The New Math In Paradise[1]

E.C. Milner,
The University of Calgary

1. Introduction

A popular lecture in mathematics has one disadvantage compared to similar talks in other subjects like medicine, geology, zoology, physics etc. — we do not have nice pictures or experiments to capture the visual attention of our audience (although one striking exception is the subject of chaos or fractals). Also, mathematics is not really a spectator sport, to understand even the most elementary parts of our subject, it is essential that the listener should understand and follow most of the small details. On the other hand, we do have one great advantage over other subjects, and that is that we do not often have to revise our lecture notes! The proof of the following theorem (which is a favourite for many mathematicians) is almost exactly the same that Euclid might have given over 2,000 years ago (Book X, Proposition 117).

Theorem 1. *$\sqrt{2}$ is irrational (i.e. is not a fraction).*

Proof. Suppose the theorem is false. Then $\sqrt{2} = \frac{p}{q}$, where we may suppose that $\frac{p}{q}$ is a fraction in lowest terms (i.e. p, q are positive integers having no common divisor). Then $p^2 = 2q^2$ is an even integer. Since the product of two odd integers is odd p must be even — say $p = 2r$ where r is also an integer. But then $q^2 = 2r^2$ is also even, and so q is even. Therefore, p and q are both even — and this is a contradiction. Therefore the theorem is true. □

This proof is an elegant illustration of the so-called method of *reductio ad absurdum*. The result is a little bit surprising since the rational numbers are all that one needs for measurements in physics; they are dense in the number line, i.e. in any interval, no matter how small, there are infinitely many "fractions". The theorem shows there are gaps in the

[1] A lecture given to the Singapore Mathematical Society, June 19, 1991.

rational line. The result is attributed Hippasus of the Pythagorean school. But the rest of the school were not too pleased with the discovery since it seemed to represent a flaw in their basic philosophy. They believed that everything could be explained in terms of whole numbers (which had mystical properties) — for example, they had a very successful theory for music based upon fractions. It is said that the Pythagoreans were at sea when Hippasus discovered his beautiful theorem, but instead of celebrating the discovery he was thrown overboard and the result kept secret for many years!

I understand that several of you in the audience today are senior high-school students who have shown exceptional promise in mathematics, and you are competing for the honour of representing Singapore in the next International Mathematical Olympiad. As you know, the questions in that competition are very difficult — especially with the time constraints imposed by an examination! You might be amused to know that many very knowledgable professors of mathematics would also have great trouble solving these problems in the alloted time. Fortunately, in the real world, speed is not all that important. But it does illustrate another feature of our subject. To solve some problems, it is not always necessary to have a great knowledge of the subject (although that is not a disadvantage!), instead one needs some fresh idea — and, of course, young people often have many fresh ideas! It is my hope that some of you will continue the serious study of mathematics, you will find it rewarding.

In my talk today, I want to describe some of the bold ideas of the German mathematician GEORG CANTOR (1845-1920) concerning the mathematics of the infinite, or the theory of sets. Most of modern pure mathematics is based upon this theory. In fact, some years ago educationalists who wanted to update the school curriculum, seeing that many graduate courses in mathematics began with a review of the axioms of set theory, concluded that this was the real stuff, and that we should prepare students for it in our schools. So the "NEW MATH" was introduced into the school curriculum, even at the elementary level. In my view this may have been a mistake, since the emphasis seems to have been placed more upon the use of certain words and definitions rather than providing students with more powerful tools to actually solve problems. However, this is a debatable point and should not distract us here - I mention it simply to explain the use of the words in the title of this talk.

The infinite has always fascinated mathematicians, and has been the source of many puzzles. Some of the earliest, and most debated, were due to the Greek philosopher Zeno (~450 BC) of Elea in southern Italy. He gave several paradoxical arguments to show that motion is impossible. His purpose was rather to show that both the opposing views of time and space held at that time were untenable. For example, one paradox goes like this. In order to go from A to B (on a line) one must first go from A to the mid-point B_1. But before that one must go from A to the mid-point B_2, and so on (diagram 1). Thus, if space is infinitely divisible, so that a finite length contains infinitely many points, then it is impossible to cover a finite length in a finite time. These so-called paradoxes of Zeno were debated in many philosophical discussions through the centuries.

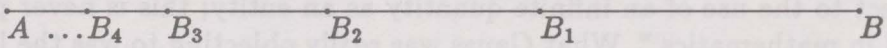

diagram 1.

A little closer to modern times, Gallileo (*Dialogues,* 1638) made the following observation:

$$\begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & & n & & \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \cdots & \updownarrow & \cdots & \\ 1^2 & 2^2 & 3^2 & 4^2 & 5^2 & & n^2 & & \end{array}$$

From this it would appear that there are just as many squares of natural numbers as there are natural numbers. But since there are clearly fewer squares than there are whole numbers, instead of anticipating the work of Cantor nearly 250 years later, he lamely concluded that the words "GREATER" and "LESS" are not applicable to infinite collections. This reminds me of a story about the physicist Crookes (of Crookes tube fame) which Paul Erdős likes to tell. Crookes noticed that when unexposed photographic plates were placed in a drawer near to one containing radium, the plates became useless. Instead of earning even greater fame, he left it for Madame Curie to discover X-rays several years later; he simply left laboratory instructions that (quite rightly!) photographic plates should not be stored near radium! For success in Science or Mathematics a certain amount of luck is needed, but more importantly, you also need an open mind.

Another type of nonsense is obtained when one applies the ordinary rules of arithmetic to infinite series. The following is an example given by Bolzano (*Paradoxien des Unendlichen*, 1851). To calculate the sum of the infinite series $S = 1 - 1 + 1 - 1 + 1 - 1 + \ldots$, we could add like this:

$$S = (1-1) + (1-1) + (1-1) + \ldots = 0 + 0 + 0 + \ldots = 0.$$

But we could equally well write:

$$S = 1 - (1-1) - (1-1) - (1-1) + \ldots = 1 - 0 - 0 - 0 - \ldots = 1,$$

and conclude that $0 = 1$!

It was probably arguments like this which C.F. Gauss (1831) (the greatest mathematician of his time) may have had in mind when he wrote: "I object to the use of an infinite quantity as an entity; this is never permitted in mathematics." What Gauss was really objecting to was the lack of distinction between a limiting process and an actual completed infinite process. For example, we can give a precise meaning to the assertion that $1/n \to 0$ as n tends to infinity, but to write $1/\infty = 0$ is just as meaningless as to write $1/0 = \infty$.

2. Cantor's discoveries

Despite the authoratitive pronouncement of Gauss (and others) Cantor ($\sim$ 1870) took the bull by the horns and proposed the following seemingly very natural definition.

Definition. Two sets A, B are equivalent or have the SAME cardinality (number of elements) if there is a one-to-one correspondence between their elements.
In other words, if there is a function $f : A \to B$ defined on A with values in B such that $f(a) \neq f(a')$ if a, a' are distinct elements of A (f is 1-1), and for every b in B there is some a in A such that $f(a) = b$ (f is onto). In this case we write $A \sim B$ or $|A| = |B|$.

Many such equivalences between infinite sets were known. For example, the correspondence between the set $S = \{1^2, 2^2, 3^2, \ldots\}$ of squares and the set of natural numbers $\mathbf{N} = \{1, 2, 3, \ldots\}$ noted by Gallileo, shows that these sets have the same cardinality. Another important example that had been known for a long time is the fact that there is a correspondence between $\mathcal{U}$ the set of real numbers x such that $0 < x < 1$ and the

set $\mathcal{R}$ of all real numbers (e.g. consider the map $f : \mathcal{U} \to \mathcal{R}$ given by $f(x) = (2x-1)/x(1-x)$).

Note that Cantor's definition only talks about the *equality* of cardinal numbers; he never actually gave a definition of *cardinal number*, although he anticipated later definitions, for he considered a cardinal number to be a *property* shared by a class of equivalent sets. He denoted by $\aleph_0$ the cardinality of the set of natural numbers $\mathbf{N} = \{1, 2, 3, \ldots\}$, which is the smallest infinite set in the sense that every infinite set contains a subset which is similar to it (this is true if one assumes the axiom of choice, or what Cantor called the "well-ordering principle").

More generally, Cantor wrote

$$|A| \leq |B|$$

to indicate that there is a one-to-one correspondence between the elements of A and a sub-collection of B. Using the same notation as in ordinary arithmetic, we also write $|A| < |B|$ if $|A| \leq |B|$ and $|B| \not\leq |A|$. The following useful theorem, is not quite as obvious as one might expect. Cantor believed it to be true but did not succeed in finding a proof; it was proved later and independently by Schröder (1896) and Bernstein (1905).

Theorem 2.1 [**Cantor-Schröder-Bernstein**] *For any sets* A, B

$$|A| \leq |B| \ \& \ |B| \leq |A| \Rightarrow |A| = |B|.$$

Proof. We can assume that A and B are disjoint sets (otherwise consider instead the sets $A' = \{(a, 1) : a \in A\}$ and $B' = \{(b, 2) : b \in B\}$). By hypothesis there are 1-1 functions $f : A \to B' \subseteq B$ and $g : B \to A' \subseteq A$. We want to show there is a function $h : A \to B$ which is 1-1 and onto.

Consider the directed graph on $A \cup B$ in which there is a directed edge from a to $f(a)$ for each $a \in A$, and also there is a directed edge from b to $g(b)$ for each $b \in B$. Every point has exactly one edge directed out from it and at most one edge directed into it. The graph naturally splits up into connected components which are of four possible different kinds: (1) an infinite path starting from some point of A, (2) an infinite path starting from some point of B, (3) an infinite path which has no starting point (and no end point), (4) a finite circuit with the same number of points from A

and B. We now define $h(a)$ for each $a \in A$ by setting $h(a) = f(a)$ if a is in a component of type (1), (3) or (4), and in case (2) we set $h(a) = b$, where b is the unique elembent in B such that $g(b) = a$. It is easy to check that h is a 1-1 map from A onto B. □

In his first paper on the theory of infinite sets Cantor (1874) proved the following theorems.

Theorem 2.2 $|\mathbf{Q}| = \aleph_0$, *where* $\mathbf{Q}$ *is the set of all rational numbers.*

Proof. Clearly $|\mathbf{N}| \leq |\mathbf{Q}|$. The reverse inequality follows from the fact that the following list includes every rational number:

$$\frac{0}{1}; \frac{1}{1}, \frac{-1}{1}; \frac{1}{2}, \frac{2}{1}, \frac{-1}{2}, \frac{-2}{1}; \frac{1}{3}, \frac{2}{2}, \frac{3}{1}, \frac{-1}{3}, \frac{-2}{2}, \frac{-3}{1}; \frac{1}{4}, \frac{2}{3}, \ldots.$$

The above list is obtained by writing down all those fractions p/q with q positive and $|p| + q$ successively equal to $1, 2, 3, \ldots$. □

Theorem 2.3 $|\mathcal{A}| = \aleph_0$, *where* $\mathcal{A}$ *is the set of all* algebraic *numbers.* (A number x is algebraic if it a root of a polynomial with integer coefficients, i.e there are integers n, $a_0, \ldots, a_n$ with $n > 0$ and $a_n \neq 0$, such that

$$p(x) = a_0 + a_1 x + a_2 x^2 + \ldots a_n x^n = 0.$$

E.g $\sqrt{2}$ is a root of $x^2 - 2 = 0$, $i\sqrt{3}$ is a root of $x^2 + 3 = 0$ etc.)

Proof. Obviously $|\mathbf{Q}| \leq |\mathcal{A}|$, since the rational number p/q is a root of $qx - p = 0$. Define the *weight* of the polynomial $p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ to be:

$$w(p) = n + |a_0| + |a_1| + \ldots + |a_n| (\geq 2).$$

Now for each integer $k \geq 2$ let

$$p_{k,1}, p_{k,2}, \ldots, p_{k,r(k)}$$

be a list of all the polynomials of weight k (there are only finitely many, so $r(k)$ is a (non-negative) integer). Now any polynomial of degree k has at most k different roots. So we can form a finite list

$$\alpha_{k,1}, \alpha_{k,2}, \ldots, \alpha_{k,s(k)}$$

which includes all the different algebraic numbers which are roots of one of the $r(k)$ polynomials of weight k. Finally, we can form the list

$$\alpha_{2,1}, \ldots, \alpha_{2,s(2)}, \alpha_{3,1}, \ldots, \alpha_{3,s(3)}, \alpha_{4,1} \ldots$$

which includes every algebraic number (in fact infinitely often). Therefore, $|\mathbf{N}| = |\mathbf{Q}| \leq |\mathcal{A}| \leq |\mathbf{N}|$. $\square$

These last two theorems, while very interesting, would not by themselves have caused too much of a stir since they did no more than confirm the seemingly obvious fact that "infinity = infinity". What made the results significant was that Cantor also proved that

NOT ALL INFINITE SETS HAVE THE SAME CARDINALITY!!!

More exactly, the previous two theorems show that the sets of rational and algebraic numbers are *countable* that is have cardinality at most $\aleph_0$, Cantor next proved that the set of all real numbers is uncountable.

Theorem 2.4 [Cantor, 1875] $|\mathbf{N}| < |\mathcal{R}|$, *where* $\mathcal{R}$ *denotes the set of all real numbers.*

Proof. Clearly $|\mathbf{N}| \leq |\mathcal{R}|$. We will assume that $|N| = |\mathcal{R}|$ and obtain a contradiction.

By our assumption there is an enumeration of the set of real numbers, i.e there is a list, say $r_1, r_2, r_3, \ldots$, which contains each real number exactly once. Consider their decimal expansions (in the usual scale of 10):

$$\begin{aligned}
r_1 &= N_1.r_{11}r_{12}r_{13}\ldots r_{1n}\ldots \\
r_2 &= N_2.r_{21}r_{22}r_{23}\ldots r_{2n}\ldots \\
r_3 &= N_3.r_{31}r_{32}u33\ldots r_{3n}\ldots \\
&\vdots \\
r_n &= N_n.r_{n1}r_{n2}r_{n3}\ldots r_{nn}\ldots \\
&\vdots
\end{aligned}$$

(there may be a slight ambiguity here since some numbers have two decimal expansions, e.g. $0.5000\ldots = 0.4999\ldots$; so to be more definite we assume that, for each n, $r_{ni} \neq 0$ for infinitely many i.)

To prove the theorem it will be enough to show that the above list is incomplete — there is at least one real number not included. To see that this is so consider the number

$$y = 0.y_1y_2y_3\ldots$$

whose n-th decimal digit is given by

$$y_n = \begin{cases} 1 & \text{if } r_{nn} \neq 1 \\ 2 & \text{if } r_{nn} = 1. \end{cases}$$

For each n, $y \neq r_n$ since $y_n \neq r_{nn}$, and so y is not in the list. □

From the last two theorems we deduce that **Corollary 2.5** $|\mathcal{R}| > |\mathcal{A}|$.

This caused quite a surprise in the mathematical world. At that time very few numbers which occur naturally in mathematics were known to be non-algebraic, or *transcendental.* It was only in 1844 that Liouville had proved that there were any transcendental numbers at all, and only the year before Cantor published his result had Hermite (1873) proved that e was transcendental. It was not untill later that π was shown to be transcendental.

Next Cantor looked for even bigger infinite sets than the set of real numbers. The first natural try was to look at the set of points in the plane (and n-dimensional space for even larger n). He was so surprised by what he found that, after proving the next theorem, he wrote to his friend Dedekind *"je le vois, mais je ne le crois pas"*. In fact, this result marked the begining of a dispute between Cantor and Kronecker, whom Cantor thought to be responsible for delaying the publication for nearly two years.

Theorem 2.6 [Cantor, 1878] *There are just as many points in n-dimensional space as there are points on a segment.*

Proof. We illustrate the idea by showing that there is a one-to-one correspondence between the unit interval $\mathcal{U}$ and the points of the unit square $\mathcal{U} \times \mathcal{U} = \{(x,y) : 0 < x,y < 1\}$. The argument works just as easily for n-dimensional space.

Obviously, $|\mathcal{U}| \leq |\mathcal{U} \times \mathcal{U}|$. We have to show that the reverse inequality holds. For this consider the map $f : \mathcal{U} \times \mathcal{U} \to \mathcal{U}$ defined as follows. For

$(x, y) \in \mathcal{U} \times \mathcal{U}$ consider the decimal expansions

$$x = 0.x_1x_2x_3\ldots, \qquad y = 0.y_1y_2y_3\ldots$$

and define

$$f(x, y) = 0.x_1y_1x_2y_2x_3y_3\ldots.$$

f establishes a 1-1 map between $\mathcal{U} \times \mathcal{U}$ and a certain subset of $\mathcal{U}$. □

Because of this, for a time Cantor thought that perhaps the sets of integers and reals represented the only two different kinds of infinity. But he soon found a whole hierarchy with the next theorem. Before we state it, let us recall that a^b denotes the cardinality of the set of all functions $f : A \to B$, where A, B are sets such that $|A| = a$ and $|B| = b$. It is easy to see that

$$|P(S)| = 2^{|S|},$$

where $P(S) = \{X : X \subseteq S\}$ is the set of all subsets of S. For we can make correspond to the subset $X \subseteq S$ the function $f_X : S \to \{0, 1\}$, which is defined by

$$f_X(x) = \begin{cases} 1 & \text{if } x \in X, \\ 0 & \text{if } x \notin X. \end{cases}$$

Incidentally, let us observe that $\mathcal{R} \sim P(\mathbf{N})$. For any set $X \subseteq \mathbf{N}$ there is a unique $\alpha_X = \sum_{x \in X} 3^{-x} \in \mathcal{U}$; this shows that $|P(\mathbf{N})| \leq |\mathcal{U}| = |\mathcal{R}|$. On the other hand, for any real number $\alpha \in \mathcal{U}$ there is a unique infinite set $X \subseteq \mathbf{N}$ such that α has the binary decimal representation $\alpha = \sum_{x \in X} 2^{-x}$, and so $|\mathcal{U}| \leq |P(\mathbf{N})|$. This shows that

$$|\mathcal{R}| = |P(\mathbf{N})| = 2^{\aleph_0}.$$

Theorem 2.7 *For any set S,*

$$|S| < |P(S)| = 2^{|S|}.$$

Proof. The map $x \mapsto \{x\}$ shows that $|S| \leq |P(S)|$. Suppose for a contradiction that there is equality so that there is a one-one onto map $f : S \to P(S)$. Consider the set $T = \{x \in S : x \notin f(x)\}$. By assumption there is some $t \in S$ such that $f(t) = T$. If $t \in T$, then we get the contradiction that $t \notin f(t) = T$. On the other hand, if $t \notin T$, then

$t \notin f(t)$ and so $t \in T$, which is again a contradiction. It follows that our assumtion is wrong and the theorem follows. □

This last theorem shows that there is no largest infinite cardinal number.

Cantor had really found it necessary to consider infinite sets from his original work on the convergence of Fourier series. Essentially, what he needed to consider was the notion of the set of *limit points* of a set of real numbers. It is not important here what these are, but a number $\alpha \in \mathcal{R}$ is called a limit point of the set $S \subseteq \mathcal{R}$ if $(\alpha - \epsilon, \alpha + \epsilon) \cap S$ is infinite for every $\epsilon > 0$. Now Cantor wanted to iterate this operation. Let S_1 be the set of limit points of S and S_2 be the set of limit points of S_1 and so on. In fact, Cantor wanted to apply this even beyond infinitely many steps, more precisely he needed to consider the set of limit points of the common intersection of all these sets S_n $(n = 1, 2 \ldots)$, say $T = \bigcap S_n$. Thus we start again taking the set T_1 of all the limit points of T and so on. For this reason he proposed that, for the purposes of counting, we needed more than just the integers, and he introduced the "number" ω to denote that ordinal number which follows the sequence of finite ordinal numbers $0, 1, 2, \ldots$; then ω is followed in turn by $\omega+1, \omega+2, \ldots, \omega+\omega = \omega.2, \omega.2+1, \ldots$, etc. Using this notation, Cantor could denote the set T by S_ω, T_1 by $S_{\omega+1}$, etc. Now-a-days, following a suggestion of von Neumann, it is usual to define an ordinal number to be the set of all smaller ordinal numbers numbers. Thus: $0 = \emptyset$, $1 = \{0\}$, $2 = \{0, 1\}, \ldots, \omega = \{0, 1, 2, \ldots\}$ etc.

After showing that $|\mathbf{N}| < |\mathcal{R}|$, the natural question to ask was whether there is some set $S \subseteq \mathcal{R}$ such that $|\mathbf{N}| < |S| < |\mathcal{R}|$? In fact Cantor considered this to be the most important question in the whole of mathematics; he conjectured that there was no such set S and this came to be known as the *continuum hypothesis*. What Cantor did show was that $\omega_1 = \{\alpha : \alpha \text{ an ordinal number such that } |\alpha| \leq \aleph_0\}$, the smallest ordinal number which follows all the *countable* ordinals, does give the next largest infinity. He denoted the cardinal number $|\omega_1|$ by $\aleph_1$ and showed (again assuming the well-ordering principle) that there is no cardinal number $\mathbf{m}$ such that $\aleph_0 < \mathbf{m} < \aleph_1$. In view of this the continuum hypothesis is the assumtion that

$$2^{\aleph_0} = \aleph_1.$$

It is now known that this can be neither proved nor disproved!

3. The paradoxes

Cantor's results about infinite sets provided mathematicians with powerful new tools and opened the way to considering new concepts like function spaces. Unfortunately, not everyone was happy. As hinted above, Kronecker in Berlin from the very begining was strongly opposed to Cantor's "new math". What he really objected to was the "non-constructiveness" of Cantor's methods. There was some point to his objection. For example, although Cantor showed that almost all real numbers are transcendental, his proof of this does not produce a single example of such a number. Kronecker proposed that all mathematical theorems should be reducible to a constructible statement about the integers, and he wrote: "The dear Lord made the whole numbers; everything else is man made." The mathematicians of that time could not swallow Kronecker's restrictions on their subject, for it meant the rejection of some of the most impressive results in mathematics. For example, after reading Linderman's famous proof that π is transcendental, Kronecker remarked to him: "what use is your beautiful proof since non-algebraic numbers do not exist".

However, while Cantor's set theory satisfactorily dealt with all the previously known paradoxes about the infinite, some troublesome new ones began to appear. Cantor had written: *By a "set" we are to understand any collection into a whole M of definite and separate objects m (called the elements of M) of our intuition or our thought.* Essentially, what this meant was that for any property p, one could collect into a set all those objects which have this property, or for any sentence $p(x)$ one can form the set $\{x : p(x) \text{ is true}\}$. The source of the trouble was the vagueness about what properties one could allow. Of the several new paradoxes that arose, the simplest was formulated by Russell. Most of the sets that we consider do not contain themselves as members; however, perhaps we should not rule out this possiblity — for example, consider the set of all abstract ideas! Anyway, Russell proposed that we consider the set

$$S = \{x : x \text{ is a set such that } x \notin x\}.$$

The rules of classical logic tell us that exactly one of the two statements (i)$S \in S$, or (ii)$S \notin S$ must hold. But if $S \in S$, then $S \notin S$, and if $S \notin S$ then $S \in S$!!! This is an embarrassing self contradiction. It is interesting to read Russell's own bibliographical account of how the paradox troubled him — after struggling with it for three years without success he was on the verge of suicide! (He did eventually find a way out with his so-called

theory of types.) Actually Cantor himself was aware that contradiction follows from allowing sets to be constructed too freely. He noted, some years before Russell discovered his paradox, that there was even trouble with the sentence "x is a set". For if we are allowed to form the set $S = \{x : x \text{ is a set}\}$, then surely S is the largest possible set since it contains every other set, but Cantor had already proved that $|S| < |P(S)|$ and this is a contradiction.

There were several other paradoxes which had a semantic flavour. One of the nicest was due to Richard. Presumably any integer which can be defined can be defined with a finite number of symbols and letters. So RICHARD considered a sentence rather like the following: "Let n be the smallest integer which cannot be defined using fewer than one hundred symbols or letters". But this contradicts the definition of n since this sentence does define n using fewer than one-hundred letters.

4. The debate

Cantor himself was not particularly worried by his own "paradox" since he correctly concluded that objects like the set of all sets simply did not exist. However, these paradoxes did provide the opposition with good ammunition, and Kronecker's earlier criticisms now found powerful and influential supporters who revived his emphasis on constructive methods. They founded the so-called *intuitionist school* of mathematics. Although this became a serious study, and one which is especially relevent to the modern developments in computer science, the philosophy was never popular among working mathematicians since, again, it meant abandoning so much. For example, the main proponent of this school of thought Brouwer (1908), proposed that we should avoid arguments like the one we used to prove Theorem 1.1 or 2.4: "The application to infinite sets of the law of the excluded middle of Aristotelian logic is inadmissible." And Poincaré even declared: "The actual infinity does not exist." It must be remarked, however, that Kronecker, Poincaré, Brouwer and their followers had themselves solved deep problems in mathematics, although one can also say that in their best works they conveniently laid aside their philosophical objections to standard mathematical methods.

Cantor's side in this debate found equally powerful supporters. None took to the defense more vigorously than Hilbert who declared: " Cantor's theory seems to me the most admirable fruit of the mathematical mind and

indeed one of the highest achievements of man's intellectual processes." He also vowed that : "No one shall drive us from the paradise which Cantor has created for us." This explains my choice for the last word in the title of this talk. My former friend D.H. Lehmer, who recently died, was well known for his important work in finite mathematics, and whenever we met he would jokingly ask for the latest news about "life in paradise".

5. The axiomatization of Set Theory

It is not possible in this lecture to fully describe the philosophical differences which crystalized during the debate about the foundations of mathematics early in this century. However, I must mention the rescue of Cantorian mathematics from the paradoxes by the successful axiomatization of set theory by Zermello (1908). Just as "point", "line" and "plane" are undefined terms in euclidean geometry, in set theory the undefined terms are "set" and "belongs to", no meaning is given to these terms. Since most of the paradoxes arose from forming sets which were either too large or involved some self reference, the main goal for axiomatizing set theory was to give precise rules to describe how sets may be formed and operated on, and, in particular, to avoid the formation of sets which are "too large" (like the set of all sets), but at the same time to legitimize all those operations that we want to use in mathematics. Nowadays, it is usual to develop set theory, and most of mathematics from Zermello's axioms (or rather a version, called ZF, which incorporates an important improvement due to Fraenkel); you must look to texts on set theory to see what these axioms are, and how all of ordinary mathematics can be developed using this language. Here we shall simply illustrate how Zermelo's axioms handled the Russell paradox. The axioms do not allow the formation of the Russel set exactly as described before, but they do allow us to form a set of the form

$$S = \{x : x \in A \text{ and } x \notin x\},$$

where A is some set *already constructed.* As before, we can still ask whether or not $S \in S$. If $S \in S$ then $S \in A$ and $S \notin S$, which is a contradiction. Similarly, if $S \notin S$ and $S \in A$, we get the contradiction that $S \in S$. However, we now conclude that $S \notin A$, and hence and $S \notin S$, there is no contradiction!

One axiom of Zermello which provoked especial criticism, was the so-called axiom of choice. One way to state this is the following

AC: If S is a set of non-empty pairwise disjoint sets, then there is a set which contains exactly one element from each member of S.

Zermello recognized that many mathematical proofs did (unwittingly!) invoke some form of this axiom. For example, the well-known proof that any bounded non-empty set of real numbers has a least upper bound. Zermello also showed that AC is equivalent to the well-ordering principle used by Cantor. Because of the non-constructiveness of the axiom, it was completly unacceptable to the intuitionists. There is a nice example of Russell to illustrate the problem. A millionaire has an infinite number of pairs of shoes and an infinite number of pairs of socks. We can very easily imagine a set which consists of exactly one shoe from each pair (e.g. the set of left ones), but how can we describe a set consisting of just one sock from each pair?!

While **AC** may look rather innocent, and most mathematicians continue to use this axiom without worrying about the foundations of their subject, it is an extremely powerful axiom. For example, assuming **AC** we can prove the following very surprising result.

Theorem 5.1 *There is a partition of the solid 3-dimensional ball into 9 pieces which can be reassembled (using only rotations and translations) into TWO solid 3-dimensional balls having the same radius as the original one.*

This may seem like the ancient alchemists dream to manufacture gold come true, but the theorem is about mathematical objects not physical ones! The theorem is known as the Hausdorff-Banach-Tarski paradox, but it is only paradoxical because it offends our intuition, it is a perfectly respecable theorem (assuming AC!).

6. Later developments

The axiomatization of set theory was completely satisfactory in so far as it avoided all the known paradoxes and at the same time provided us with a suitable language with which we could feel comfortable and actually do mathematics and, even more importantly, keep all our time-honoured theorems.

However, some were not content with that. How could we be sure that there are no new hidden paradoxes or just plain self-contradictions in

set-theory? Hilbert set himself and his school in Göttingen the ambitious task of actually *proving* that this mathematics is consistent, i.e. free from contradiction. Indeed Hilbert had already achieved great success of a related kind with his important work on the foundations of geometry. The axioms of Euclid represent a tremendous intellectual triumph in their intention, but they do not really do the job they were supposed to do — not all (in fact very few) theorems of geometry can be rigorously deduced from those axioms; Euclid used some additional unstated assumptions. However, Hilbert tidied the whole thing up so that Euclid's programme could be accomplished in a manner that met the rigorous demands of the more modern criticism. More importantly, Hilbert went one step further; he showed that the axioms of geometry were consistent *provided arithmetic is consistent.* With this success behind him, Hilbert then began the more formidable task of proving that arithmetic, and all of mathematics, is consistent.

Unfortunately, although the Hilbert school did obtain important results about formal mathematics, their main goal turned out to be an impossibility. The Austrian mathematician Kurt Gödel in the early 1930's actually *proved* that there could be no proof in mathematics that mathematics is consistent!

A proper description of Gödel's ideas cannot be given in a lecture of this kind, but something can be said about his novel idea of "arithmetizing" a mathematical proof.

Whatever else it may be, an acceptable "mathematical proof" must consist of a finite number of symbols chosen from a finite alphabet, e.g. a,b,c,...,z, A,B,...,Z, 0,1,2,..., 9, $+, -, ., \backslash, \surd, =, (,), [,], \ldots$. Consequently there are only countably many "proofs" of theorems, although some sequences of symbols will be meaningless. For example:

$$(x-1)(x+1) = x(x+1) - 1.(x+1) = (x^2+x) - (x+1) = x^2 - 1$$

may be considered to be a "proof" but $(+ ==) = .10x + 2$ is a nonsense string. Among all the nonsense strings we will find the complete works of Shakespeare since, from our point of view, these are certainly not proofs of mathematical truths. Anyway, whatever good proofs may be, and whether we can recognize them or not, there are only countably many of them. This is already an interesting observation. For, let us follow a suggestion of R. Finsler (1926) and consider the assertion "a is a transcendental number". There are proofs of this for certain values of "a", (some are very

difficult, e.g. $a = 2^{\sqrt{2}}$ is transcendental by deep theorems of Siegel and Gelfond). But by Cantor's theorem we know that there are uncountably many transcendentals and therefore there is a transcendental number a for which there can be no possible proof of the fact that a is transcendental! (Although you might wonder whether there is such a number which can be described with the allowed symbols?)

Gödel's arithmetization process associates a unique integer with any formula or proof in the following way. To each of the basic symbols of the language to be used we associate a distinct positive integer. For example, if we use the above list we could use the association: $a \Leftrightarrow 1$, $b \Leftrightarrow 2$, $c \Leftrightarrow 3$, etc. Now a statement, φ, in our language is nothing but a sequence of the symbols and so we can code this in a unique way by an integer as follows. Suppose, the symbols in the sequence which forms the given statement, taken in order, correspond to the integers

$$n_1, n_2, n_3, \ldots, n_t.$$

Then the Gödel number for this statement φ is

$$G(\varphi) = p_1^{n_1} p_2^{n_2} \ldots p_t^{n_t},$$

where $p_1, p_2, p_3, \ldots$ is the sequence of prime integers taken in increasing order. This is an effective code since, given the Gödel number $G(\varphi)$ we can recover the original sequence of symbols φ. For we just have to check how many times we can divide 2 into $G(\varphi)$ in order to find the integer which corresponds to the first symbol, then keep dividing by 3 in order to find the second symbol and so on. With this slight and inadequate hint, you may imagine that by this kind of coding, Gödel was able to translate statements about a formal system (metastatements) into statements about positive integers. Let me conclude by stating (in an informal way) two very important and remarkable theorems of Gödel (1931) which greatly influenced the philosophy of mathematics.

Theorem 6.1 *In any formal system, S, which includes formal arithmetic, there is a statement expressible in the language of S which can neither be proved nor disproved in S.*

To say that the system S is *consistent* means that, for any assertion T we cannot prove in S both of the statements "T is true" and "T is false". The statement which says "S is consistent" can be expressed in S, and the surprising fact is that:

Theorem 6.2 *The consistency of S cannot be proved in S.*

Thus it seems that in mathematics we can do no better than to believe (or hope) that our subject is consistent, there can be no formal proof that this is so. However, as F. De Sua (A.M.M. (1956), 295-305) pointed out: "If we loosely define a religion to be a discipline whose foundations rest on an element of faith, irrespective of any element of reason which may be present. Quantum mechanics for example would be a religion under this definition. But mathematics would hold the unique position of being the only branch of theology possessing a rigorous proof of the fact that it should be so classified."