Disproof

MAT231

Transition to Higher Mathematics

Fall 2014

Outline

Theorems and Propositions

Theorem (The Fundamental Theorem of Arithmetic)

Every positive integer greater than 1 can be represented in exactly one way (apart from rearrangement) as a product of one or more primes.

Proposition (Primality Test)

Let $n \in \mathbb{N}$ with $n > 1$. Then n is prime if and only if n is not divisible by any prime p with $p \leq \sqrt{n}$.

Both of these represent statements that are known to be true because proofs for them exist. Usually **theorems** are more important (and often more difficult to prove) than **propositions**.

Conjectures

Now consider the following statements:

Twin Prime Conjecture: There infinitely many primes p such that $p+2$ is also prime.

Goldbach Conjecture: Every even integer $n \geq 4$ can be expressed as a sum of two primes (not necessarily distinct), i.e., n can be written in the form $n = p_1 + p_2$, where p_1 and p_2 are primes.

Are these statements true or false?

No one knows! They seem to be true, as we have been unable to disprove them, but neither has anyone been able to prove that they are true.

A statement which seems true but for which no proof has yet been found is called a **conjecture**.

A Bit More on Prime Numbers

Question: *Is* 7153 *prime?*

Imagine that you did not have access to a calculator and you needed to answer this question. How would you do it?

A Bit More on Prime Numbers

Question: *Is* 7153 *prime?*

Imagine that you did not have access to a calculator and you needed to answer this question. How would you do it?

The *Primality Test* proposition can help us. . .

A Bit More on Prime Numbers

Question: *Is* 7153 *prime?*

Imagine that you did not have access to a calculator and you needed to answer this question. How would you do it?

The *Primality Test* proposition can help us. . .

We can try dividing 7153 by prime numbers, starting with 2, or 3 (or 7; since that is the first prime that that is not obviously not a factor), and continue until a factor is found or we come to a prime that is larger than $\sqrt{7153}$.

Okay — that can take some work, but since $84 < \sqrt{7153} < 85$, at least the amount of numbers we'll need to test is fairly limited.

A Bit More on Prime Numbers

Question: *Is* 7153 *prime?*

Imagine that you did not have access to a calculator and you needed to answer this question. How would you do it?

The *Primality Test* proposition can help us. . .

We can try dividing 7153 by prime numbers, starting with 2, or 3 (or 7; since that is the first prime that that is not obviously not a factor), and continue until a factor is found or we come to a prime that is larger than $\sqrt{7153}$.

Okay — that can take some work, but since $84 < \sqrt{7153} < 85$, at least the amount of numbers we'll need to test is fairly limited.

Now we just need an easy to find the prime numbers less than 84. . .

The Sieve of Eratosthenes

One way to generate a list of prime numbers from 2 up to some integer n is the *Sieve of Eratosthenes*.

1. Construct a list of numbers from 2 up to n.
2. Look for the first unmarked number in the list—this is a prime number. Call it p. Circle p then cross of all multiples of p in the remainder of the list.
3. Repeat the previous step until no unmarked numbers remain in the list. The circled numbers are the prime numbers up to n.

The Sieve of Eratosthenes Example

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Sieve of Eratosthenes Example

	2	**3**	~~4~~	**5**	~~6~~	**7**	~~8~~	~~9~~	~~10~~
11	~~12~~	**13**	~~14~~	~~15~~	~~16~~	**17**	~~18~~	**19**	~~20~~
~~21~~	~~22~~	**23**	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	**29**	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	**37**	~~38~~	~~39~~	~~40~~
41	~~42~~	**43**	~~44~~	~~45~~	~~46~~	**47**	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	**53**	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	**59**	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	**67**	~~68~~	~~69~~	~~70~~
71	~~72~~	**73**	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	**79**	~~80~~
~~81~~	~~82~~	**83**	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	**89**	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	**97**	~~98~~	~~99~~	~~100~~

Is 7153 Prime?

Returning to our problem: "Is 7153 a prime?", we now have a list of prime numbers to test:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 49, 61, 67, 71, 73, 79, 83.$$

$$7153 = 2 \cdot 3576 + 1$$
$$7153 = 3 \cdot 2384 + 1$$
$$7153 = 5 \cdot 1430 + 3$$
$$7153 = 7 \cdot 1021 + 6$$
$$7153 = 11 \cdot 650 + 3$$
$$7153 = 13 \cdot 550 + 3$$
$$7153 = 17 \cdot 420 + 13$$
$$7153 = 19 \cdot 376 + 9$$
$$7153 = 23 \cdot 311 + 0$$

Since we find that 7153 is a multiple of 23, we know that it is **not prime** and hence is *composite*.

As a bonus, since $17 < \sqrt{311} < 18$, we also know that 311 is prime. If this were not the case, then we would have found a prime factor of 311, and hence 7153, by the time we tried 17 as a factor of 7153.

Disproving Universal Statements: Counterexamples

Suppose S is a set and we are given a statement of the form

$$\forall x \in S, P(x).$$

To show that this is *true,* we need to show that $P(x)$ is true for all x in S.

To show is *false,* however, we merely need to show that $P(x)$ is false for at least one x in S. In other words, we need to find a *counterexample.*

If we are able to do this, we will have **disproved** the universal statement.

Disproving Universal Statements: Counterexamples

Conjecture

If n is a natural number, then $n < 3n - 2$.

Disproof. If $n = 1$, then $3n - 2 = 3 - 2 = 1$ and $1 \not< 1$.

Important note: it is **not** sufficient to say that a counterexample exists, or even to say what the counterexample is. You must *show* how the counterexample works so it is clear to the reader that it is indeed a counterexample.

In particular, saying $n = 1$ provides a counterexample to the conjecture above would not have been sufficient for an acceptable disproof.

Disproving Universal Statements: Counterexamples

Conjecture

If p is a prime number, then $2^p - 1$ is also prime.

This seems like it might be true...

p	$2^p - 1$	prime?

Disproof. The number 11 is prime but $2^{11} - 1 = 2047 = 23 \cdot 89$, so there is a prime p for which $2^p - 1$ is not prime.

Disproving Universal Statements: Counterexamples

Conjecture

If p is a prime number, then $2^p - 1$ is also prime.

This seems like it might be true...

p	$2^p - 1$	prime?
2	3	yes

Disproof. The number 11 is prime but $2^{11} - 1 = 2047 = 23 \cdot 89$, so there is a prime p for which $2^p - 1$ is not prime.

Disproving Universal Statements: Counterexamples

Conjecture

If p is a prime number, then $2^p - 1$ is also prime.

This seems like it might be true...

p	$2^p - 1$	prime?
2	3	yes
3	7	yes

Disproof. The number 11 is prime but $2^{11} - 1 = 2047 = 23 \cdot 89$, so there is a prime p for which $2^p - 1$ is not prime.

Disproving Universal Statements: Counterexamples

Conjecture

If p is a prime number, then $2^p - 1$ is also prime.

This seems like it might be true...

p	$2^p - 1$	prime?
2	3	yes
3	7	yes
5	31	yes

Disproof. The number 11 is prime but $2^{11} - 1 = 2047 = 23 \cdot 89$, so there is a prime p for which $2^p - 1$ is not prime.

Disproving Universal Statements: Counterexamples

Conjecture

If p is a prime number, then $2^p - 1$ is also prime.

This seems like it might be true...

p	$2^p - 1$	prime?
2	3	yes
3	7	yes
5	31	yes
7	127	yes

Disproof. The number 11 is prime but $2^{11} - 1 = 2047 = 23 \cdot 89$, so there is a prime p for which $2^p - 1$ is not prime.

Disproving Universal Statements: Counterexamples

Conjecture

If p is a prime number, then $2^p - 1$ is also prime.

This seems like it might be true...

p	$2^p - 1$	prime?
2	3	yes
3	7	yes
5	31	yes
7	127	yes
11	2047	no!

Disproof. The number 11 is prime but $2^{11} - 1 = 2047 = 23 \cdot 89$, so there is a prime p for which $2^p - 1$ is not prime.

Disproving Existence Statements

Next, suppose we have the statement of the form

$$\exists x \in S, P(x)$$

where S is a set.

To show that this is *true,* we need to show that $P(x)$ is true for *some* x in S, while to show this is *false*, we must show $P(x)$ is false for every x in S. Thus, to disprove the statement, we must prove the statement:

$$\forall x \in S, \sim P(x).$$

Disproving Existence Statements: Example

Consider the following very simple example.

Conjecture

There is a prime number between 61 and 67.

Note that this conjecture could restated as

Conjecture

$\exists x \in \{62, 63, 64, 65, 66\}, x$ *is prime.*

To disprove this, we must prove $\forall x \in \{62, 63, 64, 65, 66\}, x$ is not prime.

Disproof. Suppose x is an integer and $62 \leq x \leq 66$. No multiple of 2 is prime (except 2 itself), so x cannot be 62, 64, or 66. Since $63 = 7 \cdot 9$ and $65 = 5 \cdot 13$, x cannot be either of these values. Thus, x cannot be prime if $62 \leq x \leq 66$.

To Prove or Disprove...

In most non-textbook examples you are likely to come across, you won't necessarily know whether a statement is true or false.

In this case, the first thing to do is figure out whether or not the statement could be true. Often it is helpful to be skeptical, and look for a counterexample.

Conjecture

If $n \in \mathbb{Z}$ and $n^5 - n$ is even, then n is even.

This is a universal statement, so we could begin by trying some different integer values of n. We start with easiest integer to work with, 0:

n	$n^5 - n$	Is $n^5 - n$ even?	Is n even?

To Prove or Disprove...

In most non-textbook examples you are likely to come across, you won't necessarily know whether a statement is true or false.

In this case, the first thing to do is figure out whether or not the statement could be true. Often it is helpful to be skeptical, and look for a counterexample.

Conjecture

If $n \in \mathbb{Z}$ and $n^5 - n$ is even, then n is even.

This is a universal statement, so we could begin by trying some different integer values of n. We start with easiest integer to work with, 0:

n	$n^5 - n$	Is $n^5 - n$ even?	Is n even?
0	0	yes	yes

To Prove or Disprove...

In most non-textbook examples you are likely to come across, you won't necessarily know whether a statement is true or false.

In this case, the first thing to do is figure out whether or not the statement could be true. Often it is helpful to be skeptical, and look for a counterexample.

Conjecture

If $n \in \mathbb{Z}$ and $n^5 - n$ is even, then n is even.

This is a universal statement, so we could begin by trying some different integer values of n. We start with easiest integer to work with, 0:

n	$n^5 - n$	Is $n^5 - n$ even?	Is n even?
0	0	yes	yes
1	0	yes	no!

To Prove or Disprove. . .

In most non-textbook examples you are likely to come across, you won't necessarily know whether a statement is true or false.

In this case, the first thing to do is figure out whether or not the statement could be true. Often it is helpful to be skeptical, and look for a counterexample.

Conjecture

If $n \in \mathbb{Z}$ and $n^5 - n$ is even, then n is even.

This is a universal statement, so we could begin by trying some different integer values of n. We start with easiest integer to work with, 0:

n	$n^5 - n$	Is $n^5 - n$ even?	Is n even?
0	0	yes	yes
1	0	yes	no!

Disproof. Suppose $n = 1$. Then $n^5 - n = 1 - 1 = 0$, which is even since $0 = 2 \cdot 0$. Thus we have found an integer n for which $n^5 - 5$ is even but n is odd.

Examples

Conjecture

Every odd integer is the sum of three odd integers.

Conjecture

For all $a, b, c \in \mathbb{Z}$*, if* $a | bc$*, then* $a | b$ *or* $a | c$.

Conjecture

There exist prime numbers p *and* q *for which* $p - q = 97$.