Number theory 2 2024

Exercises 3

1. Let (a, b, c) be a primitive Pythagorean triple. Prove that a or b is divisible by 3, but c is not divisible by 3.

Solution. If $x \not\equiv 0 \bmod 3$, then $x^2 \equiv 1 \pmod 3$. Therefore, if $a \not\equiv 0 \pmod 3$ and $b \not\equiv 0 \pmod 3$, we have $c^2 \equiv 2 \pmod 3$. But this is not possible. Therefore, $a \equiv 0 \bmod 3$ or $b \equiv 0 \bmod 3$.

If $c \equiv 0 \pmod 3$ and $b \equiv 0 \pmod 3$, then $a^2 = c^2 - b^2 \equiv 0 \pmod 9$, which implies $a \equiv 0 \pmod 3$. Thus, $\gcd(a, b, c) \geq 3$, and (a, b, c) is not primitive.

2. Let (a, b, c) be a primitive Pythagorean triple. Prove that exactly one of the numbers a, b and c is divisible by 5.

Solution. The quadratic residues mod 5 are 0, 1 ja 4. If $a^2 \equiv b^2 \equiv 1 \pmod 5$, then $c^2 \equiv 2 \pmod 5$, which is not possible. If $a^2 \equiv 1 \bmod 5$ and $b^2 \equiv 4 \pmod 5$, then $c^2 \equiv 0 \pmod 5$, which implies $c \equiv 0 \pmod 5$.

3. Assume that it is known that the Diophantine equation

$$x^p + y^p = z^p$$

has no solutions that satisfy $xyz \neq 0$ for any odd prime p. Prove that for any $n \in \mathbb{N}$, $n \geq 3$, the Diophantine equation

$$x^n + y^n = z^n$$

has no solutions that satisfy $xyz \neq 0$.

Solution. Assume that n has an odd prime factor p. Then $n = pk$ for some $k \in \mathbb{N}^*$. If

$$x^n + y^n = z^n ,$$

then

$$(x^k)^p + (y^k)^p = x^n + y^n = z^n = (z^k)^p$$

implies $xyz = 0$.

4. Let (a, b, c) be a Pythagorean triple. Prove that

$$(ab)^4 + (bc)^4 + (ca)^4 = (c^4 - a^2b^2)^2 .$$

Solution. Expanding the right-hand side of the equation we get

$$(c^4 - a^2b^2)^2 = c^8 - 2c^4a^2b^2 + (ab)^4 .$$

Using the equation $a^2 + b^2 = c^2$, we get

$$c^8 = c^4(a^2 + b^2)^2 = (ac)^4 + 2c^4a^2b^2 + (bc)^4 .$$

Therefore,

$$c^4 - a^2b^2)^2 = (ac)^4 + 2c^4a^2b^2 + (bc)^4 - 2c^4a^2b^2 + (ab)^4 = (ab)^4 + (bc)^4 + (ca)^4 .$$

5. Prove that the Diophantine equation

$$x^2 + y^2 = 3z^2$$

has no solutions that satisfy $xyz \neq 0$.

Solution. Assume the equation has a solution with $xyz \neq 0$. We may assume that $x, y, z > 0$. Pick a solution (a, b, c) with minimal z. Considering the equation mod 3, we have $a^2 + b^2 \equiv 0 \bmod 3$. By the computations done in Exercise 1, we see that $a \equiv b \equiv 0 \bmod 3$. This implies that there are $x_0, y_0 \in \mathbb{N}^*$ such that $x = 3x_0$ and $y = 3y_0$. But this gives

$$9x_0^2 + 9y_0^2 = 3z^2\,,$$

which implies $z^2 \equiv 0 \bmod 3$ and, therefore, $z \equiv 0 \pmod 3$. Thus, there is some $z_0 \in \mathbb{N}^*$ for which $z = 3z_0$. Cancelling the factors 9, we get

$$x_0^2 + y_0^2 = 3z_0^2\,,$$

contradicting the minimality of z.

6. Use the method of infinite descent to prove that $\sqrt{2}$ is an irrational number.

Solution. Assume $m^2 = 2n^2$ is a solution with minimal m. As $m^2 \equiv 0 \bmod 2$, we have $m \equiv 0 \pmod 2$. But this implies that $m = 2m1$ for some $m_1 \in \mathbb{N}^*$, and we get $2m_1^2 = n^2$. But note that the first equation implies that $n < m$, contradicting the minimality of m.

Let $a, b, c, d \in \mathbb{N}^*$. If

$$a^2 + b^2 + c^2 = d^2,$$

then (a, b, c, d) is a *Pythagorean quadruple*. If, furthermore, $\gcd(a, b, c, d) = 1$, then (a, b, c, d) is a *primitive Pythagorean quadruple*.

7. Let $m, n, p \in \mathbb{N}^*$ and let

$$\begin{aligned} a &= 2mp \\ b &= 2np \\ c &= p^2 - (m^2 + n^2) \\ d &= p^2 + (m^2 + n^2)\,. \end{aligned}$$

Prove that (a, b, c, d) is a Pythagorean quadruple.

Solution. $d^2 - c^2 = (p^2 + (m^2 + n^2))^2 - (p^2 - (m^2 + n^2))^2 = 4p^2(m^2 + n^2) = a^2 + b^2$.