Last day of class: Dec 8

§ 6.4. Strong Induction

Strategy: To proof a goal: $\forall n \in P(n)$. prove: $\forall k \in \mathbb{N}\ (k<n, P(k)) \to P(n)$.

$n=0$: $(\underbrace{\forall k<0, P(k)}_{\text{Empty} \Rightarrow \text{True}}) \to \underbrace{P(0)}_{\text{True}}$. $\Rightarrow$ True for $n=0$.

$n=1$: $(\forall k<1, P(k)) \to P(1)$ $\Rightarrow$ $((\underbrace{k=0, P(k)}_{\text{true}}) \to \underbrace{P(1)}_{\text{True}})$.

$n=2$ $(\forall k<2, P(k)) \to P(2)$ $\Rightarrow$ $((\underbrace{k\in\{0,1\}, P(k)}_{\text{true}}) \to P(2)$.

$\vdots$ $\vdots$

Thm 6.4.1 (Division Algorithum):

$\forall m\in\mathbb{Z}^+, \forall n\in\mathbb{N}, \exists q,r\in\mathbb{N}$ such that $n=qm+r$, $r\in[0,m)$.

Proof: Let $m\in\mathbb{Z}^+$, We use strong induction on n, Let $n\in\mathbb{N}$, and assume for all $k<n$, there exist $q,r\in\mathbb{N}$, $k=qm+r \wedge r<m$.

Case 1: $n<m$: then $n=0\cdot m+n$ so $q=0$, $r=n<m$.

Case 2: $n\geq m$: by inductive hyposis, $q', r', n'\in\mathbb{N}$ such that $n-m=q'm+r$, $r'<m$. Then $n=(q'+1)m+r'$,

so take $q=q'+1$ and $r=r'$ □.

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

Thm 6.4.2: $\forall n>1$ is either a prime or a product of prime.

Proof: We use strong induction on n.

Let $n>1$: Suppose that for all k with $1<k<n$, k is either prime or a product of primes.

If n is prime, we're done.

In n is not done: there exist $a,b\in\mathbb{N}$ such that $ab=n$, $a<n$, $b<n$.

Since $a\in(1,n)$, $b\in(1,n)$. So by the induction hypothsis.

a, b are either or a product of primes. In any case,

$n = ab$ is a product of primes $\square$.

Thm 6.4.4: (Well-ordered principle): Every non-empty set of natural number has a smallest element.

Proof: Let $S \subseteq \mathbb{N}$, We'll prove by contrapositive.

S does not has a smallest element. We'll show that $S = \emptyset$.

i.e. $\forall n \in \mathbb{N} (n \notin S)$. We'll use strong induction.

Assume $\forall k < n (k \notin S)$. The contrapositive is if $k \in S$, $n \leq k$.

Therefore, if $n \in S$, it is the smallest element in S.

But in the assumption, S is empty. $n \notin S$.

Ex: Every $q \in \mathbb{Q}^+$ can be written m/n such that $m, n \in \mathbb{Z}^+$ having no common divisor > 1.

Proof: Let $q \in \mathbb{Q}^+$. Let $S = \{m \in \mathbb{Z}^+ \mid \exists n \in \mathbb{Z}^+ \ q = m/n\}$.

This is non-empty, so it has a smallest element m,

then $q = m/n$ for some $n \in \mathbb{Z}^+$,

If m/n is not in lowest term, then $\exists d > 1$ such that $d \mid m$,

$d \mid n$, But then $q = \frac{m/d}{n/d}$, $m/d = \mathbb{Z}^+$, $n/d = \mathbb{Z}^+$, So $m/d \in S$.

but $m/d < S$, it is a contradiction.