Exercise 6.20

Introduction to Discrete Mathematics
MATH 2001

SEBASTIAN CASALAINA

ABSTRACT. This is Exercise 6.20 from Hammack [Ham13, Ch. 6]:

Exercise 6.20. We say that a point $P = (x, y) \in \mathbb{R}^2$ is *rational* if both x and y are rational. In other words, P is rational if $P = (x, y) \in \mathbb{Q}^2 \subseteq \mathbb{R}^2$. An equation $F(x, y) = 0$ is said to have a *rational solution* if there exists $(x_0, y_0) \in \mathbb{Q}^2$ such that $F(x_0, y_0) = 0$. For example, the equation $x^2 + y^2 - 1 = 0$ has the rational solution $(x_0, y_0) = (1, 0)$.

Prove the following statement using any method including direct proof, proof of the contrapositive, or proof by contradiction:

The equation $x^2 + y^2 - 3 = 0$ has no rational solutions.

Solution. Assume for the sake of contradiction that the equation $F(x, y) = 0$ had a rational solution $(x_0, y_0) \in \mathbb{Q}^2$, i.e.,

$$F(x_0, y_0) = x_0^2 + y_0^2 - 3 = 0.$$

By definition, this means there are integers a_0, b_0, a_1, b_1 with b_0, b_1 not equal to zero, such that $\frac{a_0^2}{b_0^2} + \frac{a_1^2}{b_1^2} - 3 = 0$. Doing some arithmetic we arrive at the equation $a_0^2 b_1^2 + a_1^2 b_0^2 = 3b_0^2 b_1^2$, and setting $z_1 = a_0 b_1$, $z_2 = a_1 b_0$, and $z_3 = b_0 b_1$, we see that under our assumption that there exists a rational solution to the equation $F(x, y) = 0$, we may conclude that there exist integers z_1, z_2, z_3 with $z_3 \neq 0$ such that

$$z_1^2 + z_2^2 = 3z_3^2. \tag{0.1}$$

Let 3^r be the largest integer power of 3 that divides z_1, z_2, and z_3. Then, dividing equation (0.1) by 3^r, and setting $w_1 = z_1/3^r$, $w_2 = z_2/3^r$, and $w_3 = z_3/3^r$, we have integers w_1, w_2, and w_3, with

Date: March 11, 2022.

$w_3 \neq 0$, such that

$$w_1^2 + w_2^2 = 3w_3^2, \tag{0.2}$$

and such that not all three of w_1, w_2 and w_3 are divisible by 3. Observe that it follows that w_1 and w_2 are not both divisible by 3, since otherwise, the left hand side of (0.2) would be divisible by 3^2, so that $3w_3^2$ would be divisible by 3^2, which would imply that 3 divided w_3, contradicting our assumption that 3 did not divide all three of w_1, w_2, and w_3.

Now, consider equation (0.2) up to congruence modulo 3:

$$w_1^2 + w_2^2 \equiv 0 \pmod 3; \tag{0.3}$$

in other words, $w_1^2 + w_2^2$ is divisible by 3. On the other hand, given any integer w we have :

$$w^2 \equiv \begin{cases} 0 \pmod 3, & \text{if } w \equiv 0 \pmod 3, \\ 1 \pmod 3, & \text{if } w \equiv 1 \pmod 3, \\ 1 \pmod 3, & \text{if } w \equiv 2 \pmod 3. \end{cases} \tag{0.4}$$

In other words, given an integer w, the remainder of w^2 when divided by 3 is equal to 0 or 1. Consequently, from (0.3) and (0.4), we can conclude that $w_1 \equiv 0 \pmod 3$ and $w_2 \equiv 0 \pmod 3$, contradicting our assumption that w_1 and w_2 were not both divisible by 3. In other words, no matter what w_1, w_2, and w_3 are in (0.2), the left hand side has remainder 0 when divided by 3 only if both w_1 and w_2 are divisible by 3, which we assumed was not the case.

Therefore, our assumption that the equation $F(x, y) = 0$ had a rational solution $(x_0, y_0) \in \mathbb{Q}^2$ was false, and we can conclude that the equation $F(x, y) = 0$ has no rational solutions. $\square$

References

[Ham13] Richard Hammack, *Book of proof*, Creative Commons, 2013.

University of Colorado, Department of Mathematics, Campus Box 395, Boulder, CO 80309

Email address: casa@math.colorado.edu