Math 401: Introduction to Abstract Algebra
Problem Set 3[1]
due: February 18, 2019

Emily Riehl

Exercise 1. Let d be a positive integer and let n be an integer. Prove that $d \mid n$ if and only if in the unique expression $n = dq + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < d$ the remainder $r = 0$.

Exercise 2. True or false? If $a \mid c$ and $b \mid c$ then $a \cdot b \mid c$. If true, supply a proof. If false, supply a counterexample.

Exercise 3. Suppose that $p_1, \ldots, p_k$ are distinct primes and that

$$m = p_1^{a_1} \cdots p_k^{a_k} \qquad \text{and} \qquad n = p_1^{b_1} \cdots p_k^{b_k}$$

for $a_1, \ldots, a_k, b_1, \ldots, b_k \in \mathbb{N}$. Show that
(i) $\gcd(m, n) = p_1^{\min\{a_1,b_1\}} \cdots p_k^{\min\{a_k,b_k\}}$
(ii) $\mathrm{lcm}(m, n) = p_1^{\max\{a_1,b_1\}} \cdots p_k^{\max\{a_k,b_k\}}$
(iii) $mn = \mathrm{lcm}(m, n) \cdot \gcd(m, n)$.

Exercise 4. True or false? For all $n, m \in \mathbb{N}$, $mn = \mathrm{lcm}(m, n) \cdot \gcd(m, n)$. If true, supply a proof. If false, supply a counterexample.

Exercise 5. Generalize a theorem from class to show that if p is a prime number and $p \mid a_1 \cdots a_k$ for integers $a_1, \ldots, a_k$ then there exists an index i so that $p \mid a_i$.

Exercise 6. A **binary operation** on a set S is a function $\star \colon S \times S \to S$ that takes as input an ordered pair of elements of S and returns an element of S; write $(a, b) \mapsto a \star b$. The binary operation $\star$ is **associative** if for all $a, b, c \in S$, $a \star (b \star c) = (a \star b) \star c$.[2] Which of the following binary operations on $\mathbb{Z}$ are associative?
(i) The operation that assigns to the pair (a, b) the minimum of a and b.
(ii) The operation that assigns (a, b) the element a.
(iii) The operation that assigns (a, b) the element $a - b$.

Exercise 7*. Prove the division algorithm for polynomials with real coefficients. Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots a_1 x + a_0$ and $g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$ be polynomials with coefficients in $\mathbb{R}$. Show that there exist polynomials $q(x)$, $r(x)$ so that

$$f(x) = q(x) \cdot g(x) + r(x)$$

with the degree of $r(x)$ less than the degree of $g(x)$.[3] [Hint: use induction on the degree of $f(x)$.]

Dept. of Mathematics, Johns Hopkins Univ., 3400 N Charles St, Baltimore, MD 21218
E-mail address: `eriehl@math.jhu.edu`

[1] Problems labelled n* are optional (fun!) challenge exercises that will not be graded.
[2] For an associative binary operation, an unbracketed product $a \star b \star c$ can be interpreted as either $a \star (b \star c)$ or $(a \star b) \star c$. If $\star$ is not associative, then this triple product is likely not meaningful.
[3] The degree of the polynomial $g(x)$ is the highest power of x it contains, in this case m.