Sums of squares

We finally determine which integers can be written as the sum of two squares of integers!

Which integers can be represented as the sum of two perfect squares?

Select All Correct Answers:

(a) 1 ✓
(b) 2 ✓
(c) 3
(d) 4 ✓
(e) 5 ✓
(f) 6
(g) 7
(h) 8 ✓
(i) 9 ✓
(j) 10 ✓
(k) 11
(l) 12
(m) 13 ✓
(n) 14
(o) 15

Select All Correct Answers:

(a) 16 ✓
(b) 17 ✓
(c) 18 ✓

Learning outcomes:
Author(s):

(d) 19

(e) 20 ✓

(f) 21

(g) 22

(h) 23

(i) 24

(j) 25 ✓

(k) 26 ✓

(l) 27

(m) 28

(n) 29 ✓

(o) 30

Note that this sum is not necessarily unique: $25 = 5^2 + 0^2 = 4^3 + 3^2$. Try to conjecture whether or not 374^{695} can be written as the sum of two squares. We found back in the congruences chapter that n cannot be written written as the sum of two squares if $n \equiv 3 \pmod 4$. In order to establish which integers are expressible as the sum of two squares, we will find necessary and sufficient conditions for the Diophantine equation $x^2 + y^2 = n$ to have solutions.

Theorem 1. *Let $n_1, n_2 \in \mathbb{Z}$ with $n_1, n_2 > 0$. If n_1 and n_2 are expressible as the sum of two squares of integers, then $n_1 n_2$ is expressible as the sum of two squares of integers.*

Proof Participation assignment ■

Example 1. *Since* $13 = \boxed{3}^2 + \boxed{2}^2$ *and* $17 = \boxed{4}^2 + \boxed{1}^2$ *are each expressible as the sum of two squares,* $13 * 17 = 221 = \boxed{14}^2 + \boxed{-5}^2$.

We will finally prove that every prime that congruent to $1 \pmod 4$ is expressible as the sum of two squares.

Theorem 2 (Primes as sums of squares)**.** *If p is a prime such that $p \equiv 1 \pmod 4$, then there exists $x, y \in \mathbb{Z}$ such that $x^2 + y^2 = kp$ for some $k \in \mathbb{Z}$ and $0 < k < p$.*

Proof Since $p \equiv 1 \pmod 4$, we have that $\left(\dfrac{-1}{p}\right) = 1$. Thus, there exists $x \in \mathbb{Z}$ with $0 < x \leq \dfrac{p-1}{2}$ such that $x^2 \equiv -1 \pmod p$. Then, $p \mid x^2 + 1$, and we have that $x^2 + 1 = kp$ for some $k \in \mathbb{Z}$. Thus, we found x and $y = 1$. Since $x^2 + 1$ and p are positive, so is k. Also,

$$kp = x^2 + y^2 < \left(\frac{p}{2}\right)^2 + 1 < p^2$$

implies $k < p$. ■

The next theorem will finally prove that primes $p \equiv 1 \pmod 4$ and $p = 2$ can be written as the sum of two square integers.

Theorem 3. *If p is a prime number such that $p \not\equiv 3 \pmod 4$, then p is expressible as the sum of two squares of integers.*

Proof When $p = 2 = 1^2 + 1^2$, we are done.

Assume that $p \equiv 1 \pmod 4$. Let m be the least integer such that there exists $x, y \in \mathbb{Z}$ with $x^2 + y^2 = mp$ and $0 < m < p$ as in the previous theorem. We show that $m = 1$. Assume, by way of contradiction, that $m > 1$. Let $a, b \in \mathbb{Z}$ such that

$$a \equiv x \pmod m, \quad \frac{-m}{2} < a \leq \frac{m}{2}$$

and

$$b \equiv y \pmod m, \quad \frac{-m}{2} < b \leq \frac{m}{2}.$$

Then

$$a^2 + b^2 \equiv x^2 + y^2 = mp \equiv 0 \pmod m,$$

and so there exists $k \in \mathbb{Z}$ with $k > 0$ such that $a^2 + b^2 = km$. (Why?)

Now,

$$(a^2 + b^2)(x^2 + y^2) = (km)(mp) = km^2p.$$

By the participation assignment, $(a^2 + b^2)(x^2 + y^2) = (ax + by)^2 + (ay - bx)^2$, so $(ax + by)^2 + (ay - bx)^2 = km^2p$. Since $a \equiv x \pmod m$ and $b \equiv y \pmod m$,

$$ax + by \equiv x^2 + y^2 \equiv 0 \pmod m$$

and

$$ay - bx \equiv xy - yx \equiv 0 \pmod m$$

so $\dfrac{ax + by}{m}, \dfrac{ay - bx}{m} \in \mathbb{Z}$ and

$$\left(\frac{ax + by}{m}\right)^2 + \left(\frac{ay - bx}{m}\right)^2 = \frac{km^2p}{m^2} = kp.$$

Now, $\dfrac{-m}{2} < a \leq \dfrac{m}{2}$ and $\dfrac{-m}{2} < b \leq \dfrac{m}{2}$ imply that $a^2 \leq \dfrac{m^2}{4}$ and $b^2 \leq \dfrac{m^2}{4}$. Thus, $km = a^2 + b^2 \leq \dfrac{m^2}{2}$. Thus, $k \leq \dfrac{m}{2} < m$, but this contradicts that m is the smallest such integer.

Thus, $m = 1$. ■

We finish with a characterization of which integers are expressible as the sum of two square integers and some examples.

Theorem 4. *Let $n \in \mathbb{Z}$ with $n > 0$. Then n is expressible as the sum of two squares if and only if every prime factor congruent to 3 modulo 4 occurs to an even power in the prime factorization of n.*

Proof ($\Rightarrow$) Assume that p is an odd prime number and that $p^{2i+1}, i \in \mathbb{Z}$ occurs in the prime factorization of n. We will show that $p \equiv 1 \pmod 4$. Since n is expressible as the sum of two squares of integers, there exist $x, y \in \mathbb{Z}$ such that $n = x^2 + y^2$. Let $(x, y) = d, a = \dfrac{x}{d}, b = \dfrac{y}{d}$ and $m = \dfrac{n}{d^2}$. Then $(a, b) = 1$ and $a^2 + b^2 = m$. Let $p^j, j \in \mathbb{Z}$ be the largest power of p dividing d. Then $p^{(2i-1)-2j} \mid m$; since $(2i + 1) - 2j) \geq 1$, we have $p \mid m$. Now, $p \nmid a$ since $(a, b) = 1$. Thus, there exists $z \in \mathbb{Z}$ such that $az \equiv b \pmod p$. Then $m = a^2 + b^2 \equiv a^2 + (az)^2 \equiv a^2(1 + z^2) \pmod p$.

Since $p \mid m$, we have

$$a^2(1 + z^2) \equiv 0 \pmod p$$

or $p \mid a^2(1+z^2)$ or $z \equiv -1 \pmod p$. Thus, -1 is a quadratic residue modulo p, so $p \equiv 1 \pmod 4$. By contrapositive, any prime factor congruent to 3 modulo 4 occurs to an even power in the prime factorization of n as desired.

($\Leftarrow$) Assume that every prime factor of n congruent to 3 modulo 4 occurs to an even power in the prime factorization of n. Then n can be written as $n = m^2 p_1 p_2 \ldots p_r$ where $m \in \mathbb{Z}$ and $p_1, p_2, \ldots, p_r$ are distinct prime numbers equal to 2 or equivalent to 1 modulo 4. Now, $m^2 = m^2 + 0^2$, so is expressible as the sum of two squares, and each p_1 is also expressible as the sum of two squares by the theorem labeled Primes as Sums of Squares. Thus, by the first theorem of the day, n is expressible as the sum of two squares. ■

Example 2. *Determine whether 374^{695} is expressible as the sum of two squares. The prime factorization of 374 is $2 * 11 * 17$. So $374^{695} = 2^{695} 11^{695} 17^{695}$ Thus, 374^{695}*

Multiple Choice:

(a) *is*

(b) *is not* ✓

expressible as the sum of two squares.

Example 3. *Express* 4410 *as the sum of two squares by splitting into factors that can be written as the sum of two squares.*

The prime factorization of 4410 *is* $2 * 3^2 * 5 * 7^2$. *We group this into* $4410 = (\boxed{2} * \boxed{7}^2)(\boxed{3}^2 * \boxed{5}) = \boxed{98} * \boxed{45}$. *By inspection, the larger of these factors is* $\boxed{98} = \boxed{7}^2 + \boxed{7}^2$ *and the smaller is* $\boxed{45} = \boxed{6}^2 + \boxed{3}^2$.

The method from the participation assignment gives $4410 = \boxed{63}^2 + \boxed{21}^2$.