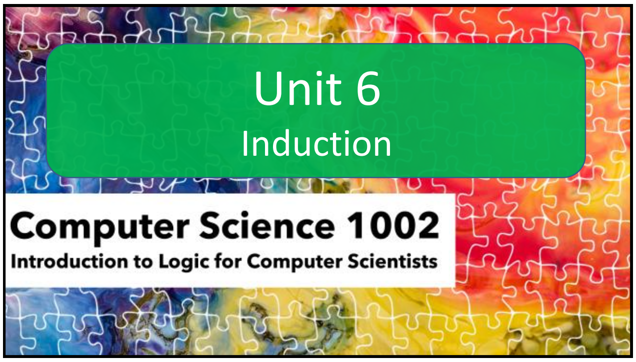
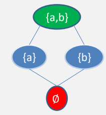


1

Order relations

- A binary relation $R \subseteq A \times A$ is an **order** if R is
  - Reflexive, Anti-symmetric, Transitive
    - $R_1 = \{(x,y) | x, y \in \mathbb{Z} \wedge x \leq y\}$
    - $SUBSETS = \{(A,B) \mid A, B \text{ are sets} \wedge A \subseteq B\}$
    - $DIVISORS = \{(x,y) \mid x, y \in \mathbb{N} \wedge x, y \geq 2 \ \wedge \exists z \in \mathbb{N} \ \ y = z \cdot x\}$
- An order may have **minimal** and **maximal** elements (maybe multiple)



2

Well-ordering principle

- **Theorem:** Any non-empty subset of natural numbers contains the minimum element
  - With respect to the usual total order $x \leq y$
    - There is smallest positive even number. Smallest composite number. Smallest square…
  - 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!

3

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).

4

- Well-ordering principle: Any non-empty subset of natural numbers contains the least element (with respect to $x \leq y$)
- 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, $n - 3 \leq 7 < n$
  - Remains to show that all possible $n - 3 \leq 7$ don't work

5

- 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.
  - 3 cases:
    - n=8. Then n=3+5.
    - n = 9. Then n=3*3
    - n = 10. Then n=10=2*5.
  - In all three cases, got a contradiction.
  - Therefore, for every $x \in \mathbb{N}$, if x >7 then x=3y+5z for some $y, z \in \mathbb{N}$.

6

7

Well-ordering principle

Theorem: Any non-empty subset of natural numbers contains the minimum element

- With respect to the usual total order $x \leq y$
  - There is smallest positive even number. Smallest composite number. Smallest square…
- 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!

8

Infinitely many primes

- *Definition:* A natural number is prime iff it is divisible only by 1 and itself. That is, n is prime iff

$$\forall z \in \mathbb{N}\ ((\exists w \in \mathbb{N}\ n = zw) \rightarrow (z = 1 \lor z = n))$$

- *Theorem*: There are infinitely many primes.

$$\forall x \in \mathbb{N}\ Prime(x) \rightarrow \exists y \in \mathbb{N} y > x \land Prime(y)$$

  – Proven by Euclid ~300BC

- $Prime(x)$ is a shorthand for $\forall z \in \mathbb{N}(\exists w \in \mathbb{N}\ x = zw) \rightarrow z = 1 \lor z = x$
- To say “infinitely many” we write that no matter what element of the domain we take, there is a larger one that has the property we are interested in (in this case, a prime).

9

Theorem: There are infinitely many primes.
$\forall x \in \mathbb{N}\ Prime(x) \rightarrow \exists y \in \mathbb{N}\ y > x \land Prime(y)$

- *Proof (by contradiction)*:
  – Assume, for the sake of contradiction, that the statement of the theorem is false:
    - So $\exists x \in \mathbb{N}\ Prime(x) \land (\forall y \in \mathbb{N} y \leq x \lor \neg Prime(y))$
  – Call this number n (universal instantiation of $\forall x$)
  – Now consider the number $\mathrm{N} = (2 \cdot 3 \cdot \ldots \cdot n) + 1$
  – There are 2 cases.
    - Either N is a prime, in which case we are done since we found a prime larger than n, contradicting our assumption.
    - or N is not prime.

10

Theorem: There are infinitely many primes.
$\forall x \in \mathbb{N}\ Prime(x) \rightarrow \exists y \in \mathbb{N}\ y > x \land Prime(y)$

Well-ordering principle: Any non-empty subset of natural numbers contains the least element (with respect to $x \leq y$)

- *Proof (continued)*:
  - Consider the number $\mathrm{N} = (2 \cdot 3 \cdot \ldots \cdot n) + 1$
  – Case 2: suppose N is not prime, that is, for some $k, q \in \mathbb{N},\ N = kq$, where $k \neq 1$ and $k \neq N$.
    - By the *well-ordering principle,* there is a smallest such k.
      – Let us use k_0 to refer to this smallest k.
    - Since $N \equiv 1\ mod\ d$ for all $d \leq n,\ k_0$ is not divisible by any $d \leq n$, and $k_0 > n$
    - So since k_0 is the smallest factor of N, k_0 itself must be prime.
    - Therefore, there exists a prime number $y > n$ by existential generalization.

11

Theorem: There are infinitely many primes.
$\forall x \in \mathbb{N}\ Prime(x) \rightarrow \exists y \in \mathbb{N}\ y > x \land Prime(y)$

- *Proof (continued)*:
  – We showed that both cases of N being prime and not being prime give us $\exists y \in \mathbb{N}\ y > n \land Prime(y)$
    - In the first case, N itself was an instantiation of $\exists y$, and in the second case, it was the smallest divisor of N.
  – There are no more cases, so we showed that $\exists y \in \mathbb{N}\ y > n \land Prime(y)$, contradicting the assumption for an arbitrary (prime) n
    - We showed that, for arbitrary n, $Prime(n) \rightarrow \exists y \in \mathbb{N}\ y > n \land Prime(y)$
  – By universal generalization,

$$\forall x \in \mathbb{N}\ Prime(x) \rightarrow \exists y \in \mathbb{N}\ y > x \land Prime(y)$$

□ (Done).

12

13

Puzzle: sum of numbers

- What is the sum of the first 100 numbers?
- That is, calculate

1+2+3+4+5+… +98+99+100.

14

Sums

- Sum notation ("sum from 1 to n"): $\sum_{i=1}^{n} i = 1 + 2 + \ldots + n$
    - Symbol Σ is the capital Greek letter sigma.
  - If $n = 3, \sum_{i=1}^{3} i = 1 + 2 + 3 = 6$.
  - The name "i" does not matter (usually i, j or k):
    - $\sum_{i=1}^{n} i = 1 + 2 + \ldots + n = \sum_{j=1}^{n} j$
  - Can start with any integer m, not just 1: $\sum_{i=4}^{n} i = 4 + 5 + \ldots + n$
    - $\sum_{i=n}^{n} i = \mathrm{n}$. If $n < m, \sum_{i=m}^{n} i = 0$.
  - Can put a function of i into the sum: $\Sigma_{i=1}^{n} i^2 = 1^2 + 2^2 + \cdots + n^2$
    - This function has to return a number, but not necessarily an integer:
    - $\sum_{i=2}^{4} \frac{1}{i} = \frac{1}{2} + \frac{1}{3} + \frac{1}{4} = \frac{6+4+3}{12} = \frac{13}{12}$

15

Products and factorial

- Can use a similar shorthand for product of lots of values:
  - $\Pi_{i=1}^{n} i = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$
    - Symbol Π is Greek letter capital pi
  - **Factorial**: another notation for $1 \cdot 2 \cdot \ldots \cdot n = \Pi_{i=1}^{n} i = n!$
    - "$n!$" is pronounced "n factorial"
  - As for sums, can start from an arbitrary integer m, and have a function of i in the product: $\Pi_{i=m}^{n} f(i) = f(m) \cdot f(m+1) \cdot \ldots \cdot f(n)$
    - For $f(i) = 1/i$, $\mathrm{m} = 2, n = 4$, $\Pi_{i=2}^{4} 1/i = 1/2 \cdot 1/3 \cdot 1/4 = 24$
    - And can use another variable name.

16

Properties of sums and products

- Let f and g be any functions with integer inputs, r any number, n, m integers.
  - Can take the first or last element out of the sum by increasing m (first element) or decreasing n (last element)
    - $\sum_{i=m}^{n} f(i) = f(m) + \sum_{i=m+1}^{n} f(i) = (\sum_{i=m}^{n-1} f(i)) + f(n)$
  - When $n < m$, $\sum_{i=m}^{n} f(i) = 0, and \; \Pi_{i=m}^{n} f(i) = 1$
  - Can add two sums with the same n, m, and multiply products
    - $(\sum_{i=m}^{n} f(i)) + (\sum_{i=m}^{n} g(i)) = \sum_{i=m}^{n} (f(i) + g(i))$
  - Can factor out a common factor in a sum (but not in a product)
    - $\sum_{i=m}^{n} r \cdot f(i) = r \cdot \sum_{i=m}^{n} f(i)$
  - Can have multiple nested sums (and products)
    - $\sum_{i=m_1}^{n_1} \sum_{j=m_2}^{n_2} f(i,j)$,
    - $\sum_{i=2}^{4} \Sigma_{j=10}^{11} i \cdot j = 2 \cdot 10 + 2 \cdot 11 + 3 \cdot 10 + 3 \cdot 11 + 4 \cdot 10 + 4 \cdot 11$=189

17

18

Puzzle: sum of numbers

- What is the sum of the first 100 numbers?
- That is, calculate

1+2+3+4+5+… +98+99+100.

19

Gauss' sum of first 100 numbers

	1	+	2	+	…	+	99	+	100	
+	100	+	99	+	…	+	2	+	1	=
=	101	+	101	+	…	+	101	+	101	= 100*101

- So 1+2+ … + 99 + 100 =$\frac{100*101}{2}$=5050
- Does this work for any n, or just n=100?

20

Claim: for any n∈ ℕ, 0+1+…+(n-1)+n=$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$

- 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 the *well-ordering principle*, if $S \neq \emptyset$, there is the least number k in S.

  - We will show that such k cannot exist.
  - By proof by cases:
    - k is either 0, or > 0
    - Case 1: k = 0
    - Case 2: k > 0
- Contradiction. So S is empty, thus the formula works for all $n \in \mathbb{N}$.

21

Claim: for any n∈ ℕ, 0+1+…+(n-1)+n=$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$

- 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 the *well-ordering principle*, if $S \neq \emptyset$, 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.
- Contradiction. So S is empty, thus the formula works for all $n \in \mathbb{N}$.

22

Claim: for any n∈ ℕ, 0+1+…+(n-1)+n=$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$

- 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 the *well-ordering principle*, if $S \neq \emptyset$, 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 by definition of a sum.
    - 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 $n \in \mathbb{N}$.

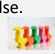
23

Structure of a proof by well-ordering principle

Want to prove: *Claim:* $\forall x \in \mathbb{N}, P(x)$ for some predicate P

Proof by contradiction.

- Suppose that $\forall x \in \mathbb{N}, P(x)$ is false.
- Take a set $S = \{x \in \mathbb{N} \mid \neg P(x)\}$



- By the well-ordering principle, there is the smallest element $k \in S$
- Prove that such k cannot exist, using the fact that it is smallest in S
  - This is where most the work is!
  - Often proof by cases: $k = 0$ or $k > 0$
- Conclude that S is empty, and, therefore, $\forall x \in \mathbb{N}, P(x)$ is true.

□ (Done).

24

Structure of a proof by well-ordering principle

Want to prove: *Claim:* $\forall x \in \mathbb{N}, P(x)$ for some predicate P

Proof by contradiction.

- Suppose that $\forall x \in \mathbb{N}, P(x)$ is false.
- Take a set $S = \{x \in \mathbb{N} \mid \neg P(x)\}$ 
- By the well-ordering principle, there is the smallest element $k \in S$
- Prove that such k cannot exist, using the fact that it is smallest in S
  - This is where most the work is!
  - Often proof by cases: $k = 0$ or $k > 0$
- Conclude that S is empty, and, therefore, $\forall x \in \mathbb{N}, P(x)$ is true.

□ (Done).

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

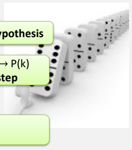
- Want to prove a statement $\forall x \in \mathbb{N}\ P(x)$.
  - Check that $P(0)$ holds
  - And whenever $P(k)$ does not hold for some k, $P(k-1)$ does not hold either
    - Contradicting well-ordering principle.
    - Contrapositive:
      - if P(k-1) holds for arbitrary k,
      - then P(k) also 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) → P(k) Is the **induction step**

Mathematical Induction principle:
If P(0) ∧ ∀ $k \in \mathbb{N}$ P(k) → P(k+1) then $\forall x \in \mathbb{N}\ P(x)$



Claim: for any n∈ $\mathbb{N}$ $P(n)$

Proof (by induction).

- *Predicate* $P(n)$ is
- *Base case:* $n = 0$. Then …. $P(0)$ is true.
- *Induction hypothesis:* Assume that $P(\ldots)$ for an arbitrary k >0
  -
- *Induction step:* show that P(k-1) implies P(k).
  - … calculations …
  - … by induction hypothesis..
  - … calculations …
- *By induction*, therefore, P(n) holds for all $n \in \mathbb{N}$.

□ (Done).

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

Proof (by induction).

- *Predicate* $P(n)$ is $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$
- *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 ∈ $\mathbb{N}$
  - Can take k instead of k-1, but k-1 makes calculations simpler.
- *Induction step:* show that P(k-1) implies P(k).
  - … calculations …
  - … by induction hypothesis..
  - … calculations …
- *By induction*, therefore, P(n) holds for all $n \in \mathbb{N}$.

□ (Done).

Claim: for any n∈ ℕ, 0+1+…+(n-1)+n=$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$

Proof (by induction).

- *Predicate* $P(n)$ is $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$
- *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 ∈ ℕ
  - Can take k instead of k-1, but k-1 makes calculations simpler.
- *Induction step:* show that P(k-1) implies P(k).
  - $\sum_{i=0}^{k} i = (\sum_{i=0}^{k-1} i)$ +k.
  - By induction hypothesis, $\sum_{i=0}^{k-1} i = \frac{(k-1)k}{2}$
  - Now, $\sum_{i=0}^{k} i = (\sum_{i=0}^{k-1} i)$ +k = $\frac{(k-1)k}{2} + k = \frac{k^2-k+2k}{2} = \frac{k^2+k}{2} = \frac{k(k+1)}{2}$
- By induction, therefore, P(n) holds for all $n \in \mathbb{N}$. □ (Done).

31

"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.

Puzzle: What is wrong with this proof?

32

33

"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.

Puzzle: What is wrong with this proof?

34

Mathematical Induction principle:
If P(0) ∧ ∀ $k \in \mathbb{N}$ P(k) → P(k+1) then ∀$x \in \mathbb{N}$ $P(x)$

- 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) ∧ ∀ $k \geq a$ P(k) → P(k+1)) → ∀$x \geq a$ $P(x)$
    - Here, ∀$x \geq a$ $P(x)$ is a shorthand for ∀$x \in \mathbb{N}$ $(x \geq a \rightarrow P(x))$
  - To prove it works, prove $P(n')$ where $n' = n - a$.
- In general, let S be a countable set, and $f: \mathbb{N} \rightarrow S$ a bijection. Then the following is equivalent to the induction principle:

$P(f(0)) \wedge \forall\, k \geq 0\ \ P(f(k)) \rightarrow P(f(k+1))) \rightarrow \forall x \in S\ \ P(x)$

35

Claim: for all $n \geq 4,\ 2^n \geq n^2$

- *Proof (by induction with basis $a = 4$):*
  - *Predicate* $P(n)$: $2^n \geq n^2$
  - *Base case*: n=4. $2^4 = 16 = 4^2$
  - *Induction hypothesis*: assume that for an arbitrary $k \geq 4$, $2^k \geq k^2$
  - *Induction step*: show that $2^k \geq k^2$ implies $2^{k+1} \geq (k+1)^2$
    - $2^{k+1} = 2 \cdot 2^k = 2^k + 2^k \geq k^2 + k^2$ (last ≥ by induction hypothesis).
    - Want: $k^2 + k^2 \geq (k+1)^2$. Since $(k+1)^2 = k^2 + 2k + 1$, need to show $k^2 \geq 2k + 1$
      - Dividing both sides of the last inequality by k: show that $k \geq 2 + \frac{1}{k}$
      - Since k ≥ 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 input size n grows, an algorithm running in time n^2 will quickly start outperforming an algorithm running in time 2^n

36

Claim: $\forall x \in \mathbb{N}$, 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

- *Proof (by induction):*
  - *Predicate* $P(n)$: $\exists y, z \in \mathbb{N}\ \ n = 3y + 5z$
  - *Base case:* $n = 8$.
    - $P(8)$ holds with $y = 1, z = 1$, since $8 = 3 \cdot 1 + 5 \cdot 1$
  - *Induction hypothesis*: assume that $P(k)$ holds for an arbitrary $k \in \mathbb{N}$, where k>7.
    - That is, $\exists y, z \in \mathbb{N}$ 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* $y' = y + 2, z' = z - 1$.
      - $k + 1 = k - 5 + 6$
    - If $z = 0$, then $y' = y - 3,\ z' = 2$
      - $k + 1 = k - 9 + 10$
  - Therefore, for every $x \in \mathbb{N}$, if x >7 then $x = 3y + 5z$ for some $y, z \in \mathbb{N}$.

37

38

Strong induction

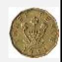
- In our well-ordering proof that every amount > 7 can be paid with 3s and 5s we needed to consider k-3, and to look at three cases.
  - n=8, n=9, n=10.
- Mathematical Induction principle:
  - $(P(0) \wedge \forall k \in \mathbb{N}\ \ P(k) \rightarrow P(k+1)) \rightarrow \forall x \in \mathbb{N}\ P(x)$
  - If first domino falls, and each domino falls on next, all dominos fall.
- Strong Induction principle:
  - $\big(\exists b \in \mathbb{N}\ \ \forall c \in \mathbb{N}\ (0 \le c \wedge c \le b \rightarrow P(c))\big)$
    $\wedge \forall k > b\ \ (\forall i \in \{0, \ldots, k-1\}\ P(i)) \rightarrow P(k))$
    $\rightarrow \forall x \in \mathbb{N}\ P(x)$
  - If first few dominos fall, and if all preceding dominos go down then the next one falls too, then all dominos fall.

39

Claim: $\forall x \in \mathbb{N}$, 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

Strong Induction:
$(\exists b \in \mathbb{N}\ \ \forall c \in \mathbb{N}\ (a \le c \wedge c \le b \rightarrow P(c))$
$\wedge \forall k > b\ \ (\forall i \in \{a, \ldots, k-1\}\ P(i)) \rightarrow P(k))$
$\rightarrow \forall x \in \mathbb{N}\ (x \ge a \rightarrow P(x))$

- *Proof (by strong induction):*
  - *Predicate* $P(n)$: $\exists y, z \in \mathbb{N}\ \ n = 3y + 5z$
  - *Base cases:* $a = 8,\ b = 10$, so $c \in \{8, 9, 10\}$
    - n=8. $8 = 3 \cdot 1 + 5 \cdot 1$, so y=1, z=1.
    - n=9. 9=3· 3, y=3, z=0
    - n=10. 10=5 · 2. y=0, z=2.
  - *Induction hypothesis*: Let k be an arbitrary natural number with $k > 10$.
    Assume that $\forall i \in \mathbb{N}$ such that $8 \le i < k$, $\exists\, y_i, z_i \in \mathbb{N}\ \ i = 3y_i + 5z_i$
  - *Induction step*: show that $P(k)$ holds



40

Claim: $\forall x \in \mathbb{N}$, 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

Strong Induction:
$(\exists b \in \mathbb{N}\ \ \forall c \in \mathbb{N}\ (a \le c \wedge c \le b \rightarrow P(c))$
$\wedge \forall k > b\ \ (\forall i \in \{a, \ldots, k-1\}\ P(i)) \rightarrow P(k))$
$\rightarrow \forall x \in \mathbb{N}\ (x \ge a \rightarrow P(x))$

- *Proof (by strong induction):*
  - *Predicate* $P(n)$: $\exists y, z \in \mathbb{N}\ \ n = 3y + 5z$
  - *Base cases:* $P(8), P(9), P(10)$ hold.
  - *Induction hypothesis*: Let k be an arbitrary natural number such that $k > 10$.
    Assume that $\forall i \in \mathbb{N}$ such that $8 \le i < k$, $\exists\, y_i, z_i \in \mathbb{N}\ \ i = 3y_i + 5z_i$
  - *Induction step*: show that $P(k)$ holds
    - Since $k \ge b$, $k - 3 \ge a$.
    - 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 $k = 3y + 5z$.
  - Therefore, for every $x \in \mathbb{N}$, if $x > 7$ then $x = 3y + 5z$ for some $y, z \in \mathbb{N}$.
  - By strong induction, get that for all x > 7, $\exists\, y, z \in \mathbb{N}$ such that x = 3y+5z.

□ (Done).

41

42

Theorem (fundamental theorem of arithmetic):
Every natural number >1 can be uniquely written as a product of primes.

- Here, assume primes are written in a specific order: say from smallest to largest.
  - For example, $12 = 2 \cdot 2 \cdot 3$, $17 = 17$, $30 = 2 \cdot 3 \cdot 5$
  - We do not consider $12 = 2 \cdot 3 \cdot 2$, because it is not in the right order.
  - Also do not consider $12 = 3 \cdot 4$, since 4 is not a prime.
- This theorem consists of two statements, which have to be proven separately.
  - *Existence*: every $n > 1$ can be written as a product of primes.
    - We will prove this using strong induction.
  - *Uniqueness*: for every $n > 1$, there cannot be two different products of primes that are both equal to n.
    - We will omit this proof here, as we need a bit more number theory to do it properly.
    - You can read it in textbook, chapter 4.3.

43

Theorem: $\forall n \in \mathbb{N}$, if $n > 1$ then n can be written as a product of primes.

Proof (by strong induction):
- *Predicate* $P(n)$: $\exists m \in \mathbb{N}, \exists$ primes $p_1 \dots p_m$ such that $n = p_1 \cdot \dots \cdot p_m$
- *Base case:* $a = b = 2$
  - 2 is prime, so $P(2)$ holds with $m = 1, p_1 = 2$
- *Induction hypothesis*: Let k be an arbitrary natural number with $k > 2$. Assume that $\forall i \in \mathbb{N}$ where $2 \leq i < k$ $\exists m_i$, $\exists$ primes $p_{1,i} \dots p_{m_i,i}$, such that $i = p_{1,i} \cdot \dots \cdot p_{m_i,i}$
- *Induction step*: show that $P(k)$ holds
  - That is, find m', primes $q_1 \dots q_{m'}$ such that $k = q_1 \cdot \dots \cdot q_{m'}$
  - We will prove the induction step by cases:
    1. k is prime
       - Easy case: $m' = 1, q_1 = k$.
    2. k is not prime.

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

44

Theorem: $\forall n \in \mathbb{N}$, if $n > 1$ then n can be written as a product of primes.

Proof (by strong induction):
- *Induction hypothesis*: Let k be an arbitrary natural number > 2. Assume that $\forall i \in \mathbb{N}$ where $2 \leq i < k$ $\exists m_i$, $\exists$ primes $p_{1,i} \dots p_{m_i,i}$, such that $i = p_{1,i} \cdot \dots \cdot p_{m_i,i}$
- *Induction step*: show that $P(k)$ holds
  - Case 1: k is prime (easy case: $m' = 1, q_1 = k$).
  - Case 2: k is not prime.
    - Then $k = a \cdot b$ for some a, b such that $2 \leq a, b < k$
    - By induction hypothesis, there are $m_a, m_b \in \mathbb{N}$, primes $p_{1,a}, \dots, p_{m_a,a}, p_{1,b}, \dots, p_{m_b,b}$ such that $a = p_{1,a} \cdot \dots \cdot p_{m_a,a}$, and $b = p_{1,b} \cdot \dots \cdot p_{m_b,b}$
    - Now $k = p_{1,a} \cdot \dots \cdot p_{m_a,a} \cdot p_{1,b} \cdot \dots \cdot p_{m_b,b}$, so $P(k)$ holds with $m' = m_a + m_b$
      - Rearrange $p_{1,a}, \dots, p_{m_a,a}, p_{1,b}, \dots, p_{m_b,b}$ from smallest to largest to get $q_1 \dots q_{m'}$
  - This completes the proof of the induction step, as there are no more cases.
- By strong induction, every $n > 1$ can be written as a product of primes.

45

Equivalence of well-ordering, induction and strong induction

- Strong induction seems stronger… but in fact, *mathematical induction, strong induction and well-ordering 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.

46

Puzzle: rabbits on an island

- A ship leaves a pair of rabbits on an island (with a lot of food).
- After a pair of rabbits reaches 2 months of age, they produce another pair of rabbits, and keep producing a pair every month thereafter.
- Which in turn start reproducing every month when reaching 2 months of age…
  - So every pair starts reproducing at 2 months, and creates a new pair every month from then on.
- How many pairs of rabbits will be on the island in n months, assuming no rabbits die?

47