

**Chapter 2:** 14, 22, 24, 25, 26, 28.

**Due date:** Wednesday, 9/12

- 14.** Show that the Principle of Well-Ordering for the natural numbers implies that 0 is the smallest natural number. Use this result to show that the Principle of Well-Ordering implies the Principle of Mathematical Induction; that is, show that if  $S \subseteq \mathbb{N}$  such that  $0 \in S$  and  $n + 1 \in S$  whenever  $n \in S$ , then  $S = \mathbb{N}$ .
- 22.** Let  $n \in \mathbb{N}$ . Use the division algorithm to prove that every integer is congruent mod  $n$  to precisely one of the integers  $0, 1, \dots, n - 1$ . Conclude that if  $r$  is an integer, then there is exactly one  $s$  in  $\mathbb{Z}$  such that  $0 \leq s < n$  and  $[r] = [s]$ . Hence, the integers are indeed partitioned by congruence mod  $n$ .
- 23.** Define the *least common multiple* of two nonzero integers  $a$  and  $b$ , denoted by  $\text{lcm}(a, b)$ , to be the nonnegative integer  $m$  such that both  $a$  and  $b$  divide  $m$ , and if  $a$  and  $b$  divide any other integer  $n$ , then  $m$  also divides  $n$ . Prove that any two integers  $a$  and  $b$  have a unique least common multiple.
- N.B. Exercise 23 is not required. It is included here for you reference, since it defines *least common multiple*.
- 24.** If  $d = \text{gcd}(a, b)$  and  $m = \text{lcm}(a, b)$ , prove that  $dm = |ab|$ .
- 25.** Show that  $\text{lcm}(a, b) = ab$  if and only if  $\text{gcd}(a, b) = 1$ .
- 26.** Prove that  $\text{gcd}(a, c) = \text{gcd}(b, c) = 1$  if and only if  $\text{gcd}(ab, c) = 1$  for integers  $a$ ,  $b$ , and  $c$ .
- N.B. The following problem (Exercise 27) is not required. It is included here for you reference, since it may be useful when solving 26 (depending on the proof strategy you use). You may use the result stated in Exercise 27, even if you have not yet proved it.
- 27.** Let  $a, b, c \in \mathbb{Z}$ . Prove that if  $\text{gcd}(a, b) = 1$  and  $a \mid bc$ , then  $a \mid c$ .
- 28.** Let  $p \geq 2$ . Prove that if  $2^p - 1$  is prime, then  $p$  must also be prime.