Math 79SI Notes

Mason Rogers

1 Introduction to Mathematical Questions and Answers

1.1 Background

At its core, doing math involves using precise *definitions* of objects and assumptions about them to prove concrete *statements* and answer interesting questions. Good definitions encapsulate the mathematically relevant properties of an object in such a way that they are useful to prove statements about that object. Over the span of the quarter, we will investigate what constitutes a good definition. But insofar as definitions are valued by their usefulness in proving statements and answering questions, we first need a good handle on what mathematical statements are.

A mathematical statement is anything that is precise enough to be deemed true or false. For example, 'two is a prime number' is a statement, which we happen to know is true. 'Four is a prime number' is also a statement, even though we know it is false. Often, statements we want to prove describe the elements of a particular set. We can say that an object is an element of that set using the symbol $\in$. For example, letting P stand for the set of prime numbers, this allows us to rewrite the statement 'two is a prime number' as $2 \in P$.

Sometimes, we want to be able to construct sets that do not have obvious names. We can do this via *set-builder notation*, which looks like this:

$$S = \{\text{objects in some other set} : \text{specific properties they satisfy}\}$$

We could then write 'the set of all odd primes' as $\{x \in P : x \text{ is odd}\}$, which would be read aloud as 'the set of all x in P such that x is odd'. As we introduce new notation, however, it is important to keep in mind that words are often more useful than symbols. For instance, 'the set of odd primes' is straightforward enough that the excess notation above is likely unhelpful. Learning when to use symbols versus words takes practice, but as a general rule of thumb, aim for clarity.

One more tool for writing mathematical statements is the use of *quantifiers* 'there exists' and 'for all', which can be represented respectively by the symbols $\exists$ and $\forall$. (You will more commonly see these symbols on a blackboard than in formal mathematical writing, but they are nonetheless important to recognize.) For instance, letting $\mathbb{N}$ denote the set of natural numbers (i.e. $\{1, 2, 3, \ldots\}$) and using product notation,[1] we could write the statement 'every

[1] It is common to denote the sum and product of a list of numbers $\{a_1, a_2, \ldots, a_k\}$ respectively as

$$\sum_{i=1}^{k} a_i \text{ and } \prod_{i=1}^{k} a_i.$$

natural number greater than 1 can be written as a product of prime numbers' as

$$\forall\ n \in \mathbb{N} \text{ such that } n > 1, \exists\ p_1, \ldots, p_k \in P \text{ such that } n = \prod_{i=1}^{k} p_i.$$

This could literally be read as 'for all n in the set of all natural numbers, there exist prime numbers p_1 through p_k such that n equals the product of the p_i'. From a conversational standpoint, this is verbose; it is less confusing to say simply 'every natural number other than 1 can be written as a product of prime numbers'. But if we wanted to prove that statement, the extra formality makes precise exactly what we need to show. That is where the math begins: we take something we suspect is true, then write it precisely and efficiently so that we can investigate it.

We will begin our journey through proof tactics with the bluntest swords the mathematician can draw: proof by construction and disproof by counterexample. In the first case, we show that an object exists by writing out exactly what it is. In the second, we show that a statement is not always true by finding a particular case in which it is false. Going through a few of these examples will start to help us feel comfortable using mathematical notation and writing proofs.

1.2 Examples

A prime number is a natural number greater than or equal to 2 whose only divisors are 1 and itself. We will let P denote the set of all prime numbers for the remainder of this section, and we seek to ask and answer several questions about P. A first question we could ask would be 'how many primes are there?' This brings us to our first proposition.

Proposition 1.1. There are infinitely many prime numbers.

Proof. First, we will translate this statement to the equivalent statement 'for any finite list of prime numbers, we can find another prime not on that list'. We can conclude the proposition from this statement because the proving the new statement will prove that there is no complete finite list of primes.

We will proceed from here by considering an arbitrary finite list of prime numbers and coming up with a prime that is not in the list. Let $L_k = \{p_1, p_2, \ldots, p_k\}$ be a list of k primes for some $k \geq 1$. Since the criterion for whether a number n is prime depends on what divides n, the best we can do is try to define a number greater than 1 which is not divisible by *any* of the primes in L_k. We therefore define

$$n_k = \left(\prod_{i=1}^{k} p_i\right) + 1.$$

Note that $n_k > 1$. Let's see what this process yields when beginning with $k = 1$ and $L_1 = \{2\}$. First, we obtain $n_1 = 2 + 1 = 3$, which is a prime not contained in L_1. Trying again with $L_2 = \{2, 3\}$, we obtain $n_2 = 2(3) + 1 = 7$, another new prime. Then we try with $L_2 = \{2, 3, 7\}$ to get $n_3 = 2(3)(7) + 1 = 43$, yet *another* new prime!

If n_k is always prime, then since it is larger than any prime in L_k, n_k is a always a *new* prime, i.e. one not contained in L_k.

Wish. Let L_k and n_k as suggested. Then n_k is a prime not contained in L_k.

Disproof of wish. We try once more with the above example. Beginning with $L_4 = \{2, 3, 7, 43\}$ gives $n_4 = 2(3)(7)(43) + 1 = 1807$, which factors as $13(139)$ and is therefore not prime. We have found a counterexample, so our procedure does *not* always give a new prime. □

Our wish is not true, but that does not necessarily derail our approach to showing that there are infinitely many primes. Regardless of whether n_k is prime, since $n_k > 1$ it must have a prime factor q. Since n_k is 1 more than a multiple of each of the primes p_i in L_k, n_k cannot be a multiple of any of the p_i. Accordingly, q cannot be one of the p_i, since n_k is a multiple of q. We conclude that q is a prime not in L_k, so $L_{k+1} = \{p_1, p_2, \ldots, p_k, q\}$ is a list of $k + 1$ primes.

We have shown that given any finite list of primes, we can come up with a prime not on that list. This proves that there are infinitely many primes. □

We now know that there are infinitely many primes. To figure this out, we tried to come up with a way to generate 'new' primes from a list of 'old' primes. We tested our procedure a little bit, and when we found out that it does not always work, we refined our procedure a bit. This is how mathematics often goes: we make an educated guess based on examples, analogies, or intuitions, see whether or not it yields the desired result, and, if not, try to improve our original strategy based on what we learned.

Of course, our procedure for coming up with a prime not in L_k is far from explicit. We can compute n_k rather quickly, but if n_k is not prime, we need to be able to find a prime factor q. Factorizing large numbers is a difficult task even for the fastest computers, and as is apparent from our examples, the suggested procedure starts generating large primes very quickly. We might wonder if we can come up with a better procedure to generate primes explicitly.

One famous historical example involves searching for primes of form $2^m + 1$ for integers $m \geq 1$. It can be shown that if $2^m + 1$ is a prime greater than 2, then $m = 2^n$ for some nonnegative integer n.[2] The interest in primes of this form goes back to the work of French mathematician Pierre de Fermat, so mathematicians define the n-th Fermat number F_n by $F_n = 2^{2^n} + 1$. We may wonder if the Fermat numbers are all prime.

Problem 1.2. Prove or disprove: All Fermat numbers are prime.

Proof. Knowing that all *primes* of form $2^m + 1$ must be Fermat numbers gives little evidence to suggest that all Fermat numbers are prime. Checking low $n = 0, 1, 2, 3$, and 4 yields $F_n = 3, 5, 17, 257$, and 65537, respectively, all of which are prime.[3] Next, we have $F_5 = 4294967297$, which is too large to check exhaustively for factors by hand. However, in 1770, Euler showed that any factor of F_n must be of form $2^{n+1}k + 1$ for some positive integer k.[4]

[2] We will prove this in two weeks, but you are welcome to try now if you want a challenge.

[3] These were the cases that Fermat knew when he conjectured that all numbers of $2^{2^n} + 1$ were prime. Without computers, checking more cases was infeasible. Would you have made the same conjecture?

[4] There is not an English version of Euler's paper, but there is a reference to an English version of a paper proving a slightly more strict requirement due to Lucas in the further reading section 1.4.

In the case $n = 5$, it therefore suffices check integers that are 1 more than a multiple of 64, i.e. $\{65, 129, 193, \ldots, 641, \ldots\}$. The first 9 possibilities of this type do not divide F_4, but the 10th does, as $F_5/641 = 6700417$. We conclude that F_5 is not prime, which is a counterexample disproving that all Fermat numbers are prime. □

The above is a good example of a statement to which one must apply a bit of cleverness to narrow down the search for a counterexample before finding one. If an integer n factors as ab then at least one of a or b must be less than or equal to $\sqrt{n}$,[5] and for $n = F_5$, we compute that $\sqrt{n}$ is just a hair above 65536. Additionally, we only need to bother checking for *prime* factors less than 65536, since any composite number at most 65536 has a prime factor less than 65536. It was known to Euler that there are 6542 primes less than or equal to $\sqrt{F_5}$, which would be too many to begin to check by hand. However, the intermediate result that any divisor of F_5 must be 1 more than a multiple of 64 narrows the search space to 209 possibilities. While checking 209 cases before the calculator had been invented may seem like drudgery, 209 cases is a much more reasonable search space to probe than 6542 cases. Indeed, it is sometimes best to think of what a counterexample *might look like* instead of blindly checking the 'first few' cases.

We finish this section with one more possible prime-generating technique. Consider the function $f(n) = n^2 + n + 41$. For $n = 1, 2, 3, 4, 5$, and 6, we have $f(n) = 43, 47, 53, 61, 71$, and 83, all of which are prime. Will this behavior continue?

Problem 1.3. Prove or disprove: The function $f(n) = n^2 + n + 41$ returns a prime for all natural numbers n.

Proof. We know that the statement holds for $n \in \{1, 2, 3, 4, 5, 6\}$. We could keep going and we would see that it holds for $n \in \{7, 8, 9, \ldots, 39\}$ as well (try a few yourself!). But when $n = 40$, $f(n) = n^2 + 2n + 1 = (n + 1)^2$, so $f(40)$ is clearly not prime. Perhaps more straightforwardly, when $n = 41$, each term is a positive multiple of 41, so their sum must be divisible by 41 and bigger than 41. We have found two counterexamples, which is one more than the number we need to conclude that the statement is false. □

This example, also due to Euler, reinforces the point that the first few examples are not always the most likely counterexamples. Indeed for any prime p, if we define $f_p(n) = n^2 + n + p$, it is clear that

$$f_p(p-1) = (p-1)^2 + 2p - 1 = (p-1)^2 + 2(p-1) + 1 = (p-1+1)^2 = p^2$$

and

$$f_p(p) = p^2 + p + p = p(p+2),$$

neither of which is prime.

Of course, it is still intriguing that $f_{41}(n)$ returns prime for all natural numbers $n < 40$. If similar behavior is observed for all f_p, then we would have a powerful mechanism for generating primes of order p^2 given any known prime p. This could be particularly useful in

[5] Why? If $a, b > \sqrt{n}$, then $ab > \sqrt{n}^2 = n$. This method of argument, 'proof by contrapositive', will be discussed more fully in week 3.

cryptography, as the common RSA cryptosystem[6] relies on working with very large prime numbers. And, as nothing seems particularly special about the choice $p = 41$, why not investigate the other f_p? As always, we will need to formulate a statement.

Problem 1.4. Prove or disprove: For all primes p, $f_p(n)$ is prime for $n \leq p - 2$.

We will disprove the claim in two ways.

Disproof 1. First, we will check for a counterexample. When $p = 2$, there is nothing to check. When $p = 3$, we must check that $f_p(1)$ is prime. Since $f_3(1) = 5$, the statement holds for $p = 3$. We move to $p = 5$, for which we must check $n \in \{1, 2, 3\}$. We have $f_5(1) = 7, f_5(2) = 11$, and $f_5(3) = 17$. At this point, the claim is starting suggest validity. Fortunately, we need only check one more case, as $f_7(1) = 9$, which is not prime. □

Disproof 2. In retrospect, however, is there a way that we could have guessed a counterexample without checking cases? Consider that $f_p(1) = p + 2$ for arbitrary p. Clearly it is not true for *every* odd prime p that $p + 2$ is prime; if this were the case, every odd number would be prime. We observe that 7 is the smallest odd prime p such that $p + 2$ is composite and conclude that $f_7(1)$ is not prime. □

As we are quickly discovering, generating large, assuredly prime numbers is a difficult task. We are also discovering that answering one question almost always leads to others, such as how we now are left to wonder what makes f_{41} special, or if there are any larger p such that f_p has the property of the problem.[7] But what is most important is to have a systematic way of asking and answering questions. In the coming weeks, we will develop more robust methods for answering questions that cannot be answered by finding a counterexample or constructing an object with desired properties directly.

1.3 Exercises

1. Write the following statement symbolically: For all p in the set of prime numbers, there exists a larger prime number q.

2. Write the following statement in English: $\forall a, b \in \mathbb{N}$ such that $\gcd(a, b) > 1$, $\exists p \in P$ such that $p \mid a$ and $p \mid b$.

3. Construct the following set using set-builder notation: the set of all prime numbers that are 1 less than a multiple of 10.

4. Describe the following set in English: $\{p \in P : p + 2 \in P\}$.

5. Primes separated by 2, 4, and 6 are known as 'twin primes', 'cousin primes', and 'sexy primes', respectively. For example, $\{17, 19\}$ are twin primes, $\{19, 23\}$ are cousin primes, and $\{23, 29\}$ are sexy primes. It is also possible to have more than two primes

[6] See further reading section 1.4 for more information.

[7] If you are interested in learning about why 41 is special in this way, which is conceptually related to why $e^{\pi\sqrt{163}}$ is *really* close to being an integer (try it), you should consider learning about algebraic number theory and elliptic curves.

in arithmetic progression with common difference 6. For instance, $\{41, 47, 53, 59\}$ are primes and thus called a 'sexy prime quadruplet'. A friend proposes that there cannot be sexy prime quintuplets, as one of the five numbers must be divisible by 5 and is therefore composite. Is your friend's argument valid? If not, identify the flaw in their reasoning.

6. A friend suggests the following algorithm for constructing primes: Starting with $p_1 = 2$, define $p_{n+1} = 2p_n + A_n$, where $A_n = (-1, -1, 1, 1, -3, -3, 3, 3, -5, -5, 5, 5, \ldots)$. Does it always return a prime? Prove your answer.

7. Prove that the set mentioned in problem 4 is infinite. (Just kidding—this is an incredibly challenging, long-standing open problem known as the Twin Prime Conjecture. Despite its apparent simplicity in formulation, it was only in 2013 that Yitang Zhang proved that for some c (in particular $c = 7(10)^6$), $\{p \in P : p + n \in P,\ \text{for some } 2 \leq n \leq c\}$ is infinite. The proof of this long-standing conjecture surprised the math world. Soon thereafter, building on the *ideas* of Zhang's proof, many mathematicians collaborated to show that some $c \leq 246$ must also work too. It is widely believed, but not known, that $c = 2$ should work, i.e. that the Twin Prime Conjecture is true. To prove it, new methods will be needed. For this homework problem, Google "Twin Prime Conjecture" and "Yitang Zhang", and write some things that you learn.)

1.4 Further Reading

Chris Caldwell "The Law of Small Numbers"	A fun and insightful read on why even many examples of a statement being true do not always provide meaningful evidence that it is.
CPZ Chapter 0	Tips and conventions for mathematical writing. Not important to memorize, but a helpful reference.
CPZ Chapter 1	Basic set theory if unfamiliar. This goes into more detail than we need; for now, you will want to be comfortable with sets, unions/intersections/complements of sets, subsets of sets, and set-builder notation.
CPZ Chapter 2.1	A more formal look at statements including truth tables, not important unless you are very interested.
CPZ Chapter 2.10	More on quantifiers $\exists$ and $\forall$.
Imre Lakatos "Proofs and Refutations" Part I	Parallels the history of the polytope and Euler characteristic, illuminating the importance of good definitions in math.
Michal Krizek "17 Lectures on Fermat Numbers" Chapter 6	Contains Lucas' proof that any factor of a Fermat number F_n must be of form $2^{n+2}k + 1$; requires basic knowledge of modular arithmetic
Wikipedia entry for RSA Cryptosystem	An application of generating very large primes in cryptography. en.wikipedia.org/wiki/RSA_(cryptosystem)

1.5 Activity

We are going to investigate what makes a mathematical definition of a physical concept useful. Imagine you are a farmer managing a few differently-shaped corn fields, and you want to know how much corn you can grow in each field. You know that this depends entirely on how much 'area' there is in each field, whatever that means. You walk to your first field, which is a square with side length 3, and ponder how you can compute its area.

Step 1 Everybody construct what they think is a mathematically precise definition of area. Your definition should be robust enough to help you compute the area of your first field, and ideally general enough that it can handle some other shapes of field. For instance, a definition like 'the amount of empty space inside a closed path' would not be a good definition. Even though it accurately captures the intuitive idea of area, it will not help you decide how much corn you can plant on this field.

Step 2 Walk to a new field, and everyone try to use their original definition to compute the area of that field. You may use trigonometry and calculus to calculate lengths, but it is important that you do not reach beyond your definition in calculating areas. For instance, if your definition of area does not encapsulate the additivity of area, you cannot say that a field consisting of two squares of side length three has twice the area calculated in step 1. Do not worry if your definition does not handle many cases easily; the goal of this activity is not to develop the most general good definition of area,[8] but to develop a sense of what makes a good mathematical definition.

Step 3 Discuss as a class which definitions are strong enough to handle the new field, which definitions might work with small tweaks, and which need major changes. Discuss which definitions provided a good estimate given our prior knowledge of area, which provided a bad estimate, and which could not provide a useful estimate. We will keep a list as a class of when and how each definition breaks down. Then go back to step 2 until there are no more fields left. Your fields are shaped as follows:

1. square of side length 3
2. square of side length 6
3. L-shape made up of three squares of side length 3
4. equilateral triangle of side length 4
5. circle of radius 5
6. bounded region between the graphs of $y = x^2 + 4$ and $y = 2x^2$
7. surface of the upper half of a ball with radius 40
8. cylinder with radius 2 and height 6
9. a square of side length 1 with an xy-coordinate system, but all points with some coordinate irrational are flooded and cannot be farmed

[8] If you are interested in learning about a robust notion of 'area' and 'volume', you will want to learn about the concept of 'measure', the study of which is known as measure theory.

Breakdown: Reflect on the most successful aspects of each definition. Think about which definitions made *computations* easy and which made *generalizations* easy. Recognize that definitions can evolve over time to handle broader circumstances, much as how when we learn about numbers in elementary school, we expand our definition of ‘number’ from what we now know as the natural numbers to the rational numbers, then to the reals, and finally to the complex numbers.