

POW 2025-18

Eunseong Kim (Daegu Science High School)

Problem

Find all integers k such that the sequence $(3n^2 + 3nk^2 + k^3)_{n=1,2,\dots}$ contains infinitely many squares.

Answer

The integers satisfying the problem conditions are precisely the integers $k \neq 0$ satisfying the following two conditions:

- The quotient of $k(3k - 4)$ by the largest square dividing it does not have a prime divisor congruent to 5 or 7 modulo 12.
- For $k = 3^\alpha r$ where $\alpha \in \mathbb{Z}_{\geq 0}$ and $3 \nmid r \in \mathbb{Z}$, either α is even and $r \equiv 1 \pmod{3}$, or α is odd and $r \equiv 2 \pmod{3}$.

Proof

We begin with examining the basic properties of the quadratic ring $\mathcal{O} = \mathbb{Z}[\sqrt{3}]$. We define a function $\mathcal{N} : \mathcal{O} \rightarrow \mathbb{Z}$ as

$$\mathcal{N}(a + b\sqrt{3}) = a^2 - 3b^2$$

Define the conjugate of $w = a + b\sqrt{3} \in \mathcal{O}$ ($a, b \in \mathbb{Z}$) as $\bar{w} = a - b\sqrt{3}$. It is straightforward to see that $\mathcal{N}(w) = w\bar{w}$ and \mathcal{N} is multiplicative.

Claim 1. $\mathbb{Z}[\sqrt{3}]$ is a Unique Factorization Domain.

Proof. We prove the stronger statement that $\mathbb{Z}[\sqrt{3}]$ is an Euclidean Domain with Euclidean function $|\mathcal{N}|$. For any $w_1, w_2 \in \mathcal{O}$ such that $w_2 \neq 0$, $w_1/w_2 = r + s\sqrt{3}$ for $r, s \in \mathbb{Q}$. Choose $m, n \in \mathbb{Z}$ such that $\alpha = r - m$ and $\beta = s - n$ are not greater than 0.5 in absolute value. Then $w_1 = w_2(m + n\sqrt{3}) + w$ where $w = (\alpha + \beta\sqrt{3})w_2 \in \mathcal{O}$. $|\mathcal{N}(w)| = |\alpha^2 - 3\beta^2||\mathcal{N}(w_2)| \leq 0.75|\mathcal{N}(w_2)| < |\mathcal{N}(w_2)|$, so $|\mathcal{N}|$ is an Euclidean function. \square

Claim 2. For $p \in \mathbb{Z}$ irreducible in \mathbb{Z} (that is, p is \pm (prime number)), there is no $n \in \mathbb{Z}$ such that $p|n^2 - 3$ if and only if p is congruent to 5 or 7 modulo 12.

Proof. Since $2|1^2 - 3$ and $3|3^2 - 3$, there is $n \in \mathbb{Z}$ with $p|n^2 - 3$ if $p \in \{\pm 2, \pm 3\}$. Now assume $|p| \geq 5$. Then p is congruent to ± 1 or ± 5 modulo 12. There is $n \in \mathbb{Z}$ with $p|n^2 - 3$ if and only if 3 is a quadratic residue modulo $|p|$. Using Legendre symbols, this is equivalent to

$$1 = \left(\frac{3}{|p|} \right) = (-1)^{\frac{|p|-1}{2}} \left(\frac{|p|}{3} \right)$$

Since p is a quadratic residue modulo 3 if and only if $|p| \equiv 1 \pmod{3}$, the above equation holds if and only if either $|p| \equiv 1 \pmod{4}$ and $|p| \equiv 1 \pmod{3}$ or $|p| \equiv 3 \pmod{4}$ and $|p| \equiv 2 \pmod{3}$, if and only if $|p| \equiv \pm 1 \pmod{12}$. Hence there is no $n \in \mathbb{Z}$ such that $p|n^2 - 3$ if and only if $p \equiv \pm 5 \pmod{12}$. \square

Claim 3. The irreducible elements of \mathcal{O} are precisely the following:

- The irreducible elements of \mathbb{Z} congruent to 5 or 7 modulo 12.
- The two (up to multiplication by a unit) irreducible factors of each irreducible element of \mathbb{Z} not congruent to 5 or 7 modulo 12.

Proof. If $w = a + b\sqrt{3} \in \mathcal{O}$ ($a, b \in \mathbb{Z}$) is an irreducible element of \mathcal{O} , so is \bar{w} since conjugation is a ring automorphism. Hence unless $w \in \mathbb{Z}$, $p := N(w) = w\bar{w}$ must be an irreducible element of \mathbb{Z} , since otherwise p has two distinct factorizations.

- $2 = (1 + \sqrt{3})(-1 + \sqrt{3})$ and $3 = (3 + 2\sqrt{3})(-3 + 2\sqrt{3})$ show that ± 2 and ± 3 are not irreducible and each has two irreducible factors.
- If $p \equiv \pm 5 \pmod{12}$, $p = a^2 - 3b^2$ implies $p|(ab^{-1})^2 - 3$ (since $p \nmid b$ and therefore $b + p\mathbb{Z}$ has an inverse in $\mathbb{Z}/p\mathbb{Z}$) contradicting Claim 2, so p is an irreducible element of \mathcal{O} .
- If $p \equiv \pm 1 \pmod{12}$, by Claim 2 $p|n^2 - 3 = (n + \sqrt{3})(n - \sqrt{3})$ for some $n \in \mathbb{Z}$. If p is an irreducible element, p must divide at least one of $n + \sqrt{3}$ and $n - \sqrt{3}$, and therefore p must divide both of them by taking conjugation. However, this implies $p|(n + \sqrt{3}) - (n - \sqrt{3}) = 2\sqrt{3}$ which is absurd. Hence p is not irreducible in \mathcal{O} . Since $\mathcal{N}(p) = p^2$, \mathcal{N} is multiplicative, and $w \in \mathcal{O}$ is a unit if $\mathcal{N}(w) = \pm 1$, we conclude that p must have two irreducible factors.

The above three cases finish the proof. \square

Claim 4. For any integer $n \neq 0$, the factorization of n in \mathcal{O} can be written in the form

$$n = (-1)^m \prod_{i=1}^k w_i \bar{w}_i \cdot \prod_{j=1}^l p_j$$

where $w_i \bar{w}_i (\neq \pm 5 \pmod{12})$ and $p_j (\equiv \pm 5 \pmod{12})$ are the prime factors of n in \mathbb{Z} , and for $n = 3^\alpha r$ ($\alpha \in \mathbb{Z}_{\geq 0}, 3 \nmid r \in \mathbb{Z}$) $m = \alpha$ if $r \equiv 1 \pmod{3}$ and $m = \alpha + 1$ if $r \equiv 2 \pmod{3}$.

Proof. Consider a factorization of $n = p_1 p_2 \cdots p_k$ in \mathbb{Z} . By Claim 3, each p_i is irreducible in \mathcal{O} if $p_i \equiv \pm 5 \pmod{12}$ and factorize into two irreducible factors otherwise. In the latter case, the factorization of p_i is $\pm w\bar{w}$ for some $w = a + b\sqrt{3} \in \mathcal{O}$ ($a, b \in \mathbb{Z}$). Since $w\bar{w} = a^2 - 3b^2 \not\equiv -1 \pmod{3}$, and furthermore $w\bar{w} \neq 3$ (if so, letting $a = 3k$ yields $3k^2 - b^2 = 1$ which is false), $p_i = w\bar{w}$ if $p_i \equiv 1 \pmod{3}$ and $p_i = -w\bar{w}$ otherwise. Hence the factorization of n is in the claimed form, where m is the number of i such that $p_i \not\equiv 1 \pmod{3}$. \square

Claim 5. For an integer $n \neq 0$, there is $w \in \mathcal{O}$ such that $\mathcal{N}(w) = n$ if and only if the following two conditions hold:

- The quotient of n by the largest square dividing it does not have a prime divisor congruent to 5 or 7 modulo 12.
- For $n = 3^\alpha r$ ($\alpha \in \mathbb{Z}_{\geq 0}, 3 \nmid r \in \mathbb{Z}$), either α is even and $r \equiv 1 \pmod{3}$, or α is odd and $r \equiv 2 \pmod{3}$.

Proof. If $w = w_1 w_2 \cdots w_k p_1 p_2 \cdots p_l$ ($w_i \notin \mathbb{Z}, p_j \in \mathbb{Z}$) is a factorization of w ,

$$\mathcal{N}(w) = w\bar{w} = \prod_{i=1}^k w_i \bar{w}_i \cdot \prod_{j=1}^l p_j^2$$

Since factorization is unique up to associates in \mathcal{O} , in the notation of Claim 4 the following conditions are necessary and sufficient for existence of $w \in \mathcal{O}$ such that $\mathcal{N}(w) = n$.

- Among p_1, p_2, \dots, p_l , each number occurs an even number of times.
- m is even.

Using Claim 4, these two conditions translate to the claimed conditions. \square

Now we return to the problem statement. If $k = 0$, the condition does not hold because $3n^2$ cannot be a square. Now assume $k \neq 0$. We want to find all k such that there are infinitely many $(n, m) \in \mathbb{Z}_{>0} \times \mathbb{Z}$ such that $3n^2 + 3nk^2 + k^3 = m^2$, or equivalently,

$$\mathcal{N}(2m + (2n + k^2)\sqrt{3}) = (2m)^2 - 3(2n + k^2)^2 = k^3(4 - 3k) \quad (1)$$

If the following conditions

$$w = a + b\sqrt{3} \in \mathcal{O} \quad (a, b \in \mathbb{Z}), \quad \mathcal{N}(w) = k^3(4 - 3k), \quad 2|a \quad (2)$$

hold, then $a + b \equiv \mathcal{N}(w) \equiv k \pmod{2}$ shows that $b \equiv k^2 \pmod{2}$. Hence whenever (2) holds with $b > k^2$, there is a corresponding $(n, m) \in \mathbb{Z}_{>0} \times \mathbb{Z}$ satisfying (1). Furthermore, there are only finitely many w that satisfy (2) with $|b| \leq k^2$, and if w satisfies (2), so does \bar{w} . This shows that the problem condition is equivalent to that infinitely many w satisfy (2).

We claim that if w satisfies all but the last condition of (2), then $w(2 + \sqrt{3})$ satisfies (2). To prove this, since $\mathcal{N}(2 + \sqrt{3}) = 1$ it suffices to show that $2|2a + 3b$,

or equivalently that b is even. If b is odd, $\mathcal{N}(w) = a^2 - 3b^2 \equiv 2 \pmod{4}$ since a is also odd. This is impossible since $\mathcal{N}(w) = k^3(4 - 3k) \equiv k^4 \pmod{4}$.

Consequently, if w satisfies $\mathcal{N}(w) = k^3(4 - 3k)$, for every $n \in \mathbb{Z}_{\geq 0}$ at least one of $(2 + \sqrt{3})^n w$ and $(2 + \sqrt{3})^{n+1} w$ satisfies (2). Since $w \neq 0$ ($\because k \neq 0$), the elements $(2 + \sqrt{3})^n w$ ($n \in \mathbb{Z}_{\geq 0}$) are all different, so there are infinitely many elements satisfying (2). We proved that (2) is equivalent to the existence of w such that $\mathcal{N}(w) = k^3(4 - 3k)$. Applying Claim 5, noting that the factor k^2 is irrelevant in the first condition and that the factor $k^2(4 - 3k)$ is irrelevant in the second condition, finishes the proof.