MATH 13150: Freshman Seminar
Unit 8

1. Prime numbers

1.1. **Primes.** A number bigger than 1 is called *prime* if its only divisors are 1 and itself. For example, 3 is prime because the only numbers dividing 3 are 1 and 3. On the other hand, 6 is not prime because 2 divides 6, and 2 is neither 1 nor 6. A number bigger than 1 that is not prime is called *composite*. Mathematicians regard 1 as a special number; it is neither prime nor composite. This is a convention which is useful for later statements.
It is not so hard to test the first 20 numbers and decide which ones are prime, and which are composite:

$2, 3, 5, 7, 11, 13, 17, 19$ are prime.

$4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20$ are composite.

For example, 17 is prime because its only divisors are 1 and 17. 18 is composite since 3 divides 18. Verifying the above assertion about primes up to 20 can be verified in a similar way.
An important fact about numbers is that every number can be factored as a product of primes in only one way. For example,

$24 = 2 \times 2 \times 2 \times 3$, while

$117 = 3 \times 3 \times 13$.

There is no choice about how to do this, other than the order in which we write the prime factors. We can write $117 = 3 \times 13 \times 3$, but we don't regard this as different from writing $117 = 3 \times 3 \times 13$.

Theorem 1.1. *(FUNDAMENTAL THEOREM OF ARITHMETIC) Any number bigger than* 1 *can be written as a product of prime numbers. Further, there is only one way to factor each number, up to reordering of the factors.*

This includes numbers that are prime numbers. When we take the number 3, we just write 3, and that is the prime factorization, i.e., it is a product of one number.
This is a very important theorem. It isn't so hard to see why every number can be written as a product of primes. It's more or less the argument you use when you find the prime factorization. For example, suppose we want to find the prime factorization of 5544.
First, we note that 5544 is even, so it is divisible by 2. Dividing by 2, we get $5544 = 2 \cdot 2772$. We keep dividing by 2 until we get an odd number:

$$5544 = 2 \cdot 2772 = 2 \cdot 2 \cdot 1386 = 2 \cdot 2 \cdot 2 \cdot 693.$$

Now we have to find a divisor of 693. We can try 3, and $693 = 3 \cdot 231$,and we keep dividing by 3 to get:

$$5544 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 231 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 77.$$

But $77 = 7 \cdot 11$ (probably you can see this yourself: if not, note that 5 does not divide 77, so then try 7, which does it for us). Since 7 and 11 are prime, we have found that

$$5544 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 7 \cdot 11$$

is the prime factorization of 5544.
The same kind of argument explains why every number can be written as a product of primes. Take a number n bigger than 1. If it is prime, then n is a product of primes (just one, but that's OK for us), so we've done it. If n is not prime, then n is a product of two smaller numbers $n = n_1 \cdot n_2$. If n_1 or n_2 is prime, we set it aside. If n_1 and/or n_2 is not prime, we can factor it into smaller numbers, etc, etc. It is pretty clear this will end up with a factorization into primes, and that is more or less what I just did with 5544.

PROBLEM: Factor 257 into a product of prime numbers.

This is actually a trick question. 257 is a prime number itself, so no work is required. $257 = 257$ solves the problem. But how would you know that 257 is prime without me telling you? You could check every number from 2 through 256, but this takes quite a long time. In the next two sections, we'll see two different ways of finding primes.

1.2. **How to tell if a number is prime.** Let's consider the following problem:

PROBLEM: Is 103 a prime?
To solve this, you can just go through the numbers from 2 to 102 and see if any of them divide 103. If one of them does, than 103 is composite. Otherwise, 103 is prime. If you try this, you'll see pretty quickly that you don't need to check all numbers. For example, you can see that 2 does not divide 103 since 103 is odd, and 2 only divides even numbers. Since 2 does not divide 103, it follows that no even number can divide 103. For example, if 6 did divide 103, this would mean that $103 = k \cdot 6$ for some number 6. But then $103 = k \cdot 3 \cdot 2$, so 2 would have divided 103, which is impossible. The same idea shows that:

Remark 1.2. *Suppose n is a number. If no prime less than n divides n, than no composite number less than n divides n, so n is prime.*

This means that to decide whether 103 is prime, we only need to go through all the primes less than 103, and see whether any of them divide 103. If one does, than 103 is not prime, and otherwise 103 is prime.
If you try doing this, you'll see that $2, 3, 5, 7, 11, 13, 17$, and 19 all do not divide 103. You can probably see that no prime between 52 and 102 is going to divide 103. For example, 59 is prime, and 59 is not going to divide 103, because if it did, $103 = 59 \cdot k$,

where k is 2 or larger. But then $59 \cdot k \geq 59 \cdot 2 > 103$, so $59 \cdot 2$ cannot be 103. So this means that we only need to check all primes less than 52.
In fact, we can stop long before we get to 52. Indeed,

Remark 1.3. *If a number n is not prime, then n must be divisible by a prime less than or equal to $\sqrt{n}$.*

For example, for $n = 103$, we only need to check primes less than or equal to $\sqrt{103}$, which is about 10.1. We express this by writing $\sqrt{103} \simeq 10.1$. So we only need to see whether any of $2, 3, 5$ or 7 divide 103. Using a calculator, you can see none of them do, so 103 is prime.
Let's think about why we can stop at $\sqrt{n}$ in the example where $n = 103$. Suppose 103 were not prime, so it factors as a product of two or more primes. We know it doesn't have 2, 3, 5, or 7 as a prime factor, but why can't 103 factor as $11 \cdot 13$? The reason is quite simple. Certainly $11 > \sqrt{103} \simeq 10.1$ and $13 > \sqrt{103} \simeq 10.1$. Then $11 \cdot 13 > \sqrt{103} \cdot \sqrt{103}$. But $\sqrt{103} \cdot \sqrt{103} = 103$, so certainly $11 \cdot 13 > 103$. Since $11 \cdot 13$ is bigger than 103, certainly $11 \cdot 13$ cannot equal 103.
We can apply the same argument to a general number n. Suppose n has no prime factors less than or equal to $\sqrt{n}$. If n were to be composite, than n would have at least two prime factors p and q, and $p > \sqrt{n}$ and $q > \sqrt{n}$. But then

$$p \cdot q > (\sqrt{n})^2 = n,$$

so it cannot be the case that $p \cdot q$ is a factor of n. This means n could not possibly have been composite, so n is prime.
This gives us the following procedure for checking whether a number n is prime.

Remark 1.4. *PROCEDURE FOR CHECKING WHETHER n IS PRIME:*
Check whether any of the primes less than or equal to $\sqrt{n}$ divides n. If one of them does, than n is composite. If none of them does, than n is prime.

For carrying out this procedure, it is useful to know how to tell whether certain small primes divide a number.

Remark 1.5. *TESTS TO DETERMINE WHETHER 2, 3, 5, OR 11 DIVIDE A NUMBER n*
(2-divisibility test) 2 *divides a number n exactly when n is even.*
(3-divisibility test) 3 *divides a number n exactly when* 3 *divides the sum of the digits of n.*
(5-divisibility test) 5 *divides a number n exactly when the last digit of n is* 0 *or* 5.
(11-divisibility test) 11 *divides a number n exactly when* 11 *divides the alternating sum of the digits of n.*

For the cases of 2 and 5, it is easy to see why these tests work; they are based on your experience of knowing what multiples of 2 and 5 can look like. We will justify the cases of 3 and 11 in a later chapter. For now, let's see how this works.

Example 1.6. *(1) The number* 23457 *is divisible by* 3 *because the sum of the digits of* 23457 *is* $2 + 3 + 4 + 5 + 7 = 21$*, which is divisible by* 3.

(2) The number 13856 *is not divisible by* 3 *because the sum of the digits of* 13856 *is* $1+3+8+5+6=23$*, and* 23 *is not divisible by* 3*.*
(3) The number 123431 *is divisible by* 11 *because the alternating sum* $1-2+3-4+3-1=0$ *is divisible by* 11 *(*0 *is a multiple of* 11 *since* $0=0\cdot 11$*. Similarly,* 0 *is divisible by any number).*
(4) The number 41327 *is divisible by* 11 *since the alternating sum* $4-1+3-2+7=11$ *is divisible by* 11*. Also the number,* 1429241 *is divisible by* 11*, since the alternating sum* $1-4+2-9+2-4+1=-11$ *is a multiple of* 11 *(*$-11=-1\cdot 11$*).*
(5) The number 32345 *is not divisible by* 11 *since the alternating sum* $3-2+3-4+5=5$ *is not divisible by* 11*.*

PROBLEM: Decide whether 263 and 323 are prime?

Let's try this for 263. Compute $\sqrt{263}\simeq 16.2$. The primes less than 16.2 are $2,3,5,7,11$ and 13. Certainly 2 and 5 do not divide 263 since 263 is not even, and does not end in 5 or 0. 3 does not divide 263 since the sum of its digits is 11, which is not divisible by 3. Similarly, 11 does not divide 263 since the alternating sum $2-6+3=-1$ is not a multiple of 11. Further, 7 and 13 do not divide 263 by a calculator check. We conclude that 263 is prime.
Let's try this for 323. $\sqrt{323}\simeq 17.9$, so we need to check that none of the primes $2,3,5,7,11,13$ or 17 divides 323. But $\dfrac{323}{17}=19$, so 17 divides 323, and 323 is not prime.

1.3. **The sieve of Eratosthenes.** There is a method for finding primes that was discovered by the ancient Greeks for finding primes. We'll illustrate it by looking for primes between 21 and 40. First, we list all the numbers from 21 to 40:

$21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40$

The idea is to cross out all numbers on the list that are composite. The numbers that remain are prime.
So first cross out multiples of 2 on the list, obtaining

$21,\ \not{2}2,23,\ \not{2}4,25,\ \not{2}6,27,\ \not{2}8,29,\ \not{3}0,31,\ \not{3}2,33,\ \not{3}4,35,\ \not{3}6,37,\ \not{3}8,39,\ \not{4}0$

When we write $\not{2}2$, that means we are crossing out 22.
Now cross out also multiples of 3 on the list, obtaining

$\not{2}1,\ \not{2}2,23,\ \not{2}4,25,\ \not{2}6,\ \not{2}7,\ \not{2}8,29,\ \not{3}0,31,\ \not{3}2,\ \not{3}3,\ \not{3}4,35,\ \not{3}6,37,\ \not{3}8,\ \not{3}9,\ \not{4}0$

Now cross out multiples of the next prime 5 on the list, obtaining

$\not{2}1,\ \not{2}2,23,\ \not{2}4,\ \not{2}5,\ \not{2}6,\ \not{2}7,\ \not{2}8,29,\ \not{3}0,31,\ \not{3}2,\ \not{3}3,\ \not{3}4,\ \not{3}5,\ \not{3}6,37,\ \not{3}8,\ \not{3}9,\ \not{4}0$

If we then cross out multiples of the next prime, which is 7, from the list, we would cross out 21, 28, and 35. They are already crossed out, so crossing out multiples of 7 does nothing more. There is a good reason for this. Indeed, if a number is still not crossed out, that means that it is not a multiple of a prime less than 7. But we have already seen in the last section that if a number less than or equal to 40 is

not divisible by a prime less than $\sqrt{40}$, which is approximately 6.3, than it is prime. Indeed, this is precisely what is stated in Remark 1.3.
The primes between 21 and 40 are the numbers remaining on the list, i.e., $23, 29, 31, 37$.

PROCEDURE FOR FINDING ALL PRIMES BETWEEN TWO NUMBERS a and b:
For each prime less than or equal to $\sqrt{b}$, cross out all multiples of the prime. The remaining numbers are the primes between a and b.

PROBLEM : List all primes from 100 to 110.

To do this, compute $\sqrt{110} \simeq 10.5$. The primes less than or equal to 10.5 are $2, 3, 5, 7$. Now list the numbers from 100 to 110:

$100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110$

and cross out multiples of 2 giving:

$\not{1}00, 101, \not{1}02, 103, \not{1}04, 105, \not{1}06, 107, \not{1}08, 109, \not{1}10$

Next, cross out multiples of 3, starting with $102 = 3 \cdot 34$, the first multiple of 3 on the list, giving:

$\not{1}00, 101, \not{1}02, 103, \not{1}04, \not{1}05, \not{1}06, 107, \not{1}08, 109, \not{1}10$

and then successively, cross out multiples of 5 (beginning with 100), and multiples of 7 (which means only cross out 105, as that is the only multiple of 7 on the list). Neither of these steps omit any new numbers. We conclude that the remaining numbers $101, 103, 107, 109$ are the primes from 100 to 110.
Using the sieve of Eratosthenes, it is not terribly difficult to list the primes up to 100. They are:

$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$

1.4. **How many primes are there?** You may have at some point wondered whether there is a largest number, or been asked this question by a kid learning about numbers. It isn't hard to see there is no largest number, which is another way of saying that there are infinitely many numbers which keep getting bigger and bigger. For example, to see that $1,000,000$ is not the largest number, you can just add one to it to get $1,000,001$, which is bigger. Or to see that $999,999,999$ is not the largest number, we can add one to get $1,000,000,000$, which is larger. In general, we can say that a number n is not the largest number, because $n + 1$ is a bigger number.
With primes, life is not so simple, because if n is a prime number, the next biggest number $n + 1$ is not going to be prime. For example, if n is not 2, then n is odd, so $n + 1$ is even, and hence composite. Nevertheless, our old friend Euclid found a way to show that there is no biggest prime number, or otherwise stated, there are infinitely many primes.

Theorem 1.7. *(credited to Euclid) There are infinitely many prime numbers.*

The outline of the argument goes like this. Suppose there were a biggest prime number p. Then there would certainly be finitely many primes, and we can say there are k primes up to p. Then we could list all the prime numbers up to p,

$p_1 = 2, p_2 = 3, \ldots, p_k = p.$

Now suppose from this list, we can produce a new prime number q that is not on the list. Since the list has all the primes up to p, this means that q must be a bigger prime number than p, so our assertion that there was a biggest prime was wrong. Hence, there can be no biggest prime.
To complete the argument, we still have to produce a new prime q not on the above list. To do this, we can multiply all the primes on the list to get:

$p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_k$, and we'll call this number N. Clearly, $N = p_1 \cdot p_2 \cdots p_k$ is the prime factorization of N.

Now, let's think about the number $N + 1$. Since every number is a product of primes (by the Fundamental Theorem of Arithmetic), there has to be a prime q dividing $N + 1$. But then q *cannot* divide N, since there is a gap of q between consecutive multiples of q. Hence, both $N + 1$ and N, which is one less than N, are not both multiples of q. Since q does not divide N, q cannot be one of the primes $p_1, \ldots, p_k$ on the list. This completes Euclid's argument.
We can understand this argument a little better by imagining that we don't know any primes beyond 5. How can we then find a bigger prime? Well, let's consider the primes up to 5:

$2, 3, 5$

and multiply them together to get the number $N = 2 \cdot 3 \cdot 5 = 30$. Now add 1 to $N = 30$ to get 31. Applying the tests we learned in the previous sections, we can see that 31 is prime, so if we didn't know about 31 already, we'd have found that 31 is prime.
If we try the same argument beginning with the list $2, 3, 5, 7$, we see that $N = 2 \cdot 3 \cdot 5 \cdot 7 = 210$, so $N + 1 = 211$. Again, using prime tests we can show 211 is prime, so we've found a new prime.

1.5. **Prime Deserts.** If you look at the list of primes up to 100, you can see that we can find 7 consecutive composite numbers starting with 90:

$90, 91, 92, 93, 94, 95, 96.$

There's a more systematic way to find 7 consecutive composite numbers. We'll start with the number 8!. Now consider the list of 7 consecutive numbers:

$8! + 2, 8! + 3, 8! + 4, 8! + 5, 8! + 6, 8! + 7, 8! + 8.$

The first number on the list, $8! + 2 = 2 \cdot (\frac{8!}{2} + 1)$, so it is not prime since 2 divides it.
The second number on the list, $8! + 3$ can be written as $8! + 3 = 3 \cdot (\frac{8!}{3} + 1)$, so it is not prime since 3 divides it. We are using the easy fact that 3 divides 8! evenly, since

$8! = 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2$ has a factor of 3 in it. Similarly, all other numbers on the list are composite. Just take a number $8! + k$ on the list, and write it as $k \cdot (\frac{8!}{k} + 1)$ to factor it as a product of smaller numbers. k divides 8!, because k is one of the factors of 8!. We call this sequence of numbers a *prime desert*. This is intended to evoke an image of someone riding a camel along a road with mile markers. The landscape is mostly desert, but there is an oasis at each mile marker that marks a prime number. Then the number of miles between any two oases is the gap between the corresponding primes. The desert is especially wide when there is a large gap between consecutive primes on the list of all primes.
We can produce a prime desert of any length that we like. For example, to produce a prime desert of length 100, we just look at the list:

$$101! + 2, 101! + 3, \ldots, 101! + 99, 101! + 100, 101! + 101.$$

Just as before, no number on this list is prime, so this is a list of 100 consecutive numbers that are not prime.
In addition to these prime deserts, there are also primes that are quite close to each other. For example, 101 and 103 are both prime, and 107 and 109 are both prime. We call two prime numbers that are within two of each other *twin primes*. For example, 1607 and 1609 are twin primes. It is believed to be the case that there are infintely many pairs of twin primes, but no one knows for sure if this is true.
There are lots of interesting things known about primes. Later, we will discuss a result that says if you start with a random 100 digit number, there is roughly a fifty/fifty chance that one of the next 240 numbers after our 100 digit number is prime.

EXERCISES: Explain your answer.

(1) Determine whether each of the following numbers is prime. If the number is not prime, give its prime factorization:
   (a) 169
   (b) 113
   (c) 187
   (d) 560
   (e) 667
   (f) 319
   (g) 851
(2) Use the sieve of Erastosthenes to find all primes from 200 to 220.
(3) Use the sieve of Erastosthenes to find all primes from 390 to 400.
(4) Find a prime that divides $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$.
(5) Explain how to find a prime desert of length 13.
(6) Find the first two primes after 500.