1 (Balkan Mathematical Olympiad 1998) Prove that there are no integers x and y satisfying $x^2 = y^5 - 4$.

PEN H15

First Solution. Assume to the contrary that $a^2 = b^5 - 4$ for some integers a and b. First consider when a is even:

Since $b^5 = a^2 + 4$ is even, b is also even. Since $a^2 + 4 = b^5$ is divisible by 2^5, we have $a^2 \equiv -4 \pmod{2^5}$. However, this is a contradiction. This is because even $x^2 \equiv -4 \ (mod\ 16)$ is not possible.

Now, consider the case when a is odd. We rewrite the equation in the form

$$b^5 = a^2 + 4 = (a + 2i)(a - 2i) \tag{1}$$

and work on $\mathbb{Z}[i] = \{x + yi \mid x, y \in \mathbb{Z}\}$, the ring of Gaussian integers. Since a is odd, we find that $a + 2i$ and $a - 2i$ are relatively prime in $\mathbb{Z}[i]$. (Indeed, if $\alpha \in \mathbb{Z}[i]$ divides both $a + 2i$ and $a - 2i$, then α also divides $(a + 2i) - (a - 2i) = 4i$. In other words, α is a divisor of $4i$. Since α also divides $a + 2i$ and since a is odd, this implies that α is a unit in $\mathbb{Z}[i]$.)

We recall that $\mathbb{Z}[i]$ is a unique factorization domain. Since $a + 2i$ and $a - 2i$ are relatively prime, $b^5 = (a + 2i)(a - 2i)$ guarantees that

$$a + 2i = \lambda_1 {\eta_1}^5, \ \ a - 2i = \lambda_2 {\eta_2}^5, \tag{2}$$

where $\eta_1, \eta_1 \in \mathbb{Z}[i]$ and λ_1, λ_2 are units in $\mathbb{Z}[i]$. Since $\lambda_1 \in \{1, -1, i, -i\}$, we get $\lambda_1 = {\lambda_1}^5$. Hence, we can write

$$a + 2i = \lambda_1 {\eta_1}^5 = (\lambda_1 \eta_1)^5 . \tag{3}$$

After setting $\lambda_1 \eta_1 = p + qi$, where $p, q \in \mathbb{Z}$, it becomes

$$a + 2i = (p + qi)^5. \tag{4}$$

Taking conjugates, we also get $a - 2i = (p - qi)^5$. It follows that

$$4i = (a + 2i) - (a - 2i) = (p + qi)^5 - (p - qi)^5 = 2 \left(5p^4 q - 10p^2 q^3 + q^5\right) i \tag{5}$$

or

$$2 = q \left(5p^3 - 10p^2 q^2 + q^4\right) . \tag{6}$$

Now, we get back in the game on $\mathbb{Z}$. Since q divides 2, we get $q \in \{-2, -1, 1, 2\}$. Reading the above equation modulo 5, $2 \equiv q^5 \ (mod\ 5)$. Since Fermat's Little Theorem says that $q^5 \equiv q \ (mod\ 5)$, we have $2 \equiv q \ (mod\ 5)$ or $q = 2$. However, plugging $q = 2$ into the above equation, we obtain $2 = 2 \left(5p^3 - 40p^2 + 16\right)$ or $3 = p^2(p - 8)$. Since p^2 divides 3, we get $p = \pm 1$. However, $p = \pm 1$ means that $p^2(p - 8) = -7, -9$. This is a contradiction. □

Second Solution. Now, assume to the contrary that $a^2 = b^5 - 4$ for some integers a and b. As in the first solution, it is easy to show that the case when a is odd is impossible. We consider the case when a is odd. So, b is also odd. Since $4 = 6^2 - 2^5$, one may rewrite the equation in the form

$$a^2 + 6^2 = b^5 + 2^5 = (b+2)\left(b^4 + (-2)b^3 + (-2)^2b^2 + (-2)^3b + (-2)^4\right). \tag{7}$$

Letting $d_1 = b + 2$ and $d_2 = b^4 + (-2)b^3 + (-2)^2b^2 + (-2)^3b + (-2)^4$, we get

$$a^2 + 6^2 = b^5 + 2^5 = d_1d_2. \tag{8}$$

We can exclude the case when $d_1 = -1$ or when $d_2 = -1$. Indeed, $d_1 = -1$ or $b = -3$ implies that

$$a^2 + 6^2 = b^5 + 2^5 = (-3)^5 + 2^5 < 0, \tag{9}$$

which is a contradiction. If $d_2 = -1$, then $b^5 + 2^5 = d_1d_2 = -d_1 = -b-2$ or $b^5 + b = (-2)^5 + (-2)$. Since the function $t \mapsto t^5 + t$ is strictly increasing, we have $b = -2$ or $a^2 = b^5 + 4 = -28 < 0$, which is a contradiction.

We now clam that the integer $b^5 + 2^5 = d_1d_2$ has a prime divisor $q \neq 3$ with $q \equiv -1 \ (mod\ 4)$.

STEP 1 We show that it is not possible that both d_1 and d_2 are divisible by 3. Indeed, if d_1 is divisible by 3, since $b \equiv d_1 - 2 \equiv -2 \ (mod\ 3)$, we find that

$$d_2 \equiv b^4 + (-2)b^3 + (-2)^2b^2 + (-2)^3b + (-2)^4 \equiv 5(-2)^4 \not\equiv 0 \ (mod\ 3). \tag{10}$$

STEP 2 If $b \equiv -1 \ (mod\ 4)$, then we get $a^2 \equiv b^5 - 4 \equiv -1 \ (mod\ 4)$, which is impossible. Hence, $b \equiv 1 \ (mod\ 4)$. Since $d_1 \equiv b + 2 \equiv -1 \ (mod\ 4)$ and since $d_1 \neq -1$, we see that $|d_1| > 1$. Since $d_1 \equiv -1 \ (mod\ 4)$ and since $|d_1| > 1$, we see that d_1 has at least one prime divisor congruent to -1 modulo 4.

STEP 3 It follows from $d_1d_2 \equiv b^5 + 2^5 \equiv 1 \ (mod\ 4)$ and from $d_1 \equiv b + 2 \equiv -1 \ (mod\ 4)$ that $d_2 \equiv -1 \ (mod\ 4)$. It follows from this and from $d_2 \neq -1$ that $|d_2| > 1$. Since $d_2 \equiv -1 \ (mod\ 4)$, this implies that d_2 also has at least one prime divisor congruent to -1 modulo 4.

Combining results from STEP 1 through STEP 3, we conclude that at least one of d_1 or d_2 has a prime divisor $q \neq 3$ with $q \equiv -1 \ (mod\ 4)$. Since q divides $b^5 + 2^5 = d_1d_2$, our claim is proved.

Now, we employ the following well-known result.

Proposition 1. *Let $p \equiv -1 \ (mod\ 4)$ be a prime. Let a and b are integers such that $a^2 + b^2$ is divisible by p . Then, both a and b are divisible by p.*

Since $a^2 + 6^2 = b^5 + 2^5$, this means that q also divides $a^2 + 6^2$. From Proposition, we see that both a and 6 are divisible by q. Since $q \equiv -1 \ (mod\ 4)$ and since q divides 6, we get $q = 3$. This is a contradiction for the choice of q.

Now, we offer two different ways to establish PROPOSITION 1.

First Proof of Proposition 1 Assume to the contrary that at least one of them are not divisible by p. Since p divides a^2+b^2, we see that none of them are divisible by p. Since p divides a^2+b^2, we obtain $a^2 \equiv -b^2 \ (mod\ p)$. Raise both sides of the congruence to the power $\frac{p-1}{2}$ and apply Fermat's Little Theorem to obtain

$$1 \equiv a^{p-1} \equiv (-1)^{\frac{p-1}{2}} b^{p-1} \equiv -b^{p-1} \equiv -1 \ (mod\ p). \tag{11}$$

This is a contradiction because p is an odd prime.

Second Proof of Proposition 1 Again, assume to the contrary that none of them are divisible by p. Since p divides a^2+b^2, we have the congruence $a^2 \equiv -b^2 \ (mod\ p)$ or $\left(ab^{-1}\right)^2 \equiv -1 \ (mod\ p)$. This means that -1 is a quadratic residue modulo p, which is a contradiction for $p \equiv -1 \ (mod\ 4)$. □

Third Solution. Just toss the Diophantine equation $x^2 = y^5 - 4$ on the field $\mathbb{Z}/11\mathbb{Z}$! It turns out that $x^2 - y^5 \equiv -4 \ (mod\ 11)$ has no solutions. Here is an example of straightforward generalizations:

Proposition 2. *Let* $p \equiv -1, 11 \ (mod\ 60)$ *be a prime. Then, the equation*

$$y^{\frac{p-1}{2}} = x^2 + 4 \tag{12}$$

has no integral solutions.

Hint. Read the equation modulo p! □