

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

Kraków Summer School in Combinatorics
at AGH University

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

Sohail Farhangi

(joint work with Richard Magner)

July 6, 2022

A local-global principle for squares

Exercise: Show that if $x \in \mathbb{Z}$ is a perfect square $(\bmod p)$ for every prime p , then x is a perfect square.

Hint: Use quadratic reciprocity and the chinese remainder theorem.

The Grunwald-Wang Theorem

Theorem

Let $n \in \mathbb{N}$ be arbitrary and suppose that $x \in \mathbb{Z}$ is such that x is an n th power modulo p for every prime p . x is either an n th 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 the local-global principle for being an n th power.

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 n th power modulo p for every prime p . Then either

- ① *n is odd and one of a, b , and c is an n th 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 arxiv 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 $p \in \mathbb{Z}[x_1, \dots, x_n]$ is a polynomial and S is either \mathbb{N} or \mathbb{Z} , then the equation

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

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 $x_1, \dots, x_n \in C_{i_0}$ 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} .

The equation $ax + by = cw^m z^n$

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 n th 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} .

The equation $ax + by = cw^m z^n$ (Continued)

Theorem

3 Suppose that

$$ax + by = cwz^n \quad (4)$$

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 n th 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} .

Similar results are obtained for systems of equations with coefficients coming from an integral domain R .

Examples, Non-examples, Open Problems

- ① $8x + 3y = wz^3$ is p.r.
- ② $3x + 13y = 2wz^3$ is p.r.
- ③ $2x + 3y = wz^n$ is not p.r. for any $n \geq 1$
- ④ $3^4 \cdot 4^2 \cdot 5^2 x + 3^2 \cdot 4^4 \cdot 5^2 y = wz^4$ is not p.r.
- ⑤ $16x + 17y = wz^8$ is **conjectured** to not be p.r.
- ⑥ $x + y = -wz$ is p.r. over \mathbb{Z} but not over \mathbb{N}
- ⑦ $2x - 10y = wz^3$ is p.r. over \mathbb{Z} but **we do not know whether it is p.r. over \mathbb{N} .**
- ⑧ $2x + 3y = wz^2$ is p.r. over $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$, $\mathbb{Z}[\sqrt{5}]$, but not \mathbb{Q}_{197}
- ⑨ $2x - 2\sqrt{2}y = wz^3$ is p.r. over $\mathbb{Z}[\sqrt{2}]$, but how about over $\mathbb{Z}[\sqrt{2}]_{\geq 0}$, or the cone of totally positive elements of $\mathbb{Z}[\sqrt{2}]$?

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

$$ax + by = cwz^n \text{ is p.r. iff } a\gamma x + b\gamma y = c\gamma w(\gamma z)^n \text{ is p.r.} \quad (5)$$

$$\Leftrightarrow ax + by = dwz^n \text{ is p.r. for some } d \in \{a, b, a + b\} \quad (6)$$

$$\Leftarrow ax + by = dw \text{ is p.r. for some } d \in \{a, b, a + b\}. \quad (7)$$

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 n th powers modulo p , then this partition contains no solutions to

$$ax + by = cwz^n. \quad (8)$$

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 .

Grunwald-Wang for 2 Variables

Theorem (F., Magner, 2022)

Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$ be such that either

- ① $4 \nmid n$ and neither of a and b are n th powers.*
- ② $4 \mid n$ and neither of a and b are $\frac{n}{2}$ th powers.*

Then there exist infinitely many primes p modulo which neither of a and b are an n th power.

Some More Exceptional Cases

Since 3 is a perfect square mod p if $p \equiv 1 \pmod{3}$ and every integer is a perfect cube mod p if $p \equiv 2 \pmod{3}$, we see that for any $b \in \mathbb{Z}$ one of 3^6 and b^4 will be a 12th power modulo p for any prime p . (Due to Hyde, Lee, and Spearman)

We can break down the Grunwald-Wang exceptional case of 16 by observing that $x^8 - 16 = (x^4 + 4)(x^4 - 4)$, so one of 4 or -4 will be a 4th power modulo p for any prime p .

36 is a 4th power modulo p if $p \not\equiv 13 \pmod{24}$ and 9 is a 4th power modulo p if $p \equiv 13 \pmod{24}$, so one of 36 and 9 will be a 4th power modulo p for any prime p .