Well-ordering principle

• **Theorem**: Any non-empty subset of natural numbers contains the least element
  – With respect to the usual total order $x \leq y$
    • There is smallest positive even number. Smallest composite number. Smallest square...
  – In general, if there is a property which is not true for some natural numbers, there is a smallest natural number for which it is not true.
  – Very useful for proofs!
    • We saw it in the proof that there are infinitely many primes
Sum of numbers formula

• Claim: for any \( n \in \mathbb{N} \), \( \sum_{i=0}^{n} i = \frac{n(n+1)}{2} \)

• Proof.
  – Suppose not.
  – Let \( S \) be a set of all numbers \( n' \) such that \( \sum_{i=0}^{n'} i \neq \frac{n'(n'+1)}{2} \). By well-ordering principle, if \( S \neq \emptyset \), then there is the least number \( k \) in \( S \).
  – Case 1: \( k=0 \). But \( \sum_{i=0}^{0} i = 0 = \frac{0(0+1)}{2} \). So formula works for \( k=0 \).
  – Case 2: \( k>0 \). Then \( k - 1 \geq 0 \).
    • So \( \sum_{i=0}^{k} i = (\sum_{i=0}^{k-1} i) + k \).
    • As \( k \) is the smallest bad number, the formula works for \( k-1 \).
    • So \( \sum_{i=0}^{k-1} i = \frac{(k-1)k}{2} \)
    • Now, \( \sum_{i=0}^{k} i = (\sum_{i=0}^{k-1} i) + k = \frac{(k-1)k}{2} + k = \frac{k^2 - k + 2k}{2} = \frac{k^2 + k}{2} = \frac{k(k+1)}{2} \)
    • So the formula works for \( k>0 \), too.
  – Contradiction. So \( S \) is empty, thus the formula works for all \( n \in \mathbb{N} \).

Gauss' proof:

\[
1 + 2 + \ldots + 99 + 100 + 100 + 99 + \ldots + 2 + 1 = 101 + 101 + \ldots + 101 + 101 = 100 \times 101
\]

So \( 1+2+\ldots+99+100 = \frac{100 \times 101}{2} \)

Works for any \( n \), not just \( n=100 \).
Mathematical induction

• Want to prove a statement \( \forall x \in \mathbb{N} \ P(x) \).
  – Check that \( P(0) \) holds
  – And whenever \( P(k) \) does not hold for some \( k \), \( P(k - 1) \) does not hold either
    • Contradicting well-ordering principle.
    • Contrapositive:
      – if \( P(k-1) \) holds for arbitrary \( k \),
      – then \( P(k) \) also must be true.
  – Conclude that \( \forall x \in \mathbb{N} \ P(x) \)
Mathematical induction

• Want to prove a statement \( \forall x \in \mathbb{N} \ P(x) \).
  – Check that \( P(0) \) holds
  – And whenever \( P(k) \) does not hold for some \( k \), \( P(k - 1) \) does not hold either
    • Contradicting well-ordering principle.
    • Contrapositive:
      – if \( P(k-1) \) holds for arbitrary \( k \),
      – then \( P(k) \) also must be true.
  – Conclude that \( \forall x \in \mathbb{N} \ P(x) \)

Proving that \( P(0) \) holds is called the **base case.**

That \( P(k-1) \) holds is an **induction hypothesis**

Proving that \( P(k-1) \rightarrow P(k) \) is the **induction step**

Mathematical Induction principle:
If \( P(0) \land \forall k \in \mathbb{N} \ P(k) \rightarrow P(k+1) \) then \( \forall x \in \mathbb{N} \ P(x) \)
Sum of numbers by induction

• Claim: for any $n \in \mathbb{N}$, $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$

• Proof (by induction).
  – $P(n)$ is $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$ (statement we are proving by induction on $n$)
  – Base case: $n=0$. Then $\sum_{i=0}^{0} i = 0 = \frac{0(0+1)}{2}$.
  – Induction hypothesis: Assume that $\sum_{i=0}^{k-1} i = \frac{(k-1)k}{2}$ for an arbitrary $k > 0$
    • That is, for an arbitrary number $n=k-1 \in \mathbb{N}$
    • Can take $k$ instead of $k-1$, but $k-1$ makes calculations simpler.
  – Induction step: show that $P(k-1)$ implies $P(k)$.
    • $\sum_{i=0}^{k} i = (\sum_{i=1}^{k-1} i) + k$.
    • By induction hypothesis, $\sum_{i=1}^{k-1} i = \frac{(k-1)k}{2}$
    • Now, $\sum_{i=1}^{k} i = (\sum_{i=1}^{k-1} i) + k = \frac{(k-1)k}{2} + k = \frac{k^2-k+2k}{2} = \frac{k^2+k}{2} = \frac{k(k+1)}{2}$
  – By induction, therefore, $P(n)$ holds for all $n \in \mathbb{N}$.
Changing the base case

• Mathematical Induction principle:
  \[(P(0) \land \forall k \in \mathbb{N} \ P(k) \rightarrow P(k+1)) \rightarrow \forall x \in \mathbb{N} \ P(x)\]

• What if want to prove it only for \( x \geq a \)?
  – Make \( a \) the base case (when \( a \geq 0 \)). For the rest, assume \( k \geq a \).
  \[(P(a) \land \forall k \geq a \ P(k) \rightarrow P(k+1)) \rightarrow \forall x \geq a \ P(x)\]
  • Here, \( \forall x \geq a \ P(x) \) is a shorthand for \( \forall x \in \mathbb{N} \ (x \geq a \rightarrow P(x)) \)
  – To prove it works, prove \( P(n') \) where \( n' = n - a \).
Changing the base case

Example: show that for all \( n \geq 4 \), \( 2^n \geq n^2 \)

– Predicate \( P(n) \): \( 2^n \geq n^2 \)
– Base case: \( n=4 \). \( 2^4 = 16 = 4^2 \)
– Induction hypothesis: assume that for an arbitrary \( k \geq a \), \( 2^k \geq k^2 \)
– Induction step: show that \( 2^k \geq k^2 \) implies \( 2^{k+1} \geq (k + 1)^2 \)
  • \( 2^{k+1} = 2 \cdot 2^k = 2^k + 2^k \geq k^2 + k^2 \)
  • \( (k + 1)^2 = k^2 + 2k + 1 \).
  • Want: \( k^2 + k^2 \geq k^2 + 2k + 1 \), so \( k^2 \geq 2k + 1 \)
    – Dividing both sides of the inequality by \( k \): \( k \geq 2 + \frac{1}{k} \)
    – Since \( k \geq 4 \), and \( 2 + \frac{1}{k} \leq 3 \), \( 2 + \frac{1}{k} \leq 3 < 4 \leq k \). So \( k \geq 2 + \frac{1}{k} \) and thus \( k^2 \geq 2k + 1 \)
  • So \( 2^{k+1} = 2 \cdot 2^k = 2^k + 2^k \geq k^2 + k^2 \geq k^2 + 2k + 1 = (k + 1)^2 \)
– By induction, for all \( n \geq 4 \), \( 2^n \geq n^2 \)

• Corollary: as \( n \) grows, an algorithm running in time \( n^2 \) will quickly outperform an algorithm running in time \( 2^n \)
Coins by induction

• Coins: $\forall x \in \mathbb{N},$ if $x > 7$ then $\exists y, z \in \mathbb{N}$ such that $x = 3y + 5z$. So any amount $> 7$ can be paid with 3s and 5s.
  
  – Predicate $P(n)$: $\exists y, z \in \mathbb{N}$ $n = 3y + 5z$
  – Base case: $P(8): y = 1, z = 1, 8 = 3 \cdot 1 + 5 \cdot 1$
  – Induction hypothesis: suppose that $P(k)$ holds
    • That is, $\exists y, z$ such that $k = 3y + 5z$
  – Induction step: show that $P(k + 1)$ holds
    • That is, show that $\exists y', z' \in \mathbb{N}$ such that $k + 1 = 3y' + 5z'$
    • Construct $y', z'$ from $y, z$
    • If $z > 0,$ then $y' = y + 2,$ $z' = z - 1$
    • If $z = 0,$ then $y' = y - 3,$ $z' = 2$
  – Therefore, for every $x \in \mathbb{N},$ if $x > 7$ then $x = 3y + 5z$ for some $y, z \in \mathbb{N}.$
Strong induction

• For our coins problem, needed not just $P(k-1)$, but $P(k-3)$, and to look at three cases.

• **Mathematical Induction** principle:
  $$(P(0) \land \forall k \in \mathbb{N} \ P(k) \rightarrow P(k+1)) \rightarrow \forall x \in \mathbb{N} \ P(x)$$

• **Strong Induction** principle:
  $$\neg \left( \exists b \in \mathbb{N} \ \forall c \in \mathbb{N} \ (0 \leq c \land c \leq b \rightarrow P(c)) \right)$$
  $$\land \forall k > b \ (\forall i \in \{0, ..., k - 1\} \ P(i)) \rightarrow P(k))$$
  $$\rightarrow \forall x \in \mathbb{N} \ P(x)$$
Equivalence of variants of induction

• Strong induction seems stronger... but in fact, mathematical induction, strong induction and well-order principles are equivalent to each other.
  – So choose the most convenient one.

• Can prove induction from well-ordering principle
  – Look at the smallest k such that \( P(k) \) does not hold

• Can prove strong induction statement by normal induction.
  – Prove \( P'(n) = \forall i < n P(n) \) by induction.

• Can prove well-ordering principle from strong induction.
Puzzle: coins

• A not-too-far-away country recently got rid of a penny coin, and now everything needs to be rounded to the nearest multiple of 5 cents...

  – Suppose that instead of just dropping the penny, they would introduce a 3 cent coin.

    • Like British three pence.

  – What is the largest amount that cannot be paid by using only existing coins (5, 10, 25) and a 3c coin?

    7c

    Any number n >7 can be paid with 3,5,10,25 coins (even just 3 and 5).
Well-ordering principle

- Any non-empty subset of natural numbers contains the least element
  - With respect to the usual total order $x \leq y$
  - Very useful for proofs!
- Coins: $\forall x \in \mathbb{N}$, if $x > 7$ then $\exists y, z \in \mathbb{N}$ such that $x = 3y + 5z$. So any amount $> 7$ can be paid with 3s and 5s.
  - Suppose, for the sake of contradiction, that there are amounts greater than 7 which cannot be paid with 3s and 5s.
  - Take a set $S$ of all such amounts. Since $S \subseteq \mathbb{N}$, and we assumed that $S \neq \emptyset$, by well-ordering principle $S$ has the least element. Call it $n$.
  - Now, look at $n - 3$; it cannot be paid by 3s and 5s either.
  - Since $n$ is the least element of $S$, $n - 3 \leq 7 < n$
  - 3 cases:
    - $n - 3 = 7$. Then $n = 10 = 2 \times 5$.
    - $n - 3 = 6$. Then $n = 9 = 3 \times 3$
    - $n - 3 = 5$. Then $n = 8 = 3 + 5$.
  - In all three cases, got a contradiction.
  - Therefore, for every $x \in \mathbb{N}$, if $x > 7$ then $x = 3y + 5z$ for some $y, z \in \mathbb{N}$.
Strong induction

- **Strong Induction principle (general form):**
  - \((\exists b \in \mathbb{N} \ \forall c \in \mathbb{N} \ (a \leq c \land c \leq b \rightarrow P(c)))\)
  - \(\land \forall k > b \ (\forall i \in \{a, \ldots, k - 1\} \ P(i)) \rightarrow P(k))\)
  - \(\rightarrow \forall x \in \mathbb{N} \ (x \geq a \rightarrow P(x))\)

- **Coins:** \(\forall x \in \mathbb{N}, \text{if } x > 7 \text{ then } \exists y, z \in \mathbb{N} \text{ such that } x = 3y + 5z.\)
  - \(P(n): \exists y, z \in \mathbb{N} \ n = 3y + 5z.\) Also, \(a=8.\)
  - Base cases: \(b = 10, \) so \(c \in \{8, 9, 10\}\)
    - \(n=8. \) \(8 = 3 \cdot 1 + 5 \cdot 1, \) so \(y=1, \) \(z=1.\)
    - \(n=9. \) \(9=3 \cdot 3, \) \(y=3, \) \(z=0\)
    - \(n=10. \) \(10=5 \cdot 5. \) \(y=0, \) \(z=2.\)
  - Induction hypothesis: Let \(k\) be an arbitrary integer such that \(k > 10.\)
    - Assume that for all \(i \in \mathbb{N}\) such that \(8 \leq i < k \) \(\exists y_i, z_i \in \mathbb{N} \ i = 3y_i + 5z_i\)
  - Induction step. Show that induction hypothesis implies that \(\exists y, z \in \mathbb{N} \ k = 3y + 5z\)
    - Since \(k \geq b, \) \(k - 3 \geq a.\) So by induction hypothesis \(\exists y_{k-3}, z_{k-3} \in \mathbb{N} \ k - 3 = 3y_{k-3} + 5z_{k-3}.\) Now take \(z=z_{k-3} \) and \(y=y_{k-3} + 1.\) Then \(k = 3y+5z.\)
  - By strong induction, get that for all \(x > 7, \exists y, z \in \mathbb{N} \text{ such that } x = 3y + 5z.\)
Puzzle: all horses are white

• Claim: all horses are white.
• Proof (by induction):
  – P(n): any n horses are white.
  – Base case: P(0) holds vacuously
  – Induction hypothesis: any k horses are white.
  – Induction step: if any k horses are white, then any k+1 horses are white.
    • Take an arbitrary set of k+1 horses. Take a horse out.
      – The remaining k horses are white by induction hypothesis.
    • Now put that horse back in, and take out another horse.
      – Remaining k horses are again white by induction hypothesis.
    • Therefore, all the k+1 horses in that set are white.
  – By induction, all horses are white.