AN ARGUMENT IS VALID IF THE CONCLUSION IS TRUE WHENEVER ALL THE ASSUMPTIONS ARE TRUE (NO MATTER WHAT PARTICULAR STATEMENTS ARE SUBSTITUTED FOR THE VARIABLES).

DEF: A PROOF IS A VALID ARGUMENT USED TO ESTABLISH A RESULT

NOTE: THE ASSUMPTIONS IN AN ARGUMENT OR A PROOF CAN BE AXIOMS, PREVIOUSLY PROVED THEOREMS, OR MAY FOLLOW FROM PREVIOUS STATEMENTS BY A MATHEMATICAL OR LOGICAL RULE.

EX: PROVE THAT IF $x \in \mathbb{R}$ AND $n \in \mathbb{N}$ IS EVEN, THEN $x^n \geq 0$.

$n \in \mathbb{N}$ IS EVEN.	(GIVEN)
$n = 2m$ FOR SOME $m \in \mathbb{N}$.	(DEF. OF EVEN NUMBER)
$x^n = x^{2m}$	(SUBSTITUTION)
$= (x^m)^2$	(RULE OF EXPONENTS)
≥ 0	($y^2 \geq 0 \ \forall y \in \mathbb{R}$)

$\square$

A PROOF SHOULD BE COMPLETE (CONTAIN ALL NECESSARY STATEMENTS) AND CONCISE (NOT CONTAIN EXTRA OR UNNEEDED STATEMENTS).

TESTING VALIDITY

TO TEST AN ARGUMENT FOR VALIDITY, FOLLOW THESE STEPS.

1. IDENTIFY THE ASSUMPTIONS AND CONCLUSION.
2. CONSTRUCT A TRUTH TABLE OF ALL THE ASSUMPTIONS AND THE CONCLUSION.
3. IF THE CONCLUSION IS TRUE IN EVERY CASE WHERE ALL THE ASSUMPTIONS ARE TRUE, THE ARGUMENT IS VALID. IF THERE IS A ROW OF ALL TRUE ASSUMPTIONS AND FALSE CONCLUSION, THE ARGUMENT IS INVALID.

EX: IS THE ARGUMENT VALID?

$p \Rightarrow q \vee \sim r$,

$q \Rightarrow p \wedge r$,

$\therefore p \Rightarrow r$.

p	q	r	$p \Rightarrow q \vee \sim r$	$q \Rightarrow p \wedge r$	$p \Rightarrow r$
T	T	T			
T	T	F			
T	F	T			
T	F	F			
F	T	T			
F	T	F			
F	F	T			
F	F	F			

EXERCISE: TEST THE VALIDITY.

a) $p \vee (q \vee r)$,

$\sim r$,

$\therefore p \vee q$.

b) $p \Rightarrow q$,

p,

$\therefore q$.

THE SIMPLE ARGUMENT b) IS VALID (WE SAW IT WITH PEPPA PIG), AND IT HAS A NAME: MODUS PONENS.

DEF: AN ARGUMENT CONSISTING OF 2 PREMISES AND A CONCLUSION IS CALLED A SYLLOGISM. THE MOST FAMOUS SYLLOGISM IS THE MODUS PONENS, LATIN FOR "METHOD OF AFFIRMING".

IF p, THEN q,

p,

THEREFORE, q.

EX: IS THE STATEMENT "$n \in \mathbb{N}$ IS EVEN $\Rightarrow n^2$ IS EVEN" TRUE?

PROVE IT. LET $n = 9866$. IS IT TRUE OR FALSE TO SAY n^2 IS EVEN?

PRINCIPLE OF MATHEMATICAL INDUCTION: IF $p(n)$ IS A STATEMENT WITH $\operatorname{dom} p = \mathbb{N}$ SUCH THAT

a) $p(1)$ IS TRUE, AND

b) $p(k)$ TRUE $\Rightarrow p(k+1)$ TRUE,

THEN $p(n)$ IS TRUE FOR ALL $n \in \mathbb{N}$.

EX: PROVE THAT $4^n - 1$ IS A MULTIPLE OF 3 $\forall n \in \mathbb{N}$.

A: $p(n)$: $4^n - 1$ IS A MULTIPLE OF 3.

i.e. $\dfrac{4^n - 1}{3} = m$ FOR SOME $m \in \mathbb{Z}$.

$\Rightarrow 4^n - 1 = 3m \Rightarrow 4^n = 3m + 1$.

a) $p(1)$: $4^1 - 1 = 4 - 1 = 3$, IS A MULTIPLE OF 3. ✓

b) ASSUME $p(k)$, PROVE $p(k+1)$.

ASSUME $4^k = 3m + 1$ FOR SOME $m \in \mathbb{Z}$. (THIS IS $p(k)$.)

$p(k+1)$: $\dfrac{4^{k+1} - 1}{3}$ IS A ~~[illegible]~~ WHOLE NUMBER?

$$\frac{4^{k+1} - 1}{3} = \frac{4 \cdot 4^k - 1}{3} = \frac{4(3m+1) - 1}{3} = \frac{12m + 4 - 1}{3} = 4m + 1 \in \mathbb{Z}. \checkmark$$

$\therefore 4^n - 1$ IS A MULTIPLE OF 3 FOR ALL $n \in \mathbb{N}$.

THE LAW OF SYLLOGISM

IS THE FOLLOWING A TAUTOLOGY?

$$[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow p \Rightarrow r$$

THE LAW OF SYLLOGISM IS:

IF $p \Rightarrow q$ AND $q \Rightarrow r$, THEN $p \Rightarrow r$.

Ex: SUPPOSE THESE 2 STATEMENTS ARE TRUE.

1) IF IT RAINS TODAY, THEN I'LL DRIVE TO SCHOOL.

2) IF I DRIVE TO SCHOOL TODAY, THEN I'LL GO OVER MY GAS BUDGET.

THEN BY THE LAW OF SYLLOGISM, WE CAN INFER ANOTHER TRUTH:

IF IT RAINS TODAY, THEN I'LL GO OVER MY GAS BUDGET.

PROVING $\exists$ STATEMENTS

HOW DO WE PROVE A STATEMENT OF THE FORM

$$\exists x \in D \ni p(x) \ ?$$

WE NEED TO FIND AT LEAST ONE $x \in D$ THAT MAKES $p(x)$ TRUE.

Ex: PROVE THAT THERE EXISTS AN EVEN NUMBER THAT CAN BE WRITTEN TWO WAYS AS THE SUM OF TWO PRIME NUMBERS.

$4 = 2+2$

$6 = 3+3$

$8 = 5+3$

$10 = 7+3 = 5+5 \Rightarrow \boxed{10}$ $\square$

Ex: PROVE $\exists x \in \mathbb{R} \ni x+5=0$.

Ex: PROVE THERE IS A MONTH OF THE YEAR WHOSE NAME HAS 3 LETTERS.

PROVING $\forall$ STATEMENTS

HOW DO WE PROVE A STATEMENT OF THE FORM

$$\forall x \in D,\ p(x)\ ?$$

THERE ARE TWO OPTIONS:

1) METHOD OF EXHAUSTION, 2) GENERALIZED PROOF.

THE METHOD OF EXHAUSTION CHECKS THAT $p(x)$ IS TRUE FOR EVERY $x \in D$. THIS IS FINE WHEN D IS SMALL, BUT BECOMES A LOT OF WORK FOR D LARGE. IF D IS INFINITE, THIS METHOD FAILS TO BE OF ANY USE.

EX: PROVE THAT EVERY EVEN NUMBER BETWEEN 4 AND 16 CAN BE WRITTEN AS THE SUM OF 2 PRIMES.

EX: PROVE THAT EVERY EVEN $n \in \mathbb{N}$ CAN BE WRITTEN AS THE SUM OF 2 PRIMES

THE GENERALIZED PROOF IS CONSTRUCTED SO THAT IT APPLIES TO EVERY POSSIBLE SITUATION. IT TAKES AS MANY NONSPECIFIC ELEMENTS OF D AS NEEDED AND PROVES THE STATEMENT, SO THAT THE PROOF IS VALID FOR ALL ELEMENTS OF D.

EX: PROVE THAT IF $a, b \in \mathbb{Z}$, THEN $10a + 8b$ IS DIVISIBLE BY 2.

A: LET $a, b \in \mathbb{Z}$. THEN $10a + 8b = 2(5a + 4b)$.

SINCE $a, b \in \mathbb{Z}$, $5a + 4b \in \mathbb{Z}$.

$\Rightarrow 2(5a + 4b)$ IS EVEN.

$\therefore 10a + 8b$ IS EVEN. $\square$

NOTICE THAT IT DOESN'T MATTER WHICH TWO INTEGERS WE CHOOSE FOR a AND b; THE ABOVE PROOF IS VALID FOR ALL SUCH CHOICES.

DISPROVING $\exists$ STATEMENTS

TO DISPROVE A STATEMENT MEANS TO PROVE ITS NEGATION. RECALL THE NEGATION OF AN EXISTENTIAL STATEMENT:

$$\sim(\exists x \in D \ni p(x)) \equiv \forall x \in D, p(x).$$

SO TO DISPROVE AN $\exists$ STATEMENT, WE MUST PROVE A $\forall$ STATEMENT, VIA METHOD OF EXHAUSTION OR GENERALIZED PROOF.

EX: DISPROVE THE STATEMENT "THERE EXISTS AN EVEN PRIME NUMBER LARGER THAN 2."

A: NEGATION IS "FOR ALL PRIME NUMBERS x LARGER THAN 2, x IS ODD."

LET $x > 2$ BE PRIME. SUPPOSE x IS EVEN. THEN $x = 2n$ FOR SOME $n \in \mathbb{N}$. $\Rightarrow \frac{x}{2} = \frac{2n}{2} = n$, SO x IS DIVISIBLE BY 2 AND IS NOT PRIME.

THIS CONTRADICTS OUR ORIGINAL STATEMENT "LET $x > 2$ BE PRIME." WE SUPPOSED x IS EVEN AND ARRIVED AT A CONTRADICTION, SO x CANNOT BE EVEN. THEREFORE, x IS ODD, AND WE HAVE PROVED THAT THERE DOES NOT EXIST AN EVEN PRIME LARGER THAN 2. $\square$

THIS IS AN EXAMPLE OF PROOF BY CONTRADICTION, WHICH WE WILL SEE IN MORE DETAIL LATER.

DISPROVING $\forall$ STATEMENTS

TO DISPROVE A $\forall$ STATEMENT, WE MUST PROVE AN $\exists$ STATEMENT:

$$\sim(\forall x \in D, p(x)) \equiv \exists x \in D \ni \sim p(x).$$

SO WE MUST FIND ONE $x \in D$ SUCH THAT $p(x)$ IS FALSE (A COUNTEREXAMPLE).

EX: DISPROVE THE STATEMENT "$\forall x \in \mathbb{R}, x < 0 \vee x > 0$".

A: NEGATION IS "$\exists x \in \mathbb{R} \ni x \geq 0 \wedge x \leq 0$".

LET $x = 0$. THEN $x \geq 0 \wedge x \leq 0$. $\square$

Ex: DISPROVE THE STATEMENT "$\forall a, b \in \mathbb{R}$, IF $a^2 = b^2$, THEN $a = b$.

Ex: PROVE OR DISPROVE: "$\forall x \in \mathbb{R}, \exists y \in \mathbb{R} \ni x + y = 0$.

GENERALIZED PROOF 1: DIRECT PROOF

A DIRECT PROOF WORKS IN A STRAIGHTFORWARD MANNER FROM ASSUMPTIONS TO SOLUTION. WE OFTEN REWRITE ASSUMPTIONS IN LOGIC NOTATION.

Ex: PROVE THAT IF $3x - 9 = 15$, THEN $x = 8$.

A: $3x - 9 = 15$

$3x = 15 + 9 = 24$

$x = \frac{24}{3} = 8$. $\square$

Ex: PROVE THAT THE SUM OF ANY TWO EVEN NUMBERS IS EVEN.

A: LET a, b BE EVEN. THEN $\exists\, c, d \in \mathbb{Z} \ni a = 2c, b = 2d$.

$a + b = 2c + 2d$

$= 2(c + d)$

$c, d \in \mathbb{Z} \Rightarrow c + d \in \mathbb{Z}$.

$\Rightarrow a + b = 2e, e \in \mathbb{Z}$.

$\therefore a + b$ IS EVEN. $\square$

Ex: PROVE THAT IF a, b ARE PERFECT SQUARES, THEN ab IS A PERFECT SQUARE.

($x \in \mathbb{Z}$ IS A PERFECT SQUARE IF $x = y^2$ FOR SOME $y \in \mathbb{Z}$.)

$a = c^2, b = d^2$ FOR SOME $c, d \in \mathbb{Z}$.

$ab = c^2 d^2$

$= (cd)^2$

$c, d \in \mathbb{Z} \Rightarrow cd \in \mathbb{Z}$.

$\therefore ab = e^2$ FOR SOME $e \in \mathbb{Z}$. ab IS A PERFECT SQUARE. $\square$

EX: PROVE THAT $\forall x \in \mathbb{R}, -x^2+2x+1 \leq 2.$

$$-x^2+2x+1 \leq 2 \iff -x^2+2x-1 \leq 0$$
$$\iff x^2-2x+1 \geq 0$$
$$\iff (x-1)^2 \geq 0 \quad \text{(TAUTOLOGY)}$$

$\therefore -x^2+2x+1 \leq 2 \ \forall x \in \mathbb{R}$ $\square$

GENERALIZED PROOF 2: PROOF BY CONTRADICTION

EXERCISE: PROVE THAT $p \Rightarrow q \equiv \sim q \Rightarrow \sim p$.

TO PROVE $p \Rightarrow q$, ONE MAY INSTEAD PROVE $\sim q \Rightarrow \sim p$. THAT IS, ASSUME THAT THE NEGATION OF THE CONCLUSION IS TRUE, AND SHOW THAT ONE OF THE ASSUMPTIONS (OR SOME OTHER WELL-KNOWN TRUTH) IS FALSE.

EX: PROVE "$\forall n \in \mathbb{N}$, IF n^2 IS EVEN, THEN n IS EVEN" BY CONTRADICTION.

A: $p(n)$: n^2 IS EVEN.
$q(n)$: n IS EVEN.

$\forall n, p(n) \Rightarrow q(n) \equiv \forall n, \sim q(n) \Rightarrow \sim p(n)$.

SO WE ASSUME THAT n IS ODD, AND SHOW THAT n^2 MUST BE ODD.

LET n BE ODD.

$n^2 = n \cdot n = (\text{ODD})(\text{ODD}) = \text{ODD}$ (PROPERTY OF MULTIPLICATION)

$\therefore n$ ODD $\Rightarrow n^2$ ODD.

$\therefore n^2$ EVEN $\Rightarrow n$ EVEN. $\square$

EX: PROVE BY CONTRADICTION THAT $y \in \mathbb{R} \setminus \mathbb{Q} \Rightarrow y+7 \in \mathbb{R} \setminus \mathbb{Q}$.

A: TO PROVE BY CONTRADICTION, ASSUME THAT $y+7 \in \mathbb{Q}$ AND SHOW THAT $y \in \mathbb{Q}$.

LET $y+7 \in \mathbb{Q}$. THEN $\exists\, a,b \in \mathbb{Z}, b \neq 0 \ni y+7 = \frac{a}{b}$.

$$\Rightarrow y = \frac{a}{b} - 7$$
$$= \frac{a}{b} - \frac{7b}{b}$$
$$= \frac{a-7b}{b} \in \mathbb{Q}$$

(CONTRADICTION)

$\therefore y+7 \in \mathbb{R} \setminus \mathbb{Q}$. $\square$

GENERALIZED PROOF 3: PROOF BY CASES

HOW DO WE PROVE "IF $x \neq 0$ OR $y \neq 0$, THEN $x^2+y^2 > 0$"?
WE NEED TO SPLIT THE PROBLEM INTO CASES, PROVING THE CONCLUSION FIRST IF $x \neq 0$, THEN IF $y \neq 0$. ANY STATEMENT OF THE FORM

$$(p \vee q) \Rightarrow r$$

CAN BE DONE THIS WAY, BECAUSE OF THE LOGICAL EQUIVALENCE

$$(p \vee q) \Rightarrow r \equiv (p \Rightarrow r) \wedge (q \Rightarrow r).$$

__EX__: PROVE "$x \neq 0$ OR $y \neq 0 \Rightarrow x^2+y^2 > 0$".

__CASE 1__: LET $x \neq 0$. THEN $x^2 > 0$, AND $y^2 \geq 0$.
$$\Rightarrow x^2+y^2 > 0.$$

__CASE 2__: LET $y \neq 0$. THEN $x^2 \geq 0$, AND $y^2 > 0$.
$$\Rightarrow x^2+y^2 > 0.$$

$\therefore$ IF $x \neq 0$ OR $y \neq 0$, THEN $x^2+y^2 > 0$. $\square$

EX: PROVE THAT $\forall m \in \mathbb{N}$, m^2+m+1 IS ODD.

CASE 1: LET m BE EVEN. THEN m^2 IS EVEN.

$\Rightarrow m^2+m$ IS EVEN.

$\Rightarrow m^2+m+1$ IS ODD.

CASE 2: LET m BE ODD. THEN m^2 IS ODD.

$\Rightarrow m^2+m$ IS EVEN.

$\Rightarrow m^2+m+1$ IS ODD.

$\therefore \forall m \in \mathbb{N}$, m^2+m+1 IS ODD. $\square$

2) NUMBERS

A SET IS A COLLECTION OF OBJECTS CALLED ELEMENTS. WE WRITE $x \in S$ TO MEAN THAT ELEMENT x IS IN SET S. A SET IS NONEMPTY IF IT HAS AT LEAST ONE ELEMENT. THE EMPTY SET IS DENOTED BY $\emptyset$.

A SUBSET OF S IS A SET T WITH THE PROPERTY $x \in T \Rightarrow x \in S$. EVERY ELEMENT OF T IS AN ELEMENT OF S. TRIVIALLY, $S \subseteq S$ AND $\emptyset \subseteq S$ (THE SYMBOL "$\subseteq$" MEANS "IS A SUBSET OF").

THE SET OF NATURAL NUMBERS $\mathbb{N} = \{1, 2, 3, \dots\}$ IS USEFUL FOR COUNTING AND FOR ORDERING. THE ORDER SYMBOLS ARE $<, \leq, >, \geq$.

SET ALGEBRA

AN OPERATION ON A SET S IS A RULE FOR COMBINING ELEMENTS OF S.

A BINARY OPERATION COMBINES PAIRS OF ELEMENTS TO PRODUCE ANOTHER.

A BINARY OPERATION $*$ IS CLOSED IF

$$x, y \in S \Rightarrow x * y \in S.$$

FOUR COMMON OPERATIONS ON NUMBERS ARE $+, -, \cdot, /$.

EX: ARE $+, -, \cdot, /$ CLOSED ON $\mathbb{N}$? PROVE OR DISPROVE.

AN ELEMENT $e \in S$ IS CALLED AN IDENTITY IF

$$e * x = x \text{ AND } x * e = x \quad \forall x \in S.$$

EX: DOES $\mathbb{N}$ HAVE AN IDENTITY UNDER $+$? UNDER $\cdot$?

IF $\exists e$ IDENTITY OF S, AN ELEMENT $x \in S$ IS CALLED INVERTIBLE WHEN $\exists y \in S \ni$

$$x * y = e \text{ AND } y * x = e.$$

THEN y IS CALLED THE INVERSE OF x.

EX: WHAT ARE THE INVERTIBLE ELEMENTS OF $\mathbb{N}$ UNDER $+, \cdot$?

A BINARY OPERATION $*$ ON S IS COMMUTATIVE IF

$$x * y = y * s \quad \forall x, y \in S.$$

IT IS ASSOCIATIVE IF

$$(x * y) * z = x * (y * z) \quad \forall x, y, z \in S.$$

THE OPERATIONS $+, \cdot$ ARE ASSOCIATIVE AND COMMUTATIVE ON $\mathbb{N}$.

EX: ROCK-PAPER-SCISSORS.

LET $M = \{r, p, s\}$ AND CONSIDER THE BINARY OPERATION THAT GIVES THE WINNER OF THE GAME:

$r * p = p * r = p$ (PAPER BEATS ROCK)

$r * s = s * r = r$ (ROCK BEATS SCISSORS)

$p * s = s * p = s$ (SCISSORS BEATS PAPER)

$p * p = p,\ r * r = r,\ s * s = s$ (TIES).

WE SEE BY THE ABOVE THAT $*$ IS COMMUTATIVE. IS IT ASSOCIATIVE?

$(r * p) * s =$

$r * (p * s) =$

A BINARY OPERATION $\cdot$ IS DISTRIBUTIVE OVER ANOTHER $+$ IF FOR ALL $a, b, c \in S$,

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \text{ AND}$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

FOR EXAMPLE, MULTIPLICATION DISTRIBUTES OVER ADDITION ON $\mathbb{N}$.

EXERCISE: PROVE THAT ADDITION DOES NOT DISTRIBUTE OVER MULTIPLICATION ON $\mathbb{N}$.

EX: LET $a, b \in \mathbb{N}$. SIMPLIFY THE FOLLOWING EXPRESSION, GIVING REASONS FOR EACH STEP.

$$[8(a+b)] + 2a =$$

A SET S WITH ORDER $\leq$ IS CALLED <u>WELL-ORDERED</u> IF EVERY NONEMPTY SUBSET T OF S HAS AT LEAST ONE SMALLEST ELEMENT. THAT IS, IF $T \subseteq S$, $T \neq \emptyset$, THEN $\exists\, s_0 \in T \ni s_0 \leq s \ \forall s \in T$.

THE SET $\mathbb{N}$ WITH THE USUAL ORDER $\leq$ IS WELL-ORDERED.

THE SET OF INTEGERS $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2 \ldots\}$ CAN BE CONSTRUCTED FROM $\mathbb{N}$; IT IS THE SET OF DIFFERENCES $\{m-n\}$ $\forall m, n \in \mathbb{N}$. THE ORDER $\leq$ ON $\mathbb{N}$ EXTENDS TO $\mathbb{Z}$,

<u>EX:</u> ARE $+, -, \cdot, /$ CLOSED ON $\mathbb{Z}$?

DOES $\mathbb{Z}$ HAVE IDENTITIES UNDER $+, \cdot$?

WHAT ARE THE INVERTIBLE ELEMENTS IN $\mathbb{Z}$ UNDER $+, \cdot$?

ON $\mathbb{Z}$, $+$ AND $\cdot$ ARE COMMUTATIVE AND ASSOCIATIVE. $-$ AND $/$ ARE NOT; HOWEVER, IF WE DEFINE $a - b = a + (-b)$ AND $a/b = a \cdot 1/b$, THEN WE HAVE COMMUTATIVITY AND ASSOCIATIVITY.

$$a - b \neq b - a, \quad \text{BUT} \quad a + (-b) = -b + a$$

$$\frac{a}{b} \neq \frac{b}{a}, \quad \text{BUT} \quad a \cdot \frac{1}{b} = \frac{1}{b} \cdot a$$

MULTIPLICATION DISTRIBUTES OVER ADDITION AND SUBTRACTION ON $\mathbb{Z}$:

$$a \cdot (b \pm c) = (a \cdot b) \pm (a \cdot c)$$
$$(a \pm b) \cdot c = (a \cdot c) \pm (b \cdot c).$$

EX: IS $\mathbb{Z}$ WELL-ORDERED?

AN INTEGER $m \in \mathbb{Z}$ IS EVEN IF $m = 2k$ FOR SOME $k \in \mathbb{Z}$.

AN INTEGER $m \in \mathbb{Z}$ IS ODD IF $m = 2k+1$ FOR SOME $k \in \mathbb{Z}$.

AN INTEGER $m > 1$ IS PRIME IF WHENEVER $m = rs$ FOR $r, s \in \mathbb{N}$, EITHER $r = 1$ OR $s = 1$.

AN INTEGER $m > 1$ IS COMPOSITE IF IT IS NOT PRIME. (i.e. $m = ab$ WITH $a, b > 1$ AND $a, b < m$, $a, b \in \mathbb{N}$)

EXAMPLES: ...

THE SET OF RATIONALS $\mathbb{Q}$ IS THE SET OF NUMBERS q THAT CAN BE WRITTEN

$$q = \frac{a}{b},\ a, b \in \mathbb{Z},\ b \neq 0.$$

$\mathbb{Q}$ CAN BE CONSTRUCTED FROM $\mathbb{Z}$ AS THE SET OF QUOTIENTS

$$\left\{ \frac{a}{b} \right\} \forall a, b \in \mathbb{Z},\ b \neq 0.$$

EXAMPLES: ...

DEDEKIND CUTS

TO CONSTRUCT THE REAL NUMBERS $\mathbb{R}$, WE CAN USE $\mathbb{Q}$ AND THE DEDEKIND CUTS. A DEDEKIND CUT OF $\mathbb{Q}$ IS A PAIR OF SUBSETS (A, B) OF $\mathbb{Q}$ THAT SATISFY THE FOLLOWING.

1) A AND B ARE NONEMPTY.

2) $A \cup B = \mathbb{Q}$.

3) A IS CLOSED DOWNWARDS: IF $q \in A$ AND $r < q$, THEN $r \in A$.

4) B IS CLOSED UPWARDS: IF $q \in B$ AND $r > q$, THEN $r \in B$.

5) A CONTAINS NO GREATEST ELEMENT: $\forall q \in A \; \exists r \in A \ni q < r$.

GIVEN $q \in \mathbb{Q}$, WE CAN FORM A DEDEKIND CUT (A, B) WHERE $A = \{x \in \mathbb{Q} : x < q\}$ AND $B = \{x \in \mathbb{Q} : x \geq q\}$. THIS IS THE DEDEKIND-CUT IDENTIFICATION OF ALL RATIONAL NUMBERS $q \in \mathbb{Q}$.

BUT WE CAN MAKE SUCH CUTS AT NONRATIONAL NUMBERS AS WELL. AN IRRATIONAL NUMBER IS ONE THAT CANNOT BE WRITTEN AS $\frac{a}{b}$, $a, b \in \mathbb{Z}$, $b \neq 0$. AN EXAMPLE IS $\sqrt{2}$.

<u>EXERCISE</u>: PROVE THAT $\sqrt{2} \notin \mathbb{Q}$.

THE FOLLOWING DEDEKIND CUT DEFINES $\sqrt{2}$:

$$A = \{x : x < 0 \text{ OR } x^2 < 2\}, \quad B = \{x : x > 0 \text{ AND } x^2 \geq 2\}.$$

THE NUMBERS DEFINED BY <u>ALL</u> DEDEKIND CUTS OF $\mathbb{Q}$ MAKE UP THE SET OF REAL NUMBERS $\mathbb{R}$. THE USUAL ORDER $\leq$ ON $\mathbb{R}$ IS INHERITED FROM $\mathbb{Q}$.

<u>EX</u>: WHICH OF $+, -, \cdot, /$ ARE CLOSED ON $\mathbb{R}$?

DOES $\mathbb{R}$ HAVE IDENTITIES UNDER $+, \cdot$?

WHAT ARE THE INVERTIBLE ELEMENTS IN $\mathbb{R}$ UNDER $+, \cdot$?

AS IN $\mathbb{Q}$, THE OPERATIONS $+, \cdot$ ARE COMMUTATIVE AND ASSOCIATIVE IN $\mathbb{R}$, AND $-, /$ ARE NOT, UNLESS YOU DEFINE THEM AS WE DID IN $\mathbb{Q}$.

INDUCTION

RECALL THE INDUCTION PRINCIPLE: IF $\operatorname{dom} p = \mathbb{N}$ SUCH THAT

a) $p(1)$ IS TRUE, AND

b) $p(k)$ TRUE $\Rightarrow p(k+1)$ TRUE,

THEN $p(n)$ IS TRUE $\forall n \in \mathbb{N}$.

EXERCISE: PROVE THE INDUCTION PRINCIPLE. (HINT: BY CONTRADICTION)

EX:

1) PROVE THAT $1+2+\dots+n = \dfrac{n(n+1)}{2}$ FOR ALL $n \in \mathbb{N}$.

2) PROVE THAT $n^3 > 2n-2 \ \forall n \in \mathbb{N}$.

3) PROVE THAT $(n+1)! \geq 2^n \ \forall n \in \mathbb{N}$.

4) PROVE THAT $6 \mid (3n^2+3n) \ \forall n \in \mathbb{N}$. ($a \mid b$: "a DIVIDES b")

SIGMA NOTATION

WE USE CAPITAL SIGMA Σ TO SHORTEN NOTATION OF LONG SUMS:

$$\sum_{i=1}^{k} a_i = a_1 + a_2 + a_3 + \dots + a_k.$$

1) a) $1 = \frac{1(1+1)}{2}$

b) SUPPOSE $1+2+\dots+k = \frac{k(k+1)}{2}$, PROVE THAT $1+2+\dots+(k+1) = \frac{(k+1)(k+2)}{2}$

$$
\begin{aligned}
1+2+\dots+(k+1) &= (1+2+\dots+k)+k+1 \\
&= \frac{k(k+1)}{2} + k+1 \quad \text{(BY THE SUPPOSITION)} \\
&= \frac{k^2+k}{2} + \frac{2k+2}{2} \\
&= \frac{k^2+3k+2}{2} = \frac{(k+1)(k+2)}{2}
\end{aligned}
$$

$\therefore 1+2+\dots+n = \frac{n(n+1)}{2} \ \forall n \in \mathbb{N}.$ $\square$

2) a) $1^3 > 2(1)-2 \Leftrightarrow 1 > 0$

b) SUPPOSE $k^3 > 2k-2$, PROVE THAT $(k+1)^3 > 2(k+1)-2$.

$$
\begin{aligned}
(k+1)^3 &= k^3+3k^2+3k+1 \\
&> (2k-2)+3k^2+3k+1 \quad \text{(BY THE SUPPOSITION)} \\
&= 3k^2+5k-1
\end{aligned}
$$

$$
\begin{aligned}
(k+1)^3 > 2(k+1)-2 &\Leftrightarrow 3k^2+5k-1 > 2k \\
&\Leftrightarrow 3k^2+3k-1 > 0 \\
&\Leftrightarrow 3k(k+1) > 1 \\
&\Leftrightarrow k(k+1) > \frac{1}{3}
\end{aligned}
$$

$\therefore n^3 > 2n-2 \ \forall n \in \mathbb{N}.$ $\square$

3) a) $(1+1)! \geq 2^1 \Leftrightarrow 2 \geq 2$ ✓

b) SUPPOSE $(k+1)! \geq 2^k$, PROVE THAT $(k+2)! \geq 2^{k+1}$

$$(k+2)! = (k+1)!(k+2)$$
$$\geq 2^k(k+2) \quad \text{(BY THE SUPPOSITION)}$$
$$= k2^k + 2^{k+1}$$
$$> 2^{k+1}$$ ✓

$\therefore (n+1)! \geq 2^n \ \forall n \in \mathbb{N}$ $\square$

4) a) $6 \mid (3 \cdot 1^2 + 3 \cdot 1) \Leftrightarrow 6 \mid 6$ ✓

b) SUPPOSE $6 \mid (3k^2+3k)$, PROVE THAT $6 \mid [3(k+1)^2+3(k+1)]$.

$$3(k+1)^2+3(k+1) = 3(k^2+2k+1)+3k+3 = (3k^2+3k)+6k+6$$
$$= 6\left(\frac{3k^2+3k}{6}+k+1\right)$$
$$= 6m \text{ FOR SOME } m \in \mathbb{N}.$$
$$\therefore 6 \mid [3(k+1)^2+3(k+1)].$$ ✓

$\therefore 6 \mid (3n^2+3n) \ \forall n \in \mathbb{N}.$ $\square$

376

EX: EXPAND. a) $\sum_{i=2}^{5} 2i^2$ b) $\sum_{j=1}^{10} 2$

EX: SIMPLIFY. a) $1+3+5+\dots+13$ b) $1+4+9+\dots+m^2$

BY THE LAWS OF ADDITION, WE HAVE THE FOLLOWING PROPERTIES.

1) $\sum_{i=m}^{n} (a_i + b_i) = \sum_{i=m}^{n} a_i + \sum_{i=m}^{n} b_i$

2) $\sum_{i=m}^{n} k a_i = k \sum_{i=m}^{n} a_i$

GENERALIZED MATHEMATICAL INDUCTION

LET $p(n)$ BE DEFINED FOR ALL $n \in \mathbb{N}$, AND LET $a \in \mathbb{N}$. IF

a) $p(a)$ IS TRUE, AND

b) FOR ALL $k \in \mathbb{N}, k \geq a$, $p(k)$ TRUE $\Rightarrow p(k+1)$ TRUE,

THEN $p(n)$ IS TRUE FOR ALL $n \in \mathbb{N} \ni n \geq a$.

EX: [redacted] IS $2^n > 2n+1 \ \forall n \in \mathbb{N}$?

$2^1 > 2(1)+1 \Leftrightarrow 2 > 3$. NO.

PROVE THAT $2^n > 2n+1 \ \forall n \geq 3$.

a) $2^3 > 2(3)+1 \Leftrightarrow 8 > 7$. ✓

b) SUPPOSE $2^k > 2k+1, k \geq 3$. PROVE THAT $2^{k+1} > 2(k+1)+1$.

$$2^{k+1} = 2 \cdot 2^k > 2(2k+1) = 4k+2$$

$$4k+2 > 2(k+1)+1 \iff 4k+2 > 2k+3$$
$$\iff 2k > 1 \quad \checkmark$$

$\therefore 2^n > 2n+1 \ \forall n \geq 3.$ $\square$

Ex : PROVE THAT $\displaystyle\sum_{i=1}^{n-1} \frac{i}{i+1} < \frac{n^2}{n+1} \ \forall n \geq 2.$

a) $\displaystyle\sum_{i=1}^{2-1} \frac{i}{i+1} < \frac{n^2}{n+1} \iff \frac{1}{1+1} < \frac{2^2}{2+1} \iff \frac{1}{2} < \frac{4}{3} \quad \checkmark$

b) SUPPOSE $\displaystyle\sum_{i=1}^{k-1} \frac{i}{i+1} < \frac{k^2}{k+1}$. PROVE $\displaystyle\sum_{i=1}^{k} \frac{i}{i+1} < \frac{(k+1)^2}{k+2}$.

$$\sum_{i=1}^{k} \frac{i}{i+1} = \sum_{i=1}^{k-1} \frac{i}{i+1} + \frac{k}{k+1}$$
$$< \frac{k^2}{k+1} + \frac{k}{k+1} = \frac{k(k+1)}{k+1} = k = \frac{k(k+2)}{k+2} = \frac{k^2+2k}{k+2}$$
$$< \frac{k^2+2k+1}{k+2} = \frac{(k+1)^2}{k+2} \quad \checkmark$$

$\therefore \displaystyle\sum_{i=1}^{n-1} \frac{i}{i+1} < \frac{n^2}{n+1} \ \forall n \geq 2.$

RECURSIVE SEQUENCES

A SEQUENCE OF NUMBERS $a_1, a_2, a_3, \ldots$ IS DEFINED RECURSIVELY IF EACH a_n FOR $n \geq n_0$ IS DEFINED IN TERMS OF SOME OR ALL OF $a_1, a_2, \ldots, a_{n_0}$.

EX: LET $a_1 = 2$, $a_2 = 4$, $a_n = 5a_{n-1} - 6a_{n-2}$ $\forall n \geq 3$. FIND a_3 AND a_4.

EX: THE FIBONACCI NUMBERS ARE THE NUMBERS IN THE FAMOUS SEQUENCE 1, 1, 2, 3, 5, 8, 13, ...

THIS SEQUENCE IS DEFINED BY

$$f_1 = f_2 = 1, \ f_n = f_{n-2} + f_{n-1} \ \forall n \geq 3.$$

CAN WE SHOW THAT $f_n < 2^n \ \forall n \in \mathbb{N}$?

STRONG MATHEMATICAL INDUCTION

LET $p(n)$ BE DEFINED FOR ALL $n \in \mathbb{N}$, LET $a \in \mathbb{N}$. IF

a) $p(1), p(2), \ldots, p(a)$ ARE TRUE, AND

b) FOR ALL $k \in \mathbb{N}$, $k \geq a$, $p(k)$ TRUE $\Rightarrow p(k+1)$ TRUE,

THEN $p(n)$ IS TRUE FOR ALL $n \in \mathbb{N}$.

EX: FOR THE FIBONACCI SEQUENCE $f_1 = f_2 = 1$, $f_n = f_{n-2} + f_{n-1}$ $\forall n \geq 3$, PROVE THAT $f_n < 2^n \ \forall n \in \mathbb{N}$.

a) $f_1 = 1 < 2^1 = 2$ ✓

$f_2 = 1 < 2^2 = 4$ ✓

$f_3 = 2 < 2^3 = 8$ ✓

b) SUPPOSE FOR $k \geq 3$, $f_1 < 2^1, f_2 < 2^2, \ldots, f_k < 2^k$. PROVE $f_{k+1} < 2^{k+1}$.

$$f_{k+1} = f_{k-1} + f_k < 2^{k-1} + 2^k < 2^k + 2^k = 2 \cdot 2^k = 2^{k+1}$$ ✓

$\therefore f_n < 2^n \ \forall n \in \mathbb{N}$. □

EX: LET $a_1 = 2$, $a_2 = 4$, $a_n = 5a_{n-1} - 6a_{n-2}$ $\forall n \geq 3$.

PROVE THAT $a_n = 2^n$ $\forall n \in \mathbb{N}$.

a) $a_1 = 2^1$, $a_2 = 2^2$, $a_3 = 5 \cdot 4 - 6 \cdot 2 = 8 = 2^3$. ✓

b) SUPPOSE FOR $k \geq 3$, $a_i = 2^i$ FOR $i = 1, 2, \ldots, k$. PROVE $a_{k+1} = 2^{k+1}$.

$$a_{k+1} = 5a_k - 6a_{k-1} = 5 \cdot 2^k - 6 \cdot 2^{k-1}$$
$$= 5 \cdot 2^k - 3 \cdot 2^k = 2 \cdot 2^k = 2^{k+1}$$ ✓

$\therefore a_n = 2^n$ $\forall n \in \mathbb{N}$. $\square$

NUMBER THEORY

LET $n, d \in \mathbb{Z}$, $d \neq 0$. WE SAY n IS DIVISIBLE BY d IF $n = dk$ FOR SOME $k \in \mathbb{Z}$. WE WRITE $d | n$ AND CALL d A DIVISOR OF n, AND n A MULTIPLE OF d. IF d DOES NOT DIVIDE n, WE WRITE $d \nmid n$.

TRANSITIVITY OF DIVISIBILITY: IF $a, b, c \in \mathbb{Z} \ni a | b$ AND $b | c$, THEN $a | c$.

PROOF: $a | b \Rightarrow \exists d \in \mathbb{Z} \ni b = ad$.

$b | c \Rightarrow \exists e \in \mathbb{Z} \ni c = be$.

$\Rightarrow c = be = (ad)e = a(de)$, $de \in \mathbb{Z}$.

$\therefore a | c$. $\square$

DIVISIBILITY BY PRIMES: EVERY $n \in \mathbb{N} \setminus \{1\}$ IS DIVISIBLE BY SOME PRIME NUMBER.

PROOF: (STRONG INDUCTION)

a) $2 \mid 2$ ✓

b) FOR $k > 2$, SUPPOSE EVERY INTEGER $m \ni 1 < m \leq k$ IS DIVISIBLE BY A PRIME. SHOW THAT $k+1$ IS DIVISIBLE BY A PRIME.

CASE 1: $k+1$ IS PRIME. THEN $(k+1) \mid (k+1)$.

CASE 2: $k+1$ IS COMPOSITE. THEN $k+1 = ab$ FOR SOME $a, b \in \mathbb{N} \setminus \{1\}$, $a, b < k+1$.

BY HYPOTHESIS, $\exists\, c$ PRIME $\ni c \mid a$. SINCE $c \mid a$ AND $a \mid (k+1)$, BY TRANSITIVITY $c \mid (k+1)$. ✓

$\therefore$ EVERY $n \in \mathbb{N} \setminus \{1\}$ IS DIVISIBLE BY A PRIME.

EX: FIND A PRIME FACTOR. a) 693 b) 1048.

THM: THERE ARE INFINITELY MANY PRIMES.

PROOF: (BY CONTRADICTION) SUPPOSE THERE ARE FINITELY MANY PRIMES, $p_1, p_2, \ldots, p_n$. CONSTRUCT A NUMBER p DEFINED BY

$$p = p_1 p_2 \cdots p_n + 1.$$

CLEARLY p IS LARGER THAN ALL THE PRIMES, SO p IS NOT EQUAL TO ANY OF THE PRIMES. HENCE p IS DIVISIBLE BY A PRIME. WITHOUT LOSS OF GENERALITY (WLOG), $p_1 \mid p$. BUT

$$\frac{p}{p_1} = \frac{p_1 p_2 \cdots p_n + 1}{p_1} = p_2 p_3 \cdots p_n + \frac{1}{p_1} \notin \mathbb{Z}, \text{ A CONTRADICTION.}$$

$\therefore$ THERE ARE INFINITELY MANY PRIMES. $\square$

QUOTIENT-REMAINDER THEOREM: IF $n \in \mathbb{Z}$ AND $d \in \mathbb{N}$,

THEN THERE EXIST UNIQUE $q, r \in \mathbb{Z}$ SUCH THAT

$$n = dq + r \text{ AND } 0 \le r < d.$$

EX: FIND $q, r \ni n = dq + r,\ 0 \le r < d$.

a) $n = 54,\ d = 4$

b) $n = -32,\ d = 7$

c) $n = 42,\ d = 70$

FUNDAMENTAL THEOREM OF ARITHMETIC

EVERY $a \in \mathbb{N} \setminus \{1\}$ CAN BE FACTORIZED UNIQUELY IN THE FORM

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

WHERE $k \in \mathbb{N}$, $\alpha_i \in \mathbb{N}\ \forall i$, AND p_i IS PRIME $\forall i$.

PROOF: THE PROOF REQUIRES THE FOLLOWING LEMMA:

EUCLID'S LEMMA: LET p BE PRIME, $a, b \in \mathbb{N}$. IF $p \mid ab$, THEN $p \mid a$ OR $p \mid b$.

FIRST, WE SHOW THAT EVERY $a \in \mathbb{N} \setminus \{1\}$ IS ~~EITHER~~ A PRIME OR A PRODUCT OF PRIMES, BY STRONG INDUCTION.

a) 2 IS PRIME. ✓

b) SUPPOSE $2, 3, \ldots, k$ ARE ALL EITHER PRIME OR PRODUCT OF PRIMES.

PROVE THAT $k+1$ IS EITHER PRIME OR PRODUCT OF PRIMES.