$\mathbb{Q} = \{ r \mid r = \frac{a}{b} ; a \in \mathbb{Z}, b \in \mathbb{N} \}$

$\sqrt{2}$ IS IRRATIONAL — PROOF BY CONTRADICTION

$$\sqrt{2} = \frac{a_*}{b_*}$$

we have an impossible situation, i.e., a contradiction

For b_* to be the minimum possible, it must be that a_* and b_* have no common factors

Square both sides to get rid of the square root, then rearrange a little bit

$$a_*^2 = 2b_*^2$$

(with $k \in \mathbb{N}$)

Aha, a_*^2 is even since it is a multiple of 2, so a_* is even and we can say $a_* = 2k$

Plug $2k$ in for a_* above and we get $(2k)^2 = 2b_*^2$ or $b_*^2 = 2k^2$ — this means b_*^2 is even!

Whoops, if a_* and b_* are both even, they have a common factor of 2

Theorem:
Every even square comes from an even number—and every even number has an even square

n	0	±1	±2	±3	±4	±5	±6	±7	±8	±9	±10	±11	…
n^2	$\boxed{0}$	1	$\boxed{4}$	9	$\boxed{16}$	25	$\boxed{36}$	49	$\boxed{64}$	81	$\boxed{100}$	121	…

Proof: We use an exhaustive (case-by-case) proof

(a) n is even $\rightarrow n = 2k$ $(k \in \mathbb{Z})$ $\rightarrow n^2 = 2(2k^2)$ $\rightarrow n^2$ is even (divisible by 2)

(b) n is odd $\rightarrow n = 2k + 1$ $(k \in \mathbb{Z})$ $\rightarrow n^2 = 2(2k^2 + 2k) + 1$ $\rightarrow n^2$ is odd

Here, n must be even or odd (*exhaustive*)—also, n is *general*, i.e., no restrictions on n

Given a claim in the form $p \rightarrow q$, we can consider using a *direct proof* as follows…

Proof. We prove the implication using a direct proof.

1. Start by assuming that the statement claimed in p is true
2. Restate your assumption in mathematical terms, as necessary
3. Use mathematical and logical derivations to relate your above assumptions to q
4. Argue that you have shown that q must be true
5. End by concluding that q is true ■

Prove the following claim: if $x, y \in \mathbb{Q}$, then $x + y \in \mathbb{Q}$

Proof. We prove the implication using a direct proof.

1. Assume that $x, y \in \mathbb{Q}$, i.e., x and y are rational.
2. Then, by definition, there are integers a, c and natural numbers b, d such that $x = a/b$ and $y = c/d$.
3. Then $x + y = (ad + bc)/bd$.
4. Since $ad + bc \in \mathbb{Z}$ and $bd \in \mathbb{N}$, $(ad + bc)/bd$ is rational (by definition).
5. Thus, we conclude from steps 3 and 4 that $x + y \in \mathbb{Q}$. ■

Given $x \in \mathbb{R}$; claim $P(x)$: if $\underbrace{4^x - 1 \text{ is divisible by } 3}_{p}$, then $\underbrace{4^{x+1} - 1 \text{ is divisible by } 3}_{q}$

Proof. We prove the claim using a direct proof.

1. Assume that p is true, i.e., $4^x - 1$ is divisible by 3.
2. This means that $4^x - 1 = 3k$ for an integer k; from this, $4^x = 3k + 1$.
3. Since $4^{x+1} = 4 \cdot 4^x$, we have $4^{x+1} = 4 \cdot (3k + 1) = 12k + 4$.

   Therefore, $4^{x+1} - 1 = 12k + 3 = 3 \cdot (4k + 1)$, which is a multiple of 3.
4. Since $4^{x+1} - 1$ is a multiple of 3, we have shown that $4^{x+1} - 1$ is divisible by 3.
5. Therefore, the statement claimed in q is true. ■

Given a claim in the form $p \rightarrow q$, we can consider using *contraposition* as follows…

Proof. We prove the implication using contraposition.

1. Start by assuming that the statement claimed in q is false
2. Restate your assumption in mathematical terms, as necessary
3. Use mathematical and logical derivations to relate your above assumptions to p
4. Argue that you have shown that p must be false
5. End by concluding that p is false ■

Given claim $P(x)$: integer x is divisible by 3 IF AND ONLY IF x^2 is divisible by 3

Proof. We prove the claim by proving each implication.

(i) We use a direct proof to prove that if x is divisible by 3, then x^2 is divisible by 3.

Assume x is divisible by 3, so $x = 3k$ for some $k \in \mathbb{Z}$.

Squaring both sides, $x^2 = 9k^2 = 3 \cdot (3k^2)$, which is also a multiple of 3.

Thus, x^2 is divisible by 3, as was to be shown.

(ii) We use contraposition to prove that if x^2 is divisible by 3, then x is divisible by 3.

Assume x is <u>not</u> divisible by 3. There are two cases for x…

Case 1. $x = 3k + 1$. Here, $x^2 = 3k(3k + 2) + 1$, so 1 more than a multiple of 3.

Case 2. $x = 3k + 2$. Here, $x^2 = 3(3k^2 + 4k + 1) + 1$, so also 1 more than a multiple of 3.

In both cases, we have shown that x^2 is <u>not</u> divisible by 3, as was to be shown. ■

Given any claim p, we can always use proof by *contradiction* to prove p…

Proof. We prove the claim by contradiction.

1. Start by assuming that the statement claimed in p is false.
2. Restate your assumption in mathematical terms, as necessary.
3. Use mathematical and logical derivations to derive a conflicting truth, i.e., a contradiction that must be false.
4. End by concluding that the assumption in step 1 is false, so p must be true. ■

Given claim $P(n)$, we construct a proof by *induction* to show $P(n)$ holds for all $n \geq n_0$:

Proof. We use induction to prove $\forall n \geq n_0 : P(n)$. [We often set $n_0 = 1$.]

1. Show that $P(n_0)$ is **T**. [Base case.]
2. Show that $P(n) \rightarrow P(n+1)$ for a *general* $n \geq n_0$. [Induction step.]

   Direct proof:
   Assume $P(n)$ is **T**.
   Show $P(n+1)$ is **T**.

   or

   Proof by contraposition:
   Assume $P(n+1)$ is **F**.
   Show $P(n)$ is **F**.
3. Conclude therefore that $P(n)$ holds for all $n \geq n_0$. ■

Prove claim $P(n) =$ "$1 + 2 + \ldots + n = \frac{n(n+1)}{2}$" using induction

Proof. We use induction to prove $\forall n \geq 1 : P(n)$.

1. **[Base case]** $P(1) = ½(1)(1 + 1) = 1$. $P(1)$ is **T**.
2. **[Induction step]** We show $P(n) \rightarrow P(n+1)$ for all $n \geq 1$ via a direct proof.

   Assume (*induction hypothesis*) that $P(n)$ is **T**.

   Prove $P(n+1)$: $1 + 2 + \ldots + n + (n+1) = \frac{(n+1)(n+2)}{2}$.

   LHS: $1 + 2 + \ldots + n + (n+1) = \underbrace{[1 + 2 + \ldots + n]} + (n+1)$

   plug in the induction hypothesis…

   $$= \frac{n(n+1)}{2} + (n+1) = \frac{1}{2}\underbrace{(n+1)}_{k}\underbrace{(n+1+1)}_{k+1}.$$
3. By induction, we have proven $P(n)$ for all $n \geq 1$. ■

Claim 3. $P(n) = n \leq 2^n$. Prove $\forall n \geq 1$, $P(n)$ is **T**.

our induction pro
prove using the Well-Ordering

Proof. We prove $\forall n \geq 1 : P(n)$ by contradiction.

Assume there is a counter-example that shows $P(n)$ to be **F**, i.e., $\exists n : n > 2^n$.

Collect all counter-examples into set B.

By the Well-Ordering Principle, set B has minimum element n_*, with $n_* > 2^{n_*}$.

Observe $1 < 2^1$, so $n_* \geq 2$, or $½ n_* \geq 1$. Next, consider $n_* - 1$: based on our initial

since $n_* \geq 2$ $\rightarrow$ $n_* - 1 \geq n_* - ½ n_* = ½ n_* > ½ 2^{n_*} = 2^{n_*-1}$

Thus, $n_* - 1 > 2^{n_*-1}$, but if $n_* - 1 \in B$, it must be smaller than n_*—a contradiction!

Therefore, we have proven that $\forall n \geq 1 : P(n)$ is **T**. ■

CSCI-2200 FOCS F 2022 Crib Sheet Exam 1 Tuesday, October 5, 2022 Hayden Fuller   Notes:

NEGATION: $a \vee b => \neg a \wedge \neg b$; $a \wedge b => \neg a \vee \neg b$; if a, then b=$a \to b => a \wedge \neg b$

$\forall x, A(x) => \exists x : \neg A(x)$; $\exists x : A(x) => \forall x \neg A(x)$

$\forall x : (\exists y : 2x - y = 0) = T$(already know x); $\exists y : (\forall x : 2x - y = 0) = F$(can't predict x);

$\exists y : (\forall x : xy = 0) = T$(x doesn't matter, y=0)

statement: $p \to q$ converse: $q \to p$ inverse: $\neg p \to \neg q$ contrapositive: $\neg q \to \neg p$

$\cup$ union; $\cap$ intersection; $\subset$ proper subset; $\subseteq$ subset(can be equal);

What type of proof is appropriate? Contradiction:

There is a prime number greater than ab

$2^{\frac{1}{p}}$ is irrational for any integer $p > 2$, given: $a, b, c, n \in \mathbb{N}, n > 2, a^n + b^n = c^n$

Contraposition:

Direct:

There is an even number grater than ab (either $ab+1$ or $ab+2$ is even)

if n and q are natural numbers, then there exists unique intergers d and r satisfying $n = dq + r$, with $d \in 0 \cup \mathbb{N}$ and $0 \le r \le q$.

Leaping induction:

Induction:

$(a+b)^n \geq a^n + b^n$, when n is a natural number.

$n^2 \le 2^n$ for all $n \geq 4$

5 divides $11^n - 6$ for all $n \geq 5$; show 5 divides $11^5 - 6$ and show for $n \geq 5$, if 5 divides $11^n - 6$, then 5 divides $11^{n+1} - 6$

Weak induction:

$11^n - 6$ is divisible by 5 if n is a natural number.

Proof Method	Situation
Direct proof	Appears clear how result follows from assumption
Contraposition	Appears clear how if result is **F**, the assumption will be **F**
Show a counter-example	Disprove an implication
Show an example	Prove something exists $\exists$
Contradiction	Prove something does not exist
Contradiction	Prove something is unique
Show for general object	Prove something is true for <u>all</u> objects
Show a counter-example	Disprove something is true for <u>all</u> objects

Given new claim $Q(n) = (n^2 \le 2^n) \wedge (2n + 1 \le 2^n)$. Prove $\forall n \geq 4$, $Q(n)$ is **T**.

we strengthen the claim, so we assume mor

Proof. We use induction to prove $\forall n \geq 4 : Q(n)$.

1. **[Base case]** For $Q(4)$, we have $4^2 \le 2^4$ and $2(4) + 1 \le 16$, both of which are **T**.
2. **[Induction step]** Assume $Q(n)$ is **T**, i.e., (i) $n^2 \le 2^n$ and (ii) $2n + 1 \le 2^n$.

   We must prove $Q(n+1)$, i.e., (i) $(n+1)^2 \le 2^{n+1}$ and (ii) $2(n+1) + 1 \le 2^{n+1}$.

   LHS (i): $(n+1)^2 = n^2 + 2n + 1 \le 2^n + 2n + 1 \le 2^n + 2^n = 2^{n+1}$. using both assumptic

   LHS (ii): $2(n+1) + 1 = 2 + 2n + 1 \le 2^n + 2^n = 2^{n+1}$. using initial assumption (ii) and the fact that $2 \le 2^n$

   Both (i) and (ii) together prove $Q(n+1)$ is **T**.
3. By induction, we have proven $Q(n)$ for all $n \geq 4$, which also proves claim $P(n)$. ■

Given claim $P(n) : n^3 \le 2^n$, prove $\forall n \geq 10$, $P(n)$ is **T** using k-leaping induction

Proof. We use 2-leaping induction to prove $\forall n \geq 10 : P(n)$.

1. **[Base cases]** For $P(10)$, we have $10^3 \le 2^{10}$, or $1000 \le 1024$, which is **T**.

   And for $P(11)$, we have $11^3 \le 2^{11}$, or $1331 \le 2048$, which is **T**.
2. **[Induction step]** Assume $n^3 \le 2^n$. We must prove $P(n+2)$, i.e., $(n+2)^3 \le 2^{n+2}$.

   LHS: $(n+2)^3 = n^3 + 6n^2 + 12n + 8 \le n^3 + n \cdot n^2 + n^2 n + n^3$

   $= 4n^3 \le 4 \cdot 2^n = 2^{n+2}$.

   For n^3 to emerge, if $n \geq 10$, observe that $6 \le n$, $12 \le n^2$, and $8 \le n^3$

   Thus, $P(n) \to P(n+2)$ is shown to be **T**.
3. By 2-leaping induction, we have proven $P(n)$ for all $n \geq 10$. ■

Consider $P(n)$, the *Fundamental Theorem of Arithmetic*, which states that for all $n \geq 2$, we can write n as the product of one or more prime numbers

Claim $Q(n)$ is $P(2) \wedge P(3) \wedge \ldots \wedge P(n)$, i.e., $2, 3, \ldots, n$ are <u>all</u> products of prime numbers

Proof. We prove by induction that $Q(n)$ is **T** for $n \geq 2$.

1. **[Base case]** $Q(2) = P(2)$, i.e., 2 is a product of prime numbers, which is **T**.
2. **[Induction step]** We show $Q(n) \to Q(n+1)$ for all $n \geq 2$ via a direct proof.

   Assume $Q(n)$ is **T**: each of $2, 3, \ldots, n$ is a product of prime numbers.
   We must prove $Q(n+1)$ is **T**: each of $2, 3, \ldots, n, n+1$ is a product of primes.

   By our induction hypothesis, $Q(n)$, observe that $2, 3, \ldots, n$ are products of primes.

   Therefore, we need only prove that $n+1$ is a product of primes—two cases:

   Case 1. $n+1$ is prime. In this case, nothing more to prove.

   Case 2. $n+1$ is not prime, so $n+1 = k\ell$, where $2 \le k, \ell \le n$. From our induction hypothesis, both $P(k)$ and $P(\ell)$ are **T**, which shows k and ℓ to be products of primes.

   Therefore, $n+1 = k\ell$ is a product of primes and $Q(n+1)$ is shown to be **T**.
3. By induction, $Q(n)$ is **T** for all $n \geq 2$. ■

Claim $Q(n)$: (i) Any $2^n \times 2^n$ grid with $n \geq 1$ minus a <u>center</u> square can be L-tiled; and (ii) Any $2^n \times 2^n$ grid with $n \geq 1$ minus a <u>corner</u> square can be L-tiled

Proof. We prove claim $Q(n)$ for all $n \geq 1$ by induction.

1. **[Base case]** $Q(1)$ holds for center and corner squares: 
2. **[Induction step]** We prove $Q(n) \to Q(n+1)$ for $n \geq 1$ using a direct proof.

   Assume $Q(n)$: (i) Any $2^n \times 2^n$ grid minus a center square can be L-tiled; and (ii) Any $2^n \times 2^n$ grid minus a corner square can be L-tiled.

   Prove $Q(n+1)$: (i) Any $2^{n+1} \times 2^{n+1}$ grid minus a center square can be L-tiled; and (ii) Any $2^{n+1} \times 2^{n+1}$ grid minus a corner square can be L-tiled.

   (i) For a $2^{n+1} \times 2^{n+1}$ grid missing a center square, ...

   (ii) For a $2^{n+1} \times 2^{n+1}$ grid missing a corner square, ...

See the rest of the proof on p