Last time, we saw how some standard facts (existence of $\sqrt{2}$, density of rationals in reals and so on) followed from the so-called “completeness axiom” for the reals.

The last thing I want to do in this chapter is to revisit decimal expansions.

In chapter 2 I showed you a machine which takes as input a non-negative real $x$ and gives as output an infinite sequence $a_0, a_1, a_2, a_3, \ldots$ of non-negative integers, with $a_0 \geq 0$ (the whole number part) and $0 \leq a_i \leq 9$ for $i \geq 1$ (the decimal digits). We could write $x = a_0.a_1a_2a_3\ldots$.

We also saw that there was no real number that you could put into the system which returned $0.99999999\cdots$. So in particular there were some infinite sequences $a_0, a_1, a_2, \ldots$ with $0 \leq 9 \leq a_i$ for all $i \geq 1$ which never show up as a decimal expansion!

This raises the question as to what $0.999999\cdots$ *means*. Here is a proposal to attach meaning to this idea.

Let $a_0, a_1, a_2, a_3, \ldots$ be an infinite sequence of non-negative integers, with $0 \leq a_i \leq 9$ for all $i \geq 1$.

For any integer $n \geq 0$ let's define a rational number $x_n$ by $x_n = a_0.a_1a_2a_3\ldots a_n$.

Formally, $x_n := \sum_{i=0}^{n} a_i 10^{-i}$, a finite sum (so there is no problem with convergence or anything).
Example: if $a_0 = a_1 = a_2 = a_3 = \cdots = 7$, then we are trying to attach a meaning to $7.7777777777\cdots$, and so far we have defined
$x_0 = 7$, $x_1 = 7.7$, $x_2 = 7.77$, $x_3 = 7.777$ and so on.

Given: an infinite sequence $a_0, a_1, a_2, \ldots$ of naturals with $0 \leq a_i \leq 9$ for all $i \geq 1$.

Define $x_n = \sum_{i=0}^{n} a_i 10^{-i}$.

It's not hard to check that $a_0 = x_0 \leq x_1 \leq x_2 \leq \cdots$. I now claim that for all $n \geq 0$ we have $x_n < a_0 + 1$.

This is because

$$\begin{aligned} x_n &= a_0 + \tfrac{a_1}{10} + \tfrac{a_2}{100} + \cdots + \tfrac{a_n}{10^n} \\ &\leq a_0 + \tfrac{9}{10} + \tfrac{9}{100} + \cdots + \tfrac{9}{10^n} \\ &= a_0 + 1 - \tfrac{1}{10^n} \\ &< a_0 + 1 \end{aligned}$$

Set $S = \{x_0, x_1, x_2, \ldots\}$. What have we just proved about $S$?

We've proved that $\forall s \in S, s < a_0 + 1$. So we've proved that $S$ is bounded above. And it's certainly non-empty, because $x_0 \in S$.

So let's define $D = D(a_0, a_1, a_2, \ldots)$ to be $\sup(S)$ (the least upper bound for $S$). We could say that $D$ is the real number associated to the abstract "decimal expansion" $a_0.a_1a_2a_3\ldots$.

Do you think that the decimal expansion of $D$ is guaranteed to be $a_0.a_1a_2a_3\ldots$?

It *cannot* be the case that the decimal expansion of $D$ is guaranteed to be $a_0.a_1a_2a_3a_4\cdots$! Because we already proved that there was no real number which had a decimal expansion of $0.99999999\cdots$, so the sequence $0, 9, 9, 9, 9, 9, \ldots$ must give rise to a real number $D = D(0, 9, 9, 9, 9, 9, \ldots)$ whose decimal expansion is *not* $0.9999999\cdots$.

So what is the real number which we are associating to $0.999999999\cdots$?

It is the least upper bound of the set $\{0, 0.9, 0.99, 0.999, 0.9999, \ldots\}$.

In other words, it is the least upper bound of the set $\{1-1, 1-\frac{1}{10}, 1-\frac{1}{100}, 1-\frac{1}{1000}, \ldots\}$.

So what is $\sup\{1-\frac{1}{10^n} \mid n \in \mathbb{Z}_{\geq 0}\}$?

*Claim.* $\sup\{1 - \frac{1}{10^n} \mid n \in \mathbb{Z}_{\geq 0}\} = 1$.

*Proof.* Do we all know what we have to do here? What does it mean to be a least upper bound? Set $S = \{1 - \frac{1}{10^n} \mid n \in \mathbb{Z}_{\geq 0}\}$. We need to check that 1 is an upper bound for $S$, and that all upper bounds $b$ of $S$ satisfy $b \geq 1$.

Well certainly $1 - \frac{1}{10^n} < 1$ for all $n \geq 0$, so 1 is certainly an upper bound.

Now assume for a contradiction that there was some upper bound $b = 1 - \epsilon$ for the set $\{1 - \frac{1}{10^n} \mid n \in \mathbb{Z}_{\geq 0}\}$, with $\epsilon > 0$. It's now the usual trick. We can choose some positive integer $N > \frac{1}{\epsilon}$, observe that $N < 10^N$ (simple proof by induction – try it!) and then deduce from $0 < \frac{1}{\epsilon} < N < 10^N$ that $0 < \frac{1}{10^N} < \epsilon$. Hence $x_N = 1 - \frac{1}{10^N} > 1 - \epsilon = b$. But $x_N \in S$, so $b$ wasn't an upper bound for $S$ after all! This a contradiction. Hence all upper bounds $b$ for $S$ satisfy $b \geq 1$.

□

I will leave you with this thought.

Let $x = 0.99999999999\cdots$. Then $10x = 9.999999999\cdots$ so $10x = 9 + x$. Hence $9x = 9$ and so $x = 1$.

Now set $y = 1 + 2 + 4 + 8 + 16 + \cdots$. Then $2y = 2 + 4 + 8 + 16 + \cdots$ so $2y = y - 1$. Hence $y = -1$.

# Chapter 7. Number theory

Disclaimer: I am a number theorist.

Number theory is the best part of maths – it is much better than stupid old analysis, because there are no epsilons or deltas. Just the good old non-negative integers $\{0, 1, 2, 3, \ldots\}$. What's not to like?

Turns out that there are infinitely many non-negative integers. In some sense, the non-negative integers is "the simplest infinite set". Turns out that the simplest infinite set is *really really hard.* Turns out that our intuition about the infinite is often quite wrong. We'll see some great examples of this when we talk about countable and uncountable infinities later on in this course.

*Example* (Fermat's Last Theorem.) If $a, b, c, n \in \mathbb{Z}_{\geq 0}$ and $n \geq 3$ and $a^n + b^n = c^n$ then at least one of $a, b, c$ equals zero.

The 1995 proof by Andrew Wiles and Richard Taylor of this theorem is, when written out in full, several volumes long (thousands of pages of complicated arithmetic algebraic geometry and modular forms and elliptic curves).

*Example* (Goldbach conjecture.) Any even integer $n \geq 4$ can be written as the sum of two prime numbers $n = p + q$.

Raised by Christian Goldbach in 1742, and still an open question today.

Conclusion: Number theory can be really difficult.

However there is a bunch of number theory which is actually quite easy, some of which even goes back 2000 years to Euclid.

Let's take a look at some of the easier stuff.

**Lemma 7.1** (division with remainder.) Say $a \in \mathbb{Z}$ and $b \in \mathbb{Z}_{\geq 1}$ are integers. Then
(i) we can write $a = qb + r$ with $q$ ("quotient") an integer, and $r$ ("remainder") an integer satisfying $0 \leq r < b$.
(ii) $q$ and $r$ are unique with this property. In other words, if $a = qb + r = q'b + r'$ with $q, q' \in \mathbb{Z}$ and $0 \leq r, r' < b$, then $q = q'$ and $r = r'$.

Examples: set $b = 10$. Then $a = 53 = 5 \times 10 + 3$, and $a = 12345 = 1234 \times 10 + 5$, and $a = -73 =(-8) \times 10 + 7$.

**Lemma 7.1** (division with remainder.) Say $a \in \mathbb{Z}$ and $b \in \mathbb{Z}_{\geq 1}$ are integers. Then
(i) we can write $a = qb + r$ with $q$ ("quotient") an integer, and $r$ ("remainder") an integer satisfying $0 \leq r < b$.
(ii) $q$ and $r$ are unique with this property. In other words, if $a = qb + r = q'b + r'$ with $q, q' \in \mathbb{Z}$ and $0 \leq r, r' < b$, then $q = q'$ and $r = r'$.

*Proof.* (i) (existence). We have $b \geq 1$ so $b \neq 0$. Set $x = \frac{a}{b}$, and define $q = \lfloor x \rfloor$. Then $q \leq x < q + 1$. Multiplying up by $b$ we see $bq \leq bx = a < bq + b$. Hence $a = bq + r$, and we must have $0 \leq r < b$. This does existence.

**Lemma 7.1** (division with remainder.) Say $a \in \mathbb{Z}$ and $b \in \mathbb{Z}_{\geq 1}$ are integers. Then
(i) we can write $a = qb + r$ with $q$ ("quotient") an integer, and $r$ ("remainder") an integer satisfying $0 \leq r < b$.
(ii) $q$ and $r$ are unique with this property. In other words, if $a = qb + r = q'b + r'$ with $q, q' \in \mathbb{Z}$ and $0 \leq r, r' < b$, then $q = q'$ and $r = r'$.

*Proof of (ii)* (uniqueness). Say $qb + r = a = q'b + r'$ with $q, q' \in \mathbb{Z}$ and $0 \leq r, r' < b$. Then $b(q - q') = r' - r$. But the left hand side is a multiple of $b$, and hence is either zero or has absolute value at least $b$. And the right hand size is the difference of two elements of $[0, b)$ and hence is in $(-b, b)$, so has absolute value strictly less than $b$. These two sides are equal, and hence must both be zero. Hence $r' - r = 0$ so $r' = r$, and $b(q - q') = 0$ so $q = q'$ (as $b \neq 0$). This does uniqueness.

□

**Definition 7.2.** If $a, b \in \mathbb{Z}$ then we say *a divides b* if there exists some $k \in \mathbb{Z}$ such that $b = ka$. We also say that $a$ is a *divisor* of $b$. Notation: we write $a \mid b$ for "$a$ divides $b$".

[technical note: it's `mid` not `vert` in LaTeX]

Happy with definition of divides?

Try some examples!

(i) Does 3 divide 6? (ii) Does 6 divide 3? (iii) Does 3 divide $-6$? (iv) Does $-3$ divide 6? (v) Does 1 divide 0? (vi) Does 0 divide 1? (vii) Does 0 divide 0? Does every integer have only finitely many divisors? (viii) If $n$ divides $ab$ then must it divide either $a$ or $b$?

Here is a technical lemma which is not hard to prove, and which we'll need later.

**Lemma 7.3.** If $d, x, y \in \mathbb{Z}$ with $d \mid x$ and $d \mid y$, then for all $\lambda, \mu \in \mathbb{Z}$ we also have $d \mid (\lambda x + \mu y)$.

*Proof.* By definition of $d \mid x$ we know there exists $k \in \mathbb{Z}$ such that $x = kd$. By definition of $d \mid y$ we know there exists $\ell \in \mathbb{Z}$ such that $y = \ell d$.

Substituting in, we see $\lambda x + \mu y = \lambda kd + \mu \ell d = (\lambda k + \mu \ell)d$. Hence $d$ divides $\lambda x + \mu y$.

□

**Euclid’s algorithm.**
We’ve seen already that every positive integer is a product of prime numbers. Here is an example. Set $N = 221$. What are the prime factors of $N$? Is $N$ prime?

What about
2519590847565789349402718324004839857 1
4292821262040320277771378360436620207 0
7595556264018525880784406918290641249 5
1508218929855914917618450280848912007 2
8449926873928072877767359714183472702 6
1896375014971824691165077613379859095 7
0009733045974880842840179742910064245 8
6918171951187461215151726546322822168 6
9987549182422433637259085141865462043 5
7679842338718477444792073993423658482 3
8242811981638150106748104516603773060 5
6201619676256133844143603833904414952 6
3443219011465754445417842402092461651 5
7233507787077498171257724679629263863 5
6373289912154831438167899885040445364 0
2352738195137863656439121201039712282 2
120720357? [all one number]

Current human science and technology is unable to break that number up into primes, and this might be the case for a long time in the future. Look up “RSA Factoring Challenge” on Wikipedia (link) to see how pathetic humankind still is at factoring. Even a number with 250 digits is beyond reach. The number on the previous slide is “RSA-2048”, a number with 617 digits, which we could not factor with currently known algorithms before the sun burns out and our planet dies in billions of years’ time, even if we used all the computers in the world.

Here’s a question I’ll talk about next time: if we have two 10000 digit numbers, how are we going to work out their highest common factor?