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.

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 visted exactly once.

We can now answer the question of whether any particlar stone will be visited in a simmple 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

$$R \div N|a$$

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 numner 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 rech the 37^{th} stone; the Diophantine equation is:

$$10x = 51y + 37$$

and its solution is not obvious.

Rewriting it as a congruence we obtain:

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

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

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

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:

$$51y = 10x - 37$$

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

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 $(S - kN) \times a$ 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 divde 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 favorite 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.