Numbers

John M. Morrison

January 13, 2022

Contents

0 The Nonnegative Integers

Here is our starting point in the numerical world. We begin with the most basic mathematical activity, counting. We will denote by $\mathbb{N}$ the set of all positive integers and use the notaton $\mathbb{N}_0$ for the set of all nonnegative integers.

We shall not repeat Peano's construction of the positive integers here. We will begin with the notion of mathematical induction. This says the following.

Induction Let S be a subset of the positive integers such that $1 \in S$ and that for all $n \in \mathbb{N}$, $n \in S \implies n+1 \in S$. Then $S = \mathbb{N}$.

This principle is a workhorse tool for proving results about the positive integers. Here is an example of a proof done using induction.

Theorem 1. *For any positive integer n,*

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

Proof. Let S denote the set of all positive integers for which this predicate holds. We begin by checking if $1 \in S$. We know that

$$\sum_{k=1}^{1} k = 1$$

and

$$\frac{1(1+1)}{2} = 1,$$

so we have that case covered.

Now assume that $n \in S$. This tells us that

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

Adding n + 1 to both sides of this equation, we see the following

$$\sum_{k=1}^{n+1} k = n+1+\sum_{k=1}^{n} k = n+1+\frac{n(n+1)}{2}.$$

Now clean up the right-hand side to see that

$$n+1+\frac{n(n+1)}{2} = \frac{2(n+1)+n(n+1)}{2} = \frac{(n+1)(n+2)}{2}.$$

It immediately follows that $n+1 \in S$, so by induction $S = \mathbb{N}$. □

Now for some post-proof commentary. Checking the case of $n = 1$ is often called checking the base case. Checking base cases is an essential part of an induction argument.

Then comes the "induction step." You *assume* as given that the theorem holds for n and you use it, along with other arguments, to show that the theorem holds for $n+1$.

On the Math Stackexchange, this question was asked, "What is the purpose of the first test in an inductive proof?" Here is my answer to that inquiry.

> Imagine a pond with an infinite linear progression of lily pads. You have a frog who, if he hops on one pad, he is guaranteed to hop on the next one. If he hops on the first pad, he'll visit them all. But if he never makes the first lily pad, all bets are off.

One other remark is in order here. There is nothing special abut 1 as the base case of induction. If you can do the induction step, and if, say, you can prove your assertion for $n = 3$, then induction gives you the result for $n \geq 3$. Why? Think about Mr. Frog. If he appears on pad 3, he will visit all of the pads after 3.

You will also notice some legerdemain with sigma notation. These identities are often very useful.

$$\sum_{k=1}^{n} a_k = a_n + \sum_{k=1}^{n-1} a_k = a_1 + \sum_{k=1}^{n} a_k.$$

They hold because all three items in the inequality represent the sum of the a_k, $1 \leq k \leq n$.

Exercises

1. Show that for an integer $n \geq 1$,

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}.$$

2. Show that for an integer $n \geq 1$,

$$\sum_{k=0}^{n} \lambda^k = \frac{1-\lambda^{n+1}}{1-\lambda}.$$

   for any $\lambda \neq 1$.

3. Prove the *telescoping sum principle*, which says for any integer $n \geq 1$,

$$\sum_{k=1} na_k - a_{k-1} = a_n - a_0,$$

   for any numbers $a_0, a_1, \cdots a_n$.

Induction has a couple of other guises which we will now discuss. One of these is the *well ordering principle*. This simply states that every nonvoid subset of the positive integers has a least element. We can prove this with induction.

Theorem 2 (Well Ordering Principle)**.** *Every nonvoid subset of the positive integers has a least element.*

Proof. We argue via the contrapositive. Let S be a subset of the integers with no least element and denote by T all elements of $\mathbb{N}$ not in S. Were $1 \in S$, then 1 would be the least element of S, so we know that $1 \in T$.

Let us assume all integers less than or equal to n are in T. Then $k \notin S$, $1 \leq k \leq n$. Were $n+1 \in S$, $n+1$ would necessarily be the least element of S; we must have $n+1 \in T$.

By induction, $T = \mathbb{N},$, so S is an empty set. We just showed that the only subset of the positive integers lacking a least element is the null set, proving the theorem. □

Embedded in this proof is a second version of induction called `strong induction`.

Strong Induction Let S be a set of positive integers so that $1 \in S$ and so $\{1, 2, 3, 4, ..n\} \subseteq S \implies n+1 \in S$. Then $S = \mathbb{N}$.

This can be proved using plain-vanilla induction. It is sometimes a useful way to formulate an induction proof.

Now let us show an application of the well-ordering principle. We say that a positive integer $n \geq 2$ is *prime* if its only divisors are 1 and itself.

Theorem 3. *Every positive integer can be written as a product of zero or more primes*

Proof. Note that 1 is the product of an the empty set, so it is the product of no primes.

We argue by the contrapositive. Let S be the set of all integers not representable as a product of primes. Were S nonvoid, it would have a least element n. If n were prime, than n is the product of the collection containing itself. Hence, n is not prime.

As a result, we can write $n = ab$, where a and b are divisors of n and $a, b \geq 2$. Each of the two factors are finite products of primes, so n must also be a finite product of primes. Therefore $n \notin S$, a contradiction. The set S has no least element and is therefore void. □

1 Divisibility of Integers

We begin by establishing some definitions and basic results. We will see that the well-ordering principle is hugely useful here. We will use the notation $\mathbb{Z}$ to denote the set of all integers.

You might ask, why not use the letter I? This notation was confected by a German-speaking mathematician, and the German word zahlen means, "to count."

If a and b are integers, we will say that a *divides* b if for some integer q, we have $b = aq$. For this, we will use the standard notation $a \mid b$.The integer q is the *quotient* of b by a. In this case we say that a and q are *divisors* of b.

Theorem 4. *Suppose d, a, b, x, y are integers and $d \neq 0$. The following hold*

1. *If $d \mid a$ and $d \mid b$, then $d \mid ax + by$.*
2. *If $d \mid a$, $d \mid -a$ and $d \mid |a|$.*
3. *If $d \mid a$ and $a \mid d$, then $a = \pm d$.*
4. *$d \mid 0$.*
5. *$1 \mid a$.*

We will now establish the famed Divison Algorithm.

Theorem 5. *Suppose that $a \in \mathbb{N}$ $b \in \mathbb{Z}$ Then there exist unique integers q and r so that $b = aq + r$ and $0 \leq r < a$.*

Proof. Put $R = \{b - an | n \in \mathbb{Z}, b - an \geq 0\}$. Let us begin by showing that R is nonvoid. Put $n = -|b|$. Then $b - an = b + a|b| \geq b + |b| \geq 0$. We see that R is nonvoid. By well ordering, it has a least nonnegative element, which we will call r. Also, we can write $r = b - aq$ for some integer q. We see that $b = aq + r$.

Next we show that $r < a$. Suppose by way of contradiction this is not true. Then $a \geq r$, so $r - a \geq 0$. But we have $r - a = b - aq - a = b - a(q + 1)$. We just showed that $r - a \in R$, a contradiction of the minimality of r. We conclude $r < a$. This establishes existence.

Now for uniqueness. Write $b = aq + r = aq' + r'$, where $0 \leq r, r' < a$. Then $r - r' = a(q - q')$, so $a \mid r - r'$ and therefore $a \mid |r - r'| < r$. This can only occur if $r = r'$ Since $r = r'$, we can conclude $q = q'$. □

Exercises

1. Prove the first theorem.
2. Show that if $d \mid a$ and $a, d > 0$ then $0 < d \leq a$.

The Division algoritm allows us to define a new function mod which we will represent as an infix binary operator. If $b = aq + r$ and $0 \leq r < a$, then we write $b \mod a = r$. Modern computer languages bake this in as a fundamental arithmetic operation. A common notation you will see for it is `b % a`.

2 The gcd Function

Suppose a and b are integers. The nonzero integer d is a *common divisor* of a and b if $d \mid a$ and $d \mid b$. Every nonzero integer has only finitely many divisors, so the common divisors of a and b constitute a finite set. It is a nonvoid set because 1 is a common divisor of a and b. Hence, there is a greatest common divisor of any two integers, provided at least one of the integers is not zero.

What about gcd(0,0)? Any integer divides zero, so there clearly cannot be a greatest one.

The domain of the gcd function is the set of all pairs of integers with at least one member of the pair not being 0.

Let us state a basic result and leave the proof as an exercise.

Theorem 6. *1. For an integer a, $\gcd(a, 0) = |a|$.*

2. For integers a and b, $\gcd(a, b) = gcd(b, a)$.

3. For integers a and b, $\gcd(a, -b) = gcd(a, b) = \gcd(|a|, |b|)$. To wit, the gcd function cares nothing about the signs of its arguments.

We are going to develop an apparatus for computing greatest commond divisors that is fast and efficient. You are encouraged to try to implment this in code.

Lemma 1. *Suppose that a, b, q, and r are integers and that $b = aq + r$. Then $\gcd(a, b) = \gcd(a, r)$.*

Proof. Suppose d is a common divisor of a and b. Then $d \mid a$ and $d \mid b$, so $d \mid b - aq = r$. Every common divisor of a and b is a common divisor of a and r.

Conversely, suppose $d \mid a$ and $d \mid r$. Then $d \mid aq + r = b$. Every common divisor of a and r is a common divisor of a and b. Hence, $\gcd(a, b) = \gcd(a, r)$.

□

Note that the q and r are not necessrily the ones yielded up by the division algorithm, but those are ofen a very good choice. So we have this identity

$$\gcd(a, b) = \gcd(a, b \mod a).$$

Repeated application of this result is called *Euclid's Algorithm*. Here we will compute $\gcd(9995, 2172)$ in a Python interactive session. Note that `%` is the mod operator in Python.

```
>>> a = 9955
>>> b = 2172
```

```
>>> a % b
1267
>>> 2172 %1267
905
>>> 1267%905
362
>>> 905 % 362
181
>>> 362 % 181
0
```

What we can glean here is this chain of equalities.

$$\begin{aligned}\gcd(9955, 2172) = \gcd(2172, 1267) = \gcd(1267, 905) \\ = \gcd(905, 362) = \gcd(362, 181 = \gcd(181, 0).\end{aligned}$$

The result is $\gcd(9955, 2172) = 181$.

3 The Fundamental Theorem of Arithmetic

We shall develop the machinery necessary to show tht every positive integer is uniquely factorable into a finite product of prime numbers. What we know now is existence: Every positive integer is a product of a finite number of primes.

Lemma 2. *Suppose that d is a common divisor of a and b. Then* $\gcd(a, b) \mid d$.

Proof. Write $ds = a$, $dt = b$. □

To make this happen we begin by making an appeal to the well ordering property.

Theorem 7 (Bezout)**.** *Suppose that a, $b \in \mathbb{Z}$ and that at least one of these integers is not zero. Then there exist integers x and y so that*

$$ax + by = \gcd(x, y).$$

Proof. Put $S = \{ax + by | x, y \in \mathbb{Z}, ax + by > 0\}$. It is easy to check that note that without loss of generality, we can assume both a and b are nonnegative by pushing the negative onto the coefficents x and y.

This is a nonvoid subset of the integers; therefore it has a least element which we will name d. Note that since d is an "integer combination" of a and b, $\gcd(a, b) \mid d$. We choose the names x and y for our coefficients, so $ax + by = d$.

Now write $d = aq + r$, where $0 \leq r < a$. If $r = 0$, then $d|a$. By way of contradiction, assume not. Then $r = d - aq = ax + by - aq = a(x - q) + by$.

Since $r > 0$, we must have $r \in S$, contradicting the minimality of r. Therefore $r = 0$, so $d \mid a$. By symmetry, $d \mid b$. We know that d is a common divisor of a and b, so $d \leq \gcd(a, b)$. But $\gcd(a, b) \mid d$, so $\gcd(a, b) \leq d$, proving our result □

Corollary 1. *If* $\gcd(a, b) = 1$ *then there are integers* x *and* y *so that* $ax+by = 1$.

We will say that integers a and b are *relatively prime* if $\gcd(a, b) = 1$. This theorem is extremely useful when thinking about prime factorization.

Theorem 8. *Suppose that* p *is prime and that* $p \mid ab$. *Then* $p \mid a$ *or* $p \mid b$.

Proof. Assume that $p \nmid a$. Since the only divisors of p are 1 and p, $\gcd(a, p) = 1$. Write $ax + py = 1$. Now multiply by b and we see that

$$b = axb + bpy$$

Since $p \mid ab$ and $p \mid bpy$, $p \mid b$. □

Corollary 2. *If a prime divides a finite product of integers, it must divide at least one of the integers.*

Proof. This is an exercise in induction. □

4 Modular Arithmetic

Let n be a positive integer. We define the relation $a \equiv b \mod n$ on $\mathbb{Z}$ to be true when $d \mid a - b$. The integer n is called the *modulus*.

This relation is an equivalence on the integers. It is reflexive because any integer divides 0. Suppose $a \equiv b \mod n$. Then $d \mid a - b$, so $d \mid b - a$; we conclude that $b \equiv a \mod n$. The relation is symmetric. Now if we have $a \equiv b \mod n$ and $b \equiv c \mod n$, $d \mid a - b$ and $d|b - c$. Adding we see that $d \mid a - c$, so $a \equiv c \mod n$. The relation is transitive and is therefore an equivalence.

If $a \equiv b \mod n$, we say that a and b are *equivalent mod* n.

We denote by $mathbbZ/n\mathbb{Z}$ the equivalence classes on $\mathbb{Z}$ under equivalence mod n.

Theorem 9. *Suppose that* a_0, a_1, b_0 *and* b_1 *are integers,* $n \in \mathbb{N}$, *and that* $a_0 \equiv b_0 \mod n$ *an d* $a_1 \equiv b_1 \mod n$. *Then the following hold.*

1. $a_0 + b_0 \equiv a_1 + b_1 \mod n$
2. $a_0 b_0 \equiv a_1 b_1 \mod n$

Proof. The first assertion is done by addition. We have $d \mid a_0 - b_0$ and $d \mid a_1 - b_1$. Consequently,

$$d \mid a_0 - b_0 + a_1 - b_1 = (a_0 + b_0) - (a_1 + b_1),$$

so

$$a_0 + b_0 \equiv a_1 + b_1 \mod n$$

.

Now let us get the second assertion. Since $d \mid a_1 - a_0$, $d \mid a_1 b_0 - a_0 b_0$. Since $d \mid b_1 - b_0$, $d \mid a_1 b_0 - a_1 b_1$. By addition, we have

$$d \mid a_0 b_0 - a_1 b_1.$$

□

We can now do arithmetic on $\mathbb{Z}/n\mathbb{Z}$. We denote by $[a]$ the equivaence class of a mod n. We can define

$$[a] + [b] = [a + b].$$

Why can we get away with this? Select $\alpha \in [a]$ and $\beta \in [b]$. Then $\alpha \equiv a \mod n$ and $\beta \equiv b \mod n$. By the teorme, $\alpha + \beta \equiv a + b \mod n$.

A similar analysis (exercise) shows that we can define

$$[a][b] = [ab].$$

Suppose $a \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then we can write $b = nq + r$, where $0 \leq r < n$. Observe that $[b] = [r]$. Therefore

$$\mathbb{Z}/n\mathbb{Z} = \{[k] | 0 \leq k < n\}.$$

Let us look at $\mathbb{Z}/6\mathbb{Z}$. In the interest of typographical simplicity we write 1 instead of [1]. Here is an addition table.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Notice that every element has an additive inverese. For $0 < k < 6$, you have $[6 - k] + [k] = 0$. Note that [0] is its own additive inverse. This analysis can be generalized for any modulus $n \in \mathbb{N}$.

Let's look at multiplication.

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	4	1

Here is an alarming fact: $[2][3] = [0]$. This tells us that neither 2 nor 3 can have a multiplicative inverse (why?). Also, $[4][3] = [0]$. Observe that $[5]$ is its own multiplicative inverse, as is, obviusly $[1]$. An elmement $[k]$ is called a *zero divisor* if for some $[m]$, $[k][m] = [0]$.

Exercises

1. Show that a zero divisor in $\mathbb{Z}/n\mathbb{Z}$ cannot have a multiplicative inverse.
2. Make the multiplication table for $\mathbb{Z}/7\mathbb{Z}$. Do you see any zero divisors? Is there any element without a multiplicative inverse other than $[0]$?
3. Show that addition in $\mathbb{Z}/n\mathbb{Z}$ is commutative and associative.
4. Show that multiplication in $\mathbb{Z}/n\mathbb{Z}$ is commutative and associative.

We will now consider this question. Are there any elements in modular arithmetic other than zero divisors or elements having multiplicative inverses?

Suppose that in mod n arithmetic that k has a multiplicative inverse. Then we can find m so that $[k][m] = [1]$. This says that $n \mid km - 1$. Choose an integer q so that $nq = km - 1$. Then $nq + k(-m) = 1$. Consequently, $\gcd(k, n) = 1$.

Conversely, suppose $gcd(k, n) = 1$. Then by Bezout's theorem there exist x and y so that $kx + ny = 1$. Hence, $kx - 1 \equiv modn$, So $[k][x] = [1]$.

We have just proven this result.

Theorem 10. *Suppose $n \in \mathbb{N}$. Then $[k] \in \mathbb{Z}/n\mathbb{Z}$ has a multiplicative inverse if and only if* $\gcd(n, k) = 1$.

Corollary 3. *If p is a prime number, every nonzero element of $\mathbb{Z}/p\mathbb{Z}$ has a multiplicative inverse.*

Now suppose $n \in \mathbb{N}$ and that $k \in \mathbb{Z}/n\mathbb{Z}$ satisfies $\gcd(n, k) > 1$. Then we have $[m] \in \mathbb{Z}/n\mathbb{Z}$ so that $m \gcd(n, k) = n$. Then $[m][gcd(n, k)] = [0]$. Since we have $1 < m, \gcd(n, k) < n$, we have shown that $\gcd(n, k)$ is a zero divisor in $\mathbb{Z}/n\mathbb{Z}$. Hence (easy exerise), any multiple of $\gcd(n, k)$ is also a zero divisor in $\mathbb{Z}/n\mathbb{Z}$.

We have a dichotomy here. If $[k] \in \mathbb{Z}/n\mathbb{Z}$, then $[k]$ has a multiplicative inverse or it is a zero divior.

5 The Rational Numbers

Consider the set of all ordered pairs (p, q) of integers where $q \neq 0$. We define an eqivalence relation on this set by defining $(p, q) \sim (r, s)$ if $ps = qr$.

Exercises

1. If $c \neq 0$, show that $(cp, cq) \sim (p, q)$.
2. Show that $(0, p) \sim (0, 1)$ for any nonzero integer p.

A *rational number* is an equivalence class on $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ under this equivalnece. The set of all rational numbers is denoted by $\mathbb{Q}$.

Lemma 3. *Suppose that* $(a, b) \sim (p, q)$ *and that* $(c, d) \sim (r, s)$. *Then* $(aq + bp, bq) \sim (cs + dr, ds)$.

Proof. Run the computation in the definitiion.

$$(aq + bp)ds = adqs + bdps$$

and

$$bq(cs + dr) = bcqs + bdqr.$$

Now use the fact that $ad = bc$ and $qr = ps$ and we are done. □

We can now define addition on the rationals by

$$(a, b) + (p, q) = (aq + bp, bq).$$

Note that we can also define subtraction via

$$(a, b) + (p, q) = (aq - bp, bq).$$

Lemma 4. *Suppose that* $(a, b) \sim (p, q)$ *and that* $(c, d) \sim (r, s)$. *Then* $(ap, bq) \sim (cr, ds)$.

Proof. An exercise □

Exercise

1. Verify that addition is commutative
2. Verify that addition is associative
3. Verify that the additive inverse of (a, b) is $(-a, b)$.
4. Show that if $(a, b) \sim (p, q)$ and $(c, d) \sim (r, s)$, then $(ap, bq) \sim (cr, ds)$.

Every nonzero element in the rationals has a multplicative inverse. The rational (a, b) is not zero if $a \neq 0$. In that case $(b, a) \cdot (a, b) = (ab, ab) = (1, 1)$.

We will say that a rational (a, b) is in *canonical form* if two conditions are met.

- The element (a, b) has $b > 0$. This can be achieved using the fact that $(a, b) \sim (-a, -b)$ and "chasing the negative upstairs."
- $\gcd(a, b) = 1$. Suppose we have (a, b) with $b > 0$. Put $d = \gcd(a, b)$. Then $(a/d, b/d) \sim (a, b)$ and $\gcd(a/d, b/d) = 1$, so any rational can be put in canonical form.

Exercise Show that if $(a, b) \sim (c, d)$, then (a, b) and (c, d) have the same canonical form.

Theorem 11. *No two distinct canonical forms are equivalent under* $\sim$.

Proof. Suppose that (p, q) and (a, b) are in canoniclal form and that $(p, q) \sim (a, b)$. Then we know that $pb = aq$. Since $\gcd(a, b) = 1$, by Bezout's theorem we can find integers x and y so that $px + qy = 1$. Multiply by a to see that

$$apx + aqy = a.$$

But $bp = aq$, so

$$a = apx + aqy = apx + bpy = p(ax + by) = p.$$

We now know that $a = p$.

Since $pb = aq = pq$, $b = q$. □

Every (a, b) is equivalent to exactly one canonical form. This form is obtained by dividing both a and b by $\gcd(a, b)$ and by kicking any negative in the denominator by negating both a and b.

The integers in $\mathbb{Q}$ are the rationsls $(n, 1)$ for $n \in \mathbb{Z}$.

5.1 Order!

We will define the relations $<$ and $\leq$ on the rationals as folllows. If (a, b) and (c, d) are in canonical form, we define $(a, b) < (c, d)$ if $ad - bc < 0$ and $(a, b) \leq (c, d)$ if $ad - bc \leq 0$. These relations satisfies the following properties.

- $<$ and $\leq$ are transitive
- $\leq$ is reflexive and for all rationals $(a, b) < (a, b)$ is false.

- $<$ is antisymmetric.
- If $(a, b) \leq (c, d)$ and $(c, d) \leq (a, b)$, $(a, b) = (c, d)$.

In common parlance, the pair (a, b) is denoted by a/b. All of the laws of fractional arithmetic apply to this set. In particular

- Addition is commutative and associative.
- The neutral element of addition is $(0, 1)$.
- The additive inverse of (a, b) is $(-a, b)$.
- Multiplication is commutative and associative.
- Every nonzero element has a multiplicative inverse.

All of the familiar rules of fractional arithmetic apply to the rationals. You are again on familiar ground. We now see the rationals as an extension of the integers. The canonical form of a ratonal is juss the fully-reduced form with any negative kicked into the numerator.

6 Disappointment

Holey, holey, holey, we shall see that the rational numbers have holes. Lots of them. In a way they are quite diaphanous.

Consider a 45-45-90 right triangle whose legs have unit length. Then, by the Pythagorean theorem, the length of the hypotenuse, c is

$$c^2 = 1 + 1 = 2.$$

We will see that there is no rational number assuming this (very real) length.

Theorem 12. *There is no rational number whose square is 2.*

Proof. Suppose such a thing exists; let its canonical form be denoted by p/q. Then

$$\frac{p^2}{q^2} = 2.$$

Multiply both sides by 2. We have $p^2 = 2q^2$. This tells us that p^2 is even. Since 2 si prime and $2 \mid p^2$, we must have $2|p$, so p is even. But, in that case, $4 \mid p^2$.

Since p^2 is divisble by 4 and equals $2q^2$, we must have $2 \mod q^2$. Hence q is even. This is a contradiction of the fact that p/q is in canonical form. The hypothesis that the rational representation exists is false. There is no rational whose square is 2. □

This argument is a pinprick that blasts the balloon. Nothing is special about 2; this argument could be extended to any integer that is not a perfect square. Even worse, if p/q is in canonical form and p and q are not both perfect squares, then there is no rational whose square is p/q. Yes, the rationals are a diaphanous affair, indeed.

7 $\mathbb{Q}$ is not Order-Complete

We will see that the rationals fail to satisfy the greatest lower bound property.

Lemma 5. *Suppose that a and b are rational numbers. Then*

$$2ab \leq a^2 + b^2.$$

Proof. Choose rationals a and b; since the square of any rational number is nonnegative, we have $0 \leq (a-b)^2$. Expanding we get

$$0 \leq a^2 + b^2 - 2ab.$$

The lemma follows immediately. □

Lemma 6. *Suppose that $p > 0$ and $p^2 > 2$. Then*

$$p > \frac{1}{2}\left(p + \frac{2}{p}\right).$$

Proof. Since $p^2 > 2$ and p is positive, we can divide both sides by $2p$ and see that

$$\frac{p}{2} > \frac{1}{p}.$$

Now add $p/2$ to both sides to get

$$p > \frac{p}{2} + \frac{1}{p} = \frac{1}{2}\left(p + \frac{2}{p}\right).$$

□

Theorem 13. *The set of all rational numbers whose square is larger than 2 has no greatest lower bound.*

Proof. By way of contradiction, assume the contrary. Let p be such a greatest lower bound. Put

$$q = \frac{1}{2}\left(p + \frac{2}{p}\right)$$

By Lemma 2, we have

$$p > q$$

We are now going to show that $q^2 > 2$. Begin by expanding.

$$q^2 = \frac{1}{4}\left(p^2 + \frac{4}{p^2} + 4\right) = 1 + \frac{p^4 + 4}{4p^2}.$$

By Lemma 2, we know that

$$\frac{p^4 + 4}{4p^2} \geq \frac{4p^2}{4p^2} = 1,$$

so we can conclude that $q^2 > 2$. We have a contradiction because q is also a greatest lower bound for this set, establishing our result. □