Maths 190 Lecture 4

- **Topic for today:** **Prime numbers**

- **Vitally important question**:

  Can you write 71 as the product of two smaller numbers?

Division

- How do we find the factors of a number?
- We say that m divides evenly into N if there is another integer k such that $m \times k = N$.
- m and k are factors of N.
- Otherwise, there is a remainder, that is

$$N = q \times m + r, \quad \text{and } 0 \leq r \leq m - 1$$

- Write the following numbers as products of smaller numbers:
  - $36 = 2 \times 18 = 2 \times 2 \times 9 = 2 \times 2 \times 3 \times 3$
  - $42 = \ldots$
  - $45 = \ldots$

Definition

- A natural number is a prime number if is cannot be expressed as a product of smaller natural numbers.

- Examples:

Prime factors

- What are the prime factors of 423?

Finding prime factors

- Pick a number between 300 and 500.
- Swap numbers with someone else.
- Find the prime factors of your number.
- Is your number prime?
- How many primes do you need to check as factors to be sure?

Prime factorization

- Theorem: Every natural number greater than one is either a prime number or can be expressed as a product of prime numbers.

- The prime factorisation of any number is unique.

Finding prime numbers

- In a search for primes, we can rule out anything that is a multiple of a prime.
- If p is prime, then $k \times p$ is not prime, for $k > 1$.
- Using the sieve cross out all multiples of 2, 3, 5, etc...
- Why don't I have to cross out multiples of 4, 6, 8, 9, etc?

How many prime numbers are there?

- How many less than 100?
- How many less than 1000?
- How many less than 1,000,000?

- Number of primes less than n is roughly $\frac{n}{\log n}$

- How many all together?

How many prime numbers are there?

- Theorem: There are *infinitely* many primes.
- Proved by Euclid, 2000 years ago.
- Proof relies on assuming that there are *not* infinitely many primes, and finding a contradiction. This shows the assumption is false.

Proof by contradiction

- We want to prove some statement, call it A.

- Start by assuming statement A is *false*.
- Follow a logical set of steps.
- End up with a contradiction.
- Therefore either there was a mistake in our logical set of steps, or our assumption was incorrect.

A simple example

- Prove that there are infinitely many positive even numbers.

- Assume that there are only finitely many positive even numbers.
- Then there must be a largest one, call it m.
- Now suppose $n = m + 2$.
- n is even, because it is the sum of two even numbers.
- $n > m$
- But we said m was the greatest even number - contradiction!

Finding a number not a multiple of...

- Suppose we have a list of numbers, say 2, 3, 7.
- How can I find a number that is *not* a multiple of any number in my list?
- Multiply them together and add 1.
- So $2 \times 3 \times 7 + 1 = 43$ is not a multiple of any of these numbers.
- In particular, the remainder when dividing by any of these numbers is 1.

Proof

- Suppose there are finitely many primes. List them from smallest to largest, $p_1, p_2, \ldots, p_s$.
- Now find the product of all these primes, and add 1.

$$N = p_1 \times p_2 \times p_3 \times \cdots \times p_s + 1$$

- By the prime factorisation theorem, N is either prime, or has a prime factorisation.

Proof continued...

- Clearly N is not a multiple of any of $p_1, \ldots p_s$. Therefore it must be prime itself.
- But $N > p_s$, which is the largest prime, so N can't be prime.
- A contradiction! Our assumption must be wrong, so there is no largest prime number; there must be infinitely many primes.

Can we find large primes?

- Note that even though we showed larger primes must exist, we did not actually find a particular one.
- It is *very* difficult to factor large numbers.
- Try it!

- Consequently it is very difficult to find large prime numbers (even though we know they exist!)

Other prime problems

- Twin primes: pairs of prime numbers p, $p + 2$
- Find some examples from your sieve.
- Unsolved problem: are there infinitely many twin primes?

- We can find *arbitrarily long* arithmetic sequences of primes.
- Proved by Green and Tao in 2004.

Important ideas from today:

- All natural numbers can be built up as products of prime numbers
- There are an infinite number of prime numbers.

For next time

- Read Section 2.5 of the textbook.
- Bring something with a **barcode** on it to the next class.