Strong-Square Divisors

V Sai Prabhav
saiprabhav.ss@gmail.com

July 14, 2025

Abstract

The Online Encyclopedia of Integer Sequences lists A167181 as the sequence of square free numbers whose prime divisors are all congruent to 3 modulo 4. In this note we prove that this sequence is identical to the sequence of numbers n with the property that if n divides a^2+b^2 then n divides both a and b.

Definition 1 (strong-square divisors)**.** *Let $n \in \mathbb{N}$. The number n is called a **strong-square divisor** if, for all $a, b \in \mathbb{N}$, the condition $n \mid a^2+b^2$ implies that $n \mid a$ and $n \mid b$. Let $\mathcal{D}$ be the set of all strong-square divisors.*

Example 1. *The integer 3 is a strong-square divisor as $x^2 \equiv 1$ or $0 \pmod 3$ for all $x \in \mathbb{N}$, so $a^2+b^2 \not\equiv 0 \pmod 3$ unless $3 \mid a$ and $3 \mid b$.*

Lemma 1. *If $n \in \mathbb{N}$ is not square free, then $n \notin \mathcal{D}$.*

Proof. If $n \in \mathbb{N}$ is not square free, then there exist $r, t \in \mathbb{N}$ such that

$$n = t^2 r,$$

where r is square free and $t > 1$. Let

$$c = (tr)^2 + (tr)^2.$$

Clearly, $n \mid c$ but $n \nmid tr$. Hence, by definition, $n \notin \mathcal{D}$. □

Corollary 1. *If $n \equiv 0 \pmod 4$, then $n \notin \mathcal{D}$ as n is not square free.*

Lemma 2. *If $n \equiv 2 \pmod 4$, then $n \notin \mathcal{D}$.*

Proof. If $n \equiv 2 \pmod 4$ then there exist $k \in \mathbb{N}$ such that $n = 4k+2$. Let

$$\begin{aligned} c &= (2k+1)^2 + (2k+1)^2 \\ &= 2(2k+1)^2 \\ &= (4k+2)(2k+1) \\ &= n(2k+1). \end{aligned}$$

Clearly, $n \mid c$ but $n \nmid (2k+1)$. Hence, $n \notin \mathcal{D}$. □

Lemma 3. *If $n \notin \mathcal{D}$, then $nm \notin \mathcal{D}$ for all $m \in \mathbb{N}$.*

Proof. If $n \notin \mathcal{D}$, then there exist $a, b \in \mathbb{N}$ such that $n \mid a^2+b^2$ but $n \nmid a$. Let $m \in \mathbb{N}$ and

$$\begin{aligned} c &= (am)^2 + (bm)^2 \\ &= m^2 \left(a^2+b^2\right). \end{aligned}$$

As $n \mid a^2+b^2$, it follows that $nm \mid m(a^2+b^2)$, and consequently, $nm \mid c$. Since $n \nmid a$, by the Euclidean Division Algorithm, we have $a = nk + r$ where $k, r \in \mathbb{N}$ and $0 < r < n$. It follows that $am = (nm)k + rm$, where $0 < rm < nm$, so $nm \nmid am$. Hence, by definition, $nm \notin \mathcal{D}$. □

Lemma 4. *Let p be a prime such that $p \equiv 1 \pmod 4$, then $p \notin \mathcal{D}$.*

Proof. From Euler's Criterion, we have that -1 is a quadratic residue modulo p since $p \equiv 1 \pmod 4$. That is, there exists $x \in \mathbb{N}$ such that

$$x^2 \equiv p - 1 \pmod p.$$

Clearly, $1^2 + x^2 \equiv 0 \pmod p$, but $p \nmid 1$. Hence, by definition, $p \notin \mathcal{D}$. □

Lemma 5. *Let p be a prime such that $p \equiv 3 \pmod 4$, then $p \in \mathcal{D}$.*

Proof. We prove this by contradiction. Suppose that $p \equiv 3 \pmod 4$ and $p \notin \mathcal{D}$. Since $p \notin \mathcal{D}$ there exist $a, b \in \mathbb{N}$ such that

$$p \mid (a^2 + b^2) \text{ and } p \nmid a \text{ or } p \nmid b.$$

If $p \mid (a^2 + b^2)$ then $a^2 + b^2 \equiv 0 \pmod p$ which implies that $-a^2 \equiv b^2 \pmod p$. Thus $-a^2$ is a quadratic residue and a^2, like any square, is a quadratic residue. Without loss of generality, we can assume that $p \nmid a$. Then $\gcd(a, p) = 1$ and thus, using Legendre symbols and noting that $\left(\frac{-1}{p}\right)$ by Euler's Criterion, we have

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

Therefore exactly one of a^2 and $-a^2$ is quadratic residue. This contradicts the fact that both a^2 and $-a^2$ are quadratic residues modulo p. □

Corollary 2. *If $n \in \mathbb{N}$, and p is a prime such that $p \equiv 1 \pmod 4$ and $p \mid n$, then $n \notin \mathcal{D}$.*

Proof. From Lemma 4, $p \notin \mathcal{D}$, and from Lemma 3, $n \notin \mathcal{D}$ if $p \mid n$. □

Lemma 6. *Let $q \in \mathbb{Z}$, and let p_1 and p_2 be coprime integers. Then q is a quadratic residue modulo p_1p_2 if and only if q is a quadratic residue modulo both p_1 and p_2.*

Proof. If q is a quadratic residue modulo p_1p_2. Then, there exist x such that $x^2 \equiv q \pmod{p_1p_2}$ which implies that $x^2 \equiv q \pmod{p_1}$ and $x^2 \equiv q \pmod{p_2}$. Conversely, if q is a quadratic residue modulo p_1 and p_2 then there exist $a_1, a_2 \in \mathbb{Z}$ such that,

$$a_1^2 \equiv q \pmod{p_1}, \quad a_2^2 \equiv q \pmod{p_2}.$$

By the Chinese Remainder Theorem, since p_1 and p_2 are coprime, there exists $x \in \mathbb{Z}$ such that

$$x \equiv a_1 \pmod{p_1}, \quad x \equiv a_2 \pmod{p_2}$$

then,

$$x^2 \equiv a_1^2 \equiv q \pmod{p_1}, \quad x^2 \equiv a_2^2 \equiv q \pmod{p_2},$$

which implies $x^2 \equiv q \pmod{p_1p_2}$. Hence, q is a quadratic residue modulo p_1p_2. □

Lemma 7. *Let n be a square free natural number. Then n can be written in the form $n = p_1p_2 \cdots p_k$, where $p_1, p_2, \ldots, p_k$ are distinct prime numbers. Then, q is a quadratic residue modulo n if and only if q is a quadratic residue modulo each p_i for $1 \leq i \leq k$.*

Proof. We proceed by induction on the number of prime factors of n. The base case, where n is a single prime p_1, is trivial. For the inductive step, assume the lemma holds for any number with $k-1$ distinct prime factors. Let $n = p_1p_2 \cdots p_k$, and write $n = n'p_k$ where $n' = p_1p_2 \cdots p_{k-1}$. By Lemma 6, q is a quadratic residue modulo n if and only if it is a quadratic residue modulo both n' and p_k. By the induction hypothesis, q is a quadratic residue modulo n' if and only if it is a quadratic residue modulo each of $p_1, \ldots, p_{k-1}$. Combining these, q is a quadratic residue modulo n if and only if it is a quadratic residue modulo each of $p_1, \ldots, p_k$. □

Lemma 8. *If $n \notin \mathcal{D}$ and n is square free, then there exists $q \in \mathbb{N}$ such that $n \nmid q$, and both q and $-q$ are quadratic residues modulo n.*

Proof. Suppose $n \notin \mathcal{D}$. Then there exist $a, b \in \mathbb{N}$ such that $a^2 + b^2 \equiv 0 \pmod{n}$, where $n \nmid a$. It follows that $a^2 \equiv -b^2 \pmod{n}$. Note that both a^2 and b^2 are quadratic residues modulo n. Let $q = a^2$, so that $b^2 \equiv -q \pmod{n}$, implying both q and $-q$ are quadratic residues modulo n. Since $n \nmid a$ and n is square free, we have $n \nmid a^2$, which implies $n \nmid q$. □

Lemma 9. *If $n \in \mathcal{D}$ and $n \nmid q$, then both q and $-q$ cannot be quadratic residues modulo n.*

Proof. Suppose that both q and $-q$ are quadratic residues modulo n. Then there exist $a, b \in \mathbb{Z}$ such that $a^2 \equiv q \pmod{n}$ and $b^2 \equiv -q \pmod{n}$. Adding these congruences, we get $a^2 + b^2 \equiv 0 \pmod{n}$, so $n \mid a^2 + b^2$. By the definition of strong-square divisors, this means $n \mid a$ and $n \mid b$, and hence $n \mid a^2$, so $n \mid q$. Hence there does not exist q such that $n \nmid q$ and both q and $-q$ are quadratic residues of n. □

Theorem 1. *The integer n is a strong-square divisor if and only if n is a square free number such that all prime factors are congruent to 3 modulo 4.*

Proof. Let $\mathcal{T}$ be the set of all square free numbers such that all prime factors are congruent to 3 modulo 4. We prove the theorem by showing that if $n \in \mathcal{T}$, then $n \in \mathcal{D}$ ($\mathcal{T} \subseteq \mathcal{D}$), and by showing that if $n \notin \mathcal{T}$, then $n \notin \mathcal{D}$ ($\mathcal{T}^c \subseteq \mathcal{D}^c$). If $n \in \mathcal{T}$, then n is of the form $n = p_1 p_2 \cdots p_k$, where $p_1, p_2, \ldots, p_k$ are prime numbers congruent to 3 (mod 4). Suppose, for the sake of contradiction, that $n \notin \mathcal{D}$. Since n is square free, by Lemma 8, there exists some $q \in \mathbb{N}$ such that both q and $-q$ are quadratic residues modulo n, and $n \nmid q$. We will show that this is not possible when $n \in \mathcal{T}$, thereby concluding that $n \in \mathcal{D}$. Suppose q is a quadratic residue modulo n. Then, by Lemma 7, $-q$ is a quadratic residue modulo n if and only if $-q$ is a quadratic residue modulo each p_i, where $1 \leq i \leq k$. Since each $p_i \in \mathcal{D}$ (by Lemma 5), $-q$ is not a quadratic residue modulo p_i (by Lemma 9). Hence, $-q$ is not a quadratic residue modulo n. Thus, the assumption that both q and $-q$ are quadratic residues modulo n leads to a contradiction. We conclude that if $n \in \mathcal{T}$, then $n \in \mathcal{D}$.

Conversely, since $\mathcal{T}$ is the set of square free numbers whose prime divisors are all congruent to 3 (mod 4), if $n \notin \mathcal{T}$, then either $p \mid n$ for some prime $p \equiv 1 \pmod{4}$, or n is even, or n is not square free. We will show that in each of these cases, $n \notin \mathcal{D}$.

Case 1: If $p \mid n$ for some $p \equiv 1 \pmod{4}$, then $n \notin \mathcal{D}$ by Corollary 2.

Case 2: If n is even, then $n \notin \mathcal{D}$ by Corollary 1 and Lemma 2.

Case 3: If n is not square free, then $n \notin \mathcal{D}$ by Lemma 1. □

Since sets $\mathcal{T}$ and $\mathcal{D}$ are equal, sequences based on these sets with elements in increasing size will be identical. This proves that the two sequences in the abstract are identical.

Acknowledgements

I wish to express my sincere gratitude to Randell Heyman for his invaluable guidance, insightful suggestions, and constant encouragement throughout the course of this research. His mentorship was instrumental in the development and refinement of this paper.