College of Saint Benedict and Saint John's University
DigitalCommons@CSB/SJU

Forum Lectures | Forum

2-2-2017

Arithmetic: math as 'pure' and 'applied'

Sunil Chetty
College of Saint Benedict/Saint John's University, schetty@csbsju.edu

Follow this and additional works at: http://digitalcommons.csbsju.edu/forum_lectures

 Part of the Mathematics Commons

Recommended Citation
Chetty, Sunil, "Arithmetic: math as 'pure' and 'applied'" (2017). *Forum Lectures*. 169.
http://digitalcommons.csbsju.edu/forum_lectures/169

This Presentation is brought to you for free and open access by DigitalCommons@CSB/SJU. It has been accepted for inclusion in Forum Lectures by an authorized administrator of DigitalCommons@CSB/SJU. For more information, please contact digitalcommons@csbsju.edu.

Thursday Forum
Arithmetic as ‘pure’ and ‘applied’

Sunil Chetty

Department of Mathematics

COLLEGE OF
Saint Benedict Saint John's
UNIVERSITY

February 2, 2017

A Quote

G.H. Hardy, in *A Mathematician's Apology*:

"[P]ure mathematics is on the whole distinctly more useful than applied. For what is useful above all is technique, and mathematical technique is taught mainly through pure mathematics. "

Natural Numbers $\mathbb{N}$

Question

What is a natural number? In other words, how does one understand the collection $0, 1, 2, \ldots$?

Three major views on developing $\mathbb{N} = \{0, 1, 2, \ldots\}$:

- Aristotelian/Empiricist
- Platonic
- Humanist

Natural Numbers $\mathbb{N}$ - Equality

Question

How does one distinguish natural numbers? Or equivalently, how does one decide if two quantities are equal and hence constitute instances of the same (abstract) natural number?

Definition

Two collections of objects have the same *cardinality* if the contents of each can be paired-up in a one-to-one way.

For a collection S, we denote its cardinality by $|S|$.

Natural Numbers $\mathbb{N}$ - Definition

The natural numbers $\mathbb{N}$ are the distinct, finite cardinalities:

- $0 = |\emptyset|$
- $1 = |\{0\}|$
- $2 = |\{0, 1\}|$

$\vdots$

Question

Should there be a number for $|\mathbb{N}| = |\{0, 1, 2, \ldots\}|$?

Arithmetic on $\mathbb{N}$ - Addition

Question

How should one define addition of two natural numbers?

Abstractly: given $m, n \in \mathbb{N}$, what is $m + n$?

We define the operation and the result of addition:

- For two disjoint collections, the *union* is the collection of all objects contained in one or the other.
- The *sum* of two numbers is the cardinality of the union of any two instances of the given numbers.

Arithmetic on $\mathbb{N}$ - Addition Properties

Properties

For any $a, b, c \in \mathbb{N}$, $a + b$ is a natural number and

- $a + b = b + a$
- $(a + b) + c = a + (b + c)$
- $a + 0 = a$

Question

How does one verify these properties with tiles?

Arithmetic on $\mathbb{N}$ - Multiplication

Question

How should one define multiplication of two natural numbers?

Abstractly: given $m, n \in \mathbb{N}$, what is $m \cdot n$?

Two approaches:

- Repeated addition: $m \cdot n = ((\cdots((n+n)+n)\cdots)+n)$
- Geometric: the cardinality of the collection of square units required to fill a rectangle of width m and length n.

Arithmetic on $\mathbb{N}$ - Multiplication Properties

Properties

For any $a, b, c \in \mathbb{N}$, $a \cdot b$ is a natural number and

- $a \cdot b = b \cdot a$
- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- $a \cdot 1 = a$
- $a \cdot (b + c) = a \cdot b + a \cdot c$

Questions

How does one verify these properties with tiles?

Arithmetic on $\mathbb{N}$ - Primes

Definition

If $p \in \mathbb{N}$ such that $p = a \cdot b$ implies $a = 1$ or $b = 1$, then m is said to be prime.

Theorem

There are infinitely many primes.

Proof.

Suppose note, i.e. there are finitely many $p_1, \ldots, p_m$. Then $N = p_1 \cdots p_m + 1$ is either prime or divisible by a prime that is not included in the list, and this is a contradiction. $\square$

Arithmetic on $\mathbb{N}$ - Euclidean Algorithm

Definition

Let $m, n \in \mathbb{N}$. If $g \in \mathbb{N}$ such that

- $g \mid m$ and $g \mid n$,
- if $d \mid m$ and $d \mid n$ implies $d \mid g$,

then $g = \gcd(m, n)$ is the *greatest common divisor* of m and n.

Theorem

Let $m, n \in \mathbb{N}$, with $m \geq n$. Define $r_0 = m$, $r_1 = n$, and for $i \geq 1$,

$$r_{i+1} = r_{i-1} - q_{i-1} \cdot r_i.$$

Then $r_N = 0$ for some N and $\gcd(m, n) = r_{N-1}$.

Arithmetic on $\mathbb{N}$ - GCD and Primes

Theorem

Let $g = \gcd(m, n)$. Then g is smallest amongst all numbers of the form $mx + ny$.

Theorem

The following are equivalent:

(i) p is prime.

(ii) if $p \mid m \cdot n$ then $p \mid m$ or $p \mid n$.

Motivating Problems

Question

Professor Gauss arrives at CSB/SJU on a Tuesday at noon to give lectures on his latest research project. If he departs after 61 days, on what day of the week does Professor Gauss leave?

Question

Professor Euler is touring a country in which each calendar month has 28 days. He gives a lecture on the day he arrives and subsequently on every sixth day (no exceptions) until his departure. If he departs 3 days after his last lecture, could his departure be on the same day of the month as his arrival?

Integers modulo n

Definition

Let $m \in \mathbb{N}$ be fixed. For $a, b \in \mathbb{Z}$ we say a and b are *congruent modulo* m if $m \mid (a - b)$.

We use the notation $a \equiv_m b$ for congruence modulo m.

Theorem

The relation $\equiv_m$ behaves like $=$ and respects both addition and multiplication: if $a \equiv_m u$ and $b \equiv_m v$

- then $a + b \equiv_m u + v$,
- then $a \cdot b \equiv_m u \cdot v$.

Integers modulo p

The set

$$\mathbb{Z}/\langle m\rangle = \{0, 1, 2, \ldots, m-1\},$$

considered with $\equiv_m$, addition, and multiplication, shares many structural properties with $\mathbb{Z}$.

If p is a prime, then $\mathbb{F}_p = \mathbb{Z}/\langle p\rangle$ enjoys a finer structure than $\mathbb{Z}$. The above theorem about GCD implies the following:

Theorem

Let p be a prime. For every $a \not\equiv_p 0$, there is some $b \in \mathbb{Z}$ such that $a \cdot b \equiv_p 1$.

Coding Theory and $\mathbb{F}_p$

Problem

Suppose one wishes to send information via a noisy channel. Can one detect if the received information contains errors? If so, is it possible to recover the intended information?

Linear codes provide a (restricted) positive solution to both parts of the problem:

- Code words are a special collection of $(c_1, \ldots, c_n) \in \mathbb{F}_p^n$.
- Determine the "minimum distance" between code words.
- Check received word against code words to find nearest neighbor.

RSA Encryption and $\mathbb{Z}/\langle m \rangle$

Problem

Can one send a message across a public channel such that only the intended recipient can read the message? Is it possible if neither party has communicated previously?

RSA Encryption

Let $m = pq$ where p and q are large primes. To receive secure messages:

- Choose $e, d \in \mathbb{N}$ such that $e \cdot d \equiv_{\Phi(m)} 1$.
- Publish e, declare messages M be encrypted/sent as M^e.
- Decrypt via $M \equiv_m M^{ed} \equiv_m (M^e)^d$.

Polynomial Arithmetic

Consider $\mathbb{Z}[x] = \left\{a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \ : \ a_i \in \mathbb{Z},\ n \in \mathbb{N}\right\}$.

$\mathbb{Z}[x]$ enjoys some key structural similarities with $\mathbb{Z}$:

- Addition and multiplication are well-defined operations.
- Every member of $\mathbb{Z}[x]$ can be factored into primes.

$\mathbb{Q}[x]$ serves as a better analogy to $\mathbb{Z}$ than $\mathbb{Z}[x]$, as it has a Euclidean Algorithm, consequently:

- GCD is defined as for $\mathbb{Z}$.
- $p(x)$ is prime if and only if $p(x)$ cannot be properly factored.

Polynomial Arithmetic

Generalizing the focus from “numbers” to “ideals” reveals more.

Definition

An *ideal* $I \subset \mathbb{Q}[x]$ is a collection of members of $\mathbb{Q}[x]$ that respects arithmetic, and if $q(x) \in I$, $r(x) \in \mathbb{Q}[x]$ then $r(x)q(x) \in I$.

Theorem

- Each ideal in $\mathbb{Q}[x]$ consists of all multiples of a single polynomial $p(x)$.
- $\langle p(x) \rangle \subset \mathbb{Q}[x]$ is prime if and only if $p(x)$ is prime.

Number Fields

Analogous to $\mathbb{Z}/\langle p \rangle$, one can consider the system $\mathbb{Q}[x]/\langle p(x) \rangle$.

Consider $p(x) = x^2 + 1$, $I = \langle x^2 + 1 \rangle$. Then

- $\mathbb{Q}[x]/I = \mathbb{Q}(i) = \{a + bi \ : \ a, b \in \mathbb{Q}\}$, where $i^2 + 1 = 0$.
- $Z[i] \subset \mathbb{Q}(i)$ is analogous to $\mathbb{Z} \subset \mathbb{Q}$.

Question

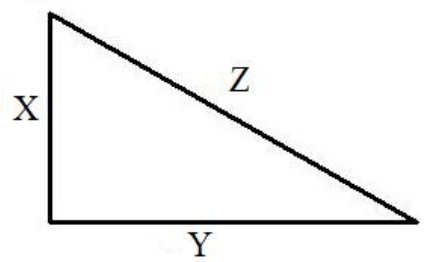
What are the primes in $\mathbb{Z}[i]$? How do they relate to primes in $\mathbb{Z}$?

Notice, for example, $2 = 1 - (-1) = 1 - i^2 = (1 + i)(1 - i)$.

Number Fields and Triangles

Problem

Determine all integer triples (x, y, z) such that $x^2 + y^2 = z^2$.



Notice in $\mathbb{Z}[i]$ one has $z^2 = x^2 + y^2 = (x + iy)(x - iy)$.

- The question about sides of a right triangle is now a factorization question in $\mathbb{Z}[i]$.
- Conclude $(x, y, z) = \left(st, \frac{s^2-t^2}{2}, \frac{s^2+t^2}{2}\right)$, with $s, t \in \mathbb{Z}$.

Finite Fields

Problem

Can one construct a *finite* field? i.e. a finite system with arithmetic structure akin to $\mathbb{Q}$?

We have already accomplished this once with $\mathbb{Z}/\langle p \rangle$.

- Suppose $K = \mathbb{Q}[x]/\langle p(x) \rangle$ and $\mathcal{O} \subset K$ mirrors $\mathbb{Z} \subset \mathbb{Q}$. If $I \subset \mathcal{O}$ is maximal then $\mathcal{O}/I$ is a field and finite.
- Moreover, $|\mathcal{O}/I| = p^n$ for the unique prime $p \in I$.

Coding theory and cryptographic structures are often better when constructed in larger finite fields.

Geometry meets Algebra

An elliptic curve $E/\mathbb{Q}$ is defined by a Weierstrass equation

$$y^2 = x^3 + ax + b, \quad \text{with } a, b \in \mathbb{Q},$$

(under some "non-singularity" conditions).

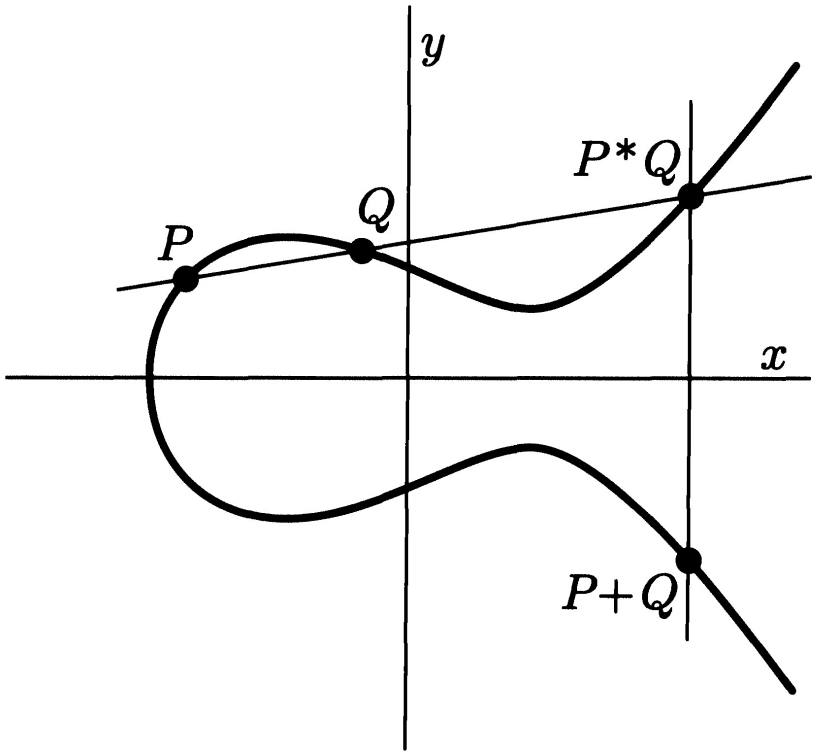
The set of rational solutions $E(\mathbb{Q})$ is defined to be

$$E(\mathbb{Q}) = \left\{(x, y) \in \mathbb{Q}^2 : \ y^2 = x^3 + ax + b\right\} \cup \{O_E\}.$$

The object O_E is called the "point at infinity."

Geometry meets Algebra

The set of points $E(\mathbb{Q})$ admits a commutative addition operation



Adding Points on a Weierstrass Cubic

Arithmetic Structure

Let $P = (x_1, y_1)$, $Q = (x_2, y_2) \in E(\mathbb{Q})$. Then

$$P + Q = (\alpha^2 - x_1 - x_2, \alpha x_3 + \beta)$$

where $y = \alpha x + \beta$ is the line connecting P and Q.

Theorem (Mordell 1922)

The group $E(\mathbb{Q})$ is finitely generated. Thus, $E(\mathbb{Q})$ decomposes

$$E(\mathbb{Q}) \cong E_{tors}(\mathbb{Q}) \times \mathbb{Z}^{r(E,\mathbb{Q})}.$$

The quantity $r(E, \mathbb{Q})$ is known as the (algebraic) *rank* of $E(\mathbb{Q})$.

EC and $\mathbb{F}_p$

Recall $\mathbb{F}_p = \mathbb{Z}/\langle p \rangle$ is a finite field when p is prime.

If $E: \ y^2 = x^3 + ax + b$ has $a, b \in \mathbb{Z}$ then one can reduce $a, b \pmod p$, and define a new curve $\tilde{E}/\mathbb{F}_p$.

The set $\tilde{E}(\mathbb{F}_p)$ still admits an addition law:

- The geometric picture is no longer meaningful.
- The algebraic formulas for addition still hold.
- $\tilde{E}(\mathbb{F}_p)$ is automatically finite.

Question

How many points can $\tilde{E}(\mathbb{F}_p)$ have?

EC and $\mathbb{F}_p$

There are p choices for $x(P)$ in $\mathbb{F}_p$:

- $x(P) = 0$ yields $(0, 0) \in \tilde{E}(\mathbb{F}_p)$
- $x(P) \neq 0$ and not a square in $\tilde{E}(\mathbb{F}_p)$ yields no points.
- $x(P) \neq 0$ and a square in $\tilde{E}(\mathbb{F}_p)$ yields two points.

One expects half of the values in $\mathbb{F}_p$ to be squares, hence $p + 1$ points in $\tilde{E}(\mathbb{F}_p)$.

Theorem (Hasse 1933)

$|\#\tilde{E}(\mathbb{F}_p) - (p + 1)| < 2\sqrt{p}$.

Elliptic Curve Cryptography

Question

Can one emulate RSA encryption with points on $E(\mathbb{F}_p)$?

1. Closure under addition/multiplication-by-n on rational points.
2. Cyclic structure: $E(\mathbb{F}_p) = \langle P \rangle$
3. Essentially the same linear equation to decrypt
4. Difficult problem: undoing addition on points of E is intractable

Elliptic Curve Cryptography

Recall: $|\#E(\mathbb{F}_p) - (p+1)| < 2\sqrt{p}$ (Hasse bound)

Plan of attack:

For (4), we ensure that $\#E(\mathbb{F}_p)$ is large.

For (2), we ensure that $\#E(\mathbb{F}_p)$ is a prime.

Two approaches:

1. Pick a random curve E over $\mathbb{F}_p$, count the points, decide if it is good.
2. Construct a curve E with a prescribed number of points.

   Note: uses factorization in a system like $\mathbb{Z}[i]$.