Fall 2022, Math 522: Week 7 Problem Set
Due: Friday, October 21st, 2022
Arithmetic Functions

Discussion problems. The problems below should be worked on in class.

(D1) *Formulas for $d(n)$ and $\sigma(n)$.* Let $d(n)$ denote the number of positive divisors of n, and let $\sigma(n)$ denote the sum of the positive divisors of n.

(a) Find $d(n)$, and $\sigma(n)$ for $n = 2, 3, \ldots, 10$ and $n = 42$.

(b) Find a formula for $d(p)$ and for $\sigma(p)$ when p is prime.

(c) Find a formula for $d(p^r)$ and $\sigma(p^r)$ when p is prime and $r \geq 1$. Express your formula for $\sigma(p^r)$ as a fraction with denominator $p - 1$.

(d) We will prove in Problem (D2) (on Friday) that $d(ab) = d(a)d(b)$ and $\sigma(ab) = \sigma(a)\sigma(b)$ whenever $\gcd(a, b) = 1$. Using **only** this fact and your formulas from part (c), find $d(n)$ and $\sigma(n)$ for $n = 15$, 30, and 36.

(e) Use the previous part and your work above to derive formulas for $d(n)$ and $\sigma(n)$ in terms of the prime factorization $n = p_1^{r_1} \cdots p_k^{r_k}$. Be sure to state any assumptions about $p_1, \ldots, p_k$ and $r_1, \ldots, r_k$.

(D2) *Multiplicative functions.* The goal for this problem is to prove that $d(n)$ and $\sigma(n)$ are multiplicative on relatively prime integers.

In what follows, let $D_n = \{d > 0 : d \mid n\}$ denote the set of positive divisors of n.

(a) Find D_4, D_{15}, and D_{60}.

(b) Given two subsets $A, B \subset \mathbb{Z}$, define $A \cdot B = \{ab : a \in A, b \in B\}$ as the set of products of an element of A by an element of B.

Find $D_3 \cdot D_5$. Then find $D_4 \cdot D_{15}$. What do you notice? How does this relate to $d(n)$ being multiplicative on relatively prime integers?

(c) Find $D_4 \cdot D_6$. Locate n so that your result equals D_n. Is it true that $d(4) \cdot d(6) = d(n)$? How does this example differ from part (b)?

(d) Formulate a conjecture for what set $D_a \cdot D_b$ coincides with.

(e) Prove that if $d \mid ab$, then $d = a'b'$ for some $a' \mid a$ and $b' \mid b$. Use this to prove your conjecture in the previous part.

(f) Argue that in part (e), if $\gcd(a, b) = 1$, then the integers a' and b' are **unique**. Is this true if the hypothesis $\gcd(a, b) = 1$ is dropped?

(g) Use parts (e) and (f) to conclude that if $\gcd(a, b) = 1$, then $d(ab) = d(a)d(b)$.

(h) Suppose $\gcd(a, b) = 1$ and that $D_a = \{a_1, a_2, a_3\}$ and $D_b = \{b_1, b_2\}$. Find $\sigma(a)$, $\sigma(b)$, and $\sigma(ab)$. Why does $\sigma(ab) = \sigma(a)\sigma(b)$ in this case?

(i) Argue that if $\gcd(a, b) = 1$, then $\sigma(ab) = \sigma(a)\sigma(b)$.

Homework problems. You must submit *all* homework problems in order to receive full credit.

Unless otherwise stated, $a, b, c, n, p \in \mathbb{Z}$ are arbitrary with $p > 1$ prime and $n \geq 2$.

(H1) Find $\phi(441)$ without using a calculator.

Hint: $441 = 3^2 7^2$.

(H2) Locate infinitely many integers n such that $10 \mid \phi(n)$.

(H3) Prove that every $n \geq 1$ satisfies $d(n) < 2\sqrt{n}$.

(H4) (a) Prove that $n \mid (\phi(n)\sigma(n) + 1)$ if n is prime.

(b) Prove that $n \nmid (\phi(n)\sigma(n) + 1)$ if $p^2 \mid n$ for some prime p.

Challenge problems. Challenge problems are not required for submission, but bonus points will be awarded for submitting a partial attempt or a complete solution.

(C1) In this problem, we will prove that $\phi(n)$ is multiplicative on relatively prime integers, as was shown for both $d(n)$ and $\sigma(n)$ in discussion.

Let $\mathbb{Z}_n^* = \{[a]_n : \gcd(a, n) = 1\}$ denote the set of units in $\mathbb{Z}_n$, and consider the function

$$\begin{aligned} f : \mathbb{Z}_{nm}^* &\longrightarrow \mathbb{Z}_n^* \times \mathbb{Z}_m^* \\ [a]_{nm} &\longmapsto ([a]_n, [a]_m). \end{aligned}$$

(a) Prove that f is well-defined, that is, if $[a]_{nm} = [b]_{nm}$, then $f([a]_{nm}) = f([b]_{nm})$.

(b) Prove that if $\gcd(n, m) = 1$, then f is one-to-one.

(c) Use the Chinese Remainder Theorem to prove that if $\gcd(n, m) = 1$, then f is onto.

(d) Use the previous parts to conclude that if $\gcd(n, m) = 1$, then $\phi(nm) = \phi(n)\phi(m)$.