Bull. Korean Math. Soc. **58** (2021), No. 6, pp. 1377–1385
https://doi.org/10.4134/BKMS.b200798
pISSN: 1015-8634 / eISSN: 2234-3016

# PRIMALITY BETWEEN CONSECUTIVE PRIMORIALS

Kiyuob Jung and Eunkyung Ko

Abstract. In this paper, we consider a general number system with a base $m$ in order to determine if a positive integer $x$ is prime. We show that the base $m$ providing the most efficient test is the primorial $p_n\sharp$ when $p_n\sharp < x < p_{n+1}\sharp$ and establish a necessary and sufficient condition for $x$ in between consecutive primorials to be determined as a prime number.

## 1. Introduction

Investigation of prime numbers has been a fundamental research field in mathematics in general, and cryptography especially. It has been studied how to determine if a number is prime for a long time and improved efficient calculation algorithm in practice. In the field of determination of prime numbers, the well known test, the *sieve of Eratosthenes*, is the method dividing $n$ by every number $m \le \sqrt{n}$. If any $m$ divides $n$, then $n$ is composite. However, this test is inefficient since it needs huge steps to determine if $n$ is prime. Since then, many results have been established to improve efficiency; Fermat's Little Theorem, Pocklington theorem in [3], AKS primality test in [1] and Elliptic Curve Primality Proving (ECPP) in [2].

In this paper, we suggest a primality test for general purpose, which means that our test does not depend on special numbers such as Fermat numbers and Mersenne numbers. In particular, we prove a necessary and sufficient condition for $x$ living in consecutive primorials to be determined as a prime number.

Let $x$ be a natural number. If the units digit of $x$ is one of 0, 2, 4, 5, 6, or 8, then $x$ is composite since 2 or 5 divides $x$. For this reason, when we determine whether $x$ is prime from only the units digit of $x$, it is enough to deal with $x$ whose the units digit is one of 1, 3, 7 and 9. In other words, we do not have to consider 60% of numbers in the decimal system determining if $x$ is prime. Furthermore, if we take the number system with a general base, we can consider less numbers when finding prime numbers in a way to remove

Received September 18, 2020; Accepted September 2, 2021.
2010 *Mathematics Subject Classification.* 11A41, 11A51, 11A63.
*Key words and phrases.* Prime number, primorial, primality.
E. Ko was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea Government (NRF-2020R1F1A1A01065912).

composite numbers. Suppose that we try to find prime numbers by checking only the units digit of given numbers. For example, we take the number system with base 36. The probability of composite numbers in this number system is about 66.67% (details in Theorem 2.1), which is higher than the probability of composite numbers 60% in the decimal system. Hence, choosing the optimal base which has higher probability of becoming a composite number is important to find prime numbers in the sense of efficiency. Thus, we focus on finding the optimal base and establish a sufficient and necessary condition determining whether an arbitrary number is a prime number by using the optimal base.

Let $n$ be a positive integer. Denote the $n$-th prime number as $p_n$. The primorial of $p_n$, denoted by $p_n\sharp$, is defined as the product of the first $n$ primes:

$$p_n\sharp = \prod_{k=1}^{n} p_k.$$

Here we state our main results:

**Theorem 1.1.** *There exists at least one prime $p$ such that $p_n\sharp < p < p_{n+1}\sharp$ for each $n \in \mathbb{N}$.*

**Theorem 1.2.** *Let $x$ be a positive integer, where $p_n\sharp < x < p_{n+1}\sharp$ with a fixed positive integer $n > 1$. Then $x$ is a prime number if and only if the following conditions hold*:

(i) *$p_n\sharp$ and $r$ are relatively prime, where $r$ is the remainder when $x$ is divided by $p_n\sharp$.*
(ii) *$p \nmid x$ for all prime $p$, where $p_{n+1} \le p < \sqrt{p_{n+1}\sharp}$.*

**Example 1.3.** We determine whether 74173 and 77291 are prime numbers or not. Note that both are in between $p_6\sharp$ and $p_7\sharp$. The remainder when $p_6\sharp = 30030$ divides 74173 and 77291 are 14113 and 17231, respectively. As $\gcd(30030, 14113) \neq 1$, we can see 74173 is composite. However, since 30030 and 17231 are relatively prime, we cannot determine whether 77291 is a prime number from Theorem 1.2(i) only. This case can be handled by Theorem 1.2 (ii). Observe that $p_7 = 17 \le p_7,\ p_8, \ldots,\ p_{127} < \sqrt{p_7\sharp} = 714.49\ldots$. Since 77291 is not divided by $p_7 = 17,\ 19, \ldots,$ and $p_{127} = 709$, we conclude that 77291 is a prime number from Theorem 1.2(ii).

*Remark* 1.4. The existence of a prime number in between $p_n\sharp$ and $p_{n+1}\sharp$ is established in Theorem 1.1, and we can find all prime numbers in between $p_n\sharp$ and $p_{n+1}\sharp$ from Theorem 1.2. Hence, if the largest prime number ($:= p_{last}$) found up to now is $p_{n+1}$, we can guarantee the existence of the prime number ($= p_{last+1}$), which is larger than $p_{last}$, in between $p_{last}$ and $p_{n+1}\sharp$.

Our work is organized as follows: In Section 2, we show that composite numbers can be removed by checking only the units digit in a general number system. We also explain why $p_n\sharp$ is the optimal base. In Section 3, we present the proof of Theorem 1.1 and Theorem 1.2 and suggest an alternative method of Theorem 1.2 in the calculation view point.

## 2. Preliminaries

### 2.1. Units digits and composite numbers

A natural number $x$ can be expressed uniquely in the form

$$x = r_n m^n + r_{n-1} m^{n-1} + \cdots + r_1 m + r_0, \tag{1}$$

where $m, n \in \mathbb{N}$, $m > 1$, $r_i \in \mathbb{Z}_m, 0 \leq i \leq n$ and $r_n \neq 0$. Conventionally, we denote

$$x = r_n r_{n-1} \cdots r_1 r_{0(m)}. \tag{2}$$

In the case when $m=10$, we omit 10 and write the number as $x=r_n r_{n-1} \cdots r_1 r_0$, which is the usual expression in the decimal system. Here, we use a notation $x_{(m,0)}$ for the units digit of $x$ in the number system with a base $m$, which means that $x_{(m,0)} := r_0$ in (2). Now it is easy to see that for all $x, m \in \mathbb{N}$ with $m > 1$, the remainder when $x$ is divided by $m$ is equal to $x_{(m,0)}$.

In the following theorem we discuss the relation between a composite number and the units digit in the number system with a base $m$.

**Theorem 2.1.** *Let $x$ and $m$ be positive integers such that $x > m > 1$. If $x_{(m,0)}$ and $m$ are not relatively prime, then $x$ is composite.*

*Proof.* Let $x$ and $m$ be positive integers with $\gcd(x, m) \neq 1$. Note that $0 \leq x_{(m,0)} < m$. Then there exists a positive integer $g > 1$ such that $x_{(m,0)} = ag$ and $m = bg$ for some $a$, $b \in \mathbb{N}$. From (1), we find that there exist $n \in \mathbb{N}, r_i \in \mathbb{Z}_m, 0 \leq i \leq n$ and $r_n \neq 0$ such that

$$\begin{aligned} x &= r_n m^n + r_{n-1} m^{n-1} + \cdots + r_1 m + x_{(m,0)} \\ &= r_n (bg)^n + r_{n-1} (bg)^{n-1} + \cdots + r_1 bg + ag \\ &= (r_n b^n g^{n-1} + r_{n-1} b^{n-1} g^{n-2} + \cdots + r_1 b + a) g, \end{aligned}$$

which implies that $x$ is composite. □

By checking out the units digit of $x$ in the number system with base $m$, we can recognize that $x$ is composite.

**Example 2.2.** Let us determine whether 7481271 is a prime number or not. In the decimal system, there is no way to recognize that 7481271 is composite by only checking the units digit 1. However, if we change the number system from decimal to hexadecimal one, we can see that 7481271 is composite by observing $7481271 = 424203303_{(6)}$ and applying to Theorem 2.1.

### 2.2. The optimal base in number system

In this section, we shall answer what is the optimal base in a number system to guarantee some efficiency we presented in the introduction. To state our results, we first introduce two well-known inequalities concerning primorials in [4] and [5], respectively;

$$p_{n+1} \leq p_n\sharp - 1 \ \forall n \geq 2 \tag{3}$$

and

$$p_{n+1}^2 < p_n\sharp \ \forall n \geq 4, \tag{4}$$

where the latter inequality is called Bonse's inequality. In [4], Bertrand's postulate states that there exists a prime number $p$ such that $n < p \leq 2n$ for each $n \in \mathbb{N}$. We also employ the usual notation for Euler's function $\phi(m)$ and the radical rad(m) for $m \in \mathbb{N}$, defined by

$$\phi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right), \ \ \mathrm{rad(m)} = \prod_{p|m} p,$$

where $p$ is a prime number. From a simple calculation, it is easy to verify that

$$\frac{\phi(m)}{m} = \frac{\phi(\mathrm{rad}(m))}{\mathrm{rad}(m)}. \tag{5}$$

**Definition.** For a positive integer $m > 1$, we define

$$\rho(m) = 1 - \frac{\phi(m)}{m}.$$

*Remark* 2.3. The function $\rho(m)$ represents the probability that an arbitrary natural number $x > m$ can be determined as composite by checking out the units digit $x_{(m,0)}$. For example, when considering the number system with a base 36, we see that $\rho(36) = 0.66\ldots$, which implies the probability that $x_{(36,0)}$ and 36 are not relatively prime. This means that $x$ has the probability $\rho(36) = 0.66\ldots$ to be determined as a composite number by checking the units digit in the number system with base 36. Hence when we try to find prime numbers by removing composite numbers first and then applying to Theorem 1.2, if we take the value $m$ with the higher $\rho(m)$ than $\rho(10)$, we are able to deal with less numbers in order to apply to Theorem 1.2. In this sense, we will say that the value $m$ with the higher $\rho(m)$ has the better efficiency.

In Figure 1 the horizontal red line is the value $\rho(10) = 0.6$ in the decimal system, and it shows that there exists a base $m$ with the better efficiency than $m = 10$ (details in Corollary 2.6).

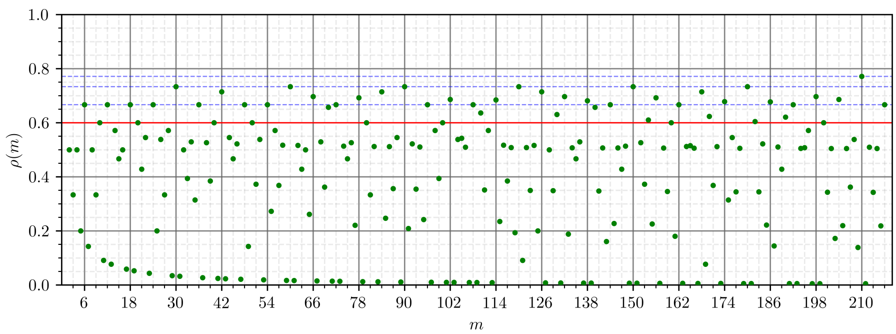


FIGURE 1. $\rho(m)$ from $m = 2$ to $m = 216$

Now, we find the optimal base $m \geq p_2\sharp$ which has the highest $\rho(m)$ when we want to determine whether a positive integer $x > p_2\sharp$ is prime or not. Notice that there exists a positive integer $n > 1$ such that $p_n\sharp < x < p_{n+1}\sharp$. Here we claim that $p_n\sharp$ is the optimal base $m$.

**Proposition 2.4.** *Let $n$ be a positive integer. Then $\rho(m) \leq \rho(p_n\sharp)$, $\forall\ 1 < m < p_{n+1}\sharp$.*

*Proof.* Let the standard decomposition of $m$ be given as

$$m = p_{a_1}^{e_1} p_{a_2}^{e_2} \cdots p_{a_u}^{e_u}, \tag{6}$$

where $p_{a_i} < p_{a_j}$ if $i < j$ and $e_i \in \mathbb{N}$, $\forall 1 \leq i \leq u$. Notice that $u \leq n$ as $1 < m < p_{n+1}\sharp$. We first claim that

$$\prod_{i=1}^{n} \left(1 - \frac{1}{p_i}\right) \leq \prod_{j=1}^{u} \left(1 - \frac{1}{p_{a_j}}\right), \tag{7}$$

where $p_{a_j}, u$ are as in (6). It is clear that (7) holds when $p_1 \leq p_{a_j} \leq p_n$, $\forall 1 \leq j \leq u$. Hence we consider the case when there exists $w \in \mathbb{N}$ such that $p_{a_w} > p_n$, where $1 \leq w \leq u$. Notice that $p_{a_j} > p_n$ for all $w \leq j \leq u$. Let

$$I := \{k \in \mathbb{N} : \forall 1 \leq j \leq w-1,\ p_k \neq p_{a_j} \text{ and } p_k \leq p_n\}$$

and

$$I^c := \{1, 2, \ldots, n\} \setminus I.$$

Note that $|I| = n - w + 1$ and $|I| \geq u - w + 1$ as $u \leq n$. Also, we find that for each $w \leq j \leq u$, $p_{a_j} > p_k$ for all $k \in I$. Thus, it follows that

$$\prod_{k \in I} \left(1 - \frac{1}{p_k}\right) \leq \prod_{j=w}^{u} \left(1 - \frac{1}{p_{a_j}}\right).$$

Therefore, we find that

$$\begin{aligned}
\prod_{j=1}^{u} \left(1 - \frac{1}{p_{a_j}}\right) &= \prod_{h=1}^{w-1} \left(1 - \frac{1}{p_{a_h}}\right) \prod_{j=w}^{u} \left(1 - \frac{1}{p_{a_j}}\right) \\
&\geq \prod_{h=1}^{w-1} \left(1 - \frac{1}{p_{a_h}}\right) \prod_{k \in I} \left(1 - \frac{1}{p_k}\right) \\
&= \prod_{i \in I^c} \left(1 - \frac{1}{p_i}\right) \prod_{k \in I} \left(1 - \frac{1}{p_k}\right) \\
&= \prod_{i=1}^{n} \left(1 - \frac{1}{p_i}\right),
\end{aligned}$$

which implies that (7) holds. Thanks to (5) and (7), we have that

$$\frac{\phi(p_n\sharp)}{p_n\sharp} = \frac{\phi(p_1 p_2 \cdots p_n)}{p_1 p_2 \cdots p_n}$$

$$
\begin{aligned}
&= \prod_{i=1}^{n}\left(1-\frac{1}{p_i}\right)\\
&\le \prod_{j=1}^{u}\left(1-\frac{1}{p_{a_j}}\right)\\
&= \frac{\phi(p_{a_1}p_{a_2}\cdots p_{a_u})}{p_{a_1}p_{a_2}\cdots p_{a_u}}\\
&= \frac{\phi(m)}{m},
\end{aligned}
$$

which concludes that

$$1-\frac{\phi(m)}{m} = \rho(m) \le \rho(p_n\sharp) = 1-\frac{\phi(p_n\sharp)}{p_n\sharp}$$

for all $1 < m < p_{n+1}\sharp$.

$\square$

*Remark* 2.5. As the condition $x > m$ in Theorem 2.1, the optimal base $m$ has to be in between 1 and $p_{n+1}\sharp$.

**Corollary 2.6.** *$\forall n \ge 2$, $\rho(10) < \rho(p_n\sharp)$.*

*Proof.* First, for $n = 2$, one can find that $\rho(10) = 0.6 < 0.66\ldots = \rho(p_2\sharp)$. Second, Proposition 2.4 implies Corollary 2.6 for all $n \ge 3$. Consequently, the proof is complete. $\square$

## 3. Determination of prime numbers

### 3.1. Proofs of the main theorems

*Proof of Theorem 1.1.* Let $n$ be a positive integer. First, for $n = 1$, there exists the prime 3 in between $p_1\sharp$ and $p_2\sharp$. Second, assume $n \ge 2$. Clearly, $2 < p_{n+1}$. By multiplying both sides by $p_n\sharp$, we have $p_n\sharp < \frac{1}{2}p_{n+1}\sharp$. Thanks to Bertrand's postulate, there exists at least one prime $p$ such that $\frac{1}{2}p_{n+1}\sharp < p < p_{n+1}\sharp$. Observing that

$$p_n\sharp \le \frac{1}{2}p_{n+1}\sharp < p < p_{n+1}\sharp,$$

the proof is complete. $\square$

*Proof of Theorem 1.2.* Let $n > 1$ be a positive integer. One can check that Theorem 1.2 holds for $n = 2$ and $n = 3$. Now we prove Theorem 1.2 for $n \ge 4$. Let $x$ be a positive integer with $p_n\sharp < x < p_{n+1}\sharp$. Let $r$ be the remainder when $x$ is divided by $p_n\sharp$. Then $x = q \cdot p_n\sharp + r$ for some $q \in \mathbb{N}$.

First, assume that $x$ is a prime number. To prove (i), suppose to the contrary that $\gcd(p_n\sharp, r) \ne 1$. Then there exists a positive integer $g > 1$ such that $r = ag$ and $p_n\sharp = bg$ for some positive integers $a$, $b$. Since

$$x = q \cdot p_n\sharp + r = qbg + ag = (qb + a)g,$$

$x$ is composite, which is a contradiction to the hypothesis, as required.

Now let $p$ be a prime number, where $p_{n+1} \leq p < \sqrt{p_{n+1}\sharp}$. The inequality $p_{n+1} \leq p_n\sharp - 1$ in (3) yields $p_n\sharp \cdot p_{n+1} < p_n\sharp \cdot p_n\sharp$, so that $\sqrt{p_{n+1}\sharp} < p_n\sharp$ as $p_n\sharp \cdot p_{n+1} = p_{n+1}\sharp$. Also, Bonse's inequality in (4) provides the inequality $p_{n+1} < \sqrt{p_{n+1}\sharp}$. Thus, (ii) is held since $p < x$ implies that $p \nmid x$.

Conversely, assume $\gcd(p_n\sharp, r) = 1$ and $p \nmid x$ for all prime $p$, where $p_{n+1} \leq p < p_n\sharp$. Suppose to the contrary that $x$ is composite. We show that this assumption leads to a contradiction to (ii). Let $x = p_{a_1}^{e_1} p_{a_2}^{e_2} \cdots p_{a_u}^{e_u}$, where $e_i \geq 1$ $\forall 1 \leq i \leq u$ and different prime numbers $p_{a_1}, p_{a_2}, \ldots, p_{a_u}$. Then, $p_{a_i} < \sqrt{p_{n+1}\sharp}$ for all $1 \leq i \leq u$ since the composite number $x$ satisfies that $x < p_{n+1}\sharp$. From (i), observe that

$$\gcd(r, p_n\sharp) = \gcd(x, p_n\sharp) = \gcd\left(p_{a_1}^{e_1} p_{a_2}^{e_2} \cdots p_{a_u}^{e_u}, p_1 p_2 \cdots p_n\right) = 1.$$

Hence, $p_{n+1} \leq p_{a_i}$ for all $1 \leq i \leq u$. Therefore, we obtain that $p_{n+1} \leq p_{a_i} \leq \sqrt{p_{n+1}\sharp}$ $\forall 1 \leq i \leq u$, which contradicts to (ii). Consequently, we conclude that $x$ is prime, as required. $\square$

### 3.2. Determination algorithm; removal of composite numbers

In summary, the determination of prime number is as follows. Let us determine whether $x \in \mathbb{N}$ is a prime number, where $p_n\sharp < x < p_{n+1}\sharp$ for each positive integer $n > 1$.

- (D1) If the units digit of $x$ is one of $0, 2, 4, 5, 6, 8$, then $x$ is composite. Otherwise go to (D2).
- (D2) Calculate the remainder $r$ when $x$ is divided by $p_n\sharp$.
- (D3) If there exists a prime $p_i$ such that $2 \leq i \leq n$ and $p_i \mid r$, then $x$ is composite. Otherwise go to (D4).
- (D4) If there does not exist a prime $p$ which divides $x$, where $p_{n+1} \leq p \leq \sqrt{p_{n+1}\sharp}$, then $x$ is prime. Otherwise $x$ is composite.

In the view of calculation, it is not easy to perform step (D4). Hence we suggest an alternative method, which is that we remove all composite numbers by using the condition $p_{n+1} \leq p \leq \sqrt{p_{n+1}\sharp}$. First, we consider the set of all numbers which is not determined as a composite number after applying to Theorem 1.2 (i). We define

$$\Psi(n) := \left\{x \in \mathbb{N} : p_n\sharp < x < p_{n+1}\sharp \text{ and } \gcd\left(x_{(p_n\sharp, 0)}, p_n\sharp\right) = 1\right\}.$$

Note that elements of $\Psi(n)$ can be either prime numbers or composite numbers.

Now, we investigate the property of the composite numbers in $\Psi(n)$. Let $y$ be a positive integer and its factorization be $p_{a_1}^{e_1} p_{a_2}^{e_2} \cdots p_{a_n}^{e_n}$ with different prime numbers $p_{a_1}, p_{a_2}, \ldots, p_{a_n}$ and positive integer $e_i \geq 1$ $\forall 1 \leq i \leq n$. We define the function $\Omega(y)$ as the number of prime divisors of $y$ counted with multiplicity:

$$\Omega(y) := \sum_{i=1}^{n} e_i.$$

**Property 3.1.** *Let $x \in \Psi(n)$ be a composite number with a fixed $n \in \mathbb{N}$. Then $2 \le \Omega(x) \le N$, where $N$ is the largest positive integer such that $p_{n+1}^N < p_{n+1}\sharp$.*

*Proof.* Clearly, as $2 \le \Omega(x)$ for all $n \in \mathbb{N}$, it is enough to show $\Omega(x) \le N$. It is obvious that there exists the largest $N \in \mathbb{N}$ such that $p_{n+1}^N < p_{n+1}\sharp$ for each $n \in \mathbb{N}$. Let $p_{n+\alpha}$ be the largest prime number such that $p_{n+\alpha} < \sqrt{p_{n+1}\sharp}$. Since $x$ is composite in $\Psi(n)$, $x$ can be written by

$$x = p_{n+1}^{e_1} p_{n+2}^{e_2} \cdots p_{n+\alpha}^{e_\alpha},$$

where $e_i \ge 0$ for all $1 \le i \le \alpha$. Note that $\Omega(x) = e_1 + e_2 + \cdots + e_\alpha$. Suppose to the contrary that $\Omega(x) > N$. Then, we see that

$$p_{n+1}^N < p_{n+1}^{\Omega(x)} = p_{n+1}^{e_1} p_{n+1}^{e_2} \cdots p_{n+1}^{e_\alpha} < p_{n+1}^{e_1} p_{n+2}^{e_2} \cdots p_{n+\alpha}^{e_\alpha} = x < p_{n+1}\sharp,$$

which contradicts to that $N$ is the largest positive integer such that $p_{n+1}^N < p_{n+1}\sharp$. Therefore, the composite number $x \in \Psi(n)$ implies $\Omega(x) \le N$. $\square$

**Example 3.2.** Here are all the elements of $\Psi(3)$ and its factorization in the following table:

TABLE 1. The elements of $\Psi(3)$ and its standard decomposition

| Prime numbers | Composite numbers |
|---|---|
| 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199 | $49 = 7 \cdot 7$, $77 = 7 \cdot 11$, $91 = 7 \cdot 13$, $119 = 7 \cdot 17$, $121 = 11 \cdot 11$, $133 = 7 \cdot 19$, $143 = 11 \cdot 13$, $161 = 7 \cdot 23$, $169 = 13 \cdot 13$, $187 = 11 \cdot 17$, $203 = 7 \cdot 29$, $209 = 11 \cdot 19$ |

Notice that the prime numbers 7, 11, 13, 17, 19, 23, and 29 are the factors of the composite numbers in Table 1. In particular, one can find that $p_4 \le 7,\ 11,\ 13 < \sqrt{p_4\sharp} = 14.49\ldots$. Theorem 1.2(ii) shows that all composite numbers in $\Psi(3)$ is divided by at least one of 7, 11, and 13.

Finally, we introduce the alternative for (D4) aforementioned. In order to obtain all prime numbers in $\Psi(n)$, we proceed the following steps.

(D'4) Calculate the largest positive integer $N$ such that $p_{n+1}^N < p_{n+1}\sharp$.
(D'5) For each $2 \le \omega \le N$, construct $\Psi(n,\omega) := \{x \in \Psi(n) : \Omega(x) = \omega\}$.
(D'6) Calculate that $\Psi(n) \setminus \{\Psi(n,2) \cup \Psi(n,3) \cup \cdots \cup \Psi(n,N)\}$.

Consequently, we consist of only prime numbers in between $p_n\sharp$ and $p_{n+1}\sharp$. Notice that elements of $\Psi(n,\omega)$ are composite possessing $w$ prime factors.

**Example 3.3.** Consider all elements of $\Psi(3)$ at Table 1. The largest positive integer $N$ satisfying $7^N < 210$ is 2. Observing that

$$\Psi(3,2) = \{49, 77, 91, 119, 121, 133, 143, 161, 169, 187, 203, 209\},$$

we obtain all prime numbers in between 30 and 210 by excluding all elements of $\Psi(3,2)$ from $\Psi(3)$.

## References

[1] M. Agrawal, N. Kayal, and N. Saxena, *PRIMES is in P*, Ann. of Math. (2) **160** (2004), no. 2, 781–793. https://doi.org/10.4007/annals.2004.160.781

[2] A. O. L. Atkin and F. Morain, *Elliptic curves and primality proving*, Math. Comp. **61** (1993), no. 203, 29–68. https://doi.org/10.2307/2152935

[3] R. Crandall and C. Pomerance, *Prime Numbers*, second edition, Springer, New York, 2005.

[4] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, sixth edition, Oxford University Press, Oxford, 2008.

[5] J. V. Uspensky and M. A. Heaslet, *Elementary Number Theory*, McGraw-Hill Book Company, Inc., New York, 1939.

Kiyuob Jung
Department of Mathematics
Kyungpook National University
Daegu 41566, Korea
*Email address*: kyjung2357@gmail.com

Eunkyung Ko
Major in Mathematics
College of Natural Sciences
Keimyung University
Daegu 42601, Korea
*Email address*: ekko@kmu.ac.kr