Two New Characterizations of Perfect Squares

Tho Nguyen Xuan

September 3, 2020

Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
Vol. XX, XXXX, No. X, XX–XX

Two New Characterizations of Perfect Squares

Nguyen Xuan Tho

School of Applied Mathematics and Informatics, Hanoi University of Science and Technology
Hanoi, Vietnam
e-mail: tho.nguyenxuan1@hust.edu.vn

Abstract: This paper proves two new characterizations of perfect squares.
Keywords: Elementary number theory, perfect squares, quadratic reciprocity
2010 Mathematics Subject Classification: 11A15, 11E04.

1 Introduction

There are some nice characterizations of perfect squares. The most common characterization is:

Theorem 1.1. *Let a be a positive integer such that the number of divisor of a is odd. Then a is a perfect square.*

A simple argument for Theorem 1.1 is: Let $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ be the prime factorization of a. Then the number of divisors of a is $(\alpha_1 + 1)(\alpha_2 + 2) \ldots (\alpha_n + 1)$. Therefore $\alpha_1 + 1,\ \alpha_2 + 1, \ldots, \alpha_n + 1$ are odd numbers. Hence $\alpha_1,\ \alpha_2, \ldots, \alpha_n$ are even. Hence a is a perfect square.

Another common characterization for perfect squares is:

Theorem 1.2. *Let a be a positive integer such that a is a square (mod p) for all but finitely many prime numbers p. Then a is a perfect square.*

Theorem 1.2 is equivalent to Theorem 3 in [2, pp. 57-58]. Motivated by the study of prime numbers of the form $x^2 + ny^2$ in [1], we will prove the following theorems:

Theorem 1.3. *Let a be a positive integer such that $a + n^2$ can be written as a sum of two squares for all positive integers a. Then a is a perfect square.*

Theorem 1.4. *Let a be a positive integer such that $a + 2n^2$ can be written as $x^2 + 2y^2$, where $x,\ y \in \mathbb{Z}^+$, for all positive integers n. Then a is a perfect square.*

2 Proof of Theorem 1.3

For a prime p and an integer x, denote $v_p(x)$ the highest power of p dividing x.
Case 1: a is odd. We show that if $p|a$ then $v_p(a)$ is even. Let $a = p^{2n+1}b$ with $p \nmid b$. If $p \equiv 3 \pmod 4$ then from $a + p^{2n+2} = x^2 + y^2$, we have $p^{n+1}|x$ and $p^{n+1}|y$. Therefore $p^{2n+2}|a$, a contradiction. Thus $p \equiv 1 \pmod 4$. So if p is a prime divisor of a with $2 \nmid v_p(a)$ then $p \equiv 1 \pmod 4$. Therefore $a \equiv 1 \pmod 4$. Because a is not a square, from Theorem 1.2, there is an odd prime q such that $\left(\dfrac{a}{q}\right) = -1$. Hence $\left(\dfrac{q}{a}\right) = -1$. Let $a = 4k + 1$. Then $\gcd(3a - 4kq, 4a) = 1$. Therefore the set of prime numbers P such that

$$P \equiv 3a - 4kq \pmod{4a} \tag{1}$$

is infinite by the Dirichlet's theorem [2, Theorem 1, pp. 251]. From (1), we have

$$P \equiv 3 \pmod 4,$$

$$P \equiv q \pmod a.$$

Therefore

$$\left(\frac{P}{a}\right) = \left(\frac{q}{a}\right) = -1.$$

Thus

$$\left(\frac{a}{P}\right) = -1.$$

Therefore

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

Thus there exists $n \in \mathbb{N}$ such that $a + n^2 \equiv 0 \pmod P$. We can take n such that $0 \le n \le \dfrac{P-1}{2}$. If we take $P > 4a$, then $a + n^2 < P^2$. Because $a + n^2 = x^2 + y^2$ and $P \equiv 3 \pmod 4$, we have

$$x \equiv y \equiv 0 \pmod P.$$

Thus $P^2 | a + n^2$, which is not possible because $0 < a + n^2 < P^2$. Therefore $v_p(a)$ is even for all prime divisors p of a. Thus a is a perfect square.
Case 2: a is even. Let $a = 2^k b$ where $2 \nmid b$. If k is odd, let $k = 2m+1$. Then $2^{2m+1}b + 2^{2m+2}n^2 = x^2 + y^2$, where $x, y \in \mathbb{Z}$. Therefore $2^m|x$ and $2^m|y$. Thus

$$2b + 4n^2 = u^2 + v^2, \tag{2}$$

where $u, v \in \mathbb{Z}$. Let $n = 4$ in (2), then $2b + 16 = u^2 + v^2$. Considering mod 8 gives $2b \equiv 2 \pmod 8$, therefore $b \equiv 1 \pmod 4$. Let $n = 1$ in (2), then $2b + 4 = u_1^2 + v_1^2$, which is impossible since $2b + 4 \equiv 6 \pmod 8$. Therefore k is even. Let $k = 2m$. Then for every positive integer n, $2^{2m}b + (2^m n)^2 = 4^m(b + n^2)$ is a sum of two squares. Hence $b + n^2$ is a sum of two squares. Therefore from **Case** 1, b is a square. So $n = 2^{2m}b$ is also a square. The proof is complete.

3 Proof of Theorem 1.4

Let p be an odd prime. Then -2 is a square (mod p) if and only if $p \equiv 1,\ 3 \pmod 8$, see [2, Proposition 5.1.3, Theorem 1, pp. 53].

Case 1: a is odd. If p is a prime divisor of a, we will show that $v_p(a)$ is even. Assume that $p^{2m+1}||a$. Then $2p^{2m+2} + a = x^2 + 2y^2$. If $p \equiv -1$ (mod 8) or $p \equiv 5$ (mod 8) then $p^{m+1}|x$ and $p^{m+1}|y$. Thus $p^{2m+2}|a$, a contradiction. Therefore $p \equiv 1$ (mod 8) or $p \equiv 3$ (mod 8). Thus $a \equiv 1$ (mod 8) or $a \equiv 3$ (mod 8).

Since a is not a perfect square, from Theorem 1.2, there exist infinitely many prime numbers q such that

$$\left(\frac{a}{q}\right) = -1. \tag{3}$$

Let $r \in \{3,\ 7\}$. Let $a = 8k + \epsilon$, where $\epsilon \in \{1, 3\}$. Then $\epsilon a \equiv 1$ (mod 8). Let $\epsilon a = 8l + 1$. Then $\gcd(8a, r\epsilon a - 8lq) = 1$. Therefore by the Dirichlet's theorem [2, Theorem 1, pp. 251], there are infinitely many prime numbers P such that

$$P \equiv r\epsilon a - 8lq \pmod{8a}.$$

Hence

$$\begin{aligned} P &\equiv r\epsilon a \equiv r \pmod 8, \\ P &\equiv -8lq \equiv q \pmod a. \end{aligned} \tag{4}$$

From (3) and (4), we have

$$\left(\frac{P}{a}\right) = \left(\frac{q}{a}\right) = (-1)^{\frac{(q-1)(a-1)}{4}} \left(\frac{a}{q}\right) = (-1)^{1+\frac{(q-1)(a-1)}{4}}.$$

Therefore

$$\begin{aligned} \left(\frac{-2a}{P}\right) &= (-1)^{\frac{P-1}{2}} \left(\frac{2}{P}\right)\left(\frac{a}{P}\right) \\ &= (-1)^{\frac{P-1}{2}+\frac{P^2-1}{8}} \left(\frac{P}{a}\right) (-1)^{\frac{(P-1)(a-1)}{4}} \\ &= (-1)^{\frac{P-1}{2}+\frac{P^2-1}{8}+\frac{(P-1)(a-1)}{4}+1+\frac{(q-1)(a-1)}{4}}. \end{aligned}$$

We want to find r such that $\left(\frac{-2a}{P}\right) = 1$, which is equivalent to

$$\frac{P-1}{2} + \frac{P^2-1}{8} + \frac{(P-1)(a-1)}{4} + \frac{(q-1)(a-1)}{4} \equiv 1 \pmod 2. \tag{5}$$

If $a \equiv 1$ (mod 8), then (5) is equivalent to

$$\frac{P-1}{2} + \frac{P^2-1}{8} \equiv 1 \pmod 2.$$

Let $r = 5$. Then from (4), $P \equiv 5 \pmod 8$. Therefore

$$\frac{P-1}{2} + \frac{P^2-1}{8} \equiv 1 \pmod 2.$$

If $a \equiv 3 \pmod 8$, then

$$\begin{aligned} \text{RHS}(5) &\equiv \frac{P-1}{2} + \frac{P^2-1}{8} + \frac{P-1}{2} + \frac{q-1}{2} \pmod 2 \\ &\equiv \frac{P^2-1}{8} + \frac{q-1}{2} \pmod 2. \end{aligned}$$

If $q \equiv 1 \pmod 4$, let $r = 5$. Then from (4), $P \equiv 5 \pmod 8$. Therefore

$$\frac{P^2-1}{8} + \frac{q-1}{2} \equiv 1 \pmod 2.$$

If $q \equiv 3 \pmod 4$, let $r = 7$. Then from (4), $P \equiv 7 \pmod 8$. Therefore

$$\frac{P^2-1}{8} + \frac{q-1}{2} \equiv 1 \pmod 2.$$

Therefore we can always choose $r \in \{5, 7\}$ such that there are infinitely many prime numbers P satisfying

$$\begin{aligned} P &\equiv r \pmod 8, \\ P &\equiv q \pmod a, \\ 1 &= \left(\frac{-2a}{P}\right). \end{aligned} \tag{6}$$

We choose a prime number $P > 4a$ satisfying (6). Let n an integer in such that

$$n^2 + 2a \equiv 0 \pmod P.$$

If $2|n$, let $n = 2n_1$. Then $P|a + 2n_1^2$.
If $2 \nmid n$, let $n_1 = |P - n|$. Then $2|n_1$. Thus $P|2(a + 2(\frac{n_1}{2})^2)$. Hence $P|a + 2(\frac{n_1}{2})^2$.
Therefore we can always find $n \in \mathbb{Z}$ such that $P|a + 2n^2$. We can assume $0 \le n \le \frac{P-1}{2}$. Let $x, y \in \mathbb{Z}^+$ such that $a + 2n^2 = x^2 + 2y^2$. Then $P|x^2 + 2y^2$. Since $P \equiv r \equiv 5, 7 \pmod 8$, $\left(\frac{-2}{P}\right) = -1$. Therefore $P|x$ and $P|y$. Thus $P^2|x^2 + 2y^2 = a + 2n^2 < P^2$, a contradiction.
Case 2: a is even. Let $a = 2^k b$, where $2 \nmid b$, $k > 0$.
Case 2.1: $k = 1$. Then $2b + 2n^2 = a + 2n^2 = x^2 + 2y^2$. Therefore $2|x$. Let $x = 2x_1$. Then $b + n^2 = 2x_1^2 + y^2$. Let $n = 8$. Then $b + 64 = 2u^2 + v^2$. Therefore $2 \nmid v$. Thus $b \equiv 2u^2 + 1 \equiv 1, 3 \pmod 8$. Thus

$$\left(\frac{-2}{b}\right) = 1. \tag{7}$$

Let $\epsilon \equiv b \pmod 8$, where $\epsilon \in \{1, 3\}$. Then $\epsilon b \equiv 1 \pmod 8$. Let $\epsilon b = 8l + 1$. Then $\gcd(8b, 5\epsilon b + 16l) = 1$. Therefore by the Dirichlet's theorem [2, Theorem 1, pp. 251], there are infinitely many prime numbers P such that

$$P \equiv 5\epsilon b + 16l \pmod{8b}.$$

Then

$$
\begin{aligned}
P &\equiv 16l \equiv -2 \pmod{b}, \\
P &\equiv 5\epsilon b \equiv 5 \pmod{8}.
\end{aligned} \tag{8}
$$

Choose $P > 4b$ satisfying (8), then from (7) and (8), we have

$$
\begin{aligned}
\left(\frac{-b}{P}\right) &= (-1)^{\frac{P-1}{2}} \left(\frac{b}{P}\right) \\
&= (-1)^{\frac{P-1}{2}} \left(\frac{P}{b}\right) (-1)^{\frac{(P-1)(b-1)}{4}} \\
&= (-1)^{\frac{P-1}{2} + \frac{(b-1)(P-1)}{4}} \left(\frac{-2}{b}\right) \\
&= (-1)^{\frac{P-1}{2}\frac{b+1}{2}} \\
&= 1.
\end{aligned}
$$

Therefore, there exists an integer $n \in (0, \frac{P}{2})$ such that $P|b + n^2$. Let $b + n^2 = x^2 + 2y^2$. Then $P|x^2 + 2y^2$. Since P is a prime number $\equiv 5$ (mod 8), $P|x$ and $P|y$. Hence $P^2|b + n^2$, impossible because $0 < n < \frac{P-1}{2}$ and $b < \frac{P}{4}$.

Case 2.2: $k > 1$. If k is even, let $k = 2m$. Then $2^{2m}b + 2^{2m+1}n^2 = a + 2(2^m n)^2 = x^2 + 2y^2$. Therefore $2^m|x$ and $2^m|y$. Thus $b + 2n^2 = x_1^2 + 2y_1^2$ for $x_1, y_1 \in \mathbb{Z}^+$. Therefore from **Case** 1, b is a square.

If k is odd, let $k = 2m + 1$. Then $2^{2m+1}b + 2^{2m+1}n^2 = a + 2(2^m n)^2 = x^2 + 2y^2$. Therefore $b + n^2 = x_1^2 + 2y_1^2$, impossible as proved in **Case** 2.1. The proof is complete.

4 Open questions:

The following theorem is proved in [2, pp. 220-221] by the Eisenstein reciprocity law:

Theorem 4.1. *Let a be an integer. Let l be an odd prime number, $l \nmid a$. Suppose that*

$$x^l \equiv a \pmod{p}$$

has solutions (mod p) for all but finitely many prime numbers p. Show that a is a perfect l power.

Question 1: Does exist an elementary proof of Theorem 4.1?

Question 2: Let p be an odd prime. Let a be an odd positive integer such that $a + pn^2$ can be written as $x^2 + py^2$, where $x, y \in \mathbb{Z}$, for all positive integers n. Does it imply that a is a perfect square?

References

[1] D. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication,* 2nd edition, Wiley (2013).

[2] K. Ireland, M. Rosen, *A Classical Introduction to Number Theory,* 2nd edition, Springer (1998).