

**Exercise 20.27**

**Abstract Algebra 1**  
**MATH 3140**

SEBASTIAN CASALAINA

ABSTRACT. This is Exercise 20.27 from Fraleigh [Fra03, §20]:

**Exercise 20.27.** Show that 1 and  $p - 1$  are the only elements of the field  $\mathbb{Z}_p$  that are their own multiplicative inverse. [*Hint:* Consider the equation  $x^2 - 1 = 0$ .]

*Solution.* If an element  $x \in \mathbb{Z}_p$  is its own multiplicative inverse, then  $x^2 = 1$ , or, equivalently,  $x^2 - 1 = 0$ . Since  $x^2 - 1 = (x + 1)(x - 1)$ , we see that

$$(x + 1)(x - 1) = 0.$$

Since  $\mathbb{Z}_p$  is a field, and therefore an integral domain, this implies that  $(x + 1) = 0$ , or  $(x - 1) = 0$ .

In the former case,  $x = -1 = p - 1$ , and in the latter case,  $x = 1$ . □

## REFERENCES

[Fra03] John Fraleigh, *A First Course in Abstract Algebra*, Seventh edition, Addison Wesley, Pearson, 2003.

UNIVERSITY OF COLORADO, DEPARTMENT OF MATHEMATICS, CAMPUS BOX 395, BOULDER, CO 80309

*Email address:* casa@math.colorado.edu