From ABC to XYZ,

or

Addition versus Multiplication

Jeff Lagarias,
University of Michigan
Ann Arbor, MI, USA

LMS Mary Cartwright Symposium,
(London, March 1, 2013)

Topics Covered

- Part 0. Introduction
- Part 1. Logic and Complexity Theory
- Part 2. Measure Theory and Ergodic Theory
- Part 3. Diophantine Equations: ABC and XYZ
- Part 4. Concluding Remarks

Part 0. Introduction

The *integers* $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2 \cdots\}$.

- The *natural numbers* are

  $\mathbb{N} = \{: \ 0, 1, 2. \cdots\}$.

  $\mathbb{N}_{>0} = \{1, 2, 3. \cdots\} = \mathbb{N} \setminus \{0\}$.

- $(\mathbb{N}, 0, +\}$ is an *additive semigroup* with unit 0.

  $(\mathbb{N}_{>0}, 1, \cdot)$ is a *multiplicative semigroup* with unit 1.

The Question

Vague Question. "Do addition and multiplication get along?"

Intent of Question. There is some incompatibility between the two arithmetic operations. They act on different scales. Can one quantify this incompatability?

- Irreducible elements of additive semigroup: there is a *unique* one: namely, $\{1\}$.

- Irreducible elements of multiplicative semigroup: there are *infinitely many*: prime numbers

- "1 *is not a prime.*"

Answers

- *Answer 0.* Asked a colleague, got this answer:

  "*They get along, using the distributive law*."

- *Answer 1.* They don't get along, in terms of a mismatch of additive and multiplicative structures.

- *Answer 2.* They sort of get along: a detente.

Part 1. Logic and Complexity Theory

- The first order theory $Th(\mathbb{N}, =, +, 0, 1)$ is called Presburger arithmetic.

  Theorem (Presburger 1929)
  Presburger arithmetic is a decidable theory.

  [Proof by quantifier elimination, one adds $0, 1, <_n$.]

- The first order theory $Th(\mathbb{N}_{>0}, =, \times, 1, p_j)$ is called Skolem arithmetic.

  Theorem (Skolem 1930; Mostowski 1952)
  Skolem arithmetic is a decidable theory.

  [Proof by quantifier elimination.]

Logic-2

First order theory $Th(\mathbb{N}, +, \times, 0, 1)$ (with distributive laws), both addition and multiplication, is Peano arithmetic.

Theorem (Gödel 1931) *Peano arithmetic is incomplete theory (if it is consistent). That is, certain sentences and their negations are not provable in the theory. Also it is undecidable to recognize which statements are theorems.*

Gödel's original incompleteness formulation was much more general. It applies to a large class of theories.

Conclusion from LOGIC: Addition and multiplication do not completely get along.

Complexity Theory -1

Theorem. (Fischer and Rabin 1974)
(1) (Upper Bound) *There is a decision procedure for Presburger arithmetic that takes (deterministic) double exponential space complexity* $O\Big(\exp(\exp cn))\Big)$ *to decide if a formula of length* n *is a theorem.*

(2) (Lower Bound) *Any decision procedure for Presburger arithmetic requires at least double exponential time complexity*.

There is a similar complexity result for Skolem arithmetic:
upper bound: triple exponential space complexity
lower bound: triple exponential time complexity.

Complexity Theory-2

- The order relation $<$ is definable in Presburger arithmetic. (*Not so* for Skolem arithmetic !)

- The definable sets in Presburger arithmetic have a nice description found by Kevin Woods (2005, 2012) [Student of A. Barvinok (Michigan)].

- The description of definable sets is in terms of sets of lattice points in cones and polyhedra in R^n, n varying.

  There is a nice connection with linear and integer programming!

Complexity Theory-3

"Finite Complexity theory": This topic is being investigated by my graduate student Harry Altman.

- The integer complexity of n is the smallest number of 1's needed to represent n using the operations of addition, multiplication, with parentheses. Denote it: $||n||$.

- Computation tree is a binary tree with operations $+$ or $\times$ at each vertex, and with 1's at the leaf nodes. Convention: Leaf nodes can be combined using $+$ operation only.

  There are finitely many trees for each n. Here $||n||$ is minimal number of leaves across all such trees.
  (The maximum number is n leaves.)

Complexity Theory-4

- **Theorem.** (K. Mahler & J. Popken 1953) *The maximum number* m *representable using exactly* n $1's$ *depends on* $n \pmod 3$ *and this* $m = 3^n$ *if* $n \equiv 0 \pmod 3$*.*

- Their result implies: For all $n \geq 1$,

$$||n|| \geq 3 \log_3 n,$$

and equality holds $\Leftrightarrow n = 3^j$, $j \geq 1$.

- It is easy to show that

$$||n|| \leq 3 \log_2 n.$$

Complexity Theory-5

- Definition: The complexity defect of an integer is

$$\delta(n) := ||n|| - 3\log_3(n).$$

- Mahler-Popken bound implies

$$\delta(n) \geq 0.$$

Here $\delta(3^k) = 0$, all $k \geq 1$.

Here $\delta(2) = 2 - 3\log_3 2 \approx 0.107$.

Here $\delta(1) = 1$.

Here $\delta(5^6) = 29 - 18\log_3 5 \approx 2.6304...$.

Complexity Theory-6

- It seems hard to compute $||n||$; known algorithms take time exponential in the input size: $\log_2 n + 1$ in binary (bits).

- Theorem. (Mahler) $||3^n|| = 3n$.

- Conjecture. $||2^n|| = 2n$.

  It is immediate that $||2^n|| \leq 2n$.

  [Equality in Conjecture has been verified by Altman and Zelinsky for all $n \leq 21$. This problem is seriously hard.]

Complexity Theory-7

- The defect value set $\mathcal{D}$ is the set of allowable values for the defect: $\mathcal{D} := \{\delta(n) : n \geq 1\}$

  The defect value partitions $\mathbb{N}_{>0}$ into equivalence classes. Two numbers can have the same defect only if one of them is a power of 3 times the other (This is necessary but not sufficient).

- **Well-Ordering Theorem.** (Altman 2012+)
  The defect value set $\mathcal{D} \subset \mathbb{R}_{\geq 0}$ is well-ordered with respect to the real number ordering. It has order type the ordinal ω^{ω}.

  For each $n \geq 1$ the set of values in the defect set having $\delta < n$ is of order type the ordinal ω^{n}.

Part 2: Measure Theory and Ergodic Theory

Measure theory: Ongoing work with V. Bergelson.

Starting point: The semigroup $(\mathbb{N}, +)$ does *not* have any translation-invariant probability measure.
Similarly, the semigroup $(\mathbb{N}, \cdot)$ has no translation-invariant probability measure.

But both semigroups are amenable. That is, they have (a lot of) translation-invariant finitely additive measures. These measures are called invariant means.

An invariant mean can be constructed using a family of exhausting sequences (Følner sets), along with a choice of ultrafilter. There are $2^{2^{\aleph_0}}$ such invariant means.

Measure Theory-2

- **Question.** How orthogonal are additive and multiplicative structures with respect to these invariant means?

- The upper (additive) Banach density $d^*(S)$ of any set $S \subset \mathbb{N}$ is
$$d^*(S) := \limsup_{N \to \infty} \left(\sup_{M \geq N} \frac{1}{N} |S \cap [M, M+N-1]|. \right)$$

- **Proposition.** *The upper (additive) Banach density $d^*(S)$ is the supremum of $m(S)$ taken over all additive invariant means m. It is a translation-invariant quantity, but is not a finitely-additive measure.*

Measure Theory -3

- **Theorem.** *For any $\epsilon > 0$ exists a subset $S_1 \subset \mathbb{N}_{>0}$ having upper additive Banach density at least $1 - \epsilon$ and with upper multiplicative Banach density 0.*

- **Theorem.** *For any $\epsilon > 0$ there exists a subset $S_2 \subset \mathbb{N}_{>0}$ having upper multiplicative Banach density 1 and with upper additive Banach density at most ϵ.*

- Sets above can be chosen to be universal: all invariant means agree on their density (for $+$ and $\times$, respectively).

  Moral: Additive and Multiplicative structures are fairly orthogonal in this weak measure theory sense.

Ergodic Theory -1

(Joint work with Sergey Neshveyev (Oslo); on arXiv:1211.3256)

This work relates to the program of Alain Connes to understand the Riemann hypothesis in terms of noncommutative geometry.

Connes studies a peculiar space, the quotient space $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}^*$ of the adeles by the multiplicative group $\mathbb{Q}^*$.

The space of adeles $\mathbb{A}_{\mathbb{Q}}$ over the number field $\mathbb{Q}$ is an additive construction. It is the restricted direct product over the real place and all nonarchimedean (prime) places of the completion of $\mathbb{Q}$ at these places. The field $\mathbb{Q}$ embeds additively on the diagonal in $\mathbb{A}_{\mathbb{Q}}$ as a discrete subgroup of the form $r = p/q \mapsto (r, r, r, r, ...)$ and the quotient $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$ is compact.

Ergodic Theory -2

The multiplicative action of $r \in \mathbb{Q}^*$also acts on the diagonal. Multiplication by r acts by sending

$$\alpha = (a_\infty, a_2, a_3, a_5, \cdots) \mapsto r\alpha := (ra_\infty, ra_2, ra_3, \cdots)$$

The quotient is not compact.

Theorem. (Connes 1995) *The action of $\mathbb{Q}^*$ on $\mathbb{A}_\mathbb{Q}$ is ergodic. That is, if Ω is a Borel measurable subset of the space $\mathbb{A}_\mathbb{Q}$ that is invariant under the $\mathbb{Q}^*$-action, i.e. $r\Omega = \Omega$ for all $r \in \mathbb{Q}^*$, then one of Ω and $\mathbb{A}_\mathbb{Q} \setminus \Omega$ has additive Haar measure* 0.

This result says that measure-theoretically the space $\mathbb{A}_\mathbb{Q}/\mathbb{Q}^*$ acts like a point. *In this sense additive and multiplicative structures don't match.*

Ergodic Theory -3

Theorem. (L-Neshveyev) *The ergodicity result is valid for adeles $\mathbb{A}_K$ over an arbitrary global field K, acted on by K^*.*

A global field K is a number field or an algebraic function field over a finite field.

This result gives a new proof of ergodicity even for $K = \mathbb{Q}$.

This proof uses averaging over all Hecke characters (grössencharacters) including the infinite order characters. On the analytic level, this proof essentially seems equivalent to existence of no zeros on the line $Re(s) = 1$ for all the Hecke L-functions.

Part 3: Diophantine Equations: ABC and XYZ equations

Consider the ABC equation $A + B = C$. It is sometimes written

$$A + B + C = 0.$$

It is a homogeneous linear Diophantine equation.
This equation imposes an additive restriction on A, B, C.

Heuristic. Constraint imposed by linear equation imposes conditions on the multiplicative properties of the allowed solutions (A, B, C). The prime factorizations of (A, B, C) cannot be arbitrary, but are *restricted in some fashion.*

Various difficult conjectures in number theory make this assertion quantitative.

Part 3: Diophantine Equations-2

Some measures of multiplicative complexity of (A, B, C):

- The height of a triple (A, B, C) is

$$H := H(A, B, C) = \max\{|A|, |B|, |C|\}$$

- The radical of a triple (A, B, C)

$$R := R(A, B, C) = \prod_{p|ABC} p$$

- The smoothness of a triple (A, B, C) is

$$S := S(A, B, C) = \max\{p : \ p \text{ divides } \ ABC\}.$$

Diophantine Equations-3

- **Example.** $(A, B, C) = (2401, -2400, -1)$

- $$\begin{aligned} 2401 &= 7^4 \\ 2400 &= 2^5 \cdot 3 \cdot 5^2 \\ 1 &= 1 \end{aligned}$$

- The height is $H = 2401$.

- The radical is $R = 2 \cdot 3 \cdot 5 \cdot 7 = 210$.

- The smoothness is $S = 7$.

Diophantine Equations-4

The ABC Conjecture concerns the relation of the height and the radical of relatively prime triples (A, B, C)
(That is, we require $gcd(A, B, C) = 1$.)

ABC Conjecture. *For each $\epsilon > 0$ there are only finitely many relatively prime solutions (A, B, C) with radical*

$$R \leq H^{1-\epsilon}.$$

Shinichi Mochizuki (RIMS-Kyoto) has announced a proof of the ABC Conjecture. If his proof holds up, this will be the theorem of the century! (It implies results of several previous Fields Medal winners.) Current status of proof: unclear.

Diophantine Equations-5

- ABC measure of inverse quality is:

$$Q^{-1}(A,B,C) := \frac{\log R(A,B,C)}{\log H(A,B,C)}$$

- ABC Conjecture says for each $\epsilon > 0$ only finitely many (relatively prime) triples (A,B,C) have inverse quality $Q^{-1}(A,B,C) < 1-\epsilon$.

- Current World Record for smallest inverse quality:

$$2 + 3^{10} \cdot 109 = 23^5.$$

It has $Q^{-1}(2, 3^{10} \cdot 109, -23^5) = 0.6135...$

Diophantine Equations-6

(Joint work with K. Soundararajan (Stanford)).

Consider a different problem: the relation of the height and the smoothness of relatively prime triples.

Basic Problem. How small can be the smoothness S be as a function of the height H,

so that:

There are (still) infinitely many relatively prime triples (A, B, C) with these values satisfying $A + B + C = 0$?

We formulate the XYZ Conjecture concerning this relation.

Diophantine Equations-7

- To avoid confusion with ABC Conjecture, we define the XYZ equation to be:

$$X + Y + Z = 0.$$

- XYZ Conjecture. There is a positive constant α_0 such that for any positive ϵ the XYZ equation $X + Y + Z = 0$ has finitely many solutions to

$$S \leq (\log H)^{\alpha_0 - \epsilon}.$$

and infinitely many solutions to

$$S \leq (\log H)^{\alpha_0 + \epsilon}.$$

Diophantine Equations-8

- Definition. Given a (primitive) solution (X, Y, Z) to the XYZ equation, assign it the smoothness exponent
$$\alpha_0(X, Y, Z) := \frac{\log S(X, Y, Z)}{\log \log H(X, Y, Z)}.$$
This is the XYZ analogue of inverse quality $Q^{-1}(X, Y, Z)$.

- The limiting exponent in the XYZ Conjecture is:
$$\alpha_0 := \liminf_{H(X,Y,Z) \to \infty} \alpha_0(X, Y, Z)$$

- The XYZ Conjecture asserts that α_0 is positive and finite.

Diophantine Equations-9

- Probabilistic Heuristic: Best constant is $\alpha_0 = 3/2$.

- This prediction is based on the distribution of numbers having only small prime factors. Counting function for this is : $\Psi(x, y)$, which counts numbers below x having all prime factors below y.

  The study of this function is called $\Psi(x, y)$-ology.
  This leads to expect solutions to the XYZ equation when

  $$\Psi(x, y)^3 \geq x.$$

  One finds that the minimal y is

  $$y = (\log x)^{3/2+o(1)}.$$

Diophantine Equations-10

Example Revisited: $(X, Y, Z) = (2401, -2400, -1)$.

$$\text{height} \qquad H(X,Y,Z) = 2401$$

$$\text{smoothness} \quad S(X,Y,Z) = 7$$

The smoothness exponent is:

$$\alpha_0(X,Y,Z) := \frac{\log S(X,Y,Z)}{\log\log H(X,Y,Z)} = \frac{\log 7}{\log\log 2401} = 0.94828...$$

This is an "unusually lucky" example. The heuristic for $X + Y = 1$ predicts limiting value $\alpha_0^* = 2$.

Diophantine Equations -11

- **Alphabet Soup Theorem** (L.-Soundararajan 2011, 2012)
  $ABC + GRH$ implies XYZ.

  This is a conditional result:

- Lower Bound Theorem
  ABC Conjecture $\Longrightarrow$ the XYZ constant $\alpha_0 \geq 1$.

- Upper Bound Theorem
  Generalized Riemann Hypothesis (GRH) $\Longrightarrow$
  the XYZ constant $\alpha_0 \leq 8$.

Diophantine Equations-12

- The exact constant α_0 is not determined by the Alphabet Soup Theorem, only its existence is asserted.

- Lower Bound Theorem assuming ABC Conjecture: This is Easy Part.

- Upper Bound Theorem assuming GRH:
  This is Harder Part.

  Stronger result: Get asymptotic formula for number of primitive solutions, valid for $\alpha_0 > 8$. Proof uses Hardy-Littlewood method (circle method).

Diophantine Equations-13

Mysterious XYZ Examples: Singular moduli (of elliptic curves)

- Let $\tau = x + iy \in \mathbb{C}$ lie in the upper half plane $\mathbb{H}$. Set $q = e^{2\pi i \tau}$ so that $|q| < 1$ lies in the unit disk.

- The elliptic modular function $j(\tau)$ generates the field of rational functions on the modular surface $\mathbb{H}/PSL(2,\mathbb{Z})$. It has a Fourier expansion

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots$$

Diophantine Equations-14

Definition. A singular modulus is a value τ that is an algebraic integer in an imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ that falls in the upper half plane $Im(\tau) > 0$.

$\mathbb{H}/PSL(2, \mathbb{Z})$ is moduli space parametrizing elliptic cuves.
A singular modulus τ corresponds to an elliptic curve having complex multiplication (CM) by an order $\mathbb{Z}[1, \tau]$ in $\mathbb{Q}(\sqrt{-d})$.

CM Theorem. (Kronecker, Fueter, Weber, ...)
The value $j(\tau)$ of a singular modulus τ is an algebraic integer generating a field that is an abelian extension of the number field $\mathbb{Q}(\sqrt{-d})$. When τ corresponds to CM by the full ring of integers in $\mathbb{Q}(\sqrt{-d})$, then this field is the Hilbert class field of $\mathbb{Q}(\sqrt{-d})$.

Diophantine Equations-15

- If $\mathbb{Q}(\sqrt{-d})$ has class number one, which happens exactly for $d = 3, 4, 7, 8, 11, 19, 43, 67, 163$, then:
  $j(\tau)$ is an ordinary integer.

- The differences of singular moduli $j(\tau_1) - j(\tau_2)$ have remarkable properties!

- Gross and Zagier (1985) showed that the differences of singular moduli have norms (as algebraic integers) that factorize completely into products of small primes. They gave an explicit formula for the factorization.

Diophantine Equations-16

- We obtain an XYZ equation using differences of three singular moduli:

  $$(j(\tau_1) - j(\tau_2)) \ + \ (j(\tau_2) - j(\tau_3)) \ + \ (j(\tau_3) - j(\tau_1)) = 0.$$

  If these come from imaginary quadratic fields of class number one, get integers!

- Example Take

  $$\tau_1 = \frac{1+\sqrt{-3}}{2}, \tau_2 = \frac{1+\sqrt{-67}}{2}, \tau_3 = \frac{1+\sqrt{-163}}{2}.$$

Diophantine Equations-17

- Then

$$j(\tau_1) - j(\tau_2) = 2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$$

$$j(\tau_2) - j(\tau_3) = 2^{15} \cdot 3^5 \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 139 \cdot 331$$

$$j(\tau_3) - j(\tau_1) = -2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$$

- Removing the common factor $2^{15} \cdot 3^3 \cdot 5^3$, we get a smooth solution

$$(X, Y, Z) = (1331, 2373926373, -2373927704)$$

to $X + Y + Z = 0$.

Diophantine Equations-18

This solution has height $H = 2373927704$, smoothness $S = 331$.

Its smoothness exponent is:

$$\alpha_0(X,Y,Z) = \frac{\log 331}{\log\log 2373927704} \approx 1.88863.$$

This example has radical

$$R = 184312146018,$$

which is rather larger than H. Not a good example for the ABC Conjecture.

Diophantine Equations-19

- Ongoing work: Reformulation of XYZ Conjecture in terms of elliptic curves over $\mathbb{Q}$. (with J. Weigandt)

- Definition: The smoothness of an elliptic curve (over $\overline{\mathbb{Q}}$) is the largest prime at which it has bad reduction.

Conclusion-1

The primes are the generators of the semigroup $(\mathbb{N}_{>0}, \times)$.

Fact. The density of primes, and their location, is influenced by the additive structure. Namely, each arithmetic progression

$$P(a,b) = \{an + b : \quad n \in \mathbb{Z}\}$$

for which greatest common divisor $(a,b) > 1$, can contain at most one prime, and this occurs only when $gcd(a,b) = p$.

Heuristic. To avoid all these arithmetic progressions, the set of primes is forced to be thin (density $\sim x/\log x$), and also to have irregular fluctuations.

Conclusion-2

This avoidance of arithmetic progressions is the basis of sieve methods in number theory.

Question. *Does this avoidance encode the essential difficulty behind the Riemann hypothesis?*

Summary. Addition and multiplication do not quite get along. In some remarkable way addition forces irregular behavior in multiplication. This talk has described their interaction across several different fields.

Thank You!

References

- H. Altman and J. Zelinsky, Numbers with integer complexity close to the lower bound, INTEGERS, Volume 12A (John Selfridge Memorial Volume) (2012), No.1.

- J. Lagarias and S. Neshveyev , Ergodicity of the action of K^* on A_K, arXiv:1211.3256

- J. Lagarias and K. Soundararajan, Smooth solutions to the abc equation: the xyz conjecture, J. Theor. Nombres Bordeaux **23** (2011), No. 1, 209–234.

- J. Lagarias and K. Soundararajan, Counting smooth solutions to the equation $A+B=C$, Proc. London Math. Soc. **104** (2012), 770–798.

- P. Kurlberg, J. Lagarias, C. Pomerance, The maximal density of product-free sets in $\mathbb{Z}/n\mathbb{Z}$, IMRN, Online access Feb. 14, 2012, doi:10.1093/imrn/rns014.

- Work partially supported by NSF grants DMS-0801029 and DMS-1101373