The Mathematics Enthusiast

Volume 13
Number 3 *Number 3*

Article 3

8-2016

The secret life of 1/n: A journey far beyond the decimal point

Christopher Lyons

The secret life of $1/n$: A journey far beyond the decimal point

Christopher Lyons
California State University, Fullerton

ABSTRACT: The decimal expansions of the numbers $1/n$ (such as $1/3 = 0.3333...$, $1/7 = 0.142857...$) are most often viewed as tools for approximating quantities to a desired degree of accuracy. The aim of this exposition is to show how these modest expressions in fact deserve have much more to offer, particularly in the case when the expansions are infinitely long. First we discuss how simply asking about the *period* (that is, the length of the repeating sequence of digits) of the decimal expansion of $1/n$ naturally leads to more sophisticated ideas from elementary number theory, as well as to unsolved mathematical problems. Then we describe a surprising theorem of K. Girstmair showing that the digits of the decimal expansion of $1/p$, for certain primes p, secretly contain deep facts that have long delighted algebraic number theorists.

Keywords: Decimal expansions, rational numbers, primitive roots, class numbers

The Mathematics Enthusiast, **ISSN 1551-3440, vol. 13, no. 3**, pp. 189-216

Introduction

If we spend enough time punching numbers into a calculator—say, as students in a science or engineering class with a lot of numbers to crunch on our weekly homework assignments—it's likely we're going to start recognizing certain decimal expansions, whether we choose to or not. For instance, I'd wager that most readers are familiar with the following decimal expansions:

$$\begin{aligned} 1/2 &= 0.5 \\ 1/3 &= 0.3333333... \\ 1/4 &= 0.25 \\ 1/5 &= 0.2 \end{aligned}$$

Many will also recognize

$$1/6 = 0.1666666...$$

But how about the expansion of 1/7? I think we've all seen it:

$$1/7 = 0.142857142857142857...$$

But perhaps the "repeating part," which is the 6 digit sequence 142857, is a little too long to stick in most people's memories unless they intentionally put it there. Similarly, some of us know the expansion:

$$1/11 = 0.0909090909...$$

but if we boost the denominator up by 2 then most probably haven't memorized

$$1/13 = 0.076923076923076923...$$

The most common view of decimal expansions like the ones above is completely pragmatic: they help us approximate certain quantities to a desired degree, and perhaps some of the digits (if we're in a situation that also involves a bit of random error, such as a scientific measurement) are not to be entirely trusted. In these settings, one might look at the examples above and perhaps use something between 2 and 10 digits out of the whole decimal expansion, and then discard the rest through the usual process of rounding. But what if we were to pay attention to *all* of the digits past the decimal point? Is there anything more interesting that these decimal expansions have to offer besides their role as everyday computational workhorses?

In this exposition, we'll explore this question for the decimal expansions of the very simple class of numbers represented above, namely $1/n$ for integers $n \geqslant 2$. These might seem like incredibly mundane strings of digits, especially if one compares them to the decimal expansion of π, which is the object of much computational and popular attention. Yet as we'll see, even the simplest questions about the expansion of $1/n$ lead to unexpectedly sophisticated ideas, and to problems that have stumped mathematicians for at least two centuries and remain unsolved even today. We'll also discuss a discovery of Kurt Girstmair from the 1990s—which of course is relatively recent in the long history of our use of decimals—that shows how some of these expansions secretly contain information about certain integers that have been studied in number theory since at least the early 1800s. So in fact the decimal expansion of $1/n$ is often far from mundane!

Here's a brief overview of the contents of this article.

In Part 1, we focus on the overall structure of the decimal expansion of $1/n$, without paying much heed to the actual digits that appear. In §1.1, we determine those values of n for which the expansion of $1/n$ consists purely of a sequence of ℓ digits that repeats forever; in this case we call ℓ the *period* of the decimal expansion of $1/n$. For a given n, it may not be clear how large ℓ can be, and in §1.2 we place a basic restriction on its size, meeting a strange-looking function along the way called *Euler's ϕ-function*. We digress for a bit in §1.3

to discuss those values of n for which ℓ is as large as possible; this brings us face-to-face with the curious idea of a *primitive root* in number theory, and with an enduring mystery. We return in §1.4 to the general question of how we can determine ℓ in terms of n, by making a significant improvement to our result from §1.2. In §1.5, we finally see what lies at the very core of this question.

Part 2 is shorter than the first, and also less detailed due to the depth of some of the topics it surveys. In this part, we return to the expansions studied in §1.3 for which the period of $1/n$ is as long as possible, and we look more closely at the repeating strings of digits they involve. In §2.1, we discuss Girstmair's result, which shows that in spite the random-looking appearance of these strings of digits, they can actually encode the values of special number theoretic quantities that were first introduced by Gauss. We describe these quantities in §2.2, after surveying a small portion of the theory of *binary quadratic forms*, a venerated and seemingly far-flung domain of 18th and 19th century number theory.

In Part 3, we quickly mention some more general statements and situations that have been omitted in the previous parts, and give some suggestions for further reading.

The Appendix contains a proof a result quoted in §1.5

To finish this introduction, let me say that this article has its origins in a talk that I've given to several undergraduate audiences. For this reason, I've chosen to keep the tone somewhat informal, to keep the pace relaxed, and to give plenty of examples. Nothing in this exposition is new, especially since the subject of periodic decimal expansions has piqued the interest of many for centuries (see [Dic] for a detailed account). There are many articles on various aspects of periodic decimal expansions that have been written for a fairly general mathematical audience, such as [JP, Lea, Ros, SF, Gir3] which are of varying levels and have some intersection with the topics discussed here. Yet most of the natural questions explored here are still unknown to even the average mathematics undergraduate, despite being understandable to anyone who has a basic familiarity with the idea of an infinite decimal expansion. In a world where mathematicians are often asked why math doesn't stop after calculus, one of the underlying motivations here is show how *nontrivial questions, sophisticated ideas, and even unsolved problems can arise from mathematical objects that are as commonplace as the decimal expansion of* $1/n$.

It's my pleasure to thank Bharath Sriraman for inviting me to turn an earlier set of notes on this topic into the present article. I also thank the various undergraduates who have listened to me speak on some of these topics and helped improve my exposition.

1 How long is the decimal expansion of $1/n$?

This part will explore the question in the title, in more than one sense. Before getting into things, I want to set down two items of notation. The first is a handy device that you've probably seen before: if a sequence of digits in a decimal expansion repeats forever, we'll indicate this by putting a line over that sequence. Three examples are:

$$1/3 = 0.\overline{3}, \qquad 1/6 = 0.1\overline{6}, \qquad 1/7 = 0.\overline{142857}.$$

The second notational device will help in situations where a decimal representations might be confused with a product. Usually we see the expression $d_1d_2d_3$ and interpret it as the product of the quantities d_1, d_2, and d_3. For this reason, I'll often use a `typewriter font` in instances where I'm viewing the variable as a decimal digit. In particular, when I write $\mathtt{d}_1\mathtt{d}_2\mathtt{d}_3$, this should be viewed as the usual decimal representation of the integer $\mathtt{d}_1 \cdot 10^2 + \mathtt{d}_2 \cdot 10 + \mathtt{d}_3$; thus if $\mathtt{d}_1 = 3, \mathtt{d}_2 = 7, \mathtt{d}_3 = 5$, then the expression $\mathtt{d}_1\mathtt{d}_2\mathtt{d}_3$ represents the integer 375 and *not* $3 \cdot 7 \cdot 5 = 105$.

1.1 Some preliminary steps

At some point in our mathematical education we come across the fact that, when we look past the decimal point, the decimal expansion of a rational number is either finite in length or it eventually repeats the same finite sequence forever. If we look specifically at the rational number $1/n$, when is its decimal expansion finite and when is it infinite? If it's infinite, when does it start out with some initial "non-repeating part" before reaching a repeating sequence (such as $1/28 = 0.03\overline{571428}$) and when is it "purely repeating" (such as $1/41 = 0.\overline{02439}$)?[1] The answer is summarized in the following:

Proposition 1.1. *Let $n \geqslant 2$ be an integer.*

(a) The decimal expansion of $1/n$ is finite if and only if n is not divisible any primes other than 2 and 5.

(b) Suppose the decimal expansion of $1/n$ is infinite (meaning n is divisible by at least one prime other than 2 or 5). Then the decimal expansion is of the form

$$1/n = 0.\overline{\mathtt{d}_1\mathtt{d}_2\ldots\mathtt{d}_\ell}$$

for some digits $\mathtt{d}_1, \ldots, \mathtt{d}_\ell$ if and only if n is divisible by neither 2 nor 5.

So looking at part (b), we see that the non-repeating portion of the decimal expansion of $1/28$ is explained by the fact that $4 = 2^2$ divides 28, while $1/41$ is purely repeating because 2 and 5 don't divide 41. I'll also note that the condition in part (b) can be stated with fewer words: instead of saying that n is divisible by neither 2 nor 5, we can say that the greatest common divisor of n and 10 is 1, which we write as $\gcd(n, 10) = 1$. We'll often use this more concise phrasing below.

Now why are the statements in Proposition 1.1 true? I don't want to dive into a full proof here, but some examples will help highlight the most interesting points. To demonstrate one direction of the statement (a), look at $n = 4000 = 2^5 \cdot 5^3$: we have

$$\frac{1}{4000} = \frac{1}{2^5 \cdot 5^3} = \frac{5^2}{2^5 \cdot 5^5} = \frac{25}{10^5} = 0.00025.$$

This trick will work in general: if $n = 2^a \cdot 5^b$, then we can write $1/n$ as some integer divided by a power of 10 (which is what it really means to have a finite decimal expansion!), simply be "adjusting" the number of 2's or 5's in the denominator to get a power of 10 and then compensating in the numerator. Looking at the other direction of (a), if the expansion of $1/n$ is finite, then this means $1/n = m/10^k$, and hence $nm = 10^k$. So a prime dividing n also divides 10^k, implying that prime is either 2 or 5.

The statement (b) is more interesting to think about because it gets to the heart of what an infinite decimal expansion is: a convergent infinite geometric series. Consider the infinite decimal expansion $0.079\overline{54}$. Writing it more verbosely as

$$\begin{aligned} 0.079\overline{54} &= 0.079 + 0.00054 + 0.0000054 + 0.000000054 + \cdots \\ &= \frac{79}{10^3} + \left(\frac{54}{10^5} + \frac{54}{10^7} + \frac{54}{10^9} + \cdots\right), \end{aligned}$$

we see that the quantity in parentheses is an infinite geometric series whose first term is $54/10^5$ and whose ratio is $1/10^2$. So by the main theorem on infinite geometric series, we can conclude

$$0.079\overline{54} = \frac{79}{10^3} + \frac{54/10^5}{1 - 1/10^2} = \frac{7}{88}.$$

This number is of course not of the form $1/n$, but it is rational and makes the point that infinite decimal expansions that are eventually periodic are always equal to rational numbers.

[1] At this point, I'm hoping these notions of "finite" vs. "infinite" decimal expansions, and "non-repeating parts", are intuitive enough. But see §1.2 for a more precise definition of these terms using the *shift operator*.

Moreover, after studying this example carefully, one can also see how similar steps will show that

$$0.\overline{\mathtt{d}_1\mathtt{d}_2\mathtt{d}_3\ldots\mathtt{d}_\ell} = \frac{m/10^\ell}{1-1/10^\ell} = \frac{m}{10^\ell-1}, \tag{1.1}$$

where

$$m = \mathtt{d}_1\cdot 10^{\ell-1} + \mathtt{d}_2\cdot 10^{\ell-2} + \cdots + \mathtt{d}_{\ell-1}\cdot 10 + \mathtt{d}_\ell,$$

i.e., m is the positive integer that in decimal notation is written as $\mathtt{d}_1\mathtt{d}_2\mathtt{d}_3\ldots\mathtt{d}_\ell$. So if $1/n = 0.\overline{\mathtt{d}_1\mathtt{d}_2\mathtt{d}_3\ldots\mathtt{d}_\ell}$, this implies $nm = 10^\ell - 1$. Since the primes 2 and 5 don't divide $10^\ell - 1$, this says they don't divide n either. Now that gives one half of the statement in (b).

We still need to convince ourselves that if $\gcd(n,10) = 1$ then the decimal expansion of $1/n$ has the form $0.\overline{\mathtt{d}_1\mathtt{d}_2\mathtt{d}_3\ldots\mathtt{d}_\ell}$. Is that obviously true? Tracing through the steps above, we find this is the same as saying that if $\gcd(n,10) = 1$ then there is exponent ℓ such that n divides $10^\ell - 1$... as it happens, this is true, and it's one of the great theorems of elementary number theory:

Theorem 1.2 (Euler's Theorem, Version 1)**.** *Suppose $n \geqslant 3$ and $\gcd(n,10) = 1$. There exists an integer $\ell \geqslant 1$ such that n divides $10^\ell - 1$.*

There's another way of stating this theorem that I find to be even more disarming, because anyone with a basic understanding of multiplication can appreciate its intrigue:

Theorem 1.3 (Euler's Theorem, Version 2)**.** *Suppose we have a positive integer $n \geqslant 3$ whose last digit (or more precisely, whose digit in the ones place) is $1, 3, 7,$ or 9. Among the list*

$$n, 2n, 3n, 4n, \ldots$$

of positive multiples of n, there is an integer of the form 999...9.

For instance, when $n = 13$, the list looks like

$$13, 26, 39, 52, 65, \ldots 999999 = 13\cdot 76923, \ldots$$

and when $n = 41$ we find

$$41, 82, 123, 164, 205, \ldots 99999 = 41\cdot 2439, \ldots$$

We can convince ourselves that Theorem 1.2 is what we need for the other half of statement (b) in Proposition 1.1, by considering the example of $n = 41$: Starting from $99999 = 10^5 - 1 = 41\cdot 2439$, we find

$$\frac{1}{41} = \frac{2439}{10^5-1} = \frac{2439/10^5}{1-1/10^5} = \frac{2439}{10^5} + \frac{2439}{10^{10}} + \frac{2439}{10^{15}} + \cdots = 0.024390243902439 = 0.\overline{02439}.$$

In §1.2 and §1.4, we'll actually derive more precise versions of Euler's Theorem. But for now we ask: why is the version in Theorem 1.2 true? Let's be skeptical and suppose that it's *not* always true. That means we believe there is some value of n such that the infinite collection of integers

$$10-1, 10^2-1, 10^3-1, \ldots \tag{1.2}$$

doesn't contain any multiples of n. To state it differently, it means that when we divide any of these integers by n, the remainder is never 0. But what could that remainder possibly be? If it's not 0, then it must be $1, 2, 3, \ldots$ or $n-1$. But our list (1.2) is infinite, and there are only finitely many possible remainders. So that must mean that we can find (at least) two places in the list where the remainder is the same; let's call that common remainder r. Spelling this out, it means we have two exponents, say ℓ_1 and ℓ_2 with $1 \leqslant \ell_1 < \ell_2$, for which

$$10^{\ell_1} - 1 = nq_1 + r, \qquad 10^{\ell_2} - 1 = nq_2 + r.$$

(This is the formal way of saying that when $10^{\ell_i} - 1$ is divided by n, the quotient is q_i and the remainder is r.) When we subtract this expressions, we find

$$n(q_2 - q_1) = (10^{\ell_2} - 1) - (10^{\ell_1} - 1) = 10^{\ell_1}(10^{\ell_2 - \ell_1} - 1).$$

Now compare the left and right sides of this: we find that $10^{\ell_1}(10^{\ell_2-\ell_1} - 1)$ is a multiple of n. Since we assumed that n and 10 have no common factor, this must mean that in fact $10^{\ell_2-\ell_1} - 1$ is a multiple of n. But this goes against our belief that nothing in the list (1.2) is a multiple of n. So with this shaken belief, we decide to switch sides: Theorem 1.2 must always be true!

1.2 The period of $1/n$: A first approach

Up to this point, we've been a little loose with some of the terminology about our decimal expansions. For instance, one might argue that all numbers $1/n$ have an infinite decimal expansion, because we can write things such as

$$\frac{1}{2} = 0.5 = 0.50000... = 0.49999...$$

Similarly, one might be find the idea of the "repeating part" of an infinite decimal expansion to be ambiguous, since we can write things like

$$1/3 = 0.\bar{3} = 0.\overline{33} = 0.\overline{33333333}.$$

We can address these and other concerns by introducing the following device:

Definition 1.4. *For a real number $\alpha \in [0, 1)$, define the* shift operator $S : \mathbb{R} \to [0, 1)$ *by*

$$S(\alpha) = \{10\alpha\},$$

where $\{x\} = x - \lfloor x \rfloor$ is the fractional part of the real number x.

For example:

$$S(\pi) = \{10\pi\} = 10\pi - \lfloor 10\pi \rfloor = 10\pi - 31,$$

which in decimal expansions looks like

$$S(3.14159265...) = \{31.4159265...\} = 0.4159265...$$

As another example,

$$S\left(\frac{3}{7}\right) = \left\{\frac{30}{7}\right\} = \left\{4 + \frac{2}{7}\right\} = \frac{2}{7},$$

which in decimal expansions looks like

$$S(0.\overline{428571}) = \left\{4.\overline{285714}\right\} = 0.\overline{285714}.$$

These examples highlight why we're calling S the "shift" operator: it shifts the decimal point one place to the right and removes any digits to the left of the (newly located) decimal point. Now several concepts may be addressed in terms of this operator:

- A real number α has a finite decimal expansion if and only if $S^k(\alpha) = 0$ for some $k \geqslant 1$. (Note: $S^k(\alpha)$ denotes the composition of S with itself k times, and is not the kth power of $S(\alpha)$. For instance, $S^3(\alpha) = S(S(S(\alpha)))$.)

- Suppose that the decimal expansion of α is infinite. This expansion is periodic (i.e., "purely repeating") if $S^\ell(\alpha) = \alpha$ for some $\ell \geqslant 1$. The smallest such ℓ is called the *period* of the decimal expansion of α. We will often just call this the period of α.

n	**Decimal expansion of** $1/n$	**Smallest positive value of** $10^\ell - 1$ **divisible by** n
3	$0.\overline{3}$	$10^1 - 1 = 3 \cdot 3$
7	$0.\overline{142857}$	$10^6 - 1 = 7 \cdot 142857$
9	$0.\overline{1}$	$10^1 - 1 = 9 \cdot 1$
11	$0.\overline{09}$	$10^2 - 1 = 11 \cdot 9$
13	$0.\overline{076923}$	$10^6 - 1 = 13 \cdot 76923$
17	$0.\overline{0588235294117647}$	$10^{16} - 1 = 17 \cdot 5882352941176470$
19	$0.\overline{052631578947368421}$	$10^{18} - 1 = 19 \cdot 52631578947368421$
21	$0.\overline{047619}$	$10^6 - 1 = 21 \cdot 47619$
23	$0.\overline{0434782608695652173913}$	$10^{22} - 1 = 23 \cdot 43478260869565217391 3$
27	$0.\overline{037}$	$10^3 - 1 = 27 \cdot 37$
29	$0.\overline{0344827586206896551724137931}$	$10^{28} - 1 = 29 \cdot 344827586206896551724137931$

Table 1: An illustration of Proposition 1.6 for small values of n

- The decimal expansion of α is eventually periodic if $S^{h+\ell}(\alpha) = S^h(\alpha)$ for some $h \geqslant 0$ and $\ell \geqslant 1$. (In the case $h = 0$, we take $S^0(\alpha) = \alpha$; this allows periodic decimal expansions to be called eventually periodic as well.)

From this point forward, we're only going to concern ourselves with the case when the decimal expansion of $1/n$ is infinite and periodic. Thus: *From now on we assume that* $n \geqslant 3$ *is not divisible by* 2 *or* 5. Equivalently, we can state this assumption as $\gcd(n, 10) = 1$ or say that the last digit of n is either 1, 3, 7, or 9.

Our true focus of Part I is:

Question 1.5. *Given* $n \geqslant 3$ *with* $\gcd(n, 10) = 1$*, what is the period (of the decimal expansion) of* $1/n$*?*

As we saw in §1.1 (see equation (1.1) above), the use of geometric series and Theorem 1.2 allows us to relate the period of $1/n$ to a certain divisibility statement:

Proposition 1.6. *Suppose* $n \geqslant 3$ *and* $\gcd(n, 10) = 1$*. The period of* $1/n$ *is equal to the smallest integer* $\ell \geqslant 1$ *such that* $10^\ell - 1$ *is divisible by* n*.*

In Table 1, we've collected a small sample of data that displays the correspondence in this proposition. As the wild variation in this table suggests, for a given value of n, it's not so clear what the period of $1/n$ will be without doing a lot of calculation. For instance, just to select a rather large and arbitrary n, do you have a reasonable guess for the period of $1/15247$?[2]

But the situation is not quite as hopeless as Table 1 suggests. To see what we can say, let's start by making a careful study of the example $1/21 = 0.\overline{047619}$. What happens if we apply the shift operator to this number several times? In decimals, the outcome can be displayed as follows:

$$0.\overline{047619} \overset{S}{\rightsquigarrow} 0.\overline{476190} \overset{S}{\rightsquigarrow} 0.\overline{761904} \overset{S}{\rightsquigarrow} 0.\overline{619047} \overset{S}{\rightsquigarrow} 0.\overline{190476} \overset{S}{\rightsquigarrow} 0.\overline{904761} \overset{S}{\rightsquigarrow} 0.\overline{047619}$$

Alternatively (remembering that the definition of S is not actually given in terms of decimal expansions), we can also display this as

$$\frac{1}{21} \overset{S}{\rightsquigarrow} \frac{10}{21} \overset{S}{\rightsquigarrow} \frac{16}{21} \overset{S}{\rightsquigarrow} \frac{13}{21} \overset{S}{\rightsquigarrow} \frac{4}{21} \overset{S}{\rightsquigarrow} \frac{19}{21} \overset{S}{\rightsquigarrow} \frac{1}{21}$$

If we look at all of the fractions produced in the sequence above, they're all of the form $a/21$ where the numerator a has two properties:

[2]The period of 1/15427 happens to be 2496. See what I mean?

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\phi(n)$	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8

Table 2: Small values of Euler's ϕ-function

1. $1 \leqslant a < 21$

2. There are no primes dividing both a and 21. Equivalently, $\gcd(a, 21) = 1$.

Is this sort of thing going to be true for $1/n$ in general? Yes, and it follows from our assumption that n is not divisible by 2 or 5. To start with, if we define the integer $c = \lfloor 10/n \rfloor$ then

$$S\left(\frac{1}{n}\right) = \frac{10}{n} - \left\lfloor \frac{10}{n} \right\rfloor = \frac{10}{n} - c = \frac{10 - cn}{n}.$$

Is the fraction $(10 - cn)/n$ written in reduced form? If not, there is a prime p dividing both n and $10 - cn$ that we'll be able to cancel from the numerator and denominator; and this means p will also divide $10 = (10 - cn) - cn$, since this is a difference of two multiples of p. But we assumed n and 10 have no common prime divisors, so this must mean that no such p exists. In other words, $(10 - cn)/n$ is indeed in reduced form, and so we can say that $S(1/n) = a/n$ where $\gcd(a, n) = 1$. Moreover, we'll have $1 \leqslant a < n$ since $S(1/n) \in (0, 1)$.

With each successive application of S, we'll be able to make a similar argument: the fact that $\gcd(n, 10) = \gcd(a, n) = 1$ can be used to show $S(a/n) = a'/n$ for some integer a' satisfying (1) $1 \leqslant a' < n$ and (2) $\gcd(a', n) = 1$. Looking at these two properties that we've highlighted, it's now worth introducing the following number-theoretic function:

Definition 1.7. *Let $m \geqslant 2$ be a positive integer.* Euler's ϕ-function *is defined to be the number $\phi(m)$ of integers a that satisfy $1 \leqslant a < m$ and $\gcd(a, m) = 1$. Equivalently, $\phi(m)$ is equal to the number of fractions in the list*

$$\frac{1}{m}, \frac{2}{m}, \ldots, \frac{m-1}{m}$$

whose reduced form looks like a/m.

For instance, among the integers $1, 2, 3, \ldots, 11$, only $1, 5, 7$, and 11 don't have any prime factors in common with 12; hence $\phi(12) = 4$. Equivalently, if we look at the fractions $1/12, 2/12, 3/12 \ldots, 11/12$, there are exactly 4 in this list that can't be simplified, namely $1/12, 5/12, 7/12$, and $11/12$. As another example, none of the integers $1, 2, 3, 4, 5, 6$ are divisible by the prime 7, hence all 6 of the fractions $1/7, 2/7, \ldots, 6/7$ are already in reduced form, and so $\phi(7) = 6$. Table 2 lists the first few values of $\phi(n)$, and gives the impression that this function behaves somewhat unpredictably. But, as we'll discuss in §1.5, this is due to the fact that $\phi(n)$ is closely tied to the prime factorization of n.

Let's summarize our discussion of the period of $1/n$ up to this point, by introducing some convenient notation: For a real number α, let

$$T_\alpha = \left\{ S^k(\alpha) \mid k \geqslant 1 \right\} \tag{1.3}$$

be the set of all real numbers that can possibly be obtained from α by repeated application of S. Also define

$$U_n = \left\{ \frac{a}{n} \;\middle|\; 1 \leqslant a < n \text{ and } \gcd(a, n) = 1 \right\}. \tag{1.4}$$

Then by assuming that the expansion of $1/n$ is periodic with period ℓ, we can say that

$$T_{1/n} = \left\{ S\left(\frac{1}{n}\right), S^2\left(\frac{1}{n}\right), \ldots, S^\ell\left(\frac{1}{n}\right) \right\}$$

and that $T_{1/n} \subseteq U_n$. Now look at the sizes of these two sets. Of course $\#T_{1/n} \leqslant \ell$, but in fact it can't be any smaller than this: if it were, we would have $S^{k_1}(1/n) = S^{k_2}(1/n)$ for some $1 \leqslant k_1 < k_2 \leqslant \ell$, and this would give

$$S^{\ell-(k_2-k_1)}\left(\frac{1}{n}\right) = S^{\ell-k_2}\left(S^{k_1}\left(\frac{1}{n}\right)\right) = S^{\ell-k_2}\left(S^{k_2}\left(\frac{1}{n}\right)\right) = S^{\ell}\left(\frac{1}{n}\right) = \frac{1}{n},$$

contradicting the fact that the period of $1/n$ is ℓ. So we have $\#T_n = \ell$. Moreover, comparing the definitions of $\phi(n)$ and U_n, we see that $\#U_n = \phi(n)$. So the inclusion $T_{1/n} \subseteq U_n$ implies:

Proposition 1.8. *If* $\gcd(n, 10) = 1$*, then the period of the decimal expansion of* $1/n$ *is at most* $\phi(n)$*.*

As a byproduct of this analysis, we can combine this proposition with Proposition 1.6 to obtain the following improvement of Theorem 1.2:

Theorem 1.9 (Euler's Theorem, Version 3)**.** *Suppose* $n \geqslant 3$ *and* $\gcd(n, 10) = 1$*. There exists an integer* $1 \leqslant \ell \leqslant \phi(n)$ *such that* n *divides* $10^\ell - 1$*.*

While it won't be our final word about the period of $1/n$, let's not overlook the fact that Proposition 1.8 already tells us something nontrivial. Indeed, looking at Table 1, it may not be clear that the period of $1/n$ is limited in any way by the size of n. But the definition of $\phi(n)$ implies that $\phi(n) \leqslant n - 1$, and so the period of $1/n$ is at most $n - 1$ as well.

1.3 Interlude: Magic and mystery

Those values of n for which the period of $1/n$ is $n - 1$ should be regarded as special, because their decimal expansions are "as large as possible." The first few values of n for which this occurs are $n = 7, 17, 19, 23, \ldots$. In general, we can only have $\phi(n) = n-1$ if n is prime, a fact which follows from the definition of $\phi(n)$. But as the examples of $n = 3, 11$, and 13 show, knowing that n is prime doesn't guarantee that the period of $1/n$ is $n - 1$. So we ask:

Question 1.10. *For which primes* $p \neq 2, 5$ *is the period of* $1/p$ *equal to* $p - 1$*?*

By dwelling upon these special kinds of primes, we'll come face-to-face with a little bit of magic and a great mystery. First for the magic: we'll look at the case of $p = 7$. Take the expansion $1/7 = 0.\overline{142857}$ and consider the associated integer $m_7 = 142857$. Now look at the first few multiples of m_7:

$$\begin{aligned} m_7 &= 142857 \\ 2m_7 &= 285714 \\ 3m_7 &= 428571 \\ 4m_7 &= 571428 \\ 5m_7 &= 714285 \\ 6m_7 &= 857142 \end{aligned}$$

If you compare the sequence of decimal digits in these 6 multiples, you see they're just cyclic permutations of one another. (That is, we can get from one to any other by removing some initial sequence of digits on the left and reattaching it to the right side.) Another example of this phenomenon comes from $1/17 = 0.\overline{0588235294117647}$. Putting $m_{17} = 588235294117647$, its first 16 multiples are

$$\begin{array}{llll} 0588235294117647, & 1176470588235294, & 1764705882352941, & 2352941176470588, \\ 2941176470588235, & 3529411764705882, & 4117647058823529, & 4705882352941176, \\ 5294117647058823, & 5882352941176470, & 6470588235294117, & 7058823529411764, \\ 7647058823529411, & 8235294117647058, & 8823529411764705, & 9411764705882352. \end{array}$$

Numbers such as m_7 and m_{17} are called *cyclic numbers*; in general a positive integer is a d-digit cyclic number if the decimal representations of its first $d-1$ multiples are cyclic permutations of the integer itself. (As with the example m_{17} above, this might require adding some copies of the digit 0 to the left side of the integer.) As you can guess, cyclic numbers are quite rare! Just as with Theorem 1.3, it's worth noting that these intriguing numbers may be appreciated even by young students.

If we assume the decimal expansion of $1/p$ has period p, why does the expansion yield a cyclic number in this way? It goes back to the fact that, under this assumption, we have $U_p = T_{1/p}$, i.e., any fraction a/p with $1 \leqslant a < p$ is equal to $S^k(1/p)$ for some $1 \leqslant k \leqslant p-1$. Thus

$$\frac{1}{p} = 0.\overline{\mathtt{d_1 d_2 d_3 \ldots d_{p-1}}} \quad \Longrightarrow \quad \frac{a}{p} = S^k\left(\frac{1}{p}\right) = 0.\overline{\mathtt{d_{k+1} \ldots d_{p-1} d_1 \ldots d_k}}$$

But arguing with geometric series as we did in (1.1), we can let m_p be the positive integer whose decimal representation is $\mathtt{d_1 d_2 d_3 \ldots d_{p-1}}$. Then

$$\frac{1}{p} = 0.\overline{\mathtt{d_1 d_2 d_3 \ldots d_{p-1}}} = \frac{m_p}{10^{p-1}-1} \quad \Longrightarrow \quad \frac{a}{p} = \frac{am_p}{10^{p-1}-1}$$

This means that

$$0.\overline{\mathtt{d_{k+1} \ldots d_{p-1} d_1 \ldots d_k}} = \frac{am_p/10^{p-1}}{1-1/10^{p-1}} = \frac{am_p}{10^{p-1}} + \frac{am_p}{10^{2(p-1)}} + \frac{am_p}{10^{3(p-1)}} + \cdots$$

Since $a < p$, we have $am_p < pm_p = 10^{p-1}-1 < 10^{p-1}$, we conclude from this that the decimal representation of am_p is $\mathtt{d_{k+1} \ldots d_{p-1} d_1 \ldots d_k}$.

In addition to cyclic numbers, there is another motivation for looking at primes p for which $1/p$ has period $p-1$. According to Proposition 1.6, when $1/p$ has period $p-1$, this means that the none of the integers

$$10-1, 10^2-1, 10^3-1, \ldots, 10^{p-2}-1$$

are divisible by p. In the language of number theory, this says that 10 is a *primitive root* of p. In general, we have the following definition:

Definition 1.11. *Let p be prime and b an integer that is not a multiple of p. We say that b is a* primitive root *of p if none of the integers*

$$b-1, b^2-1, b^3-1, \ldots, b^{p-2}-1$$

are divisible by p.

When one first encounters the idea of primitive roots in number theory, it takes awhile to digest it. In particular, it seems unclear why anyone would care about such a concept at all. But it turns out to be a big deal that, for a given prime p, we can always find at least one integer b which is a primitive root of p, because this fact makes it much easier to prove certain theorems about primes. It may also be surprising to hear that primitive roots have found uses outside of number theory: they're commonly used in cryptography, especially in the *ElGamal cryptosystem* [HPS], that we rely upon for internet security and privacy, and they've even found an application in radar and sonar technology [Sil].

Turning back to Question 1.10, let's step back and look at some data. Figure 1 gives a visual representation of the period of $1/p$ for the first 100 primes. Let p_k denote the kth prime number (so $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$). In Figure 1, the points

$$\left(k, \frac{\text{period of } 1/p_k}{p_k - 1}\right)$$

are displayed for $1 \leqslant k \leqslant 100$, so that in particular the y-coordinate is always at most 1. (In the figure you might also notice the anomalous values at $p_1 = 2$ and $p_3 = 5$; we're not supposed to consider these, so I've just set the value to 0.) Do you see a pattern in this graph? I sure don't! This is a mysterious sequence, and

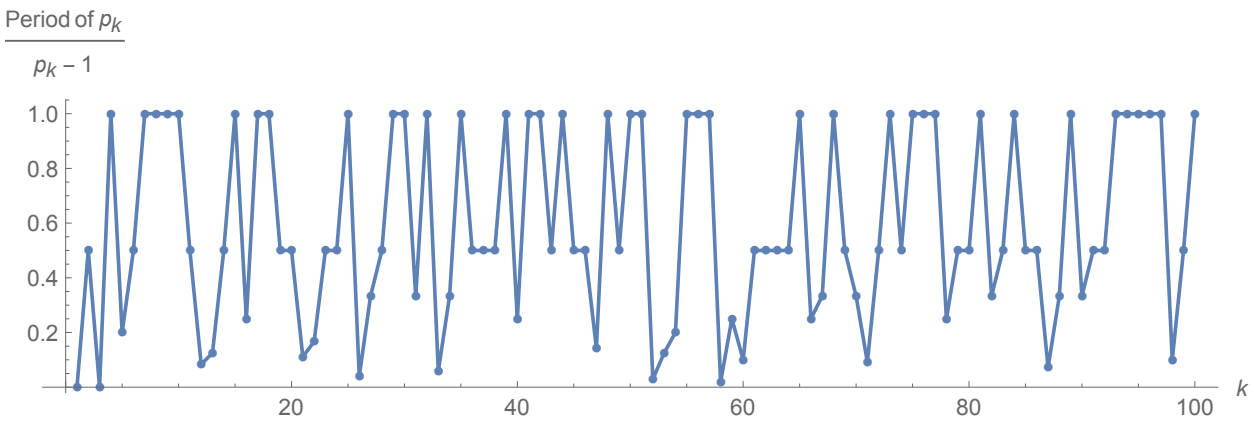

Figure 1: $\left(\frac{\text{period of } 1/p_k}{p_k - 1}\right)$ versus k

it looks like it doesn't behave in any predictable way. For instance, since you see the first 100 terms of the sequence displayed in the graph, can you use this to confidently predict what 101st term in the sequence is? I can't!

As an indication of just how little we understand the behavior of this graph, mathematicians have not even answered a question of Gauss, which asks whether there will always be points lying on the line $y = 1$ as $k \to \infty$; note that these points correspond to primes p_k for which $1/p_k$ has the maximum period $p_k - 1$. In the early twentieth century, Emil Artin gave a conjecture that, if true, would answer Gauss' question in the affirmative, and would even tell us "how often" $1/p$ has period $p - 1$:

Conjecture 1.12 (Artin)**.** *For a large "random" prime p, the probability that the decimal expansion of $1/p$ will have period p is about 37%. More precisely, when one looks at all primes $p \leqslant N$, the proportion of those for which $1/p$ has period $p - 1$ approaches*

$$\prod_{q \text{ prime}} \left(1 - \frac{1}{q(q-1)}\right) = 0.3739558136...$$

as $N \to \infty$.

In any case, we see that Question 1.10 is not so innocent as it might first seem. It shows how these everyday decimal expansions are rooted in unexpectedly mysterious and uncharted terrain.

1.4 The period of $1/n$: A refinement

Now let's go back to the more general considerations we had at the end of §1.2. As in that section, we have an integer $n \geqslant 3$ such that $\gcd(n, 10) = 1$, and we let ℓ be the period of the decimal expansion of $1/n$. To refine the result in Proposition 1.8, let's revisit the inclusion $T_{1/n} \subseteq U_n$ that we had shown. If $\ell < \phi(n)$, then there are fractions a/n inside U_n that cannot be reached by repeatedly applying the shift operator to $1/n$. So we're going to start by taking a closer look at the general elements of U_n.

Let's revisit the example of $n = 21$ again. We have

$$T_{1/21} = \left\{\frac{1}{21}, \frac{4}{21}, \frac{10}{21}, \frac{13}{21}, \frac{16}{21}, \frac{19}{21}\right\} \subseteq \left\{\frac{1}{21}, \frac{2}{21}, \frac{4}{21}, \frac{5}{21}, \frac{8}{21}, \frac{10}{21}, \frac{11}{21}, \frac{13}{21}, \frac{16}{21}, \frac{17}{21}, \frac{19}{21}, \frac{20}{21}\right\} = U_{21}$$

so the six elements in U_{21} that are not of the form $S^k(1/21)$ are

$$\left\{\frac{2}{21}, \frac{5}{21}, \frac{8}{21}, \frac{11}{21}, \frac{17}{21}, \frac{20}{21}\right\}.$$

Let's take a look at their decimal expansions:

$$\begin{aligned}
\frac{2}{21} &= 0.\overline{095238} \\
\frac{5}{21} &= 0.\overline{238095} \\
\frac{8}{21} &= 0.\overline{380952} \\
\frac{11}{21} &= 0.\overline{523809} \\
\frac{17}{21} &= 0.\overline{809523} \\
\frac{20}{21} &= 0.\overline{952380}.
\end{aligned}$$

We can see that these six fractions are all related by the shift operator S! So the following picture emerges. When we unleash S upon the 12-element set U_{21}, by applying it to its elements again and again, we wind up with a natural division of U_{21} into two 6-element subsets, namely T_{21} and its complement. Both of these subsets have the following property: within each subset, we can use S (repeatedly) to turn any one element into any other.

So what kind of picture will we get if we unleash S upon U_n for more general values of n? Let's first recall from (1.3) that the set $T_{1/n}$ is one instance of a more general construction. Fixing any element a/n inside U_n, let's now ask what can be said about $T_{a/n} = \{S^k(a/n) \mid k \geqslant 1\}$. First of all, I claim that the fraction a/n is periodic, and that its period is no larger than ℓ, the period of $1/n$. To see this, let's recall from (1.1) that if $1/n = 0.\overline{\mathtt{d_1 d_2 \ldots d_\ell}}$ and we put $m = \mathtt{d}_1 \cdot 10^{\ell-1} + \ldots + \mathtt{d}_{\ell-1} \cdot 10 + \mathtt{d}_\ell$, then the geometric series identity allows us to conclude that $1/n = m/(10^\ell - 1)$, and that n does not divide $10^k - 1$ for any $1 \leqslant k < \ell$. We're going to reverse this process to learn about the decimal expansion of a/n. Since $1 \leqslant a < n$, we can say that $am < nm = 10^\ell - 1 < 10^\ell$. So the decimal representation of am will have the form

$$am = \mathtt{e}_1 \cdot 10^{\ell-1} + \mathtt{e}_2 \cdot 10^{\ell-2} + \cdots + \mathtt{e}_{\ell-1} \cdot 10 + \mathtt{e}_\ell,$$

which we may write more succinctly as $am = \mathtt{e_1 e_2 \ldots e_\ell}$. (Just as with $\mathtt{d}_1, \mathtt{d}_2, \ldots$, some of the leading digits $\mathtt{e}_1, \mathtt{e}_2 \ldots$, might be 0.) Thus we have

$$\begin{aligned}
\frac{a}{n} &= \frac{am}{nm} \\
&= \frac{am}{10^\ell} \cdot \frac{1}{(1 - 1/10^\ell)} \\
&= \left(\frac{\mathtt{e}_1}{10} + \frac{\mathtt{e}_2}{10^2} + \cdots + \frac{\mathtt{e}_{\ell-1}}{10^{\ell-1}} + \frac{\mathtt{e}_\ell}{10^\ell}\right) \cdot \left(1 + \frac{1}{10^\ell} + \frac{1}{10^{2\ell}} + \cdots\right) \\
&= \frac{\mathtt{e}_1}{10} + \frac{\mathtt{e}_2}{10^2} + \cdots + \frac{\mathtt{e}_\ell}{10^\ell} + \frac{\mathtt{e}_1}{10^{\ell+1}} + \frac{\mathtt{e}_2}{10^{\ell+2}} + \cdots + \frac{\mathtt{e}_\ell}{10^{2\ell}} + \cdots \\
&= 0.\overline{\mathtt{e_1 e_2 \ldots e_\ell}}.
\end{aligned}$$

So indeed the period of a/n is at most ℓ. In terms of the shift operator, we can write $S^\ell(a/n) = a/n$.

Could the period of a/n be less than ℓ? If it had period $k < \ell$, that would mean (by using the same kind of geometric series argument we just used) that

$$\frac{a}{n} = \frac{m'}{10^k - 1}$$

for some integer $1 \leqslant m' < 10^k - 1$. Cross-multiplying gives $nm' = a(10^k - 1)$, so in particular n divides $a(10^k - 1)$. But by definition of U_n, a and n do not share any prime factors, and so in fact n divides $10^k - 1$. But this is a problem, because we already stated that ℓ is the smallest exponent for which n divides $10^\ell - 1$. The conclusion is therefore that the period a/n must equal ℓ.

So now we can say that, for any a/n in U_n, the set $T_{a/n}$ can be described more simply as

$$T_{a/n} = \left\{ S\left(\frac{a}{n}\right), S^2\left(\frac{a}{n}\right), \ldots, S^\ell\left(\frac{a}{n}\right) \right\}.$$

Just as we did toward the end of §1.2 for the set $T_{1/n}$, we can conclude that this set contains ℓ distinct elements (i.e., that $S^{k_1}(a/n) \neq S^{k_2}(a/n)$ whenever $1 \leqslant k_1 < k_2 \leqslant \ell$).

Here's the picture we have of U_n so far: When we apply S repeatedly to any element a/n of U_n, we generate an ℓ-element subset $T_{a/n}$. If we take two distinct elements a_1/n and a_2/n, how much do the sets $T_{a_1/n}$ and $T_{a_2/n}$ have in common? In the example of $n = 21$, we saw that were the only two extremes: Either they were actually equal (e.g., $T_{1/21} = T_{13/21}$ and $T_{2/21} = T_{8/21}$) or they were disjoint (e.g., $T_{1/n} \cap T_{2/n} = \varnothing$). And this turns out to happen in the general case as well. To see this, let's suppose that $T_{a_1/n}$ and $T_{a_2/n}$ have at least one common element, say b/n. Then for some exponents $1 \leqslant k_1, k_2 \leqslant \ell$, we have

$$S^{k_1}\left(\frac{a_1}{n}\right) = \frac{b}{n} = S^{k_2}\left(\frac{a_2}{n}\right).$$

Now apply S multiple times to this, using the fact that a_2/n has period ℓ:

$$S^{k_1+\ell-k_2}\left(\frac{a_1}{n}\right) = S^{\ell-k_2}\left(S^{k_1}\left(\frac{a_1}{n}\right)\right) = S^{\ell-k_2}\left(S^{k_2}\left(\frac{a_2}{n}\right)\right) = S^{\ell}\left(\frac{a_2}{n}\right) = \frac{a_2}{n}.$$

This shows us that a_2/n belongs to $T_{a_1/n}$, and so anything we can generate by repeatedly applying S to a_2/n can in fact be obtained by applying S to a_1/n. So we conclude that $T_{a_2/n} \subseteq T_{a_1/n}$, and a symmetric argument shows the opposite inclusion. Hence there are only two possibilities: $T_{a_1/n} \cap T_{a_2/n} = \varnothing$ or $T_{a_1/n} = T_{a_2/n}$.

So our final picture of U_n has been painted! It is divided into of a number of subsets—let's say there are k of them—that (i) each have ℓ elements and (ii) do not intersect each other. We conclude that the number of elements in U_n is equal to $k\ell$. But we also recall that $\#U_n = \phi(n)$, and this brings us to the following refinement of Proposition 1.8:

Theorem 1.13. *If* $\gcd(n, 10) = 1$*, then the period of the decimal expansion of* $1/n$ *divides* $\phi(n)$*.*

Notice that while it doesn't describe the period of $1/n$ completely, Theorem 1.13 gives us much more information than Proposition 1.8. For instance, consider what each one tells us about the period ℓ of $1/101$. Since 101 is prime, we have $\phi(101) = 100$ and so Proposition 1.8 tells us that ℓ is something between 1 and 100. But Theorem 1.13 tells us that ℓ actually divides 100, so ℓ is one of the numbers 1, 2, 4, 5, 10, 20, 25, 50, or 100. This is a much smaller list of possibilities!

To finish this section, let's return to Euler's Theorem. From Proposition 1.6, Theorem 1.13 is equivalent to saying that, when $\gcd(n, 10) = 1$, there exists an exponent $\ell \geqslant 1$ such that n divides $10^\ell - 1$, and furthermore ℓ is a divisor of $\phi(n)$. So we may put $\phi(n) = k\ell$ and conclude[3] that

$$10^{\phi(n)} - 1 = (10^\ell)^k - 1 = (10^\ell - 1)\big((10^\ell)^{k-1} + (10^\ell)^{k-2} + 10^\ell + \cdots + 1\big)$$

is also a multiple of n. So we arrive at a more faithful version of Euler's fundamental result:

Theorem 1.14 (Euler's Theorem, Version 4)**.** *For any positive integer* n *such that* $\gcd(n, 10) = 1$*, the integer* $10^{\phi(n)} - 1$ *is a multiple of* n*.*

For a prime $p \neq 2, 5$ we have $\phi(p) = p - 1$, and Theorem 1.14 gives the following fascinating elementary statement (originally due to Fermat): the integer

$$\underbrace{9999\ldots9}_{p-1 \text{ times}}$$

is divisible by p.

[3]This is just an application of the usual formula for the sum of a *finite* geometric series: When $a \neq 1$,

$$1 + a + a^2 + \cdots + a^{k-2} + a^{k-1} = \frac{a^k - 1}{a - 1}.$$

1.5 The period of $1/n$: The heart of the matter

This goal of this section is to arrive at the foundations of Question 1.5. If we're handed the integer n and we want to determine the period of the decimal expansion of $1/n$, how easy can we make this task if we want to avoid computing the actual decimal expansion?

To get to an answer, we're going to need the following fact:

Proposition 1.15. *Suppose that* $\gcd(n, 10) = 1$ *and let* ℓ *be the period of* $1/n$*. If* n *divides* $10^k - 1$ *for some* $k \geqslant 1$*, then* ℓ *divides* k*.*

The key to showing this is the geometric series connection that we've used several times by now. Assuming $10^k - 1 = nq$, we may write the decimal representation of q in the form $\mathtt{e_1 e_2 \dots e_k}$ and then find

$$\frac{1}{n} = \frac{q}{10^k - 1} = \frac{q/10^k}{1 - 1/10^k} = \frac{q}{10^k} + \frac{q}{10^{2k}} + \frac{q}{10^{3k}} + \cdots = 0.\overline{\mathtt{e_1 e_2 \dots e_k}}.$$

This shows that the decimal expansion of $1/n$ repeats the k-digit sequence $\mathtt{e_1}, \mathtt{e_2}, \dots, \mathtt{e_k}$. But the period of $1/n$ is ℓ, and so if we write $1/n = 0.\overline{\mathtt{d_1 d_2 \dots d_\ell}}$, the only way these two decimal expansions of $1/n$ can coexist is if k is a multiple of ℓ and the sequence $\mathtt{e_1}, \mathtt{e_2}, \dots, \mathtt{e_k}$ just consists of k/ℓ repetitions of the smaller sequence $\mathtt{d_1}, \mathtt{d_2}, \dots, \mathtt{d_\ell}$. Proposition 1.15 follows from this.[4]

The next result tells us that when n_1 and n_2 don't share any prime factors, we can easily figure out the period of $1/n_1 n_2$ once we know the periods of $1/n_1$ and $1/n_2$:

Theorem 1.16. *Suppose* $\gcd(n_1, 10) = \gcd(n_2, 10) = 1$*, let* $1/n_1$ *have period* ℓ_1*, and* $1/n_2$ *have period* ℓ_2*. If* $\gcd(n_1, n_2) = 1$*, then the period of* $1/n_1 n_2$ *is* $\operatorname{lcm}(\ell_1, \ell_2)$*, the least common multiple of* ℓ_1 *and* ℓ_2*.*

This theorem allows us to use a small set of facts to build up more impressive ones. For instance, let's start with the quantities

$$\frac{1}{7} = 0.\overline{142857}, \quad \frac{1}{27} = 0.\overline{037}, \quad \frac{1}{41} = 0.\overline{02439},$$

which involve relatively small denominators. Since $189 = 7 \cdot 27$ and $\gcd(7, 27) = 1$, this means that the period of $1/189$ is $\operatorname{lcm}(6, 3) = 6$; building on this, we have $7749 = 189 \cdot 41$ and $\gcd(41, 189) = 1$, so the period of $1/7749$ is $\operatorname{lcm}(6, 5) = 30$. Keep in mind we didn't do the work to calculate the actual decimal expansion of $1/7749$ but, whatever it is, it will have a period of 30! We should also note that the theorem has its limitations; for instance, you can't start from $1/3 = 0.\overline{3}$ and $1/27 = 0.\overline{0.037}$ and conclude $1/81$ has period $\operatorname{lcm}(1, 3) = 3$, because $\gcd(3, 27) \neq 1$. (In fact the period of $1/81$ is 9.)

Now let's convince ourselves that Theorem 1.16 is true. We already have ℓ_1 as the period of $1/n_1$ and ℓ_2 as the period of $1/n_2$, so let's define ℓ_3 to be the period of $1/n_1 n_2$. To show that $\ell_3 = \operatorname{lcm}(\ell_1, \ell_2)$, we're going to show that these quantities both divide each other.

First we'll show that ℓ_3 divides $\operatorname{lcm}(\ell_1, \ell_2)$. By its very definition, $\operatorname{lcm}(\ell_1, \ell_2)$ is a multiple of ℓ_1; let's say $\operatorname{lcm}(\ell_1, \ell_2) = \ell_1 c$. Since

$$10^{\operatorname{lcm}(\ell_1, \ell_2)} - 1 = (10^{\ell_1})^c - 1 = (10^{\ell_1} - 1)\Big((10^{\ell_1})^{c-1} + (10^{\ell_1})^{c-2} + \cdots + 1\Big),$$

we can conclude that n_1 divides $10^{\operatorname{lcm}(\ell_1, \ell_2)} - 1$, since it divides $10^{\ell_1} - 1$. By a completely similar argument we can conclude n_2 also divides $10^{\operatorname{lcm}(\ell_1, \ell_2)} - 1$. Now let's use the fact that $\gcd(n_1, n_2) = 1$: since n_1 and n_2 have no prime factors in common, the fact that they both divide the same integer means that their product must also divide that integer. (This is perhaps most intuitively seen by considering prime factorizations.)

[4] This argument appeals to your intuition about repeating decimal expansions, particularly when I used the words "the only way." If this feels a little slippery to you, the proposition can also be proved without resorting to decimal expansions. One can instead use the Division Algorithm (another cornerstone of elementary number theory!) to write $k = \ell q + r$, where $0 \leqslant r < \ell$, show that $10^r - 1$ is a multiple of n, and apply what we know about ℓ from Proposition 1.6.

Hence $n_1 n_2$ divides $10^{\mathrm{lcm}(\ell_1,\ell_2)} - 1$, and now we can apply our new tool, Proposition 1.15, to conclude that the period ℓ_3 of $1/n_1 n_2$ divides $\mathrm{lcm}(\ell_1, \ell_2)$.

To show that $\mathrm{lcm}(\ell_1, \ell_2)$ divides ℓ_3, we're going to wield Proposition 1.15 again. Since $n_1 n_2$ divides $10^{\ell_3} - 1$, this of course implies that n_1 divides $10^{\ell_3} - 1$, and so we conclude that ℓ_1 divides ℓ_3. We use the same argument to show that ℓ_2 divides ℓ_3 as well. Since both ℓ_1 and ℓ_2 divide ℓ_3, it follows that $\mathrm{lcm}(\ell_1, \ell_2)$ must also divide ℓ_3. (This last step exhibits a key property about least common multiples and, like the fact in the previous paragraph, may again be seen using prime factorizations.) So this gives our desired equality $\ell_3 = \mathrm{lcm}(\ell_1, \ell_2)$.

Now let's discuss Euler's ϕ-function a little more. We've already noted that, by the definitions of prime and composite, we have $\phi(n) = n - 1$ if and only if n is prime. What if n is a power of a prime? It's not too much harder to compute $\phi(p^k)$ directly from Definition 1.7. First we write out all of the numbers

$$1, 2, 3, \ldots, p^k - 1$$

and ask which ones have any prime factors in common with p^k. But the only prime factor of p^k is p, so we're really just asking how many multiples of p there are in this list. If we write out all of these the multiples, we get

$$p, 2p, 3p, \ldots, p^k - p = p(p^{k-1} - 1).$$

So there are $p^{k-1} - 1$ multiples of p here, and after crossing them all out from the first list we're left with

$$(p^k - 1) - (p^{k-1} - 1) = p^{k-1}(p - 1)$$

numbers. Therefore

$$\phi(p^k) = p^{k-1}(p - 1). \tag{1.5}$$

We can use this, for instance, along with Theorem 1.13 to say that the period of $1/7^8$ is a divisor of $7^7 \cdot (7 - 1) = 4941258$ (a fact which gives us 32 possibilities for this period).

Let me now tell you how we can calculate $\phi(n)$ for any positive integer n. In our quest for the most precise information about the period of $1/n$, we won't actually need to use this formula, but I would feel bad to leave it out after coming this far. A key property of the ϕ-function is that it is *multiplicative*, which means that

$$\phi(n_1 n_2) = \phi(n_1)\phi(n_2) \quad \text{if } \gcd(n_1, n_2) = 1.$$

Since we won't ultimately use this result, I won't try to justify this multiplicative property; but most textbooks on elementary number theory will have a proof. Now imagine that you have some integer n and you know its prime factorization. For concreteness, let's write it as

$$n = p_1^{h_1} p_2^{h_2} \cdots p_r^{h_r},$$

where $r \geqslant 1$, each p_i is prime, each $h_i \geqslant 1$, and $p_1 < p_2 < \ldots < p_r$. Since $\gcd(p_1^{h_1}, p_2^{h_2}) = 1$, we have

$$\phi(p_1^{h_1} p_2^{h_2}) = \phi(p_1^{h_1})\phi(p_2^{h_2}) = p_1^{h_1 - 1}(p_1 - 1)p_2^{h_2 - 1}(p_2 - 1).$$

We also have $\gcd(p_1^{h_1} p_2^{h_2}, p_3^{h_3}) = 1$, so

$$\phi(p_1^{h_1} p_2^{h_2} p_3^{h_3}) = \phi(p_1^{h_1} p_2^{h_2})\phi(p_3^{h_3}) = p_1^{h_1 - 1}(p_1 - 1)p_2^{h_2 - 1}(p_2 - 1)p_3^{h_3 - 1}(p_3 - 1).$$

Continuing in this fashion, we arrive at the formula

$$\phi(n) = p_1^{h_1 - 1}(p_1 - 1)p_2^{h_2 - 1}(p_2 - 1) \cdots p_r^{h_r - 1}(p_r - 1). \tag{1.6}$$

Let's take a look what this formula says about the period of $1/31941$. Its prime factorization is $31941 = 3^3 \cdot 7 \cdot 13$, and so (1.6) gives

$$\phi(31941) = 3^2 \cdot (3 - 1) \cdot 7^0 \cdot (7 - 1) \cdot 13^1 \cdot (13 - 1) = 16848.$$

(This is much better than trying to use Definition 1.7 to calculate $\phi(31941)$!) What does Theorem 1.13 then tell us about the period of 1/31941? It divides $\phi(31941) = 16848$, which ends up giving us 50 possibilities; in particular, without any further information, the period could be as large as 16848.

With a little more finesse, though, we can actually do better than this. Let's suppose we don't know the periods of $1/3^3 = 1/27$, $1/7$ and $1/13^2 = 1/169$, and just call them ℓ_{27}, ℓ_7, and ℓ_{169}. Using only the simple formula (1.5) and Theorem 1.13, we can say that ℓ_{27} divides $\phi(27) = 18$, ℓ_7 divides $\phi(7) = 6$, and ℓ_{169} divides $\phi(169) = 156$. Taking the first two of these statements, we can say that $\mathrm{lcm}(\ell_{27}, \ell_7)$ must divide $\mathrm{lcm}(18, 6) = 18$; so by Theorem 1.16, the period ℓ_{189} of $1/(27 \cdot 7) = 1/189$ divides 18. Then, as $\gcd(189, 169) = 1$, we use Theorem 1.16 once more to conclude that the period of $1/(189 \cdot 169) = 1/31941$, which equals $\mathrm{lcm}(\ell_{189}, \ell_{169})$, must divide $\mathrm{lcm}(18, 156) = 468$. This cuts down the number of possibilities for the period of 1/31941 to just 18, and implies it is no larger than 468—a bound that's 26 times smaller than the one obtained in the previous paragraph!

This example is an illustration of the way in which the period of $1/n$ is determined by the periods of the numbers $1/p^h$, for the prime powers p^h appearing in its prime factorization. Here is the general statement:

Proposition 1.17. *Suppose* $\gcd(n, 10) = 1$ *and write the prime factorization of* n *as*

$$n = p_1^{h_1} p_2^{h_2} \cdots p_r^{h_r}.$$

If ℓ_i *denotes the period of* $1/p_i^{h_i}$*, then the period of* $1/n$ *is* $\mathrm{lcm}(\ell_1, \ell_2, \ldots, \ell_r)$.

This proposition encourages us to look more closely at the periods of the fractions $1/p^k$ (with $p \neq 2, 5$). Here's the final result of this section:

Theorem 1.18. *Let* $p \neq 2, 5$ *be prime and let* $k \geqslant 1$*. Let* ℓ *be the period of* $1/p$ *and write*

$$10^{p-1} - 1 = p^b s, \tag{1.7}$$

where s *is not a multiple of* p*. Then the period of* $1/p^k$ *is given by*

$$\begin{cases} \ell & \text{if } 1 \leqslant k \leqslant b \\ \ell p^{k-b} & \text{if } k > b \end{cases}.$$

Unlike the previous theorems, I won't attempt to discuss a proof of this one because it's more complicated the proofs of our previous results. Instead, I refer the interested reader to [Ros, Lemma 4] for a proof, which relies on the theory of modular arithmetic.

I will make a few of remarks about this theorem, however. The first is that one knows $b \geqslant 1$ by Euler's (or Fermat's) Theorem. The second remark is that one can show the highest power of p dividing $10^{p-1} - 1$ is actually the same as the highest power of p dividing $10^\ell - 1$ (the proof in the Appendix shows this), so one could alternatively replace (1.7) with $10^{\ell-1} = p^b s'$, where s' is not a multiple of p.

The third and most fascinating remark is that, if one looks at the data, it's actually *very* rare to find primes p where $b > 1$. Indeed, after $p = 3$ (for which (1.7) reads $10^2 - 1 = 3^2 \cdot 1$), the next prime for which $b > 1$ is $p = 487$, and the next one after that is $p = 56598313$. These primes are called *base 10 Weiferich primes*, and no one has ever discovered any others besides these three; in fact, it's an unsolved problem to determine whether their number is finite or infinite. That is, we don't know the answer to the following question: *Are there infinitely many primes* p *for which the periods of the decimal expansions of* $1/p$ *and* $1/p^2$ *are the same?*

Turning back to $1/n$ Question 1.5, we've now come to the very heart of the problem. Thanks to elegant multiplicative structures of the integers, namely prime factorization and Euler's Theorem, the period of $1/n$ is determined by the periods of the numbers $1/p^k$ and, by some further elegance in elementary number theory (see the Appendix), these are in turn determined by the periods of the numbers $1/p$. But if we're staring at some prime p, we know from the graph in Figure 1 that it's going to be difficult to predict the period of $1/p$.

p	**Decimal expansion of** $1/p$
7	$0.\overline{142857}$
17	$0.\overline{0588235294117647}$
19	$0.\overline{052631578947368421}$
23	$0.\overline{0434782608695652173913}$
29	$0.\overline{0344827586206896551724137931}$
47	$0.\overline{0212765957446808510638297872340425531914893617}$
59	$0.\overline{0169491525423728813559322033898305084745762711864406779661}$
61	$0.\overline{0163934426229508196721311475409836065573770491803278688524459}$

Table 3: Some decimal expansions of $1/p$ with period $p-1$

It's important to emphasize the role played by the prime factorization of n here. Factoring large integers is notoriously difficult and so starting with, say, $n = 215071$ and arriving at the prime factorization $n = 449 \cdot 479$ is already a challenge. But there's an added layer of difficulty on top of that, because we still need to pin down the periods of $1/449$ and $1/479$, and that's probably not going to be easy.[5] This is what I find so fascinating about this whole quest: after all of the careful, structured analysis we've done, at the heart of our problem resides the chaotic realm depicted in Figure 1, where the secrets are far from being uncovered.

2 What can we learn from the digits of $1/p$?

In this part, we'll turn our focus to the decimal expansions of $1/p$, for a prime $p \neq 2, 5$, which we've just identified as the central figures in determining the periods of the expansions of $1/n$. Instead of starting with a prime p and asking what the period of $1/p$ will be, we're going to suppose that we're looking at a value of p for which the period is as long as possible, namely $p-1$. The (admittedly vague) question will then be:

Question 2.1. *If $p \neq 2, 5$ is a prime and the decimal expansion of $1/p$ has period $p-1$ (or equivalently, if 10 is a primitive root of p), what can be said about the repeating sequence of $p-1$ digits?*

Thus throughout this part, p will always be a prime that has 10 as a primitive root. When $p = 4k+3$ (for some integer k), we'll see that the digits of the expansion of $1/p$ are linked to profound ideas in number theory. Unlike Part 1, my goal in Part 2 won't be to prove anything but simply these convey these sophisticated ideas to the uninitiated reader.

2.1 How random-looking are the digits of $1/p$?

Let's start by looking at some data again. Table 3 lists the first few values of p for which $1/p$ has period $p-1$. Obviously this string of $p-1$ digits is going to very large when p is large, and it's a lot to take in with the naked eye. For instance, let's look at the case of $p = 47$:

$$1/47 = 0.\overline{0212765957446808510638297872340425531914893617}.$$

The first few digits are going to be fairly predictable, because we know $1/47 \approx 1/50 = 0.02$. But past a certain point the digits start looking, well, kind of *random*.

[5] I wanted to avoid discussing the use of *congruences* in this article, but if you know about them, they can make the process slightly easier. For instance, since the period of $1/479$ divides $478 = 2 \cdot 239$, you know it's either $1, 2, 239$, or 478. So by Proposition 1.6, you can check whether 479 divides each of $10-1$, 10^2-1, and $10^{239}-1$ (there's no need to check $10^{478}-1$; see Theorem 1.14), which means determining whether any of $10, 10^2$, or 10^{239} are congruent to 1 modulo 479. There are other number-theoretic tricks that can help as well, but in general these computations are still tedious.

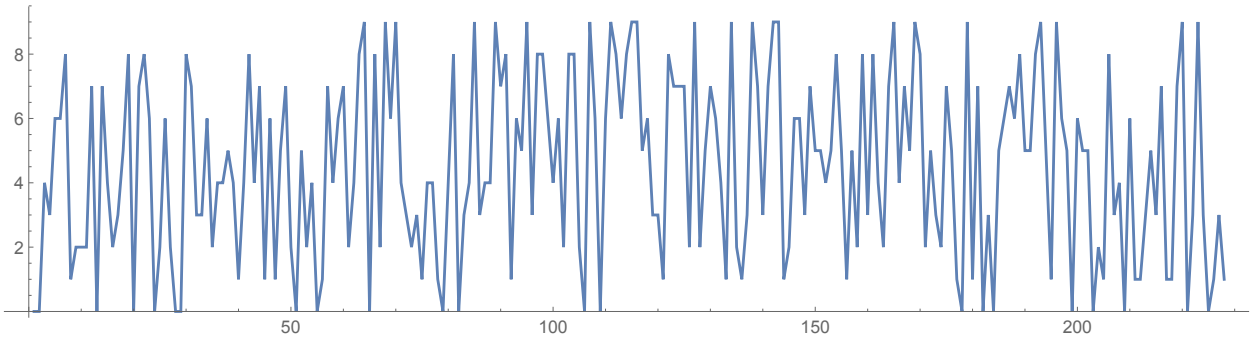

Figure 2: Plot of the 228-digit repeating sequence in the expansion of 1/229

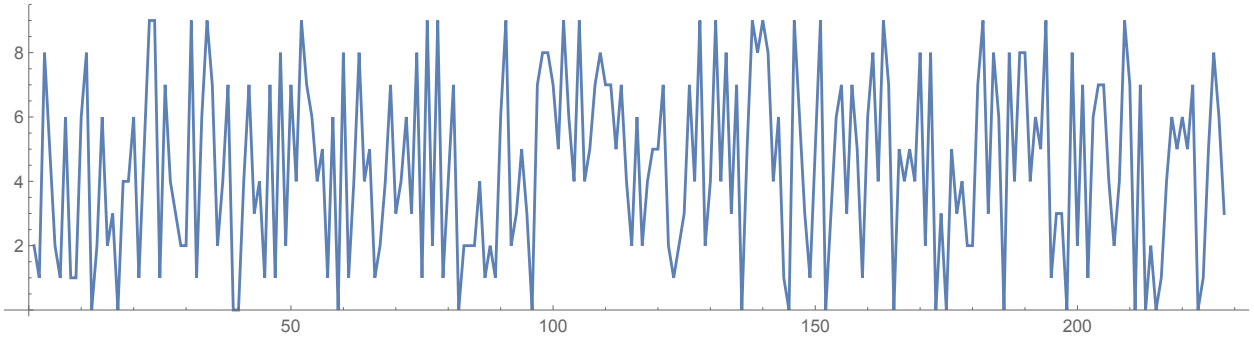

Figure 3: Plot of a random sequence of 228 decimal digits

Let me clarify two things about what I just said. First of all, the digits of 1/47 (and $1/p$ in general) are definitely *not* random. Whatever procedure I follow to calculate the decimal expansion of 1/47, as long as it's correct I'm going to get the same repeating sequence of 46 digits every time. I'm just saying that past a certain point the digits "look" random to me, and that's the second thing to clarify: this is just my opinion. You might look at those digits and feel differently.

If you don't feel this way, let me try to sway you to my side a bit. In the five rows below are strings of 35 digits. One of the rows is a string of 35 digits taken from the middle of the expansion of 1/131 (which has period 130), one of them is from the middle of the expansion of 1/229 (which has period 228), and the other three rows are strings of 35 random digits. *Which of these three rows are random strings?*

41984732824427480916030534351145038
18782860059580793714132782255045931
56165863608677584594706576115269330
64017277591261236900963254209039020
69868995633187772925764192139737991

It's pretty tough to tell.[6]

For a more visual demonstration, we can plot the digits in the sequence of repeating digits in the expansion of $1/p$, and compare the plot with a random sequence of digits. The 228-digit sequence coming from the expansion of 1/229 is plotted in Figure 2, and a sequence of 228 randomly-generated digits is given in Figure

[6]The answer is that the first row comes from 1/131 and the last row comes from 1/229.

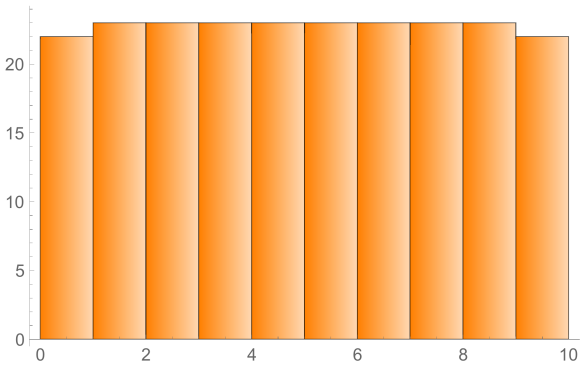

Figure 4: Digit frequency in the 228-digit repeating sequence in the expansion of 1/229

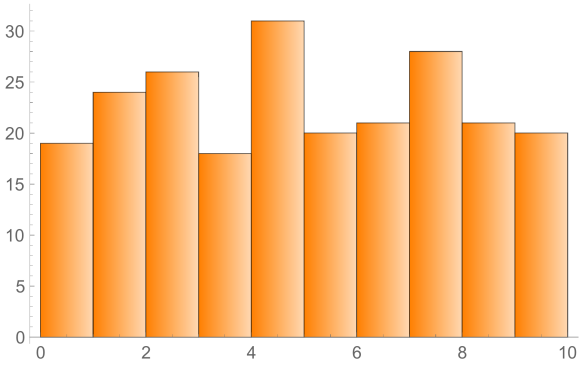

Figure 5: Digit frequency in a random sequence of 228 decimal digits

3.[7] We can see in Figure 2 that the first couple of digits in the sequence are 0's, but after that I feel like the two plots have more or less the same character.

Now this might be starting to feel like a setup to you: I've spent these last couple paragraphs trying to convince you that the digits of $1/p$ look like a random sequence, and now you're just waiting for the moment where I reveal a hidden bias in the sequence that makes it seem a lot less random. If this is your suspicion, well, you're right, that's what I'm about to do... And in fact there are several ways I can do this. For instance, I can take the sequences in Figures 2 and 3 and make a histogram of how many times each digit appears. This is done in Figures 4 and 5, and one can see there that the digits in the expansion of 1/229 are "suspiciously" well-distributed when compared with the random sequence. Alternatively, I can cite what is known as *Midy's Theorem* (see [Ros], for instance) which implies that if $1/p = 0.\overline{\mathtt{d}_1\mathtt{d}_2\ldots\mathtt{d}_{p-1}}$, then

$$\mathtt{d}_i + \mathtt{d}_{\frac{p-1}{2}+i} = 9. \tag{2.1}$$

This says that the ith digit and the $(\frac{p-1}{2}+i)$th digit are inextricably linked; in particular, the first half of the sequence completely determines the second half of the sequence.

But the hidden bias I want to tell you about is one that I feel is much deeper than the ones mentioned above, and really gives the impression that the digits of $1/p$ harbor some very startling secrets. This bias was first demonstrated by the number theorist Kurt Girstmair, and we'll describe his result in terms of another simple statistical test: if $\mathtt{e}_1, \mathtt{e}_2, \ldots \mathtt{e}_{p-1}$ is *any* string of $p-1$ digits, we'll say that the *A-statistic* of this

[7] To be more precise, the latter sequence is a computer-generated *pseudorandom* sequence, which is meant to mimic a random sequence of digits in which each digit from 0 through 9 is chosen with uniform probability and chosen independently.

p	7	17	19	23	47	59	61	97	109	113	131	149	167	179	181	193	223
$A(1/p)$	11	0	11	33	55	33	0	0	0	0	55	0	121	55	0	0	77

Table 4: A-statistic applied to the repeating sequence in the expansion of $1/p$

string is the alternating sum

$$A := \sum_{j=1}^{p-1} (-1)^j \mathtt{e}_j = -\mathtt{e}_1 + \mathtt{e}_2 - \mathtt{e}_3 + \mathtt{e}_4 - \ldots - \mathtt{e}_{p-2} + \mathtt{e}_{p-1}.$$

What should we expect about the value of A when this string $\mathtt{e}_1, \mathtt{e}_2, \ldots \mathtt{e}_{p-1}$ is truly random? If p is large and the string is of digits is random then:

(a) The value of A is likely to be close to zero (since $p-1$ is even and the expected value of each digit is the same, namely 4.5), and yet it's unlikely to actually equal zero.

(b) The value of A is just as likely to be positive as it is to be negative.

Now suppose that $1/p = 0.\overline{\mathtt{d}_1\mathtt{d}_2\ldots\mathtt{d}_{p-1}}$, and let $A(1/p)$ be the A-statistic of the sequence $\mathtt{d}_1, \mathtt{d}_2, \ldots \mathtt{d}_{p-1}$. With a little bit of work, we can make two preliminary observations about $A(1/p)$. First of all, we should expect $A(1/p)$ to be a multiple of 11. To see this, first note that the number $(10^{p-1}-1)/p$, whose decimal representation is $\mathtt{d}_1\mathtt{d}_2\ldots\mathtt{d}_{p-1}$, is divisible by 11, as the following calculation shows:

$$\frac{10^{p-1}-1}{p} = \frac{(10^2)^{\frac{p-1}{2}}-1}{p} = \frac{(10^2-1)((10^2)^{\frac{p-3}{2}} + (10^2)^{\frac{p-5}{2}} + \cdots + 1)}{p} = 11 \cdot \frac{9(100^{\frac{p-3}{2}} + 100^{\frac{p-5}{2}} + \cdots + 1)}{p}.$$

Here we're using the fact that $p-1$ is even (so that $(p-1)/2$ is an integer) and that $p \neq 11$ (so the factor of 11 on the right side doesn't get cancelled out when we divide by p). On the other hand, a well-known test for divisibility by 11 says that $(10^{p-1}-1)/p$ is a multiple of 11 if and only if the A-statistic $A(1/p) = \sum_{i=1}^{p-1}(-1)^i \mathtt{d}_i$ is a multiple of 11.

The other observation we can make is that if the $p-1$ is a multiple of 4, then $A(1/p)$ will be 0; this is less obvious, but it follows from Midy's Theorem above. Indeed, in this case $(p-1)/2$ will be even, which implies that i and $(p-1)/2+i$ are either both even or both odd. So when we split the alternating sum $A(1/p)$ into positive terms and negative terms, the formula (2.1) implies that

$$A(1/p) = \sum_{\substack{1 \leqslant i \leqslant p-1 \\ i \text{ even}}} \mathtt{d}_i - \sum_{\substack{1 \leqslant i \leqslant p-1 \\ i \text{ odd}}} \mathtt{d}_i = \frac{p-1}{4} \cdot 9 - \frac{p-1}{4} \cdot 9 = 0.$$

Notice that both of these observations are contrary to the criterion (a) that we have above for "randomness" of the sequence $\mathtt{d}_1, \mathtt{d}_2, \ldots \mathtt{d}_{p-1}$.

Now let's look at some actual data. Table 4 lists, for various p, the values of the A-statistic $A(1/p)$. Our two observations are visible in this table, but notice that there is more than we anticipated: in this small data set we see that, when p has the form $4k+3$, the statistic $A(1/p)$ is always a *positive* multiple of 11, contrary to our criterion (b) for randomness. In fact this statement holds in general, and this follows from Girstmair's theorem:

Theorem 2.2 (Girstmair 1994)**.** *For a prime number p, suppose that 10 is a primitive root of p and let $1/p = 0.\overline{\mathtt{d}_1\mathtt{d}_2\ldots\mathtt{d}_{p-1}}$. The A-statistic of the sequence $\mathtt{d}_1, \mathtt{d}_2, \ldots \mathtt{d}_{p-1}$ is given by*

$$A(1/p) = \begin{cases} 0 & \text{if } p = 4k+1 \text{ for some } k \\ 11N_p & \text{if } p = 4k+3 \text{ for some } k, \end{cases}$$

where N_p is a certain positive integer depending upon p.

This might seem like only a slight improvement upon our two observations made above, and not a very interesting conspiracy. But the statement in Theorem 2.2 is only the tip of the iceberg. As we discuss in the next section, Girstmair showed is that the integer N_p is one that has interested number theorists for centuries.

2.2 Binary quadratic forms

To get an idea about the significance of the numbers N_p appearing in Theorem 2.2, we need to consider some questions that seem far removed from our earlier ones. These are questions that have intrigued number theorists since at least the time of Fermat, and perhaps the simplest of them is the following: Which integers $n \geqslant 0$ are a sum of two squares? That is, for which n do there exists integers x, y such that $n = x^2 + y^2$? Fermat proved a theorem that gave a criterion for answering this question completely and, perhaps unexpectedly, the key step in his proof is to understand which *primes* can be written as a sum of two squares.[8] Similarly, Fermat was able to determine when a prime could be written in the form $x^2 + 2y^2$, and from this he could answer the more general question of which positive integers had this form. He could also tell when a prime, and hence any integer, had the form $x^2 + 3y^2$. But the next[9] logical question was to ask which primes could be written in the form $x^2 + 5y^2$, and Fermat was unable to provide an answer.

Successive generations of mathematicians, especially Euler, Legendre, Lagrange, and Gauss, took up the task of (verifying and) continuing Fermat's work, and were drawn into a larger landscape of equations, one that turned out to be surprisingly difficult to navigate. This larger landscape is the theory of *integral binary quadratic forms*, which are expressions of the form

$$ax^2 + bxy + cy^2,$$

where a, b, c are some fixed integers and x, y are the indeterminates. We'll usually just call these "quadratic forms" or even just "forms." The question, say, of deciding which integers are a sum of two squares can be phrased of asking which integers n are "represented" by the quadratic form $x^2 + y^2$. More generally, we say n is represented by the quadratic form $ax^2 + bxy + cy^2$ if there exist integers x, y such that

$$ax^2 + bxy + cy^2 = n.$$

Motivated by Fermat's work, one is lead to ask:

Question 2.3. *Which prime numbers are represented by a given quadratic form $ax^2 + bxy + cy^2$?*

In answering this question, it's worth noting that certain quadratic forms are less deserving of our attention than others. Specifically, if the coefficients a, b, c are all share a nontrivial factor, then any integer represented by that form must also be divisible by that factor. As one example, the only prime that the form $5x^2 - 15xy + 25y^2$ could (possibly) represent is 5 because the coefficients (and hence all of the integers it represents) are divisible by 5. As second example, the form $4x^2 - 8xy + 12y^2$ can never represent any prime because 4 divides all of the coefficients. For this reason, we'll restrict our attention to so-called *primitive* quadratic forms, which are those satisfying the condition $\gcd(a, b, c) = 1$.

Now certain quadratic forms can be seen to represent exactly the same integers, for the simple reason that they are related by a reversible substitution. To demonstrate this, let's show that the simple form $q_1(x, y) = x^2 + y^2$ represents exactly the same integers as the more complicated form

$$q_2(X, Y) = 13X^2 - 16XY + 5Y^2.$$

[8] The answer, it turns out, is that the prime must be either 2 or have the form $4k + 1$; but we're going to focus more on the process of obtaining the answer, rather than the actual answer. For the answer to which integers (prime or composite) are a sum of two squares, an internet search or a book on elementary number theory can get you started.

[9] The question of which primes have the form $x^2 + 4y^2 = x^2 + (2y)^2$ has the nearly the same answer as primes of the form $x^2 + y^2$ (just omit the prime 2), so this question isn't so interesting.

First notice that if we let $x = 2X - Y, y = -3X + 2Y$ and plug in this into the form $q_1(x, y)$, we find

$$x^2 + y^2 = (2X - Y)^2 + (-3X + 2Y)^2 = 13X^2 - 16XY + 5Y^2.$$

Thus the fact that, say, 61 is represented by $q_2(X, Y)$ will imply it's also represented by $q_1(x, y)$: starting from $61 = q_2(7, 8)$, we let $x_0 = 2 \cdot 7 - 8 = 6$, $Y_0 = -3 \cdot 7 + 2 \cdot 8 = -5$, and conclude (as you can verify directly) that $61 = q_1(6, -5)$. Conversely, since

$$\begin{cases} x = 2X - Y \\ y = -3X + 2Y \end{cases} \quad \Longrightarrow \quad \begin{cases} X = 2x + y \\ Y = 3x + 2y \end{cases}$$

we can go in the opposite direction:

$$13X^2 - 16XY + 5Y^2 = 13(2x + y)^2 - 16(2x + y)(3x + 2y) + 5(3x + 2y)^2 = x^2 + y^2$$

Given the representation $29 = 5^2 + 2^2$, we can let $X_0 = 2 \cdot 5 + 2 = 12$, $Y_0 = 3 \cdot 5 + 2 \cdot 2 = 19$, and obtain the representation $29 = q_2(12, 19)$.

In general, we can make the substitution $x = \alpha X + \beta Y$, $y = \gamma X + \delta Y$ in a quadratic form $q(x, y)$ to obtain a new quadratic form $Q(X, Y)$. If $\alpha, \beta, \gamma, \delta$ are all integers, then x, y will be integers whenever X, Y are integers; thus any n represented by $Q(X, Y)$ is represented by $q(x, y)$. In order to go in the opposite direction, we need to say that when x, y are integers, so are X, Y; this will be true when the integers $\alpha, \beta, \gamma, \delta$ satisfy the condition $\alpha\delta - \beta\gamma = 1$. [10] This motivates the following:

Definition 2.4. *Two integral binary quadratic forms $q(x, y)$ and $Q(X, Y)$ are called* equivalent *if we can transform $q(x, y)$ into $Q(X, Y)$ by using a substitution of the form $x = \alpha X + \beta Y$, $y = \gamma X + \delta Y$, where $\alpha, \beta, \gamma, \delta$ are integers that satisfy $\alpha\delta - \beta\gamma = 1$.*

Given a form $q(x, y)$, the collection of all forms that are equivalent to $q(x, y)$ is called its equivalence class.

Now suppose that we're handed two quadratic forms $q(x, y)$ and $Q(X, Y)$; is there a way to tell whether they're equivalent? We could try using the definition directly, which would mean searching for an appropriate substitution that will transform one into the other. But there are actually infinitely many possible substitutions, and this kind of guess-and-check approach doesn't present a clear way forward. Instead, mathematicians seized upon an easier feature of each quadratic form, its *discriminant*. The discriminant of $q(x, y) = ax^2 + bxy + cy^2$ is the integer $D = b^2 - 4ac$, and the story is particularly nice when $D < 0$. So we will only focus upon forms with negative discriminant; we will also restrict ourselves to forms where $a > 0$. A form $q(x, y)$ with $D < 0$ is called *positive definite*, because $q(x, y) > 0$ whenever $(x, y) \neq (0, 0)$.

The importance of the discriminant is that, as one can show by a tedious but straightforward check, equivalent quadratic forms always have equal discriminants. (For instance, you can verify in the example above that both $q_1(x, y)$ and $q_2(X, Y)$ both have discriminant -4.) To see how useful this is, notice the two quadratic forms

$$q(x, y) = 7x^2 - 3xy + y^2, \qquad Q(X, Y) = 2X^2 + 2XY + Y^2$$

are not equivalent, simply because the discriminant of $q(x, y)$ is -19 while the discriminant of $Q(X, Y)$ is -4. In other words, no matter how many substitutions as in Definition 2.4 we try, we'll never be able to turn $q(x, y)$ into $Q(X, Y)$!

In this way, the discriminant is a very handy tool for showing that certain pairs of quadratic forms are not equivalent. It naturally leads us to wonder whether the discriminant can help us completely solve the problem of equivalence:

[10] More generally, this will work exactly when $\alpha\delta - \beta\gamma = \pm 1$. But it was Gauss who suggested using substitutions satisfying the stricter condition $\alpha\delta - \beta\gamma = 1$, and that the relations between various quadratic forms are illuminated much better if one makes this small change. In any case, this will be the most relevant type of substitution for our purposes.

Question 2.5. *If two quadratic forms $q(x, y)$ and $Q(X, Y)$ both have the same discriminant D, are they necessarily equivalent?*

Let's pause at this point to acknowledge that, with all this terminology about quadratic forms and their classification, it might feel like we've diverged from the original spirit of Fermat's questions. But it turns out that the preceding question has a direct impact upon Fermat's interests: if the answer to Question 2.5 is yes, it is *much* easier to answer Question 2.3 regarding which primes—and which integers in general—are represented by a quadratic form of discriminant D.

Let me give a vague idea of what I mean when I say that Question 2.3 is "easier" to answer in this case. If we have a quadratic form $q(x, y)$ of discriminant D and a prime p, there is a certain *necessary* condition, let's call it $\mathcal{C}_D$ for short, that must be satisfied by p in order to say $q(x, y)$ can represent p. While I can't state it precisely here, a few examples can give a hint about the general character of $\mathcal{C}_D$:

- $\mathcal{C}_{-4}$: If $q(x, y)$ has $D = -4$ and $p \neq 2$, p must have the form $4k + 1$ (for some integer k) in order to be represented by $q(x, y)$.
- $\mathcal{C}_{-8}$: If $q(x, y)$ has $D = -8$ and $p \neq 2$, p must have the form $8k + 1$ or $8k + 3$ in order to be represented by $q(x, y)$.
- $\mathcal{C}_{-12}$: If $q(x, y)$ has $D = -12$ and $p \neq 2, 3$, p must have the form $3k + 1$ in order to be represented by $q(x, y)$.
- $\mathcal{C}_{-20}$: If $q(x, y)$ has $D = -20$ and $p \neq 2, 5$, p must have the form $20k + 1, 20k + 3, 20k + 7$, or $20k + 9$ in order to be represented by $q(x, y)$.

For a given discriminant D, $\mathcal{C}_D$ is not too difficult to write down if one knows the so-called Law of Quadratic Reciprocity, a standard topic in undergraduate number theory. The upshot is that when the answer to Question 2.5 is yes, the condition $\mathcal{C}_D$ is also a *sufficient* that guarantees $q(x, y)$ will represent p; when the answer is no, $\mathcal{C}_D$ is not sufficient and more complicated ideas are required to determine whether $q(x, y)$ will represents p.

For instance, it turns out that all primitive quadratic forms of discriminant -4 are equivalent, and the same is true of quadratic forms of discriminant -8 and -12. Thus the conditions $\mathcal{C}_{-4}, \mathcal{C}_{-8}$, and $\mathcal{C}_{-12}$ tell us which primes can be written in the form $x^2 + y^2$, $x^2 + 2y^2$, or $x^2 + 3y^2$. However, not all quadratic forms of discriminant -20 turn out to be equivalent. For instance, one can show that $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$ are two inequivalent forms of discriminant -20; furthermore (ignoring the primes 2 and 5), the form $x^2 + 5y^2$ only represents the primes of the form $20k + 1$ and $20k + 9$ while $2x^2 + 2xy + 3y^2$ only represents the primes of the form $20k + 3$ and $20k + 7$. Hence $\mathcal{C}_{-20}$ is not a sufficient condition for telling when a form of discriminant -20 represents a prime. In light of this fact, it seems less surprising that Fermat had difficulty determining the primes of the form $x^2 + 5y^2$.

Getting back to the basic concern of Question 2.5, it might help to view the landscape of all (primitive positive definite) quadratic forms as being divided up into infinitely many separate "states." Each state consists of all of the forms having the same discriminant D, and any given quadratic form $q(x, y)$ belongs to exactly one of these states. In fact, since equivalent forms share the same discriminant, the entire equivalence class of $q(x, y)$ is contained within a single state. If we think of each equivalence class as a "county," then each state is divided up into counties. In this map-making analogy, Question 2.5 asks whether every state contains only one county. In the states with $D = -4, -8, -12$, the answer is yes but in the state with $D = -20$, there turn out to be two counties. This means the general problem of determining whether two forms are equivalent—and thus which primes are represented by a form—is difficult.

One bit of good news, though, is that there happen to be only finitely many equivalence classes corresponding to every discriminant, i.e., each state has only finitely many counties. This is not an easy fact to prove, but once we have it we can make the following definition:

Definition 2.6. *For an integer $D < 0$, the* class number $h(D)$ *is the number of distinct equivalence classes of quadratic forms having discriminant D.*

Regarding the examples above, we have $h(-4) = h(-8) = h(-12) = 1$ and $h(-20) = 2$.

We are now *finally* ready to state Girstmair's Theorem 2.2 in a more precise manner. Remember that theorem? It had something to do with the decimal expansion of $1/p$... that seems a world away from us now, after all of this talk about quadratic forms. But that perceived distance is exactly what makes his result so surprising:

Theorem 2.7 (Girstmair 1994)**.** *For a prime number p, suppose that 10 is a primitive root of p and let $1/p = 0.\overline{\mathtt{d}_1\mathtt{d}_2\ldots\mathtt{d}_{p-1}}$. The A-statistic of the sequence $\mathtt{d}_1, \mathtt{d}_2, \ldots \mathtt{d}_{p-1}$ is given by*

$$A(1/p) = \begin{cases} 0 & \text{if } p = 4k+1 \text{ for some } k \\ 11h(-p) & \text{if } p = 4k+3 \text{ for some } k, \end{cases}$$

where $h(-p)$ is the class number of all primitive binary quadratic forms having discriminant $-p$.

For instance, we have $A(1/7) = -1 + 4 - 2 + 8 - 5 + 7 = 11$. Therefore $h(-7) = 1$, meaning that all primitive quadratic forms of discriminant -7 are equivalent to each other. We can make this statement more concrete by singling one out: all forms with $D = -7$ are equivalent to $x^2 + xy + 2y^2$. So this means it's "easy" to determine which primes are represented forms with $D = -7$. For instance, since $1^2 + 1 \cdot 2 \cdot 2^2 = 7$, the form $x^2 + xy + 2y^2$ represents 7, and hence so do all forms with $D = -7$. Moreover, the condition $\mathcal{C}_{-7}$ reads:

- $\mathcal{C}_{-7}$: If $q(x, y)$ has $D = -7$ and $p \neq 7$, p must have the form $7k + 1$, $7k + 2$, or $7k + 4$ in order to be represented by $q(x, y)$.

Since $h(-7) = 1$, the condition $\mathcal{C}_{-7}$ is sufficient, meaning that a quadratic form with $D = -7$ will represent the primes $2, 7, 11, 23, 29, 37, 43, \ldots$ and will not represent the primes $3, 5, 13, 17, 19, 31, 41, \ldots$.

Since we have $A(1/19) = 11$ and thus $h(-19) = 1$, a similar analysis can tell us which primes are represented by forms with $D = -19$. On the other hand, we see that $A(1/23) = 33$, so that $h(-23) = 3$. Therefore it takes more work, and more techniques than someone like Fermat would have had available, to determine which primes are represented by a form such as $x^2 + xy + 6y^2$, which has $D = -23$.

Now I don't want to give the impression that both of these facts are new, because the values of $h(-7)$, $h(-19)$, and $h(-23)$ have been known for a long time. But they were computed using methods that required significantly more background to carry out. What Theorem 2.7 shows is that, during all those years, there were some lowly decimal expansions who also knew these values, and they held their tongue about it all the way until the 1990s.

3 Further directions

In this conclusion, I'll indicate a few things that I didn't include in the previous parts, as well as some places where an interested reader can find out more.

3.1 Beyond base 10

One of the goals of this article is to bring out some ideas from number theory in a context that is more familiar and less intimidating than the general setting. Specifically, that context is our usual way of representing numbers using the decimal system, i.e., using the base 10. But we can also consider the *binary* expansion of $1/n$ (corresponding to base 2), or the *hexidemical* expansion of $1/n$ (corresponding to base 16), or more generally the base b expansion of $1/n$ for any integer $b \geqslant 2$.

The facts we proved in Part 1 continue hold if we consider the base b expansion of $1/n$:

- The base b expansion of $1/n$ is finite if and only if b and n are divisible by exactly the same prime numbers.
- If $\gcd(n, b) = 1$, then the base b expansion of $1/n$ is infinite and (purely) periodic.
- The length ℓ of the shortest repeating sequence in the base b expansion of $1/n$ is the smallest integer $\ell \geqslant 1$ such that $b^\ell - 1$ is divisible by n.
- When p is prime, this length ℓ divides $p - 1$, and we have $\ell = p - 1$ exactly when b is a primitive root of p.

These facts are proved with the help of the full version of Euler's Theorem, which states that n divides $b^{\phi(n)} - 1$ whenever $\gcd(n, b) = 1$. For more about these base-b expansions, see [HW].

There is also a version of Conjecture 1.12 for general b, called Artin's Primtive Root Conjecture; in particular, it predicts that, when b is not a square, there should exist infinitely many primes p having b as a primitive root. See [Mur] for more on this conjecture.

Finally, Girstmair actually stated his results not for decimal expansions, but in terms of a general base-b expansion. His result states that if $p = 4k + 3$ and b is a primitive root of p, and hence the base-b expansion of $1/p$ has period $p-1$, then the A-statistic of the repeating digits in this expansion equals $(b+1)h(-p)$. This allows us to compute other class numbers that can't be computed with decimal expansions. For instance, we can't use the A-statistic of the decimal expansion of $1/11$ to compute $h(-11)$, but we could use the binary expansion of $1/11$ to do so because 2 is a primitive root of 11.

Girstmair's most accessible account of his result is [Gir2]. The result there is a special case of more technical work in [Gir1]. The later works [Gir3] and [MT] give some extensions, such as the fact that one can compute $h(-p)$ using the base-b expansion of $1/p$ when $p = 4k + 3$ and the period is $(p - 1)/2$. (One doesn't use the A-statistic in that case, but something similarly simple.)

3.2 The virtues of abstract algebra

Most of the results in Part 1 can be proved more easily if one knows some abstract algebra, namely at the level of the rings $\mathbb{Z}/n\mathbb{Z}$ and their groups of units $(\mathbb{Z}/n\mathbb{Z})^\times$. The specific link that one needs is Proposition 1.6, which connects the period of $1/n$ (when $\gcd(n, 10) = 1$) to the smallest exponent ℓ such that n divides $10^\ell - 1$. In the language of abstract algebra, this ℓ is the same as the order of the element $[10]$ in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$. So much of our concern in Part 1 is really about trying to pin down this order.

If one understands this translation and is fluent in the language, things become easier. For instance, Euler's Theorem follows very quickly from a general theorem of Lagrange when applied to the finite group $(\mathbb{Z}/n\mathbb{Z})^\times$, whose order is $\phi(n)$. Moreover, the so-called *Chinese Remainder Theorem* says that if the prime factorization of n is

$$n = p_1^{h_1} p_2^{h_2} \cdots p_r^{h_r},$$

then we have a ring isomorphism

$$\mathbb{Z}/n\mathbb{Z} \simeq (\mathbb{Z}/p_1^{h_1}\mathbb{Z}) \oplus (\mathbb{Z}/p_2^{h_2}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p_r^{h_r}\mathbb{Z}),$$

which one can restrict to the units to give the following isomorphism of groups:

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1^{h_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{h_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{h_r}\mathbb{Z})^\times.$$

With this isomorphism in hand, one is not too far away from being able to deduce Proposition 1.17.

In this way, abstract algebra handles the elegant structural reductions that we made in Part 1 with great ease. But it doesn't have as much to offer in terms of understanding the chaotic graph in Figure 1. In other words, whether we call it the period of the decimal expansion of $1/p$ or the order of $[10]$ in $(\mathbb{Z}/p\mathbb{Z})^\times$, we still have trouble understanding how this varies as p gets larger!

3.3 Another interpretation of $h(-p)$

In addition to counting equivalence classes of binary quadratic forms of discriminant $D = -p$, there is another interpretation of the class number $h(-p)$ that arises in Girstmair's theorem: it is measures the size of the so-called *ideal class group* of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$.

Let me try to convey what this means. For a prime p, we can consider complex numbers of the form $a + b\sqrt{-p}$, where a and b are both *rational* numbers; note that this can also be written as as $a + bi\sqrt{p}$, where $i = \sqrt{-1}$. This is a subset of the set of all complex numbers that is typically denoted as $\mathbb{Q}(\sqrt{-p})$. With some effort, one can verify that if we take two numbers in $\mathbb{Q}(\sqrt{-p})$, we can add, subtract, or multiply them and we'll get another number in $\mathbb{Q}(\sqrt{-p})$; moreover, if one of them is not zero, we can divide it into the other one and again obtain something in $\mathbb{Q}(\sqrt{-p})$. We say that $\mathbb{Q}(\sqrt{-p})$ is closed under addition, subtraction, multiplication, and division, and these nice properties make $\mathbb{Q}(\sqrt{-p})$ into a *field* in the parlance of abstract algebra. More generally, we can replace p by any integer d which is squarefree (i.e., is a product of distinct primes), and we'll obtain a field denoted as $\mathbb{Q}(\sqrt{-d})$. Such fields are called *imaginary quadratic fields*.

Although they seem fairly abstract, these fields receive a lot of attention in number theory because they are related to statements about integers. For instance, if n is a positive, can it be written in the form $x^2 + 7y^2$ for some integers x, y? This is equivalent to asking if the equation

$$n = x^2 + 7y^2 \tag{3.1}$$

has integer solutions x, y. But an inspired factorization turns this equation into

$$n = (x + y\sqrt{-7})(x - y\sqrt{-7}). \tag{3.2}$$

Notice that $x \pm y\sqrt{-7}$ belong to the field $\mathbb{Q}(\sqrt{-7})$, which means we've turned our original question about *adding* certain kinds of integers into a question about *multiplying* certain kinds of numbers in $\mathbb{Q}(\sqrt{-7})$.

In fact, in (3.2) we're not just multiplying any kind of numbers in $\mathbb{Q}(\sqrt{-7})$; the assumption is that x, y are integers, and not just rational. This implies that the numbers $x \pm y\sqrt{-7}$ are what are called *algebraic integers*. I won't go into the general definition of algebraic integers, but if we let R_7 denote the collection of all algebraic integers inside the field $\mathbb{Q}(\sqrt{-7})$, then I will say the following: R_7 is closed under addition, subtraction, and multiplication, but *not* division. For this reason, R_7 is called a *ring*.

In general, one can consider the subset of all algebraic integers R_d inside $\mathbb{Q}(\sqrt{-d})$, and R_d will always be a ring. Now the world's most famous ring is $\mathbb{Z}$, the ring of integers, and one can ask how much a ring of "algebraic integers" like R_d resembles the ring of "actual integers" $\mathbb{Z}$. In particular, one incredibly useful feature of the ring $\mathbb{Z}$ is its unique factorization property: integers other than 0 and ± 1 can be factored uniquely into a product of primes (along with a factor of -1 if the integer is negative). One can also define a notion of "primes" in the rings R_d. So the question arises as to whether most elements of R_d—that is, elements besides 0, ± 1, and other numbers with complex absolute value 1—can be written as a product of prime elements in an (essentially) unique way. If so, we call R_d a "unique factorization domain", or simply a UFD.

So one motivation for wanting R_d to be a UFD is that it looks more like the usual ring of integers $\mathbb{Z}$ that we know and love. But there is another reason: it makes certain problems about integers easier to solve. A perfect example of this is equation (3.1) above. If we knew that R_7 were a UFD, we could turn (3.1) into (3.2) and use unique factorization in R_7 to determine for which n there are integer solutions x, y.

Sadly, it turns out that R_d is not always a UFD. But R. Dedekind found a way to partially repair the situation by introducing *ideals*, which are certain nice subsets of R_d. One can show that these ideals factor (in sense I won't define) uniquely into so-called *prime ideals*, which are ideals in R_d that have "prime-like" properties. Moreover, by investigating relations between these ideals, one can create from them a supplementary object known as the *ideal class group*, which is a finite set (in fact, a finite group). The size of this group is a positive integer called the *ideal class number* of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$, and we denote it as $h(-d)$.

Complicated thought it may be, the great thing about the ideal class number of $\mathbb{Q}(\sqrt{-d})$ is that it tells us whether R_d is a UFD. More precisely, R_d is a UFD if and only if the ideal class number $h(-d) = 1$. In that case, we're able to put aside the more intricate notions of ideals and prime ideals, and instead just work with the actual elements and prime elements of R_d.

Now let's get to the connection with quadratic forms: when p is a prime of the form $4k + 3$, the ideal class number of $\mathbb{Q}(\sqrt{-p})$ can be shown to equal to the number of equivalence classes of integral binary quadratic forms of discriminant $D = -p$. This is why it's safe to denote both of these things by $h(-p)$. So Girstmair's result says that when 10 is a primitive root of $p = 4k + 3$, the decimal expansion of $1/p$ can be used to calculate the ideal class group of $\mathbb{Q}(\sqrt{-p})$, and thus to determine whether the ring R_p is a UFD. In particular, the decimal expansion of $1/7$ can be used to conclude that R_7 is a UFD.

Imaginary quadratic fields are among the first examples of what are called *algebraic number fields*, which are the focus of algebraic number theory. Any introductory book on algebraic number theory will contain this material; the book [PD] presupposes less background, while books such as [Mar] or [Sam] assume a familiarity with much more abstract algebra. Another sophisticated introduction is the book [FT], which also explains the connection between the class numbers in §2.2 and the ideal class numbers discussed here. This is also explained in the excellent book [Cox], which is generally at a higher level than the preceding books, but also contains much historical material on quadratic forms that is easier to follow.

References

[Cox] D. A. Cox. *Primes of the form $x^2 + ny^2$*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication. http://dx.doi.org/10.1002/9781118400722

[Dic] L. E. Dickson. *History of the theory of numbers. Vol. I: Divisibility and primality.* Chelsea Publishing Co., New York, 1966.

[FT] A. Fröhlich and M. J. Taylor. *Algebraic number theory*, volume 27 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993.

[Gir1] K. Girstmair. The digits of $1/p$ in connection with class number factors. *Acta Arith.* **67** (1994), 381–386.

[Gir2] K. Girstmair. A "popular" class number formula. *Amer. Math. Monthly* **101** (1994), 997–1001. http://dx.doi.org/10.2307/2975167

[Gir3] K. Girstmair. Periodische Dezimalbrüche—was nicht jeder darüber weiß. In *Jahrbuch Überblicke Mathematik, 1995*, pages 163–179. Vieweg, Braunschweig, 1995.

[HW] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford University Press, Oxford, sixth edition, 2008. Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles.

[HPS] J. Hoffstein, J. Pipher, and J. H. Silverman. *An introduction to mathematical cryptography*. Undergraduate Texts in Mathematics. Springer, New York, second edition, 2014. http://dx.doi.org/10.1007/978-1-4939-1711-2

[JP] R. Jones and J. Pearce. A postmodern view of fractions and the reciprocals of Fermat primes. *Math. Mag.* **73** (2000), 83–97. http://dx.doi.org/10.2307/2691078

[Lea] W. G. Leavitt. Repeating decimals. *College Math. J.* **15** (1984), 299–308. http://dx.doi.org/10.2307/2686394

[Mar] D. A. Marcus. *Number fields*. Springer-Verlag, New York-Heidelberg, 1977. Universitext.

[Mur] M. R. Murty. Artin's conjecture for primitive roots. *Math. Intelligencer* **10** (1988), 59–67. http://dx.doi.org/10.1007/BF03023749

[MT] M. R. Murty and R. Thangadurai. The class number of $\mathbb{Q}(\sqrt{-p})$ and digits of $1/p$. *Proc. Amer. Math. Soc.* **139** (2011), 1277–1289. http://dx.doi.org/10.1090/S0002-9939-2010-10560-9

[PD] H. Pollard and H. G. Diamond. *The theory of algebraic numbers*. Dover Publications, Inc., Mineola, NY, third edition, 1998.

[Ros] K. A. Ross. Repeating decimals: a period piece. *Math. Mag.* **83** (2010), 33–45. http://dx.doi.org/10.4169/002557010X479974

[Sam] P. Samuel. *Algebraic theory of numbers*. Translated from the French by Allan J. Silberger. Houghton Mifflin Co., Boston, Mass., 1970.

[SF] M. Shrader-Frechette. Complementary rational numbers. *Math. Mag.* **51** (1978), 90–98.

[Sil] J. H. Silverman. *A friendly introduction to number theory*. Pearson, fourth edition, 2012.

California State University, Fullerton, Department of Mathematics, Fullerton, CA 92834
Email address: clyons@fullerton.edu