The digits of a fraction

1. Getting the expansion from the fraction

Suppose we try to find the digits in the base 60 expression for 1/7. Just as in elementary school we divide

$$\begin{array}{r} 0.\ 8{:}34{:}17{:}\ 8{:}34{:}17 \\ 7\overline{)\ 1.\ 0{:}\ 0{:}\ 0{:}\ 0{:}\ 0{:}\ 0{:}\ 0} \\ 1.\ 4{:}\ 2{:}\ 1{:}\ 4{:}\ 2{:}\ 1 \end{array}$$

and get a repeating expansion, in this case of period 3. Why does the repetition occur? Why of order 3? This is not quite a simple story. We can start to get some idea of how and why things are the way they are by looking at the opposite problem.

2. Getting the fraction from the expansion

Suppose we are given a repeating decimal and we want to know what fraction it comes from. For example $0.13:17:56:13:17:56:\ldots$. Let x ne the unknown frcation, so

$$x = 0.13:17:56:13:17:56:\ldots$$

How can we find out what x is? If we multiply this equation by 60^3 we get

$$\begin{aligned} 60^3 x &= 13:17:56.13:17:56:\ldots \\ &= x + 13:17:56 \\ (60^3-1)x &= 13:17:56 \\ x &= \frac{13:17:56}{59:59:59}\ . \end{aligned}$$

Exercise 1. *Express this fraction in reduced decimal form.*

A slightly more complicated case would be that where the repetition doesn't begin 'immediately:

$$x = 1.\ 0:17:\ 1:17:\ 1:17\ 1:\ldots$$

Then

$$\begin{aligned} 60x &= 1:\ 0.17:\ 1:17:\ 1:\ldots \\ 60^3 x &= 1:\ 0:17:\ 1.17:\ 1:17:\ 1:\ldots \\ (60^3-60)x &= 1:\ 0:17:\ 1-1 \\ x &= \frac{1:17:\ 0}{60^3-60} \end{aligned}$$

Exercise 2. *Express this fraction in reduced decimal form.*

3. Reasons: the inverse of a prime number

From now on I'll just work in base 10, although it should be pretty clear that what I say applies to arbitrary bases B.

It ought to be clear that repetition in the decimal expansion of a fraction has to occur, since the quotients repeat when the carries repeat, and the carries are always smaller than the divisor. But to predict excatly what the period of repetition is looks rather puzzling. It turns out to depend on some interesting properties of prime numbers and factoring.

Let's first analyze the process we carry out to get the decimal expansion and rewrite it in a simpler form. Let's look at a familiar example to start with. What is the decimal expansion of 1/7?

Write out

$$\frac{1}{7} = 0.a_1a_2a_3a_4a_5a_6a_7a_8a_9\ldots$$

where we have to find the digits a_i. How do we find a_1? If we multiply this equation by 10 we get

$$\frac{10}{7} = a_1.a_2a_3a_4a_5a_6a_7a_8a_9\ldots$$

from which we can see that $a_1 = 1$, since

$$\frac{10}{7} = 1 + \frac{3}{7}\,.$$

Next comes these calculations, if we keep going in this way :

$$\begin{aligned}
\frac{10}{7} &= \mathbf{1}.a_2a_3a_4a_5a_6a_7a_8a_9\ldots \\
\frac{10}{7} - 1 = \frac{3}{7} &= 0.a_2a_3a_4a_5a_6a_7a_8a_9\ldots \\
\frac{30}{7} &= a_2.a_3a_4a_5a_6a_7a_8a_9\ldots \\
&= \mathbf{4}.a_3a_4a_5a_6a_7a_8a_9\ldots \\
\frac{30}{7} - 4 = \frac{2}{7} &= 0.a_3a_4a_5a_6a_7a_8a_9\ldots \\
\frac{20}{7} &= a_3.a_4a_5a_6a_7a_8a_9\ldots \\
&= \mathbf{2}.a_4a_5a_6a_7a_8a_9\ldots \\
\frac{20}{7} - 2 = \frac{6}{7} &= 0.a_4a_5a_6a_7a_8a_9\ldots \\
\frac{60}{7} &= a_4.a_5a_6a_7a_8a_9\ldots \\
&= \mathbf{8}.a_5a_6a_7a_8a_9\ldots \\
\frac{60}{7} - 8 = \frac{4}{7} &= 0.a_5a_6a_7a_8a_9\ldots \\
\frac{40}{7} &= a_5.a_6a_7a_8a_9\ldots \\
&= \mathbf{5}.a_6a_7a_8a_9\ldots \\
\frac{40}{7} - 5 = \frac{5}{7} &= 0.a_6a_7a_8a_9\ldots \\
\frac{50}{7} &= a_6.a_7a_8a_9\ldots \\
&= \mathbf{7}.a_7a_8a_9\ldots \\
\frac{50}{7} - 7 = \frac{1}{7} &= 0.a_7a_8a_9\ldots
\end{aligned}$$

and then it starts to repeat. There is a simpler way to carry out the same process, at least simpler to write.

10^n	r	q
1	1	0
10	3	1
100	2	4
10^3	6	2
10^4	4	8
10^5	5	5
10^6	1	7

We are basically here calculating the powers of 10 modulo 7, and writing down the values in the second column. For example we start with $10^0 = 1$. We multi0ly thi8s by 10, which si the same as 3 modulo 7. Write 3 in the second column. In effect we are dividing 10 by 7, which gives us

$$10 = 1 \cdot 7 + 3$$

and we write $r = 3$, and then in the third column, put $q = 1$. Repeat. When we get $10^n = 1$ modulo 7, things are going to start repeating. This matches somnething we might have figured out anyway. We have

$$\begin{aligned} \frac{1}{7} &= 0.142857142857142857\ldots \\ \frac{10^6}{7} &= 142857.142857142857\ldots \\ \frac{10^6}{7} - 142857 &= 0.142857142857\ldots \\ &= \frac{1}{7} \\ 10^6 - 1 &= 7 \cdot 142857 \end{aligned}$$

so that we can see immediately from the fact that the repeat length is 6 that $10^6 = 1$ modulo 7, and furthermore that the repeating part is

$$\frac{10^6 - 1}{7} = 142857\,.$$

This always works. *To get the repeating part of* $1/n$ *calculate powers of* 10 *modulo* n *until you get* 1. *If* k *is the smallest positive integer with* $10^k = 1$ *modulo* n, *then the repreat length is* n *and the repeating part is*

$$\frac{10^k - 1}{n}$$

possibly padded with 0 *at the left to make an expression* k *digits long.*

The next question is: *What possible repeat lengths are there?*

We'll look first at the case where the fraction is $1/p$ and p is a prime number.

- *The expansion of* $1/p$ *in any base* B *has a period of repetition dividing* $p - 1$.

One interesting, maybe unexpected, thing is that it doesn't depend all that much on the base B.

To begin, suppose $1/p$ has a period of repetition N. It is easy enough to see that it has a simple repeat, starting right at the first digit to the right of the decimal point. Then as we have just seen

$$\frac{B^N - 1}{p}$$

will be equal to some integer, say n. But then

$$B^N - 1 = pn$$

which means that $B^N - 1$ is a multiple of p. In fact, a bit of though will convince you that the repetition length is the smallest N such that $B^N - 1$ is divisible by p. This can be found fairly quickly, using arithmetic **modulo** p, or **congruence arithmetic**.

4. Congruence arithmetic

Suppose q to be an integer greater than 1. Integer arithmetic modulo q is done by writing only remainders after division by q. For example, let $q = 7$. Then

$$\begin{aligned} 1+5&=6 \\ 1+6&=0 \quad \text{(since } 1+6=7 \text{ is divisible by 7)} \\ 2+6&=1 \quad \text{(since } 2+6=8 \text{ has remainder 1 after division by 7)} \\ 2\cdot 6&=5 \quad \text{(since } 2\cdot 6=12=1\cdot 7+5\text{)} \\ 2\cdot 4&=1 \quad \text{(since } 2\cdot 4=8=1\cdot 7+1\text{)} \end{aligned}$$

If the remainder of n upon division by m is r, the we write

$$n = r \ \text{ modulo } \ m\,.$$

We have already seen how to compute powers of 10 modulo 7, for example.

If N is any integer not divisible by the prime p then

$$N^{p-1} = 1 \ \text{ modulo } \ p\,.$$

We shall actually prove, because it is easier to do so, the almost equivalent result that

$$N^p = N \ \text{ modulo } \ p\,.$$

for all non-negative integers N.

The proof of this will be by induction on N.

For $N = 1$ the result is trivial. Assume it to be true for N and we shall prove it true for $N + 1$. But first we need to recall the **binomial theorem**.

Lemma.

$$(x+1)^n = x^n + nx^{n-1} + \frac{n(n-1)}{2}\,x^{n-2} + \cdots + nx + 1\,.$$

The coefficient here of x^r is

$$\frac{n(n-1)\cdots(n-(r-1))}{1\cdot 2\cdots r} = \frac{n!}{r!(n-r)!}\,.$$

Lemma. *If p prime number then all the coefficients in the binomial expansion of $(x+1)^p$ are equal to 0 modulo p except the first and the last.*

This is because as long as $r \neq 0$ or p, all the factors of the dominator of the coefficient of x^k with $0 < k < p$ are less than p, so can't cancel out the factor p in the numerator. We know at least that the coefficient is an integer because $(x+1)^p$ is obtained by multiplying p factors of $(x+1)$ together.

Now let's apply this to show that $N^p = N \ \text{ modulo } \ p$ for all N. We assume that $N^p = N$ and want to looka t $(N+1)^p$. By the lemma

$$(N+1)^p = N^p + 1 \quad \text{ modulo } p$$

but modulo p, by the induction assumption, $N^p = N$, so this gives us $(N+1)^p = N+1$ modulo p.

Lemma *If k is the smallest integer such that $N^k = 1$ modulo p and n is any other integer such that $N^n = 1$ modulo p, then $k|n$.*

Suppose $N^n = 1$ modulo p. Divide n by p to get

$$n = qp + r \ (0 \leq r < p) \ .$$

Then

$$N^n = N^q p + r = (N^p)^q N^r = N^r \text{ modulo } p$$

But this is a contradiction unless $r = 0$.

Corollary. *If k is the smallest positive number with $N^k = 1$ modulo p, then $k|p-1$.*

Corollary. *If p is a prime number, then the repeat length of the fraction $1/p$ in base B expression divides $p-1$.*

Lets' look at an example. Let $p = 1/13$. The decimal expression for $1/13$ is $0.0769230769123\ldots$. It does repeat every 12 digist, but its true repeat is 6. Thus each string of 13 conatins two repeating strings of 6 digits. Thsi is always eh way it works—the true repeat has to occur an even number of times inside every string of $p-1$.

5. Denominators that are not prime

Let's now look at some $1/n$ where n is no longer a prime number. We want n to be relatively prime to 1), so the smallest possible n is $3 \cdot 7 = 21$. We have

$$\frac{1}{21} = 0.047691047691\ldots$$

so the repeat is again 6. Where does that come from?

The explanation depends on a trick by which arithmetic modulo 21 is reduced to arithmetic modulo 3 and 7, simultaneously. We map every number modulo 21 onto a pair of numbers, the first its remainder after division by 3, the second after division by 7. For example the number 17 corresponds to $(2, 3)$. Here is a table of all pairs:

n	n modulo 3	n modulo 7
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	5
6	0	6
7	1	0
8	2	1
9	0	2
10	1	3
11	2	4
12	0	5
13	1	6
14	2	0
15	0	1
16	1	2
17	2	3
18	0	4
19	1	5
20	2	6

If you read it carefully, you will see that no pair occurs twice.

Now we make a table of powers of 10 modulo 21, but along with the corresponding pairs:

1	1	1
10	1	3
16	1	2
13	1	6
4	1	4
19	1	5
1	1	1

We see that the reason for the repeat of 6 is because the powers of 10 modulo 3 are all just 1, and because $6 = 7 - 1$, so of course $10^6 = 1$ modulo 7.

This technique works for any product of primes:

Proposition. (Chinese Remainder Theorem) *If $n = pq$, a product of two relatively prime numbers, then the map*

$$m \mapsto (m \ \ \textit{modulo} \ \ p, m \ \ \textit{modulo} \ \ p)$$

is an exact correspondence between the numbers modulo n and pairs modulo p and q.

I'll give two proofs of this, one short, the other longer but constructive.

The first proof shows directly that there are no repeats of pairs. Suppose m_1 and m_2 correspond to the same pair $a, b)$. Then

$$\begin{aligned} m_1 &= a \ \ \text{modulo} \ ; p \\ m_2 &= a \ \ \text{modulo} \ ; p \\ m_1 &= b \ \ \text{modulo} \ ; q \\ m_2 &= b \ \ \text{modulo} \ ; q \\ M = m_1 - m_2 &= 0 \ \ \text{modulo} \ ; p \\ M = m_1 - m_2 &= 0 \ \ \text{modulo} \ ; q \end{aligned}$$

The difference M is then divisible by both p and q. Say $M = p \cdot M_p$. Then $q | p \cdot M_p$ where p and q are relatively prime, so $q | M_p$ and $pq | M$, which means that modulo n the numbers m_1 and m_2 are the same. That ends the first proof.

For the second proof, we'll see how to rec0over m from it scorresponding pair (a, b).

Lemma. *If a and b are two relatively prime numbers then any equation*

$$ax = c \ \ \textit{modulo} \ \ b$$

has a unique solution modulo b, which we can find by the Euclidean algorithm.

The Euclidean algorithm gives us k and ℓ such that

$$ka + \ell b = 1 \ .$$

This says that modulo b the number k is a multiplicative inverse of a. To solve

$$ax = c \ \ \text{modulo} \ \ b$$

we multiply both sides by k to get

$$x = kc \ \ \text{modulo} \ \ b \ .$$

In the future, I'll write a^{-1} for this inverse when it makes sense.

The m we are looking for satsifies

$$m = a + Ap, \quad m = b + Bq$$

for some unknown integers A and B of which we have to find one.

$$\begin{aligned} a + Ap &= b + Bq \\ Ap &= b - a \ \text{ modulo } \ q \\ A &= (b-a)p^{-1} \ \text{ modulo } \ q \end{aligned}$$

For example, let's calculate in this way the integer modulo 77 that corresponds to $(5, 8)$ modulo 7 and 11. First of all, the Euclidean algorithm gives us

$$8 \cdot 7 - 5 \cdot 11 = 1$$

so that modulo 11 the inverse of 7 is 8.

We now want to find A such that

$$\begin{aligned} 5 + A \cdot 7 &= 8 \ \text{ modulo } \ 11 \\ A &= (8-5) \cdot 7^{-1} \ \text{ modulo } \ 11 \\ &= (8-5) \cdot 8 \ \text{ modulo } \ 11 \\ &= 24 = 2 \end{aligned}$$

and sure enough $m = 5 + 2 \cdot 7 = 8 + 11 = 19$.

If n is any integer, let $\phi(n)$ be the number of integers in the range $(0, n)$ that are relatively prime to n. This can be calculated by recursion pretty easily because

- *If $n = p^k$ where p is prime, then $\phi(n) = (p-1)p^k$.*

If $n = \prod p_i^{n_i}$ is relatively prime to B, then the repeat length of $1/n$ modulo B divides the least common multiple of the $\phi(p_i^{n_i}$.