

0.1 Using Quadratic Residues

1 The positive integers a and b are such that the numbers $15a + 16b$ and $16a - 15b$ are both squares of positive integers. What is the least possible value that can be taken on by the smaller of these two squares?

First Solution. Suppose $15a + 16b = x^2$ and $16a - 15b = y^2$, where x, y are positive integers. Solving this system of equations, we have

$$a = \frac{15x^2 + 16y^2}{15^2 + 16^2} = \frac{15x^2 + 16y^2}{13 \cdot 37}, \quad b = \frac{16x^2 - 15y^2}{15^2 + 16^2} = \frac{16x^2 - 15y^2}{13 \cdot 37}.$$

which implies that

$$15x^2 + 16y^2 \equiv 0 \pmod{13 \cdot 37} \quad \text{and} \quad 16x^2 - 15y^2 \equiv 0 \pmod{13 \cdot 37}$$

This is equivalent to

$$\begin{cases} 15x^2 + 16y^2 \equiv 0 \pmod{13} \\ 16x^2 - 15y^2 \equiv 0 \pmod{13} \end{cases} \quad \text{and} \quad \begin{cases} 15x^2 + 16y^2 \equiv 0 \pmod{37} \\ 16x^2 - 15y^2 \equiv 0 \pmod{37} \end{cases}$$

Claim 0.1.1. $x, y \equiv 0 \pmod{13 \cdot 37}$

Once we have this claim, we see that $481 \mid x$ and $481 \mid y$ (Note that $481 = 13 \cdot 37$). Let us try to see if there is any solution for a, b if $x = y = 481$. It suffices to plug in the formula for x, y above. In this case, we are lucky that $(x, y) = (481, 481)$ yields a solution $(a, b) = (14911, 481)$. Therefore the answer for this question is $\boxed{481^2}$.

It now suffices to show the claim. We will provide several methods:

Method 1. We first use Brahmagupta-Fibonacci Identity:

$$(A^2 + B^2)(X^2 + Y^2) = (AX + BY)^2 + (AY - BX)^2.$$

From the identity we obtain:

$$(15^2 + 16^2)(a^2 + b^2) = (15a + 16b)^2 + (16a - 15b)^2 = x^4 + y^4.$$

Since $15^2 + 16^2 = 13 \cdot 37$, we have $13 \cdot 37 \mid x^4 + y^4$. It then suffices to apply the following proposition for $p = 13$ and $p = 37$ to conclude that $x, y \equiv 0 \pmod{13}$ and $x, y \equiv 0 \pmod{37}$. Since 13 and 37 are relatively prime, we conclude that $x, y \equiv 0 \pmod{13 \cdot 37}$.

Proposition 0.1.1. Let p be a prime with $p \equiv 5 \pmod{8}$. Suppose that $x^4 + y^4$ is divisible by p for some integers x and y . Then both x, y are divisible by p .

Proof. Assume for contrary that at least one of them are not divisible by p . Since p divides $x^4 + y^4$, we see that none of them are divisible by p . Fermat's Little Theorem yields that $x^{p-1} \equiv y^{p-1} \equiv 1 \pmod{p}$. Since $p \equiv 5 \pmod{8}$, we have that $\frac{p-1}{4}$ is odd, so $(-1)^{\frac{p-1}{4}} = -1$. Since p divides $x^4 + y^4$, we obtain

$$x^4 \equiv -y^4 \pmod{p}.$$

Raise both sides of the congruence to the power $\frac{p-1}{4}$ to obtain

$$x^{p-1} \equiv (-1)^{\frac{p-1}{4}} y^{p-1} \equiv -y^{p-1} \pmod{p}.$$

or

$$1 \equiv x^{p-1} \equiv -y^{p-1} \equiv -1 \pmod{p}.$$

which is a contradiction since p is an odd prime. Therefore both x and y are divisible by p . \square

Method 2. This method is similar to Method 1, except that we use a different way to conclude

$$13 \cdot 37 \mid x^4 + y^4$$

We first work on the field $\mathbb{Z}/13\mathbb{Z}$ (This is a field since 13 is a prime). Then the system of congruence $15x^2 + 16y^2 \equiv 0 \pmod{13}$ and $16x^2 - 15y^2 \equiv 0 \pmod{13}$ becomes

$$\begin{bmatrix} x^2 & y^2 \\ -y^2 & x^2 \end{bmatrix} \begin{bmatrix} 15 \\ 16 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

Since the vector $\begin{bmatrix} 15 \\ 16 \end{bmatrix}$ is nonzero in $\mathbb{Z}/13\mathbb{Z}$, this implies that $\begin{bmatrix} x^2 & y^2 \\ -y^2 & x^2 \end{bmatrix}$ has zero determinant so that $x^4 + y^4 = 0$ in $\mathbb{Z}/13\mathbb{Z}$, or equivalently $x^4 + y^4 \equiv 0 \pmod{13}$.

Similarly, we can work on the field $\mathbb{Z}/37\mathbb{Z}$, and repeat the argument above. We can then obtain $x^4 + y^4 \equiv 0 \pmod{37}$. We can then proceed as in Method 1, using Fermat's Little Theorem.

Method 3. Another method is to use the quadratic reciprocity law. We first recall some of the results that are going to be used here:

Proposition 0.1.2. *Let p, q be odd primes. Then we have the following properties of Legendre symbols:*

1.

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$$

for integers a, b .

2.

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

3.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

4.

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

We first work with modulo 13. We have the congruence $15x^2 + 16y^2 \equiv 0 \pmod{13}$ or equivalently,

$$(4y)^2 \equiv -15x^2 \pmod{13}$$

If x is not divisible by 13, there exists an integer x' such that $x'x \equiv 1 \pmod{13}$. Multiplying x'^2 to both sides of the congruence above, we get

$$(4yx')^2 \equiv -15 \equiv -2 \pmod{13}$$

This means that -2 is a quadratic residue of 13. However if we compute the Legendre symbol,

$$\left(\frac{-2}{13}\right) = \left(\frac{-1}{13}\right) \left(\frac{2}{13}\right) = (-1)^{\frac{13-1}{2}} (-1)^{\frac{13^2-1}{8}} = -1$$

Contradiction. Therefore $x \equiv 0 \pmod{13}$. Since $15x^2 + 16y^2 \equiv 0 \pmod{13}$, this immediately implies that $y \equiv 0 \pmod{13}$ too.

We may apply the same method to the case modulo 37. Then again we proved the claim. \square

REFERENCES

- 1 *PEN Problem C2*, <http://www.mathlinks.ro/viewtopic.php?t=150496>