomials Modulo n

Fabián Arias
Facultad de Ciencias Básicas
Universidad Tecnológica de Bolívar
Colombia
farias@utb.edu.co

Jerson Borja and Luis Rubio
Departamento de Matemáticas y Estadística
Universidad de Córdoba
Colombia
jersonborjas@correo.unicordoba.edu.co
lrubiohernandez@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, let $\alpha(n)$ be the number of integers $0 \le a < n$ such that the polynomial congruence $f(x_1, x_2, \ldots, x_t) \equiv a \pmod{n}$ is solvable. We describe a method that allows us to determine the function α associated with polynomials of the form $c_1x_1^k + c_2x_2^k + \cdots + c_tx_t^k$. Then, we apply this method to polynomials that involve sums and differences of squares, mainly to the polynomials $x^2 + y^2$, $x^2 - y^2$, and $x^2 + y^2 + z^2$.

1 Introduction

For a polynomial $f(x_1, x_2, \ldots, x_t)$ in t variables with integer coefficients, consider the polynomial congruence

$$f(x_1, x_2, \ldots, x_t) \equiv a \pmod{n} \tag{1}$$

where n is a positive integer and a is an integer. Since the congruence (1) has solution for a if and only if it has solution for $a + qn$ for any integer q, we can assume that a belongs to a complete residue system modulo n. We will use the system of residues $I_n = \{0, 1, , \ldots, n-1\}$.

For any positive integer n, we set A_n to be the set of all $a \in I_n$ for which (1) has solution. We define $\alpha(n) = |A_n|$, where $|A_n|$ stands for the size of A_n. The following natural questions about the sets A_n and their sizes $\alpha(n)$ guide our work:

1. Give explicit descriptions of A_n for all n.
2. Find a formula for $\alpha(n)$.
3. Determine or describe all the values of n such that $\alpha(n) = n$. This is equivalent to determine if the polynomial $f(x_1, x_2, \ldots, x_t)$ is surjective when it is considered as a map $f : \mathbb{Z}_n^t \to \mathbb{Z}_n$. When this map is surjective, we will say that $f(x_1, x_2, \ldots, x_t)$ is *surjective on* n.

Some results related to these questions with respect to the polynomials x^2+y^2 and x^3+y^3 are found in [2, 3, 4].

Harrington, Jones, and Lamarche [4] solved the problem of characterizing all positive integers n such that every element in the ring $\mathbb{Z}_n$ can be represented as the sum of two squares in $\mathbb{Z}_n$, or, in our terms, that $x^2 + y^2$ is surjective on n. Such integers n are those satisfying the following two conditions:

(i) $n \not\equiv 0 \pmod 4$ and

(ii) $n \not\equiv 0 \pmod{p^2}$ for any prime $p \equiv 3 \pmod 4$ with $n \equiv 0 \pmod p$.

They also solved the problem of finding all positive integers n such that every element in $\mathbb{Z}_n$ is expressible as a sum of two squares without allowing zero as a summand. We are interested in the case where zero is allowed as a summand because in that case the sizes $\alpha(n)$ define a multiplicative function.

Burns [3] considered the general problem of representing elements of $\mathbb{Z}_n$ as the sum of two squares. He determined the sizes of the sets A_{p^n} associated with $x^2 + y^2$ as follows: First, he gave explicit descriptions of the sets A_{p^n}, and then, found the size of A_{p^n}, that is, $\alpha(n)$. One key property Burns uses is that the numbers $\alpha(n)$ define a multiplicative function, which implies that for finding $\alpha(n)$ for all positive integers n, it suffices to find $\alpha(p^n)$ where p is prime and $n \geq 1$.

Explicit formulas for the numbers $\alpha(n)$ associated with the polynomial x^3+y^3 were found by Broughan [2]. Broughan considered the fraction $\delta(n) = \alpha(n)/n$ instead of $\alpha(n)$. There is no explicit description of the sets A_{p^n} associated with $x^3 + y^3$, but some properties of $\delta(n)$ give, essentially, recursive formulas for finding $\delta(p^n)$. Again, as in [3], the associated function α is multiplicative.

For a general polynomial $f(x_1, x_2, \ldots, x_t)$, if every nonnegative integer is of the form $f(x_1, x_2, \ldots, x_t)$, then $\alpha(n) = n$ for every $n \geq 1$. This is the case for some polynomials as

$x^2 + y^2 + z^2 + w^2$ or $x^2 + y^2 - z^2$. There are theorems that characterize all nonnegative integers that are of the form $f(x_1, x_2, \ldots, x_t)$, for a given polynomial $f(x_1, x_2, \ldots, x_t)$. Three well known theorems that are important for us are the following.

Theorem 1. *(Euler) A positive integer n is expressible as a sum of two squares if and only if each prime of the form $4k + 3$ appears to an even exponent in the prime decomposition of n.*

Theorem 2. *(Gauss-Legendre) A nonnegative integer is the sum of three squares if and only if it is not of the form $4^a(8b + 7)$.*

Theorem 3. *(Lagrange) Every nonnegative integer is expressible as the sum of four squares.*

A consequence of Lagrange's theorem is that for $t \geq 4$, the polynomial $x_1^2 + x_2^2 + \cdots + x_t^2$ is surjective on n for all $n \geq 1$. Thus, concerning sums of squares, we are interested in finding formulas for $\alpha(n)$ and descriptions of the sets A_n associated with the polynomials $x^2 + y^2$ and $x^2 + y^2 + z^2$.

We prove that for a general polynomial $f(x_1, x_2, \ldots, x_t)$, the sizes $\alpha(n)$ define a multiplicative function. Therefore, for determining $\alpha(n)$ for all n, it suffices to determine $\alpha(p^n)$ for any prime number p and $n \geq 1$. This makes us focus on studying the sets A_{p^n}, where p is a prime number and $n \geq 1$.

In the case of polynomials of the form $c_1x_1^k + c_2x_2^k + \cdots + c_tx_t^k$, we prove some structural results that will permit us to find recurrence formulas for $\alpha(p^n)$, for a given prime p and $n \geq 1$. Then, we apply these results to find explicit formulas for $\alpha(p^n)$, where α is the function associated with one of the polynomials $x^2 + y^2$, $x^2 - y^2$, and $x^2 + y^2 + z^2$. With this method, we deduce some of the results related to $x^2 + y^2$ proved in [3].

The polynomials $x^2 - y^2$ and $x^2 + y^2 + z^2$ share the following property: if $n = 2^s m$ where $s \geq 0$ and m is odd, then $\alpha(n) = \alpha(2^s)m$.

In the case of $x^2 - y^2$, we show that $\alpha(2) = 2$ and $\alpha(2^s) = 3 \cdot 2^{s-2}$ for $s \geq 2$. In particular, $x^2 - y^2$ is surjective on n if and only if $n \not\equiv 0 \pmod 4$.

For the polynomial $x^2 + y^2 + z^2$, we find the explicit formula

$$\alpha(2^s) = \begin{cases} \frac{1}{3}(5 \cdot 2^{s-1} + 1), & \text{if } s \text{ is odd;} \\ \frac{2}{3}(5 \cdot 2^{s-2} + 1), & \text{if } s \text{ is even.} \end{cases}$$

It follows, from this formula, that $x^2 + y^2 + z^2$ is surjective on n if and only if $n \not\equiv 0 \pmod 8$.

2 The multiplicative family associated with a polynomial

For an arbitrary family of nonempty sets $\{A_n\}_{n \in \mathbb{Z}^+}$, where $A_n \subseteq I_n$ for all n, we define the function $\alpha : \mathbb{Z}^+ \to \mathbb{Z}^+$ associated with $\{A_n\}_n$ by $\alpha(n) = |A_n|$ for all n. Note that $\alpha(1) = 1$. The first thing we do is to define suitable conditions on the family $\{A_n\}_n$ so that the associated function α is multiplicative.

2.1 Multiplicative families and polynomials

If n and m are integers such that $1 \leq m \leq n$, we define

$$\begin{aligned} A_n(m) &:= \{s \in I_n : s \equiv a \pmod{m} \text{ for some } a \in A_m\} \\ &= \{a + jm : a \in A_m, 0 \leq j < n/m\}. \end{aligned}$$

We call a family $\{A_n\}_n$ *multiplicative*, if whenever $n = m_1 m_2$ with m_1 and m_2 relatively prime, the equality $A_n = A_n(m_1) \cap A_n(m_2)$ holds. This condition on the family of sets $\{A_n\}_n$ guaranties that the associated function α is multiplicative.

Lemma 4. *If $\{A_n\}_n$ is a multiplicative family, then the associated function α is multiplicative.*

Proof. Let $n = m_1 m_2$ where m_1 and m_2 are relatively prime. We decompose $A_n(m_1)$ as the disjoint union of subsets $B(a, m_1) := \{a + jm_1 : 0 \leq j < m_2\}$, where $a \in A_{m_1}$. Similarly, $A_n(m_2)$ is the disjoint union of subsets $B(b, m_2) = \{b + jm_2 : 0 \leq j < m_1\}$, where $b \in A_{m_2}$. Then,

$$A_n(m_1) \cap A_n(m_2) = \bigcup_{a \in A_{m_1}, b \in A_{m_2}} (B(a, m_1) \cap B(b, m_2)).$$

Note that $c \in B(a, m_1) \cap B(b, m_2)$ if and only if $c \equiv a \pmod{m_1}$ and $c \equiv b \pmod{m_2}$; moreover, by the Chinese remainder theorem, there is exactly one solution in I_n of the system of congruences $x \equiv a \pmod{m_1}, x \equiv b \pmod{m_2}$. This means that $B(a, m_1) \cap B(b, m_2)$ has exactly one element. Since the sets $B(a, m_1) \cap B(b, m_2)$, for $a \in A_{m_1}, b \in A_{m_2}$, are pairwise disjoint, we have $|A_n(m_1) \cap A_n(m_2)| = |A_{m_1}| \cdot |A_{m_2}|$. Now, if the family $\{A_n\}_n$ is multiplicative, then we have $\alpha(n) = |A_n| = |A_n(m_1) \cap A_n(m_2)| = |A_{m_1}| \cdot |A_{m_2}| = \alpha(m_1)\alpha(m_2)$. Thus, the associated function α is multiplicative. □

Now we define two conditions on $\{A_n\}_n$ that will be sufficient to show that $\{A_n\}_n$ is multiplicative.

MT1. For positive integers m and n, if m divides n and $a \in A_n$, then $a \bmod m \in A_m$, where $a \bmod m$ is the residue of a when a is divided by m.

MT2. If $n = m_1 m_2$ where m_1 and m_2 are relatively prime, and if $a_1 \in A_{m_1}$, $a_2 \in A_{m_2}$ and a is the unique solution in I_n to the system of congruences $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$, then $a \in A_n$.

Note that if $\{A_n\}_n$ satisfies condition MT1 and m divides n, then $A_n \subseteq A_n(m)$.

Lemma 5. *If $\{A_n\}_n$ satisfies MT1 and MT2, then $\{A_n\}_n$ is multiplicative.*

Proof. Let us suppose that $n = m_1 m_2$ for relatively prime m_1 and m_2. Since $\{A_n\}_n$ satisfies MT1, we have $A_n \subseteq A_n(m_1) \cap A_n(m_2)$. To prove the other inclusion, let us take $a \in A_n(m_1) \cap A_n(m_2)$. Then, there exist $a_1 \in A_{m_1}$ and $a_2 \in A_{m_2}$ such that $a \equiv a_1 \pmod{m_1}$ and $a \equiv a_2 \pmod{m_2}$ and, since $\{A_n\}_n$ satisfies MT2, it follows that $a \in A_n$. This shows that $A_n = A_n(m_1) \cap A_n(m_2)$. Hence, $\{A_n\}_n$ is multiplicative. □

If we assume that the family of sets $\{A_n\}_n$ satisfy conditions MT1 and MT2, then, by Lemmas 4 and 5, the associated function α is multiplicative. Thus, to determine the values of α on all positive integers, it is enough to determine $\alpha(p^n)$ for all primes p, and $n \geq 1$. This leads us to study the sets A_{p^n} for powers of primes p^n.

Condition MT1 on the family $\{A_n\}_n$ implies that if p is prime and $n \geq 1$, then $A_{p^n} \subseteq A_{p^n}(p^{n-1})$. For $n \geq 1$, we define $N_{p^n} := A_{p^n}(p^{n-1}) \setminus A_{p^n}$ and call these sets, the *N-sets* of the prime p.

Lemma 6. *Let p be a prime number and $n \geq 1$. Then*

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

Proof. The size of $A_{p^n}(p^{n-1})$ is $p \cdot |A_{p^{n-1}}| = p\alpha(p^{n-1})$. Then

$$\alpha(p^n) = |A_{p^n}(p^{n-1}) \setminus N_{p^n}| = |A_{p^n}(p^{n-1})| - |N_{p^n}| = p\alpha(p^{n-1}) - |N_{p^n}|.$$

□

Now, we focus on the sizes of the sets N_{p^n} for $n \geq 1$.

We are interested in those families of sets $\{A_n\}_n$, where A_n is the set of elements $a \in I_n$ such that the congruence $f(x_1, x_2, \ldots, x_t) \equiv a \pmod{n}$ is solvable. We refer to the function α associated with this family $\{A_n\}_n$, as the *function associated with $f(x_1, x_2, \ldots, x_t)$*.

Proposition 7. *The family $\{A_n\}_n$ associated with a polynomial $f(x_1, x_2, \ldots, x_t)$ is multiplicative. In particular, the function α associated with $f(x_1, x_2, \ldots, x_t)$ is multiplicative.*

Proof. The family $\{A_n\}_n$ associated with $f(x_1, x_2, \ldots, x_t)$ trivially satisfies MT1. Towards MT2, assume that $f(a_1, a_2, \ldots, a_t) \equiv a_1 \pmod{m_1}$ and $f(b_1, b_2, \ldots, b_t) \equiv a_2 \pmod{m_2}$, where $a_i, b_j \in \mathbb{Z}$, m_1 and m_2 are relatively prime, $n = m_1 m_2$, $a_i \in I_{m_i}$, $i = 1, 2$. Let a be the only solution in I_n of the system of congruences $x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}$. By the Chinese remainder theorem, for each $j = 1, 2, \ldots, t$, there exists $c_j \in \mathbb{Z}$ such that $c_j \equiv a_j \pmod{m_1}$ and $c_j \equiv b_j \pmod{m_2}$. Since f is a polynomial, $f(c_1, c_2, \ldots, c_t) \equiv f(a_1, a_2, \ldots, a_t) \equiv a_1 \equiv a \pmod{m_1}$ and $f(c_1, c_2, \ldots, c_t) \equiv f(b_1, b_2, \ldots, b_t) \equiv a_2 \equiv a \pmod{m_2}$. It follows that $f(c_1, c_2, \ldots, c_t) \equiv a \pmod{n}$, that is, $a \in A_n$. The result follows by Lemmas 4 and 5. □

Remark 8. Let us consider r families $\{A_n^{(i)}\}_n$, $i = 1, 2, \ldots, r$, where $A_n^{(i)} \subseteq I_n$. For each $n \geq 1$, we set $A_n := \bigcap_{i=1}^r A_n^{(i)}$. Assume that $A_n \neq \varnothing$ for all n. If the r families satisfy MT1 (resp. MT2), then the family $\{A_n\}_n$ satisfy MT1 (resp. MT2).

When $\{A_n^{(i)}\}_n$ is the family associated with some polynomial $f_i(x_1^{(i)}, \ldots, x_{t_i}^{(i)})$, and the intersections $A_n = \bigcap_{i=1}^r A_n^{(i)}$ are nonempty, the family $\{A_n\}_n$ is multiplicative. In this case, the associated function α counts the number of elements $a \in I_n$ such that the system of congruences

$$f_i(x_1^{(i)}, \ldots, x_{t_i}^{(i)}) \equiv a \pmod{n},\ i = 1, 2, \ldots, r$$

is solvable.

2.2 The multiplicative family associated with $c_1x_1^k + c_2x_2^k + \cdots + c_tx_t^k$

We now study the multiplicative function α and the sets A_{p^n} 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 $c_1, c_2, \ldots, c_t \in \mathbb{Z}, k \geq 1$. To determine the value of α at prime powers, we need to understand the sets A_{p^n} and N_{p^n}. The following lemmas give useful properties of these sets.

Lemma 9. *Let $\{A_n\}_n$ be the family associated with the polynomial $c_1x_1^k + c_2x_2^k + \cdots + c_tx_t^k$. 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. Suppose $a \in A_{p^n}$ and*

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

where $m_1, m_2 \ldots, m_t \in \mathbb{Z}$, and suppose that at least one m_i is not divisible by p. If $n \geq 2s+1$, then $a + jp^n \in A_{p^{n+1}}$ for all j such that $0 \leq j < p$.

Proof. Suppose that $c_1m_1^k + c_2m_2^k + \cdots + c_tm_t^k \equiv a \pmod{p^n}$. Then, there is some integer w such that $c_1m_1^k + c_2m_2^k + \cdots + c_tm_t^k = a + wp^n$. Assume that p does not divide m_1. Write $k = p^sk_0$, where $s \geq 0$ and p does not divide k_0. Let $0 \leq j < p$. Since p does not divide $c_1m_1^{k-1}k_0$, the congruence $c_1m_1^{k-1}k_0x + w \equiv j \pmod{p}$ has solution for x in $\mathbb{Z}$; so, there are integers d and e such that $c_1m_1^{k-1}k_0d + w = j + ep$. By the binomial theorem,

$$\begin{aligned}(m_1 + dp^{n-s})^k &= m_1^k + km_1^{k-1}dp^{n-s} + \sum_{2\leq t\leq k} \binom{k}{t} m_1^{k-t}d^tp^{t(n-s)} \\ &= m_1^k + m_1^{k-1}k_0dp^n + \sum_{2\leq t\leq k} \binom{k}{t} m_1^{k-t}d^tp^{t(n-s)}.\end{aligned}$$

Since $n \geq 2s+1$, for $t \geq 2$ we have $t(n-s) \geq 2(n-s) = n + (n-2s) \geq n+1$. Then

$$(m_1 + dp^{n-s})^k \equiv (m_1^k + m_1^{k-1}k_0dp^n) \pmod{p^{n+1}}.$$

Therefore, modulo p^{n+1}, we have

$$\begin{aligned}c_1(m_1 + dp^{n-s})^k + \cdots + c_tm_t^k &\equiv (c_1m_1^k + \cdots + c_tm_t^k) + c_1m_1^{k-1}k_0dp^n \\ &\equiv a + wp^n + c_1m_1^{k-1}k_0dp^n \\ &\equiv a + (w + c_1m_1^{k-1}k_0d)p^n \\ &\equiv a + jp^n + ep^{n+1} \\ &\equiv a + jp^n.\end{aligned}$$

Hence, $a + jp^n \in A_{p^{n+1}}$. ☐

Lemma 10. *Let p be a prime number and consider the N-sets N_{p^n} associated with the polynomial $c_1x_1^k + c_2x_2^k + \cdots + c_tx_t^k$. If p does not divide $c_1, \ldots, c_t$, then*

$$N_{p^n} \subseteq \{p^ka : a \in N_{p^{n-k}}\},$$

for every $n > k+1$.

Proof. If $b \in N_{p^n}$, then $b \in A_{p^n}(p^{n-1})$ and thus, $b = c + jp^{n-1}$ for some $c \in A_{p^{n-1}}$ and $0 \leq j < p$. Since $c \in A_{p^{n-1}}$, there are integers $m_1, \ldots, m_t$ such that $c_1 m_1^k + \cdots + c_t m_t^k \equiv c \pmod{p^{n-1}}$. Note that if p^s is the highest power of p that divides k, then $k \geq p^s \geq 2^s \geq 2s$; thus, if $n > k+1$, then $n-1 \geq 2s+1$. Therefore, if some m_i is not divisible by p, then by Lemma 9, $b = c + jp^{n-1} \in A_{p^n}$, a contradiction. It follows that all the m_i are divisible by p. Since $n-1 > k$, we have p^k divides c and we get the congruence $c_1(m_1/p)^k + \cdots + c_t(m_t/p)^k \equiv c/p^k \pmod{p^{n-k-1}}$. Hence $c/p^k \in A_{p^{n-k-1}}$.

We claim that $c/p^k + jp^{n-k-1} \in N_{p^{n-k}}$. On the contrary, if $c_1 q_1^k + \cdots + c_t q_t^k \equiv c/p^k + jp^{n-k-1} \pmod{p^{n-k}}$ for some integers $q_1, \ldots, q_t$, then by multiplying by p^k we obtain that $c_1(pq_1)^k + \cdots + c_t(pq_t)^k \equiv c + jp^{n-1} \pmod{p^n}$, that is, $b = c + jp^{n-1} \in A_{p^n}$, a contradiction. Thus, if $a := c/p^k + jp^{n-k-1}$, then $a \in N_{p^{n-k}}$ and $b = c + jp^{n-1} = p^k a$. This ends the proof. ∎

We now define a condition on the prime p and the polynomial, in such a way that the reverse inclusion in Lemma 10 holds. Most of the cases we are interested in satisfy this condition. When this condition fails, we must find another way to tackle the problem of finding $\alpha(p^n)$ for $n \geq 1$.

Let p be a prime and $f(x_1, \ldots, x_t)$ be any polynomial with coefficients in $\mathbb{Z}$. We say that a non-negative 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 $q_1, \ldots, q_t$.

Lemma 11. *The following statements are true.*

1. *For every prime number p and $k \geq 1$, k is an exponent of p in x^k.*
2. *If $p = 2$ or p is prime with $p \equiv 1 \pmod 4$, then 1 is an exponent of p in the polynomial $x^2 + y^2$.*
3. *If p is prime and $p \equiv 3 \pmod 4$, then 2 is an exponent of p in the polynomial $x^2 + y^2$.*
4. *The integer 2 is an exponent of the prime number 2 in the polynomial $x^2 + y^2 + z^2$.*

Proof. (1) If p^k divides m^k, then p divides m and $m^k/p^k = (m/p)^k$.

(2) If p divides an integer of the form $x^2 + y^2$, then $(x^2 + y^2)/p$ is a sum of two squares by Theorem 1.

(3) If $p \equiv 3 \pmod 4$ divides an integer of the form $x^2 + y^2$, then $(x^2 + y^2)/p^2$ is a sum of two squares by Theorem 1.

(4) Suppose 4 divides $m_1^2 + m_2^2 + m_3^2$ for integers m_1, m_2 and m_3. Then $m_1^2 + m_2^2 + m_3^2$ is even, which implies that two out of the three integers m_1, m_2 and m_3 are odd and one is even, or the three, m_1, m_2 and m_3 are even. In the first case, say $m_1 = 2w_1 + 1, m_2 = 2w_2 + 1$ and $m_3 = 2w_3$. Then, we have $m_1^2 + m_2^2 + m_3^2 = 4(w_1^2 + w_2^2 + w_1 + w_2 + w_3^2) + 2$, which is not divisible by 4. Hence, m_1, m_2 and m_3 are even. So, we can write $m_1 = 2w_1, m_2 = 2w_2, m_3 = 2w_3$ and, therefore, $m_1^2 + m_2^2 + m_3^2 = 4(w_1^2 + w_2^2 + w_3^2)$. This ends the proof. ∎

Note that if e is an exponent of a prime p in a polynomial $f(x_1, x_2, \ldots, x_t)$, then any positive multiple of e is also an exponent of p in $f(x_1, x_2, \ldots, x_t)$.

Lemma 12. *If an exponent e of a prime p in the polynomial $c_1x_1^k + \cdots + c_tx_t^k$ divides k, then $\{p^k a : a \in N_{p^{n-k}}\} \subseteq N_{p^n}$ for $n > k$.*

Proof. If $p^k a \in A_{p^n}$ where $a \in N_{p^{n-k}}$, then there are integers $m_1, \ldots, m_t$ such that $c_1m_1^k + \cdots + c_tm_t^k \equiv p^k a \pmod{p^n}$. Since e divides k, we have k is an exponent of p in $c_1x_1^k + \cdots + c_tx_t^k$. Then, we can write $(c_1m_1^k + \cdots + c_tm_t^k)/p^k = c_1q_1^k + \cdots + c_tq_t^k$ for some integers $q_1, \ldots, q_t$. Therefore, $c_1q_1^k + \cdots + c_tq_t^k \equiv a \pmod{p^{n-k}}$, that is, $a \in A_{p^{n-k}}$, a contradiction. Thus, $p^k a \in N_{p^n}$ for all $a \in N_{p^{n-k}}$. □

An application of Lemma 10 and 12 tells us that if there is an exponent of p in $c_1x_1^k + c_2x_2^k + \cdots + c_tx_t^k$ that divides k, then for all $n > k + 1$ we have

$$N_{p^n} = \{p^k a : a \in N_{p^{n-k}}\}. \tag{2}$$

For a set of integers A, mA denote the set $\{ma : a \in A\}$. Then $N_{p^n} = p^k N_{p^{n-k}}$ for all $n > k + 1$. Therefore, if $n = qk + r$, where $2 \leq r \leq k + 1$, we have

$$N_{p^n} = p^k N_{p^{n-k}} = p^{2k} N_{p^{n-2k}} = \cdots = p^{kq} N_{p^r}. \tag{3}$$

We set $n_r := |N_{p^r}|$, for $2 \leq r \leq k+1$. By (3), it follows that if $n > 1$ and $n \equiv r \pmod{k}$, then $|N_{p^n}| = |N_{p^r}| = n_r$.

Proposition 13. *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, and p does not divide $c_1, \ldots, c_t$. Then*

$$\alpha(p^n) = p\alpha(p^{n-1}) - n_r \tag{4}$$

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

Proof. The result follows from the fact that $|N_{p^n}| = |N_{p^r}| = n_r$ and Lemma 6. □

It is not difficult to deduce, from (4), the following explicit formulas for $\alpha(p^n)$.

Corollary 14. *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.*

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

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

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

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

For the sets N_{p^r} with $2 \leq r \leq k+1$, we have the following result.

Proposition 15. *Consider the* N*-sets associated with the polynomial* $c_1x_1^k + c_2x_2^k + \cdots + c_tx_t^k$*. Let* p *be a prime number that does not divide* $c_1, \ldots, c_t$ *and let* p^s *be the highest power of* p *that divides* k*. If* $2s + 2 \leq r \leq k+1$*, then*

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

Moreover,

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

and 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. Recall that $A_{p^r} \subseteq A_{p^r}(p^{r-1})$ and $N_{p^r} = A_{p^r}(p^{r-1}) \setminus A_{p^r}$. We show that $a + jp^{r-1} \in A_{p^r}$ for any $a \in A_{p^{r-1}}$ with $a \neq 0$ and $0 \leq j < p$. In fact, if $a \in A_{p^{r-1}}$ and $a \neq 0$, then there are integers $m_1, \ldots, m_t$ such that

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

If p divides all the m_i, then p^{r-1} divides a, since $r - 1 \leq k$. But $0 \leq a < p^{r-1}$ and $a \equiv 0 \pmod{p^{r-1}}$ imply $a = 0$, a contradiction. We conclude that some m_i is not divisible by p. So, by Lemma 9, we have $a + jp^{r-1} \in A_{p^r}$ for any $0 \leq j < p$.

This implies that if $a + jp^{r-1} \in N_{p^r}$, then $a = 0$; therefore, all elements in N_{p^r} have the form jp^{r-1}, where $0 \leq j < p$. Thus, we have $N_{p^r} \subseteq \{jp^{r-1} : 0 \leq j < p\}$. Since $0 \notin N_{p^r}$, we conclude that $N_{p^r} \subseteq \{jp^{r-1} : 0 < j < p\}$.

In the case where $r = k+1$, if $j \in A_p$, $0 < j < p$, then $c_1m_1^k + c_2m_2^k + \cdots + c_tm_t^k \equiv j \pmod{p}$ for some integers $m_1, \ldots, m_t$. Hence, $c_1(pm_1)^k + c_2(pm_2)^k + \cdots + c_t(pm_t)^k \equiv jp^k \pmod{p^{k+1}}$, and this shows that $jp^k \in A_{p^{k+1}}$. Thus, $N_{p^{k+1}} \subseteq \{jp^k : j \notin A_p, 0 < j < p\}$.

Finally, if we have $c_1m_1^k + c_2m_2^k + \cdots + c_tm_t^k \equiv jp^k \pmod{p^{k+1}}$ for some $m_1, m_2, \ldots, m_t$, and $(c_1m_1^k + c_2m_2^k + \cdots + c_tm_t^k)/p^k = c_1q_1^k + c_2q_2^k + \cdots + c_tq_t^k$ for some integers $q_1, q_2, \ldots, q_t$, then $c_1q_1^k + c_2q_2^k + \cdots + c_tq_t^k \equiv j \pmod{p}$, which shows that $j \in A_p$ if and only if $jp^k \in A_{p^{k+1}}$. Hence, $N_{p^{k+1}} = \{jp^k : j \notin A_p, 0 < j < p\}$. □

If p does not divide k in Proposition 15, then $s = 0$ and the inclusion $N_{p^r} \subseteq \{jp^{r-1} : 0 < j < p\}$ holds for $2 \leq r \leq k+1$.

To determine the values $\alpha(p^n)$ for all $n \geq 1$ (if the conditions of Proposition 13 hold), our strategy is composed by the following steps:

1. Determine $\alpha(p) = |A_p|$. Here, we have to determine A_p separately.

2. Determine the sets N_{p^r} for $r = 2, \ldots, k+1$. Then $n_r = |N_{p^r}|$ for $r = 2, \ldots, k+1$

3. We apply (4) to obtain a recurrence formula for $\alpha(p^n)$.

4. We find an explicit formula for $\alpha(p^n)$ from the recurrence formula in step (3), or using Corollary 14.

2.3 The polynomial x^k

We illustrate our ideas by considering the multiplicative function α of the polynomial $f(x) = x^k$, where $k \geq 1$ is a given integer. For simplicity, we assume that p is any prime that does not divide k.

The steps we follow are

1. Determine A_p and $\alpha(p)$.

2. Determine $N_{p^2}, \ldots, N_{p^{k+1}}$ and the numbers $n_2, \ldots, n_{k+1}$.

3. Determine the recurrence given by (4).

4. Give explicit formulas for $\alpha(p^n)$.

For the first step, we have A_p is the set of elements $a \in I_p = \{0, 1, \ldots, p-1\}$ such that the congruence $x^k \equiv a \pmod{p}$ is solvable. If $a \neq 0$, then a is a k-th power residue modulo p. Therefore, we have $A_p = \{a \in I_p : a \text{ is a } k\text{-th power residue modulo } p\} \cup \{0\}$. If $d = \gcd(k, p-1)$, then there are $(p-1)/d$ k-th power residues modulo p and so

$$\alpha(p) = (p-1)/d + 1. \tag{5}$$

Now, for the N-sets $N_{p^2}, \ldots, N_{p^{k+1}}$ we have the following result.

Lemma 16. *Assume that p does not divide k. For $r = 2, \ldots, k$,*

$$N_{p^r} = \{jp^{r-1} : 0 < j < p\}.$$

Moreover

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

Proof. Since p does not divide k and k is an exponent of p in x^k, by Proposition 15 we have $N_{p^r} \subseteq \{jp^{r-1} : 0 < j < p\}$ for $r = 2, \ldots, k$ and $N_{p^{k+1}} = \{jp^k : 0 < j < p \text{ and } j \notin A_p\}$.

To prove that $\{jp^{r-1} : 0 < j < p\} \subseteq N_{p^r}$ when $2 \leq r \leq k$, let us take $0 < j < p$ and assume that $jp^{r-1} \in A_{p^r}$. Then $m^k \equiv jp^{r-1} \pmod{p^r}$ for some integer m. So, p divides m and since $k \geq r$, we deduce that p^r divides jp^{r-1}. Therefore, p divides j, which is a contradiction. Hence $jp^{r-1} \in N_{p^r}$. $\square$

For $r = 2, \dots, k+1$, we set $n_r = |N_{p^r}|$. From Lemma 16 and (5) it follows that

$$n_r = \begin{cases} p-1, & \text{for } r = 2, \dots, k; \\ (d-1)(p-1)/d, & \text{for } r = k+1. \end{cases}$$

By Proposition 13 and Corollary 14 we get our recurrence formula, and it is not difficult to deduce the explicit formula in the following proposition.

Proposition 17. *Let p be a prime, $n, k \geq 1$ and $d = \gcd(k, p-1)$. If α is the multiplicative function associated with the polynomial x^k, then we have the following recurrence formula*

$$\alpha(p^n) = \begin{cases} p\alpha(p^{n-1}) - (d-1)(p-1)/d, & \text{if } n \equiv 1 \pmod{k}; \\ p\alpha(p^{n-1}) - p + 1, & \text{if } n \not\equiv 1 \pmod{k}. \end{cases}$$

Moreover, if $n \equiv r \pmod{k}$ where $1 \leq r \leq k$, then

$$\alpha(p^n) = \frac{p^{n+k-1} - p^{r-1}}{d \cdot \left(\frac{p^k - 1}{p-1}\right)} + 1. \tag{6}$$

Remark 18. We can determine $\alpha(p^n)$ in the general case (without the restriction that p does not divide k) in the following way. Let $P(k, m)$ be the set of k-th power residues modulo m. We have that, for $0 < a < p^n$, the congruence $x^k \equiv a \pmod{p^n}$ is solvable if and only if there exist $r \geq 0$ such that $rk \leq n$ and $b \in P(k, p^{n-rk})$ such that $a = p^{rk} b$. To see this, if $x^k \equiv a \pmod{p^n}$ is solvable and p does not divide a, we take $r = 0$ and $b = a$. In case p divides a, we find that p divides x and the congruence $(x/p)^k \equiv a/p^k \pmod{p^{n-k}}$ is solvable. If p does not divide a/p^k, we take $r = 1$ and $b = a/p^k$. If we continue in this way we obtain the desired result. It follows that

$$A_{p^n} = \{0\} \cup \bigcup_{r=0}^{\lfloor \frac{n}{k} \rfloor} p^{rk} P(k, p^{n-rk}),$$

and therefore,

$$\alpha(p^n) = 1 + \sum_{r=0}^{\lfloor \frac{n}{k} \rfloor} |P(k, p^{n-rk})|.$$

For instance, assume p is odd, $k = p^s$ where $s \geq 1$ and k does not divide n. Then, for $r \geq 0$ we have

$$|P(k, p^{n-rk})| = \frac{p^{n-rk-1}(p-1)}{\gcd(p^{n-rk-1}(p-1), p^s)} = \begin{cases} p-1, & \text{if } n - rk - 1 \leq s; \\ p^{n-rk-s-1}(p-1), & \text{if } n - rk - 1 > s. \end{cases}$$

See, for example, [5, Chapter 4, Sec. 2]. So, we can write

$$\alpha(p^n) = 1 + \sum_{0 \leq r < \lceil \frac{n-s-1}{k} \rceil} p^{n-rk-s-1}(p-1) + \sum_{\lceil \frac{n-s-1}{k} \rceil \leq r \leq \lfloor \frac{n}{k} \rfloor} (p-1).$$

3 Sums and differences of squares

In this section we apply our ideas to the polynomials $x^2+y^2, x^2+y^2+z^2$ and x^2-y^2. In each case, we determine formulas for $\alpha(p^n)$. We also show how to determine explicitly the sets A_{p^n} and answer the question about determining all n such that the given polynomial is surjective on n.

3.1 The polynomial x^2+y^2

We consider the polynomial $f(x,y)=x^2+y^2$ and its associated function α. By using our method, we obtain the results about the size of the sets A_{p^n} found in [3, 4].

Lemma 19. *For any prime number p, we have $\alpha(p)=p$.*

Proof. Let us show that every element in $I_p=\{0,1,\dots,p-1\}$ is expressible as the sum of two squares modulo p. It is known that there are $(p+1)/2$ elements in I_p that are squares modulo p. Then, for a given $a\in I_p$, there are $(p+1)/2$ elements in I_p that are expressible as $a-x^2$ modulo p. Since $2(p+1)/2=p+1$ and I_p has p elements, there is an element in I_p that is expressible simultaneously as $a-x^2$ and y^2 modulo p, for some $x,y\in I_p$. This implies that $x^2+y^2\equiv a \pmod p$. □

We now calculate $\alpha(2^n)$ for all $n\geq 1$. By Lemma 11, the prime 2 has exponent 1 in x^2+y^2.

An easy computation gives us the following:

$$A_2=\{0,1\},\ A_4=\{0,1,2\},\ A_8=\{0,1,2,4,5\}.$$

and

$$A_4(2)=\{0,1,2,3\},\ A_8(4)=\{0,1,2,4,5,6\}.$$

Then, $N_4=\{3\}$ and $N_8=\{6\}$, that is, $n_2=1$ and $n_3=1$. Now, by applying Corollary 14, for n odd we have

$$\begin{aligned}\alpha(2^n)&=2^{n-1}\alpha(2)-\frac{2^{n-1}-1}{2^2-1}(2+1)\\&=2^n-(2^{n-1}-1)\\&=2^{n-1}+1,\end{aligned}$$

and for n even

$$\begin{aligned}\alpha(2^n)&=2^{n-1}\alpha(2)-\frac{2^{n-1}-2}{2^2-1}(2+1)-1\\&=2^n-(2^{n-1}-2)-1\\&=2^{n-1}+1.\end{aligned}$$

Therefore, for all $n\geq 1$

$$\alpha(2^n)=2^{n-1}+1.$$

Remark 20. By applying our method we obtain explicit descriptions of the sets A_{2^n} for all $n \geq 1$, as follows. First of all, we determine N_{2^n} for all $n \geq 2$. Note that $N_{2^2} = \{3 \cdot 2^{2-2}\}$ and $N_{2^3} = \{3 \cdot 2^{3-2}\}$. For $n > 3$, we can write $n = 2q + r$, where $r \in \{2, 3\}$. It follows by (3) that $N_{2^n} = \{2^{2q}a : a \in N_{2^r}\} = \{2^{n-r}a : a \in N_{2^r}\}$. Then, it is easy to see that

$$N_{2^n} = \{3 \cdot 2^{n-2}\} = \{2^{n-2} + 2^{n-1}\}$$

for all $n \geq 2$.

We recall that

$$A_{2^n} = \{a + a_{n-1}2^{n-1} : a \in A_{2^{n-1}}, a_{n-1} \in \{0, 1\}\} \setminus N_{2^n}.$$

By an induction argument on n, it is not difficult to show that for all $n \geq 1$, A_{2^n} consists of all elements of the form

$$a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + \cdots + a_{n-1} \cdot 2^{n-1} \tag{7}$$

where

1. $a_0, a_1, a_2, \ldots, a_{n-1} \in \{0, 1\}$,
2. $a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + \cdots + a_{i-1} \cdot 2^{i-1} \in A_{2^i}$, $i = 1, \ldots, n-1$.

Now, assume that an element of the form (7) is not in A_{2^n}. Then there is some i, $2 \leq i \leq n$, such that $a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + \cdots + a_{i-1} \cdot 2^{i-1} \in N_{2^i}$. Since $N_{2^i} = \{2^{i-2} + 2^{i-1}\}$, we see that $a_0 = \cdots = a_{i-3} = 0$ and $a_{i-2} = a_{i-1} = 1$. So,

$$a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + \cdots + a_{n-1} \cdot 2^{n-1} = 2^{i-2} + 2^{i-1} + a_i 2^i + \cdots + a_{n-1}2^{n-1}.$$

Conversely, all elements of the form $2^{i-2} + 2^{i-1} + a_i 2^i + \cdots + a_{n-1}2^{n-1}$, where $a_i, \ldots, a_{n-1} \in \{0, 1\}$ are not in A_{2^n}. Therefore, A_{2^n} is the set of all integers of the form (7) such that the first two nonzero coefficients are not consecutive.

With this description of A_{2^n}, we can also calculate $\alpha(2^n)$. In fact, there are 2^{n-i-2} elements of the form $2^{i-2} + 2^{i-1} + a_i 2^i + \cdots + a_{n-1}2^{n-1}$ for $2 \leq i \leq n$. So,

$$\alpha(2^n) = 2^n - \sum_{i=2}^{n} 2^{n-i} = 2^n - (2^{n-1} - 1) = 2^{n-1} + 1.$$

Now, we compute $\alpha(p^n)$ where p is an odd prime. In this case, the highest power of p that divides 2 is p^0, so by Proposition 15 we have $N_{p^2} \subseteq \{jp : 0 < j < p\}$ and $N_{p^3} = \varnothing$, since $A_p = I_p$ by Lemma 19.

Proposition 21. *Let p be a prime such that $p \equiv 3 \pmod 4$ and $n \geq 2$. Then $N_{p^2} = \{jp : 0 < j < p\}$ and $N_{p^3} = \varnothing$. The recurrence formula for $\alpha(p^n)$ is given by*

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

An explicit formula for $\alpha(p^n)$ *is*

$$\alpha(p^n) = \begin{cases} \frac{p}{p+1}(p^n+1), & \textit{if } n \textit{ is odd;} \\ \frac{1}{p+1}(p^{n+1}+1), & \textit{if } n \textit{ is even.} \end{cases}$$

Proof. It only remains to prove that $\{jp : 0 < j < p\} \subseteq N_{p^2}$, that is, $jp \notin A_{p^2}$ if $0 < j < p$. By contradiction, assume that $jp \in A_{p^2}$. Then, there are integers m_1, m_2 and w such that $m_1^2 + m_2^2 = jp + wp^2$. This implies that p divides $m_1^2 + m_2^2$, and by Theorem 1, p appears with even exponent in the prime decomposition of $m_1^2 + m_2^2$. In particular, p^2 divides $m_1^2 + m_2^2$, and the equation $m_1^2 + m_2^2 = jp + wp^2$ implies that p divides j, a contradiction. This proves that $N_{p^2} = \{jp : 0 < j < p\}$.

We have $n_2 = p - 1$ and $n_3 = 0$. By Proposition 13, we obtain a recurrence formula for $\alpha(p^n)$

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

Note that $\alpha(p^0) = 1$. Then, it is easy to deduce the explicit formula

$$\alpha(p^n) = \begin{cases} \frac{p}{p+1}(p^n+1), & \text{if } n \text{ is odd;} \\ \frac{1}{p+1}(p^{n+1}+1), & \text{if } n \text{ is even.} \end{cases}$$

□

Let p be a prime number such that $p \equiv 3 \pmod 4$. We can give a description of the set A_{p^n} for $n \geq 1$. By proceeding as in the case of A_{2^n}, we have A_{p^n} consists of all integers of the form

$$a_0 + a_1 \cdot p + a_2 \cdot p^2 + \cdots + a_{n-1} \cdot p^{n-1} \tag{8}$$

where

1. $a_0, a_1, a_2, \ldots, a_{n-1} \in \{0, 1, \ldots, p-1\}$,

2. $a_0 + a_1 \cdot p + a_2 \cdot p^2 + \cdots + a_{i-1} \cdot p^{i-1} \in A_{p^i}$, $i = 1, \ldots, n-1$.

By induction on n, and using that $N_{p^n} = p^2 N_{p^{n-2}}$ for $n > 3$, $N_{p^2} = \{jp : 0 < j < p\}$ and $N_{p^3} = \varnothing$, we obtain that

$$N_{p^n} = \begin{cases} \varnothing, & \text{if } n > 1 \text{ is odd;} \\ \{jp^{n-1} : 0 < j < p\}, & \text{if } n \text{ is even.} \end{cases}$$

This implies that an element of the form (8) is in A_{p^n} if and only if its first nonzero term has the form $a_i p^i$ with i even.

Proposition 22. *Let* p *be a prime such that* $p \equiv 1 \pmod 4$ *and* n *be a positive integer. Then,* $N_{p^2} = N_{p^3} = \varnothing$. *Moreover,* $\alpha(p^n) = p^n$ *for all* $n \geq 1$.

Proof. We know that $N_{p^3} = \varnothing$. To prove that $N_{p^2} = \varnothing$, it remains to prove that $jp \in A_{p^2}$ if $0 < j < p$. In fact, if $0 < j < p$, then, by Lemma 19, there are integers w_1, w_2 and w such that $w_1^2 + w_2^2 = j + wp$. Since $p \equiv 1 \pmod 4$, by Theorem 1, the product $p(w_1^2 + w_2^2)$ is a sum of two squares, say $p(w_1^2 + w_2^2) = m_1^2 + m_2^2$. Therefore, $m_1^2 + m_2^2 = p(w_1^2 + w_2^2) = p(j + wp) = jp + wp^2$. Thus, we have shown $A_{p^2} = I_{p^2}$ and therefore, $N_{p^2} = \varnothing$.

By Proposition 13, the following recurrence formula holds

$$\alpha(p^n) = \begin{cases} p, & \text{if } n = 1; \\ p\alpha(p^{n-1}), & \text{if } n > 1. \end{cases}$$

This implies that $\alpha(p^n) = p^n$ for all $n \geq 1$. □

3.2 The polynomial $x^2 + y^2 + z^2$

In this section we consider the polynomial $f(x, y, z) = x^2 + y^2 + z^2$ and its associated function α.

By Lemma 11 we have 2 is an exponent of the prime 2 in $x^2 + y^2 + z^2$. By direct computations, we check easily that $A_2 = \{0, 1\}$, $A_4 = \{0, 1, 2, 3\}$, $A_8 = \{0, 1, 2, 3, 4, 5, 6\}$, and we see that $N_4 = \varnothing$ and $N_8 = \{7\}$. From Proposition 13, it follows that

$$\alpha(2^n) = \begin{cases} 2, & \text{if } n = 1; \\ 2\alpha(2^{n-1}), & \text{if } n \text{ is even}; \\ 2\alpha(2^{n-1}) - 1, & \text{if } n > 2 \text{ is odd}. \end{cases}$$

The corresponding explicit formula is

$$\alpha(2^n) = \begin{cases} \frac{1}{3}(5 \cdot 2^{n-1} + 1), & \text{if } n \text{ is odd}; \\ \frac{2}{3}(5 \cdot 2^{n-2} + 1), & \text{if } n \text{ is even}. \end{cases}$$

We now describe explicitly the sets A_{2^n}. It is not difficult to show that

$$N_{2^n} = \begin{cases} \varnothing, & \text{if } n \text{ is even}; \\ \{7 \cdot 2^{n-3}\}, & \text{if } n \geq 2 \text{ is odd}. \end{cases}$$

For $n \geq 2$ odd, we have $N_{2^n} = \{2^{n-3} + 2^{n-2} + 2^{n-1}\}$. So the set A_{2^n} consists of all integers $a_0 + a_1 2 + \cdots + a_{n-1}2^{n-1}$ that are not of the form $2^i + 2^{i+1} + 2^{i+2} + a_{i+3}2^{i+3} + \cdots + a_{n-1}2^{n-1}$ for some odd i with $0 \leq i \leq n - 3$.

Now, we consider the case where p is an odd prime. We cannot apply Proposition 13 because there is no exponent of p in $x^2 + y^2 + z^2$, so we treat this case in a slightly different way using Lemma 10. In order to do this, we take into account that odd primes are divided into 4 families depending on their residue modulo 8. The multiplication table of $\{1, 3, 5, 7\}$ modulo 8 is shown in Table 1.

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Table 1: Multiplication modulo 8

Recall that, by Theorem 2, a nonnegative integer is representable as the sum of three squares if and only if it is not of the form $4^a(8b+7)$. From Table 1, we can deduce the following facts:

1. Dividing a number that is not of the form $4^a(8b+7)$ by a prime of the form $8k+1$, gives a number that is not of the form $4^a(8b+7)$. That is, if p is a prime of the form $8k+1$, then 1 is an exponent of p in $x^2+y^2+z^2$.

2. Dividing a number that is not of the form $4^a(8b+7)$ by the square of a prime of the form $8k+3, 8k+5$ or $8k+7$ gives a number that is not of the form $4^a(8b+7)$. Thus, if p is a prime of the form $8k+3, 8k+5$ or $8k+7$, then 2 is an exponent of p in $x^2+y^2+z^2$.

Lemma 23. *If p is an odd prime and m is a sum of three squares, then there exists $c \in \mathbb{Z}$ such that $pm - cp^2$ is the sum of three squares.*

Proof. If pm is a sum of three squares, then we can take $c = 0$. Suppose that pm is not the sum of three squares. Then one of the following cases holds:

1. p is of the form $8k+3$ and m is of the form $4^a(8b+5)$,

2. p is of the form $8k+5$ and m is of the form $4^a(8b+3)$,

3. p is of the form $8k+7$ and m is of the form $4^a(8b+1)$.

We will show that in any case, $pm-2p^2$ is not of the form $4^a(8b+7)$. If $a > 0$, then $pm-2p^2$ is not divisible by 4, so $pm-2p^2$ is not of the form $4^a(8b+7)$. Therefore, $pm-2p^2$ is a sum of three squares.

Now, assume that $a = 0$. In case 1 we have $pm - 2p^2 = (8k+3)(8b+5) - 2(8k+3)^2 = (8k+3)[8(b-2k-1)+7]$, which is a number of the form $8k+5$ and it is the sum of three squares. In case 2, $pm-2p^2 = (8k+5)(8b+3) - 2(8k+5)^2 = (8k+5)[8(b-2k-1)+1]$, which is a number of the form $8k+5$ and it is also the sum of three squares. In case 3, $pm-2p^2 = (8k+7)(8b+1) - 2(8k+7)^2 = (8k+7)[8(b-2k-2)+3]$, which is a number of the form $8k+5$ and it is the sum of three squares. $\square$

Proposition 24. *Let p be an odd prime number. Then $\alpha(p^n) = p^n$ for all $n \geq 1$.*

Proof. First of all, by Lemma 19, every element in $I_p = \{0, 1, \ldots, p-1\}$ is the sum of two squares modulo p and so, every element in I_p is the sum of three squares. This means that $A_p = \{0, 1, \ldots, p-1\}$ and $\alpha(p) = p$.

By Proposition 15, we have $N_{p^2} \subseteq \{jp : 0 < j < p\}$ and $N_{p^3} = \varnothing$.

We show that $jp \in A_{p^2}$ for all $0 < j < p$. In fact, since $j \in A_p$, there are integers w_1, w_2, w_3 and w_4 such that $w_1^2 + w_2^2 + w_3^2 = j + w_4 p$. By Lemma 23, there exists $c \in \mathbb{Z}$ such that $p(w_1^2 + w_2^2 + w_3^2) - cp^2 = u_1^2 + u_2^2 + u_3^2$ for some integers u_1, u_2 and u_3. Hence, $u_1^2 + u_2^2 + u_3^2 = p(w_1^2 + w_2^2 + w_3^2) - cp^2 = pj + w_4 p^2 - cp^2 = jp + (w_4 - c)p^2$, and this shows that $jp \in A_{p^2}$. Thus, $N_{p^2} = \varnothing$ and, consequently, $N_{p^n} = \varnothing$ for all $n \geq 2$. From this, it follows that $\alpha(p^n) = p^n$ for all $n \geq 1$. $\square$

Now we can determine all integers n such that $x^2 + y^2 + z^2$ is surjective on n. If we write $n = 2^s m$, where m is odd, then we have $\alpha(n) = \alpha(2^s)\alpha(m) = \alpha(2^s)m$. Thus, $\alpha(n) = n$ if and only if $\alpha(2^s) = 2^s$, and this last equality holds if and only if $s \leq 2$. Then, $x^2 + y^2 + z^2$ is surjective on n if and only if $n \not\equiv 0 \pmod 8$.

3.3 The polynomial $x^2 - y^2$

We make the computations of $\alpha(p^n)$ for the function associated with the polynomial $x^2 - y^2$.

We will use the following result [1, Theorem 13.4].

Theorem 25. *A positive integer n can be represented as the difference of two squares if and only if n is not of the form $4k + 2$.*

By Theorem 25, each element $a \in I_n$ that is not of the form $4k+2$ belongs to A_n. So the only elements in I_n that possibly do not belong to A_n are those that have the form $4k + 2$. It is easy to see that $A_2 = \{0, 1\}$. So, $\alpha(2) = 2$.

Proposition 26. *For any integer $n \geq 2$, A_{2^n} is the set of all elements in I_{2^n} that are not of the form $4k + 2$. Moreover, for each $n \geq 2$*

$$\alpha(2^n) = 3 \cdot 2^{n-2}. \tag{9}$$

Proof. Let $n \geq 2$. By Theorem 25, it only remains to prove that no element of the form $4k + 2$ is in A_{2^n}. Suppose, on the contrary, that $4k + 2 \in A_{2^n}$ for some k. Then there are integers m_1, m_2, w such that $m_1^2 - m_2^2 = 4k + 2 + w2^n$. It follows that $m_1^2 - m_2^2$ is even. Then, m_1 and m_2 are even or both of them are odd. In any case we obtain that $m_1^2 - m_2^2$ is divisible by 4. This yields that 4 divides 2, which is absurd.

Now, we determine the size of A_{2^n}. The elements in I_{2^n} of the form $4k+2$ are $2, 6, \ldots, 2^n - 2$. Then, there are 2^{n-2} elements in I_{2^n} of the form $4k + 2$. Thus, $\alpha(2^n) = 2^n - 2^{n-2} = 3 \cdot 2^{n-2}$. $\square$

Lemma 27. *If p is an odd prime, then p has exponent 1 in $x^2 - y^2$.*

Proof. Suppose $p = 2r + 1$ and p divides $m_1^2 - m_2^2$ for integers m_1 and m_2. If $(m_1^2 - m_2^2)/p$ is not a difference of two squares, then $m_1^2 - m_2^2 = p(4k + 2)$ for some k, and $m_1^2 - m_2^2 = (2r + 1)(4k + 2) = 4(2rk + r + k) + 2$. This contradicts Theorem 25. □

Proposition 28. *If p is an odd prime, then $\alpha(p^n) = p^n$ for all $n \geq 1$.*

Proof. Let p be an odd prime. The proof that every element in $I_p = \{0, 1, \ldots, p - 1\}$ is a difference of two squares modulo p is similar to the proof of Lemma 19. In particular, it follows that $\alpha(p) = p$.

By Proposition 15, we have $N_{p^2} \subseteq \{jp : 0 < j < p\}$ and $N_{p^3} = \varnothing$.

We show that if $0 < j < p$, then $jp \in A_{p^2}$. Since p is odd, p does not divide 4. This fact implies that there exists an integer b such that $4b \equiv j \pmod{p}$. Then $4b = j + wp$ for some w and

$$(p + b)^2 - (p - b)^2 = 4bp = jp + wp^2,$$

which shows that $jp \in A_{p^2}$.

Thus, we have $N_{p^2} = \varnothing$. It follows that $N_{p^n} = \varnothing$ for all $n \geq 2$ and $\alpha(p^n) = p^n$ for all $n \geq 1$. □

We now determine all integers $n \geq 1$ such that $x^2 - y^2$ is surjective on n. Again, if we write $n = 2^s m$, where m is odd, then we have $\alpha(n) = \alpha(2^s)m$. Therefore, $\alpha(n) = n$ if and only if $\alpha(2^s) = 2^s$, which holds if and only if $s \leq 1$. Thus, $x^2 - y^2$ is surjective on n if and only if $n \not\equiv 0 \pmod{4}$.

Remark 29. For the function α associated with a polynomial of the form $\pm x_1^2 \pm x_2^2 \pm \cdots \pm x_t^2$ with $t \geq 2$, different from $x^2 + y^2, x^2 - y^2$ and $x^2 + y^2 + z^2$, we have $\alpha(n) = n$ for all n. This is a consequence of Lagrange's four-square theorem and the fact that every integer can be expressed in the form $x^2 + y^2 - z^2$.

4 Acknowledgments

The authors thank the referee for the useful suggestions that helped to improve this paper.

References

[1] D. M. Burton, *Elementary Number Theory*, 7th ed., McGraw-Hill, 2011.

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

[3] R. Burns, Representing numbers as the sum of squares and powers in the ring $\mathbb{Z}_n$, preprint, 2017. Available at `https://arxiv.org/abs/1708.03930`.

[4] 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.

[5] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Second Edition, Springer-Verlag, 1990.

2010 *Mathematics Subject Classification*: Primary 11A07; Secondary 11B13, 11B37, 11B83.
Keywords: polynomial congruence, recurrence formula, sum of squares.

Received February 21 2019; revised version received August 13 2019; September 11 2019. Published in *Journal of Integer Sequences*, September 23 2019.

Return to Journal of Integer Sequences home page.