Analogies Between Numbers and Functions

William Cherry
University of North Texas

Hanoi, July 2010

Integers

- The integers $\mathbf{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ form one of the most basic objects one can consider in mathematics.
- Yet, many basic questions about $\mathbf{Z}$ remain unanswered, or have very complicated answers.
  - **Fermat's Last Theorem.** For $n \geq 3$ find all integer solutions to the equation $x^n + y^n = z^n$. **Answer:** All solutions also satisfy $xyz = 0$.
  - Given an integer a, decide whether a is prime or not. If not, what are its prime factors?
    - Is 12123212343212345432123456543212345676543212345678765432 1 prime? If not, what are its prime factors?
    - The elementary school procedures for answering these questions are not practical for large numbers, but both questions (prime or not and what are the factors) are answered together.
    - Modern mathematical techniques make it rather "easy" for a computer to determine whether an integer is prime or not.
    - It is still quite hard to find the factors of a very large number (although it is not proven that it must be hard), and modern computer security algorithms are based on the assumption that is difficult to factor large numbers.

Integers

- The integers $\mathbf{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ form one of the most basic objects one can consider in mathematics.
- Yet, many basic questions about $\mathbf{Z}$ remain unanswered, or have very complicated answers.
  - **Fermat's Last Theorem.** For $n \geq 3$ find all integer solutions to the equation $x^n + y^n = z^n$. **Answer:** All solutions also satisfy $xyz = 0$.
  - Given an integer a, decide whether a is prime or not. If not, what are its prime factors?
  - If p is a prime number, on average how many numbers do you have to go foward before reaching the next prime?
    - For example, 509 is prime. How many numbers forward should we expect to have to go to be sure we will find another prime?
  - Are there infinitely many primes p such that p and $p + 2$ are both prime?
    - Such primes are called "twin primes." Here are some examples: 3 and 5, 5 and 7, 11 and 13, 17 and 19, 521 and 523.
  - Which integers can be written as the sum of two primes?
    Goldbach Conjecture: All even integers > 2 can be written as a sum of two primes.

Rings

- An aspect of mathematics that can be surprising to new students is that sometimes considering a more general situation can make a problem easier, and even when it does not, it can provide additional insight into the problem.
- The integers $\mathbf{Z}$ are an example of what we call a commutative ring. A **ring** is a set R with two operations, addition $(+)$ and multiplication $(\cdot)$.
  - Part of the definition of a ring is that the set R with the operation $(+)$ forms an Abelian group, which in particular means that for any r in R, the element $-r$ is also in R.
  - One requires the addition operation $(+)$ to be commutative, but the multiplication may not be. For example, the set of $n \times n$ matrices form a ring, but the multiplication is not commutative.
  - One calls a ring "commutative" when the multiplication is also commutative.
- Another example of a ring is the set of one-variable polynomials with complex coefficients, which we denote as $\mathbf{C}[t]$.

Similarities Between Integers and Polynomials

- It turns out the polynomial ring $\mathbf{C}[t]$ shares many properties with the ring of integers $\mathbf{Z}$.
  - For example, the Euclidean division algorithm applies to both $\mathbf{Z}$ and $\mathbf{C}[t]$.

$$\begin{array}{r|l} 6359 & 17 \\ \hline 51 & 374 \\ \hline 125 & \\ 119 & \\ \hline 69 & \\ 68 & \\ \hline 1 & \end{array} \qquad \begin{array}{r|l} 2t^3 - 7t^2 + 14t - 1 & t - 5 \\ \hline 2t^3 - 10t^2 & 2t^2 + 3t + 29 \\ \hline 3t^2 + 14t & \\ 3t^2 - 15t & \\ \hline 29t - 1 & \\ 29t - 145 & \\ \hline 144 & \end{array}$$

  - In $\mathbf{Z}$ we know to stop because $1 < 17$. In $\mathbf{C}[t]$ we know to stop because 144 has degree 0, which is smaller than the degree of $t - 5$.
  - The fact that we have a way to measure "size" in both $\mathbf{Z}$ and $\mathbf{C}[t]$ is an important similarity.

A Consequence of the Division Algorithm

- A subset I of a commutative ring R is called an **ideal** if
  - $a, b \in I \quad \Rightarrow \quad a + b \in I$
  - $a \in I$ and $r \in R \quad \Rightarrow \quad ra \in I$.
- **Examples**
  - The "even" numbers $I = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$ is an ideal in $\mathbf{Z}$.
  - The set of polynomials $I = \{f(t) \in \mathbf{C}[t] : f(0) = 0\}$ is an ideal in $\mathbf{C}[t]$.
- An ideal is said to be **principal** if
  - $\exists a \in I$ such that $\forall b \in I, \exists r \in R$ such that $b = ra$.
  - Such an a is called a **generator** of the ideal I.
  - The ideal of even numbers in $\mathbf{Z}$ is generated by 2.
  - The ideal of polynomials in $\mathbf{C}[t]$ vanishing at the origin is generated by the polynomial t.
- A commutative ring R (without zero divisors) is called a **principal ideal domain** if every ideal in R is principal.
- $\mathbf{Z}$ and $\mathbf{C}[t]$ are principal ideal domains.
  - Let I be an ideal in $\mathbf{Z}$ or $\mathbf{C}[t]$ and let a be a smallest element in $I \setminus \{0\}$
  - Let b be an element of I. Divide b by a to get $b = qa + r$, with r "smaller than" a. Since a is smallest, $r = 0$. Hence, $b = qa$, and so a generates I.

The Stothers/Mason Theorem for Polynomials

Definition

Given a polynomial $P(t) = (t - a_1)^{m_1} \cdots (t - a_n)^{m_n}$ *factored as a product of powers of distinct irreducible factors, define the* **square free part** $S(P)$ *(also often called the "radical" of* P*) by*

$$S(P)(t) = (t - a_1) \cdots (t - a_n).$$

Example

If $P(t) = t^2(t-1)^3(t+1)$*, then* $S(P)(t) = t(t-1)(t+1)$.

Theorem (Stothers/Mason)

Let $f(t)$*,* $g(t)$*, and* $h(t)$ *be relatively prime polynomials in* $\mathbf{C}[t]$ *such that* $f + g = h$*. Then, either all of* f*,* g*, and* h *are constant, or*

$$\max\{\deg f, \deg g, \deg h\} \leq \deg S(fgh) - 1.$$

The Stothers/Mason Theorem for Polynomials

Theorem (Stothers/Mason)

Let $f(t)$, $g(t)$, and $h(t)$ be relatively prime polynomials in $\mathbf{C}[t]$ such that $f + g = h$. Then, either all of f, g, and h are constant, or

$$\max\{\deg f, \deg g, \deg h\} \leq \deg S(fgh) - 1.$$

Examples

- $t + (1 - t) = 1$
  - $\max\{\deg t, \deg(1 - t), \deg 1\} = 1$
  - $S = t(1 - t)$ so $\deg S = 2$.
- $t^3 + (1 - t)^3 = 3t^2 - 3t + 1$
  - $\max\{\deg t^3, \deg(1 - t)^3, \deg(3t^2 - 3t + 1)\} = 3$
  - $S = t(1 - t)(3t^2 - 3t + 1)$ so $\deg S = 4$.

The Stothers/Mason Theorem for Polynomials

Theorem (Stothers/Mason)

Let $f(t)$, $g(t)$, and $h(t)$ be relatively prime polynomials in $\mathbf{C}[t]$ such that $f + g = h$. Then, either all of f, g, and h are constant, or

$$\max\{\deg f, \deg g, \deg h\} \leq \deg S(fgh) - 1.$$

Corollary

It is impossible to find distinct complex numbers a, b, and c, and non-zero complex numbers A, B, and C such that

$$A(t-a)^k + B(t-b)^m = C(t-c)^n,$$

unless $\max\{k, m, n\} \leq 2$.

Fermat's Theorem for Polynomials

Corollary (Fermat for Polynomails)

If f, g and h are relatively prime polynomails in $\mathbf{C}[t]$ and $n \geq 3$ such that

$$f^n + g^n = h^n,$$

then f, g, and h are all constant.

Proof.

- $S(f^n g^n h^n) = S(fgh)$ so $\deg S \leq 3 \max\{\deg f, \deg g, \deg h\}$.
- $\max\{\deg f^n, \deg g^n, \deg h^n\} = n \max\{\deg f, \deg g, \deg h\}$.
- By Stothers/Mason,

$$\begin{aligned} n \max\{\deg f, \deg g, \deg h\} &= \max\{\deg f^n, \deg g^n, \deg h^n\} \\ &\leq \deg S - 1 \leq 3 \max\{\deg f, \deg g, \deg h\} - 1, \end{aligned}$$

so $n < 3$. □

Fermat's Theorem for Polynomials

Corollary (Fermat for Polynomails)

If f, g and h are relatively prime polynomails in $\mathbf{C}[t]$ and $n \geq 3$ such that

$$f^n + g^n = h^n,$$

then f, g, and h are all constant.

Remark

$n \geq 3$ above is best possible. Notice that

$$(t^2 - 1)^2 + (2t)^2 = (t^2 + 1)^2.$$

Do you see a connection here to Pythagorean triples? (You should!)

Proof of Sothers/Mason

Proof.

- Let
$$W = \begin{vmatrix} f & g \\ f' & g' \end{vmatrix} = \begin{vmatrix} g & h \\ g' & h' \end{vmatrix} = - \begin{vmatrix} f & h \\ f' & h' \end{vmatrix}.$$
- Without loss of generality, assume $\deg f \geq \deg g \geq \deg h$.
- Observe $\deg W \leq \deg g + \deg h - 1$.
- Observe also that if $(t - a)$ divides fgh with multiplicity m, then $(t - a)^{m-1}$ divides W.
- Let G be the GCD of W and fgh.

$$\deg S(fgh) \geq \deg(fgh) - \deg G \geq \deg(fgh) - \deg W \geq \deg f + 1$$

□

ABC-Conjecture for Integers

Definition

Given an integer $a = \pm p_1^{m_1} \cdots p_n^{m_n}$ *factored as a product of powers of distinct primes, define the* **square free part** $S(a)$ *(also often called the "radical" of* a*) by*

$$S(a) = p_1 \cdots p_n$$

Example

If $a = 360 = 2^3 \cdot 3^2 \cdot 5$*, then* $S(a) = 2 \cdot 3 \cdot 5 = 30$.

Question

If a*,* b *and* c *are relatively prime integers such that* $a + b = c$*, then must*

$$\max\{|a|, |b|, |c|\} \leq CS(abc)$$

for some constant C*?*

Why not $S(abc) - 1$? and why the constant C?

- When we measure the "size" of an integer a, we use $|a|$.
- When we measure the "size" of a polynomial f, we use $\deg f$.
- Note that for $a, b \in \mathbf{Z}$, we have $|ab| = |a||b|$.
- Whereas for $f, g \in \mathbf{C}[t]$, we have $\deg(fg) = \deg f + \deg g$.
- Thus, we should think of $\deg f$ as like $\log |a|$, since $\log |ab| = \log |a| + \log |b|$.
- If we translate

$$\max\{\deg f, \deg g, \deg h\} \leq \deg S - 1,$$

we get

$$\max\{\log |a|, \log |b|, \log |c|\} \leq \log |S| - 1.$$

Exponentiating tells us

$$\max\{|a|, |b|, |c|\} \leq e^{\log |S| - 1} = \frac{|S|}{e}.$$

- But nothing told us we should use "natural" logarithm. We have $\log_\gamma |ab| = \log_\gamma |a| \log_\gamma |b|$ for any base γ, so we pose the question replacing e^{-1} by some constant C.

Exercise

$$2^{n+1} \mid (3^{2^n} - 1)$$

Solution.

- Proof by induction.
- When $n = 0$, clearly 2 divides $3 - 1$.
-

$$\begin{aligned} 3^{2^{n+1}} - 1 &= 3^{2 \cdot 2^n} - 1 \\ &= \left(3^{2^n}\right)^2 - 1 \\ &= \underbrace{(3^{2^n} - 1)}_{\text{divisible by } 2^{n+1}} \underbrace{(3^{2^n} + 1)}_{\text{even}} \end{aligned}$$

□

ABC-Conjecture for Integers

Question

If a, b and c are relatively prime integers such that $a + b = c$, then must

$$\max\{|a|, |b|, |c|\} \leq CS(abc)$$

for some constant C?

The answer is NO! (these examples due to Jastrzebowski and Spielman)

- $\underbrace{1}_{a} + \underbrace{(3^{2^n} - 1)}_{b} = \underbrace{3^{2^n}}_{c}$
- $\max\{|a|, |b|, |c|\} = 3^{2^n}$
- Since $3^{2^n} - 1 = 2^{n+1}u$ for some integer u, $S(abc) \leq 1 \cdot 3 \cdot 2u$
- There is no constant C such that $3^{2^n} \leq C \cdot 3 \cdot 2u = C \cdot 6 \cdot \dfrac{3^{2^n} - 1}{2^{n+1}}$

ABC-Conjecture for Integers

Although I have been trying to convince you that considering an analogy between numbers and polynomial functions can be a worthwhile and productive activity, we have just seen that the integers $\mathbf{Z}$ is, in a sense, a more subtle ring than $\mathbf{C}[t]$. Still, one can suspect things aren't too far off, and there is a well-known conjecture that is more or less analogous to the Stothers/Mason theorem.

Conjecture (Masser and Oesterlé's *ABC*-Conjecture)

Give $\varepsilon > 0$, there exists a constant $C(\varepsilon)$, depending only on ε, such that for any triple of relatively prime integers $a + b = c$, we have

$$\max\{|a|, |b|, |c|\} \leq C(\varepsilon) S(abc)^{1+\varepsilon}.$$

Fermat's Last Theorem

In the polynomial case, we saw that the Stothers/Mason theorem implies the polynomial version of Fermat's last theorem. The ABC-Conjecture does not seem to quite imply Fermat's Last Theorem for Integers, but it almost does.

Proposition (Asymptotic Fermat)

If the ABC-Conjecture is true, then there exists a natural number n_0 such that for all $n \geq n_0$, the only integer solutions to the equation $x^n + y^n = z^n$ are such that $xyz = 0$.

Proof.

- It is sufficient to prove there is no relatively prime solution.
- Suppose x, y, and z are relatively prime with $x^n + y^n = z^n$.
- Apply the ABC-Conjecture with $a = x^n$, $b = y^n$, and $c = z^n$.
- $\max\{|x|^n, |y|^n, |z|^n\} \leq C(\varepsilon)|xyz|^{1+\varepsilon}$
- Hence, $|xyz|^n = |x|^n \cdot |y|^n \cdot |z|^n \leq C(\varepsilon)^3 |xyz|^{3(1+\varepsilon)}$.
- This is impossible as soon as n is big enough that $2^{n-3(1+\varepsilon)} \geq C(\varepsilon)$. □

Absolute Values

- We saw that an important part of creating an analogy between integers and polynomials was that we had a way to measure the "size" of both integers and polynomials.
- We measured the size of an integer by its absolute value, but it turns out there is more than one type of absolute value on $\mathbf{Z}$.

Definition

An absolute value on $\mathbf{Z}$ *is a function, which we write* $|\ |$ *from* $\mathbf{Z}$ *to* $\mathbf{R}$ *such that*

AV 1. $|a| \geq 0 \forall a \in \mathbf{Z}$ *and* $|a| = 0 \quad \Leftrightarrow \quad a = 0.$

AV 2. $|ab| = |a||b|.$

AV 3. $|a + b| \leq |a| + |b|$

p-Adic Absolute Values

- Let p be a prime number.
- Let a be a non-zero integer.
- Write $a = p^n u$, where p and u are relatively prime.
- Define $|a|_p = p^{-n} \leq 1$.
- Now, suppose $a = p^n u$ and $b = p^m v$ with p and uv relatively prime.
- Clearly, $|ab|_p = p^{-(n+m)} = |a|_p |b|_p$.
- What about $|a + b|_p$?
- Suppose $n \geq m$. Then, $a + b = p^n u + p^m v = p^m (p^{n-m} u + v)$.
- Then,

$$\begin{aligned} |a + b|_p = |p^m (p^{n-m} u + v)|_p &= |p^m|_p |p^{n-m} u + v|_p \\ &\leq |p^m|_p \cdot 1 = p^{-m} \leq p^{-m} + p^{-n} = |a|_p + |b|_p. \end{aligned}$$

- Notice that $I = \{a \in \mathbf{Z} : |a|_p < 1\}$ is precisely the ideal of multiples of p, *i.e.,* the ideal generated by p.

Absolute Values on $\mathbf{Z}$

Theorem (Ostrowski)

If $|\ |'$ is an absolute value on $\mathbf{Z}$, then either

(i) $|\ |' = |\ |_0$, *where* $|\ |_0$ *is defined by* $|a|_0 = \begin{cases} 0 & \text{if } a = 0 \\ 1 & \text{if } a \neq 0. \end{cases}$

(ii) $|\ |' = |\ |^\lambda$ *for some* $0 < \lambda \leq 1$, *where here* $|\ |$ *denotes the "usual" absolute value on* $\mathbf{Z}$.

(iii) $|\ |' = |\ |_p^\lambda$ *for some* $\lambda > 0$.

Remark

Coming up with a proof by yourself or together with your classmates of Ostrowski's Theorem is a challenging, but not extraordinarily difficult, exercise. Try it with your friends during the remainder of the summer school, and don't try to look it up in a book or on the internet first!

Remark

- *The absolute value* $|\ |_0$ *is called the* **trivial** *absolute value.*
- *The usual absolute value* $|\ |^\lambda$ *is called* **Archimedean** *because for any* $|a| > 0$ *and* $M > 0$, *there exists a natural number* n *such that* $|na| > M$.
  A story (which may not be true): **Archimedes:** *No matter how big your bath tub and no matter how small your spoon, you can eventually fill your bathtub by adding water a spoonful at a time.*
- *The p-adic absolute values* $|\ |_p$ *satisfy the property that* $|a+b|_p \leq \max\{|a|_p, |b|_p\}$, *so adding can never make things bigger. In particluar* $|na|_p \leq |a|_p$ *for all natural numbers* n. *These absolute values are called* **non-Archimedean**.

Product Formula

Proposition (Product Formula)

If a is an integer then, $|a| \cdot \prod_{\text{primes } p} |a|_p = 1$.

Example

- $|12| = 12$, $|12|_2 = 1/4$, $|12|_3 = 1/3$, and $|12|_p = 1$ if $p > 3$.

Proof.

- Let a be an integer.
- Factor a into a product of prime powers: $a = \pm p_1^{m_1} \cdots p_n^{m_n}$.
- $|a|_{p_j} = p^{-m_j}$
- $|a|_p = 1$ if $p \notin \{p_1, \ldots, p_n\}$.

□

Complex Analysis

I began this lecture by explaining a connection between integers and polynomial functions. Polynomial functions are not the only kinds of functions that can help us understand the integers.

Definition

If z is a complex variable and $f(z)$ is a complex function defined for all z in the complex plane $\mathbf{C}$ such that

$$f'(z) = \lim_{h \to 0} \frac{f(z+h) - f(z)}{h}$$

exists for all $z \in \mathbf{C}$, then we call f entire. Note that here h is also a complex variable.

The set of all entire functions forms a ring. Recently, many things have been learned about number theory by studying entire functions as well as polynomials.

Jensen Formula

Proposition (Mean Value Property)

If $f(z)$ is an entire function and does not have any zeros for $|z| \leq r$, then

$$\int_0^{2\pi} \log|f(re^{i\theta})| \frac{d\theta}{2\pi} = \log|f(0)|.$$

This formula is no longer true if f has zeros. But, one can add some correction factors to account for the zeros.

Theorem (Jensen Formula)

Let $f(z)$ be an entire function such that $f(0) \neq 0$. Then,

$$\int_0^{2\pi} \log|f(re^{i\theta})| \frac{d\theta}{2\pi} = \log|f(0)| + \sum_{z \text{ s.t. } f(z)=0 \text{ and } |z|<r} \log\left(\frac{r}{|z|}\right)^{m_z},$$

where m_z is the multiplicity of the zero.

Comparing the Jensen Formula and the Product Formula

- If we take the logarithm of the product formula, we get for a in $\mathbf{Z}$,
$$\log|1| \;=\; \log|a| \;+\; \sum_{p \text{ prime}} \log|a|_p.$$
- Compare with the Jensen formula that says for an entire function
$$\log|f(0)| \;=\; \int_0^{2\pi} \log|f(re^{i\theta})| \frac{d\theta}{2\pi} \;-\; \sum_{|z|<r} \log\left(\frac{r}{|z|}\right)^{m_z}.$$
- For fixed r and θ define $|f|_{r,\theta} = |f(re^{i\theta})|$.
  - $|f|_{r,\theta}$ is almost an Archimedean absolute value, except that we might have $|f|_{r,\theta} = 0$ even if $f \neq 0$.
- For $|z| < r$, define $|f|_{r,z} = \log\left(\frac{|z|}{r}\right)^{m_z}$.
  - $|\ |_{r,z}$ is a non-Archimedean absolute value just like $|\ |_p$.
- **Jensen Formula:** $\log|f(0)| \;=\; \int_0^{2\pi} \log|f|_{r,\theta} \frac{d\theta}{2\pi} \;+\; \sum_{|z|<r} |f|_{r,z}.$

Institute of Mathematics in Hanoi

- The field of mathematics that studies commutative rings, *i.e.*, generalizations of $\mathbf{Z}$ and $\mathbf{C}[t]$, is called commutative algebra. The Institute here in Hanoi has many active researchers in this area.
- Mathematicians study analysis, similar to complex analyis, but related to the p-adic absolute values I discussed today. The Institute here also has several experts in p-adic analysis.
- Osgood noticed a connection between number theory and a branch of complex analysis called Nevanlinna Theory or Value Distribution Theory. Value Distribution Theory has a long history here in Hanoi because Le Van Thiem was one of the pioneers of this field of mathematics. Vojta, independent of Osgood, also discovered the connection between Value Distribution Theory and Number Theory and created an extensive "dictionary" relating the two fields; in particular he interpreted the Jensen Formula as the analog of the Product Formula in number theory as I described before. Important progress in both Value Distribution Theory and Number Theory has resulted from Vojta's connections between the fields. Again, some researchers here in Hanoi are quite familiar with these connections and work in related areas.

Thank You!

- Notes for this lecture will be posted at:
  `http://wcherry.math.unt.edu/pubs/hanoi2010.pdf`