Erdős–Turán Theorem and Eulerian Integers

Erik Füredi[a] and Katalin Gyarmati[b]

[a]ELTE Eötvös Loránd University Faculty of Science, Budapest 1117, Hungary, email: erikfuredi@gmail.com

[b]ELTE Eötvös Loránd University, Department of Algebra and Number Theory, Budapest 1117, Hungary, email: katalin.gyarmati@gmail.com

2025. 10. 12.

Abstract

Our work is motivated by the fact that the norms of the Eulerian integers are related to the sums of form $a^2 - ab + b^2$, providing a natural generalization for problems concerning products over sums or differences of integers. Let E be the set of Eulerian integers. We define $\omega_{\mathbb{N}}(x)$ as the number of distinct prime divisors of $x \in \mathbb{N}$, and $\omega_E(x)$ as the number of distinct Euler prime divisors of $x \in E$. By the Erdős–Turán theorem, if $\mathcal{A} \subset \mathbb{Z}^+$ and $|\mathcal{A}| = 3 \cdot 2^{k-1}$ ($k \in \mathbb{Z}^+$), then $\omega_{\mathbb{N}}(\prod_{a,b\in\mathcal{A},a\neq b}(a+b)) \geq k+1$. We prove that if $\mathcal{A} \subset E$ is a finite set and $\rho \in E$, then the value of $\omega_E(\prod_{a,b\in\mathcal{A},a\neq b}(a+\rho b))$ has a lower bound of order $\log|\mathcal{A}|$. Consequently, we provide lower bounds for $\mathcal{A} \subset \mathbb{N}$ for both $\omega_{\mathbb{N}}(\prod_{a,b\in\mathcal{A},a\neq b}(a^2+ab+b^2))$ and $\omega_{\mathbb{N}}(\prod_{a,b\in\mathcal{A},a\neq b}(a^2-ab+b^2))$. We also give an upper bound for the minimum of $\omega_{\mathbb{N}}(\prod_{a,b\in\mathcal{A},a\neq b}(a^2+

2020 Mathematics Subject Classification: Primary: 11B75, 11B83, 11D99, 11R04.

Keywords and phrases: Eulerian integer, Euler prime, prime, Erdős–Turán theorem.

Research supported by the Hungarian National Research Development and Innovation Funds KKP133819.

$ab+b^2$)) with a computer program, if $|\mathcal{A}| \le 8$ and sets whose largest element is relatively small. Furthermore, using a Diophantine number theoretical lemma of Győry, Sárközy, and Stewart, we give a lower bound of order $\log|\mathcal{A}|$ for $\omega_{\mathbb{N}}(\prod_{a\in\mathcal{A},b\in\mathcal{B}}(f(a,b)))$ for a specific class of polynomials $f \in \mathbb{Z}[x,y]$ and finite sets $\mathcal{A},\mathcal{B} \subset \mathbb{Z}$.

1 Introduction

In 1934, Erdős and Turán proved their celebrated theorem, stated below as Theorem A [3]:

Theorem A [Erdős–Turán]. *If $k \in \mathbb{N}$, $\mathcal{A} \subseteq \mathbb{N}$ and $|\mathcal{A}| \ge 3\cdot 2^{k-1}$ is finite set then*

$$\omega_{\mathbb{N}}(\prod_{\substack{a,b\in\mathcal{A}\\ a\neq b}}(a+b)) \ge k+1,$$

where, for $n \in \mathbb{N}$, $\omega_{\mathbb{N}}(n)$ denotes the number of distinct positive prime factors of n.

Later, an improved version of this result was presented in the Erdős–Surányi book [2], where the lower bound was proved for $|\mathcal{A}| \ge 2^k+1$. In 1986, Győry, Stewart, and Tijdeman [5] generalized the theorem to two different sets, proving the following result:

Theorem B. *There exists an effectively computable positive constant c such that if $\mathcal{A},\ \mathcal{B} \subseteq \mathbb{Z}^+$ are finite sets and $|\mathcal{A}| \ge |\mathcal{B}| \ge 2$, then*

$$\omega_{\mathbb{N}}(\prod_{a\in\mathcal{A},\ b\in\mathcal{B}}(a+b)) \ge c\log|\mathcal{A}|.$$

In 1988, Erdős, Stewart, and Tijdeman [1] proved that the lower bound in Theorem B cannot be improved significantly:

Theorem C. *For any $\varepsilon > 0$ and all sufficiently large integers k, there exist sets $\mathcal{A}$ and $\mathcal{B}$ such that* $|\mathcal{A}| = k$, $|\mathcal{B}| = 2$, and

$$\omega_{\mathbb{N}}(\prod_{a\in\mathcal{A},\ b\in\mathcal{B}}(a+b)) < \left(\frac{1}{8}+\varepsilon\right)(\log|\mathcal{A}|)^2\log\log|\mathcal{A}|.$$

Inspired by these previous results, we studied whether the Erdős–Turán Theorem holds in the ring of Eulerian integers. For this, we will use the following notations: let $\omega = \dfrac{-1+i\sqrt{3}}{2}$, a third root of unity, and let E denote the ring of Eulerian integers, i.e., $E = \{a + b\omega : \ a, b \in \mathbb{Z}\}$. Furthermore, for $x \in E$, $\omega_E(x)$ denotes the number of distinct prime divisors of the Eulerian integer x (in the above notation, two primes are considered distinct if they are not associated). Then the analogue of Theorem A among Eulerian integers is as follows:

Theorem 1. *Let $\mathcal{A} \subseteq E$ be a finite set such that $|\mathcal{A}| \geq 2$. Then*

$$\omega_E(\prod_{\substack{a,b\in\mathcal{A}\\ a\neq b}} (a+b)) > \frac{\log(|\mathcal{A}|-1) - \log 18}{\log 2}.$$

Our proof utilizes the Law of Cosines alongside the method of Erdős and Turán.

It is natural to ask whether a similar statement holds for the product of sums of the type $a + \rho b$, where ρ is an arbitrary Eulerian integer. We proved the following:

Theorem 2. *Let $\rho \in E$. Then, there exists a constant c that depends only on ρ such that for any finite set $\mathcal{A} \subseteq E$*

$$\omega_E(\prod_{\substack{a,b\in\mathcal{A}\\ a\neq b}} (a+\rho b)) > \frac{\log|\mathcal{A}|}{\log 3} - c.$$

The above theorem, combined with the multiplicative property of the norm $N(a + b\omega) = a^2 - ab + b^2$ in the ring of Eulerian integers, yields surprising corollaries for rational integers.

Corollary 1. *If $\mathcal{A} \subseteq \mathbb{Z}^+$ is a finite nonempty set, then*

$$\omega_{\mathbb{N}}(\prod_{\substack{a,b\in\mathcal{A}\\ a\neq b}} (a^2-ab+b^2)) > \frac{\log|\mathcal{A}| - \log 38}{2\log 3}.$$

Corollary 2. *If $\mathcal{A} \subseteq \mathbb{Z}^+$ is a finite nonempty set, then*

$$\omega_{\mathbb{N}}(\prod_{\substack{a,b\in\mathcal{A}\\ a\neq b}} (a^2+ab+b^2)) > \frac{\log|\mathcal{A}| - \log 146}{2\log 3}.$$

These two corollaries motivated us to ask whether the Erdős-Turán theorem can be generalized to arbitrary two-variable polynomials and two different sets. We conjecture the following:

Conjecture 1. *If $f \in \mathbb{Z}[x,y]$ is a two-variable polynomial that is not decomposable as $f(x,y) = g(x)h(y)$, where $g, h \in \mathbb{Z}[x]$, then there exists a constant c that depends only on the polynomial f, such that if $\mathcal{A}$, $\mathcal{B} \subseteq \mathbb{Z}^+$ are finite sets and $|\mathcal{A}| \geq |\mathcal{B}| \geq 2$, then*

$$\omega_{\mathbb{N}}(\prod_{a\in\mathcal{A}, b\in\mathcal{B}} (f(a,b))) \geq c \log |\mathcal{A}|.$$

However, while we could not prove this conjecture in its full generality, we were able to handle an important special case:

Theorem 3. *Let $n \geq 2$ be a positive integer, $f(x,y) = \sum_{i=1}^{n-1} r_i x^{m_i} y^{i-1} + r_n y^{n-1} \in \mathbb{Z}[x,y]$ be a polynomial where $m_1, m_2, \ldots, m_{n-1}$ are nonnegative integers and the coefficients r_i are positive. Then there exists an effectively computable positive constant c such that if $\mathcal{A}$ and $\mathcal{B} \subseteq \mathbb{Z}^+$ are finite sets, where $|\mathcal{A}| \geq |\mathcal{B}| \geq 2n-2$, then*

$$\omega_{\mathbb{N}}\Big(\prod_{a\in\mathcal{A}, b\in\mathcal{B}} (f(a,b))\Big) \geq c \log |\mathcal{A}|.$$

The proof of Theorem 3 relies on a theorem of Győry, Sárközy and Stewart [4] and utilizes Vandermonde determinants. Interestingly, this general theorem implies a lower bound of logarithmic magnitude, similar to Corollary 2 (but not to Corollary 1).

If $f(a,b) = a^2 + ab + b^2$, we used a Python program to examine the smallest possible values of $\omega_{\mathbb{N}}\left(\prod_{a,b\in\mathcal{A}, a\neq b}(a^2+ab+b^2)\right)$ for sets of positive integers $\mathcal{A}$ with $3-8$ elements. Our analysis focused on sets whose elements were bounded by a few hundred, specifically considering primitive sets (where the greatest common divisor of all elements is 1). The Table 1 shows our such results.

Size of $\mathcal{A}$	Maximal allowed element	Minimum number of different prime divisors	Examples
3	400	3	28868 pcs, e.g. {1,2,3}, {1,2,4}, {388,395,399}
4	400	4	5 pcs: {1,2,4,8}, {1,3,9,18}, {1,3,9,27}, {1,4,16,22}, {1,9,15,18}
5	200	5	2 pcs: {1,2,4,8,16}, {1,3,9,27,81}
6	200	6	1 pc: {1,2,4,8,16,32}
7	150	7	1 pc: {1,2,4,8,16,32,64}
8	100	9	3 pcs, e.g.: {2,3,4,6,9,12,18,36}

Table 1: The smallest possible values of $\omega_{\mathbb{N}}\left(\prod_{a,b\in\mathcal{A},a\neq b}(a^2+ab+b^2)\right)$ for special sets $\mathcal{A}$ with $3-8$ elements

As a continuation of this work, we plan to generalize Theorem 3 to an arbitrary homogeneous polynomial $f(x,y)$, focusing initially on the single-set problem where we seek the bound

$$\omega_{\mathbb{N}}\left(\prod_{a,b\in\mathcal{A}}(f(a,b))\right)\geq c\log|\mathcal{A}|.$$

However, the full proof will involve significant further complications and will be presented in a subsequent paper.

2 Proofs

Proof of Theorem 1. Let us plot the elements of the set $\mathcal{A}$ on the complex plane. The lines $y=0$, $y=\sqrt{3}x$ and $y=-\sqrt{3}x$ divide $\mathbb{C}\backslash\{0\}$ into six half-open, half-closed sectors; among these, one must contain at least $(|\mathcal{A}|-1)/6$ elements of $\mathcal{A}$. Let $\mathcal{A}_0$ be the subset of $\mathcal{A}$ containing these elements. Thus,

$$\mathcal{A}_0\subset\mathcal{A},\quad |\mathcal{A}_0|\geq\frac{|\mathcal{A}|-1}{6}.$$

Figure 1 shows the partition into six parts.

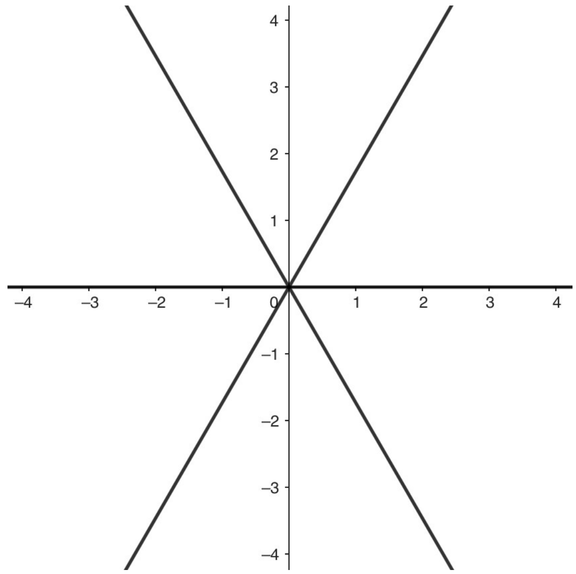

Figure 1: The partition of $\mathbb{C}\backslash\{0\}$ into six parts

For $x \in \mathbb{C}$, denote the absolute value of x by $|x|$. Then, the norm of an Eulerian integer $a \in E$ is $N(a) = |a|^2$. Since the angle between vectors of any two Eulerian integers in $\mathcal{A}_0$ is an acute angle, by the law of sines for $a, b \in \mathcal{A}_0$

$$|a + b| > \max\{|a|, |b|\}. \tag{1}$$

Since $\mathcal{A}_0 \subseteq \mathcal{A}$,

$$\omega_E\Big(\prod_{\substack{a,b\in\mathcal{A}\\ a\neq b}} (a + b)\Big) \geq \omega_E\Big(\prod_{\substack{a,b\in\mathcal{A}_0\\ a\neq b}} (a + b)\Big)$$

Let us list the odd-norm Euler prime divisors of $\prod_{\substack{a,b\in\mathcal{A}\\ a\neq b}}(a + b)$ by choosing exactly one of the prime divisors associated with each other (arbitrarily).

Let these be $\pi_1, \pi_2, \pi_3, \ldots, \pi_s$. We prove that

$$s > \frac{\log(|\mathcal{A}| - 1) - \log 18}{\log 2}. \tag{2}$$

This implies Theorem 1. We then prove (2) by contradiction. Suppose that

$$s \leq \frac{\log(|\mathcal{A}| - 1) - \log 18}{\log 2}. \tag{3}$$

We recursively define a sequence of sets

$$\mathcal{A}_0 \supseteq \mathcal{A}_1 \supseteq \mathcal{A}_2 \supseteq \cdots \supseteq \mathcal{A}_s$$

such that

$$(4)\qquad |\mathcal{A}_{i+1}| \geq \frac{|\mathcal{A}_i|}{2}$$

if $0 \leq i \leq s-1$, and

$$(5)\qquad a, b \in \mathcal{A}_{i+1},\ \alpha \in \mathbb{N}, \pi_{i+1}^{\alpha} \mid a+b \quad \Leftrightarrow \quad \pi_{i+1}^{\alpha} \mid a, \quad \text{and } \pi_{i+1}^{\alpha} \mid b.$$

To do this, we first divide the mod π_{i+1} reduced residue classes into two groups, U_i and V_i, such that a reduced residue class n and its additive inverse $-n$ never fall into the same group (since $2 \nmid \pi_{i+1}$ they are different reduced residue classes). We then partition the set $\mathcal{A}_i$ into two subsets $\mathcal{A}_{i,0}$ and $\mathcal{A}_{i,1}$, by writing each element $a \in \mathcal{A}_i$ in the form $a = \pi_{i+1}^{\gamma} a_0$, where $\pi_{i+1} \nmid a_0$. Let $a \in \mathcal{A}_{i,0}$ if $a_0 \in U_i$ and $a \in \mathcal{A}_{i,1}$ if $a_0 \in V_i$. It is clear that, for $j \in \{0, 1\}$, we have

$$(6)\qquad a, b \in \mathcal{A}_{i,j},\ \alpha \in \mathbb{N}, \pi_{i+1}^{\alpha} \mid a+b \quad \Leftrightarrow \quad \pi_{i+1}^{\alpha} \mid a, \quad \text{and } \pi_{i+1}^{\alpha} \mid b,$$

since if $a = \pi_{i+1}^{\gamma} a_0,\ b = \pi_{i+1}^{\delta} b_0$ (where $\pi_{i+1} \nmid a_0, b_0$) we consider two cases.

Case 1: $\gamma \neq \delta$. Then $\pi_{i+1}^{\min\{\gamma,\delta\}} \mid a+b$, but $\pi_{i+1}^{\min\{\gamma,\delta\}+1} \nmid a+b$. This implies (5).

Case 2: $\gamma = \delta$. Then

$$a + b = \pi_{i+1}^{\gamma}(a_0 + b_0),$$

where $a_0, b_0 \in U_i$ or $a_0, b_0 \in V_i$. Due to the definition of the sets U_i and V_i, it is impossible that $a_0 \not\equiv -b_0 \mod \pi_{i+1}$, i.e. $\pi_{i+1} \nmid a_0 + b_0$. That is, $\pi_{i+1}^{\gamma} \mid a+b$, but $\pi_{i+1}^{\gamma+1} \nmid a+b$. Since $\pi_{i+1}^{\gamma} \mid a, b$, this also verifies (5).

Next, we turn to the recursive definition of the sets $\mathcal{A}_0 \supseteq \mathcal{A}_1 \supseteq \mathcal{A}_2 \supseteq \cdots \supseteq \mathcal{A}_s$. If the sets $\mathcal{A}_0 \supseteq \mathcal{A}_1 \supseteq \mathcal{A}_2 \supseteq \cdots \supseteq \mathcal{A}_i$ are already constructed with the desired property, then let $\mathcal{A}_{i+1}$ simply be the set with the larger number of elements between $\mathcal{A}_{i,0}$ and $\mathcal{A}_{i,1}$. If the numbers of elements are equal, then we can arbitrarily choose which subset should be $\mathcal{A}_{i+1}$. Then both (4) and (5) are satisfied.

For all odd-norm Euler primes $\pi_1, \pi_2, \ldots, \pi_s$ we have that

$$(7)\qquad a, b \in \mathcal{A}_s,\ \alpha \in \mathbb{N}, \pi_i^{\alpha} \mid a+b \quad \Leftrightarrow \quad \pi_i^{\alpha} \mid a, \quad \text{and } \pi_i^{\alpha} \mid b,$$

and, by (3) and (4),

$$|\mathcal{A}_s| \geq \frac{|\mathcal{A}_0|}{2^s} \geq \frac{|\mathcal{A}| - 1}{6 \cdot 2^s} \geq 3.$$

Let a, b, c be three distinct elements of $\mathcal{A}_s$. Let us write the prime factorization of $a+b, a+c, b+c$ in the ring of Eulerian integers:

$$a+b = \varepsilon_1 2^{\gamma_0}\pi_1^{\gamma_1}\pi_2^{\gamma_2}\dots\pi_s^{\gamma_s},$$
$$a+c = \varepsilon_2 2^{\beta_0}\pi_1^{\beta_1}\pi_2^{\beta_2}\dots\pi_s^{\beta_s},$$
$$b+c = \varepsilon_3 2^{\alpha_0}\pi_1^{\alpha_1}\pi_2^{\alpha_2}\dots\pi_s^{\alpha_s}.$$

It is clear that, by (7),

$$\pi_1^{\gamma_1}\pi_2^{\gamma_2}\dots\pi_s^{\gamma_s} \mid a, b.$$

Furthermore, we must have

$$2^{\gamma_0} \nmid a, b.$$

To see this, suppose, for example, that $2^{\gamma_0} \mid a$. Then, since we already established that $\pi_1^{\gamma_1}\pi_2^{\gamma_2}\dots\pi_s^{\gamma_s} \mid a$, we would have $2^{\gamma_0}\pi_1^{\gamma_1}\pi_2^{\gamma_2}\dots\pi_s^{\gamma_s} \mid a$, and consequently

$$|a+b| = |2^{\gamma_0}\pi_1^{\gamma_1}\pi_2^{\gamma_2}\dots\pi_s^{\gamma_s}| \leq |a|,$$

which contradicts (1). Similarly, we can show that $2^{\gamma_0} \nmid b$. Then, the exponent of 2 in the prime factorization of a and b must be the same. Otherwise $2^{\gamma_0} \nmid a+b$. Consequently, the exponent of 2 is identical in a, b, and c. Let

$$a = 2^t a_1,$$
$$b = 2^t b_1,$$
$$c = 2^t c_1,$$

where the norms of the Eulerian integers a_1, b_1, c_1 are odd. Substituting these into the factorizations above, we get:

$$a_1 + b_1 = \varepsilon_1 2^{\gamma_0 - t}\pi_1^{\gamma_1}\pi_2^{\gamma_2}\dots\pi_s^{\gamma_s}$$
$$a_1 + c_1 = \varepsilon_2 2^{\beta_0 - t}\pi_1^{\beta_1}\pi_2^{\beta_2}\dots\pi_s^{\beta_s}$$
$$b_1 + c_1 = \varepsilon_3 2^{\alpha_0 - t}\pi_1^{\alpha_1}\pi_2^{\alpha_2}\dots\pi_s^{\alpha_s}.$$

where $\pi_1^{\gamma_1}\pi_2^{\gamma_2}\dots\pi_s^{\gamma_s} \mid a_1, b_1$. So

$$|a_1|, |b_1| \geq |\pi_1^{\gamma_1}\pi_2^{\gamma_2}\dots\pi_s^{\gamma_s}|.$$

We prove that $\gamma_0 - t \geq 2$. We consider two cases.

Case 1: $|a_1| \neq |b_1|$. By symmetry, we may assume that $|a_1| > |b_1|$. So,

$$|a_1| > |\pi_1^{\gamma_1}\pi_2^{\gamma_2}\dots\pi_s^{\gamma_s}|$$
$$|b_1| \geq |\pi_1^{\gamma_1}\pi_2^{\gamma_2}\dots\pi_s^{\gamma_s}|.$$

If the norm of $x \in E$ Eulerian integer is denoted by $N(x) = |x|^2$, then

$$N(a_1) > N(\pi_1^{\gamma_1}\pi_2^{\gamma_2}\dots\pi_s^{\gamma_s}),$$

but $\pi_1^{\gamma_1}\pi_2^{\gamma_2}\dots\pi_s^{\gamma_s} \mid a_1$, so $N(\pi_1^{\gamma_1}\pi_2^{\gamma_2}\dots\pi_s^{\gamma_s}) \mid N(a_1)$, i.e.,

$$N(a_1) \geq 2N(\pi_1^{\gamma_1}\pi_2^{\gamma_2}\dots\pi_s^{\gamma_s})$$
$$|a_1| \geq \sqrt{2}|\pi_1^{\gamma_1}\pi_2^{\gamma_2}\dots\pi_s^{\gamma_s}|.$$

Since $a, b \in \mathcal{A}_0$, the angle between a and b is $\gamma < 60°$, and thus, the angle between a_1 and b_1 is also $\gamma < 60°$. By the law of cosines,

$$\begin{aligned}|a_1 + b_1|^2 &= |a_1|^2 + |b_1|^2 + 2\cos\gamma|a_1|\cdot|b_1| \\ &\geq |a_1|^2 + |b_1|^2 + 2\cos 60°|a_1|\cdot|b_1| \\ &= |a_1|^2 + |b_1|^2 + |a_1|\cdot|b_1| \\ &\geq (1 + \sqrt{2}^2 + 1\cdot\sqrt{2})|\pi_1^{\gamma_1}\pi_2^{\gamma_2}\dots\pi_s^{\gamma_s}|^2 \\ &> 4|\pi_1^{\gamma_1}\pi_2^{\gamma_2}\dots\pi_s^{\gamma_s}|^2,\end{aligned}$$

which, in the first case, gives $\gamma_0 - t \geq 2$.

Case 2: $|a_1| = |b_1|$. In this case, the angle γ between a_1 and b_1 falls in the interval $(0°, 60°)$, the law of cosines yields

$$\sqrt{3}|a_1| < |a_1 + b_1| < 2|a_1|.$$

Now $|a_1 + b_1| = 2^{\gamma_0 - t}|\pi_1^{\gamma_1}\pi_2^{\gamma_2}\dots\pi_s^{\gamma_s}|$, which leads to a contradiction in the case of $|a_1| = |b_1| = |\pi_1^{\gamma_1}\pi_2^{\gamma_2}\dots\pi_s^{\gamma_s}|$. Thus $|\pi_1^{\gamma_1}\pi_2^{\gamma_2}\dots\pi_s^{\gamma_s}|^2 \mid |a_1|^2$ implies

$$|a_1| \geq \sqrt{2}|\pi_1^{\gamma_1}\pi_2^{\gamma_2}\dots\pi_s^{\gamma_s}|.$$

Then $|a_1 + b_1| \geq \sqrt{3}|a_1| \geq \sqrt{6}|\pi_1^{\gamma_1}\pi_2^{\gamma_2}\dots\pi_s^{\gamma_s}|$; thus,

$$|a_1 + b_1|^2 = 2^{2(\gamma_0 - t)}|\pi_1^{\gamma_1}\pi_2^{\gamma_2}\dots\pi_s^{\gamma_s}|^2 > 2^2|\pi_1^{\gamma_1}\pi_2^{\gamma_2}\dots\pi_s^{\gamma_s}|^2$$

and thus $\gamma_0 - t \geq 2$. Similarly, $\beta_0 - t \geq 2$ and $\alpha_0 - t \geq 2$. So, $a_1 + b_1$, $a_1 + c_1$ and $b_1 + c_1$ are numbers divisible by $2^2 = 4$ (in the ring E), i.e.,

$$a_1 + b_1 = 4x,$$
$$a_1 + c_1 = 4y,$$
$$b_1 + c_1 = 4z,$$

where x, y, z are Eulerian integers. This shows that $a_1 = 2(x + y - z)$ is divisible by 2, i.e., a_1 is twice an Eulerian integer. This contradicts the assumption that the norm of a_1 is odd. Since our initial assumption (3) leads to a contradiction, the original statement of Theorem 1 follows.

Proof of Theorem 2. In the case $\rho = -1$, if for π an Euler prime such that $|\mathcal{A}| \geq |\pi|^2 + 1$, then there are two distinct Eulerian integers in $\mathcal{A}$ whose difference is divisible by π. Thus, $\omega_E(\prod_{\substack{a,b\in\mathcal{A}\\ a\neq b}}(a-b))$ is at least the number of pairwise not associated Euler primes whose absolute value not greater than $\sqrt{|\mathcal{A}|-1}$, which is at least the number of rational primes not greater than $\sqrt{|\mathcal{A}|-1}$. This can be estimated from below for sufficiently large sets $\mathcal{A}$ by the positive constant multiple of $\frac{\sqrt{|\mathcal{A}|-1}}{\log(\sqrt{|\mathcal{A}|-1})}$, from which the theorem can be stated for this case as well. We can assume that

$$\rho \neq 1 \quad \text{and} \quad \rho \neq -1$$

the theorem has already been proven for $\rho = 1$ (see Theorem 1).

Every Euler prime has an associated π such that $\mathrm{Arg}(\pi) \in [0°, 60°)$. Henceforth, we will focus only on these associates, and let $\mathcal{P}$ be the set of all such Euler primes. Thus,

$$\mathcal{P} = \{\pi : \ \pi \text{ is an Euler prime and } \mathrm{Arg}(\pi) \in [0°, 60°)\}.$$

The following lemma is the cornerstone of the proof of the theorem.

Lemma 1. *Let $\rho_0 \in E$ and π be an Euler prime such that $\pi \nmid \rho_0$, $\delta \in \mathbb{N}$, where $\pi^\delta \mid 1 + \rho_0$, but $\pi^{\delta+1} \nmid 1 + \rho_0$. Then, the reduced residue classes mod $\pi^{\delta+1}$ can be partitioned into three disjoint groups, C_1, C_2, C_3, such that for $1 \leq i \leq 3$,*

$$a, b \in C_i \quad \Rightarrow \quad \pi^{\delta+1} \nmid a + \rho_0 b.$$

Proof of Lemma 1. Let us list the reduced residue classes mod $\pi^{\delta+1}$: $r_1, r_2, \dots, r_m$. These can be divided into three groups using a greedy algorithm such that

$$r_i, \ -\rho_0 r_i$$

never fall into the same group. Indeed, assume that the elements $r_1, r_2, \dots, r_{i-1}$ have been correctly assigned. When assigning r_i, we must ensure that r_i falls into a different group than both the group of

$$-\rho_0 r_i \quad \text{and} \quad -\rho_0^{-1} r_i. \tag{8}$$

We have three groups, C_1, C_2, C_3. Since the elements in (8) exclude at most two groups (i.e., the groups to which $-\rho_0 r_i$ and $-\rho_0 r_i^{-1}$ are assigned), a conflict can only arise if r_i itself is an excluded element:

$$r_i \equiv -\rho_0 r_i \pmod{\pi^{\delta+1}}$$

or (which is equivalent anyway)

$$r_i \equiv -\rho_0^{-1} r_i \pmod{\pi^{\delta+1}}$$

(since in the case of $r_i \equiv -\rho_0 r_i \pmod{\pi^{\delta+1}}$ r_i and $-\rho_0 r_i$ are definitely in the same group, given that they are identical).

But this case cannot occur since

$$r_i \equiv -\rho_0 r_i \pmod{\pi^{\delta+1}}$$

implies

$$\pi^{\delta+1} \mid (1+\rho_0) r_i,$$

where r_i and π are relatively primes, so

$$\pi^{\delta+1} \mid 1+\rho_0,$$

which contradicts the conditions of the lemma.

We now divide the rest of the proof of Theorem 2 into two cases based on whether ρ is the negative of an Euler prime power in $\mathcal{P}$ with a positive integer exponent. (Recall that $\mathcal{P}$ contains Euler primes π such that $\operatorname{Arg}(\pi) \in [0°, 60°)$).

Case 1: Assume that ρ is not the negative of a power of an Euler prime $\theta \in \mathcal{P}$, i.e., ρ is not of the form $\rho = -\theta^\gamma$ with $\theta \in \mathcal{P}$, $\gamma \in \mathbb{N}$.

Before the next lemma, we introduce a new notation. Let $\rho \in E$ and π be an Euler prime, such that $\operatorname{Arg}(\pi) \in [0°, 60°)$. Write ρ in the form

$$\rho = \pi^\gamma \rho_0,$$

where $\pi \nmid \rho_0$ (here, $\rho_0 \neq -1$). Then, write $1+\rho_0$ in the form

$$1+\rho_0 = \pi^\delta \sigma,$$

where $\pi \nmid \sigma$. Let $c(\pi, \rho)$ denote the

$$c(\pi, \rho) \stackrel{\text{def}}{=} \gamma + \delta \geq 0$$

integer. It is clear that if

$$\pi \nmid \rho(1+\rho)$$

then $c(\pi,\rho)=0$. Thus,

$$c(\rho) \stackrel{\text{def}}{=} \prod_{\substack{\pi \mid \rho(1+\rho) \\ \operatorname{Arg}(\pi)\in[0^\circ,60^\circ)}} \pi^{c(\pi,\rho)},$$

the value of which solely depends on ρ. Let $\tau(c(\rho))$ denote the number of distinct divisors of $c(\rho)$ in the ring of Eulerian integers E, where two associated divisors δ and $\varepsilon\delta$ are considered distinct if $\varepsilon \neq 1$.

Then, Theorem 2 will be proved with the constant

$$c = \frac{\log(\tau(c(\rho))^2+2)}{\log 3}.$$

Namely, we will prove that if $|\mathcal{A}| = 3^s(\tau(c(\rho))^2+2)$ for an $s\in\mathbb{N}$, then, in the first case, $\omega_E(\prod_{\substack{a,b\in\mathcal{A}\\ a\neq b}}(a+\rho b)) > s$.

Lemma 2. *Let $\rho\in E$, $\mathcal{A}\subset E$ be a finite set and π an Euler prime such that $\operatorname{Arg}(\pi)\in[0^\circ,60^\circ)$ and $-\rho$ is not a power of π with a positive integer exponent. Then there exists a set $\mathcal{B}\subset\mathcal{A}$ such that*

$$|\mathcal{B}| \geq \frac{|\mathcal{A}|}{3},$$

and if $a,b\in\mathcal{B}$, for every integer $u\geq c(\pi,\rho)$,

$$\pi^u \mid a+\rho b \quad\Rightarrow\quad \pi^{u-c(\pi,\rho)} \mid a,\ b. \tag{9}$$

Proof of Lemma 2. Let

$$\rho = \pi^\gamma \rho_0,$$

where $\pi\nmid\rho_0$, and

$$1+\rho_0 = \pi^\delta\sigma,$$

where $\pi\nmid\sigma$. Then, $1+\rho_0\neq 0$. Let us write all elements of the set $\mathcal{A}$ in the form

$$a = \pi^\alpha a_0,$$

where $\pi\nmid a_0$, and let C_1,C_2,C_3 be the partition of the reduced residue classes $\bmod \pi^{\delta+1}$ according to Lemma 1. Let

$$\mathcal{B}_1 \stackrel{\text{def}}{=} \{a\in\mathcal{A}:\ a=\pi^\gamma a_0,\ \pi\nmid a_0,\ a_0\in C_1\}$$

$$\mathcal{B}_2 \stackrel{\text{def}}{=} \{a\in\mathcal{A}:\ a=\pi^\gamma a_0,\ \pi\nmid a_0,\ a_0\in C_2\}$$

$$\mathcal{B}_3 \stackrel{\text{def}}{=} \{a\in\mathcal{A}:\ a=\pi^\gamma a_0,\ \pi\nmid a_0,\ a_0\in C_3\}.$$

Let $\mathcal{B}$ be the set with the most elements among $\mathcal{B}_1,\ \mathcal{B}_2,\ \mathcal{B}_3$ (if there are several sets with the same number of elements, we choose $\mathcal{B}$ to be any of them). Obviously

$$|\mathcal{B}| \geq \frac{|\mathcal{A}|}{3}.$$

It remains is to prove that (9) holds for $\mathcal{B}$. For this, we write

$$a = \pi^{\alpha} a_0 \quad \text{and} \quad b = \pi^{\beta} b_0$$

in the form where $\pi \nmid a_0, b_0$. Then, a_0 and b_0 are elements of the same C_i set, say $a_0, b_0 \in C_1$. We then distinguish two cases.

Case I: $\alpha \neq \beta + \gamma$. Then,

$$\pi^{\min\{\alpha,\beta+\gamma\}} \mid a + \rho b \ (= \pi^{\alpha} a_0 + \pi^{\gamma} \rho_0 \pi^{\beta} b_0),$$

but

$$\pi^{\min\{\alpha,\beta+\gamma\}+1} \nmid a + \rho b \ (= \pi^{\alpha} a_0 + \pi^{\beta+\gamma} \rho_0 b_0).$$

We also have

$$\pi^{\alpha} \mid a \quad \text{and} \quad \pi^{\beta} \mid b$$
$$\pi^{\min\{\alpha,\beta+\gamma\}-\gamma} \mid a, b,$$
$$\pi^{\min\{\alpha,\beta+\gamma\}-c(\pi,\rho)} \mid a, b,$$

and thus the lemma is proved in this case.

Case II: $\alpha = \beta + \gamma$. Then,

$$a + \rho b = \pi^{\alpha} a_0 + \pi^{\beta+\gamma} \rho_0 b_0 = \pi^{\beta+\gamma}(a_0 + \rho_0 b_0).$$

By Lemma 1 $\pi^{\delta+1} \nmid a_0 + \rho_0 b_0$, so

$$\pi^{\beta+\gamma} \mid a + \rho b, \tag{10}$$

but

$$\pi^{\beta+\gamma+\delta+1} \nmid a + \rho b,$$
$$\pi^{\beta+c(\pi,\rho)+1} \nmid a + \rho b. \tag{11}$$

Since

$$\pi^{\beta} \mid \pi^{\beta+\gamma} \ \text{ and } \ \pi^{\beta+\gamma} = \pi^{\alpha} \mid a, \quad \text{we have} \quad \pi^{\beta} \mid a,\ b. \tag{12}$$

Thus, the lemma follows from (10), (11), and (12) in this case completing the proof of the lemma.

Let us list the Euler prime divisors of the product $\prod_{\substack{a,b\in\mathcal{A}\\ a\neq b}}(a+\rho b)$ with arguments in the interval $[0°, 60°)$ (of which every Euler prime divisor has exactly one associate)

$$\pi_1, \pi_2, \dots, \pi_s.$$

Suppose that

$$s \leq \frac{\log(|\mathcal{A}|/(\tau(c(\rho))^2+2))}{\log 3} = \frac{\log(|\mathcal{A}|) - \log(\tau(c(\rho))^2+2)}{\log 3},$$

from which we aim to obtain a contradiction. We then recursively define

$$\mathcal{A}_0 \overset{\text{def}}{=} \mathcal{A} \supset \mathcal{A}_1 \supset \mathcal{A}_2 \supset \cdots \supset \mathcal{A}_s$$

of sets such that

$$|\mathcal{A}_i| \geq \frac{|\mathcal{A}_{i-1}|}{3},$$

and if $u \geq c(\pi_i, \rho)$,

$$a, b \in \mathcal{A}_i,\ \pi_i^u \mid a+\rho b \quad \Rightarrow \quad \pi_i^{u-c(\pi_i,\rho)} \mid a,\ b.$$

This is easy to do, given $\mathcal{A}_0, \mathcal{A}_1, \dots, \mathcal{A}_{i-1}$. We then apply Lemma 2, with the choice $\mathcal{A} = \mathcal{A}_{i-1}$ and $\pi = \pi_i$, and the resulting set $\mathcal{B}$ gives $\mathcal{A}_i$. Then,

$$|\mathcal{A}_s| \geq \frac{|\mathcal{A}_{s-1}|}{3} \geq \frac{|\mathcal{A}_{s-2}|}{3^2} \geq \cdots \geq \frac{|\mathcal{A}_0|}{3^s} = \frac{|\mathcal{A}|}{3^s} \geq \tau(c(\rho))^2+2,$$

and for each of the primes $\pi_1, \pi_2, \dots, \pi_s$, we have that if $u \geq c(\pi_i, \rho)$,

$$a, b \in \mathcal{A}_s,\ \pi_i^u \mid a+\rho b \quad \Rightarrow \quad \pi_i^{u-c(\pi_i,\rho)} \mid a,\ b. \tag{13}$$

In the following, we denote $\Phi(a,b)$ to be the Eulerian integer defined as:

$$\Phi(a,b) = \frac{a}{\gcd(a,b)} + \rho\frac{b}{\text{gcd(a,b)}}.$$

If

$$a = \varepsilon_1 \pi_1^{\alpha_1}\pi_2^{\alpha_2}\dots\pi_s^{\alpha_s}$$

and

$$b = \varepsilon_2 \pi_1^{\beta_1}\pi_2^{\beta_2}\dots\pi_s^{\beta_s},$$

where $\varepsilon_1^6 = 1 = \varepsilon_2^6$, $\alpha_1, \alpha_2, \dots, \alpha_s, \beta_1, \beta_2, \dots, \beta_s \in \mathbb{N}\cup\{0\}$ and $\pi_1, \pi_2 \dots, \pi_s \in \mathcal{P}$, then

$$\gcd(a,b) = \pi_1^{\min\{\alpha_1,\beta_1\}}\pi_2^{\min\{\alpha_2,\beta_2\}}\dots\pi_s^{\min\{\alpha_s,\beta_s\}}.$$

We prove the following:

Lemma 3.

$$|\{\Phi(a,b):\ a,b\in\mathcal{A}_s\}|\le\tau(c(\rho)).$$

Proof of Lemma 3. For $a,b\in\mathcal{A}_s$, write $a+\rho b$ in the form

$$\begin{aligned}a+\rho b&=\varepsilon\pi_1^{\alpha_1}\cdots\pi_s^{\alpha_s}\\&=\underbrace{\left(\varepsilon\pi_1^{\min\{c(\pi_1,\rho),\alpha_1\}}\cdots\pi_s^{\min\{c(\pi_s,\rho),\alpha_s\}}\right)}_{u}\cdot\underbrace{\left(\pi_1^{\alpha_1-\min\{c(\pi_1,\rho),\alpha_1\}}\cdots\pi_s^{\alpha_s-\min\{c(\pi_s,\rho),\alpha_s\}}\right)}_{v}\\&\overset{\text{def}}{=}uv,\end{aligned}$$

where $\varepsilon^6=1$. If $\alpha_i\ge c(\pi_i,\rho)$, then, according to (13),

$$\pi_i^{\alpha_i-c(\pi_i,\rho)}\mid a,b,$$
$$\pi_i^{\alpha_i-\min\{c(\pi_i,\rho),\alpha_i\}}\mid a,b.$$

If $\alpha_i<c(\pi_i,\rho)$, then

$$\pi_i^{\alpha_i-\min\{c(\pi_i,\rho),\alpha_i\}}=1\mid a,b.$$

Since this holds for all $1\le i\le s$; thus, $v\mid a$ and $v\mid b$, so $v\mid\gcd(a,b)$. It follows that

$$\frac{a}{\gcd(a,b)}+\rho\frac{b}{\gcd(a,b)}\mid\frac{a}{v}+\rho\frac{b}{v}=u.$$

Furthermore,

$$u\mid\pi_1^{c(\pi_1,\rho)}\cdots\pi_s^{c(\pi_s,\rho)}\mid c(\rho).$$

Thus, $\Phi(a,b)\mid c(\rho)$, which completes the proof of the lemma.

From the lemma, it is clear that

$$|\{(\Phi(a,b),\Phi(b,a)):\ a,b\in\mathcal{A}_s\}|\le\tau(c(\rho))^2. \tag{14}$$

Let $t=\tau(c(\rho))^2$. Since $|\mathcal{A}_s|\ge\tau(c(\rho))^2+2=t+2$, we can select $t+2$ distinct elements from $\mathcal{A}_s$. Let a denote the first of these elements, and let $b_1,b_2,\dots,b_{t+1}$ denote the others. By (14),

$$|\{(\Phi(a,b_i),\Phi(b_i,a)):1\le s\le t+1\}|\le\tau(c(\rho))^2=t.$$

By the pigeonhole principle, there exist different i and j such that

$$(\Phi(a,b_i),\Phi(b_i,a))=(\Phi(a,b_j),\Phi(b_j,a)).$$

Let

$$\Phi(a,b_i)=\Phi(a,b_j)=z_1$$

and

$$\Phi(b_i,a)=\Phi(b_j,a)=z_2.$$

The pairs $\frac{a}{\gcd(a,b_i)}$, $\frac{b_i}{\gcd(a,b_i)}$ and $\frac{a}{\gcd(a,b_j)}$, $\frac{b_j}{\gcd(a,b_j)}$ are the solutions of the same system of two linear equations (with two unknowns)

$$x+\rho y=z_1$$
$$\rho x+y=z_2.$$

Since $\det\begin{bmatrix}1&\rho\\ \rho&1\end{bmatrix}\neq 0$, the above system of equations has an unique solution, i.e.

$$\frac{a}{\gcd(a,b_i)}=\frac{a}{\gcd(a,b_j)} \tag{15}$$

$$\frac{b_i}{\gcd(a,b_i)}=\frac{b_j}{\gcd(a,b_j)} \tag{16}$$

From (15), it follows that gcd $(a,b_i)=$ gcd (a,b_j), and by substituting this into (16) we obtain, $b_i=b_j$, which is a contradiction. This proves the theorem in Case 1.

Case 2: There is an Euler prime $\theta\in\mathcal{P}$ with argument $[0°,60°)$ and a positive integer γ such that $\rho=-\theta^\gamma$.

Lemma 2 of the proof of the previous part and the notation $c(\pi,\rho)$ for Euler primes with argument $[0°,60°)$ that are not θ, can still be applied, in which case $\rho=\rho_0$ and $1+\rho_0=\pi^\delta\sigma$. Consequently, if $\mathcal{A}\subset E$ is a finite set and π is an Euler prime with argument in the interval $[0°,60°)$, which is different from θ, there exists a set $\mathcal{B}\subset\mathcal{A}$ for which $|\mathcal{B}|\geq\frac{|\mathcal{A}|}{3}$, such that for every integer $u\geq c(\pi,\rho)$ and $a,b\in\mathcal{B}$, $\pi^u\mid a+\rho b \quad\Rightarrow\quad \pi^{u-c(\pi,\rho)}\mid a,\ b$. The proof proceeds similarly. Finally, we can divide the set by θ as follows:

Lemma 4. *Let $\theta\in\mathcal{P}$ be an Euler prime with argument in the interval $[0°,60°)$ and let γ be a positive integer such that $\rho=-\theta^\gamma$. Then, if $\mathcal{A}\subset E$ is a finite set, there exists a subset $\mathcal{B}\subset\mathcal{A}$ such that $|\mathcal{B}|\geq\frac{|\mathcal{A}|}{2}$, and if $a,b\in\mathcal{B}$, $a\neq b$, then $\theta^k\mid a+\rho b=a-\theta^\gamma b$ implies $\theta^{k-\gamma}\mid a,b$.*

Proof of Lemma 4. We begin by writing the elements of the set $\mathcal{A}$ in the form $\theta^\alpha a_0$, where $\theta \nmid a_0$, $0 \le \alpha \in \mathbb{Z}$ and $a_0 \in E$. We then partition $\mathcal{A}$ into two subsets:

$$\mathcal{A}_1 = \{\theta^\alpha a_0 = a \in \mathcal{A} : \ \theta \nmid a_0, \ \left[\frac{\alpha}{2\gamma}\right] \equiv 0 \pmod 2\}$$

and

$$\mathcal{A}_2 = \{\theta^\alpha a_0 = a \in \mathcal{A} : \ \theta \nmid b_0, \ \left[\frac{\alpha}{2\gamma}\right] \equiv 1 \pmod 2\}.$$

Here, 0 can be arbitrarily partitioned into either of the two sets. Let $\mathcal{B}$ be the larger of $\mathcal{A}_1$ and $\mathcal{A}_2$ (or either one if they have the same cardinality). Consider any two distinct elements $a, b \in \mathcal{B}$. If these elements are written in the form $a = \theta^{\alpha_a} a_0$ and $b = \theta^{\alpha_b} b_0$, the absolute difference of their exponents, $|\alpha_a - \alpha_b|$, cannot be γ. Thus, in the case of $a, b \in \mathcal{B}$, $(a \ne b)$, the highest exponent of θ that divides the numbers a and ρb $(= -\theta^\gamma b)$ must be different. Thus, in the case of $\theta^k \mid a + \rho b = a - \theta^\gamma b$, $\theta^k \mid a, \rho b$, so $\theta^{k-\gamma} \mid a, b$. This completes the proof of Lemma 4.

Now we consider the case when $-\rho = \theta^\gamma$, where $0 < \gamma \in \mathbb{Z}$ and $\theta \in \mathcal{P}$. Let

$$c(\theta, \rho) \stackrel{\text{def}}{=} \gamma,$$

and let

$$c(\rho) \stackrel{\text{def}}{=} \prod_{\substack{\pi \mid \rho(1+\rho) \\ \operatorname{Arg}(\pi) \in [0°, 60°)}} \pi^{c(\pi,\rho)}.$$

(Here the product runs on the prime divisors of $\rho(1+\rho)$, where the prime divisors in this case also include θ.)

Then the method used in Case 1 will also be applicable: Let us list the Euler prime divisors of $\prod_{\substack{a,b \in \mathcal{A} \\ a \ne b}} (a + \rho b)$ whose arguments lie in the interval $[0°, 60°)$: $\pi_1, \pi_2, \dots, \pi_s$. Suppose that

$$s \le \frac{\log(|\mathcal{A}|/(\tau(c(\rho))^2 + 2))}{\log 3} = \frac{\log(|\mathcal{A}|) - \log(\tau(c(\rho))^2 + 2)}{\log 3},$$

Our aim is to derive a contradiction from this assumption.

We then recursively define a sequence of sets

$$\mathcal{A}_0 \stackrel{\text{def}}{=} \mathcal{A} \supset \mathcal{A}_1 \supset \mathcal{A}_2 \supset \cdots \supset \mathcal{A}_s$$

for which

$$|\mathcal{A}_i| \ge \frac{|\mathcal{A}_{i-1}|}{3},$$

and if $u \geq c(\pi_i, \rho)$,

$$a, b \in \mathcal{A}_i,\ \pi_i^u \mid a + \rho b \quad \Rightarrow \quad \pi_i^{u-c(\pi_i,\rho)} \mid a,\ b.$$

This is easy to do, since, given $\mathcal{A}_0, \mathcal{A}_1, \dots, \mathcal{A}_{i-1}$, we can apply Lemma 2 or Lemma 4. $\mathcal{A} = \mathcal{A}_{i-1}$ and $\pi = \pi_i$. We use Lemma 4 exactly when $-\rho$ is a power of π with a positive integer exponent, and the resulting set $\mathcal{B}$ gives $\mathcal{A}_i$. Instead of the halving obtained in Lemma 4, we can also third the set there. Then,

$$|\mathcal{A}_s| \geq \frac{|\mathcal{A}_{s-1}|}{3} \geq \frac{|\mathcal{A}_{s-2}|}{3^2} \geq \dots \geq \frac{|\mathcal{A}_0|}{3^s} = \frac{|\mathcal{A}|}{3^s} \geq \tau(c(\rho))^2 + 2,$$

and for each of the primes $\pi_1, \pi_2, \dots, \pi_s$, the following holds: if $u \geq c(\pi_i, \rho)$,

$$a, b \in \mathcal{A}_s,\ \pi_i^u \mid a + \rho b \quad \Rightarrow \quad \pi_i^{u-c(\pi_i,\rho)} \mid a,\ b. \tag{17}$$

In the following, let $\Phi(a, b)$ be the Eulerian integer defined as:

$$\Phi(a, b) = \frac{a}{\gcd(a, b)} + \rho \frac{b}{\mathrm{gcd(a,b)}}.$$

Similarly to Lemma 3,

$$|\{\Phi(a, b) :\ a, b \in \mathcal{A}_s\}| \leq \tau(c(\rho))$$

now holds with the same reasoning.

From this, it is clear that

$$|\{(\Phi(a, b), \Phi(b, a)) :\ a, b \in \mathcal{A}_s\}| \leq \tau(c(\rho))^2. \tag{18}$$

Then, let $t = \tau(c(\rho))^2$. Since $|\mathcal{A}_s| \geq \tau(c(\rho))^2 + 2 = t + 2$, we can select $t + 2$ distinct elements from $\mathcal{A}_s$. We denote the first element by a, and the others by $b_1, b_2, \dots, b_{t+1}$. Then, by (18),

$$|\{(\Phi(a, b_i), \Phi(b_i, a)) : 1 \leq s \leq t + 1\}| \leq \tau(c(\rho))^2 = t.$$

Thus, by the pigeonhole principle, there exist distinct i and j such that

$$(\Phi(a, b_i), \Phi(b_i, a)) = (\Phi(a, b_j), \Phi(b_j, a)).$$

Let

$$\Phi(a, b_i) = \Phi(a, b_j) = z_1$$

and

$$\Phi(b_i, a) = \Phi(b_j, a) = z_2.$$

Then, $\frac{a}{\gcd(a,b_i)}$, $\frac{b_i}{\gcd(a,b_i)}$ and $\frac{a}{\gcd(a,b_j)}$, $\frac{b_j}{\gcd(a,b_j)}$ are the solutions of the same system of linear equations with two unknowns

$$x + \rho y = z_1$$

$$\rho x + y = z_2.$$

Since $\det \begin{bmatrix} 1 & \rho \\ \rho & 1 \end{bmatrix} \neq 0$, the above system of linear equations has an unique solution, i.e.,

$$\frac{a}{\gcd(a,b_i)} = \frac{a}{\gcd(a,b_j)} \tag{19}$$

$$\frac{b_i}{\gcd(a,b_i)} = \frac{b_j}{\gcd(a,b_j)} \tag{20}$$

Then, by (19), $\gcd(a,b_i) = \gcd(a,b_j)$, but then, by (20), $b_i = b_j$, which is a contradiction. Our result now follows.

Proof of Corollary 1. Since $\omega = \frac{-1+\sqrt{3}i}{2}$ is a root of unity in the ring of Eulerian integers E, we use the notation corresponding to the proof of Case 1 of Theorem 2: $c(\omega) = 1$ and $\tau(c(\omega)) = 6$. Thus, the lower bound on the number of distinct Eulerian prime factors (ω_E) follows directly from the proof of Theorem 2:

$$\omega_E\left(\prod_{\substack{a,b\in\mathcal{A}\\ a\neq b}}(a+\omega b)\right) > \frac{\log|\mathcal{A}| - \log(\tau(c(\omega))^2+2)}{\log 3} = \frac{\log|\mathcal{A}| - \log 38}{\log 3}.$$

We connect this result to the rational prime factors by observing that the product $\prod(a^2 - ab + b^2)$ is the norm of the product $\prod(a+\omega b)$:

$$\prod_{\substack{a,b\in\mathcal{A}\\ a\neq b}}(a^2-ab+b^2) = N\left(\prod_{\substack{a,b\in\mathcal{A}\\ a\neq b}}(a+\omega b)\right) = \prod_{\substack{a,b\in\mathcal{A}\\ a\neq b}}(a+\omega b)(a+\omega^2 b).$$

For any rational prime p, the product p factors in E into at most two distinct conjugate Eulerian primes. Thus, the number of distinct rational prime factors, $\omega_{\mathbb{N}}$, of the product is at least half the number of distinct Eulerian prime factors ω_E.

Therefore, this implies:

$$\omega_{\mathbb{N}}\left(\prod_{\substack{a,b\in\mathcal{A}\\ a\neq b}}(a^2-ab+b^2)\right) > \frac{1}{2}\left(\frac{\log|\mathcal{A}| - \log 38}{\log 3}\right),$$

which is the required result.

Proof of Corollary 2. This proof is similar to the proof of Corollary 1. Since $-\omega$ is an Eulerian integer that is a root of unity and $-\omega+1 = \frac{3-\sqrt{3}i}{2} = \sqrt{3}i(\frac{-1-\sqrt{3}i}{2})$ is an Euler prime, with the notation corresponding to the proof of Case 1 of Theorem 2, $c(-\omega) = -\sqrt{3}i\omega$ and $\tau(c(-\omega)) = \tau(-\sqrt{3}i\omega) = 12$.

Thus, the lower bound on the number of distinct Euler prime factors (ω_E) follows directly from the proof of Theorem 2 (with $\rho = -\omega$):

$$\omega_E\left(\prod_{\substack{a,b\in\mathcal{A}\\ a\neq b}}(a-\omega b)\right) > \frac{\log|\mathcal{A}| - \log(\tau(c(-\omega))^2+2)}{\log 3} = \frac{\log|\mathcal{A}| - \log 146}{\log 3}.$$

We relate this result to the rational prime factors by noting that the product $\prod(a^2+ab+b^2)$ is the norm of the product $\prod(a-\omega b)$:

$$\prod_{\substack{a,b\in\mathcal{A}\\ a\neq b}}(a^2+ab+b^2) = N\left(\prod_{\substack{a,b\in\mathcal{A}\\ a\neq b}}(a-\omega b)\right) = \prod_{\substack{a,b\in\mathcal{A}\\ a\neq b}}(a-\omega b)(a-\omega^2 b).$$

The number of distinct rational prime factors, $\omega_{\mathbb{N}}$, of the rational product $\prod(a^2+ab+b^2)$ is related to the number of distinct Euler prime factors ω_E. Since any rational prime p is the product of at most two distinct conjugate Euler prime factors, we have $\omega_{\mathbb{N}} \geq \omega_E/2$. This implies:

$$\omega_{\mathbb{N}}\left(\prod_{\substack{a,b\in\mathcal{A}\\ a\neq b}}(a^2+ab+b^2)\right) > \frac{1}{2}\left(\frac{\log|\mathcal{A}| - \log 146}{\log 3}\right),$$

which yields the required result.

Proof of Theorem 3. Let $n \geq 2$ be an integer. We define the sets $\mathcal{A}'$ and $\mathcal{B}'$ in $\mathbb{Z}^n$ for the elements of the sets $\mathcal{A}$ and $\mathcal{B}$:

$$\mathcal{A}' = \{(r_1x^{m_1}, r_2x^{m_2}, \dots, r_{n-1}x^{m_{n-1}}, 1) : x \in \mathcal{A}\}$$

$$\mathcal{B}' = \{(1, y, y^2, \dots, y^{n-2}, r_ny^{n-1}) : y \in \mathcal{B}\}$$

Since $|\mathcal{A}| \geq |\mathcal{B}|$, we have $|\mathcal{A}'| \geq |\mathcal{B}'| \geq 2n-2$.

The following theorem is included in the paper of Győry, Sárközy, and Stewart [4]:

Theorem D. [Győry-Sárközy-Stewart] *Let $n \geq 2$ be an integer, and let $\mathcal{A}, \mathcal{B} \subset (\mathbb{Z}^+)^n$ be finite sets such that $|\mathcal{A}| \geq |\mathcal{B}| \geq 2n-2$. If for every vector in $\mathcal{A}$ the n-th coordinate is 1, and any n vectors in $\mathcal{B} \cup \{(0,\ldots,0,1)\}$ are linearly independent, then there exists an effectively computable positive constant c for which*

$$\omega_{\mathbb{N}}\left(\prod_{\substack{(a_1,\ldots,a_n)\in\mathcal{A}\\(b_1,\ldots,b_n)\in\mathcal{B}}}(a_1b_1+a_2b_2+\cdots+a_nb_n)\right) > c\log|\mathcal{A}|.$$

To ensure we can apply Theorem D, we must verify that its conditions hold for our sets $\mathcal{A}'$ and $\mathcal{B}'$.

1. The n-th coordinate of every vector in $\mathcal{A}'$ is 1.

2. We show that any n distinct vectors from $\mathcal{B}' \cup \{(0,\ldots,0,1)\}$ are linearly independent.

Condition 1 is immediate. We proceed to prove Condition 2.

Case 1: All n vectors are from $\mathcal{B}'$. Let the vectors correspond to $y_1, y_2, \ldots, y_n \in \mathcal{B}$. The determinant of the matrix formed by these vectors is proportional to a Vandermonde determinant:

$$\begin{vmatrix} 1 & 1 & \ldots & 1 \\ y_1 & y_2 & \ldots & y_n \\ \ldots & \ldots & \ldots & \ldots \\ y_1^{n-2} & y_2^{n-2} & \ldots & y_n^{n-2} \\ r_ny_1^{n-1} & r_ny_2^{n-1} & \ldots & r_ny_n^{n-1} \end{vmatrix} = r_n \cdot \prod_{1\leq i<j\leq n}(y_j-y_i) \neq 0.$$

Since the elements y_i are distinct and $r_n \neq 0$, the determinant is non-zero, proving linear independence.

Case 2: One vector is $(0,\ldots,0,1)$. Let the $n-1$ vectors correspond to $y_1, y_2, \ldots, y_{n-1} \in \mathcal{B}$, and the n-th vector be $\mathbf{e}_n = (0,\ldots,0,1)$. The determinant of the matrix formed by these vectors is found by cofactor expansion along the last column:

$$\begin{vmatrix} 1 & 1 & \dots & 1 & 0 \\ y_1 & y_2 & \dots & y_{n-1} & 0 \\ \dots & \dots & \dots & \dots & \dots \\ y_1^{n-2} & y_2^{n-2} & \dots & y_{n-1}^{n-2} & 0 \\ r_n y_1^{n-1} & r_n y_2^{n-1} & \dots & r_n y_{n-1}^{n-1} & 1 \end{vmatrix} = 1 \cdot \begin{vmatrix} 1 & 1 & \dots & 1 \\ y_1 & y_2 & \dots & y_{n-1} \\ \dots & \dots & \dots & \dots \\ y_1^{n-2} & y_2^{n-2} & \dots & y_{n-1}^{n-2} \end{vmatrix} \neq 0.$$

The resulting subdeterminant is a non-zero Vandermonde determinant since y_i are distinct. Thus, the vectors are linearly independent.

Since the assumptions are met, we apply Theorem D to the sets $\mathcal{A}'$ and $\mathcal{B}'$:

$$\omega_{\mathbb{N}}\left(\prod_{\substack{\mathbf{a}\in\mathcal{A}'\\ \mathbf{b}\in\mathcal{B}'}} \mathbf{a}\cdot\mathbf{b}\right) > c\log|\mathcal{A}'| = c\log|\mathcal{A}|,$$

where the inner product $\mathbf{a}\cdot\mathbf{b}$ yields:

$$\begin{aligned} \mathbf{a}\cdot\mathbf{b} &= (r_1x^{m_1})(1) + (r_2x^{m_2})(y) + \cdots + (r_{n-1}x^{m_{n-1}})(y^{n-2}) + (1)(r_ny^{n-1}) \\ &= r_1x^{m_1} + r_2x^{m_2}y + \cdots + r_{n-1}x^{m_{n-1}}y^{n-2} + r_ny^{n-1} = f(x,y). \end{aligned}$$

Thus,

$$\omega_{\mathbb{N}}\left(\prod_{x\in\mathcal{A},y\in\mathcal{B}} f(x,y)\right) > c\log|\mathcal{A}|$$

for an effectively computable positive constant c, as required.

References

[1] P. Erdős, C. L. Stewart and R. Tijdeman, *Some diophantine equations with many solutions*, Compos. Math. 66(1) (1988), 37-56.

[2] P. Erdős and J. Surányi, *Topics in the Theory of Numbers*, Springer US, New York, N.Y., 2003.

[3] P. Erdős and P. Turán, *On a problem in the elementary theory of numbers*, Am. Math. Mon. 41 (1934), 608-611.

[4] K. Győry, A. Sárközy and C. L. Stewart, *On the number of prime factors of integers of the form* $ab+1$, Acta Arith. 74 (1996), 365-385.

[5] K. Győry, C. L. Stewart and R. Tijdeman, *On prime factors of sums of integers. I.*, Compos. Math. 59, 81-88 (1986).