Analysis HW #3

Dyusha Gritsevskiy

January 2019

Problem (1)**.** Prove (for integers) that if $a = q \cdot b + r$ then $\gcd(a, b) = \gcd(b, r)$.

Solution. Consider the set $Y = \{r \in \mathbb{Z}^+ \mid r \text{ divides } b\}$. We will make use of the following claim:

Claim 0.1. If $k \in Y$, then $k \mid qb + r$ iff $k \mid r$.

Proof. ($\implies$): Since $k \in Y$, $k \mid b$. Thus, $b = xk$ for some integer x. So $qb = k(qx)$, and qx is a positive integer, so $k \mid qb$. Thus, $qb = yk$ for some integer y[1]. Thus $qb + r = ky + r = k(y + r/k)$, so k must divide r. Hence $k \mid r$.

($\impliedby$): Since $k \in Y$, $k \mid b$. Thus, $b = xk$ for some (positive) integer x. But also $k \mid r$, so $r = yk$ for some (positive) integer y. Hence $qb + r = qxk + yk = k(qx + y)$; hnce, $k \mid qb + r$ since $qx + y$ is a positive integer. □

Now, consider the set $X = \{r \in \mathbb{Z}^+ \mid r \text{ divides } r\}$, and $Z = \{r \in \mathbb{Z}^+ \mid r \text{ divides } qb + r\}$. By definition, $\gcd(b, r) \in Y$ and $\gcd(b, r) \in X$; by the claim, $\gcd(b, r) \in Z$. Again by definition, $\gcd(a, b) = \gcd(qb + r, b) \in Z$ and $\gcd(a, b) \in Y$; by the claim, $\gcd(a, b) \in X$. Hence, both greatest common divisors are in the set of possible divisors $X \cup Y \cup Z$. But since $X \cup Y \cup Z$ has a unique greatest element, $\gcd(a, b) = \gcd(b, r)$. □

Problem (2)**.** Prove that for any natural numbers a, b, there are integers u, w so that $\gcd(a, b) = u \cdot a + w \cdot b$.

Solution. Write $a = bq + r$ and $b = rq_1 + r_1$; continuing the Euclidean algorithm, we get that $r = r_1 q_2 + r_2$, $r_1 = r_2 q_3 + r_3$, etc, until $r_{n-2} = r_{n-1} q_n + r_n$ and $r_{n-1} = 0$. By (1), we know that $\gcd(a, b) = \gcd(b, r) = \gcd(r_{n-1}, 0) = r_{n-1}$. By induction, we can work upwards to write r_{n-1} as a linear combination of a and b; thus, $\gcd(a, b)$ is some integral linear combination of a and b, as desired. □

[1] In particular, $y = qx$.

Problem (3)**.** Let p be prime (meaning a natural number so that the only natural numbers dividing p are p and 1). Suppose p divides $a \cdot b$. Prove that p divides a or divides b.

Solution. □

Problem (Rudin 1.2)**.** Prove that there is no rational number whose square is 12.

Solution. If $x^2 = 12$, then $x^2 = 2^2 \cdot 3$, so $(x/2)^2 = 3$; since $x/2$ is rational iff x is rational, suffices to show that there is no rational number whose square is 3. Since $3 > 2$, we showed in class that it suffices to show that there exists no $x > 1 \in \mathbb{Q}$ that can be written as $\frac{n}{m}$ with $0 < m < n$; i.e., if $n, m \in \mathbb{N}$ and $0 < m < n$, then $(\frac{n}{m})^2 \neq 3$.

We prove this by strong induction on n.

Fix n. By induction assume that if $k < n$ and $0 < l < k$, then $(\frac{k}{l})^2 \neq 3$. Fix $m < n$ such that $m > 0$. Have to show that $(\frac{n}{m})^2 \neq 12$. Suppose for contradiction that $(\frac{n}{m})^2 = 3$. Then $nn = 3mm$, so $3 \mid nn$. Since 3 is prime in $3 \mid nn$, $3 \mid n$ or $3 \mid n$, so $3 \mid n$. In other words, we can write n as $3k$[2]. Thus $(3k)(3k) = 3mm$; by cancellation, $3kk = mm$. So $3 \mid mm$, so $3 \mid m$. Since we can write $m = 3l$, we know that $l < m$. In addition, $m < n$, so $l < n$. Therefore, we get that

$$\begin{aligned} 3 \cdot k \cdot k &= 3 \cdot l \cdot 3 \cdot l \\ k \cdot k &= 3 \cdot l \cdot l \\ \left(\frac{k}{l}\right)^2 &= 3 \end{aligned}$$

which contradicts the induction hypothesis. Thus, there exists on rational number whose square is 3; hence there exists no rational number whose square is 12. □

Problem (Rudin 1.4)**.** Let E be a nonempty subset of an ordered set; suppose α is a lower bound of E and β is an upper bound of E. Prove that $\alpha \leq \beta$.

Solution. By trichotomy, suffices to show that $a \not> b$. Suppose for contradiction that $a > b$. Since a is a lower bound, $\exists x \in E$ s.t. $x \geq a$. Since b is an upper bound and $x \in E$, $x \leq b$. Hence $a \leq b$, so we get a contradiction. □

[2] Where k is a positive natural!

Problem (Rudin 1.5)**.** Let A be a nonempty set of real numbers which is bounded below. Let $-A$ be the set of all numbers $-x$, where $x \in A$. Prove that $\inf A = -\sup(-A)$.

Solution. Since A is nonempty and bounded below, and the reals are Dedekind-complete, $\inf A$ exists. Let $\inf A = x$. Thus, it suffices to show that $-x = \sup(-A)$. To do this, we must show two things:

First, that $-x$ is an upper bound. Suppose for contradiction that $\exists a \in -A$ s.t. $a > -x$. By properties of order, $-a < x$. But since $a \in -A$, by definition of $-A$, we must have that $-a \in A$. But x is a lower bound for A, so $-a < x$ is a contradiction. got 'em!

Second, that $-x$ is the least upper bound. To do this, suppose that there is some $p \in \mathbb{R}$ such that $p < x$ and p is an upper bound for $-A$. Since $p \in \mathbb{R}$, it's hard to work with, so let $q \in \mathbb{Q}$ be some rational such that $p < q < -x$[3]. Since $q > p$, it suffices to show that q is not an upper bound for $-A$, i.e., $\exists \gamma \in -A$ s.t. $\gamma > q$. Consider $\gamma = \frac{-x+q}{2}$. It is easy to check that $q < \gamma < -x$. By properties of order, $-q > -\gamma > x$. Since x is an infimum for A, and we know that $-q \in A$, and $-\gamma$ is between the two, $-\gamma \in A$. Hence, $\gamma \in -A$. But $\gamma > q$, a contradiction. got 'em! ☐

Problem (4.3.1)**.** Prove **Proposition 4.3.3**: Let x, y, z be rational numbers. Then

(a) We have $|x| \geq 0$. Also $|x| = 0$ if and only if x is 0.
(b) We have $|x + y| \leq |x| + |y|$.
(c) We have the inequalities $-y \leq x \leq y$ if and only if $y \geq |x|$. In particular, we have $-|x| \leq x \leq |x|$.
(d) We have $|xy| = |x||y|$. In particular, $|-x| = |x|$.
(e) We have $d(x, y) \geq 0$. Also, $d(x, y) = 0$ if and only if $x = y$.
(f) $d(x, y) = d(y, x)$.
(g) $d(x, z) \leq d(x, y) + d(y, z)$.

Solution. (a). Part I ($|x| \geq 0$):
Case I ($x > 0$): in this case, x is positive; hence, $|x| = x > 0$.
Case II ($x < 0$): in this case, x is negative; hence, $|x| = -x$. Since x is negative, $x = -d$ for some positive rational d. Hence $|x| = -(-d) = (-1)(-1)(d) = d > 0$.
Case III ($x = 0$): Then $|x| = 0 \geq 0$.

[3]We can do this due to the density of the rationals in the reals.

Part II:

($\implies$): suppose that $|x| = 0$. Assume that in addition, $x > 0$. By definition of absolute value, $|x| = x > 0$; by trichotomy of order, $|x|$ cannot both equal zero and be greater than zero; hence, we get a contradiction, so $x \not> 0$. Now assume that in addition, $x < 0$. By definition of absolute value, $|x| = -x$; by Part I, $|x| \geq 0$. Thus, either $|x| = 0$ or $|x| > 0$. But if $|x| = 0$, then because $|x| = -x$, $x = -|x| = -0 = 0$, a contradiction. Hence, if $|x| = 0$, $x \not> 0$ and $x \not< 0$, so by trichotomy, $x = 0$.

($\impliedby$): suppose that $x = 0$. Then $|x| = x = 0$ by definition.

(b). If $x = 0$, then $|x+y| = |0+y| = |y| = 0+|y| = |0|+|y| = |x|+|y|$, with an identical argument holding if $y = 0$. Hence, we only need to consider the cases where x and y are positive or negative. Without loss of generality, assume $y > x$.

Case I ($y > x > 0$): Since y and x are both positive, $x + y$ is also positive, so $|x + y| = x + y$, $|x| = x$, and $|y| = y$. Hence, $|x + y| = |x| + |y| \implies |x + y| \leq |x| + |y|$.

Case II ($y > 0 > x$): Since $y > x$, by properties of order, $y + x > 0$. Hence, $|x+y| = x+y$. Since $y > 0$ and $x < 0$, $|y| = y$ and $|x| = -x$, respectively. Thus, suffices to show that $x+y \leq y-x$. Since x is negative, $x = -d$ for some positive rational d. Thus, suffices to show that $y - d \leq y - (-d) = y + d$, which is true by properties of order.

Case III ($0 > y > x$): $y = -c$ for some positive rational c, and $x = -d$ for some positive rational d. Hence $|x+y| = |-c-d| = |-(c+d)|$, and since $c+d$ is positive, $-(c+d)$ is negative, so $|-(c+d)| = -(-(c+d)) = (-1)(-1)(c+d) = c+d$. Also, $|x| = |-d| = d$, and $|y| = |-c| = c$. But $c+d \leq c+d$, so $|-(c+d)| \leq |x|+|y|$, so $|x + y| \leq |x| + |y|$.

(c). ($\implies$): Suppose that $-y \leq x \leq y$. We have three cases:

Case I ($x = 0$): Thus $-y \leq 0 \leq y$. But $|x| = 0$, and $y \geq 0$, so $y \geq |x|$.

Case II ($x > 0$): $|x| = x$; thus, suffices to show that $y \geq x$. But this is given.

Case III ($x < 0$): $|x| = -x$; thus, suffices to show that $y \geq -x$. We know that $-y \leq x$; by properties of order, $-(-y) \geq -x \implies y \geq -x$.

($\impliedby$): By (a), $|x| \geq 0$, so $y \geq 0$. We have three natural cases:

Case I ($x = 0$): In this case, $y \geq 0 \implies y \geq x$. By properties of order, $y \geq x \implies -y \leq -x = -0 = 0 = x$. hence $-y \leq x \leq y$.

Case II ($x > 0$): In this case, $|x| = x$, so $y \geq x$. By properties of order, $-y \leq -x$. Since x is positive, $-x < x$ by properties of order (since x is positive), so $-y \leq x \leq y$.

Case III ($x < 0$): In this case, $x = -d$ for some positive rational d. Hence $|x| = -x = -(-d) = d$. Thus $y \geq d$. By properties of order, $-y \leq -d$. Thus $-y \leq x$. Since $-y \leq x$ and $y \geq d$, suffices to show that $x \leq d$. But $x = -d \leq d$ is true since d is positive, so we are done.

(d). If $x = 0$, then $|xy| = |0y| = |0| = 0 = 0 \cdot |y| = |0||y| = |x||y|$; an identical argument holds when $y = 0$. Thus, we can assume that x and y are nonzero. Without loss of generality, let $y > x$. Then we have three cases:

Case I ($y > x > 0$): In this case, x and y are positive, so xy is positive; thus, $|xy| = xy$, $|x| = x$, and $|y| = y$. Since $xy = x \cdot y$, $|xy| = |x||y|$.

Case II ($y > 0 > x$): In this case, y is positive, and $x = -d$ for some positive rational d. Hence xy is negative; in particular, $xy = -dy = -(dy)$, where dy is a positive rational since d and y are both positive rationals. Thus $|xy| = -(xy) = -(-dy) = dy$. Since x is negative, $|x| = -x = -(-d) = d$; since y is positive, $|y| = y$. Combining the two, we get that $|x||y| = dy = |xy|$.

Case III ($0 > y > x$): Since x and y are negative, $x = -d$ and $y = -c$ for positive rationals d and c, respectively. Hence $xy = (-d)(-c) = (-1)d(-1)c = dc$; thus, xy is positive, so $|xy| = xy = dc$. Since x and y are negative, $|x| = -x = -(-d) = d$, and $|y| = -y = -(-c) = c$. Hence, $|xy| = dc = |x||y|$.

(e). By definition, $d(x, y) = |x - y|$. Since $x - y$ is a rational number, by (a), $|x - y| \geq 0$. In addition, by (a), $|x - y| = 0$ if and only if $x - y = 0$. But $d(x, y) = |x - y|$, and $x - y = 0 \iff x = y$, so $d(x, y) = 0 \iff x = y$.

(f). $d(x, y) = |x - y| = |-(y - x)| = |y - x| = d(y, x)$, where we used part (d) for the third equality.

(g). Let $a = x - y$, and $b = y - z$. By (b), $|a + b| \leq |a| + |b|$. Hence, $|x - y + y - z| \leq |x - y| + |y - z|$. Thus, $|x - z| \leq d(x, y) + d(y, z)$. Thus, $d(x, z) \leq d(x, y) + d(y, z)$. □

Problem (4.3.3)**.** Prove **Proposition 4.3.10**: Let x, y be rational numbers, and let n, m be natural numbers.

(a) We have $x^n x^m = x^{n+m}$, $(x^n)^m = x^{nm}$, and $(xy)^n = x^n y^n$.
(b) Suppose $n > 0$. Then we have $x^n = 0$ if and only if $x = 0$.
(c) If $x \geq y \geq 0$, the $x^n \geq y^n \geq 0$. If $x > y \geq 0$ and $n > 0$, then $x^n > y^n \geq 0$.
(d) We have $|x^n| = |x|^n$.

Solution. (a). For the first part, n and m are, conveniently, naturals, so we can fix n and induct on m.

Base case ($m = 0$): $x^n x^0 = x^n 1 = x^n = x^{n+0}$.

Inductive case: suppose $x^n x^m = x^{n+m}$. Then $x^n x^{m++} = x^n x^m x$ by definition of exponentiation, which equals $x^{n+m} x$ by the inductive hypothesis, which equals $x^{(n+m)++}$ by the definition of exponentiation, which closes the induction.

For the second part, we do the same thing:

Base case ($m = 0$): $(x^n)^m = (x^n)^0 = 1 = x^0 = x^{n0} = x^{nm}$.

Inductive step: suppose $(x^n)^m = x^{nm}$. Then we get that

$$\begin{aligned}(x^n)^{m++} &= (x^n)^m \cdot x^n \\ &= x^{nm} \cdot x^n \\ &= x^{nm+n} && \text{(By part I)} \\ &= x^{n \times (m++)}\end{aligned}$$

which closes the induction.

For the last part, we do the same thing, but we induct on n:

Base case ($n = 0$): $(xy)^n = (xy)^0 = 1 = 1 \cdot 1 = x^0 y^0 = x^n y^n$.

Inductive step: suppose that $(xy)^n = x^n y^n$. Then we have that

$$\begin{aligned}(xy)^{n++} &= (xy)^n (xy) \\ &= x^n y^n xy \\ &= x^n x y^n y \\ &= x^{n++} y^{n++}\end{aligned}$$

which closes the induction.

(b). ($\Longrightarrow$): suppose $x^n = 0$; we want to show that $x = 0$. Let's do this by induction!

Base case ($n = 1$): we know that $x^1 = 0$; hence, $x^{0++} = 0$, so $x^0 \cdot x = 0$, so $1 \cdot x = 0$. We know at least one of $1, x$ must be zero by one of our lemmas of rational numbers; hence, $x = 0$.

Inductive step: suppose $x^n = 0 \implies x = 0$. Then $x^{n++} = 0 \implies x^n \cdot x = 0$, which implies that either x^n is zero or x is zero (or both). In the latter case, we're done. In the former case, x^n is zero so $x = 0$ by the inductive hypothesis; which closes the induction.

($\Longleftarrow$): Since $n > 0$, $n = d++$ for some natural d. If $x = 0$, $x^n = x^{d++} = x^d \cdot x = x^d \cdot 0 = 0$.

(c). We do the first part by inducting on n.

Base case ($n = 0$): Clearly $1 \geq 1 \geq 0$, so $x^n \geq y^n \geq 0$.

Inductive step: suppose that $x^n \geq y^n \geq 0$. Since $y^n \geq 0$ by the inductive hypothesis and $y \geq 0$ by assumption, $y^{n++} = y^n \times y \geq 0$. Since $x^n \geq y^n$ by the inductive hypothesis and $x \geq y$ by assumption, $x^{n++} = x^n x \geq y^n y = y^{n++}$ by properties of order.

The second part is identical to the first part, except we start the induction with $n = 1$ and observe that if $a > b$ and $c > d$, then $ac > bd$.

(d). Let's do this by induction. If we're lucky, we won't need to do casework.

Base case ($n = 0$): $|x^0| = |1| = 1 = |x|^0 = |x|^n$.

Inductive step: suppose $|x^n| = |x|^n$. Then $|x^{n++}| = |x^n x| = |x^n||x| = |x|^n|x| = |x|^{n++}$, where we used properties of absolute value and the inductive hypothesis at the second and third equivalences, respectively. □

Problem (4.3.4)**.** Prove **Proposition 4.3.12**: Prove **Proposition 4.3.10** for integers instead of rationals.

Solution. (a). If n and m are positive, this follows from **Proposition 4.3.10**. If n is zero, $x^n x^m = x^0 x^m = 1x^m = x^m = x^{0+m} = x^{n+m}$ where m is zero holds identically; $(x^0)^m = 1^m = 1 = x^0 = x^{0m} = x^{nm}$; $(xy)^0 = 1 = 1 \cdot 1 = x^0 y^0$. If m is negative, then $m = -d$ for some positive integer d, so all the properties hold for n and d. The negative sign is equivalent at the end.

(b). Same argument as (a).

(c). Same argument as (b).

(d). Same argument as (c). □

Problem (4.3.5)**.** Prove that $2^N \geq N$ for all positive integers N.

Proof. We proceed by induction (we can do this because positive integers=positive naturals, where induction holds).

Base case ($n = 1$): $2^1 = 2^0 \cdot 2 = 1 \cdot 2 = 2 \geq 1$.

Inductive step: suppose $2^N \geq N$. Then $2^{N++} = 2^N \cdot 2 \geq N \cdot 2$ by the inductive hypothesis. Thus, suffices to show that $N \cdot 2 \geq N++$. We prove this using induction:

Base case ($n = 1$): $N \cdot 2 = 1 \cdot 2 = 2 \geq 2 = 1++ = N++$.

Inductive step: suppose $N \cdot 2 \geq N++$. We want to show that $N++ \cdot 2 \geq (N++)++$. We do this as follows:

$$\begin{aligned} N++ \cdot 2 &= (N+1) \cdot 2 \\ &= N \cdot 2 + 1 \cdot 2 \\ &= N \cdot 2 + 2 \\ &\geq N++ + 2 && \text{(By the inductive hypothesis)} \end{aligned}$$

$$= N + + + 1 + 1$$
$$= (N + +) + + + 1$$
$$\geq (N + +) + +.$$

This closes both inductions. □

Problem (6)**.** Prove for natural n, rational b, and rational $p \geq 0$, that if $p^n < b$ then there is a rational $q > p$ so that $q^n < b$.

Proof. Consider the number $x \in \mathbb{R}$ such that $x^n = b$.

Claim 0.2. If $0 < a^n < b^n$ with a and b positive rationals, and $n > 0$, then $a < b$.

Proof. We prove this via induction.

Base case ($n = 1$): Clearly $a < b \implies a < b$.

Inductive step: suppose that $a^n < b^n \implies a < b$. Then if $a^{n++} < b^{n++}$, since a and b are positive, $a^n a < b^n b \implies a^n < b^n \frac{b}{a}$. If $\frac{b}{a} > 1$, then by properties of order, $a^n < b^n$; by the induction hypothesis, $a < b$, a contradiction. If $\frac{b}{a} = 1$, then $b = a$, then $a^n = b^n$, so $a^{n++} = b^{n++}$, contradicting trichotomy. Hence, $\frac{a}{b} < 1$, which means that $a < b$. □

Using the density of the rationals in the reals, we can □

Problem (7)**.** Suppose $\mathbb{R}_{\text{other}} \supseteq \mathbb{Q}, \geq_{\text{other}}$ is a linear order on $\mathbb{R}_{\text{other}}$ agreeing with the usual order on $\mathbb{Q}$. Suppose $\mathbb{R}$ with $\leq_{\text{other}}$ is Dedekind complete, Archimedean, and the rationals are dense in $\mathbb{R}_{\text{other}}$. Prove that $\mathbb{R}_{\text{other}}$ is isomorphic to $\mathbb{R}$ over the rationals, meaning there is a bijection $f : \mathbb{R} \to \mathbb{R}_{\text{other}}$ so that $f|_{\mathbb{Q}}$ is the identity, and $x \leq y$ iff $f(x) \leq_{\text{other}} f(y)$.