A CHARACTERIZATION OF PRIMES BASED ON EULERIAN NUMBERS

Takashi Agoh
Department of Mathematics, Tokyo University of Science, Noda, Chiba, Japan
agoh_takashi@ma.noda.tus.ac.jp

Received: 6/13/22, Revised: 1/21/23, Accepted: 3/24/23, Published: 4/24/23

Abstract

In this paper, we first establish a new characterization of primes based on Eulerian numbers, which is closely related to the well-known Wilson's theorem. Subsequently, by applying this result, we derive some necessary conditions for twin primes.

1. Introduction

Many kinds of characterizations of primes are known in the literature (see, e.g., [7,10] and the references therein). Among them, the most concise and celebrated one is Wilson's theorem stating that an integer $n \geq 2$ is prime if and only if

$$(n-1)! \equiv -1 \pmod{n}. \tag{1.1}$$

This theorem has been generalized in various directions and applied in many branches of mathematics such as number theory, group theory, combinatorics, etc.

Let $A(n,k)$ be the Eulerian number defined by the number of permutations on the set $\{1,2,\ldots,n\}$ with exactly k ascents. In what follows, we assume that $A(0,0) = 1$, $A(n,0) = 0$ for $n \geq 1$, and $A(n,k) = 0$ if $n < k$ by convention. These numbers appear in the so-called Worpitzky identity (cf., e.g., [5])

$$x^n = \sum_{k=0}^{n} \binom{x+n-k}{n} A(n,k) \quad (n \geq 0), \tag{1.2}$$

and they can be calculated explicitly by the formula

$$A(n,k) = \sum_{i=0}^{k} (-1)^i \binom{n+1}{i} (k-i)^n \quad (0 \leq k \leq n). \tag{1.3}$$

DOI: 10.5281/zenodo.7858993

In addition, it is also commonly known that

$$A(n,k)=\sum_{i=1}^{k}(-1)^{k-i}i!S(n,i)\binom{n-i}{k-i}\quad(1\le k\le n),$$

where $S(n,i)$ is the Stirling number of the second kind. A small table of $A(n,k)$ with $1\le k\le n\le 10$ can be found in the OEIS [8]: A008292. As is well-known, these Eulerian numbers satisfy the symmetric property

$$A(n,k)=A(n,n+1-k) \tag{1.4}$$

and the triangular recurrence relation

$$A(n+1,k)=kA(n,k)+(n+2-k)A(n,k-1), \tag{1.5}$$

which can be proved in various ways, for instance, by induction on n and k, or, by applying (1.2) and its variations (for reference, see, e.g., [3, Chapter 14]).

The sum of $A(n,k)$ for $k=1,2,\ldots,n$ is the total number of permutations of the numbers from 1 to n, i.e., the order of the symmetric group S_n. Thus, one has

$$\sum_{k=1}^{n}A(n,k)=n!\quad(n\ge 1). \tag{1.6}$$

In this paper, we take advantage of the fact that formula (1.6) and Wilson's theorem are inseparable, in order to find a characterization of primes.

In Section 2, as our main result, we establish a new characterization of primes based on Eulerian numbers. In Section 3, by applying this result, we derive a rather simple necessary condition for twin primes. In addition, we discuss some specific conditions for twin primes with the help of formula (1.3), which are suitable for practical use. We conclude this paper by asking certain questions related to special pairs of prime numbers and Carmichael numbers.

We wish to point out beforehand that the methods and techniques we are going to use are extremely elementary, and thereby, there is no prior knowledge required to understand all the contents of this paper.

2. The Main Result

In this section, by connecting formula (1.6) with Wilson's theorem, we will establish a characterization of primes based on Eulerian numbers, as stated below.

Theorem 2.1. *An integer $n\ge 2$ is prime if and only if the congruences*

$$A(n-1,k)\equiv 1\pmod{n}\quad \textit{for}\ \ 1\le k\le\left\lfloor\frac{n}{2}\right\rfloor \tag{2.1}$$

hold.

Before giving a proof, we note that, in view of the symmetric property (1.4), the range of k given in (2.1) can be extended to $1 \le k \le n-1$ if necessary, although there are duplicates in the values of $A(n-1,k)$'s.

Proof. First, we assume that $n = p$ is prime. Then, formula (1.3) provides

$$A(p-1,k) = \sum_{i=0}^{k} (-1)^i \binom{p}{i} (k-i)^{p-1} \quad (0 \le k \le p-1).$$

Since $\binom{p}{i} \equiv 0 \pmod{p}$ unless $i = 0$ or p, we have, by Fermat's little theorem,

$$A(p-1,k) \equiv k^{p-1} \equiv 1 \pmod{p},$$

which verifies that (2.1) holds true for $n = p$. Conversely, assuming that (2.1) holds for any fixed $n \ge 2$, we shall prove that n is prime. Summing up $A(n-1,k)$ over $k = 1, 2, \ldots, n-1$, we get

$$\sum_{k=1}^{n-1} A(n-1,k) \equiv n-1 \equiv -1 \pmod{n},$$

which implies that $(n-1)! \equiv -1 \pmod{n}$ by using (1.6) replacing n by $n-1$. So that n must be prime by Wilson's theorem, and the proof is complete. □

The above proof is interesting in that two congruences (1.1) and (2.1) cooperate with each other to achieve a common goal. Incidentally, it may be worth stating that $A(p-1,k)$ can be evaluated modulo p^2 using $q_p(a) := (a^{p-1}-1)/p$, the Fermat quotient with base a, $p \nmid a$. Actually, for $1 \le k \le p-1$, it follows that

$$A(p-1,k) \equiv pq_p(k) + 1 + \sum_{i=1}^{k-1} (-1)^i \binom{p}{i} \pmod{p^2} \quad \text{(cf. [1, Section 3])}.$$

It should be also stated that the above characterization of primes relying on (2.1) might not be so practical when n is large, for the reason that it requires a lot of computation to find rapidly growing Eulerian numbers; but even if so, we believe that our characterization of primes is intriguing and meaningful from a theoretical point of view, just like with Wilson's theorem.

We observe below certain systems of congruences, which are very similar to, but slightly different from the system of (2.1).

Proposition 2.2. *For any integer $n \ge 1$, the system of congruences*

$$kA(n-1,k) \equiv k \pmod{n} \quad \textit{for } 1 \le k \le \left\lfloor \frac{n}{2} \right\rfloor \tag{2.2}$$

is equivalent to that of congruences

$$A(n,k) \equiv 1 \pmod{n} \quad \textit{for } 1 \le k \le \left\lfloor \frac{n+1}{2} \right\rfloor. \tag{2.3}$$

Proof. Let us consider (1.5) shifted from n to $n-1$, namely,

$$A(n,k) = kA(n-1,k) + (n+1-k)A(n-1,k-1).$$

This recurrence relation can be written after rearranging the terms as

$$A(n,k) - 1 = k\,(A(n-1,k)-1) + (n+1-k)\,(A(n-1,k-1)-1) + n,$$

which leads to the congruence

$$A(n,k) - 1 \equiv k\,(A(n-1,k)-1) - (k-1)\,(A(n-1,k-1)-1) \pmod{n},$$

and thus, (2.2) implies (2.3). Conversely, assuming that (2.3) holds, we have

$$k\,(A(n-1,k)-1) \equiv (k-1)\,(A(n-1,k-1)-1) \pmod{n}.$$

Take here sequentially $k = 1, 2, 3, \ldots$, and so on up to $\lfloor \frac{n}{2} \rfloor$, to obtain (2.2). □

We note in passing that (2.1) implies (2.2) (and thus, (2.3)), but the reverse implication is not true, for the reason that k is not always relatively prime to n if n is a composite number.

3. Application to Twin Primes

In this section, based on Theorem 2.1, we derive a rather simple necessary condition for twin primes by means of Eulerian numbers. In addition, by using formula (1.3), we discuss some practical conditions for twin primes.

Twin primes have been investigated extensively for a long time from various points of view. It is conjectured that there are infinitely many pairs of twin primes (the so-called *twin prime conjecture*), but it still remains unsettled as one of the great open questions in mathematics. The number of pairs of twin primes below 10^n $(n = 1, 2, 3, \ldots)$ is listed in a table of the OEIS [8]: A007508. Despite the twin prime conjecture there is an outstanding result established by Viggo Brun in 1919, which asserts that the series obtained by adding the reciprocals of the twin primes such that

$$B := \left(\frac{1}{3} + \frac{1}{5}\right) + \left(\frac{1}{5} + \frac{1}{7}\right) + \left(\frac{1}{11} + \frac{1}{13}\right) + \left(\frac{1}{17} + \frac{1}{19}\right) + \cdots$$

converges to a definite number, which is now called *Brun's constant*. Precisely,

$$B \approx 1.90216054.$$

This result means that twin primes become increasingly rare as we examine larger ranges. For more details, see, e.g., the classic books by Rademacher [9, Chapter 15] and Ribenboim [10, Chapter 4, III].

As clearly seen, any pair of twin primes except $(3,5)$ is of the form $(6a-1, 6a+1)$ with some integer $a \geq 1$. It is also known that, for an integer $n > 1$, the pair $(n, n+2)$ consists of twin primes if and only if the following congruence holds:

$$4\,((n-1)!+1) \equiv -n \pmod{n(n+2)},$$

which is a very nice generalization of Wilson's theorem conceived by Clement [4].

Apart from these prominent aspects, Theorem 2.1 allows us to derive a rather simple necessary condition for twin primes by means of Eulerian numbers.

Theorem 3.1. *For an odd integer $n \geq 3$, if a pair $(n, n+2)$ consists of twin primes, then it follows that*

$$A(n+1,k) \equiv \begin{cases} 1 \pmod{n(n+2)} & \text{for } \ k=1; \\ \dfrac{n+4}{2} \pmod{n(n+2)} & \text{for } \ 2 \leq k \leq \dfrac{n+1}{2}. \end{cases} \tag{3.1}$$

Proof. Recalling (1.5), we have the following recurrence relations:

$$\begin{aligned} A(n-1,k) &= kA(n-2,k) + (n-k)A(n-2,k-1); \\ A(n,k) &= kA(n-1,k) + (n+1-k)A(n-1,k-1); \\ A(n+1,k) &= kA(n,k) + (n+2-k)A(n,k-1), \end{aligned}$$

which are valid for all $k \geq 1$. By sequentially substituting the previous formula into the next, we see that $A(n+1,k)$ for $k \geq 1$ can be expressed as follows:

$$\begin{aligned} &\text{(i)} \quad A(n+1,1) = A(n-1,1) = 1; \\ &\text{(ii)} \quad A(n+1,2) = 4A(n-1,2) + (3n-2)A(n-1,1); \\ &\text{(iii)} \quad A(n+1,k) = k^2 A(n-1,k) \\ &\qquad\qquad + (2kn+4k-2k^2-n-2)A(n-1,k-1) \\ &\qquad\qquad + (n+2-k)^2 A(n-1,k-2) \quad \text{for } \ 3 \leq k \leq \frac{n+1}{2}. \end{aligned} \tag{3.2}$$

Now, assume that $(n, n+2)$ is a pair of twin primes. Since n is an odd prime, we have $A(n-1,k) \equiv 1 \pmod{n}$ for $1 \leq k \leq \frac{n-1}{2}$ by Theorem 2.1. Therefore, we obtain from (3.2) that

$$A(n+1,k) \equiv \begin{cases} 1 \pmod{n} & \text{for } \ k=1; \\ 4-2 \equiv 2 \pmod{n} & \text{for } \ k=2; \\ k^2 + (4k-2k^2-2) + (2-k)^2 \equiv 2 \pmod{n} \\ \quad \text{for } \ 3 \leq k \leq \dfrac{n+1}{2}. \end{cases} \tag{3.3}$$

Similarly, since $n+2$ is prime, we get $A(n+1,k) \equiv 1 \pmod{n+2}$ for $1 \leq k \leq \frac{n+1}{2}$ again by Theorem 2.1. Noting that $\gcd(n, n+2) = 1$ and based on the Chinese

remainder theorem, it follows from (3.3) that

$$A(n+1,k) \equiv \begin{cases} 1 \pmod{n(n+2)} & \text{for } k=1; \\ \dfrac{n^2+3n+4}{2} \equiv \dfrac{n+4}{2} \pmod{n(n+2)} & \text{for } 2 \le k \le \dfrac{n+1}{2}. \end{cases}$$

So we are done with (3.1). Note that the case for $k = 1$ can be excluded from (3.1) if one wants, since it unconditionally holds regardless of twin primes. □

Remark 1. From (3.2) (ii) we have $A(n+1,2) \equiv 4A(n-1,2) - 2 \pmod{n}$. So the condition $A(n+1,2) \equiv (n+4)/2 \equiv 2 \pmod{n}$ derived from (3.1) yields

$$2^2 A(n-1,2) \equiv 2^2 \pmod{n}.$$

Next, since $A(n+1,k) \equiv 2 \pmod{n}$ for $k \ge 3$, we get from (3.2) (iii),

$$\begin{aligned} 2 \equiv & k^2 A(n-1,k) - 2(k-1)^2 A(n-1,k-1) \\ & + (k-2)^2 A(n-1,k-2) \pmod{n}. \end{aligned}$$

Take $k = 3$ and use the previous result for $k = 2$ to obtain $3^2 A(n-1,3) \equiv 3^2 \pmod{n}$. Repeating a similar procedure, it can be finally shown that

$$k^2 A(n-1,k) \equiv k^2 \pmod{n} \quad \text{for all } 1 \le k \le \frac{n-1}{2}. \tag{3.4}$$

Considering the case where $\gcd(k,n) \neq 1$, we see that (3.4), which is a consequence of (3.1), does not mean that n is prime. Aside from that, (3.1) implies that $n+2$ is prime. In fact, (3.1) reduces modulo $n+2$ to

$$A(n+1,k) \equiv \frac{n+4}{2} \equiv 1 \pmod{n+2} \quad \text{for all } 1 \le k \le \frac{n+1}{2}.$$

This conclusion implies from Theorem 2.1 that $n+2$ is surely prime.

Using an explicit expression of $A(n,k)$ in (1.3), it is possible to paraphrase some of the congruences in (3.1) into more specific and convincing forms.

Corollary 3.2. *Given an integer $n > 1$, if $(n, n+2)$ is a pair of twin primes, then the following congruences hold:*

$$\begin{aligned} &\text{(a)} \quad 2^{n+1} \equiv \frac{3n}{2} + 4 \pmod{n(n+2)}; \\ &\text{(b)} \quad 3^{n+1} \equiv 4n + 9 \pmod{n(n+2)}; \\ &\text{(c)} \quad 3^{n+2} - 2^{n+4} \equiv -5 \pmod{n(n+2)}. \end{aligned}$$

Proof. By a direct use of formula (1.3) we have

$$\begin{aligned} &\text{(i)} \quad A(n+1,2) = 2^{n+1} - (n+2); \\ &\text{(ii)} \quad A(n+1,3) = 3^{n+1} - (n+2)2^{n+1} + \frac{1}{2}(n+1)(n+2). \end{aligned} \tag{3.5}$$

For congruence (a), we have only to substitute (3.5) (i) into (3.1) with $k = 2$. Congruence (b) can be obtained by substituting (3.5) (ii) into (3.1) with $k = 3$ and then applying (a). To deduce (c), just combine (a) and (b). Of course, if any two of (a), (b), and (c) hold, then so do the rest. □

Remark 2. We proved the above corollary as an easy application of (3.1), but the referee of this paper kindly pointed out that one can deduce a more generalized congruence of (a) and (b) as a direct consequence of Fermat's little theorem. To carry it out, assume that $(n, n+2)$ is a pair of twin primes and a is an integer coprime to $n(n+2)$. Then, Fermat's little theorem provides $a^{n+1} \equiv a^2 \pmod{n}$ and $a^{n+1} \equiv 1 \pmod{n+2}$. So combining these yields

$$a^{n+1} \equiv \frac{a^2-1}{2}n + a^2 \pmod{n(n+2)}. \tag{3.6}$$

Thus, (a) and (b) are just the special cases of (3.6) for $a = 2$ and 3, respectively.

As is generally known, an integer $n \geq 2$ that satisfies *Fermat's congruence*

$$a^{n-1} \equiv 1 \pmod{n}$$

for 'all' integers a with $\gcd(a, n) = 1$ is either a prime number or a Carmichael number. In light of this fact, it is clear that (3.6) always holds if both n and $n+2$ are prime or Carmichael. Note that $\gcd(n, n+2) = 1$ whenever n is odd. The same can be said if one of n and $n+2$ is prime while the other is Carmichael. A list of the first few Carmichael numbers can be found in the OEIS [8]: A002997.

Concerning the above matter, the following questions arise.

Question 1. Is there a case where both n and $n+2$ are Carmichael?

It is not certain, but we presume that probably such a case cannot occur. In addition, it seems that almost nothing is known about the distance between two consecutive Carmichael numbers, to the best of our knowledge.

Question 2. Are there infinitely many pairs $(n, n+2)$ in which one of n and $n+2$ is prime (resp. Carmichael) and the other is Carmichael (resp. prime)?

Here are a few examples of pairs satisfying the conditions in this question:

$$(561, 563),\ (1103, 1105),\ (2465, 3467),\ (2819, 2821),\ (6599, 6601),\ (41039, 41041).$$

We cannot say for sure at this stage, but as n increases, these pairs appear to be very sparsely interspersed. It should be mentioned that, in their celebrated paper [2], Alford, Granville, and Pomerance have proved that there are infinitely many Carmichael numbers. Furthermore, it was verified in Harman's work [6] that, for a sufficiently large x, there are more than $x^{1/3}$ Carmichael numbers up to x.

Taking these results into account, the answer to the latter question can be expected to be affirmative, although it will be not so easy to ascertain the truth.

Acknowledgements. The author would like to thank Andrew Granville for his insightful advice on how to give a concise proof of Theorem 2.1. Furthermore, the author is very grateful to the anonymous referee and the editor for many helpful comments and corrections, which improved the quality of this paper.

References

[1] T. Agoh, A note on the Wilson quotient, *Integers* **22** (2022), #A86.

[2] W. R. Alford, A. Granville, and C. Pomerance, There are infinitely many Carmichael numbers, *Ann. of Math.* (2), **139** (1994), 703–722.

[3] Ch. A. Charalambides, *Enumerative Combinatorics*, Chapman & Hall/CRC, Boca Raton, London, New York, Washington, D.C., 2002.

[4] P. A. Clement, Congruences for sets of primes, *Amer. Math. Monthly* **56** (1949), 23–25.

[5] L. Comtet, *Advanced Combinatorics: The Art of Finite and Infinite Expansions*, rev. enl. ed. Dordrecht, Netherlands: Reidel, 1974.

[6] G. Harman, Watt's mean value theorem and Carmichael numbers, *Int. J. Number Theory* **4** (2008), 241–248.

[7] W. Narkiewicz, *The Development of Prime Number Theory: From Euclid to Hardy and Littlewood*, Springer Monogr. Math., Springer-Verlag, Berlin, 2000.

[8] OEIS Foundation Inc. (2022), The On-Line Encyclopedia of Integer Sequences, available online at http://oeis.org.

[9] H. Rademacher, *Lectures on Elementary Number Theory*, Blaisdell Pub. Co., New York, Toronto, London, 1964.

[10] P. Ribenboim, *The New Book of Prime Number Records*, Springer-Verlag, New York, Berlin, Heidelberg, 3rd. ed. 1996.