The Fields Institute for Research in Mathematical Sciences

SIMMER

The University of Toronto
Mathematics Network

May 1997 Presentation Topic
Numbers Ancient and Modern
W. Traves[1]

We present a sampling of interesting questions relating to numbers of various sorts, followed by the answers to these questions and a brief history and description of the concepts involved. We hope you will find this material useful and interesting, both for yourself and your students.

A Sampling of Questions

Prime Numbers

Our concept of *number* has evolved over time from the natural numbers to the integers, and soon thereafter, to the rationals. From there the concepts of real and complex numbers were eventually developed.

Algebra over the integers is already an interesting subject. We call an integer p a *prime* number if its only divisors are ± 1 and $\pm p$. (Exception: the numbers ± 1 themselves are not called prime; they are called *units* instead).

Question 1: Can you show that there are infinitely many prime numbers?

There are many interesting questions about prime numbers. For instance, are there any primes with 100 digits? How many primes like this are there? These questions have become more important in recent years since constructing (and breaking!) many computer security systems depends on being able to factor huge numbers.

The Greeks

The rational numbers were a favourite of the Greeks, whose world view depended heavily on aesthetics and order. It was felt that any geometric quantity occurring could be represented by a rational number.

Question 2: Using a line segment (designated to be of length one), a straight edge and a compass, construct the diagonal of a square of side length one. That is, using these tools (all available to the Greeks!), construct a line segment that is the diagonal of a square of side length one. Can you show that this side length is not a rational multiple of the unit length? Phrased another way, can you show that $\sqrt{2}$ is not a rational number?

[1]Edited for **SIMMER**, with solutions and additional material added, by Philip Spencer.

When this fact was discovered, it caused quite a sensation. Not only was a mathematical idea proven incorrect, but a whole philosophy was discredited.

Orderings

Let's turn our attention to the way that numbers are ordered. Of course, we all know how to count and this puts a natural ordering on the rational numbers: $\frac{1}{2} \leq 1 \leq 2 \leq \frac{5}{2}$. I hope to show you later that ordering numbers is actually a rather difficult and deep problem.

The positive integers have a nice property: there is a smallest positive integer (namely, 1). In fact, even if you throw away the number 1, or even if you throw away a whole collection of numbers (as long as you don't throw them all away!), there will still be among the remaining numbers one which is the smallest. This is called the *well-ordering principle.*

However, the rational numbers with their natural ordering do not satisfy the well-ordering principle.

Question 3: Show that there is no smallest positive rational number. This suggests that the Greek notion of an *atom* (a smallest indivisible amount) might not exist.

It is a surprising result from set theory that every set admits a well-ordering. Therefore, we *can* order the positive rational numbers in such a way that (a) for any two distinct numbers, one is larger than the other; and (b) in any collection of numbers (other than the empty set, of course), there's always a smallest number. However, this ordering is not at all the same as the usual ordering!

Question 4: Try to find an ordering on the positive rational numbers which has these properties.

Real Numbers

One might think that there is a natural ordering on the real numbers: compare them digit by digit. You'd be right, but there is a complication: the digit representation of a real number need not be unique.

Question 5: Show that $0.999\ldots = 1$. We say there are two ways to represent the number 1 in decimal notation. Are there any other ways to represent the number 1 in decimal notation?

This suggests that real numbers are much more complicated than ordinary old rational numbers. It is quite hard to get a hold of a real number: we need to know all of its digits. This really disturbed me when I was first learning mathematics. If this is the case, in what sense do we know that the number $\pi = 3.14\ldots$ exists?

Monkeys

There are lots of interesting questions concerning the size of the integers. Of course, there are infinitely many integers but some odd things can happen.

Question 6: Two monkeys (Abe and Bonzo) come upon a clearing containing two barrels (A and B) and an infinite number of coconuts, conveniently labeled with the positive integers. Abe suggests two ways of filling the barrels. The monkeys can do this very fast, so that we can ask what will happen when ALL the coconuts are in the barrels. Which method should Bonzo agree to?

(A) Abe puts 100 coconuts in barrel A (his barrel) and 1 in barrel B (Bonzo's barrel), 1000 coconuts in barrel A and 2 in barrel B, 10000 in barrel A and 3 in barrel B, *et cetera*.

(B) Abe puts 100 coconuts in barrel B and removes the smallest numbered coconut in barrel B and puts it in barrel A, then puts 100 more coconuts in barrel B and removes the smallest coconut (there are now 199 coconuts in barrel B) from barrel B and puts it in barrel A. He continues in this way.

Intuitively it seems obvious that there are more real numbers than rational numbers and more rational numbers than integers. What do you think about the relative sizes of such infinite collections of numbers? In what sense do we mean that there are more reals than integers? These are interesting questions to ponder.

Candyman's Dilemma

Question 7: John checks his pocket and finds he has less money than the cost of a comic book ($1.05). Instead, he decides to buy candy at the corner store. There are three types of candy: Appletarts (A) at 3 cents each, Butterscotch Kisses (B) at 5 cents each, and Cinamonos (C) at 7 cents each. John says, *if I buy only Appletarts then I will have 2 cents left over, if I buy only Butterscotch Kisses then I will have 4 cents left over and if I buy only Cinamonos then I will have 5 cents left.* How much money does John have in his pocket?

We'll discuss this, and other similar problems, in terms of formulas known to ancient Chinese mathematicians. We'll also explain how modern mathematics studies these problems using *modular arithmetic*.

In the integers modulo 7, there are only seven numbers: 0, 1, 2, 3, 4, 5, and 6. You can divide 3 by 2 in this number system: the quotient is 5, since 2 times 5 equals 3 in arithmetic modulo 7.

Question 8: Try to show that you can *always* divide any number by any non-zero number, in the integers modulo 7. Can this still be done in the integers modulo 12?

Question 9: In the integers modulo 7, compute 2^7, 3^7 and 5^7 (there is a clever way to do this last one). What do you notice? Can you prove your conjecture?

Solutions

Solution to Question 1. Every non-zero integer has a prime factor. For any positive integer n, the number $n!$ is divisible by all the positive integers from 1 to n inclusive, and so the number $1 + n!$ is not divisible by any of them. Therefore, all of the prime factors of $1 + n!$ must be greater than n.

This proves that, for any positive integer n, there are prime numbers which are greater than n. Therefore, there are infinitely many prime numbers.

Solution to Question 2. Let the line segment be PQ. Use the standard ruler-and-compass technique for constructing perpendiculars (found in most textbooks) to draw a perpendicular line L to PQ through Q. With the centre of the compass at Q and its tip at P, draw a circle, passing through L at point R. Now PQ and QR are two adjacent sides of a square of side length 1. Draw the line segment PR; this is the desired diagonal, whose length is $\sqrt{2}$.

This length is not a rational multiple of the original side length. In other words, there is no rational number a/b which equals $\sqrt{2}$. Here are two proofs of this (each proof uses that fact that, if $a/b = \sqrt{2}$, then the equation $a^2 = 2b^2$ would have to be satisfied):

> **Proof #1**: Let k be the number of times 2 occurs as a factor of a, and l the number of times 2 occurs as a factor of b. Then 2 occurs $2k$ times (an even number) as a factor of a^2, but $2l + 1$ times (an odd number) as a factor of of $2b^2$. No number is both even and odd, so the numbers a^2 and $2b^2$ must be different (since 2 appears as a factor a different number of times).
>
> Therefore, no rational number a/b can equal $\sqrt{2}$.
>
> **Proof #2**: Write a/b in lowest terms, in which a and b have no common factors. This means that a and b are not both even.
>
> However, if $a^2 = 2b^2$, then a would have to be even. That means we can write $a = 2k$ for some integer k. The equation now becomes $4k^2 = 2b^2$, so $2k^2 = b^2$, which implies b would have to be even as well, contradicting the fact that a/b is in lowest terms.
>
> Therefore, no rational number a/b can equal $\sqrt{2}$.

Proof #1 is a little more elegant, but it requires that one first prove the theorem that all positive integers can be written uniquely (except for the order) as a product of positive prime numbers.

Solution to Question 3. For any positive rational number r, $r/2$ is a smaller one. Therefore, there is no smallest positive rational number.

Solution to Question 4. There are many ways to do this. One way is to compare positive rational numbers by asking, for each number r,

> What is the largest integer needed to write r in the form a/b where a and b are positive integers?

Answering this question gives a positive integer $N(r)$ for each positive rational number r. For example, $N(1/4) = 4$ since $1/4$ can't be written using anything smaller than a 4, but $N(2/4) = 2$ since $2/4$ can be written as $1/2$ which uses nothing larger than a 2.

Now we can compare positive rational numbers r and s by comparing $N(r)$ to $N(s)$ (and when there is a tie, i.e. when $N(r) = N(s)$, use the usual ordering). For example: $1/2$ comes before $1/4$ in this new ordering (because $N(1/2) = 2 < 4 = N(1/4)$). Also $2/3$ comes before 3 (because $N(2/3) = 3 = N(3/1)$, and since there is a tie, we use the usual ordering, in which $2/3 < 3$).

In this ordering 1 is the smallest positive rational number (every other number must have an integer > 1 in either numerator or denominator).

In fact, any non-empty collection of positive rational numbers has a smallest number in this new ordering. To prove this, look at all the positive integers $N(r)$ that correspond to the numbers r in the collection. Pick the smallest one of these; call it N. There are only finitely many positive rational numbers r for which $N(r) = N$ (for there are only finitely many fractions you can build out of the numbers 1 through N), so there are only finitely many numbers r in the collection for which $N(r) = N$. An ordered, finite set always has a smallest element, so there is a smallest number r for which $N(r) = N$, and this number r will be the smallest in the entire collection.

Solution to Question 5. There are many arguments that can be used to try to convince someone that $0.999\ldots = 1$. One common one is to note that $0.333\ldots = 1/3$, and multiplying both sides by 3 gives you $0.999\ldots = 3/3 = 1$. However, none of these arguments can be considered a mathematical proof until two fundamental questions are answered: (1) What *is* a real number? (2) What does an infinite decimal like $0.999\ldots$ actually *mean*?

We discuss these questions briefly in the **Concepts** section below, concluding that a real number can be defined to be a "Cauchy sequence" of rational numbers, and two such sequences $a_1, a_2, \ldots$ and $b_1, b_2, \ldots$ define the same real number if the distance $|a_n - b_n|$ between corresponding terms converges to zero.

The infinite decimal $0.999\ldots$ means the real number defined by the sequence of finite decimals $0, 0.9, 0.99, 0.999, \ldots$, while $1.000\ldots$ means the sequence $1, 1.0, 1.00, 1.000, \ldots$ (which is the constant sequence $1, 1, 1, \ldots$). These two sequences describe the same real number because the differences between corresponding terms are $1 - 0 = 1, 1 - 0.9 = 0.1, 1 - 0.99 = 0.01, 1 - 0.999 = 0.001, \ldots$ and this sequence is converging to zero.

However, even though the two decimals $1.000\ldots$ and $0.999\ldots$ each represent the same real number 1, there are no other decimals which do. In fact, the *only* time in which two decimals represent the same real number is when, if you write them as a sequence of digits making sure that their decimal points line up, they are of the form

$$\begin{array}{ll} sA000\ldots & \text{and} \\ sB999\ldots & \end{array}$$

where s stands for a sequence of digits that is in common to the two numbers, B is a digit from 0 to 8, and $A = B + 1$ (in our example, s is empty, $A = 1$, and $B = 0$). The decimal point has been omitted from the notation.

Here's a proof that this is the only case in which different decimals give rise to the same number. Write the decimals as above (lining up their decimal points). Skip over any beginning digits that are in common to both (call this digit sequence "s") until you reach the first digit that is different. Let A and B be the differing digits, with $A > B$.

The first infinite decimal describes a sequence whose terms from some point on are finite decimals of the form $sA, sAX, sAXY, \ldots$. If all the digits after A are zeros, these terms are all equal to the rational number x given by the finite decimal sA. Otherwise, at least one subsequent digit C is non-zero, and all the terms from that point on are greater than or equal to the rational number x given by the finite decimal $sA \ldots C$.

The second infinite decimal describes a sequence whose terms from some point on are finite decimals of the form $sB, sBP, sBPQ, \ldots$. If all the subsequent digits are 9's, these terms are $sB9, sB99, \ldots$, all of which are less than the rational number y given by the finite decimal $s(B+1)$. If at least one subsequent digit D is less than 9, then the terms from some point on are of the form $sB \ldots D \ldots$ which are all less than the rational number y given by the finite decimal $sB \ldots (D+1)$.

The difference between corresponding terms is always at least $x - y$, as the term from the first decimal is at least x and the term from the second one is at most y.

If $x > y$, these differences are always greater than the fixed positive number $x - y$ and therefore cannot converge to zero, so the decimals describe different real numbers. The only time they can describe the same real number is when $x = y$. This only happens in the case when x is given by sA (which only happens when the first decimal is of the form $sA000\ldots$) and y is given by $s(B+1)$ (which only happens when the second is of the form $sB999\ldots$), and only when $A = B + 1$.

Solution to Question 6. Obviously, after each step, under option (A) Abe's barrel will have many many more coconuts than Bonzo's, and under option (B) Bonzo's barrel will have many many more coconuts than Abe's. If these monkeys can only do finitely much work, it would clearly be to Bonzo's advantage to choose option (B).

However, things change radically if the monkeys can complete their task (working infinitely fast), assigning each coconut to a final resting place in either barrel A or barrel B:

Under option (A), each barrel will end up with the same number of coconuts, while under option (B), barrel A will get all the coconuts and barrel B will get none. So it's actually better for Bonzo to choose option (A)!

Here's why. Under option (A), it is clear that an infinite number of coconuts get placed into each barrel. It is a (strange at first glance, but nevertheless true) fact that any two infinite sets of positive integers are the same size: they can be placed in one-to-one correspondence with each other. In this particular problem, you can set up the correspondence as follows: match the lowest-numbered coconut in A with the lowest one in B, match the second-lowest one in A with the second-lowest one in B, and so on. Every coconut gets matched in this way.

Under option (B), though, things are different. Once a coconut is placed into barrel A, it is never removed; that is its final resting place. However, whenever a coconut (let's say it's number n) is placed into barrel B, it will eventually be removed and put into barrel A. This is because there are at most $n-1$ smaller-numbered coconuts in B, one of which is removed during each turn, so after at most $n-1$ turns coconut n will become the smallest-numbered coconut in barrel B and will be removed on the next turn. Therefore, when all coconuts are in their final resting place, Abe will have them all!

Solution to Question 7. In the language of congruences, we say that *a is congruent to b modulo m*, written $a \equiv b \pmod{m}$, if $a-b$ is divisible by m.

This problem can be restated as: find a number x (the number of cents John has) which is less than 105 and which satisfies the three congruences

$$\begin{aligned} &x \equiv 2 \pmod{3},\\ &x \equiv 4 \pmod{5}, \text{ and}\\ &x \equiv 5 \pmod{7}. \end{aligned}$$

The first congruence means $x = 3k+2$ for some integer k. Plugging this into the second congruence yields $3k+2 \equiv 4 \pmod{5}$, and therefore

$$3k \equiv 4-2 \equiv 2 \pmod{5}$$

How do we solve this? We cannot simply divide 2 by 3, since $2/3$ is not an integer. However, the theory in question 8 below shows that in arithmetic modulo a prime, one *can* always divide by any non-zero number. So there is some number k for which $3k \equiv 2 \pmod{5}$. That means that if we keep adding 5 to the right-hand side 2 (which doesn't affect the congruence), we will eventually reach a multiple of 3. Let's do it, adding 5 until we get a multiple of 3:

$$3k \equiv 2 \equiv 7 \equiv 12 \pmod{5}$$

and now we can divide by 3 to get $k \equiv 4 \pmod{5}$, so $k = 5l+4$ for some integer l, and therefore $x = 3k+2 = 15l+14$. Plugging this into the final congruence, we obtain that $15l+14 \equiv 5 \pmod{7}$, so $15l \equiv -9 \pmod{7}$.

We could solve this by the same procedure as above, but it is easier to note that $15 \equiv 1 \pmod{7}$ and therefore

$$l \equiv 15l \equiv -9 \equiv 5 \pmod{7}.$$

Finally, we rewrite the last congruence as $l = 7m+5$ for some integer m, and plug this in to the formula $x = 15l+14$ to obtain $x = 105m+89$. We know $0 \leq x < 105$ so m must be zero, and therefore $x = 89$. John has 89 cents in his pocket.

A procedure for solving systems of simultaneous congruences was known to the ancient Chinese, and the theorem that guarantees the existence of a solution (under appropriate conditions on the numbers involved) is known as the *Chinese Remainder Theorem*.

Solution to Question 8. Let a and b be integers modulo 7, with b non-zero. We want to show that there is a unique quotient q for the division "a divided by b". Look at the numbers $b \times 0, b \times 1, \ldots, b \times 6$.

No two of these are equal to each other: if $b \times x = b \times y$ (in arithmetic modulo 7), that means 7 divides the difference $bx - by$ (in ordinary arithmetic). Because 7 is prime, the fact that 7 divides $b(x - y)$ means that either 7 divides b (which it doesn't, since b is a number from 1 to 6), or else 7 divides $x - y$. This means x and y are equal modulo 7. So, in mod 7 arithmetic, the only time $b \times x = b \times y$ is when $x = y$. (The same thing is true in arithmetic modulo any prime number).

Therefore, the seven numbers $b \times 0, b \times 1, \ldots, b \times 6$, being seven different members of the set $\{0, 1, 2, 3, 4, 5, 6\}$ (which only has seven members), must together make up the entire set. That means there is exactly one value of q for which $b \times q = a$, proving that division of a by b is well defined.

This works in arithmetic modulo any prime number, but not in arithmetic modulo non-primes. For instance, in arithmetic modulo 12, 3 times 4 equals 0, so you cannot divide by 3 (if you could, you could divide both sides by 3 to get $4 = 0$, which is not true). However, you can still divide by any non-zero number which is relatively prime to 12.

Solution to Question 9. In the integers modulo 7, $2^7 = 2$, $3^7 = 3$, and $5^7 = 5$. (The last one can be done easily by noting that $5 \equiv -2 \pmod 7$, so $5^7 \equiv (-1)^7 2^7 \equiv -2 \equiv 5$).

It appears that $a^7 \equiv a \pmod 7$ for any a, and this is in fact true.

It's clearly true when $a = 0$, so let's think about nonzero a.

In the integers modulo 7 the sequence $a, a^2, a^3, \ldots$ must eventually repeat itself (there are only seven different numbers available). So there are some two powers which are equal, say a^n and a^m with $n > m$. This means $a^m(a^{n-m} - 1) = 0$ and we can divide by a^m to deduce that $a^{n-m} - 1 = 0$.

We have now shown that some power of a equals 1 (modulo 7). Let m be the smallest such exponent, so that $a^m = 1$ but the m numbers $1, a, a^2, \ldots, a^{m-1}$ are all distinct.

Divide the six numbers $1, 2, 3, 4, 5, 6$ into categories by placing two numbers b and c into the same category if $b = a^k c$ for some k. (This works because the relationship just described is a symmetric and transitive one: if $b = a^k c$ and $c = a^l d$, then $b = a^{k+l} d$, so if b and c are to go together and c and d are to go together, then b and d are to go together as well).

Each category has exactly m members, because if b is in the category, then the other members of the category are $ba, ba^2, \ldots, ba^{m-1}$. Therefore, if n is the number of categories, the product mn equals the total number of numbers we placed into categories: namely, 6.

This proves that m is a factor of 6. We know $a^m = 1$, so $a^{mn} = 1^n = 1$, so $a^6 = 1$, which proves that $a^7 = a$ (in the integers modulo 7). This same thing is true in the integers modulo any prime p: $a^p \equiv a \pmod p$ for all a.

History and Concepts

Numbers

The natural numbers (1, 2, ...; some authors include 0 as well) were probably the first mathematical concepts ever considered. Adequate for counting possessions, they were not adequate for describing transactions (in which the number of objects involved does not completely describe the situation unless there is also knowledge of whether the objects were gained or lost). Therefore, a new concept was considered: the integers $(\ldots, -2, -1, 0, 1, 2, \ldots)$. The collection of integers is usually denoted $\mathbf{Z}$ (or $\mathbb{Z}$ on a blackboard where bold-face is unavailable); this is because 19th century mathematics was dominated by German mathematicians and the integers are called *Zahlen* in German).

The algebraic structure of the integers is very rich and is the subject of *Number Theory.* Questions about the distribution of prime numbers are among the most difficult open problems in mathematics. One amazing result is that, for large numbers N, the number of primes from 1 to N is on the order of $N/\log(N)$; this fact (which can be stated more precisely) is known as the Prime Number Theorem.

The integers are adequate for describing whole quantities but not portions of quantities. For this purpose, a new concept must be defined: that of a *rational number.* A rational number can be defined to be a pair of integers r and s (with s non-zero), representing r pieces, where s pieces make up a whole. We write this pair of numbers using the notation $\frac{r}{s}$, and we consider two pairs $\frac{r}{s}$ and $\frac{m}{n}$ to be the same rational number if $nr - ms = 0$.

(Mathematical sophisticates would say that the rational numbers are *equivalence classes* of pairs (r, s) under the equivalence relation that relates (r, s) to (m, n) if and only if $nr - ms = 0$, and that the equivalence class of the pair (r, s) is denoted r/s).

Rational Numbers and the Greeks

The Greeks really liked the rational numbers. It's not an exaggeration to say that they worshipped them. There was a cult, founded by the geometer Pythagoras, which held that the world was beautiful because its structure and order could be expressed in mathematical terms by ratios of integers. One of the central tenets of the Pythagorean world view was that geometric quantities could always be expressed in terms of rational numbers. The cult went into decline after it was realized that the diagonal length of a square of side length 1 is not a rational number. They tried to keep this knowledge a secret because it was such an embarrassment to their world view.

Since not all lengths are expressible within it, the rational number system, although adequate for counting possessions, recording transactions, and counting portions of things, is inadequate for measuring lengths. A new kind of number must be constructed for that purpose. The square root of 2 is an example of this new kind of number: it measures the length of the diagonal of a square of side length 1, but it is not one of the familiar rational numbers so beloved by the Greeks.

Real Numbers

These new numbers are called *real numbers*. This is a terribly unfortunate nomenclature, partly because it suggests that other number systems don't relate to reality (though in fact they do). It's also unfortunate because it's not entirely clear that these "real numbers" exist at all; only in the past few hundred years have they been defined in a way that demonstrates their existence.

Real numbers need to be able to describe lengths and other continuous quantities, even ones not representable by rational numbers (like the diagonal of a unit square). In short, they need to be able to describe all possible locations on the "number line". How can we construct such numbers out of rational numbers (the only kind that we so far know to exist)?

There are two ways. One is to describe a location on the number line by saying which rational numbers lie below it and which lie above it. A real number can then be defined as a partition of the rationals into two groups, satisfying certain properties (like the fact that everything in group 1 must be less than everything in group 2).

Another way (a little less elegant but more useful for writing down real numbers) is to describe a location on the number line by a sequence of rational numbers which form better and better approximations to it. One can then define a real number to be any such sequence of rational numbers.

Not all sequences converge to a single location on the number line, so we consider only *Cauchy sequences*. These are sequences such that, for any positive number ϵ (no matter how small), there is some place in the sequence such that, from that point on, all terms are within ϵ of each other. This guarantees that the sequence is forming better and better approximations to a single location on the number line.

Two sequences $a_1, a_2, \ldots$ and $b_1, b_2, \ldots$ may define the same location on the number line. This happens if the differences $a_1 - b_1, a_2 - b_2, \ldots$ are converging to zero (meaning that, for any positive number ϵ, all the differences from some point on are smaller than ϵ in absolute value). In this case, we call the sequences "equivalent".

Now we define a real number to be an equivalence class of Cauchy sequences of rational numbers (that is, each Cauchy sequence defines a real number, and two Cauchy sequences define the same real number if and only if they are equivalent). This should remind you of the way rational numbers were defined as pairs of integers, with two pairs (r, s) and (m, n) defining the same rational number if and only if $nr - ms = 0$.

We can write real numbers in decimal notation, for example, $\pi = 3.1415\ldots$. What this means is we are looking at the real number defined by the following sequence of rational numbers: $3, 3.1, 3.14, 3.141, 3.1415, \ldots$ (this is a Cauchy sequence because, for any n, after the nth term all terms agree to n decimal places and hence are within $1/10^n$ of each other). Any decimal expression defines a Cauchy sequence of rational numbers (by truncating at successive decimal places), and hence every decimal expression defines a real number.

Orderings and Sizes

In the questions it was mentioned that every set admits a well-ordering. For the rationals it was not too hard to write one down. But it is just about impossible to write one down for the real numbers! Only through abstract theoretical arguments can one prove that a well-ordering exists. This abstract proof does not provide any nice easy way to actually write one down.

Another interesting property is that there are the same number of rational numbers as there are integers (even though the rational numbers contain all the integers and more besides!), but there are *more* real numbers than there are integers.

The well-ordering constructed in the solution to question 4 provides a way to put the positive rational numbers into 1-1 correspondence with the positive integers (which is what it means to say that there are as many positive rational numbers as positive integers): for every positive rational number r, there are only finitely many other numbers s for which $N(s) \leq N(r)$, so there are only finitely many numbers s which are smaller than r under the new ordering. This means that if you start with the smallest positive rational number, label it "1", label the next smallest "2", and so on, you will eventually reach every postive rational number r. In this way, every positive rational number r gets matched with a positive integer, leaving nothing out.

However, the real numbers can *not* be put into 1-1 correspondence with the integers. There's a famous argument called *Cantor's diagonalization argument* which proves this; we will not go any further into this here.

Modular Arithmetic

Imagine a clock on a world which has seven hours. The clock face is divided into seven equal segments. One can add clock times together to get new clock times: for example, 5 hours after 4 o'clock it is 2 o'clock. Therefore, the addition law defined on this clock face is such that $4 + 5 = 2$.

Note that this is the same sort of thing as a congruence statement on the integers: when "4", "5", and "2" stand for integers instead of clock-face hours, then it is no longer true that $4 + 5 = 2$, but what is true is that $4 + 5 = 9$ and $9 \equiv 2 \pmod 7$.

Rather than work with integers and congruence relations modulo 7, it is often easier to work with a new number system (called a *finite field*) which has only seven numbers: 0, 1, 2, 3, 4, 5, and 6. These can be added or multiplied together, with the result always being in the same number system; for instance, $5 \times 4 = 6$ in this number system.

We have seen in the questions that division is well-defined in this number system, and the cancellation law holds. This is why the procedure used in solving question 7 is guaranteed to work (as long as we are working modulo a prime number).

In arithmetic modulo non-primes, the cancellation law no longer holds. For example, in arithmetic modulo 12, 3×4 is the product of two non-zero numbers which gives you zero. In such number systems, you cannot divide by all non-zero numbers. However, the structure of these number systems is still rich with important theoretical properties.

Other Number Systems

There are plenty of other number systems; we mention just a few.

The definition of real numbers by Cauchy sequences relied on a notion of what the "distance" between two rational numbers r and s is. Normally, this distance is defined to be $d(r, s) = |r - s|$, and it is to this notion of distance we are referring when we say things like "the terms must be within ϵ of each other". However, there are other notions of distance which satisfy all the properties a distance function needs to satisfy. These other notions of distance have a more algebraic flavour and are very important in number theory.

For instance, consider the prime number 3. For each integer n, define the *weight* $W(n)$ of n to be the number of times 3 divides n. For each rational number m/n, define its weight $W(m/n)$ to be $W(m) - W(n)$. Now define the distance between two rational numbers r and s to be $d(r, s) = 3^{-W(r-s)}$.

Notice that two integers are very close together if their difference is divisible by a high power of 3. This is a pretty weird distance function, but it satisfies all the properties a distance function has to satisfy, so we can define the notion of Cauchy sequences of rational numbers with respect to this distance function. This collection of Cauchy sequences forms a number system called the 3-adic numbers, in the same way that the usual Cauchy sequences of rational numbers form the real number system.

In the same way, one can define "p-adic numbers" for any prime p.

Other interesting number systems include the *algebraic numbers*, that is, numbers which can be described as roots of polynomial equations with rational coefficients. An example of an algebraic number is $\sqrt{2}$, a root of the equation $x^2 - 2 = 0$. For a while people wondered whether all real numbers might be algebraic, but the answer is no. In fact, there are many more non-algebraic real numbers than there are algebraic ones: the algebraic numbers can be put into 1-1 correspondence with the integers, but the real numbers cannot. π and e are examples of non-algebraic real numbers.

Finally, there are the complex numbers. These can be defined as pairs of real numbers (a, b), typically written in the notation $a+bi$. With the appropriate definition of addition and multiplication, the pair $0 + 1i$ (usually written just as "i") squares to give -1. The fundamental importance of the complex numbers is given by

> **The Fundamental Theorem of Algebra.** Every polynomial with coefficients in the complex numbers has a root that is a complex number.

This is not true for the real numbers (for example, the equation $x^2 + 1 = 0$ has no real-valued roots), and it is what makes the complex numbers so useful, especially when trying to talk about geometry in algebraic terms.