Number Theory I
Spring 2018

Assignment 8.3
Due March 7

Exercise 1. For $n \in \mathbb{N}$, prove that

$$\sum_{d|n} (-1)^{n/d} \varphi(d) = \begin{cases} 0 & \text{if } n \text{ is even,} \\ -n & \text{if } n \text{ is odd.} \end{cases}$$

[*Suggestion:* If n is odd, argue that $(-1)^{n/d} = -1$ for all d. Otherwise write $n = 2^k m$ with m odd and $k \geq 1$ and show that

$$\sum_{d|n} (-1)^{n/d} \varphi(d) = \sum_{d|2^{k-1}m} \varphi(d) - \sum_{d|m} \varphi(2^k d).]$$ [1]

Exercise 2. Modify the proof of Gauss' result on φ to show that for $n \in \mathbb{N}$

$$\sum_{a=1}^{n} (a, n) = \sum_{d|n} d\varphi\left(\frac{n}{d}\right) = n \sum_{d|n} \frac{\varphi(d)}{d}.$$

Exercise 3. Let G be a group and $g \in G$ with $\operatorname{ord}(g) = n$.

a. Prove that the function $c : \mathbb{Z}/n\mathbb{Z} \to \langle g \rangle$ given by $c(a + n\mathbb{Z}) = g^a$ is well-defined.

b. Show that c is a bijection. [*Suggestion:* According to exercise 5.3.3, it suffices to show c is surjective.]

c. Show that c is operation-preserving, i.e. that $c((a+n\mathbb{Z})+(b+n\mathbb{Z})) = c(a+n\mathbb{Z})\cdot c(b+n\mathbb{Z})$ for all a, $b \in \mathbb{Z}$.

This shows that any cyclic group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. That is, up to relabelling, there is only one cyclic group of order n for each $n \in \mathbb{N}$.

[1] It occurs to me that this approach requires an additional fact which we haven't proven. Namely, that if $(m, n) = 1$ and $d|mn$, then $d = d_1 d_2$ where $d_1|m$ and $d_2|n$. This can be easily proven using Béout's lemma or the Fundamental Theorem of Arithmetic. In the context of the problem at hand this means that the divisors of $n = 2^k m$ must all have the form $d = 2^j \ell$, where $0 \leq j \leq k$ and $\ell|m$.