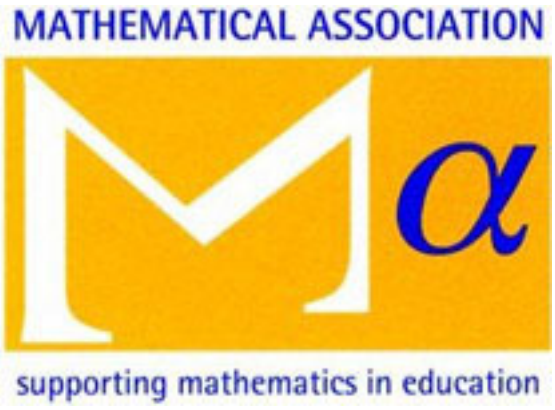

Acknowledgement I'd like to thank John Durran who first showed me a chunked up M-group. His program, written in APL is fantastically more beautiful than the BASIC program given earlier. For further reading you might like to try

[1] *The fascination of groups* by F. J. Budden (C.U.P.)
[2] *Topics in algebra* by I. N. Herstein (Wiley).

NICK MACKINNON

Winchester College

Modular arithmetic and cryptography

J. B. READE

Even the purest of pure mathematics can have a crucial influence on practical problems. In this article we show how a topic in pure mathematics (modular arithmetic) originally pursued for its own interest only, turns out to have unexpected application to an area of communication theory (cryptography). The fact that at the present time it is easy to construct large prime numbers but very difficult to factorise large composite numbers has made it possible to devise simple codes which are uncrackable by known methods.

The modulus

We take a positive integer m which we call the *modulus* and we identify any pair of integers which differ by a multiple of m. For example, if $m = 4$, then $1 = 5 = 9 = 13 = -3 = -7$ etc. We shall write, for example,

$$2 = 6 \,|4|$$

and say 2 equals 6 *modulo* 4.

Situations in real life where we are unconsciously working with a modulus are the 24-hour clock ($m = 12$; e.g. $17.30 = 5.30 =$ half past 5) and days of the week ($m = 7$; e.g. 23 March, 30 March fall on the same day of the week since $23 = 30 \,|7|$). Observe that, for example, if $m = 7$, then any integer is equal to one of the numbers 0, 1, 2, 3, 4, 5, 6 and to find which one we simply divide by 7 and take the remainder. For example, $34 = 6 \,|7|$, and there are essentially only 7 different numbers when the modulus is 7. In general if the modulus is m there are only m essentially different numbers namely $0, 1, 2, \ldots, m - 1$.

Arithmetic with a modulus

For example, with $m = 4$ we have

$$1 + 1 = 2 \quad \text{but} \quad 2 + 2 = 4 = 0.$$

We can draw up a *Cayley table* which gives a complete description of addition with modulus 4 and another for multiplication:

$+4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times 4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Subtraction goes similarly but division is where the problems start.

Example 1 $m = 4$ What is $2/3$? Suppose $2/3 = x$. Then $3x = 2$. We can solve this equation by referring to the Cayley table for multiplication with modulus 4. We simply look for a 2 in the row corresponding to 3 and obtain the answer for x by observing which column we are in. In this case $x = 2$. So $2/3 = 2$ (modulo 4).

Example 2 $m = 4$ What is $3/2$? Suppose $3/2 = x$. Then $2x = 3$. But row 2 hasn't got a 3 in it. So the equation $2x = 3$ has *no solution* (modulo 4) and $3/2$ *does not exist* in this case.

Example 3 $m = 4$ What is $2/2$? If we put $2/2 = x$ we get $2x = 2$ which has *two solutions* $x = 1$ or 3. So $2/2$ has *two values* namely 1 and 3 (modulo 4).

The above examples show that in some cases divsion is possible with a unique value, but that it may sometimes happen that division is impossible or yields more than one value. This is actually a phenomenon we have all met before in ordinary arithmetic, though it may not have been put in these terms. In ordinary arithmetic division is possible and with a unique value *provided* we are not dividing by zero. Division by zero is impossible except in the case $0/0$ where division is non-unique, in fact $0/0 =$ anything since the equation $0x = 0$ is satisfied by any x.

Referring to the Cayley table for multiplication with modulus 4 it is easy to see that division by 1 or 3 will always produce a unique value since the rows for 1 and 3 each contain all the numbers 0, 1, 2, 3 once and once only. Division by 0 or 2 is either impossible or non-unique. Looking now at the table for multiplication with modulus 5 we see that in this case unique division is possible by any number except zero:

$\times 5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

The general rule is that unique division is possible when dividing by any number n which is *coprime* with the modulus m, i.e., m, n have no common factors.

Powers and roots

For $m = 5$ we can draw up a table of powers as follows:

x	x^2	x^3	x^4	x^5
0	0	0	0	0
1	1	1	1	1
2	4	3	1	2
3	4	2	1	3
4	1	4	1	4

Observe that

$$\sqrt{1} = (1 \text{ or } 4) = \pm 1,$$

$$\sqrt{4} = (2 \text{ or } 3) = \pm 2,$$

but that $\sqrt{2}$, $\sqrt{3}$ don't exist. This is not unlike the situation in ordinary arithmetic where certain numbers have two square roots (positive numbers) and certain numbers have no square root (negative numbers).

Every number has a unique cube root modulo 5 but only 0, 1 have a 4th root and 1 has four 4th roots. Every number is its own 5th root (modulo 5).

The general rule for saying when a unique nth root exists modulo m is quite complicated. We can give an answer in certain cases. For example, if $m = p$, a prime, the rule is that there is a unique nth root if n is coprime with $p - 1$. Observe that in the example above we have $m = p = 5$ and $p - 1 = 4$ so we expect to be able to take unique nth roots for $n = 1$ and 3 which is exactly what we found.

Example $m = p = 11$ We have $p - 1 = 10$ so we can, for example, take unique cube roots. To find $x^{1/3}$ systematically we solve

$$u = \tfrac{1}{3} |10|; \quad \text{i.e. } 3u = 1 |10|.$$

In fact, multiplying both sides by 3, we get

$$-u = 9u = 3 |10| \quad \text{and} \quad u = -3 = 7 |10|.$$

(N.B. Multiplication or division of an equation is only valid by a number which is coprime with the modulus.) We therefore find

$$x^{1/3} = x^7 |11|.$$

Hence, for example,

$$2^{1/3} = 2^7 = 128 = 7 |11| \quad \text{and} \quad 3^{1/3} = 3^7 = 2187 = 9 |11|,$$

which can be confirmed by observing that

$$7^3 = 343 = 2\,|11| \quad \text{and} \quad 9^3 = 729 = 3\,|11|.$$

The case $m = pq$ where p, q are prime is the one we need for the application to cryptography. The rule here is that unique nth roots exist when n is coprime with $(p-1)(q-1)$.

Example $m = pq = 10$ We have $(p-1)(q-1) = 4$ so, for example, $x^{1/3}$ exists uniquely. Solving $u = 1/3\,|4|$ we get $u = 3$ (see the Cayley table for multiplication modulo 4). Therefore, for example,

$$2^{1/3} = 2^3 = 8\,|10| \quad \text{and} \quad 3^{1/3} = 3^3 = 27 = 7\,|10|,$$

which is confirmed by observing

$$8^3 = 512 = 2\,|10| \quad \text{and} \quad 7^3 = 343 = 3\,|10|.$$

Application to cryptography

The application is based on the fact that, whereas computer programmes exist which can find 50 digit primes in seconds, when it comes to factorising 100 digit numbers into prime factors, the only available computer programmes *at the present time* take centuries. This makes it possible for *me* to construct 100 digit numbers $m = pq$ where p, q are 50 digit primes which *you* will be unable to factorise.

To set up a code which exploits the above fact we need a *coding modulus* $m = pq$ ($\geqslant 26$) and a *coding power* c coprime with $(p-1)(q-1)$. For example, we can take $m = 33$, $c = 3$ since 3 is coprime with $(p-1)(q-1) = 20$.

To encode a message we convert letters to numbers by taking $A = 01$, $B = 02$, $C = 03$ etc, and take the cubes of these numbers modulo 33. Suppose the message is

HAVE A NICE DAY.

We get, converting to numbers,

08 01 22 05 01 14 09 03 05 04 01 25,

and, cubing each number (modulo 33) gives

17 01 22 26 01 05 03 27 26 31 01 16.

To decode the message we need the *decoding power* d which is obtained by solving $d = 1/3\,|20|$. In fact, $d = 7$. Taking 7th powers (modulo 33) of successive pairs of digits in the encoded message we recover the original message in its numerical form and hence its verbal form.

In practice the coding modulus is a 100 digit number obtained by multiplying together two 50 digit primes. The numerical message is encoded by grouping its digits in blocks of 100 and taking the encoding power of each block. To decode one has to know the prime factors of the coding modulus in

order to be able to work out the decoding power. Each receiver publishes his personal coding modulus and coding power but keeps the prime factors of his coding modulus (and his decoding power) a secret. Anyone can then send him a message but he is the only one who can decode it.

Exercises

1. Show that for coding modulus 29, possible coding powers are 3, 5. Find the corresponding decoding powers.
2. Show that for coding modulus 55, possible coding powers are 3, 7. Find the corresponding decoding powers.
3. Decode the following message given that the coding modulus is 35 and coding power is 5:

11 15 24 20 13 01 14 11 01 20 24 01 22 10 23 30 08 01 11 11 30 13 01 14.

4. What do you think the possible coding powers are for the coding modulus 30? Check your answer by trying a few examples.
5. Why is 2 never a possible coding power?

Further reading

S. Landau, Primes, codes and the National Security Agency, *Notices of the American Math. Soc.*, **30**, 7–10 (1983).
C. Pomerance, Recent developments in primality testing, *Math. Intelligencer*, **3**, 97–105 (1981).

J. B. READE

Department of Mathematics, The University, Manchester M13 9PL

A singular impact?

MATTHEW LINTON

While I worked at Teeside Polytechnic I had some difficulty in arriving in the morning by 9.00. Not being an early bird my desire was to pull into the car-park at 8.58, but this I did not seem able to achieve. If I left home at 8.15 the journey was smooth and trouble-free, and I was at my parking place by 8.50. Whereas if I left a moment later there were a couple more cars at the estate exit, each succeeding roundabout and set of traffic lights was busier, and eventually I drove into the car-park at 9.05—not only five minutes late, but also quite likely finding the spaces all full and having to resort to street parking. It seemed that no matter how I varied my start time the arrival interval of 8.50 to 9.05 was somehow inaccessible to me. Of course some