Homework 2 - Modern Algebra (Math 541) - S17

27 de febrero de 2017

Due on March 3, 2017

Mandatory (from Artin's Algebra):
2.6.10, 2.7.1, 2.8.1, 2.8.4, 2.8.6, 2.8.8, 2.8.10, 2.9.1 (see problem **b.** below), 2.9.2, 2.9.4.

-Additional mandatory problems:

a. Let us consider two positive integers $m, n \in \mathbb{Z}$. Recall that we define its *greatest common divisor* as the largest positive integer d such that d divides both to m and to n. In other words, it is the unique integer d such that d divides both m and n and such that if e is another integer dividing m and n, them e divides d. We usually denote the greatest common divisor of m and n as $\gcd(m, n)$.

Let us also consider $m\mathbb{Z} + n\mathbb{Z}$ as the set $\{mr + ns : r, s \in \mathbb{Z}\}$.

Prove: (1) $m\mathbb{Z} + n\mathbb{Z}$ is a subgroup of $\mathbb{Z}^+$ (the aditive group of the integers). (2) $m\mathbb{Z} + n\mathbb{Z} = \gcd(m, n)\mathbb{Z}$ as subgroups of $\mathbb{Z}^+$.

b. The following problem gives another approach to multiplicative groups in modular arithmetic.

Let n be a positive integer and denote by $\mathbb{Z}/n\mathbb{Z}$ the set of equivalence classes of the integers mod n, i.e., $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots\}$. Consider the set $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} : \exists \bar{c} \in \mathbb{Z}/n\mathbb{Z} \text{ with } \bar{a} \cdot \bar{c} = \bar{1}\}$.

Prove: (1) $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ is a multiplicative group. (2) $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = 1\}$. (3) When is $(\mathbb{Z}/n\mathbb{Z} - \{\bar{0}\}, \times)$ a group?

c. Compute the last two digits of the 100th power of 2.

Recommended: 2.7.2 and 2.7.4 were discussed in class. Review them and try 2.7.5.