§10.2 PROOF BY STRONG INDUCTION

TO SHOW $P(1) \wedge P(2) \wedge P(3) \wedge \ldots$

(1) BASIS: SHOW EXPLICITLY THAT $P(1)$ IS TRUE (OR WHATEVER FIRST CASE IS)

(2) STRONG INDUCTION: SHOW THAT $\underbrace{(P(1) \wedge P(2) \wedge \ldots \wedge P(n))}$ $\Rightarrow P(n+1)$

KEY DIFFERENCE: ASSUME $P(k)$ FOR $1 \leq k \leq n$, NOT JUST $P(n)$.

ex. THM. EVERY INTEGER $n \geq 2$ HAS A PRIME FACTORIZATION.

PROOF: PROOF BY STRONG INDUCTION.
(BASIS) OBSERVE THAT FOR $n=2$, 2 IS PRIME.
THUS 2 IS ITS OWN PRIME FACTORIZATION.

(STRONG INDUCTION) NOW WE ASSUME ALL INTEGERS $2 \leq k \leq n$ HAVE PRIME FACTORIZATIONS AND MUST SHOW $n+1$ HAS A PRIME FACTORIZATION.

(CASE 1) IF $n+1$ IS PRIME, THEN IT IS ITS OWN PRIME FACTORIZATION ✓

(CASE 2) IF $n+1$ IS NOT PRIME, THEN WE HAVE $n+1 = ab$ FOR SOME INTEGERS $2 \leq a, b \leq n$.
BOTH a & b HAVE PRIME FACTORIZATIONS, SAY

$$a = p_1 p_2 \cdots p_j \quad \& \quad b = p_1' p_2' \cdots p_k'.$$

THEN

$$n+1 = ab = (p_1 p_2 \cdots p_j)(p_1' p_2' \cdots p_k')$$

IS A PRIME FACTORIZATION OF $n+1$. ∎

ex. Every natural number n can be written as a sum of distinct non-negative integer powers of 2.

Proof: We proceede by strong induction.

(Basis) Observe that $1 = 2^0$, thus the result holds for $n = 1$.

(Strong induction) Now assume the result holds for all natural numbers $\leq n$. We must show the result holds for $n+1$.

Let ℓ be the largest integer such that $2^\ell \leq n+1$.
Set $m = (n+1) - 2^\ell$, so $n+1 = 2^\ell + m$.
Since $2^\ell \geq 1$, it follows that $0 \leq m \leq n$.

(Case 1) If $m = 0$ then $n+1 = 2^\ell$ ✓

(Case 2) If $1 \leq m \leq n$ then by (strong induction) hypothesis, the result holds for m. Let

$$m = 2^{a_1} + 2^{a_2} + \dots + 2^{a_j}$$

and it follows that

$$n+1 = 2^\ell + 2^{a_1} + 2^{a_2} + \dots + 2^{a_j}.$$

All that remains is to show that $\ell \neq a_i$ for any $1 \leq i \leq j$. That is, that all powers of 2 are <u>distinct</u>.

Suppose, for sake of contradiction, that $\ell = a_i$ for some specific i. Then

$$\begin{aligned} n+1 &= 2^\ell + 2^{a_1} + 2^{a_2} + \dots + 2^{a_j} \\ &\geq 2^\ell + 2^\ell \\ &= 2^{\ell+1}. \end{aligned}$$

Therefore $2^{\ell+1} \leq n+1$. But this contradicts the fact that ℓ is the largest integer such that $2^\ell \leq n+1$.

§10.3 PROOF BY SMALLEST COUNTEREXAMPLE

Outline for Proof by Smallest Counterexample

Proposition The statements $S_1, S_2, S_3, S_4, \ldots$ are all true.

Proof. (Smallest counterexample)

(1) Check that the first statement S_1 is true.

(2) For the sake of contradiction, suppose not every S_n is true.

(3) Let $k > 1$ be the smallest integer for which S_k is **false**.

(4) Then S_{k-1} is true and S_k is false. Use this to get a contradiction. ■

ex. FOR EVERY INTEGER $n \geq 7$, THERE EXIST POSITIVE INTEGERS a & b SUCH THAT $n = 2a + 3b$.

PROOF: (PROOF BY SMALLEST COUNTEREXAMPLE)

(1) FIRST OBSERVE THAT $7 = 2 \cdot 2 + 3 \cdot 1$ & $8 = 2 \cdot 1 + 3 \cdot 2$, SO THE RESULT HOLDS FOR $n = 7$ & $n = 8$.

(2) FOR SAKE OF CONTRADICTION, SUPPOSE NOT EVERY INTEGER $n \geq 7$ CAN BE WRITTEN AS $2a + 2b$ FOR SOME POSITIVE INTEGERS a, b.

(3) LET $k > 1$ BE THE SMALLEST INTEGER ≥ 7 FOR WHICH NO SUCH a, b EXIST.

(4) SINCE RESULT HOLDS FOR $n = 7, 8$, WE KNOW $k \geq 9$, AND $k - 2 \geq 7$. SINCE $k-2$ IS LESS THAN SMALLEST INTEGER ≥ 7 FOR WHICH NO SUCH a, b EXIST, WE HAVE POSITIVE INTEGERS x, y WITH $k - 2 = 2x + 3y$. THEN

$$k = (k-2) + 2 = 2x + 3y + 2 = 2(x+1) + 3y.$$

SETTING $a = x + 1 \in \mathbb{Z}$ AND $b = y \in \mathbb{Z}$, WE SEE $k = 2a + 3b$. THIS CONTRADICTS THE DEFINITION OF k (SEE PART (3)). ■

(COULD WE HAVE USED STRONG INDUCTION INSTEAD?)

ex. $\forall n \in \mathbb{N}$, $24 \mid (5^{2n} - 1)$.

Proof. (Proof by smallest counterexample)
First observe that for $n = 1$, $5^2 - 1 = 25 - 1 = 24 \cdot 1$
show that $24 \mid (5^{2n} - 1)$.

Now assume, for sake of contradiction, that it is not true that $24 \mid (5^{2n} - 1)$ for all $n \in \mathbb{N}$.
Let k be the smallest positive integer such that $24 \nmid (5^{2k} - 1)$.

Then $24 \mid (5^{2(k-1)} - 1)$, and so $5^{2(k-1)} - 1 = 24x$ for some $x \in \mathbb{N}$.

Multiplying both sides by 25 gives

$$25 \cdot 5^{2(k-1)} - 25 = 25 \cdot 24x$$

$$5^{2k} - 1 = 25 \cdot 24x + 24 = 24(25x + 1),$$

with $25x + 1 \in \mathbb{Z}$. Therefore $24 \mid 5^{2k} - 1$. $\Rightarrow\Leftarrow$

This is a contradiction. Thus our assumption is false & it is true that $24 \mid (5^{2n} - 1)$ $\forall n \in \mathbb{N}$. ∎