Gerald’s Column
by Gerald Fitton

During the last few months I have been discussing Modulus Arithmetic and Modulus Algebra. Quite by chance Andy Marks posted a problem to Archive-on-Line the answer to which requires some familiarity with Modulus Algebra. How can I resist the opportunity to include a discussion of his problem and the means of solution?

Andy’s Problem is not a simple one so, this month, I shall discuss a similar but simpler problem. Next month I shall extend my analysis to problems similar to Andy’s.

Before I launch into this intriguing subject I have a couple of contributions from a person who has been described to me as “***The*** Sherwin A Hall of Cambridge?” I expect that Sherwin will be surprised to know of his fame!

Schema

In Archive August 2001 (Page 80) I said that I hadn’t included a file of the encryption method using Schema because I couldn’t find the modulus function. It has taken me a little time to get around to it but it was Sherwin who ‘put me right’.

On the Archive monthly disc you will find the Schema file [Code_S]. This file encodes and decodes the phrase “Gerald Fitton” using the ‘one way’ modulus function.

Simple Encoding

Also Sherwin has sent me a couple of interesting Basic programs which he has called “BlackBox”. These programs execute a simple encoding and decoding algorithm based on the method I suggested in the August 2001 issue of Archive (Page 78).

The method is to convert the characters to Extended ASCII Codes (numbers between 0 and 255 inclusive which I call x) and then apply the ‘one way’ function y = (x*m+s) mod 256 to obtain the encoded code number, y.

Sherwin has provided two versions; both are on the Archive monthly disc. The first version uses fixed values for m (the multiplier) and s (the shift) whilst the second requires the user to enter their ‘Public Key’ for encoding and a ‘Private Key’ for decoding.

Sherwin’s description of the use of the second version of “BlackBox” is as follows:

“Drag the file to be encoded to the BlackBox icon (on the iconbar) or click on the iconbar icon to bring up a window and then drag the file to that window. Enter the Public Keys to encode it and save the output as a BlackBox file. To decode the BlackBox file, drag it to the iconbar icon or the window as just described. Enter the Private Keys and click on Continue. The output will be the decoded file, the filetype of which has been stored (in the encoded file). The correct filetype icon will appear in the Save window. If the WIMP hasn’t ‘seen’ that icon then there will be a vacant space in the Save window where the icon should be. Despite this, you can still drag the ‘ghost’ icon to a filer window where a substitute icon will appear.”

Sherwin used this exercise to practice writing a program in multitasking Basic. He decided to use Dr Wimp and he wishes to acknowledge the help he has been given by Ray Favre who is the author of the Dr Wimp articles. You can download the latest version of Dr Wimp from Ray's web site at http://www.argonet.co.uk/users/rayfavre/.

Of course the degree of security is limited and the encryption is vulnerable to a 'Trial and Error' attack but, for a simple encoding method (such as that asked for by Mr P R Boxall) it works, it works well and it is fast. I recommend it to you.

Andy's Problem

Andy Marks posted the following question on Archive-on-Line:

"A theatre has a show running where tickets are £9.50 per adult and £5.75 per child. On one night, the total takings was £3,625. How many children's and how many adult's tickets were sold that night?

"I've tried everything my memory of Maths from school will let me do! Please help, it's driving me mad! I know I could try Trial and Error, but I just feel there must be a Mathematical Method."

Trial and Error

Our Editor Paul Beverley, Bas Lago, Rex Palmer (and others) provided Basic programs which generate all possible solutions. If you have the Archive disc then double click on the file [Prog3] and the full set of sixteen different solutions will be displayed. One of these sixteen solutions is that the audience consists of 34 children and 361 adults.

These simple Basic programs use Trial and Error and not an analytical method. I think that by "a Mathematical Method" Andy means an analytical method.

Numbers

One way of expressing Andy's Problem Mathematically is that he requires the solution (the values of x and y) which satisfy the equation: a*x + b* y = c. The feature of this problem which makes even those with a good grade in A Level Mathematics (and many who have an Honours Degree in Mathematics) take a mental step backwards is that the solution, x and y, indeed a, b and c too, are Natural Numbers.

So let's say something about numbers in general. Have a look at the table below.

ℕ	=	{0, 1, 2, 3, 4, 5, 6, . . . }		=	Natural (counting) numbers
ℤ	=	ℕ	+ {0, −1, −2, −3, . . . }	=	Integers (whole numbers)
ℚ	=	ℤ	+ {¼, ½, ¾, . . . }	=	Rational numbers (fractions)
ℝ	=	ℚ	+ {±√2, π, e, . . . }	=	Real numbers (smooth continuum)
ℂ	=	ℝ	+ {√−1, (1 + √−1), . . . }	=	Complex (and imaginary) numbers

Although I use an equal sign in the table, the curly brackets, {}, show that this is not an ordinary equation in which ℕ is some variable or constant number the value of which might be found by solving an equation.

In words the first mathematical statement should be read as: “The symbol ℕ represents the set of all Natural (counting) numbers such as 1, 2, 3, 4, 5, 6, etc”.

Those of you who are interested might wish to look back to my series of articles starting with the January 1998 issue of Archive in which I discuss about five different types of number used by Mathematicians. The starting point is the Natural Numbers.

The Philosophical Bit

My articles would not be complete without what one of my correspondents has called my “Philosophical Meanderings”. If you think they are an unwarranted distraction then please bear with me or skip to the next section.

A saying to which I don’t subscribe is: “God Created the Natural Numbers; all others (meaning Types of Number) are the work of Man”.

I tend to agree with Galileo who wrote (about the Nature of the Physical World), “Nature’s great book is written in Mathematical Language” and with the eminent Physicist and Member of the Royal Society, Sir James Jeans who said, “No one except a Mathematician need ever hope fully to understand those branches of science which try to unravel the Fundamental Nature of the (Physical) Universe”. Later in his book “The Mysterious Universe” Sir James writes, “The (Physical) Universe can be best pictured . . . as consisting of pure thought, the thought . . . (of) a Mathematical Thinker”.

Whatever the Nature of the Physical Universe there is no doubt that our (Scientific) picture of it (and how it works) has many features in common with the “pure thought” which we know as Mathematics. I do not believe that “Man created the (Mathematical) Universe in his own Image”, a view which used to be popular when I was at school. Nevertheless it seems to me a remarkable coincidence that something as abstract as the ‘Mathematical thoughts of Mankind’ find a mirror in the workings of the Universe within which we eke out our Physical existence.

I ask whether we have invented Mathematics or discovered it. Also, having found that “The Answer to Everything (Physical)” is not quite “42” but Mathematics, I wonder whether we have stumbled upon a divine secret or a coincidence.

Complex Numbers

Problems involving Natural Numbers are difficult because (as I describe in the 1998 articles) this set of numbers restricts the mathematical operations which you can apply to them. Let me explain. Some problems (for example about waves) require that you accept that the answer might be a complex number. Generally these problems are simpler to resolve (than Natural Number Problems like Andy’s) because there is always a solution even when the equation to be solved is something such as x^2 = −1.

Real Numbers

If the Domain of answers is restricted to Real Numbers then an equation such as x^2 = −1 has no solution because we are not allowed to take the square root of a negative number.

At school the Algebra which we are taught is designed to have answers which are Real Numbers. The most important single feature of Real Numbers is that they fill up every possible gap on the Number Line. Let me emphasise this point. Every possible gap between the numbers 1 and 2 is filled with a Real Number—there are no spaces for other numbers left. We can solve equations such as 7*x = 1 by using one of the points on the number line between 0 and 1. We call it one seventh and we arrive at the solution by dividing both sides of the equation by 7.

Natural Numbers

If the Domain of Answers is restricted to Natural Numbers then we are not allowed to use division unless the result is another Natural Number. There is no solution to the problem 7*x = 1 and we are not allowed to divide both sides of the equation by 7.

Diophantine Problems

Once upon a time the only numbers which we (Mankind) knew about were the Natural Numbers. The Algebra of Natural Numbers which was taught in the Great Universities of that era (such as the one at Alexandria) could, and still can be used to solve problems such as that set by Andy.

One of the ‘Professors’ at Alexandria in the third century AD (Circa 250 AD) was a clever Mathematician called Diophantus. Pierre de Fermat (of ‘Last Theorem’ fame) was greatly inspired by Diophantus’ work. Much of Fermat’s work and practically all of Diophantus’ work was concerned with Natural Numbers.

Andy’s Problem can be stated Mathematically as “Find x and y given a, b and c and the equation a*x + b* y = c”. We all know that’s not all there is to it. The ‘catch’ is that all the values in this equation (a, b, c, x and y) are Natural Numbers.

A Simple Equation

Let’s start with the equation 38*x = 608. This equation can be solved using the Algebra which you were taught at school. I shall call this Algebra ‘Real Number Algebra’.

When you use Real Number Algebra you are allowed to use Division. Putting it rather loosely “Division works in Real Number Algebra”. More rigorously I could say that “Division exists and (with one notable exception) gives consistent results”. The ‘notable exception’ is division by zero. Using the Mathematical operation of Division on both sides of the equation produces the result 38*x/38 = 608/38. The left hand side reduces to x because we know that 38/38 gives the ‘magic number’ 1. The right hand side reduces to the Real Number 16—which just happens to be a Natural Number too! So we’re lucky.

We’ve converted our Natural Number equation to a Real Number equation, done some Real Number sums and discovered that our answer is not only a Real Number but also the Natural Number which is the unique answer that we sought.

The Generalization Method

I have described a potent Mathematical Method. What we have done is to start with a ‘simple problem’ and make it more complicated by Generalizing it.

We have taken the problem out of the Domain of Natural Numbers (which, somewhat naïvely, you might think of as a ‘simpler’ Domain) and rewritten it as a problem in the Domain of Real Numbers. By the way, there are Real Number problems (such as an analysis of wave motion) which are best solved by taking the problem into the Domain of Complex Numbers. Having used sophisticated tools from the more general Domain (not available in the restricted Domain) we find that solving the problem is much easier.

The ‘clever bit’ is being able to recognise when the solution (in the more general Domain) is applicable to the restricted Domain and when the answer implies that no solution exists in the restricted Domain. Let me clarify this statement with a simple example.

Suppose that the equation required for solution in the Natural Number problem was not 38*x = 608 but 38*x = 627. Of course we can still convert this Natural Number problem into one involving Real Numbers. The answer to the Real Number problem (obtained using the Real Number operation of Division) is 16½. This is a Real Number (indeed it is a Rational Number) but it is not a Natural Number.

It is no use bemoaning our fate. We have to recognise that the equation 38*x = 627 has no solution in the Domain of Natural Numbers.

If the question which lead to this last equation was: “The price per item is 38 pence, the Sales Receipts are 627 pence; how many were sold?” then the answer has to be something along the lines of: “This question is a load of old rubbish!”. Too many people insist that they can discuss the answer in terms of “sixteen and a bit”—but they shouldn’t! If they do this then it is they who are talking a “load of old rubbish!”

A Harder Equation

Now let’s try to solve the Natural Number equation 38*x + 23*y = 1390.

There is no way that the Method of Generalization which I’ve just described is of any use at all. Neither 38 nor 23 divide exactly into 1390. Anyway, what can we do with the bits?

Let me assure you that this equation as a Natural Number equation has a unique solution.

There is only one possible solution. Some 1700 years or more ago the expatriate Ancient Greek Diophantus was teaching his students how to solve equations like this one. His method is not a Trial and Error method but one devised in the only Algebra known at that time, the Algebra of Natural Numbers.

Remainders

The ‘trick’ discovered by this ex-pat Greek was that the solution to equations like this can be found by studying Remainders. These days the Mathematics of Remainders is called Modulus Mathematics. As another ‘by-the-way’, Arithmetic is doing sums—Spreadsheets do sums; Algebra is about manipulating symbols—Spreadsheets can’t do Algebra. So if we have a problem such as finding the solution to 38*x + 23*y = 1390 we can use a spreadsheet to do the Arithmetic only after we’ve done the Algebra.

So here’s some Modulus Algebra.

Let me introduce a number without giving you a reason—we’ll come back to it later, honest! The number I shall introduce you to is the Natural Number 20.

Multiply through our equation by 20 to get: 38*x*20 + 23*y*20 = 1390*20.

The Algebra

Now we find the Remainder after Division by 23.

Using a Spreadsheet this Remainder is returned by the function mod(number,modulus) using 23 as the modulus. I want you to realise that this sort of Division is not the same as Real Number Division. The essential difference is that when we use mod(,) we find a Remainder and this Remainder is a Natural Number. The ‘left over bits’ are Natural Number Remainders rather than Fractions (Rational Numbers) so the whole of this Modulus 23 operation takes place in the Domain of Natural Numbers. We do not use the Real Number operation of Division; we do not generate fractions.

The next line is mod(38*20*x,23) + mod(23*20*y,23) = mod(1390*20,23).

Let’s try to evaluate the second term, mod(23*20*y,23). Remember that y has to be a Natural Number. Because of the multiplier 23 in the number 23*20*y, it has to be exactly divisible by 23. This second term of the equation reduces to zero.

Now look at the term on the right hand side of the equation, mod(1390*20,23). This can be evaluated using a spreadsheet—or you can use the ‘Long Division’ method (with Remainders). I was taught long division and Remainders at school but, I think, nowadays such Arithmetic lessons are dominated by the hand calculator! Hand calculators don’t return Remainders.

It is the Remainder after (1390*20) is divided by 23 that we want. The Remainder is 16.

So that leaves us with the first term of the equation, mod(38*20*x,23). Of course there is something special about the multiplier 20 or I wouldn’t have chosen it. We can split up this modulus expression using the Multiplication Rule which I described in the October 2001 issue of Archive (Vol 15 No 1 P25). Applying this Rule we have:

mod(38*20*x,23) = mod(38*20,23) * mod(x,23)

The reason that I chose the special multiplier 20 is because mod(38*20,23) = 1; I suggest that you try it and see. 38*20 = 760 and, after division by 23, the Remainder is 1.

Substituting 1 for mod(38*20,23) we find: mod(38*20*x,23) = mod(x,23). Furthermore, x has to be less than 23 for a unique solution (I'm not going to prove this—I can do but I don't want to digress too far—so take my word for it). This gives us mod(x,23) = x.

We've (half) solved the equation 38*x + 23*y = 1390. This (half) answer is that x = 16.

The Special Multiplier

How did I just happen to pick the number 20 as the number which will reduce the difficult expression 38*x to the simple x (after using the modulus 23 operation)? It is because the number 20 is the 'Multiplicative Inverse' of 38 (using modulus 23). Multiplying by the 'Multiplicative Inverse' of a number (in Modulus Algebra) has much in common with the Real Number operation of Division. In both cases of solving algebraic problems we try to reduce the coefficient of x to 1.

You will find a description of the algorithm which finds a 'Multiplicative Inverse' in the September and October 2001 issues of Archive. You'll see that the algorithm is not a Trial and Error algorithm. Custom functions are available (on the Archive monthly disc) in both PipeDream and Fireworkz format for finding the 'Inverse Multiplier' of any number which is within the range of the Floating Point Emulator.

The Other Half

Already we have half the solution to 38*x + 23*y = 1390. It is x = 16.

We can do a similar 'trick' using as our special multiplier 5 and finding the Remainders after dividing by 38. The solution is y = mod(1390*5,38) = 34.

Now check the full solution. 38*16 + 23*34 = 1390. Wow! What is more, this solution is unique. Let me emphasise that there is only one solution to this Diophantine Equation and we have found it using a method which is over 1700 years old. Furthermore the method is an Analytical method, not a Trial and Error method.

A Spreadsheet

On the Archive monthly disc I have included a spreadsheet called [Unique] in both PipeDream and Fireworkz format. The spreadsheet can be used to set up and solve Diophantine problems which have a unique answer. The spreadsheet uses a couple of custom functions, [c_HCF] and [c_Inv] which you have seen before.

I have to thank Rex Palmer and Tonnie Demarteau for their contributions to this [Unique] spreadsheet and to the [ManySolns] spreadsheet which I will present next month.

My thanks also to Steve Ellacott of the University of Brighton for his help in providing references and inspiration as well as checking my Mathematics.

Summary

We have not yet solved Andy's Problem, 950*x + 575* y = 362500. Andy's Problem has sixteen different solutions one of which has x =16 and another has y = 34. The problem we have solved, 38*x + 23*y = 1390, is related to Andy's Problem—but you'll have to wait until next month to discover the relationship.

Andy's Problem is a Problem in the Natural Number Domain.

Sometimes problems which are stated in terms of a restricted Domain can be Generalized to become a problem in a more Generalized Domain. Andy's Problem does not yield to this approach.

Andy's Problem is an example of problems studied and solved by an ex-pat Ancient Greek called Diophantus who taught at Alexandria over 1700 years ago. It does not use a Trial and Error technique but an Analytical technique which requires us to calculate the 'Multiplicative Inverse' of the coefficients in the equation.

We have met this 'Multiplicative Inverse' in the context of modern encryption techniques. It is built into the BlackBox encryption program written by Sherwin Hall and into the RSA Public Key encryption system which I described last month.

Finally

You can email or write to me at the addresses given in Paul's Fact File.

Please note that we no longer have a telephone or fax.