Journal of Integer Sequences, Vol. 17 (2014),
Article 14.7.4

Representing Integers as the Sum of Two Squares in the Ring $\mathbb{Z}_n$

Joshua Harrington, Lenny Jones, and Alicia Lamarche
Department of Mathematics
Shippensburg University
Shippensburg, PA 17257
USA
JSHarrington@ship.edu
lkjone@ship.edu
al5903@ship.edu

Abstract

A classical theorem in number theory due to Euler states that 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 in the prime factorization of z. One can consider a minor variation of this theorem by not allowing the use of zero as a summand in the representation of z as the sum of two squares. Viewing each of these questions in $\mathbb{Z}_n$, the ring of integers modulo n, we give a characterization of all integers $n \geq 2$ such that every $z \in \mathbb{Z}_n$ can be written as the sum of two squares in $\mathbb{Z}_n$.

1 Introduction

We begin with a classical theorem in number theory due to Euler [5].

Theorem 1. *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 in the prime factorization of z.*

Euler's complete proof of Theorem 1 first appeared in a letter to Goldbach [5], dated April 12, 1749. His proof uses a technique known as the *method of descent* [2], which was first used by Fermat to show the nonexistence of nontrivial solutions to certain Diophantine equations. Note that, according to Theorem 1, the positive integer 9, for example, can be written as the sum of two squares. Since there is only one way to write 9 as the sum of two squares, namely $9 = 3^2 + 0^2$, we conclude that 0^2 is allowed as a summand in the representation as the sum of two squares for the integers described in Theorem 1. So, a somewhat natural question to ask is the following.

Question 2. What positive integers z can be written as the sum of two nonzero squares?

A complete answer to Question 2 does not seem to appear in the literature. However, a partial answer is given by the following classical result [2, Thm. 367 and Thm. 368, pp. 299–300].

Theorem 3. *Let $n > 1$ be an integer. Then there exist $u, v \in \mathbb{Z}$, with $\gcd(u, v) = 1$, such that $n = u^2 + v^2$ if and only if -1 is a quadratic residue modulo n.*

While it is not our main concern in this article, we nevertheless provide, for the sake of completeness, an answer to Question 2 in the same flavor as Theorem 1. The next two results [2, 3] are well-known, and so we omit the proofs. The first of these results is originally due to Diophantus.

Lemma 4. *The set of positive integers that can be written as the sum of two squares is closed under multiplication.*

Lemma 4 allows us to establish the following partial answer to Question 2.

Proposition 5. *Let $p \equiv 1 \pmod 4$ be a prime, and let a be a positive integer. Then there exist nonzero squares x^2 and y^2 such that $p^a = x^2 + y^2$.*

To provide a complete answer to Question 2, we let $\mathcal{Z}$ denote the set of all integers described in Theorem 1, and we ask the following, somewhat convoluted, question.

Question 6. Which integers $z \in \mathcal{Z}$ actually do require the use of zero when written as the sum of two squares?

Certainly, the integers z that answer Question 6 are squares themselves, and therefore we have that $z = c^2$, for some positive integer c, and no integers $a > 0$ and $b > 0$ exist with $z = c^2 = a^2 + b^2$. In other words, $\sqrt{z}$ is not the third entry in a Pythagorean triple (a, b, c). Pythagorean triples (a, b, c) can be described precisely in the following way.

Theorem 7. *The triple (a, b, c) is a Pythagorean triple if and only if there exist integers $k > 0$ and $u > v > 0$ of opposite parity with $\gcd(u, v) = 1$, such that*

$$a = (u^2 - v^2)k, \quad b = (2uv)k \quad \text{and} \quad c = (u^2 + v^2)k.$$

Thus, we have the following.

Theorem 8. *Let $\widehat{\mathcal{Z}}$ be the set of positive integers that can be written as the sum of two nonzero squares. Then $z \in \widehat{\mathcal{Z}}$ if and only if $z \in \mathcal{Z}$, and if z is a perfect square, then $\sqrt{z} = (u^2+v^2)k$ for some integers $k > 0$ and $u > v > 0$ of opposite parity with* $\gcd(u, v) = 1$.

However, a closer look reveals a somewhat more satisfying description for the integers $z \in \widehat{\mathcal{Z}}$ in Theorem 8, similar in nature to the statement of Theorem 1.

Theorem 9. *Let $\widehat{\mathcal{Z}}$ be the set of positive integers that can be written as the sum of two nonzero squares. Then $z \in \widehat{\mathcal{Z}}$ if and only if all prime factors q of z with $q \equiv 3 \pmod 4$ have even exponent in the prime factorization of z, and if z is a perfect square, then z must be divisible by some prime $p \equiv 1 \pmod 4$.*

Proof. Suppose first that $z \in \widehat{\mathcal{Z}}$. Then $z \in \mathcal{Z}$ and all prime factors q of z with $q \equiv 3 \pmod 4$ have even exponent in the prime factorization of z by Theorem 1. So, suppose that $z = c^2$ for some positive integer c, and assume, by way of contradiction, that z is divisible by no prime $p \equiv 1 \pmod 4$. By Theorem 8, we can write $c = (u^2 + v^2)\, k$ for some integers $k > 0$ and $u > v > 0$ of opposite parity with $\gcd(u, v) = 1$. Since no prime $p \equiv 1 \pmod 4$ divides z, we have that no prime $p \equiv 1 \pmod 4$ divides $u^2 + v^2$. Note that $u^2 + v^2$ is odd, and so every prime q dividing u^2+v^2 is such that $q \equiv 3 \pmod 4$. Thus, by Theorem 1, every prime divisor of $u^2 + v^2$ has even exponent in the prime factorization of $u^2 + v^2$. In other words, $u^2 + v^2$ is a perfect square. Hence, $u^2 + v^2 \in \widehat{\mathcal{Z}}$, and by Theorem 8, we have that

$$\sqrt{u^2 + v^2} = \left(u_1^2 + v_1^2\right) k_1,$$

for some integers $k_1 > 0$ and $u_1 > v_1 > 0$ of opposite parity with $\gcd(u_1, v_1) = 1$. We can repeat this process, but eventually we reach an integer that is the sum of two distinct squares that has a prime factor $q \equiv 3 \pmod 4$ that occurs to an odd power in its prime factorization. This contradicts Theorem 1, and completes the proof in this direction.

If z is not a perfect square and every prime factor q of z with $q \equiv 3 \pmod 4$ has even exponent in the prime factorization of z, then z can be written as the sum of two squares by Theorem 1; and moreover, these squares must be nonzero since z is not a square itself. Thus, $z \in \widehat{\mathcal{Z}}$ in this case. Now suppose that z is a perfect square and z is divisible by some prime $p \equiv 1 \pmod 4$. Let $z = p^{2e} \prod_{i=1}^{t} r_i^{2e_i}$ be the canonical factorization of z into distinct prime powers. By Proposition 5, there exist integers $u > v > 0$, such that $p^{2e} = u^2 + v^2$. Then

$$z = \left(u \prod_{i=1}^{t} r_i^{e_i}\right)^2 + \left(v \prod_{i=1}^{t} r_i^{e_i}\right)^2 \in \widehat{\mathcal{Z}},$$

and the proof is complete. □

Remark 10. The method of proof used to establish the first half of Theorem 9 is reminiscent of Fermat's method of descent [2].

In this article, we move the setting from $\mathbb{Z}$ to $\mathbb{Z}_n$, the ring of integers modulo n, and we investigate a modification of Question 2 in this new realm. Investigations of variations of Question 2, when viewed in $\mathbb{Z}_n$, do appear in the literature. For example, Fine [1] asked if rings other than $\mathbb{Z}$ satisfy one, or both, of the following slightly-generalized conditions of Theorem 3:

1. If $r \in R$ and -1 is a quadratic residue modulo r, then $r = \pm(u^2 + v^2)$;

2. If $r = u^2 + v^2$ with $\gcd(u, v) = 1$, then -1 is a quadratic residue modulo r.

In particular, Fine showed that $\mathbb{Z}_n$ satisfies condition 2., and that $\mathbb{Z}_{p^a}$ satisfies both condition 1. and 2., when $p \equiv 3 \pmod 4$ is prime and $a \geq 2$.

Another variation of Question 2 viewed in $\mathbb{Z}_n$ was considered by Wegmann [6]. For any $k \in \mathbb{Z}_n$, he determined the least positive integer s such that the congruence

$$k \equiv x_1^2 + x_2^2 + \cdots + x_s^2 \pmod n,$$

is solvable with $x_i \in \mathbb{Z}_n$.

In this article, we are concerned with another variation of Question 2 in $\mathbb{Z}_n$. In our investigations, we discovered for certain values of n that every element in $\mathbb{Z}_n$ can be written as the sum of two nonzero squares. It is our main goal to characterize, in a precise manner, these particular values of n. For the sake of completeness, we also characterize those values of n such that every $z \in \mathbb{Z}_n$ can be written as the sum of two squares where the use of zero is allowed as a summand in such a representation of z.

2 Preliminaries and notation

To establish our results, we need some additional facts that follow easily from well-known theorems in number theory. We state these facts without proof. The first proposition follows immediately from the Chinese remainder theorem, while the second proposition is a direct consequence of Hensel's lemma.

Proposition 11. *[3] Suppose that $m_1, m_2, \ldots, m_t$ are integers with $m_i \geq 2$ for all i, and $\gcd(m_i, m_j) = 1$ for all $i \neq j$. 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 y such that $y^2 \equiv c \pmod M$ if and only if there exist $y_1, y_2, \ldots, y_t$ such that $y_i^2 \equiv c_i \pmod{m_i}$.*

Proposition 12. *[4] Let p be a prime, and let z be an integer. If there exists x such that $x^2 \equiv z \pmod p$, then there exists x_k such that $x_k^2 \equiv z \pmod{p^k}$ for every integer $k \geq 2$.*

Throughout this article, we let $\left(\frac{a}{p}\right)$ denote the Legendre symbol, where p is a prime and $a \in \mathbb{Z}$. For an integer $n \geq 2$, we define

$$\mathcal{S}_n := \left\{ s \in \mathbb{Z} \,\middle|\, 1 \leq s < n \quad \text{and } s \equiv x^2 \pmod n \text{ for some } x \in \mathbb{Z} \right\},$$

and

$$\mathcal{S}_n^0 := \mathcal{S}_n \cup \{0\}.$$

Then for a given $z \in \mathbb{Z}_n$, a pair $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ such that

$$x^2 + y^2 \equiv z \pmod{n} \tag{1}$$

is called a *nontrivial solution* to (1), provided $x^2 \equiv a \pmod{n}$ and $y^2 \equiv b \pmod{n}$ for some $a, b \in \mathcal{S}_n$. A solution (x, y) to (1), where either $x^2 \equiv 0 \pmod{n}$ or $y^2 \equiv 0 \pmod{n}$, is called a *trivial solution*. For the sake of convenience, if (x, y) is a solution to (1), we abuse notation slightly by writing $x^2, y^2 \in \mathcal{S}_n$ or $\mathcal{S}_n^0$.

3 Not allowing zero as a summand

In this section we prove the main result in this article, but first we prove a lemma.

Lemma 13. *Let z and $a \geq 1$ be integers. Let $p \equiv 1 \mod 4$ and $q \equiv 3 \pmod{4}$ be primes. Then each of the congruences*

$$x^2 + y^2 \equiv z \pmod{2} \tag{2}$$
$$x^2 + y^2 \equiv z \pmod{p^a} \tag{3}$$
$$x^2 + y^2 \equiv z \pmod{q}. \tag{4}$$

has a solution. Moreover, with the single exception of $z \equiv 0 \pmod{q}$, we can choose a solution where either $x^2 \not\equiv 0 \pmod{m}$ or $y^2 \not\equiv 0 \pmod{m}$ with $m \in \{2, p^a, q\}$.

Proof. Clearly, (2) always has a solution with $x^2 \equiv 1 \pmod{2}$. We show now that (3) always has a solution with $y^2 \not\equiv 0 \pmod{p^a}$. Suppose first that $z \equiv 0 \pmod{p^a}$. By Proposition 5, there exist positive integers x^2 and y^2 such that $x^2 + y^2 = p^a$. Then, since neither x^2 nor y^2 is divisible by p^a, we have a desired solution to (3). Now suppose that $z \not\equiv 0 \pmod{p^a}$. Let $\gcd(z, p^a) = p^b$ with $b < a$, and write $z = z'p^b$. Consider the arithmetic progression

$$\mathcal{A}_k := 4p^{a-b}k + p^{a-b}(1 - z') + z'.$$

Note that for any integer k, we have that $\mathcal{A}_k \equiv z' \pmod{p^a}$ and $\mathcal{A}_k \equiv 1 \pmod{4}$. Then, since $\gcd\left(4p^{a-b}, p^{a-b}(1 - z') + z'\right) = 1$, it follows from Dirichlet's theorem on primes in an arithmetic progression that $\mathcal{A}_k$ contains infinitely many primes $r \equiv 1 \pmod{4}$. For such a prime r, Theorem 9 tells us that there exist nonzero integers x^2 and y^2 such that $x^2+y^2 = p^b r$. Observe that x^2 and y^2 cannot both be divisible by p^a. Hence, since $p^b r \equiv z \pmod{p^a}$, we have a solution to (3), where, after relabeling if necessary, $y^2 \not\equiv 0 \pmod{p^a}$.

We show next that (4) always has a solution. If $z \equiv 0 \pmod{q}$, then we can take $x^2 \equiv y^2 \equiv 0 \pmod{q}$. If $z \not\equiv 0 \pmod{q}$, then we consider the arithmetic progression

$$\mathcal{B}_k := 4qk + q(3 + z) + z.$$

Note here that $\mathcal{B}_k \equiv z \pmod q$ and $\mathcal{B}_k \equiv 1 \pmod 4$ for any integer k. As before, since $\gcd(4q, q(3+z)+z) = 1$, it follows from Dirichlet's theorem that $\mathcal{B}_k$ contains infinitely many primes $r \equiv 1 \pmod 4$. Thus, by Proposition 5, there exist nonzero integers x^2 and y^2 such that $x^2 + y^2 = r$ for such a prime r. Clearly, not both x^2 and y^2 are divisible by q. Hence, with the exception of $z \equiv 0 \pmod q$, we have a solution to (4) where we can choose $y^2 \not\equiv 0 \pmod q$. □

Theorem 14. *Let $n \geq 2$ be an integer. Then, for every $z \in \mathbb{Z}_n$, (1) has a nontrivial solution if and only if*

1. $n \not\equiv 0 \pmod{q^2}$ *for any prime* $q \equiv 3 \pmod 4$ *with* $n \equiv 0 \pmod q$
2. $n \not\equiv 0 \pmod 4$
3. $n \equiv 0 \pmod p$ *for some prime* $p \equiv 1 \pmod 4$
4. *Also, when $n \equiv 1 \pmod 2$, we have the following additional conditions. Write $n = 5^k m$, where $m \not\equiv 0 \pmod 5$. Then either*
   (a) *$k \geq 3$, with no further restrictions on m, or*
   (b) *$k < 3$ and $m \equiv 0 \pmod p$ for some prime $p \equiv 1 \pmod 4$.*

Proof. Suppose first that, for every $z \in \mathbb{Z}_n$, (1) has a nontrivial solution. Let q be a prime divisor of n. Then there exist $a^2, b^2, c^2, d^2, e^2, f^2 \in \mathcal{S}_n$, such that

$$a^2 + b^2 \equiv q \pmod n, \tag{5}$$
$$c^2 + d^2 \equiv -1 \pmod n \quad \text{and} \tag{6}$$
$$e^2 + f^2 \equiv 0 \pmod n. \tag{7}$$

Suppose that $q \equiv 3 \pmod 4$ is a prime such that $n \equiv 0 \pmod{q^2}$. Then we have from (5) that

$$a^2 + b^2 = kq^2 + q = q(kq+1), \tag{8}$$

for some nonzero $k \in \mathbb{Z}$. However, (8) contradicts Theorem 1, since clearly q divides $q(kq+1)$ to an odd power. This proves that 1. holds.

If $n \equiv 0 \pmod 4$, then we have from (6) that $c^2 + d^2 \equiv 3 \pmod 4$, which is impossible since the set of all squares modulo 4 is $\{0, 1\}$. Hence, 2. holds.

We see from (7) that $e^2 \equiv -f^2 \pmod q$ for every prime $q \equiv 3 \pmod 4$ with $n \equiv 0 \pmod q$. Since $\left(\frac{-1}{q}\right) = -1$ for primes $q \equiv 3 \pmod 4$, we deduce that $e \equiv f \equiv 0 \pmod q$. Hence, if $n \equiv 1 \pmod 2$ and n is divisible by no prime $p \equiv 1 \pmod 4$, it follows from (1) that $e \equiv f \equiv 0 \pmod n$, which contradicts the fact that $e^2, f^2 \in \mathcal{S}_n$. From (2), if $n \equiv 0 \pmod 2$, then we can write $n = 2m$, where $m \equiv 1 \pmod 2$. By hypothesis, there exist $s^2, t^2 \in \mathcal{S}_n$ such that $s^2 + t^2 \equiv m \pmod n$. If m is divisible by no prime $p \equiv 1 \pmod 4$, then as before, since $\left(\frac{-1}{q}\right) = -1$ for primes $q \equiv 3 \pmod 4$, we conclude that $s \equiv t \equiv 0$

(mod m). But $s^2+t^2 \equiv 1 \pmod 2$ which implies, without loss of generality, that $s \equiv 0 \pmod 2$. Therefore, $s \equiv 0 \pmod n$, which contradicts the fact that $s^2 \in \mathcal{S}_n$. Thus, 3. holds.

Assume now that $n \equiv 1 \pmod 2$, and write $n = 5^k m$, where $m \not\equiv 0 \pmod 5$. Consider first the possibility that $k = 1$ and no prime $p \equiv 1 \pmod 4$ divides m. To rule this case out, we assume first that $\left(\frac{m}{5}\right) = 1$. By hypothesis, there exist $s^2, t^2 \in \mathcal{S}_n$ such that $s^2+t^2 \equiv m \pmod n$. If $m = 1$, then $n = 5$ and this is impossible since the set of nonzero squares modulo 5 is $\{1, 4\}$. If $m > 1$ then every prime divisor q of m is such that $q \equiv 3 \pmod 4$. So, we must have, as before, that $s \equiv t \equiv 0 \pmod m$. Therefore, since $s^2, t^2 \in \mathcal{S}_n$, we deduce that $s^2 \not\equiv 0 \pmod 5$ and $t^2 \not\equiv 0 \pmod 5$. Since $\left(\frac{m}{5}\right) = 1$, it follows modulo 5 that $s^2, t^2, m \in \{1, 4\}$. But then again, $s^2+t^2 \equiv m \pmod 5$ is impossible. If $\left(\frac{m}{5}\right) = -1$, then the proof is identical, except that the representation $s^2+t^2 \equiv 2m \pmod n$ is impossible since modulo 5 we have $m \in \{2, 3\}$, which implies that $s^2+t^2 \equiv 2m \pmod 5$ is impossible.

The possibility that $k = 2$ and no prime $p \equiv 1 \pmod 4$ divides m can be ruled out in a similar manner by using the fact that the nonzero squares modulo 25 are $\{1, 4, 6, 9, 11, 14, 16, 19, 21, 24\}$, and reducing the situation to an examination of the representations:

$$s^2+t^2 \equiv \begin{cases} 1 \pmod{25}, & \text{if } m = 1; \\ m \pmod{25}, & \text{if } m > 1 \text{ and } \left(\frac{m}{5}\right) = 1; \\ 2m \pmod{25}, & \text{if } m > 1 \text{ and } \left(\frac{m}{5}\right) = -1. \end{cases}$$

This completes the proof of the theorem in this direction.

Now suppose that conditions 1., 2., 3. and 4. hold, and let z be a nonnegative integer. Our strategy here is to use Lemma 13 and Proposition 11 to piece together the solutions for each distinct prime power dividing n to get a nontrivial solution to (1).

We consider two cases: $n \equiv 0 \pmod 2$ and $n \equiv 1 \pmod 2$. If $n \equiv 0 \pmod 2$, then we can write

$$n = 2\left(\prod_{i=1}^{s} p_i^{a_i}\right)\prod_{i=1}^{t} q_i,$$

where $s \geq 1$, $t \geq 0$, $p_i \equiv 1 \pmod 4$ and $q_i \equiv 3 \pmod 4$. Note that $t = 0$ is a possibility, and in this case, we define the empty product $\prod_{i=1}^{t} q_i$ to be 1. Since $s \geq 1$, we have from Lemma 13 that there exist solutions to (2) and (3) where respectively $x^2 \not\equiv 0 \pmod 2$ and $y^2 \not\equiv 0 \pmod{p_i^{a_i}}$. Then, using Proposition 11 to piece together the solutions for x^2 and y^2 modulo each modulus in $\{2, p_1^{a_1}, \ldots, p_t^{a_t}\}$, we get a nontrivial solution to (1).

We now turn our attention to the case $n \equiv 1 \pmod 2$, and write

$$n = 5^k\left(\prod_{\substack{i=1 \\ p_i \neq 5}}^{s} p_i^{a_i}\right)\prod_{i=1}^{t} q_i.$$

where $p_i \equiv 1 \pmod 4$ and $q_i \equiv 3 \pmod 4$ are primes. Suppose first that $k \leq 2$. Then it is easy to check that the only solutions to

$$x^2+y^2 \equiv 1 \pmod{5^k}$$

have either $x^2 \equiv 0 \pmod{5^k}$ or $y^2 \equiv 0 \pmod{5^k}$. However, we can always choose a solution with $x^2 \not\equiv 0 \pmod{5^k}$. Since $k \leq 2$, we have that $s \geq 1$ so that there exists a prime $p \equiv 1 \pmod 4$ that divides n, with $p \neq 5$. Hence, by Lemma 13, (3) always has a solution where $y^2 \not\equiv 0 \pmod{p^a}$. This allows us again to use Proposition 11 to get a nontrivial solution to (1).

Suppose next that $k \geq 3$. If $s \neq 0$, then as before, we can invoke Lemma 13 and Proposition 11 to achieve a nontrivial solution to (1). So, assume that $s = 0$. We show that the congruence

$$x^2 + y^2 \equiv z \pmod{5^k}, \tag{9}$$

always has a solution where $x^2 \not\equiv 0 \pmod{5^k}$ and $y^2 \not\equiv 0 \pmod{5^k}$. Since $x^2 + y^2 = 5^k$ has a solution (by Theorem 9) with neither x^2 nor y^2 divisible by 5^k, it follows that (9) has a nontrivial solution when $z \equiv 0 \pmod{5^k}$. Now suppose that $z \not\equiv 0 \pmod{5^k}$. We know from Lemma 13 that (9) has a solution with $y^2 \not\equiv 0 \pmod{5^k}$. If $z \notin \mathcal{S}_{5^k}$, then it must be that $x^2 \not\equiv 0 \pmod{5^k}$ as well, which gives us a nontrivial solution. So, let $z \in \mathcal{S}_{5^k}$. Since $-24 \equiv 1 \in \mathcal{S}_5$, it follows from Proposition 12 that, for any integer $k \geq 2$, there exists x such that

$$x^2 \equiv -24 \pmod{5^k}, \tag{10}$$

with $x^2 \not\equiv 0 \pmod{5^k}$. We can rewrite (10) as

$$x^2 + 5^2 \equiv 1 \pmod{5^k}, \tag{11}$$

which implies that (3) has a nontrivial solution when $z \equiv 1 \pmod{5^k}$–provided that $k \geq 3$, which we have assumed here. Also, note that this nontrivial solution to (11) has $x^2 \not\equiv 0 \pmod 5$. Hence, for any $z \in \mathcal{S}_{5^k}$ with $z \not\equiv 0 \pmod 5$, we see that multiplying (11) by z yields a nontrivial solution to (3) for these particular values of z. Now suppose that $z \in \mathcal{S}_{5^k}$ with $z \equiv 0 \pmod 5$. Then $z - 1 \equiv 4 \pmod 5$ and, by Proposition 12, we have, for any integer $k \geq 2$, that there exists $x \not\equiv 0 \pmod{5^k}$ such that $x^2 \equiv z - 1 \pmod{5^k}$. That is,

$$x^2 + 1 \equiv z \pmod{5^k},$$

and hence we have a nontrivial solution to (1) in this last case, which completes the proof of the theorem. $\square$

The first 25 values of n satisfying the conditions of Theorem 14 are

$$10, 13, 17, 26, 29, 30, 34, 37, 39, 41, 50, 51, 53, 58, 61, 65, 70, 73, 74, 78, 82, 85, 87, 89, 91.$$

This sequence is A240109 in the Online Encyclopedia of Integer Sequences.

4 Allowing zero as a summand

For the sake of completeness, we address now the situation when trivial solutions are allowed in (1). The main theorem of this section gives a precise description of the integers n such that, for any $z \in \mathbb{Z}_n$, (1) has a solution (x, y) with $x^2, y^2 \in \mathcal{S}_n^0$. Certainly, the proof of this result builds off of Theorem 14 since every value of n for which there exists a nontrivial solution to (1) will be included here as well. From an analysis of the proof of Theorem 14, it is easy to see that allowing 0 as a summand does not buy us any new values of n here under the restrictions found in parts 1. and 2. of Theorem 14. However, it turns out that the restrictions in parts 3. and 4. of Theorem 14 are not required. More precisely, we have:

Theorem 15. *Let $n \geq 2$ be an integer. Then, for every $z \in \mathbb{Z}_n$, the congruence (1) has a solution (x, y) with $x^2, y^2 \in \mathcal{S}_n^0$ if and only if the following conditions hold:*

1. $n \not\equiv 0 \pmod{q^2}$ *for any prime* $q \equiv 3 \pmod 4$ *with* $n \equiv 0 \pmod q$
2. $n \not\equiv 0 \pmod 4$.

Proof. We show first that condition 3. of Theorem 14 is not required here. Suppose that every prime divisor p of n is such that $p \equiv 3 \pmod 4$. Certainly, if $z \in \mathbb{Z}_n$ is such that $z \equiv a^2 \pmod n$ for some $a \in \mathbb{Z}_n$, then (1) has a solution (x, y), with $x^2, y^2 \in \mathcal{S}_n^0$; namely $(a, 0)$. So, we need to show that (1) has a solution (x, y) with $x^2, y^2 \in \mathcal{S}_n^0$ for every nonsquare $z \in \mathbb{Z}_n$. To begin, we claim that (1) has a solution modulo p when $z = -1$, which is not a square modulo p. For $a \in \mathbb{Z}_p$, if $\left(\frac{a}{p}\right) = 1$ and $\left(\frac{a+1}{p}\right) = -1$, then $\left(\frac{-a-1}{p}\right) = 1$. Thus,

$$a + (-a - 1) \equiv -1 \pmod p.$$

Such an element $a \in \mathbb{Z}_p$ must exist, otherwise all elements of $\mathbb{Z}_p$ would be squares, which is absurd. Now, any nonsquare $z \in \mathbb{Z}_p$ can be written as $-(-z)$, where $\left(\frac{-z}{p}\right) = 1$. Therefore, $\left(\frac{-za}{p}\right) = \left(\frac{-z(-a-1)}{p}\right) = 1$, and we have that

$$(-za) + (-z)(-a - 1) \equiv z \pmod p.$$

Then we can use Proposition 12 to lift this solution modulo p to a solution modulo p^a, where p^a is the exact power of p that divides n. Finally, we use Proposition 11 to piece together the solutions for each of these prime powers to get a solution modulo n.

To see that the restrictions in part 4. of Theorem 14 are not required here, we note that the restriction that m be divisible by some odd prime $p \equiv 1 \pmod 4$ is not required by the previous argument. Therefore, to complete the proof of the theorem, it is enough to observe that every element in $\mathbb{Z}_5$ and $\mathbb{Z}_{25}$ can be written as the sum of two elements in $\mathcal{S}_5^0$ and $\mathcal{S}_{25}^0$, respectively. □

The first 25 values of n satisfying the conditions of Theorem 15 are

$$2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19, 21, 22, 23, 25, 26, 29, 30, 31, 33, 34, 35, 37, 38.$$

This sequence is A243609 in the Online Encyclopedia of Integer Sequences.

5 Future considerations

Theorem 14 and Theorem 15 consider the situation when the entire ring $\mathbb{Z}_n$ can be obtained as the sum of two squares. When this cannot be attained, how badly does it fail; and is there a measure of this failure in terms of n? There are certain clues to the answers to these questions in the proof of Theorem 14, but we have not pursued the solution in this article.

6 Acknowledgments

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

References

[1] B. Fine, Sum of squares rings, *Canad. J. Math* **29** (1977), 155–160.

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

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

[4] M. Nathanson, *Elementary Methods in Number Theory*, Springer-Verlag, 2000.

[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.

[6] H. Wegmann, Quadratsummen in Restklassenringen. *Elem. Math.* **38** (1983), 36–39.

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

(Concerned with sequences A240109, and A243609.)

Received April 1 2014; revised versions received June 10 2014; June 12 2014. Published in *Journal of Integer Sequences*, June 21 2014.

Return to Journal of Integer Sequences home page.