Our Primitive Roots

Chris Lyons

Abstract

When n is not divisible by 2 or 5, the decimal expansion of the number $1/n$ is an infinite repetition of some finite sequence of r digits. For instance, when $n = 7$ we know that $1/7 = 0.142857142857142857...$ which repeats the 6-digit sequence 142857. Given n, how long can r possibly be? We'll start by exploring this simple question, which will ultimately lead us to the notion of *primitive roots* and to a long standing unsolved problem.

Then we'll narrow our focus to the expansion of $1/p$ when p is prime. In the case when p is of the form $4k + 3$ and the repeating sequence is "as long as possible," it turns out that these seemingly mundane digits actually encode a deep property of the prime number p.

1 Decimal expansions of rational numbers

At some point in your mathematical education, you've learned the following distinction between rational and irrational real numbers: roughly speaking, *the decimal expansions of rational numbers are always either finite in length or eventually periodic, while the decimal expansions of irrational numbers never terminate and are never periodic.* I want to focus on the decimal expansions of rational numbers. These are, in a mathematical sense, "everyday objects." Indeed, whether you chose to or not, I'm sure you've memorized at least a few of them. For instance, you probably know

$$\begin{aligned} 1/2 &= 0.5 \\ 1/3 &= 0.3333333... \\ 1/4 &= 0.25 \\ 1/5 &= 0.2 \\ 1/6 &= 0.1666666... \end{aligned}$$

How about the expansion of 1/7? You've certainly 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 your memory. Similarly, you may know the expansion:

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

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

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

which repeats the 6 digit sequence 076923.

Of course we could talk about fractions that look different than $1/n$, e.g., 7/3, 19/16, etc. But any fraction is just a multiple of $1/n$ for some n, so we'll stick to $1/n$ for our discussion. Much (though not all) of what we'll say is relatively simple to extend to more general fractions.

Before proceeding further, let's remember a handy notational device that you've also probably seen before: if a sequence of digits repeats, we just put a line over that sequence to indicate this. Three examples are:

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

When does the decimal expansion of $1/n$ terminate, and when does it go on forever? If it does go on forever, when does it start out with some initial "non-repeating part" before reaching a repeating sequence? The answer is summarized in the following:

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

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

(b) Suppose the decimal expansion of $1/n$ does not terminate (meaning n is divisible by at least one prime not equal to 2 or 5). Then the decimal expansion is of the form

$$1/n = 0.\overline{a_1 a_2 \dots a_r}$$

for some digits $a_1, \dots, a_r$ if and only if n is divisible by neither 2 nor 5.

As an example of (b), notice that the decimal expansions $1/6 = 0.1\overline{6}$ and $1/12 = 0.08\overline{3}$ both begin with a short non-repeating sequence, and this can be explained by the fact that both 6 and 12 are divisible by 2.

Proof. If you're used to writing proofs, then you can probably come up with one after awhile by playing around with some examples to see what's going on. (For instance, you might notice that

$$\frac{1}{80} = \frac{5^3}{10^4} = \frac{125}{10000} = 0.0125$$

and that

$$\frac{1}{12} = \frac{1}{100} \cdot \frac{25}{3} = \frac{1}{100}\left(8 + \frac{1}{3}\right) = 0.08\overline{3},$$

and think about some other similar examples; why have I written them in this way?) Once you have the idea, it becomes a matter of carefully setting up the right notation to cover the general case. Since this gets a little messy and will lead us off on a sidetrack, we'll omit the proof. □

We're only going to concern ourselves with the case when the decimal expansion is infinite and has no "non-repeating part." Thus: *From now on we assume that $n \geq 2$ is divisible by neither 2 nor 5.* Equivalently, we assume that $\gcd(n, 10) = 1$; often we describe this situation by saying that *n is coprime to 10.*

So we're assuming that the decimal expansion is just an infinite repetition of some finite sequence. There's a little bit of ambiguity here. For instance, all three of the expressions

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

are accurate, but the first is the most efficient. Here's how we handle this ambiguity:

Definition 1.2. *We'll say that the* period of $1/n$ *is the length of the smallest repeating sequence in the decimal expansion of $1/n$.*

Hence the period of $1/3$ is 1 and the period of $1/7$ is 6. (I should warn you that this terminology may not be standard, but it will be convenient for us.)

Now let's explore this notion of period by looking at a list of decimal expansions of $1/n$ for the first few values of n that are not divisible by 2 or 5:

$$\begin{aligned}
1/3 &= 0.\overline{3} \\
1/7 &= 0.\overline{142857} \\
1/9 &= 0.\overline{1} \\
1/11 &= 0.\overline{09} \\
1/13 &= 0.\overline{076923} \\
1/17 &= 0.\overline{0588235294117647 0} \\
1/19 &= 0.\overline{052631578947368421} \\
1/21 &= 0.\overline{047619} \\
1/23 &= 0.\overline{0434782608695652173913} \\
1/27 &= 0.\overline{037} \\
1/29 &= 0.\overline{0344827586206896551724137931} \\
1/31 &= 0.\overline{032258064516129}
\end{aligned}$$

Let's start looking for patterns, even some vague ones. For starters, we notice that the periods seem to be getting longer as n increases. However, at $n = 21$ and $n = 27$, the period becomes short again. Why? Well, a good guess is that it has something to do with the fact that 21 and 27, although of comparable size with numbers like 19, 23, and 29, are both divisible by smaller numbers (3 and 7). So a rough first guess could be: *If n is divisible only by small primes, then the period of the expansion of $1/n$ will be relatively small.* This would seem to imply in particular that if n is a large prime number then the period of $1/n$ should be large. This is what's happening for $n = 17, 19, 23, 29$, and 31. But if we go a little higher, this philosophy runs into trouble:

$$1/37 = 0.\overline{037}, \qquad 1/41 = 0.\overline{02439}, \qquad 1/73 = 0.\overline{01369863}$$

Compared to the size of n, these expansions have pretty small periods! If you were to make a table of the periods of $1/n$ as n grows, even if you just restricted to prime values of n, you would find that patterns are hard to come by.

2 Primitive roots

To say anything further, we need to think about how we go from infinite repeating decimal expansions back to fractions. Let's write

$$1/n = 0.\overline{a_1 a_2 \dots a_r}$$

where each a_i is a decimal digit between 0 and 9 and r is the period of $1/n$. Let's have m be the integer which, in decimal notation, is written as $a_1 a_2 \dots a_r$. (Example: when $n = 13$ we have $1/13 = 0.\overline{076923}$ so in this case $m = 076923 = 76923$.) Then what the decimal expansion actually means is

$$\frac{1}{n} = \frac{m}{10^r} + \frac{m}{10^{2r}} + \frac{m}{10^{3r}} + \dots = \sum_{j=1}^{\infty} \frac{m}{10^{jr}}.$$

We use the geometric series formula to get the right side into a nice closed form:

$$\frac{1}{n} = \sum_{j=1}^{\infty} \frac{m}{10^{jr}} = m \sum_{j=1}^{\infty} \left(\frac{1}{10^r}\right)^j = \frac{m/10^r}{1 - 1/10^r} = \frac{m}{10^r - 1}.$$

Put another way, we have $10^r - 1 = mn$, which means that n divides $10^r - 1$. In fact, we have the following stronger statement:

Proposition 2.1. *The period of* $1/n$ *is the smallest integer* $r \geq 1$ *such that* n *divides* $10^r - 1$.

Proof. We've already shown that if the period of $1/n$ is r, then n divides $10^r - 1$. What remains is to show the following: if $1 \leq s < r$, then $10^s - 1$ is not divisible by n.

Assume for contradiction that we have $10^s - 1 = nq$. Then we can just reverse the work we did above: we have

$$\frac{1}{n} = \frac{q}{10^s - 1} = \sum_{j=1}^{\infty} \frac{q}{10^{jr}}.$$

Notice that if the decimal representation of q is $d_1 d_2 \dots d_\ell$, then we have $\ell \leq s$ (because q divides $10^s - 1$, which is the s-digit number 999...99). So the sum on the right represents a repeating decimal expansion of period s. Since $s < r$, and r was defined to be the period of $1/n$, this is a contradiction. □

As an example of this, consider $n = 7$. We have

$$\begin{aligned} 10^1 - 1 = 9 = 3^2; \qquad & 10^2 - 1 = 99 = 3^2 \cdot 11; \\ 10^3 - 1 = 999 = 3^3 \cdot 37; \qquad & 10^4 - 1 = 9999 = 3^2 \cdot 11 \cdot 101; \\ 10^5 - 1 = 99999 = 3^2 \cdot 41 \cdot 271; \qquad & 10^6 - 1 = 999999 = 3^3 \cdot 7 \cdot 11 \cdot 13 \cdot 37. \end{aligned}$$

Since $r = 6$ is the smallest positive integer such that $10^r - 1$ is divisible by 7, it follows that the period of $1/7$ is equal to 6 (which we've already seen before).

Believe it or not, it's actually advantageous to phrase Proposition 2.1 in more abstract language. If you're familiar with the language of congruences, then the proposition above is equivalent to saying the following:

Proposition 2.2. *The period of* $1/n$ *is the smallest integer* $r \geq 1$ *such that* $10^r \equiv 1 \pmod{n}$.

But the abstraction doesn't stop there. We can in turn rephrase this using basic notions from abstract algebra. Don't worry if you don't have background in this, because we'll just be briefly "passing through" this world. You can just gloss over the unknown technical terms and pay attention to the concrete consequences in Proposition 2.4 below... and take it as an advertisement for the power of abstract algebra!

In abstract algebra you learn, for every integer $m \geq 1$, about the ring of congruence classes modulo m, which is denoted as $\mathbb{Z}/m\mathbb{Z}$. (Sometimes this ring is also denoted as $\mathbb{Z}_m$, although number theorists tend to furrow their brows at this notation... What makes them so fussy? The keyword is "p-adic integers.") Inside of this ring is the group of multiplicative units, denoted $(\mathbb{Z}/m\mathbb{Z})^\times$. Since we're assuming that n is coprime to 10, this means that the congruence class $[10] \in \mathbb{Z}/n\mathbb{Z}$ is actually contained in the group $(\mathbb{Z}/n\mathbb{Z})^\times$. Using this terminology, Proposition 2.1 can be rephrased as:

Proposition 2.3. *The period of* $1/n$ *equals the order of the congruence class* $[10]$ *in the group* $(\mathbb{Z}/n\mathbb{Z})^\times$.

This formulation, while perhaps unpleasantly abstract at first, is powerful because it leads more directly to the following concrete consequences:

Proposition 2.4. *Suppose that* $n = p_1^{k_1} p_2^{k_2} \dots p_d^{k_d}$ *is the prime factorization of* n*, with each* $k_i \geq 1$*. Then*

(a) The period of $1/n$ *must divide*

$$p_1^{k_1 - 1}(p_1 - 1) p_2^{k_2 - 1}(p_2 - 1) \dots p_d^{k_d - 1}(p_d - 1).$$

(b) Let the period of $1/p^{k_i}$ *be* r_i*. Then the period of* $1/n$ *is equal to the least common multiple*

$$\operatorname{lcm}(r_1, r_2, \dots, r_d).$$

Proof. One can show that the size of the group $(\mathbb{Z}/n\mathbb{Z})^\times$ is

$$\varphi(n) = p^{k_1-1}(p_1-1)p^{k_2-1}(p_2-1)\dots p^{k_d-1}(p_d-1),$$

where φ is the *Euler phi function*. By the basic theory of finite groups (specifically, Lagrange's Theorem), the order of any element in $(\mathbb{Z}/n\mathbb{Z})^\times$ divides the order of the group, so we get part (a).

Part (b) follows from a result in number theory or ring theory (depending upon your taste) called the *Chinese Remainder Theorem*. This result says

$$(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/p_1^{k_1}\mathbb{Z}) \oplus (\mathbb{Z}/p_2^{k_2}\mathbb{Z}) \oplus \dots \oplus (\mathbb{Z}/p_d^{k_d}\mathbb{Z}),$$

and then yields

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1^{k_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{k_2}\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/p_d^{k_d}\mathbb{Z})^\times.$$

This second isomorphism is what is needed to show (b). □

This proposition is quite an eyeful, but if you step back from it, you'll notice that it says that the prime factorization of n is very important in determining the period of $1/n$. In fact it says that we'll be able to understand the period of $1/n$, for any n, if we're able to understand the period of $1/p^k$ for primes p and $k \geq 1$.

Instead of considering the larger case when n is a general power of a prime number, we'll just focus our attention on the first rung of this ladder by letting n be prime. *From now on, we assume that $p \neq 2, 5$ is a prime.* In this case Proposition 2.4 says the following:

Corollary 2.5. *The period of $1/p$ divides $p-1$.*

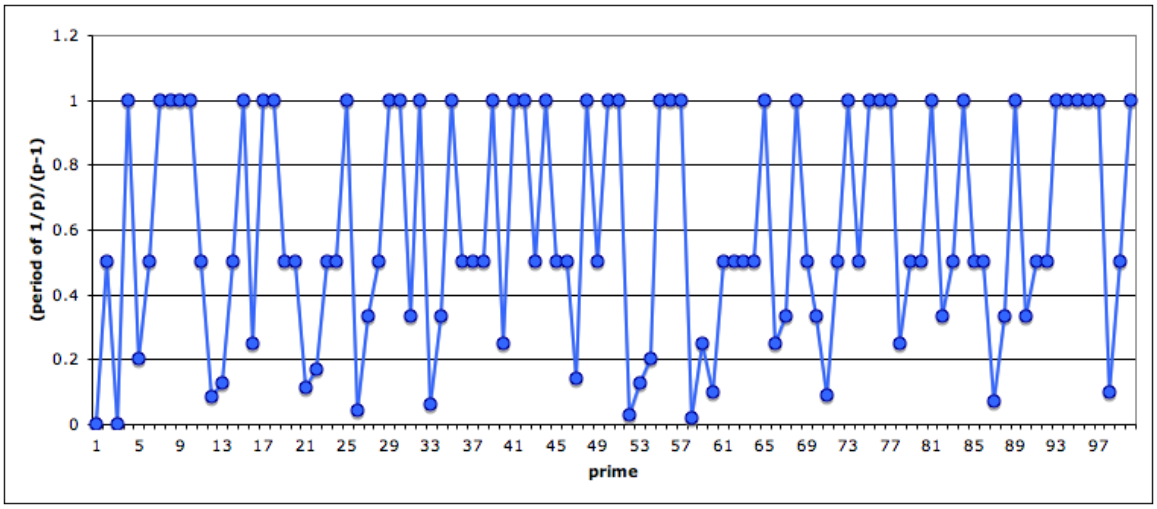
So for instance, I may not know off the top of my head what the period of $1/997$ is, but I do know that it has to divide $996 = 2^2 \cdot 3 \cdot 83$. Thus the period belongs to the (relatively small!) set of possibilities

$$\{1, 2, 3, 4, 6, 12, 83, 166, 249, 332, 498, 996\}.$$

Let's explore the periods of $1/p$ for the some small primes. We've just said that the period of $1/p$ divides the integer $p-1$. Let p_k denote the kth prime number (so $p_1 = 2, p_2 = 3, p_3 = 5, \dots$). In the chart below, I've plotted the points

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

for $1 \leq k \leq 100$. (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.)



See a pattern? I sure don't. This is a mysterious sequence, and 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.

Let's focus on a specific part of the graph: Each of the points whose y-value is 1 represents a prime p for which the period of $1/p$ is equal to the longest possible value, $p-1$. We actually have a special name for such primes; before we give it, we have to introduce some funny terminology from number theory:

Definition 2.6. *Choose a positive integer $b \geq 1$ which is coprime to p. We say that b* is a primitive root of *p if none of the numbers*

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

are divisible by p.

A theorem called *Fermat's Little Theorem* tells us that p will always divide $b^{p-1}-1$, so another way of saying this is: b is a primitive root of p if $r = p-1$ is the smallest value of $r \geq 1$ for which p divides $b^r - 1$. This notion of a primitive root is sort of weird, and it's definitely a valid question to ask why number theorists care about this at all. Unfortunately it would take too long to explain this point, but I will say that primitive roots have turned out to be useful even outside number theory, for instance in cryptography ("Diffie-Hellman key exchange") and even radar and sonar technology ("Costas array").

Anyway, if you think about what it means for 10 to be a primitive root of p, you'll see by our earlier discussion that you can express the idea using decimal expansions:

Corollary 2.7. *The period of $1/p$ equals $p-1$ exactly when 10 is a primitive root of p.*

The prime numbers p for which the period of $1/p$ is $p-1$ correspond to the points with y-value 1 in the graph above. That graph is so crazy that we don't even know the answer to the following basic question: as we look farther and farther to the right (i.e., as $k \to \infty$), do we continue to see points with y-value 1? This turns out to be an old question, and Gauss took a guess:

Conjecture (Gauss). *There are infinitely many primes p such that $1/p$ has period $p-1$. Equivalently, there are infinitely many primes p such that 10 is a primitive root of p.*

Despite a lot of study by many good mathematicians, we still don't know the answer to this question, and this is remarkable: who would have thought that there are still unanswered questions about something as mundane as the decimal expansions of rational numbers?

3 Other bases

Before we talk about other things, I'm obliged to make the following remark, which is one that's often heard about problems in elementary number theory: "There's nothing special here about the base 10." That is, we've been considering the *decimal* expansions of $1/n$ because, well, that's what we're used to. But there are other ways to expand numbers; for instance, we can compute 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 $b \geq 2$.

Here are some general facts that hold if we consider the base b expansion of $1/n$ (which you may compare to the case $b = 10$ discussed above):

- 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 b and n are coprime (that is, if $\gcd(n, b) = 1$), then the base b expansion of $1/n$ consists of a finite sequence of digits that repeats infinitely often.

- The length r of the shortest repeating sequence in the base b expansion of $1/n$ is the smallest integer $r \geq 1$ such that $b^r - 1$ is divisible by n.
- When p is prime, this length r divides $p-1$, and we have $r = p-1$ exactly when b is a primitive root of p.
- When b is not a square, then Emil Artin generalized Gauss' conjecture above by postulating that that there are infinitely many primes p such that b is a primitive root of p.

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

Now we're going to return to decimal expansions and narrow our focus: *From now on p will be a prime for which the period of $1/p$ equals $p-1$.* When p is large, this means the repeating sequence of $p-1$ digits is pretty long. Let's look at $p = 47$, which has a period of 46:

$$1/47 = 0.\overline{02127659574468085106382978723404255319148936 17}.$$

The first few digits will 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*.

Of course the digits of the decimal expansion of $1/p$ aren't actually random at all, but what I mean is this: If we take out a string of digits from the middle of the decimal expansion of $1/p$ and compare it with actual random strings of digits, can we tell the difference? Let's try it. 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 as period 130), one of them is from the middle of the expansion of 1/227 (which has period 226), and the other three rows are strings of 35 random digits. *Which of these three rows are random strings?*

41984732824427480916030534351145038

18782860059580793714132782255045931

56165863608677584594706576115269330

64017277591261236900963254209039020

58515283842794759825327510917030567

It's pretty tough to tell with the naked eye. The answer is that the first row comes from 1/131 and the last row comes from 1/227.

So now that we've convinced ourselves that these strings look somewhat random to our eyes, let's go beyond this and use a statistical test. There tons of tests that we could apply here, but I want to focus on one particular test for randomness. As we'll see, this test is going to fail when applied to the digits of $1/p$, and it will fail in a spectacular way. Here's the test: if $c_1 c_2 \ldots c_{p-1}$ is *any* string of $p-1$ digits, we'll say that the *A-statistic* of this string is the alternating sum

$$A := \sum_{j=1}^{p-1} (-1)^j c_j = -c_1 + c_2 - c_3 + c_4 - \ldots - c_{p-2} + c_{p-1}.$$

Now if $c_1 c_2 \ldots c_{p-1}$ is a truly random string of digits (to be more precise for those who know probability: assuming the digits are chosen with uniform probability from 0 through 9, and chosen independently) and p is large then:

(a) The value of A is likely to be close to zero (since $p-1$ is even and the expected value of all digits 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.

Knowing what ought to happen for random strings of $p-1$ digits, let's now apply the A-statistic to the digits of $1/p$. In the following table, the numbers in the left column are the first few primes p for which $1/p$ has period $p-1$. If $1/p = 0.\overline{a_1 a_2 \dots a_{p-1}}$, then the right column is the A-statistic of the string $a_1 a_2 \dots a_{p-1}$.

prime p for which period of $1/p$ equals $p-1$	**A-statistic applied to repeating digits of $1/p$**
7	11
17	0
19	11
23	33
29	0
47	55
59	33
61	0
97	0
109	0
113	0
131	55
149	0
167	121
179	55
181	0
193	0
223	77

Let's evaluate the "randomness" of the digits of $1/p$ based upon the A-statistic. First off, in half of the cases, A is exactly equal to zero, which we said above in (a) is unlikely to happen in the random case. Secondly, in the cases when it's nonzero, A is never actually negative, which conflicts with our criteria (b) for randomness. So, if this sort of behavior continues for larger and larger primes, then these expansions don't look very random at all through the lens of the A-statistic! This is already interesting, but let's look a little more closely at the positive numbers in the right column: they're all multiples of 11. This peculiar behavior of the digits of $1/p$ was observed only within the last 20 years, by number theorist Kurt Girstmair:

Theorem 4.1 (Girstmair 1994)**.** *Suppose that p is a prime number such that the period of $1/p$ is $p-1$. If $1/p = 0.\overline{a_1 a_2 \dots a_{p-1}}$, then the A-statistic of the string $a_1 a_2 \dots a_{p-1}$ is*

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

where h_p is a certain positive integer depending upon p.

A looming question is: when $p = 4k+3$, what is this integer h_p?

5 Class numbers

To answer that question, we have make a foray into the world of *algebraic number theory*. If $p = 4k+3$ for some k, let's consider the following set of complex numbers:

$$R_p := \left\{ a + b\left(\frac{1+i\sqrt{p}}{2}\right) \;\middle|\; a, b \in \mathbb{Z} \right\} \subseteq \mathbb{C}.$$

This set is closed under addition, subtraction, and multiplication and is, in the parlance of abstract algebra, a *ring*. The world's most famous ring is $\mathbb{Z}$, the ring of integers. Number theorists were originally interested

in questions about elements of the ring $\mathbb{Z}$, but they eventually found out that, to answer some of these questions, it's actually very helpful to relate them to this more exotic ring R_p.

Here's an example of what I mean. If we fix p a prime as above (e.g., $p = 7, 19, 23, 47, 59, \ldots$), can we find two integers x and y such that

$$x^2 + py^2 = 1000?$$

(This is an example of a *Diophantine equation*, and is the kind of thing that has motivated the development of a lot of number theory throughout history.) This is a pretty easy question to answer if you use a computer (or even just pencil and paper) to check through small values of x and y. But how about finding solutions to

$$x^2 + py^2 = 10^{747}$$

when x and y are integers? With a big number like 10^{747} on the right, your computer would never be able to search through all possible values of x and y. But it turns out that this equation is related to the ring R_p. Indeed, a little bit of tedious algebra shows that we can rewrite it as

$$\left(\frac{x-y}{2} + y\left(\frac{1+i\sqrt{p}}{2}\right)\right)\left(\frac{x+y}{2} - y\left(\frac{1+i\sqrt{p}}{2}\right)\right) = 2^{745}5^{747}.$$

Notice that if $x^2 + py^2 = 10^{747}$, then either x and y are both odd or both even, so $(x-y)/2$ and $(x+y)/2$ are integers and therefore the two factors on the left side both belong to R_p. So the question is converted from a question about adding certain elements in the ring $\mathbb{Z}$ to one about multiplying certain elements in the ring R_p.

Using knowledge of properties of R_p, number theorists can tell whether solutions of the equation above exist. But sometimes this question is easier to answer than other times. Indeed, just like the familiar notion of "prime number" in the ring $\mathbb{Z}$, there is a notion of "prime element" in the ring R_p. Since we have the highly useful fact in $\mathbb{Z}$ that prime factorizations are unique, we can ask: is there a similar version of unique factorization in R_p? It turns out that if R_p has the unique factorization property, then it's *much* easier to decide whether $x^2 + py^2 = 10^{747}$ has solutions.

To tell whether we have unique factorization in the ring R_p, there is an extremely important quantity associated to R_p called its *class number*. This is a positive integer and it has the following key property:

Fact. *R_p has the unique factorization property exactly when its class number equals 1.*

For this and other reasons, number theorists care a great deal about trying to compute the class numbers of the rings R_p. And now, if you haven't already guessed it, it's time to tell you what h_p is back in Theorem 4.1:

Theorem 5.1 (Girstmair)**.** *With the same conditions as in Theorem 4.1, let $p = 4k+3$. Then the A-statistic of the repeating digits of $1/p$ is equal to $11h_p$, where h_p is the class number of R_p.*

For instance, looking at our earlier table, we conclude that R_7 and R_{19} both have class number 1, and hence have the unique factorization property. On the other hand, R_{23} has class number 3 and R_{47} has class number 5, and so they don't have unique factorization. This tells us that it's much easier to answer the question about the existence of solutions to $x^2 + 7y^2 = 10^{747}$ and $x^2 + 19y^2 = 10^{747}$ than it is for $x^2 + 23y^2 = 10^{747}$ and $x^2 + 47y^2 = 10^{747}$.

Given the importance of class numbers, number theorists have spent a lot of energy coming up with ways to compute them. What Girstmair's result says is that, if 10 is a primitive root of $p = 4k + 3$, the class number h_p can be computed just by adding and subtracting digits of $1/p$ in an easy way, which is an astonishingly simple rule. Or from a slightly different angle, his result shows that there was an important number theoretic property about the prime number p that was hidden all along within the digits of $1/p$. Who knew that lowly decimal expansions could contain such deep secrets!

6 Further Reading

The most accessible account of Girstmair's result (which also contains an alternative discussion of the class number h_p) is:

> K. Girstmair. A "popular" class number formula. *Amer. Math. Monthly*, Vol. 101, No. 10 (Dec., 1994), pp. 997-1001

The result there, which is the one discussed in this exposition, is a special case of more technical work here:

> K. Girstmair. The digits of $1/p$ in connection with class number factors. *Acta Arith.*, Vol. 67, No. 4 (1994), pp. 381-386.

In a different direction, Murty and Thangadurai have studied the digits of the (decimal or other base) expansion of $1/p$ when the period is not necessarily $p-1$:

> M. Ram Murty and R. Thangadurai. The class number of $\mathbb{Q}(\sqrt{-p})$ and the digits of $1/p$. *Proc. Amer. Math. Soc.*, Vol. 139, No. 4 (2011), pp. 1277-1289.