LECTURE 21: Strong induction continued

1. $k \to k+1$
2. $n \to n+1$
3. $n+1 \to n+1$

The only difference between weak and strong induction is the number of inductive hypotheses made in the inductive step.

WEAK

$P(1) \to P(2) \to \cdots \to P(k) \to P(k+1)$

STRONG

$P(1)\ P(2)\ P(3) \cdots P(k-2)\ P(k-1)\ P(k) \to P(k+1)$

we need multiple induction hypotheses

Fundamental Theorem of Arithmetic Every integer n, $n>1$, can be written as a product of primes (unique up until order of the prime factors, i.e. $2\times7\times11 = 11\times2\times11 = \ldots$)

Examples $24 = [4\times6] = 2\times2\times2\times3 = 2^3\cdot3^1$ ← $\cdot$ is multiplication

$100 = 2\times50 = 2\times2\times25 = 2\times2\times5\times5 = 2^2\cdot5^2$

$512 = 2^9$ ← product of primes

Proof Let $P(n)$: n can be written as a product of primes

BASE CASE: $n=2$ we can verify that $2 = 2^1$ and since 2 is a prime number 2^1 is a valid product of primes. ✓

INDUCTIVE CASE: ⚠ If we were doing weak induction we would assume $P(k)$ is true, and show $P(k+1)$

what we know to be true thanks to strong induction

Instead: We assume that $P(i)$ is true for $2 \le i \le k$, in other words: every number smaller or equal to k can be decomposed. — STRONG INDUCTION HYPOTHESIS

BASE CASE $2 \le i \le k$

Let's consider the integer $k+1$.

[Because we are interested in decomposing $k+1$ as a product of primes, then it is normal to ask first: is $k+1$ prime or not?]

- CASE 1: $k+1$ is PRIME, then it is its own decomposition, therefore $P(k+1)$ is TRUE ✓
- CASE 2: $k+1$ is not prime, it is COMPOSITE

  By DEFINITION of "COMPOSITE" this means there exists

  $\exists\, a,b \in \mathbb{Z},\ a>1,\ b>1,\ k+1 = a\cdot b$

  Because $a < k+1$ and $b < k+1$, by induction hypothesis, there is a prime factor decomposition for both a and b, and therefore a prime decomposition for $a\cdot b = k+1$.

How to translate COMPOSITE to definition?

$x \in A \setminus B$ → $x \in A$ AND $x \notin B$

n is even → $\exists k \in \mathbb{Z},\ n = 2k$

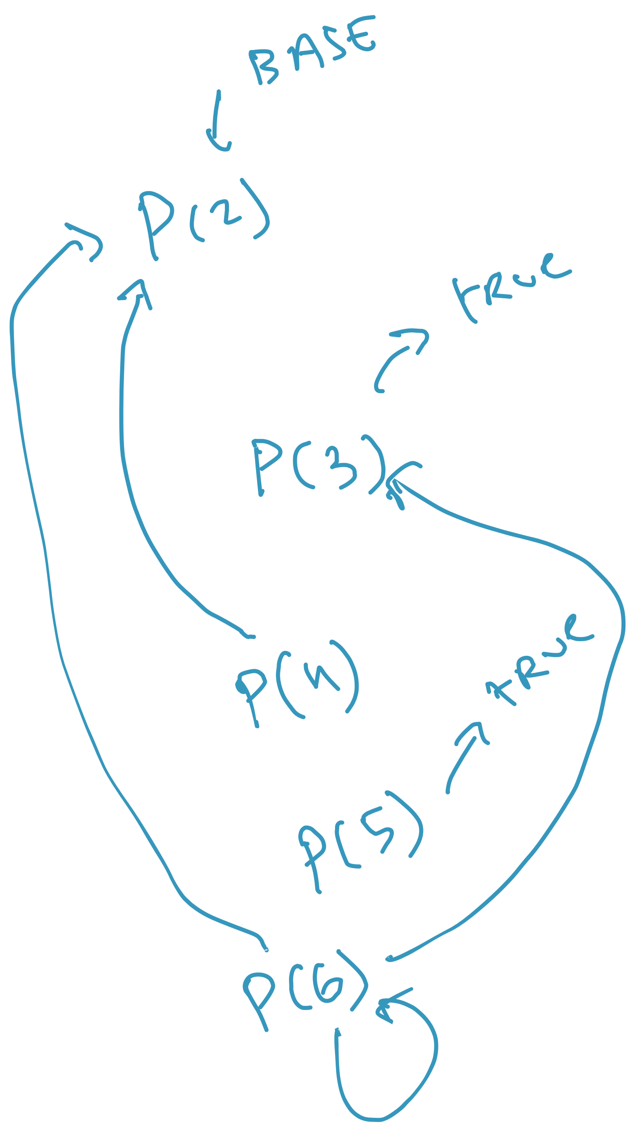
$\exists\, a,b \in \mathbb{Z},\ a>1,\ b>1,\ n = a\cdot b$

without this condition then every integer (including prime numbers) would be considered "composite"

$7 \to 1\times7\times1$

Therefore we have shown that $P(k+1)$ is true.

CONCLUSION: We can conclude by strong induction that $P(n)$ is true for all $n \ge 2$ ($n > 1$)



Binary Decomposition Theorem

Every number n can be written in binary form

$$n = b_k 2^k + b_{k-1}2^{k-1} + \cdots + b_2 2^2 + b_1 2^1 + b_0 2^0$$

b_k is the k-th bit, $b_k = 0$ or $b_k = 1$

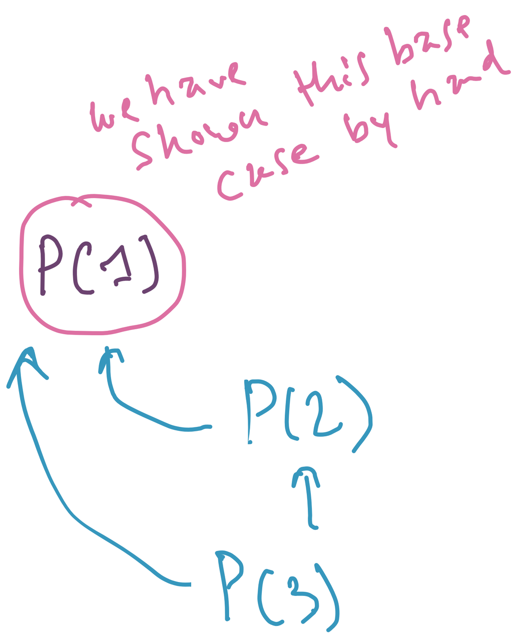
Examples: $4 = 1\cdot2^2$ $\qquad 7 = 1\cdot2^2 + 1\cdot2^1 + 1\cdot2^0$

Some binary numbers

0	000 ← even
1	001 ← odd
2	010 ← even
3	011 ← odd
4	100 ←
5	101 ← odd

$\forall n,\ P(n)$

$\forall n \ge 5,\ P(n)$



PROOF.

WEAK INDUCTION | STRONG INDUCTION

$P(n)$: n can be written (uniquely) in binary

BASE CASE. $n=1$, for $n=1$, we have the decomposition $1 = 1\cdot2^0$ ✓

INDUCTIVE CASE

Weak: We assume that $P(k)$ is true and we want to show $P(k+1)$ is true.

Strong: We assume that for all i, $1 \le i \le k$, $P(i)$ is true. We want to show that $P(k+1)$ is true.

CASE 1 is similar as strong induction, because in the strong induction we only rely on the previous number

CASE 1 $k+1$ is odd. Therefore it can be expressed as

$k+1 = k + 1\cdot2^0$

don't care about p

$k+1 = 2p+1$

($1\cdot2^0$ is just a fancy way of rewriting 1)

We can then, by inductive hypothesis, decompose k, and then set the lowest bit to 1. — details

$k+1$ is odd therefore k is even

$k = \ldots\ldots\ldots 0$ ← last bit

- because k is smaller, by inductive hypothesis we can decompose it
- because k is even, its last bit is 0
- FINALLY to combine the decompositions of k and 1 to get $k+1$, we simply take the decomposition of k and set the lowest bit of this to 1 to get a decomposition of $k+1$

CASE 2 is much more complicated because you have to transition from k to $k+1$.

Hint: Consider that you are adding two numbers with a CARRY

```
  111   ← CARRIES
 100111
 000001
 ------
 101000
```

CASE 2 $k+1$ is even. Therefore it can be expressed as $k+1 = 2p$ (for $p \in \mathbb{Z}$) and because $p < k+1$, we can apply the inductive hypothesis on p to get a binary decomposition. When multiplying we are shifting the bits by one base

```
  5     100
2x5    1000
```

CONCLUSION: We have shown by strong induction $P(n)$ is true