Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk—Kronecker

We are going to try to take this idea, but instead of starting with the integers, we will begin with the ring $\mathbb{R}[x]$, where $\mathbb{R}$ is a field.

$\mathbb{R}[x]$ is the set of all polynomials with coefficients in $\mathbb{R}$.

It has been known for a long time that $\mathbb{R}[x]$ and $\mathbb{Z}$ have a lot in common.

- they are both rings; i.e., they are endowed with a sum and a product.

$$(x+3)+(x^2+1)=x^2+x+4,$$

$$(x+3)(x+1)=x^2+4x+3.$$

- They both have a division algorithm.

- The Euclidean algorithm applies to both.

- In $\mathbb{Z}$, every number factors uniquely (up to units) into primes; in $\mathbb{R}[x]$ every polynomial factors uniquely (up to units) into irreducible polynomials.

- In $\mathbb{Z}$, when we mod out by a prime we obtain a finite field; in $\mathbb{R}[x]$, when we mod out by an irreducible polynomial we get a field that is a finite-dimensional $\mathbb{R}$-vector space.

The similarities are so strong that often theorems for one ring are later shown to have analogues in the other ring.

Example: Fermat's Last Theorem.

THEOREM: Let n be an integer > 2. Then the equation $a(x)^n + b(x)^n = c(x)^n$ has no non-constant solutions in $\mathbb{R}[x]$.

This is much easier to prove that the real Fermat's Last Theorem, and it was proved before the real Fermat's Last Theorem. This shows a general principal: generally analogues are easier to prove for polynomial rings than for the integers. This doesn't always hold, but it appears to hold most of the time.

Let's develop the analogy between $\mathbb{Z}$ and $\mathbb{R}[x]$. If we think about what was first developed after the integers, it was the rational numbers.

$$(3, 7) \to 3/7$$

We can do the same thing with $\mathbb{R}[x]$—take ratios of two polynomials—as long as the denominator is nonzero.

$$(x + 1, x^2 + 3) \to (x + 1)/(x^2 + 3).$$

The set of all such fractions is called *the ring of rational functions* and is denoted by

$$\mathbb{R}(x).$$

Just as the rational numbers form a field, the ring of rational functions form a field.

What was developed next?

I'll have to draw a picture, but the next things that were discovered were algebraic numbers.

The algebraic numbers are roots of nonzero polynomials with integer coefficients. We denote the set of algebraic numbers by

$$\overline{Q}$$

E.g., $\sqrt{3}$ is a root of $x^2 - 3$; $\rho = (\sqrt{5} + 1)/2$ is a root of $x^2 - x - 1$. These are both irrational algebraic numbers.

Can we mimic this construction? Yes!

Consider all functions that are roots of nonzero polynomials (in, let's say, the variable t) with coefficients in $\mathbb{R}[x]$. These are called the *algebraic functions* and are denoted by

$$\overline{\mathbb{R}(x)}.$$

E.g.,

$$\sqrt{x^2+5}$$

is a root of

$$t^2-(x^2+5)=0;$$

$$(x^5+1)^{2/3}+1$$

is a root of

$$(t-1)^3-(x^5+1)^2=0.$$

So far, we haven't even been able to construct π. After all, it has been proved that π is not an algebraic number. Numbers that are not a root of a nonzero polynomial with integer coefficients are called *transcendental numbers*. Cantor showed that nearly all real numbers are transcendental.

How do we construct real numbers?

We do this by taking limits of rational numbers.

E.g.,

$$\pi$$

is the limit of the sequence

$$3, 3.1, 3.14, 3.141, 3.1415, \ldots.$$

How can we mimic this?

Let's first look at things things that are limits of polynomials.

E.g.,

$$f(x) = 3 + x + 4x^2 + x^3 + 5x^4 + 9x^6 \ldots$$

is the limit of the polynomials

$$3, 3 + x, 3 + x + 4x^2, 3 + x + 4x^2 + x^3,$$

$$3 + x + 4x^2 + x^3 + 5x^4, \ldots.$$

The correct analogue of real numbers appears to be very close to power series. Power series are like polynomials, but we can have terms of arbitrarily large degree. This isn't quite the correct analogue, however.

The reason this isn't quite right is that rational functions like $1/x$ can never be approximated in this way. Besides, when we construct the real numbers we allow rational approximations.

To correct this, we allow negative powers of x.

We define

$$\mathbb{R}[[x, x^{-1}; \sigma]]$$

to be the set of all elements of the form

$$\sum_{j=-M}^{\infty} c_j x^j$$

where M is a nonnegative integer and the c_j are in $\mathbb{R}$.

We call these "almost" power series the *Laurent power series*. This is the correct analogue of $\mathbb{R}$.

So to recap, we have the following correspondences:

$$\mathbb{Z} \to \mathbb{R}[x]$$

$$\mathbb{Q} \to \mathbb{R}(x)$$

$$\overline{\mathbb{Q}} \to \overline{\mathbb{R}(x)}$$

$$\mathbb{R} \to \mathbb{R}[[x, x^{-1}]].$$

In fact, we could continue and find the analogue of the complex numbers. As it turns out, the correct analogue is the algebraic closure of the Laurent power series; it is obtained by adjoining all roots of x (at least for base fields of characteristic 0).

Since we have such a nice correspondence, it is natural to ask if we can find a nice correspondence between elements of $\mathbb{R}$ and the elements of $\mathbb{R}[[x, x^{-1}]]$. The answer is 'no' in general, but for many nice numbers there is a nice corresponding power series.

First, what is the correct analogue of a natural number n in $\mathbb{R}[x]$?

Most combinatorialists agree that the "correct" analogue of a number n is the polynomial

$$[n]_x := (x^n - 1)/(x-1) = 1 + x + x^2 + \cdots + x^{n-1}.$$

Notice that when we substitute $x = 1$ into the expression for $[n]_x$ we obtain n.

From this we can make many nice functions:

$$[n]_x! := [n]_x[n-1]_x \cdots [1]_x.$$

Just as before, when we set $x = 1$ we obtain $n!$. (Note that $[n]_x! \neq [n!]_x$.)

We can also make analogues of binomial coefficients.

$$\binom{n}{j}_x := [n]_x!/[j]_x![n-j]_x!.$$

Again, setting $x = 1$ gives us back the ordinary binomial coefficient.

Cauchy's binomial theorem

$$(1+cx)(1+cx^2)\cdots(1+cx^n) = \sum_{j=0}^{n} \binom{n}{j}_x c^j x^{j(j+1)/2}.$$

Notice that this is a generalization of the ordinary binomial theorem. If we set $x = 1$ in both sides, the LHS becomes $(1+c)^n$ and the RHS becomes

$$\sum_{j=0}^{n} \binom{n}{j} c^j.$$

This is one instance where an analogue of a theorem about the integers has an analogue in the ring of polynomials and it is harder to prove the polynomial analogue.

Notice that we now have an element-wise map that sends a natural number to a polynomial. But can we find analogues of other real numbers?

Yes!

In fact, there is an analogue of π, which we'll denote by $[\pi]_x$.

How do we construct $[\pi]_x$?

Let's begin with Euler's factorization of the sine function.

$$\sin(x) = x - x^3/3! + x^5/5! - x^7/7! + x^9/9! - \cdots.$$

This is the Taylor series (power series) expansion of $\sin(x)$.

Euler knew that this function had zeros at $x = 0, \pm\pi, \pm 2\pi, \pm 3\pi, \ldots$.

Euler also knew that if you know all the roots of a polynomial and their multiplicities, you can reconstruct the polynomial (up to a constant). E.g., $1-2x-x^2+2x^3$ has roots $0, 1/2, 1, -1$. We can then reconstruct it from these roots as follows

$$x-2x^2-x^3+2x^4 = x(1-x/(1/2))(1-x/1)(1-x/(-1))$$

$$= x(1-2x)(1-x)(1+x).$$

Euler figured one should be able to do the same thing with power series, which are, after all, "non-terminating" polynomials.

Euler's factorization:

roots:

$$0, \pm\pi, \pm 2\pi, \pm 3\pi, \ldots.$$

Factorization:

$$\sin(x) =$$

$$x(1-x/\pi)(1-x/(-\pi))(1-x/2\pi)(1-x/(-2\pi))\cdots$$

$$= x(1 - x^2/\pi^2)(1 - x^2/4\pi^2)(1 - x^2/9\pi^2)\cdots.$$

Let's set $x = \pi/2$. Then $\sin(\pi/2) = 1$ and the RHS becomes

$$\pi/2 \cdot (1 - 1/4)(1 - 1/16)(1 - 1/36) \cdots.$$

In other words

$$2/\pi = \frac{3}{4} \cdot \frac{15}{16} \cdot \frac{35}{36} \cdots.$$

This means

$$\pi = 2 \cdot \frac{2 \times 2}{1 \times 3} \cdot \frac{4 \times 4}{3 \times 5} \cdot \cdots.$$

This is Wallis's formula.

This gives us a way of giving an analogue of π.

$$[\pi]_x = [2]_x \cdot \frac{[2]_x \times [2]_x}{[1]_x \times [3]_x} \cdot \frac{[4]_x \times [4]_x}{[3]_x \times [5]_x} \cdot \cdots .$$

Now we use the fact that

$$[n]_x = 1 + x + \cdots + x^{n-1} = (x^n - 1)/(x - 1)$$

to obtain

$$[\pi]_x := (1 - x^2) \prod_{j=1}^{\infty} \frac{(1 - x^{2j})^2}{(1 - x^{2j-1})^2}.$$

If we take the Taylor series of

$$[\pi]_x$$

about $x = 0$, we find that

$$[\pi]_x = 1+2x+x^4-2x^5+x^6+2x^7-3x^8+2x^{10}+\cdots.$$

It has integer coefficients.

Just as one can ask questions whether or not π is rational, algebraic, or has a normal expansion (more on that later), we can ask similar questions about $[\pi]_x$.

Transcendence

The transcendence of π was proved by Lindemann. One can ask the same question for $[\pi]_x$. Is it the root of a nonzero polynomial with polynomial coefficients?

As it turns out, $[\pi]_x$ is also transcendental.

To explain how this is done, we give a theorem of Fatou.

THEOREM: (FATOU) Let

$$F(x) = a_0 + a_1 x + a_2 x^2 + \cdots$$

be a power series with integer coefficients and suppose that $F(x)$ has radius of convergence 1. Then either $F(x)$ is transcendental, or there exist natural numbers n and d such that

$$F(x)(1 - x^n)^d$$

is a polynomial.

Notice that

$$[\pi]_x := (1-x^2)\prod_{j=1}^{\infty}\frac{(1-x^{2j})^2}{(1-x^{2j-1})^2}$$

has integer coefficients and it has radius of convergence 1. It is easy to check that we cannot "cancel" the denominator with $(1-x^n)^d$ and so by Fatou's theorem $[\pi]_x$ is transcendental.

In fact, it is not so difficult to prove Fatou's theorem and so we see that—in accordance with our principal—it is easier to prove transcendence of $[\pi]_x$ than the transcendence of π.

NORMALITY

We recall the basic facts about normality.

A real number c is said to be normal in base b if the probability of finding some digit string among the digits of c is the same as if we were to search among some random sequence of digits.

E.g.,

$$.0101010101\cdots$$

is not normal in base 2. Although the probability that a given digit is 0 is 1/2 and the probability that it is 1 is 1/2, not all strings have the expected probability. For example, the probability that a string of two consecutive digits is 00 is 0 when it should be 1/4.

E.g., The Champernowne number

$$0.12345678910111213141516\cdots$$

is a normal number in base 10. (Is it normal in base 3? No idea.)

It is conjectured that numbers like $e, \pi, \log 2, \sqrt{3}$ are normal in every base $b \geq 2$.

Do we have an analogue of the normality property for power series?

Yes!

Let b be a natural number ≥ 2 and let

$$a_0 + a_1 x + a_2 x^2 + \cdots$$

be a power series with integer coefficients. Then we can reduce the coefficients mod b. E.g., if $b = 3$,

$$11 + 3x + 14x^2 + 9x^3 + 7x^4 + \cdots$$

is equal to

$$2 + 0x + 2x^2 + 0x^3 + x^4 + \cdots$$

mod 3.

When we reduce mod b, all our coefficients are now in $\{0, 1, \ldots, b-1\}$.

We can ask if the probability that a string of d consecutive coefficients is equal to a given string is what one would expect in a random power series ($1/b^d$).

With normality, it appears that we at last see a major difference between real numbers and Laurent power series.

THEOREM: Let $F(x)$ be an integer power series and suppose that $F(x)$ is algebraic. Then $F(x)$ mod b is NEVER normal.

The well-known constants such as π, e, $\sqrt{5}$, log 2 and 7 are called *periods* (Zagier and Kontsevich). Irrational periods are conjectured to have normal expansions in every base $b \geq 2$. On the other hand, power series analogues of periods (for example, $[\pi]_x$, are conjectured to have non-normal expansions mod b for every base $b \geq 2$.

What do you think?

It can be easily shown that $[\pi]_x$ mod 2 is not normal.

Recall that

$$1 + 2x + x^4 - 2x^5 + x^6 + 2x^7 - 3x^8 + 2x^{10} + \cdots.$$

Mod 2 this becomes

$$1 + x^4 + x^6 + x^8 + x^12 + \cdots.$$

Notice that the only exponents with nonzero coefficients are the even powers. This can be shown easily using the expression for $[\pi]_x$ and the fact that $P(x^2) = P(x)^2$ mod 2 for every polynomial $P(x)$.

I am not sure about $[\pi]_x$ mod other bases, but presumably a similar phenomenon occurs.

More generally, one can talk about the *complexity* of a power series with coefficients in $\{0, 1, \ldots, b-1\}$. Given an integer n, we let $f(n)$ denote the number of strings of length n which occur as a string of consecutive coefficients in the power series.

E.g., If we look at $[\pi]_x$ mod 2, we see that 10, 00, 01 occur, but 11 does not occur as a string of consecutive coefficients. Thus $f(2) = 3$. A normal number base b must have $f(n) = b^n$.

Question: Let $f_b(n)$ denote the complexity function associated to $[\pi]_x$ mod b. Is it true that there is some n such that $f_b(n) < b^n$?