

Proof: using strong induction on  $n$

let  $n \in \mathbb{N}$ . Assume that for every  $0 < k < n$ , there exists  $q, r \in \mathbb{N}$  that  $k = qm + r$  and  $r < m$

Case 1:  $n < m$ : let  $q = 0$  and  $r = n$ , then  $qm + r = r = n$ , and  $r < m$ .

Case 2:  $n \geq m$ : let  $k = nm$ . Since  $m \in \mathbb{Z}^+$ ,  $k \in \mathbb{N}$ . Since  $n \geq m$ ,  $k \geq 0$ . So by inductive hypothesis, there exist  $q, r \in \mathbb{N}$  that  $k = qm + r$  and  $r < m$ . Let  $q' = q + 1$ ,  $r' = r$ , then  $q'm + r = (q + 1)m + r = km + m = (n - m)m + m = m = n$ ,  $r' = r < m$ .

Recall:  $n > 1$  is prime if  $\neg \exists a \in \mathbb{N} \exists b \in \mathbb{N} (n = ab \wedge a < n \wedge b < n)$

Thm 6.4.2: every natural number is either prime or a product of two primes.

Rough work:  $P(n) = \begin{cases} \text{prime} \\ \text{product of primes} \end{cases}$

Strong induction:

Given

$n \in \mathbb{N}$

$\forall k \in \mathbb{N}$   $k$  is either a prime or a product of primes.

Goal

$n$  is prime /  $n$  is product of primes.

Proof: We use strong induction. Assume  $n \in \mathbb{N}$ ,  $n > 1$ .

Suppose that for all  $k$  that  $1 \leq k < n$ ,  $k$  is either prime or a product of primes.

If  $n$  is prime, we're done.

Assume  $n$  is not prime, then there exist  $a, b \in \mathbb{N}$  that  $n = ab$ ,  $a < n$  and  $b < n$ . Since  $a < n$ ,  $b > 1$ .

Similarly, since  $b < n$ ,  $a > 1$ . So by inductive hypo,  $a$  and  $b$  are prime or product of primes. Therefore  $n = ab$  is a product of primes.  $\square$ .

Ex: define a sequence  $T_n$  by  $T_1 = T_2 = T_3 = 1$   
 and  $T_n = T_{n-1} + T_{n-2} + T_{n-3}$   
 Proof that  $T_n < 2^n$  for all  $n \geq 1$ .

Proof: We use strong induction. Let  $n \geq 1$ . Assume that for all  $k$  with  $1 \leq k < n$ ,  $T_k < 2^k$ .

Base cases:  $n=1, 2, 3$ .  $T_n = 1$  and  $2^n > T_n$ .

Inductive cases:  $n \geq 4$ . Then  $T_n = T_{n-1} + T_{n-2} + T_{n-3}$ .

$$< 2^{n-1} + 2^{n-2} + 2^{n-3} \\ = \frac{7}{8} 2^n < 2^n.$$

Thm 6.4.4. well ordering principle.

Every non-empty subset of natural number have smallest element.

Roughwork:

$\forall S \subseteq \mathbb{N} (S \neq \emptyset \rightarrow S \text{ has a smallest number})$ .

Proof:

Let  $S \subseteq \mathbb{N}$ . We'll prove the contrapositive. Assume  $S$  does not have a smallest element. we'll show  $\forall n \in \mathbb{N} n \notin S$ .

We use strong induction. Let  $n \in \mathbb{N}$ . Assume that for every  $k < n$ ,  $k \notin S$ .

Then if  $n \in S$ , it is a smallest element.

But  $S$  does not have smallest, so  $n \notin S$ .