Multiplying and dividing whole numbers: why it is more difficult than you might think

Professor Timothy Gowers FRS

22 May 2007

Introduction: Professor Robin Wilson, Gresham Professor of Geometry:

Good evenings, ladies and gentlemen. It is a great privilege and pleasure to welcome you all here today, especially those who are visiting Gresham College for the very first time. I would like to extend a very special welcome to our speaker today, Professor Tim Gowers of Trinity College, Cambridge, Rouse Ball Professor of Mathematics, and probably known to you best as a winner of the Fields Medal in Mathematics, which is awarded for exceptional performance in mathematics. It is very, very rare for anyone to get one, and we are delighted that Tim Gowers, who won the Fields Medal in 1998, is speaking to us today. So I will hand over to Tim, who is talking about multiplying and dividing whole numbers.

Professor Tim Gowers

Thank you very much. One of the occupational hazards of being a mathematician is that you occasionally have to talk to non-mathematicians who have very little idea about what it is that mathematicians do. There are various questions that come up, of which two are relevant to what I am going to talk about today. One is: how can there be such a thing as research in mathematics? When people are at school, their experience is that maths is just handed down from on high, and that is what there is, and how could one then discover more maths? Surely that is what there was, the stuff that you learnt at school, and it is difficult to see how you could develop more of that. Then, some people make a bit more of an effort and then think, well, is it just multiplying larger and larger numbers together or something like that? So you then have to take a deep breath and say, well no, it is not quite like that.

I want to give some idea of what research in maths is like, so I have decided to talk about multiplying larger and larger numbers together. But there is a slight twist of course, which is that the focus is not so much on 'Let's take some really super-big numbers and spend the next hour multiplying them together,' it is more like the general question of how to go about it. Later on, I shall talk about the companion question - if you have got a number that is a product of two other numbers multiplied together, how can you find those two numbers, so how can you factorise? That is another school topic - you are given a number and you are asked to factorise it, but again, it is a topic that gets a bit more complicated if the numbers get bigger, and there are good reasons for being interested in that question, which I will come to later on.

But just to get warmed up, let us actually do a bit of multiplication, and just to prove that I have not cheated, I am going to ask for somebody in the audience, anybody who feels like it, to suggest to me a four-digit number, and then someone else to suggest another four-digit number, and we will multiply them together and just remind ourselves how the process works.

[Audience Member - 5079]

5079. Yes, another volunteer over there?

[Audience Member - 3636]

3636, right. I am curious. Looking around, I should think the average age in this audience is such that most people here probably did at some stage in their lives learn how to do long multiplication before the age of calculators and so on. For the younger people in the audience, I am just curious to know, do they teach long multiplication in schools, or is it just a ridiculous thing because, when you have got two numbers like that, you can just plug them in your calculator, or would you know in principle how to multiply them together? You would? Okay, I am very glad to hear that it is still being taught! So let's just quickly do it then...

What do you do? Let's take 9 times 3636, and then we will do 7 times 3636, then we will do nought times 3636, and 5 times 3636.

Let us take a more general number. I am making life harder for myself rather than easier. So let us have 36-something else? 94 okay. So we are not going to do it the other way, because we are not going to have any special properties. All right, 5079 times 3694.

So let's do 9 times 3694... 9 fours are 36, so I carry a 3; 9 nines are 81, so that's 84, carry 8; 9 sixes 54, so that's 62; 9 threes are 27, 33. If anyone spots me making a mistake, please shout!

7 fours, if I put a zero there, 7 fours, 28; 7 nines 63, so that's 65; 7 sixes are 42, plus 6 is 48; 7 threes are 21, plus the 4, is 25.

Now I can do a nice easy one - put 2 noughts, and then some more noughts, and then 5 3694. Well, I could divide it by 2 or something instead, but let's just this... First of all 3 noughts. Five fours are 20; five 9s are 45, plus the 2 is 7; 5 sixes are 30, plus the 4, is 34; 5 threes are 15, plus the 3 is 18, and then we have a nice last stage when we add all this up together...

6; 4 and 8, 12; 2 and 5 is 7, plus 1; 3 and 8 is 11; 3 and 5, that's 8, plus 7, 15, and then I carried a one, so it's 16; 7. 18761826 - slightly surprised that it came out in that nice form.

Now, I am going to get this calculation in a minute, but I want the answer, so let's just write it slightly smaller up here - 18761826. Actually, I think the talk should perhaps have been given a different title, which is 'Why it's easier than you think' because actually what I am going to focus on to start with is better methods, that take less long, of multiplying numbers together, but the sense in which it is more difficult is that there is more to say about the whole question of multiplying large number than you might think, the general theory of it.

Now, there is a nice trick - but, before we go to the nice trick, let's just think about what we were doing here and why it works. This is something that may be taught a little bit less at schools but not not at all I hope - that was a deliberate two 'nots' there; I hope it is taught somewhat. But let us just think a little bit about why this method works, because that will help later on.

The idea is that 5079 we think of as 5 thousand, plus nought hundred, which I had perhaps better not worry about here. In a way, I also tempted to cheat and change that nought into something else just to be a bit more general, but let us not worry. So plus 70, plus 9, times 3694. In order to work that out, you say, well, it is 9 times 3694; plus 70 times 3694; plus 5000 times 3694. Then you use the rule that, say you want to work out 70 times 3694, you work out 7 times 3694 and stick a nought on the end. So that is what we did: we had the 3 numbers - 9 times 3694, and then 70 or 7 times 3994, shifted by one, with a nought on the end; and 5 times 3694, shifted with 3 noughts on the end. That is basically why the method works, so we reduce the calculation to multiplying this number by single digit numbers, and then putting noughts on the end, and then there is a bit of addition at the end, but addition is somehow easy and a relief after you have done the multiplication, so that stage we do not worry about so much.

I am beginning to regret more and more that that was not more than a zero, but I think I will press on with the numbers that I was given! It was 3694, so let's split that up as well in the same way, and then I can illustrate a different method that is also quite nice.

Now I have split up both numbers, and a different way of organising what is basically the same calculation, but it is a better way of organising it, is to say, if you want to multiply these things together, then you have got to do 5,000 times this, and 5,000 times this, and 5,000 times this, and 5,000 time this; and 70 times this, and 70 times this, and 70 times this, and 70 times this; and 9 times this, and 9 times this, and 9 times this, and 9 times this.

One idea that you can do when you do that process is to think let's connect together all the various sums that are going to have a particular number of zeros on at the end. I will do that very systematically.

How can I multiply one of these numbers by one of these numbers and not get a single zero on the end? It's going to have to be just a 9 times a 4, because everything else involves zero. So I've got the 9 times 4 term, which gives me 36.

Now, how many things are going to end up with one zero on the end? Well, there will be 70 times 4, and 9 times 90. Let us not worry about the 70, but think of it as 7, and a 9 here, and then put a nought on at the end. So I put a nought on, and I have got 7 fours, that is 28, plus 9 nines is 81, and 81 plus 28 is 109. So I will put 109 there. That is the one zero contribution.

How do I get two zeros? Well, if there were a hundreds term here, there would be 3 ways: I would have the hundred thing times the 4; the 70 times a 90; and a 9 times 600. As it happens, we are lucky, so to speak, that there isn't a hundreds term there, so we have just got two ways of getting two zeros, and they are: 9 times 600, and 90 times 70. Forgetting the two zeros part, you get 54, that is 9 times 6, 54 plus 63, and 54 plus 63 is 117. So I have got two zeros and a 117. So that is two zeros.

How do I get three zeros? Well, I can get it with 5 times 4 - I will write something down now, - that's 5 times 4. One zero here would have to go with two zeros, which it cannot. Two zeros with one zeros, so 6 times 7, that's a 42; and finally, 9 times 3, which is 27, so that is 89. Nearly there.

Four zeros, how do I get four zeros? I could have one with three, that is 45, or three with one, that is the 21. 45 plus 21 is 66.

Five zeros, could only happen if I had got 5,000 times 600, so that is 30 plus five zeros, by which I really mean 30 times five zeros - well, 30 times one...

Last of all, how do I get six zeros? I have to 5,000 times 3,000, so I get 15 with six zeros on the end. Let us put that, 15000000. Well, I was instructed not to write too far down on the whiteboard - I am sorry about that, but the calculation just pulled me down there, but most of the time, I will try to avoid that.

Let us now add all this together and just write the answer up here. I have got a 6 there. An advantage of doing it this way, you will notice there are an awful lot of zeros here. The numbers that come up, if one thinks about it, cannot be all that big, and so the addition part is actually easier than the addition part in the other method.

So we get 6; and then we get 3 plus 9 is 12, carry one; 7, that's 8, one nought on, plus 9, is 11, so that's a 1 carry 1; so it's 2, 3, plus 9, is 12; 2 plus 8 is 10, plus 6 is 16; 6 gives you 7, 1876... what is that 2 doing there?! That is very curious? How many digits? One, two, three, four, five, six, seven, eight, and I have got a nine digit number there, so I must have done something very, very stupid... I must have done something stupid round about here... One plus one, that's 11 - oh yes, just cross that out! So 11, one plus one is 10, 18, 26. I just wrote a 2 for no reason at all I think!

Anyway, it is quite reassuring-ish that we have got the same number that we had before! After a little fudge factor, we got the same number that we had by the previous method.

What I want to talk about now is to talk about a method of multiplying 2 numbers that is a lot faster than this, if the numbers are huge. If the numbers are too small, like 4 digits, then just the brain ache you get from thinking about the method is not worth it - you might as well just do it the stupid way. It takes slightly longer, but at least you did not have to use your brain. But if you have got 2 numbers that are 1,000 digits long or something, and you can save 25% on the time that it takes, or in fact a lot more, but even a small saving on the time is really worth it, especially if, as sometimes happens, you are running a computer programme for which it is important to be able to multiply large numbers together quickly.

Perhaps I should say is that one reason, that is a good reason, for being interested, quite a lot of what I am talking about is so-called public key cryptography, which is the method that is used these days for doing things like encrypting your credit card details so that somebody else cannot steal them. That involves a certain amount of number theory - the branch of maths that is involved with things like prime numbers and factorising and that kind of thing - and in order to get this system to work, you will be dealing with large numbers and you will need to be able to multiply them together in a hurry. So any speeding up of your basic method of multiplying large numbers converts into a much quicker way of encrypting your credit card details, and a small saving in time if you are a company that is encrypting millions of credit card details every day really makes a huge difference. So this is not just to show that you can actually do it more quickly; I am actually going to talk about a method that really is used in real life and it is rather important.

Let us imagine ourselves with 2 absolutely huge numbers: 2 thousand-digit numbers. Let's just give ourselves a crude idea of roughly how many little operations, i.e. multiplying one-digit numbers or adding one-digit numbers, we will need to do, if we want to multiply 2 1,000-digit numbers together.

At the very least, if you think about the first method, let is just imagine we have got number one laid out like that, and number 2 laid out like that. What happened with the first method? Well, we took the last digit of this number and multiplied it by this. If this had 1,000 digits, we would have to do about 1,000 steps as we went through multiplying by a one-digit number. So about 1,000 steps, and then we have dealt with the last digit of this number. Another 1,000 steps, and we would have dealt with the second last digit of this number; another 1,000... We get 1,000 times 1,000, so ordinary long multiplication takes round about a million steps. It is not much fun doing a million calculations of that kind, so it would be quite nice if we could find a quicker way.

What about the second method, does that actually help us? Well, with the second method, we still had to compare every single digit of this number with every single digit of this number. We connected them together in a clever way, but we nevertheless had to do one multiplication for every digit you could choose here and every digit you could choose here, and there are 1,000 ways of choosing a digit here, 1,000 ways of choosing a digit here, so at least 1,000 times 1,000 operations are necessary, so again, you need at least a million operations. I am not saying precisely what I mean by an operation, but I hope you get some idea that the number of steps is around a million if you use either of those two methods.

You might think, well, what else could you do? This is an example of what makes mathematical research so interesting. You look at a problem like that and you think surely there isn't anything else you could do, and then you discover that somebody has actually come up, somewhere in the world, with an incredibly clever method that actually improves on this one million. There are varying degrees of cleverness that you can go in for, and one of the simpler ones is easy enough to explain. I do not know what your backgrounds are - probably varying quite a lot - but I think if you have done a bit of long multiplication, I hope you will be able to follow what I am going to say next.

The idea is to use what mathematicians like to call a divide and conquer strategy. Here is what we will do... I will draw a different picture of the 2 numbers.

We have got one 1,000 digit here, and I am just going to split it up into its first 500 digits, which I will call Number A, so that is a 500 digit number, and it is followed by its next 500 digit number, and I will just designate that B. So B represents the last 500 digits, and A represents what happens if you subtract B and divide by 10 to the 500. Then the other number we just think of as C times - not C times D, but C times one followed by lots of noughts plus D.

So there are our 2 numbers. We will do a long multiplication type process to this lot of 4 numbers. Let us first of all look at the contribution that has no zeros on the end, and that will be B times D. So I have got a B, D here, let's write B times D.

Now I am going to have a contribution that has got 500 zeros on the end, and that will be A followed by 500 zeros times the D, or else the B times the C followed by 500 zeros, and if I multiply those numbers together, I will get... A times D, plus B times C, followed by 500 noughts.

Then the third thing I will do is something which is followed by 1,000 nought, and that is if I multiply the A part and the C part, so A with lots of noughts and C with lots of noughts, gives me A times C, followed by 1,000 noughts.

Then we will just add these numbers together. We will add B times D, which is a number that is one 500-digit number times another 500-digit number; and we will have AD plus BC, that is some 500-digit numbers multiplied together with 500 noughts on the end; and A times C with 1,000 noughts on the end. So this is rather like long multiplication, except that instead of splitting the numbers into 1,000 little blocks of one-digit each, I am just splitting them into 2 blocks of 500 digits each, but it is the same idea behind the procedure for multiplying them together.

What this has told us so far is that, if I can work out A times C, A times D, B times C, and B times D, then we will be in good shape. Now, to multiply 2 1,000-digit numbers together, it took roughly the square of this number operations - I had one digit from each number, so that took about a million, which was 1,000 squared, and the same argument works for 500. So if I want to work out B times D, it's going to be about 500 times 500 operations, and 500 times 500 is 250,000, so it will take me 250,000 operations to work out B times D; 250,000 operations to work out A times D; 250,000 operations to work out B times C; 250,000 operations to work out A times C - 250,000 times 5, equals one million.

Most people would look at that and think, well, that was a nice idea, but it does not get us anywhere, and go off and have a cup of tea or something, but mathematicians have this stupid habit of thinking, well... do I really have to give up at this point? Let's just have a look at this thing. I really do not need to work out all 4 numbers - A times C, B times D, A times D, and B times C. What I really need is A times C, B times D, and those two added together. I do not care what these two numbers were themselves, I just need to know what they are added together. Then the following bright idea can occur to one?

I am going to go a bit more algebraic and use the notation BD for B times D, because it makes things a little bit more convenient. I have got 4 numbers - A, B, C and D - and I want to know the numbers AC, AD plus BC, and BD. I like adding and subtracting because, compared with multiplication, they are much, much easier, and I really hate multiplying - I want to do as few multiplications as possible. So the obvious way of doing it will involve 4 different multiplications and one addition, so can we do better than that? The answer is yes.

Of course the answer is yes, or I wouldn't have gone on like this! Right, so, how do we do it?

What we will do is a little trick, which is we work out what is A plus B times C plus D. Before I go any further, just notice, to work out A plus B, you just have to do an addition, and addition is sort of cheap, easy operation; same with C plus D.

A and B have 500 digits each, so how many digits has A plus B got? Either 500 or 501, so not much larger than A itself, so we don't have to worry that this number will suddenly become much, much bigger or anything like that. It has got roughly the same number of digits as A and B themselves.

This is a nice easy multiplication to do, and what does it tell us, with a bit of algebra here, which incidentally is just the same as long multiplication in a sense - we work out A times C, then A times D, and B times C, and B times D - so we get AC plus AD plus BC plus BD. So with just one multiplication, we have got that.

This was the thing we did not want to do, so let's just forget that one for a moment. We would like to know AD plus BC, but let's - supposing instead we just do 3 multiplications, and we do A times C, B times D, and A plus B times C plus D.

Once we do that, if we subtract the AC and the BD from this answer, what do we get? AD plus BC, which is precisely the third number that we wanted to calculate.

So how many multiplications have we done? Just three - A times C, B times D, and A plus B times C plus D - and then a little bit of addition and subtraction afterwards. How many operations did that take us? Well, each one was 250,000, because these are about 500-digit numbers, so the total is not 4 times 250,000, but 3 times 250,000, which equals 750,000. So instead of a million operations, we manage with three-quarters of a million operations! Of course, at this point, I think even a non-mathematician will think, well, perhaps we should not stop there? We have a little clever idea for multiplying large numbers together - can anyone see what to do? I expect a few people can.

We just do it again, but when we work out A times C, and B times D, and A plus B times C plus D, don't do it by long multiplication and take 250,000 operations, do it by this clever method, and instead of taking - basically, each time you apply the clever method, you save yourself 25% on the time that you took before. So you save yourself 25%, but for goodness sake, when you are doing these calculations, save 25% on those as well, and then your total saving is 25% followed by another 25%, which give you three-quarters times three-quarters, which equals nine-sixteenths, and nine-sixteenths is not much over a half. So now, if we apply this clever idea twice, we actually have now taken only half the amount of time that we would have taken before... but of course we do not have to stop there. We have got 250-digit numbers, so we can do it more and more times.

Just to give a rough estimate, how many times can we keep dividing the length of our numbers by 2? Well, if they started off as 1,000-digit numbers, that's about 2 to the 10, so maybe about 10 times you can halve the length of your numbers, and each time you do it twice, you sort of roughly halve the length of the calculation, so you can halve the length of the calculation about 5 times. I am being slightly generous to myself here? So you can divide the length of the calculation by about 32, which takes you from a million down to more like 30,000, or let us say 40,000 because I cheated slightly in my very rough estimates. Now, you have to agree, even if 750,000 is not much better than a million, 40,000 really is going to take your computer a lot less time than a million.

It turns out that that is not the end of the story. I want to discuss a little bit more of an advanced idea. I am not going to discuss it in an advanced way at all, but there is an idea that leads to a saving that is so good that multiplying 2 very large numbers, say 2 n-digit numbers, is almost like multiplying one n-digit number by just one very small number. So in the case of 2 1,000-digit numbers, it is like reducing the problem to something about as difficult as multiplying a 1,000 digit number by, say, a 6-digit number or something like that, which is a really remarkable saving on what you would do if you just applied ordinary long multiplication, the sort of thing that, until you've seen how it is done, you would think could not be possible, but it is.

I am going to discuss a concept that is very important in many parts of mathematics, called 'convolutions'. It is a rather alarming word perhaps, but the concept is not very difficult, and it is connected with how you multiply polynomials together, and that is very much what we were doing when we did the second method of long multiplication. So if you do not like Xs, imagine that this x is 10, and this A and B are some numbers. Let me just remind you what the idea is that I am talking about, and that this will be generalising.

If I wanted to multiply 35 by 46, I would take the 3 times the 4 and put 2 noughts, because that is 10 squared, and then the 3 times 6 and the 5 times 4 would be just a 10 to the one, which would be a sort of x, and the 5 times 6 would give me a 30, with nothing on the end.

Similarly, in general, when you multiply AX plus B times CX plus D and you connect according to the power of X, so when X squared comes from the A and the C, so we get A times C times X squared. The X comes from the A times a D and a B times a C - that is just AD plus BC. The constant term, or the X to the nought term, which equals one, is just the B times the D and you get a BD.

I am going to just generalise this more and more. This is something that maybe, if you have not done it a few times, you think... eh, I don't want to do that one! X squared plus BX plus C times EX squared plus DX plus F... but once you have done one of these, you suddenly get the general pattern and that is what I want to get across.

The general pattern here is very similar to what we had with the second method of long multiplication. We have power of X to the 4, which can only come from an X squared on an X squared, so we have A times E - that's what I've written here. X cubed can come from pairing this term with this term, or this term with this term, so that gives me AD plus BE, and there is my X cubed. Then the X squared term comes from A with F, B with D, or C with E - there it is, down there - and the X term comes from either B with F, or C with D, and the X to the nought term is just C times F.

You can see the general pattern emerging. You have the 2 brackets. You fix the power you want, and you sort of do that term with that term, that term with that term, that term with that term, that term with that term, that term with that term, that term with that term... until you reach the end of one of your brackets, and then you have got the relevant term.

The problem that arises a lot in mathematics is getting notation for things. How are we going to notate what happens in general?

It is fine with this, and fine with X squared, and with X cubed, I could have AX cubed - I could ABCD and EFGH in the other bracket. After a while, I start to run out of letters. What if I want to talk about a general polynomial that might have degree N for some positive number N and I'm not telling you what the N is... How do I notate that?

Eventually, you just have to give up. You cannot use letters of the alphabet any more, or you can't N different letters of the alphabet, especially if you don't know what N is, so you just have one name, but you put a little number by it, so the coefficients, as they are called, the numbers that were A, B, C and D, are now called AN, AN minus1, all the way down to A1 A0, and BN, BN minus 1, down to B nought, and you have to think of those as just any old numbers that you put in front of X to the N, X to the N minus 1. Because we have run out of names, we have to have this system for naming them.

Then what is the coefficient of the X to the 2N? Well, that can only come by pairing AN with BN, so we get AN with BN. Then you get AN with BN minus 1, and AN minus 1 with BN... Again, I hope you can sort of see the pattern emerging. Each time I go along one of these rows, this number goes from N, N minus one, N minus 2, and then the other one goes upwards - N minus 2, N minus one, N.

Similarly, here, this goes N, N minus one, N minus 2, M minus 3, and this one goes up from N minus 3, N minus 2, N minus one, up to N.

The middle term starts with AN and B0, and then AN minus one and B1, and you go all the way down and you get to A1BN minus 1, A0, BN, etc. etc. right down to the last one. That is not quite the last one - the last one has slipped off the bottom. There, the very last one is A0 B0 - can that be seen? Yes, there it is - A0 B0.

Even if you did not follow the justification for that, just take it from me that here are 2N minus one I think different numbers, and if you can work out all these numbers, then you can work out the product of this expression with this expression, and if X is 10, then these could represent just numbers that you want to multiply together.

The process that takes the sequence of numbers A0 to AN and B0 to BN to this bunch of numbers is called convolution, and it just comes up all the time because multiplying polynomials comes up a lot of the time as well.

The details are not so important - the general message is there is a thing called convolution. It is what you do when you do long multiplication by the second method. If you know how to do convolutions quickly, you know how to do multiplication quickly.

But the trouble with convolution is, as you have just seen, it is a little bit of a complicated operation. You have got these funny numbers - taking this times this, plus this times this, plus this times this, plus this times this, plus this times this, and it is all a bit of a complicated, not very pleasant looking thing. Wouldn't it be nice if instead we did something called point wise multiplication were, if you had your 2 sequences, you just took A0 times the corresponding B0, and A1 times the corresponding B1? If you did that, then you could make the mistake that many, many generations of school children have made, and multiply 3X plus 5 times 2X plus 7, where we multiply the 3 by the 2 and we get 6X, and the 5 by the 7 and we get 35, and so that is the answer. It is the sort of the thing my children would say and then they say 'not' at the end! It's a generational thing.

Or the alternative would be, to be really ingenious and say 6X squared plus 35, so we multiply the 3X by the 2X and get 6X squared, and the 5 by the 7 and get 35, and never stop to think, well, if we had swapped the 2X with the 7, would we then have multiplied the 3X by the 7 and the 5 by... and things like that. Those sorts of questions do not occur to everybody, unfortunately.

But nevertheless, we have this lament that convolution was a rather horrible complicated thing, whereas point wise, or point by point multiplication is a lovely, easy thing to do, and it is a terrible shame that when you are multiplying numbers, you have to do this convolution thing instead of point wise multiplication.

This is where a piece of mathematical magic comes into play, something called Fourier transforms. Fourier transforms have the wonderful property that they turn convolutions into point wise multiplication. Just to say a little bit more about what that means. There is something called the Fourier transform - that is the bit that I am really not going to explain, but it takes a sequence of numbers, and you put it into a sort of little machine, it chugs away, and produces a new sequence of numbers. That new sequence of numbers you traditionally stick a hat on the old sequence of numbers and that is what you've got when you have done the Fourier transform.

The Fourier transform has the wonderful property, as I have just said, that convolutions turn into point wise multiplications. What do I mean by that? I mean that this diagram, well... I will try and stop myself saying this diagram commutes, but that is what I really want to say, for professional mathematicians... but what it means is, if I do a convolution of two original sequences, and I look at what happens to their Fourier transforms, I find that their Fourier transforms just do a point wise multiplication.

Or to put it another way, if I take my two original sequences, I have two choices about what I could do. Either I can work out their convolution directly, and that was that really horrible, unpleasant thing; or I can put them into the Fourier transform machine and find 2 new sequences, and those ones, I just have to do a nice easy point wise multiplication, and then they have to sort of go backwards through the machine, and when you put them back, you will get back to your original - convolution of your original 2 sequences. So the point wise product, over here, turns into, when you do an inverse - so this machine has a property you can put things in this way and it turns things into their Fourier transforms, and then you can put them in this way, and it takes the Fourier transform and gives you back the original sequence. It is a bit like logs actually - have you done logs? There is a sort of logarithm machine. If you don't like multiplying, stick them in a log machine, add, and then push them backwards through the log machine, and you get the product. Fourier transform is like a super-sophisticated machine that, instead of turning addition into multiplication or multiplication into addition, turns convolution into this simple point wise multiplication.

So as long as you know how to work out the Fourier transform, then you have got a nice, easy way of convolving. You take the Fourier transform, you do the point wise product, and you do the inverse Fourier transform. That raises one very obvious question - is the Fourier transform something that is easy to work out? If the Fourier transform is very hard to work out, then this is not going to be an extremely good method for working out convolutions. Then there is another miracle; something called the fast Fourier transform, and as its name suggests, it is something that can be done rather quickly. So if you put all those ideas together, the fact that long multiplication, what it is really asking is that you should be able to do a convolution, and that convolutions are made much easier if you can take Fourier transforms, and that

Fourier transforms can be done really surprisingly quickly, you put all that together - there is some quite serious mathematical theory going into that - and it ends up telling you that you can do much, much more quick - you can multiply numbers much, much more quickly than long multiplication - not just a bit more quickly. This trick certainly saves quite a lot. Using the fast Fourier transform, you could get it down from - so, here we got down from a million to whatever it was, about 40,000. Using fast Fourier transform, we might get down to more like 2,000 or 3,000 or something like that, so you get a really huge saving.

Here we have an example of a typical open problem in mathematics. I have not told you enough for you to be able to go away and think about it or anything, but the question is, could we do even better than the fast Fourier transform method? The answer is nobody knows, and it is one of those things where, not only does nobody know a better method, but the answer might be no. There might not be any better method than that, and nobody has the faintest idea how you would show that you cannot do better than some method. How would you show that some clever person could not come along and do an even better method? Somehow, that belongs to a branch of maths called complexity theory. It is the problem in general of trying to show that certain problems cannot be done easily, say by a computer, and the problems of complexity theory really are very, very hard indeed.

Now, I am going to come to the second part, where we talk about dividing or factorising numbers. So that is all I have to say about multiplication. It is harder than you think in that the theory that goes into it is harder than you think, but it is easier than you think in that it does not take as long as you think if you use that theory. The Fourier transform really has revolutionised a lot of algorithms that are used in the real world.

Let us take a number like, say, 437, and think about the question of whether it is a prime number or not. This is a very, very traditional school exercise - what do we do? We say, well, does 2 go into it? No. Does 3 go into it? Well, let us add the digits... we get 14, and 14 is not a multiple of 3, so 3 does not go into it. Does 5 go into it? No, because it ends in a 7. Does 7 go into it? No, because if I subtract 7, I get 430 and 7 goes into 420, so it obviously does not go into 430. Does 9 go into it? No, because 3 didn't go into it. We only have to look at prime numbers here. Does 11 go into 437? Well, you may know a little test, that if the odd digits add up to the same as the even digits... something like that ... 11 doesn't go into it. In fact, 11 goes into 440, so it obviously doesn't go into 437. Does 13 go into it? Well, let's add 13 to this, and we'll get 450, and does 13 go into 450? No, because it is 2 times 5 times 9 times... another 5 or something, so 13 doesn't go into it. This is getting slightly dull, but we know that if this is going to be factorisable, we will have to reach a factor by the time we get to the square root of 437, which is around about 20, because then the number that you are trying to go into it will overtake the number that it would have to multiply by and so we would have already checked it. So let us just press on a little bit longer. 13 doesn't, what about 17? Well, if I subtract 17, I get 420, and 17 doesn't go into 420, because that's 10 times 6 times 7. How about 19, well, 3 nines are 57, and if I subtract 57 from 430, I get 380, does 19 go into 380? Yes, it does. It is 20 nineteens, so this is actually 23 times 19.

Imagine we have got a 1,000-digit number, and we would like to decide whether that is a prime number. Try to think how long it might take.

If we do not want to keep tabs as we are going along of every single number and whether it is prime or not, which is going to make us take even longer, it is probably better just to see whether one goes into it, 2 goes into it, 3 goes into, 4 goes into it, 5 goes into it, and so on. This has 1,000 digits, so we know that by the time we have tested all the numbers up to 10 to the 500 or so, and whether they go into this number, we will be all right. Not much fun testing whether a number goes into a 1,000-digit number when that number itself has something like 500-digits! But let us just be very, very generous to ourselves, and suppose that you could do, on your cleverly programmed computer, which you certainly could not actually, a million such tests every second - so a million numbers, you can test whether you can go into this 1,000-digit number every single second.

Write that million down. Let's be very generous and suppose there are 100 seconds per minute, and 100 minutes per hour, and 100 hours per day, and 1,000 days per year... so that is how many operations you could do every single year. How many noughts have I got? Fifteen... so I have got 10 to the 15 - I manage to do 10 to the 15 tests per year. How many years do I need? Well, if you are up with what 10 to the 500 actually means, you will find the answer is 10 to the 485 years, and when you have done that, you have worked out whether that number is a prime or not! As you can see, the drawback with that is it really is a terribly bad method to use.

I think this is a case where it is even more remarkable that there are fast ways of deciding whether a number is a prime or not, and I'm going to give some slight idea of how that is done and some slight idea - actually, the other thing about this, if you have got a number that is given to you and it happens to be a product of 2 very large numbers, can you find what those 2 large numbers are? That is something where there are methods that are cleverer and quicker than just pure trial and error, but not that much cleverer and quicker, and it is because nobody has found really good methods for that problem - so I will just say again what the problem is: it is the problem you're given a number that's a product of 2 very large, say, prime numbers, and you have to find what those 2 prime numbers were. There are not really good quick methods for that. If there were, you would have to start worrying about credit card transactions on the internet. In a way, it is good news that factorisation is hard, but that should raise a little paradoxical thought. I have just told you that it is very hard to decide what the factors of a number are, but not so hard to decide whether a number is prime. So that must mean, if what I have just said is not rubbish, that sometimes you can tell that a number is not prime, even though you cannot say what the factors are, because if it was difficult to say what the factors are, but easy to say whether it has got some factors, it must mean that there are ways of saying that a number has some factors without actually telling you what the factors are. That's a remarkable fact - again, totally unexpected if you're not a research mathematician, where you sort of get used to surprising things happening! I will give some indication of how that could possibly be the case. It looks as though it cannot be the case, but it can.

Just think a little bit about a very, very quick discussion of factorisation. I said there are not any really good methods of factorisation, but there are at least some tricks that work sometimes, and here is one of them.

Let us take a number 6351. I wanted a bigger one actually - let's not go for 6351. No, I will stick with that - sorry, it's fine. Does it divide by 3? What have I done? Oh yes, okay! Let's go for another one then! Okay, I'm not going to be defeated by this... so let's go for 8051. We have a little clue, that I first of all went for 6351 and now I have decided, no, I won't do 6351, I will do 8051 instead. That gives a slight clue about how one might go about factorising this.

Well, I have not got time to wait for somebody to have a brainwave, so I am going to do something which I really hate doing, which is just leap straight to the answer.

What happens if you add one to 63? You get 64. If you add one to 80, you get 81. What do numbers 64 and 81 have in common? They are squares. 8051 equals - this is the little trick - 8100 minus 49, and 8100 is a perfect square, and 49 is a perfect square, so we can write this as 90 squared minus 7 squared, and that is 90 plus 7 times 90 minus 7, another thing that I hope everyone under the age of 18 absolutely has at their fingertips! That is 83 times 97. That is a much better choice, because 83 and 97 are prime numbers, and that is what I meant to do in the first place, but instead I went for 73 times 87, and 87 is divisible by 3 - that was my stupid mistake.

That way, it is rather a nice way in fact of coming up with really huge numbers that you can factorise quite quickly, and it also gives an idea of a general method for searching for factors that is a little bit more systematic in a way than just pure trial and error. What you could do is you could say, well, let's just see if I can find some small square that I can add to this to get a big square. In this case, I thought I could try one, 8052 - is that a square? Not really. What about adding 4? 8055 - no. Then I keep going and I get to 49 -

if I add 49 to this, I get 8100. Oh yes, that is a nice perfect square. Had I had that method in mind, I could have not bored you with the factorisation of 437, because if I add 4 to it, I get 441, which is 21 squared, and so this is 21 plus 2 times 21 minus 2, and there it is for you - 21 plus 2 times 21 minus 2.

The problem with this method is there is absolutely no guarantee with the number you started with that when you start adding some small squares, you will suddenly hit upon a nice big square. Why should that ever happen? Actually it will happen, if the number can be factorised, but the problem's not whether it will happen or not, it is just that it might take such a long time to happen that you would be trying so many things that it would not be any better than the trial and error thing that you were trying to avoid. All I will say about this is there is a cleverer method that starts with this basic idea and develops it a bit more. As I said before, mathematicians have this ridiculous thing of just not giving up when they seem to reach the end of the road, just trying to push and push and push and push, and people have pushed and pushed in this instance and got a method that, if I spent the whole hour, I could have explained that method, but I have got other things that I want to talk about.

In fact, in my final five minutes, I want to go back to this question that I raised a moment ago, of how it could ever be possible to prove that a number was not prime without showing that it was a product of two smaller numbers.

It is based on something called modular arithmetic or, to give it its more friendly name, clock arithmetic. Clock arithmetic is the sort of arithmetic we all do. If it is 10 o'clock, then what time will it be in 7 hours? It will be 5 o'clock, because we visualise a clock, and we go 2 and that gets you to nought, and then the other 5 hours get you to five. So every time you pass 12, you are back to zero again. This is not a normal clock. This is a clock with 13 hours instead of 12. That is because, for various reasons, prime number clocks are much more useful and significant in mathematics than numbers like 12 that are composite, because they can be built up out of twos and threes and things. But just to get the feel of clock arithmetic, let's do some.

So what is 3 plus 4? It is 7. What's 9 plus 10? It is 6 of course. What does that mean? It means if it is 9 o'clock, and there are 13 hours in the day, then 10 hours later, it will be 6 o'clock, and 10 hours later, it will be same as minus 3 hours later because there are 13 hours in the day, and that's why adding 10 is the same as subtracting 3 and we get to 6. Similarly, 12 plus 3 - we can look at the picture for that one - 12, goes to nought, to one, to 2. In a normal clock, if you were doing it with clock arithmetic, the convention would be instead of writing 12, you would write nought. Here, instead of writing 13, I have written nought.

You do not just add, you can also multiply. What does 5 times 5 mean? It means, well, I do 5 five times, so I go round 5 hours to 5, another five hours to 10, another five hours to 2, 5 hours to 7, and 5 hours to 12, and 5 times 5 is indeed 12. Another way of working out 5 times 5 and getting 12 is to say 5 times 5 is 25, and then when you subtract off 13 from 25, you get 12. So 5 times 5 goes... 25, and how do you get to 25? You go once round, and then another 12, and that gets you to that 12, so that is another justification for the statement that 5 times 5 is 12.

7 times 10? Well, it starts to get a bit boring to go 7, then another 7, and another 7, 10 times, so there, it is quicker to say, well, 7 times 10 is 70 in normal arithmetic. In clock arithmetic, what you do is you divide by 13 and take the remainder. Thirteens into 70, they go into 65 and leave a remainder of 5, and there we are, 7 times 10 equals 5 - that is the remainder when you divide 7 times 10 by 13.

Next is a thing called Fermat's Little Theorem, not to be confused with Fermat's Last Theorem, which is the famous result that was solved a few years ago. Fermat's Little Theorem has been known for centuries. It says that if you take a prime number clock and raise some non-zero number to a power, you get one.

Let us just illustrate that with a clock of size 5, say, so you have got 5 hours a day. Let's take 3 - so I am saying P equals 5, and A equals 3. So I have got to work out A to the P minus one, so that is 3 to the 5 minus one, that is 3 to the 4, and I have got 5 hours a day, so 3 to the 4 is 81. What is the remainder when you divide 81 by 5? It is one, and that is exactly what this theorem tells you you will always get when you do a comparable calculation.

Let us have another example. The theorem says with any clock with a prime number of hours a day, you will use that to form clock arithmetic or modular arithmetic, to give it its proper mathematical name, and you take any number and raise it to a power of P minus one, then you get one. Let us have a more complicated example.

See what happens if we work out 2. It is very important that nobody interrupts at this point. If you work out 2, raised to the power 90, and I have got a 91 hour clock. So off we go, we are going to work out the powers of 2, and the rule is that every time I get above 91, I can work out the remainder on division by 91. So here, the powers of 2. I will start with one - that is 2 to the nought, so I get 2, 4, 8 - there are quicker ways of doing this, but actually I think, for simplicity, I am just going to do it in the really basic way, so just working them out - no clever methods at all. 64 - now it starts to get slightly more complicated. The next one is not 128, but 128 minus 91, which is 37. Now I am back to doubling mode - 37 doubled is 74, doubled is 148, and I have got to subtract 91 again, so that is 148 down to 57, and then I double that and that is 114, take away 91 is 23, I hope... I will just check that one because it is very important not to make a mistake... I think that is okay. 46 - double 46, and I get 92, which... nice, it is one!

If you have ever tried working out powers of 2 and looking at their last digits, just in ordinary base 10 arithmetic, you get 2, 4, 8, 16, 32, 64, 128, 256, and the last digits go 2, 4, 8, 6, 2, 4, 8, 6... and you can see, once you begin to repeat, you must carry on repeating. Once I have got to this one, it is going to have to keep going through this sequence over and over again.

So let us see what that tells us. That is nought, one, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12... when we get to 12, I am back to where I started, and I want to work out 2 to the 90. If doing it 12 times gets me back to where I started, then so does doing it 84 times, because 84 is 7 twelves, so if I do it 84 times, so I've got 2 to the 84, equals one, in this funny 91 hour thing. 2 to the 84 is one, so 2 to the 85 is 2, 2 to the 86 is 4, 2 to the 87 is 8, 2 to the 88 is 16, 2 to the 89 is 32, and 2 to the 90 is 64.

Oh dear, I have just told you a little theorem that says that A to the P minus one always gives you one, and now I have taken A as 2, and P as 91, and I have worked out 2 to the 91 minus one, and I have not got one. I have got 64. So what is the solution to this little problem? Well, all schoolchildren are taught if you are ever going to use a mathematical fact, make sure you are absolutely certain that all the things that are required by that fact really are true. So what are they?

We really have had a number P, we really have had that we've taken A to the P minus one... the only thing that we haven't checked is that 91 is a prime. Is 91 a prime? No, 91 is a carefully chosen number that is the smallest number that is not prime but is not completely obviously not prime! It is my favourite - it is 7 times 13. But what you have to notice about this method is that what we have done here is actually established that 91 is not a prime without knowing that it was 7 times 13. It is not a prime because this theorem did not work, and the theorem always works when it is a prime, and so it is not a prime.

For very big numbers, that is a much better method. Unfortunately, it does not always work. That is another situation like the factorisation methods. You keep on trying various tests, and if your number passes all those tests, then the chances that it is not prime are really incredibly small, so you can be as confident as you like that it is prime. Very, very recently actually, people have come up with a genuine short method for testing whether numbers are prime. Again, it doesn't tell you what the factors are if it is not prime.

I am now out of time, but I have just given you at least some glimpse of how sometimes it is possible to prove that numbers are composite without actually factorising them.