Generalizations of the Grunwald-Wang Theorem and Applications to Ramsey Theory

Howard University Mathematics Colloquium

Based on http://math.colgate.edu/ integers/x18/x18.pdf

Sohail Farhangi (joint work with Richard Magner)
Slides available on sohailfarhangi.com

September 1, 2023

Overview

Table of Contents

The Grunwald-Wang Theorem

Exercise: Suppose that $x \in \mathbb{Z}$ is such that $x = y^2 \pmod{p}$ has a solution for every prime p. Show that x is a perfect square.

Theorem

Let $n \in \mathbb{N}$ be arbitrary and suppose that $x \in \mathbb{Z}$ is such that x is an nth power modulo p for every prime p. x is either an nth power or $8|n$ and $x = 2^{\frac{n}{2}}y^n = 16^{\frac{n}{8}}y^n$.

W. Grunwald [7] in 1933 proved an incorrect version of this theorem since he failed to find the exceptional case when $8|n$. G. Whaples [15] in 1942 gave another incorrect proof of Grunwald's Theorem. S. Wang [13],[14] in 1948 found the counter example of 16 and gave a proof of the corrected theorem in his doctoral thesis.

The Exceptional case of $x = 16$

It is clear that $16 = 2^4$ is not an 8th power in $\mathbb{N}$. To see that 16 is an 8th power modulo p for every prime p, we observe that

$$x^8 - 16 = (x^4 - 4)(x^4 + 4) = (x^2 - 2)(x^2 + 2)(x^2 - 2x + 2)(x^2 + 2x + 2)$$

We note that the discriminant of the last 2 factors is -4. Since one of $2, -2$, and -4 will be a square modulo p, we see that $x^8 - 16$ will have a root modulo p.

The Grunwald-Wang Theorem intuitively says that 16 is the only obstruction to a certain local-global principle.

Grunwald-Wang for 3 Variables

Theorem (F., Magner, 2023)

Let $n \in \mathbb{N}$ be arbitrary and suppose that $a, b, c \in \mathbb{Z}$ are such that at least one of a, b, and c is an nth power modulo p for every prime p. Then either

1. *n is odd and one of a, b, and c is an nth power.*
2. *n is even and either one of a, b, and c is an $\frac{n}{2}$th power, or $4|n$ and each of a, b, and c is an $\frac{n}{4}$th power.*

In our paper we also address the situation for a general number field K with ring of integers $\mathcal{O}_K$.

This number theory is needed because one of the most commonly used partitions in the Ramsey Theory of diophantine equations are the Rado c_p-partitions. Given a prime p, the c_p-partition is $\mathbb{N} = \bigcup_{i=1}^{r} C_i$ where C_i consists of those natural numbers whose first non-zero digit in the base p expansion is i.

Some Exceptional Cases

It is clear that we still have an exceptional case if $8|n$ and one of a, b, and c is of the form $2^{\frac{n}{2}}y^n$.

A new exceptional case is found with $n = 4$, $a = 3^4 \cdot 4^2 \cdot 5^2$, $b = 3^2 \cdot 4^4 \cdot 5^2$, and $c = a + b = 3^2 \cdot 4^2 \cdot 5^4$.

There are more exceptional cases that actually show up from the 2 variable situation.

Table of Contents

Ramsey Theory Preliminaries

Definition

If $p \in \mathbb{Z}[x_1, \cdots, x_n]$ is a polynomial and S is a set such as $\mathbb{N}$, $\mathbb{Z} \setminus \{0\}$, or the ring of integers $\mathcal{O}_K$ of some number field K, then the equation

$$p(x_1, \cdots, x_n) = 0 \tag{1}$$

is **partition regular (p.r.) over** S if for any partition $S = \sqcup_{i=1}^r C_i$ there exists $1 \leq i_0 \leq r$ and $x_1, \cdots, x_n \in C_{i_0}$ satisfying (1).

The equation $x + y = 2z + 1$ is **NOT** partition regular over $\mathbb{N}$ as seen by considering the partition $\mathbb{N} = (2\mathbb{N}) \sqcup (2\mathbb{N} + 1)$.
The equation $x + y = z$ **is** partition regular over $\mathbb{N}$, and this can be proven using Ramsey's theorem about complete graphs.

Polynomial Equations and Partition Regularity

1. $x + y = z$ is p.r. over $\mathbb{N}$ (Schur [12])
2. $xy = z$ is p.r. over $\mathbb{N}$ (corollary of Schur)
3. $ax + by = dz$ is p.r. over $\mathbb{N}$ if and only if $d \in \{a, b, a+b\}$ (special case of Rado's Theorem [10])
4. $ax = wz^n$ is p.r. over $\mathbb{N}$ if and only if $\sqrt[n]{a} \in \mathbb{N}$. (See [3])
5. $x + y = wz$ is p.r. over $\mathbb{N}$ (Bergelson-Hindman [2],[8])
6. $x - y = q(z)$ with $q \in x\mathbb{Z}[x]$ is p.r. over $\mathbb{N}$ (Bergelson [1, Page 53])
7. $x + y = z^2$ is not non-trivially p.r. over $\mathbb{N}$ (Csikvári, Gyarmati and Sárkozy [4], see also Green and Lindqvist [6])
8. It is open as to whether $x^2 + y^2 = z^2$ is p.r. over $\mathbb{N}$ [5].
9. It is open as to whether $z = xy + x$ is p.r. over $\mathbb{N}$ [11].
10. $z = x^y$ is p.r. over $\mathbb{N}$, but $z = x^{y+1}$ is open. Sahasrabudhe [11]

Table of Contents

When is $ax + by = cw^m z^n$ p.r.?

Theorem (F., Magner 2022)

Let $m, n \in \mathbb{N}$ and $a, b, c \in \mathbb{Z} \setminus \{0\}$.

1. *If $m, n \geq 2$, then the equation*
$$ax + by = cw^m z^n \tag{2}$$
is p.r. over $\mathbb{Z} \setminus \{0\}$ if and only if $a + b = 0$.
2. *If one of $\frac{a}{c}$, $\frac{b}{c}$, or $\frac{a+b}{c}$ is a nth power in $\mathbb{Q}$, then the equation*
$$ax + by = cwz^n \tag{3}$$
is p.r. over $\mathbb{Z} \setminus \{0\}$. If $\mathbb{Q}$ is replaced with $\mathbb{Q}^+$ then $\mathbb{Z} \setminus \{0\}$ can be replaced with $\mathbb{N}$. This holds when $\mathbb{Z}$ and $\mathbb{Q}$ are replaced by a general integral domain R and its field of fractions K.

When is $ax + by = cw^m z^n$ p.r.? (Continued)

Theorem (F., Magner 2022)

3 *Suppose that*

$$ax + by = cwz^n \tag{4}$$

is p.r. over $\mathbb{Q} \setminus \{0\}$.

- (a) *If n is odd then one of $\frac{a}{c}$, $\frac{b}{c}$, or $\frac{a+b}{c}$ is an nth power in $\mathbb{Q}$.*
- (b) *If $n \neq 4, 8$ is even then one of $\frac{a}{c}$, $\frac{b}{c}$, or $\frac{a+b}{c}$ is a $\frac{n}{2}$th power in $\mathbb{Q}$. We used Fermat's Last Theorem here!*
- (c) *If n is even, then either one of $\frac{a}{c}$, $\frac{b}{c}$, or $\frac{a+b}{c}$ is a square in $\mathbb{Q}$, or $(\frac{a}{c})(\frac{b}{c})(\frac{a+b}{c})$ is a square in $\mathbb{Q}$.*

Table of Contents

Examples

$$-x - y = wz \text{ is p.r. over } \mathbb{Z} \setminus \{0\} \text{ but not } \mathbb{N}. \tag{5}$$

$$-8x + 2y = wz^3 \text{ is p.r. over } \mathbb{Z} \setminus \{0\}, \text{ but what about } \mathbb{N}? \tag{6}$$

$$4x + 5y = 2wz^2 \text{ is p.r. over } \mathbb{N}[\sqrt{2}] \text{ but not } \mathbb{Z} \setminus \{0\}. \tag{7}$$

$$3^4 \cdot 4^2 \cdot 5^2 x + 3^2 \cdot 4^4 \cdot 5^2 y = wz^4 \text{ is not p.r. over } \mathbb{Z} \setminus \{0\}. \tag{8}$$

(In light of slide 7, this result required additional work.)

More Examples

$$16x + 17y = wz^8 \text{ remains open.} \tag{9}$$

$$(2^{12} - 33)x + 33y = wz^8 \text{ remains open.} \tag{10}$$

$$\begin{aligned} 16x_1 + 17y_1 &= w_1 z_1^8 \\ (2^{12} - 33)x_2 + 33y_2 &= w_2 z_2^8 \text{ is not p.r. over } \mathbb{Z} \setminus \{0\} \text{ as a system.} \end{aligned} \tag{11}$$

$$\begin{aligned} 16x_1 + 17y_1 &= w_1 z_1^8 \\ 33x_2 - 17y_2 &= w_2 z_2^8 \text{ remains open.} \end{aligned} \tag{12}$$

Table of Contents

Ultrafilters

Definition

Let S be a set. $p \subseteq \mathcal{P}(S)$ is an *ultrafilter* if it satisfies the following properties:

1. (i) The empty set is not a member of p, i.e., $\emptyset \notin p$,
2. (ii) if $A \in p$ and $A \subseteq B$ then $B \in p$,
3. (iii) if $A, B \in p$ then $A \cap B \in p$,
4. (iv) for any $A \subseteq S$, either $A \in p$ or $A^c \in p$.

Ultrafilters on S can also be viewed as finitely additive $\{0,1\}$-valued measures on the collection of subsets of S. They are useful in the study of Ramsey Theory, because if $S = \bigcup_{i=1}^{r} C_i$ is a finite partition and p is an ultrafilter, then there exists exactly one $1 \leq i_0 \leq r$ for which $C_{i_0} \in p$ (see also [9, Theorem 5.7]).

The Stone-Čech Compactification of a semigroup

Let $(S, \cdot)$ be a discrete semigroup and let βS denote the Stone-Čech compactification of S. In other words, βS is a compact Hausdorff space into which S embeds. Furthermore, if X is a compact Hausdorff space and $f : S \to X$ is a function, then there exists a unique continuous function $\tilde{f} : \beta S \to X$ for which $\tilde{f}|_S \equiv f$. The semigroup operatoration of S can be extended to a semigroup operation on βS in a natural fashion, and we once again denote the extended operation by $\cdot$. We let $K(\beta S, \cdot)$ denote the smallest ideal of $(\beta S, \cdot)$, and we let $E(K(\beta S, \cdot))$ denote the idempotent elements of $K(\beta S, \cdot)$. It is well known that the points of βS can be taken to be ultrafilters on S, so a minimal idempotent ultrafilter p refers to an element of $E(K(\beta S, \cdot))$. When working with structures such as $\mathbb{N}$ that naturally admit two different semigroup structures, we may also speak of additively minimal idempotent ultrafilters versus multiplicatively minimal idempotent ultrafilters.

Applications to Ramsey Theory

While $\overline{E(K(\beta\mathbb{N},+))} \cap E(K(\beta\mathbb{N},\cdot)) = \emptyset$, there exists $p \in \overline{E(K(\beta\mathbb{N},+))} \cap E(K(\beta\mathbb{N},\cdot))$. For $A \in p$, there exists

1. $x, y, z \in A$ satisfying $x + y = z$,
2. $x, y, z \in A$ satisfying $xy = z$,
3. $x, y, z \in A$ satisfying $ax + by = dz$ provided $d \in \{a, b, a + b\}$,
4. $x, w, z \in A$ satisfying $ax = wz^n$ provided $\sqrt[n]{a} \in \mathbb{N}$,
5. $w, x, y, z \in A$ satisfying $x + y = wz$,
6. $x, y, z \in A$ satisfying $x - y = p(z)$ provided $p(z) \in z\mathbb{Z}[z]$.

In particular, all of the positive results of slide 10 can be proven using the special ultrafilter p. Consequently, we would like to know what other integral domains possess such a special ultrafilter p.

Homomorphically finite integral domains

Definition

An integral domain R is **Homorphically finite** if for each $r \in R \setminus \{0\}$ we have $[R : rR] < \infty$. Equivalently, R is **Homomorphically finite** if every non-injective ring homomorphism $\phi : R \to R'$ has finite image.

If R is the ring of integers of a finite extension K of $\mathbb{Q}$, then R is homomorphically finite. On the otherhand, if R is an infinite integral domain, then $R[x]$ is not homomorphically finite.

Theorem (F., Magner, 2023)

1. *If the integral domain R is a homomorhpically finite, then*
$$\overline{E(K(\beta R,+))} \cap E(K(\beta R,\cdot)) \neq \emptyset. \tag{13}$$
2. *If the integral domain R is not homomorhpically finite, then*
$$\overline{E(K(\beta R,+))} \cap \overline{E(K(\beta R,\cdot))} = \emptyset. \tag{14}$$

References I

[1] V. Bergelson.
Ergodic Ramsey theory—an update.
In *Ergodic theory of* $\mathbf{Z}^d$ *actions (Warwick, 1993–1994)*, volume 228 of *London Math. Soc. Lecture Note Ser.*, pages 1–61. Cambridge Univ. Press, Cambridge, 1996.

[2] V. Bergelson.
Ultrafilters, IP sets, dynamics, and combinatorial number theory.
In *Ultrafilters across mathematics*, volume 530 of *Contemp. Math.*, pages 23–47. Amer. Math. Soc., Providence, RI, 2010.

[3] J. Byszewski and E. Krawczyk.
Rado's theorem for rings and modules.
J. Combin. Theory Ser. A, 180:105402, 28, 2021.

References II

[4] P. Csikvári, K. Gyarmati, and A. Sárközy.
Density and Ramsey type results on algebraic equations with restricted solution sets.
Combinatorica, 32(4):425–449, 2012.

[5] P. Erdős and R. L. Graham.
Old and new problems and results in combinatorial number theory, volume 28 of *Monographies de L'Enseignement Mathématique [Monographs of L'Enseignement Mathématique]*.
Université de Genève, L'Enseignement Mathématique, Geneva, 1980.

[6] B. J. Green and S. Lindqvist.
Monochromatic solutions to $x + y = z^2$.
Canad. J. Math., 71(3):579–605, 2019.

References III

[7] W. Grunwald.
Ein allgemeiner existenzsatz für algebraische zahlkörper.
Journal für die reine und angewandte Mathematik, 169:103–107, 1933.

[8] N. Hindman.
Monochromatic sums equal to products in $\mathbb{N}$.
Integers, 11(4):431–439, 2011.

[9] N. Hindman and D. Strauss.
Algebra in the Stone-Čech compactification: Theory and applications.
De Gruyter Textbook. Walter de Gruyter & Co., Berlin, second revised and extended edition, 2012.

References IV

[10] R. Rado.
Studien zur Kombinatorik.
Math. Z., 36(1):424–470, 1933.

[11] J. Sahasrabudhe.
Exponential patterns in arithmetic Ramsey theory.
Acta Arith., 182(1):13–42, 2018.

[12] I. Schur.
Uber die kongruenz $x^m + y^m = z^m \pmod{p}$.
Jahresber. Dtsch. Math, 25:114–117, 1916.

[13] S. Wang.
A counter-example to Grunwald's theorem.
Ann. of Math. (2), 49:1008–1009, 1948.

References V

[14] S. Wang.
On Grunwald's theorem.
Ann. of Math. (2), 51:471–484, 1950.

[15] G. Whaples.
Non-analytic class field theory and Grünwald's theorem.
Duke Math. J., 9:455–473, 1942.