Public Key Cryptography

How mathematics allows us to send our most secret messages quite openly without revealing their contents - except only to those who are supposed to read them

The mathematical ideas needed to follow the explanation are relatively simple. As a help for those who might need a reminder about some of the ideas or words, additional material has been added at the end to give a little more detail about certain points.

Public Key Cryptography

Frank Tapson

The headings in the right-hand margin indicate where detailed help on that particular item can be found. Since this is hyper-text document (when viewed on the computer) items printed in red are 'clickable'. That is, they can be pointed at with the mouse and clicked on so as to bring them to the screen. After reading the item concerned, the use of the command 'Back' will return you to your previous place in the document.

To save unnecessary repetition, throughout this topic, the word 'number' is to be taken to mean only positive whole numbers (and zero).

For many centuries secret messages had to be transmitted by using a key and/or method known only to those who were meant to share in the contents of those messages. Clearly, with such systems, there were always difficulties in distributing these keys or systems so that they did not fall into the wrong hands.

A breakthrough was made (in 1977) by Rivest, Shamir and Adleman (which is why the initials RSA are often attached to this system), when they devised a sytem using two keys. One key is used to put the message into cipher, and this key can be broadcast to the world so there is no distribution problem. This key is known as the **Public Key**. In addition to the Public Key another number (known as the *modulus)* is also published. The other **Key**, which is needed to decipher the message, is kept secret by the individual(s) for whom the message(s) is, or are, intended.

modulo arithmetic page 6

The system, based on some relatively simple ideas in **modulo arithmetic**, will be explained here by means of a numerical example, using only the smallest numbers it is possible to use. First of all it is necessary to set up the necessary numbers which will be used, by following this routine.

General Routine	Example
1. Choose two **prime numbers** p,q	$p = 2 \quad q = 5$
2. Set $m = p \times q$	$m = 2 \times 5 = 10$
3. Set $A = (p - 1) \times (q - 1)$	$A = 1 \times 4 = 4$
4. Choose a number E which is less than A and has no factors in common with A.	$E = 3$
5. Find a number D so that $(D \times E) - 1$ is a **multiple** of A.	$D = 7$ since $(3 \times 7) - 1 = 20$

prime numbers page 11

multiple page 15

E (= 3) is used to Encipher the message and is published.

m (= 10) is the *modulus* and is used to do the division where a remainder is required and is also published.
In this very simple case, 10 is easy to use since the remainder on division by 10 must be the last digit of the number being divided.

D (= 7) is used to Decipher the message and is **not** published.

Now let us use the values just worked out to put a message into cipher.

The numbers we work with must be one less than the value of m. In this case m = 10 means we cannot use a number bigger than 9. As we shall be working, initially, with the values of the individual letters, this means we cannot have more than 9 letters. Since the normal alphabet contains 26 letters, we need to use a sub-set of the alphabet.

So, being limited to a small 'alphabet' of only 9 letters, it makes good sense to choose those which are most commonly used -

A D E H N O R S T

with each taking the corresponding numerical values

1 2 3 4 5 6 7 8 9

For our message we will use the single word "DOOR".

First write out the message in plain text -

D O O R

change all letters into their corresponding values -

2 6 6 7

raise all values to the **power** of E (= 3) -

2^3 6^3 6^3 7^3

which produces the values -

8 216 216 343

Finally find the remainder when each of those is divided by m (= 10) -

8 6 6 3

So the final message in cipher is 8663

To decipher, a similar process is used except that D is used in place of E in finding the power.

Write out the message in its cipher form -

8 6 6 3

raise all values to the power of D (= 7) -

8^7 6^7 6^7 3^7

which is within range of a calculator and produces the values -

2097152 279936 279936 2187

Find the remainder when divided by m (= 10) -

2 6 6 7

and change those values back into letters -

D O O R

[*One for you.* Using the same values for D and m decipher 5 7 2 9]

powers
page 12

What has been done so far offers no security at all for two reasons.

1. The values of E and m have to be made public and, in this case, they are so small it would be easy to see that since $m = 10$, the p and q must be 2 and 5. From that the value of A could be found and, since E is also known, then D could be found.

However, this defect can be overcome by making p and q very very large so that the factoring of m is next to impossible. And that is done in practice.

2. A much bigger fault is that putting only one letter at a time into cipher must mean that each letter will always have the same value in its cipher form throughout the message. This immediately makes the final cipher message breakable by using a simple frequency count.

This defect is overcome by grouping letters (and their values) together and putting each complete group into cipher.

large primes
page 11

To provide an example of this grouping idea we need to work with new values since, as we have already seen, m must be bigger than the largest value to be worked on.

So, now we use $m = 115$ $E = 83$ $D = 35$

[*One for you.* What values of p and q were used?]

Using the same message as before: "DOOR", its letter values are 2667. Working in groups of two, this splits into 26 and 67 and it is those two numbers which are acted on by the ciphering process.

Each has to be raised to the power of E (= 83) and then the remainder found after division by m (= 115)

So we need to evaluate: $26^{23} \pmod{115}$ and $67^{23} \pmod{115}$

Directly calculating the values of large powers is beyond the capability of most calculators, though some can do it if a modulo arithmetic is involved, and so can some computer-based calculators. However, the calculations needed here can be done on a hand-held calculator using a particular technique.

techniques for large powers
page 13

Whatever way it is done, the answers required are

$$26^{83} \equiv 16 \pmod{115}$$

and

$$67^{83} \equiv 28 \pmod{115}$$

and the final cipher message is 16 28

Notice how the clue of the doubled up letters in the middle has gone.

Deciphering would require the evaluation of 16^{35} and 28^{35} using the same value of m for the divider.

[*One for you.* Using the same D,m decipher 43 52]

Note this is still a completely insecure system because

- $m = 115$ is easy to factorise.
  This is overcome in real life by using very large primes.
- even taking 2 letters at a time it would be vulnerable to a frequency count.
  This is overcome by using very much larger groups.

But doing both of those requires the use of a computer and specially written programs.

Signatures

In this system, it is intended that a message is put **into** cipher using *E* and deciphered using *D*. But in fact, the values of *E* and *D* are interchangeable in their function. That is, it is also possible put a message **into** cipher with *D* and decipher with *E*. This might seem at first sight to be of no use. But in fact it has a very important function and is used in authenticating messages.

Consider two correspondents, Sean and Nora. Each has their own (different) *E* and *m* values which are public and known to everyone. Each has their own *D* value which is known only to themselves. Sean is sending a message to Nora and it is important that Nora can know without any doubt that the message does indeed come from Sean. This (very much simplified) is one way it can be done.

First of all Sean writes out the message:

NORA SEND SARA TEN ROSES SEAN SEAN

changes it into numbers:

5671 8352 8171 935 76838 8315 8315

enciphers his **second signature only** using his (private) ***D*** value (and *m*):

5671 8352 8171 935 76838 8315 9761

enciphers the complete message using Nora's publicly known *E* and *m* values:

2889 4751 6413 214 31924 4223 6587

On receiving it, Nora uses her private *D* (and *m*) values to produce:

NORA SEND SARA TEN ROSES SEAN TROA

She extracts the 'gibberish' TROA on the end and, knowing that the message is supposed to be from Sean, she uses his ***E*** value on it (9761) to get:

NORA SEND SARA TEN ROSES SEAN SEAN

and the only one who could have made that possible is Sean (or should be!)

Trivial? Yes that is, but think about a message from Sean to his bank telling them to transfer 10,000 pounds from his account to Sara's - it is no longer trivial then!

[*One for you.* What is the weakness of the signature system given here?]

As a challenge try to decipher this message which was encrypted with *E* = 67 and *m* = 111.

86 91 37 109 21 22 86 77 69 17 19 17

There is a signature in the message which was encrypted by a sender whose public keys are *E* = 41 and *m* = 119. What is the sender's name?

For the really ambitious, try your cipher-breaking skills on this message.

All I will tell you is that it uses the same 9-letter alphabet as before, and that neither *p* nor *q* contains more than 2 digits; there were 18 letters in the original message, enciphered in groups of two.

156 326 34 33 333 292 229 199 169

Modulo arithmetic is also known as **clock arithmetic**, or **remainder arithmetic**, and there is a very good reason for both of those names as we shall see.
Modulo arithmetic is a form of arithmetic which uses only a limited set of the whole numbers {0, 1, 2, 3, 4, 5, 6, 7 . . . . . }. It is always defined by the size of the limited set to be used, and that size is called the *modulus.*
A modulus of ***n*** means that the first ***n*** elements of the whole-number set must be used.

For example: A modulus of 3 means use 0, 1, 2
A modulus of 6 means use 0, 1, 2, 3, 4, 5
A modulus of 20 means use 0, 1, 2, 3, 4, 5 . . . . 17, 18, 19

Note

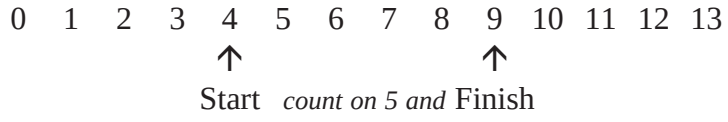
- The set to be used always starts with 0
- No numbers may be left out
- The set ends with the number which is **1 less** than the modulus

To do arithmetic with a limited set of numbers requires that we re-look at what the various operations of arithmetic mean.

addition

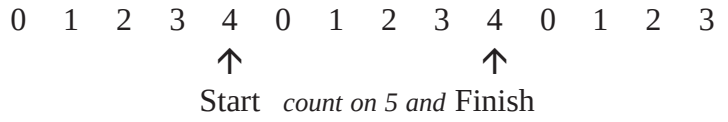
In our 'normal' system, adding one number to another can be done by having the numbers in an ordered line, starting at one number, counting on the amount of the other number, and recording the number we finish at.

For example: 4 + 5 can be modelled as

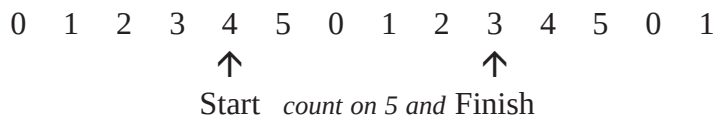


In modulo arithmetic the equivalent arrangement of the number line requires the same limited set of numbers to be repeated

For example: In modulo 5



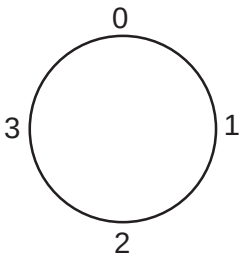
or in modulo 6



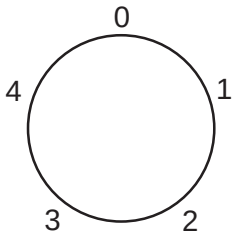
Note

- The answer clearly depends upon the size of the modulus
- The starting number must be less than the modulus *(for the moment)*
- The number of places to be counted on can be bigger than the modulus

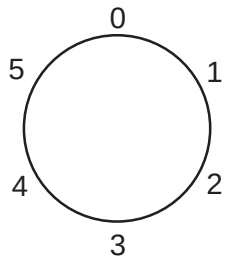
Since the 'number line' in modulo arithmetic requires the same limited set of numbers to be repeated it makes good sense to use 'number circles' like this -



modulo 4



modulo 5



modulo 6

Reminding us, as they do, of clock faces gives rise to the name **clock arithmetic**. They can be seen to work for addition exactly like the number line did, provided only that we remember to move clockwise round the circles. That is, in the direction in which the numbers are increasing.

Next we look at the problem of what to do with numbers that are bigger than, or equal to, the modulus. One way it can be done is by thinking of them in relation to the appropriate size of circle.

For example: What is 6 + 8 in modulo 5?

6 = 0 + 6 so, starting at 0 and counting on 6 places finishes at 1

8 = 0 + 8 so, starting at 0 and counting on 8 places finishes at 3

And 6 + 8 becomes 1 + 3 in module 5 which is 4.

Another way it can be done is by first adding the given numbers (6 + 8) in the usual way (= 14) and then changing the answer into modulo 5

14 = 0 + 14 so, starting at 0 and counting on 14 places finishes at 4

However it is done it is now possible to make **addition** tables for this arithmetic.

modulo **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

modulo **5**

+	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

modulo **6**

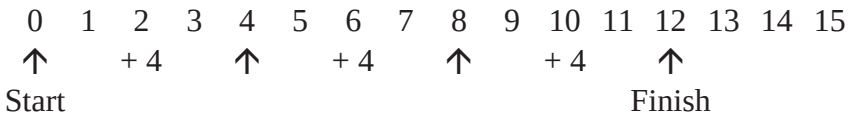
+	**0**	**1**	**2**	**3**	**4**	**5**
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Note how well patterned these tables are, so much so that it is easy to write an addition table for any modulus.

[*One for you.* Write addition tables for modulo 7 and modulo 8]

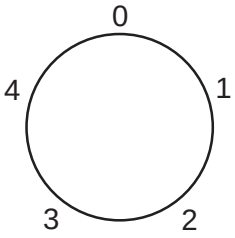
multiplication

As with addition, we must first see how multiplication works in 'normal' arithmetic.
Consider the statement 3 × 4
This means, "put together 3 lots of 4" *(or 4 lots of 3)*
In other words, 3 × 4 is a short way of writing 4 + 4 + 4 *(or 3 + 3 + 3 +3)*
On the number line, 4 + 4 + 4 can be modelled as



And we can see that the answer is 12 *(which is hardly a surprise!)*
To do the same sum in modulo arithmetic needs the modulus to be stated.

We will evaluate 3 × 4 in modulo 5 by counting 4 + 4 + 4 on a modulo 5 clock
First, 4 + 4 takes us to 3
then, 3 + 4 takes us to 2
So, 3 × 4 (*mod* 5) is 2



[*One for you.* Count 3 + 3 + 3 + 3 on the same clock]

using remainders

It is awkward working in modulo arithmetic and having to refer to the tables any more than necessary. It is much easier to work within our 'ordinary' number system and change answers into their modulo arithmetic equivalent.

Suppose we want 4 × 5 in modulo 6
We know that 4 × 5 = 20, but what is it in modulo 6?
Thinking of the modulo 6 clock, starting at 0, every time we move 6 places we get back to 0
So, 6, 12, 18 will all get us back to 0,
which leaves only 2 places more to get to 20
This is the same as saying,
"Count in 6's and stop when you are about go past the number you have (in this case 20), then whatever you have left (in this case 2) will be the number you want."
Or, in a much shorter phrase:
"Divide by 6 and keep the **remainder**."
20 ÷ 6 = 3 remainder 2
It is this 'trick' which gives modulo arithmetic its other name of
remainder arithmetic
Formally it is written:
20 ≡ 2 (mod 6)
Note the symbol is ≡ which is read as "is congruent to"
and not = which is read as "equals"

remainder
page 15

Using remainders we can now write out some **multiplication** tables for this arithmetic.

modulo **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

modulo **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

modulo **6**

×	**0**	**1**	**2**	**3**	**4**	**5**
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

The first thing to notice is that the tables are completely symmetrical about the leading diagonal *(top left to bottom right)* which demonstrates how modulo multiplication is **commutative** *(3 × 4 = 4 × 3 etc.)* just as 'normal' multiplication is.

commutative
page 15

We now come to our first problem with this arithmetic.

Consider the equation $3x = 1$

To find the value of x we need to find a number which, on being multiplied by 3 gives the answer 1

With our 'ordinary' number system we would immediately say that the answer is 1 ÷ 3 or 1/3 but modulo arithmetic does not admit fractions and we must refer to the appropriate multiplication tables.

In modulo 4: $3 \times 3 = 1$ so $x = 3$

In modulo 5: $3 \times 2 = 1$ so $x = 2$

In modulo 6: no solution can be found,
since $3 \times x$ equals either 0 or 3 (!)

If the equation is changed to $3x = 3$ then solutions can be found in modulo 4 and 5 but, in modulo 6 we have

$3 \times 1 = 3$ $\quad 3 \times 3 = 3$ $\quad 3 \times 5 = 3$

So there are three solutions: 1, 3 and 5

And thus we find that in modulo arithmetic, a simple equation might have

- no solution
- one solution
- several solutions

Rules can be given to summarise this, which allow us to know in advance, whether or not a given equation can be solved for any given modulus, and how many solutions it might have. But perhaps the most useful thing to know is that, if the modulus is prime, then all possible equations will have a unique solution; that is, there will be one, and only one, solution.

[*One for you.* Write out the modulo 8 multiplication table.]

Working with remainders, as we did to develop the multiplication tables, it easy to write out tables to give the values of x x^2 x^3 x^4 x^5 and so on.
Here are the tables for modulo 4, 5 and 6

modulo **4**

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

modulo **5**

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

modulo **6**

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

We will merely note that these tables seem even more irregular than those for simple multiplication and this time, even the case for a prime modulus does not seem to offer a guarantee of regular behaviour.

[*One for you.* Investigate powers in modulo arithmetic. Look at both higher values of x and other values for the modulus.]

prime numbers

One number is said to be a **factor** of another number if it divides into it exactly.

For example: 3 is a factor of 6; 4 is a factor of 12;
2 is a factor of 18; and so on

Note

- 1 is a factor of ALL other numbers.
- Every number is a factor of itself.

A number may have several factors.

For example: 12 has the factors 1, 2, 3, 4, 6, 12
16 has the factors 1, 2, 4, 8, 16
25 has the factors 1, 5, 25
17 has the factors 1, 17

Note

- Every number, except 1, has **at least two** factors.

A **prime number** is a number which has two, and only two, factors.

For example: The first 15 prime numbers are
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47

Note

- 1 is NOT a prime number (it has only one factor).
- There is no end to the list of prime numbers.
- Numbers (other than 1) which are NOT prime are **compound numbers**.
- Prime numbers are usually called just 'primes'.

Primes are thought of as the 'building blocks' for numbers in the sense that all the other numbers can be made from them by using multiplication.

For example: $12 = 2 \times 2 \times 3$ which can be written $2^2 \times 3$
$20 = 2 \times 2 \times 5$ or $2^2 \times 5$
$25 = 5 \times 5$ or 5^2
$15600 = 2 \times 2 \times 2 \times 2 \times 3 \times 5 \times 5 \times 13$ or $2^4 \times 3 \times 5^2 \times 13$

Note

- There is only ever **one** way this can be done.
- A re-arrangement of the primes is NOT a different way.

large primes

In public key cryptography it is obviously important that the modulus (m) cannot be easily factorized or else the whole system would be in jeopardy.
Typically the values of p and q used to generate m are each of the order of 100 digits (and more) long. This gives a number for m which will be over 200 digits long. At present such large numbers can take years to factorize even with the largest and fastest computers. And then, for the highest level of security the key-values are changed at regular intervals.

In working only with positive whole numbers a **power**, or **index**, is written as a superscript to some other number to indicate how many of the other numbers are to be multiplied together. The other number is called the **base**.

For example: In 2^3 the power is 3 and the base is 2;
so it means that 3 lots of 2 have to be multiplied together.
$2 \times 2 \times 2$ which = 8
3^2 means 3×3 which = 9
5^2 means 5×5 which = 25
3^3 means $3 \times 3 \times 3$ which = 27
7^5 means $7 \times 7 \times 7 \times 7 \times 7$ which = 16807

Note

- If the power is 0, the answer is always 1 ($958^0 = 1$)
- If the power is 1, the answer is the number itself ($37^1 = 37$)

Using a Calculator

In this particular work the use of a calculator is essential, and a 'scientific' model is easiest to use.
The key required will be marked with something like x^y or it may be the INVerse function of some other key. *(Look in the manual)*
To use it, simply enter the value for x, press the x^y key, enter the value for y (the power) and then press [=]

For example: To work out 7^5 press: [7] [x^y] [5] [=]

Note [ ] *is used to show a particular key is meant, so* [5] *means the key labelled* 5

If only a basic calculator is available the work is much more tedious, especially for a large power, involving a lot of keying. Using the memory helps but can save only a few key-strokes.
If the calculator has a constant facility *(look in the manual)* then the number of key-strokes can be reduced considerably.
For instance, on one calculator, keying in [7] [×] [×] would mean that every time the [=] was pressed after that, whatever was in the display would be multiplied by 7

For example: 7^5 would require: [7] [×] [×] [=] [=] [=] [=]
Note [=] *is only pressed 4 times (1 less than the power)*
and that you do have to be careful in counting!

techniques for large powers

Calculating the values of large powers is beyond the capability of most calculators, though some can do it if a modulo arithmetic is involved. However, the size of the numbers being used here can be handled on a calculator by using a particular technique. It is based upon the fact that if, after a series of multiplications have been carried out, the only answer that is needed is the remainder, then it is possible to work out the multiplications using remainders at each stage and still produce the same final answer. This allows the work to be done on an ordinary hand-held calculator.

We will work with the values given in the example on page 4.
This requires the value of 26^{13} (*mod* 115) to be found.

finding a remainder
page 14

First a particular sequence is developed based upon squaring:

$26^1 = 26$

$26^2 = 676$ which is bigger than m (= 115) and so the remainder, after dividing by 115 is found to replace it.

It is 101 and this allows us to write -

$26^2 \equiv 101 \pmod{115}$

Now, to find 26^4 which is $(26^2)^2$ it is only necessary to work with the remainder ($101^2 = 10201$) and then find the remainder for that. It is 81

$26^4 \equiv 81 \pmod{115}$

and so on . . .

$26^8 \equiv 6 \pmod{115}$

$26^{16} \equiv 36 \pmod{115}$

$26^{32} \equiv 31 \pmod{115}$

$26^{64} \equiv 41 \pmod{115}$

This is far enough since the next step would be 2^{128} and 128 is bigger than the value of E (= 83) which will be used.

Now determine how the E value of 83 can be made only by the addition of powers of 2 (1, 2, 4, 8 etc.).

$$83 = 1 + 2 + 16 + 64$$

laws of indices
page 15

This together, with the laws of indices gives us -

$$26^{83} \equiv 26^{(1 + 2 + 16 + 64)} \equiv 26^1 \times 26^2 \times 26^{16} \times 26^{64}$$

Since we only require the remainder at the end we can do the multiplication using the remainder values already worked out -

$$26 \times 101 \times 36 \times 41 = 3875976$$

which, after dividing by 115 has a remainder of 16 so,

$$26^{83} \equiv 16 \pmod{115}$$

In a similar way, using 67 instead of 26 in the above process we have -

$$67^{83} \equiv 67^{(1 + 2 + 16 + 64)} \equiv 67^1 \times 67^2 \times 67^{16} \times 67^{64}$$

which gives -

$$67 \times 4 \times 101 \times 6 = 162408$$

and

$$67^{83} \equiv 28 \pmod{115}$$

Asked to find the remainder when 17 is divided by 3 can be done easily without a calculator.

For example: $17 \div 3 = 5$ with a remainder of 2
We can show this as: $17 = 5 \times 3 + 2$
Or, explaining it another way
5 lots of 3 were removed from 17 and 2 was left over.

Note

- A remainder is also known as a **residue**.
- The remainder must always be LESS than the divisor

divisor
page 15

If the same sum is done on a calculator we get

$17 \div 3 = 5.6666667$

which might be recognised as $5\frac{2}{3}$ in decimal form.

This is not very useful when trying to find a remainder if the numbers are big enough to warrant the use of a calculator.
Like, what is the remainder when 1721 is divided by 47?
The calculator gives

$1721 \div 47 = 36.617021$

But what is the remainder? (*It certainly is* NOT 0.617021)
Let us note that 47 went into 1721: 36 times with a fraction (0.617021) left over.
Put another way, 36 lots of 47 were removed from 1721 and some was left over - but how big was that 'some'?

36 lots of 47 is $36 \times 47 = 1692$

That means 1692 was removed and $1721 - 1692 = 29$
So, the remainder must have been 29

Check: $36 \times 47 + 29 = 1721$ ✓

Here is another method, using the same example.

$1721 \div 47 = 36.617021$
Subtract the whole number part (36) to leave the fraction (0.617021)
Multiply this by the divisor (47) to get 29 - which is the remainder.

Note that, depending upon the calculator, in this last part it may sometimes be necessary to round the given answer to the nearest whole number.

If several cases have to be handled this is a very good method and can be speeded up by placing the divisor in the memory at the beginning.

in other words

One number is said to be a **multiple** of another number if the first number is equal to the second number multiplied by some whole number.

multiple

For example: 12 is a multiple of 4 since $12 = 4 \times 3$
20 is a multiple of 5 since $20 = 5 \times 4$

Note

- A number is considered to be a multiple of itself since $x = x \times 1$

Any division sum is made up of 4 parts, all of which are named.
The number which has to be divided, or shared out, is called the **dividend**.
The number which must do the dividing, is called the **divisor**.

divisor

The number giving the answer, is called the **quotient**.
The number giving the amount left over, is called the **remainder**.

remainder

dividend ÷ divisor = quotient + remainder

For example: In the sum $27 \div 4 = 6$ with 3 left over
27 is the dividend
4 is the divisor
6 is the quotient
3 is the remainder.

Note

- The remainder can be zero.

An operation (such as + - × ÷) which combines two numbers is said to be **commutative** if the order in which the two numbers are placed makes no difference to the answer.

commutative

For example: addition **is** commutative since $3 + 4 = 4 + 3$
multiplication **is** commutative since $2 \times 5 = 5 \times 2$
subtraction **is not** commutative since $7 - 1 \neq 1 - 7$
division **is not** commutative since $6 \div 3 \neq 3 \div 6$

The three principal rules which determine how numbers written using index notation may be combined are known as the **laws of indices**.

laws of indices

They are

$$b^m \times b^n = b^{m+n} \qquad b^m \div b^n = b^{m-n} \qquad (b^m)^n = b^{mn}$$

Two special cases which follow from these are

$$b^0 = 1 \qquad b^{-n} = \frac{1}{b^n}$$

For example: $2^3 \times 2^6 = 2^{3+6} = 2^9 = 512$ $\qquad 2^5 \div 2^2 = 2^{5-2} = 2^3 = 8$

Note

- The two numbers being combined must have the same values for b