Some Results About Prime Numbers
Pre-class, Week 4

Number theory is the field of mathematics that studies properties of numbers, specifically positive integers and certain subsets of the positive integers, and their relationships. If you haven't already, check out `https://www.math.brown.edu/~jhs/frintch1ch6.pdf` (first 11 pages) for a neat introduction to number theory including examples of some fun number theory questions. Number theory is also the breeding ground for many open questions in mathematics. If you look at the list of "open conjectures" on this Wikipedia page, you will notice that most are from the field of number theory. Sadly, among the list of "proven conjectures", number theory is not the majority. In other words, number theory conjectures are easy to make and state, but hard to prove. During this week, we will learn some old and newer results/conjectures related to prime numbers specifically.

Sieve of Eatosthenes: To determine if a number n is prime, we can use trial division. In fact, it is enough to try dividing by numbers up to $\sqrt{n}$ since any composite number n has a divisor d such that $1 < d \leq \sqrt{n}$. Furthermore, it is enough to test dividing by prime numbers smaller than $\sqrt{n}$ since the smallest divisor of n greater than 1 will have to be a prime. This process is reasonably fast for small n's but trial division becomes very inefficient quickly for testing primality of one number n. Still, this idea can efficiently determine all the primes less than a given certain number using a simple and ingenuous approach called the *Sieve of Eratosthenes*, named after the Greek mathematician Eratosthenes.

We start out by writing all the integers from 2 to n and then sieving out the composite numbers. In the first step, we circle 2, the first number in the list, and cross out all the other multiples of 2 from the list. We then move to the next integer not struck out, 3, and circle it, and cross out all the other multiples of 3 from the list. We continue crossing out until we remove all the multiples of the numbers not exceeding $\sqrt{n}$. At that point, we circle all the remaining numbers larger than $\sqrt{n}$.

1. Apply the Sieve of Eratosthenes to find all the primes less than 100.

	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~~

Once we start this process, one immediate question comes to mind: "Are there infinitely many primes?" In other words, if we continue the sieve for a while, will all numbers eventually be struck out or will there be numbers left? We hope that there will be some numbers left since there are many internet security protocols using really large prime numbers. But, how do we really know that there are infinitely many primes? Euclid considered this same question back in the day (check out the exact date on a history page) and came up with an idea similar to the following.

Suppose there are only a finite number of primes, say $p_1, p_2, \ldots, p_r$ and consider $n = p_1 p_2 \cdots p_r + 1$. Clearly $n > p_i$ for $i = 1, 2, \ldots, r$, so n must be composite (by our assumption that p_i are the only primes). Using prime factorization of integers (which we will prove), there must be p_k which divides n. Note that p_k also divides $p_1 p_2 \cdots p_r$, therefore p_k divides $1 = n - p_1 p_2 \cdots p_r$, which is a contradiction since 1 does not have any factors besides itself.

This proves:
Theorem 1: (Euclid) There are infinitely many primes.

Another question about the sieve might come to your mind: "Can we have an arbitrarily large gap between two primes?" So maybe we don't cross off all numbers after some point, but maybe cross off a long chunk of them? Indeed, this happens.

Proposition 2: Given any $N > 1$, there exist consecutive N composite numbers.

proof: Let $a = (N+1)! + 2$. Since $2, 3, 4, \ldots, N+1$ all divide $(N+1)!$, then $k+2 | (N+1)! + (k+2)$ for all $k = 0, 1, 2, \ldots, N-1$. But $(N+1)! + (k+2) = a + k$, which are exactly N consecutive numbers $a, a+1, a+2, \ldots, a+N-1$.

Now that we got a positive answer in this direction, we consider the other direction: "Is it possible to have infinitely primes close to each other?" Since two consecutive numbers cannot be prime both, we need to have them at least two apart. A **twin prime** is either of a pair of primes that are two apart, such as 3 or 5; 5 or 7; 11 or 13; 17 or 19; and 29 or 31.

2. a. Find four other twin prime pairs (i.e. 8 total primes). For this one, don't look up online but come up with a method of your own.

41 & 43 59 & 61

71 & 73 101 & 103

b. Did you notice any properties that twin primes should have from your investigation?

must be $\equiv 1$ & $\equiv 5$ mod 6

The Twin Prime Conjecture (TPC) states that there are infinitely many twin prime pairs. There has been awesome recent results in this specific area, following a breakthrough paper by Yitang Zhang in 2013. His result showed that there are infinitely many pairs of primes that lie between N and $N + 70,000,000$ for some N. The reason why this result is related to the TPC is that TPC claims that if we keep the gap between numbers to be 2, i.e. N and $N + 2$, then there are infinitely many pairs of primes that lie in that gap. Although 70,000,000 may look like it's far from 2, it is still a finite number, which did not exist before. Read more about this result in a nice, accessible Quanta article. In addition to the novelty of the result in a field that has been begging for answers for years, there is a very interesting personal story behind the paper. When this paper came out, Professor Zhang was working as a lecturer (non-tenured contract position) at the University of New Hampshire after having failed to find a more stable academic job, did not have any previous outstanding work and was 58 (or 57?) years old. See more about his life including what he is up to now at `https://en.wikipedia.org/wiki/Yitang_Zhang`.

After Zhang's paper, many mathematicians immediately set out to improve Check out Polymath8 project page listing works done by a collaborative effort on this area. As you can see, the gap has been brought down to 246 (without assuming any other results) and down to 6 or 12 (assuming generalized or just plain Elliott-Halberstam conjecture). Finally, a funny personal connection. One of the people who work in this field, Yalçın Yıldırım, was my first senior thesis advisor in my undergraduate.

3. Another famous number theory conjecture is Goldbach conjecture. This conjecture states that every even integer greater than two is the sum of two prime numbers.

a. Test the conjecture is true up to 30.

$4 = 2+2$
$6 = 3+3$
$8 = 3+5$
$10 = 3+7$

$12 = 7+5$
$14 = 7+7$
$16 = 13+3$
$18 = 13+5$
$20 = 13+7$

$22 = 19+3$
$24 = 19+5$
$26 = 19+7$
$28 = 23+5$
$30 = 23+7$

b. The conjecture has been tested up to 4×10^{17}. Can you think of an algorithm to test it yourself for large numbers (maybe not 4×10^{17} large, but larger than 1000)?

```
primes = [...]   # list of primes < n
for n in range(4, 2000, 2):
    i, j = 0, len(primes)-1
    while primes[i] + primes[j] != n:
        if primes[i]+primes[j] < n:
            i += 1
        elif primes[i]+primes[j] >n:
            j -= 1
    print(f"{n} = {primes[i]} + {primes[j]}")
```

c. The Goldbach conjecture is also known as the Strong Goldbach conjecture. The weaker version says: "all odd numbers greater than 5 are the sum of three odd primes." Explain why the strong conjecture implies the weak conjecture. (Side note: There is a proof of this weaker version by Harald Helfgott which seems to be accepted widely, but is not published. Read more at https://blogs.scientificamerican.com/roots-of-unity/goldbach-variations/.)

d is odd so $d=2k+1$ & we want 3 primes to sum to d

$d-3$ is even so if $d-3$ has 2 primes that sum to it, use thos primes $+3$ to obtain d.

And, to end, here is an appropriate quote on primes by none other than famous Gauss, a fan of number theory as expressed in another quote "Mathematics is the queen of the sciences and number theory is the queen of mathematics."

"The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. It has engaged the industry and wisdom of ancient and modern geometers to such an extent that it would be superfluous to discuss the problem at length... Further, the dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated." (Carl Friedrich Gauss, Disquisitiones Arithmeticae, 1801)

You can find any interesting sequence online at the Online Encyclopedia of Integer Sequences. Check out the Twin primes list: https://oeis.org/A001097.