Assignment 2 – All 2 parts – Math 412

Due in class: Thursday, Sept. 12, 2019

Textbook exercises:[1]
Section 1.3: 10 (WI), 17
Section 2.1: 6, 4
Section 2.2: 14 (14(c) will be WI)

1 1.3.10

First let us suppose that p is prime. Moreover we can express any element $a \in \mathbb{Z}$ as $a = p_1 ... p_n$, where p_i are primes. Now we have the prime factorization of a. p must either be in this prime factorization or not.

- Suppose there exists some p_k such that $p = p_k$. We have that $a = p_k(p_1 ... p_{k-1} p_{k+1} ... p_n)$. Here we can see that $p \mid a$.
- Suppose that there is no p_i such that $p = p_i$. Since we have assumed that p is prime we know that if p itself is not in the factorization of a, they will not share any common factors. It follows that $(a, p) = 1$.

Now let us suppose that we have p is not prime. Then we can express p as a product of primes. $p = p_1 ... p_n$. We can show that given p, we can construct a such that $(a, p) > 1$ and $p \nmid a$. Say $a = p_1 ... p_{n-1}$ so $(a, p) = a$. Then we have that $p > a$ so $p \nmid a$.

2 1.3.17 do later

If $(a, b) = p$ we can say that $(a^2, b^2) = p^2$. We can factorize a, b and order the primes, q_i in increasing order, remembering that p is a factor of both. $a = q_1 1 ... q_k p q_{k+1} ... q_n$, $b = q_1$

3 2.1.6

Suppose that $a \equiv b \pmod{n}$ and $k \mid n$. We can say that there exists α such that $n = k\alpha$. Also by definition of mod, $n \mid a - b$, so there exists β such that $a - b = \beta n$. We have that $a - b = \beta n = \beta k \alpha = (\alpha\beta)k$. So $k \mid a - b$ and it follows that $a \equiv b \pmod{k}$.

[1] From Hungerford's *Abstract algebra, An introduction, Third edition*

Other exercises:

(1) (WI) Prime factorization, gcds, and lcms. Let a and b be non-zero integers and let $p_1, \ldots, p_k > 0$ be the positive primes that divide a or b (or both!). Write

$$a = up_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \quad \text{and} \quad b = vp_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$$

with $u, v \in \{\pm 1\}$ and $e_i, f_i \geq 0$ (recall from class that u, v, and the e_i and f_i are unique).

(a) Show that $a \mid b$ if and only if $e_i \leq f_i$ for all $i = 1, 2, \ldots, k$.

(b) Show that

$$\gcd(a, b) = p_1^{g_1} p_2^{g_2} \cdots p_k^{g_k}$$

where $g_i = \min(e_i, f_i)$.

(c) The *least common multiple* of a and b is the smallest positive integer that is divisible by both a and b. It is denoted $\operatorname{lcm}(a, b)$ or simply $[a, b]$ (like the gcd is sometimes denoted simply (a, b)). Show that

$$\operatorname{lcm}(a, b) = p_1^{h_1} p_2^{h_2} \cdots p_k^{h_k}$$

where $h_i = \max(e_i, f_i)$.

(d) Show that $ab = (a, b)[a, b]$.

(2) Suppose p is a prime number and $a \in \mathbf{Z}$.

(a) Let $n \in \mathbf{Z}_{\geq 0}$. Show that if $p \mid a^n$, then $p^n \mid a^n$.

(b) Let $e \in \mathbf{Z}_{\geq 0}$. We say that p^e *exactly divides* a (written $p^e \mid\mid a$) if $p^e \mid a$ and $p^{e+1} \nmid a$. Let $b \in \mathbf{Z}$. Let $b \in \mathbf{Z}$ and suppose $p^e \mid\mid a$ and $p^f \mid\mid b$. Show that $p^{e+f} \mid\mid ab$.

(c) Suppose $p^e \mid\mid a$ and $p^f \mid\mid b$. Show $p^{\min(e,f)} \mid b$. Show by example that it can happen that $p^{\min(e,f)}$ does not exactly divide $a + b$.

(3) Let $n \in \mathbf{Z}_{\geq 1}$. Show that for $a \in \mathbf{Z}$, its congruence class modulo n is given by

$$[a] = \{a + nk : k \in \mathbf{Z}\}.$$

(4) Write out addition and multiplication tables for $\mathbf{Z}/4\mathbf{Z}$. (The tables for $\mathbf{Z}/5\mathbf{Z}$ and $\mathbf{Z}/6\mathbf{Z}$ are in example 2 of §2.2 of the textbook.)