Mathematics, Measurement and Money Transcript

Date: Tuesday, 24 May 2016 - 6:00PM

Location: Museum of London

24 May 2016

Mathematics, Measurement and Money
Joint London Mathematical Society Lecture

Professor Norman Biggs

London School of Economics

The Awakening: Ancient Mesopotamia (c.3000-1500 BC)

By about 3200 BC a large settlement had been established at Uruk in Mesopotamia, and a clear social hierarchy was in operation. A few of the higher-ranking citizens controlled the economic life of the city by administering the distribution of resources. Archaeologists have found many small clay tablets that were used to record these administrative mechanisms. The tablets have been inscribed by making marks in the wet clay: some of the marks are pictograms representing commodities of various kinds, and others are symbols representing numbers. When dry the tablets are almost indestructible, and it is this fact that provides us with (currently) the best evidence of how the use of numbers was developing around the end of the fourth millennium BC.

The evidence suggests that the development of the art of writing was closely linked to the use of symbols for representing numbers. Both written text and number-symbols arose in response to the need for keeping account of the various things that were important in the early agrarian economies. The number-symbols were the original tools of mathematics, and as such they played an important part in the process we call civilization.

Later, in the third millennium BC, the economic organization of society became more complex, and correspondingly sophisticated ways of dealing with numbers were developed. The procedures were based on the number sixty. For example, since the number we write as 75 is equal to *one* sixty and *fifteen* units, it was represented by combining the signs for *one* and *fifteen*. For larger numbers, the units were sixty-sixties (our 60 x 60 = 3600), sixty-sixty-sixties (our 60 x 60 x 60 = 216 000), and so on. This is known as a **sexagesimal system**, from the Latin word for sixty.

The fact that these numbers were written on clay tablets, so many of which have survived, provides us with splendid evidence of how mathematics was being used around 2000 BC. Although the sexagesimal system itself is no longer with us, it is remarkable that the number 60 still plays a major part in the management of our daily lives. If you have ever wondered why each hour has 60 minutes, you can blame the Mesopotamians. The historical reason for the success of the system was the fact that it could be used to carry out the numerical operations required by the administrators who controlled the economic life of the region. These operations are what we call **arithmetic.** Essentially they are a clever form of juggling with number-signs, so that the answers to certain practical questions can be obtained.

These notes are based on extracts from the book *Quite Right: The Story of Mathematics, Measurement, and Money*, published by Oxford University Press in 2016.

This so-called ‘elementary’ arithmetic was the basis of the science of **measurement**—the assignment of a number to an object in order to describe one of its characteristic properties. Nowadays a measurement is expressed as a number of standard units: so my height is 185 centimetres, and this number of centimetres is counted out on a tape-measure. It is reasonable to assume that simple measurements of **length** were being made in this way long before we have any written record of them. Originally the units were determined by parts of the human body; for example, the length of a human forearm (about 50 centimetres) would have been a useful unit for domestic purposes, such as carpentry and building houses. When written records began, a unit of roughly this size is mentioned in many of them. The actual name varies from place to place, but we use the Latin name *cubit*, which is of course much later.

Some of the earliest written evidence about measurements is related to larger units, used for measuring the size of a plot of land. The advent of settled farming was inevitably accompanied by the notion that certain pieces of land belonged to certain family groups and, in due course, it led to problems that could only be solved by mathematical methods. How much land do I have? If I wish to divide it equally between my two children, how should I do it? Such were the original problems of geometry, literally earth-measurement.

Some very early tablets from Uruk show attempts to compute the size of a field by multiplying two lengths. For the scribes in Uruk, and for us, **area** is a two-dimensional concept**.** An area-measure is defined as the product of two length-measures, and is therefore expressed in units like the *square metre*. For example, a rectangular field with sides of length 7 metres and 4 metres has an area of 7 x 4 square metres. In a simple case like this the square metres are quite obvious, and we can work out that the answer is 28 simply by counting the squares.

A fundamental difficulty is that most fields have irregular shapes, and so the area units cannot be laid out as they are in a rectangle. When we try to cover an irregular field with a grid of squares there will be many squares that lie partly inside and partly outside the field, and there is no easy way of accounting for them. At some point in the third millennium BC this difficulty was resolved by the discovery of one of the most important results in the

whole of geometry:

the area of a triangle is half the base times the height.

This is one of the most useful results in the whole of mathematics. The difficulty of dividing our triangular field into little square pieces has been overcome by some very simple imaginary operations. The importance of the result is dramatically increased when we realize that any figure bounded by straight lines can be divided into triangles, and hence its area can be measured exactly. For example the area of a four-sided field can be calculated exactly by measuring the length of a diagonal and the heights of the two triangles into which the diagonal divides the field. This process of triangulation was to become the basis of the art of surveying, as illustrated in John Cullyer's *Gentleman's and Farmer's Assistant* (1813).

Another problem that arose naturally in the early civilizations was the measurement of **volume.** In the Old Babylonian period the economic organization of the larger settlements depended on storing large amounts of grain and distributing it to the inhabitants. Records on clay tablets suggest that the grain was stored in pits of a standard size, one rod (about 6 metres) square and one cubit (about 50 centimetres) deep. The resulting measure was a *volume-sar*.

In order to distribute the grain to the people a different kind of volume-measure was used. It was known as a *sila*, and it was determined by the capacity of a suitable vessel. A sila was very roughly equivalent to a litre in modern terms, so the vessel was similar in size to those in which drinks are now sold. A very interesting clay tablet deals with the problem of making a sila-vessel, as well as providing several remarkable insights into the mathematical achievements of the time. Suppose we want to make a vessel with the capacity of one sila, in the form of a cylinder with a circular base. The problem is: given the diameter of the base, how high should the vessel be? The solution requires several pieces of data, including the fact that one volume-sar contains 21600 sila, and the relationships between the units of length that were in use at that time:

30 *fingers* = 1 *cubit*, 12 *cubits* = 1 *rod*.

Given these rules, it follows by arithmetic that one sila is the same as 180 'cubic-fingers'. Since 180 = 6 x 6 x 5, a sila could have been measured with a vessel having a square base with sides of length 6 fingers and a height of 5 fingers.

The problem is to determine the height of a sila-measure in cylindrical form, if the diameter of the circular base is 6 fingers. First, we must find the area of the circular base. Counting little squares does not work with a circle, so such calculations had to be done by approximate rules, and we must be careful not to confuse these rules with our modern formulas involving the number we denote by π (the Greek letter pi). The rule stated on this tablet is to multiply the diameter by three, then multiply the result by itself, and then take the twelfth part; so the area of the base in 'square fingers' is

This works out as 27. Given that one sila is 180 cubic fingers, the height of the vessel must be 180 divided by 27, or six and two-thirds fingers.

There is another, quite different, way of measuring quantities. It is called **weight** and is based on the simple fact that objects possess a mysterious property that makes them difficult to lift and move. It must have been clear to the early farmers that different materials possess this property in different degrees: a bucket full of water has less weight than the same bucket full of sand, so weight is not simply another way of measuring volume. We must also remember that the physical foundations of the concept of weight were not clarified until the seventeenth century AD, and so we must avoid using the words 'gravity' and 'mass'. The ancient idea of weight was based on experience, rather than theory. Because the weight of an object is not immediately apparent to the human eye (unlike length and volume), the measurement of weight had to be done by a mechanical device which could produce clearly visible results.

As we have seen, units of measurement appear to have had humble origins. They were based on local practices, and varied in time as well as place. As civilization took a firmer hold, the rulers of empires and kingdoms would try to assert their power by making laws about the units, and issuing **standard weights and measures** to define them. In Mesopotamia the need for standardization had been recognized by about 2100 BC. From this period there are tablets inscribed with hymns to the goddess Nanshe, giving thanks for the standardization of the size of the reed basket (possibly the sila measure mentioned above), and a measure known as a *ban*, believed to be 10 silas. Nanshe was the deity responsible for social justice, which suggests that uniformity of these measures was seen as a means of ensuring fairness in the distribution of grain. However, attempts to enforce the uniformity of weights and measures have traditionally met with limited success.

Another feature of life in the early settlements was **money**. A clay tablet dating from around 1950 BC is inscribed with a proclamation from the king of Eshnunna. It provides explicit evidence of the various functions of money at that time. The primitive social functions are represented by fines for causing injury. For example, if you were guilty of 'biting a man's nose' you would have to pay about *500 grams of silver*, but a 'slap in the face' would cost you less. It is clear from this tablet, and many others, that the use of silver as a form of money was

well established by the beginning of the second millennium BC. Of course, most people in Mesopotamia did not have any silver, and for them alternative forms of money were used.

A New Beginning: Early Modern Europe (c.1600-1800 AD)

By the end of the sixteenth century, arithmetic was playing an important part in many aspects of everyday life. Consequently there was a demand for skilled arithmeticians—in particular, for people who could make reliable tables to assist those who had to do the calculations. One such work was the *Tafelen van Interest* (1582) written by Simon Stevin, an accountant and engineer who lived in Bruges. The same author's *De Thiende* (1585) was a work of a different kind. In this book he advocated the use of **decimal fractions**, and explained why they were superior for computational purposes to the 'vulgar' fractions, like , then in use. It is safe to say that few people understood the reasons behind them. That was hardly surprising, since the textbooks of the day offered little or no explanation.

Decimal fractions soon found many applications, and their usefulness was enhanced when tables of **logarithms** became available. In order to *multiply* two given numbers, we simply look up their logarithms in a table, and *add* them. The answer is the number whose logarithm is this sum. In order to divide one number by another, we subtract the logarithm of the second number from the logarithm of the first.

The first person to devise a practical system of this kind was a Scottish nobleman, John Napier. His table of logarithms was published in 1614. It was intended specifically for some trigonometrical calculations, and the system was quite complicated, but to Napier goes the credit for the original invention, and for the word *logarithm*. The creation of a more practical system came a few years later. Henry Briggs, Professor at Gresham College in London, discussed the problem with Napier, and they agreed on some technical details. They decided that, for any numbers and the logarithms of , and should satisfy the basic rule

This condition is not quite enough to define the logarithm uniquely: a little more information is needed. Since the decimal notation for numbers and fractions was now being widely used, Napier and Briggs agreed to choose 10 as the number whose logarithm is 1. That was the origin of what became known as *common* logarithms. Compiling tables of common logarithms was hard work, but their usefulness for calculations in navigation and astronomy was immediately recognized, and by the end of the 1620s such tables were available for numbers up to 100 000. For over 300 years these tables of logarithms and antilogarithms were in constant use wherever arithmetical calculations were needed, in science, industry and commerce.

Stevin's work on decimals was read by Thomas Harriot, an Englishman who produced an enormous amount of original mathematics in the late sixteenth and early seventeenth centuries. Among his papers there is one that deals with **compound interest**. Harriot made a new contribution which is highly significant, not just for its specific content, but because it foreshadowed several of the most important mathematical discoveries of the seventeenth century. His motivation was the observation that if interest is added more frequently than once a year, but at the same equivalent rate, then the yield will be greater. He denoted the annual rate of interest by (for example corresponds to percent), so one pound invested for one year will yield pounds. But if the interest is added twice yearly at the rate of then the yield at the end of one year is

You should convince yourself that this is slightly more than If the interest is added three times a year, at the rate then the yield is which is greater still, and so on. The question is: what happens when the compounding is done with greater and greater frequency, say times per year, but at the same equivalent rate?

Harriot considered what happens when is allowed to become arbitrarily large: this is what we now refer to as *continuous compounding*. As an example, he calculated that 100 pounds invested at 10 percent for seven years, with continuous compounding, will yield approximately 201 pounds, 7 shillings, and 6.06205 pence. The significant point is that the yield does not become arbitrarily large: even though the calculation produces infinitely many terms, their sum has a definite **limit**, which can be calculated to any required degree of accuracy.

About 50 years after Harriot, Isaac Newton applied himself to the study of limiting processes. His work was the foundation of what we now call 'calculus', and he also studied infinite series like the one used by Harriot. In these early researches Newton had also made important discoveries in optics, mechanics, and astronomy, and he continued his work in the relative obscurity of Cambridge until, in 1687, he published his great work, the *Mathematical Principles of Natural Philosophy*, usually referred to as the *Principia*, part of its Latin title. It contained a description of the physical world that explains almost everything that we encounter in our daily lives, from the movement of the planets to the flight of a tennis ball. The *Principia* made Newton famous far beyond the narrow confines of academe.

In 1696 Newton's life took a new turn, when he was appointed to the position of Warden of the Tower Mint in London. He soon became involved in the problems of the English currency, which was at that time undergoing a major revision of the silver coins. When, in 1699, the post of Master of the Mint fell vacant, Newton was appointed to the post. He continued as Master until his death in 1727, and throughout that period he had to wrestle with the problems created by a currency of coins made of precious metal. Here is a short extract from one of his many reports to the Treasury, written in 1701.

The Lewis d'or passes for fourteen livres and the Ecu or French crown for three livres and sixteen sols. At which rate the Lewis d'or is worth 16s 7d sterling, supposing the Ecu worth 4s 6d as it is reckoned in the court of exchange and I have found it by some Assays. The proportion therefore between Gold and Silver is now become the same in France as it has been in Holland for some years.

Few people could make sense of all this. Those involved in the daily round of trade and commerce carried small money-scales and weights so that they could check the weight of the French gold Lewis d'or coins and the English gold guineas that circulated concurrently.

Newton's calculus was expressed in a notation that was awkward and obscure. Fortunately the same ideas were soon re-discovered by Leibniz, and expressed in a more convenient notation, which we still use today. And so, by the beginning of the eighteenth century, there was a solid mathematical foundation for the great flowering of scientific thought that we call The Enlightenment. The impact of the new scientific approach was most noticeable in France, where it confronted a social hierarchy that was still medieval in many respects, and it may or may not have been a coincidence that, in the 1780s, French scholars began to study the mechanics of voting procedures. Among those who wrote on this subject were the academicians Jean-Charles de Borda, the Marquis de Condorcet, and the Marquis de Laplace. When the Revolution began in 1789, these men were all involved, and quite soon afterwards they found themselves part of a different kind of revolution — in measurement.

By this time the need for standards of weight and measure was acknowledged in all the developed nations. However, in the British Isles the bushel measure of capacity varied from place to place, while in France the lingering medieval system of government meant that all kinds of weights and measures were determined locally. The new revolutionary assembly appointed a committee to consider the matter, and in March 1791 they recommended that the standard of length should be one ten-millionth part of the length of a meridian from the North Pole to the equator. The proposed unit should be named the *metre*.

The work on the new **metric system** began in 1792. The plan was to determine, by the traditional method of triangulation, the length of a section of the meridian that runs through Dunkirk and Barcelona. Of course, the lengths and angles had to be measured with extreme accuracy.

It was also agreed that the unit of weight, to be known as the *gramme* (now usually written *gram*), should be the weight of a volume of pure water equal in size to a cube with sides of one-hundredth of a metre. Since this was impractical as a physical definition, it would be represented by a standard object, a kilogram (equal to 1000 grams) made of a suitable metal. Despite many setbacks, the establishment of the new Metric System was authorized by a decree issued in 1795.

Sadly, the adoption of the Metric System did not begin well. Partly this was because some of the innovations were so awkward that failure was almost inevitable failure. But the most serious problem was the innate opposition of the majority of the French people, whatever their revolutionary zeal, towards any new form of measurement. Nevertheless, in due course the Metric System was adopted by most nations of the world, thus vindicating the vision of the French mathematicians and scientists who set it up. A few countries retained their traditional quaint terminology for units of measurement, but most of them (including the UK since 1963) have now chosen to define these units in terms of the international metric standards.

Today and Tomorrow: Two Global Problems (1970 onwards)

Isaac Newton's position as Master of the Mint had made him a wealthy man, and when he died in 1727 he left a considerable fortune, much of it in shares. But not all his investments had been successful. The popular belief that shares in the South Sea Company would increase in value had been based on nothing more than a rumour; consequently the South Sea Bubble was destined to burst, and it duly did so, causing Newton financial pain. He is reported to have said that, for all his mathematical abilities, he 'could not calculate the madness of the people'.

Throughout the eighteenth and nineteenth centuries the fledgling financial markets of Newton's day grew into great birds of prey, offering countless opportunities for speculation. In addition to stocks and shares, people could speculate on such things as annuities, insurance, and foreign exchange. A chart taken from a book published in 1893 shows the fluctuations in two versions of the exchange rate between London and Paris for the year 1888. The diagrams show a marked degree of irregularity, even though they have been smoothed by taking weekly averages. Nowadays the rates change very frequently, and if the time-period was one hour rather than one year, the diagrams would look much the same. The 'madness of the people' remains the major factor that causes changes in the price of a financial asset, and that is much harder to predict than factors described by the laws of physics.

The first person to attempt to make a mathematical model of the movements of asset prices was a young French mathematician, Louis Bachelier. In 1900 he presented his doctoral thesis entitled *Théorie de la Spéculation*, in which he laid the foundations for the subject that is now known as Financial Mathematics. His work was truly remarkable, because he was able to work out many of the essential features of the problem, even though the rigorous mathematical foundations were not sorted out until later.

Bachelier's model has since been amended and extended, but the basic ideas can still be explained in a way that Leibniz would have understood. The aim is to describe how the price of an asset varies as a function of time In a small time , the change in is and since the numerical value of is a purely arbitrary measure, it makes sense to consider the ratio The now-standard model assumes that is the sum of two contributions, one deterministic, and one random. The first one is an underlying trend, which contributes a change proportional to the time-interval, say The second one is a contribution resulting from the 'madness of the people', which we denote by It is assumed that the quantities and are characteristics of the asset, and they can be calculated from data on how the price has changed in the past. So this model leads to the equation

Realistically, the behaviour of must be determined by rule that takes account of the fact that the time intervals must be allowed to vary, and become arbitrarily small. A subtle blend of probability and calculus is needed in order to set up a proper model of this situation.

Bachelier's thesis remained unnoticed for many years, although there were several theoretical advances that justified his insights. In the 1920s the theory required to prove the existence of a mathematical model in which is normally distributed was developed by Norbert Wiener, and in the 1930s Andrey Kolmogorov strengthened the foundations of probability theory. Finally, from about 1944 onwards Kiyosi Itô showed how equations involving differentials of non-deterministic processes can be solved. These advances led to the subject that we now call Stochastic Analysis. It is still a very active area of research in the twenty-first century, partly because Bachelier's model of asset prices has become a fundamental tool in the real world of finance.

Consider, for example, the *option*. In its simplest form, an option gives a speculator the right to buy an asset at a fixed price at some future time If, at that time, the market price of the asset is greater than then the speculator will take up the option and gain an amount ; otherwise she will not do so, and will gain nothing. The option can be traded at any intermediate time and its value at that time, , clearly depends in some way on the asset price The obvious question is: If the probability distribution of is given, what is the probability distribution of

The key is the No-Arbitrage Principle, sometimes paraphrased as 'there is no free lunch'. It must not be possible for a trader to make a guaranteed profit simply by switching from one asset to another, however rapidly the transactions are made. In particular, the holder of an option should not be able to make a profit by exchanging it with the asset on which it is based. In 1973 Fischer Black and Myron Scholes saw how to combine this principle with Bachelier's model, and using the tools of stochastic analysis they obtained an equation for the relationship between the asset price and the value of an option based on that asset. The theory was extended later that year by Robert Merton. One attractive feature of the Black-Scholes-Merton equation is that it has a close relation to the equation governing the flow of heat, which had been studied by mathematicians and physicists for almost two hundred years.

The fact that tractable models were available led to a spectacular boom in the trading of options of all kinds. The Black-Scholes-Merton equation provided an explicit formula for option-pricing, which was a powerful, but misleading, incentive. The apparent ease of applying 'the formula' concealed the fact that it is based upon a mathematical model, which inevitably over-simplifies the real situation. Sadly, many of the people responsible for this boom understood very little about the mathematics or the assumptions on which it is based. Even if they were aware of the problems, they believed that the operation of the financial markets would automatically correct unsound decisions. The trading in options became increasingly bizarre, and the baroque convolutions of this activity reached heights that were, literally, fantastic: the alleged value of the options being traded was many times the value of all the world's real resources. It was the South Sea Bubble again, and again it burst.

As well as exotic options, the world of modern banking has another feature that tends to propel it into the realms of fantasy. Vast sums of money can be transferred in an instant, far more quickly than it has taken you to read this sentence. At the humble level of personal banking this affects us all directly, because the traditional methods of payment by cash or by cheque are gradually being displaced by payment using plastic cards. When you pay your bills using a plastic card, you are simply authorizing alterations to the information stored in some computers.

Money, in the form of coins and jewels, was traditionally kept under lock and key. Wealthy medieval families would use a strong box with a large key, both of which were carefully concealed. Later, the box might be kept in the vaults of a bank, behind securely locked doors. In both cases a potential thief might be aware of the location of the box, but in order to steal the money he would need to find the keys. An analogous principle was applied to the sending of secret messages for military and diplomatic purposes: the means of communication might be easily discovered, but the 'keys' had to be kept secret. The result was a long-running battle in which the code-makers tried to make better keys, and the code-breakers sought for better ways of finding them.

Nowadays **cryptography** is a routine part of our everyday lives, although we may not always be aware of it. But, as always, we are acutely aware of the need to keep our money secure. Because a great deal of our money is not kept in a tangible form, but in the form of information, the problem of keeping our money safe and the problem of keeping our messages secret have become almost identical. The messages initiated by our plastic cards must be sent and received safely: if all the parties involved are to be kept happy, the entire operation must be carried out with a high level of confidentiality

At a practical level, it is clear that the basic tools of the code-makers have been introduced into our financial

affairs. My plastic card has a 16-digit number on the front, and another shorter number on the back, and it contains a 'chip' that can do some mysterious operations with these numbers. I also have a 'pin' (Personal Identification Number) which I must memorize and supply whenever I use my card. These numbers form a kind of cryptographic key. But, as we shall now explain, the most sophisticated modern cryptosystems differ from the traditional ones in the way that the keys are used.

A feature of all the traditional systems was that a single key was used by the sender to encrypt the message and by the receiver to decrypt it. The problem with this procedure was that a separate and secure method for communicating the key was required, before the parties could begin to use the system. A radical new approach was developed in the 1970s, based on a different way of using keys. The fundamental idea is that a typical user, let us call him Bob, has two keys, a 'public key' and a 'private key'. The public key is used to encrypt messages that other people wish to send to Bob, and the private key is used by Bob to decrypt these messages. The security of the system depends on ensuring that Bob's private key cannot be found easily, even though everyone knows his public key

The basis of **public-key cryptography** was proposed by Whitfield Diffie and Martin Hellman in 1976, but they did not set up a working system. That was done in the following year by Ronald Rivest, Adi Shamir and Leonard Adleman, and their system, known as RSA, became famous almost overnight, mainly because it was described by Martin Gardner, in one of his monthly articles in the *Scientific American*.

RSA is in fact a collection of several algorithms. The first is a procedure that enables a user (say Bob) to calculate two numerical keys. We call them his *private key* and his *public key*. Bob begins by choosing two numbers and which must be prime numbers. Then he uses and to calculate three other numbers, denoted by , and The number is just times and, although the numbers are large, we know that can be found easily by long multiplication. For the numbers and Bob must ensure that the product is congruent to modulo this too can be done quite easily. The numbers and comprise Bob's public key, and he makes them available to everyone. But is his private key, and he keeps this number secret, together with the prime numbers and that he used to define .

To complete the RSA system, two more algorithms are needed: one for encrypting messages and one for decrypting them. The input to the encryption algorithm is the original message, together with the public values of and The input to the decryption algorithm is the encrypted message, together with the private value of (and). When someone (say Alice) wishes to send Bob a message, she uses his public key to encrypt it, and Bob uses his private key to decrypt it. As a consequence of the way in which the keys have been chosen, the algorithm for decryption is the inverse of the algorithm for encryption. In other words, the decrypted message is the same as the original one.

The effectiveness of RSA depends on two things. It is efficient, because the encryption and decryption algorithms used by Alice and Bob are easy, in a technical sense that can be made precise. On the other hand, it is believed to be secure, because no one has found an easy way of decrypting the encrypted message without knowing Bob's private key. We do not have an 'easy' algorithm for calculating the private numbers and even though the public numbers and are known. Unfortunately, this is not a proven fact in mathematical terms.

When Martin Gardner first wrote about RSA in the *Scientific American*, he illustrated the strength of the system by challenging his readers to find the prime factors of a certain number with 129 digits. It took 17 years to solve this problem, using the combined efforts of over 600 people. Subsequently, cash prizes were offered for factoring other large numbers, and numbers with up to 232 digits were successfully factored. But (as far as we know) there was no breakthrough. No fundamentally new ideas were discovered, the successes being made as a result of minor improvements in strategy and the deployment of computing resources. If an easy way of solving such problems were found, there would be serious consequences.

Can mathematics keep us safe?

This question deserves to be considered in a wider context, even if the answer is inconclusive. On the evolutionary scale of billions of years, the period covered in this talk is but the blink of an eye. In a mere 5000 years mathematics has helped to transform the human condition, and it has become our best hope of understanding that condition. But we cannot overlook the fact that, in the wrong hands, mathematics can create enormous problems. In the next hundred years there will surely be progress (of the traditional kind), and mathematics will help to make it happen. On the other hand, humankind is now faced with the real possibility of extinction. Is mathematics a safeguard against extremism of all kinds, or is it a dangerous weapon? It would be good to end with a comforting reference to the lessons of history, but the lessons provide us only with hope, not certainty.