Recap :

PMI : $P : \mathbb{N} \to \{T, F\}$ s.t. $P(1)$ holds, and $\forall i \in \mathbb{N}$, $P(i) \Rightarrow P(i+1)$. Then $\forall n \in \mathbb{N}$, $P(n)$ holds.

We used PMI to prove the following :
$\forall n$, $\forall (x, y) \in [2^n] \times [2^n]$, the $2^n \times 2^n$ board with (x, y) removed can be covered using non overlapping trominoes.

Suppose we had to prove a weaker claim :
" $\forall n$, $\exists (x, y) \in [2^n] \times [2^n]$ s.t. the $2^n \times 2^n$ board with (x, y) removed can be covered using non-overlapping trominoes."

It can be tempting to define the induction predicate as :
$P(n)$: $\exists (x, y) \in [2^n] \times [2^n]$ s.t. the $2^n \times 2^n$ board with (x, y) removed can be covered using non-overlapping trominoes."

However, this predicate does not suffice (why ?)

Strong PMI : $P : \mathbb{N} \to \{T, F\}$ s.t. $P(1)$ holds, and $\forall i \in \mathbb{N}$, $(P(1) \wedge \dots \wedge P(i)) \Rightarrow P(i+1)$. Then $\forall n \in \mathbb{N}$, $P(n)$ holds.

We used strong PMI to analyse the 'unstacking game' : any strategy in this game will produce same score.

Lecture 06: Using Induction for Basic Number Theory

$\mathbb{N} = \{1, 2, 3, \dots\}$

$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$

Both $\mathbb{N}$ and $\mathbb{Z}$ are endowed with operations $+$, $-$, $\times$

Using just properties of '$\times$' we defined prime and composite numbers, and proved that every natural number is either prime, or can be expressed as product of primes. Today, we will prove that the prime decomposition is unique.

Theorem 6.1 [Fundamental Thm of Arithmetic]

$\forall\, n > 1$, $\exists k$ and UNIQUE non decreasing seq. of primes $(p_1, p_2, \dots, p_k)$ s.t. $n = p_1 \cdot p_2 \cdot \dots \cdot p_k$

What properties of $\mathbb{N}$ do we need for proving this?

To prove Thm 6.1, we need the following lemma, which looks very obvious at first

Lemma 6.1 [Euclid's Lemma]

$\forall$ prime p, $\forall\, a, b$, if p divides $a \cdot b$, then p divides a or p divides b (or both).

First, let us formally define 'p divides b'.

Def 6.1 Let $a, b \in \mathbb{Z}$. We say that a divides b if $\exists\, c \in \mathbb{Z}$ s.t. $b = a \cdot c$.

It follows from the definition of 'divides' that

- if a divides b, b divides c, then a divides c.
- if a divides b, a divides c, then $\forall\, r, s \in \mathbb{Z}$, a also divides $rb + sc$.
- if a divides b, then a also divides $b \cdot c$ $\left(\begin{smallmatrix}\text{for all}\\ c \in \mathbb{Z}\end{smallmatrix}\right)$

We will now prove Lemma 6.1.

Last class, someone asked a good question: using prime decomp. of a and b, we know that $a = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ and $b = q_1 \cdot q_2 \cdot \ldots \cdot q_\ell$. We are given that p divides $a \cdot b = p_1 \cdot \ldots \cdot p_k \cdot q_1 \cdot \ldots \cdot q_\ell$. Isn't it "obvious" that $p \in \{p_1, p_2, \ldots, p_k, q_1, \ldots, q_\ell\}$, from def^n of primes and the definition of "x divides y"? Unfortunately, this does not follow from the def^n of primes, and the def^n of "x divides y".

This part is not in syllabus

Consider the set of complex numbers $S = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$. Similar to 'primes', we define "irreducibles" in this set. A number $x \in S$ is irreducible if $\forall\, a, b \in S \setminus \{+1, -1\}$ $x \neq a \cdot b$. The numbers 2, 3, $1 + \sqrt{-5}$, $1 - \sqrt{-5}$ are irreducible. Note that 5 is not irreducible since $5 = (-\sqrt{-5})\sqrt{-5}$. However, check that 3 divides $(1 + \sqrt{-5})(1 - \sqrt{-5})$.

To prove Lemma 6.1, we will need another 'obvious-looking' claim (which you will prove in the next tutorial).

notation: $n \,\%\, n_0$: $n \bmod n_0$

Claim 6.1: $\forall\, n, n_0 \in \mathbb{N}$, $\exists\, q \in \mathbb{N} \cup \{0\}$, $r \in \{0, 1, \dots, n_0 - 1\}$ s.t. $n = q \cdot n_0 + r$.

$q = \left\lfloor \frac{n}{n_0} \right\rfloor$

Proof of Lemma 6.1 (if p divides $a \cdot b$, then p div. a, or p div. b)

Suppose p divides $a \cdot b$.
Let $T = \{ n \in \mathbb{N} : p \text{ divides } n \cdot b \}$

$p \in T$, $a \in T$. Therefore set is nonempty subset of $\mathbb{N}$. By WOP, this set has a minimal element, say n_0.

Claim: n_0 divides every element in T.

Proof: Suppose, on the contrary, $\exists\, n \in T$ s.t. n_0 does not divide n.

Then there exists $q \in \mathbb{N} \cup \{0\}$, $r \in \{1, 2, \ldots, n_0 - 1\}$ s.t. $n = q \cdot n_0 + r$. (using Claim 6.1)

p divides $n \cdot b$ and $n_0 \cdot b$ (since both are in T).
let $n \cdot b = k \cdot p$, $n_0 \cdot b = k_0 \cdot p$.

Therefore $r \cdot b = (n - q \cdot n_0) \cdot b$
$= (k - q k_0) p$. $r \neq 0$, and $r \in T$.

because n_0 does not divide n.

p divides $r \cdot b$.

But this is a contradiction, since $r < n_0$ ∎

Note that $p \in T$, $a \in T$. n_0 divides $p \Rightarrow n_0 = p$ or $n_0 = 1$.

If $n_0 = p$, then p divides a.
If $n_0 = 1$, then $n_0 \in T \Rightarrow$ p divides b.
∎

e

Lemma 6.2: For any prime p, for any natural numbers $x_1 \ldots x_n$, if p divides $x_1 \cdot x_2 \cdot \ldots \cdot x_n$, then $\exists\, i \in [n]$ s.t. p divides x_i.

Proof: PROOF BY STRONG INDUCTION.

Consider the predicate
$Q_p(n)$: for all $x_1 \in \mathbb{N}$, $x_2 \in \mathbb{N}$, $\cdots$, $x_n \in \mathbb{N}$, if p divides $x_1 \cdot x_2 \cdot \ldots \cdot x_n$, then $\exists\, i \in [n]$ s.t. p divides x_i.

Base cases: $n = 1$ $Q_p(1)$ holds ✓
$n = 2$ $Q_p(2)$ holds (lemma 6.1) ✓

Induction step: $\forall n \geq 2$, $\big(Q_p(2) \wedge Q_p(n)\big) \Rightarrow Q_p(n+1)$.

Proof of induction step: Consider any $x_1, \cdots, x_n, x_{n+1}$
Let $y_1 = x_1, \cdots, y_{n-1} = x_{n-1}$, $y_n = x_n \cdot x_{n+1}$

We are given that p divides $x_1 \cdot \ldots \cdot x_{n+1} = y_1 \cdot \ldots \cdot y_n$.

Using $Q_p(n)$, $\exists\, i \in \{1, 2, \ldots, n\}$ s.t. p divides y_i.

If p divides y_i for some $i < n$, then it also divides x_i.

If p divides $y_n = x_n \cdot x_{n+1}$, then using $Q_p(2)$, p either divides x_n or x_{n+1}.

This proves the induction step.

Using strong induction, $\forall n \in \mathbb{N}$, $Q_p(n)$ holds. ▨

We are now ready to prove Theorem 6.1 :

Theorem 6.1 [Fundamental Thm of Arithmetic]

$\forall\, n > 1$, $\exists\, k$ and UNIQUE non decreasing seq. of primes $(p_1, p_2, \ldots, p_k)$ s.t. $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$

Proof: We have already shown that every natural number can be decomposed into a product of primes. Suppose, on the contrary, this decomposition is not unique for some n. Take the smallest such number, say n_0.

That is, $\exists\, k, \ell$ and primes $p_1 \le p_2 \le \ldots \le p_k$, $q_1 \le q_2 \le \ldots \le q_\ell$ s.t. $n_0 = p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_\ell$.

Case 1: $p_k = q_\ell$.

Then if we consider n_0 / p_k, this number is greater than 1, and this is a smaller number with non-unique prime decomposition.
Hence $p_k \neq q_\ell$.

Case 2: $p_k < q_\ell$.
q_ℓ divides LHS. Using Lemma 6.2, $\exists\, i \in [k]$

s.t. q_ℓ divides p_i. But this is not possible since $p_1 \leq p_2 \leq \dots \leq p_k < q_\ell$.

∎

Summary:

1. Def.ⁿ of "a divides b"
2. Using WOP / PMI, it follows that
   - every natural number can be expressed as prod. of primes (i)
   - for every n, n_0, $\exists\, q \in \mathbb{Z}$, $r \in \{0, \dots, n_0 - 1\}$ s.t. $n = q \cdot n_0 + r$ (ii)
   - prime p divides $a \cdot b \Rightarrow$ p divides a or p divides b (iii)
     (uses WOP + (ii))
   - every natural number $n > 1$ has a unique prime factorization (iv)
     (uses WOP + (iii))