Ideas of mathematical proof

Slides Week 25

Euclid's theorem on infinity of primes. Proof strategies: pigeon-hole principle, by contrapositive, case-by-case. Converse statements. Pythagoras theorem and its converse. Mersenne and Fermat primes.

Example

Let $\mathscr{U} = \mathbb{Z}$.

Is $\forall x \, \forall y \, ((x - y = 0) \Rightarrow (x^2 = y^2))$ true or false?

For implication, we only need to verify $x^2 = y^2$ when the condition $x - y = 0$ is true (because implication is automatically true if the premise is false).

Here, $x - y = 0 \Rightarrow x = y \Rightarrow x^2 = y^2$, as required.

Example

Let $\mathscr{U} = \mathbb{R}$. Is $\forall x\, \exists y\, (x + y = 2x)$ true or false?

It is true: for any given x choose $y = x$.

Example

Let $\mathscr{U} = \mathbb{R}$. Is $\exists x\, \exists y\, ((xy = 1) \wedge (x + y = 0))$ true or false?

It is false: if $x + y = 0$, then xy is negative or 0.

Tautologies and contradictions with quantifiers

Definition

A statement with quantifiers

is a tautology if it is always true,

is a contradiction if it is always false.

Example

$(\forall x\,\forall y\; P(x,y)) \Rightarrow (\exists x\,\exists y\; P(x,y))$ is a tautology,

provided the universe of discourse is not empty.

Example

Is $((\exists x\, P(x)) \wedge (\exists x\, Q(x)) \Rightarrow \exists x\, (P(x) \wedge Q(x))$

a tautology or not?

We guess not: if there are – possibly different – elements making $P(x)$ true and $Q(x)$ true,

it does not always imply that there is an element

making $P(x)$ and $Q(x)$ true simultaneously (needed for R.H.S.).

But a concrete example is needed:

e.g. $\mathscr{U} = \mathbb{N}$, $P(x) = (x < 5)$, $Q(x) = (x > 8)$.

Proof "strategies"

"Direct" proofs.

Sometimes for proving a theorem $P \Rightarrow Q$

we derive Q from P directly

("directly" means not by contradiction or contraposition.)

Example

Prove that if k is even, then k^2 is even.

Indeed, $k = 2m$ for $m \in \mathbb{Z}$,

whence $k^2 = 4m^2 = 2 \cdot 2m^2$, divisible by 2, as req.

Proving $\forall x\, P(x)$

where $P(x)$ may be a compound statement.

Proof must be general, for all $x \in \mathscr{U}$;

just considering a few examples is not enough.

Example

Let $\mathscr{U} = \mathbb{N}$. Prove $\forall k\, (k^2 + k \text{ is even})$.

Proof: If k is even, then k^2 is even, the sum is even.

If k is odd, then k^2 odd, the sum odd+odd is even.

We considered all possible cases, checked for any k,

hence $\forall k\, (k^2 + k \text{ is even})$ is true.

Refuting $\forall x\, P(x)$

To show that $\forall x\, P(x)$ is false

(in other words: to disprove it, or refute it),

just one counterexample is enough.

Example

Show that $\forall k\, (k^2 + 1 \text{ is even})$ is false.

For example: for $k = 2$, $k^2 + 1 = 5$ is not even.

Agrees with negation rule: $\forall x\, P(x)$ is false

is the same as $\neg(\forall x\, P(x))$ is true, which is $\exists x\, \neg P(x)$.

Proving $\exists x\, P(x)$.

Producing one $x \in \mathscr{U}$ such that $P(x)$ is true is enough.

But to show that $\exists x\, P(x)$ is false, the argument must be general: $P(x)$ is false for all $x \in \mathscr{U}$.

Also agrees with negation rules: $\exists x\, P(x)$ is false

is the same as $\neg(\exists x\, P(x))$ is true,

equivalent to $\forall x \neg P(x)$.

So to show that $\exists x\, P(x)$ is false, we must show that $\neg P(x)$ is true for all $x \in \mathscr{U}$,

that is, $P(x)$ is false for all $x \in \mathscr{U}$.

Proof by contradiction.

Recall: any statement P is equivalent to $\neg P \Rightarrow F$

(where F is a contradiction — any statement that is always false).

Already seen examples of proof by contradiction:

- Cantor's theorem that $\mathbb{R}$ is uncountable.
- k^2 even $\Rightarrow$ k even.
- $\sqrt{2} \notin \mathbb{Q}$.

Example

Suppose that $k \in \mathbb{Z}$ is such that

k^3 is not divisible by 5.

Prove that then k is not divisible by 5.

Proof by contradiction.

Suppose the opposite: k is divisible by 5,

that is, $k = 5s$ for $s \in \mathbb{Z}$. Then

$k^3 = (5s)^3 = 5s \cdot 5s \cdot 5s = 5 \cdot (25s^3)$ is divisible by 5

— contradiction (with the given property).

Hence the assumption is false, so k is not divisible by 5.

Euclid's theorem on infinity of the set of primes

There are infinitely many prime numbers.

Proof by contradiction:

suppose the opposite (negation):
there are only finitely many primes.

Then we can list them all: $p_1, p_2, \ldots, p_n$.

Consider $m = p_1 \cdot p_2 \cdots p_n + 1$.

This number is not divisible by any of the primes p_i,

as it has remainder 1 after division by p_i.

(Even more rigorously: if m was divisible by p_i, then
$1 = m - p_1 \cdots p_n$ would also be divisible by p_i, so
$1 = p_i k$, a contradiction, as $1 < p_i \leq p_i k$.)

Infinitely many primes (cont'd)

Recall: opposite: all primes are $p_1, p_2, \ldots, p_n$;

$m = p_1 \cdot p_2 \cdots p_n + 1$ is not divisible by any p_i.

But by the prime factorization theorem
(which we proved by cumulative induction in week 1),

m $\underline{\text{is a product of primes}}$,

and all primes are these p_i by our assumption,

so m must be divisible by some p_j.

Contradiction: m both divisible by p_j, and not.

Thus, assumption of the opposite implies a contradiction,

hence theorem is true: there are infinitely many primes.$\square$

Pigeon-hole principle:

"One cannot put 5 pigeons in 4 cages
so that there be at most one pigeon in each cage."

Proof by contradiction: suppose the opposite, that it is possible.

Then there are at most $1 \times 4 = 4$ pigeons,

so $5 \leq 4$, a contradiction.

Hence the assumption is false, as required. $\square$

The nickname **pigeon-hole principle** indicates that this type of argument is being used (sometimes much less obvious, where 'cages' are to be invented).

Example

38 students had a test where they got marks ranging from 7 to 15. Prove that then there are at least 5 students with the same mark.

Proof. The marks $7, 8, \ldots, 15$ are 9 'cages'.

Suppose the opposite:

cannot find 5 students with the same mark,

so every cage 'contains' at most 4 students.

Then there are at most $4 \times 9 = 36$ students,

so $38 \leq 36$, a contradiction.

Hence the assumption is false, as required. $\square$

Example

Suppose that 11,000 points are chosen in a square 100×100 cm. Prove that one can **always** find 5 points that can be covered by a disc of radius 1.5 cm.

(This means, for **any** choice of 11,000 points....)

Proof (in two stages). Divide the square into $50 \times 50 = 2,500$ square boxes 2×2 cm.

Claim: some of these boxes contains at least 5 points.

Proof by contradiction:

if each box contains at most 4 points,

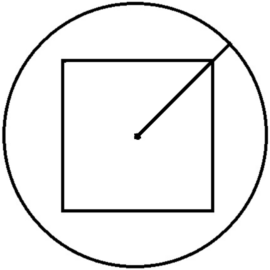
then there are at most $4 \times 2,500 = 10,000$ points,

so $11,000 \leq 10,000$, a contradiction.

Example (continued)

Recall: we proved that there is a 2×2 box containing 5 points.

This box 2×2 is covered by the disc of radius 1.5 cm centred at the centre of the box, since $\sqrt{2} < 1.5$:



Thus, there are 5 points covered by such a disc. $\square$

Remarks on pigeon-hole principle

1. In advanced mathematical books or papers, they would simply write:

"...By the pigeon-hole principle,
one of these 2×2 squares
contains at least 5 points..."

(without detailed proof by contradiction).

2. Often such questions are attempted by trying to consider "the worst case". But it is often quite difficult to justify that this is a worst case....

Proof by contraposition (= by contrapositive)

This is a variation of proof by contradiction applied to conditional implication.

Namely, $P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$.

Proof by truth table:

P	Q	$P \Rightarrow Q$	$\neg P$	$\neg Q$	$\neg Q \Rightarrow \neg P$
T	T				
T	F				
F	T				
F	F				

Proof by contraposition (= by contrapositive)

This is a variation of proof by contradiction applied to conditional implication.

Namely, $P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$.

Proof by truth table:

P	Q	$P \Rightarrow Q$	$\neg P$	$\neg Q$	$\neg Q \Rightarrow \neg P$
T	T	T			
T	F	F			
F	T	T			
F	F	T			

Proof by contraposition (= by contrapositive)

This is a variation of proof by contradiction applied to conditional implication.

Namely, $P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$.

Proof by truth table:

P	Q	$P \Rightarrow Q$	$\neg P$	$\neg Q$	$\neg Q \Rightarrow \neg P$
T	T	T	F		
T	F	F	F		
F	T	T	T		
F	F	T	T		

Proof by contraposition (= by contrapositive)

This is a variation of proof by contradiction applied to conditional implication.

Namely, $P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$.

Proof by truth table:

P	Q	$P \Rightarrow Q$	$\neg P$	$\neg Q$	$\neg Q \Rightarrow \neg P$
T	T	T	F	F	
T	F	F	F	T	
F	T	T	T	F	
F	F	T	T	T	

Proof by contraposition (= by contrapositive)

This is a variation of proof by contradiction applied to conditional implication.

Namely, $P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$.

Proof by truth table:

P	Q	$P \Rightarrow Q$	$\neg P$	$\neg Q$	$\neg Q \Rightarrow \neg P$
T	T	T	F	F	T
T	F	F	F	T	F
F	T	T	T	F	T
F	F	T	T	T	T

The corresponding columns are the same, as required.

Example

Let $\mathscr{U} = \mathbb{N}$.

If $P := (x^2 < 25)$, then $Q := (x < 5)$.

That is, $P \Rightarrow Q$.

We prove $\neg Q \Rightarrow \neg P$ instead, which is equivalent.

Indeed, if $\neg Q$ is true, $x \geq 5$,

then $x^2 \geq 25$, which means that $\neg P$ is true.

Thus, we proved $\neg Q \Rightarrow \neg P$, so $P \Rightarrow Q$ is true.

One of previous examples:

Example

Suppose that x^2 is odd. Prove that x is odd.

We proved $Q =$ "x is odd" by contradiction:

derived from $\neg Q$ that x^2 is even,

which was a contradiction with the condition "x^2 is odd".

The same as proving (x^2 is odd) $\Rightarrow$ (x is odd) by contrapositive:

we actually proved (x is even) $\Rightarrow$ (x^2 is even).

Implicit universal quantifiers

When we prove (x^2 is odd) $\Rightarrow$ (x is odd),

we actually mean that this is true for all $x \in \mathbb{N}$.

So this is in fact proving that

$\forall x \in \mathbb{N}$ (x^2 is odd) $\Rightarrow$ (x is odd) is true.

Similarly, in many other cases.

Example

$(x^2 > 4) \Rightarrow ((x < -2) \vee (x > 2))$

is actually $\forall x \in \mathbb{R}\ (x^2 > 4) \Rightarrow ((x < -2) \vee (x > 2))$.

Converse statements

Definition

For an implication $P \Rightarrow Q$,

its **converse** is $Q \Rightarrow P$.

In general, the converse is not equivalent to the original statement.

The same with universal quantifier:

$\forall x\,(P(x) \Rightarrow Q(x))$ has converse $\forall x\,(Q(x) \Rightarrow P(x))$.

Example

Let $\mathscr{U} = \mathbb{R}$.

Let $P(x) := (x > 3)$, and $Q(x) := (x^2 > 9)$.

Then $\forall x\,(P(x) \Rightarrow Q(x))$ is true.

But the converse $\forall x\,(Q(x) \Rightarrow P(x))$ is false:

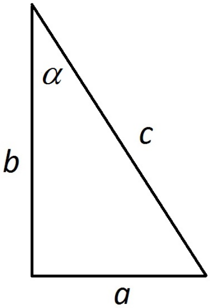
say, $(-4)^2 > 9$ is true but $-4 > 3$ is false.

When the converse is true, it is another theorem.

Pythagoras theorem

Pythagoras theorem

For any right triangle $\triangle ABC$ *with* $\angle C = 90^\circ$, *the lengths of sides* $AB = c$, $BC = a$, $AC = b$ *satisfy* $c^2 = a^2 + b^2$.



... Attempt: $a = c \cdot \sin\alpha$ and $b = c \cdot \cos\alpha$, where $\alpha = \angle BAC$, then "easily"

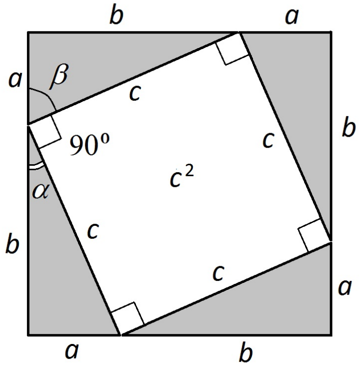
$$a^2 + b^2 = (c\sin\alpha)^2 + (c\cos\alpha)^2 = c^2(\sin^2\alpha + \cos^2\alpha)$$

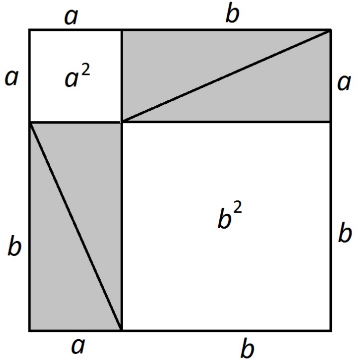
$$= c^2 \quad \text{because} \quad \sin^2\alpha + \cos^2\alpha = 1, \text{ "as is well known".}$$

But how do we know that $\sin^2\alpha + \cos^2\alpha = 1$?
from the Pythagoras theorem?
then this is not a good proof (a 'circle').

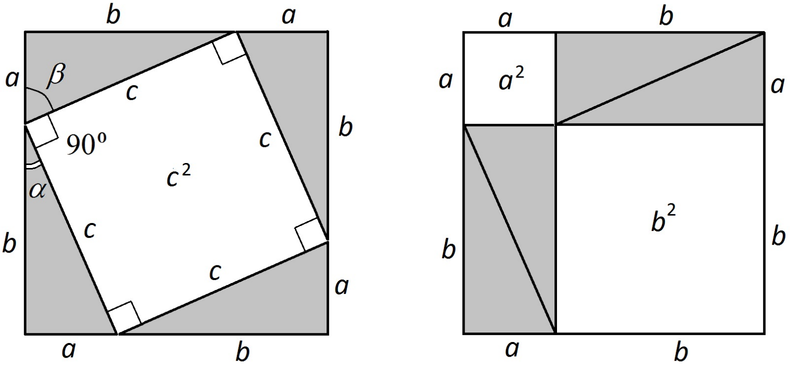
Proof of Pythagoras theorem.

Consider a square $(a+b) \times (a+b)$. First arrange four copies of the triangle as on the left picture. n





The sum of angles is 180°, so the sum of acute angles is $\alpha + \beta = 90°$. Hence the angles of the central quadrangle are all 90°. The sides are all c, so it is a square, area c^2.



Then arrange four copies of our triangle as on the right. Since the sum of acute angles is 90°, the two pairs of our triangle form two rectangles $a \times b$, and the remaining area $=$ two squares $a \times a$ and $b \times b$, with areas a^2 and b^2. Simply by the areas: $c^2 = a^2 + b^2$. $\square$

Converse of the Pythagoras theorem

Converse of the Pythagoras theorem

If in a triangle $\triangle ABC$

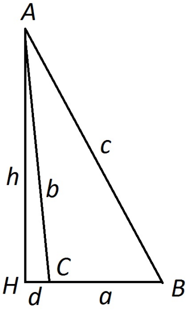
with side lengths $AB = c$, $BC = a$, $AC = b$,

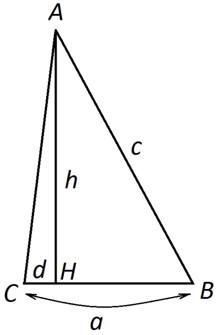
we have $c^2 = a^2 + b^2$, *then* $\angle C = 90^\circ$.

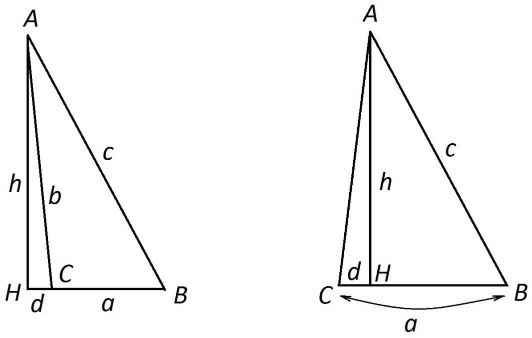
This is not the same as Pythagoras theorem! Has to be proved.

Proof of Converse Pythagoras theorem

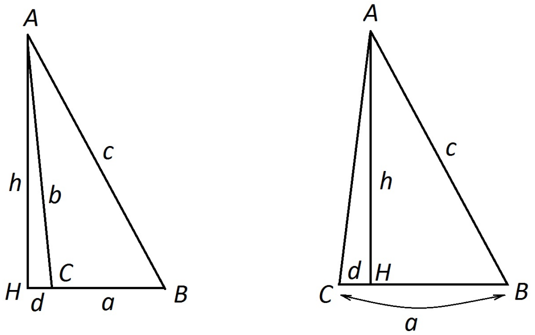
Proof by contradiction. Suppose the opposite: $\angle C \neq 90^\circ$. Then the perpendicular dropped from A to the side BC or its extension has base $H \neq C$. We have two cases: H is further from B than C, or closer to B than C.







If H is further from B than C, let $HC = d$. By the Pythagoras theorem applied to $\triangle AHC$ we have $b^2 = d^2 + h^2$, and by the Pythagoras theorem applied to $\triangle AHB$ we have $c^2 = (a + d)^2 + h^2 = a^2 + 2ad + d^2 + h^2$; substituting we obtain $c^2 = a^2 + 2ad + b^2$. But $c^2 = a^2 + b^2$ by hypothesis, so $0 = 2ad$, a contradiction.



If H is closer to B than C, let again $HC = d$. By the Pythagoras theorem applied to $\triangle AHC$ we have $b^2 = d^2 + h^2$, and by the Pythagoras theorem applied to $\triangle AHB$ we have $c^2 = (a-d)^2 + h^2 = a^2 - 2ad + d^2 + h^2$; substituting we obtain $c^2 = a^2 - 2ad + b^2$. But $c^2 = a^2 + b^2$ by hypothesis, so $0 = -2ad$, a contradiction.

Thus, we obtained a contradiction in all cases, which proves that the assumption that $\angle C \neq 90^\circ$ is false, so $\angle C = 90^\circ$, as req. $\square$

Recall:

Implication rule (proved earlier):

$A \Rightarrow B \equiv \neg A \vee B.$

Case-by-case proofs

If the premise of an implication splits into several cases, then simply prove the implication in each case.

Indeed, proving $P \Rightarrow Q$, where $P \equiv P_1 \vee P_2$:

$$\begin{aligned} P \Rightarrow Q &\equiv (P_1 \vee P_2) \Rightarrow Q \\ &\equiv \neg(P_1 \vee P_2) \vee Q \quad \text{implication rule} \\ &\equiv (\neg P_1 \wedge \neg P_2) \vee Q \quad \text{de Morgan law} \\ &\equiv (\neg P_1 \vee Q) \wedge (\neg P_2 \vee Q) \quad \text{distributivity} \\ &\equiv (P_1 \Rightarrow Q) \wedge (P_2 \Rightarrow Q) \quad \text{implication rule.} \end{aligned}$$

A similar calculation can be done if there are more than two cases: $P \equiv P_1 \vee P_2 \vee \cdots \vee P_k$.

Example

If $3 \nmid m \in \mathbb{N}$, then $3 \mid (m^2 - 1)$.

Possible remainders after division by 3 are 1 or 2.
Hence the condition $3 \nmid m$ splits into two cases:
$m = 3k + 1$ or $m = 3k + 2$.

Consider each case:

If $m = 3k + 1$, then $m^2 - 1 = (3k + 1)^2 - 1$
$= 9k^2 + 6k + 1 - 1 = 3(3k^2 + 2k)$ is divisible by 3.

If $m = 3k + 2$, then
$m^2-1 = (3k+2)^2-1 = 9k^2+12k+4-1 = 3(3k^2+4k+1)$
is divisible by 3.

All is proved: we considered all cases. $\square$

Proving $P \Leftrightarrow Q$

Proving $P \Leftrightarrow Q$ means proving both $P \Rightarrow Q$ and $Q \Rightarrow P$ (recall: converse is not always true, proving just one direction does not prove the other!).

This is often read: "P is a necessary and sufficient condition for Q"

or, which is the same: "Q is a necessary and sufficient condition for P",

or: "P holds if and only if Q holds".

Example (Pythagoras)

Since we proved in both directions, we do have

$$\angle C = 90^\circ \ \Leftrightarrow \ a^2 + b^2 = c^2 \ \text{ in } \triangle ABC.$$

Example

Prove that $|x+1| = |x| + 1 \Leftrightarrow x \geq 0$.

"$\Leftarrow$": easy:

for $x \geq 0$ also $x + 1 \geq 0$,

so on the left $|x+1| = x + 1$, and $|x| = x$,

so the equation is $x + 1 = x + 1$, true.

Example (continued)

Prove that $|x+1| = |x| + 1 \Leftrightarrow x \geq 0$.

"$\Rightarrow$": by contradiction:

suppose $x < 0$, two cases: $x \leq -1$ and $-1 \leq x < 0$.

If $x \leq -1$, then the equation is $-x - 1 = -x + 1$,

$-1 = 1$, a contradiction.

If $-1 \leq x < 0$, then the equation is $x + 1 = -x + 1$,

$x = 0$, a contradiction as $x < 0$ in this case.

Thus a contradiction in all cases, which means that the assumption $x < 0$ is false, so $x \geq 0$, as req. $\square$

Mersenne primes

An example of proof by contrapositive.

Example

If $2^n - 1$ is a prime for $n \in \mathbb{N}$, then n is a prime.

Remark: This type of primes are called Mersenne primes. It is still an open problem whether there are infinitely many such primes!

Useful formula (geometric series)

Use the well-known formula

$$a^u - 1 = (a-1)(a^{u-1} + a^{u-2} + \cdots + a + 1)$$

simply proved by expanding brackets on the right;

also known from the sum of geometric series:

$$1 + a + \cdots + a^{u-2} + a^{u-1} = \frac{a^u - 1}{a - 1}.$$

Mersenne primes continued

...Proving: $2^n - 1$ is a prime $\Rightarrow$ n is a prime.

Proof by contrapositive: assume n is not a prime and derive that then $2^n - 1$ is not a prime.

Not a prime: $n = st$ for $s, t \in \mathbb{N}$ with $s > 1$ and $t > 1$. Then

$$\begin{aligned} 2^n - 1 &= 2^{st} - 1 \\ &= (2^s)^t - 1 \\ &= (2^s - 1)(2^{s(t-1)} + 2^{s(t-2)} + \cdots + 2^s + 1). \end{aligned}$$

On the right both factors are > 1, since $s > 1$ and $t > 1$, so $2^n - 1$ is not a prime, as required.

Thus, we proved $2^n - 1$ is a prime $\Rightarrow$ n is a prime. $\square$

Fermat primes

Example

If $2^n + 1$ is a prime for $n \in \mathbb{N}$,

then $n = 2^k$ for $k \in \mathbb{N}$.

Remark. This type of primes are called Fermat primes. It is still an open problem whether there are infinitely many such primes!

Another formula (works only for odd powers):

$$a^{2u+1}+1 = (a+1)(a^{2u}-a^{2u-1}+a^{2u-2}-\cdots(-1)^k a^{2u-k}\pm\cdots),$$

simply proved by expanding brackets on the right.

Useful formula for odd powers

$$a^{2u+1}+1 = (a+1)(a^{2u}-a^{2u-1}+a^{2u-2}-\cdots(-1)^k a^{2u-k}\pm\cdots),$$

expanding brackets on the right:

$$\begin{aligned}(a+1)(a^{2u} - a^{2u-1} + a^{2u-2} \cdots\cdots) \\ &= a^{2u+1} - a^{2u} + a^{2u-1} - a^{2u-2} \cdots\cdots \\ &\qquad + a^{2u} - a^{2u-1} + a^{2u-2} - \cdots\cdots + 1 \\ &= a^{2u+1} + 0 + 0 \cdots + 1\end{aligned}$$

Fermat primes continued

... Proving $2^n + 1$ is a prime $\Rightarrow n = 2^k$.

Proof by contrapositive: assume that

$n \neq 2^k$ and derive that then $2^n + 1$ is not a prime.

By assumption, n is divisible by some odd integer > 1,

so that $n = s(2t + 1)$ for $s, t \in \mathbb{N}$ and $t > 0$.

$$\begin{aligned} \text{Then } 2^n + 1 &= 2^{s(2t+1)} + 1 \\ &= (2^s)^{2t+1} + 1 \\ &= (2^s + 1)(2^{s(2t)} - 2^{s(2t-1)} + \cdots). \end{aligned}$$

On the right both factors are > 1, since $t > 0$, so $2^n + 1$ is not a prime, as required. $\square$

Recap of "Elements of Mathematical Logic"

Logical statements: operations (connectives), logical laws, logical equivalence, truth tables, tautology, contradiction, implication, converse.

Predicate calculus: quantifiers, negation rules with quantifiers, translation of natural language sentences into logical expressions.

Proof strategies: proof by contradiction, by contraposition, case-by-case proofs, examples of proofs by contradiction ($\sqrt{2} \notin \mathbb{Q}$, infinity of the set of primes).