# Homework #1 Solutions

**1.1.2.** Note that every number of the form $a - bk$ with $k \in \mathbf{Z}$ is an integer, because the set of integers is closed under addition and multiplication. Let $S$ be the set of all such integers, i.e., all the numbers of the form $a - bk$ with $k \in \mathbf{Z}$, which are *positive*. We claim that $S \neq \emptyset$. Indeed, because $a$ and $b$ are positive by assumption, if we take $k = -1$, then $a - bk = a + b$ is positive, so $a + b \in S$. Therefore $S$ is a nonempty set of positive integers, so, by the well-ordering property, $S$ has has a smallest element, and this is the desired positive integer.

**1.1.4.** (a) This is true. Let $\alpha$ be a rational number and $\beta$ an irrational number, and suppose that $\alpha + \beta$ is rational. Because the set of rational numbers is closed under subtraction, it follows that $\beta = (\alpha + \beta) - \alpha$ is rational, contrary to assumption. Thus $\alpha + \beta$ must be irrational.
(b) This is false. If $\beta$ is irrational, then $-\beta$ is irrational as well (otherwise $\beta$ would be rational), but $\beta + (-\beta) = \beta - \beta = 0$ is rational.
(c) This is false in general for a somewhat dumb reason. For any irrational number $\beta$, $0 \cdot \beta = 0$ is rational. However, if $\alpha$ is a *nonzero* rational number, then $\alpha\beta$ must be irrational. Indeed, because $\alpha \neq 0$, $\alpha^{-1}$ is a rational number, so if $\alpha\beta$ is rational, then $\beta = \alpha^{-1}(\alpha\beta)$ is rational as well (because the set of rational numbers is closed under multiplication), a contradiction.
(d) This is super false (if it were true, algebraic number theory would be dramatically less interesting). For example, the number $\sqrt{2}$ is irrational (we will give the classic proof of this fact later), but $\sqrt{2} \cdot \sqrt{2} = \sqrt{2}^2 = 2$ is rational.

**1.1.6.** Let $S$ be a nonempty set of negative integers, and define $T = \{-n : n \in S\}$. Then $T$ is a nonempty set of *positive* integers, so, by the well-ordering property, $T$ has a smallest element $t$. Since $t$ is of the form $-s$ for some $s \in S$, $-t = -(-s) = s \in S$, and we claim that $-t$ is the greatest element of $S$. To see this, let $n \in S$ be arbitrary. Then $-n \in T$, so, because $t$ is the smallest element of $T$, we have $t \leq -n$. It follows that $n \leq -t$. Thus $-t$ is greater than or equal to every element of $S$, so $-t$ is the greatest element of $S$, as claimed.

**1.1.8.** (a) We have $[-1/4] = -1$.
(b) We have $[-22/7] = [-3 - (1/7)] = -4$.
(c) We have $[5/4] = [1 + (1/4)] = 1$.
(d) We have $[[1/2]] = [0] = 0$.
(e) We have $[[3/2] + [-3/2]] = [1 + (-2)] = [-1] = -1$.
(f) We have $[3 - [1/2]] = [3 - 0] = [3] = 3$.

**1.1.16.** We will use the fact that, for any real number $y$, $[y]$ is the largest integer less than or equal to $y$. First, by definition, $[-x] \leq -x$, so $x \leq -[-x]$, and thus $-[-x]$ is an integer greater than or equal to $x$. Now let $m$ be any integer satisfying $x \leq m$. We then have $-m \leq -x$, so, by the maximality of $[-x]$, we must have $-m \leq [-x]$, which gives $-[-x] \leq m$. Therefore $-[-x]$ is the least integer greater than or equal to $x$.

*Date*: January 26, 2018.

**1.1.32.** We begin by subdividing the unit interval $[0,1]$ into the $n$ half-open subintervals $[(i-1)/(n+1), i/(n+1))$, $1 \le i \le n$, and the closed interval $[n/(n+1), 1]$ (so we have subdivided $[0,1]$ into $n+1$ subintervals). Consider the numbers $0 = \{0\alpha\}, \{\alpha\}, \dots, \{n\alpha\}, 1$, each of which lies in $[0,1]$. We will assume throughout that these numbers are distinct, explaining what to do if this assumption fails at the end of the proof (see also the remarks following the solution). Under this assumption, there are $n+2$ numbers, each of which must lie in one of the $n+1$ subintervals defined above. It follows that one of the subintervals must contain two of the numbers. We consider two cases, the first being that in which there is a subinterval $[(i-1)/(n+1), i/(n+1))$, $1 \le i \le n$, which contains two of the numbers. Since 1 does not lie in this subinterval, this means that there are integers $j, k$ with $0 \le j < k \le n$ such that $\{j\alpha\}$ and $\{k\alpha\}$ lie in $[(i-1)/(n+1), i/(n+1))$. Thus $|\{k\alpha\} - \{j\alpha\}| < 1/(n+1)$ (the distance between any two numbers in a half-open interval of length $1/(n+1)$ must be less than $1/(n+1)$). Taking $a = k - j$ and $b = [k\alpha] - [j\alpha]$, we have $a, b \in \mathbf{Z}$, $1 \le a \le n$, and

$$\begin{aligned} |a\alpha - b| &= |(k-j)\alpha - ([k\alpha] - [j\alpha])| \\ &= |(k\alpha - [k\alpha]) - (j\alpha - [j\alpha])| = |\{k\alpha\} - \{j\alpha\}| < \frac{1}{n+1}. \end{aligned}$$

Thus $a$ and $b$ have the desired properties, so we have addressed the first case. We now consider the complementary case in which the only subinterval containing two of the numbers is $[n/(n+1), 1]$. In this case, 0 is not in the subinterval, but 1 is, so there is an integer $a$ with $1 \le a \le n$ such that $|\{a\alpha\} - 1| \le 1/(n+1)$ (the distance between any two numbers in a closed interval of length $1/(n+1)$ is less than or equal to $1/(n+1)$). Letting $b = [a\alpha] + 1$, we have $b \in \mathbf{Z}$ and

$$|a\alpha - b| = |a\alpha - ([a\alpha] + 1)| = |(a\alpha - [a\alpha]) - 1| = |\{a\alpha\} - 1| \le \frac{1}{n+1}.$$

Thus $a$ and $b$ have the desired properties, completing the argument for the second case.

In the event that the numbers in the list $0 = \{0\alpha\}, \{\alpha\}, \dots, \{n\alpha\}, 1$ are not distinct, first observe that none of the fractional parts are equal to 1 (since by their definition, fractional parts of real numbers lie in $[0,1)$). So this means that there are integers $j, k$ with $0 \le j < k \le n$ such that $\{k\alpha\} = \{j\alpha\}$, whence $|\{k\alpha\} - \{j\alpha\}| = 0$. Taking $a = k - j$ and $b = [k\alpha] - [j\alpha]$, we have $a, b \in \mathbf{Z}$, $1 \le a \le n$, and the computation used in the proof of the first case above shows that $|a\alpha - b| = 0$. In particular $|a\alpha - b| \le 1/(n+1)$. This completes the proof in full generality.

The possibility that the numbers in the list $0 = \{0\alpha\}, \{\alpha\}, \dots, \{n\alpha\}, 1$ are not distinct in the proof for Exercise 1.1.32 is annoying (it is all right if you did not address it in your proof, but you should be aware that it is a possibility). In some sense, however, the possibility is uninteresting (almost by definition). The point is that the numbers can fail to be distinct only if $\alpha$ is rational. (If you look at the final portion of the proof, you will see that, when this occurs, we actually have $|a\alpha - b| = 0$, i.e., $a\alpha = b$, whence $\alpha = b/a$, so $\alpha$ is rational.) But Diophantine approximation is only interesting for *irrational* $\alpha$ (it is not very exciting to approximate a rational number by other rational numbers).

**1.1.34.** To simplify the writing of the proof, let us call an ordered pair $(q, p)$ consisting of a positive integer $q$ and an integer $p$ satisfying $|\alpha - (p/q)| \le 1/q^2$ *$\alpha$-good.* We first want to show that, if $q$ is a fixed positive integer, then there are at most finitely many $\alpha$-good pairs with first coordinate equal to $q$. Equivalently, we want to show that there are only finitely many integers $p$ such that $|\alpha - (p/q)| \leq 1/q^2$. To this end, assume that $p$ is an integer such that $(q, p)$ is $\alpha$-good, i.e., such that $|\alpha - (p/q)| \leq 1/q^2$. This last inequality may be rewritten as $-(1/q^2) \leq \alpha - (p/q) \leq 1/q^2$. Considering the first inequality $-(1/q^2) \leq \alpha - (p/q)$ and solving for $p$ gives the inequality

$$p \leq q\alpha + \frac{1}{q}.$$

Similarly, solving the inequality $\alpha - (p/q) \leq 1/q^2$ for $p$ yields

$$q\alpha - \frac{1}{q} \leq p.$$

Thus $p$ lies in the closed interval $[q\alpha - (1/q), q\alpha + (1/q)]$. The desired finiteness follows from this, because an interval of finite length can contain at most finitely many integers.

For our proof of the main assertion, we argue by contradiction. Therefore we will assume that there are only finitely many positive integers $q$ such that there exists an $\alpha$-good pair with first coordinate equal to $q$. By the claim established above, this means that there are only finitely many $\alpha$-good pairs. Now note that, because $\alpha$ is assumed to be irrational, for any $\alpha$-good pair $(q, p)$, the number $|q\alpha - p|$ is positive (any absolute value is nonnegative, and if $|q\alpha - p| = 0$, then $\alpha = p/q$ is rational, contrary to assumption). As there are only finitely many $\alpha$-good pairs, it follows that there are only finitely many such positive numbers. We may therefore choose a positive integer $n$ such that $1/n < |q\alpha - p|$ for all $\alpha$-good pairs $(q, p)$. (This is why we need to know that the number of $\alpha$-good pairs is finite. For an infinite set of positive numbers, such an integer $n$ may fail to exist. For example, if we consider the set of numbers of the form $1/2^m$ for $m \in \mathbf{Z}^+$, there does not exist a positive integer $n$ satisfying $1/n < 1/2^m$ for all such $m$.)

We now apply Dirichlet's approximation theorem to obtain integers $a, b$ with $1 \leq a \leq n$ and $|a\alpha - b| < 1/n$. As $a \leq n$, $1/n \leq 1/a$, so we may divide both sides of the previous inequality by $a$ to obtain $|\alpha - (b/a)| < 1/(na) \leq 1/a^2$. Thus $(a, b)$ is an $\alpha$-good pair. But this implies, by our choice of $n$ above, that $1/n < |a\alpha - b|$, a contradiction. Therefore our initial assumption that the set of positive integers $q$ in question is finite must be false, i.e., we may conclude that there are in fact infinitely many such positive integers $q$.