$P(a)$
$P(a+1)$
⋮
$P(b)$
$P(a) \wedge P(a+1) \wedge \cdots \wedge P(b) \to P(b+1)$
$P(a) \wedge P(a+1) \wedge \cdots \wedge P(b+1) \to P(b+2)$
$P(a) \wedge P(a+1) \wedge \cdots \wedge P(b+2) \to P(b+3)$

Fibonacci sequence

Define a sequence $a_0, a_1, \ldots$ by $a_0 = 0$, $a_1 = 1$, $a_n = a_{n-1} + a_{n-2}$ for $n \geq 2$.

0 1 1 2 3 5 8 13 21 ...

THM: For all $n \geq 0$, $a_n \leq 2^n$

Proof: Base cases

Define sequence $b_0, b_1, \ldots$ by $b_0 = 0$, $b_1 = 1$, $b_n = b_{n-1} + b_{n-2} + 1$ for $n \geq 2$

b:	0	1	2	4	7	12	20	33	... 54
Fib a:	0	1	1	2	3	5	8	13	21
$3a_i$:	0	3	3	6	9	15	24	39	63
$3a_{n-1}$:	-1	2	2	5	8	13	23	38	62

THM: For all integers $n \geq 0$, $b_n \leq 3a_n$

Proof: Base cases ($n=0$) need $b_0 \leq 3a_0$; $b_0 = 0$ $3a_0 = 0$ $0 \leq 0$ ✓
($n=1$) $b_1 \leq 3a_1$; $b_1 = 1$ $3a_1 = 3$ $1 \leq 3$ ✓

Ind step: Suppose $k \geq 1$ and $b_i \leq 3a_i$ for $0 \leq i < k$ [want $b_k \leq 3 \cdot a_k$]

Then $b_k = b_{k-1} + b_{k-2} + 1$ (def of seq)

$\leq 3a_{k-1} + 3 \cdot a_{k-2} + 1$ (ind. hyp applies to $k-1, k-2$

$x = a+b+c$

$a \leq d$

$a \le d$
$b \le e$
$x \le d+e+c$

$\le 3a_{k-1} + 3 \cdot a_{k-2} + 1$ (ind. hyp applies to $k-1, k-2$ b/c $0 \le k-1, k-2 < k$)

$= 3(a_{k-1} + a_{k-2}) + 1$

$= 3a_k + 1$ (def of seq)

$\le 3a_n$

THM: For all integers $n \ge 1$, $b_n \le 3a_n - 1$ strengthen inductive hypothesis

Base cases: $(n=1)$: want $b_1 \le 3a_1 - 1$ $\quad b_1 = 1$ $\quad 3a_1 - 1 = 2$ $\quad 1 \le 2$ ✓

$(n=2)$: $\quad b_2 \le 3a_2 - 1$ $\quad b_2 = 2$ $\quad 3a_2 - 1 = 2$ $\quad 2 \le 2$ ✓

Ind. step: Let $k > 2$ and suppose $b_i \le 3a_i - 1$ for $1 \le i < k$

Then $b_k = b_{k-1} + b_{k-2} + 1$ (def seq) (ind hyp)

$\le 3a_{k-1} - 1 + 3a_{k-2} - 1 + 1$

$= 3a_{k-1} + 3a_{k-2} - 1 - 1 + 1$

$= 3(a_{k-1} + a_{k-2}) - 1 = 3a_k - 1$

THM: $\forall n \in \mathbb{Z}$, $n \ge 6 \to \exists a,b,c \in \mathbb{N}$ s.t. $n = 3a+4b+7c$

Proof: Base cases: $(n=6)$ $\quad 6 = 3 \cdot 2 + 4 \cdot 0 + 7 \cdot 0$ ($2 \in \mathbb{N}$, $0 \in \mathbb{N}$) so $\exists a,b,c \in \mathbb{N}$ s.t. $6 = 3a+4b+7c$ (namely $a=2, b=0, c=0$)

$(n=7)$ $\quad 7 = 3 \cdot 0 + 4 \cdot 0 + 7 \cdot 1$

$(n=8)$ $\quad 8 = 3 \cdot 0 + 4 \cdot 2 + 7 \cdot 0$

Ind step: Suppose $k > 8$ and for all i, $6 \le i < k$, $\exists a',b',c'$ s.t. $i = 3a'+4b'+7c'$

need $6 \le k-3 < k$ to apply ind. hyp $\quad k \ge 9$

Then $k = k-3 + 3$

and $\exists a', b', c' \in \mathbb{N}$ s.t. $k-3 = 3a' + 4b' + 7c'$ (ind hyp)

and $k = k-3+3 = 3a' + 4b' + 7c' + 3$

$= 3(a'+1) + 4b' + 7c'$

$\hookrightarrow a'+1 \in \mathbb{N}$ b/c $a' \in \mathbb{N}$

so $\exists a,b,c \in \mathbb{N}$ s.t. $k = 3a + 4b + 7c$ (namely $a = a'+1$, $b = b'$, $c = c'$)

Primes

$\forall x \in \mathbb{Z}, x \geq 2 \rightarrow \underbrace{\exists p \in \mathbb{Z} \text{ s.t. } p \text{ is prime} \wedge p \mid x}_{P(x)}$

THM: Every integer greater than 1 is divisible by some prime

Proof: Base case ($n=2$): [need $p \mid 2$ for some prime p; let $p=2$: $2 \mid 2$]

Ind. step: Suppose $k > 2$ and for all $i \in \mathbb{Z}$ s.t. $2 \leq i < k$, $\exists p$ s.t. $p \mid i$

[want: $\exists p$ s.t. $p \mid k$]

Two cases: 1) k is prime. $k \mid k$ so $\exists p$ (namely $p=k$) s.t. $p \mid k$

2) k is not prime

then $\exists a \in \mathbb{Z}$ s.t. $a \mid k$ and $2 \leq a \leq k-1$ (def prime)

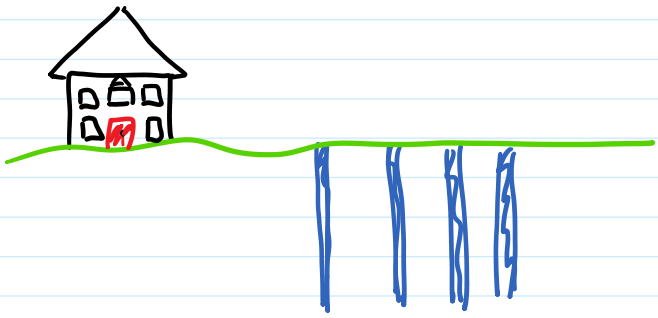
and so $\exists p \in \mathbb{Z}$ s.t. p is prime and $p \mid a$ (ind hyp)

Now $p \mid a$ and $a \mid k$

so $p \mid k$ (trans. of $\mid$)

so $\exists p \in \mathbb{Z}$ s.t. p prime and $p \mid k$

In both cases, $\exists p \in \mathbb{Z}$ s.t. p prime $\wedge$ $p \mid k$



Well-ordering principle: Let S be a non-empty set of integers such that all elements of S are greater than or equal to some integer a.

Then S has a least element

$\{4, 8, 9, -7, 104, \ldots\}$

all ≥ -4

THM (Quotient/Remainder Theorem): For any integer n and positive integer d, there exist unique integers q and r such that

$$n = d \cdot q + r \quad \text{and} \quad 0 \le r < d$$

Proof: Uniqueness

Suppose $n \in \mathbb{Z}, d \in \mathbb{Z}^+$, $n = d \cdot q + r$ and $n = d \cdot q' + r'$ for $q, q', r, r' \in \mathbb{Z}$ with $0 \le r, r' < d$

Suppose further that $q \neq q'$ or $r' \neq r'$

Suppose $q \neq q'$. Assume without loss of generality, that $q > q'$

then $q = q' + k$ for some $k \in \mathbb{Z}^+$

now $d \cdot q + r = d \cdot (q' + k) + r = d \cdot q' + r'$

$$dk + r = r' < d$$

but $dk + r \ge d + 0 = d$ ⇒⇐

So $q = q'$ and hence $r \neq r'$.

Then $d \cdot q + r = d \cdot q' + r' = dq + r'$

so $r = r'$ ⇒⇐

∴ $q = q'$ and $r = r'$

Existence Sketch of weak ind. proof: Show for $n \ge 0$

Base cases: $(n = 0)$ $n = d \cdot \underbrace{0}_{q} + \underbrace{n}_{r}$

$(n = d - 1)$

Ind: $n = d \cdot q + r$ $\quad 0 \le r \le d-1$

$n+1 = d \cdot q + (r+1)$ if $0 \le r < d-1$

$= (d+1) \cdot q + 0$ if $r = d-1$

Now show that if it works for pos. n, it works for neg. n

Using well-ordering (Sketch) Let $S = \{ n - dk \mid k \text{ for some } k \in \mathbb{Z} \text{ s.t. } n - dk \ge 0 \}$

For any $n \in \mathbb{Z}$, can find k s.t. $n - dk \in S$

So S is non-empty, and all elts ≥ 0

∴ by well ordering, S has some min elt — that's the r for QRT.

k that put r in S is the q

Suppose $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$

Let $S = \{ n - d \cdot k \mid k \in \mathbb{Z} \text{ and } n - d \cdot k \ge 0 \}$

Then S is non-empty: if $n \ge 0$ then $n - d \cdot 0 = n \in S$

(let $k = 0$: $n - d \cdot 0 = n \ge 0$)

(let $k=0$; $n-d\cdot 0 = n \geq 0$)

if $n < 0$ then $n - dn = n(1-d)$
where $n<0$ and $1-d \leq 0$
b/c $d \geq 1$

so $n-dn$ is neg. 0
or neg. neg
so $n-dn \geq 0$
and so $n-dn \in S$

All $i \in S$ satisfy $i \geq 0$

So by well-ordering, S has a least element; call it x. this will be the r promised by QRT

this will be the q promised by QRT

$\exists k \in \mathbb{Z}$ s.t. $x = n - d\cdot k$; find k (def of S)

$x \geq 0$ and $x \in \mathbb{Z}$ (def of S; $n, d, k \in \mathbb{Z}$ so $n-dk \in \mathbb{Z}$)

Suppose $x \geq d$ [want contradiction so can conclude $x < d$]

Then $n - d\cdot(k+1) = n - d\cdot k - d = x - d \geq d - d = 0$

so $n - d\cdot(k+1) \geq 0$ hence $n - d\cdot(k+1) \in S$ ($k \in \mathbb{Z} \to k+1 \in \mathbb{Z}$; def S)

Now $x \leq n - d(k+1) = x - d$ (x is smallest in S)

so $0 \leq -d$; hence $d \leq 0$, contradicting $d \in \mathbb{Z}^+$

$\Rightarrow\Leftarrow$

$\therefore x < d$

Now $x = n - d\cdot k$, and $n = d\cdot k + x$ where $k, x \in \mathbb{Z}$ and $0 \leq x < d$

So $\exists q, r \in \mathbb{Z}$ s.t. $n = d\cdot q + r$ and $0 \leq r < d$
(namely $q = k$, $r = x$)