A NEW REPRESENTATION OF INTEGERS AND SOME RESULTS ON PRIME CONJECTURES

MAODONG YE

Abstract

This paper proposes a new method for representing integers. Based on this method, we reveal the structure of multiplicative subgroups in the quotient ring of integers modulo π_k and their relationship with the set of primes, present a directed tree construction method for primes, and give necessary and sufficient conditions for a number of the form n^2+1 to be prime. Meanwhile, the Goldbach's conjecture has been proven.

Keywords: prime base representation; multiplicative subgroups of integer quotient rings; prime tree; forbidden number; set of numbers intersected with a primes

0

Many things have multiple facets. Some things cannot be seen clearly from the usual perspective. However, looking at them from a different angle may reveal new aspects that were previously unnoticed.

Integers are no exception. While the decimal representation is convenient for calculations, it lacks clear patterns in divisibility.

This paper proposes a new representation of integers, revealing significant information regarding their divisibility. Based on this novel integer representation, the following results are obtained:

1. Reveal the structure of the multiplicative subgroup in the quotient ring of the integer ring modulo π_k and its relationship with the set of prime numbers, thereby establishing a directed tree structure for prime numbers.

2. Provide necessary and sufficient conditions for numbers of the form n^2+1 to be prime.

3. Prove the Goldbach conjecture that every even integer greater than 2 can be expressed as the sum of two prime numbers.

1

Let $\mathbb{Z}_+$ denote the set of positive integers. For $k \in \mathbb{Z}_+$, let p_k denote the k-th prime number. For definiteness, we set

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ \ldots$$

and so on. In addition, let $\pi_k = p_1 p_2 \cdots p_k$.

We consider an ancient problem in number theory: the Chinese Remainder Theorem. As a

special case, consider the system of linear congruences:

$$\begin{cases} x \equiv \alpha_1 \pmod{p_1} \\ x \equiv \alpha_2 \pmod{p_2} \\ \quad \vdots \\ x \equiv \alpha_k \pmod{p_k} \end{cases} \tag{1.1}$$

with $0 \leq \alpha_i < p_i$.
(In this paper, we use lowercase $m \pmod{n}$ to indicate that the value on one side of the congruence is taken from the congruence group $\{0, 1, 2, \ldots, n-1\}$.)
The solution to this system of congruences can be found in standard number theory textbooks.
Theorem A[1]. Let $e_i = M_i M_i^{-1}$, where $M_i = \pi_k / p_i$, and M_i^{-1} satisfy $M_i M_i^{-1} \equiv 1 \pmod{p_i}$. Then the general solution to system (1.1) is

$$x \equiv \sum_{i=1}^{k} \alpha_i e_i \pmod{\pi_k}. \tag{1.2}$$

Moreover, the solution is unique modulo π_k.

The following theorem restates the above result in another form.

Theorem 1.1. *Let $a \in \{0, 1, \ldots, \pi_k - 1\}$, and let $a \equiv \alpha_i \pmod{p_i}$ with $0 \leq \alpha_i < p_i$ for $1 \leq i \leq k$. Then the set of vectors*

$$P_k = \{(\alpha_1, \alpha_2, \ldots, \alpha_k)\}$$

is in one-to-one correspondence with the set of integers on the interval $A_k = [0, \pi_k - 1]$. □

Denote this correspondence by ρ_k, so that for $a \in [0, 1, \ldots, \pi_k - 1]$, a and the vector $\rho_k(a) = (\alpha_1, \alpha_2, \ldots, \alpha_k)$ can be regarded as "equal".

For simplicity, we write

$$a = (\alpha_1 \ \alpha_2 \ \ldots \ \alpha_k)_\rho$$

where the α_i are determined by (1.1). The subscript ρ after the parentheses indicates that each component satisfies (1.1) and $0 \leq \alpha_i < p_i$.
When there is no ambiguity, the subscript ρ may be omitted.

Definition 1.1. Let $a \in A_k$. The representation $a = (\alpha_1 \ \alpha_2 \ \ldots \ \alpha_i \ \ldots \ \alpha_k)_\rho$ is called the *k-digit prime base representation* of a. The position of the i-th component is called the *i-th digit position* or *digit position i*. The number α_i is called *the value on the i-th digit position*, or the *i-th digit position value*.

From Definition 1.1, it follows that there are exactly π_k numbers representable in the k-digit prime base, corresponding to the elements of A_k.

This representation is reasonable because the mapping ρ_k defined by (1.1) is compatible. When extending from P_k to P_{k+1}, the first k digits keep unchanged,with only the (k+1)-th digit appended.

A 1-digit prime base representation set P_1 has only two numbers: $0 = (0), \quad 1 = (1)$.
A 2-digit prime base representation set P_2 is an extension of 1-digit prime-base representation, containing six numbers:

$$0 = (0\ 0), \quad 1 = (1\ 1), \quad 2 = (0\ 2),$$
$$3 = (1\ 0), \quad 4 = (0\ 1), \quad 5 = (1\ 2).$$

The left-hand sides are the usual decimal representations.

From (1.1), the number of digits in the prime base representation of a number a can be extended to any finite length.

Proposition 1.1. *If $p_{m-1} \leq a < p_m$, then $\alpha_i = a$ for $i = m, m+1, \ldots$, i.e., all position values starting from digit position m are equal to a.* □

Definition 1.2. We call the digit position m satisfying the above condition the *static position* of a. The previous digit position $m-1$ is called the *last position*. The number m is called the *total length* of a.

The number a enters a static state starting from the m-th digit position. The position values from the first digit position to the static position reflect the structural information of a.

Definition 1.3. If the prime base representation of a number is extended to the static position or beyond, we call this representation the *total prime base representation* of the number.

0 and 1 are two particularly special numbers. In the total prime base representation, all digit position values of 0 are 0, while all digit position values of 1 are 1. They are the only two numbers whose static position is digit position 1.

From (1.1) we also have:

Proposition 1.2. *If the value of digit position k in the number a is 0, then a contains the factor p_k.* □

Proposition 1.3. *If two numbers a and b are coprime, then their digit positions with a value of 0 are different, and vise versa* □

Proposition 1.4. *In the prime base representation of a prime p_m, the value at the m-th digit position (i.e., the last digit position) is 0, and its static position is at the $(m+1)$-th position. Among the digit position values of the prime base representation of a prime, there is exactly one 0. Within the set of numbers with a total length $m+1$, there exists exactly one such prime number p_m.* □

Proposition 1.5. *The set of numbers with total length $m+1$ has $p_{m+1}-p_m$ consecutive integers, with the smallest being the prime p_m.* □

In the prime base representation, another case where there is only a unique 0 occurs when the number is a power of a prime p_m, p_m^k with $k \geq 2$. In this scenario, the value at digit position m is 0, but its static position must be greater than $m+1$.

Additionally, in the prime base representations of all other composite numbers, there are at least two digit positions with a value of 0.
From this we obtain:

Theorem 1.2. *A number is prime if and only if, in its total prime base representation, there is exactly one 0 at the last position, and the following position is the static position.* □

Definition 1.4. The unique 0 of a prime p_m at digit position m is called the *marking zero* of p_m.

Theorem 1.3. *Let $a, b \in P_k$, $a = (\alpha_1\ \alpha_2\ \ldots\ \alpha_k)$, $b = (\beta_1\ \beta_2\ \ldots\ \beta_k)$, $c = (\gamma_1\ \gamma_2\ \ldots\ \gamma_k)$. If $a + b = c \in P_k$, then*

$$\gamma_i \equiv \alpha_i + \beta_i \pmod{p_i} \quad i = 1, 2, \ldots, k.$$

Or written as

$$c = (\alpha_1 + \beta_1\ \alpha_2 + \beta_2\ \ldots\ \alpha_k + \beta_k)_\rho \quad i = 1, 2, \ldots, k.$$

Here the subscript ρ indicates that the values inside the parentheses satisfy $\gamma_i \equiv a_i + \beta_i \pmod{p_i}$ and $0 \leq \gamma_i < p_i$.

This follows directly from (1.1). If $c > \pi_k$, the addition of a and b can be performed in P_{k+1}. □

From Theorem 1.3, we note that $a+1 = (\alpha_1+1\ \alpha_2+1\ \ldots\ \alpha_k+1)_\rho$. More generally, for small integers j,

$$a+j = (\alpha_1+j\ \alpha_2+j\ \ldots\ \alpha_k+j)_\rho \tag{1.2}$$

where the subscript ρ remains in effect.

Similarly, we have:

Theorem 1.4. *Let $a, b \in P_k$, $a = (\alpha_1\ \alpha_2\ \ldots\ \alpha_k)$, $b = (\beta_1\ \beta_2\ \ldots\ \beta_k)$. If $c = a - b > 0$, then*

$$c = (\alpha_1-\beta_1\ \alpha_2-\beta_2\ \ldots\ \alpha_k-\beta_k)_\rho, \quad i = 1, 2, \ldots, k.$$

Here again, the subscript ρ indicates the requirement $0 \le \gamma_i < p_i$. □

The above two operations also hold when a and b are in total prime base representation, without any additional restrictions.

Theorem 1.5. *Let $a = (\alpha_1\ \alpha_2\ \ldots\ \alpha_k) \in P_k$, and let j be a positive integer. If $ja \in P_k$, then*

$$ja = (j\alpha_1\ j\alpha_2\ \ldots\ j\alpha_k)_\rho.$$

When $ja > \pi_k - 1$, it is necessary to extend the digit position to $k+1$ or higher. □

Definition 1.5. When $\pi_{k-1} \le a < \pi_k$, we call the k-digit prime base representation of a the *minimal prime base representation* of a.

The minimal prime base representation of a having k-digit means $\pi_{k-1} \le a < \pi_k$. If the last component α_k is removed, the number corresponding to the resulting prime base representation belongs to P_{k-1} and is less than a.

We now consider the extension from k-digit prime base representation to $(k+1)$-digit prime base representation.
Extending from P_k to P_{k+1} means adding a $(k+1)$-th component $\beta \in \{0, 1, \ldots, p_{k+1}-1\}$ to each k-dimensional vector corresponding to a number in P_k. The number of elements in the extended set becomes π_{k+1}, with the general form $(\alpha_1\ \alpha_2\ \ldots\ \alpha_k\ \beta)_\rho$, where each vector corresponds bijectively to the integers in the interval $[0, \pi_{k+1}-1]$.

Proposition 1.6. *For $a = (\alpha_1\ \alpha_2\ \ldots\ \alpha_k) \in P_k$, if*

$$\beta = \alpha_{k+1} \equiv a \pmod{p_{k+1}}, \tag{1.3}$$

then the value of a remains unchanged after adding β to the $(k+1)$th digit position of a, i.e., $a = (\alpha_1\ \alpha_2\ \ldots\ \alpha_k\ a_{k+1})$.

This follows from the one-to-one correspondence in P_{k+1} when (1.3) is added to (1.1). □

Definition 1.6. Let $a = (\alpha_1\ \alpha_2\ \ldots\ \alpha_k) \in P_k$, and let

$$\alpha_{k+1} \equiv a \pmod{p_{k+1}}.$$

We call $(\alpha_1\ \alpha_2\ \ldots\ \alpha_k\ \alpha_{k+1})_\rho$ the *natural extension* of $a = (\alpha_1\ \alpha_2\ \ldots\ a_k)$.

Similarly, the natural extension of a can be continued to the static position, and the number represented remains a.

Definition 1.7. Let $\pi_{k-1} \le a < \pi_k$. In the total prime base representation of a, the minimal prime base representation is the first k digits. If the static position is at the m-th digit position, then the positions from $k+1$ to m are called the *natural extension segment.*

Thus, for a number a with $\pi_{k-1} \le a < \pi_k$, its prime base representation is divided into three segments: the first k positions are the minimal prime base representation segment, the positions from $k+1$ to m are the natural extension segment, and the rest are the number a.

Returning to our previous discussion, consider adding the $(k+1)$-th component β when extending to P_{k+1}. When

$$\beta \neq \alpha_{k+1} \equiv a \pmod{p_{k+1}},$$

there are $p_{k+1} - 1$ other choices.

Theorem 1.6. *Let $a = (\alpha_1\ \alpha_2\ \dots\ \alpha_k) \in P_k$. If $\beta \in \{0, 1, \dots, p_{k+1} - 1\}$, then*

$$(\alpha_1\ \alpha_2\ \dots\ \alpha_k\ \beta)_\rho = a + j\pi_k. \tag{1.4}$$

where the relationship between β and j will be given in the proof.

Proposition 1.6 states that when $\beta = \alpha_{k+1}$, $j = 0$ in (1.4).
Proof. We provide the relation between β and j. Let

$$\pi_k \equiv r_{k+1} \pmod{p_{k+1}}, \quad a \equiv \alpha_{k+1} \pmod{p_{k+1}},$$

and

$$\beta \equiv \alpha_{k+1} + jr_{k+1} \pmod{p_{k+1}} \tag{1.5}$$

Note that here $r_{k+1} \not\equiv 0 \pmod{p_{k+1}}$.
By the addition rule of Theorem 1.3, in P_{k+1}, we have

$$\begin{aligned}(\alpha_1\ \alpha_2\ \dots\ \alpha_k\ \beta)_\rho &= (\alpha_1\ \alpha_2\ \dots\ \alpha_k\ \alpha_{k+1} + jr_{k+1})_\rho \\ &= (\alpha_1\ \alpha_2\ \dots\ \alpha_k\ \alpha_{k+1})_\rho + (0\ 0\ \dots\ 0\ jr_{k+1})_\rho \\ &= a + j\pi_k.\end{aligned}$$

Thus, when $\beta \equiv \alpha_{k+1} + jr_{k+1} \pmod{p_{k+1}}$, the equation (1.4) holds. □

The prime base representation of integers can be displayed using a table of prime base representations. Similar to a function table, it is used to look up the prime base representation of small integers: take a plane coordinate system with the horizontal axis (rightward) representing primes p_k in increasing order ($k = 1, \dots, m$) and the vertical axis (downward) representing consecutive integers in $[1, n]$. Fill in the corresponding remainder at each intersection to form an integer prime base table.

Returning to equation (1.2) of Theorem A at the beginning of the paper:

$$x \equiv \sum_{i=1}^{k} \alpha_i e_i \pmod{\pi_k}$$

This is equivalent to finding the decimal representation of x given its prime base representation $x = (\alpha_1, \alpha_2, \dots, \alpha_k)$. Theorem A already gives the decimal value of x in terms of $M_i M_i^{-1}$. However, this representation is not yet the clearest answer. The proof is also relatively complex, and the issue has not been fully resolved.

Let e_i be the number whose prime base representation has 1 at the i-th digit position and 0 elsewhere:

$$e_i = (0\ \dots\ 0\ 1\ 0\ \dots\ 0) \quad i = 1, 2, \dots, k \tag{1.6}$$

The quantity $M_i M_i^{-1}$ in Theorem A is exactly e_i. However, e_i can be represented in other ways besides $M_i M_i^{-1}$; using (1.6) is simpler and more precise.

Based on the previous discussion of basic properties of prime base representation, Theorem A can be rewritten as follows:

Theorem A′. Let e_i $(i = 1, 2, \ldots, k)$ be as in (1.6). If the prime base representation of x is $(\alpha_1, \alpha_2, \ldots, \alpha_k)$, then

$$x = (\alpha_1\ \alpha_2\ \ldots\ \alpha_k) \equiv \sum_{i=1}^{k} \alpha_i e_i \pmod{\pi_k}. \tag{1.7}$$

This congruence follows directly from Theorems 1.3 and 1.5. □

Equation (1.7) is the final form of Theorem A. The difference from (1.2) is that it does not require numbers like $M_i M_i^{-1}$ to express e_i, nor does it require a roundabout proof. It truly returns to the basis representation in linear algebra.

As an equality, (1.7) holds both in prime base representation and in decimal representation. Taking the decimal representation of each e_i gives the decimal representation of x. There are multiple ways to compute the decimal representation of e_i based on the previous propositions and theorems.

We illustrate with examples. Let $a = (\alpha_1\ \alpha_2\ \ldots\ \alpha_k)$. From (1.7):

When $k = 2$: $e_1 = (1\ 0) = 3, \quad e_2 = (0\ 1) = 4$
$a \equiv 3\alpha_1 + 4\alpha_2 \pmod{6}$.

When $k = 3$: $e_1 = (1\ 0\ 0) = 15, \quad e_2 = (0\ 1\ 0) = 10, \quad e_3 = (0\ 0\ 1) = 6$
$a \equiv 15\alpha_1 + 10\alpha_2 + 6\alpha_3 \pmod{30}$.

When $k = 4$: $e_1 = (1\ 0\ 0\ 0) = 105, \quad e_2 = (0\ 1\ 0\ 0) = 70, \quad e_3 = (0\ 0\ 1\ 0) = 126, \quad e_4 = (0\ 0\ 0\ 1) = 120$
$a \equiv 105\alpha_1 + 70\alpha_2 + 126\alpha_3 + 120\alpha_4 \pmod{210}$.

When $k = 5$: $e_1 = (1\ 0\ 0\ 0\ 0) = 1155, \quad e_2 = (0\ 1\ 0\ 0\ 0) = 1540, \quad e_3 = (0\ 0\ 1\ 0\ 0) = 1386,$
$e_4 = (0\ 0\ 0\ 1\ 0) = 330, \quad e_5 = (0\ 0\ 0\ 0\ 1) = 210,$
$a \equiv 1155\alpha_1 + 1540\alpha_2 + 1386\alpha_3 + 330\alpha_4 + 210\alpha_5 \pmod{2310}$.

These are all conversion formulas from prime base representation to decimal representation.

2

Let $\mathbb{Z}$ denote the set of integers and $\mathbb{Z}_+$ the set of positive integers. Here are some results in algebra concerning the ring of integers and its quotient rings.

The set $\mathbb{Z}$ of integers forms a ring under addition and multiplication. For $k \in \mathbb{Z}_+$, the set $I_{\pi_k} = \pi_k\mathbb{Z}$ is an ideal in $\mathbb{Z}$.

Let $\mathbb{Z}_{\pi_k} = \mathbb{Z}/\pi_k\mathbb{Z}$ denote the quotient ring of integers consisting of congruence classes modulo π_k. This integer quotient ring has π_k cosets as elements of $\mathbb{Z}_{\pi_k}$. Let the number set $\{0, 1, \ldots, \pi_k - 1\}$ as the set of representatives of the cosets of $\mathbb{Z}_{\pi_k}$, denoted Q_k.

Let $\overline{E}_{\pi_k}$ be the set of cosets formed by all elements in $\mathbb{Z}_{\pi_k}$ that are multiplicatively invertible. Then $\overline{E}_{\pi_k}$ constitutes a subgroup under the coset multiplication in the ring of integers. Let $E_{\pi_k} \subset Q_k$ be the set of representatives of the cosets in $\overline{E}_{\pi_k}$. Then elements in E_{π_k} form a multiplicative group under multiplication modulo π_k.

Theorem 2.1. *E_{π_k} consists of all integers in the interval $[1, \pi_k]$ that are coprime with π_k, i.e.,*

$$E_{\pi_k} = \{a \mid a \in [1, \pi_k], \gcd(a, \pi_k) = 1\}. \tag{2.1}$$

Proof. Since it contains no prime factors $p_1, p_2, \ldots, p_k$,all elements in E_{π_k} are invertible, and these are the only invertible elements in the interval $[1, \pi_k]$. □

Theorem 2.2. *The elements of E_{π_k} consist of 1, all primes in the integer interval $[p_{k+1}, \pi_k]$, and all possible products of these primes lying within the aforementioned interval.*

Proof. First, $1 \in E_{\pi_k}$. Suppose $a \in E_{\pi_k}$ and $a < p_{k+1}$. Then $\gcd(a, \pi_k) > 1$, so $a \in [p_{k+1}, \pi_k]$. Factorizing a: if a is a prime, then a is a prime in $[p_{k+1}, \pi_k]$. If a is composite, since $\gcd(a, \pi_k) = 1$, it must be a product of prime factors in $[p_{k+1}, \pi_k]$ with product not exceeding π_k. □

Theorem 2.3. *Except for the number 1, the smallest element of E_{π_k} is p_{k+1}. Moreover, if $a \in E_{\pi_k}$, $a \neq 1$ and $a < p_{k+1}^2$, then a is prime.* □

According to (2.1) and the definition of the Euler's function, it can be obtained:

Theorem 2.4. *[1] The number of elements in $\overline{E}_{\pi_k}$ or E_{π_k} is $\varphi(\pi_k) = \prod_{i=1}^{k}(p_i - 1)$, where $\varphi(n)$ is Euler's function.* □

For the sake of certainty, in the subsequent discussion of this paper, we will take the number set described in Theorem 2.1 as E_{π_k} .

Definition 2.1. The coset of $\overline{E}_{\pi_k}$ represented by $e \in E_{\pi_k}$ is denoted as $\Gamma_{k,e}$.

Theorem 2.5. $\Gamma_{k,e} = \{e + j\pi_k \mid j \in \mathbb{Z}\}$.

This follows because the ideal of $\mathbb{Z}_{\pi_k} = \mathbb{Z}/\pi_k\mathbb{Z}$ is $I_{\pi_k} = \pi_k\mathbb{Z}$. □

Definition 2.2. The set P_k^+ represents the set of all integers whose prime factors are greater than p_k (including primes greater than p_k).

Theorem 2.6. *Let $a \in P_k^+$, then there exists a unique $q \in E_{\pi_k}$ such that the coset $\Gamma_{k,q}$ of $\overline{E}_{\pi_k}$ satisfies $a \in \Gamma_{k,q}$.*

Proof. Let $a \equiv q \pmod{\pi_k}$ with $0 \leq q < \pi_k$. Then there exists $j \in \mathbb{Z}$ such that $a = q + j\pi_k$. Since $a \in P_k^+$, a has no factors less than p_{k+1}, so neither does q, i.e., $\gcd(q, \pi_k) = 1$. Since $0 \leq q < \pi_k$, we have $q \in E_{\pi_k}$, that is $a \in \Gamma_{k,q}$, and q is unique. □

From Theorem 2.6 we immediately obtain:

Theorem 2.7. $P_k^+ = \bigcup_{e \in E_{\pi_k}} \Gamma_{k,e}$. □

Since the $\Gamma_{k,e}$ are pairwise disjoint, the union in the above Theorem2.7 is actually a direct sum.

The multiplicative subgroup formed by the elements in E_{π_k} described in this section with respect to multiplication modulo π_k,

$$\begin{array}{ll} \text{When } k = 2: & \pi_2 = 6, \quad E_{\pi_2} = \{1, 5\} \\ \text{When } k = 3: & \pi_3 = 30, \quad E_{\pi_3} = \{1, 7, 11, 13, 17, 19, 23, 29\} \end{array}$$

These are simple multiplicative groups modulo π_k.

3

It is straightforward to determine whether a number is prime based on its prime base representation. Theorem 1.2 states that a necessary and sufficient condition for a number to be prime is that its total prime base representation contains exactly one zero, located at the last position.

As previously stated, for a number a with $\pi_{k-1} \leq a < \pi_k$, its prime base representation is

divided into three segments: the first k digits constitute the minimal prime base representation segment, the position from $k+1$ to m form the natural extension segment, followed by the number a.

Related to determine whether a number is prime, we also need to define an important digit position.

Definition 3.1. If for a number a, $p_s \leq \sqrt{a} < p_{s+1}$, then the s-th digit position is called the *prime localization position* of a.

For $a > 121$, the prime localization position lies in the natural extension segment.

Theorem 3.1. *In the total prime base representation of a number a, the set of primes corresponding to the digit positions with values 0 is exactly the set of all factors of a, without multiplicity.* □

Theorem 3.2. *A number a is prime if and only if all position values in its prime base representation before (and including) the prime localization position are non-zero.* □

Theorem 3.3. *Let $a, b \in P_k$, $a = (\alpha_1\ \alpha_2\ \dots\ \alpha_k)$, $b = (\beta_1\ \beta_2\ \dots\ \beta_k)$, then*

$$ab \equiv (\alpha_1\beta_1\ \alpha_2\beta_2\ \dots\ \alpha_k\beta_k)_\rho \pmod{\pi_k} \tag{3.1}$$

The multiplication in parentheses is the usual multiplication, and then the prime modulus is taken.

Proof. This follows from $ab \equiv \alpha_i\beta_i \pmod{p_i}$ and the definition of prime base representation. □

It has been determined in Section 2 that the number set $\{0, 1, \dots, \pi_k - 1\}$ serves as the set of cosets representatives Q_k for $\mathbb{Z}_{\pi_k}$.

Theorem 3.4. *Let $P_k = \{(\alpha_1\ \alpha_2\ \dots\ \alpha_k)\}$ be the set of all numbers with k-digit prime base representation. Then*

$$P_k = \{(\alpha_1\ \alpha_2\ \dots\ \alpha_k)\} = Q_k. \tag{3.2}$$

Moreover, addition and digit multiplication in Q_k are addition and multiplication modulo π_k.

Proof. By Theorem 1.1, the set $\{(\alpha_1\ \alpha_2\ \dots\ \alpha_k)\}$ is exactly the set $\{0, 1, \dots, \pi_k - 1\}$, i.e., it is the set of coset representatives in $\mathbb{Z}_{\pi_k}$. By Theorems 1.3 and 3.3, the consistency of addition and multiplication follows. □

Proposition 3.1. *Let $a = (\alpha_1\ \alpha_2\ \dots\ \alpha_k) \in Q_k$. Then a necessary condition for $a > p_k$ to be prime is that all $\alpha_i \neq 0$.* □

Definition 3.2. If all position values of $a = (\alpha_1\ \alpha_2\ \dots\ \alpha_k)$ are non-zero, then a is called *k-position non-zero* (or non-zero).

In Section 2, we defined the set E_{π_k}, which consists of all intergers in $[1, \pi_k]$ coprime to π_k, and which forms a multiplicative group under multiplication modulo π_k.

Theorem 3.5. *For $Q_k = \{(\alpha_1\ \alpha_2\ \dots\ \alpha_k)\}$, the set of all numbers with non-zero k-digit prime position representations forms the multiplicative group E_{π_k} modulo π_k in $\mathbb{Z}_{\pi_k}$, i.e.,*

$$E_{\pi_k} = \{(\alpha_1\ \alpha_2\ \dots\ \alpha_k) \mid \alpha_i \neq 0\}. \tag{3.3}$$

Proof. First, the set $\{(\alpha_1\ \alpha_2\ \dots\ \alpha_k) \mid \alpha_i \neq 0\} \subset Q_k$. Second, since $\alpha_i \neq 0$, we have

$$\gcd((\alpha_1\ \alpha_2\ \dots\ \alpha_k), p_i) = 1, \quad 1 \leq i \leq k.$$

This holds only for the set $\{(\alpha_1\ \alpha_2\ \dots\ \alpha_k) \mid \alpha_i \neq 0\}$. □

Theorem 3.5 shows that the multiplicative subgroup E_{π_k} of the integer quotient ring $\mathbb{Z}_{\pi_k} = \mathbb{Z}/\pi_k\mathbb{Z}$ has an explicit representation in prime base representation, given by (3.3).

Theorem 3.6. *Let H_i denote the cyclic group of order p_i formed by $\{1, 2, \dots, p_i\}$. Then E_{π_k} is the direct product of its k cyclic groups:*

$$E_{\pi_k} = H_1 \otimes H_2 \otimes \cdots \otimes H_k.$$

This follows directly from (3.3). □

Definition 3.3. Let $(\alpha_1\ \alpha_2\ \dots\ \alpha_{k-1}\ \alpha_k\ \alpha_{k+1}\ \dots\ \alpha_n)$ be the prime base representation of a number. For the segment $(\alpha_1\ \alpha_2\ \dots\ \alpha_{k-1}\ \alpha_k)$, the segment $(\alpha_{k+1}\ \dots\ \alpha_n)$ is called its *successor*, and $(\alpha_1\ \alpha_2\ \dots\ \alpha_{k-1}\ \alpha_k)$ is called the *prefix* of the segment $(\alpha_{k+1}\ \dots\ \alpha_n)$. The only requirement for a segment is that it is non-empty, i.e., $1 < k < n$.

Proposition 3.2. *If two numbers have the same prime base representation for the first k digits, then their difference is $j\pi_k$, $j \in \mathbb{Z}$.*

Proof. The first k digits of the difference of the two numbers are all zero, and thus divisible by $\pi_k \mid (0\ \dots\ 0\ \alpha_{k+1}\ \dots\ \alpha_n)$. □

In Definition 2.1, that the coset of $\overline{E}_{\pi_k}$ represented by $e \in E_{\pi_k}$ is denoted $\Gamma_{k,e}$. From Theorem 2.5 we obtain:

Theorem 3.7. *If $e \in E_{\pi_k}$, then all successors of e form the set of positive integers in the coset $\Gamma_{k,e}$.*

Proof. This is because if $e_1 \in \Gamma_{k,e}$, then $e_1 - e = j\pi_k$ for some $j \in \mathbb{Z}$. □

By Theorem 2.7, $P_k^+ = \bigcup_{e \in E_{\pi_k}} \Gamma_{k,e}$, we immediately obtain:

Theorem 3.8. *All primes greater than p_k are contained in the set $\bigcup_{e \in E_{\pi_k}} \Gamma_{k,e}$, i.e., in the successors of the set E_{π_k} shown in equation (3.3).* □

Theorem 3.9. *For any $e = (a_1\ a_2\ \dots\ a_k) \in E_{\pi_k}$ ($a_i \neq 0$), the corresponding coset $\Gamma_{k,e}$ contains infinitely many primes.*

Proof. This is because $\Gamma_{k,e} = \{e + j\pi_k \mid j \in \mathbb{Z}\}$, and since $e \in E_{\pi_k}$, i.e., $\gcd(e, \pi_k) = 1$, by the following Theorem B, the arithmetic progression $e + j\pi_k$ contains infinitely many primes. □

Theorem B[2] (Dirichlet). If $k > 0$, $l > 0$, and $\gcd(k, l) = 1$, then there are infinitely many primes of the form $kn + l$.

We now study the relationship between E_{π_k} and $E_{\pi_{k+1}}$.

Following the method of Theorem 1.6, we extend E_{π_k} to $E^1_{\pi_{k+1}}$: for any $a = (\alpha_1\ \alpha_2\ \dots\ \alpha_k) \in E_{\pi_k}$, add $\beta \in \{0, 1, \dots, p_{k+1}-1\}$ to the $(k+1)$-th digit position to obtain $a_\beta = (\alpha_1, \alpha_2, \dots, \alpha_k, \beta)_\rho$. Extending all elements of E_{π_k} in this way yields $E^1_{\pi_{k+1}}$. Since E_{π_k} contains all possible non-zero elements, $E^1_{\pi_{k+1}}$ contains the prime p_{k+1} with marking zero. Remove other elements with 0 at the $(k+1)$-th digit position from $E^1_{\pi_{k+1}}$, and the remaining is $E_{\pi_{k+1}}$.
Thus we clearly have:

Theorem 3.10. $E^1_{\pi_{k+1}} \supset E_{\pi_{k+1}}$. □

For the multiplicative subgroup E_{π_k} modulo π_k, we now construct a non-zero tree, or prime tree. Primes are "hanging" on the non-zero tree, and can be classified according to their position on the tree.

As the root of the non-zero tree, $(1) \in E_{\pi_1}$ extends to E_{π_2} with three branches, i.e., after adding the second digit position values $\{0, 1, 2\}$:

$$(1\ 1) = 1, \quad (1\ 0) = 3, \quad (1\ 2) = 5.$$

Here, $(1\ 0) = 3$ is a prime, and the value 0 at the second digit position is the marking zero of prime 3, which does not extend further. The remaining two branches, $1 = (1\ 1)$ and $5 = (1\ 2)$, form E_{π_2}. The corresponding cosets are $\Gamma_{2,1}$ and $\Gamma_{2,5}$, or more explicitly $\Gamma_{(1\ 1)}$ and $\Gamma_{(1\ 2)}$. The advantage of this notation is that all positive elements of the coset Γ are successors of its subscript.

The two branches can be extended to E_{π_3}. Since $p_3 = 5$, the successors of $(1\ 1) = 1$ are five numbers:

$$(1\ 1\ 1) = 1,\ (1\ 1\ 2) = 7,\ (1\ 1\ 3) = 13,\ (1\ 1\ 4) = 19,\ (1\ 1\ 0) = 25.$$

The successors of $(1\ 2) = 5$ are also five numbers:

$$(1\ 2\ 0) = 5,\ (1\ 2\ 1) = 11,\ (1\ 2\ 2) = 17,\ (1\ 2\ 3) = 23,\ (1\ 2\ 4) = 29.$$

The above ten numbers are exactly $E^1_{\pi_3}$.

To convert $E^1_{\pi_3}$ to E_{π_3}, simply remove the numbers with 0 in the third digit position. Retain the non-extending prime 5 branch (1 2 0) and remove the composite 25 branch (1 1 0). Thus, all primes in E_{π_3} appear, belonging to two branches: (1 1) and (1 2), with 8 sub-branches. They form the set $E_{\pi_3} = \{1, 7, 11, 13, 17, 19, 23, 29\}$. From the successor connections, a three-level directed tree is formed.

Similarly, $E^1_{\pi_4}$ can be constructed as follows:

1 (1 1 1 1)	7 (1 1 2 0)	13 (1 1 3 6)	19 (1 1 4 5)
31 (1 1 1 3)	37 (1 1 2 2)	43 (1 1 3 1)	∗49 (1 1 4 0)
61 (1 1 1 5)	67 (1 1 2 4)	73 (1 1 3 3)	79 (1 1 4 2)
∗91 (1 1 1 0)	97 (1 1 2 6)	103 (1 1 3 5)	109 (1 1 4 4)
∗121 (1 1 1 2)	127 (1 1 2 1)	∗133 (1 1 3 0)	139 (1 1 4 6)
151 (1 1 1 4)	157 (1 1 2 3)	163 (1 1 3 2)	∗169 (1 1 4 1)
181 (1 1 1 6)	∗187 (1 1 2 5)	193 (1 1 3 4)	199 (1 1 4 3)
11 (1 2 1 4)	17 (1 2 2 3)	23 (1 2 3 2)	29 (1 2 4 1)
41 (1 2 1 6)	47 (1 2 2 5)	53 (1 2 3 4)	59 (1 2 4 3)
71 (1 2 1 1)	∗77 (1 2 2 0)	83 (1 2 3 6)	89 (1 2 4 5)
101 (1 2 1 3)	107 (1 2 2 2)	113 (1 2 3 1)	∗119 (1 2 4 0)
131 (1 2 1 5)	137 (1 2 2 4)	∗143 (1 2 3 3)	149 (1 2 4 2)
∗161 (1 2 1 0)	167 (1 2 2 6)	173 (1 2 3 5)	179 (1 2 4 4)
191 (1 2 1 2)	197 (1 2 2 1)	∗203 (1 2 3 0)	∗209 (1 2 4 6)

Here, after removing the branches with 0 in the fourth digit position, each branch of the original E_{π_3} extends to 6 branches of E_{π_4}. There are 48 branches in E_{π_4} (composite numbers are marked with asterisks). In addition, non-extending prime branches such as $7 = (1\ 1\ 2\ 0)$ are retained.

Continuing this process, all successors of each element $(\alpha_1\ \alpha_2\ \ldots\ \alpha_k)$ in E_{π_k} form its positive coset $\Gamma_{(\alpha_1\ \alpha_2\ \ldots\ \alpha_k)}$. They are all located in the directed tree rooted at the tree node

$(\alpha_1\ \alpha_2\ \ldots\ \alpha_k)$.

From the above, we can observe the tree structure of the entire non-zero set E_{π_k}, with primes attached to this tree structure. That is, for every positive integer $k > 1$, among the tree nodes of length k, except for elements of E_{π_k}, there is a unique non-extending node p_k.

From the extending branches of the prime tree, we can intuitively identify which primes are unrelated and which share a "bloodline". The length of the common prefix between two primes correlates with their degree of similarity.

4

In this section, we discuss the primality of the sequence n^2+1 ($n \in \mathbb{Z}_+$) and give necessary and sufficient conditions for n^2+1 to be prime.

From Theorem 3.2 in Section 3, we have:

Proposition 4.1. *Let $n \in \mathbb{Z}_+$, and let the prime base representation of n^2+1 up to its prime localization position s be*

$$n^2+1 = (\beta_1\ \beta_2\ \ldots\ \beta_i\ \ldots\ \beta_s). \tag{4.1}$$

Then n^2+1 is prime if and only if all digit values β_i in (4.1) are non-zero. □

Clearly, for n^2+1 to be prime, n must be even, except $n = 1$.

From the definition of the prime localization position (Definition 3.1), we immediately obtain:

Proposition 4.2. *Let p_r be the largest prime satisfying $p_r < n$, i.e., r is the last position of n, then r is the prime localization position s of n^2+1, i.e., $r = s$ and $p_r = p_s$. In other words, the prime localization position s of n^2+1 is the last position of n, that is, the digit position before the static position.*

This is because for even n, p_r is the largest prime less than $\sqrt{n^2+1}$. □

Proposition 4.3. *Let the prime base representation of n be*

$$n = (\alpha_1\ \alpha_2\ \ldots\ \alpha_i\ \ldots\ \alpha_r\ n\ n). \tag{4.2}$$

Then for β_i in (4.1), we have

$$\beta_i \equiv \alpha_i^2 + 1 \pmod{p_i} \quad i = 1, 2, \ldots, r. \tag{4.3}$$

This follows directly from Theorem 3.3 and Theorem 1.3. □

In summary, we have obtained:

Theorem 4.1. *Let*

$$n = (\alpha_1\ \alpha_2\ \ldots\ \alpha_i\ \ldots\ \alpha_r\ n\ n)$$

and

$$n^2+1 = (\beta_1\ \beta_2\ \ldots\ \beta_i\ \ldots\ \beta_s) = (\beta_1\ \beta_2\ \ldots\ \beta_i\ \ldots\ \beta_r)$$

Then n^2+1 is prime if and only if all β_i are non-zero, where $\beta_i \equiv \alpha_i^2 + 1 \pmod{p_i}$ $i = 1, 2, \ldots, r$. □

Thus, whether n^2+1 is prime is closely related to whether the quadratic congruence equation

$$x^2+1 \equiv 0 \pmod{p_i} \tag{4.4}$$

has solutions. The question of whether equation (4.4) has a solution has long been resolved.

Theorem C (Euler's Criterion)[2]. Let p be an odd prime. Then the quadratic congruence equation

$$x^2 \equiv a \pmod{p}$$

has a solution if and only if

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

From this we immediately obtain:

Theorem 4.2. *The congruence equation* (4.4)

$$x^2 \equiv -1 \pmod{p}$$

has a solution if and only if $p = 4k+1$. □

In other words, equation (4.4) has solutions only when the prime p_i is of the form $p_i = 4k+1$. Clearly, its two solutions x_1, x_2 within the residue class $\{0, 1, 2, \ldots, p_i - 1\}$ satisfy $x_1 + x_2 = p_i$.

Definition 4.1. Primes of the form $p = 4k+1$ are called 4^+ primes. The solutions x_1, x_2 to the quadratic congruence equation (4.4) are called the *forbidden number* of the 4^+ prime p_i, denoted z_{i1} and z_{i2}.

Table 4.1. Forbidden numbers of 4^+ primes less than 100: (mod p)

p_i	5	13	17	29	37	41	53	61	73	89	97
z_{i1}	2	8	4	12	6	32	30	50	46	34	22
z_{i2}	3	5	13	17	31	9	23	11	27	55	75

Theorem 4.1 can now be rewritten as:

Theorem 4.3. *Let* $n > 2$ *have prime base representation*

$$n = (\alpha_1\ \alpha_2\ \ldots\ \alpha_i\ \ldots\ \alpha_r\ n\ n),$$

where α_r *is the position value at the last position. Then* n^2+1 *is prime if and only if, for all* 4^+ *primes* p_i *in* $(\alpha_1\ \alpha_2\ \ldots\ \alpha_i\ \ldots\ \alpha_r)$*, the corresponding position values* α_i *are not forbidden numbers, i.e.,*

$$\alpha_i \not\equiv z_{i1} \text{ or } \alpha_i \not\equiv z_{i2} \pmod{p_i}. \tag{4.5}$$

□

From the above, since n is even, for prime 5, its forbidden numbers can be changed to 2 and 8 modulo 10. That is, if n^2+1 is prime, the units digit of n in decimal must be 0, 4, or 6 (except for the first prime 2).

5

Now we study the problem of representing even numbers as the sum of two prime numbers.

Definition 5.1. If an even number b can be expressed as the sum of two primes, then b is said to satisfy the G-condition, and the pair of primes is called a G-representation of b.

Although Theorems 5.1 and 5.2 below are not closely related to the proof of the Goldbach's conjecture, they demonstrate that the method of prime basis representation for integers is a powerful tool for addressing G-representation problems. Their proofs are almost self-evident.

First, we study the representation of even numbers using primes from $\Gamma_{(1\ 1)}$ and $\Gamma_{(1\ 2)}$.

For any even number $a \geq 2$, there are only three possible prefixes for its first two digit positions: (0 0), (0 1), and (0 2). For primes representing them, except for the prefix (1 0) (prime 3), the other prime prefixes are only (1 1) and (1 2). Here we only discuss the latter two cases.

Theorem 5.1.
If the prefix of an even number is (0 1)*, then the only possible prefix combination for the two primes in its*
G-representation is (1 2) + (1 2)*;*
if the prefix of an even number is (0 2)*, then the only possible prefix combination for the two primes in its*
G-representation is (1 1) + (1 1)*;*
if the prefix of an even number is (0 0)*, then the only possible prefix combination for the two primes in its*
G-representation is (1 1) + (1 2). □

In other words, except for prime 3, even numbers with prefix (0 1) can only be represented as the sum of primes from the coset $\Gamma_{(1\ 2)}$; even numbers with prefix (0 2) can only be represented as the sum of primes from the coset $\Gamma_{(1\ 1)}$; even numbers with prefix (0 0) can only be represented as the sum of primes from $\Gamma_{(1\ 2)}$ and $\Gamma_{(1\ 1)}$.

From this, roughly speaking, the number of prime pairs representing (0 1)-type even numbers is about the same as for (0 2)-type, while for (0 0)-type it is about twice as many.

Theorem 5.2. *Let* $2a$ *be an even number,* $a \in \mathbb{Z}_+$*, and let* p_k *be the smallest prime satisfying* $p_k \geq a$*. If in the prime base representation of* $2a$*, the position value at the* i*-th digit position* $(i \geq k)$ *is a prime* q_i*, then the even number* $2a$ *satisfies the G-condition. Moreover, all such prime pairs* (p_i, q_i) *form all G-representations of* $2a$*.*

This is because for $j \geq k$, the position value at the j-th digit position before the last position is $2a - p_j$. □

We now study the problem of representing even numbers as the sum of two prime numbers, namely the Goldbach's conjecture.

Definition 5.2. Let $\mathbb{Z}_2^-$ denote the set of even integers greater than 24.

Definition 5.3. Let $a = (\alpha_1\ \ldots\ \alpha_i\ \ldots\ \alpha_k)$ and $b = (\beta_1\ \ldots\ \beta_i\ \ldots\ \beta_k)$. If for some i, $\alpha_i = \beta_i$, then a and b are said to intersect at the i-th digit position; if for all digit positions $i \in \{1, 2, \ldots, k\}$, $\alpha_i \neq \beta_i$, then the two numbers are said to be completely non-intersecting in all k digit positions, or simply a and b are non-intersecting.

Let the prime base representation of an even number a be $a = (0\ \alpha_2\ \ldots\ \alpha_s)$, where s is the prime localization position of a. Let the prime base representation of a prime $q < a$ up to digit

position s be $q = (1\ q_2\ \dots\ q_s)$.

By Definition 5.3, the even number a and prime q are completely non-intersecting up to s if the corresponding values from digit position 1 to s are all different: $\alpha_i \neq q_i, \quad i = 1, 2, \dots, s$.

Theorem 5.3. *Let $a - q \neq 1$, here a is even number and $q(q < a)$ is a prime, then $a - q$ is prime if and only if prime q is completely non-intersecting with a up to s, unless the intersecting digit position is the marking zero position of the prime $a - q$.*

Proof. If for some i,

$$\alpha_i \equiv q_i \pmod{p_i}, \quad i = 1, 2, \dots, s,$$

then the i-th digit position value of $a - q$ is 0, and unless this intersecting digit position is the marking zero position for prime $a - q$, otherwise, $a - q$ is not prime. Conversely, if prime q and a is completely non-intersecting in all digit positions s, then all position values of $a - q$ from 1 to s are non-zero, and $a - q$ is prime. □

Note that when $a - q \leq p_s$, if $a - q$ is prime, then the marking zero position of prime $a - q$ lies within the prime localization position of a, where a and q have equal values. At this digit position, we can determine whether $a - q$ is prime based on Theorem 1.2 by checking if this 0 is the marking zero of $a - q$.

For this case, we can also proceed as follows: since $a > 4$, $s < a/2$, so if $q_1 + q_2 = a$, then one prime must be less than $a/2$. Therefore, for q in Theorem 5.3, we only need to consider primes less than $a/2$. Thus, using all primes less than $a/2$ to test the G-condition of even number a will not miss any cases. (However, in the proof of the following theorem, this situation does not arise.)

Goldbach's conjecture is the following theorem.

Theorem 5.4. *Every even number in the set $\mathbb{Z}_2^-$ has a G-representation.*

Proof. We will use the following lemmas to gradually provide the proof, with the argumentation basis being Theorem 5.3.

First, consider the prime base representation of prime 3: $p_2 = 3 = (1\ 0\ 3\ 3\ 3\ \dots)$. For even numbers $a > p_2+1$, there are only two cases: either intersecting with prime 3 or not intersecting. If an even number a intersects with prime 3, then its second digit position value is 0, or some digit position value from the third digit position to the prime localization position of a is 3. We denote the set of such numbers as $X[p_2]$.

Definition 5.4. Let the even numbers a such that $a > p_i + 1$, and denote the set of numbers where $\mathbb{Z}_2^-$ intersects with p_i as $X[p_i]$.

Definition 5.5. Let $\alpha_2 \in [0, 1, 2]$. The notation $(0\ \alpha_2)_X$ denotes the set of even numbers in prime base representation with prefix $(0\ \alpha_2)$. Also, $(0\ \mathrm{x}\ \alpha_3)_X$ denotes the set of even numbers in prime base representation where the third digit position value is α_3 and the second digit position is arbitrary. Additionally, if a certain digit position value in the prefix is p^+ (where p is prime), it indicates that p appears at some position from this digit position to the even number's prime localization position. Other cases are analogous. All the above operations are performed up to the even number's prime localization position.

From the above definitions, we have:

Lemma 5.1. *$X[p_2] = \{(0\ 0)_X, (0\ \mathrm{x}\ 3^+)_X\}$. If $a \in \mathbb{Z}_2^- - X[p_2]$, then a does not intersect with p_2, i.e., $a - 3$ is prime. Thus, all even numbers in $\mathbb{Z}_2^- - X[p_2]$ have a G-representation.* □

Definition 5.6. The subsets in $X[p_i]$ are called the intersecting subsets of prime p_i.

Similarly, since $p_3 = 5 = (1\ 2\ 0\ 5\ 5\ 5\ \dots)$, we have:

Lemma 5.2. $X[p_3] = \{(0\ 2)_X, (0\ \mathrm{x}\ 0)_X, (0\ \mathrm{x}\ \mathrm{x}\ 5^+)_X\}$. □

Consider the set $X[p_2] \cap X[p_3]$. Even numbers in this set intersect with both primes p_2 and p_3, meaning they cannot form a G-representation with p_2 and p_3. This also means that even numbers in $\mathbb{Z}_2^- - (X[p_2] \cap X[p_3])$ have a G-representation with p_2 or p_3.

From Lemmas 5.1 and 5.2, we immediately obtain:

Lemma 5.3. $X[p_2] \cap X[p_3] = \{(0\ 0\ 0)_X, (0\ 2\ 3^+)_X, (0\ 0\ \mathrm{x}\ 5^+)_X, (0\ \mathrm{x}\ 0\ 3^+)_X, (0\ \mathrm{x}\ 3^+\ 5^+)_X\}$.

The intersecting subsets in $X[p_2] \cap X[p_3]$ are obtained by performing intersection operations on the intersecting subsets from $X[p_2]$ and $X[p_3]$, respectively. □
It is easy to see that the smallest number in $X[p_2] \cap X[p_3]$ is $30 = (0\ 0\ 0\ 2)$. That is, when $a \in \mathbb{Z}_2^-$ and $a < 30$, $a \notin (X[p_2] \cap X[p_3])$, so a has a G-representation.

Lemma 5.4. *Let the even number $a = (0\ \alpha_2\ \dots\ \alpha_i\ \dots\ \alpha_k) \in Q_k$. Then there are infinitely many primes completely non-intersecting with a.*

Proof. First, from the construction of the multiplicative group E_{π_k}, there are at least $\prod_{i=2}^{k}(p_i - 2)$ elements in E_{π_k} that do not intersect with a. Second, by Theorems 3.8 and 3.9, there are infinitely many primes completely non-intersecting with a. □

Lemma 5.5. *Let $h_k = \min\{h \mid h \in \bigcap_{i=2}^{k} X[p_i]\}$. Then as k increases, h_k is an increasing sequence tending to infinity.*

Proof. Clearly, $h_k \geq h_{k-1}$. We now prove that it tends to infinity.

Let $h_k = (0\ \alpha_2\ \alpha_3\ \dots\ \alpha_j) \in \bigcap_{i=2}^{k} X[p_i]$ be the smallest number in $\bigcap_{i=2}^{k} X[p_i]$, where $j = s_{h_k}$ is the prime localization position of h_k.
If h_k and p_{k+1} are non-intersecting, then $h_k \notin X[p_{k+1}]$, therefore

$$h_{k+1} = \min\{h \mid h \in \bigcap_{i=2}^{k+1} X[p_i]\} > h_k$$

If h_k and p_{k+1} are intersecting, since h_k is a number with fixed digit position values, by Lemma5.4, it can only be contained in a finite number of intersecting subsets of l consecutive primes at most, i.e., there exists $l \geq 1$, such that

$$h_k \in X[p_{k+i}] \quad (i = 1, 2, \dots, l)$$

and for the number $n = k + l + 1$, it has

$$h_k \notin X[p_n]$$

It also has

$$h_n = \min\{h \mid h \in \bigcap_{i=2}^{n} X[p_i]\} > h_k$$

Thus, as k tends to infinity, h_k is an increasing sequence tending to infinity. □

Lemma 5.5 shows that even numbers in $\mathbb{Z}_2^- \cap \{0, h_k\}$ all have a G-representation with some prime from the set $\{p_2, p_3, \dots, p_k\}$. Since h_k tends to infinity, every even number in $\mathbb{Z}_2^-$ has a G-representation.

Theorem 5.4 is thus proved. □

References

1. Yan Songyuan, *Number Theory for Computing*, pp. 113, 69, Springer, 2nd Edition, 2002. (Chinese translation)

2. Hua Luogeng, *Introduction to Number Theory*, pp. 258, 40, Science Press, 1957. (Chinese edition)

DEPARTMENT OF MATHEMATICS, ZHEJIANG UNIVERSITY, HANGZHOU 310027,
PEOPLE'S REPUBLIC OF CHINA
Email address: ymd@zju.edu.cn