

Solutions to Homework 9, Math 310

For these problems, you may use any of the stated properties of natural numbers, integers and rational numbers in the hand-out (both proved and merely stated but not proved). But, mention the property you are using in some recognizable way (for example: lemma such and such, or state it or...). You could also use any of the induction methods we have done in class or previous homeworks.

- (1) Show that for any two rational numbers a, b , $|a - b| \geq ||a| - |b||$.

Proof. Since $||a| - |b|| = |a| - |b|$ or $|b| - |a|$, we only need to show that $|a - b| \geq |a| - |b|$ and $|a - b| \geq |b| - |a|$. To show the first, by triangle inequality, we have $|a| = |a - b + b| \leq |a - b| + |b|$ and thus we get $|a - b| \geq |a| - |b|$. For the second, similarly, we have $|b| = |b - a + a| \leq |b - a| + |a|$ and since $|a - b| = |b - a|$, we get, $|a - b| \geq |b| - |a|$, which proves the result. \square

- (2) Let $S \subset \mathbb{Z}$ be a non-empty subset which is bounded below. That is, there exists an integer M so that for all $s \in S$, $s \geq M$. Show that S has a least element. Give an example (with a reasonable argument) where similar statement fails for a subset of \mathbb{Q} .

Proof. We have done this in class. Consider the set $T = \{s - M + 1 \mid s \in S\}$. Since $s \geq M$ for all $s \in S$, we see that $s - M + 1 \in \mathbb{N}$ for all $s \in S$ and thus T is a non-empty subset of \mathbb{N} . By Theorem 1.1, T has a minimal element say, t . One easily checks then, $t + M - 1 \in S$ is the least element of S . \square

- (3) Show that if $a, b \in \mathbb{Z}$ with $ab = 0$, then a or b is zero.

Proof. This is Property 14 stated in the notes on page 10, without proof. If you quote it, it is fine, but do make sure that you know how to prove it.

We may assume that $a \neq 0$ and then show that if $ab = 0$, then $b = 0$. Since $a \neq 0$, we must have by well-ordering (which also is true for \mathbb{Z}, \mathbb{Q} , easily) either $a < 0$ or $a > 0$. The two cases are similar. So, let us assume that $a > 0$. Thus by lemma 2.3, $a \in \mathbb{N}$. If $b \neq 0$, similarly, we get that $b \in \mathbb{N}$ or $-b \in \mathbb{N}$. But, $ab = 0$ means $a(-b) = 0$ and thus we get that $ac = 0$ if $c \in \mathbb{N}$ where $c = \pm b$. This is not possible, since $ac \in \mathbb{N}$ and $0 \notin \mathbb{N}$. \square

- (4) Use division algorithm and the usual definition of prime number (You should be able to prove the division algorithm from the properties we have stated, though you may assume it for this

problem) show that given a prime number p and any $a \in \mathbb{N}$, there exists unique integers a_0, a_1, \dots, a_k for some k with $0 \leq a_i < p$ such that $a = a_0 + a_1p + a_2p^2 + \dots + a_kp^k$. (This is usually called the p -adic expansion of a). What would happen if we tried to do the same for any $a \in \mathbb{Z}$?

Proof. Proof is by induction on a . So, let $P(a)$ be the predicate that $a = a_0 + a_1p + a_2p^2 + \dots + a_kp^k$ for some k and $0 \leq a_i < p$.

If $a < p$, we may take $a_0 = a$ and $a_i = 0$ for $i > 0$. So, $P(a)$ is true for all $a < p$. Next we will show that $(P(a) \forall a < N) \Rightarrow P(N)$, which will finish the proof by one of our induction principles.

So assume the result for all $a \in \mathbb{N}$ with $a < N$. We will show that $P(N)$ is true. By division algorithm, we have

$$N = qp + a_0 \tag{1}$$

for some $q, a_0 \in \mathbb{Z}$ with $q \geq 0$ and $0 \leq a_0 < p$. If $q = 0$, then $N < p$ and we have seen that $P(N)$ is true. So, we may assume that $q \in \mathbb{N}$. If $q \geq N$, then $qp \geq Np > N$ and thus $N = qp + a_0 > N$, which is impossible. So, $q < N$ and thus by induction, we have a_1, \dots, a_k with $0 \leq a_i < p$ so that $q = a_1 + a_2p + a_3p^2 + \dots + a_kp^{k-1}$. Substituting this in equation 1, we get,

$$\begin{aligned} N &= qp + a_0 = a_0 + p(a_1 + a_2p + \dots + a_kp^{k-1}) \\ &= a_0 + a_1p + a_2p^2 + \dots + a_kp^k. \end{aligned}$$

with $0 \leq a_i < p$, proving that $P(N)$ is true. Thus by induction, we have proved what we set out to prove.

If $a \in \mathbb{Z}$ with $a < 0$, we can use division algorithm as before, but we see that there can not be any k such that $a = \sum_{i=0}^k a_i p^i$, since the right hand side is positive while the left side is negative. So, the only possibility is that we have an infinite sum (purely formally, with no convergence in the usual sense). If you learn more number theory, such expressions will be made sense of (convergence in an appropriate context) and they are called p -adic numbers. \square

- (5) For any rational number r , define the set $S(r)$ to be, $S(r) = \{a \in \mathbb{N} \mid ar \in \mathbb{Z}\}$. Show that for rational numbers r, s , the intersection of $S(r)$ and $S(s)$ is not empty. Also, show that if $a \in S(r)$ and $b \in S(s)$ then $ab \in S(rs)$.

Proof. If $a \in S(r)$, and $b \in S(s)$, by definition, we have $ar \in \mathbb{Z}$ and $bs \in \mathbb{Z}$ and thus $abrs \in \mathbb{Z}$, showing that $ab \in S(rs)$. By lemma 3.1, for any $r \in \mathbb{Q}$, $S(r) \neq \emptyset$. So, let a, b as before (which exists since they are non-empty). Then I claim that $ab \in S(r) \cap S(s)$, proving our result. Since $ar \in \mathbb{Z}$ and $b \in \mathbb{N}$, we have $abr \in \mathbb{Z}$. So, $ab \in S(r)$. An identical argument shows that $ab \in S(s)$ and thus $ab \in S(r) \cap S(s)$. \square

- (6) Let $S(r)$ for a rational number r be defined as above. Show that there exists an $n \in \mathbb{N}$ (depending on r) such that $S(r) = \{an \mid a \in \mathbb{N}\}$. Define a relation on \mathbb{Q} as follows. If $r, s \in \mathbb{Q}$, $r \sim s$ if $S(r) = S(s)$. Show that this an equivalence relation.

Proof. Since $S(r) \neq \emptyset$, by induction we have a least element $n \in S(r)$. Let $A = \{an \mid a \in \mathbb{N}\}$. Since $nr \in \mathbb{Z}$, we see that for any $a \in \mathbb{N}$, $(an)r = a(nr) \in \mathbb{Z}$ and thus $an \in S(r)$ proving $A \subset S(r)$.

Now, let $b \in S(r)$. By division algorithm, we can write $b = qn + t$ with $q, t \in \mathbb{Z}$ and $0 \leq t < n$. If $q \leq 0$, we get $b \leq t < n$. But, we have assumed that n is the least element in $S(r)$ and thus $b \geq n$. So, we get that $q > 0$ and thus $q \in \mathbb{N}$. Since $br \in \mathbb{Z}$ and $qnr \in \mathbb{Z}$, we get $tr = br - qnr \in \mathbb{Z}$. If $t > 0$, we get $t \in S(r)$, but $t < n$ contradicting the minimality of n . Thus $t = 0$ and hence $b = qn \in A$. This shows that $S(r) = A$.

The above is an equivalence relation is stright forward. Clearly $r \sim r$ since $S(r) = S(r)$. If $r \sim s$, we have $S(r) = S(s)$ and then clearly $s \sim r$. Similarly, if $r \sim s, s \sim t$, then we have $S(r) = S(s)$ and $S(s) = S(t)$ implying $S(r) = S(t)$ which in turn implies that $r \sim t$. \square