Algebra: Chapter 0 Exercises

Chapter 2, Section 4

David Melendez

June 13, 2017

Problem 4.9. Prove that if m, n are positive integers such that $\gcd(m, n) = 1$, then $C_{mn} \cong C_m \times C_m$.

Solution. We know that the order of $C_m \times C_n$ is mn, so we just have to prove that $C_m \times C_n$ has an element of order mn.

Proposition. $|([1]_m, [1]_n)| = mn$

Proof. We're looking for the smallest k such that $k \equiv 0 \mod m$ and $k \equiv 0 \mod n$. By definition, we have $k = \operatorname{lcm}(m, n) = mn$. □

■

Problem 4.11. Given that $x^d = 1$ can have at most d solutions in $(\mathbb{Z}/p\mathbb{Z})$ for prime p, prove that the multiplicative group $G = (\mathbb{Z}/p\mathbb{Z})^*$ is cyclic. (Hint: let $g \in G$ be an element of maximal order; show that $h^{|g|} = 1$ for all $h \in G$)

Solution. Let $g \in G$ be an element of maximal order. By exercise 1.15, we know that $|h|$ divides $|g|$ for all $h \in G$, so $h^{|g|} = 1$. Since $h^{|g|} = 1$ for all $h \in G$, there are at least $|G|$ solutions to the equation $x^d = 1$ in $\mathbb{Z}/p\mathbb{Z}$. It then follows that $|G| \leq |g|$ by the given theorem in the problem, so $|G| = |g|$ and therefore G is cyclic. ■