Chapter 5

Decimal Fractions

In converting common fractions into decimal fractions, confining our interest to proper fractions, we find the following cases:

$$\frac{3}{5} = 0.6, \qquad \frac{3}{40} = 0.075 \tag{I}$$

in which the decimal terminates, i.e., the final digit is zero.

$$\frac{1}{3} = 0.\bar{3}333\ldots, \qquad \frac{1}{7} = 0.\overline{142857}142857\ldots \tag{II}$$

where the decimal fraction consists of a group of digits repeated over and over, marked by overbars. This group is called the period of the decimal. In fractions of this class the period begins immediately after the decimal point.

$$\frac{5}{6} = 0.8\bar{3}33\ldots, \qquad \frac{7}{30} = 0.2\bar{3}333\ldots \tag{III}$$

which are also periodic. However, here the period does not begin immediately after the decimal point.

The first example is trivial, for we can convert the given fraction into one having a power of 10 as a denominator: $\frac{3}{5} = \frac{6}{10} = 0.6$. In fact *a terminating decimal fraction can occur only if a/b has a denominator of the form $b = 2^{\alpha}5^{\beta}$.* Suppose $b = 2^{\alpha}5^{\beta}$. If $\alpha > \beta$ ($\alpha < \beta$) by multiplying numerator and denominator by $5^{(\alpha-\beta)}$ $[2^{(\beta-\alpha)}]$, we can convert the given fraction into one that has 10^{α} $[10^{\beta}]$ as denominator. For example,

$$\frac{3}{40} = \frac{3}{2^3 5} = \frac{5^2}{5^2} \cdot \frac{3}{2^3 \cdot 5} = \frac{75}{10^3} = \frac{75}{1000} = 0.075.$$

But if the denominator contains a factor different from 2 or 5, this is impossible — for example $7 \cdot b$ can never equal any power of 10. Thus in general we cannot transform a common fraction with an arbitrary denominator into a terminating decimal fraction.

And usually when converting a proper fraction into a decimal, we find that the long division becomes an infinite process. As an example consider $\frac{3}{41}$:

$$\begin{array}{r@{}l}
 & 0.\overline{07317} \\
41 & \overline{)3} \\
 & 30 \\
 & 300 \\
 & \underline{287} \\
 & 130 \\
 & \underline{123} \\
 & 70 \\
 & \underline{41} \\
 & 290 \\
 & \underline{287} \\
 & 3
\end{array}$$

Reaching the remainder 3, we pause, for we recognize this to be identical with the dividend. If the division were to be continued, then the sequence of quotients would repeat itself, i.e., $\frac{3}{41} = 0.\overline{07317}$ is infinitely repeating—the infinite process of division is periodic.

At first glance the periodicity may seem to result from the fact that there are only ten digits which may appear in the quotient, i.e., that every decimal fraction is periodic. However, this is impossible because we can construct examples of non-periodic decimal fractions, e.g., 0.101001000100001 . . . , where the nth 1 is followed by n zeros. Furthermore we can find decimals with very long periods—try $\frac{1}{17}$ which has sixteen digits in its period—so that some digits must reappear. The key to this process is not found in the quotients. Rather we must look to the remainders.

Suppose a/b is a reduced fraction; then there are $b - 1$ possible remainders. Zero is excluded, for the termination of the decimal fraction is identical with $b = 2^{\alpha}5^{\beta}$—the case completely dismissed. Thus we consider the cases where b contains primes other than 2 and 5—and in particular we restrict our attention to case (II) where all the prime factors of b are different from 2 and 5. We will show that *if a/b is a reduced fraction and b is coprime to* 10, *then the period begins just after the decimal point,* i.e., that $(b, 10) = 1$ characterizes the fraction of case (II).

Suppose we find a remainder equal to some later remainder, i.e., $r_k = r_{k+\lambda}$. This certainly must happen, for there are only $b - 1$ possible remainders. If the assertion is true, then the first such remainder must in fact be the numerator of the fraction, for the dividend is counted as a remainder. From $r_k = r_{k+\lambda}$, we easily conclude that $r_{k+1} = r_{k+\lambda+1}$. But to show that the period must begin as early as possible, we must work backwards. We arrive at r_k and $r_{k+\lambda}$ from:

$$10r_{k-1} = q_k \cdot b + r_k, \qquad 10r_{k+\lambda-1} = q_{k+\lambda} \cdot b + r_{k+\lambda}.$$

Subtracting, we have

$$10(r_{k-1} - r_{k+\lambda-1}) = b(q_k - q_{k+\lambda}).$$

But b is coprime to 10, so that by Euclid's lemma b divides

$$r_{k-1} - r_{k+\lambda-1}, \qquad \text{i.e.,} \qquad r_{k-1} - r_{k+\lambda-1} = m \cdot b.$$

But since all $r_\nu < b$ and the absolute value of the difference of two numbers less than b must itself be less than b, i.e., $|r_{k-1} - r_{k+\lambda-1}| < b$, we have $r_{k-1} - r_{k+\lambda-1} = 0$, or $r_{k-1} = r_{k+\lambda-1}$. So that if b is coprime to 10 (the essential point used in the proof) and $r_k = r_{k+\lambda}$, then stepwise we can show that all the remainders with indices differing by λ must be equal. Hence in case (II), the periodicity must start as early as possible — we are sure that it begins immediately after the decimal.

How long is the period of such a fraction? If λ denotes the length of the period, we have found that $\lambda \leq b - 1$. For the fraction, $\frac{1}{7}$, λ is 6, for $\frac{1}{17}$ it is 16, while 3 has a period of one digit. We can improve this inequality considerably. *In fact, the only residues (remainders) that can appear must be coprime to b.* If r_k is coprime to b, then rewriting

$$10r_k = q_{k+1} \cdot b + r_{k+1}$$

as

$$r_{k+1} = 10r_k - q_{k+1} \cdot b,$$

we see that, since $(10, b) = 1$ and $(r_k, b) = 1$, r_{k+1} and b can have no divisor in common. As a/b is reduced, i.e., $(a, b) = 1$, we can show stepwise that each of the remainders is coprime to b, for the preceding one is also. Thus only residues coprime to b can appear.

If b is a prime, then all the integers less than b are coprime to b. In other cases the number of coprime residues is considerably smaller. Let us introduce the customary notation: $\phi(b)$ denotes the number of residues coprime to b. In number theory, $\phi(n)$ is known as Euler's function — a function quite interesting on its own merits which we shall consider again. Here we give only a few numerical examples easily computed by inspection. First we note that $\phi(b) \leq b - 1$.

$$\begin{aligned} &\phi(2) = 1, \quad &&\phi(3) = 2, \quad &&\phi(4) = 2, \quad &&\phi(5) = 4, \\ &\phi(6) = 2, &&\phi(7) = 6, &&\phi(8) = 4, &&\phi(9) = 6, \\ &\phi(10) = 4, \ldots . \end{aligned}$$

Not only is $\lambda \leq b - 1$, but as we have just shown, $\lambda \leq \phi(b) \leq b - 1$. Moreover, not all numbers less than $\phi(b)$ can serve as length of a period. Shortly we shall prove the essential result: λ must be a divisor of $\phi(b)$. For $\frac{1}{7}$, $\lambda = \phi(7) = 6$; while for $\frac{3}{41}$, $\lambda = 5$ which is a divisor of $\phi(41) = 40$. However, if we did not know that $\frac{3}{41}$ has a period of length 5, we could only say that λ was one of the numbers 2, 4, 5, 8, 10, 20, or 40, the divisors of $\phi(41)$ — which one we could not foretell. In general the best that may be said is that λ is among the divisors of $\phi(b)$, where $\lambda = \phi(b)$ is counted as a divisor.

Let us consider in detail the example $\frac{1}{7}$

$$
\begin{array}{r@{}l}
 & 0.\overline{142857} \\
7\overline{)} & 1 \\
 & 10 \\
 & \underline{\ 7} \\
 & 30 \\
 & \underline{28} \\
 & 20 \\
 & \underline{14} \\
 & 60 \\
 & \underline{56} \\
 & 40 \\
 & \underline{35} \\
 & 50 \\
 & \underline{49} \\
 & 1
\end{array}
\qquad
\begin{array}{ccc}
 & 1 & \\
5 & & 3 \\
4 & & 2 \\
 & 6 &
\end{array}
$$

and look into the remainders which appear in the order: 1, 3, 2, 6, 4, 5, that can be written as a cycle. Since all the possible remainders of 7 are included in this cycle, we can write down $\frac{2}{7}$ immediately. Its sequence of remainders must begin with 2 and continue in the order: 2, 6, 4, 5, 1, 3. Hence $\frac{2}{7} = 0.285714$. Similarly $\frac{5}{7} = 0.714285$. And the other multiples of $\frac{1}{7}$ could be found by a cyclic interchange of the remainders.

Next let us examine $\frac{1}{21}$. First what is $\phi(21)$? Instead of counting the numbers coprime to 21, it is easier to count and eliminate those numbers less than or equal to 21 that have factors in common with it. Of such numbers seven are three-fold and three seven-fold; but we have counted 21 twice, so that there are nine numbers less or equal to 21 that are not coprime to it. Hence $\phi(21) = 21 - 9 = 12$. Hence we expect λ to be either 2, 3, 4, 6, or 12.

$$
\begin{array}{r@{}l}
 & 0.\overline{047619} \\
21\overline{)} & 1 \\
 & 10 \\
 & 100 \\
 & \underline{\ 84} \\
 & 160 \\
 & \underline{147} \\
 & 130 \\
 & \underline{126} \\
 & 40
\end{array}
$$

```
   21
  190
  189
    1
```

Here we find $\lambda = 6$ and the sequence of remainders: 1, 10, 16, 13, 4, 19. Clearly we can read off $\frac{16}{21} = 0.761907$. And similarly we could write down $\frac{10}{21} \cdot \frac{13}{21} \cdot \frac{4}{21}$, and $\frac{19}{21}$. However, as the remainder 2 does not appear in this list, we cannot write down $\frac{2}{21}$. Let us form this decimal fraction:

```
     0.095238
 21)2
    20
    200
    189
     110
     105
       50
       42
        80
        63
        170
        168
          2
```

Here λ is again 6 and the new sequence of residues is: 2, 20, 11, 5, 6, 17, which we derived by considering the first possible remainder missing from the previous list. It is clear that the second scheme cannot contain any residues belonging to the first, for if it did, as the periodicity begins just after the decimal point, both sequences would be identical. Thus we have found all possible remainders, a fact to be proved later, and we suspect *that the period is indeed independent of the numerator.*

We are working with the reduced fractions a/b, i.e., $(a, b) = 1$, of the sort where b is coprime to 10; and we have found that the period begins immediately after the decimal point, i.e., $r_k = r_{k+\lambda}$ and $a = r_0 = r_\lambda$. What does this mean? Writing out the division we have:

$$\begin{aligned} 10r_0 &= b \cdot q_1 + r_1 \\ 10r_1 &= b \cdot q_2 + r_2 \\ &\vdots \\ 10r_{\lambda-2} &= b \cdot q_{\lambda-1} + r_{\lambda-1} \\ 10r_{\lambda-1} &= b \cdot q_\lambda + r_\lambda . \end{aligned}$$

Multiplying the first equation by $10^{\lambda-1}$, the second by $10^{\lambda-2}$, . . . , the last but one by 10, we have:

$$\begin{aligned}
10^{\lambda} \cdot r_0 &= b \cdot q_1 10^{\lambda-1} + r_1 \cdot 10^{\lambda-1} \\
10^{\lambda-1} \cdot r_1 &= b \cdot q_2 10^{\lambda-2} + r_2 \cdot 10^{\lambda-2} \\
\vdots \quad &\qquad \vdots \qquad\qquad\quad \vdots \\
10^2 \cdot r_{\lambda-2} &= b \cdot q_{\lambda-1} \cdot 10 + r_{\lambda-1} 10 \\
10 \cdot r_{\lambda-1} &= b \cdot q_{\lambda} + r_{\lambda} .
\end{aligned}$$

When these are added, except for the first and last, the factors involving the r's will cancel, so we obtain:

$$10^{\lambda} r_0 = b(q_1 10^{\lambda-1} + q_2 10^{\lambda-2} + \cdots + q_{\lambda-1} 10 + q_{\lambda}) + r_{\lambda} = b \cdot Q + r_{\lambda},$$

where Q, the expression in parentheses, is the period written in the form of an integer, e.g., $\frac{1}{7} = 0.\overline{143857}$,

$$Q = 10^5 + 4 \cdot 10^4 + 2 \cdot 10^3 + 8 \cdot 10^2 + 5 \cdot 10 + 7 = 142857.$$

Since $r_0 = r_{\lambda} = a$, we have $10^{\lambda} a - a = b \cdot Q$ of $a(10^{\lambda} - 1) = b \cdot Q$. And as a and b are coprime, b divides $10^{\lambda} - 1$. This tells us two things:

1. *there is a λth power of* 10 *which diminished by* 1 *is divisible by* b;
2. λ *is independent of* a, for clearly λ is the smallest such exponent that we could choose such that $10^{\lambda} - 1$ is divisible by b.

Thus the results we obtained in the case $b = 21$ are not fortuitous—necessarily the period of $\frac{1}{21}$ has the same length as that of $\frac{2}{21}$. On closer examination of the sequences of residues:

$$\frac{1}{21} \quad \text{yielding} \quad 1,\ 10,\ 16,\ 13,\ 4,\ 19,$$

$$\frac{2}{21} \quad \text{yielding} \quad 2,\ 20,\ 11,\ 5,\ 8,\ 17,$$

we see that there is indeed a relation between them, namely those of the second sequence are twice the corresponding one of the first, diminished by 21, if necessary, to produce a residue less than 21, e.g., from 16 we have $2 \cdot 16 = 32$ and $32 - 21 = 11$, the third residue of the second sequence, etc.

Now we can easily show that *the length of the period,* λ, *must be a divisor of* $\phi(b)$. Dividing b into 1, we obtain a sequence of residues: $1, r_1, r_2, \ldots, r_{\lambda-1}$, all of which are coprime to b. If the number of these does not exhaust $\phi(b)$, then we can choose some other residue coprime to b, say r_0', and dividing this by b, obtain a new sequence of residues: $r_0', r_1', \ldots, r_{\lambda-1}'$, which must be of the same length as the first. All members of this second scheme must be different from those of the previous one. For if not, since one residue entirely determines the whole sequence of residues, if a remainder of both sequences were identical, then the second would merely be the first all over again. But r_0' is not contained in the first.

Hence we have found 2λ residues which are all different. These may or may not exhaust $\phi(b)$. If not, we find a third set of residues, λ in number, different from the preceding, efc. Since $\phi(b)$ is finite, eventually we must exhaust it by forming new and entirely different sequences of residues, which can only occur in sets containing λ each. Thus $\phi(b)$ must be a multiple of λ.

$$\phi(b) = k \cdot \lambda(b),$$

where we write $\lambda(b)$ to emphasize the dependence of λ on b. As examples we have:

$\phi(21) = 12,$	$\lambda(21) = 6,$	$k = 2,$
$\phi(41) = 40,$	$\lambda(41) = 5,$	$k = 8,$
$\phi(\ 7) = \ 6,$	$\lambda(\ 7) = 6,$	$k = 1.$

Let us return to the first conclusion we drew from the relation $a(10^\lambda - 1) = b \cdot Q$, namely: $10^\lambda - 1$ is divisible by b. To derive a more abstract result from this, we note that $x^k - 1$ is divisible algebraically by $x - 1$, i.e., $(x^k - 1) = (x - 1)(x^{k-1} + x^{k-2} + \cdots + 1)$. Replacing x by 10^λ, we have: $10^{\lambda \cdot k} - 1 = (10^\lambda - 1)X$, where X is a polynomial in 10^λ. Since this is an algebraic identity, we may choose such a k that $10^{k\lambda} = 10^{\phi(b)}$. And as a plays no role in determining λ or k, putting $a = 1$, we have $10^\lambda - 1 = bQ$. This gives $10^{\phi(b)} - 1 = bQX$. Whence we conclude: $10^{\phi(b)} - 1$ *is divisible by b, provided* $(10, b) = 1$—a theorem on integers, one having nothing to do with fractions.

This is the famous Fermat–Euler theorem. If p is a prime, $\phi(p) = p - 1$, the formula reads $10^{p-1} - 1$ is divisible by P, provided $p \neq 2, 5$. This theorem was known to Fermat, one of the very greatest mathematicians of the 17th century, if not of all time—a jurist whose contributions to mathematics, his hobby, made him immortal, whereas his jurisprudence is forgotten. Euler put the theorem in its most general form, which we shall shortly produce, but the essential idea is due to Fermat. Let us make a few examples: Taking p as small as possible, i.e., 3, we have $10^2 - 1 = 99$ is divisible by 3; or for $p = 7$, we have $10^6 - 1 = 999999$ is divisible by 7 (recall $10^6 - 1 = 7.142859$).

Here we have the special number 10 in our formula, as a result of the fact that we used the decimal system to write our fractions. However, the whole argument could be reproduced using a g-adic number system, in which $\alpha\beta\gamma$ means $\alpha g^2 + \beta g + \gamma$ and, $\alpha\beta\gamma$ means $\alpha g^{-1} + \beta g^{-2} + \gamma g^{-3}$, defining periodic decimal fractions in the same way. (To the mathematician the discussion of these different number systems isn't very interesting, for they are merely notations that have nothing to do with the fundamental nature of numbers. The one that we use is merely a linguistic heritage—probably a biological accident in that we have 10 fingers—although our language does have remnants of other systems of notation, notably dozen, score, and gross.)

Thus we may replace 10 by any number coprime to b, and obtain: $g^{\phi(b)} - 1$ *is divisible by b, provided that g and b are coprime,* the Fermat–Euler theorem in its most general formulation. This theorem we see provides the background for the systematic study of decimal fractions.

Let us make an example: $2^{p-1} - 1$ is divisible by p, where p is a prime greater than 2.

$p = 3$:	$2^2 - 1 = 4 - 1 = 3$	divisible by 3;	
$p = 5$:	$2^4 - 1 = 16 - 1 = 15$	divisible by 5;	
$p = 7$:	$2^6 - 1 = 64 - 1 = 63$	divisible by 7;	
$p = 11$:	$2^{10} - 1 = 1024 - 1 = 1023$	divisible by 11 ,	etc.

To satisfy curiosity we state here Fermat's Last Theorem. We could show that there are infinitely many integers, the so-called Pythagorean numbers, that satisfy the equation $a^2 + b^2 = c^2$, e.g., $3^2 + 4^2 = 5^2$, $5^2 + 12^2 = 13^2$, etc. Fermat claimed there were no integers satisfying $a^n + b^n = c^n$ for $n > 2$. We do now know that this is true for many n, but it is still not proved in full generality. In part the interest of the theorem lies in the provocative way in which it was first stated. Fermat wrote the assertion on his copy of Diophantus together with the remark, "...I have discovered a truly marvellous demonstration which this margin is too narrow to contain." However, the importance of the theorem lies not in its content, but in the mathematics developed in the attempts to prove it—the efforts to do so in the 19th Century yielded the new field of algebraic number theory and the notion of ideal numbers developed first by Kummer.

To close this chapter, let us set the converse problem: *Given a periodic decimal fraction, to what common fraction does it belong*? We have $a(10^\lambda - 1) = bQ$, where Q is the period of the decimal fraction read as an integer. Thus $a/b = Q/(10^\lambda - 1)$. For example, to what common fraction does $0.\overline{09}$ belong? Here $Q = 9$, $\lambda = 2$, so that $a/b = 9/(10^\lambda - 1) = 9/99 = 1/11$.

Finally we note that the third case, which has not been treated here, that in which the period of the decimal fraction does not begin immediately after the decimal point, is the mixed case in which b has a divisor in common with 10.

Note to Chapter 5

In recent years some remarkable applications of the Fermat–Euler theorem have come to light. It was a surprise to many people to learn that a procedure was developed whereby a secret message could be encoded and the person encoding the message would not be able to reverse the process and decode the message. The procedure is as follows. Let N be a very large number which has at least two prime factors. Assume for simplicity that $N = p_1p_2$, the product of two large primes. Then $\phi(N) = (p_1 - 1)(p_2 - 1)$. Now, if p_1 and p_2 are very large, then it could take a computer hundreds of years to factor N, and hence a person knowing only N could never really determine $\phi(N)$. Let E and D be two integers satisfying $ED = \phi(N) + 1$. The person encoding the message is given the numbers N and E. As shown above, he cannot know D. Let us assume he has a message M (given in the form of a large number, say). Then he encodes the message by computing M^E, dividing this by N, and computing the remainder R. In other words, $M^E - R$ is exactly divisible by N. Then R will be the encoded message. It is not possible to decode this message without knowing D. To decode the message, one simply takes R^D and computes the remainder after dividing by N. This is based on the fact that $R^D \equiv M^{ED} \equiv M^{\phi(N)+1} \equiv M \pmod{N}$ by Euler's theorem. As a simple example, take $N = 33, \phi(N) = 20, E = 7, D = 3, M = 2$. Since $2^7 \equiv 29 \pmod{33}$, the encoded message is $R = 29$. To decode the message, note that $29^3 \equiv 2 \pmod{33}$.