On Wilson's Theorem and Polignac Conjecture

by
Cong Lin, Li Zhipeng

ABSTRACT. We introduce Wilson's Theorem and Clement's result and present a necessary and sufficient condition for p and $p+2k$ to be primes where $k \in \mathbb{Z}^{+}$. By using Simionov's Theorem, a generalized form of Wilson's Theorem, we derive improved version of Clement's result and characterization of Polignac twin primes which parallels previous characterizations. A straightforward method for determining the coefficients in the derivation is also discussed.

1. INTRODUCTION

Prime numbers, whole numbers that are not the products of two smaller numbers, are the bases of the arithmetics. In the nineteenth century it was shown that the number of primes less than or equal to n approaches $n/(\log_e n)$ (as n gets very large); so a rough estimate for the nth prime is $n \log_e n$. The Sieve of Eratosthenes is still the most efficient way of finding all very small primes (e.g., those less than 1,000,000). However, most of the largest primes are found using special cases of Lagrange's Theorem from group theory. In 1984 Samuel Yates defined a titanic prime to be any prime with at least 1,000 digits. When he introduced this term there were only 110 such primes known; now there are over 1000 times that many! And as computers and cryptology continually give new emphasis to search forever-larger primes, this number will continue to grow. The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. There are still many open questions relating to prime numbers, among which are the famous Twin Primes Conjecture and Goldbach's Conjecture [1].

In relation to the unsolved conjectures, the properties of prime numbers were studied and several theorems and corollaries developed. In 1849, Alphonse de Polignac (1817-1890) made the general conjecture that for any positive integer k, there are infinitely many pairs of primes differ by $2k$. The case for which $k = 1$ is the twin primes case. Since then, numerous attempts to prove this conjecture had been made. Based on heuristic considerations, a law (the twin prime conjecture) was developed, in 1922, by Godfrey Harold Hardy (1877-1947) and John Edensor Littlewood (1885-1977) to estimate the density of twin primes [2]. Twin prime characterization was discussed later by Clement in 1949 [3]. But an effective approach to the conjecture remains undeveloped. It is thus worthwhile to re-examine the derivation of Clement's result from a more fundamental theorem in number theory, the Wilson's Theorem. By generalizing and improving Wilson's Theorem and Clement's result, a superior approach to Polignac Conjecture can be adapted to obtain useful partial results to the mysterious problems.

2. Wilson's Theorem and Clement's result

Wilson derived his theorem on sufficient and necessary condition for a number p to be prime.

Theorem 1 $(p-1)! \equiv -1 \pmod{p}$ iff p is prime. (1)

In 1949, Clement [3, 6] formulated another theorem based on Wilson's Theorem. The following is our derivation of Clement's result,

Theorem 2 $4[(p-1)!+1] \equiv -p \pmod{p(p+2)}$ iff p, $p+2$ are primes. (2)

Proof. Obviously, $p+2$ is not prime when $p=2$. So we exclude $p=2$ from our discussion, i.e. p and $p+2$ are odd prime numbers. By Wilson's Theorem, when $p \neq 2$,

$$\begin{array}{rrcll} & (p-1)! & \equiv & -1 \pmod{p} & \text{iff } p \text{ is odd prime.} \\ \Rightarrow & (p-1)!+1 & \equiv & 0 \pmod{p} & \text{iff } p \text{ is odd prime.} \\ \Rightarrow & 4[(p-1)!+1] & \equiv & 0 \pmod{p} \text{ and } p \neq 4 & \text{iff } p \text{ is odd prime.} \\ \Rightarrow & 4[(p-1)!+1] & \equiv & -p \pmod{p} \text{ and } p \neq 4 & \text{iff } p \text{ is odd prime.} \end{array} \quad (3)$$

Similarly,

$$\begin{array}{rrcll} & (p+1)!+1 & \equiv & 0 \pmod{p+2} & \text{iff } p+2 \text{ is odd prime.} \\ \Rightarrow & (p^2+p)(p-1)!+1 & \equiv & 0 \pmod{p+2} & \text{iff } p+2 \text{ is odd prime.} \\ \Rightarrow & [(p+2)(p-1)+2](p-1)!+1 & \equiv & 0 \pmod{p+2} & \text{iff } p+2 \text{ is odd prime.} \\ \Rightarrow & 2(p-1)!+1 & \equiv & 0 \pmod{p+2} & \text{iff } p+2 \text{ is odd prime.} \\ \Rightarrow & 2[2(p-1)!+1] & \equiv & 0 \pmod{p+2} & \text{iff } p+2 \text{ is odd prime.} \\ \Rightarrow & 2[2(p-1)!+1]+(p+2) & \equiv & 0 \pmod{p+2} & \text{iff } p+2 \text{ is odd prime.} \\ \Rightarrow & 4[(p-1)!+1]+p & \equiv & 0 \pmod{p+2} & \text{iff } p+2 \text{ is odd prime.} \\ \Rightarrow & 4[(p-1)!+1] & \equiv & -p \pmod{p+2} & \text{iff } p+2 \text{ is odd prime.} \end{array} \quad (4)$$

From (3) and (4), $4[(p-1)!+1] \equiv -p \pmod{p(p+2)}$ iff p and $p+2$ are odd prime numbers. □

3. Derivation from Wilson's Theorem for Polignac Conjecture

In the derivation of Clement's result, a method of determining unknown coefficients has been applied. This method is used to combine two congruence identities into one. Suppose we have

$$f_1(p) + C_1 \equiv 0 \pmod{p} \text{ and } g(\lambda) f_1(p) + C_2 \equiv 0 \pmod{p+\lambda},$$

where $(p, p+\lambda) = 1$ and $(g(\lambda), p(p+\lambda)) = 1$, we establish two congruences:

$$Xg(\lambda)[f_1(p) + C_1] + Yp \equiv 0 \pmod{p}$$

and
$$X[g(\lambda)f_1(p) + C_2] + Y(p+\lambda) \equiv 0 \pmod{p+\lambda}.$$

If we choose X and Y in such a way that $(X, p) = 1$ and $(X, p+\lambda) = 1$, and

$$Xg(\lambda)C_1 = XC_2 + Y\lambda,$$

then (3) and (4) is equivalent to

$$Xg(\lambda)f_1(p) + Yp + XC_2 + Y\lambda \equiv 0 \pmod{p(p+\lambda)}. \quad (5)$$

Specifically, in deriving Clement's result, we used $X = 2$ and $Y = 1$. This method can be employed again in attempting the Polignac Conjecture which states that for every positive number k, there are infinitely many pairs of primes in the form of p and $p + 2k$. We propose a necessary and sufficient condition when p and $p + 2k$ are primes.

Theorem 3 Suppose $p \nmid 2k(2k)!$ and p is odd. Then we have

$$2k(2k)![(p-1)! + 1] \equiv [1 - (2k)!]p \pmod{p(p+2k)}$$

iff p and $p + 2k$ are odd primes.

Proof. From Wilson's theorem, we have

$$(p-1)! + 1 \equiv 0 \pmod{p} \text{ iff } p \text{ is odd prime.}$$

$$(p+2k-1)! + 1 \equiv 0 \pmod{p+2k} \text{ iff } p+2k \text{ is odd prime.}$$

The Left hand side of the second congruence can be rewritten as

$$\begin{aligned}(p+2k-1)(P+2k-2)\cdots p(p-1)! + 1 &\equiv (-1)(-2)\cdots(-2k)(p-1)! + 1 \\ &\equiv (2k)!(p-1)! + 1 \\ &\equiv 0 \pmod{p+2k}.\end{aligned}$$

By setting $\lambda = 2k$, $g(\lambda) = (2k)!$, $f_1(p) = (p-1)!$, $C_1 = C_2 = 1$, $X = 2k$ and $Y = (2k)! - 1$ in (5), we obtain

$$2k(2k)![(p-1)! + 1] \equiv [1 - (2k)!]p \pmod{p(p+2k)}$$

iff p and $p + 2k$ are odd primes, assuming $p \nmid 2k(2k)!$ and p is odd. □

For example, when $k = 2$, we have, $p \nmid 96$, $96[(p-1)!+1] \equiv -23p \pmod{p(p+4)}$ iff p and $p+4$ are odd primes.

4. Simionov's Generalization of Wilson's Theorem

By elementary mathematical manipulations, we can generalize Wilson's Theorem. Simionov had found out the following generalization of Wilson's Theorem [4]

Theorem 4 Let k be a positive integer less than or equal to p. Then

$$(k-1)!(p-k)! \equiv (-1)^k \pmod{p} \text{ iff } p \text{ is a prime.}$$

Proof. By Wilson's Theorem,

$$\begin{aligned}
& (p-1)! \equiv -1 \pmod{p} && \text{iff } p \text{ is prime.}\\
\Leftrightarrow\ & (p-1)(p-2)(p-3)\cdots(p-k+1)(p-k)! \equiv -1 \pmod{p} && \text{iff } p \text{ is prime.}\\
\Leftrightarrow\ & (-1)(-2)(-3)\cdots(-k+1)(p-k)! \equiv -1 \pmod{p} && \text{iff } p \text{ is prime.}\\
\Leftrightarrow\ & (-1)^{k-1}(1)(2)(3)\cdots(k-1)(p-k)! \equiv -1 \pmod{p} && \text{iff } p \text{ is prime.}\\
\Leftrightarrow\ & (-1)^{k-1}(-1)^{k-1}(1)(2)(3)\cdots(k-1)(p-k)! \equiv (-1)^k \pmod{p} && \text{iff } p \text{ is prime.}\\
\Leftrightarrow\ & (-1)^{k-1}(-1)^{k-1}(k-1)!(p-k)! \equiv (-1)^k \pmod{p} && \text{iff } p \text{ is prime.}\\
\Leftrightarrow\ & (k-1)!(p-k)! \equiv (-1)^k \pmod{p} && \text{iff } p \text{ is prime.} \quad \square
\end{aligned}$$

Besides Simionov's result, other generalizations include

Corollary 1 (Partial consequence of Goldbach's Conjecture [5]) For two distinct odd prime numbers, p_1, p_2 and a positive odd integer p such that $p+1 = p_1 + p_2$, we have $(p-p_1)!(p-p_2)! \equiv -1 \pmod{p}$ iff p is prime.

Corollary 2 For integers k_1 and k_2 such that $0 \le k_1 < k_2 < p$ and $k_2 - k_1 \equiv 1 \pmod{2}$, we have $k_1!k_2!(p-k_1-1)!(p-k_2-1)! \equiv -1 \pmod{p}$ if p is prime.

However, these generalizations are less significant compared to Sinionov's Theorem. A direct consequence of Simionov's Theorem can be obtained by substituting $k = \frac{p+1}{2}$ into the equation in Theorem 4.

Theorem 5 $[(\frac{p-1}{2})!]^2 \equiv (-1)^{\frac{p+1}{2}}$ iff p is odd prime.

Proof. This result can also be directly derived from Wilson's Theorem as shown below, for an odd integer p,

$$\begin{aligned}
& (p-1)(p-2)(p-3)\cdots(\tfrac{p+1}{2})(\tfrac{p-1}{2})\cdots 3\cdot 2\cdot 1 \equiv -1 \pmod{p} && \text{iff } p \text{ is odd prime.}\\
\Leftrightarrow\ & [(p-1)\cdot 1][(p-2)\cdot 2][(p-3)\cdot 3]\cdots[(\tfrac{p+1}{2})(\tfrac{p-1}{2})] \equiv -1 \pmod{p} && \text{iff } p \text{ is odd prime.}\\
\Leftrightarrow\ & (-1)(-4)(-9)\cdots(-(\tfrac{p-1}{2})^2) \equiv -1 \pmod{p} && \text{iff } p \text{ is odd prime.}\\
\Leftrightarrow\ & (-1^2)(-2^2)(-3^2)\cdots[-(\tfrac{p-1}{2})^2] \equiv -1 \pmod{p} && \text{iff } p \text{ is odd prime.}\\
\Leftrightarrow\ & (-1)^{\frac{p-1}{2}}[(\tfrac{p-1}{2})!]^2 \equiv -1 \pmod{p} && \text{iff } p \text{ is odd prime.}
\end{aligned}$$

$$\begin{aligned}
\Leftrightarrow \quad & (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}[(\tfrac{p-1}{2})!]^2 \equiv (-1)(-1)^{\frac{p-1}{2}} \pmod p \text{ iff } p \text{ is odd prime.} \\
\Leftrightarrow \quad & [(\tfrac{p-1}{2})!]^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p \text{ iff } p \text{ is odd prime.} \quad \square
\end{aligned}$$

As the calculation for the factorial of a number can be tremendous, this result can reduce the computation for determining the primality of a number, as $[(\frac{p-1}{2})!]^2$ is much smaller than $(p-1)!$, especially for large p. Hence, Simionov's finding can be viewed as an improvement of Wilson's Theorem. We can take this approach when solving Twin Prime Conjecture and Polignac Conjecture.

5. Derivation from Simionov's Theorem for Polignac Conjecture

From Simionov's result, we use the method of the mathematical manipulations mentioned in Section 3 to derive a sufficient and necessary condition for twin prime numbers to exist, i.e. for p and $p+2$ to be primes.

Theorem 6

$$2[(\frac{p-1}{2})!]^2 + (-1)^{\frac{p-1}{2}}(5p+2) \equiv 0 \pmod{p(p+2)}$$

iff p and $p+2$ are odd prime numbers.

Proof. From Theorem 5, for odd integer p, we have

$$\begin{aligned}
& [(\tfrac{p-1}{2})!]^2 + (-1)^{\frac{p-1}{2}} \equiv 0 \pmod p \quad \text{iff } p \text{ is odd prime.} \\
\Rightarrow \quad & 2[(\tfrac{p-1}{2})!]^2 + 2(-1)^{\frac{p-1}{2}} \equiv 0 \pmod p \quad \text{iff } p \text{ is odd prime.} \\
\Rightarrow \quad & 2[(\tfrac{p-1}{2})!]^2 + (-1)^{\frac{p-1}{2}}(2+5p) \equiv 0 \pmod p \quad \text{iff } p \text{ is odd prime.}
\end{aligned}$$

Similarly for $p+2$, we have

$$\begin{aligned}
& [(\tfrac{p+1}{2})!]^2 + (-1)^{\frac{p+1}{2}} \equiv 0 \pmod{p+2} \quad \text{iff } p+2 \text{ is odd prime.} \\
\Rightarrow \quad & 8[(\tfrac{p+1}{2})!]^2 + 8(-1)^{\frac{p+1}{2}} \equiv 0 \pmod{p+2} \quad \text{iff } p+2 \text{ is odd prime.} \\
\Rightarrow \quad & 8(\tfrac{p+1}{2})^2[(\tfrac{p-1}{2})!]^2 + (-8)(-1)^{\frac{p-1}{2}} \equiv 0 \pmod{p+2} \quad \text{iff } p+2 \text{ is odd prime.} \\
\Rightarrow \quad & 2(p^2+2p+1)[(\tfrac{p-1}{2})!]^2 + [5(p+2)-8]^{\frac{p-1}{2}} \equiv 0 \pmod{p+2} \quad \text{iff } p+2 \text{ is odd prime.} \\
\Rightarrow \quad & 2[(\tfrac{p-1}{2})!]^2 + (5p+2)(-1)^{\frac{p-1}{2}} \equiv 0 \pmod{p+2} \quad \text{iff } p+2 \text{ is odd prime.}
\end{aligned}$$

Consequently, $2[(\frac{p-1}{2})!]^2 + (5p+2)(-1)^{\frac{p-1}{2}} \equiv 0 \pmod{p(p+2)}$ iff p and $p+2$ are odd primes. $\square$

If we use the same method again on the pair of congruences:

$$[(\frac{p-1}{2})!]^2 + (-1)^{\frac{p-1}{2}} \equiv 0 \pmod p \text{ iff } p \text{ is odd prime,}$$

$$[(\frac{p+2k-1}{2})!]^2 + (-1)^{\frac{p+2k-1}{2}} \equiv 0 \pmod{p+2k} \text{ iff } p+2k \text{ is odd prime}$$

and setting $X = 4^k(2k)$ and $Y = (2k-1)!!^2(-1)^{\frac{p-1}{2}} - 4^k(-1)^{\frac{p+2k-1}{2}}$ in (5) where $(2n-1)!!$ denotes $\prod_{i=1}^{n}(2i-1)$, the following result can be easily obtained.

Theorem 7 Suppose $p \nmid (2k-1)!!^2$ and p is odd. Then

$$2k(2k-1)!!^2[(\frac{p-1}{2})!]^2+(-1)^{\frac{p-1}{2}}[(2k-1)!!^2(p+2k)+4^k(-1)^{k+1}p] \equiv 0 \pmod{p(p+2k)}$$

iff p and $p+2k$ are primes.

This is a necessary and sufficient condition for p and $p+2k$ to be primes assuming $p \nmid (2k-1)!!^2$ and p is odd. For example, when $k=2$, we have, supposing $p \nmid 9$ and p is odd, $36[(\frac{p-1}{2})!]^2+(-1)^{\frac{p-1}{2}}[36-7p] \equiv 0 \pmod{p(p+4)}$ iff p and $p+4$ are primes.

6. Conclusion

In this paper, we have proposed necessary and sufficient conditions for p and $p+2k$ to be primes where $k \in \mathbb{Z}^+$(Theorem 3 and Theorem 7). Unfortunately, because of the tedious calculation of the factorial of a large number, these theorems may not be very effective in searching for large twin primes. Though Theorem 7 reduces significantly the number of computational steps of Theorem 3, it is still a daunting task to calculate $(\frac{p-1}{2})!$ when p becomes very large. Moreover, as we cannot prove that there are infinitely many numbers satisfying the condition yet, we cannot solve the Polignac Conjecture. Thus, we need to further improve these theorems or look for other alternative routes in attempting the Twin Prime Conjecture and the Polignac Conjecture.

7. Acknowledgement

We would like to express our gratitude to Assoc Prof Choi Kwok Pui of National University of Singapore in guiding us in the project on Benford's Law which led us to examine the goodness-of-fit for prime number distribution to the Benford's distribution. While tackling this intriguing problem, we extended our knowledge of primes and obtained the results stated in this paper along the way.

References

[1] Chen J.R., Shao P. C., *Goldbach hypothesis*, Shenyang: Liaoning Education Press, (1987).

[2] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, Oxford Science Publications, (1979).

[3] P.A. Clement, *Congruences for sets of primes*, American Mathematical Monthly, vol. 56, p.23-25, (1949).

[4] W.J. Le Veque, *Fundamentals of Numbers Theory*, New York, Dover, (1996)

[5] Hale Unsal, *Unsolved Problems about Prime Numbers*, Cankaya University (2002).

[6] *Introduction to twin primes and Brun's constant computation*,
http://numbers.computation.free.fr/Constants/Primes/twin.html (2002).

HWA CHONG JUNIOR COLLEGE, 661 BUKIT TIMAH ROAD, SINGAPORE 269734