Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
2022, Volume 28, Number 1, Pages 75–80
DOI: 10.7546/nntdm.2022.28.1.75-80

Two theorems on square numbers

Nguyen Xuan Tho

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

Received: 2 February 2021 **Revised:** 16 November 2021
Accepted: 11 February 2022 **Online First:** 14 February 2022

Abstract: We show that if a is a positive integer such that for each positive integer n, $a + n^2$ can be expressed $x^2 + y^2$, where $x, y \in \mathbb{Z}$, then a is a square number. A similar theorem also holds if $a + n^2$ and $x^2 + y^2$ are replaced by $a + 2n^2$ and $x^2 + 2y^2$, respectively.
Keywords: Elementary number theory, Square numbers, Quadratic reciprocity.
2020 Mathematics Subject Classification: 11A15, 11E04.

1 Introduction

An integer a of the form n^2, where $n \in \mathbb{Z}$, is called a square number. A simple characterization of square numbers is the following.

Theorem 1.1. *Let a be a positive integer. Let $d(a)$ be the number of positive divisors of a. Then a is a square number if and only if $d(n)$ is odd.*

Theorem 1.1 can be proved by looking at the prime factorization of a. Let $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ be the prime factorization of a. Then $d(a) = (\alpha_1 + 1)(\alpha_2 + 2) \cdots (\alpha_n + 1)$. Of course, $d(a)$ is odd if and only if $\alpha_1 + 1,\ \alpha_2 + 1, \dots, \alpha_n + 1$ are odd, which is equivalent to $\alpha_1,\ \alpha_2, \dots, \alpha_n$ are even. So, $d(a)$ is odd if and only if a is a square number.

Another nice theorem for square numbers, a special case of the Grunwald–Wang theorem [2], proved in [1, Theorem 3, pp. 57–58], states that

Theorem 1.2. *Let a be a positive integer such that a is a square $\pmod{p}$ for all but finitely many prime numbers p. Then a is a square number.*

In this paper, we will prove the following theorems.

Theorem 1.3. *Let a be a positive integer such that for each positive integer n, there exist integers x, y such that $a + n^2 = x^2 + y^2$. Then a is a square number.*

Theorem 1.4. *Let a be a positive integer such that for each positive integer n, there exist integers x, y such that $a + 2n^2 = x^2 + 2y^2$. Then a is a square number.*

For the rest of this paper, $v_p(x)$ denotes the highest power of a prime number p dividing x, and (x/b) denotes the Jacobi symbol for odd integers b. See Rosen [1, Chapter 5] for the basic properties of Jacobi symbols.

2 Proof of Theorem 1.3

Case 1. a is odd. We will show that if p is a prime divisor of a, then $v_p(a)$ is even. Assume by contrary that $v_p(a)$ is odd. Then $a = p^{2r+1}b$, where $r \in \mathbb{N}$, $b \in \mathbb{Z}^+$ with $p \nmid b$.

If $p \equiv 3 \pmod 4$, let $x, y \in \mathbb{Z}$ such that $a + p^{2r+2} = x^2 + y^2$. Since $(-1/p) = -1$ and $v_2(a) = 2r + 1 < 2r + 2$, we have $p^{r+1}|x$ and $p^{r+1}|y$. Therefore, $p^{2r+2}|x^2 + y^2 - p^{2r+2} = a$, impossible. Therefore, $p \equiv 1 \pmod 4$. So if p is a prime divisor of a with $2 \nmid v_p(a)$, then $p \equiv 1 \pmod 4$. Therefore, $a \equiv 1 \pmod 4$.

Since a is not a square number, then from Theorem 1.2, there exists an odd prime q such that $(a/q) = -1$. Hence,

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

Let $a = 4a_1 + 1$, where $a_1 \in \mathbb{N}$. Since $\gcd(a, a_1) = (a, q) = 1$ and $2 \nmid a$, we have $\gcd(3a - 4a_1 q,\, 4a) = 1$. Therefore, the set of prime numbers P such that

$$P \equiv 3a - 4a_1 q \pmod{4a} \tag{2}$$

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

$$\begin{cases} P & \equiv 3 \pmod 4, \\ P & \equiv q \pmod a. \end{cases} \tag{3}$$

From (1) and (3) we have

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

Hence,

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

Therefore,

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

Thus, there exists $s \in \mathbb{N}$ such that $a + s^2 \equiv 0 \pmod P$. We can assume further that $0 \le s \le (P-1)/2$. If we take $P > 4a$, then $a + s^2 < P^2$. Let $z, w \in \mathbb{Z}$ such that $a + s^2 = z^2 + w^2$.

From (3) we have $P \equiv 3 \pmod 4$. Since $P|a+s^2 = z^2+w^2$, we have $P|z$ and $P|w$. Thus, $P^2|z^2+w^2 = a+s^2$, impossible since $0 < a+s^2 < P^2$. Therefore, $2|v_p(a)$ for all prime divisors p of a. Thus, a is a square number.

Case 2. a is even. Let $a = 2^k b$, where $k, b \in \mathbb{Z}^+$ and $2 \nmid b$.

- k is odd. Let $k = 2m+1$, where $m \in \mathbb{N}$. For each positive integer n, there exist $x, y \in \mathbb{Z}$ such that $a + (2^{m+1}n)^2 = x^2 + y^2$. Hence, $2^{2m+1}b + 2^{2m+2}n^2 = x^2+y^2$. Therefore, $2^m|x$ and $2^m|y$. Let $u = x/2^m$ and $y = y/2^m$. Then $u, v \in \mathbb{Z}$ and

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

  In (4), let $n = 4$. Then $2b + 16 = u^2+v^2$. Since $2 \nmid b$, we have $2 \nmid u$ and $2 \nmid v$. Hence,

$$2b \equiv u^2 + v^2 \equiv 2 \pmod 8.$$

  Therefore, $b \equiv 1 \pmod 4$. In (4), let $n = 1$, then $2b + 4 = u_1^2 + v_1^2$, where $u_1, v_1 \in \mathbb{Z}$, impossible since $2b+4 \equiv 6 \pmod 8$ and $u_1^2 + v_1^2 \equiv 2 \pmod 8$.

- k is even. Let $k = 2m$, where $m \in \mathbb{Z}^+$. Then for each positive integer n, there exist integers x, y such that $2^{2m}b + (2^m n)^2 = x^2+y^2$. Hence, $4^m|x^2+y^2$. Therefore, $2^m|x$ and $2^m|y$. Let $u = x/2^m$ and $v = y/2^m$. Then $u, v \in \mathbb{Z}$ and

$$b + n^2 = u^2 + v^2.$$

From Case 1, b is a square number. Hence, $n = 2^{2m}b$ is a square number.
The proof is complete. □

3 Proof of Theorem 1.4

Case 1. a is odd. Let p be a prime divisor of a. We will show that $v_p(a)$ is even. Assume that $v_p(a)$ is odd. Then $v_p(a) = 2m+1$, where $m \in \mathbb{N}$. Then there exist $x, y \in \mathbb{Z}$ such that

$$2p^{2m+2} + a = x^2 + 2y^2. \tag{5}$$

- $p \equiv -1, 5 \pmod 8$. Then $(-2/p) = -1$, see [1, Proposition 5.1.3, p. 53] for a proof. From (5), we have $p^{m+1}|x$ and $p^{m+1}|y$. Thus $p^{2m+2}|x^2+y^2-2p^{2m+2} = a$, impossible.

- $p \equiv 1, 3 \pmod 8$. This is true for all prime divisors of a. Hence, $a \equiv 1, 3 \pmod 8$. Since a is not a square number, from Theorem 1.2, there exist infinitely many odd prime numbers q such that

$$\left(\frac{a}{q}\right) = -1. \tag{6}$$

Let $r \in \{3,\, 7\}$.

Let $a = 8k + \epsilon$, where $k \in \mathbb{N}$ and $\epsilon \in \{1,3\}$. Then $\epsilon a \equiv 1 \pmod 8$. Let $\epsilon a = 8l + 1$, where $l \in \mathbb{N}$. Since $\gcd(a,l) = \gcd(a,q) = 1$ and $2 \nmid aq$, we have $\gcd(8a, r\epsilon a - 8lq) = 1$. Therefore, by Dirichlet's Theorem [1, Theorem 1, pp. 251], there exist infinitely many prime numbers P such that

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

Hence,

$$\begin{cases} P & \equiv r\epsilon a \equiv r \pmod 8, \\ P & \equiv -8lq \equiv q \pmod a. \end{cases} \tag{7}$$

From (6) and (7), we have

$$\left(\frac{P}{a}\right) = \left(\frac{q}{a}\right) = (-1)^{(q-1)(a-1)/4}\left(\frac{a}{q}\right) = (-1)^{1+(q-1)(a-1)/4}. \tag{8}$$

From (8) we have

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

We want to find r such that $(-2a/P) = 1$, which is equivalent to

$$\frac{P-1}{2} + \frac{P^2-1}{8} + \frac{(P-1)(a-1)}{4} + \frac{(q-1)(a-1)}{4} \equiv 1 \pmod 2. \tag{9}$$

If $a \equiv 1 \pmod 8$, then (9) is equivalent to

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

Let $r = 5$. Then from (7), $P \equiv 5 \pmod 8$. Therefore,

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

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

$$\begin{aligned}\text{LHS(9)} &\equiv \frac{P-1}{2} + \frac{P^2-1}{8} + \frac{P-1}{2} + \frac{q-1}{2} \pmod 2 \\ &\equiv \frac{P^2-1}{8} + \frac{q-1}{2} \pmod 2.\end{aligned}$$

If $q \equiv 1 \pmod 4$, let $r = 5$. Then from (7), $P \equiv 5 \pmod 8$. 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 (7), $P \equiv 7 \pmod 8$. 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 exist infinitely many prime numbers P satisfying

$$\begin{cases} P &\equiv r \pmod{8}, \\ P &\equiv q \pmod{a}, \\ 1 &= \left(\dfrac{-2a}{P}\right). \end{cases} \tag{10}$$

Let P be a prime number satisfying (10) and $P > 4a$. Let x be an integer such that

$$x^2 + 2a \equiv 0 \pmod{P}.$$

If $2|x$, let $s = x/2$. Then $P|a + 2s^2$.
If $2 \nmid x$, let $x_1 = |P - x|$. Then $2|x_1$. Let $s = x_1/2$. Since $P|2(a + 2(x_1/2)^2)$, we have $P|a + 2s^2$.

Therefore, there exists $s \in \mathbb{Z}$ such that $P|a + 2s^2$. We can assume $0 \le s \le (P-1)/2$. Let $z, w \in \mathbb{Z}$ such that $a + 2s^2 = z^2 + 2w^2$. Then $P|z^2 + 2w^2$. Since $P \equiv r \equiv 5, 7 \pmod{8}$, we have $(-2/P) = -1$. Therefore, $P|z$ and $P|w$. Thus, $P^2|z^2 + 2w^2 = a + 2s^2$, impossible since $0 < a + s^2 < P^2$.

Case 2. a is even. Let $a = 2^k b$, where $b, k \in \mathbb{Z}^+$ and $2 \nmid b$.

Case 2.1. $k = 1$. Then for each positive integer n, there exist $x, y \in \mathbb{Z}$ such that $2b + 2n^2 = x^2 + 2y^2$. Therefore, $2|x$. Let $x_1 = x/2$. Then

$$b + n^2 = 2x_1^2 + y^2. \tag{11}$$

In (11), let $n = 8$. Then there exist $u, v \in \mathbb{Z}$ such that $b + 64 = 2u^2 + v^2$. Therefore, $2 \nmid v$. Thus

$$b \equiv 2u^2 + 1 \equiv 1, 3 \pmod{8}.$$

It follows from [1, Proposition 5.2, page 57] that

$$\left(\frac{-2}{b}\right) = 1. \tag{12}$$

Let $\epsilon_1 \equiv b \pmod{8}$, where $\epsilon_1 \in \{1, 3\}$. Then $\epsilon_1 b \equiv 1 \pmod{8}$. Let $\epsilon b = 8l_1 + 1$, where $l_1 \in \mathbb{Z}$. Since $\gcd(l_1, b) = 1$ and $2 \nmid bl_1$, we have $\gcd(8b, 5\epsilon_1 b + 16l_1) = 1$. Therefore, by Dirichlet's Theorem [1, Theorem 1, pp. 251], there are infinitely many prime numbers P such that

$$P \equiv 5\epsilon_1 b + 16l_1 \pmod{8b}.$$

Thus,

$$\begin{cases} P &\equiv 16l_1 \equiv -2 \pmod{b}, \\ P &\equiv 5\epsilon_1 b \equiv 5 \pmod{8}. \end{cases} \tag{13}$$

Let P be a prime satisfying (13) and $P > 4b$. Then from (12) and (13), we have

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

Therefore, there exists $s \in \mathbb{N}$ such that $s < P/2$ and $P|b+s^2$. From (11), there exist $z,\ w \in \mathbb{Z}$ such that $b+s^2 = z^2+2w^2$. Since $P \equiv 5 \pmod 8$, we have $(-2/P) = -1$. Therefore, $P|z$ and $P|w$. Hence, $P^2|b+s^2$, impossible because $0 < s < P/2$ and $b < P/4$.

Case 2.2. $k > 1$.

- k is even. Let $k = 2m_1$, where $m_1 \in \mathbb{Z}^+$. Then for each positive integer n, there exist $x, y \in \mathbb{Z}$ such that $2^{2m}b + 2^{2m+1}n^2 = a + 2(2^m n)^2 = x^2 + 2y^2$. Therefore, $2^m|x$ and $2^m|y$. Thus, $b+2n^2 = u^2+2v^2$, where $u = x/2^m \in \mathbb{Z}$ and $v = y/2^m \in \mathbb{Z}$. Therefore, from Case 1, b is a square number. Hence $a = 2^{2m_1}b$ is a square number.
- k is odd. Let $k = 2m_1 + 1$, where $m_1 \in \mathbb{N}$. Then for each positive integer n, there exist $x, y \in \mathbb{Z}$ such that $2^{2m+1}b + 2^{2m+1}n^2 = a + 2(2^m n)^2 = x^2 + 2y^2$. Similar to the case k is even, we will have $b + n^2 = u^2 + 2v^2$, where $u = x/2^m$ và $v = y/2^m$, which is impossible as proved in Case 2.1.

The proof is complete. □

4 An open question

The following case of the Grunwald–Wang theorem [2] is also proved in [1, pp. 220–221] via 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 $\pmod p$ for all but finitely many prime numbers p. Then a is a perfect l power.

Question. *Does there exist an elementary proof of Theorem 4.1?*

References

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

[2] Wang, S. (1950). On Grunwald's theorem, *Annals of Mathematics, Second Series*, 51(2), 471—484.