Scientific Research Publishing

Advances in Pure Mathematics, 2022, 12, 624-637
https://www.scirp.org/journal/apm
ISSN Online: 2160-0384
ISSN Print: 2160-0368

Group-Theoretic Remarks on Goldbach's Conjecture

Liguo He[1], Gang Zhu[2]

[1]Department of Mathematics, Shenyang University of Technology, Shenyang, China
[2]College of Teacher Education, Harbin University, Harbin, China
Email: helg-lxy@sut.edu.cn, Zhugang@habu.edu.cn

How to cite this paper: He, L.G. and Zhu, G. (2022) Group-Theoretic Remarks on Goldbach's Conjecture. *Advances in Pure Mathematics*, **12**, 624-637.
https://doi.org/10.4236/apm.2022.1211048

Received: October 8, 2022
Accepted: November 6, 2022
Published: November 9, 2022

Abstract

The famous strongly binary Goldbach's conjecture asserts that every even number $2n \geq 8$ can always be expressible as a sum of two distinct odd prime numbers. We use a new approach to dealing with this conjecture. Specifically, we apply the element order prime graphs of alternating groups of degrees $2n$ and $2n-1$ to characterize this conjecture, and present its six group-theoretic versions; and further prove that this conjecture is true for $p+1$ and $p-1$ whenever $p \geq 11$ is a prime number.

Keywords

Alternating Group, Element Order Prime Graph, Goldbach's Conjecture, Centralizer

1. Introduction

The famous *Strongly Binary Goldbach Conjecture* [1] [2] asserts that for every even number $2n \geq 8$, there exist distinct odd primes p, q such that $2n = p + q$. If this situation does occur, $2n$ is called *a Goldbach's number*. The conjecture is a well-known unsolved problem dating from 1742 due to C. Goldbach. It is commonly considered as an extremely difficult problem of analytic number theory these days. Considering the fundamental role of finite groups (especially, the alternating group A_n of degree $n \geq 5$) in solving the radical solution problem of polynomial equations of degree 5 or more (due to E. Galois, for example, see [3]), we are inspired to attack the Goldbach's problem by appealing to the finite group theory and especially, the alternating group A_n of degree $n \geq 8$. The following Theorem B partially confirms our guess (although its proof is short), it also shows that there exist infinitely many Goldbach's numbers. It is achieved via [1] that all even numbers $2n \leq 4 \times 10^{18}$ are Goldbach's numbers (as of the year

2013) except possibly when n is a prime.

Let G be a finite group and $\pi(G)$ the set of prime factors of its order. The element order prime graph $\Gamma(G)$ of G is a graph whose vertex-set $\mathcal{V}(G)$ is just $\pi(G)$, and two vertices p,q are joined by an edge whenever G contains an element of order pq. The edge set of $\Gamma(G)$ is denoted by $\mathcal{E}(G)$. This graph is also referred to as Gruenberg-Kergel graph of G. Regarding this graph, we refer to [4] [5] for more detailed information. For groups G_1 and G_2, if $\mathcal{V}(G_1)\subseteq\mathcal{V}(G_2)$ and $\mathcal{E}(G_1)\subseteq\mathcal{E}(G_2)$, then $\Gamma(G_1)$ is said to be a subgraph of $\Gamma(G_2)$ and denoted by $\Gamma(G_1)\le\Gamma(G_2)$. Furthermore, if $\mathcal{V}(G_1)$ is a proper subset of $\mathcal{V}(G_2)$, or $\mathcal{E}(G_1)$ is a proper subset of $\mathcal{E}(G_2)$, then $\Gamma(G_1)$ is called a proper subgraph of $\Gamma(G_2)$ and written as $\Gamma(G_1)<\Gamma(G_2)$. Following convention, we write $\pi(x)$ for the prime-counting function which stands for the number of primes not exceeding the positive real number x. By A_n, denote the alternating group of degree n. For a Sylow p-subgroup P of A_n, $C_{A_n}(P)$ (resp. $N_{A_n}(P)$) indicates the centralizer (resp. normalizer) of P in A_n. For two sets S_1 and S_2, the difference set $S_2-S_1=\{x\,|\,x\in S_2 \text{ but } x\notin S_1\}$, whose cardinality is indicated by $|S_2-S_1|$.

In this paper, by using the methods of element order prime graph and group character, we prove the following results.

Theorem A *Assume the above notation and the even integer* $2n\ge 8$. *Then the following assertions are equivalent.*

1) The even number $2n$ is a Goldbach's number.

2) $\Gamma(A_{2n-1})$ is a proper subgraph of $\Gamma(A_{2n})$.

3) $\left|\mathcal{E}(A_{2n})-\mathcal{E}(A_{2n-1})\right|\ge 1$.

4) $\left|\mathcal{E}(A_{2n})-\mathcal{E}(A_{2n-1})\right|\ge 1$ when both $\Gamma(A_{2n-1})$ and $\Gamma(A_{2n})$ are connected graphs.

5) $\left|\pi\left(C_{A_{2n}}(P)\right)-\pi\left(C_{A_{2n-1}}(P)\right)\right|\ge 1$ for some odd prime p with $n<p\le 2n-3$ and some $P\in Syl_p(A_{2n-1})$.

6) $\left|\pi\left(N_{A_{2n}}(P)\right)-\pi\left(N_{A_{2n-1}}(P)\right)\right|\ge 1$ for some odd prime p with $n<p\le 2n-3$ and some $P\in Syl_p(A_{2n-1})$.

7) $dim\mathscr{U}(A_{2n})>dim\mathscr{U}(A_{2n-1})$ for the biprimary spaces $\mathscr{U}(A_{2n})$ and $\mathscr{U}(A_{2n-1})$.

Actually the edge number difference $\left|\mathcal{E}(A_{2n})-\mathcal{E}(A_{2n-1})\right|$ is exactly the number of expressions of $2n$ as sum of two distinct odd primes. This expression number seems to be limitless as n approaches infinity. The inequality $\left|\mathcal{E}(A_{2n})-\mathcal{E}(A_{2n-1})\right|\ge 1$ also implies that A_{2n} and A_{2n-1} can be recognizable each other by prime graphs, but in general it is impossible between A_{2n+1} and A_{2n}. For instance, if $4\le n\le 29$, it can be verified by GAP [6] that $\left|\mathcal{E}(A_{2n+1})-\mathcal{E}(A_{2n})\right|=0$ just when $n\in\{6,9,12,14,15,18,19,21,24,26,27,29\}$. (For the GAP command codes, see the **Appendix**). We mention that Theorem 1 in [7] shows that A_n can be characterized by the full set of its element orders when $n\ge 5, n\ne 6,10$.

Applying the prime graphic approach of finite groups, we also prove a class of

even numbers to be Goldbach's numbers.

Theorem B *Assume that* $p \geq 11$ *is an odd prime. Then the Strongly Binary Goldbach Conjecture is true for* $p+1$ *and* $p-1$.

Unless otherwise stated, the notation and terminology is standard, as presented in [8] [9] [10].

2. Prime Graph

The following observation is a basic but crucial fact, which appears as Proposition 1.1 in [11] without proof there. We restate it in the language of prime graph.

Lemma 2.1. Let A_n denote the alternating group of degree $n \geq 8$.

1) For distinct odd primes $p, q \in \mathcal{V}(A_n)$, the edge $pq \in \mathcal{E}(A_n)$ if and only if $p+q \leq n$.

2) For distinct primes $2, p \in \mathcal{V}(A_n)$, the edge $2p \in \mathcal{E}(A_n)$ if and only if $p+4 \leq n$.

Proof. Let p, q be different odd primes. If $p+q \leq n$, it is no loss to pick the element $(1,2,\cdots,p)(p+1,\cdots,p+q) \in A_n$. If $p+4 \leq n$, it is no loss to choose the element $(1,2,\cdots,p)(p+1,p+2)(p+3,p+4) \in A_n$, the "if" part is obtained.

If the edge $pq \in \mathcal{E}(A_n)$, then A_n contains an element x of order pq, and x has disjoint cycle product expression $x = c_1 c_2 \cdots c_t$ with cycle lengths $|c_i| = m_i$ and the order of x is the least common multiple $[m_1, m_2, \cdots, m_t]$ which equals pq, and thus $m_i = p^{\alpha} q^{\beta}$ with $0 \leq \alpha, \beta \leq 1$. Since also $\sum_{i=1}^{t} m_i \leq n$, we get $p+q \leq n$. (This can also be attained by Corollary 1 of [12].) If A_n has an element x of order $2p$, then its disjoint cycle product expression contains at least two even cycles (*i.e.*, their cycle lengths are even numbers), the even cycles are either 2-cycles or $2p$-cycles, hence $p+4 \leq n$, the "only if" part is achieved. □

The following is Part 2 of Theorem A.

Theorem 2.2. The Strongly Binary Goldbach's conjecture is true for $2n(\geq 8)$ if and only if the element order prime graph $\Gamma(A_{2n-1})$ is a proper subgraph of $\Gamma(A_{2n})$.

Proof. For odd prime p, $p+4 \leq 2n$ if and only if $p+4 \leq 2n-1$. Thus Lemma 2.1 yields that $2p$ is an edge of $\Gamma(A_{2n-1})$ if and only if it is also an edge of $\Gamma(A_{2n})$. Hence if $\Gamma(A_{2n-1})$ is a proper subgraph of $\Gamma(A_{2n})$, then there exist distinct odd primes p, q such that the edge $pq \in \mathcal{E}(A_{2n})$ but $pq \notin \mathcal{E}(A_{2n-1})$, thus Lemma 2.1 implies $p+q \leq 2n$ and $p+q > 2n-1$, which forces $2n = p+q$, as desired. The reverse statement is immediate by $\pi(A_{2n}) = \pi(A_{2n-1})$. □

The following is Part 3 of Theorem A.

Corollary 2.3. The Strong Binary Goldbach's conjecture is valid for $2n(\geq 8)$ if and only if $|\mathcal{E}(A_{2n}) - \mathcal{E}(A_{2n-1})| \geq 1$.

Proof. Since $\pi(A_{2n}) = \pi(A_{2n-1})$, we reach that $\Gamma(A_{2n-1})$ is a proper subgraph of $\Gamma(A_{2n})$ if and only if $\mathcal{E}(A_{2n-1})$ is a proper subset of $\mathcal{E}(A_{2n})$, that is, $|\mathcal{E}(A_{2n}) - \mathcal{E}(A_{2n-1})| \geq 1$. Thus the desired result follows from Theorem 2.2. □

Because $|\mathcal{E}(A_{2n}) - \mathcal{E}(A_{2n-1})| \geq 0$ is an integer, it is easy to see that

$\left|\mathcal{E}\left(A_{2n}\right)-\mathcal{E}\left(A_{2n-1}\right)\right|\geq 1$ if and only if $\left|\mathcal{E}\left(A_{2n}\right)-\mathcal{E}\left(A_{2n-1}\right)\right|>0$. A little bit of difference between the two expressions is of meaningful sometimes in order to prove this conjecture when the method of analytic number theory is applied.

Let the alternating group A_n permute the symbol set $\Omega=\{1,2,\cdots,n\}$ and write $A_t\left(\leq A_n\right)$ as $A_{(s,s+t)}$ in order to indicate the moved elements to be at most in the symbol subset $\{s,s+1,\cdots,s+t\}\subseteq\Omega$. For $s+t<r<r+m\leq n$, write $A_{(s,s+t)}\times A_{(r,r+m)}<A_n$ to denote the inner direct product of $A_{(s,s+t)}$ and $A_{(r,r+m)}$ in A_n.

Lemma 2.4. Let q be a prime with $n/2<q\leq n-2$ and $n\geq 8$, and let $Q=\langle x\rangle\in Syl_q\left(A_n\right)$ for some element $x\in A_n$ of order q. Assume that Q just permutes the symbol subset $\{1,2,\cdots,q\}$. Then $\left|C_{A_n}\left(x\right)\right|=\left|C_{A_n}\left(Q\right)\right|=q\dfrac{(n-q)!}{2}$ and $\left|N_{A_n}\left(Q\right)\right|=(q-1)q\dfrac{(n-q)!}{2}$. Furthermore, $C_{A_n}\left(x\right)=C_{A_n}\left(Q\right)=Q\times A_{(q+1,n)}$ and $N_{A_n}\left(Q\right)=\left(Q\rtimes C_{q-1}\right)\times A_{(q+1,n)}$ where C_{q-1} is a cyclic subgroup of $A_{(1,q)}$ with order $q-1$ and the subgroup $Q\rtimes C_{q-1}$ is a Frobenius group.

Proof. For the element $x\in Q$ of order q, then it is a q-cycle and so $C_{A_n}\left(x\right)=C_{A_n}\left(Q\right)$. Using the crucial observation $x^g=\left(i_1^g,i_2^g,\cdots,i_q^g\right)$ for any $g\in A_n$, we may deduce $C_{A_n}\left(Q\right)=Q\times A_{(q+1,n)}$ and so $\left|C_{A_n}\left(Q\right)\right|=q\dfrac{(n-q)!}{2}$. Note that if $x=(1,2,\cdots,q)$, then $x^g=x$ implies

$$\left(1^g,2^g,\cdots,q^g\right)=(1,2,3,\cdots,q)=(q,1,2,\cdots,q-1)=\cdots=(2,3,\cdots,q,1).$$

For $g\in N_{A_n}\left(Q\right)$, we have $x^g=x^k\in Q$ for some $1\leq k\leq q-1$, and x^k is still a q-cycle. If there exists $h\in N_{A_n}\left(Q\right)$ such that $x^h=x^k$, then $x^{hg^{-1}}=x$ and so $hg^{-1}\in C_{A_n}\left(Q\right)$ and $h\in gC_{A_n}\left(Q\right)$. Thus we may further obtain that $N_{A_n}\left(Q\right)\leq A_{(1,q)}\times A_{(q+1,n)}$. Note that we have $gC_{A_n}\left(Q\right)=C_{A_n}\left(Q\right)g$ for $g\in N_{A_n}\left(Q\right)$ as $C_{A_n}\left(Q\right)\trianglelefteq N_{A_n}\left(Q\right)$

For $1\leq m\leq q-1$, each of x and x^m is q-cycle, so both of them are conjugate, *i.e.*, $x^m=x^h$, $h\in S_n$ (which denotes the symmetric group of degree n). We may choose the element h in A_n. As $x\in A_{(1,q)}$, we get $x^m\in A_{(1,q)}$. If h is an odd permutation, we may replace h with the disjoint cycle product yh, where $y=(q+1,q+2)$ and $q\leq n-2$. We see $x^{yh}=x^h=x^m$. For $h\in A_n$, we may further derive that $h\in A_{(1,q)}\times A_{(q+1,n)}$ and $h\in N_{A_n}\left(Q\right)$, this is because x^m and x lie in Q.

For $1\leq m<n\leq q-1$, let $x^m=x^{g_1}$ and $x^n=x^{g_2}$ for $g_1,g_2\in A_n$, we claim $C_{A_n}\left(Q\right)g_1\neq C_{A_n}\left(Q\right)g_2$. If otherwise, $x^{g_1}=x^{g_2}$ and so $x^n=x^m$, then $x^{n-m}=1$, this is a contradiction since the order of x is q. Hence we deduce $\left|N_{A_n}\left(Q\right)/C_{A_n}\left(Q\right)\right|=q-1$. The N/C Theorem further yields $N_{A_n}\left(Q\right)/C_{A_n}\left(Q\right)\cong C_{q-1}$. Since $N_{A_n}\left(Q\right)\leq A_{(1,q)}\times A_{(q+1,n)}$, it follows via Dedekind identity that

$$N_{A_n}\left(Q\right)=\left(N_{A_n}\left(Q\right)\cap A_{(1,q)}\right)\times A_{(q+1,n)}=N_{A_{(1,q)}}\left(Q\right)\times A_{(q+1,n)}.$$

Since also Q is a normal Sylow q-subgroup of $N_{A_{(1,q)}}\left(Q\right)$ and $\left|Q\right|=q$, the Schur-

Zassenhaus theorem yields that $N_{A_{(1,q)}}(Q)=Q\rtimes C_{q-1}$ for some $C_{q-1}<A_{(1,q)}$. Note that the following equality

$$\frac{\left|N_{A_{(1,q)}}(Q)\right|}{|Q|}=\frac{\left|N_{A_{(1,q)}}(Q)\right|\left|A_{(q+1,n)}\right|}{|Q|\left|A_{(q+1,n)}\right|}=\left|N_{A_n}(Q)/C_{A_n}(Q)\right|=q-1.$$

Therefore, we conclude that $N_{A_n}(Q)=\left(Q\rtimes C_{q-1}\right)\times A_{(q+1,n)}$. Because $C_{A_{(1,q)}}(Q)=Q$, we reach that C_{q-1} acts fixed-point-freely on Q, it follows via ([9], Theorem 8.1.12) that $Q\rtimes C_{q-1}$ is a Frobenius group. The proof is complete. □

Observe that the above result actually shows that both $N_{A_{2n}}(Q)$ and $N_{A_{2n-1}}(Q)$ have the same Frobenius subgroups of order pq.

Lemma 2.5. Let the natural number $n\geq 4$ and the primes q with $n<q\leq 2n-3$, then

1) The number of edges incident to vertices q of $\Gamma(A_{2n})$ is equal to $\sum_{n<q\leq 2n-3}\left|\pi\left(A_{2n-q}\right)\right|$ which equals $\sum_{n<q\leq 2n-3}\pi(2n-q)$.

2) The number of edges incident to vertices q of $\Gamma(A_{2n-1})$ is equal to $\sum_{n<q\leq 2n-3}\left|\pi\left(A_{2n-1-q}\right)\right|$ which equals $\sum_{n<q\leq 2n-3}\pi(2n-1-q)$.

Proof. For $n<q\leq 2n-3$, if $\mathcal{E}(A_{2n})$ contains edge pq, then A_{2n} has an element g of order pq which can be uniquely written in the form $g=g_pg_p$ with p-part g_p and q-part g_q of g, thus $g_p\in C_{A_{2n}}\left(g_q\right)$, Lemma 2.4 yields that $p\in\pi\left(A_{2n-q}\right)$. Conversely, if $p\in\pi\left(A_{2n-q}\right)$, then $p+q\leq 2n$ for odd p and $4+q\leq 2n$ for $p=2$, Lemma 2.1 yields A_{2n} has an element g of order pq. Note that if $2\in\pi\left(A_{2n-q}\right)$, then 2 divides $(2n-q)!/2$, thus $2n-q\geq 5$ so that $4+q<2n$. It is straightforward that

$$\sum_{n<q\leq 2n-3}\left|\pi\left(A_{2n-q}\right)\right|=\sum_{n<q\leq 2n-3}\pi(2n-q).$$

Part 1 follows. And Part 2 can be derived in a similar manner. □

Theorem 2.6. Let the natural number $n\geq 4$, then

$$\left|\mathcal{E}(A_{2n})-\mathcal{E}(A_{2n-1})\right|=\sum_{3\leq p<n}\left(\pi(2n-p)-\pi(2n-1-p)\right).$$

Proof. By Lemma 2.5, we see

$$\left|\mathcal{E}(A_{2n})-\mathcal{E}(A_{2n-1})\right|=\sum_{n<q\leq 2n-3}\left(\pi(2n-q)-\pi(2n-1-q)\right).$$

It is easy to see that $\pi(2n-q)-\pi(2n-1-q)$ equals either 1 or else 0. If $\pi(2n-q)-\pi(2n-1-q)=1$, then there exists a unique odd $p<n$ such that the edge $pq\in\mathcal{E}(A_{2n})-\mathcal{E}(A_{2n-1})$, Lemma 2.1 yields $2n-1<p+q\leq 2n$ and so $q=2n-p$, thus $q\in\pi\left(A_{2n-p}\right)$ but $q\notin\pi\left(A_{2n-1-p}\right)$, hence $\pi(2n-p)-\pi(2n-1-p)=1$, and vice versa. Therefore we conclude that

$$\sum_{n<q\leq 2n-3}\left(\pi(2n-q)-\pi(2n-1-q)\right)=\sum_{3\leq p<n}\left(\pi(2n-p)-\pi(2n-1-p)\right),$$

yielding the desired result. □

The prime number theorem (PNT for short) with the best known error term is

$$\pi(x)=\mathrm{li}(x)+O\left(x\exp\left(-c(\log x)^{3/5}(\log\log x)^{-1/5}\right)\right)$$

for some strictly positive constant c. This can be found in ([13], p 250) and the definition of $\mathrm{li}(x)$ is in ([13], p 257) where $\mathrm{li}(x)$ is denoted $\mathrm{Li}(x)$. Under the Riemman's hypothesis, it is known via [1] that the PNT has a concise form $|\pi(x)-\mathrm{li}(x)|<\frac{\sqrt{x}\log x}{8\pi}$. We may set $\pi(x)=\mathrm{li}(x)+h(x)\frac{\sqrt{x}\log x}{8\pi}$ for some function $h(x)$ satisfying $|h(x)|<1$. Thus it seems natural to estimate the above expression of Theorem 2.6 by using the PNT, but it is necessary to deeply extract $h(x)$. Note that in order to prove $|\mathcal{E}(A_{2n})-\mathcal{E}(A_{2n-1})|\geq 1$, it is enough to prove $|\mathcal{E}(A_{2n})-\mathcal{E}(A_{2n-1})|>0$. For any enough small positive number ε, we may let $\overline{h}(x)=\varepsilon h(x)$, then $|\overline{h}(x)|<\varepsilon$ and the PNT has form $\pi(x)=\mathrm{li}(x)+\overline{h}(x)\frac{\sqrt{x}\log x}{8\pi\varepsilon}$, which seems more useful. Without Riemann's hypothesis, we may also present a similar form for $\pi(x)$. Although these observations seem to be interesting, we are still intent to handle the conjecture by appealing to the method associated closely with the finite group theory in this paper.

Lemma 2.7. Let $n\geq 6$. If $\Gamma(A_{2n})=\Gamma(A_{2n-1})$, then $\Gamma(A_{2n})=\Gamma(A_{2n-2})$.

Proof. It is evident that $\Gamma(A_{2n-2})\leq\Gamma(A_{2n})$. Under the hypothesis above, we shall prove $\Gamma(A_{2n})\leq\Gamma(A_{2n-2})$.

Assume that A_{2n} contains an element of odd order pq. Since $\Gamma(A_{2n})=\Gamma(A_{2n-1})$, it follows that A_{2n-1} also contains an element of odd order pq, then $p+q\leq 2n-1$ by Lemma 2.1, consequently $p+q\leq 2n-2$ (as the sum $p+q$ is even), thus we conclude that A_{2n-2} has an element of odd order pq.

Assume now that A_{2n} has an element x of order $2p$. Then the product expression of disjoint cycles of x contains at most some 2-cycles, p-cycles or $2p$-cycles. If its expression has all cycles of three types, then $2+p+2p\leq 2n$ and so $4+p\leq 2n-2$ (as $p\geq 3$), Lemma 2.1 implies that A_{2n-2} owns elements of order $2p$. Because a single even cycle is an odd permutation, it follows that if the expression exactly contains one type of cycles, then the only possibility is of $2p$-cycles, we get $2(2p)\leq 2n$ and so $4+p\leq 2n-2$, as wanted. Therefore we are reduced to the case where the expression precisely contains two types of cycles.

If x is a product of some 2-cycles and p-cycles, then the number of 2-cycle factors in the product expression of disjoint cycles of x is even number, say $2t$. When $t\geq 2$, we know $4+p\leq 2n-2$ (as $2t\cdot 2+p\leq 2n$). When $t=1$, we see that the odd number $4+p\leq 2n-1$. If A_{2n-2} contains no element of order $2p$, then $4+p>2n-2$ (again by Lemma 2.1), hence $4+p=2n-1$, that is, $2n=5+p$. Since $n\geq 6$, we get that $p\neq 5$, and thus $\Gamma(A_{2n})$ has edge $5p$ but $\Gamma(A_{2n-1})$ has not, hence $\Gamma(A_{2n-1})<\Gamma(A_{2n})$, a contradiction. Hence A_{2n-2} con-

tains elements of order $2p$, as desired. If x is a product of some 2-cycles and $2p$-cycles, then we obtain that $2+2p \le 2n$ and so $4+p \le 2n-1$, thus the same argument as the preceding paragraph yields the desired result.

If x is a product of some p-cycles and $2p$-cycles, then $p+2(2p) \le 2n$ and so $4+p \le 2n-2$, as required. The proof is finished. □

The following is the former part of Theorem B.

Theorem 2.8. Let $p \ge 7$ be a prime, then $p+1$ is a Goldbach's number.

Proof. It is evident that $8 = 5+3$, thus we may assume $p \ge 11$. If $\Gamma(A_{p+1}) = \Gamma(A_p)$, then Lemma 2.7 yields $\Gamma(A_{p+1}) = \Gamma(A_{p-1})$. However, this is impossible since $\Gamma(A_{p+1})$ has vertex p, which is not a vertex of $\Gamma(A_{p-1})$. Thus we obtain that $\Gamma(A_{p+1}) > \Gamma(A_p)$, then Lemma 2.1 yields that $p+1$ is just a Goldbach's number, as desired. □

Theorem 2.9. Let $2n \ge 8$. If $\Gamma(A_{2n}) < \Gamma(A_{2n+1})$, then $2n = p+3$ for some odd prime $p > 3$.

Proof. For the distinct odd primes p, q, if the edge $pq \in \mathcal{E}(A_{2n+1})$, then $p+q \le 2n+1$, and so $p+q \le 2n$, Lemma 2.1 yields the edge $pq \in \mathcal{E}(A_{2n})$. Thus there exists some edge $2p \in \mathcal{E}(A_{2n+1})$ but not in $\mathcal{E}(A_{2n})$. Lemma 2.1 shows that $4+p \le 2n+1$ but $4+p > 2n$, which forces $2n+1 = p+4$, and so $2n = p+3$. Also $2n \ge 8$ and so $p > 3$, it follows that $2n$ is a Goldbach's number, as desired. □

The following is the latter part of Theorem B.

Theorem 2.10. Let $p \ge 11$ be a prime, then $p-1$ is a Goldbach's number.

Proof. Since $p \in \mathcal{V}(A_p)$ but not in $\mathcal{V}(A_{p-1})$, it follows that $\Gamma(A_{p-1}) < \Gamma(A_p)$, then Theorem 2.9 yields that $p-1$ is a Goldbach's number, as wanted. □

Proposition 2.11. It is true that $\pi(x) - \pi(6x/7) \ge 1$ for $x \ge 37$.

Proof. See Theorem 2 of [14]. □

The next consequence shows that there are infinitely many Goldbach's numbers.

Corollary 2.12. For each $n \ge 5$, there exists at least two Goldbach's numbers $2m-2, 2m$ satisfying $\frac{12n-7}{7} < 2m-2, 2m \le 2n$.

Proof. By Proposition 2.11, there is a prime p with $\frac{12n}{7} < p < 2n$ for $n \ge 19$. Applying Theorems 2.8 and 2.10, we get that $p-1, p+1$ are Goldbach's numbers and $\frac{12n-7}{7} < p-1, p+1 \le 2n$, we may take $2m-2 = p-1$ and $2m = p+1$. For $5 \le n \le 18$, it is routine to check that there exist Goldbach's numbers $2m-2, 2m$ satisfying $\frac{12n-7}{7} < 2m-2, 2m \le 2n$, as claimed. □

The following result reduces the Strongly Binary Goldbach's conjecture to the situation where both graphs $\Gamma(A_{2n})$ and $\Gamma(A_{2n-1})$ connected, which is Part 4 of Theorem A.

Theorem 2.13. Let $n \ge 4$, the graph $\Gamma(A_{2n-1})$ or $\Gamma(A_{2n})$ is disconnected, then $2n$ is a Goldbach's number.

Proof. By Theorem 1 of [5], the element order prime graphs of alternating groups on five or more symbols have at most three components. Table Id of [5] implies that $\Gamma(A_{2n})$ can not have three components. If $\Gamma(A_{2n})$ has two components, then Table Ib of [5] implies $2n = p+1$ for odd prime p, the result follows from Theorem 2.8. If $\Gamma(A_{2n})$ has one component and $\Gamma(A_{2n-1})$ has two components, then the application of Theorem 3.2 yields the result. □

Theorem 2.14. It is valid that $1 \le \left|\mathcal{E}(A_{2n}) - \mathcal{E}(A_{2n-1})\right| \le 6$ when $4 \le n \le 30$.

Proof. By using GAP [6], we may compute that the edge number differences $\left|\mathcal{E}(A_{2n}) - \mathcal{E}(A_{2n-1})\right|$ when $4 \le n \le 30$. (For GAP command codes, see the **Appendix**). Set $d(n) = \left|\mathcal{E}(A_{2n}) - \mathcal{E}(A_{2n-1})\right|$, the specific results are listed in the following **Table 1**. □

3. Centralizer

We use $C_G(g)$ to denote the centralizer of g in G, *i.e.* $C_G(g) = \{x \in G \mid xg = gx\}$.

Theorem 3.1. The even number $2n \ge 8$ is a Goldbach's number if and only if there exists an element $g \in A_{2n-1}$ of odd prime order such that $\pi\left(C_{A_{2n-1}}(g)\right)$ is a proper subset of $\pi\left(C_{A_{2n}}(g)\right)$.

Proof. Set A_{2n} to act on the symbol set $\Omega = \{1,2,\cdots,2n-1,2n\}$; and A_{2n-1} on the symbol set $\Omega_1 = \{1,2,\cdots,2n-1\}$. Suppose that $2n$ is a Goldbach's number. Then $2n = s+t$ for distinct odd primes $s > t$. Pick $g = (1,2,\cdots,s) \in A_{2n-1}$ and so $x = (s+1, s+2, \cdots, 2n) \notin A_{2n-1}$, we have $x \in C_{A_{2n}}(g)$. If $t \in \pi\left(C_{A_{2n-1}}(g)\right)$, then since $(t,s) = 1$, it follows via Lemma 2.4 that there is an element $(a_1, a_2, \cdots, a_t) \in C_{A_{2n-1}}(g)$ satisfying all $s+1 \le a_i \le 2n-1$, which forces $t + s \le 2n-1$, this contradiction shows $t \notin \pi\left(C_{A_{2n-1}}(g)\right)$. Conversely, if $\pi\left(C_{A_{2n-1}}(g)\right)$ is a proper subset of $\pi\left(C_{A_{2n}}(g)\right)$ for some element g (in A_{2n-1}) of order s, then there exists prime $t \in \pi\left(C_{A_{2n}}(g)\right) - \pi\left(C_{A_{2n-1}}(g)\right)$, thus $C_{A_{2n}}(g)$ contains element x of order t, but $C_{A_{2n-1}}(g)$ contains no element of order t. Note that t must be an odd prime. Hence A_{2n} has an element, say gx, of order st. Note that $(s,t) = 1$. However, A_{2n-1} does not contain any element of order st. If this is not the case, let $z \in A_{2n-1}$ be of order st, then z^t is of order s and conjugate to g, say $z^t = g^h$ for some $h \in A_{2n}$, and z^s has order t. Thus $C_{A_{2n-1}^h}(g^h)$ contains the element z^s of order t. This is a contradiction since

$$\pi\left(C_{A_{2n-1}}(g)\right) = \pi\left(\left(C_{A_{2n-1}}(g)\right)^h\right) = \pi\left(C_{A_{2n-1}^h}(g^h)\right).$$

Hence A_{2n} contains element of order st, but not for A_{2n-1}, the application of Lemma 2.1 yields $2n = s+t$, as required. □

Table 1. Edge number differences $d(n)$ for $4 \le n \le 30$.

n	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$d(n)$	1	1	1	1	2	2	2	2	3	2	2	3	2	3
n	18	19	20	21	22	23	24	25	26	27	28	29	30	
$d(n)$	4	1	3	4	3	3	5	4	3	5	3	3	6	

For any prime $n < p < 2n$, the Sylow p-subgroup P of A_{2n-1} is of order p, which is also a Sylow p-subgroup of A_{2n}, denoted by $P \in Syl_p(A_{2n})$. Hence Theorem 3.1 can also be expressed as the following version, which is Part 5 of Theorem A.

Corollary 3.2. The even number $2n \geq 8$ is a Goldbach's number if and only if there exists an odd prime $n < p \leq 2n-3$ such that $\left|\pi\left(C_{A_{2n}}(P)\right) - \pi\left(C_{A_{2n-1}}(P)\right)\right| \geq 1$ for some $P \in Syl_p(A_{2n-1})$.

Proof. Following from Theorem 3.1. Note that $C_{A_{2n-1}}(g) = C_{A_{2n-1}}(P)$ and $C_{A_{2n}}(g) = C_{A_{2n}}(P)$ for $1 \neq g \in P$, $P \in Syl_p(A_{2n-1})$ and $n < p \leq 2n-3$. □

Corollary 3.3. The even number $2n \geq 8$ is a Goldbach's number if and only if there exists an odd prime $n < q \leq 2n-3$ such that $C_{A_{2n}}(Q)$ contains elements of order pq but $C_{A_{2n-1}}(Q)$ does not contains elements of order pq for some $q \neq p \in \pi(A_{2n-1})$.

Proof. Immediate from Corollary 3.2. □

For the distinct odd primes p, q, it is easy to see that the group G has elements of order pq if and only if G has a cycle subgroup of order pq. However, even if G has a subgroup of order pq, G need not contain elements of order pq. For the primes $p > q$ with $p \equiv 1 \bmod q$, we may construct the semidirect product $G = P \rtimes Q$ with $|P| = p$, $|Q| = q$ and $Q \leq Aut(P)$. Here G is indeed a Frobenius group of order pq. The following is a general result, which is a direct consequence of G. Higman's theorem in [15].

Theorem 3.4. Let G be a pq-group. Then G has no element of order pq if and only if G is a Frobenius group.

Proof. The pq-group G has no pq-element if and only if G has only elements of prime power orders, thus Higman's theorem [15] yields $G = P \rtimes Q$ (P, Q possibly interchangeable) and Q acts fixed-point-freely on P. Applying Theorem 8.1.12 in [9], we know G is a Frobenius group. Conversely, a pq-Frobenius group obviously contains no element of order pq. □

By Problem 6.16 of [8], it follows that $|Q| < \frac{1}{2}|P|$ for the odd Frobenius group $G = P \rtimes Q$.

Corollary 3.5. Let G be a $\{p, q\}$-separable group, and p, q be distinct odd prime divisors of $|G|$. Then G contains no element of order pq if and only if Hall $\{p, q\}$-subgroups of G are Frobenius groups.

Proof. Omitted. □

As shown above, pq-group need not contain element of order pq but this does not really affect the existence of elements of order pq in the difference set $N_{A_{2n}}(Q) - N_{A_{2n-1}}(Q)$, the following result indeed shows both $N_{A_{2n}}(Q)$ and $N_{A_{2n-1}}(Q)$ has the same Frobenius subgroups, which is Part 6 of Theorem A.

Theorem 3.6. The even number $2n \geq 8$ is a Goldbach's number if and only if there exists an odd prime $n < q \leq 2n-3$ such that $\left|\pi\left(N_{A_{2n}}(Q)\right) - \pi\left(N_{A_{2n-1}}(Q)\right)\right| \geq 1$ for some $Q \in Syl_q(A_{2n})$.

Proof. For the prime $n < q \leq 2n-3$ and $Q \in Syl_p(A_{2n})$, the application of

Lemma 2.4 yields that

$$\pi\left(N_{A_{2n}}(Q)\right)=\{q\}\cup\pi\left(C_{q-1}\right)\cup\pi\left(A_{(q+1,2n)}\right)$$

and

$$\pi\left(N_{A_{2n-1}}(Q)\right)=\{q\}\cup\pi\left(C_{q-1}\right)\cup\pi\left(A_{(q+1,2n-1)}\right),$$

thus we have that

$$\pi\left(N_{A_{2n}}(Q)\right)-\pi\left(N_{A_{2n-1}}(Q)\right)=\pi\left(A_{(q+1,2n)}\right)-\pi\left(A_{(q+1,2n-1)}\right).$$

Using Lemma 2.4 again, it follows that

$$\pi\left(C_{A_{2n}}(Q)\right)=\{q\}\cup\pi\left(A_{(q+1,2n)}\right) \text{ and } \pi\left(C_{A_{2n-1}}(Q)\right)=\{q\}\cup\pi\left(A_{(q+1,2n-1)}\right),$$

hence we get that

$$\pi\left(C_{A_{2n}}(Q)\right)-\pi\left(C_{A_{2n-1}}(Q)\right)=\pi\left(A_{(q+1,2n)}\right)-\pi\left(A_{(q+1,2n-1)}\right).$$

Therefore, we conclude that

$$\left|\pi\left(N_{A_{2n}}(Q)\right)-\pi\left(N_{A_{2n-1}}(Q)\right)\right|=\left|\pi\left(C_{A_{2n}}(Q)\right)-\pi\left(C_{A_{2n-1}}(Q)\right)\right|.$$

Corollary 3.2 implies the desired result. □

The next result may be compared with Corollary 3.3 replacing $C_{A_{2n-1}}(Q)$ and $C_{A_{2n}}(Q)$ by $N_{A_{2n-1}}(Q)$ and $N_{A_{2n}}(Q)$, respectively.

Theorem 3.7. The even number $2n\geq 8$ is a Goldbach's number if and only if there exists an odd prime $n<q\leq 2n-3$ such that $N_{A_{2n}}(Q)$ contains elements of order pq but $N_{A_{2n-1}}(Q)$ does not contains elements of order pq for some $q\neq p\in\pi\left(A_{2n-1}\right)$.

Proof. If $2n\geq 8$ is a Goldbach's number, then we may write $2n=q+p$ for odd primes $q>p$. Set $x=(1,2,\cdots,q)$ and $Q=\langle x\rangle$. Corollary 3.2 yields p divides $\left|C_{A_{2n}}(Q)\right|$ and so there exists element g of order pq with $g\in C_{A_{2n}}(Q)\leq N_{A_{2n}}(Q)$ but p does not divides $\left|C_{A_{2n-1}}(Q)\right|$. (Thus $C_{A_{2n-1}}(Q)$ does not contain any element of order pq.) If $N_{A_{2n-1}}(Q)$ has elements of order pq, then Lemma 2.4 implies pq divides $\left|Q\rtimes C_{q-1}\right|$, and $Q\rtimes C_{q-1}$ contains elements of order pq. However, this is impossible since Lemma 2.4 also yields $Q\rtimes C_{q-1}$ is a Frobenius group and Corollary 3.5 shows $Q\rtimes C_{q-1}$ has no element of order pq. The proof is completed. □

We mention that A_n ($n\geq 4$) can be characterized by the full set of orders of normalizers of its Sylow's subgroups as stated in Theorem 1 of [16].

4. Group Algebra

In fact, the strongly binary Goldbach's conjecture is also expressed in the language of group algebra. Let G be a finite group, and $p,q\in\pi(G)$ be distinct odd primes. Set

$$s(p,q,g)=\sum_{\substack{x\in G\\ o(g)=pq}} g^x.$$

It is easy to see that $s(p,q,g) \in Z(\mathbb{C}[G])$, where $Z(\mathbb{C}[G])$ denotes the center of group algebra $\mathbb{C}[G]$ of the group G over complex field $\mathbb{C}$ and it is a subalgebra of the group algebra $\mathbb{C}[G]$. By Theorem 2.4 of [8], we see that all conjugacy class sums of G form a basis of $Z(\mathbb{C}[G])$. The space linearly spanned by all possible $s(p,q,g)$'s is written as $\mathscr{U}(G) = \mathcal{L}(s(p,q,g) \mid g \in G, \text{distinct odd primes } p,q \in \pi(G))$ and we call $\mathscr{U}(G)$ as a *biprimary space* of G, then $\mathscr{U}(G)$ is a subspace of $Z(\mathbb{C}[G])$. It is evident that $dim(\mathscr{U}(A_{2n-1})) \le dim(\mathscr{U}(A_{2n}))$. Fix

$$\tilde{s}(p,q,g) = \sum_{\substack{g \in A_{2n-1}, x \in A_{2n} \\ o(g)=pq}} g^x,$$

and

$$\tilde{\mathscr{U}}(A_{2n-1}) = \mathscr{L}(\tilde{s}(p,q,g) \mid g \in A_{2n-1}, \text{distinct odd primes } p,q \in \pi(A_{2n-1}))$$

It is clear that $\tilde{\mathscr{U}}(A_{2n-1}) \le \mathscr{U}(A_{2n})$ and $dim\mathscr{U}(A_{2n-1}) = dim\tilde{\mathscr{U}}(A_{2n-1})$.

The above observations imply the next result, which covers Part 7 of Theorem A.

Theorem 4.1. There exist different odd primes p,q with $2n = p+q \Leftrightarrow dim(\mathscr{U}(A_{2n-1})) < dim(\mathscr{U}(A_{2n})) \Leftrightarrow \tilde{\mathscr{U}}(A_{2n-1}) < \mathscr{U}(A_{2n})$

Proof. Omitted. □

In fact, the basis vectors $s(p,q,g)'s$ are computable. Set $s_1, s_2, \cdots, s_r$ to be a basis of the biprimary space $\mathscr{U}(A_{2n})$ ($n \ge 8$) and each s_i stands for some $s(p,q,g)$ in a suitable order. Let $\{e_1, e_2, \cdots, e_t\}$ be the full set of central primitive idempotent elements of group algebra $\mathbb{C}[A_n]$, let $\{K_1, K_2, \cdots, K_t\}$ be the full set of class sums of A_n, then we have

$$(s_1, s_2, \cdots, s_r) = (K_1, K_2, \cdots, K_t) A_{tr},$$

where the (i,j)-entries a_{ij} of A_{tr} is either 1 or else 0.

The application of Theorem 2.12 of [8], we conclude

$$(e_1, e_2, \cdots, e_t) = (K_1, K_2, \cdots, K_t) \frac{1}{|A_n|} \overline{X}^{\mathrm{T}} C,$$

where $\overline{X}$ is the complex conjugate matrix of X and X is the character table of A_n, which is viewed as a matrix; the superscript T denotes transpose; and C is a diagonal matrix whose diagonal entries are all degrees $\chi_i(1)$ of irreducible characters χ_i of A_n. By the proof of Theorem 2.18 of [8], we know $|A_n| I = XD\overline{X}^{\mathrm{T}}$, where I is the identity matrix, D is a diagonal matrix whose diagonal entries are the sizes $|\mathcal{K}_i|$ of conjugacy classes $\mathcal{K}_i$ of A_n, thus $(\overline{X}^{\mathrm{T}})^{-1} = \frac{1}{|A_n|} XD$. We may deduce

$$(K_1, K_2, \cdots, K_t) = (e_1, e_2, \cdots, e_t) C^{-1} XD$$

and so

$$(s_1, s_2, \cdots, s_r) = (e_1, e_2, \cdots, e_t) C^{-1} XDA_{tr}$$

We may further derive

$$(s_1, s_2, \cdots, s_r) = (e_1, e_2, \cdots, e_t) M_{tr},$$

$$M_{tr} = \begin{pmatrix} \frac{\chi_1(s_1)}{\chi_1(1)} & \frac{\chi_1(s_2)}{\chi_1(1)} & \cdots & \frac{\chi_1(s_r)}{\chi_1(1)} \\ \frac{\chi_2(s_1)}{\chi_2(1)} & \frac{\chi_2(s_2)}{\chi_2(1)} & \cdots & \frac{\chi_2(s_r)}{\chi_2(1)} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\chi_t(s_1)}{\chi_t(1)} & \frac{\chi_t(s_2)}{\chi_t(1)} & \cdots & \frac{\chi_t(s_r)}{\chi_t(1)} \end{pmatrix}.$$

Theorem 3.7 of [8] implies the entries $\frac{\chi_i(s_j)}{\chi_i(1)}$ are algebraic integers. The $\chi_i's$ are all irreducible characters of A_n. Since the two sets of vectors are linearly independent respectively, it follows that the rank $R(M_{rt})$ of M_{rt} is equal to *r*.

Using character theory, we may also extract some more specific information regarding elements of order *pq* in *G*. For examples, if there exists an irreducible character of *G* which is neither *p*-rational nor *q*-rational, then *G* has *pq*-elements, which is a variation of Lemma 14.2 of [8].

Proof of Theorem A. Follows from Theorem 2.2, Corollary 2.3, Theorem 2.13, Corollary 3.2, Theorem 3.6 and Theorem 4.1.

Proof of Theorem B. Follows from Theorems 2.8 and 2.10.

Acknowledgements

This work was supported by National Natural Science Foundation of China (Grant No.12171058). The first author wishes to thank Prof. J. X. Bi for many helpful conversations on element order sets of finite simple groups and almost simple groups, especially on A_n and S_n for $n \geq 5$.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Goldbach's Conjecture. https://en.wikipedia.org/wiki/Goldbach

[2] Li, K. (2022) A New Method to Study Goldbach Conjecture. *Applied Mathematics*, **13**, 68-76. https://doi.org/10.4236/am.2022.131006

[3] Isaacs, I.M. (1994) Algebra: A Graduate Textbook. Brooks/Cole, Pacific Grove.

[4] Lucido, M.S. (1999) Prime Graph Components of Finite Almost Simple Groups. *Rendiconti del Seminario Matematico della Università di Padova*, **102**, 1-22. (Addendum, 2002, **107**, 89-90).

[5] Williams, J.S. (1981) Prime Graph Components of Finite Groups. *Journal of Algebra*, **69**, 487-513. https://doi.org/10.1016/0021-8693(81)90218-0

[6] (2012) GAP-Groups Algorithms, and Programming, Version 4.5. https://www.gap-system.org

[7] Gorshkov, I.B. (2013) Recognizability by Spectrum of Alternating Groups. *Algebra and Logic*, **52**, 41-46. https://doi.org/10.1007/s10469-013-9217-x

[8] Isaacs, I.M. (1976) Character Theory of Finite Groups. Academic Press, New York.

[9] Kurzweil, H. and Stellmacher, B (2004) The Theory of Finite Groups: An Introduction. Springer-Verlag, New York. https://doi.org/10.1007/b97433

[10] Lewis, M. (2008) An Overview of Graphs Associated with Character Degrees and Conjugacy Class Sizes in Finite Groups. *Rocky Mountain Journal of Mathematics*, **38**, 175-211. https://doi.org/10.1216/RMJ-2008-38-1-175

[11] Vasil'e, A.V. and Vdovin, E.P. (2005) An Adjacency Criterion for the Prime Graph of a Finite Simple Group. *Algebra and Logic*, **44**, 381-406. https://doi.org/10.1007/s10469-005-0037-5

[12] Miller, W. (1987) The Maximum Order of an Element of a Finite Symmetric Group. *The American Mathematical Monthly*, **94**, 497-506. https://doi.org/10.1080/00029890.1987.12000673

[13] Cohen, H. (2007) Number Theory Volume II: Analytic and Modern Tools. Springer-Verlag, New York.

[14] Rosser, J.S. and Schoenfeld, L. (1962) Approximate Formulas for Some Functions of Prime Numbers. *Illinois Journal of Mathematics*, **6**, 64-94. https://doi.org/10.1215/ijm/1255631807

[15] Higman, G. (1957) Finite Groups in Which Every Element Has Prime Power Order. *Journal of the London Mathematical Society*, **s1-32**, 321-334. https://doi.org/10.1112/jlms/s1-32.3.321

[16] Bi, J.X. (2001) Characterization of Alternating Groups by Orders of Normalizers of Sylow Subgroups. *Algebra Colloquium*, **8**, 13-15.

Appendix. GAP Command Codes

The following GAP function is applied to computing the element order set of A_n.

```
jsqa:=function(n)
 local Al, ccreps, L, S;
 Al:=ConjugacyClasses(AlternatingGroup(n))
 ccreps:=List(Al, Representative);
 L:=List(ccreps, Order);
 S:=Set(L);
 return S;
 end;
```

The following GAP command codes are used to compute $\left|\mathcal{E}\left(A_i\right)-\mathcal{E}\left(A_{i-1}\right)\right|$ when $5 \le i \le 60$.

```
> for i in [5..60] do
>  g := Difference(jsqa(i),jsqa(i-1));
>  for x in g do
>   ord := x;
>   n := FactorsInt(ord);
>   s := Size(n);
>   if s = 2 then
>   if n[1] <> n[2] then
>  Print(ord,":");
>  fi;fi;od;
>  Print( "::","\n");
>  od;
```