p	q	p∧q	p∨q	p⊕q	p→q	p↔q
T	T	T	T	F	T	T
T	F	F	T	T	F	F
F	T	F	T	T	T	F
F	F	F	F	F	T	T

TABLE 7 Logical Equivalences Involving Conditional Statements.

$p \to q \equiv \neg p \vee q$
$p \to q \equiv \neg q \to \neg p$
$p \vee q \equiv \neg p \to q$
$p \wedge q \equiv \neg(p \to \neg q)$
$\neg(p \to q) \equiv p \wedge \neg q$
$(p \to q) \wedge (p \to r) \equiv p \to (q \wedge r)$
$(p \to r) \wedge (q \to r) \equiv (p \vee q) \to r$
$(p \to q) \vee (p \to r) \equiv p \to (q \vee r)$
$(p \to r) \vee (q \to r) \equiv (p \wedge q) \to r$

$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws

TABLE 1 Set Identities.

Identity	*Name*
$A \cap U = A$ $A \cup \emptyset = A$	Identity laws
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Domination laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws
$\overline{(\overline{A})} = A$	Complementation law
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive laws
$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \emptyset$	Complement laws

- **Definition of Set Minus**

$$A - B = A \cap \overline{B}$$

To prove A=B:

1. Prove that A ⊆ B
   a. assume an arbitrary element x in A
   b. show that this element must also be in B
2. Prove that B ⊆ A
   a. assume an arbitrary element x in B
   b. show that this element must also be in A

Mod

Recall: a ≡ b (mod m) means a = b + km for so integer k (and assuming m is a positive integer)

Suppose a ≡ b (mod m) and c ≡ d (mod m).

Claim: a+c ≡ b+d (mod m) (***Addition works!***)

Claim: a–c ≡ b–d (mod m) (***Subtraction works!***)

Claim: ac ≡ bd (mod m) (***Multiplication works!***)

Some proofs. Let a = b + km and c = d + jm.

So a+c = b+km+d+jm = (b+d) + (k+j)m ≡ b+d (mod m)

So ac = (b+km)(d+jm) = bd + (bj+dk+kjm)m ≡ bd (mod m)

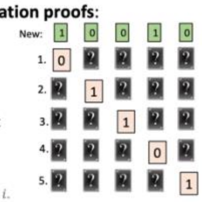
If p is prime, then for any positive int a<p, there exists a unique positive a^{-1}<p s.t. $aa^{-1} \equiv 1 \ (mod\ p)$

Inverse of a can only be calculated if p and a are relatively prime!

Diagonalization

General format for **diagonalization proofs**:

- Arrange items in a table
- Look at the elements along the main diagonal
- Manipulate each diagonal element and put them together to create a *new row* that is guaranteed **not** to be in the table
  - Is the new row the same as row i of the table?
  - **No**: its i^{th} bit is different from the string in row i.



$z \in Z^+$	$f(z) \in [0,1]$		digit 1 of f(z)	digit 2 of f(z)	digit 3 of f(z)	digit 4 of f(z)	...
1	0	0.	0	0	0	0	...
2	$\pi/10$	0.	3	1	4	1	...
3	0.149	0.	1	4	9	0	...
4	$e/10$	0.	2	7	1	8	...
⋮	⋮						

Guide for Induction Proofs

- Restate the claim you are trying to prove
- **Base case**: Prove the claim holds for the "first" value of n
  - Prove $P(n_0)$ is true
- **Inductive Step**: Prove that $P(k) \to P(k+1)$ for an arbitrary integer k in the desired range.
  - Let k be an arbitrary integer with $k \geq n_0$
  - Assume $P(k)$
  - Show that $P(k+1)$ holds
- Conclusion: explain that you've proven the desired claim.

Remember that the inductive step is like "climbing up the ladder", so it needs to cover the first rung we get on (the base case) as well!

Important note: Your base case should be *included* at the beginning of the domain of the inductive step

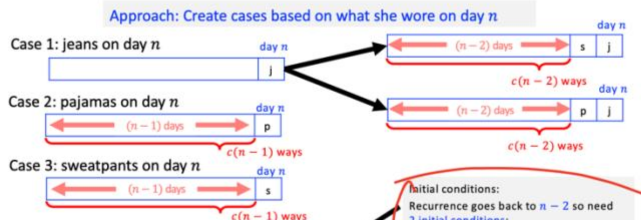
Equivalently: Show $P(k-1) \to P(k)$

Example: Katie's Pandemic Outfits

Katie has three outfit choices while social distancing. Each day she wears either pajamas, sweatpants, or jeans. Her only rule is that she never wears jeans on two or more days in a row.

Let $c(n)$ represent the number of ways Katie can choose outfits across n days, $n \geq 0$. Find a recurrence relation for $c(n)$ including the initial conditions

Approach: Create cases based on what she wore on day n



Sum counts across all cases to get:
$c(n) = 2c(n-1) + 2c(n-2)$
With initial conditions:
$c(0) = 1, \quad c(1) = 3$

Initial conditions:
Recurrence goes back to $n-2$ so need 2 initial conditions:
- Easiest to do 0 days and 1 day (but could do 1 day and 2 days)
- $c(0) = 1$ (1 way to choose over 0 days, i.e., **1 way to do nothing**)
- $c(1) = 3$ (3 ways to choose over 1 day)

$$C(n) = \begin{cases} \text{Case 1: } c(n-2) + c(n-2) = 2 \Leftarrow \\ \text{Case 2: } c(n-1) = \Leftarrow \\ \text{Case 3: } c(n-1) = \Leftarrow \end{cases}$$

......

Strong Induction as Dominos

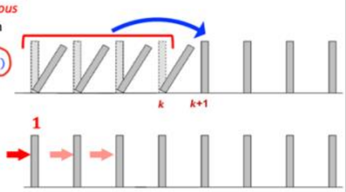
Let $P(n)$ be a predicate.

Goal: Prove that $P(n)$ is true for all $n \in Z^+$

Step 1: [Strong] Inductive Step

If you can knock down *all the previous* dominos, then you can knock down the **k+1st** one.

$[P(1) \wedge P(2) \wedge \cdots \wedge P(k)] \to P(k+1)$



Step 2: Base Case(s)

You can knock down the first domino(s) $P(1)$

Possibly also: $P(2)$ and $P(3)$ and more

Therefore, you can knock down all dominos.

10

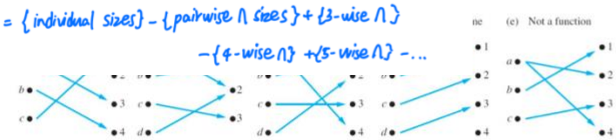
	Weak induction	.vs	Strong Induction
Basic Step	P(1)	Same	P(1)
Inductive Step	$\forall k \in Z^+ [P(k) \to P(k+1)]$		$\forall k \in Z^+ [P(1) \wedge \ldots \wedge P(k) \to P(k+1)]$
Conclusion	$\forall n \in Z^+ P(n)$	Same	$\forall n \in Z^+ P(n)$

(1) Strong Induction 有更充分的条件
(2) 能weak Induction的一定能strong Induction, 反之不然

Review:

1. (cardinality) $|S|$: the number of elements in S.
2. (Cartesian Product) $A \times B = \{(a,b) \mid a \in A, b \in B\}$
   $A \times B \times \dots \times N = \{(a,b,\dots,n) \mid a \in A, b \in B, \dots n \in N\}$
3. $S \cap T$, $S \cup T$, $\bar{S}$, $S - T$
4. subset, proper set, disjoint
5. Power set: $P(S) = \{A \mid A \subseteq S\}$
6. $A \subseteq B \land B \subseteq A \Rightarrow A = B$
7. $\overline{A \cup B} = \bar{A} \cap \bar{B}$
8. $|S| = n \Rightarrow |P(S)| = 2^n$
9. $|A \cup B| = |A| + |B| - |A \cap B|$
   $|A \cap B| = |A| + |B| - |A \cup B|$
10. $|A+B+C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$
    $|\bigcup_i A_i| = \{\text{individual sizes}\} - \{\text{pairwise} \cap \text{sizes}\} + \{3\text{-wise} \cap\}$
    $- \{4\text{-wise} \cap\} + \{5\text{-wise} \cap\} - \dots$

Functi



If $f: A \to B$ is one-to-one, then $|A| \le |B|$

If $f: A \to B$ is onto, then $|A| \ge |B|$

Suppose that $f: A \to B$.

To show that f is injective Show that if $f(x) = f(y)$ for arbitrary $x, y \in A$ with $x \neq y$, then $x = y$.

To show that f is not injective Find particular elements $x, y \in A$ such that $x \neq y$ and $f(x) = f(y)$.

To show that f is surjective Consider an arbitrary element $y \in B$ and find an element $x \in A$ such that $f(x) = y$.

To show that f is not surjective Find a particular $y \in B$ such that $f(x) \neq y$ for all $x \in A$.

Find the last digit of $(38475393)^{324334}$

Solution:

Use mod 10 to find the last digit.

In mod 10,

$$
\begin{aligned}
(38475393)^{324334} &\equiv (3)^{324334} && (mod\ 10)\\
&\equiv (3^2)^{324334/2} && (mod\ 10)\\
&\equiv (9)^{324334/2} && (mod\ 10)\\
&\equiv (-1)^{324334/2} && (mod\ 10)\\
&\equiv (-1)^{some\_even\_power} && (mod\ 10)\\
&\equiv 1 && (mod\ 10)
\end{aligned}
$$

Thus the last digit of $(38475393)^{324334}$ is 1.

- Computing x^n mod m has 2 cases:
  - Case 1: n **is even**, $n = 2k$
    - $x^n \equiv (x^k)^2$ (mod m)
  - Case 2: n **is odd**, $n = 2k+1$
    - $x^n \equiv (x^k)^2 \cdot x$ (mod m)

Examples (or not!) of Functions

1. Is there a function getChild, with domain/codomain both the set of all people, and getChild(x) = y iff y is the child of x?
   ① Some x has no child
   ② Some x has ≥2 children
   A. Yes
   B. No
2. Is there a function getMother, with domain/codomain both the set of all people, and getMother(x) = y iff y is the mother of x?
   Not everyone has exactly one mother.
   A. Yes
   B. No
3. Is there a function f: ℝ → ℝ with $f(x) = y$ iff $x = y^2$?
   ① Some $x\ (<0)$ has no square root
   ② Some $x\ (>0)$ has 2 square roots.
   A. Yes
   B. No
4. Is there a function f: ℝ → ℝ with f(x) = y iff y = 1/x²
   $x = 0$ has no mapping
   A. Yes
   B. No

One-to-one correspondence.

– If $f: A \to B$ is 1-1, then $|A| \le |B|$.

– If $f: A \to B$ is 1-1 and onto, then $|A| = |B|$.

The Schroeder-Bernstein Theorem: If

$$|A| \le |B| \text{ and } |B| \le |A|$$

then

$$|A| = |B|.$$

(We will use this result w/o proof.)

Proof: $f(x)$ is one-to-one

Let $f: \mathbb{R} \to \mathbb{R}$, $f(x) = 2x + 4$.
Prove: f is one-to-one.

Goal: Prove logical expression

$\forall a_1, a_2 \in \mathbb{R}, [f(a_1) = f(a_2)] \to (a_1 = a_2)$

Let a_1, a_2 be arbitrary real numbers

Assume $f(a_1) = f(a_2)$

$2a_1 + 4 = 2a_2 + 4$
$2a_1 = 2a_2$
$a_1 = a_2$

So $a_1 = a_2$

Thus f is one-to-one

Let $f: \mathbb{R} \to \mathbb{R}$, $f(x) = 2x + 4$.
Prove: f is onto.

Goal: Prove expression

$\forall b \in \mathbb{R}, \exists a \in \mathbb{R}$ such that $f(a) = b$

Let b be an arbitrary real number.

Consider $a = \frac{b}{2} - 2$

Note that a is a real number, and thus in the domain of f.

So $2a = b - 4$
$2a + 4 = b$
So $f(a) = b$
So $f(a) = b$

Side work:
$f(a) = b$
$2a + 4 = b$
$2a = b - 4$
$a = \frac{b}{2} - 2$

⑩ Composition of functions 复合函数

Def: $(g \circ f)(x) = g(f(x))$. We can only compose $g \circ f$ when $\text{codom}(f) \subseteq \text{dom}(g)$

Inverses and Composition

Special Properties:

(1) Bijections have inverse

For bijection $A \to B$, $|A| = |B|$

f, g **onto** $\to g \circ f$ **onto**

$g, g \circ f$ onto $\not\to$ f onto

Generalized Pigeonhole Principle

- If there are P pigeons in H pigeonholes, then there must be at least $\lceil \frac{P}{H} \rceil$ pigeons in some hole

$\lceil \frac{P}{H} \rceil$: ceil 上 (向上取整)

Decimal Digits

Prove:
For every integer n, there exists a multiple of n that has only 0s and 1s in its decimal expansion.

1
11
111
1,111
11,111
111,111
1,111,111
11,111,111
⋮

- **(Holes)** A number can have n possible values (mod n)
- **(Pigeons)** Consider the first $n+1$ integers written with just 1s: {1, 11, 111, …}
- **By the pigeonhole principle**, there exist distinct numbers x, y both written with only $1's$, that have the same value ($mod\ n$). That is, $x \equiv y\ (mod\ n)$.
- Consider the number $x - y$ (WLOG, assume $x > y$)
  - Since $x \equiv y\ (mod\ n)$, we know that $x - y$ is a multiple of n
  - Since x and y are both written with all 1s, then $x - y$ has only 1s and 0s in its decimal expansion
  - So the number $x - y$ satisfies the proposition.

14

Some Countable Sets	Some Uncountable Sets
$\mathbb{Z}^+$	$\mathbb{R}$
$\mathbb{N}, \mathbb{Z}$	$[0, 1]$
$\mathbb{Q}$	$\mathbb{R} - \mathbb{Q}$
$\mathbb{Z} \times \mathbb{Z}$	$P(\mathbb{Z})$
and many more!	and many more!

Definition: A set S is **countable** iff $|S| \le |\mathbb{Z}^+|$

(otherwise it's *uncountable*)