

Beautiful Mathematics

1. PRINCIPLE OF MATHEMATICAL INDUCTION

The set of *natural numbers* is the set of positive integers $\{1, 2, 3, \dots\}$ and is denoted by \mathbb{N} . The *Principle of Mathematical Induction* is a statement about the natural numbers. It says:

Definition (Principle of Mathematical Induction). If S is a subset of the natural numbers such that

- (1) $1 \in S$, and
- (2) whenever $k \in S$, so is $k + 1$,

then $S = \mathbb{N}$.

In other words, the Principle of Mathematical Induction says that the only subset of the natural numbers with the two properties listed above is \mathbb{N} .

Theorem 1. $1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$

Proof. We want to prove this theorem using the Principle of Mathematical Induction as we have stated it. Let S be the set of all natural numbers for which the theorem is true. That is, let $S = \{n \in \mathbb{N} : 1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}\}$. We want to show that $S = \mathbb{N}$. We do this by showing that S has properties (1) and (2).

For (1), we need to check that $1^2 = \frac{1(1+1)(2 \cdot 1 + 1)}{6}$. This is true, so S satisfies property (1). For (2), let $k \in S$. We must show that $k + 1 \in S$. Since $k \in S$, the theorem holds for k , i.e., $1^2 + 2^2 + 3^2 + \dots + k^2 = \frac{k(k+1)(2k+1)}{6}$. We want to show that this formula holds for $k + 1$. By using the formula for k (which we have assumed to be true), we can prove the corresponding formula for $k + 1$. Adding $(k + 1)^2$ to both sides of the equation for k , we get:

$$1^2 + 2^2 + 3^2 + \dots + k^2 + (k + 1)^2 = \frac{k(k + 1)(2k + 1)}{6} + (k + 1)^2.$$

Now we do some algebraic manipulations to the right hand side to see that it is what we want.

$$\begin{aligned}
 \frac{k(k+1)(2k+1)}{6} + (k+1)^2 &= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} \\
 &= \frac{(k+1)[k(2k+1) + 6(k+1)]}{6} \\
 &= \frac{(k+1)[(2k^2+k) + (6k+6)]}{6} \\
 &= \frac{(k+1)[2k^2+7k+6]}{6} \\
 &= \frac{(k+1)(k+2)(2k+3)}{6}
 \end{aligned}$$

Therefore $k+1 \in S$, and by the Principle of Mathematical Induction, $S = \mathbb{N}$. □

Sometimes one wants to prove something by induction that is not true for all natural numbers, but only for those bigger than a given natural number. A slightly more general principle that we can use to do this is the following.

If $m_0 \in \mathbb{N}$ and $S \subset \mathbb{N}$ such that (1) $m_0 \in S$, and (2) whenever $k \in S$ and $k \geq m_0$, so is $k+1$, then $\{n \in \mathbb{N} : n \geq m_0\} \subseteq S$.

The Principle of Mathematical Induction is the special case of this principle when $m_0 = 1$. Now we are able to use induction starting anywhere, not just at 1. For example, which is bigger: $n!$ or 2^n ? For $n = 1, 2$, and 3 , we get $1! < 2^1$, $2! < 2^2$, and $3! < 2^3$. But when $n = 4$, the inequality switches because $4! = 24 > 16 = 2^4$. When $n = 5$, $5! = 120 > 32 = 2^5$. If you think about it a bit, eventually $n!$ is much bigger than 2^n . In both situations we are multiplying n numbers together, but for 2^n we are always multiplying by 2 whereas the numbers we multiply by for $n!$ get larger and larger. While it is not true that $n! > 2^n$ for every natural number (since it is not true for $n = 1, 2$, and 3), we can use the more general form of mathematical induction to prove that it is true for all natural numbers greater than or equal to 4.

Theorem 2. $n! > 2^n$ for $n \geq 4$.

Proof. We use the second version of induction stated above with $m_0 = 4$. Let S be the set of natural numbers for which the theorem is true. As we saw before, $4! = 24 > 16 = 2^4$. Therefore, $4 \in S$. Thus, property (1) is satisfied. For (2), assume that $k \geq 4$ and that $k \in S$, i.e., $k! > 2^k$. We must show that $(k+1)! > 2^{k+1}$. Multiplying both sides of the inequality for k (which is assumed to

be true) by $k + 1$, we have that $(k + 1)! = (k + 1)k! > (k + 1)2^k$. Since $k \geq 4$, $k + 1 > 2$. Therefore

$$(k + 1)! > (k + 1)2^k > 2 \cdot 2^k = 2^{k+1}.$$

Thus, $k + 1 \in S$, verifying property (2). This proves the theorem by induction. \square

So far we have discussed two versions of mathematical induction. Now we are going to consider a third version. Suppose that T is a non-empty subset of \mathbb{N} . Does there have to be a smallest number in T ? Well, certainly the set $\{1, \frac{1}{2}, \frac{1}{3}, \dots, \frac{1}{n}, \dots\}$ has no smallest element. But this set is a subset of the rational numbers, not the natural numbers. You should convince yourself that such a non-empty subset of \mathbb{N} must have a smallest element. This is called the *Well-Ordering Principle*. For those of you who did not feel comfortable accepting the Principle of Mathematical Induction as a valid assumption, then what we are about to show is that if you accept the Well-Ordering Principle, which is easier to believe, then the Principle of Mathematical Induction must be true. In other words we can prove the following theorem.

Theorem 3. *The well-ordering principle implies the principle of mathematical induction.*

Proof. Assume that the Well-Ordering Principle is true. Suppose that S satisfies properties (1) and (2) of the Principle of Mathematical Induction. We must show that $S = \mathbb{N}$. Let $T = \mathbb{N} - S$. That is, T is the set of all natural numbers that are not in S . Therefore, showing that $S = \mathbb{N}$ is the same as showing that $T = \emptyset$. We are going to prove this by using the Well-Ordering Principle.

Suppose that $T \neq \emptyset$. Then, by the Well-Ordering Principle, T has a smallest element, call it t_0 . Since S satisfies property (1), 1 is an element of S . Thus, 1 is not an element of T . Therefore $t_0 \neq 1$. So t_0 must be bigger than 1. In other words, $t_0 - 1 > 0$. Thus, $t_0 - 1 \in \mathbb{N}$. Now let $k = t_0 - 1$. Since $k < t_0$, $k \in S$ (since t_0 is the smallest natural number NOT in S). But then by property 2, $t_0 = k + 1 \in S$. This is impossible because, by the definition of T , an element cannot be in both S and T . This contradicts our assumption that T was not the empty set, which completes the proof. \square

To test our understanding of induction, we conclude this section with a puzzle. Let n be any natural number. Is it true that every set of n people consists of people with the same age? Of course this is true in the trivial case $n = 1$. But for an other choice of n this is certainly false. However, using mathematical induction, it seems that we can prove that every set of n people must consist of people with the same age.

Theorem (?). For each natural number n , every set of n people consists of people with the same age.

Proof. The case $n = 1$ is clear. Suppose this is true for all $n = k$. We must show that every set of $k + 1$ people consists of people of the same age. Let $\{p_1, p_2, \dots, p_k, p_{k+1}\}$ be any set of $k + 1$ people. The set $S_1 = \{p_2, \dots, p_k, p_{k+1}\}$ is a set of k people. Therefore, by the induction hypothesis, the people in S_1 all have the same age. Similarly, the set $S_2 = \{p_1, p_2, \dots, p_k\}$ consists of people with the same age. Person number 2, p_2 , is in both sets. Therefore, everyone in S_1 has the same age as p_2 , and everyone in S_2 has the same age as p_2 . So everyone in $\{p_1, p_2, \dots, p_k, p_{k+1}\}$ is the same age as p_2 . In other words, this set consists of people with the same age. Therefore by induction, this is true for all n . \square

What is going on here? Is mathematics inconsistent or is there an error in the proof?

2. DIVISIBILITY AND PRIME NUMBERS

Recall that for natural numbers m and n , we say that m divides n or m goes into n if $n = mk$ for some natural number k . The notation we use for this is $m|n$. So for example, $2|4$ and $5|35$.

Definition. $p \in \mathbb{N}$ is a prime number if $k|p$ implies that $k = 1$, or $k = p$ and $k \neq 1$.

The first several prime numbers are 2, 3, 5, 7, 11, 13, 17, 19, and 23. Is there a biggest prime? The answer is that there is no biggest prime, but the proof is not so easy. The ancient Greeks knew this fact, and the proof that they used is so beautiful that it will forever be the standard proof that there is no biggest prime number. Before we can recreate this proof, we will need to know some basic facts about prime numbers.

Lemma 4. Every natural number that is neither 1 nor a prime can be factored into a product of primes.

This is a fact that you have most likely known since grade school. What it says is that the prime numbers are the building blocks of the natural numbers. To prove this fact we will need to use a stronger version of mathematical induction, called the *Principle of Complete (or Strong) Mathematical Induction*. It says:

Definition (Principle of Complete Mathematical Induction). If $S \subset \mathbb{N}$ such that

- (1) $1 \in S$, and

(2) $k + 1 \in S$ whenever $\{1, 2, \dots, k\} \subset S$, then $S = \mathbb{N}$.

Don't believe it? Well the same proof that we used for the Principle of Mathematical Induction also proves this principle. Now we move on to the proof of our lemma.

Proof of Lemma 4. Let S be the set of natural numbers for which the lemma is true. We want to show that $S = \mathbb{N}$ by Complete Induction. Trivially, $1 \in S$. Suppose that $\{1, 2, \dots, k\} \subset S$. We must show that $k + 1 \in S$. Consider $k + 1$. Note that $k + 1 \neq 1$. If $k + 1$ is a prime number, then we are done. If $k + 1$ is not prime, then $k + 1 = lm$ where $l, m \in \mathbb{N}$ and neither of them is 1 (by the definition of a prime number). Therefore both l and m must be less than $k + 1$. Thus, they are elements of the set $\{1, 2, \dots, k\}$. So by the induction hypothesis, each of l and m are either primes or products of primes. Therefore $k + 1$ is a product of primes. So, by complete induction, the lemma is proven. \square

Corollary 5. *If $n \in \mathbb{N}$ and $n \neq 1$, then n is divisible by at least one prime number.*

Proof. Let $n \neq 1$. If n is prime, then it is divisible by itself. If not, then n is a product of primes (by Lemma 4), so it is divisible by any prime in the product. \square

With this little corollary, we are now ready to give the famous proof that there is no biggest prime number.

Theorem 6. *There is no largest prime number.*

Proof. Let p be any prime number. We must show that there is a prime larger than p . There is no easy formula to produce a prime number every time, but we can do the following neat trick. Let M be the product of all primes less than or equal to p , plus 1. That is, $M = (2 \cdot 3 \cdot 5 \cdots p) + 1$. If M is prime then we are done since $M > p$. If M is not prime, then, by Corollary 5, it must be divisible by a prime. So, $q|M$ for some prime q . Notice that q cannot be any of the primes less than or equal to p . This is true since if $q \leq p$, then $q|(2 \cdot 3 \cdot 5 \cdots p)$, which implies that q divides $M - (2 \cdot 3 \cdot 5 \cdots p) = 1$. But this is impossible since the only number that divides 1 is itself. Therefore q is a prime number bigger than p . \square

If p and $p + 2$ are both prime, then they are called *twin primes*. For example, 3 and 5, 5 and 7, and 11 and 13 are twin primes. We know there is no biggest prime, but is there a biggest set of twin primes? This is a famous unsolved problem. No one in the world knows the answer to this

question, which is known as the “Twin Prime Problem.” Most mathematicians have thought about this problem at least a little bit, and some mathematicians have devoted their lives to solving it. Needless to say, anyone who solves this problem will gain instant fame, at least in the mathematical community.

There are also some questions about how many primes there are. Of course there are infinitely many, but these questions deal with how often they appear as one moves through the counting numbers. We want to deal with one such question.

Suppose $a_1 + a_2 + \cdots + a_n + \cdots$ is a series with $a_n \geq 0$ for all n . Recall that such a series *converges* if and only if there exists a K such that $a_1 + a_2 + \cdots + a_n \leq K$ for all n . This definition may differ from the one you are used to from calculus, but you can check that this gives an equivalent definition. Recall that the *harmonic series*, $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \cdots$, diverges.

Theorem 7. *The harmonic series diverges.*

Proof. We must show that we can get partial sums that are arbitrarily large. The way we will do this is by showing that we can find partial sums that are larger than any given number. That is, we show that for each natural number K , there is a partial sum of the harmonic series that is greater than K . (This implies that the sequence of partial sums of the series is unbounded.)

To see this, begin with the following observation: since $\frac{1}{3}$ is larger than $\frac{1}{4}$, the sum $\frac{1}{3} + \frac{1}{4}$ is larger than $\frac{1}{4} + \frac{1}{4}$. Thus the partial sum

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4}$$

of the harmonic series is greater than,

$$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{4},$$

which is 2. Similarly, each of $\frac{1}{5}$, $\frac{1}{6}$, and $\frac{1}{7}$ is greater than $\frac{1}{8}$, so

$$\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}$$

is greater than

$$\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8},$$

which is $\frac{4}{8} = \frac{1}{2}$. Thus the partial sum

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}$$

is greater than

$$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{4} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8},$$

which is $2\frac{1}{2}$.

This process can be continued. Each of the terms of the harmonic series from $\frac{1}{9}$ through $\frac{1}{15}$ is greater than $\frac{1}{16}$, so

$$\frac{1}{9} + \frac{1}{10} + \frac{1}{11} + \frac{1}{12} + \frac{1}{13} + \frac{1}{14} + \frac{1}{15} + \frac{1}{16}$$

is greater than

$$\frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16},$$

which is $\frac{8}{16} = \frac{1}{2}$. Hence the partial sum

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \frac{1}{10} + \frac{1}{11} + \frac{1}{12} + \frac{1}{13} + \frac{1}{14} + \frac{1}{15} + \frac{1}{16}$$

of the harmonic series is greater than

$$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{4} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16},$$

which is 3.

Similarly, the terms from $\frac{1}{17}$ to $\frac{1}{32}$ add up to more than $\frac{1}{2}$, as do those from $\frac{1}{33}$ to $\frac{1}{64}$, and so on. So as we take more and more terms into account, we add more and more $\frac{1}{2}$'s. This shows that by taking enough terms from the harmonic series, the partial sums can be made greater than any number we like. In other words, for any K , there are partial sums of the harmonic series that are greater than K , which proves that the harmonic series diverges. \square

Suppose that m_1, m_2, m_3, \dots is a sequence of natural numbers with $m_i < m_{i+1}$ for every i . In some sense, the sum $\frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3} + \dots$, measures how many numbers we have in the sequence. For example, if the m_i 's consist of all of the natural numbers, then this sum diverges by Theorem 7. If we only take powers of 2, then it converges. So in this sense there are more natural numbers than there are powers of 2.

If p_j is the j -th prime number, does the sum

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{p_j} + \dots,$$

converge? Certainly as we list the primes, they seem to thin out. So does this series converge? In fact it does not. The proof that it does not gives us an alternate proof that there are infinitely many primes. The proof is not easy, so we need to build up to it.

Lemma 8. *If $a_i \geq 0$ for all i , and $a_1 + a_2 + \dots$ converges, then there exists a j such that the “tail end of the series”, $a_{j+1} + a_{j+2} + \dots < \frac{1}{2}$.*

Proof. Suppose $a_1 + a_2 + \dots = s$. Then by definition, we can choose a j such that $a_1 + a_2 + \dots + a_j$ is within $\frac{1}{2}$ of s . In other words, the tail end of the series is less than $\frac{1}{2}$. \square

Lemma 9. *Let n be a natural number. Then there exist natural numbers r and s such that $n = r^2s$ and s contains no perfect squares besides 1.*

For example, suppose $n = 120 = 2^3 \cdot 3 \cdot 5$. In order to choose the proper r and s , we want to pick out the perfect squares. In other words, we need to pull off the even powers of primes: $120 = (2^2)(2 \cdot 3 \cdot 5)$. Then we choose $r = 2$ and $s = 2 \cdot 3 \cdot 5$. The only factors of s are 2, 3, and 5. Thus s is not divisible by a perfect square other than 1, and $r^2s = 120$. Now we prove this for a general n .

Proof of Lemma 9. If $n = 1$, then choose r and s to be 1. Given $n \neq 1$, let $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ be a factorization of n into primes (guaranteed to exist by Lemma 4), where $p_i \neq p_j$ if $i \neq j$, and each α_i is a natural number. The idea now is to take off as many even powers of primes as possible to build r^2 . For example, if α_1 is even, then we want to make $p_1^{\alpha_1}$ a part of r^2 (since we do not want s to contain any perfect squares). If α_1 is odd, then we make $p_1^{\alpha_1-1}$ a factor of r^2 . To do this in a concise way, we do the following. Let $[\frac{\alpha_i}{2}]$ be the biggest integer that is less than or equal to $\frac{\alpha_i}{2}$. Thus, if α_i is even, then $\alpha_i = 2m$ for some integer m . Hence, $\frac{\alpha_i}{2} = m$ is an integer and so $[\frac{\alpha_i}{2}] = \frac{\alpha_i}{2} = m$. If α_i is odd, then $\alpha_i = 2l + 1$ for some integer l . Thus, $\frac{\alpha_i}{2} = l + \frac{1}{2}$ is not an integer. Therefore $[\frac{\alpha_i}{2}] = l$. Notice that in both cases, $\alpha_i - 2[\frac{\alpha_i}{2}]$ is either 0 or 1. Now we can explain how to remove the perfect squares. Choose $r = p_1^{[\frac{\alpha_1}{2}]} \dots p_k^{[\frac{\alpha_k}{2}]}$. Then $r^2 = p_1^{2[\frac{\alpha_1}{2}]} \dots p_k^{2[\frac{\alpha_k}{2}]}$ divides n , and $s = \frac{n}{r^2}$ is either 1 or a product of distinct primes. Therefore $n = r^2s$ and s contains no perfect squares. \square

Now we are ready to prove the following theorem.

Theorem 10. *The series consisting of the sum of the reciprocals of the prime numbers diverges.*

Proof. Consider $\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{p_j} + \dots$. If this series converged, then Lemma 8 would imply that there is a j such that $\frac{1}{p_{j+1}} + \frac{1}{p_{j+2}} + \dots < \frac{1}{2}$. Fix j . We will show that this is impossible by an ingenious proof discovered 300 years ago by Euler. For each $N \in \mathbb{N}$, let

$$\mathcal{F}_N = \{n \in \mathbb{N} : n \leq N \text{ and the only primes dividing } n \text{ are among } p_1, \dots, p_j\}.$$

We will take 1 to be an element of \mathcal{F}_N . Consider the set $S = \{n \leq N : n \notin \mathcal{F}_N\}$. If $n \in S$, then n is divisible by some prime p_i , with $i > j$. By counting the multiples p_{j+1} , there are at most $\frac{N}{p_{j+1}}$ elements of S that are divisible by p_{j+1} . Similarly, there are at most $\frac{N}{p_{j+2}}$ elements of S that are divisible by p_{j+2} . So the number of elements of S is less than

$$N \cdot \left(\frac{1}{p_{j+1}} + \frac{1}{p_{j+2}} + \dots \right),$$

which is less than $N \cdot \frac{1}{2}$. The number of elements of S is N minus the number of elements of \mathcal{F}_N . Since the number of elements of S is less than $\frac{N}{2}$, the number of elements of \mathcal{F}_N is greater than $\frac{N}{2}$. Now we want to find a K such that the number of elements of \mathcal{F}_N is less than or equal to K .

Suppose that $n \in \mathcal{F}_N$. Write $n = r^2 s$ where $r, s \in \mathbb{N}$ and s contains no perfect squares except for 1 (which can be done by Lemma 9). We want to estimate the number of elements of \mathcal{F}_N by multiplying the number of r 's by the number of s 's. The number of r 's is less than or equal to \sqrt{N} since each such r satisfies $r^2 \leq N$. From the definition of s , each s is of the form $p_1^{\delta_1} p_2^{\delta_2} \cdots p_j^{\delta_j}$ where δ_i is either 0 or 1. Basically, to build an s , we must make it out of the first j primes so that it is in \mathcal{F}_N , but we can only take each prime at most one time since s is assumed to have no perfect squares as factors. In other words, for each of the first j primes, we either take it or leave it to build s . Therefore the number of possible s 's is at most 2^j . So the number of elements in $\mathcal{F}_N \leq \sqrt{N} \cdot 2^j$. Therefore $\frac{N}{2} < \sqrt{N} \cdot 2^j$. Equivalently, $N < \sqrt{N} \cdot 2^{j+1}$, or $\sqrt{N} < 2^{j+1}$. This has to be true for every N , but j is fixed. So we have contradicted the assumption that $\frac{1}{p_{j+1}} + \frac{1}{p_{j+2}} + \dots < \frac{1}{2}$. Therefore $\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{p_j} + \dots$ diverges. \square

What about twin primes? Certainly if the sum of the reciprocals of the twin primes diverged, then that would imply that there are infinitely many of them. However, a very hard theorem of Brun says that this series converges.

3. CONGRUENCES

Is $2^{17094} + 3$ divisible by 7? This number is way too big for a calculator to handle. So what do we do? By the end of this section we will be able to look at this number and know quickly that 7 does not divide it.

The definition of divisibility of natural numbers can easily be extended to integers. If a, b are integers, then $a|b$ means that there is an integer c such that $ac = b$. The common notation for the set of integers is \mathbb{Z} . Next we introduce an idea that is actually quite familiar to us.

Definition. Let $m \in \mathbb{N}$, $m > 1$. For $a, b \in \mathbb{Z}$, a is congruent to b modulo m , denoted $a \equiv b \pmod{m}$, if $b - a$ is divisible by m .

When we tell time, the hours are expressed “modulo 12.” If we take $m = 12$ in the above definition, then $1 \equiv 13 \pmod{12}$ since $13-1=12$. Also, $6 \equiv -18 \pmod{12}$ since $-18 - 6 = -24$ and -24 is divisible by 12. Note that $a \equiv b \pmod{m}$ is equivalent to saying that a and b leave the same remainder upon division by m . The proof of this is the following. If $a = bm+r$ and $b = lm+q$, where r and q are the remainders when dividing by m , then $a - b = km + r - (lm + q) = m(k - l) + r - q$. So if $r = q$, then $a - b = m(b - l)$. Thus it is divisible by m . Therefore $a \equiv b \pmod{m}$. Conversely, if $a \equiv b \pmod{m}$, then $m|(a - b)$ and $m|m(b - l)$, so $m|(r - q)$. But $0 \leq r < m$ and $0 \leq q < m$ (since they are remainders), so $r - q = 0$. Therefore $r = q$.

Theorem 11. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$(i) \quad (a + c) \equiv (b + d) \pmod{m}$$

$$(ii) \quad ac \equiv bd \pmod{m}$$

Proof. (i) Given $a - b = km$ for some k and $c - d = lm$ for some l , then $(a + c) - (b + d) = (a - b) + (c - d) = km + lm = (k + l)m$, a multiple of m .

(ii) Given $a - b = km$ for some k and $c - d = lm$ for some l , then $ac - bd = ac - ad + ad - bd = a(c - d) + d(a - b) = a(lm) + d(km) = (al + dk)m$, a multiple of m . \square

So congruences work a lot like equations. A special case of the second part of the above theorem is:

Corollary 12. If $a \equiv b \pmod{m}$ then $a^2 \equiv b^2 \pmod{m}$.

Using the principle of mathematical induction, we can prove the following more general result.

Corollary 13. If $a \equiv b \pmod{m}$ and $n \in \mathbb{N}$ then $a^n \equiv b^n \pmod{m}$.

Proof. The case $n = 1$ is true by assumption. Suppose that $a^k \equiv b^k \pmod{m}$. We must show that $a^{k+1} \equiv b^{k+1} \pmod{m}$. Since $a \equiv b \pmod{m}$, $aa^k \equiv bb^k \pmod{m}$ by Theorem 11. Therefore $a^{k+1} \equiv b^{k+1} \pmod{m}$. \square

One thing that we should notice is that every number is congruent to its remainder. For example, $2^3 \equiv 1 \pmod{7}$. By the previous corollary, $(2^3)^k \equiv 1^k \pmod{7}$. What does this tell us about the

example at the beginning of the section? Well, $17094 = 3(5698)$, so $2^{17094} = (2^3)^{5698}$. Therefore,

$$2^{17094} = (2^3)^{5698} \equiv 1^{5698} \pmod{7} \equiv 1 \pmod{7}.$$

Thus, the remainder of $2^{17094} + 3$ when divided by 7 is $1+3=4$. In other words, $2^{17094} + 3$ is not divisible by 7.

Is $(289)(722)(38)(3219)$ divisible by 8? Well, $289 \equiv 1 \pmod{8}$, $722 \equiv 2 \pmod{8}$, $38 \equiv 6 \pmod{8}$ and $3219 \equiv 3 \pmod{8}$. So by Theorem 11, this big product is congruent to $1 \cdot 2 \cdot 6 \cdot 3 = 36$ modulo 8, which is congruent to 4 modulo 8. Therefore the answer is no.

Is 9,792,345,782 divisible by 3? If you remember from grade school, there is a special fact about dividing by 3, which is that a number is divisible by 3 if the sum of its digits is divisible by 3. Now assuming this fact we can answer this question by adding up the digits. This is a rather large number. Note that we can shorten our work even further if we add modulo 3. This gives the same answer by Theorem 11. But where does this special fact about dividing by 3 come from? Notice that

$$9,792,345,782 = 2 + 8 \cdot 10 + 7 \cdot 10^2 + 5 \cdot 10^3 + \cdots + 9 \cdot 10^9.$$

Since $10 \equiv 1 \pmod{3}$, $10^k \equiv 1 \pmod{3}$ for every $k \in \mathbb{N}$ by Corollary 13. Therefore

$$9,792,345,782 \equiv (2 + 8 + 7 + 5 + \cdots + 9) \pmod{3}.$$

In other words, this number is congruent to the sum of its digits modulo 3. Furthermore, its remainder when divided by 3 is the same as the remainder of $2 + 8 + 7 + 5 + \cdots + 9$ when divided by 3 (which is 2). With these ideas we can easily prove this special fact about dividing integers by 3 in general.

Theorem. *An integer is divisible by 3 if and only if the sum of its digits is divisible by 3. More generally, the remainder when a positive integer is divided by 3 is the same as the remainder when the sum of its digits is divided by 3.*

Proof. The number that is written $a_n a_{n-1} \dots a_1 a_0$, where each a_i is in the set $\{0, 1, 2, \dots, 9\}$ with $a_n \neq 0$, is equal to $a_0 + a_1 \cdot 10 + \cdots + a_n \cdot 10^n$. Since $10^k \equiv 1 \pmod{3}$ for every $k \in \mathbb{N}$, the number is congruent to $(a_0 + a_1 + \cdots + a_n) \pmod{3}$. So the number and the sum of its digits leave the same remainder upon division by 3. \square

Can this trick be used when dividing by a number other than 3? Well, the important fact in the proof was that $10^k \equiv 1 \pmod{3}$ for all k . Well, $10^k \equiv 1 \pmod{9}$ for all k too. So the above

theorem holds for 9. What about 11? Since $10 \equiv -1 \pmod{11}$, $10^2 \equiv (-1)^2 \pmod{11} \equiv 1 \pmod{11}$, and $10^3 \equiv (-1)^3 \pmod{11} \equiv -1 \pmod{11}$. Therefore $10^k \equiv 1 \pmod{11}$ if k is even, and $10^k \equiv -1 \pmod{11}$ if k is odd. Thus, if we have a number $a_0 + a_1 \cdot 10 + \cdots + a_n \cdot 10^n$, it is congruent to $a_0 - a_1 + a_2 - a_3 + \cdots$ modulo 11.

In Lemma 4, we saw that every number can be represented as a product of primes. Is it possible for a number have two representations as a product of prime numbers? In other words, can you factor a large number into a product of primes and have your friend factor the same number into a product of primes with the two of you getting different answers? In a trivial way this is possible. For example $15 = 3 \cdot 5$ and $15 = 5 \cdot 3$. But this is not what we mean. Besides the order, can we have different factorizations?

Theorem 14 (The Fundamental Theorem of Arithmetic). *Every natural number greater than 1 is a unique product (up to the order of the factors) of prime numbers.*

Proof. We know that we can factor every $n \neq 1$ into a product of primes. What we must prove is uniqueness. Suppose to the contrary that there exist natural numbers with at least two different prime factorizations. Then there would be a smallest such, say N , by the Well-Ordering Principle. Thus

$$N = p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_l,$$

where p_i and q_i are all prime. At least one of the q 's is different from all of the p 's since we have assumed the two factorizations to be different. But this means that for every i and j , $p_i \neq q_j$, since if $p_{i_0} = q_{j_0}$, then $\frac{N}{p_{i_0}} = \frac{N}{q_{j_0}}$ would be smaller than N and would not have a unique factorization, contradicting the definition of N . Therefore, all of the p 's are different from all of the q 's. In particular, $p_1 \neq q_1$. Suppose that $p_1 < q_1$ (etc. if $q_1 < p_1$). Let

$$M = N - (p_1 \cdot q_2 \cdots q_l) = (p_1 \cdot p_2 \cdots p_k) - (p_1 \cdot q_2 \cdots q_l),$$

which is greater than 0. Note that $p_1 | M$. We can also write

$$M = (q_1 \cdot q_2 \cdots q_k) - (p_1 \cdot q_2 \cdots q_l) = (q_1 - p_1)q_2 \cdots q_l.$$

Since $q_2 \cdots q_l < N$, its prime factorization is unique. M 's prime factorization is also unique since $M < N$. Similarly, $q_1 - p_1$ has a unique prime factorization. Since $p_1 | M$, M 's unique factorization has a p_1 in it. M 's unique factorization is the unique factorization of $(q_1 - p_1)$ times $q_2 \cdots q_l$. Since

all of the q 's are different from p_1 , $(q_1 - p_1)$ must have p_1 as a factor. Thus, $q_1 - p_1 = p_1 \cdot k$ for some k . But then $q_1 = p_1(k + 1)$, so $p_1 | q_1$, which contradicts p_1 and q_1 being distinct primes. \square

For example, $3^{12} \cdot 7^9 \cdot 19^8$ and $3^{11} \cdot 7^8 \cdot 19^9$ have the same primes, 3, 7, and 19 dividing them, but they must be different numbers. Once we see that there are 12 factors of 3 in the first number, and only 11 factors of 3 in the other, they must be different.

Consider the number $22 \cdot 26$. Note that 4 divides this number, since 2 divides both 22 and 26, but 4 does not divide 22 nor does it divide 26. Suppose that p is a prime number that divides $22 \cdot 26$. Must p divide either 22 or 26? Well, $22 \cdot 26 = 2 \cdot 11 \cdot 1 \cdot 13$. Thus p must be either 2, 11 or 13, and therefore divides either 22 or 26. This is just a special case of the following fact. Its proof uses the Fundamental Theorem of Arithmetic.

Corollary 15. *If p is prime and $p | ab$, then $p | a$ or $p | b$.*

Proof. Write canonical decompositions of a and b into primes, $a = p_1 \cdots p_n$ and $b = q_1 \cdots q_m$. So $ab = (p_1 \cdots p_n)(q_1 \cdots q_m)$. Since $p | ab$, $ab = ps$ for some $s \in \mathbb{N}$. Suppose $s = r_1 \cdots r_l$ as a product of primes. Then $ab = ps = pr_1 \cdots r_l$. Since prime factorizations are unique, p must be one of the primes $p_1, \dots, p_n, q_1, \dots, q_m$. If p is one of the p_i 's, then $p | a$. If it is one of the q_j 's, then it divides b . \square

We saw in Theorem 11, that it is possible to do “modular arithmetic.” In other words, we can add and multiply modulo a fixed natural number m in a well-defined way. This means that we can also subtract modulo m , since $a - b$ is just $a + (-b)$. But can we divide modulo m ? Consider the following example. If we divide both sides of $8 \equiv 22 \pmod{7}$ by 2, we get the congruence $4 \equiv 11 \pmod{7}$. However, $3 \cdot 3 \equiv 3 \cdot 1 \pmod{6}$, but we cannot divide both sides of this modular equation by 3 to get another modular equation since 3 is not congruent to 1 modulo 6. So we cannot divide in general. But why did dividing work in the first example and not in the second. The first example is a special case of the following theorem.

Theorem 16. *If p is prime and p does not divide a , and if $ax \equiv ay \pmod{p}$, then $x \equiv y \pmod{p}$.*

Proof. By definition, $ax \equiv ay \pmod{p}$ means that p divides $ax - ay = a(x - y)$. By the previous corollary, p must divide either a or $x - y$. Since p does not divide a , it must divide $x - y$. Therefore $x \equiv y \pmod{p}$. \square

The theorem we have just proved is very useful. Let $S = \{1, 2, 3, \dots, 18\}$. If 19 does not divide a natural number b , then $b \equiv s \pmod{19}$ for some $s \in S$. Suppose that a is a natural number that is not divisible by 19. Let $T = \{a \cdot 1, a \cdot 2, a \cdot 3, \dots, a \cdot 18\}$. No element of T is divisible by 19. Therefore every element of T is congruent to an element of S by the contrapositive of Theorem 16. Furthermore, no two elements of T are congruent to each other modulo 19. Therefore, the product of all members of S is congruent to the product of all the members of T . Why would we care about that? Well, if you multiply the elements of S , you will get $18!$. The product of the elements of T is $18! \cdot a^{18}$. Thus, $18! \equiv 18! \cdot a^{18} \pmod{19}$. Since every element of S is not divisible by 19, $18!$ is not divisible by 19 either. By Theorem 16, we can divide both sides of our modular equation to get $1 \equiv a^{18} \pmod{19}$, or $a^{18} \equiv 1 \pmod{19}$. This fact is an example of a more general result. The proof is just a generalization of what we just did for 19.

Theorem 17 (Fermat's Little Theorem). *If p is prime and a is a natural number not divisible by p , then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. Let $S = \{1, 2, 3, \dots, p-1\}$ and let $T = \{a \cdot 1, a \cdot 2, a \cdot 3, \dots, a \cdot (p-1)\}$. No element of T is divisible by p since if a prime divides a product it must divide one of the factors. Therefore every element of T is congruent to an element of S by Theorem 16. Also, no two elements of T are congruent to each other modulo p . Therefore the product of all members of S is congruent to the product of all members of T . Therefore $(p-1)! \cdot a^{p-1} \equiv (p-1)! \pmod{p}$. Since $(p-1)!$ is not divisible by p , we can divide both sides by $(p-1)!$ to get $a^{p-1} \equiv 1 \pmod{p}$. \square

Fermat's Little Theorem is a very important theorem. We will see that the encoding that is crucial to being able to send secure messages depends heavily on this theorem.

Lemma 18. *If p is prime and a is not divisible by p , then a has a multiplicative inverse modulo p , i.e., there exists an integer b such that $ab \equiv 1 \pmod{p}$.*

Before proving this lemma, let us look at a few examples. Let $p = 3$ and $a = 2$. Then we can take $b = 2$ since $2 \cdot 2 = 4 \equiv 1 \pmod{3}$. If $p = 5$ and $a = 3$, then $b = 2$ works since $3 \cdot 2 \equiv 1 \pmod{5}$.

Proof of Lemma 18. Take S and T as in the proof of Fermat's Little Theorem. Recall that the elements of T , in some order, are congruent to the elements of S . Some element of T is congruent to 1 modulo p . The elements of T can all be expressed as a times something. Therefore if ab is that element of T , then b is the multiplicative inverse of a modulo p . \square

We can also prove Lemma 18 using just the statement of Fermat's Little Theorem.

Alternate Proof of Lemma 18. From Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$. Since $a^{p-1} \equiv a \cdot a^{p-2}$, we just take $b \equiv a^{p-2}$ as the inverse of a . \square

One corollary of Lemma 18 is that we can solve equations modulo p .

Corollary 19. *If p is prime and a is not divisible by p , then for every c , the equation $ax \equiv c \pmod{p}$ has a solution x .*

Consider the example $58x \equiv 17 \pmod{23}$. It is not immediately obvious that this equation has a solution. If we had a multiplicative inverse modulo 23 for 58, say b , then $x = 17b$ would be a solution. This shows us how to prove the corollary in general.

Proof of Corollary 19. Let b be a multiplicative inverse for a modulo p , i.e. $ab \equiv 1 \pmod{p}$. Let $x = bc$. Then $ax = abc \equiv 1 \cdot c \pmod{p} \equiv c \pmod{p}$. \square

Now fix a prime p . For which a is the multiplicative inverse of a congruent to a modulo p ? In other words, for which a is $a^2 \equiv 1 \pmod{p}$. This may seem like a difficult question to answer, but in fact it is not. If $a^2 \equiv 1 \pmod{p}$, then p divides $a^2 - 1 = (a - 1)(a + 1)$. Therefore p divides $a - 1$ or p divides $a + 1$. So $a - 1 \equiv 0 \pmod{p}$ or $a + 1 \equiv 0 \pmod{p}$. That is, $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p} \equiv (p - 1) \pmod{p}$.

What is $(p - 1)! = 1 \cdot 2 \cdot 3 \cdots (p - 2) \cdots (p - 1)$ modulo p ? Since none of the factors is divisible by p , each one has a multiplicative inverse modulo p . The only ones that are their own inverse are 1 and $p - 1$. Among the rest, each one is a multiplicative inverse for one of the others. So by pairing each of these numbers with their inverse, the product $2 \cdot 3 \cdots (p - 2) \equiv 1 \pmod{p}$. Therefore $(p - 1)! \equiv (p - 1) \pmod{p} \equiv -1 \pmod{p}$.

Definition. *The greatest common divisor of $a, b \in \mathbb{N}$, denoted $\gcd(a, b)$, is the largest $d \in \mathbb{N}$ such that $d|a$ and $d|b$.*

In high school you probably had to calculate lots of greatest common divisors. One way to calculate the greatest common divisor is to look at the prime factorizations of the two numbers. For example, if we want to find $\gcd(24, 36)$, then we consider $24 = 2^4 \cdot 3$ and $36 = 2^2 \cdot 3^2$. Now look at the different primes. The primes that 24 and 36 have in common are 2 and 3. The greatest number of factors of 2 of each is 2. The greatest number of factors of 3 in each is 1. Therefore, $\gcd(24, 36) = 2^2 \cdot 3 = 12$.

Definition. a and b are *relatively prime* if $\gcd(a, b) = 1$. Equivalently, there is no prime that divides both a and b .

In some ways, if two numbers are relatively prime, then they behave like prime numbers. For example, we have proved that if a prime divides a product then it must divide at least one of the factors (Corollary 15). Using this fact we can prove the following.

Lemma 20. *If $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.*

Proof. If $\gcd(a, bc) \neq 1$ then there exists a prime p , such that $p|a$ and $p|bc$. By Corollary 15, either $p|b$ or $p|c$. Therefore, either $p|\gcd(a, b)$ or $p|\gcd(a, c)$. \square

Recall that we proved $ab \equiv ac \pmod{p}$, where p is prime, and p does not divide a , then $b \equiv c \pmod{p}$ (Theorem 11). This does not work in general if p is not prime. For example, $6 \cdot 2 \equiv 8 \cdot 2 \pmod{4}$, but 6 is not equivalent to 8 modulo 4 and 4 does not divide 2. Notice that although 4 does not divide 2 they do have a common factor.

Lemma 21. *If $ab \equiv ac \pmod{m}$, $m \in \mathbb{N}$, and if $\gcd(a, m) = 1$, then $b \equiv c \pmod{m}$.*

Proof. We are given that $m|(ab - ac)$ and $\gcd(a, m) = 1$. We want to show that $m|(b - c)$. Consider the prime decompositions of $ab - ac = a(b - c) = p_1 \cdots p_n$, and $m = q_1 \cdots q_l$. Since $m|a(b - c)$, $a(b - c) = mk$ for some k . Since prime factorizations are unique, each q_i must be equal to some p_j . Since $\gcd(a, m) = 1$ none of the q_i 's is a factor of a . Therefore every q_i divides $(b - c)$. Thus $m|(b - c)$. \square

This lemma is going to give us a generalization of Fermat's Little Theorem that is crucial for cryptography.

Given $m \in \mathbb{N}$, $m > 1$, $R = \{0, 1, \dots, m - 1\}$ is the set of all possible remainders modulo m , also called a "complete set of residues modulo m ." If k is any integer, then there is a unique $s \in R$ such that $k \equiv s \pmod{m}$. If m is prime, then every element of R except 0 is relatively prime to m . If m is not prime some elements of R are relatively prime to m and some are not. For example, if $m = 12$, then $R = \{0, 1, \dots, 11\}$. The subset of R consisting of numbers relatively prime to m is $\{1, 5, 7, 11\}$.

There is a function Φ , called the *Euler Φ -function*, such that $\Phi(m)$ is the number of remainders modulo m that are relatively prime to m . We have just verified that $\Phi(12) = 4$. We have also seen that if p is a prime, $\Phi(p) = p - 1$. In fact, if $\Phi(m) = m - 1$ then m must be prime since all of

$\{1, 2, \dots, m-1\}$ would be relatively prime to m . In other words, m would have no factor between 1 and m . Therefore, the Euler Φ -function of m is $m-1$ exactly when m is prime.

Recall that if $\gcd(a, m) = 1$ and $\gcd(b, m) = 1$, then $\gcd(ab, m) = 1$ (Lemma 20). We also showed that we can divide both sides of an equation modulo m by any number relatively prime to m (Lemma 21). Let $S = \{1, r_2, r_3, \dots, r_{\Phi(m)}\}$ be the set of remainders modulo m that are relatively prime to m . Let a be any natural number relatively prime to m and let $T = \{a, a \cdot r_2, a \cdot r_3, \dots, a \cdot r_{\Phi(m)}\}$. If $m = 12$ and $a = 5$ then there are $\Phi(12) = 4$ elements of S , $S = \{1, 5, 7, 11\}$, and $T = \{5 \cdot 1, 5 \cdot 5, 5 \cdot 7, 5 \cdot 11\}$. One can check that every element of T is congruent to an element of S , and no two of them are congruent to the same element. Therefore,

$$1 \cdot 5 \cdot 7 \cdot 11 \equiv 5 \cdot 1 \cdot 5 \cdot 5 \cdot 7 \cdot 5 \cdot 11 \pmod{12} \equiv 5^4 \cdot 1 \cdot 5 \cdot 7 \cdot 11 \pmod{12}.$$

Since $1 \cdot 5 \cdot 7 \cdot 11$ is relatively prime to 12, we can divide both sides of the above equation by $1 \cdot 5 \cdot 7 \cdot 11$ to get $1 \equiv 5^{\Phi(12)} \pmod{12}$, or equivalently, $5^{\Phi(12)} \equiv 1 \pmod{12}$. This is a special case of the following theorem.

Theorem (Euler's Theorem). *If $m \in \mathbb{N}$, $m > 1$ and $\gcd(a, m) = 1$, then $a^{\Phi(m)} \equiv 1 \pmod{m}$.*

Proof. Let $S = \{1, r_2, r_3, \dots, r_{\Phi(m)}\}$ be the set of remainders modulo m that are relatively prime to m . Let a be any natural number relatively prime to m and let $T = \{a, a \cdot r_2, a \cdot r_3, \dots, a \cdot r_{\Phi(m)}\}$. Then as in the proof of Fermat's Little Theorem, every element of T must be congruent to an element of S , and no two of them are congruent to the same element. In other words we can pair up the elements from the two sets. To prove the first of these two statements, let $a \cdot r_i$ be an element of T . Upon division by m , $a \cdot r_i$ leaves some remainder, say s . Thus, $a \cdot r_i \equiv s \pmod{m}$. To show that s is in S , we must show that $\gcd(m, s) = 1$. Since $a \cdot r_i = s + km$ for some integer k , if s has a common factor l with m , then l will divide $a \cdot r_i$. By Lemma 20, $\gcd(a \cdot r_i, m) = 1$. Therefore $l = 1$. To prove the second statement, suppose that $a \cdot r_i$ and $a \cdot r_j$ have the same remainder modulo m . Then $a \cdot r_i \equiv a \cdot r_j \pmod{m}$. Since a is relatively prime to m , we can divide both sides of this equation by a . Therefore $r_i \equiv r_j \pmod{m}$, but this implies that $r_i = r_j$. Thus, $a \cdot r_i = a \cdot r_j$. This proves that the sets S and T can be paired, up to congruence. Therefore, as in the proof of Fermat's Little Theorem, the product of all elements in S is congruent to the product of all elements in T . That is, $1 \cdot r_2 \cdots r_{\Phi(m)} \equiv a \cdot ar_2 \cdots ar_{\Phi(m)} \pmod{m} \equiv a^{\Phi(m)} \cdot 1 \cdot r_2 \cdots r_{\Phi(m)} \pmod{m}$. Since $1 \cdot r_2 \cdots r_{\Phi(m)}$ is relatively prime to m , we divide both sides of the equation by it to get $1 \equiv a^{\Phi(m)} \pmod{m}$. This proves the theorem. \square

Remember that if m is prime then $\Phi(m) = m - 1$ and $\gcd(a, m) = 1$ is equivalent to saying that m does not divide a . So if m is prime, then Euler's Theorem is just Fermat's Theorem.

There is an amazing application of this that was noticed about 25 years ago and has become an important tool in cryptography. The goal is to be able to receive messages in such a way that we can decode them and no one else can. Any message can be turned in to a positive number. For example, let $a = 11$, $b = 12$, $c = 13$, ... , $z = 36$, blank=37, and comma=38. Then the word "bad boy" is 12111437122535. The question is, is there a way for anyone in the world to send us an encoded message that no one besides us could decipher? By a message, we mean a natural number M . *Public Key Cryptography* is the idea that the receiver tells the whole world how to send messages, but only the receiver can decode them. This is called the *RSA method*. In this method, the receiver announces a large number N and another natural number e . A message can be any number $M < N$. If it is longer than that, then it must be sent in pieces. The sender encodes M as follows: Let S be determined by $M^e \equiv S \pmod N$, $0 \leq S < N$. Then S is sent to the receiver. The trick now is to be able to find M without anyone else being able to. The receiver knows a decoder d such that $S^d \equiv (M^e)^d \pmod N \equiv M^{ed} \pmod N \equiv M \pmod N$. So how do we pick d ?

Suppose we want to find the greatest common divisor of 36 and 66. Of course we can do this by factoring each of these two numbers, but there is another way to approach this problem. Since 36 divides into 66 once leaving a remainder of 30,

$$66 = 36 \cdot 1 + 30.$$

Since 30 divides into 36 once leaving a remainder of 6,

$$36 = 30 \cdot 1 + 6.$$

Since 6 divides into 30 five times with no remainder,

$$30 = 6 \cdot 5.$$

This means that 6 has to be the greatest common divisor. Why? Well, suppose that you have a common divisor of 36 and 66. Then, by definition, it has to divide 36 and 66. Therefore it has to divide $30 = 66 - 36 \cdot 1$. But then it has to divide $6 = 36 - 30 \cdot 1$. So it has to divide 6. Therefore any common divisor of 36 and 66 must divide 6. On the other hand, 6 divides 30, so it divides $36 = 30 \cdot 1 + 6$. Thus it also divides $66 = 36 \cdot 1 + 30$. Therefore 6 is the greatest common divisor.

Note that all of the reasoning was done systematically using the above calculations. This will lead to an algorithm for finding the greatest common divisor. There is another benefit of our work. Notice that we are able to express 6 in terms of 30 and 36. Since $6 = 36 - 30 \cdot 1$ and $30 = 66 - 36 \cdot 1$,

$$6 = 36 - 30 \cdot 1 = 36 - (66 - 36 \cdot 1) \cdot 1 = 36 - 66 \cdot 1 + 36 \cdot 1 = 36 \cdot 2 + 66 \cdot 1.$$

Therefore we have written 6 as a linear combination of 36 and 66. By a *linear combination* of integers a and b , we mean an expression of the form $ax + by$ where x and y are integers.

The *Euclidean Algorithm* is a way of finding the greatest common divisor of two natural numbers and of writing that greatest common divisor as a linear combination of the two natural numbers. The Euclidean Algorithm is the following:

Given a and b . Suppose $a > b$. Divide b into a and get a quotient q and a remainder r . That is,

$$a = bq + r, \text{ where } 0 \leq r < b.$$

Now divide r into b to get

$$b = rq_1 + r_1, \text{ where } 0 \leq r_1 < r.$$

Now divide r_1 into r to get

$$r = r_1q_2 + r_2, \text{ where } 0 \leq r_2 < r_1.$$

Notice that the remainders are decreasing. If we continue this process, we eventually have to get a remainder of zero. In other words, there is an n such that

$$r_{n-2} = r_{n-1}q_n + r_n, \text{ where } 0 \leq r_n < r_{n-1}$$

and

$$r_{n-1} = r_nq_{n+1}.$$

Then r_n is the greatest common divisor. To prove this, we must show two things:

- (1) every common divisor of a and b divides r_n , and
- (2) r_n is a common divisor.

To prove the first statement, suppose that d is a common divisor of a and b . Then d divides $r = a - bq$. Since d divides b and r , it divides $r_1 = b - rq_1$. Since d divides r and r_1 , it divides $r_2 = r - r_1q_2$. Continuing in this way, we can show that d must divide r_{n-2} and r_{n-1} . Therefore it divides r_n . To prove the second statement, we use the same type of argument, but in the other direction. Since $r_{n-1} = r_nq_{n+1}$, r_n divides r_{n-1} . Therefore it divides $r_{n-2} = r_{n-1}q_n + r_n$. We continue in this way, working our way up through the above set of equations until we get that r_n

divides r_1 and r , so that it also divides $b = rq_1 + r_1$ and $a = bq + r$. This proves that r_n is the greatest common divisor of a and b .

Let us find $\gcd(3, 8)$ using the Euclidean Algorithm.

$$8 = 3 \cdot 2 + 2$$

$$3 = 2 \cdot 1 + 1$$

$$2 = 1 \cdot 2$$

Therefore, $\gcd(3, 8) = 1$. To find $\gcd(1320, 231)$, the Euclidean Algorithm says to do the following.

$$1320 = 231 \cdot 5 + 165$$

$$231 = 165 \cdot 1 + 66$$

$$165 = 66 \cdot 2 + 33$$

$$66 = 33 \cdot 2$$

Therefore, $\gcd(1320, 231) = 33$.

It is also important to note that r_n is a linear combination of a and b . This is achieved by working our way backwards through the list of equations used in the Euclidean Algorithm, beginning with $r_n = r_{n-2} - r_{n-1}q_n$, as we did in the above example with $\gcd(36, 66) = 6$. Therefore we have the following corollary of the Euclidean Algorithm.

Corollary 22. *The greatest common divisor of two numbers is a linear combination of those numbers.*

This general fact is useful by itself. It gives another proof of Lemma 15.

Alternate Proof of Lemma 15. We want to prove that if p is prime and $p|ab$ then either $p|a$ or $p|b$. Suppose $p|ab$ and that p does not divide a . So we must show that $p|b$. Since p is a prime and it does not divide a , $\gcd(p, a) = 1$. Thus, by the previous corollary, there exist integers x and y such that $xp + ya = 1$. If we multiply through by b , then $xpb + yab = b$. Since p divides ab , it divides yab . Therefore, $p|(xpb + yab) = b$. \square

Corollary 22 also gives an easy proof of uniqueness in the Fundamental Theorem of Arithmetic.

Proof. Suppose $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l}$, with p_i and q_j all prime. A corollary of Lemma 18 is that if p is a prime dividing the product $a_1 a_2 \cdots a_n$, then $p|a_i$ for some i . (One can prove this corollary by induction.) Therefore p_1 divides q_j for some j . Since they are both prime, $p_1 = q_j$. Continuing in this way, all of the p 's are q 's. \square

Expressing the greatest common divisor of two numbers as a linear combination of those numbers is also important for RSA encryption. For example, let $N = 15$, $\Phi(N) = 8$, and $e = 3$. We announce N and e to the world, and keep $\Phi(N)$ secret. If a sender has a message M , then they must send us the number $R \equiv M^e \pmod{15}$. So if $M = 7$, then the sender sends $7^3 \equiv 49 \cdot 7 \pmod{15} \equiv 4 \cdot 7 \pmod{15} \equiv 13 \pmod{15}$. Therefore $R = 13$. Since we only see R , we must compute the de-coder d in order to get back M . If e and $\Phi(N)$ are relatively prime, then the Euclidean Algorithm gives us a method for finding numbers d and x , such that $ed + x\Phi(N) = 1$. In our example, the Euclidean Algorithm tells us that $1 = 3 \cdot 3 + (-1)8$. Thus $d = 3$. Now we decode the message,

$$R^d = 13^3 \equiv (-2)^3 \pmod{15} \equiv -8 \pmod{15} \equiv 7 = M.$$

4. IRRATIONAL NUMBERS

After the integers, the next simplest type of numbers are the rational numbers. They are those numbers $\frac{m}{n}$, where m and n are integers, $n \neq 0$, and $\frac{m_1}{n_1} = \frac{m_2}{n_2}$ if $m_1 n_2 = m_2 n_1$. We use the symbol \mathbb{Q} to denote the set of all rational numbers. We can find the set of integers inside of the rationals by identifying $\frac{m}{1}$ with m . It is very easy to define the arithmetic of rational numbers in terms of the arithmetic of the integers. We define $(\frac{m_1}{n_1}) \cdot (\frac{m_2}{n_2}) = \frac{m_1 m_2}{n_1 n_2}$, and $\frac{m_1}{n_1} + \frac{m_2}{n_2} = \frac{m_1 + m_2}{n_1 + n_2}$. So the question is: are there any other numbers besides the rational numbers?

Consider a square with the length of each side equal to 1. Then we know by the Pythagorean Theorem that the length of a diagonal of such a square is $\sqrt{2}$. In other words, the length of the diagonal squared, i.e., multiplied by itself, is 2. What kind of number is $\sqrt{2}$?

Theorem 23. $\sqrt{2}$ is irrational, i.e., there is no rational number $\frac{m}{n}$ such that $\frac{m}{n} \cdot \frac{m}{n} = 2$. Equivalently, there do not exist integers m and n with $\frac{m^2}{n^2} = 2$.

Before we give the proof of this theorem, we prove the following lemma.

Lemma 24. If m^2 is an even integer, then m is even.

Proof. We could use Lemma 15 to give a quick proof of this lemma. But there is also an elementary proof. Suppose m is odd. Then, $m = 2k + 1$ for some k , and $m^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ is odd. Therefore, if m is odd then so is m^2 . So if m^2 is even, then m is even. \square

Proof of Theorem 23. Suppose $\frac{m^2}{n^2} = 2$. We can reduce $\frac{m}{n}$ to lowest terms. Suppose $\frac{m_0}{n_0} = \frac{m}{n}$ and $\frac{m_0}{n_0}$ is in lowest terms, i.e, $\gcd(m_0, n_0) = 1$. Since $\frac{m_0^2}{n_0^2} = 2$, $m_0^2 = 2n_0^2$. This says that m_0^2 is even, so m_0 is even by the previous lemma. Therefore $m_0 = 2k$ for some k . Thus, $(2k)^2 = 2n_0^2$, or $4k^2 = 2n_0^2$, which implies $2k^2 = n_0^2$. Since n_0^2 is even, n_0 is even. Therefore, $2|n_0$ and $2|m_0$, which implies $\frac{m_0}{n_0}$ is not in lowest terms. This contradicts our assumption that there was such a fraction $\frac{m}{n}$. \square

This proof goes back to the ancient Greeks and appears in Euclid's Elements. The elegance of this argument is an example of what mathematicians find so wonderful about mathematics. This theorem is nice, but it can be made more general than it is.

Theorem 25. *If p is prime, then \sqrt{p} is irrational.*

Proof. Suppose $\frac{m^2}{n^2} = p$. We can reduce $\frac{m}{n}$ to lowest terms. Suppose $\frac{m_0}{n_0} = \frac{m}{n}$ and $\frac{m_0}{n_0}$ is in lowest terms, i.e, $\gcd(m_0, n_0) = 1$. Since $\frac{m_0^2}{n_0^2} = p$, $m_0^2 = pn_0^2$. This implies that $p|m_0^2$. By Lemma 15, $p|m_0$. Therefore $m_0 = pk$ for some k . Thus, $(pk)^2 = pn_0^2$, or $p^2k^2 = pn_0^2$, which implies $pk^2 = n_0^2$. Since $p|n_0^2$, $p|n_0$. Therefore, $p|n_0$ and $p|m_0$, which implies $\gcd(m_0, n_0) \geq p$. This contradicts our assumption that \sqrt{p} was rational. \square

What about $\sqrt{12}$? Well, $\sqrt{12} = \sqrt{4 \cdot 3} = 2\sqrt{3}$. If $2\sqrt{3}$ were rational, then we could divide it by 2 to get another rational number. But if we do this we get $\sqrt{3}$ which we know is irrational. What about $\sqrt{9}$? Since $9 = 3^2$, $\sqrt{9} = 3$ which is rational. What about $\sqrt{6}$? This one is a bit trickier. It is true that $\sqrt{6} = \sqrt{2} \cdot \sqrt{3}$, but the product of two irrational numbers is not necessarily irrational. For example, $3 = \sqrt{3} \cdot \sqrt{3}$. Suppose that it is rational, say $\frac{m}{n} = \sqrt{6}$. Then $m^2 = 6n^2$. Consider the prime factorization of m^2 . It is obtained by squaring the prime factorization of m . Therefore, every prime that divides m must appear as a factor of m^2 an even number of times. Similarly, every prime that divides n must appear as a factor of n^2 an even number of times. Since $m^2 = 6n^2$, both 2 and 3 divide m^2 . Therefore, 2^{2k} and 3^{2l} each divide m^2 , for some natural numbers k and l . However, since n^2 has an even number of factors of 2 and 3 (possibly 0), $6n^2$ must have an odd number of factors of 2 and 3 (because multiplying by 6 adds one extra factor of 2 and one extra

factor of 3). But this is impossible if $m^2 = 6n^2$ since prime factorizations are unique. Thus, $\sqrt{6}$ is not rational. This proof can be generalized to prove the following theorem.

Theorem 26. *The square root of a natural number is rational only if it is an integer (i.e., the natural number is a perfect square).*

Proof. To prove this, let L be any natural number and suppose that $\sqrt{L} = \frac{m}{n}$, where m and n are integers. Thus, $Ln^2 = m^2$. Suppose that the canonical decompositions of m , n , and L into primes are

$$\begin{aligned} m &= p_1^{\alpha_1} \cdots p_t^{\alpha_t} \\ n &= q_1^{\beta_1} \cdots q_u^{\beta_u} \\ L &= r_1^{\gamma_1} \cdots r_v^{\gamma_v}. \end{aligned}$$

Claim: each γ_i is even. Consider $r_i^{\gamma_i}$. If r_i is not equal to any q_j , then $r_i^{\gamma_i} = p_l^{\alpha_l}$ for some l . Thus $\gamma_i = 2\alpha_l$. If $r_i = q_j$ for some j , then $r_i^{\gamma_i} q_j^{2\beta_j} = r_i^{\gamma_i+2\beta_j}$. This equals $p_k^{2\alpha_k}$ for some k . Therefore, $\gamma_i + 2\beta_j = 2\alpha_k$, which implies that $\gamma_i = 2\alpha_k - 2\beta_j$. Thus, every γ_i is even. Let $\gamma_i = 2\delta_i$, where δ_i is an integer. Therefore,

$$L = r_1^{2\delta_1} \cdots r_v^{2\delta_v} = (r_1^{\delta_1} \cdots r_v^{\delta_v})^2.$$

In other words, L is a perfect square. □

What about more general roots, like $\sqrt[3]{2}$? Is this rational?

Theorem 27. *If n is a natural number and R is a natural number, then $\sqrt[n]{R}$ is rational only if it is an integer.*

Proof. This is essentially the same proof as the one for Theorem 26. Suppose that $\sqrt[n]{R} = \frac{a}{b}$, where a and b are integers. Then, $Ra^n = b^n$. Suppose that the canonical decompositions of a , b , and R into primes are

$$\begin{aligned} a &= p_1^{\alpha_1} \cdots p_t^{\alpha_t} \\ b &= q_1^{\beta_1} \cdots q_u^{\beta_u} \\ R &= r_1^{\gamma_1} \cdots r_v^{\gamma_v}. \end{aligned}$$

Claim: each γ_i is a multiple of n . Consider $r_i^{\gamma_i}$. If r_i is not equal to any q_j , then $r_i^{\gamma_i} = p_l^{\alpha_l}$ for some l . Thus $\gamma_i = n\alpha_l$. If $r_i = q_j$ for some j , then $r_i^{\gamma_i} q_j^{n\beta_j} = r_i^{\gamma_i+n\beta_j}$. This equals $p_k^{2\alpha_k}$ for some k .

Therefore, $\gamma_i + n\beta_j = 2\alpha_k$, which implies that $\gamma_i = n\alpha_k - n\beta_j$. Thus, every γ_i is a multiple of n . Let $\gamma_i = n\delta_i$, where δ_i an integer. Therefore,

$$R = r_1^{n\delta_1} \cdots r_v^{n\delta_v} = (r_1^{\delta_1} \cdots r_v^{\delta_v})^n.$$

Thus, $\sqrt[n]{R} = r_1^{\delta_1} \cdots r_v^{\delta_v}$, which is an integer. \square

In mathematics, once you solve one problem, new problems arise. For example, is $\sqrt[3]{\frac{9}{11}}$ rational? This question is not answered by the previous theorem, but we can still use the ideas from the proof to solve it. Suppose $\sqrt[3]{\frac{9}{11}} = \frac{a}{b}$. Then $\frac{9}{11} = \frac{a^3}{b^3}$, which implies that $9b^3 = 11a^3$. Next we compare the prime decompositions of $9b^3$ and $11a^3$. Notice that since 11 is prime and it does not divide 9, it must be one of the primes in the factorization of b . Therefore b^3 has $3k$ factors of 11 for some natural number k . It is also true that a^3 has $3l$ factors of 11 for some integer $l \geq 0$. This implies that $11a^3$ has $3l + 1$ factors of 11. Therefore $3l + 1 = 3k$, which is impossible. This contradicts our assumption that $\sqrt[3]{\frac{9}{11}}$ was rational. More generally we could have asked: When is $\sqrt[k]{\frac{m}{n}}$ rational? This question is left to the reader.

Is $\sqrt{2} + \sqrt{3}$ rational? We know that the sum of two rational numbers must be rational. But the sum of two irrational numbers does not necessarily have to be irrational. For example, $(2 - \sqrt{6}) + \sqrt{6} = 2$. So we need to do some more work to figure this out. The instinctive reaction is that this is not a rational number. Proceeding as we have thus far, suppose it is a rational number, call it r . Then $\sqrt{3} = r - \sqrt{2}$.

$$\sqrt{3} = r - \sqrt{2} \Rightarrow 3 = r^2 - 2\sqrt{2}r - 2 \Rightarrow 5 = r(r - 2\sqrt{2}) \Rightarrow \frac{5}{r} = r - 2\sqrt{2} \Rightarrow \frac{5}{r} - r = -2\sqrt{2}.$$

Dividing both sides of this last equation by -2 implies $\sqrt{2} = -\frac{1}{2}(\frac{5}{r} - r)$, which is a rational number. Since $\sqrt{2}$ is irrational, we have a contradiction.

One can ask all sorts of questions like this, and some of them are quite hard. When studying irrational numbers, one realizes that some are easier to work with than others. For example, $\sqrt{2}$ is a root of the equation $x^2 - 2 = 0$. Such a number is called *algebraic*.

Definition. A real number is *algebraic* if it is a root of a polynomial equation with integer coefficients.

Let $x = \sqrt{2} + \sqrt{3}$. This is not a rational, as we saw before, but it is algebraic.

$$x = \sqrt{2} + \sqrt{3} \Rightarrow x - \sqrt{2} = \sqrt{3} \Rightarrow (x - \sqrt{2})^2 = 3.$$

Since $x^2 - 2\sqrt{2} + 2 = (x - \sqrt{2})^2 = 3$,

$$x^2 - 1 = 2\sqrt{2} \Rightarrow (x^2 - 1)^2 = (2\sqrt{2})^2 = 8 \Rightarrow (x^2 - 1)^2 - 8 = 0.$$

Not all real numbers are algebraic. The two most famous ones are π and e . A number that is not algebraic is called *transcendental*. That is, it is not a root of a polynomial equation with integer coefficients. To prove that π and e are transcendental is not so easy. The proof that e is transcendental is the easier of the two and can be found in Spivak. We do not prove that π and e are transcendental here. However, we will prove that most numbers are transcendental, which is much easier to do.

The rational numbers were created from the natural numbers. What we do now is show how to “construct” the real numbers, denoted by \mathbb{R} , from the rational numbers. Before we do this, we will discuss the crucial property that distinguishes the real numbers from the rational numbers.

Definition. A subset, S , of the real numbers is said to have an *upper bound*, b , if $s \leq b$ for every element s in S .

Consider the set $\{x : x > 4\}$. This set has no upper bound, because every number greater than 4 is in this set. For the set $\{x : x = \frac{1}{n}, n \in \mathbb{N}\}$, any number greater than or equal to 1 is an upper bound. Clearly then, there is no biggest upper bound. But there may be a smallest one, a *least upper bound*. In this example, the least upper bound is 1. Any other upper bound must be bigger than 1 since 1 is in the set. What about $\{x : x^2 < 2\}$? Does this have a least upper bound? Certainly every number greater than or equal to $\sqrt{2}$ is an upper bound. But is there one smaller than $\sqrt{2}$? If $t < \sqrt{2}$, then choose a number s , $t < s < \sqrt{2}$. Then, $t^2 < s^2 < 2$. Therefore, s is in the set and is bigger than t . Thus, t cannot be an upper bound for the set. This means that $\sqrt{2}$ is the least upper bound.

The key question is this: does every non-empty set that has an upper bound have a least upper bound? If the universe of numbers that we are considering is the rational numbers, then the answer is no. Within the real numbers there is a least upper bound. *The Completeness Property* of the real numbers says: if $S \neq \emptyset$ and S has an upper bound, then S has a least upper bound. As mentioned before, the rational numbers are not “complete.” When we construct the real numbers, we will see that they possess the completeness property.

The Intermediate Value Theorem states: If $f : [a, b] \rightarrow \mathbb{R}$ is a continuous function such that $f(a) < 0$ and $f(b) > 0$, then there is a c in the interval (a, b) with $f(c) = 0$. This is a very

important theorem that is used heavily in calculus. But how is it actually proved? If f is a function rational numbers rather than real numbers, then this theorem is not true. For example, let $f(x) = x^2 - 2$, where $f : \{x \in \mathbb{Q} : 0 \leq x \leq 2\} \rightarrow \mathbb{Q}$. Then f is continuous, $f(0) = -2 < 0$ and $f(2) = 2 > 0$. However, the only solution to $f(x) = 0$ in this interval is $\sqrt{2}$ which is not rational and is therefore not in the domain of f . So the proof of the Intermediate Value Theorem must use a fact about \mathbb{R} that is not true for \mathbb{Q} , namely the Completeness Property.

Proof of Intermediate Value Theorem. The idea of the proof is to locate the first place where the function is zero. Let $S = \{x \in [a, b] : f(t) < 0 \text{ for all } t \in [a, x]\}$. We want to show that the least upper bound of this set is a root of f . We know that S is non-empty because it has a as an element, and that S has b as an upper bound. By the completeness property of the real numbers, S has a least upper bound, call it c . Claim: $f(c) = 0$. We do this by showing that $f(c)$ cannot be greater than zero, nor less than zero. Note that by the definition of S , if x is in S and $a \leq t \leq x$, then t is in S . This implies that if $a \leq t \leq x$ and t is not in S , then x is not in S . Therefore, any number greater than a that is not an element of S is an upper bound for S .

Suppose $f(c) > 0$. Then since f is continuous at c , there is a $\delta > 0$ such that $f(c - \delta) > 0$. This implies that $c - \delta$ is an upper bound for S . Therefore, $c - \delta$ is an upper bound that is smaller than c . But this is impossible because c is the least upper bound for S . Therefore $f(c) \leq 0$.

Suppose now that $f(c) < 0$. Again by continuity, there is a $\delta > 0$ such that $f(c + \delta) < 0$. Thus, $c + \delta$ is in S and $c < c + \delta$. Therefore c is in S and there is an element of S greater than it. This contradicts the fact that c is an upper bound for S . Therefore $f(c) = 0$. \square

We saw that $\sqrt{2}$ is not a rational number. But what is it exactly? We made the rationals out of the natural numbers. How can we make the real numbers? One way of doing this is with sequences. It is a fairly complicated way of constructing the reals. Another way is with decimals. We are going to talk about a different construction that is not difficult, just time consuming. The idea is to start with the set of rational numbers and build the set of real numbers from them. The name of the method is called *Dedekind cuts*. The idea is that a real number r will be the set $\{x \in \mathbb{Q} : x < r\}$. Now this does not make sense the way it is written since we have used r to define itself, but it gives the idea. Formally, define a real number \underline{r} to be a subset of \mathbb{Q} with the following properties.

- (1) $\underline{r} \neq \mathbb{Q}$ and $\underline{r} \neq \emptyset$.
- (2) If $x \in \underline{r}$ and $y < x$, $y \in \mathbb{Q}$, then $y \in \underline{r}$.
- (3) There is no largest element in \underline{r} .

For example, the set $\underline{\mathbf{3}} = \{x \in \mathbb{Q} : x < 3\}$. There is a technical reason for wanting to have the third property. Without this property, we would not be able to distinguish between the set $\{x \in \mathbb{Q} : x \leq 3\}$ and the set $\{x \in \mathbb{Q} : x < 3\}$. That is, there would not be another real number between these two different sets.

This is the definition of the real numbers. Of course we have to verify that this definition satisfies all of the properties that real numbers are supposed to have. If q is any rational number, we let $\underline{\mathbf{q}} = \{x \in \mathbb{Q} : x < q\}$. Clearly, every such $\underline{\mathbf{q}}$ is a real number. That is, it satisfies the properties listed above. Notice that property (3) is satisfied because the rational numbers have the property that between any two rationals is another rational.

Theorem 28. $\underline{\sqrt{2}} = \{x \in \mathbb{Q} : x^2 < 2 \text{ or } x < 0\}$ is a real number.

Proof. We need to check that the three properties of real numbers are satisfied by this set. Certainly $\underline{\sqrt{2}}$ is not the empty set since $-3 \in \underline{\sqrt{2}}$. It is also not equal to the set of all rational numbers since 10 is not in $\underline{\sqrt{2}}$. This verifies property (1).

Now we prove property (2). Suppose that $x \in \underline{\sqrt{2}}$ and that $y < x$. We must show that $y \in \underline{\sqrt{2}}$. It is natural to consider two cases here, depending on why x is in $\underline{\sqrt{2}}$. If $x \leq 0$ and $y < x$ then $y < 0$, so $y \in \underline{\sqrt{2}}$. Assume $x > 0$. Then $x^2 < 2$. If $y < 0$ then $y \in \underline{\sqrt{2}}$. If $y \geq 0$ then $0 \leq y < x$. Therefore, $y^2 < x^2 < 2$. Thus, $y \in \underline{\sqrt{2}}$.

To prove property (3), we need to show that $\underline{\sqrt{2}}$ has no biggest element. In other words, if $x \in \underline{\sqrt{2}}$ then we must show that there is a $z > x$ such that $z \in \underline{\sqrt{2}}$. If $x \leq 0$ then pick $z = 1$. Suppose $x > 0$. Then we know that $x^2 < 2$. We want to find a rational number that is slightly bigger than x , so that its square is still less than 2. Suppose $t > 0$ and t is a “small” rational number. Let $z = x + t$. Then $z^2 = x^2 + 2xt + t^2$. Clearly if t is sufficiently small, $2xt + t^2 < 2 - x^2$, so $z^2 < 2$, proving property (3). \square

The formal definition of the set of real numbers is: the sets of rational numbers satisfying the above three properties. If this is the definition of the set of real numbers, how do we add two of them? Well, there is a natural way to do this. Suppose that $\underline{\mathbf{r}}$ and $\underline{\mathbf{s}}$ are real numbers. One possibility is to define $\underline{\mathbf{r}} + \underline{\mathbf{s}}$ to be the union of the two sets, but this is no good. For example, with such a definition $\underline{\sqrt{2}} + \underline{\sqrt{2}} = \underline{\sqrt{2}}$. We certainly do not want this to be true. So we define $\underline{\mathbf{r}} + \underline{\mathbf{s}} = \{x + y : x \in r \text{ and } y \in s\}$. Before going any further, we need to show that this definition makes sense, i.e. that $\underline{\mathbf{r}} + \underline{\mathbf{s}}$, defined in this way, satisfies the three properties of a real number.

Theorem 29. *If $\underline{\mathbf{r}}$ and $\underline{\mathbf{s}}$ are real numbers, then $\underline{\mathbf{r}} + \underline{\mathbf{s}}$ is a real number.*

Proof. (1) $\underline{\mathbf{r}} + \underline{\mathbf{s}} \neq \emptyset$ there exists $x_0 \in \underline{\mathbf{r}}$ and $y_0 \in \underline{\mathbf{s}}$, so $x_0 + y_0 \in \underline{\mathbf{r}} + \underline{\mathbf{s}}$.

(2) Suppose that if $x + y \in \underline{\mathbf{r}} + \underline{\mathbf{s}}$ and $z < x + y$. We must show that $z \in \underline{\mathbf{r}} + \underline{\mathbf{s}}$. If $z < x + y$, then $z - y < x$, so it is in $\underline{\mathbf{r}}$. Therefore $z = (z - y) + y$ is in $\underline{\mathbf{r}} + \underline{\mathbf{s}}$.

(3) Suppose $x + y \in \underline{\mathbf{r}} + \underline{\mathbf{s}}$. We must find a $z > x + y$ such that $z \in \underline{\mathbf{r}} + \underline{\mathbf{s}}$. Since $\underline{\mathbf{r}}$ and $\underline{\mathbf{s}}$ are real numbers, they satisfy property (3), so there are numbers $x_1 \in \underline{\mathbf{r}}$ with $x_1 > x$, and $y_1 \in \underline{\mathbf{s}}$ with $y_1 > y$. Then $x_1 + y_1 > x + y$ and is in $\underline{\mathbf{r}} + \underline{\mathbf{s}}$.

□

We have defined all of the rational numbers as real numbers. In particular, $\underline{\mathbf{0}} = \{x \in \mathbb{Q} : x < 0\}$. But we need to verify that $\underline{\mathbf{0}}$ behaves the way it is supposed to.

Theorem 30. $\underline{\mathbf{0}} + \underline{\mathbf{r}} = \underline{\mathbf{r}}$ for every real number $\underline{\mathbf{r}}$.

Proof. Suppose $\underline{\mathbf{r}}$ is a set satisfying properties (1), (2), and (3). $\underline{\mathbf{0}} + \underline{\mathbf{r}} = \{x + y : x < 0, y \in \underline{\mathbf{r}} \text{ and } x \in \mathbb{Q}\}$. To show that $\underline{\mathbf{r}}$ and $\underline{\mathbf{0}} + \underline{\mathbf{r}}$ are the same set, we will show that $\underline{\mathbf{r}} \subset \underline{\mathbf{0}} + \underline{\mathbf{r}}$ and that $\underline{\mathbf{0}} + \underline{\mathbf{r}} \subset \underline{\mathbf{r}}$.

If $y \in \underline{\mathbf{r}}$, let $y_1 \in \underline{\mathbf{r}}$ with $y_1 > y$. Such an number exists since $\underline{\mathbf{r}}$ has no biggest element. Therefore, $y - y_1, 0$. Thus $y - y_1 \in \underline{\mathbf{0}}$. So $y = (y - y_1) + y_1 \in \underline{\mathbf{0}} + \underline{\mathbf{r}}$. Therefore $\underline{\mathbf{r}} \subset \underline{\mathbf{0}} + \underline{\mathbf{r}}$.

If $x + y \in \underline{\mathbf{0}} + \underline{\mathbf{r}}$, then $x + y < y$ since $x < 0$. Since $\underline{\mathbf{r}}$ has property (2), $x + y \in \underline{\mathbf{r}}$. Therefore $\underline{\mathbf{0}} + \underline{\mathbf{r}} \subset \underline{\mathbf{r}}$. □

What about multiplication? Given what we just did, the natural thing to do is to look at the set of all products. But this is a bad idea. If this was the definition we chose for multiplication, then

$$\underline{\mathbf{0}} \cdot \underline{\mathbf{0}} = \{xy : x < 0 \text{ and } y < 0\} = \{z \in \mathbb{Q} : z > 0\}.$$

The set $\{z \in \mathbb{Q} : z > 0\} \neq \underline{\mathbf{0}}$, which is what we would want, and is not even a real number since it fails property (2). Before we deal with multiplication, we will define what it means for one real number to be bigger than or equal to another real number. Define $\underline{\mathbf{r}} \leq \underline{\mathbf{s}}$ if $\underline{\mathbf{r}} \subseteq \underline{\mathbf{s}}$. This is reasonable since it works for the rational numbers. That is, if p and q are rational numbers, then $\underline{\mathbf{p}} \subseteq \underline{\mathbf{q}}$ if and only if $p \leq q$. $\underline{\mathbf{0}} \leq \underline{\mathbf{r}}$ means that a real number is *positive* if and only if it contains every negative rational number. This seems strange, but now we can define the product of two positive real numbers. If $\underline{\mathbf{r}} \geq \underline{\mathbf{0}}$ and $\underline{\mathbf{s}} \geq \underline{\mathbf{0}}$, then define

$$\underline{\mathbf{r}} \cdot \underline{\mathbf{s}} = \{x \in \mathbb{Q} : x < 0\} \cup \{yz : y \in \underline{\mathbf{r}}, y \geq 0 \text{ and } z \in \underline{\mathbf{r}}, z \geq 0\}.$$

Of course we have to check that $\underline{r} \cdot \underline{s}$ is in fact a real number. This is left as an exercise. Next we define how to multiply in general. If $\underline{r} < \underline{0}$ and $\underline{s} \geq \underline{0}$, then $\underline{r} \cdot \underline{s} = (-\underline{r}) \cdot \underline{s}$. If $\underline{r} \geq \underline{0}$ and $\underline{s} < \underline{0}$, then $\underline{r} \cdot \underline{s} = \underline{r} \cdot (-\underline{s})$. If $\underline{r} < \underline{0}$ and $\underline{s} < \underline{0}$, then $\underline{r} \cdot \underline{s} = (-\underline{r}) \cdot (-\underline{s})$.

Now things are going to get messy because we want to talk about sets of real numbers. So we will be dealing with sets of sets. For $S \subset \mathbb{R}$ and $\underline{b} \in \mathbb{R}$, we define \underline{b} to be an *upper bound of S* as before. If $\underline{b} \geq \underline{s}$ for all $\underline{s} \in S$. But what does this mean? Remember that $\underline{b} \geq \underline{s}$ means that $\underline{s} \in \underline{b}$. This must be true for every $\underline{s} \in S$. Therefore $\bigcup\{\underline{s} : \underline{s} \in S\} \subset \underline{b}$. As before, we define \underline{c} to be a *least upper bound of S* if:

- (1) \underline{c} is an upper bound, and
- (2) $\underline{c} \leq \underline{b}$ for every \underline{b} that is an upper bound.

The key property that we want the real numbers to have is the completeness property. Without this property, calculus would not be possible. As you can imagine, proving this will get quite messy given the definition we have.

Theorem 31. *Every non-empty set of real numbers that has an upper bound has a least upper bound.*

Let us first think about what the least upper bound of such a set should be. Recall that an upper bound \underline{b} of set S must have the property that it contains the union of all the real numbers $\underline{s} \in S$. Certainly the union itself possesses this property, and is therefore less than or equal to any other upper bound. Therefore it is the least upper bound for S . However, this only makes sense if it is a real number. The proof that it is a real number is left as an exercise.