A Bridge Between Additive Combinatorics and the Infinitude of Prime Numbers

Hikmet Burak Özcan

İzmir Institute of Technology

19 November 2021

Outline

1. Introduction and Motivation

2. A Quick Survey of Additive Combinatorics and Some Instruments from Additive Combinatorics

3. Our Results

4. References

A **prime number** (or a **prime**) is a natural number greater than 1 that cannot be written as a product of two smaller natural numbers.

Prime numbers have been studied since ancient Greek. They proved two remarkable results:

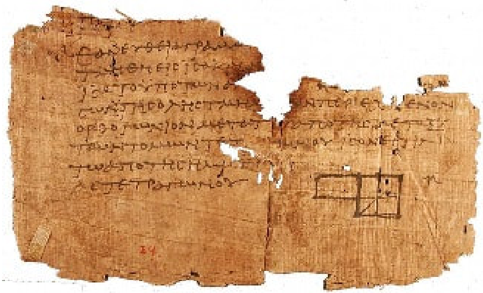

Figure: One of the oldest surviving fragments of Euclid's Elements.

Fundamental Theorem of Arithmetic

Every natural number $n > 1$ is either a prime number or represented as a product of prime numbers

$$n = \prod_{i=1}^{k} p_i^{\alpha_i} = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

where $\alpha_i \in \mathbb{N}$ for all $i = 1, 2, \dots, k$.

Furthermore, this representation is **unique** up to the ordering.

Euclid's Theorem (300 B.C.)

There are infinitely many prime numbers.

A classic *reductio ad absurdum*

Euclid's Proof: Suppose for contradiction that there are only finitely many prime numbers $p_1, p_2, \ldots, p_n$. Multiplying all the prime numbers and adding 1, let us get a new number

$$P = p_1 p_2 \cdots p_n + 1$$

Then, P is a natural number that is greater than 1, however it is not divisible by any prime number. It contradicts the fundamental theorem of arithmetic. Therefore, there must be infinitely many prime numbers.

$\sim$ 2000 years after Euclid

Euler's Theorem (1737)

Analysis **Number Theory**

Let $p_1 < p_2 < \cdots$ be the list of all prime numbers. Then, the series

$$\sum_{i=1}^{\infty} \frac{1}{p_i} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \ldots$$

is divergent.

Leonhard Euler

- **Euler's result** is much stronger than Euclid's.
- **Euler's proof** is based on the connection between prime numbers and infinite series:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{i=1}^{\infty} \left(1 - \frac{1}{p_i^s}\right)^{-1},$$

  where $s > 1$ and p_i denotes the i^{th} prime.
- **Euler's approach** inspired Dirichlet and formed the main idea of *Dirichlet's Theorem on Arithmetic Progressions*.

Dirichlet's Theorem on Arithmetic Progressions (1837)

For any two positive coprime integers a and b, the arithmetic progression

$$a, a+b, a+2b, a+3b, \cdots$$

contains infinitely many primes.

- For instance, there are infinitely many primes of the form **4k + 3** :

$$3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, \cdots$$

- In fact, Dirichlet showed using Euler's idea that

$$\sum_{p \equiv a (mod\ b)} \frac{1}{p},$$

is a divergent series.

- For instance,

$$\sum_{p \equiv 3 (mod\ 4)} \frac{1}{p} = \frac{1}{3} + \frac{1}{7} + \frac{1}{11} + \frac{1}{19} + \frac{1}{23} + \frac{1}{31} + \frac{1}{43} + \cdots$$

is a divergent series.

One of Our Motivations

- Dirichlet's Theorem on Arithmetic Progressions is considered as the beginning of **analytic number theory**.

"*The theorem was never about the theorem. It was always about the proof.* "

-Micheal Bode-

Today, many mathematicians from various branches of the discipline still continue to provide new proofs of both Euclid's and Euler's Theorem.

Some of the most notable proofs of Euclid's Theorem:

- Furstenberg's proof that uses the basic instruments of topology.
- Alpoge's and Granville's proofs that use van der Waerden's Theorem.
- Elsholtz's proofs that uses results from number theory, additive combinatorics, and infinite Ramsey theory.

A subtle proof of Euler's Theorem:

- Erdős' combinatorial proof.

To find more proofs of Euclid's Theorem, we strongly recommend the surveys of Meštrović and Granville.

A Quick Survey of Additive Combinatorics and Some Instruments from Additive Combinatorics

A finite sequence

$$a_1 < a_2 < \cdots < a_k$$

of $k > 1$ numbers is called a **k-term arithmetic progression** if there exists a constant $d > 0$ such that

$$a_{i+1} - a_i = d,$$

for all $i = 1, \ldots, k - 1$.

van der Waerden's Theorem (1927)

If positive integers are colored with finitely many colors,

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \cdots$$

then there exists a monochromatic k-term arithmetic progression for any positive integer $k > 1$.

- This is a very first result in additive combinatorics.

The **upper density of a subset** A of positive integers, which is denoted by $\bar{d}(A)$ and defined as

$$\bar{d}(A) = \limsup_{N\to\infty} \frac{|A \cap \{1, \ldots, N\}|}{N}.$$

- In 1936, Erdős and Turán's conjectured that there exists a 3-term arithmetic progression in every subset of positive integers with positive upper density.
- The Erdős-Turán conjecture was shown by Roth in 1953.
- After that, Szemerédi proved its extended version for $k \geq 4$ and so the extended Erdős-Turán conjecture was referred as **Szemerédi's Theorem**.

One of the Generalizations of Szemerédi's Theorem

Polynomial van der Waerden's Theorem

(Bergelson & Leibman)

Let $p_1, p_2, ..., p_k \in \mathbb{Z}[x]$, where $p_i(0) = 0$ for all $i = 1, 2, \ldots, k$, and let $r \in \mathbb{Z}^+$. For any $r - coloring$ of $\mathbb{Z}$, there exist $a \in \mathbb{Z}$ and $d \in \mathbb{Z} \setminus \{0\}$ such that

$$a, \quad a + p_1(d), \quad a + p_2(d), \quad \cdots, \quad a + p_k(d)$$

are of the same color.

- Indeed, Bergelson & Leibman showed Polynomial van der Waerden's Theorem for an arbitrary integral domain instead of $\mathbb{Z}$.
- They also proved Polynomial Szemerédi's Theorem.

Green - Tao Theorem (2004)

The sequence of prime numbers contains arbitrarily long arithmetic progressions.

- $199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089$ is a 10-term arithmetic progression of primes with difference 210.
- Later, Tao and Ziegler demonstrated the polynomial version of the Green-Tao Theorem.

p-adic Order

Let $a \in \mathbb{Z} \setminus \{0\}$. Given any prime number p, the ***p*-adic order**(or ***p*-adic valuation**) of a is the largest power of p dividing a and it is denoted by $\nu_p(a)$. By convention, $\nu_p(0) = \infty$.
For instance,

- $\nu_2(10) = 1$ & $\nu_2(24) = 3$ & $\nu_2(10{+}24) = 1$ & $\nu_2(10.24) = 4$.

In general, for any two integers $a, b \in \mathbb{Z}$,

- $\nu_p(ab) = \nu_p(a) + \nu_p(b)$,
- $\nu_p(a+b) \geq \min\{\nu_p(a), \nu_p(b)\}$.

Provided that $\nu_p(a) \neq \nu_p(b)$,

- $\nu_p(a+b) = \{\nu_p(a), \nu_p(b)\}$.

A New Proof of Euclid's Theorem via Additive Combinatorics

Theorem

There are infinitely many prime numbers in the positive integers.

Proof [*Göral, Sertbaş, Ö. (2021)*, (accepted)]

Suppose that

$$p_1 = 2, p_2 = 3, \ldots, p_m$$

are all prime numbers in the positive integers. Define

$$\mathcal{C} : \mathbb{Z} \longrightarrow \Big(\{0,1\} \times \{0,1\} \Big)^m \cup \{\clubsuit\}$$

as

$$\mathcal{C}(n) = \begin{cases} \left(\begin{cases} 1 & p_i \mid n \\ 0 & p_i \nmid n \end{cases}, \nu_i(n) \pmod 2 \right)_i, & \textit{if} \quad n \neq 0 \\ \clubsuit, & \textit{if} \quad n = 0. \end{cases}$$

Then, $\mathcal{C}$ is a coloring of $\mathbb{Z}$ with finitely many colors.

Choose the following two polynomials in $\mathbb{Z}[x]$

$$f_1(x) = x \quad \text{and} \quad f_2(x) = p_1 \cdots p_m x,$$

By the Polynomial van der Waerden Theorem, we find two integers a and $d \neq 0$ such that

$$a, \quad a + f_1(d) = a + d, \quad a + f_2(d) = a + p_1 \cdots p_m d$$

have the same color.
Notice that a is non-zero.

Let $p \in \{p_1, p_2, \ldots, p_m\}$ be a prime number with $p|a$. Since

$$a \quad \& \quad a+d$$

have the same color, we have $p|d$.

- **Case I:** Suppose $\nu_p(d) < \nu_p(a)$
  As $a \quad \& \quad a+d$ have the same color,

  $$\nu_p(a) \equiv \nu_p(a+d) \pmod 2. \tag{1}$$

  Since $\nu_p(d) < \nu_p(a)$, we obtain that

  $$\nu_p(a+d) = \nu_p(d). \tag{2}$$

  By (1) and (2), we see that

  $$\nu_p(a) \equiv \nu_p(d) \pmod 2.$$

As $\nu_p(d) < \nu_p(a)$, we have that

$$\nu_p(d) \leq \nu_p(a) - 2.$$

On the other hand, we know that

$$a + d \quad \& \quad a + p_1 \cdots p_m d$$

have the same color.
This implies that

$$\nu_p(a+d) \equiv \nu_p(a + p_1 \cdots p_m d) \pmod 2.$$

By (2), we infer that

$$\nu_p(d) \equiv \nu_p(a + p_1 \cdots p_m d) \pmod 2. \tag{3}$$

As $\nu_p(d) \leq \nu_p(a) - 2$ and $p \in \{p_1, \ldots, p_m\}$, we deduce that

$$\nu_p(a + p_1 \cdots p_m d) = \nu_p(d) + 1. \tag{4}$$

Therefore, we obtain from (3) and (4) that

$$\nu_p(d) \equiv \nu_p(d) + 1 \pmod 2, \tag{5}$$

which is a contradiction.

- **Case II:** Suppose $\nu_p(a) \leq \nu_p(d)$
  Then, we have that

$$\nu_p(a) < \nu_p(p_1 \cdots p_m d). \tag{6}$$

This gives that

$$\nu_p(a) = \nu_p(a + p_1 \cdots p_m d).$$

Moreover, we have that

$$p|a \quad \& \quad p|a+p_1\cdots p_m d.$$

Hence, we have either

$$a = a+p_1\cdots p_m d \quad \text{or} \quad -a = a+p_1\cdots p_m d$$

In the **former case**, $d = 0(\rightarrow\leftarrow)$
In the **latter case**,

$$-2a = p_1\cdots p_m d \implies -a = p_2\cdots p_m d.$$

This shows that $p|a \quad \forall p \in \{p_2,\dots,p_m\}$. Hence,

$$\nu_p(a) = \nu_p(-a) = \nu_p(d)+1 \quad \forall p \in \{p_2,\dots,p_m\}.$$

This is a contradiction, since $\nu_p(a) \leq \nu_p(d)$ for all p dividing a. □

A New Proof of Euler's Theorem via Additive Combinatorics

Euler's Theorem

Let $p_1 < p_2 < \cdots$ be the list of all prime numbers. Then, the series

$$\sum_{i=1}^{\infty} \frac{1}{p_i} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \dots$$

is divergent.

Proof [*Göral, Sertbaş, Ö. (2021)*, (accepted)]

Suppose that the series

$$\sum_{i=1}^{\infty} \frac{1}{p_i} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \dots$$

is convergent. This means that

$$\sum_{i>m} \frac{1}{p_i} \leq \frac{1}{2},$$

for some positive integers m.
Let

$$A := \{a \in \mathbb{Z}^+ \;:\; p|a \implies p \in \{p_1, \dots, p_m\}\} \quad \& \quad a_1 < a_2 < \cdots$$

be consecutive terms of A.

One can verify that

$$\lim_{n\to\infty}(a_{n+1} - a_n) = \infty.$$

One also check that

$$\bar{d}(A) = \limsup_{N\to\infty} \frac{|A \cap \{1, \ldots, N\}|}{N} = 0.$$

However, for each positive N,

$$N - |A \cap \{1, \ldots, N\}| \leq \sum_{i>m} \left\lfloor \frac{N}{p_i} \right\rfloor \leq \sum_{i>m} \frac{N}{p_i} \leq \frac{N}{2}$$

This gives that $\bar{d}(A) \geq \frac{1}{2}$, a contradiction.
Therefore,

$$\sum_{i=1}^{\infty} \frac{1}{p_i} \longrightarrow \infty. \quad \square$$

The Green-Tao Theorem in Domains

- We will show the Green-Tao Theorem in polynomial rings over integral domains with several variables.

Theorem (*Göral, Sertbaş, Ö.* (2021), (accepted))

Let D be an integral domain and $n \geq 2$ and

$$A_k := \{p(x_1, \ldots, x_n) \in D[x_1, \ldots, x_n] \ : \ \deg(p) \leq k\},$$

where $k \geq 1$. Then, there exist two polynomials $f, g \in D[x_1, \ldots, x_n]$ with $g \neq 0$ such that for all $h \in A_k$, $f + gh$ is an irreducible polynomial that includes all the indeterminates $x_1, \ldots, x_n$.

Proof

Let $R := D[x_1, \dots, x_{n-1}]$ and choose the polynomials $f, g \in R[x_n]$ as

$$f(x_n) = x_n^{k+3} + x_1 \cdots x_{n-1} \quad \text{and} \quad g(x_n) = x_1^2.$$

Then the polynomials $f + gh$ are of the form

$$(f + gh)(x_n) = x_n^{k+3} + h \cdot x_1^2 + x_1 \cdots x_{n-1},$$

where $h = h(x_1, \dots, x_n) \in A_k$.
Observe that

- $f + gh$ includes all the indeterminates $x_1, \cdots, x_n$, for all $h \in A_k$.
- $f + gh$ are of degree $k + 3$ in terms of x_n.
- Hence, the leading coefficients of these polynomials are 1 w.r.t the variable x_n and all the other coefficients contain the variable x_1.

Note that

- If h does not contain the variable x_n, then the constant term of the polynomial $f + gh$ is

$$h \cdot x_1^2 + x_1 \cdots x_{n-1}.$$

- Otherwise, it is $x_1 \cdots x_{n-1}$.
- $R = D[x_1, \ldots, x_{n-1}]$ and $D[x_2, \ldots, x_{n-1}]$ are integral domains.
- $(x_1) \subseteq R$ is a principal prime ideal of R.

Notice that for any $h \in A_k$,

- All the coefficients of $f + gh$ except the leading one are contained in (x_1).
- The constant term of $f + gh$ is not contained in $(x_1)^2$ in either case.

Thus, by Eisenstein's Criterion, we conclude that $f + gh$ is irreducible in $R[x_n] = D[x_1, \ldots, x_n]$ for each $h \in A_k$. □

References

- L. Alpoge, *Van der Waerden and the Primes*, The American Mathematical Monthly **122** (2015), no. 8, 784-785.

- Bergelson, V., Leibman, A. (1996). Polynomial extensions of van der Waerden's and Szemerédi's theorems. *J. Amer. Math. Soc.* 9(3): 725–753.

- D'Agostino, S. (2020). Mathematicians will never stop proving the prime number theorem, *Quanta Magazine*. `www.quantamagazine.org/mathematicians-will-never-stop-proving-the-prime-number-theorem-20`

- Elsholtz, C. (2021). Fermat's last theorem implies Euclid's infinitude of primes, *Amer. Math. Monthly*, 128(3): 250–257.

- P. Erdős, *Uber die Reihe* $\sum \frac{1}{p}$, Mathematica (Zutphen), B7 (1938) 1-2.

- Erdős, P., Turán, P. (1936). On some sequences of integers. *J. London Math. Soc.* 11(4): 261–264.

- L. Euler, *Variae observationes circa series infinitas*, Com. Acad. Scient. Petropl., **9** (1744), 160–188. Online at https://scholarlycommons.pacific.edu/euler-works.

References

- H. Furstenberg, *On the infinitude of primes*, American Mathematical Monthly, **62** (1955), 353.

- Furstenberg, H. (1977). Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions. *J. Anal. Math.* 31: 204–256.

- Granville, A. (2017). A panoply of proofs that there are infinitely many primes. *London Math. Soc. Newsletter*. 472: 23–27.

- Granville, A. (2017). Squares in arithmetic progressions and infinitely many primes. *Amer. Math. Monthly*. 124(10): 951–954.

- Green, B., Tao, T. (2008). The primes contain arbitrarily long arithmetic progressions. *Ann. of Math. (2).* 167(2): 481–547. `doi.org/10.4007/annals.2008.167.481`

- R. Meštrović, Euclid's theorem on the infinitude of primes: A historical survey of its proofs, https://arxiv.org/pdf/1202.3670.pdf

- Roth, K. (1953). On certain sets of integers. *J. London Math. Soc.* 28(1): 104–109.

References

- Szemerédi, E. (1969). On sets of integers containing no four elements in arithmetic progression. *Acta Math. Acad. Sci. Hungar.* 20: 89–104.
- Szemerédi, E. (1975). On sets of integers containing no k elements in arithmetic progression. *Acta Arith.* 27: 199–245.
- Tao, T., Ziegler, T. (2008). The primes contain arbitrarily long polynomial progressions. *Acta Math.* 201(2): 213–305.
- Van der Waerden, B. L. (1927). Beweis einer Baudetschen Vermutung. *Nieuw Arch. Wisk.* 15: 212–216.

THANK YOU