J. Appl. Math. & Informatics Vol. **27***(2009), No. 1 - 2, pp. 89 - 96*
Website: http://www.kcam.biz

THE GENERALIZATION OF CLEMENT'S THEOREM ON PAIRS OF PRIMES

HEONSOO LEE* AND YEONYONG PARK

ABSTRACT. In this article, we show a generalization of Clement's theorem on the pair of primes. For any integers n and k, integers n and $n+2k$ are a pair of primes if and only if $2k(2k)![(n-1)!+1]+((2k)!-1)n \equiv 0 \pmod{n(n+2k)}$ whenever $(n,(2k)!) = (n+2k,(2k)!) = 1$. Especially, n or $n+2k$ is a composite number, a pair $(n, n+2k)$, for which $2k(2k)![(n-1)!+1]+((2k)!-1)n \equiv 0$ $(\text{mod } n(n+2k))$ is called a pair of pseudoprimes for any positive integer k. We have pairs of pseudorimes $(n, n+2k)$ with $n \leq 5 \times 10^4$ for each positive integer $k(4 \leq k \leq 10)$.

AMS Mathematics Subject Classification : 11A41, 11A41, 11Y11
Key words and phrases : Prime, pair of primes, Fermat's theorem, Wilson's theorem, Clement's theorem

1. Introduction

For every even number $2k$ are there infinitely many pairs of consecutive primes which differ by $2k$? That is conjectured by Polignac(1849). When $k=1$, this is the famous twin prime conjecture. For a positive integer k, we define pairs of primes with difference $2k$ between primes as follows.

Definition 1.1. Let p_n be the n-th prime number. A pair of primes (p_n, p_n+2k) is called a cousin ([sexy], [octy]) prime for an integer $k = 2([k=3],\ [k=4])$. If $p_{n+1} = p_n + 2k$ then a pair of primes (p_n, p_{n+1}) called a consecutive pair of primes. A consecutive pair of primes is called a consecutive cousin ([sexy], [octy]) prime when an integer $k = 2([k=3],\ [k=4])$.

If (p_n, p_n+2k) is a consecutive pair of primes then it is a pair of primes. Generally, the inverse is not true.

Received March 24, 2008. Accepted October 5, 2008. *Corresponding author.

For example, pairs of primes $(7,11)$,$(13,17)$,$(19,23)$,$\cdots$, $(739,743)$, $\cdots$ are cousin primes and also consecutive cousin primes. Because there is no three primes of the form p_n, p_n+2, p_n+4 apart from 3, 5, 7. Pairs of primes $(5,11)$, $(7,13)$, $(11,17)$, $\cdots$, $(751,757)$, $\cdots$ are sexy primes but not consecutive sexy primes. $(23,29)$, $(31,37)$, $(47,53)$, $\cdots$, $(727,733)$, $\cdots$ are sexy primes and also consecutive sexy primes. Pairs of primes $(3,11)$, $(5,13)$, $(11,19)$ and $(71,79)$ are octy primes but not consecutive octy primes. On the other hand $(89,97)$, $(359,367)$, $(389,397)$ and $(491,499)$ are consecutive octy primes.

2. The counting function $\pi_{2,2k}(x)$.

Define the counting function $\pi_{2,2k}(x)$ of pairs of primes (p_n, p_n+2k) by

$$\pi_{2,2k}(x) = \sharp\{p \leq x \mid (p,\ p+2k) \in P_{2,2k}\}, \tag{2.2}$$

where $P_{2,2k}$ is the set of all pairs of primes with difference $2k$. The function $Li_{2,2k}(x)$ which was introduced by Hardy and Littlewood can be an approximation to $\pi_{2,2k}(x)$ as $x \to \infty$ by the following asymptotic formula([1]).

$$\pi_{2,2k}(x) \sim Li_{2,2k}(x) = 2c_2 \int_2^x \frac{dt}{(\ln t)^2} \prod_{p>2, p|k} \frac{p-1}{p-2},$$

where $c_2 = \prod_{2<p\in P} \left(1 - \frac{1}{(p-1)^2}\right) = 0.660161815846870\cdots$.

Define the counting function $\pi^*_{2,2k}(x)$ of pairs of primes (p_n, p_{n+1}) with $p_{n+1} = p_n + 2k$ by

$$\pi^*_{2,2k}(x) = \sharp\{p_n \leq x \mid (p_n, p_{n+1}) \in P^*_{2,2k}\},$$

where $P^*_{2,2k}$ is the set of all pairs $(p_n, p_{n+1}(= p_n + 2k))$ of consecutive primes with difference $2k$.

Approximating functions $Li^*_{2,4}(x)$, $Li^*_{2,6}(x)$ and $Li^*_{2,8}(x)$, which are formulated by Lee and Park([2], [3]), approximate to $\pi^*_{2,4}(x)$, $\pi^*_{2,6}(x)$ and $\pi^*_{2,8}(x)$ as $x \to \infty$ by the following asymptotic formulas.

$$\pi^*_{2,4}(x) \approx Li^*_{2,4}(x) = 2c_2 \int_2^x \frac{dt}{(\ln t)^2} \tag{2.1}$$

$$\pi^*_{2,6}(x) \approx Li^*_{2,6}(x) = 4c_2 \int_2^x \frac{dt}{(\ln t)^2} - 9c_3 \int_2^x \frac{dt}{(\ln t)^3} \tag{2.2}$$

$$\begin{aligned}\pi^*_{2,8}(x) &\approx Li^*_{2,8}(x) \\ &= 2c_2 \int_2^x \frac{dt}{(\ln t)^2} - 2\frac{9}{2}c_3 \int_2^x \frac{dt}{(\ln t)^3} + \frac{27}{2}c_4 \int_2^x \frac{dt}{(\ln t)^4}\end{aligned} \tag{2.3}$$

where $c_3 = \prod_{5 \leq p} \frac{p^2(p-3)}{(p-1)^3} = 0.635166354604271 \cdots$ and $c_4 = \prod_{5 \leq p < \infty} \frac{p^3(p-4)}{(p-1)^4} = 0.307494878758327 \cdots$. Lee and Park([2], [3]) counted $\pi^*_{2,4}(7 \times 10^{10}) = 161805194$, $\pi^*_{2,6}(7 \times 10^{10}) = 294161183$ and $\pi^*_{2,8}(7 \times 10^{10}) = 133295081$ using several dozens of personal computers, code written in Pascal and the algorithm employed the classic sieve of Eratosthenes to carry out an exhaustive generation and enumeration of the primes. Also, Lee and Park([2], [3]) computed $Li^*_{2,4}(\leq 7 \times 10^{10}) = 161797059.8$, $Li^*_{2,6}(7 \times 10^{10}) = 294182628.5$ and $Li^*_{2,8}(7 \times 10^{10}) = 133284728.6$.

3. The generalization of Clement's theorem on pairs of primes

Fermat discovered a theorem about 1640 which is known as *Fermat's Theorem**([4]).

Theorem 3.1 (Fermat). *Let p be a prime and a be any integer. Then*

$$a^p \equiv a \pmod{p}.$$

If a is not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}. \tag{3.1}$$

Fermat's Little Theorem is the basis for many other results in Number Theory and is the basis for methods of checking whether numbers are prime which are still in use on today's electronic computers. Using the classical congruence (3.1) of Fermat, Wilson discovered the following theorem([5]).

Theorem 3.2(Wilson). *If an integer $n > 1$ is a prime then*

$$(n-1)! + 1 \equiv 0 \pmod{n}. \tag{3.2}$$

Moreover, the converse of Wilson's theorem is true. Indeed, if $n > 1$ is a natural number that is not a prime, then $n = st$, with $1 < s, t < n-1$, so s divides n and $(n-1)!$, and therefore $(n-1)! \equiv -1 \pmod{n}$. So Wilson's theorem gives a characterization of prime number. A characterization of twin primes $(n, n+2)$ is given by Clement([6]).

Theorem 3.3(Clement). *The integers n and $n+2$ are a pair of primes if and only if*

$$4[(n-1)! + 1] + n \equiv 0 \pmod{n(n+2)}.$$

*Fermat's Little Theorem

The following theorem is a generalization of Clement's theorem on the pair of primes with difference $2k$ between primes.

Theorem 3.4 (Generalization of Clement's theorem). *Let n and k be positive integers. For any positive integer k, integers n and $n+2k$ are a pair of primes if and only if*

$$2k(2k)![(n-1)!+1]+((2k)!-1)n \equiv 0 \pmod{n(n+2k)}, \tag{3.3}$$

whenever $(n,(2k)!)=(n+2k,(2k)!)=1$.

Remark 3.5. The case $k=1$ in (3.3) is Clement's theorem. Substituting 2 for k in (3.3), integers n and $n+4$ are cousin primes if and only if $96[(n-1)!+1]+23n \equiv 0 \pmod{n(n+4)}$, whenever $(n,24)=(n+4,24)=1$. The case $k=3$ in (3.3), integers n and $n+6$ are sexy primes if and only if $4320[(n-1)!+1]+719n \equiv 0 \pmod{n(n+6)}$, whenever $(n,720)=(n+6,720)=1$.

The Proof of Theorem 3.4. If n and $n+2k$ are primes, then

$$(n-1)!+1 \equiv 0 \pmod{n} \tag{3.4}$$

and

$$(n+2k-1)!+1 \equiv 0 \pmod{n+2k} \tag{3.5}$$

by Wilson's theorem. Using elementary calculations, it follows that

$$\begin{aligned}(n+2k-1)! &= (n+2k-1)(n+2k-2)\cdots(n+2k-(2k+1))!\\ &\equiv (-1)(-2)\cdots(-2k)(n-1)! \qquad \pmod{n+2k}\\ &\equiv (-1)^{2k}(2k)!(n-1)! \qquad \pmod{n+2k}\\ &\equiv (2k)!(n-1)! \qquad \pmod{n+2k}.\end{aligned}$$

Hence we have

$$(n+2k-1)! \equiv (2k)!(n-1)! \pmod{n+2k}. \tag{3.6}$$

By (3.5) and (3.6), $(2k)!(n-1)!+1 \equiv 0 \pmod{n+2k}$, so

$$(2k)!(n-1)!+1 = t(n+2k) \tag{3.7}$$

for some integer t. Therefore we get

$$(2k)!(n-1)!+1 \equiv 2kt \pmod{n}.$$

Since $(n-1)! \equiv -1 \pmod{n}$ in (3.4), it follows that

$$-(2k)! + 1 \equiv 2kt \pmod{n}. \tag{3.8}$$

Multiplying (3.7) by $2k$,

$$2k(2k)!(n-1)! + 2k = 2kt(n+2k). \tag{3.9}$$

By (3.8) and (3.9), we have

$$2k(2k)!(n-1)! + 2k \equiv (1-(2k)!)(n+2k) \pmod{n(n+2k)}.$$

Hence, we have

$$2k(2k)![(n-1)!+1] + ((2k)!-1)n \equiv 0 \pmod{n(n+2k)}.$$

Conversely, let the congruence be satisfied. Since

$$2k(2k)![(n-1)!+1] + ((2k)!-1)n \equiv 0 \qquad \pmod{n},$$

we can easily deduce that $(n-1)!+1 \equiv 0 \pmod{n}$ because n and $(2k)!$ are relatively primes. And so, n is a prime by Wilson's theorem. Secondarily, it holds that

$$2k(2k)![(n-1)!+1] + ((2k)!-1)n \equiv 0 \pmod{n+2k}.$$

By using equality,

$$\begin{aligned} &2k(2k)![(n-1)!+1] + ((2k)!-1)n \\ &= 2k(2k)!(n-1)! + ((2k)!-1)(n+2k) + 2k, \end{aligned}$$

it follows that

$$2k(2k)!(n-1)! + 2k \equiv 0 \pmod{n+2k}. \tag{3.10}$$

Set $A = (n+2k-1)(n+2k-2)(n+2k-3)(n+2k-4)\cdots(n+1)n$. Then we get

$$\begin{aligned} A = {} & (n+2k)(n+2k-2)(n+2k-3)(n+2k-4)\cdots(n+1)n \\ & -(n+2k-2)(n+2k-3)(n+2k-4)\cdots(n+1)n \\ = {} & (n+2k)(n+2k-2)(n+2k-3)(n+2k-4)\cdots(n+1)n \\ & -(n+2k)(n+2k-3)(n+2k-4)\cdots(n+1)n \\ & +2(n+2k)(n+2k-4)\cdots(n+1)n \\ & -2\times 3(n+2k)(n+2k-5)\cdots(n+1)n \\ & \qquad \vdots \\ & -(2k-1)!n. \end{aligned}$$

The last term in the above equality is $-(2k-1)!n = -(2k-1)!(n+2k) + 2k(2k-1)!$ and so we have $A \equiv 2k(2k-1)! \pmod{n+2k}$. Multiplying by A in the both sides of the congruence (3.10), we have

$$\begin{aligned} 2k(2k)!(n+2k-1)! + (2k)(2k)(2k-1)! &= 2k(2k)![(n+2k-1)!+1] \\ &\equiv 0 \qquad \pmod{n+2k}. \end{aligned}$$

Since $(2k)!$ and $n+2k$ are relatively prime, it follows that $(n+2k-1)!+1 \equiv 0 \pmod{n+2k}$. And so, $n+2k$ is also a prime by Wilson's theorem. □

When $4 \leq k$, the condition $(n,(2k)!) = (n+2k,(2k)!) = 1$ in theorem 3.4. seems to be essential. For instance, if $322560[(n-1)!+1] + 40319n \equiv 0 \pmod{n(n+8)}$ then $(n, n+8)$ is a pair of primes? Generally, it is not true. For $n \leq 5 \times 10^4$, the pais of integers (9,17), (15,23),(21,29),(35,43), (45,53), (63,71) and (105,113) are not prime pairs when $k = 4$. In the case $k = 5$(respectively $k = 6$), the pais of integers (9,19), (27,37),(63,73),(189,199), (567,577),(63,71) and (105,113) (respectively (25,37), (35,47),(55,67),(77,89) and (385,397)) are not satisfied.

Definition 3.6. Let n and k be positive integers and let n or $n+2k$ be a composite number. A pair $(n, n+2k)$, for which

$$2k(2k)![(n-1)!+1] + ((2k)!-1)n \equiv 0 \pmod{n(n+2k)} \tag{3.11}$$

is called a pair of pseudoprimes.

Unfortunately, the huge value of the factorial makes (3.11) of few practical use to find pair of large prime with difference $2k$ between primes. To find pairs of pseudoprimes $(n, n+2k)$ with $n \leq 5 \times 10^4$ for some positive integer k, the following results ware calculated by Mathematica 4.1. We are only concerned with the primality test and modular in the number theory package of Mathematica 4.1([7]).

(1) $k = 4$: There are only seven pairs of pseudoprimes as follows. (9,17), (15,23), (21,29), (35,43), (45,53), (63,71) and (105,113)

(2) $k = 5$: There are only six pairs of pseudoprimes as follows. (9,19), (21, 31), (27,37), (63,73), (189,199) and (567,577)

(3) $k = 6$: There are only five pairs of pseudoprimes as follows. (25,37), (35,47), (55,67), (77,89) and (385,397)

(4) $k = 7$: There are 37 pairs of pseudoprimes as follows. (9, 23), (15, 29), (27, 41), (33, 47), (39, 53), (45, 59), (65, 79), (75, 89), (99, 113), (117, 131), (135, 149), (143, 157), (165, 179), (225, 239), (243, 257), (297, 311),

(405, 419), (429, 443), (495, 509), (585, 599), (825, 839), (1215, 1229), (1287, 1301), (1485, 1499), (2025, 2309), (2673, 2687), (2925, 2939), (5265, 5279), (6075, 6089), (6435, 6449), (10725, 10739), (11583, 11597), (15795, 15809), (19305, 19319), (26325, 26339), (32175, 32189), (34749, 34763)

(5) $k = 8$: There are 76 pairs of pseudoprimes as follows. (15, 31), (21, 37), (27, 43), (45, 61), (55, 71), (63, 79), (81, 97), (91, 107), (135, 151), (147, 163), (165, 181), (175, 191), (195, 211), (225, 241), (297, 313), (315, 331), (351, 367), (385, 401), (405, 421), (441, 457), (525, 541), (585, 601), (637, 653), (675, 691), (693, 709), (735, 751), (891, 907), (975, 991), (1053, 1069), (1155, 1171), (1215, 1231), (1287, 1303), (1365, 1381), (2145, 2161), (2205, 2221), (2457, 2473), (2673, 2689), (2695, 2711), (2835, 2851), (3003, 3019), (3375, 3391), (3675, 3691), (3861, 3877), (4095, 4111), (5005, 5021), (5103, 5119), (5265, 5281), (5733, 5749), (5775, 5791), (6075, 6091), (6435, 6451), (6825, 6841), (8085, 8101), (8505, 8521), (10125, 10141), (11907, 11923), (12285, 12301), (12375, 12391), (13365, 13381), (15015, 15031), (17325, 17341), (17875, 17891), (19845, 19861), (22113, 22129), (22275, 22291), (27027, 27043), (30375, 30391), (32175, 32191), (33075, 33091), (34125, 34141), (35035, 35051), (36855, 36871), (40095, 40111), (43875, 43891), (45045, 45061), (47775, 47791)

(6) $k = 9$: There are 35 pairs of pseudoprimes as follows. (25, 43), (35, 53), (49, 67), (55, 73), (65, 83), (85, 103), (91, 109), (119, 137), (175, 193), (221, 239), (245, 263), (275, 293), (539, 557), (595, 613), (715, 733), (935, 953), (1001, 1019), (1105, 1123), (1309, 1327), (2125, 2143), (2275, 2293), (2695, 2713), (3185, 3198), (3575, 3593), (5005, 5023), (6125, 6143), (6545, 6563), (7735, 7753), (9163, 9181), (9625, 9643), (10829, 10843), (11375, 11393), (35035, 35053), (38675, 38693), (45815, 45833)

(7) $k = 10$: There are 90 pairs of pseudoprimes as follows. (9, 29),(21, 41), (27, 47), (33, 53), (39, 59), (51, 71), (63, 83), (77, 97), (81, 101), (117, 137), (119, 139), (143, 163), (153, 173), (171, 191), (209, 229), (221, 241), (231, 251), (243, 263), (273, 293), (297, 317), (399, 419), (429, 449), (441, 461), (459, 479), (567, 587), (627, 647), (663, 683), (741, 761), (819, 839), (833, 853), (891, 911), (1001, 1021), (1071, 1091), (1197, 1217), (1287, 1307), (1463, 1483), (1539, 1559), (1547, 1567), (1617, 1637), (1701, 1721), (1881, 1901), (1911, 1931), (2079, 2099), (2187, 2207), (2223, 2243), (2261, 2281), (2457, 2477), (2673, 2693), (2907, 2927), (3003, 3023), (3861, 3881), (3927, 3947), (3969, 3989), (4199, 4219), (4389, 4409), (4617, 4637), (4851, 4871), (5967, 5987), (6237, 6257), (6561, 6581), (6669, 6689), (6783, 6803), (7007, 7027), (7497, 7517), (8019, 8039), (8151, 8171), (8721, 8741), (9009, 9029), (9477, 9497), (11781, 11801), (11907, 11927), (12393, 12413), (13167, 13187), (15309, 15329),

(15561, 15581), (17901, 17921), (18711, 18731), (20349, 20369), (22113, 22133), (22491, 22511), (24057, 24077), (24453, 24473), (26163, 26183), (27489, 27509), (32487, 32507), (35343, 35363), (37179, 37199), (39501, 39521), (46683, 46703), (47481, 47501)

References

1. G.H. Hardy and J.E. Littlewood, *Some problems of "Partitio Numerrorum", III: On the expression of a number as a sum of primes*, Acta Math., **44** (1923), 1-70. Reprinted in Collected papers of G.H. Hardy, Clarendon Press, Oxford, V. 3(1966), 561-630
2. Y.Y. Park and H.S. Lee, *On the sevral differences between primes*, J. Appl. Math. & Computing **13**(2003), 37-51
3. H.S. Lee and Y.Y. Park, *On the primes with* $p_{n+1} - p_n = 8$ *and the sum of their reciprocals*, J. Appl. Math. & Computing **22**(2006), 441-452
4. D.M. Burton, *Elementary number theory*, McGraw-Hill, 1980, 97-98
5. P. Ribenboim, *The new book of prime number records*, Springer, 1996, 25-26
6. P.A. Clement, *Congruences fo sets of primes*, Am. Math. Mon., **56**(1949), 23-25
7. Stephen Wolfram, *The Mathematica book 4th ed.*, Wolfram Media/Combridge University Press, 1999

Heonsoo Lee received his Ph.D at Mokpo National University under the direction of Yeonyong Park. Since 2003 he has been at the Mokpo National University as a lecturer. His research interests focus on the theory of the computation of gaps of the prime number.

Department of Mathematics, Mokpo National University, Chonnam 534-729, Korea
e-mail:leehs@mokpo.ac.kr

Yeonyong Park received his Ph.D at KAIST under the direction of Hong Oh Kim. Since 1992 he has been at the Mokpo National University as a faculty. His research interests focus on the theory of harmonic analysis and the computation of gaps of the prime number.

Department of Mathematics, Mokpo National University, Chonnam 534-729, Korea
e-mail:yypark@mokpo.ac.kr