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

9th Polish Combinatorial Conference

Based on https://arxiv.org/abs/2105.02190

(To appear)

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

September 20, 2022

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 in 1933 proved an incorrect version of this theorem since he failed to find the exceptional case when $8|n$. G. Whaples in 1942 gave another incorrect proof of Grunwald's Theorem. S. Wang 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)

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 $\mathcal{O}_K$.

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.

Ramsey Theory Preliminaries

Definition

If $p \in \mathbb{Z}[x_1, \cdots, x_n]$ is a polynomial and S is a set such as $\mathbb{N}$, $\mathbb{Z}$, 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).

Polynomial Equations and Partition Regularity

1. $x + y = z$ is p.r. over $\mathbb{N}$ (Schur)
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)
4. $x + y = wz$ is p.r. over $\mathbb{N}$ (Bergelson-Hindman)
5. $x - y = q(z)$ with $q \in x\mathbb{Z}[x]$ is p.r. over $\mathbb{N}$ (Bergelson)
6. $x + y = z^2$ is not non-trivially p.r. over $\mathbb{N}$ (Csikvári, Gyarmati and Sárkozy)
7. It is open as to whether $x^2 + y^2 = z^2$ is p.r. over $\mathbb{N}$.
8. It is open as to whether $z = xy + x$ is p.r. over $\mathbb{N}$.
9. $z = x^y$ is p.r. over $\mathbb{N}$ but $z = x^{y+1}$ remains open (Sahasrabudhe).

Our Main Result

Theorem

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 $\mathbb{Z}$ 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 $\mathbb{Z}$. If $\mathbb{Q}$ is replaced with $\mathbb{Q}^+$ then $\mathbb{Z}$ can be replaced with $\mathbb{N}$. This holds when $\mathbb{Z}$ and $\mathbb{Q}$ are replaced by a general integral domain R its field of fractions K.

Our Main Result (Continued)

Theorem

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 $\mathbb{Q}$.*

Examples

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

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

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

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

(In light of slide 5, this result required additional work.)

More Examples

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

The live talk ended here.

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

$$\begin{aligned} 16x_1 + 17y_1 &= w_1z_1^8 \\ (2^{12} - 33)x_2 + 33y_2 &= w_2z_2^8 \text{ is not p.r. over } \mathbb{Z} \text{ as a system.} \end{aligned} \tag{11}$$

$$\begin{aligned} 16x_1 + 17y_1 &= w_1z_1^8 \\ 33x_2 - 17y_2 &= w_2z_2^8 \text{ remains open} \end{aligned} \tag{12}$$

Proof Sketch of 1

Suppose that $m, n \geq 2$. To show that $ax + by = cw^m z^n$ is not partition regular when $b \neq -a$, we use the nonlinear Rado conditions of Barrett, Lupini, and Moreira. For the converse we observe that

$$ax - ay = cwz^n \text{ is p.r. } \Leftarrow a(ax) - a(ay) = (aw)^m(az)^n \text{ is p.r.}$$

$$\Leftarrow x - y = ca^{m+n-2}w^m z^n \text{ is p.r. } \Leftarrow x - y = ca^{m+n-2}z^{m+n} \text{ is p.r.}$$

Proof Sketch of 2

If $\gamma^n \in \{\frac{a}{c}, \frac{b}{c}, \frac{a+b}{c}\}$ for some $\gamma \in \mathbb{Q}$, then

$$ax + by = cwz^n \text{ is p.r. iff } a\gamma x + b\gamma y = c\gamma w(\gamma z)^n \text{ is p.r.} \tag{13}$$

$$\Leftrightarrow ax + by = dwz^n \text{ is p.r. for some } d \in \{a, b, a+b\} \tag{14}$$

$$\Leftarrow ax + by = dw \text{ is p.r. for some } d \in \{a, b, a+b\}. \tag{15}$$

Proof Sketch of 3

For a prime p we may construct the partition $\mathbb{N} = \sqcup_{i=1}^{p-1} C_i$, where C_i is the set of all integers whose first non-zero digit in its base p expansion is i. If p is a prime for which none of ac^{-1}, bc^{-1}, or $(a+b)c^{-1}$ are nth powers modulo p, then this partition contains no solutions to

$$ax + by = cwz^n. \tag{16}$$

It now suffices to apply our generalization of the Grunwald-Wang Theorem. We obtain similar results for rings of integers $\mathcal{O}_K$ of number fields K, and some of these results also have analogues over a general integral domain R.