POLYNOMIALS WHOSE REDUCIBILITY IS RELATED TO THE GOLDBACH CONJECTURE

PETER BORWEIN, KWOK-KWONG STEPHEN CHOI, AND CHARLES L. SAMUELS

Abstract. We introduce a collection of polynomials F_N, associated to each positive integer N, whose divisibility properties yield a reformulation of the Goldbach conjecture. While this reformulation certainly does not lead to a resolution of the conjecture, it does suggest two natural generalizations for which we provide some numerical evidence. As these polynomials F_N are independently interesting, we further explore their basic properties, giving, among other things, asymptotic estimates on the growth of their coefficients.

1. Introduction

Let $\mathcal{P}$ denote the set of odd primes. One of the oldest unsolved problems in mathematics concerns the set $\mathcal{P}+\mathcal{P}=\{p+q : p,q\in\mathcal{P}\}$.

Conjecture 1.1 (Goldbach Conjecture)**.** If $N>4$ is an even integer, then $N\in\mathcal{P}+\mathcal{P}$.

If N is any positive integer, we say that the *Goldbach conjecture holds for* N if $N\in\mathcal{P}+\mathcal{P}$. Otherwise, we say the *the Goldbach conjecture fails for* N. Of course, we make no attempt here to prove the Goldbach Conjecture, however we wish to study a related collection of polynomials. In order to construct these polynomials, we let $\chi_{\mathcal{P}}:\mathbb{N}\to\{0,1\}$ denote the indicator function of $\mathcal{P}$. That is,

$$\chi_{\mathcal{P}}(n)=\begin{cases}1 & \text{if } n \text{ is an odd prime,}\\ 0 & \text{otherwise.}\end{cases}$$

Furthermore, for each positive integer N, we define

$$R(N)=\sum_{n=1}^{N-1}\chi_{\mathcal{P}}(n)\chi_{\mathcal{P}}(N-n)$$

so that $R(N)$ counts the number of ways to write N as a sum of two odd primes. We note that $R(N)=0$ if and only if $N\notin\mathcal{P}+\mathcal{P}$. To each positive integer N, we associate a polynomial $F_N\in\mathbb{Z}[x]$ given by

$$F_N(z)=\sum_{k=0}^{N-1}\left(\sum_{n=1}^{N-1}\chi_{\mathcal{P}}(n)z^{kn}\right)^2.$$

Our first result discusses the divisibility properties of F_N for each N and connects F_N to the Goldbach conjecture. We write Φ_N to denote the Nth cyclotomic polynomial.

Theorem 1.2. *If N is a positive integer then the following conditions hold.*

Date: May 7, 2010.
Research of all authors is supported by NSERC of Canada.

(i) Φ_{2N} *divides* F_N*.*
(ii) Φ_N *divides* F_N *if and only if the Goldbach conjecture fails for* N*.*

The second statement of Theorem 1.2 is closely related to the Goldbach conjecture and yields two immediate consequences.

Corollary 1.3. *Suppose* $N > 4$ *is an integer.*
(i) If N *is odd then* Φ_N *divides* F_N*.*
(ii) If F_N/Φ_{2N} *is irreducible then the Goldbach conjecture holds for* N*.*

Early numerical evidence seems to suggest that F_N/Φ_{2N} is, in fact, irreducible for all even integers $N > 4$. If this is the case, then the Goldbach conjecture would follow. Similarly, it appears that, for odd integers $N > 5$, we have that $F_N/(\Phi_N\Phi_{2N})$ is irreducible. Although this is not relevant to the Goldbach conjecture, we find it independently interesting.

Conjecture 1.4. If $N > 5$ is an integer then the following conditions hold.
(i) If N is even, then
$$\frac{F_N}{\Phi_{2N}}$$
is irreducible.
(ii) If N is odd, then
$$\frac{F_N}{\Phi_{2N}\Phi_N}$$
is irreducible.

As we have noted, Conjecture 1.4 (i) would imply the Goldbach conjecture. However, the converse is possibly false. Indeed, F_N/Φ_{2N} could be reducible but still not divisible by Φ_N. As such, we should view Conjecture 1.4 as being significantly harder than the Goldbach conjecture, and therefore, not likely within reach using current techniques. Nonetheless, we find it interesting to see the Goldbach conjecture in this context.

As evidence in favor of Conjecture 1.4, we have found that it holds for all $N \le 50$. For even N, the first few polynomials F_N/Φ_N are given in the following list.

$$\begin{aligned}
F_6/\Phi_{12} = {} & z^{46} + z^{44} - z^{40} - z^{38} + 3\,z^{36} + 4\,z^{34} + z^{32} - 3\,z^{30} - 2\,z^{28} + 3\,z^{26} \\
& + 5\,z^{24} + 2\,z^{22} - 2\,z^{18} - z^{16} + 2\,z^{14} + 5\,z^{12} + 3\,z^{10} - z^{8} - 3\,z^{6} + 4\,z^{2} + 4 \\
F_8/\Phi_{16} = {} & z^{90} - z^{82} + 3\,z^{76} + z^{74} - 3\,z^{68} - z^{66} + 2\,z^{64} + 4\,z^{62} + 3\,z^{60} + z^{58} \\
& - 2\,z^{56} - 4\,z^{54} + 2\,z^{52} - z^{50} + 5\,z^{48} + 4\,z^{46} - 2\,z^{44} + 4\,z^{42} - z^{40} \\
& - 4\,z^{38} + 2\,z^{36} - 2\,z^{34} + 6\,z^{32} + 4\,z^{30} + z^{28} + 2\,z^{26} - 4\,z^{24} - 2\,z^{18} \\
& + 9\,z^{16} + 3\,z^{12} + 3\,z^{10} - 7\,z^{8} + z^{6} + 9 \\
F_{10}/\Phi_{20} = {} & z^{118} + z^{116} - z^{108} - z^{106} + z^{104} + z^{102} + 2\,z^{100} + 3\,z^{98} + z^{96} - z^{94} \\
& - z^{92} - z^{90} + z^{86} + z^{84} + 4\,z^{82} + 4\,z^{80} + 2\,z^{76} + 2\,z^{74} - z^{72} - z^{70} \\
& - 2\,z^{66} + 2\,z^{64} + 9\,z^{62} + 5\,z^{60} + 4\,z^{56} - 4\,z^{52} + 3\,z^{48} + z^{44} + 7\,z^{42} + 8\,z^{40} \\
& + 2\,z^{38} + z^{34} - 3\,z^{30} + z^{28} + 3\,z^{26} + z^{24} + 6\,z^{22} + 8\,z^{20} + 2\,z^{16} \\
& + 4\,z^{14} - 3\,z^{12} - 4\,z^{10} + 3\,z^{8} + z^{6} + 9\,z^{2} + 9.
\end{aligned}$$

Now we give the analogous list but for odd N.

$$\begin{aligned} F_7/(\Phi_7\Phi_{14}) &= z^{48} - z^{46} + z^{38} + z^{36} - z^{34} - z^{32} + 3\,z^{28} - 3\,z^{26} + 2\,z^{24} \\ &\quad + z^{20} - z^{18} - 2\,z^{16} + 3\,z^{14} - z^{10} + z^8 + z^6 - 4\,z^2 + 4 \\ F_9/(\Phi_9\Phi_{18}) &= z^{100} - z^{94} + z^{86} + 2\,z^{84} + z^{82} - z^{80} - 2\,z^{78} - z^{76} + 3\,z^{72} \\ &\quad + 4\,z^{68} - z^{66} + z^{64} - 4\,z^{62} + 3\,z^{58} + z^{54} - 2\,z^{52} + 4\,z^{50} + 4\,z^{48} \\ &\quad - z^{46} - z^{44} - 5\,z^{42} + 3\,z^{40} + 6\,z^{36} - 2\,z^{34} + z^{32} + z^{30} + 4\,z^{28} \\ &\quad - z^{26} - 4\,z^{24} - 2\,z^{22} + 2\,z^{20} + 7\,z^{18} - z^{16} - z^{14} + 2\,z^{12} + 3\,z^{10} \\ &\quad + 2\,z^8 - 8\,z^6 + 9 \\ F_{11}/(\Phi_{11}\Phi_{22}) &= z^{120} - z^{118} + z^{106} - z^{104} + 2\,z^{100} - z^{98} - z^{96} + z^{92} - z^{90} \\ &\quad + 2\,z^{88} - 2\,z^{86} + z^{84} - z^{82} + 3\,z^{80} - 3\,z^{74} + 4\,z^{70} - 4\,z^{68} + 2\,z^{66} \\ &\quad + z^{64} - 2\,z^{62} + 4\,z^{60} - 2\,z^{58} + z^{52} - 4\,z^{46} + 4\,z^{44} - z^{42} + 4\,z^{40} \\ &\quad - 2\,z^{38} + z^{36} - 2\,z^{34} - z^{32} + 4\,z^{30} + 2\,z^{28} - 5\,z^{26} - 4\,z^{24} + 6\,z^{22} \\ &\quad + 2\,z^{20} - z^{18} + z^{16} - 2\,z^{14} + z^{10} + z^8 + z^6 - 9\,z^2 + 9. \end{aligned}$$

Indeed, we have found that the right hand sides on the above lists are all irreducible over $\mathbb{Z}$.

Because of their relevance to the Goldbach conjecture, it may also be interesting to study the number of roots of F_N that lie on the unit circle. In view of Theorem 1.2 (i), it is clear that F_N has at least $\varphi(2N)$ such roots. For even integers $N > 4$, if F_N has no other roots on the unit circle, then the Goldbach conjecture would follow from Theorem 1.2 (ii). Our numerical evidence suggests this to be the case. Furthermore, when N is odd, we know that F_N must, in fact, have at least $\varphi(2N)+\varphi(N)$ roots on the unit circle. Again, our evidence suggests that there are no others. Also, the identity

$$\varphi(2N) = \begin{cases} 2\varphi(N) & \text{if } N \text{ is even} \\ \varphi(N) & \text{if } N \text{ is odd.} \end{cases}$$

holds for all positive integers N. So we pose the following strengthening of the Goldbach conjecture.

Conjecture 1.5. If $N > 5$ is an integer then F_N has precisely $2\varphi(N)$ roots on the unit circle.

Similar to our note above, the converse of Conjecture 1.5 is not necessarily true. F_N could have many roots on the unit circle while still not being divisible by Φ_N. Once again, this conjecture should be regarded as more difficult than the Goldbach conjecture.

We have computed the number of roots of F_N on the unit circle for $N \le 50$ and have found that Conjecture 1.5 holds for those F_N. This complete list is given in Table 1 including the number of roots inside, on and outside the unit circle for each F_N.

It is worth noting that, in our construction of F_N, the set of odd primes may be replaced with any subset of $\mathbb{N}$. In this way, one may attempt to prove theorems analogous to those stated above. One such example, which is of particular interest in number theory, arises in the following way.

TABLE 1. Location of roots of F_N

N	$2\varphi(N)$	$[\lvert z\rvert < 1 \quad \lvert z\rvert = 1 \quad \lvert z\rvert > 1]$
6	4	[16 4 30]
7	12	[4 12 44]
8	8	[24 8 66]
9	12	[8 12 92]
10	8	[16 8 102]
11	20	[16 20 104]
12	8	[48 8 186]
13	24	[40 24 200]
14	12	[40 12 286]
15	16	[40 16 308]
16	16	[36 16 338]
17	32	[36 32 348]
18	12	[56 12 510]
19	36	[40 36 536]
20	16	[80 16 626]
21	24	[60 24 676]
22	20	[64 20 714]
23	44	[56 44 736]
24	16	[92 16 950]
25	40	[84 40 980]
26	24	[100 24 1026]
27	36	[108 36 1052]
28	24	[92 24 1126]
29	56	[100 56 1132]
30	16	[132 16 1534]
31	60	[128 60 1552]
32	32	[144 32 1746]
33	40	[136 40 1808]
34	32	[144 32 1870]
35	48	[160 48 1900]
36	24	[168 24 1978]
37	72	[136 72 2024]
38	36	[180 36 2522]
39	48	[172 48 2592]
40	32	[184 32 2670]
41	80	[176 80 2704]
42	24	[200 24 3138]
43	84	[184 84 3176]
44	40	[244 40 3414]
45	48	[252 48 3484]
46	44	[228 44 3598]
47	92	[244 92 3620]
48	32	[288 32 4098]
49	84	[260 84 4168]
50	40	[264 40 4302]

The Liouville function $\lambda : \mathbb{N} \to \{-1, 1\}$ is the completely mulitplicative function such that $\lambda(p) = -1$ at every prime p. Now define the set

$$\mathcal{L} = \{n \in \mathbb{N} : \lambda(n) = -1\}.$$

It is a direction of our future research to examine the analogs of F_N that are obtained by using the above contruction with $\mathcal{L}$ in place of $\mathcal{P}$. Perhaps this strategy can yield a proof that every positive even integer $N > 2$ satisfies $N \in \mathcal{L} + \mathcal{L}$. On the surface, such a result appears to be easier than the Goldbach conjecture, and therefore, is possibly within reach.

One can also consider weighted forms of F_N. Similar to the study of the prime number theorem, instead of using the above indicator function of $\mathcal{P}$, we use the weighted form

$$\widetilde{\chi}_{\mathcal{P}}(n) = \begin{cases} \log n & \text{if } n \in \mathcal{P}, \\ 0 & \text{otherwise} \end{cases}$$

and define the corresponding polynomials $\widetilde{F}_N$ by

$$\widetilde{F}_N(z) = \sum_{k=0}^{N-1} \left(\sum_{n=1}^{N-1} \widetilde{\chi}_{\mathcal{P}}(n) z^{kn} \right)^2.$$

It is clear that $\widetilde{F}_N(z)$ do not have integer coefficients, so we might expect different types of results regarding these polynomials. Nonetheless, we believe they yield another interesting route for future research.

2. Properties of the polynomials F_N

Now that we understand the relevance of the polynomials F_N to the Goldbach conjecture, we consider some of their additional properties. We begin with the following result regarding their symmetry.

Theorem 2.1. *If N is a positive integer then $F_N(z) = F_N(-z)$.*

Theorem 2.1 certainly implies that if $\Phi_N(z)$ divides $F_N(z)$ then so does $\Phi_N(-z)$. Furthermore, we know that if M is an odd integer then $\Phi_{2M}(z) = \Phi_M(-z)$. Combining these observations with Theorem 1.2 (ii), we obtain the following corollary.

Corollary 2.2. *If M is an odd integer and $N = 2M$ then the following conditions are equivalent.*

(i) Φ_N divides F_N.
(ii) Φ_M divides F_N.
(iii) The Goldbach conjecture fails for N.

Suppose now that, for any positive integer M, ζ_M is a primitive Mth root of unity. We may view Corollary 2.2 as examining the value of $F_N(\zeta_M)$ when M is a certain divisor of N. Next, we consider the values of $F_N(\zeta_M)$ when M is an arbitrary divisor of M. We write $[x]$ to denote the largest integer less than or equal to x.

Theorem 2.3. *If $N > 4$ is an integer and $M \mid N$ then the following conditions hold.*

(i) If M is odd then

$$F_N(\zeta_M) \geq N \sum_{n=1}^{[N/2M]} R(2nM).$$

(ii) If M is even then

$$F_N(\zeta_M) \geq N \sum_{n=1}^{N/M} R(nM).$$

Applying Theorems 2.3 and 1.2 (ii) immediately yield the following simpler lower bound on $F_N(\zeta_M)$.

Corollary 2.4. *If $N > 4$ is an integer and $M \mid N$, then $F_N(\zeta_M) \geq NR(N)$ with equality when $M = N$.*

The case $M = N$ may not be the only case of equality in Corollary 2.4. In fact, if M is odd and $N = 2M$, then it can be shown that $F_N(\zeta_M) = NR(N)$ as well. This result also provides a strengthening of one direction of Theorem 1.2 (ii). If Φ_M ever divides F_N, then it follows from Corollary 2.4 that $R(N) = 0$. In other words, we have established the following statement.

Corollary 2.5. *Suppose $N > 4$ is an integer and $M \mid N$. If Φ_M divides F_N then the Goldbach conjecture fails for N.*

The converse of Corollary (2.5) is certainly false. Otherwise, Φ_1 would divide F_N for every odd N, and it certainly does not. When restricted to even integers, it is likely true, but only because the Goldbach conjecture would imply that the hypothesis is always false. In fact, in view of Theorem 1.2, such a statement is equivalent to the Goldbach conjecture.

3. The coefficients of F_N

Let us now turn our attention to understanding the coefficients of F_N. For this purpose, we note that $\deg F_N \leq 2(N-1)^2$ and write

$$F_N(z) = \sum_{m=0}^{2(N-1)^2} a_{N,m} z^m.$$

It is easy to see that the constant term in F_N is given by the formula

$$a_{N,0} = \left(\sum_{n=1}^{N-1} \chi_{\mathcal{P}}(n) \right)^2 = (\pi(N-1)-1)^2$$

where $\pi(N-1)$ denotes the number of primes $p \leq N-1$. Furthermore, by multiplying out the terms in the definition of F_N, we obtain an explicit formula for all other coefficients of F_N.

Theorem 3.1. *Let N be a positive integer. We have that*

$$a_{N,m} = \sum_{d \mid m} \sum_{n=\max\{0,d-N\}+1}^{\min\{N,d\}-1} \chi_{\mathcal{P}}(n)\chi_{\mathcal{P}}(d-n)$$

for all $0 < m \leq 2(N-1)^2$.

Among other things, Theorem 3.1 shows that

$$a_{N,m} \leq \sum_{d|m} R(d)$$

with equality whenever $0 < m \leq N$. We can rephrase the case of equality by saying that

$$a_{N,m} = \sum_{d|m} \sum_{n=1}^{d-1} \chi_{\mathcal{P}}(n)\chi_{\mathcal{P}}(d-n) \tag{3.1}$$

whenever $0 < m \leq N$. If M is another integer with $M \geq N$, then $a_{M,m} = a_{N,m}$ for all m satisfying $0 < m \leq N$. For simplicity, we may now write

$$a(m) = a_{N,m}$$

where $N \geq m$. If m is odd, then all divisors of m are also odd, so we conclude that $a(m) = 0$. Hence, it is only interesting to consider the situation where m is even, in which case the coefficients seem to behave in a rather subtle way. However, we can obtain lower bounds in relation to other famous arithmetic functions. Before proceeding, we recall that $\omega(n)$ denotes the number of distinct prime factors of n and $d(n)$ denotes the number of divisors of n.

Theorem 3.2. *If $m > 1$ is an integer then*

$$a(2m) \geq \omega(m) - \begin{cases} 1 & \text{if } m \equiv 2 \bmod 4, \\ 0 & \text{otherwise.} \end{cases} \tag{3.2}$$

Moreover, if the Goldbach conjecture is true, then

$$a(2m) \geq d(m) - \begin{cases} 2 & \text{if } m \text{ is even,} \\ 1 & \text{otherwise.} \end{cases} \tag{3.3}$$

We note that the right hand side of (3.2) is always positive for $m > 2$. So taking an integer $n > 4$, we have that $a(n) = 0$ if and only if n is odd. It is also worth observing that the right hand sides of (3.2) and (3.3) are sometimes equal, namely when m is prime. In general, however, $d(m)$ is much larger than $\omega(m)$ so that our bound under the Goldbach conjecture is stronger than the analogous unconditional bound.

For a positive integer M, it is also of interest to study the summatory function

$$A(M) = \sum_{m=1}^{2M} a(m).$$

As a consequence of Theorem 3.2, we are able to give both conditional and unconditional lower bounds on $A(M)$. Before stating the corollary, we recall that the Euler-Mascheroni constant γ is given by

$$\gamma = \lim_{N\to\infty} \left(\sum_{n=1}^{N} \frac{1}{n} - \log n \right) = 0.5772\ldots$$

and Mertens' constant is defined by

$$B_1 = \lim_{N\to\infty} \left(\sum_{p\leq N} \frac{1}{p} - \log\log N \right) = 0.2615\ldots$$

where the sum is taken over primes $p \leq N$.

Corollary 3.3. *There exist a constant c_1 such that*

$$A(M) \geq M \log\log M + \left(B_1 - \frac{1}{4}\right) M + c_1 \frac{M}{\log M} \tag{3.4}$$

for all sufficiently large integers M. If the Goldbach conjecture holds, then there exists a constant c_2 such that

$$A(M) \geq M \log M + \left(2\gamma - \frac{5}{2}\right) M + c_2 M^{\frac{131}{416}} \tag{3.5}$$

for all sufficiently large integers M.

The proof of the first statement of Theorem 3.2 uses the fact that $R(2p) > 0$ whenever p is an odd prime. Indeed, We always have that $2p = p + p$, so we obtain a positive lower bound on $R(2d)$ whenever d is an odd prime divisor of m. While the inequality (3.4) takes advantage of this fact, it uses only the trivial bound $R(2d) \geq 0$ in all other cases.

However, it is well-known that the set of positive integers m with $R(2m) = 0$ must have density zero in the even integers. In fact, Montgomery and Vaughan [6] gave a stronger result. They showed that each inteval $[1, x)$ may contain at most $O(x^{1-\delta})$ integers m with $R(2m) = 0$, where $1 > \delta > 0$. Using this fact, we are able to produce a somewhat deeper result improving the unconditional lower bound of Corollary 3.3. While the following statement is certainly an improvement over (3.4), the previous one is still worthwhile because of the relative simplicity of its proof.

Theorem 3.4. *There exists a real number C such that*

$$A(M) \geq M \log M + CM$$

for all sufficiently large M.

Note that the main term in Theorem 3.4 is the same as that of (3.5), an inequality for which we needed to assume the Goldbach conjecture. The only difference lies in the constant in front of the error term.

Generally speaking, our proof takes advantage of the fact that $R(2m) > 0$ for 'most' positive integers m. However, there is reason to believe that $R(2m)$ is not only positive, but quite large most of the time. Using the circle method to study the Goldbach's problem, Hardy and Littlewood [3] conjectured an asymptotic formula. For this purpose, we define the twin primes constant

$$C_2 = \prod_{p>2} \left(1 - \frac{1}{p-2}\right)$$

and state the following conjecture.

Conjecture 3.5 (Hardy and Littlewood)**.** We have that

$$R(2n) \sim 2C_2 \frac{n}{\log^2 n} \prod_{\substack{p \mid n \\ p>2}} \frac{p-1}{p-2}$$

as n tends to infinity.

We now obtain the following conditional results regarding $a(2m)$ and $A(M)$. We write $p^\ell \| m$ if p^ℓ divides m but $p^{\ell+1}$ does not.

Theorem 3.6. *If Conjecture 3.5 holds then*

$$\frac{4C_2 m}{\log^2 m} \lesssim a(2m) \lesssim \frac{8C_2 m}{\log^2 m} \prod_{p^l \| m} \frac{p - 2/p^l}{p-2} \tag{3.6}$$

and

$$A(M) \sim \frac{4\pi^2 C_2 M^2}{3 \log^2 M}. \tag{3.7}$$

4. Proofs of the results from section 1

Proof of Theorem 1.2. To prove (i), we must show that $F_N(e^{\pi i/N}) = 0$. To see this, note that

$$\begin{aligned} F_N(e^{\pi i/N}) &= \sum_{k=0}^{N-1} \left(\sum_{n=1}^{N-1} \chi_{\mathcal{P}}(n) e^{\frac{\pi i k n}{N}} \right)^2 \\ &= \sum_{k=0}^{N-1} \sum_{m=1}^{N-1} \sum_{n=1}^{N-1} \chi_{\mathcal{P}}(m)\chi_{\mathcal{P}}(n) e^{\frac{\pi i k(m+n)}{N}} \\ &= \sum_{m=1}^{N-1} \sum_{n=1}^{N-1} \chi_{\mathcal{P}}(m)\chi_{\mathcal{P}}(n) \sum_{k=0}^{N-1} e^{\frac{\pi i k(m+n)}{N}}. \end{aligned}$$

The product $\chi_{\mathcal{P}}(m)\chi_{\mathcal{P}}(n) = 0$ unless m and n are both odd primes. In this case, we certainly have that $m+n$ is even so that

$$\sum_{k=0}^{N-1} e^{\frac{\pi i k(m+n)}{N}} = \sum_{k=0}^{N-1} e^{\frac{2\pi i k((m+n)/2)}{N}}. \tag{4.1}$$

Of course, $0 < (m+n)/2 < N$ implying that the right hand side of (4.1) equals zero. In other words, we have shown that

$$\chi_{\mathcal{P}}(m)\chi_{\mathcal{P}}(n) \sum_{k=0}^{N-1} e^{\frac{\pi i k(m+n)}{N}} = 0$$

for all $1 \le m, n < N$, verifying (i).

To establish (ii), let ζ be a primitive Nth root of unity. We have immediately that

$$\begin{aligned} F_N(\zeta) &= \sum_{k=0}^{N-1} \left(\sum_{n=1}^{N-1} \tau(n) \zeta^{kn} \right)^2 \\ &= \sum_{k=0}^{N-1} \sum_{m=1}^{N-1} \sum_{n=1}^{N-1} \chi_{\mathcal{P}}(m)\chi_{\mathcal{P}}(n) \zeta^{k(m+n)} \\ &= \sum_{m=1}^{N-1} \sum_{n=1}^{N-1} \chi_{\mathcal{P}}(m)\chi_{\mathcal{P}}(n) \sum_{k=0}^{N-1} \zeta^{k(m+n)}. \end{aligned}$$

We know that

$$\sum_{k=0}^{N-1} \zeta^{k(m+n)} = 0$$

unless $m+n \equiv 0 \mod N$. In our case, this may occur only when $m+n=N$, implying that

$$F_N(\zeta) = \sum_{n=1}^{N-1} \chi_{\mathcal{P}}(n)\chi_{\mathcal{P}}(N-n) \sum_{k=0}^{N-1} \zeta^{kN} = NR(N).$$

If $R(N)=0$ then $F_N(\zeta)=0$ showing that Φ_N must divide F_N. On the other hand, if Φ_N divides F_N, it is obvious that $F_N(\zeta)=0$ so that $R(N)=0$. □

Let us now proceed with the proof of Corollary 1.3.

Proof of Corollary 1.3. To prove (i), it is clear that, if N is odd, , we cannot write N as a sum of two odd primes. It follows from Theorem 1.2 (ii) that Φ_N divides F_N.

To establish (ii), we note that the constant term in F_N is given by

$$\left(\sum_{n=1}^{N-1} \chi_{\mathcal{P}}(n)\right)^2,$$

which is at least 4 whenever $N \geq 6$. This means that F_N/Φ_{2N} cannot be equal to Φ_N. Therefore, if it is irreducible, then it cannot be divisible by Φ_N and it follows from Theorem 1.2 (i) that $N \in \mathcal{P}+\mathcal{P}$. □

5. Proofs of the results from section 2

Proof of Theorem 2.1. It follows directly from the definition that

$$F_N(-z) = \sum_{k=0}^{N-1} \left(\sum_{n=1}^{N-1} (-1)^{kn} \chi_{\mathcal{P}}(n) z^{kn}\right)^2. \tag{5.1}$$

If n is even, we certainly have that $\chi_{\mathcal{P}}(n)=0$. Otherwise, we have that $(-1)^n=-1$, which implies that $(-1)^{kn}\chi_{\mathcal{P}}(n) = (-1)^k\chi_{\mathcal{P}}(n)$ for all n. Using (5.1), we find that

$$F_N(-z) = \sum_{k=0}^{N-1} \left((-1)^k \sum_{n=1}^{N-1} \chi_{\mathcal{P}}(n) z^{kn}\right)^2 = \sum_{k=0}^{N-1} \left(\sum_{n=1}^{N-1} \chi_{\mathcal{P}}(n) z^{kn}\right)^2 = F_N(z)$$

which completes the proof. □

In view of Theorem 2.1, we obtain our proof of Corollary 2.2 almost immediately.

Proof of Corollary 2.2. In view of Theorem 1.2, we immediately have that (i) if and only if (iii). To finish the proof, we will show that (i) if and only if (ii). To see this, note that since M is odd, we have that $\Phi_N(z) = \Phi_M(-z)$. Furthermore, Theorem 2.1 implies that $\Phi_N(z)$ divides $F_N(z)$ if and only if $\Phi_N(-z)$ divides F_N and the result follows. □

Proof of Theorem 2.3. Suppose that $a=1$ if M is odd and $a=0$ if M is even. We must show that

$$F_N(\zeta_M) \geq N \sum_{1 \leq k \leq N/(2^a M)} R(2^a kM).$$

From the definition of F_N, we have that

$$\begin{aligned}F_N(\zeta_M) &= \sum_{k=0}^{N-1} \sum_{2<p_1,p_2\le N-1} \zeta_M^{k(p_1+p_2)}\\ &= \sum_{2<p_1,p_2\le N-1} \sum_{i=0}^{N/M-1} \sum_{k=0}^{M-1} \zeta_M^{(iM+k)(p_1+p_2)}\\ &= \frac{N}{M} \sum_{2<p_1,p_2\le N-1} \sum_{k=0}^{M-1} \zeta_M^{k(p_1+p_2)}.\end{aligned}$$

Now the inner summation over k is zero unless $(p_1+p_2)/M \in \mathbb{Z}$. Hence we have

$$\begin{aligned}F_N(\zeta_M) &= N \sum_{1\le \ell\le 2(N-1)/M} \sum_{\substack{2<p_1,p_2\le N-1\\ p_1+p_2=\ell M}} 1\\ &= N \left\{ \sum_{1\le\ell\le N/M} + \sum_{N/M+1\le\ell\le 2(N-1)/M} \right\} \sum_{\substack{2<p_1,p_2\le N-1\\ p_1+p_2=\ell M}} 1\\ &= N \sum_{1\le\ell\le N/(2^a M)} R(2^a \ell M) + N \sum_{N/M+1\le\ell\le 2(N-1)/M} \sum_{\substack{2<p_1,p_2\le N-1\\ p_1+p_2=\ell M}} 1\\ &\ge N \sum_{1\le\ell\le N/(2^a M)} R(2^a\ell M).\end{aligned}$$

and the result follows. □

Proof of Corollary 2.4. If M is even, we have that

$$F_N(\zeta_M) \ge N \sum_{n=1}^{N/M} R(nM) \ge NR\left(\frac{N}{M}\cdot M\right) = NR(N).$$

If M is odd and N is even, then $N/2M \in \mathbb{N}$ so it follows that

$$F_N(\zeta_M) \ge N \sum_{n=1}^{N/2M} R(2nM) \ge NR\left(2\cdot\frac{N}{2M}\cdot M\right) = NR(N).$$

Finally, if M and N are both odd, then $NR(N) = 0$ so that

$$F_N(\zeta_M) \ge N \sum_{n=1}^{[N/2M]} R(2nM) \ge 0 = NR(N).$$

□

Proof of Corollary 2.5. If $\Phi_M \mid F_N$ then we have that $F_N(\zeta_M) = 0$. It follows from Corollary 2.4 that $R(N) = 0$. □

6. Proofs of the results from section 3

Proof of Theorem 3.1. We first note that

$$\begin{aligned}
F_N(z) &= \sum_{k=0}^{N-1}\left(\sum_{n=1}^{N-1}\chi_{\mathcal{P}}(n)z^{kn}\right)^2 \\
&= \sum_{k=0}^{N-1}\sum_{m=1}^{N-1}\sum_{n=1}^{N-1}\chi_{\mathcal{P}}(m)\chi_{\mathcal{P}}(n)z^{k(m+n)} \\
&= \sum_{m=0}^{2(N-1)^2}\left(\sum_{d|m}\sum_{\substack{n_1+n_2=d\\ 1\le n_1,n_2<N}}\chi_{\mathcal{P}}(n_1)\chi_{\mathcal{P}}(n_2)\right)z^m \\
&= \sum_{m=0}^{2(N-1)^2}\left(\sum_{d|m}\sum_{n=\max\{0,d-N\}+1}^{\min\{N,d\}-1}\chi_{\mathcal{P}}(n)p(d-n)\right)z^m
\end{aligned}$$

establishing the theorem. □

Proof of Theorem 3.2. Using (3.1), we have immediately that

$$a(2m) = \sum_{d|2m}\sum_{n=1}^{d-1}\chi_{\mathcal{P}}(n)\chi_{\mathcal{P}}(d-n).$$

However, it is clear that

$$\sum_{n=1}^{d-1}\chi_{\mathcal{P}}(n)\chi_{\mathcal{P}}(d-n) = 0$$

whenever d is odd, which implies that

$$\begin{aligned}
a(2m) &= \sum_{\substack{d|2m\\ d\text{ even}}}\sum_{n=1}^{d-1}\chi_{\mathcal{P}}(n)\chi_{\mathcal{P}}(d-n) \\
&= \sum_{d|m}\sum_{n=1}^{2d-1}\chi_{\mathcal{P}}(n)\chi_{\mathcal{P}}(2d-n). \qquad (6.1)
\end{aligned}$$

We now use (6.1) to prove (3.2). If p is an odd prime, we have that $\chi_{\mathcal{P}}(p)\chi_{\mathcal{P}}(2p-p) = 1$ implying

$$\sum_{n=1}^{2p-1}\chi_{\mathcal{P}}(n)\chi_{\mathcal{P}}(2p-n) \ge 1. \qquad (6.2)$$

Now let $\omega_{\text{odd}}(m)$ denote the number of distinct odd prime divisors of m and consider three cases according to the residue class of m modulo 4.

(i) First assume that m is odd. In this case, we have that $\omega_{\text{odd}}(m) = \omega(m)$ and $m \not\equiv 2 \bmod 4$. The inequality (6.2) holds for every odd prime divisor or m. Combining this observation with (6.1), we find that

$$a(2m) \ge \omega_{\text{odd}}(m) = \omega(m)$$

completing the proof in this case.

(ii) Now assume that $m \equiv 0 \bmod 4$. It is easily verified that

$$\sum_{d|4} \sum_{n=1}^{7} \chi_{\mathcal{P}}(n)\chi_{\mathcal{P}}(8-n) = 1,$$

and then it follows from (6.1) and (6.2) that

$$a(2m) \geq \omega_{\text{odd}}(m) + 1.$$

Since 2 divides m, we have that $\omega_{\text{odd}}(m) = \omega(m) - 1$ establishing the result in this case.

(iii) Finally, we consider the case that $m \equiv 2 \bmod 4$. Again, m is even so that $\omega_{\text{odd}}(m) = \omega(m) - 1$, and we conclude from (6.1) and (6.2) that $a(2m) \geq \omega_{\text{odd}}(m)$. This completes the proof of (3.2).

To establish (3.3), we assume that the Goldbach Conjecture holds. Hence, we have that

$$\sum_{n=1}^{2d-1} \chi_{\mathcal{P}}(n)\chi_{\mathcal{P}}(2d-n) \geq 1 \tag{6.3}$$

for all divisors d of m with $d \notin \{1, 2\}$. Here we consider two cases.

(i) Suppose first that m is odd. Here, we have that (6.3) holds for all divisors d of m different than 1. This gives

$$\begin{aligned} a(2m) = \sum_{d|m} \sum_{n=1}^{2d-1} \chi_{\mathcal{P}}(n)\chi_{\mathcal{P}}(2d-n) &= \sum_{\substack{d|m \\ d\neq 1}} \sum_{n=1}^{2d-1} \chi_{\mathcal{P}}(n)\chi_{\mathcal{P}}(2d-n) \\ &\geq \sum_{\substack{d|m \\ d\neq 1}} 1 = d(m) - 1 \end{aligned}$$

completing the proof in this case.

(ii) In the case that m is even, we have that (6.3) holds except when $d = 1$ or $d = 2$. Therefore, we have that

$$\begin{aligned} a(2m) = \sum_{d|m} \sum_{n=1}^{2d-1} \chi_{\mathcal{P}}(n)\chi_{\mathcal{P}}(2d-n) &= \sum_{\substack{d|m \\ d\notin\{1,2\}}} \sum_{n=1}^{2d-1} \chi_{\mathcal{P}}(n)\chi_{\mathcal{P}}(2d-n) \\ &\geq \sum_{\substack{d|m \\ d\notin\{1,2\}}} 1 = d(m) - 2 \end{aligned}$$

which completes the proof in this case as well.

□

We are immediately prepared to give our proof of Corollary 3.3.

Proof of Corollary 3.3. Since $a(m) = 0$ whenever m is odd, we have that

$$A(M) = \sum_{n=1}^{2M} a(m) = \sum_{m=1}^{M} a(2m). \tag{6.4}$$

Applying the first statement of Theorem 3.2, we obtain that

$$A(M) \geq \sum_{m=1}^{M} \omega(m) - \sum_{m=1}^{M} g(m) \tag{6.5}$$

where

$$g(m) = \begin{cases} 1 & \text{if } m \equiv 2 \bmod 4 \\ 0 & \text{otherwise.} \end{cases}$$

Whenever $M \geq 3$, we have that

$$\sum_{m=1}^{M} g(m) = 1 + \sum_{m=3}^{M} g(m) \leq 1 + \frac{M-2}{4} = \frac{M}{4} + \frac{1}{2}$$

which, when combined with (6.5), yields

$$A(M) \geq \sum_{m=1}^{M} \omega(m) - \frac{M}{4} - \frac{1}{2} \tag{6.6}$$

for all $M \geq 3$. It is well-known (see [2], page 355) that

$$\sum_{m=1}^{M} \omega(m) = M \log\log M + B_1 M + O\left(\frac{M}{\log M}\right)$$

which implies the existence of a positive constant C and a positive integer $\mathcal{M}$ such that

$$\sum_{m=1}^{M} \omega(m) \geq M \log\log M + B_1 M - C\frac{M}{\log M}$$

holds for all $M \geq \mathcal{M}$. Combining this with (6.6), we find that

$$A(M) \geq M \log\log M + \left(B_1 - \frac{1}{4}\right) M - C\frac{M}{\log M} - \frac{1}{2}.$$

It is obvious that $M/\log M \geq 1/2$ for sufficiently large M. Thus, we find that

$$A(M) \geq M \log\log M + \left(B_1 - \frac{1}{4}\right) M - (C+1)\frac{M}{\log M}$$

for sufficiently large M and we complete the proof by taking $c_1 = -(C+1)$.

Now we proceed with our proof of the second statement assuming the Goldbach Conjecture. Using the second statement of Theorem 3.2 we get that

$$A(M) \geq \sum_{m=1}^{M} \left(d(m) - \begin{cases} 2 & \text{if } m \text{ is even} \\ 1 & \text{otherwise.} \end{cases} \right)$$

implying that

$$A(M) \geq \sum_{m=1}^{M} d(m) - \frac{3}{2}M. \tag{6.7}$$

Using the results of [4], we find that

$$\sum_{m=1}^{M} d(m) = M \log M + (2\gamma - 1)M + O(M^{\frac{131}{416}}).$$

In other words, there exists a positive constant C such that

$$\sum_{m=1}^{M} d(m) \geq M \log M + (2\gamma - 1)M - CM^{\frac{131}{416}}$$

For all sufficiently large M. Combining this with (6.7) and setting $c_2 = -C$, we find that

$$A(M) \geq M \log M + \left(2\gamma - \frac{5}{2}\right) M + c_2 M^{\frac{131}{416}}$$

for all sufficiently large integers M. □

Proof of Theorem 3.4. Write $E(X)$ to denote the number of even integers in $[1, 2X)$ for which the Goldbach conjecture fails. By the results of [6], there exist positive constants c and δ such that

$$E(X) \leq cX^{1-\delta}. \tag{6.8}$$

In view of the results of [5], one may take $\delta = 0.086$. Recently Pintz announced that $\delta = 1/3$ is admissible in (6.8).

In view of (6.4), we have that

$$A(M) = \sum_{m=1}^{M} \sum_{d|m} \sum_{n=1}^{2d-1} \chi_{\mathcal{P}}(n)\chi_{\mathcal{P}}(2d-n)$$

for all M. By interchanging the order of the summation over m and d, we get that

$$\begin{aligned} A(M) &= \sum_{d=1}^{M} \sum_{m \leq M/d} \sum_{n=1}^{2d-1} \chi_{\mathcal{P}}(n)\chi_{\mathcal{P}}(2m-n) \\ &= \sum_{d=1}^{M} \left[\frac{M}{d}\right] R(2d). \end{aligned}$$

Relabelling the indices, we have shown that

$$A(M) = \sum_{m=1}^{M} \left[\frac{M}{m}\right] R(2m).$$

and it follows that

$$A(M) \geq \sum_{k=1}^{[\log_2 M]} \sum_{m=2^{k-1}}^{2^k - 1} \left[\frac{M}{m}\right] R(2m) \tag{6.9}$$

for all positive integers M.

We now wish to examine each individual sum $\sum_{m=2^{k-1}}^{2^k-1} \left[\frac{M}{m}\right] R(2m)$. For this purpose, let $B = B_k$ be the number of even integers in $[2^k, 2^{k+1})$ for which the Goldbach conjecture fails. Then we have

$$\begin{aligned} \sum_{m=2^{k-1}}^{2^k-1} \left[\frac{M}{m}\right] R(2m) &\geq \sum_{\substack{2^{k-1} \leq m \leq 2^k - 1 \\ R(2m) \neq 0}} \left[\frac{M}{m}\right] \\ &\geq \sum_{\substack{2^{k-1} \leq m \leq 2^k - 1 \\ R(2m) \neq 0}} \left(\frac{M}{m} - 1\right). \end{aligned}$$

Of course, M/m is decreasing as a function of m, so the smallest possible value of the above summation occurs when the first B even integers in the interval $[2^k, 2^{k+1})$ fail the Goldbach conjecture. Consequently, we conclude that

$$\begin{aligned}\sum_{m=2^{k-1}}^{2^k-1}\left[\frac{M}{m}\right]R(2m) &\geq \sum_{m=2^{k-1}+B}^{2^k-1}\left(\frac{M}{m}-1\right)\\ &= \left(M\sum_{m=2^{k-1}+B}^{2^k-1}\frac{1}{m}\right)-(2^k-2^{k-1}-B)\end{aligned}$$

and we conclude that

$$\sum_{m=2^{k-1}}^{2^k-1}\left[\frac{M}{m}\right]R(2m) \geq \left(M\sum_{m=2^{k-1}+B}^{2^k-1}\frac{1}{m}\right)-2^{k-1}. \tag{6.10}$$

It is well-known that

$$\sum_{n\leq x}\frac{1}{n} = \log x+\gamma+O(x^{-1})$$

where γ is the Euler-Mascheroni constant. Hence we have

$$\sum_{m=2^{k-1}+B}^{2^k-1}\frac{1}{m} = k\log 2-\log(2^{k-1}+B)+O(2^{-k}).$$

Using (6.8), we have $B \leq c2^{k(1-\delta)}$, which implies that

$$\begin{aligned}\sum_{m=2^{k-1}+B}^{2^k-1}\frac{1}{m} &\geq k\log 2-\log\left(2^{k-1}+c2^{k(1-\delta)}\right)-c_0 2^{-k}\\ &= k\log 2-(k-1)\log 2-\log\left(1+c2^{-k\delta+1}\right)-c_0 2^{-k}\\ &= \log 2-\log\left(1+c2^{-k\delta+1}\right)-c_0 2^{-k}\end{aligned}$$

for some constant $c_0 > 0$. Combining this with (6.10), we obtain

$$\sum_{m=2^{k-1}}^{2^k-1}\left[\frac{M}{m}\right]R(2m) \geq M\left(\log 2-\log\left(1+c2^{-k\delta+1}\right)-c_0 2^{-k}\right)-2^{k-1}$$

for every positive integer k. Now applying this with (6.9) we find that

$$\begin{aligned}A(M) &\geq \sum_{k=1}^{[\log_2 M]}\sum_{m=2^{k-1}}^{2^k-1}\left[\frac{M}{m}\right]R(2m)\\ &\geq \sum_{k=1}^{[\log_2 M]}\left(M\left(\log 2-\log\left(1+c2^{-k\delta+1}\right)-c_0 2^{-k}\right)-2^{k-1}\right).\end{aligned}$$

and it follows that

$$\begin{aligned}A(M) \geq M\log 2[\log_2 M] &- M\sum_{k=1}^{[\log_2 M]}\log\left(1+c2^{-k\delta+1}\right)\\ &- c_0 M\sum_{k=1}^{[\log_2 M]}2^{-k}-\sum_{k=1}^{[\log_2 M]}2^{k-1}.\end{aligned} \tag{6.11}$$

Now notice that

$$\sum_{k=1}^{[\log_2 M]} 2^{-k} \leq \sum_{k=1}^{\infty} 2^{-k} = 1$$

and

$$\sum_{k=1}^{[\log_2 M]} 2^{k-1} = \sum_{k=0}^{[\log_2 M]-1} 2^{k} = \frac{2^{[\log_2 M]} - 1}{2-1} \leq M - 1 < M.$$

Also, since $\log(1+x) \leq x$ for $x > 0$, we have

$$\sum_{k=1}^{[\log_2 M]} \log\left(1 + c2^{-k\delta+1}\right) \leq 2c \sum_{k=1}^{[\log_2 M]} 2^{-k\delta} \leq \frac{2c}{2^{\delta}-1}.$$

Combining these with (6.11), we find that

$$\begin{aligned} A(M) &\geq M[\log_2 M]\log 2 - \frac{2cM}{2^{\delta}-1} - c_0 M - M \\ &\geq M\log M - M\left(\log 2 + \frac{2c}{2^{\delta}-1} + c_0 + 1\right) \end{aligned}$$

and the result follows by taking

$$C = -\left(\log 2 + \frac{2c}{2^{\delta}-1} + c_0 + 1\right).$$

□

Proof of Theorem 3.6. In view of (3.1), for $1 \leq m \leq M$ we have that

$$a(2m) = \sum_{d|m} R(2d) \sim 4C_2 \sum_{d|m} \frac{d}{\log^2(2d)} \prod_{\substack{p|d \\ p>2}} \frac{p-1}{p-2}. \tag{6.12}$$

To establish the asymptotic lower bound for $a(2m)$, we write, for convenience $f(d) = \prod_{\substack{p|d \\ p>2}} \frac{p-1}{p-2}$. Then we have

$$\sum_{d|m} \frac{df(d)}{\log^2(2d)} \geq \sum_{d|m} \frac{df(d)}{\log^2(2m)}.$$

Since $df(d)$ is multiplicative, we obtain that

$$\begin{aligned} \sum_{d|m} df(d) &= \prod_{p^l \| m} \sum_{d|p^l} df(d) \\ &= \prod_{p^l \| m} \left(1 + pf(p) + p^2 f(p) + \cdots + p^l f(p)\right) \\ &= \prod_{p^l \| m} \left(1 + \left(\frac{p-1}{p-2}\right) p \frac{p^l - 1}{p-1}\right) \\ &= \prod_{p^l \| m} \frac{p^{l+1} - 2}{p-2} \\ &\geq \prod_{p^l \| m} p^l = m. \end{aligned}$$

Therefore,

$$a(2m) \geq \frac{4C_2 m}{\log^2(2m)} \sim \frac{4C_2 m}{\log^2 m}.$$

For the upper bound, we apply the partial summation formula to obtain that

$$\sum_{d|m} \frac{df(d)}{\log^2(2d)} = \frac{\sum_{d\leq m} df(d)}{\log^2(2m)} + 2\int_1^m \frac{\sum_{\substack{d\leq t\\ d|m}} df(d)}{t\log^3(2t)}dt.$$

We see that

$$\begin{aligned}\int_1^m \frac{\sum_{\substack{d\leq t\\ d|m}} df(d)}{t\log^3(2t)}dt &\leq \int_1^{\sqrt{m}} \frac{\sum_{d\leq t} df(d)}{t\log^3(2t)}dt + \int_{\sqrt{m}}^m \frac{\sum_{d|m} df(d)}{t\log^3(2t)}dt \\ &\sim \int_1^{\sqrt{m}} \frac{2t}{\log^3(2t)}dt + \sum_{d|m} df(d)\left(\frac{1}{2\log^2(2t)}\bigg|_{\sqrt{m}}^m\right) \\ &\leq O\left(\frac{m}{\log^3 m}\right) + \frac{\sum_{d|m} df(d)}{2\log^2(2m)}.\end{aligned}$$

Hence

$$\sum_{d|m} \frac{df(d)}{\log^2(2d)} \lesssim 2\frac{\sum_{d\leq m} df(d)}{\log^2(2m)},$$

and therefore,

$$a(2m) \lesssim \frac{8C_2}{\log^2 m}\prod_{p^l\|m}\frac{p^{l+1}-2}{p-2} = \frac{8C_2 m}{\log^2 m}\prod_{p^l\|m}\frac{p-2/p^l}{p-2}$$

establishing (3.6).

To prove (3.7), we write

$$\Omega(n) = \begin{cases} 0 & \text{if } n \text{ is odd,} \\ nf(n) & \text{if } n \text{ is even.}\end{cases}$$

From [3], we know that the generating function of $\Omega(n)$ has a simple pole at $s = 2$ with residue 1. In other words, we have that

$$\sum_{n=1}^{\infty} \frac{\Omega(n)}{n^s} \sim \frac{1}{s-2}, \qquad \Re(s) > 2,$$

so by the Wiener-Ikehara Theorem (e.g. see Theorem 7.7 of [1]), we have

$$\sum_{n\leq M} \Omega(n) \sim M^2.$$

Translating back to our definition, we have

$$\sum_{m\leq M} mf(m) \sim 2M^2. \tag{6.13}$$

In view of (6.12)

$$\begin{aligned} A(M) &= \sum_{1\le m\le M} a(2m) \\ &= \sum_{1\le m\le M} \left[\frac{M}{m}\right] R(2m) \\ &\sim 4C_2 \sum_{1\le m\le M} \left[\frac{M}{m}\right] \frac{mf(m)}{\log^2(2m)}. \end{aligned}$$

We first write

$$\begin{aligned} \sum_{1\le m\le M} \left[\frac{M}{m}\right] \frac{mf(m)}{\log^2(2m)} &= \sum_{1\le k\le M} k \sum_{\substack{1\le m\le M \\ [M/m]=k}} \frac{mf(m)}{\log^2(2m)} \\ &= \sum_{1\le k\le M-1} k \sum_{\substack{1\le m\le M \\ M/(k+1)<m\le M/k}} \frac{mf(m)}{\log^2(2m)} + \frac{Mf(M)}{\log^2(2M)} \\ &\sim \sum_{1\le k\le M-1} k \sum_{\substack{1\le m\le M \\ M/(k+1)<m\le M/k}} \frac{mf(m)}{\log^2(2m)}. \end{aligned}$$

By the partial summation formula, we have

$$\begin{aligned} \sum_{\substack{1\le m\le M \\ M/(k+1)<m\le M/k}} \frac{mf(m)}{\log^2(2m)} &= \int_{M/(k+1)}^{M/k} \frac{1}{\log^2(2t)} d\sum_{m\le t} mf(m) \\ &= \frac{\sum_{m\le t} mf(m)}{\log^2(2t)}\Bigg|_{M/(k+1)}^{M/k} + 2\int_{M/(k+1)}^{M/k} \frac{\sum_{m\le t} mf(m)}{t\log^3(2t)} dt \\ &\sim \frac{2t^2}{\log^2(2t)}\Bigg|_{M/(k+1)}^{M/k} + 2\int_{M/(k+1)}^{M/k} \frac{2t^2}{t\log^3(2t)} dt \\ &= 2\left(\frac{(M/k)^2}{\log^2(2M/k)} - \frac{(M/(k+1))^2}{\log^2(2M/(k+1))}\right) + 4\int_{M/(k+1)}^{M/k} \frac{t}{\log^3(2t)} dt \qquad (6.14) \end{aligned}$$

by (6.13). We now sum the right hand side of (6.14) over k with $1 \le k \le M-1$. The first term equals

$$\begin{aligned} &2\sum_{1\le k\le M-1} k\left(\frac{(M/k)^2}{\log^2(2M/k)} - \frac{(M/(k+1))^2}{\log^2(2M/(k+1))}\right) \\ &= 2\sum_{1\le k\le M-1} \frac{kM^2}{k^2\log^2(2M/k)} - 2\sum_{2\le k\le M} \frac{(k-1)M^2}{k^2\log^2(2M/k)} \qquad (6.15) \\ &= \frac{2M^2}{\log^2(2M)} - \frac{2M}{\log^2 2} + 2M^2 \sum_{2\le k\le M} \frac{1}{k^2\log^2(2M/k)}. \end{aligned}$$

By the partial summation formula again, we have that

$$\begin{aligned}\sum_{1<k\le M}\frac{1}{k^2\log^2(2M/k)} &= \frac{\sum_{1<k\le x}\frac{1}{k^2}}{\log^2(2M/x)}\Bigg|_1^M - 2\int_1^M \frac{\sum_{1<k\le t}\frac{1}{k^2}}{t\log^3(2M/t)}dt\\ &= \frac{\sum_{2\le k\le M}\frac{1}{k^2}}{\log^2 2} - 2\int_2^M \frac{\sum_{k=2}^\infty \frac{1}{k^2}+O(1/t)}{t\log^3(2M/t)}dt\\ &= \frac{\sum_{k=2}^\infty\frac{1}{k^2}}{\log^2 2} + O(1/M) - 2\sum_{k=2}^\infty\frac{1}{k^2}\int_2^M\frac{dt}{t\log^3(2M/t)} + O\left(\int_2^M\frac{dt}{t^2\log^3(2M/t)}\right).\end{aligned}$$

Now observe that

$$\int_2^M \frac{dt}{t\log^3(2M/t)} = \frac{1}{2}\int_2^M d\log^{-2}(2M/t) = \frac{1}{2\log^2 2} - \frac{1}{2\log^2 M}$$

and

$$\begin{aligned}\int_2^M \frac{dt}{t^2\log^3(2M/t)} &= -\int_2^M \frac{dt^{-1}}{\log^3(2M/t)}\\ &= -\frac{1}{M\log^3 2} + \frac{1}{2\log^3 M} + 3\int_2^M \frac{dt}{t^2\log^4(2M/t)} = O(\log^{-3} M).\end{aligned}$$

Therefore,

$$\sum_{2\le k\le M}\frac{1}{k^2\log^2(2M/k)} = \sum_{k=2}^\infty \frac{1}{k^2}\frac{1}{\log^2 M} + O(\log^{-3} M)$$

and hence, the first term of (6.14) after summing over k is

$$(6.16)\qquad \sim \frac{2M^2}{\log^2(2M)} + 2\left(\sum_{k=2}^\infty\frac{1}{k^2}\right)\frac{M^2}{\log^2 M} \sim 2\left(\sum_{k=1}^\infty \frac{1}{k^2}\right)\frac{M^2}{\log^2 M} = \frac{\pi^2}{3}\cdot\frac{M^2}{\log^2 M}.$$

Similarly, the second term of (6.14) after summing over k is given by

$$\begin{aligned}&2\sum_{1\le k\le M-1} k\int_{M/(k+1)}^{M/k}\frac{dt^2}{\log^3(2t)}\\ &\qquad = 2\sum_{1\le k\le M-1} k\left\{\frac{t^2}{\log^3(2t)}\Bigg|_{M/(k+1)}^{M/k} + 3\int_{M/(k+1)}^{M/k}\frac{tdt}{\log^4(2t)}\right\}\\ &\qquad = 2\sum_{1\le k\le M-1} k\left\{\frac{(M/k)^2}{\log^3(2M/k)} - \frac{(M/(k+1))^2}{\log^3(2M/(k+1))}\right\} + O\left(\frac{M^2}{\log^3 M}\right)\\ (6.17)\qquad &\qquad = O\left(\frac{M^2}{\log^3 M}\right)\end{aligned}$$

by a similar argument used to treat (6.15) except with $\log^3(\cdot)$ in the place of $\log^2(\cdot)$. Hence in view of (6.14),(6.16) and (6.17), we have

$$\sum_{1\le m\le M}\left[\frac{M}{m}\right]\frac{mf(m)}{\log^2(2m)} \sim \frac{\pi^2}{3}\cdot\frac{M^2}{\log^2 M}.$$

Therefore,

$$A(M) \sim \frac{4\pi^2 C_2 M^2}{3\log^2 M}.$$

This proves (3.7) and completes the proof of Theorem 3.6. □

References

[1] P.T. Bateman and H.G. Diamond, *Analytic number theory*, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2004, An introductory course.

[2] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, Fifth edition. The Clarendon Press, Oxford University Press, New York, 1979

[3] G.H. Hardy and J.E. Littlewood, *Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes*, Acta Math. **44** (1923), no. 1, 1–70.

[4] M.N. Huxley, *Exponential sums and lattice points III*, Proc. London Math. Soc. (3) **87** (2003), no. 3, 591–609

[5] H. Li, *The exceptional set of Goldbach numbers. II*, Acta Arith. **92** (2000), no. 1, 71–88.

[6] H.L. Montgomery and R.C. Vaughan, *The exceptional set in Goldbach's problem*, Collection of articles in memory of Juriĭ Vladimirovič Linnik, Acta Arith., **27** (1975), 353–370.

Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada V5A 1S6,