Rigour and Metamathematics.

As we have seen the methods of calculus led to some difficulties of foundational nature.

As we have seen the methods of calculus led to some difficulties of foundational nature.

1. How do you define the derivative?

As we have seen the methods of calculus led to some difficulties of foundational nature.

1. How do you define the derivative?

2. How can we know when the minimum value of a function is attained at some point? (Compare Gauss' first proof of the fundamental theorem of algebra.)

As we have seen the methods of calculus led to some difficulties of foundational nature.

1. How do you define the derivative?

2. How can we know when the minimum value of a function is attained at some point? (Compare Gauss' first proof of the fundamental theorem of algebra.)

3. If a continuous function is such that $f(0) = 0$ and $f(1) = 1$, is there necessarily a point x in $(0, 1)$ where $f(x) = 1/2$?

As we have seen the methods of calculus led to some difficulties of foundational nature.

1. How do you define the derivative?

2. How can we know when the minimum value of a function is attained at some point? (Compare Gauss' first proof of the fundamental theorem of algebra.)

3. If a continuous function is such that $f(0) = 0$ and $f(1) = 1$, is there necessarily a point x in $(0, 1)$ where $f(x) = 1/2$?

4. Exactly what is a real number?

As we have seen the methods of calculus led to some difficulties of foundational nature.

1. How do you define the derivative?

2. How can we know when the minimum value of a function is attained at some point? (Compare Gauss' first proof of the fundamental theorem of algebra.)

3. If a continuous function is such that $f(0) = 0$ and $f(1) = 1$, is there necessarily a point x in $(0, 1)$ where $f(x) = 1/2$?

4. Exactly what is a real number?

These questions were not studied systematically until the 19:th century, with the works of Cauchy, Weierstrass, Dedekind, Cantor and others. Strangely enough it seems that the last question was attacked somewhat later than the two first.

As we have seen the methods of calculus led to some difficulties of foundational nature.

1. How do you define the derivative?

2. How can we know when the minimum value of a function is attained at some point? (Compare Gauss' first proof of the fundamental theorem of algebra.)

3. If a continuous function is such that $f(0) = 0$ and $f(1) = 1$, is there necessarily a point x in $(0, 1)$ where $f(x) = 1/2$?

4. Exactly what is a real number?

These questions were not studied systematically until the 19:th century, with the works of Cauchy, Weierstrass, Dedekind, Cantor and others. Strangely enough it seems that the last question was attacked somewhat later than the two first. Here we will discuss it first, but only briefly.

We take as our starting point the number system of integers, which we consider given (by God, according to Kronecker). From there, it is no great problem to arrive at the system (field) of rational numbers, all ratios of integers.

We take as our starting point the number system of integers, which we consider given (by God, according to Kronecker). From there, it is no great problem to arrive at the system (field) of rational numbers, all ratios of integers. It was known already to the Pythagorean school that there ‘are’ numbers that can not be rational, like the length of the diagonal in a unit square. Here, (real) numbers were thought of in an intuitive way, as corresponding to points on a line, but no formal definition was given, and as we saw this had to wait until almost our time.

We take as our starting point the number system of integers, which we consider given (by God, according to Kronecker). From there, it is no great problem to arrive at the system (field) of rational numbers, all ratios of integers. It was known already to the Pythagorean school that there 'are' numbers that can not be rational, like the length of the diagonal in a unit square. Here, (real) numbers were thought of in an intuitive way, as corresponding to points on a line, but no formal definition was given, and as we saw this had to wait until almost our time.

Why is it important to have a formal definition?

We take as our starting point the number system of integers, which we consider given (by God, according to Kronecker). From there, it is no great problem to arrive at the system (field) of rational numbers, all ratios of integers. It was known already to the Pythagorean school that there 'are' numbers that can not be rational, like the length of the diagonal in a unit square. Here, (real) numbers were thought of in an intuitive way, as corresponding to points on a line, but no formal definition was given, and as we saw this had to wait until almost our time.

Why is it important to have a formal definition? You need it in order to *prove* statements about the reals.

There are (at least) two ways of constructing the reals from the rational numbers. The first is the method of *Cauchy sequences*, which probably is a formalization of the idea of a decimal expansion.

There are (at least) two ways of constructing the reals from the rational numbers. The first is the method of *Cauchy sequences*, which probably is a formalization of the idea of a decimal expansion. It is clear by long division that any rational number can be written in terms of a decimal expansion. One observes that

1. A rational number has a finite decimal expansion if and only if its denominator is a product of 2:s and 5:s. (Exercise 1!)

There are (at least) two ways of constructing the reals from the rational numbers. The first is the method of *Cauchy sequences*, which probably is a formalization of the idea of a decimal expansion. It is clear by long division that any rational number can be written in terms of a decimal expansion. One observes that

1. A rational number has a finite decimal expansion if and only if its denominator is a product of 2:s and 5:s. (Exercise 1!)

2. A decimal expansion is the expansion of a rational number if and only if it is periodic from a certain point on. (Exercise 2!)

There are (at least) two ways of constructing the reals from the rational numbers. The first is the method of *Cauchy sequences*, which probably is a formalization of the idea of a decimal expansion. It is clear by long division that any rational number can be written in terms of a decimal expansion. One observes that

1. A rational number has a finite decimal expansion if and only if its denominator is a product of 2:s and 5:s. (Exercise 1!)

2. A decimal expansion is the expansion of a rational number if and only if it is periodic from a certain point on. (Exercise 2!)

From here, the step is not long to define a real number as an *arbitrary* decimal expansion.

There are (at least) two ways of constructing the reals from the rational numbers. The first is the method of *Cauchy sequences*, which probably is a formalization of the idea of a decimal expansion. It is clear by long division that any rational number can be written in terms of a decimal expansion. One observes that

1. A rational number has a finite decimal expansion if and only if its denominator is a product of 2:s and 5:s. (Exercise 1!)

2. A decimal expansion is the expansion of a rational number if and only if it is periodic from a certain point on. (Exercise 2!)

From here, the step is not long to define a real number as an *arbitrary* decimal expansion. In principle, this is fine, but it is too tied to the decimal system and awkward for abstract mathematics. (If we choose binary representation, do we get the same numbers?)

Instead we take as our definition that the real numbers are all limits of all convergent sequences of rational numbers.

Instead we take as our definition that the real numbers are all limits of all convergent sequences of rational numbers. But how can we define convergent sequence if we have not defined what it converges to?

Instead we take as our definition that the real numbers are all limits of all convergent sequences of rational numbers. But how can we define convergent sequence if we have not defined what it converges to? This is where the idea of a Cauchy seuence comes in: A sequence x_n is a Cauchy sequence if

$$\lim_{n,m \to \infty} |x_n - x_m| = 0.$$

Instead we take as our definition that the real numbers are all limits of all convergent sequences of rational numbers. But how can we define convergent sequence if we have not defined what it converges to? This is where the idea of a Cauchy seuence comes in: A sequence x_n is a Cauchy sequence if

$$\lim_{n,m\to\infty} |x_n - x_m| = 0.$$

Given the real numbers, one can prove that any Cauchy sequence is convergent. Then, conversely, one defines a real number as an equivalence class of Cauchy sequences: $x_n \sim y_n$ if $|x_n - y_n| \to 0$.

Instead we take as our definition that the real numbers are all limits of all convergent sequences of rational numbers. But how can we define convergent sequence if we have not defined what it converges to? This is where the idea of a Cauchy seuence comes in: A sequence x_n is a Cauchy sequence if

$$\lim_{n,m\to\infty} |x_n - x_m| = 0.$$

Given the real numbers, one can prove that any Cauchy sequence is convergent. Then, conversely, one defines a real number as an equivalence class of Cauchy sequences: $x_n \sim y_n$ if $|x_n - y_n| \to 0$.

The other way to define the real numbers is by the *Dedekind cut*. (Not to be confused with the Hip-hop artist 'Dedekind cut'.) This corresponds to another way of approximating real numbers by rationals.

By definition, a Dedekind cut is a partition of the set of rational numbers into two subsets A and$B$, such that ($A \cup B = \mathbb{Q}$) and any element a in A is smaller that any element b in B. A Dedekind cut corresponds to the real number $x = \sup A = \inf B$, so we can define the set of real numbers as the set of Dedekind cuts.

By definition, a Dedekind cut is a partition of the set of rational numbers into two subsets A and$B$, such that ($A \cup B = \mathbb{Q}$) and any element a in A is smaller that any element b in B. A Dedekind cut corresponds to the real number $x = \sup A = \inf B$, so we can define the set of real numbers as the set of Dedekind cuts.

After this, when we have the definition of the real numbers firmly established, one can go on and prove things like

1. A continuous function on a closed bounded set attains its maximum and minimum values.

2. The intermediate value theorem.

By definition, a Dedekind cut is a partition of the set of rational numbers into two subsets A and$B$, such that ($A \cup B = \mathbb{Q}$) and any element a in A is smaller that any element b in B. A Dedekind cut corresponds to the real number $x = \sup A = \inf B$, so we can define the set of real numbers as the set of Dedekind cuts.

After this, when we have the definition of the real numbers firmly established, one can go on and prove things like

1. A continuous function on a closed bounded set attains its maximum and minimum values.

2. The intermediate value theorem.

And, the stage is also set for a precise notion of limits and derivatives.

Interlude: other sorts of numbers.

We have discussed rational numbers and real numbers, but even prior to that people had been discussing intermediate classes of numbers, like algebraic numbers (and transcendental numbers). By definition, a number is *algebraic* if it solves some equation

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots . a_0 = 0,$$

where a_j are rational – or integers, which amounts to the same thing.

Interlude: other sorts of numbers.

We have discussed rational numbers and real numbers, but even prior to that people had been discussing intermediate classes of numbers, like algebraic numbers (and transcendental numbers). By definition, a number is *algebraic* if it solves some equation

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots . a_0 = 0,$$

where a_j are rational – or integers, which amounts to the same thing. It is *transcendental* if it is not algebraic. Clearly, all rational numbers are algebraic (they solve $x - a_0 = 0$) and of course $\sqrt{2}$ is an example of a non rational algebraic number. The numbers π and e are examples of transcendental numbers.

Interlude: other sorts of numbers.

We have discussed rational numbers and real numbers, but even prior to that people had been discussing intermediate classes of numbers, like algebraic numbers (and transcendental numbers). By definition, a number is *algebraic* if it solves some equation

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + ...a_0 = 0,$$

where a_j are rational – or integers, which amounts to the same thing. It is *transcendental* if it is not algebraic. Clearly, all rational numbers are algebraic (they solve $x - a_0 = 0$) and of course $\sqrt{2}$ is an example of a non rational algebraic number. The numbers π and e are examples of transcendental numbers.

How does one prove that a number is not *algebraic*?

This is in general a very difficult thing – e g it is far from easy to prove that π and e are not algebraic.

This is in general a very difficult thing – e g it is far from easy to prove that π and e are not algebraic. But, here is a relatively easy criterion, due to Liouville:

This is in general a very difficult thing – e g it is far from easy to prove that π and e are not algebraic. But, here is a relatively easy criterion, due to Liouville:

Assume that a is algebraic but not rational and let p/q be a rational number. How close can p/q be to a?

This is in general a very difficult thing – e g it is far from easy to prove that π and e are not algebraic. But, here is a relatively easy criterion, due to Liouville:

Assume that a is algebraic but not rational and let p/q be a rational number. How close can p/q be to a? We have $P(a) = 0$, where P is a polynomial with integer coefficients and

$$|P(p/q)q^n| \geq 1, \quad |P(p/q)| \geq q^{-n},$$

since it is an integer which is not zero if p/q is close to a.

This is in general a very difficult thing – e g it is far from easy to prove that π and e are not algebraic. But, here is a relatively easy criterion, due to Liouville:

Assume that a is algebraic but not rational and let p/q be a rational number. How close can p/q be to a? We have $P(a) = 0$, where P is a polynomial with integer coefficients and

$$|P(p/q)q^n| \geq 1, \quad |P(p/q)| \geq q^{-n},$$

since it is an integer which is not zero if p/q is close to a. But

$$|P(p/q)| = |P(a) - P(p/q)| \leq \max_{[a,p/q]} |P'||a - p/q|.$$

This is in general a very difficult thing – e g it is far from easy to prove that π and e are not algebraic. But, here is a relatively easy criterion, due to Liouville:

Assume that a is algebraic but not rational and let p/q be a rational number. How close can p/q be to a? We have $P(a) = 0$, where P is a polynomial with integer coefficients and

$$|P(p/q)q^n| \geq 1, \quad |P(p/q)| \geq q^{-n},$$

since it is an integer which is not zero if p/q is close to a. But

$$|P(p/q)| = |P(a) - P(p/q)| \leq \max_{[a,p/q]} |P'||a - p/q|.$$

Hence,

$$|a - p/q| \geq Cq^{-n};$$

we can not approximate a very well with rationals.

This is in general a very difficult thing – e g it is far from easy to prove that π and e are not algebraic. But, here is a relatively easy criterion, due to Liouville:

Assume that a is algebraic but not rational and let p/q be a rational number. How close can p/q be to a? We have $P(a) = 0$, where P is a polynomial with integer coefficients and

$$|P(p/q)q^n| \geq 1, \quad |P(p/q)| \geq q^{-n},$$

since it is an integer which is not zero if p/q is close to a. But

$$|P(p/q)| = |P(a) - P(p/q)| \leq \max_{[a,p/q]} |P'||a - p/q|.$$

Hence,

$$|a - p/q| \geq Cq^{-n};$$

we can not approximate a very well with rationals.

This way we can construct many numbers that are not algebraic, by taking non rational numbers that *can* be very well approximated by rationals. (Try!)

Metamathematics

After the successful clarification of the foundations of analysis, it became natural to ask similar questions about other parts of mathematics. From this emerged the desire to construct 'all mathematics' as a formal system, based only on logic and a few other clearly stated axioms. In fact, in 'Principia Mathematica' by Russel and Whitehead, the goal was to construct mathematics from logic only. One pioneer in this work was Gottlob Frege, and his 'Begriffsschrift' from 1879, was a main influence in the subsequent developments.

Metamathematics

After the successful clarification of the foundations of analysis, it became natural to ask similar questions about other parts of mathematics. From this emerged the desire to construct ‘all mathematics’ as a formal system, based only on logic and a few other clearly stated axioms. In fact, in ‘Principia Mathematica’ by Russel and Whitehead, the goal was to construct mathematics from logic only. One pioneer in this work was Gottlob Frege, and his ‘Begriffsschrift’ from 1879, was a main influence in the subsequent developments.

One motivation for this was to ensure that mathematical reasoning was really correct, or more precsiely that the system was *consistent*. This means that it is impossible to derive a contradiction from it, something which is generally formulated as the impossibility to prove that $0 = 1$. The idea was that once it was made precise what a legitimate mathematical argument is, it would be impossible to make mistakes. Ideally one should even be able to *prove* that the system is consistent.

A further question along the same lines is: Is it possible to find a mechanical procedure that given a mathematical statement written in formal language, decides if it holds or not.

A further question along the same lines is: Is it possible to find a mechanical procedure that given a mathematical statement written in formal language, decides if it holds or not. A main theme in the work on these questions, which ultimately lead to mainly negative answers, goes back to the *Liar's paradox*:

1. A person says 'I am lying'. Is the statement true or not?

A further question along the same lines is: Is it possible to find a mechanical procedure that given a mathematical statement written in formal language, decides if it holds or not. A main theme in the work on these questions, which ultimately lead to mainly negative answers, goes back to the *Liar's paradox*:

1. A person says ‘I am lying’. Is the statement true or not?

The first reference to the liar's paradox in mathematics is perhaps from Cantor's theory of (infinite) *Cardinal numbers*. Two sets are said to have the same cardinality if there is a bijection between them.

A further question along the same lines is: Is it possible to find a mechanical procedure that given a mathematical statement written in formal language, decides if it holds or not. A main theme in the work on these questions, which ultimately lead to mainly negative answers, goes back to the *Liar's paradox*:

1. A person says 'I am lying'. Is the statement true or not?

The first reference to the liar's paradox in mathematics is perhaps from Cantor's theory of (infinite) *Cardinal numbers*. Two sets are said to have the same cardinality if there is a bijection between them. Looking first at finite sets, it is clear that e g all sets of five elements have the same cardinality, and we can use this idea to define the number 'five'. Cantor's idea was to apply the same principle to any sets.

A further question along the same lines is: Is it possible to find a mechanical procedure that given a mathematical statement written in formal language, decides if it holds or not. A main theme in the work on these questions, which ultimately lead to mainly negative answers, goes back to the *Liar's paradox*:

1. A person says 'I am lying'. Is the statement true or not?

The first reference to the liar's paradox in mathematics is perhaps from Cantor's theory of (infinite) *Cardinal numbers*. Two sets are said to have the same cardinality if there is a bijection between them. Looking first at finite sets, it is clear that e g all sets of five elements have the same cardinality, and we can use this idea to define the number 'five'. Cantor's idea was to apply the same principle to any sets. Do the sets of rational numbers and of real numbers have the same cardinality? No, the set of rational numbers is smaller (there exists an injective map from the rationals to the reals, but not a bijection).

We recall first the simple proof that the rationals have the same cardinality as the natural numbers, i e the set of rational numbers is *countable*: We can list them in an infinite sequence $\{r_n\}$.

We recall first the simple proof that the rationals have the same cardinality as the natural numbers, i e the set of rational numbers is *countable*: We can list them in an infinite sequence $\{r_n\}$. It is clearly enough to do this for the positive rational numbers (why?). Since any positive rational number can be written $r = p/q$ where p, q are natural numbers we can partition $Q = \cup A_n$ where A_n is the finite set of rationals with $p + q = n$. This way we can list them by first listing A_2, then A_3 etc.

We recall first the simple proof that the rationals have the same cardinality as the natural numbers, i e the set of rational numbers is *countable*: We can list them in an infinite sequence $\{r_n\}$. It is clearly enough to do this for the positive rational numbers (why?). Since any positive rational number can be written $r = p/q$ where p, q are natural numbers we can partition $Q = \cup A_n$ where A_n is the finite set of rationals with $p + q = n$. This way we can list them by first listing A_2, then A_3 etc.

On the other hand, the set of real numbers is not countable. In fact, assume x_n is a sequence containing of real numbers. Then we can easily find a number that is not in the list, by changing x_n at the $n : th$ place in the decimal expansion.

We recall first the simple proof that the rationals have the same cardinality as the natural numbers, i e the set of rational numbers is *countable*: We can list them in an infinite sequence $\{r_n\}$. It is clearly enough to do this for the positive rational numbers (why?). Since any positive rational number can be written $r = p/q$ where p, q are natural numbers we can partition $Q = \cup A_n$ where A_n is the finite set of rationals with $p + q = n$. This way we can list them by first listing A_2, then A_3 etc.

On the other hand, the set of real numbers is not countable. In fact, assume x_n is a sequence containing of real numbers. Then we can easily find a number that is not in the list, by changing x_n at the $n : th$ place in the decimal expansion.

It is also easy to see that the set of algebraic numbers is countable, since the set of solutions of algebraic equations with integer coefficients that are bounded by n and with degree less than n is finite.

We recall first the simple proof that the rationals have the same cardinality as the natural numbers, i e the set of rational numbers is *countable*: We can list them in an infinite sequence $\{r_n\}$. It is clearly enough to do this for the positive rational numbers (why?). Since any positive rational number can be written $r = p/q$ where p, q are natural numbers we can partition $Q = \cup A_n$ where A_n is the finite set of rationals with $p + q = n$. This way we can list them by first listing A_2, then A_3 etc.

On the other hand, the set of real numbers is not countable. In fact, assume x_n is a sequence containing of real numbers. Then we can easily find a number that is not in the list, by changing x_n at the $n : th$ place in the decimal expansion.

It is also easy to see that the set of algebraic numbers is countable, since the set of solutions of algebraic equations with integer coefficients that are bounded by n and with degree less than n is finite. Hence there are transcendental numbers; in fact, most numbers are transcendental.

Cantor proved:

Theorem

Let A be a set and $P(A)$ be the set of all subsets of A. Then the cardinality of A is strictly smaller than the cardinality of $P(A)$.

Bevis.

Assume that $f : A \to P(A)$ is a bijection. Set

$$B = \{a \in A; a \notin f(a)\}.$$

Now, $B = f(b)$ for some b in A, since f is surjective. Then $b \in B$ if and only if $b \notin B$, which is a contradiction. $\square$

Notice that the proof gives that there is not even any surjection from A to $P(A)$. Now let A be the 'set of all sets'. Then $P(A) \subset A$, so there is clearly a surjection from A to $P(A)$. Contradiction!

Cantor proved:

Theorem

Let A be a set and $P(A)$ be the set of all subsets of A. Then the cardinality of A is strictly smaller than the cardinality of $P(A)$.

Bevis.

Assume that $f : A \to P(A)$ is a bijection. Set

$$B = \{a \in A; a \notin f(a)\}.$$

Now, $B = f(b)$ for some b in A, since f is surjective. Then $b \in B$ if and only if $b \notin B$, which is a contradiction. $\square$

Notice that the proof gives that there is not even any surjection from A to $P(A)$. Now let A be the 'set of all sets'. Then $P(A) \subset A$, so there is clearly a surjection from A to $P(A)$. Contradiction! This is *Russel's Paradox*.

Thus we have been able to derive a contradicition ‘within the system’; except that the meaning of the system that we work in has not been given a clear formal meaning. Frege’s objective was precisely to give a formal system in which mathematics could be formulated, but Russel’s paradox showed that it was too liberal: Contradictions could also be formulated within the system.

Thus we have been able to derive a contradicition ‘within the system’; except that the meaning of the system that we work in has not been given a clear formal meaning. Frege’s objective was precisely to give a formal system in which mathematics could be formulated, but Russel’s paradox showed that it was too liberal: Contradictions could also be formulated within the system. Therefore Frege wrote in a note just before publishing his work that he had learned about this problem, but that he was hopeful it could be fixed:

...habe Ich doch kein zweifel das der weg zur lösung gefunden ist..

Thus we have been able to derive a contradicition ‘within the system’; except that the meaning of the system that we work in has not been given a clear formal meaning. Frege’s objective was precisely to give a formal system in which mathematics could be formulated, but Russel’s paradox showed that it was too liberal: Contradictions could also be formulated within the system. Therefore Frege wrote in a note just before publishing his work that he had learned about this problem, but that he was hopeful it could be fixed:

...habe Ich doch kein zweifel das der weg zur lösung gefunden ist..

In spite of this, Frege’s ’Begriffschrift’ has had a great influence and is considered to be where *predicate logic* was introduced. In ‘Principia Mathematics’ (1910-13), Russel and Whitehead formulated a ‘theory of types’, that was designed to eliminate all paradoxes, but it is probably correct that it has not had a great impact. (Reputedly it is the one book in history that **no one** has read; not even the authors, since neither of them read what the other wrote.)

At about the same time as Principia Mathematica the Zermelo-Fraenkel set theory was developed. The objective was to describe precisely which operations that are permittable in mathematics, and in particular what is a legitimate way to define a set. Everything in the ZF-theory is a set, in particular a number is a set, a function is a set etc.

At about the same time as Principia Mathematica the Zermelo-Fraenkel set theory was developed. The objective was to describe precisely which operations that are permittable in mathematics, and in particular what is a legitimate way to define a set. Everything in the ZF-theory is a set, in particular a number is a set, a function is a set etc. On the other hand, not any property defines a set, and e g the ‘set of all sets’ does not exist, which offered a way out of Russel’s paradox.

At about the same time as Principia Mathematica the Zermelo-Fraenkel set theory was developed. The objective was to describe precisely which operations that are permittable in mathematics, and in particular what is a legitimate way to define a set. Everything in the ZF-theory is a set, in particular a number is a set, a function is a set etc. On the other hand, not any property defines a set, and e g the ‘set of all sets’ does not exist, which offered a way out of Russel’s paradox.

Now it seemed that the case was closed, in the sense that nobody had found any paradoxes or contradictions that could be formulated within the system. But, can we be sure that this does not happen in the future?

At about the same time as Principia Mathematica the Zermelo-Fraenkel set theory was developed. The objective was to describe precisely which operations that are permittable in mathematics, and in particular what is a legitimate way to define a set. Everything in the ZF-theory is a set, in particular a number is a set, a function is a set etc. On the other hand, not any property defines a set, and e g the ‘set of all sets’ does not exist, which offered a way out of Russel’s paradox.

Now it seemed that the case was closed, in the sense that nobody had found any paradoxes or contradictions that could be formulated within the system. But, can we be sure that this does not happen in the future? Can we *prove* that the system is consistent? Again, how do we prove that we cannot prove something?

This situation was clarified by Gödel in 1931. He proved that it is impossible to prove that set theory is consistent, without introducing a more powerful theory, whose consistency would then be even more dubious. (The same thing goes for arithmetics.) This is Gödel's second incompleteness theorem and it follows from Gödel's first incompleteness theorem:

Theorem

In any sufficiently strong system (like arithmetics or set theory), there are statements that can be neither proved nor disproved. (Unless the system is inconsistent, and then we can both prove and disprove the statement.)

Theorem

In any sufficiently strong system (like arithmetics or set theory), there are statements that can be neither proved nor disproved. (Unless the system is inconsistent, and then we can both prove and disprove the statement.)

Bevis.

We associate to any formula or statement in the theory a number – the 'Gödel number'. This way statements about formulas become statements about numbers. E g the statement 'there is a proof of formula n', becomes a statement in the theory; like 'there is a sequence of numbers that are Gödel numbers of formulas, such that each formula follows from the preceeding one by one of our laws of deduction, which starts with the Gödel number of an axiom and ends with n'. In the same way, statements about formulas are given Gödel numbers. Then one shows that there is a Gödel number of a statement, n, that says 'the statement with Gödel number n cannot be proven'. Then the statement can be neither proved nor disproved. □

Why is that?

Why is that?

If we can prove the statement, it follows that it cannot be proven, so we have a contradiction in the system. On the other hand, if we can disprove it, we have proved it!

Why is that?

If we can prove the statement, it follows that it cannot be proven, so we have a contradiction in the system. On the other hand, if we can disprove it, we have proved it!

It now also follows that we cannot prove the consistency of the system: If we can prove the consistency we have proved that the statement is not provable – so we have proved it.

Why is that?

If we can prove the statement, it follows that it cannot be proven, so we have a contradiction in the system. On the other hand, if we can disprove it, we have proved it!

It now also follows that we cannot prove the consistency of the system: If we can prove the consistency we have proved that the statement is not provable – so we have proved it.

Gödel's theorems were a fatal blow to Hilbert's formalist program in mathematics. It also lead to further discussion about which kind of reasoning that is permitted.

Why is that?

If we can prove the statement, it follows that it cannot be proven, so we have a contradiction in the system. On the other hand, if we can disprove it, we have proved it!

It now also follows that we cannot prove the consistency of the system: If we can prove the consistency we have proved that the statement is not provable – so we have proved it.

Gödel's theorems were a fatal blow to Hilbert's formalist program in mathematics. It also lead to further discussion about which kind of reasoning that is permitted. E g : Are proofs by contradiction acceptable? Does the law of the excluded middle hold: Either a statement holds or the negation of that statement holds.

Example

Are there irrational numbers a and b such that a^b is rational?

Example

Are there irrational numbers a and b such that a^b is rational?

Yes; let $a = b = \sqrt{2}$. Let $c = \sqrt{2}^{\sqrt{2}}$. Either c is rational, and we are done. If c is not rational, look at $c^{\sqrt{2}} = \sqrt{2}^2 = 2$, and we are done again.

Example

Are there irrational numbers a and b such that a^b is rational?

Yes; let $a = b = \sqrt{2}$. Let $c = \sqrt{2}^{\sqrt{2}}$. Either c is rational, and we are done. If c is not rational, look at $c^{\sqrt{2}} = \sqrt{2}^2 = 2$, and we are done again.

The *constructivist viewpoint* in mathematics does not accept the law of excluded middle, or proofs by contradiction. The onle acceptable proof of the existence of something is to construct it. This viewpoint has gained new popularity with the appearance of computer science.

Example

Are there irrational numbers a and b such that a^b is rational?

Yes; let $a = b = \sqrt{2}$. Let $c = \sqrt{2}^{\sqrt{2}}$. Either c is rational, and we are done. If c is not rational, look at $c^{\sqrt{2}} = \sqrt{2}^2 = 2$, and we are done again.

The *constructivist viewpoint* in mathematics does not accept the law of excluded middle, or proofs by contradiction. The onle acceptable proof of the existence of something is to construct it. This viewpoint has gained new popularity with the appearance of computer science. Other controversial statements that are sometimes used in mathematical proofs are:

1. The axiom of choice

Example

Are there irrational numbers a and b such that a^b is rational?

Yes; let $a = b = \sqrt{2}$. Let $c = \sqrt{2}^{\sqrt{2}}$. Either c is rational, and we are done. If c is not rational, look at $c^{\sqrt{2}} = \sqrt{2}^2 = 2$, and we are done again.

The *constructivist viewpoint* in mathematics does not accept the law of excluded middle, or proofs by contradiction. The onle acceptable proof of the existence of something is to construct it. This viewpoint has gained new popularity with the appearance of computer science. Other controversial statements that are sometimes used in mathematical proofs are:

1. The axiom of choice
2. The continuum hypothesis.

Applications of the axiom of choice:

Say that two real numbers x and y are equivalent if $x - y$ is rational. This is an equivalence relation, and we can partition

$$\mathbb{R} = \bigcup_{i \in I} A_i$$

where A_i are the equivalence classes. If we believe in the axiom of choice, we can form a new set B that contains exactly one element from each equivalence class. We can also arrange that $B \subset [-1, 1]$. Then

$$\mathbb{R} = \bigcup_{q \in Q} B + q.$$

Hence, $\mathbb{R}$ is the union of countably many translates of B.

Applications of the axiom of choice:

Say that two real numbers x and y are equivalent if $x - y$ is rational. This is an equivalence relation, and we can partition

$$\mathbb{R} = \bigcup_{i \in I} A_i$$

where A_i are the equivalence classes. If we believe in the axiom of choice, we can form a new set B that contains exactly one element from each equivalence class. We can also arrange that $B \subset [-1, 1]$. Then

$$\mathbb{R} = \bigcup_{q \in Q} B + q.$$

Hence, $\mathbb{R}$ is the union of countably many translates of B. What is the measure of B?