Lecture 4 - The Fundamental Theorem of Arithmetic

Recall that a natural number $p \in \mathbb{N}$ is called prime if its only divisors are 1 and itself; by convention, 1 is not considered prime, and so the first few primes are

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$$

In this lecture we'll prove an important result called "the fundamental theorem of arithmetic" which shows that prime numbers are the building blocks of the natural numbers, in the sense that every natural can be written as a product of primes. The proof will require us to use a proof technique known as "mathematical induction," and so we'll start this lecture by first describing induction.

The idea with induction is that we want to prove ~~make~~ some statement dependent on an integer N by relating it to statements about $N-1$, and possibly also $N-2$ and $N-3$ and $N-4$ and ... This process is easiest to explain with an example.

Example

Find a formula for the sum of the first N powers of 2, starting from power 0, and prove this formula is correct.

First let's collect some data by making a table containing these sums:

N	$\sum_{i=0}^{N-1} i$	$=$
1	$2^0 = 1$	$=1$
2	$2^0 + 2^1 = 1+2$	$=3$
3	$2^0+2^1+2^2 = 1+2+4$	$=7$
4	$2^0+2^1+2^2+2^3 = 1+2+4+8$	$=15$
5	$1+2+4+8+16$	$=31$
6	$1+2+4+8+16+32$	$=63$

We may notice that our sums $\sum_{i=0}^{N-1} 2^i$ equals $2^N - 1$ in each example above, and so we may conjecture that for each $N \in \mathbb{N}$, $\sum_{i=1}^{N-1} 2^i = 2^N - 1$.

If this is true, then it should be that

$$1+2+4+8+\cdots+2^{99}+2^{100}$$

is equal to $2^{101}-1$. We can write some simple code in Sage to test this:

```
def sum_of_powers(N):
    sum = 0
    for i in range(0,N)
        sum += 2^i
    return sum
```

Evaluating sum-of-powers(101) tells us

$$\sum_{i=0}^{101} 2^i = 2{,}535{,}301{,}200{,}456{,}458{,}802{,}993{,}406{,}410{,}751$$

Evaluating $2^{101}-1$ in Sage also gives the same answer, so we feel confident in our conjecture. But how can we prove it?

It's easy for us to directly verify the conjecture for the smallest values of N, such as $N=1$:

$$\sum_{i=0}^{1-1} 2^i = \sum_{i=0}^{0} 2^i = 2^0 = 1 = 2^1 - 1$$

For a large value of N, let's try to relate our conjecture to smaller values of N:

$$\sum_{i=0}^{N-1} 2^i = 2^{N-1} + \sum_{i=0}^{N-2} 2^i$$

if we knew the conjecture held for $N-1$, meaning

$$\sum_{i=0}^{N-2} 2^i = 2^{N-1} - 1$$

then we could write

$$\sum_{i=0}^{N-1} 2^i = 2^{N-1} + \sum_{i=0}^{N-2} 2^i$$
$$= 2^{N-1} + 2^{N-1} - 1$$

But

$$\begin{aligned}2^{N-1}+2^{N-1}-1 &= 2\cdot 2^{N-1}-1\\ &= 2^{N}-1\end{aligned}$$

and so if we know the conjecture works for $N-1$, we can show it also holds for N.

We've already verified the conjecture for $N=1$, so the above argument tells us the conjecture works for $N=2$. Once we know the conjecture holds for $N=2$, the above argument shows us that it holds for $N=3$ as well — but then we apply the argument again to get the result for $N=5$, and $N=6$, and $N=7$, and $N=8$, ... Thus we have shown that for every $N\in\mathbb{N}$,

$$\sum_{i=0}^{N-1} 2^{i} = 2^{N}-1.$$

Notice our proof above has two important pieces: we did need to directly verify the conjecture for $N=1$ (this is called the <u>base case</u>), and we need to show that if the conjecture hold for $N-1$, it also holds for N (this is the <u>inductive step</u>).

Let's do another ~~a more~~ example:

Theorem

For each $n \in \mathbb{N}$, $8 \mid 3^{2n} - 1$.

Pf

First we directly verify the base case when $n = 1$. If $n = 1$, then $3^{2n} - 1 = 3^2 - 1 = 9 - 1 = 8$, and $8 \mid 8$.

For the inductive step we want to show that $8 \mid 3^{2n} - 1$, assuming $8 \mid 3^{2(n-1)} - 1$. If $8 \mid 3^{2(n-1)} - 1$, then we can write

$$3^{2(n-1)} - 1 = 3^{2n-2} - 1 = 8j$$

for some $j \in \mathbb{N}$. Now we'll try to manipulate $3^{2n} - 1$ to work this $8j$ in.

$$\begin{aligned}
3^{2n} - 1 &= 3^{2n+2-2} - 1 \\
&= 3^{2+2n-2} - 1 \\
&= 3^2 \cdot 3^{2n-2} - 1 \\
&= 9 \cdot 3^{2n-2} - 1 \\
&= 9 \cdot 3^{2n-2} - 1 - 8 + 8 \\
&= 9 \cdot 3^{2n-2} - 9 + 8 \\
&= 9 \cdot (3^{2n-2} - 1) + 8 \\
&= 9 \cdot 8j + 8 \\
&= 8(9j + 1)
\end{aligned}$$

Thus $8 \mid 3^{2n} - 1$.

□

Now we have most of what we'll need to prove the fundamental theorem of arithmetic, but we also need a few simple facts about primes.

Lemma

Let $a, b \in \mathbb{N}$ and suppose $p \in \mathbb{N}$ is a prime number. If $p | ab$, then $p | a$ or $p | b$.

Pf

Suppose, without loss of generality, that $p \nmid a$. We then need to show that $p | b$. Notice that because $\gcd(p,a) = 1$ (the only divisors of p are 1 and p, but by assumption $p \nmid a$, so 1 is the only thing that divides both a and p), there exist integers x and y solving the equation

$$ax + py = 1.$$

Thus

$$abx + pby = b.$$

By assumption, $p | ab$, so $ab = pj$ for some j, and we may write

$$\begin{aligned} & pjx + pby = b \\ \Rightarrow\ & p(jx + pb) = b \\ \Rightarrow\ & p | b. \end{aligned}$$

□

This lemma easily extends to products of any (finite) number of values.

Lemma

Let $a_1, a_2, \dots, a_n \in \mathbb{N}$ and suppose $p \mid a_1 \cdots a_n$, p a prime. Then $p \mid a_i$ for some $1 \leq i \leq n$.

Pf

Exercise. Think inductively. $\square$

Now we reach the dénouement:

Theorem (The Fundamental Theorem of Arithmetic)

Every $m \in \mathbb{N}$ can be factored into a product of prime numbers,

$$m = p_1 \cdot p_2 \cdot \dots \cdot p_n$$

and this factorization is unique, up to re-ordering the primes $p_1, \dots, p_n$.

Pf

Throughout the proof we will assume $m \geq 2$, and you can think about the case $m = 1$ as an exercise.

We proceed by induction. For the base case notice if $m = 2$, then the prime factorization is trivial: $2 = p_1$. (Be sure you understand why this is the only possibility.)

Now suppose that for each $2 \leq q < m$, we know q has a prime factorization.

If m is prime, we have its prime factorization immediately. If m is not prime, then it can be written as a product of two numbers,

$$m = q_1 q_2$$

but $2 \leq q_1, q_2 < m$ and so our induction hypothesis gives us prime factorizations of q_1 and q_2 — say

$$q_1 = p_1 p_2 \cdots p_n$$
$$q_2 = p_1' p_2' \cdots p_r'$$

and thus we have a prime factorization for m,

$$m = p_1 p_2 \cdots p_n p_1' p_2' \cdots p_r'.$$

This shows every natural number $m \geq 2$ may be written as a product of primes.

Now we show the prime factorization is unique. Suppose m had two prime factorizations,

$$m = p_1 \cdot p_2 \cdot \ldots \cdot p_n$$
$$m = p_1' \cdot p_2' \cdots p_r'$$

Notice that $p_1 | m$, so $p_1 | p_1' \cdots p_r'$. By our earlier lemma, $p_1 | p_i'$ for some p_i'. But this means $p_1 = p_i'$. Rearranging the p_i''s as necessary, we may assume $p_1 = p_1'$. Dividing both prime factorizations by $p_1 = p_1'$, we have

$$p_2 p_3 \cdots p_n = p_2' p_3' \cdots p_r'$$

But we can just rinse and repeat to get $p_2 = p_2'$, $p_3 = p_3'$, and so on. If $n = r$, we'd be done. Showing n must equal r is left as an exercise for you. □