Number Story

Number Story

From Counting to Cryptography

PETER M. HIGGINS

COPERNICUS BOOKS

An Imprint of Springer Science+Business Media

Peter M. Higgins, BA, BSc, PhD
Department of Mathematical Sciences, University of Essex
Wivenhoe Park, Colchester, UK

Published in the United States by Copernicus Books,
An imprint of Springer Science+Business Media, LLC

Mathematics Subject Classification (2000): 11-01
British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Control Number: 2007936363

ISBN 978-1-84800-000-1 e-ISBN 978-1-84800-001-8

Printed on acid-free paper.

9 8 7 6 5 4 3 2 1

Springer Science+Business Media

springer.com

Preface

Numbers are unique, there is nothing like them and this book reveals something of their mysterious nature. Numbers are familiar to everyone and are our mainstay when we feel the need to bring order to chaos. In our own minds they epitomize measured rationality and are the key tool for expressing it. However, do they really exist? They certainly don't exist the way cats and football teams exist, or even the way colors and feelings exist, but more in the way that words exist. Words have meanings and the meaning of a number, what the number 'is', is about overall matchings that allow us to measure and compare things that might otherwise have little in common, such as the value of oil, of a taxi cab, and of the services of its driver.

And collectively numbers represent the one thing in the world that is free and inexhaustible. It is therefore natural to try and understand them as much as we can.

The opening chapters of this book will re-acquaint the reader with numbers, both seen as individuals and taken all together. Throughout the first four chapters, we generally stick to discussing ordinary, whole counting numbers. The fifth chapter looks at some practical issues surrounding number use that, by involving arithmetic operations, lead us out of an environment where everything is given in solid, discrete chunks.

Chapter 6 explains how it is that through carrying out the standard operations on numbers, we discover new number types, including the irrational. In the subsequent chapter we visit infinite collections and see how they can be compared to one another and how the set of real numbers as we call them knit together to form the number line, something we examine with a mathematical magnifying glass later in the book.

The historical development of Number History is, like all history, a complex thing but one that seems to have resolved itself to the extent that number systems now enjoy agreed status among mathematicians and certainly form a central pillar of our understanding of the world. Throughout the text we inform the reader of various historical snippets associated with the evolution of the subject and a little about individual number pioneers. This culminates in Chapters 9 and 10 where we summarize the development that took place in Europe during the formative period from the 16th to the end of the 19th centuries.

And we do look at direct applications of numbers, most notably in Chapter 8, which is all about chance, and again in Chapter 12 that concerns itself with the clandestine world of codes and secret ciphers, which have proved the major new field of applications of pure number ideas.

The book is written to be read straight through by any interested reader although dipping and browsing might be equally rewarding. We do however provide one final chapter, *For Connoisseurs*, in which some of the particular claims and examples in the text are worked through in mathematical language for the benefit of those readers who would appreciate complete explanation. An asterisk in the text indicates that more is said on the topic in the notes of the final chapter. This is the only chapter of the book that makes free use of mathematical notation and ideas. The level of difficulty here varies as determined by the nature of the material in question but all readers will be able to glean something from examining some of the notes at the end of the book. Finally there is a short closing section giving direction to other fine books and Web sites for you to enjoy.

I hope this little book will allow my readers to grasp something of a very big story, the Story of Numbers.

Colchester, England, 2007 Peter M Higgins

chapter 1

The First Numbers

'All is number', said Pythagoras over 2,500 years ago. By this he meant that, at its deepest level, reality is mathematical in nature and could be expressed in terms of numbers and the ratios between them. Was he right? The short answer is no, as he himself is said to have discovered.

It is true that the disciples of Pythagoras revealed how aspects of the world were governed by number. Pythagoras is best known for his celebrated theorem that explains how the lengths of the sides of a right-angled triangle are related to one another. The modern interpretation of this is that the exact distance between two points can be found from their co-ordinates. This discovery provided a tool allowing the precise calculation of spatial separation from other measurements and so represented a real breakthrough. More surprisingly perhaps, Pythagoras is said to have discovered that pure musical harmony is determined by simple ratios. Flushed with success, it must have seemed to the Pythagoreans that any aspect of the world would yield to analysis through number, for these were astonishing revelations. The clarity and simplicity

offered by the laws of Pythagoras was of a kind never previously encountered.

It came therefore as a shock when Pythagoras found that numbers themselves rebelled against his rule, for he is credited with also discovering that certain lengths constructed in his geometry were impossible to express as simple fractions the way his philosophy demanded. In particular, he found that you cannot measure the diagonal of a square with the same units with which you measure the sides. However fine you make the scale, the tip of your diagonal will always lie between two of your scale marks. This is due to the fundamental nature of numbers, and has nothing to do with limitations on the accuracy of your ruler or the sharpness of your vision. It is a mathematical fact of life. What might be dismissed by us however as an annoying curiousity was viewed as a catastrophe by the Pythagoreans, for it undermined their whole outlook by which they sought to explain nature through simple number ratios. Even from these early classical times then, there were problems with the view that everything could be reduced to numbers.

Despite their limitations however, numbers have not retreated but rather crowd into our lives relentlessly. As far back as the early 17th century, Galileo advocated as a guiding principle that we should measure everything we can and learn to measure those things we cannot. Embracing this philosophy has yielded rich results and in calling for a measurement we are being asked to produce a number.

There is however a natural resentment provoked when this seems to be taken too far. Attempts to call upon numbers as a tool for understanding music and poetry often meet with scorn. The very idea spoils the magic and it is natural to sneer at the possiblity and hope for failure. In this it still seems that we are on safe ground

as numbers rapidly begin to lose authority in the artistic realms. To be sure, music has a mathematical side to it, as Pythagoras discovered, and that aspect is well worth understanding. However, a purely analytical approach to the arts yields pretty thin results. Good music is not produced by calculations, and the more this avenue is explored the poorer the offerings produced.

Mistakes along these lines are in any case far from new. Right throughout history and across cultures we can find examples where numerical ideas are introduced in a misguided way that eventually leads to nothing of interest. To simply assert, for example, that even numbers are female and odd numbers male, or the reverse, is not helpful. Artificial attempts to make up the laws of nature have never worked and say more about the human mind than they do about the real world: simple ideas designed to appeal to our fancy may be comforting and even fun, but are rarely true.

As a backlash to the constant call for numbers and percentages, there is an agressive tendency in the arts today to reject anything to do with systematic or scientific thinking. This is a frame of mind that some great artists, Leonardo da Vinci for one, would have found puzzling. I wonder if this yearning to be released from the straitjacket of logical thinking is more born of frustration, stemming from a lack of creativity, which is blamed on the way numbers have taken over our lives. Constantly measuring things seems to be the very opposite of spontaneity, leading to a dislike of numbers that are seen as a tiresome and inhibiting burden. Perhaps the very way we think has become enslaved by the rule of numbers that acts as a limitation on us all, retarding freedom of thought and spirit.

Let me assure you nonetheless that numbers are not evil but rather are naturally interesting. The problems we may have with

them, and the destructive uses they may be put to, are of our own making. It is best on the one hand to appreciate that there are going to be limitations to their legitimate uses but, on the other, admit that it is not always easy to tell in advance where those limitations will lie. One surprising facet of numbers is the odd way they have of invading other branches of math and science, quite out of the blue. For example, until around 30 years ago no-one had any idea that the so-called trapdoor functions on which our internet security codes are based would come about through ideas about ordinary numbers, but more of that part of the story later.

Galileo (1564–1642) was right in his belief in the value of measurement[1]—perhaps we should however add the modern caveat that we should resist the temptation to pretend that we have measured something when we have not. How often, for instance, do we hear in modern life an expert say that he is 90% sure of an outcome—not 92% or 88%, but 90%. The figure lacks true meaning if there is no way of calculating it. However, we often feel obliged to produce a number even when we do not have one so we can fall into the trap of simply making them up in order to sound more authoritative. In the absence of real information, a vague statement may be correct and a precise one with a number in it merely a form of wishful thinking made in order to sound more informed and convincing in the face of uncertainty.

Most times when we meet up with numbers, we are called on to interpret them in a particular context, which might be about money, people, or the pressure of a gas. However, the subject of this book is the numbers themselves and how our understanding

1 Although a relatively minor figure, Nicholas of Cusa (1401–1464) had advocated two centuries earlier that knowledge must be based on measurement.

of them continues to evolve. It is only right that we begin by examining the kind of thoughts we have when we come across these mysterious things called numbers.

How Should We Think About Numbers?

When we mention a particular number, let us say for example, sixteen, all of us have a mental picture of the two numerals 16. This is somewhat unfair to the number in question as we are immediately stereotyping sixteen as $10 + 6$. Why should we think of sixteen as $10 + 6$ when it could equally well be described as $9 + 7$ or, more symmetrically as $8 + 8$? This habit, of course, comes from our unswerving use of the number ten as the base of our number system: our expression of a number implicitly displays it as a sum of powers of the number ten. For instance, when we write 2008 we mean $2 \times 1000 + 0 \times 100 + 0 \times 10 + 8 \times 1$. As you may know, we would be equally entitled to use another base such as twelve for our number system and different civilizations of the past did indeed use different bases: the Mayans sometimes used twenty, the Babylonians employed base sixty, while modern computing systems are based on two or small powers of two such as four, eight, and sometimes even base sixteen, which is known as *hexadecimal*. Since $16 \times 16 = 256$ we can cover that many possibilities with two symbols in base 16 (although we need to introduce new individual symbols for the six numbers normally denoted by 10, 11, 12, 13, 14, and 15). Two hexadecimal digits are all you need to represent any number in the range from 0 to 255 inclusive, a common spread used, for example, to specify colors. As we shall see in a later chapter, comparison of numbers in different bases can also be used in

subtle ways to reveal the nature of how numbers order themselves into a line.

We shall say more about this in due course but we should first ask the more fundamental question: Why do we introduce a base at all when we want to deal with numbers? You might think that there is no way of coping with number matters without referring to some base or other. However, we do just that more often than you may realize in everyday life. Suppose for example we have a childrens' party where we want to give every child a toy. All that matters is that there are at least as many toys as children and we can check this without counting: we could simply write each child's name on a toy and as long as we don't run out of toys before we have exhausted all their names, no-one will go away disappointed. In doing this we establish that the number of toys is at least as great as the number of children and we do it without counting up either collection. We do not need to know how many children or how many toys we have in order to show that the number of toys is sufficient. We therefore have solved this problem about numbers without introducing base ten or any other base to do our calculation. This example also serves to show that number is very much about pairing members of one set with another, a very important idea.

Use of a particular base does allow us however to express numbers in an efficient and uniform manner that makes it easy to compare one number to another and to perform the arithmetical operations that arise through counting. A base of a number system is akin to placing a grid scale on a map. It is not intrinsic to the object but is rather like a system of co-ordinates imposed on top as an instrument of control. Our choice of base is arbitrary in character and the exclusive use of base ten saddles us all with a blinkered

view of the set of counting numbers, $1, 2, \cdots$. Only by lifting this veil can we see numbers face-to-face for what they truly are.

Various local number systems cropped up in many cultures, but all exploited the grouping of collections into equal size lots, often of size ten. The efficacy of a base in your arithmetic only comes into its own once you introduce the *positional principle* in representing numbers where the value of a numeral depends on its place within the number string. No ancient society, not even the sophisticated Greeks, developed a complete positional numbering system such as we have where the value of a numeral depends on its position within the number and full use is made of a zero symbol to indicate that a certain power of the base is absent (recall our example of 2008). It was in the early centuries of the first millenium that such a complete numbering system came into being in India, with a symbol for 0 called *sunya*, which is the Hindi word for empty. It passed to Europe via the Arabs so that our number system is known as Hindu–Arabic.

Not having a proper positional approach to arithmetic is a real handicap for most practical purposes. Yet not being mentally trapped in a base ten world did make it easier and more natural to study numbers in their own right. The freedom the Ancients enjoyed by default we may reclaim for ourselves simply by shedding the base ten mantle for a time and thinking of numbers in terms of the intrinsic properties they may or may not enjoy.

Having emancipated ourselves in this way, we see that it is more natural to focus on the special factorization properties of a number as these correspond to appealing geometric displays. The number sixteen for example is a perfect square, naturally represented by a four-by-four square of dots, and since four is itself a square we notice that sixteen is a perfect fourth power as it is equal to

$2^4 = 2 \times 2 \times 2 \times 2$. In fact sixteen is the first number after 1 that is a perfect fourth power, making it very special indeed. This is a reason why it is often used as a base itself in computing systems, as opposed to base ten, which is the traditional base we use for the accidental reason that we have ten digits on our hands.

If we suspend the habit of thinking of numbers simply as servants of the science of measurement, and take a little time to study them without reference to anything else, much is revealed that otherwise would remain hidden. The natures of individual numbers can manifest themselves in ordered patterns in nature, like the spiral head of a sunflower, (which represents a so-called Fibonacci Number), and so are worthy of a thorough investigation in their own right. Simple questions about numbers, such as how they may be written as the sum of squares, have led to mathematical structures of great beauty and intricacy. Instinctively mathematicians will follow signposts of that kind as they often lead to very unexpected destinations that would not be stumbled upon in any other way.

For convenience I shall still write the individual numbers that I call your attention to in the usual way in base ten but we will not be emphasising that representation: rather we shall regard it more as a name for the number we are presently thinking about.

The Structure of Numbers

One of the glories of numbers is a fact so self-evident that it may easily be overlooked—they are all different. Each number has its own structure, its own character if you like and the personality of individual numbers is important. Take the number six. Six is

a product of two smaller numbers, namely two and three, and so forms what we might call a *rectangular number*: one that can be represented as a rectangular array of dots. A number n that can be written as a product of two smaller numbers, $n = a \times b$ say, can be drawn as an $a \times b$ rectangle of dots. (We normally save time and space by writing the product $a \times b$ of a pair of unspecified numbers, a and b, simply as ab.) Rectangular numbers are more often called *composite numbers* as they are composed of smaller factors. Numbers that are not rectangular in this way are known as *primes*. Prime numbers such as 2, 7, and 101 cannot be displayed as a proper rectangle but rather only as a single line of dots. In words, a number is prime if it *cannot* be written as the product of two smaller factors. (A definition that precludes 1 from joining the list of primes: the first prime is 2.) The primes are structurally important as they form the multiplicative building blocks from which all numbers can be put together: for example 60 is a composite number that is a product of prime numbers: $60 = 2 \times 2 \times 3 \times 5$. Any composite number can be broken down into a product of factors which, if not themselves prime, can be broken down further until we recover the *prime factorization* of our number. It turns out that this factorization is unique—there is only one way to factor a number as a product of primes. However you attack the factorization of your number, if you keep factoring its factors you will always end up with the same collection of prime factors. This is a crucial property of numbers that is exploited in diverse applications of the subject from coding to logic. Indeed perhaps the greatest unsolved problem in all mathematics is the Riemann Conjecture, which is intimately connected with this so called Fundamental Theorem of Arithmetic that says that the prime factorization of a number is unique.*

It is hard to over emphasise the importance of the uniqueness of prime factorization. Reading this, you may wonder at the fuss. To be sure, if prime factorization were not unique, everyone would have heard about it by now. True as that is, the following example shows that it is not the kind of thing that can be taken for granted. Consider the numbers in the sequence, $1, 5, 9, 13, 17, 21, \cdots$: that is the numbers of the form $1 + 4n$, as n takes on the successive values $0, 1, 2, 3, 4, 5, \cdots$. This collection of numbers forms a multiplicative number system in its own right in that if we multiply any two numbers from this sequence together, we remain within the sequence: for example $9 \times 17 = 153 = 1 + (4 \times 38)$. Some numbers, like 153, can be factorized into a product of other numbers in the set of numbers formed by the sequence. Some however cannot, in which case let us call the number *primal*. Ordinary primes in the sequence, such as 5 and 13 are primal, as is 9, as 9 cannot be factorized within the set ($9 = 3 \times 3$ but 3 is not in our set).

It is clear that any number in this sequence can be broken down into a product of primal numbers: we argue just as with primes for either the given number is already primal, or it is not, in which case it can be broken into smaller factors from the set that we break down further until this can be done no more and we are left with a product of primal numbers. However, primal factorization is not always unique: $693 = 21 \times 33 = 9 \times 77$, which gives two different primal factorizations of $693 = 1 + (4 \times 173)$.

The moral of the story is that uniqueness of prime factorization is special, and, although familiar, is not self-evident for here we have a similar number system in which it does not apply.

Returning to our featured number 6, we note that the property of being rectangular is hardly a remarkable one. However 6 is also a

triangular number: since $6 = 1 + 2 + 3$ it can naturally be regarded as a triangular array of six dots with one in the first row, two in the second, and three in the third. The previous triangular number is $3 = 1 + 2$ and the next is $10 = 1 + 2 + 3 + 4$. We usually allow 1 to be admitted among the list of triangular numbers as well so that the first five of them are 1, 3, 6, 10, and 15. The 10 and 15 triangles can respectively be seen in the pin array of 10-pin bowling and the 15-ball rack of red balls in snooker. Triangular numbers form a more exclusive set than the class of the very common rectangular numbers.

The number 6 is also what we might call a choice number: the number of ways of choosing a pair from a group of four children numbers six in all. If the children are Alex, Bart, Caroline, and Daniel the six pairs we may form can be listed as AB, AC, AD, BC, BD, and CD, where we are paying no regard to the order in which we list the children within a pair, meaning for example that we regard AB and BA as representing the same pair. It turns out that any triangular number is also a choice number in a similar way as the nth triangular number is also the number of ways of choosing a pair from a family of $n + 1$ objects. Again we shall explain this further in Chapter 4.

The fact that $6 = 1 + 2 + 3$ has another interpretation that occurs much more rarely in the infinity of the number system as this sum shows that 6 is the sum of all its smaller factors. The Pythagoreans called such numbers *perfect*. One should always be wary of a seductive name but on this occasion it is not misplaced: for a number to be the *sum* of its factors in this way does suggest it has a special internal balance and it is one that is indeed very rare. The next four perfect numbers are 28, 496, 8128, and 33,550,336. A lot is known about the even perfect numbers but, to this day,

no-one has been able to answer the basic question of the Ancients as to whether there are infinitely many of these special numbers, although there is a correspondence between them and a particular class of prime numbers. What is more, no-one has found an odd one, nor proved that there can be no odd perfect number. Will we ever find out?

Finally 6 has a truly unique property in that it is both the sum and product of all of its smaller factors: $6 = 1 \times 2 \times 3 = 1 + 2 + 3$ and it is also the sum and product of a sequence of consecutive numbers. There is certainly no other number like this. Indeed it is often easy enough to find peculiar properties of small numbers that characterize them—for instance 3 is the only number that is the sum of all the previous numbers while 2 is the only even prime (making it the oddest prime of all).

The nth triangular number arises from summing all the numbers from 1 up to n together. If we replace addition by multiplication in this idea we get what are known as the *factorial* numbers. The first factorial is 1, the second is $2 \times 1 = 2$, and the third, as we have already seen, is $3 \times 2 \times 1 = 6$. Factorials come up constantly in counting and enumeration problems such as the chances of being dealt a certain type of hand in a card game like poker. For that reason they have their own notation: the nth factorial is denoted by $n! = n \times (n-1) \times \cdots \times 2 \times 1$. The triangular numbers grow reasonably quickly, at about half the rate of the squares, but the factorials grow much faster and soon pass into the millions and millions: for example $10! = 3,628,800$. The exclamation mark, a notation introduced by Christian Krempe in 1808, alerts us to this rather alarming rate of growth.

It is fair to say that small numbers tend to be more special than larger ones—the closer a number is to the beginning of the number

line, the more likely it is to display some genuinely unique trait. This however is only a rule of thumb and some large and very large numbers turn out to be intrinsically special. The number 12 is an *abundant* number meaning that it is exceeded by the sum of the factors less than itself: $1 + 2 + 3 + 4 + 6 = 16$. It is rare for an odd number to be abundant and no small odd number is. However it is possible and the first example turns out to be 945. Readers might care to check for themselves that when we sum all the factors of 945 the result is the larger number 975. It is possible, if you know a bit about these things, to see this coming: $945 = 3^3 \times 5 \times 7$, a standard formula then gives that the sum of the factors, *including the original number*, will then be given by $(1 + 3 + 9 + 27)(1 + 5)(1 + 7)$ from which, upon subtracting 945, the figure of 975 results.*

Mathematicians who are intimately connected with number theory can get to know individual numbers so well that they become old friends. A famous conversation between Hardy and Ramanujan concerned the number 1729 of a taxi cab. When Hardy carelessly suggested the number was dull, the little Indian genius immediately disabused him, pointing out that 1729 was the smallest number that was the sum of two cubes in two distinct ways: $1729 = 1^3 + 12^3 = 9^3 + 10^3$.

There are numbers that are especially annoying such as 561. It behaves a lot like a prime number without being one. A basic property of a prime number p that is particularly important in coding theory is that it satisfies the Fermat Lemma which says that for any number a, a^p leaves the same remainder as does a when divided by p. For example, if we take the prime $p = 5$ and put $a = 8$ we can check that both the numbers 8 and $8^5 = 32,768$ leave the remainder 3 when divided by 5. However this is not generally

the case for composite numbers p: for example if we replace the prime 5 by the composite number $p = 4$ and put $a = 7$ we see that the remainders when 7 and $7^4 = 2401$ are divided by 4 are respectively 3 and 1 and so are not the same. It would be convenient if this property provided a test for whether or not a number p were prime but it does not. The composite numbers p that always pass this test are called the *Carmichael Numbers* and $561 = 3 \times 11 \times 17$ is the smallest of them. These numbers are rare but, coincidentally perhaps, Ramanujan's number, 1729, turns out to be another one, as is 2821. In the year 1992 it was proved nevertheless by Alford, Granville, and Pomerance that, as with the primes, Carmichael numbers continue without end so there is no way past them.

Primes are elusive in a way that some other types of numbers are not. If we want, for example, a very large square, we just write down a big number and multiply that number by itself and there we have it. However, although it has been known since before the time of Euclid (300BC) that there are infinitely many primes*, they are not so easy to generate and it seems that we need to go out hunting for them. We cannot manufacture primes the way we can with the squares—we are limited to testing one odd number after another, although there are various tricks that facilitate the endless search. On the one hand no-one has proved that it is impossible to find a way of readily generating primes at will, but on the other hand, no-one can can claim to have yet succeeded in doing so.

Primes are common enough among the first few thousand numbers but they slowly become rarer and rarer as we move into the realm of the very large. This is not surprising as a large number has potentially more possible factors than a small one. At any time in the history of mathematics, there is a largest known prime number. The current champion has over four million digits and would

take a month just to write down in ordinary base 10 notation. It can however be written as one less than a power of two: $2^{13,466,917} - 1$. Since there are always larger prime numbers waiting in the wings to be discovered, the pre-eminent status of this number is but a passing thing.[2]

However an example of an extraordinarily large number with a special status that can never be lost is

$$8080\ 17424\ 79451\ 28758\ 86459\ 90496\ 17107$$
$$57005\ 75436\ 80000\ 00000.$$

This is the size of the so-called *Monster sporadic group*. A little explanation is in order. A *group* can be thought of for our purposes as the collection of all symmetries of an object: movements such as reflections and rotations that leave a patterned object such as a square or wallpaper design looking as it did before. Mathematical groups are a topic that only emerged in the early 19th century from the study of the solutions of certain equations involving powers of orders higher than two. However they have proved strikingly pervasive, penetrating almost all of mathematics and physics: crystallography and coding are but two fields where they arise. The short explanation for this is that they give an algebraic hold on the geometric notion of symmetry, allowing us to perform calculations based around that idea.

Mathematics always searches for ways in which complicated objects are made up of smaller and simpler parts. A *simple group*

2 Indeed it has passed during the preparation of this book: at the time of writing the largest known prime is the 44th so called Mersenne prime, $2^{32,582,657} - 1$ found in 2006. The record is being broken regularly at present thanks to the international GIMPS project that has enlisted tens of thousands of enthusiasts working with their computers searching in parallel. See http://primes.utm.edu/largest.html.

is to groups what a prime number is to numbers, in that a simple group cannot be built from smaller groups, in a sense that can be made precise, but need not concern us here. There are four main sources of simple groups but, in addition to these types there are exactly 26 so-called sporadic simple groups that lie outside of the mainstream. It is now known that there are no more than these 26 exceptional groups. They are simple in the technical sense only and generally are enormous in size and complexity. The Monster is the largest of them all and was constructed in 1982 by Robert Greiss as a group of rotations of 196,883-dimensional space. The size of the Monster is the 54-digit number given above. That number is therefore special and will remain special for all time. It is a permanent feature of the mathematical landscape. The extent of its significance will only be revealed as years go by and the full story of numbers unfolds.

chapter 2

Discovering Numbers

Despite their familiarity, it should be appreciated that numbers have no physical existence but rather are abstractions elicited from the real world. Two sets are said to have the same number if the members of the sets can be paired off, one against the other, as in Seven Brides for Seven Brothers. The number of one finite set is less than that of the other if the first can be paired off with just a portion of the second, as in our example where we gave toys to the children at the party. This gives the set of counting numbers a natural ascending order. Since we all have been taught to count from childhood it is not easy to appreciate what a difficult idea counting represents. It must have been hard to realise and put into words that a pair of rabbits and a couple of days are instances of the same thing. The practical upshot of course is that the man with the rabbits has one meal for each of the next two days.

Once we have grasped the notion of number it is natural to give names to the first few of them: one, two, three, four etc are the ones

we use. If we did not go beyond this stage the process would be little different than that whereby we recite the letters of the alphabet in a particular order. The contexts are not entirely parallel however: the first twenty-six numbers have the natural order mentioned above whereas the order of the letters of the alphabet is quite arbitrary: although the *names* of our numbers could be anything we fancy, the natural ordering of the numbers is intrinsic and is not something of our making. It is the arbitrary nature of the order that we impose on the alphabet that accounts for the effort children are called on to make so as to remember the order in which letters appear in the dictionary.

What is adequate for the alphabet however is not good enough for numbers as the first set is finite—we reach the end after inventing twenty-six names, while the collection of numbers is infinite and stretches away indefinitely. What is more, in practice we need to make use of lots of numbers—any civilization will need to be able to count into the hundreds and thousands on occasion so there is a call to devise some kind of number identification that goes beyond the naive approach of creating an ever-growing list of different words for different numbers.

We can mitigate against this difficulty a little by agreeing that certain numbers are represented by a single symbol: for instance in Roman numerals X and V stand for ten and five respectively. However the fundamental problem would still remain, that being that it is impractical, indeed impossible to have a single unique symbol for every number. Sooner or later we are forced to make use of the *Addition Principle* whereby some numbers are represented as the sum of two smaller ones. For instance, in Roman numerals there is no special symbol for fifteen—we just write XV to indicate the number that results from taking a group of ten and adjoining to it a group of five.

It would seem that the discovery of the Addition Principle is a very natural one for we see it put to use in all the ancient civilizations of the Middle East, Europe, and Asia. Additions based on ten were also prevalent. As mentioned before, the ancient Bablyonians made use of both base twelve and base sixty from which come the worldwide practices of dividing the day into twenty-four hours and the full circle into 360 degrees. Another remnant of base sixty is in French where there are no new names for numbers past 60 up till 100: 70 is soixante-dix (60 and 10), 80 is quatre-vingt (four twenties), 90 is quatre-vingt-dix etc. Belgian French speakers however grew tired of this and introduced the new names septante, octante, nonante etc for these numbers. Most number systems however took up the option of grouping into tens, which allowed for the recording of fairly large numbers through use of a short string of symbols. Unfortunately the Just Good Enough Principle was generally adopted: once a way of writing numbers was invented that was adequate for day-to-day business it became completely entrenched and no effort seemed to have been made to improve further and certainly not to replace it with one that was better.

Even the mathematically sophisticated Greeks did not take basic arithmetic seriously enough to break free of a quite primitive notation. One explanation for this is that matters of accounting were considered the province of mere slaves and quite unworthy of higher study. Whatever the reason, the pattern of reckoning of the Greeks was little more advanced than in other ancient cultures. (Indeed the Babylonian system was fundamentally superior, as will be explained.) It could well have been that ancient accountants had a host of practical tricks for doing their sums—certainly they made good use of simple devices such as the abacus (counting board) and no doubt had their own idiosyncratic methods of mental arithmetic that were communicated to the next generation by

word of mouth and through example. That part of the History of Mathematics is largely lost with only accidental glimpses being available to the modern scholar.

The Greeks represented the numbers 1–9 by the first nine letters of their alphabet, and used a similar string of symbols for the multiples of ten from 10–90, while a further set of nine stood for each of the numbers 100 through to 900. For example, λ and β stood respectively for 30 and for 2 so that the number 32 was written as $\lambda\beta$. At first glance this may look as efficient as our notation but it is not. The Addition Principle is being exploited but no real use is being made of position. If we swap the digits of 32 we get the different number 23. However that does not apply to $\beta\lambda$, which could still only mean $2 + 30 = 32$. The Greek version of 23 would have been $\kappa\gamma$, as κ stood for 20, while γ was the third letter of the Greek alphabet and so could stand for 3. In this way all numbers up to one thousand can be recorded by strings of length no more than three. In the early days of the system, that might have proved fairly adequate. Before too long though, it became necessary to deal with numbers going into the thousands. Rather than start from scratch, the old system was modified in an ad hoc fashion in order to cope. It became understood that putting a comma before a symbol meant that symbol was to be multiplied by 1000 so that, for example $,\alpha$ was the representation of 1000. This must have proved good enough for practical purposes.

There were sporadic attempts to do better. In the third century AD the Greek mathematician Diophantus went one step further in using a dot to indicate that the preceding number was multiplied by a myriad (10,000). He gave the example $,\alpha\tau\lambda\alpha.\ ,\varepsilon\sigma\iota\delta$ which we accordingly translate as 13,315,214 as the number $1000 + 300 + 30 + 1$ represented by the first group of four symbols is multiplied by ten thousand because that quartet is followed by a dot, while

the latter four stand for 5000 + 200 + 10 + 4 in turn. In this way we see that it is not too difficult to adapt what might appear a clumsy system to write down numbers running into the millions. Indeed Archimedes in the 3rd century BC could boast in his book the *Sand Reckoner* that he could represent a number greater than the number of grains of sand required to fill the universe (at least the universe of the Greek World).

We might still object that this way of representing numbers would not lend to pen and paper arithmetic. However that is a very modern objection as the ancient world did not have cheap paper. Difficult sums were performed on counting frames so their method of writing numbers only had to be good enough to record the answers and the ingredients that made them up. Number notation did not need to go far beyond a shorthand for writing out numbers in words, and so it never did.

The origin of the system of Roman numerals is very obscure but was probably Etruscan, which was a civilization that pre-dated the Romans on what is now the Italian penisula. Roman numerals were indeed used by the Romans and persisted right through medieval times and survive, mainly for decorative purposes, in modern European culture. In addition to the symbols for one, five and ten mentioned above were also symbols for fifty, one hundred, five hundred and one thousand, which were respectively L, C, D, and M. That a film was made in 2003 is indicated at the end of the credits by the Roman numerals MMIII, while the year 1673 was written MDCLXXIII. Similarly to the Greek system, the Romans embellished their number symbols to indicate multiplication by a large power of ten. For example two hundred thousand and one million could be indicated by placing boxes around the symbols II and X respectively to show these quantities were to be increased by a factor of one hundred thousand.