Homework 10

due Thursday, November 11, 14:00

Problem 1. Let $m, k \in \mathbb{Z}_+$ and $a \in (\mathbb{Z}/m\mathbb{Z})^\times$. Show that

$$\operatorname{ord}(a^k) = \frac{\operatorname{ord}(a)}{(\operatorname{ord}(a), k)}.$$

Problem 2. Let $m \in \mathbb{Z}_+$ be a positive integer such that $\mathbb{Z}/m\mathbb{Z}$ has a primitive root. Show the following generalization of Wilson's Theorem:

$$\prod_{x \in (\mathbb{Z}/m\mathbb{Z})^\times} x = -1.$$

Problem 3.

a) Let p be an odd prime. Show that the equation $x^4 = -1$ has a solution in $\mathbb{Z}/p\mathbb{Z}$ if and only if

$$p \bmod 8 = 1 \bmod 8,$$

and has exactly 4 solutions in that case.

b) Let $m \in \mathbb{Z}_+$ and write $m = 2^{i_0} p_1^{i_1} \cdots p_k^{i_k}$ for distinct odd primes $p_1, \ldots, p_k$, $i_0 \geq 0$, and $i_1, \ldots, i_k \geq 1$. Show the equation $x^4 = -1$ has a solution in $\mathbb{Z}/m\mathbb{Z}$ if and only if

$$i_0 \in \{0, 1\} \quad \text{and} \quad p_j \bmod 8 = 1 \bmod 8 \quad \text{for all } j \in \{1, \ldots, k\},$$

and has exactly 4^k solutions in that case.

Problem 4. The n–th *Fermat number* is $F_n = 2^{2^n} + 1$ (the exponent is 2^n).

a) Show that $\operatorname{ord}_{F_n} 2 \leq 2^{n+1}$.

A remark on notation: for coprime $a \in \mathbb{Z}$ and $m \in \mathbb{Z}_+$, the expressions $\operatorname{ord}_m a$, $\operatorname{ord}_m [a]_m$, and $\operatorname{ord}\, [a]_m$ all mean the same thing, the order of $[a]_m$ in $(\mathbb{Z}/m\mathbb{Z})^\times$.

b) Suppose p is a prime divisor of F_n, show that $\operatorname{ord}_p 2 = 2^{n+1}$.

Hint: first show that $\operatorname{ord}_p 2 \mid 2^{n+1}$ to deduce that $\operatorname{ord}_p 2$ is a power of 2 and must divide 2^n if $\operatorname{ord}_p 2 < 2^{n+1}$.

c) Use the previous part to show that $p = 2^{n+1}k + 1$ for some $k \in \mathbb{Z}_+$.