Exercise 11. Given $m \in \mathbb{Z}$, we say that m is *even* if $m/2 \in \mathbb{Z}$, and m is *odd* otherwise.

(a) Show that if m is odd, $m = 2n + 1$ for some $n \in \mathbb{Z}$. [*Hint:* choose n such that $n < m/2 < n + 1$.]

(b) Show that if p and q are odd, so are $p \cdot q$ and p^n, for any $n \in \mathbb{Z}_+$.

(c) Show that if $a > 0$ is rational, then $a = m/n$ for some $m, n \in \mathbb{Z}_+$ where not both m and n are even. [*Hint:* Let n be the smallest element of the set $\{x \mid x \in \mathbb{Z}_+ \text{ and } x \cdot a \in \mathbb{Z}_+\}$.]

(d) *Theorem:* $\sqrt{2}$ *is irrational.*

Proof.

(a) Let $m \in \mathbb{Z}$ be an odd number; then $m/2 \notin \mathbb{Z}$, so that by exercise 1.4.9-b) there exists a unique $n \in \mathbb{Z}$ such that $n < m/2 < n + 1$. This implies that $2n < m < 2n + 2$. The only integer verifying this inequality is $2n + 1$, so $m = 2n + 1$.

(b) Let $p, q \in \mathbb{Z}$ be odd numbers. From the previous point, there exist $a, b \in \mathbb{Z}$ such that $p = 2a + 1$ and $q = 2b + 1$. This gives us $p \cdot q = (2a+1)(2b+1) = 2\,(a\,(2b+1)+b)+1$, so that $p \cdot q = 2m + 1$ for some $m \in \mathbb{Z}$, and thus is odd.

   Let $A = \{n \in \mathbb{Z} \mid p^n \text{ is odd}\}$. Since p is odd, we have $1 \in A$. Suppose that $n \in \mathbb{Z}_+$ such that $n \in A$. Then p^n is odd, and $p^{n+1} = p \cdot p^n$ is the product of two odd numbers. Therefore p^{n+1} is odd, so that $n+1 \in A$ and A is inductive. We conclude that $A = \mathbb{Z}_+$, which is the expected result.

(c) Let $a > 0$ be a rational number and $A = \{x \in \mathbb{Z}_+ \mid x \cdot a \in \mathbb{Z}_+\}$. There exist 2 integers p, q with $q \neq 0$ such that $a = p/q$. We have $q \cdot a = p$ and $a > 0$, so that p and q are either both positive, or both negative. Let us further suppose that $p > 0$ and $q > 0$. Then $q \cdot a \in A$, so that $A \neq \varnothing$. Therefore A has a smallest element $m \in \mathbb{Z}_+$. We have $m \cdot a = n \in \mathbb{Z}_+$. If both m and n are even, then $(m/2) \cdot a = n/2 \in \mathbb{Z}_+$, so that $m/2 \in A$. Since $m > 0$, this leads to $m/2 < m$, which contradicts the fact that m is the smallest element of A. Therefore $a = n/m$ where not both m and n are even.

(d) Suppose that $\sqrt{2} = n/m$ with n and m not both even. Then $2m^2 = n^2$, so that n^2 is even. If n were odd, then n^2 would also be odd; so n is even, and there exists $p \in \mathbb{Z}$ such that $n = 2p$. From this we deduce that $4p^2 = 2m^2$, so that $2p^2 = m^2$. Therefore m^2 is even, and so is m. This is a contradiction with n and m not being both even, so $\sqrt{2}$ is irrational. $\square$