Residue rings of models of Peano Arithmetic

Paola D'Aquino

Università della Campania "L. Vanvitelli"

Z75 - Oxford

10 September 2024

joint work with A. Macintyre

In 2014 Zilber asked the following question:

If $\mathcal{M}$ is a nonstandard model of full Arithmetic ($\mathcal{M} \equiv \mathbb{N}$), and n is a nonstandard element of $\mathcal{M}$ congruent to 1 modulo all standard integers, does the ring $\mathcal{M}/n\mathcal{M}$ interpret Arithmetic?

NO

This motivated the model theoretic analysis of the residue rings $\mathcal{M}/n\mathcal{M}$ where $\mathcal{M}$ is a model of Peano Arithmetic, and $1 < n \in \mathcal{M}$

Peano Arithmetic *PA*

Let $\mathcal{L} = \{+, \cdot, 0, 1, <\}$. A model of *PA* is the positive part of a discretely ordered ring satisfying the induction for all definable subsets

$$\forall \overline{y}((\theta(0, \overline{y}) \wedge \forall x(\theta(x, \overline{y}) \to \theta(x+1, \overline{y}))) \to \forall x \theta(x, \overline{y}))$$

for all formulas $\theta(x, \overline{y})$ in $\mathcal{L}$.

Clearly, $(\mathbb{N}, +, \cdot, 0, 1, <)$ is a model of *PA*. If $\mathcal{M} \models PA$ and $\mathcal{M} \ncong \mathbb{N}$ then $\mathcal{M}$ is a nonstandard models of *PA*.

The positive part of $\prod_D \mathbb{Z}$, where D is a non principal ultrafilter, is a non standard model of *PA*.

If $\mathcal{M} = \mathbb{Z}$, and p is a prime in $\mathbb{Z}$, $k > 0$

- $\mathbb{Z}/p^k\mathbb{Z}$ is a Henselian local ring with maximal ideal $p\mathbb{Z}/p^k\mathbb{Z}$
- $\mathbb{Z}/p^k\mathbb{Z}$ is a finite chain ring, i.e. the ideals are linearly ordered
- $\mathbb{Z}/p^k\mathbb{Z} \cong \mathbb{Z}_p/p^k\mathbb{Z}_p$, where $\mathbb{Z}_p$ is the ring of p-adic integers

Ax, Elementary theory of finite fields, in 1968:

- The theory of all $\mathbb{Z}/p\mathbb{Z}$ as p varies is decidable
- For fixed prime p the theory of $\mathbb{Z}/p^k\mathbb{Z}$ as k varies is decidable
- The theory of all $\mathbb{Z}/p^k\mathbb{Z}$ as p and k vary is decidable
- The existential theory of $\mathbb{Z}/m\mathbb{Z}$, $m \in \mathbb{Z}$, $m > 1$ is decidable

If $\mathcal{M} = \mathbb{Z}$, and p is a prime in $\mathbb{Z}$, $k > 0$

- $\mathbb{Z}/p^k\mathbb{Z}$ is a Henselian local ring with maximal ideal $p\mathbb{Z}/p^k\mathbb{Z}$
- $\mathbb{Z}/p^k\mathbb{Z}$ is a finite chain ring, i.e. the ideals are linearly ordered
- $\mathbb{Z}/p^k\mathbb{Z} \cong \mathbb{Z}_p/p^k\mathbb{Z}_p$, where $\mathbb{Z}_p$ is the ring of p-adic integers

Ax, Elementary theory of finite fields, in 1968:

- The theory of all $\mathbb{Z}/p\mathbb{Z}$ as p varies is decidable
- For fixed prime p the theory of $\mathbb{Z}/p^k\mathbb{Z}$ as k varies is decidable
- The theory of all $\mathbb{Z}/p^k\mathbb{Z}$ as p and k vary is decidable
- The existential theory of $\mathbb{Z}/m\mathbb{Z}$, $m \in \mathbb{Z}$, $m > 1$ is decidable

If $\mathcal{M} = \mathbb{Z}$, and p is a prime in $\mathbb{Z}$, $k > 0$

- $\mathbb{Z}/p^k\mathbb{Z}$ is a Henselian local ring with maximal ideal $p\mathbb{Z}/p^k\mathbb{Z}$
- $\mathbb{Z}/p^k\mathbb{Z}$ is a finite chain ring, i.e. the ideals are linearly ordered
- $\mathbb{Z}/p^k\mathbb{Z} \cong \mathbb{Z}_p/p^k\mathbb{Z}_p$, where $\mathbb{Z}_p$ is the ring of p-adic integers

Ax, Elementary theory of finite fields, in 1968:

- The theory of all $\mathbb{Z}/p\mathbb{Z}$ as p varies is decidable
- For fixed prime p the theory of $\mathbb{Z}/p^k\mathbb{Z}$ as k varies is decidable
- The theory of all $\mathbb{Z}/p^k\mathbb{Z}$ as p and k vary is decidable
- The existential theory of $\mathbb{Z}/m\mathbb{Z}$, $m \in \mathbb{Z}$, $m > 1$ is decidable

Open problem in Ax, Elementary theory of finite fields:

Is the elementary theory of $\{\mathbb{Z}/m\mathbb{Z} : m \in \mathbb{Z}, m > 1\}$ decidable?

YES due to Derakhshan and Macintyre in 2023. The proof uses the decidability of the ring of finite adèles

$\mathbb{A}_{\mathbb{Q}}^{f} = \{f \in \prod_{p \in P} \mathbb{Q}_p | f(p) \in \mathbb{Z}_p$ except for finitely many p's $\}$

Let $\mathcal{M} \models PA$ non standard, and $p \in \mathcal{M}$ then

p is prime iff p is irreducible iff p is maximal (i.e. $\mathcal{M}/p\mathcal{M}$ is a field)

GOAL: Given $n \in \mathcal{M}$ what can we say on the model theory of $\mathcal{M}/n\mathcal{M}$?

• $n = p$ (Macintyre, 1982)

• $n = p^k$, where $p, k \in \mathcal{M}$, p is a prime and $k > 1$
(D'A. and Macintyre, 2017 $<$ ... ?)

• $1 < n$ composite
(D'A. and Macintyre 2022 $<$ ... ?)

For 2) we use mainly AKE principle in valuation theory.

2) and 3) are connected via (a kind of "converse" of)
Feferman-Vaught Theorem (1959)

Let $\mathcal{M} \models PA$ non standard, and $p \in \mathcal{M}$ then

p is prime iff p is irreducible iff p is maximal (i.e. $\mathcal{M}/p\mathcal{M}$ is a field)

GOAL: Given $n \in \mathcal{M}$ what can we say on the model theory of $\mathcal{M}/n\mathcal{M}$?

• $n = p$ (Macintyre, 1982)

• $n = p^k$, where $p, k \in \mathcal{M}$, p is a prime and $k > 1$
(D'A. and Macintyre, 2017 $<$ ... ?)

• $1 < n$ composite
(D'A. and Macintyre 2022 $<$ ... ?)

For 2) we use mainly AKE principle in valuation theory.

2) and 3) are connected via (a kind of "converse" of) Feferman-Vaught Theorem (1959)

Let $\mathcal{M} \models PA$ non standard, and $p \in \mathcal{M}$ then

p is prime iff p is irreducible iff p is maximal (i.e. $\mathcal{M}/p\mathcal{M}$ is a field)

GOAL: Given $n \in \mathcal{M}$ what can we say on the model theory of $\mathcal{M}/n\mathcal{M}$?

- $n = p$ (Macintyre, 1982)

- $n = p^k$, where $p, k \in \mathcal{M}$, p is a prime and $k > 1$
(D'A. and Macintyre, 2017 $<$ ... ?)

- $1 < n$ composite
(D'A. and Macintyre 2022 $<$ ... ?)

For 2) we use mainly AKE principle in valuation theory.

2) and 3) are connected via (a kind of "converse" of) Feferman-Vaught Theorem (1959)

Let $\mathcal{M} \models PA$ non standard, and $p \in \mathcal{M}$ then

p is prime iff p is irreducible iff p is maximal (i.e. $\mathcal{M}/p\mathcal{M}$ is a field)

GOAL: Given $n \in \mathcal{M}$ what can we say on the model theory of $\mathcal{M}/n\mathcal{M}$?

• $n = p$ (Macintyre, 1982)

• $n = p^k$, where $p, k \in \mathcal{M}$, p is a prime and $k > 1$
(D'A. and Macintyre, 2017 $<$ ... ?)

• $1 < n$ composite
(D'A. and Macintyre 2022 $<$ ... ?)

For 2) we use mainly AKE principle in valuation theory.

2) and 3) are connected via (a kind of "converse" of) Feferman-Vaught Theorem (1959)

$n = p$ **prime**

1) If p is standard then $\mathcal{M}/p\mathcal{M} \cong \mathbb{F}_p$

2) If p is non standard then $\mathcal{M}/p\mathcal{M}$ is a *pseudofinite fields*, i.e.

- characteristic 0 field, hence perfect
- has a unique extension of each degree $m \geq 1$
- p.a.c., i.e. every absolutely irreducible curve over $\mathcal{M}/p\mathcal{M}$ has a $\mathcal{M}/p\mathcal{M}$-rational point

By Ax, $\mathcal{M}/p\mathcal{M}$ is an infinite model of the theory of finite fields, equivalently, it is elementarily equivalent to a non-principal ultraproduct of finite fields, equivalently it is elementarily equivalent to a non-principal ultraproduct of prime finite fields.

$n = p$ **prime**

1) If p is standard then $\mathcal{M}/p\mathcal{M} \cong \mathbb{F}_p$

2) If p is non standard then $\mathcal{M}/p\mathcal{M}$ is a *pseudofinite fields*, i.e.

- characteristic 0 field, hence perfect
- has a unique extension of each degree $m \geq 1$
- p.a.c., i.e. every absolutely irreducible curve over $\mathcal{M}/p\mathcal{M}$ has a $\mathcal{M}/p\mathcal{M}$-rational point

By Ax, $\mathcal{M}/p\mathcal{M}$ is an infinite model of the theory of finite fields, equivalently, it is elementarily equivalent to a non-principal ultraproduct of finite fields, equivalently it is elementarily equivalent to a non-principal ultraproduct of prime finite fields.

$n = p$ prime

1) If p is standard then $\mathcal{M}/p\mathcal{M} \cong \mathbb{F}_p$

2) If p is non standard then $\mathcal{M}/p\mathcal{M}$ is a *pseudofinite fields*, i.e.

- characteristic 0 field, hence perfect
- has a unique extension of each degree $m \geq 1$
- p.a.c., i.e. every absolutely irreducible curve over $\mathcal{M}/p\mathcal{M}$ has a $\mathcal{M}/p\mathcal{M}$-rational point

By Ax, $\mathcal{M}/p\mathcal{M}$ is an infinite model of the theory of finite fields, equivalently, it is elementarily equivalent to a non-principal ultraproduct of finite fields, equivalently it is elementarily equivalent to a non-principal ultraproduct of prime finite fields.

$n = p$ **prime**

1) If p is standard then $\mathcal{M}/p\mathcal{M} \cong \mathbb{F}_p$

2) If p is non standard then $\mathcal{M}/p\mathcal{M}$ is a *pseudofinite fields*, i.e.

- characteristic 0 field, hence perfect
- has a unique extension of each degree $m \geq 1$
- p.a.c., i.e. every absolutely irreducible curve over $\mathcal{M}/p\mathcal{M}$ has a $\mathcal{M}/p\mathcal{M}$-rational point

By Ax, $\mathcal{M}/p\mathcal{M}$ is an infinite model of the theory of finite fields, equivalently, it is elementarily equivalent to a non-principal ultraproduct of finite fields, equivalently it is elementarily equivalent to a non-principal ultraproduct of prime finite fields.

$n = p^k$

Remark. The expression p^k has an unambigous meaning in any model $\mathcal{M}$ of PA since there is a formula $\theta(x, y, z)$ (in fact a Δ_0-formula) in the language of PA that defines the graph of exponentiation in any model of PA.

The p-adic valuation v_p on $\mathcal{M}$ induces in a natural way a valuation v (a *truncated valuation*) on $\mathcal{M}/p^k\mathcal{M}$ which takes values in $[0, k]$ which is a Presburger TOAG.

TOAG =Truncated Ordered Abelian Groups

• Axiomatization in the language containing $+, <, 0, \tau$
• Characterization of a Presburger TOAG
• A Presburger TOAG is completely determined by the type of the penultimate element.

(D'A., Derakhshan and Macintyre, 2021).

$n = p^k$

Remark. The expression p^k has an unambigous meaning in any model $\mathcal{M}$ of PA since there is a formula $\theta(x, y, z)$ (in fact a Δ_0-formula) in the language of PA that defines the graph of exponentiation in any model of PA.

The p-adic valuation v_p on $\mathcal{M}$ induces in a natural way a valuation v (a *truncated valuation*) on $\mathcal{M}/p^k\mathcal{M}$ which takes values in $[0, k]$ which is a Presburger TOAG.

TOAG =Truncated Ordered Abelian Groups

- Axiomatization in the language containing $+, <, 0, \tau$
- Characterization of a Presburger TOAG
- A Presburger TOAG is completely determined by the type of the penultimate element.

(D'A., Derakhshan and Macintyre, 2021).

$n = p^k$

Remark. The expression p^k has an unambigous meaning in any model $\mathcal{M}$ of PA since there is a formula $\theta(x, y, z)$ (in fact a Δ_0-formula) in the language of PA that defines the graph of exponentiation in any model of PA.

The p-adic valuation v_p on $\mathcal{M}$ induces in a natural way a valuation v (a *truncated valuation*) on $\mathcal{M}/p^k\mathcal{M}$ which takes values in $[0, k]$ which is a Presburger TOAG.

TOAG =Truncated Ordered Abelian Groups

- Axiomatization in the language containing $+, <, 0, \tau$
- Characterization of a Presburger TOAG
- A Presburger TOAG is completely determined by the type of the penultimate element.

(D'A., Derakhshan and Macintyre, 2021).

$n = p^k$

Remark. The expression p^k has an unambigous meaning in any model $\mathcal{M}$ of *PA* since there is a formula $\theta(x, y, z)$ (in fact a Δ_0-formula) in the language of *PA* that defines the graph of exponentiation in any model of *PA*.

The *p*-adic valuation v_p on $\mathcal{M}$ induces in a natural way a valuation v (a *truncated valuation*) on $\mathcal{M}/p^k\mathcal{M}$ which takes values in $[0, k]$ which is a Presburger TOAG.

TOAG =Truncated Ordered Abelian Groups

- Axiomatization in the language containing $+, <, 0, \tau$
- Characterization of a Presburger TOAG
- A Presburger TOAG is completely determined by the type of the penultimate element.

(D'A., Derakhshan and Macintyre, 2021).

$\mathcal{M}/p^k\mathcal{M}$ is a Henselian local ring for any $p, k \in \mathcal{M}$

The residue field of $\mathcal{M}/p^k\mathcal{M}$ is either $\mathbb{F}_p$ if p is standard, or a characteristic 0 pseudofinite field if p nonstandard.

The principal ideals of $\mathcal{M}/p^k\mathcal{M}$ are generated by p^j for $0 < j \leq k$, and are linearly ordered by the divisibility condition with minimum (0) and maximum (p)

$\mathcal{M}/p^k\mathcal{M} \cong R/(x)$ where R is a henselian valuation domain of characteristic 0, unramified, the same residue field, and the value group Γ of R is a $\mathbb{Z}$-group (i.e. a model of Presburger), x a non unit in R.

If $\mathcal{M}$ is nonstandard then we have two cases

Case 1. If p is standard then $\mathcal{M}/p^k\mathcal{M}$ is isomorphic to $S/\alpha S$ where $S \equiv \mathbb{Z}_p$ and $\alpha \in S$ non unit

Case 2. If p is nonstandard then $\mathcal{M}/p^k\mathcal{M}$ is isomorphic to $S/\alpha S$ where $S \equiv k[[\Gamma]]$ where k is a pseudofinite field of characteristic 0 and Γ is a $\mathbb{Z}$-group and $\alpha \in S$ non unit

Conversely, any such $S/\alpha S$ is elementarily equivalent to some $\mathcal{M}/p^k\mathcal{M}$ for some $\mathcal{M}$ model of PA.

Theorem

Suppose S is as in Cases 1 and Case 2 above, and α is a non-unit and $\alpha \neq 0$. Then $S/\alpha S$ is elementarily equivalent to an ultraproduct of $\mathbb{Z}/p^k\mathbb{Z}$, for p prime and $k > 0$.

Corollary

The elementary theories of the $\mathcal{M}/p^k\mathcal{M}$ are exactly the elementary theories of the $S/\alpha S$ not a unit

Theorem

1. $\mathcal{M}/p^k\mathcal{M}$ are pseudofinite (or finite) rings.
2. The theory of the class $\{\mathcal{M}/p^k\mathcal{M} : p, k \in \mathcal{M},\ p \text{ prime},\ k > 0\}$ coincides with the theory of the class $\{\mathbb{Z}/p^m\mathbb{Z} : p, m \in \mathbb{Z}\ p \text{ prime},\ m > 0\}$.
3. The theory of the class $\{\mathcal{M}/p^k\mathcal{M} : p, k \in \mathcal{M},\ p \text{ prime},\ k > 0\}$ is decidable (by Ax)

n composite:

1. $n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$ where s is standard
2. $n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$ where s is nonstandard

Case 1: this is straightfoward since

$$\mathcal{M}/n\mathcal{M} \cong \mathcal{M}/p_1^{k_1}\mathcal{M} \times \ldots \times \mathcal{M}/p_s^{k_s}\mathcal{M}$$

Case 2: $\mathcal{M}/n\mathcal{M} \ncong \prod_{i \leq s} \mathcal{M}/p_i^{k_i}\mathcal{M}$ but we proved

$$\mathcal{M}/n\mathcal{M} \equiv \prod_{i \leq s} \mathcal{M}/p_i^{k_i}\mathcal{M}$$

Question: When is a commutative unital ring R elementarily equivalent to $\prod_{i \in I} R_i$ for some commutative unital rings R_i's?

We isolate a set of axioms in the ring language, whose models are exactly the rings which are elementarily equivalent to a product of connected unital rings (D'A. and Macintyre, 2023)

A commutative unital ring R is connected if the only idempotents ($x^2 = x$) are 0 and 1, and $0 \neq 1$.

Examples: integral domains, local rings

It turns out that $\mathcal{M}/n\mathcal{M}$ is a model of our axioms.

Theorem (Fefermann-Vaught, 1959)

There is an effective procedure such that to any $\mathcal{L}$-formula $\theta(x_0,\ldots,x_k)$ it associates a formula $\Phi(y_0,\ldots,y_m)$ in the language of Boolean algebras $\mathcal{L}_B$ and a *partition*

$$(\theta_0(x_0,\ldots,x_k),\ldots,\theta_m(x_0,\ldots,x_k))$$

of $\mathcal{L}$-formulas such that for any given family of $\mathcal{L}$-structures $(\mathcal{A}_i)_{i\in I}$ and any $\bar{f}\in\prod_{i\in I}\mathcal{A}_i$

$$\prod_{i\in I}\mathcal{A}_i\models\theta(\bar{f}) \quad \text{iff} \quad \mathcal{P}(I)\models\Phi([\![\theta_0(\bar{f})]\!],\ldots,[\![\theta_m(\bar{f})]\!]),$$

where $[\![\varphi(\bar{f})]\!]=\{i\in I:\mathcal{A}_i\models\varphi(\overline{f(i)})\}$ for any $\mathcal{L}$-formula φ.

If $R = \prod_{i \in I} R_i$ where R_i are connected then the Boolean algebra $\mathcal{P}(I)$ is the set of idempotents of R (connectness of R_i is crucial), with a natural Boolean structure defined on it, and it is easily interpretable in R.

If R is a commutative unital ring

- $\mathbb{B}$ is the Boolean algebra of idempotents of R
- R_e (the fibers) for each idempotent e of R, and

$$R_e \text{ is connected iff } e \text{ is an atom}$$

We work in a **one sorted** language, the ring language.

Theorem (DM)

For every $\mathcal{L}_{rings}$-formula $\theta(x_0, \ldots, x_k)$ there is a partition $(\theta_0(x_0, \ldots, x_k), \ldots, \theta_m(x_0, \ldots, x_k))$ of ring formulas, and a Boolean algebra formula $\psi(y_0, \ldots, y_m)$ so that for all $f_0, \ldots, f_k \in R$, where R is a ring satisfying *AXIOMS*, and $\mathbb{B}$ is the Boolean algebra of idempotents of R

$$R \models \theta(\overline{f}) \qquad \text{iff} \qquad \mathbb{B} \models \psi([\![\theta_0(\overline{f})]\!], \ldots, [\![\theta_m(\overline{f})]\!]) \tag{1}$$

where $\overline{f} = f_0, \ldots, f_k$.

Corollary

If R is a commutative unital ring and a model of *AXIOMS* then $R \equiv \prod_e R_e$, e atoms of $\mathbb{B}$.

Theorem

$\mathcal{M}/n\mathcal{M}$ is a model of *AXIOMS*.

Theorem (CRT)

Let $\mathcal{M}$ be a model of PA and A a bounded Δ_0-definable set in $\mathcal{M}$. Let f and r be Δ_0-functions such that $f(a_1), f(a_2)$ are pairwise coprime for all $a_1, a_2 \in A$ and $a_1 \neq a_2$, and $r(a) < f(a)$ for all $a \in A$. Suppose there exists $w \in \mathcal{M}$ divisible by all elements of $f(A)$. Then there exists $u < \prod_{a \in A} f(a)$ such that $u \equiv r(a) (\text{mod } f(a))$ for all $a \in A$.

Let Q be the set of maximal prime powers q dividing n.

$r \in \mathcal{M}/n\mathcal{M}$ is an idempotent iff for each $q \in Q$, q divides $r^2 - r$, so q divides one, and only one, of r or $r - 1$.

The atoms in $\mathbb{B}$ are those r s.t. for a unique $q \in Q$, $r \equiv 1 (\text{mod } q)$, and $r \equiv 0 (\text{mod } q')$ for all other $q' \in Q$.
By Δ_0-CRT there are such r for each q.

The idempotents in $\mathbb{B}$ are identified with (Δ_0-definable) subsets of Q

The atoms correspond to the subsets $Q - \{q\}$, as q varies in Q.

To each atom e we associate the unique prime power q_e such that $q_e \not| e$.

It is easy to show now that

$$(\mathcal{M}/n\mathcal{M})_e \cong \mathcal{M}/q_e\mathcal{M}.$$

So, the elements of the localized ring at e can be identified with elements of $\mathcal{M}$ which are $< q_e \leq n$.

Note that $\mathcal{M}/n\mathcal{M}$ and the full product $\prod_{q \in Q} \mathcal{M}/q\mathcal{M}$ have the same idempotents.

CRT is crucial for showing that the ring $\mathcal{M}/n\mathcal{M}$ satisfies our axioms. So,

$$\mathcal{M}/n\mathcal{M} \equiv \prod_{q \in Q} \mathcal{M}/q\mathcal{M}$$

An $\mathcal{L}$-structure $\mathcal{M}$ is pseudofinite* if every $\mathcal{L}$-sentence true in $\mathcal{M}$ is true in some finite $\mathcal{L}$-structure.

This is equivalent to saying that $\mathcal{M}$ is elementarily equivalent to an ultraproduct of finite $\mathcal{L}$-structures.

Theorem (D'A and Macintyre, 2024)

Let I be an index set (either finite or infinite). If $(\mathcal{M}_i)_{i \in I}$ are pseudofinite* $\mathcal{L}$-structures then $\prod_{i \in I} \mathcal{M}_i$ is pseudofinite*.

Corollary

$\mathcal{M}/n\mathcal{M}$ is a pseudofinite structure.