A NEW VIEW OF THE NATURAL NUMBER SET N

It will be another million years, at least, before we understand the primes.

— *Paul Erdös*

Bao Qi Feng[a,*], Louis Feng[b], Dong Ning Zhao[c]

[a] *Department of Mathematical Sciences, Kent State University at Tuscarawas, New Philadelphia, OH 44663, USA.*

[b] *Department of Computer Sciences, University of California, Davis Campus, Davis, CA 94947 USA.*

[c] *Retired, 3255 Holly Hill Dr., Falls Church, VA 22042, USA.*

Abstract

In 1981, Paul Pritchard [1], [2] created remarkably a new sieve for finding all prime numbers in the natural number set N. In this article we give a new instruction of N, from which we can see a new view of the distribution of prime numbers in the set N. We also give a strictly mathematical proof for the Pritchard Sieve for offering it a solid mathematical support. Finally we give new proofs for the infinitude and the asymptotic density formula of the primes number set P in the natural number set N respectively.

1. Introduction

To improve the *Eratosthenes' Sieve* for finding prime numbers by computer, in 1981, Paul Pritchard [1], [2] created remarkably a new sieve for finding all prime numbers in the natural number set N, which is called the *Dynamic Wheel Sieve*. The Pritchard's Sieve starts a singleton set $W_0 = \{1\}$, and the first two prime numbers $p_1 = 2$ and $p_2 = 3$ with only using additions and multiplications step by step to construct an infinite sequence of nonempty finite sets

$$U_1,\ U_2,\ U_3,\ \cdots,$$

in which U_1 does not contain the multiples of 2, U_2 does not contain the multiples of 2 and 3, U_3 does not contain the multiples of 2, 3 and 5, and so on. In each wheel sifting out one

* Corresponding author

2010 Mathematics Subject Classification: 10H32, 11A41, 11B25, 11N35

Keywords and Phrases. Arithmetic progression, asymptotic density, composite number, least prime factor, prime number, sieve, *Eratosthenes' Sieve*.

E-mail address bfeng@kent.edu (B. Feng); zfeng@ucdavis.edu (L. Feng).

prime number, we finally get all prime numbers in N because the process of constructing the finite set of U_k can be proceeded infinitely.

The Pritchard's Sieve motivates us to afresh learning the natural number set N. It leads to yield an elegant construction of N, from which we discover a new view of the distribution of the prime numbers in the natural number set N. In this article we also give a strictly mathematical proof for Pritchard's Sieve. Using Pritchard Algorithm we give an example to find all primes among 1 to 200, from which we can see what a beautiful mind Pritchard's is! Finally we give new proofs for the infinitude and the asymptotic density formula of the primes number set P in the natural number set N respectively.

2. Definitions And Properties

Let $a,\ b \in N$, saying a, b relatively prime if $(a, b) = 1$, where (a, b) represents the greatest common factor of a and b. Let the set of all prime numbers be $P = \{p_1, p_2, \cdots\}$, where $p_1 = 2,\ p_2 = 3$ and $p_i < p_j$, if $i < j$. For $k \geq 1$ denote $\pi_k = \prod_{i=1}^{k} p_i,\ \ \pi_0 = 1$, and $C_0 = N$. For $k \geq 1$, define

$$S_k = \{a \in C_0 : lpf(a) = p_k\}$$

where $lpf(a)$ denotes the least prime factor of a. Define

$$C_k = \{a \in C_0 : (a, \pi_k) = 1\}.$$

S_k is called the k^{th}-*shell* of N and C_k is called the k^{th}-*core* of N.

Theorem 1 *The sequence of sets $\{C_k\}$ is strictly decreasing and*

$$\lim_{k\to\infty} C_k = \bigcap_{k=1}^{\infty} C_k = \{1\}.$$

Proof. If $x \in C_k$, then $(x, \pi_k) = 1 \ \Rightarrow\ (x, \pi_{k-1}) = 1 \Rightarrow\ x \in C_{k-1}$, so $C_k \subset C_{k-1}$ for all k. Adding that $p_k \in C_{k-1}$, but $p_k \notin C_k$ for all $k \in N$. Hence $\{C_k\}$ is strictly decreasing sequence.
If $x \in \bigcap_{k=1}^{\infty} C_k$, then $(x, \pi_k) = 1$ for all $k \in N$, which imply $x = 1$. Hence $\lim_{k\to\infty} C_k = \bigcap_{k=1}^{\infty} C_k = \{1\}$. □

Theorem 2 *There are the following relations between the shells and the cores of N, if $k \geq 1$, then*

(1) $S_k \subset C_{k-1}$,
(2) $S_k \cap C_k = \phi$,
(3) $C_{k-1} = S_k \cup C_k$,
(4) $S_k = p_k C_{k-1}$,
(5) $C_k = C_{k-1} - p_k C_{k-1}$,

Proof. (1) $x \in S_k \Rightarrow lpf(x) = p_k \Rightarrow (x, \pi_{k-1}) = 1 \Rightarrow x \in C_{k-1}$.

(2) If $x \in S_k \cap C_k \Rightarrow lpf(x) = p_k$ and $(x, \pi_k) = 1$. It is contradictory. Hence $S_k \cap C_k = \phi$.

(3) $x \in C_{k-1} \Rightarrow (x, \pi_{k-1}) = 1$. If $lpf(x) = p_k \Rightarrow x \in S_k$, or if $lpf(x) > p_k \Rightarrow x \in C_k$. Hence $C_{k-1} \in S_k \cup C_k$. The another direction is following Theorem 1 and (1) of this theorem.

(4) $x \in S_k \Leftrightarrow lpf(x) = p_k \Leftrightarrow x = ap_k$, where $(a, \pi_{k-1}) = 1 \Leftrightarrow x \in p_k C_{k-1}$.

(5) From (2), (3) and (4). □

From Theorem 2(1) we have an equivalent representation of S_k

$$S_k = \{a \in C_{k-1} : lpf(a) = p_k\}.$$

Theorem 3 *For any $k \in N$, the collection of sets $\{S_1, S_2, \cdots, S_k, C_k\}$ forms a partition of N; that is*
(1) $S_i \cap S_j = \phi$, $i \neq j$, $1 \leq i, j \leq k$; *and* $S_i \cap C_k = \phi$, $1 \leq i \leq k$;
(2) $N = S_1 \cup \cdots \cup S_k \cup C_k$.

Proof. (1) Fix $k \in N$. Suppose $S_i \cap S_j \neq \phi$, $i \neq j, 1 \leq i, j \leq k$, then there is $x \in S_i \cap S_j$. That is $p_i = lpf(x)$ and $p_j = lpf(x)$, which implies $p_i = p_j$ and $i = j$. Contradicting with $i \neq j$. That $S_i \cap C_k = \phi$, $1 \leq i \leq k$ is obvious.

(2) If $x \in N$, then $lpf(x) = p_s$ for some $s \in N$. If $1 \leq s \leq k$, then $x \in S_s$; If $s > k$, then $(x, \pi_k) = 1$, which implies $x \in C_k$. Thus, $N \subset S_1 \cup \cdots \cup S_k \cup C_k$. The another direction is obvious. □

Theorem 4 *For any $k \in N$,*
(1) min $S_k = p_k$. *If $x \in S_k$ and $x \neq p_k$, then x is a composite number.*
(2) *The least element of the set $C_k - \{1\}$ must be a prime number, and it is p_{k+1} exactly.*

Proof. (1) Obviously.

(2) Let $m = \min(C_k - \{1\})$. Suppose that m has a factor $d \in N$, $d \leq m$. If $1 \neq d < m$, then $d \notin C_k$, which implies $d \in S_j$, for some j, $1 \leq j \leq k$ by Theorem 3(2). Thus, $p_j \mid d$, which implies $p_j \mid m$. It is impossible, since $(m, \pi_k) = 1$. That is $d = m$. Hence m is a prime number. Since p_{k+1} is the least prime number in $C_k - \{1\}$, so $m = p_{k+1}$. □

Theorem 5 (1) *If* $\pi_k \le n < \pi_{k+1}$, *for some* $k \in N$, *then*

$$P\{n\} \subset \{p_1, p_2, \cdots, p_k\} \cup C_k\{n\}.$$

(2) *If* $p_s^2 \le n < p_{s+1}^2$, $p_s, p_{s+1} \in P$ *for some* $s \in N$, *then*

$$P\{n\} = \{p_1, \cdots, p_s\} \cup (C_s\{n\} - \{1\}),$$

where we use the notation $A\{n\} = \{a \in A : a \le n\}$.

Proof. (1) It is obvious that

$$P\{n\} = \{p_1, \cdots, p_k\} \cup \{p \in P \ : \ p_{k+1} \le p \le n\} \subset \{p_1, \cdots, p_k\} \cup C_k\{n\}.$$

(2) It is clear that

$$P\{n\} \subset \{p_1, \cdots, p_s\} \cup (C_s\{n\} - \{1\}), \text{ and } P\{n\} \supset \{p_1, \cdots, p_s\}.$$

If $x \in C_s\{n\} - \{1\}$, then $x \le n$, and $(x, p_i) = 1$, $1 \le i \le s$. Suppose x is composite number, then x is divided by a prime number p, which satisfies that $p \le p_s \le \sqrt{x} < p_{s+1}$, it is absurd from $(x, \pi_s) = 1$. That is $C_s\{n\} - \{1\}$ consists of prime numbers only, and $C_s\{n\} - \{1\} \subset P\{n\}$. Hence

$$P\{n\} = \{p_1, \cdots, p_s\} \cup (C_s\{n\} - \{1\}).$$

□

3. The Structures of C_k, S_k and N.

For next discussion we need the following lemmas.

Lemma 1 *Suppose that* $a, d \in N$, $p_k \in P$ *with* $(p_k, d) = 1$. *Let*

$$A = \{a_q : a_q = a + (q-1)d, q \ge 1\}$$

and

$$a_i = a + (i-1)d, \qquad 1 \le i \le p_k,$$

$$[a_i] = \{a_i + (q-1)dp_k : q \ge 1\}, \quad 1 \le i \le p_k.$$

Then the collection of sets $\{[a_i] : 1 \le i \le p_k\}$ *is a partition of* A; *that is*

(1) $[a_i] \cap [a_j] = \phi$, *if* $i \ne j$, $1 \le i, j \le p_k$, *and*

(2) $A = \bigcup_{i=1}^{p_k} [a_i]$.

Proof. (1) Suppose $x \in [a_i] \cap [a_j]$, then $x = a_i + (q_i - 1)dp_k = a_j + (q_j - 1)dp_k \Rightarrow a_i - a_j = (q_i - q_j)dp_k = (i - j)d \Rightarrow i - j = (q_i - q_j)p_k$, where $i \neq j$, $1 \leq i, j \leq p_k$. Thus, $p_k \mid |i - j|$, but $0 \leq |i - j| < p_k \Rightarrow i = j$. Contradiction. Hence $[a_i] \cap [a_j] = \phi$.

(2) We just need to verify that $A \supset \bigcup_{i=1}^{p_k} [a_i]$. Suppose that $x \in A$, then there is $q \in N$ such that $x = a + (q - 1)d$. From the division algorithm we have $q - 1 = bp_k + r$, $0 \leq r < p_k$, where $b = 0, r = q - 1$ if $0 \leq q - 1 < p_k$; or $b > 0$, if $q - 1 \geq p_k$. Then $x = a + (bp_k + r)d = a + rd + bp_k d = a_i + bp_k d$, where $i = r + 1 \leq p_k$. It implies $x \in [a_i]$. Hence $A \subset \bigcup_{i=1}^{p_k} [a_i]$. □

Lemma 2 *For any given $a, d \in N$, $p_k \in P$ with $(p_k, d) = 1$, there exists a term a_m, which is the unique one of the first p_k terms of the arithmetic progression*

$$\{a_n : a_n = a + (n - 1)d, \quad n \geq 1\},$$

such that $p_k \mid a_m$.

Proof. It follows the properties of cyclic group. □

The following two theorems exhibit the structures of C_k and S_k. Combining them with Theorem 3, we have an elegant view to the natural number set of N.

Theorem 6 *Suppose that $k \in N$. The set C_k consists of $\prod_{i=1}^{k}(p_i - 1)$ many arithmetic progressions with the common difference of π_k. They form a partition of C_k. Precisely,*

$$C_k = \bigcup_{i=1}^{\prod_{j=1}^{k}(p_j - 1)} [a_i],$$

where

$$a_i \in C_{k-1},\ 1 \leq a_i < \pi_k,\ \textit{and}\ (a_i, \pi_k) = 1$$

and

$$[a_i] = \{a_i + \pi_k(q - 1) : q \geq 1\},\ \textit{for}\ 1 \leq i \leq \prod_{j=1}^{k}(p_j - 1),$$

are disjoint.

Proof. Use the induction on k. When $k = 1$,

$$\begin{aligned} C_1 &= \{a \in C_0 : (a, \pi_1) = 1\} = \{a \in C_0 : (a, 2) = 1\} \\ &= \{1, 3, 5, 7, \cdots\} = \{1 + 2(q - 1) : q \geq 1\} \\ \bigcup_{i=1}^{\prod_{j=1}^{k}(p_j - 1)} [a_i] &= \bigcup_{i=1}^{1} [a_i] = [a_1]. \\ \text{and} \quad a_1 &\in C_{k-1} = C_0, \quad 1 \leq a_1 < \pi_1 = 2, \text{and } (a, \pi_1) = 1 \text{ which imply } a_1 = 1. \\ \text{Thus,} \quad [a_1] &= \{1 + \pi_1(q - 1) : q \geq 1\} = \{1 + 2(q - 1) : q \geq 1\}. \end{aligned}$$

The theorem holds in the case of $k = 1$. Assume that the theorem holds for $k \geq 1$. Notice that the general term of the *i-th* equivalent class $[a_i]$ in C_k is

$$[a_i] = \{a_i + \pi_k(q-1) : q \geq 1\},$$

where

$$a_i \in C_{k-1},\ 1 \leq a_i < \pi_k, \text{ and } (a_i, \pi_k) = 1.$$

Let

$$b_t = a_i + \pi_k(t-1), \quad 1 \leq t \leq p_{k+1}.$$

By Lemma 1,

$$[a_i] = \bigcup_{t=1}^{p_{k+1}} [b_t],$$

where $[b_t] = \{d_q : d_q = b_t + \pi_{k+1}(q-1),\ q \geq 1\},\ 1 \leq t \leq p_{k+1}$, are disjoint. That means each arithmetic progression $[a_i]$ with the common difference π_k in C_k can be split into p_{k+1} many of arithmetic progressions with the common difference π_{k+1}. By Lemma 2, since $(\pi_k, p_{k+1}) = 1$, there exists a unique term b_j in $\{b_1, \cdots, b_{p_{k+1}}\}$, such that $p_{k+1} \mid b_j$, so we have $p_{k+1} \nmid b_t$, if $t \neq j$, and $1 \leq t \leq p_{k+1}$. That means there are $p_{k+1} - 1$ many of arithmetic progressions with the common difference π_{k+1} in each equivalence class $[a_i]$ of C_k, and every element in these progressions is relatively prime with p_{k+1}. Hence C_{k+1} consists of $(p_{k+1} - 1)\prod_{i=1}^{k}(p_i - 1) = \prod_{i=1}^{k+1}(p_i - 1)$ many of arithmetic progressions with the common difference π_{k+1} and from Lemma 1 we know that they form a partition of C_{k+1}. The conclusion holds by the induction. □

Theorem 7 *Suppose that $k \geq 2$. Then the set S_k consists of $\prod_{i=1}^{k-1}(p_i - 1)$ many arithmetic progressions with the common difference of π_k. They form a partition of S_k. Precisely,*

$$S_k = \bigcup_{i=1}^{\prod_{j=1}^{k-1}(p_j-1)} [a_i],$$

where

$$a_i \in p_k C_{k-1},\ 1 \leq a_i < \pi_k,$$

and

$$[a_i] = \{a_i + \pi_k(q-1) : q \geq 1\},\ for\ 1 \leq i \leq \prod_{j=1}^{k-1}(p_j - 1),$$

are disjoint.

Proof. From the proof of Theorem 6 we know that S_{k+2} consists of $\prod_{i=1}^{k}(p_i - 1)$ many of arithmetic progressions with the common difference π_{k+1}, and they form a partition of S_{k+1}. Replacing $k+1$ by k, the conclusion holds. □

Base on the discussion above, we have a new view of structure of the natural number set of N as follows.

Theorem 8 *Suppose N is the positive integer set and S_k and C_k are the k^{th}-shell and k^{th}- core of N, and $m \geq 2$. Then*

$$N = S_1 \cup C_1 = [2] \cup \left(\bigcup_{k=2}^{m} \bigcup_{i=1}^{\prod_{j=1}^{k-1}(p_j-1)} [a_i^{(k)}] \right) \bigcup \left(\bigcup_{i=1}^{\prod_{j=1}^{m}(p_j-1)} [b_i^{(m)}] \right),$$

where

$$[2] = \{2 + \pi_1(q-1) : q \geq 1\},$$

$$a_i^{(k)} \in p_k C_{k-1},\ 1 \leq a_i^{(k)} < \pi_k,$$

$$[a_i^{(k)}] = \{a_i^{(k)} + \pi_k(q-1) : q \geq 1\},\ \ for\ \ 1 \leq i \leq \prod_{j=1}^{k-1}(p_j - 1);$$

and

$$b_i^{(m)} \in C_{m-1},\ 1 \leq b_i^{(m)} < \pi_m,\ and\ (b_i^{(m)}, \pi_m) = 1$$

$$[b_i^{(m)}] = \{b_i^{(m)} + \pi_m(q-1) : q \geq 1\},\ \ for\ \ 1 \leq i \leq \prod_{j=1}^{m}(p_j - 1).$$

Proof It follows Theorems 3, 6, and 7. □

4. The Densities of C_k, S_k in N.

Let A be a subset of N and $A(n)$ be the counting function of the set A:

$$A(n) = |A\{n\}|,$$

where $|A|$ is the cardinality of the set A. Recall that A has asymptotic density $d(A)$, if the following limit

$$d(A) = \lim_{n\to\infty} \frac{A(n)}{n}$$

exists. It is clear that $d(N) = 1$.

Lemma 3 (1) *If $A \subset N$ and $B \subset N$, and $A \cap B = \phi$, then $d(A \cup B) = d(A) + d(B)$.*
(2) *If arithmetic progression $A = \{a_n\}$ with common difference d, then $d(A) = 1/d$.*

Proof (1) is clear from the definition of asymptotic density. For (2), let

$$A = \{a_n = a_1 + (n-1)d : n \geq 1\}.$$

Then,

$$d(A) = \lim_{n\to\infty} \frac{n}{a_1 + (n-1)d} = \frac{1}{d}.$$

□

Theorem 9 *Suppose that $k \geq 1$. Then the asymptotic densities $d(S_k)$ and $d(C_k)$ of the sets S_k and C_k are*

$$d(S_1) = \frac{1}{2},$$

$$d(S_k) = \frac{1}{p_k}\prod_{i=1}^{k-1}\left(1 - \frac{1}{p_i}\right), \quad for \quad k \geq 2$$

and

$$d(C_k) = \prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)$$

respectively.

Proof. Firstly, we know that $S_1 = \{a \in C_0 : lpf(a) = p_1 = 2\} = \{2 + 2(q-1) : q \geq 1\}$. By Lemma 3(2), $d(S_1) = 1/2$. Next, from Theorem 6 we knew that

$$C_k = \bigcup_{i=1}^{\prod_{j=1}^{k}(p_j-1)} [a_i],$$

where

$$a_i \in C_{k-1},\ 1 \leq a_i < \pi_k,\ \text{and}\ (a_i, \pi_k) = 1$$

and

$$[a_i] = \{a_i + \pi_k(q-1) : q \geq 1\},\ \text{for}\ 1 \leq i \leq \prod_{j=1}^{k}(p_j - 1),$$

are disjoint. From Lemma 3(2), we know $d([a_i]) = 1/\pi_k$ for all $1 \leq i \leq \prod_{j=1}^{k}(p_j - 1)$. $[a_i] \cap [a_j] = \phi$, when $i \neq j$, which implies by Lemma 3(1) that

$$d\left(C_k\right) = \sum_{i=1}^{\prod_{j=1}^{k}(p_j-1)} d([a_i]) = \sum_{i=1}^{\prod_{j=1}^{k}(p_j-1)} \frac{1}{\pi_k} = \frac{1}{\pi_k}\prod_{j=1}^{k}(p_j - 1) = \prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right).$$

Similarly, use Theorem 7, if $k \geq 2$, then

$$S_k = \bigcup_{i=1}^{\prod_{j=1}^{k-1}(p_j-1)} [a_i],$$

where

$$a_i \in p_k C_{k-1},\ 1 \le a_i < \pi_k,$$

and

$$[a_i] = \{a_i + \pi_k(q-1) : q \ge 1\},\ \text{ for } 1 \le i \le \prod_{j=1}^{k-1}(p_j - 1),$$

are disjoint. It implies by Lemma 3

$$d(S_k) = \sum_{i=1}^{\prod_{j=1}^{k-1}(p_j-1)} d([a_i]) = \sum_{i=1}^{\prod_{j=1}^{k-1}(p_j-1)} \frac{1}{\pi_k} = \frac{1}{\pi_k}\prod_{j=1}^{k-1}(p_j-1) = \frac{1}{p_k}\prod_{i=1}^{k-1}\left(1-\frac{1}{p_i}\right).$$

□

From the discussions above, we have an identity about primes.

Theorem 10 *Let the set of all prime numbers be $P = \{p_1, p_2, \cdots\}$, where $p_1 = 2,\ p_2 = 3$ and $p_i < p_j$, if $i < j$. Then for all $m \ge 2$*

$$\sum_{k=2}^{m} \frac{1}{p_k}\prod_{j=1}^{k-1}\left(1-\frac{1}{p_i}\right) + \prod_{i=1}^{m}\left(1-\frac{1}{p_i}\right) = \frac{1}{2}.$$

Proof The conclusion follows Lemma 3, Theorems 8 and 9. □

The identity in Theorem 10 is amazing, but it doesn't offer any relation between p_m and p_{m+1}.

Theorem 11 *Suppose $k \ge 2$, then the values of the counting functions $C_k(n),\ C_{k-1}(n)$ and $S_k(n)$ at $n = \pi_k$ are respectively*

$$C_k(\pi_k) = \prod_{i=1}^{k}(p_i - 1), \quad S_k(\pi_k) = \prod_{i=1}^{k-1}(p_i - 1)$$

and

$$C_{k-1}(\pi_k) = p_k \prod_{i=1}^{k-1}(p_i - 1).$$

Proof. The first two equalities follow Theorem 6 and Theorem 7 immediately. The last equality holds from Theorem 2(3). □

The Theorem 11 shown us that in the set $\{1, 2, \cdots, \pi_k\}$ $(k \ge 2)$, there are exactly $\prod_{i=1}^{k-1}(p_i - 1)$ many numbers, which has the least prime factor p_k; there are exactly $\prod_{i=1}^{k}(p_i - 1)$ many numbers, which are relatively prime with π_k and there are exactly $p_k \prod_{i=1}^{k-1}(p_i - 1)$ many numbers, which are relatively prime with π_{k-1}.

5. The Pritchard Algorithm

The following result is the base of the Pritchard Algorithm.

Theorem 12 *Let* $W_0 = \{1\}$, $p_1 = 2$, $p_2 = 3$, $\pi_1 = p_1$, *and* $\pi_2 = p_1p_2$. *Define*

$$U_1 = \{c + \pi_1(q-1) : 1 \le q \le p_2, \text{ and } c \in W_0\},$$

$$V_1 = p_2W_0 \text{ and } W_1 = U_1 - V_1, \text{ and } p_3 = \min(W_1 - \{1\}).$$

Define

$$U_2 = \{c + \pi_2(q-1) : 1 \le q \le p_3, \text{ and } c \in W_1\},$$

$$V_2 = p_3W_1 \text{ and } W_2 = U_2 - V_2 \text{ and } p_4 = \min(W_2 - \{1\}).$$

In general, for $k \ge 2$, *let* $\pi_k = \prod_{i=1}^{k} p_i$, *and* $p_{k+1} = \min(W_{k-1} - \{1\})$. *Define*

$$U_k = \{c + \pi_k(q-1) : 1 \le q \le p_{k+1}, \text{ and } c \in W_{k-1}\},$$

$$V_k = p_{k+1}W_{k-1} \; W_k = U_k - V_k, \quad \text{and } p_{k+2} = \min(W_k - \{1\}.$$

Then for each $k \ge 1$,

(1) $U_k = C_k\{\pi_{k+1}\}$;
(2) $V_k = S_{k+1}\{\pi_{k+1}\}$ *and* $V_k \subset U_k$;
(3) $W_k = C_{k+1}\{\pi_{k+1}\}$;
(4) $|U_k| = p_{k+1}\prod_{i=1}^{k}(p_i - 1)$, $|V_k| = \prod_{i=1}^{k}(p_i - 1)$ *and* $|W_k| = \prod_{i=1}^{k+1}(p_i - 1)$.
(5) p_{k+2} *exists, it is a prime and* $p_{k+2} > p_{k+1}$;

Proof. Using the induction on k. First of all, if $k = 2$, then $p_2 = 3$. By the definitions of U, V, and W, we have

$$U_1 = c + \pi_1(q-1) : 1 \le q \le p_2, c \in W_0\} = \{1 + 2(q-1) : 1 \le q \le 3\} = \{1, 3, 5\},$$

$$V_1 = p_2\, W_0 = \{3\} \text{ and } W_1 = U_1 - V_1 = \{1, 5\} \text{ and } p_3 = \min W_1 = \{1\} = 5.$$

We see that $p_3 > p_2$. The same computation we have

$$U_2 = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29\},$$

$V_2 = p_3W_1 = \{5, 25\}$ and $W_2 = \{1, 7, 11, 13, 17, 19, 23, 29\}$ and $p_4 = \min W_2 = \{1\} = 7$.

It is easy to check $(1) - (5)$ hold for $k = 2$. Similarly, we can check immediately that $(1) - (5)$ hold for $k = 3$.

Suppose that $(1) - (5)$ hold for $1, 2, \cdots, k$ $(k \ge 3)$.

(1) By the definition we know that

$$U_{k+1} = \{c + \pi_{k+1}(q-1) : 1 \le q \le p_{k+2}, \text{ and } c \in W_k\}.$$

If $a \in U_{k+1}$, then there exist $c \in W_k$ and q, $1 \le q \le p_{k+2}$, such that $a = c + \pi_{k+1}(q-1)$. Notice that $c \in W_k = C_{k+1}\{\pi_{k+1}\}$ implies $c \le \pi_{k+1}$, which implies $a \le \pi_{k+1} + \pi_{k+1}(q-1) = q\pi_{k+1} \le \pi_{k+2}$. Moreover, $(c, \pi_{k+1}) = 1$ implies $(a, \pi_{k+1}) = 1$, hence $a \in C_{k+1}\{\pi_{k+2}\}$. That means

$$U_{k+1} \subseteq C_{k+1}\{\pi_{k+2}\}.$$

On the other hand, from the construction of U_{k+1} and the inductive hypothesis we know that

$$|U_{k+1}| = p_{k+2}|W_k| = p_{k+2}\prod_{i=1}^{k+1}(p_i - 1).$$

By Theorem 11,

$$C_{k+1}(\pi_{k+2}) = p_{k+2}\prod_{i=1}^{k+1}(p_i - 1).$$

Hence $U_{k+1} = C_{k+1}\{\pi_{k+2}\}$.

(2) From the definition of $V_{k+1} = p_{k+2}W_k$, if $b \in V_{k+1}$, there exists $c \in W_k$, such that $b = p_{k+2}c$. That $c \in W_k = C_{k+1}\{\pi_{k+1}\}$ implies $(c, \pi_{k+1}) = 1$ and $c \le \pi_{k+1}$, hence $b \le p_{k+2}\pi_{k+1} = \pi_{k+2}$ and $f(b) = p_{k+2}$. That means $b \in S_{k+2}\{\pi_{k+2}\}$. Hence

$$V_{k+1} \subseteq S_{k+2}\{\pi_{k+2}\}.$$

On the other hand, from the construction of $V_{k+1} = p_{k+2}W_k$, we have

$$|V_{k+1}| = |W_k| = \prod_{i=1}^{k+1}(p_i - 1).$$

By Theorem 11,

$$S_{k+2}(\pi_{k+2}) = \prod_{i=1}^{k+1}(p_i - 1).$$

Hence $V_{k+1} = S_{k+2}\{\pi_{k+2}\}$.

(3) From Theorem 2 and the hypothesis of the induction we have $S_{k+2}\{\pi_{k+2}\} \subseteq C_{k+1}\{\pi_{k+2}\} = U_{k+1}$, hence $V_{k+1} \subseteq U_{k+1}$. Thus,

$$\begin{aligned} W_{k+1} &= U_{k+1} - V_{k+1} = C_{k+1}\{\pi_{k+2}\} - S_{k+2}\{\pi_{k+2}\} \\ &= (C_{k+1} - S_{k+2})\{\pi_{k+2}\} = C_{k+2}\{\pi_{k+2}\}. \end{aligned}$$

(4) In the proof of (2) and (3), we proved already that

$$|U_{k+1}| = p_{k+2}\prod_{i=1}^{k+1}(p_i - 1) \text{ and } |V_{k+1}| = \prod_{i=1}^{k+1}(p_i - 1).$$

For the last one, Theorem 11 implies

$$|W_{k+1}| = C_{k+2}(\pi_{k+2}) = \prod_{i=1}^{k+2}(p_i - 1).$$

By the induction, $(1) - (4)$ hold for all $k \geq 1$.

(5) From (4) we have $|W_k| = \prod_{i=1}^{k+1}(p_i - 1) \geq 2 \;\; \Rightarrow \;\; W_k - \{1\} \neq \phi$, so by The Least Integer Principle $p_{k+2} = \min W_k - \{1\}$ exists, and hence by Theorem 1, for all $k \geq 2$,

$$p_{k+2} = \min(W_k - \{1\}) = \min(C_{k+1} - \{1\}) > \min(C_k - \{1\}) = \min(W_{k-1} - \{1\}) = p_{k+1}.$$

□

Theorem 12 shown an important fact: For any $k \in N$, W_k covers all numbers besides the multiples of $p_1, p_2, \cdots, p_{k+1}$ in the set $\{1, 2, \cdots, \pi_{k+1}\}$. It means that we do not miss any prime number when we get the prime numbers from finding the least element of $(W_k - \{1\})$ for each positive integers $k \geq 3$.

From theorem 12 we have the algorithm of Pritchard for finding $P\{n\}$.

Algorithm (Pritchard) Let $n \geq 6$, and let $W_0 = \{1\}$, $p_1 = 2$, $p_2 = 3$, and $\pi_1 = p_1$. Define

$$U_1 = \{c + \pi_1(q-1) : q = 1, 2, p_2, \text{ and } c \in W_0\}, \;\; V_1 = p_2 W_0 \;\text{ and }\; W_1 = U_1 - V_1.$$

Let $\pi_2 = p_1 p_2$ and $p_3 = \min(W_1 - \{1\})$. Define

$$U_2 = \{c + \pi_2(q-1) : 1 \leq q \leq p_3, \text{ and } c \in W_1\},$$

$$V_2 = p_3 W_1, \quad W_2 = U_2 - V_2 \;\; and \;\; p_4 = \min(W_2 - \{1\}.$$

In general, for $k \geq 2$, let $\pi_k = \prod_{i=1}^{k} p_i$ and $p_{k+1} = \min(W_{k-1} - \{1\})$. Define

$$U_k = \{c + \pi_k(q-1) : 1 \leq q \leq p_{k+1}, \text{ and } c \in W_{k-1}\},$$

$$V_k = p_{k+1} W_{k-1}, \quad W_k = U_k - V_k \;\text{ and }\; p_{k+2} = \min(E_k - \{1\}).$$

If $\pi_t \leq n < \pi_{t+1}$ for some t in N, let $E_t = W_t\{n\}$. Define

$$E_{k+1} = E_k - p_{k+2} E_k\{n\}, \;\; if \quad k \geq t,$$

and

$$p_{k+3} = \min(E_{k+1} - \{1\}), \quad if \;\; k \geq t,$$

If $p_s^2 \leq n < p_{s+1}^2$ for some $s \in N$, stop the process and let

$$P\{n\} = \{p_1, p_2, \cdots, p_s\} \cup (E_{s-1} - \{1\}).$$

Then $P\{n\}$ is the set of all primes numbers in $N\{n\}$.

Example Find all prime numbers between 1 and 200.

First of all we have $W_0 = \{1\}$, $p_1 = 2$, $p_2 = 3$, and $\pi_1 = 2$, then by the definitions we have

$$U_1 = \{c + \pi_1(q-1) : q = 1, 2, p_2, \text{ and } c \in W_0\} = \{1, 3, 5\}$$

and

$$V_1 = p_2 W_0 = \{3\} \text{ and } W_1 = U_1 - V_1 = \{1, 5\}.$$

Moreover, $p_3 = \min(W_1 - \{1\}) = 5$ and $\pi_2 = p_1 p_2 = 6$. Next we have

$$U_2 = \{c + \pi_2(q-1) : 1 \le q \le p_3, \text{ and } c \in W_1\} = \{1, 7, 13, 19, 25, 5, 11, 17, 23, 29\},$$

and

$$V_2 = p_3 W_1 = \{5, 25\} \text{ and } W_2 = U_2 - V_2 = \{1, 7, 13, 19, 11, 17, 23, 29\}.$$

Thus $p_4 = \min(W_2 - \{1\}) = 7$ and $\pi_3 = p_1 p_2 p_3 = 30$, and

$$U_3 = \{c + \pi_3(q-1) : 1 \le q \le p_4, \text{ and } c \in W_2\}.$$

Precisely,

$$U_3 = \left\{ \begin{array}{rrrrrrr} 1, & 31, & 61, & 91, & 121, & 151, & 181, \\ 7, & 37, & 67, & 97, & 127, & 157, & 187, \\ 11, & 41, & 71, & 101, & 131, & 161, & 191, \\ 13, & 43, & 73, & 103, & 133, & 163, & 193, \\ 17, & 47, & 77, & 107, & 137, & 167, & 197, \\ 19, & 49, & 79, & 109, & 139, & 169, & 199, \\ 23, & 53, & 83, & 113, & 143, & 173, & 203, \\ 29, & 59, & 89, & 119, & 149, & 179, & 209 \end{array} \right\}$$

and

$$V_3 = p_4 W_2 = \{7, 49, 91, 133, 77, 119, 161, 203\},$$

$$W_3 = U_3 - V_3 = \left\{ \begin{array}{rrrrrr} 1, & 31, & 61, & 121, & 151, & 181, \\ 37, & 67, & 97, & 127, & 157, & 187, \\ 11, & 41, & 71, & 101, & 131, & 191, \\ 13, & 43, & 73, & 103, & 163, & 193, \\ 17, & 47, & 107, & 137, & 167, & 197, \\ 19, & 79, & 109, & 139, & 169, & 199, \\ 23, & 53, & 83, & 113, & 143, & 173, \\ 29, & 59, & 89, & 149, & 179, & 209 \end{array} \right\}.$$

Notice $\pi_3 = 30 < 200 < \pi_4 = 210$ we know from Theorem 5(1) that $\{2, 3, 5, 7\} \cup W_3$ covers all prime numbers between 1 and $\pi_4 = 210$. The problem just asks to find all prime

numbers between 1 and 200, so W_3 is big enough for solving the problem. Sifting out all numbers bigger than 200 from W_3, we have

$$E_3 = W_3\{200\} = \left\{ \begin{array}{llllll} 1, & 31, & 61, & 121, & 151, & 181, \\ 37, & 67, & 97, & 127, & 157, & 187, \\ 11, & 41, & 71, & 101, & 131, & 191, \\ 13, & 43, & 73, & 103, & 163, & 193, \\ 17, & 47, & 107, & 137, & 167, & 197, \\ 19, & 79, & 109, & 139, & 169, & 199, \\ 23, & 53, & 83, & 113, & 143, & 173, \\ 29, & 59, & 89, & 149, & 179, & \end{array} \right\}.$$

Let $p_5 = \min(E_3 - \{1\}) = 11$, then

$$p_5 E_3\{200\} = \{11, 121, 143, 187\}.$$

Sifting out the multiples of 11 from E_3, we have

$$E_4 = E_3 - p_5 E_3\{200\} = \left\{ \begin{array}{llllll} 1, & 31, & 61, & 151, & 181, & \\ 37, & 67, & 97, & 127, & 157, & \\ 41, & 71, & 101, & 131, & 191, & \\ 13, & 43, & 73, & 103, & 163, & 193, \\ 17, & 47, & 107, & 137, & 167, & 197, \\ 19, & 79, & 109, & 139, & 169, & 199, \\ 23, & 53, & 83, & 113, & 173, & \\ 29, & 59, & 89, & 149, & 179, & \end{array} \right\}.$$

Let $p_6 = \min(E_4 - \{1\}) = 13$, then

$$p_6 E_4\{200\} = \{13, 169\}.$$

Sifting out the multiples of 13 from E_4, we have

$$E_5 = E_4 - p_6 E_4\{200\} = \left\{ \begin{array}{llllll} 1, & 31, & 61, & 151, & 181, & \\ 37, & 67, & 97, & 127, & 157, & \\ 41, & 71, & 101, & 131, & 191, & \\ 43, & 73, & 103, & 163, & 193, & \\ 17, & 47, & 107, & 137, & 167, & 197, \\ 19, & 79, & 109, & 139, & 199, & \\ 23, & 53, & 83, & 113, & 173, & \\ 29, & 59, & 89, & 149, & 179, & \end{array} \right\}.$$

Let $p_7 = \min(E_5 - \{1\}) = 17$. Since $p_6^2 = 169 < 200 < p_7^2 = 289$, stop the process and we have

$$P\{200\} = \{2, 3, 5, 7, 11, 13\} \cup (E_5 - \{1\}).$$

6. Applications

A new proof of the infinitude of the prime number set P follows Theorem 12 immediately.

Theorem 13 *There are infinitely many prime numbers.*

Notice Before proving this theorem we like to point out that we never use the infinitude of the prime number set P until now in this article. This will not cause ambiguous for readers. In particular, at the beginning of Theorem 12 or the Pritchard algorithm, we just assume the numbers of 2, and 3 are primes; and the rest, we were using the induction to construct the numbers, which are defined by $p_{k+1} = \min(W_{k-1} - \{1\})$, $k \geq 2$, and proved they are primes with all properties we shown in sections 2 and 3. The key for proving the infinitude of the prime number set P is that the procedure of constructing the set sequences of U_k, V_k, and W_k can be proceeded infinitely. The kernel is $W_k - \{1\} \neq \phi$, for all $k \in N$.

Proof. From Theorem 12 we know that $|W_k - \{1\}| = \prod_{i=1}^{k+1}(p_i - 1) - 1 \geq 1$, hence $W_k - \{1\} \neq \phi$ and $\min(W_k - \{1\})$ exists, it is prime p_{k+2} by Theorem 4(2):

$$\min(W_k - \{1\}) = \min(C_{k+1}\{\pi_{k+1}\} - \{1\}) = p_{k+2}.$$

and $p_{k+1} > p_k$ for any $k \geq 1$ by Theorem 12 (5). The procedure of constructing the sequences of sets U_k, V_k, and W_k in Theorem 12 can be proceeded infinitely because of $|W_k| = \prod_{i=1}^{k+1}(p_i - 1) \geq 2$, for all $k \geq 1$. Thus, we have a strictly increasing infinite sequence of prime numbers $\{p_k\}$. Hence there are infinite many prime numbers. □

We give a new proof of the asymptotic density formula of the set P in N.

Theorem 14 *Define* $\pi(n) = P(n)$. *Then*

(1) $\pi(n) \leq C_k(n) + k$ *for any* $k \in N$;
(2) $\pi(n) = C_s(n) + s - 1$, *if* $p_s^2 \leq n < p_{s+1}^2$ *for some* $s \in N$;
(3) $d(P) = 0$.

Proof. (1) is clear from Theorem 5 (1); and (2) follows Theorem 5 (2). For (3), from (1) we have

$$\frac{\pi(n)}{n} \leq \frac{1}{n}C_k(n) + \frac{k}{n},$$

Taking the limit as $n \to \infty$, and with the help of Theorem 8,

$$d(P) \leq d(C_k) = \prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right) \quad for\ all\ k \in N.$$

Let $k \to \infty$, we have

$$0 \leq d(P) \leq \prod_{i=1}^{\infty}\left(1 - \frac{1}{p_i}\right) = 0;$$

that is $d(P) = 0$. □

References

[1] P. Pritchard, A sublinear additive sieve for finding prime numbers. Communications of the ACM **24**(1)(1981) 18-23.

[2] P. Pritchard, Explaining the wheel sieve, Acta Informat. **17** (1982) 477-485.