# Worksheet 9

Math 392, Abstract Algebra

Monday, February 1, 2021

1. In $\mathbb{Z}_{13}$, ...

   (a) Convince yourselves that

   $$\bar{1} \cdot \bar{2} \cdot \bar{3} \cdot \bar{4} \cdot \bar{5} \cdot \bar{6} \cdot \bar{7} \cdot \bar{8} \cdot \bar{9} \cdot \overline{10} \cdot \overline{11} \cdot \overline{12} = -\bar{1},$$

   because you've got $\bar{1}$ in there, and $\overline{12} = -\bar{1}$, and the ones in the middle come in pairs that are inverse to one another: $\bar{2} \cdot \bar{7} = \bar{1}$, and $\bar{3} \cdot \bar{9} = \bar{1}$, and so on.

   (b) Convince yourselves

   $$\bar{1} \cdot \bar{2} \cdot \bar{3} \cdot \bar{4} \cdot \bar{5} \cdot \bar{6} = \overline{12} \cdot \overline{11} \cdot \overline{10} \cdot \bar{9} \cdot \bar{8} \cdot \bar{7},$$

   because $\overline{12} = -\bar{1}$ and $\overline{11} = -\bar{2}$ and so on.

   (c) Thus if $a = \bar{1} \cdot \bar{2} \cdot \bar{3} \cdot \bar{4} \cdot \bar{5} \cdot \bar{6}$ then $a^2 = -\bar{1}$.

2. Convince yourselves that the same idea works in $\mathbb{Z}_{17}$ to give an element $a$ with $a^2 = -\bar{1}$.

3. Convince yourselves that the same idea does *not* work in $\mathbb{Z}_{19}$.

4. Challenge: turn this idea into a general proof that if $p \equiv 1 \pmod 4$, then the element

   $$a = \bar{1} \cdot \bar{2} \cdots \overline{\tfrac{p-1}{2}}$$

   in $\mathbb{Z}_p$ satisfies $a^2 = -\bar{1}$.