The Stepping-stone Problem

N stepping-stones are arranged in a circle and are numbered 0 to $N - 1$. The rules of the game are that starting on stone number 0, you are allowed to move clockwise by *a* steps in each move. The question is first – is it possible to arrive at stone number *R*? and if so, how many moves *n* will it take?

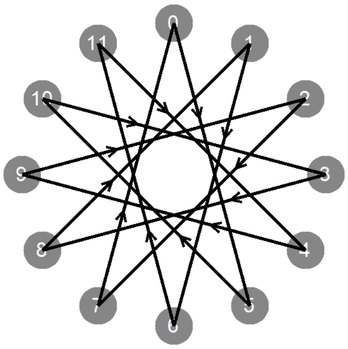
The easy bit

For example: if there are 12 stones and you are allowed to move 5 steps each time, how long will it take you to reach stone number 4? The sequence goes like this:

0 > 5 > 10 > 3 > 8 > 1 > 6 > 11 > 4

We arrive at stone number 4 after 8 moves. If you continue the sequence you will find that you visit all the stones exactly once before returning to stone number 0.

We can illustrate this in the following way:



But this is not always the case. If we are allowed to move by 3 steps each time, it is easy to see that we will never reach stone number 4 because the sequence this time goes like this:

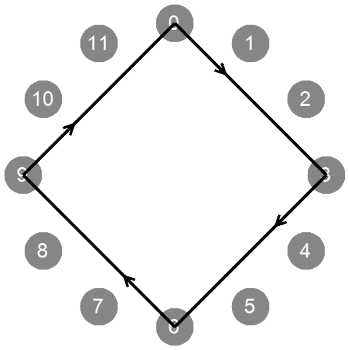
0 > 3 > 6 > 9 > 0 > 3 . . .

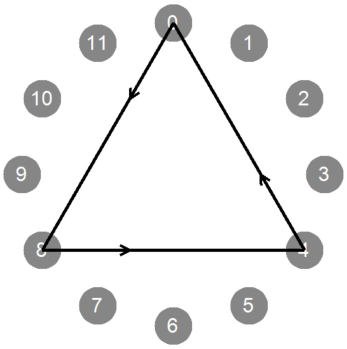
and it is immediately obvious why. It is because 12 (the number of stones) is divisible by 3 and therefore always repeats after 12 / 3 = 4 moves.

If we are allowed to move by 8 steps the sequence is:

0 > 8 > 4 > 0 > 8 . . .

and the sequence has length 3.





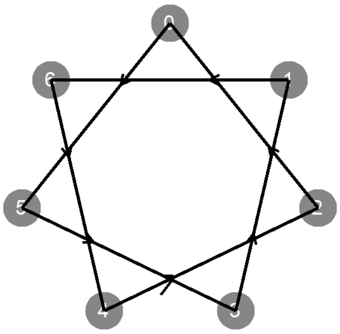
Why is this? The answer is that, although 12 is not divisible by 8, the two numbers have a common factor of 4 and it is this that determines the length of the sequence. It immediately follows that if the two numbers have no common factor, the length of the sequence will be equal to the number of stones ie – all the stones will be visited exactly once.

We can now answer the question of whether any particular stone will be visited in a simple way. The stone *R* will be visited if and only if *R* is divisible by the highest common factor of *N* and *a*.

ie if

$$R \div N|a$$

In *N* is prime, then, obviously, all values of *a* (not equal to *N*) will result in all stones being visited once before returning to the starting point. e.g if *n* = 7 and *a* = 5 we have:



The hard bit

OK – so we know whether or not a solution is possible; how do we find out how many moves it is going to take?

What we are asking for is the number of *a*'s which equal a whole number of *N*'s plus *R*. ie we are looking for a solution to the Diophantine equation:

$$a\,x = N\,y + R$$

where *x* and *y* are, of course, integers.

Now, unlike ordinary linear equations, there is no analytical method of solving this problem (ie there is no formula for *x* in therms of *N, a* and *R*) and the easiest way is simply to go on adding *a* repeatedly, subtracting *N* whenever you can until you reach the desired number *R*. This is a trivial task on a computer:

```
Function Diophantine(N, a, R)
Dim s as integer = 0
For i as integer = 1 to N
     s += a
     if s > N then s -= N
     if s = R then return i
next
return 0
```

We know that, if a solution is possible, it must occur in the first *N* moves so if no solution is found, the For ... next loop terminates and the function returns 0.

There are techniques involving modular arithmetic for simplifying the problem if *N* and/or *a* are very large because we can replace the equation with a congruence:

$$a\,x \;\equiv_N\; R$$

which reads: '*ax* is congruent to *R* modulo *N*' and basically says that *ax* leaves a remainder of *R* when divided by *N*.

Now since we are only interested in the remainder, we can add (or subtract) *N* from the right hand side as many times as we want without upsetting the congruence. If we find a number that is divisible by *a* we are home and dry! eg suppose that $N = 51$ and $a = 10$ and we want to know how many moves it will take to reach the 37th stone; the Diophantine equation is:

$$10\,x \;=\; 51\,y \;+\; 37$$

and its solution is not obvious.

Rewriting it as a congruence we obtain:

$$10\,x \;\equiv_{51}\; 37$$

Now the idea is to add 51 to the right hand side as many times as necessary to make the number divisible by 10. Obviously we must add 3 more 51's making

$$10\,x \;\equiv_{51}\; 190$$

Now an important theorem in modular arithmetic says that, providing the modulus does not share a factor with the number you are dividing by, you can divide both sides of a congruence as if it was an equality. So in this case we can divide through by 10 obtaining:

$$x \;\equiv_{51}\; 19$$

giving us the simplest answer $x = 19$.

(Even if the modulus shares some factors with the divisor you can still divide through provide you divide the modulus by the shared factors too.)

Another technique is to solve for *y* first rather than *x*.

The same equation can also be written as:

$$51\,y \;=\; 10\,x \;-\; 37$$

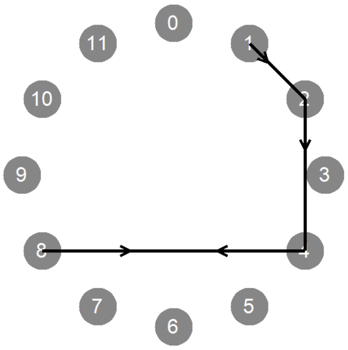
i.e. $$51\,y \;\equiv_{10}\; -37 \;\equiv_{10}\; 3$$

This time we see that we must add 15 10's to the 3 on the right hand side to make a multiple of 51 giving us the answer $y = 3$ which, of course gives us $x = 19$ by substituting back into the original equation.

The Multiplicative Stepping-stone Problem

Suppose that instead of starting on stone 0 and *adding a* each move, you start on stone 1 and *multiply* by *a*. Let us take *N* =- 12 and investigate the sequences obtained for different values of *a*:

a = 1   1 > 1 > [1 >] . . .
a = 2   1 > 2 > 4 > 8 > [4 > 8 >] . . .
a = 3   1 > 3 > 9 > [3 > 9 >] . . .
a = 4   1 > 4 > [4 >] . . .
a = 5   1 > 5 > [1 > 5 >] . . .
a = 6   1 > 6 > 0 > [0 >] . . .
a = 7   1 > 7 > [1 > 7 >] . . .
a = 8   1 > 8 > 4 > 0 > [0 >] . . .
a = 9   1 > 9 > [9 >] . . .
a = 10 1 > 10 > 4 > [4 >] . . .
a = 11 1 > 11 > [1 > 11 >] . . .



It would appear from this that the sequence very quickly enters a short repeating pattern.

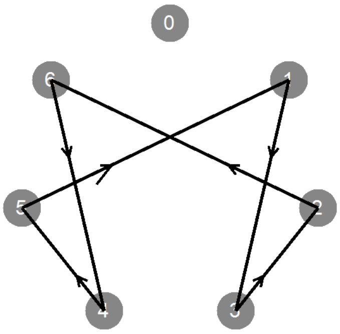
What happens if we start from a different stone, eg 2?

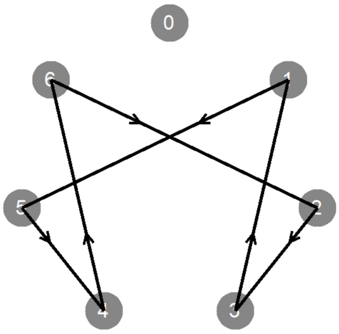
a = 1   2 > 2 > [2 >] . . .
a = 2   2 > 4 > 8 > [4 > 8 >] . . .
a = 3   2 > 6 > 0 > [0 >] . . .
a = 4   2 > 8 > [0 >] . . .
a = 5   2 > 10 > 8 > 4 > [8 > 4 >] . . .
a = 6   2 > 0 > [0 >] . . .
a = 7   2 > 2 > [2 >] . . .
a = 8   2 > 4 > 0 > [0 >] . . .
a = 9   2 > 6 > [6 >] . . .
a = 10 2 > 8 > [8 >] . . .
a = 11 2 > 10 > [2 > 10 >] . . .

Some of the sequences are the same, some different but all are, as before, rather short. But perhaps this is because the number 12 has many factors. Let us try with a prime number eg 7:

a = 1   1 > 1 > [1 >] . . .
a = 2   1 > 2 > 4 > [1 > 2 > 4 >] . . .
a = 3   1 > 3 > 2 > 6 > 4 > 5 > [1 > 3 > 2 > 6 > 4 > 5 >] . . .
a = 4   1 > 4 > [1 > 4 >] . . .
a = 5   1 > 5 > 4 > 6 > 2 > 3 > [1 > 5 > 4 > 6 > 2 > 3 >] . . .
a = 6   1 > 6 > [1 > 6 >] . . .

Again, most of the repeating cycles are quite short but the cases of *a* = 3 and *a* = 5 are interesting because they visit all of the stones (with the exception of stone number 0 of course.)





Now we can write this problem as a Diophantine equation as follows:

$$a^x = N y + R$$

or alternatively $$a^x \equiv_N R$$

(You might object that in calculating the sequence we have repeatedly taken the modulus *before* multiplying by the next number whereas the congruence above implies that we take the modulus *after* doing all the multiplications. Do not worry. The modulus of ($S - kN$) × a is obviously equal to the modulus of $S \times a$ because the modulus of kN is zero.)

Suppose we wish to solve this congruence for the case $a = 3$, $N = 7$ and $R = 4$. Using the same technique as before, we keep adding N to the right hand side and each time we reach a multiple of a, we can divide through to simplify things. e.g.:

$$3^x \equiv_7 4 \equiv_7 11 \equiv_7 18$$

Dividing by 9 $$3^{(x-2)} \equiv_7 2 \equiv_7 9$$

Dividing by 9 again $$3^{(x-4)} \equiv_7 1$$

Now the simplest solution to this equation is if (x – 4) equals 0 i.e. $x = 4$ which is the answer we seek.

Let us investigate what goes wrong if there is no solution. Let's try $a = 6$, $N = 7$ and $R = 4$.

$$6^x \equiv_7 4 \equiv_7 11 \equiv_7 18$$

so $$6^{(x-1)} \equiv_7 3 \equiv_7 10 \equiv_7 17 \equiv_7 24$$

and $$6^{(x-2)} \equiv_7 4$$

but we have been here before so there is no solution.

The connection with cyclic numbers

The sequence 1 > 3 > 2 > 6 > 4 > 5 > 1 > . . . crops up when you try to divide 1 by 7

10 over 7 = 1 remainder 3
30 over 7 = 4 remainder 2
20 over 7 = 2 remainder 6
60 over 7 = 8 remainder 4
40 over 7 = 5 remainder 5
50 over 7 = 7 remainder 1

The sequence appears in the list of remainders. This is because at each stage you take the remainder, multiply it by 10 and then divide by 7 to get the next remainder. The reason this process produces the same remainder sequence as the example with $a = 3$ above is that 10 and 3 are congruent (mod 7)

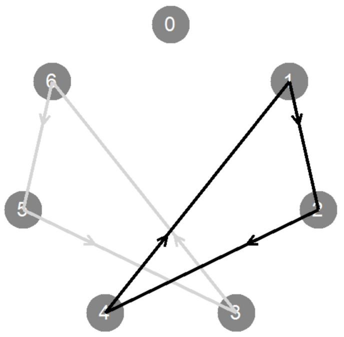
My favourite cyclic number (in base 10) is 0588235294117647 and is the repeated pattern of digits produced when you divide 1 by 17. This suggests that $a = 10$, $N = 17$ should produce a complete repeating sequence. Let's see if it does:

1 > 10 > 15 > 14 > 4 > 6 > 9 > 5 > 16 > 7 > 2 > 3 > 13 > 11 > 8 > 12 > 1

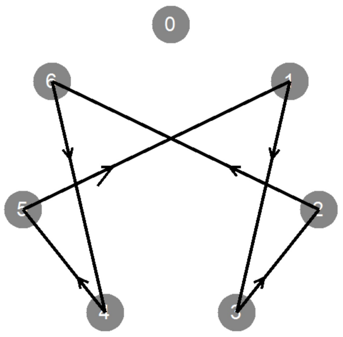
For further information about cyclic numbers, see my article with the same name.

Fermat's Little Theorem

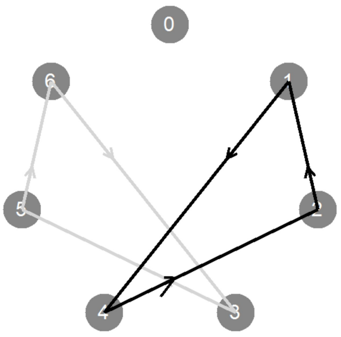
Lets have a look at an example when *n* is prime e.g. $N = 7$. The following diagrams have $a = 2$, 3, 4, 5 and 6. Each diagram shows the principal route which includes the starting point $x = 1$ in black with other routes with different starting points shown in grey.



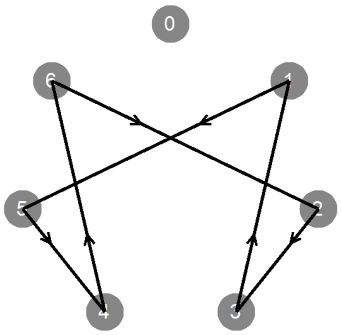
$a = 2$



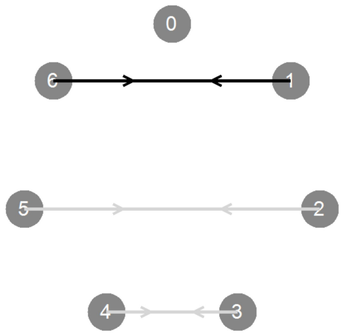
$a = 3$



$a = 4$



$a = 5$



$a = 6$

First of all we can note that if *a* is greater than *N* (e.g. if $a = 12$ say) then the route followed will be identical to the route followed when $a = 5$ (because $12 \equiv_7 5$) so these are the only case we need to consider.

Secondly we note that the 6 case fall into a number of groups. When $a = 3$ or $a = 5$, all the stones are visited once. When $a = 2$ and $a = 4$, there are two possible sequences, each of length 3; and when $a = 6$ there are three possible sequences each of length 2. The reason for the lengths of these sequences is because 6 ($N - 1$) has factors 2, 3 and 6. If we had chosen $N = 11$ then we would find that the sequences would have lengths 2, 5 and 10. In general we can conclude that, provided *N* is prime, whatever the value of *a* and whatever the starting point *x*, the length of the sequence will always be a factor of $N - 1$.

The consequence of this observation is that, whatever the value of *a* and *x*, if we take $N - 1$ steps, the last step will always take us take to the starting point again. In symbols we are saying that

$$x \times a^{N-1} \equiv_N x$$

For example, if I $x = 5$, $a = 6$ and $N = 11$ then $5 \times 6^{10} = 302330880 \equiv_{11} 5$

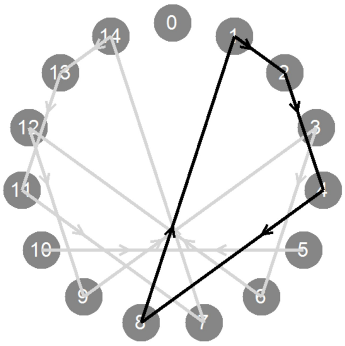
Moreover, if we start from stone *a* (i.e. we put $x = a$) then we have (with *N* prime)

$$a^N \equiv_N a$$

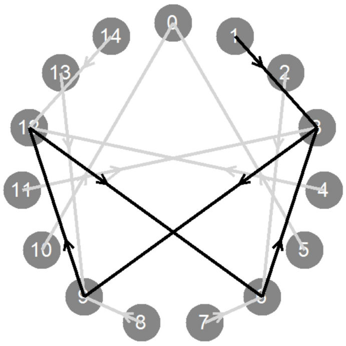
which is Fermat's Little Theorem.

Euler's extension to Fermat's theorem

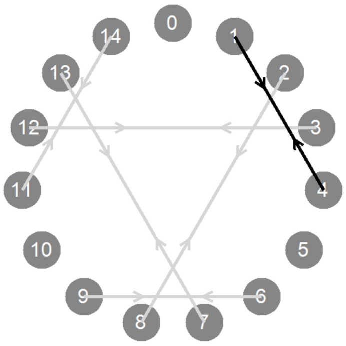
Now let us consider what happens when *N* is the product of two primes e.g. *N* = 15 Here are the 13 possible sequences starting at 1 with other starting points shown in grey.



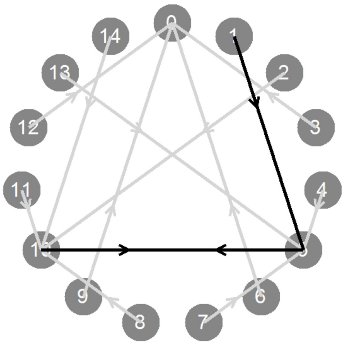
a = *2*



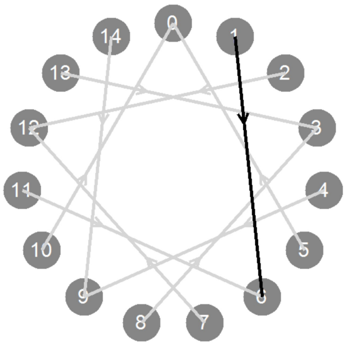
a = *3*



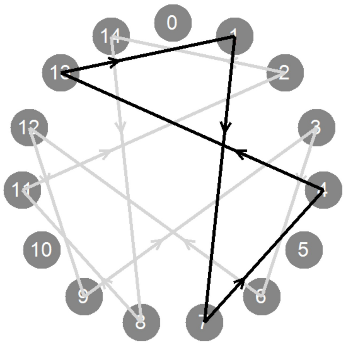
a = *4*



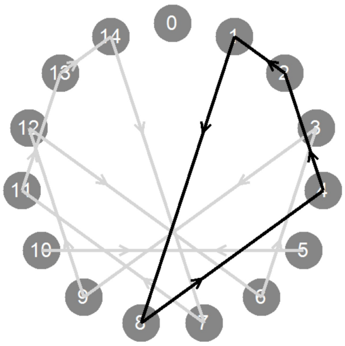
a = *5*



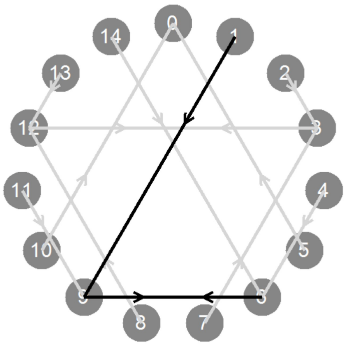
a = *6*



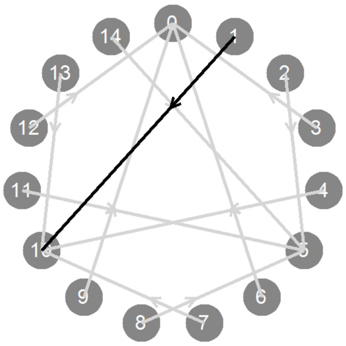
a = *7*



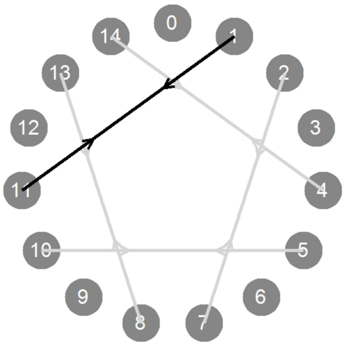
a = *8*



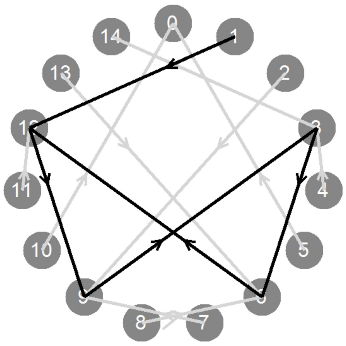
a = *9*



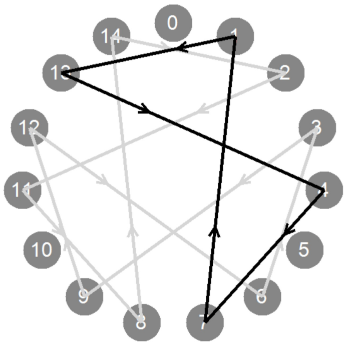
a = *10*



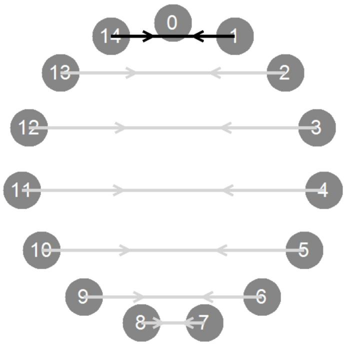
a = *11*



a = *12*



a = *13*



a = 14

Since 14 (= 15 – 1) has factors 2, 7 and 14 we might expect to find sequences of each of these lengths but what we actually find is this:

$a \setminus x$	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	0, 4	0, 4	0, 4	0, 4	0, 2	0, 4	0, 4	0, 4	0, 4	0, 2	0, 4	0, 4	0, 4	0, 4
3	1, 4	1, 4	0, 4	1, 4	1, 1	0, 4	1, 4	1, 4	0, 4	1, 1	1, 4	0, 4	1, 4	1, 4
4	0, 2	0, 2	0, 2	0, 2	0, 1	0, 2	0, 2	0, 2	0, 2	0, 1	0, 2	0, 2	0, 2	0, 2
5	1, 2	1, 2	1, 1	1, 2	0, 2	1, 1	1, 2	1, 2	1, 1	0, 2	1, 2	1, 1	1, 2	1, 2
6	1, 1	1, 1	0, 1	1, 1	1, 1	0, 1	1, 1	1, 1	0, 1	1, 1	1, 1	0, 1	1, 1	1, 1
7	0, 4	0, 4	0, 4	0, 4	0, 1	0, 4	0, 4	0, 4	0, 4	0, 1	0, 4	0, 4	0, 4	0, 4
8	0, 4	0, 4	0, 4	0, 4	0, 2	0, 4	0, 4	0, 4	0, 4	0, 2	0, 4	0, 4	0, 4	0, 4
9	1, 2	1, 2	0, 2	1, 2	1, 1	0, 2	1, 2	1, 2	0, 2	1, 1	1, 2	0, 2	1, 2	1, 2
10	1, 1	1, 1	1, 1	1, 1	0, 1	1, 1	1, 1	1, 1	1, 1	0, 1	1, 1	1, 1	1, 1	1, 1
11	0, 2	0, 2	0, 1	0, 2	0, 2	0, 1	0, 2	0, 2	0, 1	0, 2	0, 2	0, 1	0, 2	0, 2
12	1, 4	1, 4	0, 4	1, 4	1, 1	0, 4	1, 4	1, 4	0, 4	1, 1	1, 4	0, 4	1, 4	1, 4
13	0, 4	0, 4	0, 4	0, 4	0, 1	0, 4	0, 4	0, 4	0, 4	0, 1	0, 4	0, 4	0, 4	0, 4
14	0, 2	0, 2	0, 2	0, 2	0, 2	0, 2	0, 2	0, 2	0, 2	0, 2	0, 2	0, 2	0, 2	0, 2

(The first number is the 'tail' i.e. the number of steps before the sequence enters a loop and the second number is the length of the loop. Starting values which have no tail are highlighted in red.)

Surprisingly, there are no loops of length 7 at all; instead there are many loops of length 2 and 4. This is because the what is important is not $N – 1$ (= 14) but $p – 1$ (= 2) and $q – 1$ (= 4).

Of particular interest are the cells highlighted in yellow in which the starting value x is equal to the step value a. These always have no tail and in this case the loop length is never greater than 4.

Now Euler showed that the loop length could never be greater than $(p – 1)(q – 1)$ which in this case is 8. The reason for the longest loop length only being half this is that $p – 1$ and $q – 1$ have a common factor of 2. It is only if $p = 2$ that will generate the maximum length. (For example, if N = 14 and the step factor is 3 you will find a sequence of length 6). In general, I believe that the longest loop will equal to $(p – 1)(q – 1)/\text{HCF}(p, q)$ but I do not have a proof of this.

In any case, it follows that $a^{(p\ -\ 1)(q\ -\ 1)+1} \ \equiv_{pq} \ a$

For example, taking $p = 3$ and $q = 5$, $7^{(2\times4+1)} \ = \ 40353607 \ \equiv_{15} \ 7$

A more formal proof of Fermat's Little Theorem

The argument on page 6 relies of two observations: firstly, every starting number results in a loop and secondly, all the possible loops have the same length. These statements can be proved as follows:

Suppose that a certain starting number x does not result in a loop. If this is the case it must enter a loop at some later stage. (For example, look at the diagram on page 4 where the sequence goes 1, 2, 4, 8, 4, 8, …) It follows that there must be a number x' (= 4 in the example) which has two different pre-images x_1 and x_2. i.e. $x_1 a \equiv_N x'$ and $x_2 a \equiv_N x'$ Or to put it another way

$$x_1 a = n_1 N + x' \quad \text{and} \quad x_2 a = n_2 N + x'$$

Subtracting these equations we get

$$(x_1 - x_2) a = n_3 N$$

Now if N is prime, either $(x_1 - x_2)$ is divisible by N or a is divisible by N. Since neither of these are possible, (both being less than N) all starting numbers must be part of a loop.

The second statement is easily proved as well. If there exists a (shortest) loop of length s starting at $x = 1$ which goes $1 \rightarrow a \rightarrow a^2 \rightarrow \ldots \rightarrow a^s = 1$ (mod N) then there will exist a second loop also of length s which goes $k \rightarrow ka \rightarrow ka^2 \rightarrow \ldots \rightarrow ka^s = k$ (mod N). There are two possibilities; either this loop is entire or it consists of two or more identical sections. If the latter than there must be a number ka^t where $t < s$ which is also equal to k (mod N). i.e. $ka^t \equiv_N k$

Now it is possible to divide through by k but only if k and N are co-prime. Obviously if N is prime (and $k < N$), this condition is met so $a^t \equiv_N 1$ But this contradicts our assumption that s is the shortest loop starting at 1. It follows that all loops must have length s.

Taken together, we have now proved that, providing N is prime, all starting numbers result in an immediate loop whose length must be a factor of $N - 1$. It follows that all loops will return to their starting number after $N - 1$ steps. (Those loops which are shorter that $N - 1$ will return after 2 or more loops). So what we are saying is that for any prime p

$$xa^{(p-1)} \equiv_p x$$

There are several other ways you can state the theorem: for example, putting $x = 1$ we can say that $a^{(p-1)}$ must leave a remainder of 1 when divided by p. Alternatively, putting $x = a$, we can say that a^p must leave a remainder of a when divided by p. Or again, $a^p - a$ must be divisible by p.

Fermat's Little Theorem is widely used to test large numbers to see if they might be prime. The test is not infallible but if you can show that, for example, $2^N - 2$ is not divisible by N then N is definitely not prime.

A more formal proof of Euler's Theorem

The following lemmas are easily proved

I. If $X \equiv_a r$ and $X \equiv_b r$ then $X \equiv_{ab} r$ provided that *a* and *b* are co-prime

II. If $X \equiv_a 1$ then $X^n \equiv_a 1$

Now if *p* and *q* are two different primes then from Fermat's Little theorem

$$X^{(p-1)} \equiv_p 1 \quad \text{and} \quad X^{(q-1)} \equiv_q 1$$

By Lemma II

$$\left(X^{(p-1)}\right)^{(q-1)} \equiv_p 1 \quad \text{and} \quad \left(X^{(q-1)}\right)^{(p-1)} \equiv_q 1$$

But

$$\left(X^{(p-1)}\right)^{(q-1)} = \left(X^{(q-1)}\right)^{(p-1)} = X^{(p-1)(q-1)}$$

Therefore by Lemma I

$$X^{(q-1)(p-1)} \equiv_{pq} 1$$

Therefore

$$X^{(p-1)(q-1)+1} \equiv_{pq} X$$

(Incidentally the proof can be extended to apply to numbers with any number of different primes $N = pqr...$)

RSA encryption

When you make a secure payment over the internet what happens is this. The bank sends you a 120 digit number *N* (whose factors known only to the bank are *p* and *q*) the bank also sends you a smaller random number *E*. Both these numbers are public.

You code you card details etc. into a number *X* and calculate $Y = X^E$ (mod *N*) (efficient algorithms exist for calculating moduli without having to calculate X^N explicitly.

Now the bank knows that if you raise *X* to the power of $(p-1)(q-1)+1$ (mod *N*) you will return to the original number X so all the bank has to do is calculate Y^$((p-1)(q-1)+1-E)$