THE AMERICAN MATHEMATICAL
MONTHLY MAA

An Official Publication of the Mathematical Association of America

Taylor & Francis
Taylor & Francis Group

The American Mathematical Monthly

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/uamm20

The Green-Tao Theorem and the Infinitude of Primes in Domains

Haydar Göral, Hikmet Burak Özcan & Doğa Can Sertbaş

To cite this article: Haydar Göral, Hikmet Burak Özcan & Doğa Can Sertbaş (2022): The Green-Tao Theorem and the Infinitude of Primes in Domains, The American Mathematical Monthly, DOI: 10.1080/00029890.2022.2141543

To link to this article: https://doi.org/10.1080/00029890.2022.2141543

Published online: 02 Dec 2022.

The Green-Tao Theorem and the Infinitude of Primes in Domains

Haydar Göral, Hikmet Burak Özcan, and Doğa Can Sertbaş

Abstract. We first prove an elementary analogue of the Green-Tao Theorem. The celebrated Green-Tao Theorem states that there are arbitrarily long arithmetic progressions in the set of prime numbers. In fact, we show the Green-Tao Theorem for polynomial rings over integral domains with several variables. Using the Generalized Polynomial van der Waerden Theorem, we also prove that in an infinite unique factorization domain, if the cardinality of the set of units is strictly less than that of the domain, then there are infinitely many prime elements. Moreover, we deduce the infinitude of prime numbers in the positive integers using polynomial progressions of length three. In addition, using unit equations, we provide two more proofs of the infinitude of prime numbers. Finally, we give a new proof of the divergence of the sum of reciprocals of all prime numbers.

1. INTRODUCTION. One may ask why mathematicians still give new proofs of the same theorems over and over again, even though they have already been established. For example, what was Euler's intention in giving a new proof of the infinitude of prime numbers about 2000 years after Euclid? This interesting question may be answered with the words of Michael Bode [5], a mathematics professor at Queensland University of Technology in Australia:

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

It is generally advantageous to approach problems from different perspectives. This allows one to gain various insights and points of view on theorems. For instance, Euler's proof of the infinitude of primes identified connections between analysis and number theory. Similarly, Alpoge's proof [1] of the infinitude of primes using additive combinatorics reveals the deep connection between additive number theory and multiplicative number theory. Moreover, these associations show that many subdisciplines of mathematics are closely related, and they take advantage of each other. To illustrate this point, the Pythagorean Theorem has at least 371 proofs [27] and the infinitude of primes has at least 183 proofs [24], and these proofs apply many different techniques of mathematics. In this paper, we extend this idea by offering new proofs of the infinitude of primes and the divergence of the sum of reciprocals of all primes. For this purpose, we survey the fundamental results of additive combinatorics so that the reader can see how the historical development led to contemporary topics in the discipline.

The first proof of the infinitude of prime numbers dates back to 300 BC and is attributed to Euclid. The proof of this famous result, which we know as Euclid's Theorem, is based on the fact that every positive integer greater than 1 has a prime divisor. In 1737, Euler [13, Theorema 19] provided a new proof of Euclid's Theorem using the divergence of the harmonic series

doi.org/10.1080/00029890.2022.2141543
MSC: Primary 70B05, Secondary 01A45

$$\sum_{k=1}^{\infty} \frac{1}{k} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots .$$

In fact, Euler proved the following result.

Euler's Theorem. *Let $p_1 < p_2 < \cdots$ be the list of all prime numbers. Then, the series*

$$\sum_{i=1}^{\infty} \frac{1}{p_i} \tag{1}$$

is divergent.

One can immediately see that Euler's Theorem implies Euclid's Theorem. Unlike Euclid's proof, however, Euler's proof is based on the following connection between prime numbers and infinite series:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1} . \tag{2}$$

Here, $s > 1$ is any real number and $\mathbb{P}$ is the set of all prime numbers. His approach inspired Dirichlet and formed the main idea of Dirichlet's Theorem on arithmetic progressions (see [6, Chapter 1]). The aformentioned theorem of Dirichlet is considered as the beginning of analytic number theory. Hence, this progress illustrates the underlying point of Bode's assertion. On the other hand, the function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

which was first introduced by Euler for real numbers $s > 1$, was also considered by Riemann in [28] for complex numbers s with $\Re(s) > 1$. He proved that $\zeta(s)$ has a meromorphic continuation to the whole complex plane except for a simple pole at $s = 1$ with residue 1. Then he established a link between the zeros of the function $\zeta(s)$ and the distribution of prime numbers. In 1896, Hadamard [23] and de la Vallée Poussin [7] proved independently the Prime Number Theorem using the ideas introduced by Riemann in [28], particularly the analytic properties of the function $\zeta(s)$. Recall that the Prime Number Theorem states that the prime counting function $\pi(n)$ is asymptotic to the function $\frac{n}{\log n}$, that is to say

$$\lim_{n \to \infty} \frac{\pi(n) \log n}{n} = 1.$$

Today, many mathematicians from various branches of the discipline still continue to provide new proofs of both Euclid's and Euler's Theorems. To give some examples, one of the most interesting proofs of Euclid's Theorem is Furstenberg's proof [14] that uses the basic instruments of topology. Another remarkable proof of Euclid's Theorem is that of Alpoge [1] who gave a proof using van der Waerden's Theorem. Using the same theorem of van der Waerden, Granville [20] also demonstrated the infinitude of prime numbers based on Alpoge's proof. Elsholtz [9] also gave some proofs of Euclid's Theorem in his recent paper, using results from number theory, additive combinatorics, and infinite Ramsey theory. If we look at the alternative proofs of Euler's Theorem in the literature, Erdős [10] has offered a combinatorial proof.

There are several proofs of both Euclid's Theorem and Euler's Theorem that use elementary number theory [30], geometry [18], valuation theory [31], and ring theory [25]. We refer the reader to the surveys of Meštrović [24] and Granville [19] to find more proofs of the infinitude of prime numbers.

Szemerédi's Theorem is another example of a theorem with several different proofs. Before mentioning it, we introduce some of the basics related to 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 $i = 1, \ldots, k-1$. In 1927, van der Waerden [36] showed that if positive integers are colored with finitely many colors, then there exists a monochromatic k-term arithmetic progression for any positive integer $k > 1$. This is a very first example in additive combinatorics. Nine years later, Erdős and Turán [12] proposed a conjecture which establishes van der Waerden's Theorem for $k = 3$. In order to explain this result, we first recall *the upper density of a subset* A of positive integers, which is denoted by $\bar{d}(A)$ and defined as

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

Erdős and Turán's conjecture states that there exists a 3-term arithmetic progression in every subset of positive integers with positive upper density. If we consider this question for an arbitrary positive integer $k > 1$, it can be observed that the extended Erdős-Turán conjecture implies van der Waerden's Theorem. To see this, note that if we divide the positive integers into finitely many disjoint subsets, namely

$$\mathbb{Z}^+ = \bigsqcup_{i=1}^{k} P_i,$$

where $P_i \cap P_j = \emptyset$ for any $i \neq j$, then we can find a subset $P_i \subset \mathbb{Z}^+$ such that the upper density of P_i is positive. The Erdős-Turán conjecture was shown by Roth [29] in 1953. After that, Szemerédi [32,33] proved its extended version for $k \geq 4$, where the proof included many new ideas and techniques. Thereafter, the extended Erdős-Turán conjecture was referred as Szemerédi's Theorem. Using ergodic theory, Furstenberg [15] provided a different proof of Szemerédi's Theorem, whereas Gowers [17] applied Fourier analytic techniques to obtain the same result. Moreover, Furstenberg's ergodic theoretical proof led to many generalizations of Szemerédi's Theorem. For instance, Furstenberg and Katznelson [16] proved the multidimensional Szemerédi Theorem, while Bergelson and Leibman [2] showed the polynomial version of it. Hence, Szemerédi's Theorem, like Euclid's Theorem, can also be regarded as an example that supports Bode's idea. Another open problem in additive combinatorics is Erdős' conjecture mentioned in [11]. It states that for a subset A of positive integers, if the series

$$\sum_{a\in A} \frac{1}{a} \tag{3}$$

is divergent, then A contains a k-term arithmetic progression for any positive integer $k \geq 3$. This conjecture was shown by Bloom and Sisask [4] for the case $k = 3$ in their very recent work. Even though the general case remains an open question, some special cases support the truth of this conjecture. For example, Green and Tao [21] proved the existence of a k-term arithmetic progression in the set of all prime numbers for each positive integer $k \geq 3$. Later, Tao and Ziegler [34] demonstrated the polynomial version of the Green-Tao Theorem. Considering the question from a different point of view, an analogue of the Green-Tao Theorem in $\mathbb{Z}[x]$ was shown by Pambuccian [26].

In this paper, we first show an elementary analogue of the Green-Tao Theorem in polynomial rings over integral domains with several variables. Following this, we prove the infinitude of prime elements in infinite unique factorization domains with few units using a generalization of Polynomial van der Waerden's Theorem [3]. Thanks to this technique, we obtain a new proof of Euclid's Theorem in Section 3 which allows us to improve Alpoge's and Granville's proofs simultaneously in terms of the number of elements in the corresponding progression. Furthermore, we give two more proofs of the infinitude of prime numbers in Section 4 by focusing on the number of solutions of a unit equation. Finally, we provide a proof of Euler's Theorem using the notion of upper density.

2. THE GREEN-TAO THEOREM IN DOMAINS. The main goal of this section is to prove an elementary analogue of the celebrated Green-Tao Theorem. In fact, we show that the Green-Tao Theorem is valid in polynomial rings over integral domains with several variables using Eisenstein's Criterion (see [8, Section 9.4, Proposition 13]).

Eisenstein's Criterion. *Let D be an integral domain and*

$$p(x) = x^n + \cdots + a_1 x + a_0$$

a polynomial in $D[x]$ with $n \geq 1$. Suppose that there exists a prime ideal $\mathfrak{p}$ of D such that

- *$a_i \in \mathfrak{p}$ for all $i = 0, \ldots, n-1$,*
- *$a_0 \notin \mathfrak{p}^2$.*

Then, $p(x)$ is an irreducible polynomial in $D[x]$.

Now, we are ready to prove our first result.

Theorem 1. *Let D be an integral domain and $n \geq 2$. Assume that A_k is the set of all polynomials in $D[x_1, \ldots, x_n]$, which have total degree at most $k \geq 1$. 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 $R = D[x_1, \ldots, x_{n-1}]$. Choose the polynomials $f, g \in R[x_n]$ as

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

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 $x_1, \dots, x_n$, for all $h \in A_k$. As the polynomials $h \in A_k$ have total degrees at most k, the polynomials $f + gh$ are of degree $k + 3$ in terms of x_n. Hence, the leading coefficients of these polynomials are 1 with respect to the variable x_n and all the other coefficients contain the variable x_1. 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 $x_1 \cdots x_{n-1}$. Since D is an integral domain, the rings $R = D[x_1, \dots, x_{n-1}]$ and $D[x_2, \dots, x_{n-1}]$ are integral domains as well. Also, observe that the principal ideal $(x_1) \subseteq R$ is a prime ideal of R, as the quotient ring $R/(x_1) \simeq D[x_2, \dots, x_{n-1}]$ is an integral domain. Note that for any $h \in A_k$, all the coefficients of $f + gh$ except the leading one are contained in (x_1). Furthermore, the constant term of $f + gh$ is not contained in $(x_1)^2$ in either case. Thus, by Eisenstein's Criterion, we deduce that $f + gh$ is irreducible in $R[x_n] = D[x_1, \dots, x_n]$ for each $h \in A_k$. ■

3. THE INFINITUDE OF PRIMES AND THE GENERALIZED POLYNOMIAL VAN DER WAERDEN THEOREM.

This section begins with the proof of the infinitude of prime elements in infinite unique factorization domains which have few units. To show this, we use an extension of the Polynomial van der Waerden Theorem to infinite integral domains, which can be obtained by [3, Corollary 7.11].

Generalized Polynomial van der Waerden Theorem. *Assume that D is an infinite integral domain and r is a positive integer. If $f_1(x), \dots, f_k(x)$ are polynomials in $D[x]$ with $f_1(0) = \cdots = f_k(0) = 0$, then for any r-coloring of D there exist $a \in D$ and $d \in D \setminus \{0\}$ such that $a, a + f_1(d), \dots, a + f_k(d)$ are of the same color.*

Let D be a unique factorization domain and $a \in D \setminus \{0\}$. Given any prime element $p \in D$, the *p-adic valuation* of a is the largest power of p dividing a and it is denoted by $\nu_p(a)$. By convention, $\nu_p(0) = \infty$ which is a symbol that is greater than every natural number. For any two elements $a, b \in D$, we have that

$$\nu_p(ab) = \nu_p(a) + \nu_p(b), \tag{4}$$

$$\nu_p(a + b) \geq \min\{\nu_p(a), \nu_p(b)\}. \tag{5}$$

Provided that $\nu_p(a) \neq \nu_p(b)$, we also have

$$\nu_p(a + b) = \min\{\nu_p(a), \nu_p(b)\}. \tag{6}$$

Using the properties of the p-adic valuation, we can prove our second result.

Theorem 2. *Let D be an infinite unique factorization domain and $D^\times$ denote the set of units in D. Assume that $|D^\times| < |D|$. Then, there are infinitely many prime elements in D which are not associated to each other.*

Proof. Assume that $p_1, \dots, p_m$ are the only (non-associated) prime elements in D. We first show that if $|D^\times| < |D|$, then $D^\times$ is a finite set. Suppose not, that is $D^\times$ contains at least countably many elements. Since D is a unique factorization domain, we see that every nonzero element $n \in D$ can be uniquely expressed as

$$n = u \prod_{i=1}^{m} p_i^{\nu_i(n)},$$

where $u \in D^{\times}$ and $\nu_i(n)$ is the p_i-adic valuation of n. This indicates that there are also countably many elements in D, which contradicts the assumption $|D^{\times}| < |D|$. Thus, we derive that $D^{\times}$ has only finitely many elements. Assume that $u_1, \ldots, u_s$ are all elements in $D^{\times}$. Define

$$\mathcal{C} : D \longrightarrow \Big(\{0, 1\} \times \{0, 1\}\Big)^{m} \cup \{\clubsuit\} \tag{7}$$

as

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

Then, $\mathcal{C}$ is a coloring of D with finitely many colors. Choose the following $2s$ polynomials from $D[x]$:

$$f_1(x) = u_1 x, \ f_2(x) = u_2 x, \ \ldots, \ f_s(x) = u_s x,$$
$$f_{s+1}(x) = u_1 \pi x, \ f_{s+2}(x) = u_2 \pi x, \ \ldots, \ f_{2s}(x) = u_s \pi x,$$

where $\pi = p_1 \cdots p_m$. Note that $f_i(0) = 0$ and $f_{s+i}(0) = 0$, for all $i = 1, \ldots, s$. By the Generalized Polynomial van der Waerden Theorem, there are a and $d \neq 0$ in D such that

$$\mathcal{C}(a) = \mathcal{C}\big(a + f_1(d)\big) = \cdots = \mathcal{C}\big(a + f_s(d)\big) = \mathcal{C}\big(a + f_{s+1}(d)\big) = \cdots = \mathcal{C}\big(a + f_{2s}(d)\big).$$

In other words,

$$a, \ a + u_1 d, \ \ldots, \ a + u_s d, \ a + u_1 \pi d, \ \ldots, \ a + u_s \pi d$$

have the same color. Notice that if a were zero, then the elements in the progression would have $\clubsuit$ color, which means that they are all zero. But this contradicts the fact that d is nonzero. Thus, a must be nonzero. Now, let us choose a prime element p dividing a. As $1 \in \{u_1, \ldots, u_s\}$, a and $a + d$ have the same color. Hence, p also divides $a + d$ which implies that p divides d. Suppose that $\nu_p(d) < \nu_p(a)$. As a and $a + d$ have the same color,

$$\nu_p(a) \equiv \nu_p(a + d) \pmod 2. \tag{8}$$

Since $\nu_p(d) < \nu_p(a)$, we obtain using (6) that

$$\nu_p(a + d) = \nu_p(d). \tag{9}$$

By (8) and (9), 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, $a + d$ and $a + \pi d$ have the same color. This implies that

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

By (9), we infer that

$$\nu_p(d) \equiv \nu_p(a + \pi d) \pmod 2. \tag{10}$$

As $\nu_p(d) \leq \nu_p(a) - 2$ and $p \in \{p_1, \dots, p_m\}$, we deduce from (4) and (6) that

$$\nu_p(a + \pi d) = \nu_p(d) + 1. \tag{11}$$

Therefore, we obtain from (10) and (11) that

$$\nu_p(d) \equiv \nu_p(d) + 1 \pmod{2}, \tag{12}$$

which is a contradiction. Hence, we must have $\nu_p(a) \leq \nu_p(d)$. Then, we see that

$$\nu_p(a) < \nu_p(u_i \pi d) \tag{13}$$

for all $i = 1, \dots, s$. By (6), we obtain that

$$\nu_p(a) = \nu_p(a + u_1 \pi d) = \cdots = \nu_p(a + u_s \pi d). \tag{14}$$

Moreover, $a, a + u_1\pi d, \dots, a + u_s \pi d$ are all divisible by p, since these $s + 1$ elements have the same color. Therefore, we also have the equalities in (14) for the primes that do not divide a. Hence, we see that (14) holds for all prime numbers $p \in \{p_1, \dots, p_m\}$. This indicates that a and $a + u_i \pi d$ are a unit multiple of each other for each $i = 1, \dots, s$, as D is a unique factorization domain. But there are s units in D and $1 \in D^\times$. Thus, we get that

$$a = a + u_i \pi d$$

for some $i = 1, \dots, s$. This shows that $u_i \pi d = 0$. Since D is a domain, $d = 0$ which contradicts the fact that d is nonzero. Consequently, there are infinitely many prime elements in D. ■

As a consequence of Theorem 3, one can also show the infinitude of prime elements in the integers by choosing only four polynomials, since ±1 are the only units in the integers. In fact, the number of polynomials can be reduced to two in order to prove the existence of infinitely many prime numbers. This may be seen as an improvement of [**1**, **20**] in the sense of the length of the corresponding progression.

Proposition 1. *There are infinitely many prime elements in the positive integers.*

Proof. Suppose that $\{p_1, p_2, \dots, p_m\}$ is the complete list of all prime elements in the positive integers, where $p_1 = 2$ and $m \geq 2$. Replacing D with $\mathbb{Z}$ in (7), we obtain a coloring $\mathcal{C}$ of $\mathbb{Z}$. Choose the following two polynomials in $\mathbb{Z}[x]$

$$f_1(x) = x \quad \text{and} \quad f_2(x) = \pi x,$$

where $\pi = p_1 \cdots p_m$. By the Generalized Polynomial van der Waerden Theorem, we find two integers a and $d \neq 0$ such that

$$a, a + d, a + \pi d$$

have the same color. Using the same argument given in the proof of Theorem 3, we have that a is nonzero and each prime divisor p of a also divides d. If $\nu_p(d) < \nu_p(a)$, then we have the same contradiction given in (12). Therefore, we must have $\nu_p(a) \leq \nu_p(d)$. Similar to (13), we obtain that

$$\nu_p(a) < \nu_p(\pi d).$$

By (6), we have that

$$\nu_p(a) = \nu_p(a + \pi d).$$

Moreover, p divides both a and $a + \pi d$. As ± 1 are only units in $\mathbb{Z}$ and p is an arbitrary prime divisor of a, we have two possible cases: either $a = a + \pi d$ or $-a = a + \pi d$. In the former case, we can easily get that $d = 0$, which is a contradiction. The latter case also yields that

$$-2a = \pi d. \tag{15}$$

As $p_1 = 2$, we get that

$$-a = p_2 \cdots p_m d. \tag{16}$$

This shows that p divides a for every $p \in \{p_2, \ldots, p_m\}$. By (4) and (16), we obtain that

$$\nu_p(a) = \nu_p(-a) = \nu_p(d) + 1$$

for every $p \in \{p_2, \ldots, p_m\}$. This leads to a contradiction, because we have that $\nu_p(a) \leq \nu_p(d)$ for each prime divisor p of a. In conclusion, there are infinitely many prime elements in the positive integers. ■

4. THE INFINITUDE OF PRIMES AND UNIT EQUATIONS.

The main objective in this section is to present two more proofs of Euclid's Theorem based on a result of Győry [22]. Using the same fact, we also give a proof of Euler's Theorem.

Fact 1 ([22]). *Let $S = \{p_1, \ldots, p_m\}$ be a finite set of prime numbers. Then, the equation*

$$x + y = 1$$

has only finitely many solutions in $\{\pm p_1^{\alpha_1} \cdots p_m^{\alpha_m} \mid \alpha_1, \ldots, \alpha_m \in \mathbb{Z}\}$.

Theorem 3. *There are infinitely many prime numbers.*

First Proof of Theorem 3. Suppose that there are finitely many prime numbers. Let us list them as $p_1, \ldots, p_m$. By the fundamental theorem of arithmetic, prime factorizations of the numerators and denominators of all nonzero rational numbers are of the form $\pm p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ for some $\alpha_1, \ldots, \alpha_m \in \mathbb{Z}_{\geq 0}$. This means that

$$\{\pm p_1^{\alpha_1} \cdots p_m^{\alpha_m} \mid \alpha_1, \ldots, \alpha_m \in \mathbb{Z}\} = \mathbb{Q}^\times.$$

By Fact 1, we know that the equation

$$x + y = 1, \tag{17}$$

has only finitely many solutions in $\{\pm p_1^{\alpha_1} \cdots p_m^{\alpha_m} \mid \alpha_1, \ldots, \alpha_m \in \mathbb{Z}\}$. However, for each $x \in \mathbb{Q}^\times$ with $x \neq 1$, we know that $(x, 1 - x)$ is a solution of equation (17), where $1 - x \in \mathbb{Q}^\times$. This shows that we can find infinitely many solutions of equation (17) in $\{\pm p_1^{\alpha_1} \cdots p_m^{\alpha_m} \mid \alpha_1, \ldots, \alpha_m \in \mathbb{Z}\}$, which contradicts Fact 1. Therefore, there are infinitely many prime numbers. ■

One can observe that if there are finitely many prime numbers, then Fact 1 implies that the length of arithmetic progressions in the natural numbers must be bounded. This leads to another proof of the infinitude of prime numbers.

Second Proof of Theorem 3. Suppose that $p_1, \ldots, p_m$ are all the prime numbers. Let $a_0, a_1, \ldots a_k$ be an arithmetic progression of length $k+1$ in the positive integers. Then, there exists a nonzero positive integer d such that

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

for all $i = 0, \ldots, k-1$. For that reason, there are k solutions

$$\left(\frac{a_{i+1}}{d}, \frac{-a_i}{d} \right)$$

of the unit equation

$$x + y = 1, \tag{18}$$

where $x, y \in \{\pm p_1^{\alpha_1} \cdots p_m^{\alpha_m} \mid \alpha_1, \ldots, \alpha_m \in \mathbb{Z}\}$. By Fact 1, we know that equation (18) has only finitely many solutions in $\{\pm p_1^{\alpha_1} \cdots p_m^{\alpha_m} \mid \alpha_1, \ldots, \alpha_m \in \mathbb{Z}\}$. Let r denote the number of solutions of equation (18). Then, we must have $k \leq r$. This shows that the length of arithmetic progressions in the positive integers can be at most $r+1$. This is a contradiction, since we have arbitrarily long arithmetic progressions in the positive integers. Therefore, there are infinitely many prime numbers. ■

Finally, we can introduce a new proof of Euler's Theorem. To achieve this, we need the following lemma.

Lemma 1. *Let $A = \{a_n \mid n \geq 1\}$, where $\{a_n\}$ is a sequence of strictly increasing positive integers. If the difference between consecutive terms of A tends to infinity, then the upper density of A equals zero, namely*

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

Proof. Let k be an arbitrary positive integer. By the assumption, there exists a positive integer $N = N(k)$ such that

$$a_{n+1} - a_n \geq k \tag{19}$$

for all $n \geq N$. As $\{a_n\}$ is a sequence of strictly increasing positive integers, we have that

$$a_{n+1} - a_n \geq 1 \tag{20}$$

for each $n = 0, 1, \ldots, N-1$. This yields that $a_N \geq N$. Choose any integer $X \geq ka_N$. As $a_N \geq N$, we have $X \geq kN$. By (19), there exist at most $\left\lfloor \frac{X - a_N}{k} \right\rfloor$ terms of $\{a_n\}$ between a_N and X. Combining $a_N \geq N$ with (20), we derive that the cardinality of $A \cap \{1, \ldots, X\}$ can be at most $N + \frac{X-N}{k}$. Therefore, we have that

$$\frac{|A \cap \{1, \ldots, X\}|}{X} \leq \frac{N + \frac{X-N}{k}}{X} \leq \frac{1}{k} + \frac{1}{k} = \frac{2}{k}. \tag{21}$$

Since k is arbitrary, we obtain from inequality (21) that $\bar{d}(A) = 0$. ■

Now, we can give our proof of Euler's Theorem:

Proof of Euler's Theorem. Suppose that the series given in (1) is convergent. Then, there exists a positive integer m such that

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

Let A denote the set of positive integers whose prime divisors are only $p_1, \ldots, p_m$ and $a_1 < a_2 < \cdots$ be consecutive terms of A. Let us first see that

$$\lim_{n\to\infty} (a_{n+1} - a_n) = \infty, \tag{22}$$

which can also be deduced by [35, Satz 12]. Assume to the contrary that the limit of the sequence $(a_{n+1} - a_n)$ does not diverge. This means that there is a number $M > 0$ such that we have a subsequence of $(a_{n+1} - a_n)$ which is bounded by M. By the pigeonhole principle, there exists a positive integer $k \leq M$ such that

$$a_{n+1} - a_n = k$$

for infinitely many n. Therefore, we have

$$\frac{a_{n+1}}{k} - \frac{a_n}{k} = 1$$

for infinitely many n. Let $k = q_1^{\beta_1} \cdots q_r^{\beta_r}$, where q_i is a prime number and $\beta_i \in \mathbb{N}$ for each $i = 1, \ldots, r$. Then we obtain that

$$x + y = 1$$

has infinitely many solutions in

$$\{p_1^{\alpha_1} \cdots p_m^{\alpha_m} q_1^{\beta_1} \cdots q_r^{\beta_r} \mid \alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_r \in \mathbb{Z}\},$$

which contradicts Fact 1. Thus, we must have

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

Combining Lemma 1 and equation (22), we get that $\bar{d}(A) = 0$. But if we count the elements in $\{1, \ldots, N\}$ that do not belong to A, we see that

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

for each positive N. This gives that $\bar{d}(A) \geq \frac{1}{2}$, which is a contradiction as $\bar{d}(A) = 0$. Hence,

$$\sum_{i=1}^{\infty} \frac{1}{p_i}$$

is a divergent series. ■

[1] Alpoge, L. (2015). van der Waerden and the primes. *Amer. Math. Monthly*. 122(8): 784–785. doi.org/10.4169/amer.math.monthly.122.8.784

[2] Bergelson, V., Leibman, A. (1996). Polynomial extensions of van der Waerden's and Szemerédi's theorems. *J. Amer. Math. Soc.* 9(3): 725–753. doi.org/10.1090/S0894-0347-96-00194-4

[3] Bergelson, V., Leibman, A. (1999). Set-polynomials and polynomial extension of the Hales-Jewett theorem. *Ann. of Math. (2)*. 150(1): 33–75. doi.org/10.2307/121097

[4] Bloom, T. F., Sisask, O. (2020). Breaking the logarithmic barrier in Roth's theorem on arithmetic progressions. arxiv.org/pdf/2007.03528.pdf

[5] 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-20200722/

[6] Davenport, H. (1980). *Multiplicative Number Theory. Graduate Texts in Mathematics*, Vol. 74, 2nd ed. New York: Springer-Verlag.

[7] de la Vallée Poussin, C. J. (1896). Recherches analytiques sur la théorie des nombres premiers. Première partie: La fonction $\zeta(s)$ de Riemann et les nombres premiers en général, *Ann. Soc. Sci. Bruxelles*. 20: 183–256.

[8] Dummit, D. S., Foote, R. M. (2004). *Abstract Algebra*, 3rd ed. Hoboken, NJ: Wiley.

[9] Elsholtz, C. (2021). Fermat's last theorem implies Euclids infinitude of primes, *Amer. Math. Monthly*, 128(3): 250–257. doi.org/10.1080/00029890.2021.1856544

[10] Erdős, P. (1938). Über die Reihe $\sum \frac{1}{p}$. *Mathematica, Zutphen B 7*: 1–2.

[11] Erdős, P. (1981). On the combinatorial problems which I would most like to see solved. *Combinatorica*. 1: 25–42. doi.org/10.1007/BF02579174

[12] Erdős, P., Turán, P. (1936). On some sequences of integers. *J. London Math. Soc.* 11(4): 261–264. doi.org/10.1112/jlms/s1-11.4.261

[13] Euler, L. (1744). Variae observationes circa series infinitas. *Comment. Acad. Sci. Imp. Petropol.* 9: 160–188.

[14] Furstenberg, H. (1955). On the infinitude of primes. *Amer. Math. Monthly*. 62(5): 353. doi.org/10.2307/2307043

[15] Furstenberg, H. (1977). Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions. *J. Anal. Math.* 31: 204–256. doi.org/10.1007/BF02813304

[16] Furstenberg, H., Katznelson, Y. (1978). An ergodic Szemerédi theorem for commuting transformations. *J. Anal. Math.* 34: 275–291. doi.org/10.1007/BF02790016

[17] Gowers, W. T. (2001). A new proof of Szemerédi's theorem. *GAFA, Geom. Funct. Anal.* 11: 465–588. doi.org/10.1007/s00039-001-0332-9

[18] Göral, H. (2020). p-adic metrics and the infinitude of primes. *Math. Mag.* 93(1): 19–22. doi.org/10.1080/0025570X.2020.1679574

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

[20] Granville, A. (2017). Squares in arithmetic progressions and infinitely many primes. *Amer. Math. Monthly*. 124(10): 951–954. doi.org/10.4169/amer.math.monthly.124.10.951

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

[22] Győry, K. (1979). On the number of solutions of linear equations in units of an algebraic number field. *Comment. Math. Helv.* 54: 583–600. doi.org/10.1007/BF02566294

[23] Hadamard, J. (1896). Sur la distribution des z'eros de la fonction $\zeta(s)$ et ses cons'equences arithm'etiques. *Bull. Soc. Math. France*. 24: 199–220. doi.org/10.24033/bsmf.545

[24] Meštrović, R. (2018). Euclid's theorem on the infinitude of primes: a historical survey of its proofs (300 B.C.–2017). arxiv.org/pdf/1202.3670.pdf

[25] Özcan, H. B., Taşkın, S. (2020). Rings with few units and the infinitude of primes. *Hacet. J. Math. Stat.* 49(6): 2071–2073. doi.org/10.15672/hujms.649706

[26] Pambuccian, V. (2014). The Green-Tao theorem on primes in arithmetical progressions in the positive cone of $\mathbb{Z}[X]$. *Elem. Math.* 69(1): 30–32. doi.org/10.4171/em/242

[27] Ratner, B. (2009). Pythagoras: Everyone knows his famous theorem, but not who discovered it 1000 years before him. *J. Target. Meas. Anal. Mark.* 17: 229–242. doi.org/10.1057/jt.2009.16

[28] Riemann, B. (1859). Über die Anzahl der Primzahlen unter einer gegebenen Grösse. *Monatsber. Akad. Berlin*. 671–680.

[29] Roth, K. (1953). On certain sets of integers. *J. London Math. Soc.* 28(1): 104–109. doi.org/10.1112/jlms/s1-28.1.104

[30] Saidak, F. (2006). A new proof of Euclid's theorem. *Amer. Math. Monthly*. 113(10): 937–938. doi.org/10.1080/00029890.2006.11920383

[31] Seki, S. (2018). Valuations, arithmetic progressions, and prime numbers. *Notes Number Theory Discrete Math.* 24(4): 128–132. doi.org/10.7546/nntdm.2018.24.4.128-132

[32] Szemerédi, E. (1969). On sets of integers containing no four elements in arithmetic progression. *Acta Math. Acad. Sci. Hungar.* 20: 89–104. doi.org/10.1007/BF01894569

[33] Szemerédi, E. (1975). On sets of integers containing no k elements in arithmetic progression. *Acta Arith.* 27: 199–245. doi.org/10.4064/AA-27-1-199-245

[34] Tao, T., Ziegler, T. (2008). The primes contain arbitrarily long polynomial progressions. *Acta Math.* 201(2): 213–305. doi.org/10.1007/s11511-008-0032-5

[35] Thue, A. (1908). Bermerkungen über gewisse Näherungsbrüche algebraischer Zahlen. *Skrift. Vidensk. Selsk. Christ.* no. 3.

[36] Van der Waerden, B. L. (1927). Beweis einer Baudetschen Vermutung. *Nieuw Arch. Wisk.* 15: 212–216.

HAYDAR GÖRAL (MR Author ID: 1013641) graduated from İstanbul Bilgi University and earned his doctoral degree in mathematics from Université Claude Bernard Lyon 1. He is now an assistant professor at İzmir Institute of Technology. He is interested in number theory and mathematical logic.
Department of Mathematics, Faculty of Sciences, İzmir Institute of Technology, 35430, İzmir, TURKEY.
haydargoral@iyte.edu.tr

HİKMET BURAK ÖZCAN (MR Author ID: 1421138) graduated from İzmir University of Economics in 2016 and received his M.Sc. degree in mathematics from Dokuz Eylül University in 2020. He is currently a Ph.D. candidate in the Department of Mathematics at İzmir Institute of Technology. He is interested in number theory.
Department of Mathematics, Faculty of Sciences, İzmir Institute of Technology, 35430, İzmir, TURKEY.
hikmetozcan@iyte.edu.tr

DOĞA CAN SERTBAŞ (MR Author ID: 1181789) graduated from İzmir University of Economics in 2011. He got his M.Sc. degree in mathematics from University of Bonn in 2015 and his doctoral degree in mathematics from Koç University in 2020. Now, he is an assistant professor at Çukurova University in Adana. He is interested in number theory and cryptography.
Department of Mathematics, Faculty of Sciences, Çukurova University, 01330, Adana, TURKEY.
dsertbas@cu.edu.tr