Journal of Integer Sequences, Vol. 18 (2015),
Article 15.11.3

Special Numbers in the Ring $\mathbb{Z}_n$

Samuel S. Gross
Noblis, Inc.
Falls Church, VA 22042
USA
samuel.gross@noblis-nsp.com

Joshua Harrington
Department of Mathematics
Cedar Crest College
Allentown, PA 18104
USA
Joshua.Harrington@cedarcrest.edu

Abstract

In a recent article, Nowicki introduced the concept of a special number. Specifically, an integer d is called *special* if for every integer m there exist solutions in non-zero integers a, b, c to the equation $a^2 + b^2 - dc^2 = m$. In this article we investigate pairs of integers (n, d), with $n \geq 2$, such that for every integer m there exist units a, b, and c in $\mathbb{Z}_n$ satisfying $m \equiv a^2 + b^2 - dc^2 \pmod{n}$. By refining a recent result of Harrington, Jones, and Lamarche on representing integers as the sum of two non-zero squares in $\mathbb{Z}_n$, we establish a complete characterization of all such pairs.

1 Introduction

The following definition was recently stated by Nowicki [4].

Definition 1. We call a positive integer d *special* if for every integer m there exist non-zero integers a, b, and c so that $a^2 + b^2 - dc^2 = m$.

The necessary conditions of the following theorem were proven by Nowicki, while Lam [3] later provided the sufficient conditions.

Theorem 2. *An integer d is special if and only if d is of the form q or $2q$ where either $q = 1$ or q is a product of primes all congruent to 1 modulo 4.*

With this complete representation of special numbers, the following theorem follows from Dirichlet's theorem on primes in arithmetic progression (see Theorem 8 below) and the Chinese remainder theorem. For completeness, we provide a proof of this theorem in Section 4.

Theorem 3. *For any odd integer $n \geq 3$, any d with $\gcd(d, n) = 1$, and any integer m, there exist integers a, b, and c such that $a^2 + b^2 - dc^2 \equiv m \pmod{n}$.*

In light of Theorem 3, we give the following definition, which imposes a unit restriction on a, b, and c.

Definition 4. We say that d is *unit-special* in $\mathbb{Z}_n$ if for an integer m, there exist units a, b, and c in $\mathbb{Z}_n$ with $a^2 + b^2 - dc^2 \equiv m \pmod{n}$.

We note that the requirement that a, b, and c be units in $\mathbb{Z}_n$ ensures that a^2, b^2, and c^2 are non-zero in $\mathbb{Z}_n$. Although one could loosen this restriction to just require a^2, b^2, and c^2 to be non-zero, this is not the setting that we investigate in this article. Among the results in this article, we provide the following complete characterization of unit-special numbers in $\mathbb{Z}_n$.

Theorem 5. *Let n be a positive integer. An integer d is unit-special in $\mathbb{Z}_n$ if and only if the following three conditions hold:*

- *n is not divisible by 2 or 3.*
- *If $p \equiv 3 \pmod{4}$ is prime and p divides n, then $\gcd(d, p) = 1$.*
- *If 5 divides n, then $d \equiv \pm 2 \pmod{5}$.*

To establish Theorem 5 we first refine a recent result of Harrington, Jones, and Lamarche [2] on representing integers as the sum of two non-zero squares in the ring $\mathbb{Z}_n$, stated below.

Theorem 6. *Let $n \geq 2$ be an integer. The equation*

$$x^2 + y^2 \equiv z \pmod{n}$$

has a non-trivial solution ($x^2, y^2 \not\equiv 0 \pmod{n}$) for all z in $\mathbb{Z}_n$ if and only if all of the following are true.

1. *q^2 does not divide n for any prime $q \equiv 3 \pmod{4}$.*
2. *4 does not divide n.*
3. *n is divisible by some prime $p \equiv 1 \pmod{4}$.*

4. *If n is odd and $n = 5^k m$ with $\gcd(5, m) = 1$ and $k < 3$, then m is divisible by some prime $p \equiv 1 \pmod 4$.*

At the end of their article, Harrington, Jones, and Lamarche ask the following question.

Question 1. *Theorem 6 considers the situation when the entire ring $\mathbb{Z}_n$ can be obtained as the sum of two non-zero squares. When this cannot be attained, how badly does it fail?*

In this article, we address Question 1 in a slightly refined setting. In particular, we prove the following theorem.

Theorem 7. *Let $n \geq 2$ be an integer. For a fixed integer z, there exist units a and b in $\mathbb{Z}_n$ such that $a^2 + b^2 \equiv z \pmod n$ if and only if all of the following hold:*

- *If $p \equiv 3 \pmod 4$ is a prime dividing n, then $\gcd(z, p) = 1$.*
- *If 5 divides n, then $z \not\equiv \pm 1 \pmod 5$.*
- *If 3 divides n, then $z \equiv 2 \pmod 3$.*
- *If 2 divides n and 4 does not, then $z \equiv 0 \pmod 2$.*
- *If 4 divides n and 8 does not, then $z \equiv 2 \pmod 4$.*
- *If 8 divides n, then $z \equiv 2 \pmod 8$.*

We again note that the requirement that a and b are units in $\mathbb{Z}_n$ ensures that a^2 and b^2 are non-zero in $\mathbb{Z}_n$. Since Question 1 does not have the unit restriction, Theorem 7 does not give a complete answer to the question. However, it does provide sufficient conditions in the setting of Question 1. Although the majority of this article focuses on the refined setting where a and b are units in $\mathbb{Z}_n$, we do briefly investigate the more general setting of Question 1 and provide a result in this direction.

2 Preliminaries and notation

We will make use of the following results and definitions from classical number theory (see, for example [1]).

Theorem 8 (Dirichlet)**.** *Let a, b be integers such that $\gcd(a, b) = 1$. Then the sequence $\{ak + b\}$, over integers k, contains infinitely many primes.*

Definition 9. Let p be an odd prime. The *Legendre symbol* of an integer a modulo p is given by

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a non-zero square modulo } p; \\ -1, & \text{if } a \text{ is not a square modulo } p; \\ 0, & \text{if } a \equiv 0 \pmod p. \end{cases}$$

Theorem 10. *Let $p \geq 7$ be a prime. There exist non-zero elements $t, u, v,$ and w in $\mathbb{Z}_p$ such that*

$$\left(\frac{u}{p}\right) = \left(\frac{u+1}{p}\right) = 1, \qquad \left(\frac{v}{p}\right) = \left(\frac{v+1}{p}\right) = -1,$$

$$\left(\frac{w}{p}\right) = -\left(\frac{w+1}{p}\right) = 1, \qquad \text{and} \qquad \left(\frac{t}{p}\right) = -\left(\frac{t+1}{p}\right) = -1.$$

The following result can be found in a book of Suzuki's [5] and is originally due to Euler.

Theorem 11. *A positive integer z can be written as the sum of two squares if and only if all prime factors q of z with $q \equiv 3 \pmod 4$ occur with even exponent.*

The following theorem, which follows immediately from the Chinese remainder theorem, appears in Harrington, Jones, and Lamarche's article.

Theorem 12. *Suppose that $m_1, m_2, \ldots, m_t$ are all pairwise relatively prime integers ≥ 2, and set $M = m_1 m_2 \cdots m_k$. Let $c_1, c_2, \ldots, c_t$ be any integers, and let $x \equiv c \pmod M$ be the solution of the system of congruences $x \equiv c_i \pmod{m_i}$ using the Chinese remainder theorem. Then there exists a y such that $y^2 \equiv c \pmod M$ if and only if there exist $y_1, y_2, \ldots, y_t$ such that $y_i^2 \equiv c_i \pmod{m_i}$.*

3 Sums of squares in $\mathbb{Z}_n$

We begin by examining when integers are a sum of two unit squares modulo n. Later we shall relax this condition and only require both squares to be non-zero modulo n.

Let us first examine the case when the modulus is a power of 2.

Theorem 13. *Let k be a positive integer. For a fixed integer z, there exist units a and b in $\mathbb{Z}_{2^k}$ such that $a^2 + b^2 \equiv z \pmod{2^k}$ if and only if one of the following is true:*

- $k = 1$ *and* $z \equiv 0 \pmod 2$*;*
- $k = 2$ *and* $z \equiv 2 \pmod 4$*;*
- $k \geq 3$ *and* $z \equiv 2 \pmod 8$.

Proof. We computationally check that the theorem is true for $k \leq 3$.

Suppose $k > 3$. If $a^2 + b^2 \equiv z \pmod{2^k}$, then $a^2 + b^2 \equiv z \pmod 8$. Thus, we deduce that $z \equiv 2 \pmod 8$.

Conversely, suppose that $z \equiv 2 \pmod 8$. We proceed with a proof by induction on k. We have already established the base case $k \leq 3$. Suppose that the theorem holds for $k - 1$ so that that there are units a and b in $\mathbb{Z}_{2^{k-1}}$ such that $a^2 + b^2 \equiv z \pmod{2^{k-1}}$. Then for some odd integer t and some integer $r \geq k - 1$ we can write

$$a^2 + b^2 = z + t2^r.$$

If $r \geq k$, then $a^2 + b^2 \equiv z \pmod{2^k}$, as desired. So suppose that $r = k - 1$. Then

$$\begin{aligned} a^2 + (b + 2^{k-2})^2 &= a^2 + b^2 + b2^{k-1} + 2^{2k-4} \\ &= z + t2^{k-1} + b2^{k-1} + 2^{2k-4} \\ &= z + 2^{k-1}(t + b) + 2^{2k-4}. \end{aligned}$$

Since $k \geq 4$, we know that $2^{2k-4} \equiv 0 \pmod{2^k}$. Also, since b was chosen to be a unit in $\mathbb{Z}_{2^{k-1}}$, then b must be odd. Thus, $t + b$ is even and we deduce that $2^{k-1}(t + b) \equiv 0 \pmod{2^k}$. Hence,

$$a^2 + (b + 2^{k-2})^2 \equiv z \pmod{2^k}.$$

It follows that $b + 2^{k-2}$ is an odd integer and is therefore a unit in $\mathbb{Z}_{2^k}$, as desired. □

We next treat the case where the modulus is a power of an odd prime. The following is an application of Hensel's Lifting Lemma. We provide the proof here for completeness.

Lemma 14. *For an odd prime p and integer z, suppose there are non-zero elements a and b_1 in $\mathbb{Z}_p$ such that $a^2 + b_1^2 \equiv z \pmod{p}$. Then for any positive integer k, the integer a is a unit in $\mathbb{Z}_{p^k}$ and there exists a unit b_k in $\mathbb{Z}_{p^k}$ such that $a^2 + b_k^2 \equiv z \pmod{p^k}$.*

Proof. Suppose that $a^2 + b_1^2 \equiv z \pmod{p}$ for some non-zero elements a and b_1 in $\mathbb{Z}_p$. Then for some integer t_1, $a^2 + b_1^2 = z + t_1 p$. Let $b_2 \equiv b_1 - t_1 p(2b_1)^{-1} \pmod{p^2}$, and note that b_2 is a unit in $\mathbb{Z}_{p^2}$. It follows that

$$\begin{aligned} a^2 + b_2^2 &\equiv a^2 + (b_1 - t_1 p(2b_1)^{-1})^2 \pmod{p^2} \\ &\equiv a^2 + b_1^2 - t_1 p \pmod{p^2} \\ &\equiv z + t_1 p - t_1 p \pmod{p^2} \\ &\equiv z \pmod{p^2}. \end{aligned}$$

Since a is also a unit modulo p^2, this proves the result for $k = 2$. The remainder of the theorem now follows by induction on k with

$$a^2 + b_{k+1}^2 \equiv z \pmod{p^{k+1}},$$

where $b_{k+1} \equiv b_k - t_k p^k (2b_k)^{-1} \pmod{p^k}$ with t_k satisfying $a^2 + b_k^2 = z + t_k p^k$. □

An appropriate converse for Lemma 14 can be stated, however the information contained in such a statement varies with the modulus. Specifically, we can easily prove the following two theorems after verifying the base case $k = 1$ and applying Lemma 14.

Theorem 15. *Let k be a positive integer. For a fixed integer z, there exist units a and b in $\mathbb{Z}_{3^k}$ with $a^2 + b^2 \equiv z \pmod{3^k}$ if and only if $z \equiv 2 \pmod{3}$.*

Theorem 16. *Let k be a positive integer. For a fixed integer z, there exist units a and b in $\mathbb{Z}_{5^k}$ with $a^2 + b^2 \equiv z \pmod{5^k}$ if and only if $z \not\equiv \pm 1 \pmod{5}$.*

For powers of primes that are 1 modulo 4, we have the following theorem which is a bit more general then Lemma 14.

Theorem 17. *Let $p \geq 13$ be a prime with $p \equiv 1 \pmod 4$ and let k be a positive integer. For every integer z, there exist units a and b in $\mathbb{Z}_{p^k}$ such that $a^2 + b^2 \equiv z \pmod{p^k}$.*

Proof. We show that the result holds for $k = 1$ and the remainder of the proof will follow from Lemma 14. So let $k = 1$. First suppose that $z \equiv 0 \pmod p$. Since $p \equiv 1 \pmod 4$, we know that -1 is a square modulo p. Thus, we can let

$$a^2 \equiv 1 \pmod p \qquad \text{and} \qquad b^2 \equiv p - 1 \pmod p$$

so that $a^2 + b^2 \equiv z \pmod p$, where a and b are units modulo p.

Now suppose that $z \not\equiv 0 \pmod p$. Since $p \geq 7$, we can use Theorem 10 to choose u such that

$$\left(\frac{u}{p}\right) = \left(\frac{u-1}{p}\right) = \left(\frac{z}{p}\right).$$

It follows that

$$\left(\frac{uz}{p}\right) = \left(\frac{-(u-1)z}{p}\right) = 1.$$

Thus, letting

$$a^2 \equiv uz \pmod p \qquad \text{and} \qquad b^2 \equiv -(u-1)z \pmod p$$

proves the result for $k = 1$ since $u, u-1$, and z are all units modulo p. □

In the next corollary, which provides an extension of Theorem 6 to our new unit-setting, we piece together the information in Theorem 17 using the Chinese remainder theorem as stated in Theorem 12.

Corollary 18. *Let $n \geq 13$ be an odd integer not divisible by 5 and with all prime divisors congruent to 1 modulo 4. Then for any fixed integer z, there exist units a and b in $\mathbb{Z}_n$ with $a^2 + b^2 \equiv z \pmod n$.*

We now turn our attention to primes that are 3 modulo 4.

Theorem 19. *Let $p \geq 7$ be a prime with $p \equiv 3 \pmod 4$ and let k be a positive integer. For a fixed integer z, there exist units a and b in $\mathbb{Z}_{p^k}$ with $a^2 + b^2 \equiv z \pmod{p^k}$ if and only if z is a unit in $\mathbb{Z}_{p^k}$.*

Proof. First suppose that the a and b are units modulo p^k with $a^2 + b^2 \equiv z \pmod{p^k}$. If z is not a unit modulo p^k, then $z \equiv xp \pmod{p^k}$ for some integer x, whence $z \equiv 0 \pmod p$. It follows that $a^2 \equiv -b^2 \pmod p$. However, this leads to a contradiction since

$$\left(\frac{-b^2}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{b^2}{p}\right) = -1.$$

For the converse, we show that the result holds for $k = 1$ and the remainder of the proof will follow from Lemma 14. In this case, choose u from Theorem 10 such that

$$\left(\frac{u}{p}\right) = -\left(\frac{u-1}{p}\right) = \left(\frac{z}{p}\right).$$

It follows that

$$\left(\frac{uz}{p}\right) = \left(\frac{-(u-1)z}{p}\right) = 1.$$

Thus, letting

$$a^2 \equiv uz \pmod{p} \qquad \text{and} \qquad b^2 \equiv -(u-1)z \pmod{p}$$

proves the result for $k = 1$ since $u, u-1$, and z are all units modulo p. □

Piecing together Theorems 13,15,16,17, and 19 using the Chinese remainder theorem as stated in Theorem 12 provides a proof for Theorem 7. We note once more that Theorem 7 provides some insight in to Question 1.

The following two corollaries are immediate consequences of Theorem 7.

Corollary 20. *Suppose n is odd and not divisible by 3 or 5. If z is a unit modulo n, then there exist units a and b in $\mathbb{Z}_n$ such that $a^2 + b^2 \equiv z \pmod{n}$.*

Corollary 21. *If n is even, then no unit can be written as the sum of two square units.*

To further address Question 1, in the following theorem we loosen the restriction that a and b are units in $\mathbb{Z}_{p^k}$ and instead only require a^2 and b^2 to be non-zero modulo p^k.

Theorem 22. *Let $p \geq 7$ be a prime with $p \equiv 3 \pmod{4}$ and let k be a positive integer. For a fixed non-zero element $z \in \mathbb{Z}_{p^k}$, there exist elements a and b with a^2 and b^2 each non-zero in $\mathbb{Z}_{p^k}$ such that $a^2 + b^2 \equiv z \pmod{p^k}$ if and only if $z \equiv xp^r \pmod{p^k}$ for some unit x in $\mathbb{Z}_{p^k}$ and some non-negative even integer $r < k$.*

Proof. Suppose that a^2 and b^2 are non-zero elements in $\mathbb{Z}_{p^k}$ with $a^2 + b^2 \equiv z \pmod{p^k}$. If z is a unit in $\mathbb{Z}_{p^k}$, then we may write $z \equiv zp^0 \pmod{p^k}$ which proves the result. Suppose, then, that z is not a unit in $\mathbb{Z}_{p^k}$. Since $z \not\equiv 0 \pmod{p^k}$, then we can write $z \equiv xp^r \pmod{p^k}$ for some unit $x \in \mathbb{Z}_{p^k}$ and some positive integer $r < k$. Thus,

$$a^2 + b^2 = xp^r + cp^k = p^r(x + cp^{k-r}),$$

for some $c \in \mathbb{Z}$. It follows that p divides $a^2 + b^2$, but p does not divide $x + cp^{k-r}$ since x is a unit in $\mathbb{Z}_{p^k}$. Hence, p^r divides $a^2 + b^2$, but p^{r+1} does not. Since $p \equiv 3 \pmod{4}$, it follows by Theorem 11 that r must be even.

Conversely, suppose that $z \equiv xp^r \pmod{p^k}$ for some unit $x \in \mathbb{Z}_{p^k}$ and some non-negative even integer $r < k$. Since x is a unit in $\mathbb{Z}_{p^k}$, it follows by Theorem 19 that there exist units

u and v such that $u^2+v^2 \equiv x \pmod{p^k}$. Since r is an even integer, we may define $a \equiv up^{r/2} \pmod{p^k}$ and $b \equiv vp^{r/2} \pmod{p^k}$. Notice that a^2 and b^2 are non-zero in $\mathbb{Z}_{p^k}$ since $r < k$. Furthermore,

$$\begin{aligned} a^2+b^2 &\equiv \left(up^{r/2}\right)^2 + \left(vp^{r/2}\right)^2 \pmod{p^k} \\ &\equiv u^2p^r + v^2p^r \pmod{p^k} \\ &\equiv xp^r \pmod{p^k}. \end{aligned}$$

This completes the proof of the theorem. □

The Chinese remainder theorem as stated in Theorem 12 along with Theorems 6 and 22 partially answers Question 1 when n is not divisible by 2 or 3.

4 Special numbers in $\mathbb{Z}_n$

For convenience and completeness, we restate and prove Theorem 3.

Theorem. *For any odd integer $n \geq 3$, any unit d in $\mathbb{Z}_n$, and any integer m, there exist integers a, b, and c such that $a^2+b^2-dc^2 \equiv m \pmod{n}$.*

Proof. Let $n \geq 3$ be an integer and let d be a unit in $\mathbb{Z}_n$. By the Chinese remainder theorem and Theorem 8 there exists some prime p satisfying

$$p \equiv 1 \pmod{4} \qquad \text{and} \qquad p \equiv d \pmod{n}.$$

It follows from Theorem 2 that such a prime must be a special number. Therefore, for any integer m, there exist integers a, b, and c such that $a^2+b^2-pc^2 = m$. In this case a, b, and c will satisfy

$$a^2+b^2-dc^2 \equiv m \pmod{n}.$$

This proves the theorem. □

Our main goal in this section is to prove Theorem 5. To do this, we first establish three lemmas.

Lemma 23. *Let k be a positive integer. Then there are no unit-special numbers modulo 2^k or 3^k.*

Proof. The theorem can be checked computationally for $k = 1$. Let $p \in \{2, 3\}$ and $k > 1$. Suppose that d is unit-special in $\mathbb{Z}_{p^k}$. Then there exist units a, b, and c in $\mathbb{Z}_{p^k}$ such that $a^2+b^2-dc^2 \equiv z \pmod{p^k}$ for all $z \in \mathbb{Z}_{p^k}$. It follows that $a^2+b^2-dc^2 \equiv z \pmod{p}$. However, since d is not unit-special in $\mathbb{Z}_p$, there is some element $z \in \mathbb{Z}_p$ that cannot be written in this form. Therefore d cannot be unit-special in $\mathbb{Z}_{p^k}$. □

Lemma 24. *Let k be a positive integer. An integer d is unit-special in $\mathbb{Z}_{5^k}$ if and only if $d \equiv \pm 2 \pmod 5$.*

Proof. The theorem can be verified computationally for $k = 1$. If d is unit-special in $\mathbb{Z}_{5^k}$ for some $k > 1$, then d is also unit-special modulo 5 whence $d \equiv \pm 2 \pmod 5$.

Conversely, suppose that $k > 1$ and $d \equiv \pm 2 \pmod 5$. Let m be any fixed integer. Then there exist units a, b, and c modulo 5 such that $a^2 + b^2 - dc^2 \equiv m \pmod 5$. As such, by Lemma 14 there exists a unit $b_k \in \mathbb{Z}_{5^k}$ with

$$a^2 + b_k^2 \equiv m + dc^2 \pmod{5^k}.$$

Therefore the result holds for all positive integers k. □

Lemma 25. *For an odd positive integer n not divisible by 3 or 5, if d is a unit in $\mathbb{Z}_n$, then d is unit-special in $\mathbb{Z}_n$.*

Proof. Let d be a unit modulo n, and fix $m \in \mathbb{Z}_n$. We proceed with two cases as to whether or not $m + d$ is a unit modulo n.

Suppose $m + d$ is a unit modulo n, then by Corollary 20 we may obtain units a and b modulo n such that

$$a^2 + b^2 \equiv m + d \pmod n.$$

The result follows by choosing $c \equiv 1 \pmod n$.

Now suppose that $m + d$ is not a unit modulo n. Factor n as

$$n = \left(\prod_{i=1}^{t} p_i^{e_i}\right) \cdot \left(\prod_{j=1}^{r} q_j^{f_j}\right)$$

where each p_i is distinct with $m + d \not\equiv 0 \pmod{p_i}$, and each q_j is distinct with $m + d \equiv 0 \pmod{q_j}$. Then it follows from Corollary 20 that there exist units a_i and b_i in $\mathbb{Z}_{p^{e_i}}$ such that $a_i^2 + b_i^2 \equiv m + d \pmod{p_i}$. Now, notice that since d is a unit modulo n, then d is also a unit modulo q_j. We deduce that $m + 4d \not\equiv 0 \pmod{q_j}$, since otherwise

$$m + d \equiv 0 \pmod{q_j} \equiv m + 4d \pmod{q_j}$$

would imply that $4 \equiv 1 \pmod{q_j}$. This cannot happen since n is not divisible by 3. Thus, $m + 4d$ is a unit in $\mathbb{Z}_{q_j}$. It follows from Corollary 20 that there exist units a_i' and b_i' in $\mathbb{Z}_{q_j^{f_j}}$ such that

$$(a_i')^2 + (b_i')^2 \equiv m + 4d \pmod{q_j^{f_j}}.$$

Next, we use the Chinese remainder theorem to choose a, b, and c which satisfy the system of congruences

$$a \equiv a_i \pmod{p_i^{e_i}} \qquad a \equiv a_i' \pmod{q_j^{f_j}}$$

$$b \equiv b_i \pmod{p_i^{e_i}} \qquad b \equiv b_i' \pmod{q_j^{f_j}}$$

and

$$c \equiv 1 \pmod{p_i^{e_i}} \qquad\qquad c \equiv 2 \pmod{q_j^{f_j}}.$$

This ensures that a, b, and c are units in $\mathbb{Z}_n$ with $a^2 + b^2 - dc^2 \equiv m \pmod{n}$. □

The following Corollary follows from Lemma 25 and Theorem 3.

Corollary 26. *Let n be an odd positive integer with $n \notin \{1, 3, 5, 9, 25\}$. Then every integer can be written as the sum of three non-zero squares in $\mathbb{Z}_n$.*

Proof. Write $n = 3^r 5^t m$ with m relatively prime to 3 and 5. First suppose that $m \neq 1$. Since -1 is a unit in $\mathbb{Z}_m$, it follows from Lemma 25 that for any integer z there exist units a_1, b_1, and c_1 in $\mathbb{Z}_m$ such that $a_1^2 + b_1^2 + c_1^2 \equiv z \pmod{m}$. Theorem 3 implies that there exist integers a_2, b_2, and c_2 such that $a_2^2 + b_2^2 + c_2^2 \equiv z \pmod{3^r 5^t}$. Using the Chinese remainder theorem as stated in Theorem 12, there exist a, b, and c such that $a^2 + b^2 + c^2 \equiv z \pmod{n}$. Such a choice of a ensures that $a^2 \equiv a_1^2 \pmod{m}$. Since a_1 is relatively prime to m we see that m does not divide a^2. Thus, n does not divide a^2. This shows that a^2 is non-zero in $\mathbb{Z}_n$. Similar arguments show that b^2 and c^2 are non-zero in $\mathbb{Z}_n$.

Now suppose that $m = 1$ so that $n = 3^r 5^t$. Following the Hensel Lifting argument of Lemma 14, it is easy to show that for a positive integer k, if z can be written as the sum of three non-zero squares in $\mathbb{Z}_{3^{k-1}}$, then it can also be written as the sum of three non-zero squares in $\mathbb{Z}_{3^k}$. We check computationally that every integer can be written as the sum of three non-zero squares in $\mathbb{Z}_{3^3}$. Thus, for $k \geq 3$, we can write every integer as the sum of three non-zero squares in $\mathbb{Z}_{3^k}$. The same argument shows that we can also write every integer as the sum of three non-zero squares in $\mathbb{Z}_{5^3}$. Using an argument similar to the one in the first paragraph of the proof, it then follows that if $r \geq 3$ or $t \geq 3$, every integer can be written as the sum of three non-zero squares in $\mathbb{Z}_n$. The remaining finite number of cases can easily be confirmed computationally. □

We are now in a position to prove Theorem 5.

Proof of Theorem 5. Lemma 23 implies that if d is unit-special in $\mathbb{Z}_n$, then n is not divisible by 2 or 3. It follows from Lemma 24 that if 5 divides n, then $d \equiv \pm 2 \pmod{5}$. Now suppose that n is divisible by some prime $p \equiv 3 \pmod{4}$. If d is unit-special in $\mathbb{Z}_n$, then we may obtain units a, b, c modulo n such that

$$a^2 + b^2 - dc^2 \equiv 0 \pmod{n}.$$

It would then follow that

$$a^2 + b^2 - dc^2 \equiv 0 \pmod{p}.$$

If $d \equiv 0 \pmod{p}$, then this would contradict Theorem 19. As such, we conclude $\gcd(d, p) = 1$.

To prove the converse, we first show that if n is odd, 5 does not divide n, and n is not divisible by any prime $p \equiv 3 \pmod{4}$, then every integer is unit-special in $\mathbb{Z}_n$. To see this, let m and d be fixed integers. By Corollary 18, there exist units a and b in $\mathbb{Z}_n$ such that $a^2 + b^2 \equiv m + d \pmod{n}$. Since m is chosen arbitrarily, this shows that d is unit-special in $\mathbb{Z}_n$ since

$$a^2 + b^2 - d \cdot (1)^2 \equiv m \pmod{n}.$$

This observation together with Theorem 12, Lemma 24, and Lemma 25 finishes the proof of the theorem. □

5 Acknowledgments

The authors would like to thank the anonymous referee for suggestions that improved this article.

References

[1] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, fifth edition, Oxford University Press, 1979.

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

[3] P. C. Lam, Representation of integers Using $a^2 + b^2 - dc^2$, *J. Integer Seq.* **18** (2015), Article 15.8.6.

[4] A. Nowicki, The numbers $a^2 + b^2 - dc^2$, *J. Integer Seq.* **18** (2015), Article 15.2.3.

[5] J. Suzuki, *Euler and Number Theory: A Study in Mathematical Invention*, Leonhard Euler: Life, Work and Legacy, Studies in the History of Philosophy of Mathematics, **5**, Robert E. Bradley and C. Edward Sandifer, eds., Elsevier, 2007.

2010 *Mathematics Subject Classification*: Primary 11E25; Secondary 11A07.
Keywords: sum of squares, ring of integers modulo n, congruence.

Received August 1 2015; revised versions received September 18 2015; September 30 2015. Published in *Journal of Integer Sequences*, November 25 2015. Order of authors switched, January 11 2016.

Return to Journal of Integer Sequences home page.