Math 431 - Real Analysis
Solutions to Homework due August 27

Question 1. Use the nine axioms introduced in class to prove the following. Be sure to cite which axioms you are proving. In what follows, let $a, b, c \in \mathbb{R}$.

(a) $a > 0$ if and only if $-a < 0$.

(b) $-1 < 0$

(c) $a > 0$ if and only if $a^{-1} > 0$.

(d) If $a > 0$ and $b < 0$, then $a \cdot b < 0$.

(e) If $a < b$ and $c < 0$, then $c \cdot a > c \cdot b$.

Solution 1.

(a) For any $a \in \mathbb{R}$, Axiom 4 guarantees the existence of $-a \in \mathbb{R}$ such that $a + (-a) = 0$. Assume that $0 < a$. By Axiom 7, we have that $-a = 0 + (-a) < a + (-a) = 0$. Thus, $-a < 0$. Conversely, if $-a < 0$, then again by Axiom 7, we have that $0 = (-a) + a < 0 + a = a$. Thus, $0 < a$. Therefore, $a > 0$ if and only if $-a < 0$. $\square$

(b) Notice that $-1 \neq 0$. Assume, to the contrary, that $-1 > 0$. Then, by 1a, $1 < 0$, which is not true (proven in class). By Axiom 6, the only possibility is that $-1 < 0$. $\square$

(c) First, we will show that if $a > 0$, then $a^{-1} > 0$. Assume, to the contrary, that $a^{-1} \leq 0$. First note that $a^{-1} \neq 0$ since, if it were, then $1 = a \cdot a^{-1} = a \cdot 0 = 0$, a contradiction. Thus, we are left to assume that $a^{-1} < 0$. By 1a, we know that $-a^{-1} > 0$. Since $a > 0$ and $-a^{-1} > 0$, then Axiom 8 gives us that

$$-1 = a \cdot (-a^{-1}) > 0,$$

a contradiction.

Next, we show that if $a^{-1} > 0$, then $a > 0$. As before, assume, to the contrary, that $a \leq 0$. Again, $a \neq 0$ since, if it were, then $1 = a^{-1} \cdot a = a^{-1} \cdot 0 = 0$, a contradiction. Thus, we are left to assume that $a < 0$. By 1a, we have that $-a > 0$ and thus, by Axiom 8,

$$-1 = (-a) \cdot a^{-1} > 0,$$

a contradiction. $\square$

(d) If $b < 0$, then by 1a, we know that $0 < -b$. Since $a > 0$ and $-b > 0$, then by Axiom 8, $-ab = a \cdot (-b) > 0$. By Axiom 7, we get that

$$0 = -ab + ab > ab.$$

Thus, $ab < 0$. $\square$

(e) Since $a < b$, by Axiom 7, we have that

$$0 = a + (-a) < b + (-a) = b - a.$$

By 1d, since $b - a > 0$ and $c < 0$, then $c(b - a) < 0$. By Axiom 3, this is equivalent to $cb - ca < 0$. By Axiom 7, we get that

$$cb = cb - ca + ca < 0 + ca = ca.$$

Thus, $cb < ca$. $\square$

Question 2. Let $n \in \mathbb{Z}$ and $x, y \in \mathbb{R}$ and consider the following expression:

$$(x-y)\sum_{k=0}^{n-1} x^k y^{n-1-k}.$$

(a) For $n = 1, 2, 3$, evaluate the above expression and expand & simplify as much as possible.

(b) Using your observations from (a), conjecture a general pattern.

(c) Prove your conjectured pattern from (b).

Solution 2.

(a) For $n = 1$, our sum yield only 1 and thus our expression is $x - y$.
For $n = 2$, we have

$$(x-y)(y+x) = xy + x^2 - y^2 - xy = x^2 - y^2.$$

For $n = 3$, we have

$$(x-y)(y^2+xy+x^2) = xy^2 + x^2y + x^3 - y^3 - xy^2 - x^2y = x^3 - y^3.$$

(b) In general, we conjecture that

$$(x-y)\sum_{k=0}^{n-1} x^k y^{n-1-k} = x^n - y^n.$$

(c) We prove our conjectured expression by expanding the left hand side. Doing so yields

$$\begin{aligned}(x-y)\sum_{k=0}^{n-1} x^k y^{n-1-k} &= x\sum_{k=0}^{n-1} x^k y^{n-1-k} - y\sum_{k=0}^{n-1} x^k y^{n-1-k} \\ &= \sum_{k=0}^{n-1} x^{k+1} y^{n-1-k} - \sum_{k=0}^{n-1} x^k y^{n-k}\end{aligned}$$

In our remaining expression, we wish to re-index our first sum to match the entries in the second sum. To do so, we replace $k+1$ with j. This yield the new sum

$$\sum_{j=1}^{n} x^j y^{n-j}.$$

Thus, we have

$$(x-y)\sum_{k=0}^{n-1} x^k y^{n-1-k} = \sum_{j=1}^{n} x^j y^{n-j} - \sum_{k=0}^{n-1} x^k y^{n-k}.$$

Notice that the first and second sums now have the same entries, except that the starting and ending values of the indices differ. Thus, most terms will cancel, except for the one corresponding to $j = n$ in the first sum and $k = 0$ in the second sum; these correspond to the terms x^n and y^n, respectively. Thus, we obtain our desired result:

$$(x-y)\sum_{k=0}^{n-1} x^k y^{n-1-k} = x^n - y^n.$$

$\square$

Question 3. Show that if $2^n - 1$ is prime, then n is prime. A prime number of the form $2^n - 1$ is called a *Mersenne prime*. Hint: Prove the contrapositive and use your conjectured equation from 2b in your proof.

Solution 3.
We will instead prove the contrapositive statement: "If n is composite, then $2^n - 1$ is composite." Since n is composite, then $n = a \cdot b$ where $1 < a, b < n$. Thus, we have that

$$2^n - 1 = 2^{ab} - 1 = 2^a 2^b - 1.$$

We can use the equation from 2b:

$$(x - y) \sum_{k=0}^{n-1} x^k y^{n-1-k} = x^n - y^n$$

with $x = 2^a, y = 1$, and $n = b$. Doing so yields

$$\begin{aligned} 2^n - 1 = 2^{(ab)} - 1 &= (2^a)^b - 1^b \\ &= (2^a - 1) \sum_{k=0}^{b-1} (2^a)^k \cdot 1^{b-1-k} \\ &= (2^a - 1) \sum_{k=0}^{b-1} 2^{ak}. \end{aligned}$$

Since $a \in \mathbb{Z}$, then $2^a - 1 \in \mathbb{Z}$; similarly, since $a, b, k \in \mathbb{Z}$, then $\sum_{k=0}^{b-1} 2^{ak} \in \mathbb{Z}$. Also, since $a > 1$, then $2a - 1 > 1$. Lastly, since $a, b > 1$, then $\sum_{k=0}^{b-1} 2^{ak} > 1$. Thus, we have written $2^n - 1$ as a product of two positive integers, each greater than 1 and so $2^n - 1$ is composite.

Having proven the contrapositive, the original statement "if $2n - 1$ is prime, then n is prime" is also true. $\square$

Question 4. Show that if $2^n + 1$ is prime, then n is a power of 2. A prime number of the form $2^{2^m} + 1$ is called a *Fermat prime*. Hint: As with (3), prove the contrapositive and use your 2b equation.

Solution 4. We instead prove the contrapositive statement "If n is not a power of 2, then $2^n + 1$ is composite." Since n is not a power of 2, then n is divisible by some prime $p \neq 2$. Since 2 is the only even odd number, p is necessarily odd. Thus, we can write $n = pr$ where $1 < r < n$. Now, consider $2^n + 1 = 2^{rp} + 1$. Since n is odd, then $(-1)^n = -1$. So, using our equation from 2b with $x = 2^r, y = -1$, and $n = r$, we get:

$$\begin{aligned} 2^{rp} + 1 &= (2^r)^p - (-1)^p \\ &= (2^r + 1) \sum_{k=0}^{p-1} (2^r)^k (-1)^{p-1-k} \end{aligned}$$

Since $1 < r < n$, we have that $1 < 2^r + 1 < 2^{rp} + 1$.. Furthermore, $\sum_{k=0}^{p-1} (2^r)^k (-1)^{p-1-k} \in \mathbb{Z}$. Thus, $2^n + 1$ has a non-trivial divisor and therefore composite.

Having proven the contrapositive, the original statement "if $2^n + 1$ is prime, then n is a power of 2" holds true as well. $\square$

Question 5. Consider the set

$$\mathcal{Q} = \left\{ \frac{p}{q} \,\middle|\, p, q \in \mathbb{Z}, q \neq 0 \right\}.$$

Define a relation $\sim$ on $\mathcal{Q}$ given by

$$\frac{p_1}{q_1} \sim \frac{p_2}{q_2} \text{ if and only if } p_1 q_2 = p_2 q_1.$$

Below, we will show that $\sim$ is an *equivalence relation*, and therefore be able to define the rational numbers $\mathbb{Q}$ as the set of *equivalence classes of elements in* $\mathcal{Q}$.

(a) Reflexivity: Show that $\dfrac{p_1}{q_1} \sim \dfrac{p_1}{q_1}$.

(b) Symmetry: Show that if $\dfrac{p_1}{q_1} \sim \dfrac{p_2}{q_2}$, then $\dfrac{p_2}{q_2} \sim \dfrac{p_1}{q_1}$.

(c) Transitivity: Show that if $\dfrac{p_1}{q_1} \sim \dfrac{p_2}{q_2}$ and $\dfrac{p_2}{q_2} \sim \dfrac{p_3}{q_3}$, then $\dfrac{p_1}{q_1} \sim \dfrac{p_3}{q_3}$.

Solution 5.

(a) Notice that trivially $p_1 q_1 = p_1 q_1$; thus, $\dfrac{p_1}{q_1} \sim \dfrac{p_1}{q_1}$.

(b) Assume that $\dfrac{p_1}{q_1} \sim \dfrac{p_2}{q_2}$. Then, $p_1 q_2 = p_2 q_1$.. This is, of course, equivalent to $p_2 q_1 = p_1 q_2$. Thus, $\dfrac{p_2}{q_2} = \dfrac{p_1}{q_1}$.

(c) Assume that $\dfrac{p_1}{q_1} \sim \dfrac{p_2}{q_2}$ and $\dfrac{p_2}{q_2} \sim \dfrac{p_3}{q_3}$. Then, $p_1 q_2 = p_2 q_1$ and $p_2 q_3 = p_3 q_2$. Multiplying the first equation by q_3, we get

$$q_3 p_1 q_2 = q_3 p_2 q_1.$$

Using the second equality, we can substitute into $p_2 q_3$ to get

$$q_3 p_1 q_2 = (q_3 p_2) q_1 = p_3 q_2 q_1.$$

Thus, since $q_3 p_1 q_2 = p_3 q_2 q_1$ and $q_2 \neq 0$, we can multiply through by q_2^{-1} to get $p_1 q_3 = p_3 q_1$, as desired. Thus, $\dfrac{p_1}{q_1} \sim \dfrac{p_3}{q_3}$.