Four Squares Theorem For Rational Numbers

Introduction. The following are well known results:

(1) Every positive integer can be written as the sum of four squares (Lagrange's four-square theorem).
(2) A positive integer n can be written as the sum of three squares if and only if n is not of the form $n = 4^k(8m+7)$ for nonnegative integers k and m (Legendre's three-square theorem).
(3) A positive integer n can be written as a sum of two squares if and only if its prime decomposition contains no factor p^k, where $p \equiv 3 \pmod 4$ and k is odd (Fermat's two-square theorem).

The problem addressed here is whether those results can be extended to rational numbers.

Four-square theorem for rational numbers. Every positive rational number can be written as the sum of the squares of four rational numbers.

Proof. Let $r = \frac{a}{b}$, with $a, b \in \mathbb{Z}^+$ be a positive rational number. By Lagrange's four-square theorem ab can be written as a sum of four (integer) squares $ab = x_1^2 + x_2^2 + x_3^2 + x_4^2$, hence

$$r = \frac{a}{b} = \frac{ab}{b^2} = \left(\frac{x_1}{b}\right)^2 + \left(\frac{x_2}{b}\right)^2 + \left(\frac{x_3}{b}\right)^2 + \left(\frac{x_4}{b}\right)^2,$$

hence, r can be written as the sum of four squares of rational numbers. □

Three-square theorem for rational numbers. A positive rational number can be written as the sum of the squares of three rational numbers if and only if ab is not of the form $n = 4^k(8m + 7)$ for nonnegative integers k and m.

Proof. Let $r = \frac{a}{b}$, with $a, b \in \mathbb{Z}^+$ be a positive rational number. By Legendre's three-square theorem ab can be written as a sum of three (integer) squares if an only if ab is not of the form $ab = 4^k(8m + 7)$ for nonnegative integers k and m. Hence, if ab is not of that form we have $ab = x_1^2 + x_2^2 + x_3^2$ and

$$r = \frac{a}{b} = \frac{ab}{b^2} = \left(\frac{x_1}{b}\right)^2 + \left(\frac{x_2}{b}\right)^2 + \left(\frac{x_3}{b}\right)^2.$$

That proves the "if" part.

For the "only if" part, assume that r can be written as the sum of three squares:

$$r = \frac{a}{b} = \frac{ab}{b^2} = \left(\frac{x_1}{y_1}\right)^2 + \left(\frac{x_2}{y_2}\right)^2 + \left(\frac{x_3}{y_3}\right)^2.$$

Clearing denominators we get

$$aby_1^2y_2^2y_3^2 = (bx_1y_2y_3)^2 + (by_1x_2y_3)^2 + (by_1y_2x_3)^2,$$

hence $aby_1^2y_2^2y_3^2 = 4^k(8m+7)$ for nonnegative integers k and m. Each factor on the left can be written as a power of 2 times an odd number: $a = 2^\alpha a'$, $b = 2^\beta b'$, $y_i = 2^{k_i}y_i'$ $(i = 1,2,3)$, where a', b', y_1', y_2', y_3' are all odd. The number of factors 2 on the left and right hand sides must be the same, hence $\alpha + \beta + 2k_1 + 2k_2 + 2k_3 = 2k$, and after dividing by 4^k we get $a'b'y_1'^2y_2'^2y_3'^2 = 8m+7$, or equivalently, $a'b'y_1'^2y_2'^2y_3'^2 \equiv -1 \pmod 8$. Since the square of an odd number is always 1 modulo 8 we have that $a'b' \equiv -1 \pmod 8$, and hence $a'b' = 8m'+7$ for some nonnegative m', which implies $ab = 2^{\alpha+\beta}(8m'+7)$, and this completes the proof. ☐

Two-square theorem for rational numbers. A positive rational number can be written as the sum of two rational numbers if and only if the prime decomposition of ab contains no factor p^k, where $p \equiv 3 \pmod 4$ and k is odd.

Proof. Let $r = \frac{a}{b}$, with $a, b \in \mathbb{Z}^+$ be a positive rational number. By the two-squares theorem, ab is the sum of two (integer) squares if and only if the prime decomposition of ab contains no factor p^k, where $p \equiv 3 \pmod 4$ and k is odd. If ab verifies that condition then we have $ab = x_1^2 + x_2^2$ for some integers x_1, x_2, hence

$$r = \frac{a}{b} = \frac{ab}{b^2} = \left(\frac{x_1}{b}\right)^2 + \left(\frac{x_2}{b}\right)^2.$$

That proves the "if" part.

For the "only if" part, assume that r can be written as the sum of two squares:

$$r = \frac{a}{b} = \frac{ab}{b^2} = \left(\frac{x_1}{y_1}\right)^2 + \left(\frac{x_2}{y_2}\right)^2.$$

Clearing denominators we get

$$aby_1^2y_2^2 = (bx_1y_2)^2 + (by_1x_2)^2\,,$$

hence $aby_1^2y_2^2$ is the sum of two squares and must verify that its prime decomposition contains no factor p^k, where $p \equiv 3 \pmod 4$ and k is odd. Since all prime factors of $y_1^2y_2^2$ have even exponent, any odd exponent must occur in the prime factors of ab. Hence, the prime decomposition of ab cannot contain a factor p^k, where $p \equiv 3 \pmod 4$ and k is odd. ☐

For completion we add:

One-square theorem for rational numbers. Let $r = \frac{a}{b}$, with $a, b \in \mathbb{Z}^+$ be a positive rational number. Then, r is the square of a rational number if and only if ab is a square.

Proof. Obvious and left as an exercise.

Corollary. A positive rational number $r = \frac{a}{b}$ $(a, b \in \mathbb{Z}^+)$ can be written as the sum of the squares of n rational numbers if and only if ab can be written as the sum of n (integer) squares.

Miguel A. Lerma - 8/1/2024