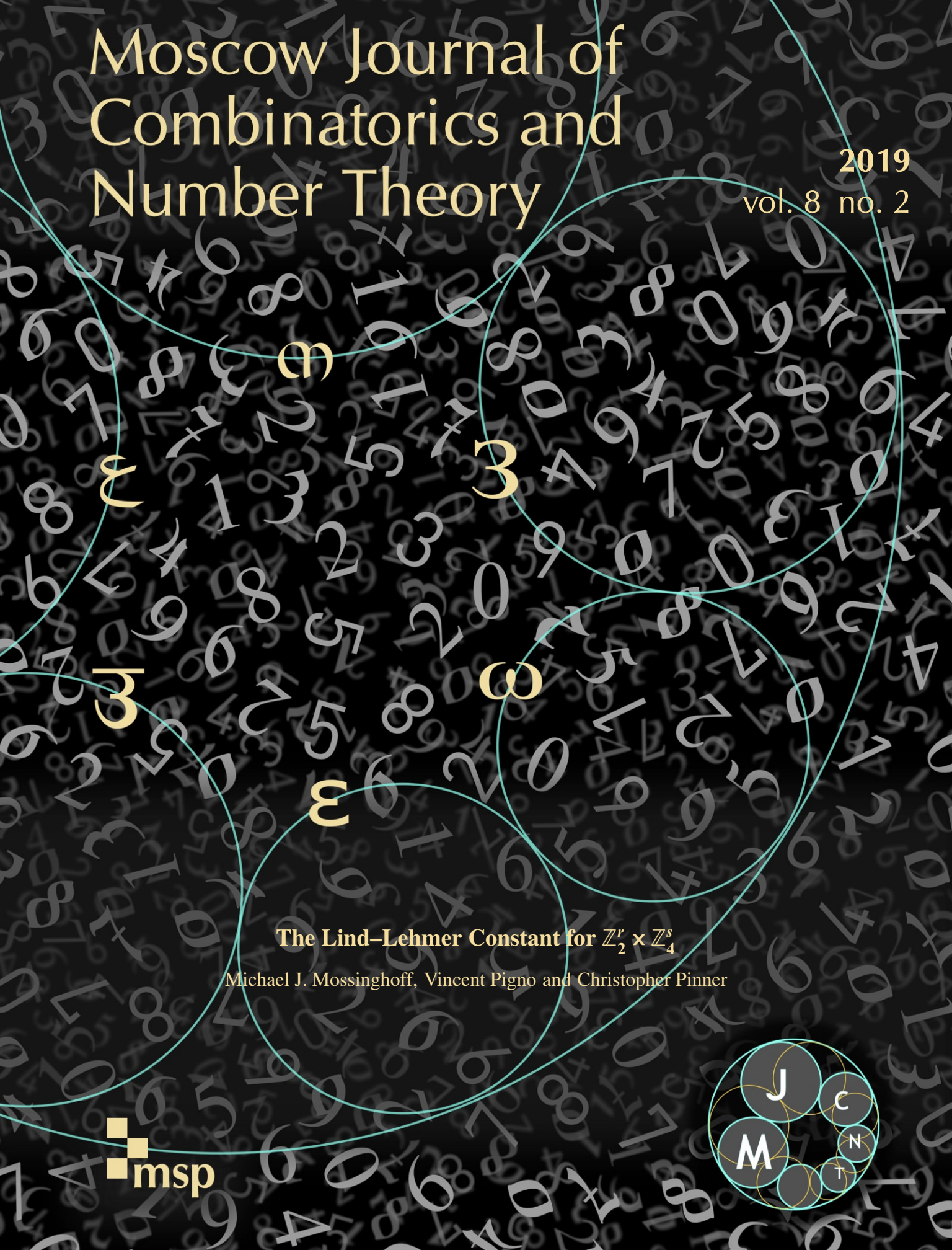
Moscow Journal of Combinatorics and Number Theory

2019
vol. 8 no. 2



The Lind–Lehmer Constant for $\mathbb{Z}_2^r \times \mathbb{Z}_4^s$

Michael J. Mossinghoff, Vincent Pigno and Christopher Pinner

msp

msp

Moscow Journal of Combinatorics and Number Theory
Vol. 8, No. 2, 2019
dx.doi.org/10.2140/moscow.2019.8.151

The Lind–Lehmer Constant for $\mathbb{Z}_2^r \times \mathbb{Z}_4^s$

Michael J. Mossinghoff, Vincent Pigno and Christopher Pinner

For a finite abelian group the Lind–Lehmer constant is the minimum positive logarithmic Lind–Mahler measure for that group. Finding this is equivalent to determining the minimal nontrivial group determinant when the matrix entries are integers.

For a group of the form $G = \mathbb{Z}_2^r \times \mathbb{Z}_4^s$ with $|G| \geq 4$ we show that this minimum is always $|G| - 1$, a case of sharpness in the trivial bound. For $G = \mathbb{Z}_2 \times \mathbb{Z}_{2^n}$ with $n \geq 3$ the minimum is 9, and for $G = \mathbb{Z}_3 \times \mathbb{Z}_{3^n}$ the minimum is 8. Previously the minimum was only known for 2- and 3-groups of the form $G = \mathbb{Z}_p^k$ or $\mathbb{Z}_{p^k}$. We also show that a congruence satisfied by the group determinant when $G = \mathbb{Z}_p^r$ generalizes to other abelian p-groups.

1. Introduction

Recall that for a polynomial $F(x_1, \ldots, x_k)$ in $\mathbb{Z}[x_1, \ldots, x_k]$, one defines the traditional logarithmic Mahler measure by

$$m(F) = \int_0^1 \cdots \int_0^1 \log |F(e^{2\pi i x_1}, \ldots, e^{2\pi i x_k})| \, dx_1 \cdots dx_k.$$

Lind [2005] viewed $[0, 1]^k$ as the group $(\mathbb{R}/\mathbb{Z})^k$ and generalized the Mahler measure to arbitrary compact abelian groups. In particular, for the finite abelian group

$$G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \tag{1}$$

and $F \in \mathbb{Z}[x_1, \ldots, x_k]$, we define the *logarithmic Lind–Mahler measure* by

$$m_G(F) = \frac{1}{|G|} \sum_{x_1=1}^{n_1} \cdots \sum_{x_k=1}^{n_k} \log |F(e^{2\pi i x_1/n_1}, \ldots, e^{2\pi i x_k/n_k})|.$$

Writing

$$w_n := e^{2\pi i/n},$$

we plainly have

$$m_G(F) = \frac{1}{|G|} \log |M_G(F)|,$$

This work was supported in part by a grant from the Simons Foundation (#426694 to Mossinghoff).
MSC2010: primary 11R06; secondary 11B83, 11C08, 11G50, 11T22, 43A40.
Keywords: Lind–Lehmer constant, Mahler measure, group determinant.

where

$$M_G(F) := \prod_{j_1=1}^{n_1} \cdots \prod_{j_k=1}^{n_k} F(w_{n_1}^{j_1}, \ldots, w_{n_k}^{j_k}) \in \mathbb{Z}.$$

The close connection of the Lind–Mahler measure to the group determinant was explored by Vipismakul [2013]. Recall that for a finite group $G = \{g_1, \ldots, g_N\}$ one assigns a variable x_g for each g in G and defines the group determinant, $\mathscr{D}_G(x_{g_1}, \ldots, x_{g_N})$, to be the determinant of the $N \times N$ matrix whose ij-th entry is $x_{g_i g_j^{-1}}$, a homogeneous polynomial of degree N in the x_g. From Dedekind's factorization of the group determinant of an abelian group in terms of the group characters [Dedekind 1968, pp. 420–421] (see also [Lang 1978, p. 89], or the historical survey [Conrad 1998]), it is readily seen that for a group of the form (1) we have

$$\mathscr{D}_G(a_{g_1}, \ldots, a_{g_N}) = M_G(F), \quad F(x_1, \ldots, x_k) := \sum_{g=(m_1,\ldots,m_k)\in G} a_g\, x_1^{m_1} \cdots x_k^{m_k}. \tag{2}$$

Analogous to the classical Lehmer problem [1933], we can ask for the minimal positive $m_G(F)$, and to this end we define the *Lind–Lehmer constant* for G by

$$\lambda(G) := \min\{|M_G(F)| > 1 : F \in \mathbb{Z}[x_1, \ldots, x_k]\}.$$

We use $|M_G(F)|$ rather than $m_G(F)$ or $|M_G(F)|^{1/|G|}$ so that we are dealing with integers; of course the minimal positive logarithmic measure will be $(1/|G|)\log\lambda(G)$. As Lind observed, for $|G| \geq 3$ we always have the trivial bound

$$\lambda(G) \leq |G| - 1, \tag{3}$$

achieved, for example, by

$$F(x_1, \ldots, x_k) = -1 + \prod_{i=1}^{k} \left(\frac{{x_i}^{n_i} - 1}{x_i - 1} \right).$$

Lind also showed that for prime powers p^α with $\alpha \geq 1$ we have

$$\lambda(\mathbb{Z}_{p^\alpha}) = \begin{cases} 3 & \text{if } p = 2, \\ 2 & \text{if } p \geq 3, \end{cases} \tag{4}$$

achieved with $x^2 + x + 1$ if $p = 2$ and $x + 1$ if $p \geq 3$. Lind's results for cyclic groups were extended by Kaiblinger [2010] and Pigno and Pinner [2014] so that $\lambda(\mathbb{Z}_m)$ is now known if $892\,371\,480 \nmid m$. The value for the p-group $\mathbb{Z}_p^k$ was recently established by De Silva and Pinner [2014], but little is known for direct products involving at least one term $\mathbb{Z}_{p^\alpha}$ with $\alpha \geq 2$.

Here we are principally interested in the case of 2-groups

$$G = \mathbb{Z}_{2^{\alpha_1}} \times \cdots \times \mathbb{Z}_{2^{\alpha_k}}. \tag{5}$$

It was shown in [DeSilva and Pinner 2014] that for all $k \geq 2$

$$\lambda(\mathbb{Z}_2^k) = 2^k - 1, \tag{6}$$

a case of equality in (3). We establish two main results regarding the Lind–Lehmer constant for groups of the form (5). First, we prove that equality occurs in (3) whenever G is a 2-group whose factors are all $\mathbb{Z}_2$ or $\mathbb{Z}_4$.

Theorem 1.1. *If $G = \mathbb{Z}_2^r$ or $\mathbb{Z}_4^s$ or $\mathbb{Z}_2^r \times \mathbb{Z}_4^s$, then*

$$\lambda(G) = \max\{3, |G| - 1\}.$$

Second, we show that this is not true for all 2-groups: if we allow $\alpha_i \geq 3$ in (5) then (3) need not be sharp.

Theorem 1.2. *For $n \geq 3$*

$$\lambda(\mathbb{Z}_2 \times \mathbb{Z}_{2^n}) = 9,$$

achieved with $F(x, y) = y^2 + y + 1$.

Crucial to our proofs of these statements will be a congruence satisfied by $M_G(F)$ when G is an abelian p-group. This generalizes a result [DeSilva and Pinner 2014, Lemma 2.1] for groups of the form $G = \mathbb{Z}_p^k$; see also [Vipismakul 2013, Theorem 2.1.2].

Lemma 1.3. *If p is a prime and*

$$G = \mathbb{Z}_{p^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p^{\alpha_k}}, \tag{7}$$

then

$$M_G(F) \equiv F(1, \ldots, 1)^{|G|} \bmod p^k.$$

By the correspondence (2) this gives us a congruence satisfied by the group determinant, when the variables are integers and G is of the form (7),

$$\mathscr{D}_G(a_{g_1}, \ldots, a_{g_N}) \equiv \left(\sum_{g \in G} a_g\right)^N \bmod p^k.$$

Notice that for the p-group (7) we have

$$M_G(F) = \prod_{t_1=0}^{\alpha_1} \cdots \prod_{t_k=0}^{\alpha_k} N_{t_1,\ldots,t_k}(F),$$

where

$$N_{t_1,\ldots,t_k}(F) = \prod_{\substack{j_1=1 \\ (j_1, p^{\alpha_1}) = p^{t_1}}}^{p^{\alpha_1}} \cdots \prod_{\substack{j_k=1 \\ (j_k, p^{\alpha_k}) = p^{t_k}}}^{p^{\alpha_k}} F(w_{p^{\alpha_1}}^{j_1}, \ldots, w_{p^{\alpha_k}}^{j_k}) \in \mathbb{Z}.$$

Since $|1 - w_{p^\alpha}^j|_p < 1$ and the $N_{t_1,\ldots,t_k}(F)$ are integers, we have

$$N_{t_1,\ldots,t_k}(F) \equiv F(1, \ldots, 1)^{\varphi(p^{\alpha_1 - t_1}) \cdots \varphi(p^{\alpha_k - t_k})} \bmod p. \tag{8}$$

In particular if $p \mid F(1, \ldots, 1)$ we have $p \mid N_{t_1,\ldots,t_k}(F)$ for all t_i and $|G| p^k \mid M_G(F)$. So, in view of (3), we can assume for the p-group (7) that $p \nmid F(1, \ldots, 1)$ for any F achieving $\lambda(G)$.

Thus, in the case of 2-groups we can assume an F with minimal measure has $F(1,\dots,1)$ odd, and by Lemma 1.3 we see that

$$M_G(F) \equiv 1 \bmod 2^k. \tag{9}$$

Note this immediately produces (6).

Similarly for 3-groups we can assume that an F with minimal measure has $3 \nmid F(1,\dots,1)$ and $M_G(F) \equiv \pm 1 \bmod 3^k$. This produces another case of equality in (3):

$$\lambda(\mathbb{Z}_3^k) = 3^k - 1,$$

as observed in [DeSilva and Pinner 2014]. For $G = \mathbb{Z}_3 \times \mathbb{Z}_{3^n}$, we have $M_G(F) \equiv \pm 1 \bmod 9$ and so we immediately obtain the minimal measure for an additional family of 3-groups.

Theorem 1.4. *For $n \ge 1$*

$$\lambda(\mathbb{Z}_3 \times \mathbb{Z}_{3^n}) = 8,$$

achieved with $F(x, y) = y + 1$.

Section 2 of this article is devoted to the proof of Lemma 1.3, Section 3 establishes Theorem 1.1, and Section 4 proves Theorem 1.2.

2. Proof of Lemma 1.3

We proceed by induction on $\alpha_1 + \cdots + \alpha_k$. If $G = \mathbb{Z}_p$ then, as in (8), we can just use that $|w_p - 1|_p = p^{-1/(p-1)} < 1$; since $M_G(F) \in \mathbb{Z}$ and $M_G(F) \equiv F(1)^p \bmod (1 - w_p)$ we see that $M_G(F) \equiv F(1)^p \bmod p$.

Set

$$g(x_1,\dots,x_k) = \prod_{l_1=1}^{p^{\alpha_1}} \cdots \prod_{l_k=1}^{p^{\alpha_k}} F(x_1^{l_1},\dots,x_k^{l_k})$$

and let I be the ideal in $\mathbb{Z}[x_1,\dots,x_n]$ generated by $x_1^{p^{\alpha_1}} - 1, \dots, x_k^{p^{\alpha_k}} - 1$. Expanding, we have

$$g(x_1,\dots,x_k) = \sum_{0 \le \ell_1 < p^{\alpha_1}} \cdots \sum_{0 \le \ell_k < p^{\alpha_k}} a(\ell_1,\dots,\ell_k)\, x_1^{\ell_1} \cdots x_k^{\ell_k} \bmod I.$$

We set

$$\begin{aligned} S &:= \sum_{j_1=1}^{p^{\alpha_1}} \cdots \sum_{j_k=1}^{p^{\alpha_k}} g(w_{p^{\alpha_1}}^{j_1},\dots,w_{p^{\alpha_k}}^{j_k}) \\ &= \sum_{0 \le \ell_1 < p^{\alpha_1}} \cdots \sum_{0 \le \ell_k < p^{\alpha_k}} a(\ell_1,\dots,\ell_k) \sum_{j_1=1}^{p^{\alpha_1}} \cdots \sum_{j_k=1}^{p^{\alpha_k}} w_{p^{\alpha_1}}^{j_1\ell_1} \cdots w_{p^{\alpha_k}}^{j_k\ell_k} \\ &= a(0,\dots,0)\, p^{\alpha_1+\cdots+\alpha_k}. \end{aligned}$$

If $(j_1, p^{\alpha_1}) = \cdots = (j_k, p^{\alpha_k}) = 1$, then for these $\varphi(p^{\alpha_1}) \cdots \varphi(p^{\alpha_k})$ values we have

$$g(w_{p^{\alpha_1}}^{j_1},\dots,w_{p^{\alpha_k}}^{j_k}) = M_G(F).$$

Suppose that $(j_1, p^{\alpha_1}) = p^{t_1}, \ldots, (j_k, p^{\alpha_k}) = p^{t_k}$ with at least one $t_j \neq 0$, and with $t_i = \alpha_i$ for exactly $L \geq 0$ of the t_i. Suppose without loss of generality that $t_i = \alpha_i$ for any $i = 1, \ldots, L$ and $t_i < \alpha_i$ for any $i = L+1, \ldots, k$. For these $\varphi(p^{\alpha_{L+1}-t_{L+1}}) \cdots \varphi(p^{\alpha_k - t_k})$ values, applying the induction hypothesis to $G' = \mathbb{Z}_{p^{\alpha_{L+1}-t_{L+1}}} \times \cdots \times \mathbb{Z}_{p^{\alpha_k - t_k}}$, we have

$$\begin{aligned} g(w_{p^{\alpha_1}}^{j_1}, \ldots, w_{p^{\alpha_k}}^{j_k}) &= M_{G'}(F(1, \ldots, 1, x_{L+1}, \ldots, x_k))^{p^{t_1+\cdots+t_k}} \\ &= (F(1, \ldots, 1)^{p^{(\alpha_{L+1}-t_{L+1})+\cdots+(\alpha_k-t_k)}} + hp^{k-L})^{p^{t_1+\cdots+t_k}} \\ &\equiv F(1, \ldots, 1)^{|G|} \bmod p^{k-L+\alpha_1+\cdots+\alpha_L+t_{L+1}+\cdots+t_k}. \end{aligned}$$

Hence these $(p-1)^{k-L} p^{(\alpha_{L+1}-t_{L+1}-1)+\cdots+(\alpha_k-t_k-1)}$ terms contribute

$$\varphi(p^{\alpha_{L+1}-t_{L+1}}) \cdots \varphi(p^{\alpha_k - t_k}) F(1, \ldots, 1)^{|G|} \bmod p^{\alpha_1+\cdots+\alpha_k}$$

to S. Thus

$$\begin{aligned} 0 &\equiv \varphi(p^{\alpha_1}) \cdots \varphi(p^{\alpha_k}) M_G(F) + (p^{\alpha_1+\cdots+\alpha_k} - \varphi(p^{\alpha_1}) \cdots \varphi(p^{\alpha_k})) F(1, \ldots, 1)^{|G|} \\ &\equiv (p-1)^k p^{\alpha_1+\cdots+\alpha_k-k} (M_G(F) - F(1, \ldots, 1)^{|G|}) \bmod p^{\alpha_1+\cdots+\alpha_k} \end{aligned}$$

and the statement follows. □

3. Proof of Theorem 1.1

To prove Theorem 1.1, we require the following lemma.

Lemma 3.1. *Suppose that $F \in \mathbb{Z}[x_1, \ldots, x_n]$, and let I denote the ideal of $\mathbb{Z}[x_1, \ldots, x_n]$ generated by $x_1^{n_1} - 1, \ldots, x_k^{n_k} - 1$. Then $F(w_{n_1}^{j_1}, \ldots, w_{n_k}^{j_k}) = 0$ for all $1 \leq j_i \leq n_i$ if and only if $F \in I$.*

Proof. Plainly any F in I will have $F(w_{n_1}^{j_1}, \ldots, w_{n_k}^{j_k}) = 0$ for all $0 \leq j_i < n_i$. Conversely, suppose that $F(w_{n_1}^{j_1}, \ldots, w_{n_k}^{j_k}) = 0$ for all $0 \leq j_i < n_i$. Clearly any F can be reduced mod I to a polynomial of degree less than n_i in each x_i:

$$F(x_1, \ldots, x_k) = \sum_{t_1=0}^{n_1-1} \cdots \sum_{t_k=0}^{n_k-1} a(t_1, \ldots, t_k)\, x_1^{t_1} \cdots x_k^{t_k} \bmod I.$$

Since $\sum_{j_i=0}^{n_i-1} w_{n_i}^{(t_i-T_i)j_i} = 0$ if $t_i \not\equiv T_i \bmod n_i$ (and n_i otherwise) we have

$$a(T_1, \ldots, T_k) = \frac{1}{n_1 \cdots n_k} \sum_{j_1=0}^{n_1-1} \cdots \sum_{j_k=0}^{n_k-1} F(w_{n_1}^{j_1}, \ldots, w_{n_k}^{j_k})\, w_{n_1}^{-T_1 j_1} \cdots w_{n_k}^{-T_k j_k}.$$

So $a(T_1, \ldots, T_k) = 0$ for all $0 \leq T_i < n_i$ and $F = 0 \bmod I$. □

We now proceed to the proof of our first principal result.

Proof of Theorem 1.1. Suppose that $G = \mathbb{Z}_{2^{\alpha_1}} \times \cdots \times \mathbb{Z}_{2^{\alpha_k}}$ with $2^{\alpha_i} = 4$ for $1 \leq i \leq s$ and $2^{\alpha_i} = 2$ for $s+1 \leq i \leq k$. We write $r = k - s$. In view of (4) and (6) we may assume that $k \geq 2$ and $s \geq 1$. Suppose that $F(x_1, \ldots, x_k)$ has

$$1 < |M_G(F)| < |G| - 1 = 2^{k+s} - 1,$$

where

$$M_G(F) = \prod_{\substack{u_1,\dots,u_s=\pm 1,\pm i\\ u_{s+1},\dots,u_k=\pm 1}} F(u_1,\dots,u_k). \tag{10}$$

Suppose that one of the nonunits $F(u_1,\dots,u_k)$ in the product (10) has at least one of its u_j complex, say $u_1 = \pm i$, and set $G' = \mathbb{Z}_{2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{2^{\alpha_k}}$. Plainly we may write

$$M_G(F) = AB,$$

with

$$A := M_{\mathbb{Z}_2 \times G'}(F), \quad B := M_{G'}(F(i,x_2,\dots,x_k)F(-i,x_2,\dots,x_k)).$$

From (9) we know that $M_G(F)$ and A, and hence B, are all congruent to 1 mod 2^k. Also B will be of the form $|a+ib|^2$ and hence cannot be negative. Since it contains a nonunit we have $B > 1$; hence $B \ge 2^k + 1$. If $A \ne 1$ then $|A| \ge 2^k - 1$ and $|M_G(F)| \ge (2^k-1)(2^k+1) = 4^k - 1 \ge |G| - 1$, so we must have $A = 1$. Thus if $F(u_1,u_2,\dots,u_k)$ is a nonunit with $u_j = \pm i$, we may assume that the $F(u_1,\dots,u_k)$ with $u_j = \pm 1$ are units. We have two possibilities for the $F(u_1,\dots,u_k)$ in the product (10):

(a) There is at least one nonunit $F(u_1,\dots,u_k)$ with some $u_j = \pm i$.

(b) $F(u_1,\dots,u_k)$ is a unit whenever any of the $u_j = \pm i$.

With I denoting the ideal generated by the $x_j^{2^{\alpha_j}} - 1$, and splitting the x_1-dependence into even and odd exponents $p(x_1) = \alpha(x_1^2) + x_1\beta(x_1^2)$, we can write

$$F(x_1,\dots,x_k) = \sum_{\substack{0\le\varepsilon_2,\dots,\varepsilon_s\le 3,\\ 0\le\varepsilon_1,\varepsilon_{s+1},\dots,\varepsilon_k\le 1}} a(\varepsilon_1,\varepsilon_2,\dots,\varepsilon_k)(x_1^2)\, x_1^{\varepsilon_1} x_2^{\varepsilon_2}\cdots x_k^{\varepsilon_k} \bmod I.$$

Since $F(1,\dots,1) = \sum a(\varepsilon_1,\varepsilon_2,\dots,\varepsilon_k)(1)$ is odd, we know that at least one of the $a(\varepsilon_1,\varepsilon_2,\dots,\varepsilon_k)(1)$ is odd. Replacing F by $x_1^{\delta_1}\cdots x_n^{\delta_n}F$ with $0 \le \delta_1, \delta_{s+1},\dots,\delta_k \le 1$ and $0 \le \delta_2,\dots,\delta_s \le 3$, and reducing mod I, to reshuffle the $a(\varepsilon_1,\dots,\varepsilon_k)(x_1^2)$, and replacing F by $-F$ as necessary, we can assume that

$$F(1,\dots,1) \equiv 1 \bmod 4, \quad a(0,\dots,0)(1) \text{ is odd.} \tag{11}$$

Case (a): Suppose we have nonunits in the product (10) with complex u_j. Reordering and taking $x_j \mapsto \pm x_1 x_j$ for $2 \le j \le s$ and $x_j \mapsto \pm x_j$ for $s < j \le k$ as necessary, we assume that the first of these is $\gamma_1 = F(i,1,\dots,1)$. If (after the transformations) there are other nonunits with complex entries in positions other than the first, by reordering and substituting x_j with $x_j x_2$ as necessary for $j \ge 3$, we may assume that $\gamma_2 = F(\pm i, i, \pm 1,\dots,\pm 1)$. If there are still nonunits with $u_j = \pm i$, $j \ge 3$, then, after reordering and substitutions, we have a nonunit $\gamma_3 = F(\pm i, \pm i, i, \pm 1,\dots,\pm 1)$. We repeat this, h times say, until there are no new nonunits with a complex u_j, $j > h$. That is, for some $1 \le h \le s$, we have h nonunits $\gamma_j = F(a_{j1},\dots,a_{jk})$ with $a_{jj} = i$, $a_{j\ell} = \pm i$ for $1 \le \ell < j$ and $a_{j\ell} = \pm 1$ for $h < \ell \le k$, and $F(u_1,\dots,u_k)$ is a unit whenever $u_\ell = \pm i$ with $h < \ell \le s$ if $h < s$. Adjusting as above we can assume that (11) holds.

Since the $F(\pm 1, u_2, \dots, u_k)$ are all units, with $F(1, \dots, 1) = 1$, and

$$a(0, \dots, 0)(1) = \frac{2}{|G|} \sum_{\substack{u_2, \dots, u_s = \pm i, \pm 1 \\ u_1, u_{s+1}, \dots, u_k = \pm 1}} F(u_1, \dots, u_k)$$

is odd, plainly the $F(\pm 1, u_2, \dots, u_k)$ must all be 1. Applying Lemma 3.1, we may therefore assume that

$$F(x_1, \dots, x_k) = 1 + (x_1^2 - 1) \sum_{\substack{0 \le \varepsilon_2, \dots, \varepsilon_s \le 3, \\ 0 \le \varepsilon_1, \varepsilon_{s+1}, \dots, \varepsilon_k \le 1}} a(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_k)\, x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k}.$$

Notice that the $F(\pm i, u_2, \dots, u_k) \in \mathbb{Z}[i]$ will all have odd real part and even imaginary part. Moreover, writing $\pi = (1 - i)$, where $\pi^2 \mid 2$, we have $u_j \equiv 1 \bmod \pi$ for any $u_j = \pm 1$ or $\pm i$, and the $F(\pm i, u_2, \dots, u_k)$ must all be congruent mod π^3 in $\mathbb{Z}[i]$. Since $|\pi|_2 = 2^{-1/2}$, plainly two units $\pm 1, \pm i$ in $\mathbb{Z}[i]$ cannot be congruent mod π^3 unless they are equal. If $h \ge 2$ then we know that the $F(\pm i, \pm 1, u_3, \dots, u_k)$ will all be units and so must be all 1 or all -1. Replacing F by $x_1^2 F$ we can assume that they are all 1. Applying Lemma 3.1 we get

$$F(x_1, \dots, x_k) = 1 + (x_1^2 - 1)(x_2^2 - 1) \sum_{\substack{0 \le \varepsilon_3, \dots, \varepsilon_s \le 3, \\ 0 \le \varepsilon_1, \varepsilon_2, \varepsilon_{s+1}, \dots, \varepsilon_k \le 1}} a(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_k)\, x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k}.$$

Likewise, if $h \ge 3$ we have that $F(\pm i, \pm i, \pm 1, u_4, \dots, u_k)$ are all units and congruent to 1 mod 4, so these must all equal 1. Applying the lemma and repeating up to $F(\pm i, \dots, \pm i, \pm 1, u_{h+1}, \dots, u_k)$, we deduce that

$$F(x_1, \dots, x_k) = 1 + \prod_{j=1}^{h} (x_j^2 - 1) \sum_{\substack{0 \le \varepsilon_{h+1}, \dots, \varepsilon_s \le 3, \\ 0 \le \varepsilon_1, \dots, \varepsilon_h, \varepsilon_{s+1}, \dots, \varepsilon_k \le 1}} a(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_k)\, x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k}.$$

If $s > h$, we further have that the $F(\pm i, \dots, \pm i, u_{h+2}, \dots, u_k)$ are all units. If $h \ge 2$ they will all be congruent to 1 mod 4 and so must all equal 1. If $h = 1$ then they are all 1 or all -1 and, by replacing F by $x_1^2 F$ if necessary, we may assume they are all 1. Writing

$$F(x_1, \dots, x_k) = 1 + \prod_{j=1}^{h} (x_j^2 - 1)\big(f(x_{h+2}, \dots, x_k) + x_{h+1} g(x_{h+2}, \dots, x_k) \bmod (x_{h+1}^2 + 1)\big),$$

separating into real and imaginary parts and applying Lemma 3.1 to f and g, we get that $f, g = 0 \bmod I$. Repeating for each variable, we find that

$$F(x_1, \dots, x_k) = 1 + \prod_{j=1}^{h} (x_j^2 - 1) \prod_{j=h+1}^{s} (x_j^2 + 1) \sum_{0 \le \varepsilon_1, \dots, \varepsilon_k \le 1} a(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_k)\, x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k}.$$

Suppose that there are $t \ge 1$ conjugate pairs of nonunits $F(a_{j1}, \dots, a_{jk}) = \gamma_j$. Then plainly

$$\gamma_j = a_j + i b_j, \qquad a_j \equiv 1 \bmod 2^s, \quad b_j \equiv 0 \bmod 2^s. \tag{12}$$

Trivially we have $|\gamma_j|^2 \geq 5$, and if $t \geq r+s$ then

$$|M_G(F)| \geq 5^t \geq 5^r \cdot 5^s > 2^r \cdot 4^s - 1,$$

so we can assume that

$$t \leq r+s-1. \tag{13}$$

If $t \leq r$ then, using $x_i \mapsto -x_i$ as necessary for γ_1, and for the subsequent γ_j reordering and using the transformation $x_\ell \mapsto x_\ell x_j$ if $u_j = -1$ to remove any $u_\ell = -1$ with $\ell > j$, we can assume that the r-tuples $(u_{s+1}, \ldots, u_k)$ achieving the γ_j take the form

$$(1, \ldots, 1), \quad (\pm 1, 1, \ldots, 1), \quad (\pm 1, \pm 1, 1, \ldots, 1), \quad \ldots, \quad (\overbrace{\pm 1, \ldots, \pm 1}^{t-1}, 1, \ldots, 1)$$

(here we are focusing on the u_j with $j > s$, which recall are taking the values ± 1). In particular, $F(u_1, \ldots, u_k)$ will be a unit if $u_j = -1$ for any $s+t \leq j \leq k$. (If $s \geq 2$, the units will all be 1; if $s = 1$ we may need to take $x_1^2 F$ to make the value when $u_{s+t} = -1$ and hence the rest equal 1.) Successively applying the lemma again, we find

$$F(x_1, \ldots, x_k) = 1 + \prod_{j=1}^{h} (x_j^2 - 1) \prod_{j=h+1}^{s} (x_j^2 + 1) \prod_{j=s+t}^{k} (x_j + 1) R$$

with

$$R = \sum_{0 \leq \varepsilon_1, \ldots, \varepsilon_{s+t-1} \leq 1} a(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{s+t-1})\, x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_{s+t-1}^{\varepsilon_{s+t-1}}.$$

Hence we obtain

$$\gamma_j = a_j + i b_j, \qquad a_j \equiv 1 \bmod 2^{s+r+1-t}, \quad b_j \equiv 0 \bmod 2^{s+r+1-t}.$$

From (13) and (12) this is plainly also valid if $t > r$. Thus, we have

$$|M_G(F)| = |\gamma_1| \cdots |\gamma_t| \geq (2^{r+s+1-t} - 1)^{2t} > 2^{2t(r+s+1/2-t)} \geq 2^{2(r+s-1/2)} \geq 2^{r+2s}$$

for $r \geq 1$. If $r = 0$ and $t \geq 2$ then we have $s \geq 2$, and from (12) we obtain

$$|M_G(F)| \geq (2^s - 1)^{2t} > 2^{2t(s-1/2)} \geq 2^{4s-2} > 4^s.$$

Finally if $t = 1$ and $r = 0$ then, since $F(i, 1, \ldots 1)$ and its conjugate are the only nonunits, we know that $F(\pm i, -1, u_3, \ldots, u_k)$ are all units and so equal 1. Hence we can add an extra factor $(x_2 + 1)$ to get

$$|M_G(F)| \geq (2^{s+1} - 1)^2 > 2^{2s}.$$

Case (b): Since $a(0, \ldots, 0)(1)$ is odd, we know that $a(0, \ldots, 0)(-1)$ is odd. Since the $F(\pm i, u_2, \ldots, u_k)$ are all units and

$$a(0, \ldots, 0)(-1) = \frac{1}{|G|/2} \sum_{\substack{u_1 = \pm i \\ u_2, \ldots, u_s = \pm i, \pm 1 \\ u_{s+1}, \ldots, u_k = \pm 1}} F(u_1, \ldots, u_k)$$

is odd, plainly the $F(\pm i, u_2, \dots, u_k)$ must all be 1 or all be -1. Replacing F by $x_1^2 F$ we assume $F(\pm i, u_2, \dots, u_k) = 1$. Applying Lemma 3.1 to the real and imaginary parts we can assume that

$$F(x_1, \dots, x_k) = 1 + (x_1^2 + 1) \sum_{\substack{0 \le \varepsilon_2, \dots, \varepsilon_s \le 3, \\ 0 \le \varepsilon_1, \varepsilon_{s+1}, \dots, \varepsilon_k \le 1}} a(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_k)\, x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k}.$$

Notice that all the $F(\pm 1, u_2, \dots, u_k)$ satisfy $F(\pm 1, u_2, \dots, u_k) \equiv F(1, \dots, 1) \equiv 1 \bmod \pi^3$. Hence if $s > 1$, the units $F(\pm 1, \pm i, u_3, \dots, u_k)$ are all 1. Applying the lemma and repeating we obtain

$$F(x_1, \dots, x_k) = 1 + \prod_{j=1}^{s} (x_j^2 + 1) \sum_{0 \le \varepsilon_1, \dots, \varepsilon_k \le 1} a(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_k)\, x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_k^{\varepsilon_k}.$$

Hence we have

$$M_G(F) = M_{\mathbb{Z}_2^k}(f),$$

where

$$f(x_1, \dots, x_k) = 1 + 2^s \sum_{0 \le \varepsilon_1, \dots, \varepsilon_k \le 1} A(\varepsilon_1, \dots, \varepsilon_k)\, x_1^{\varepsilon_1} \cdots x_k^{\varepsilon_k}.$$

Suppose that there are t elements $f(\pm 1, \dots, \pm 1)$ that are not ± 1. If $t \ge k + s - 1$ then plainly $|M_G(F)| \ge 3^t \ge 3^{k+s-1} > 2^{k+s}$ since $k + s \ge 3$, so we assume that $t \le k + s - 2$. Sending $x_j \mapsto -x_j$ we assume that one of them is $f(1, \dots, 1) = \gamma_1$. If $t > 1$ then, reordering and mapping x_ℓ to $x_\ell x_j$ if we have $\ell > j$ with $u_\ell = u_j = -1$, we can assume that the remaining values are $\gamma_2 = f(-1, 1, \dots, 1)$, $\gamma_3 = f(a_{31}, a_{32}, 1, \dots, 1)$, $\dots$, $\gamma_t = f(a_{t1}, \dots a_{t(t-1)}, 1, \dots, 1)$. If $t \le k$ then we will have $f(u_1, \dots, u_k) = 1$ whenever $u_j = -1$ for some $t \le j \le k$, and applying the lemma we find

$$f(x_1, \dots, x_k) = 1 + 2^s \prod_{j=t}^{k} (x_j + 1) \sum_{0 \le \varepsilon_1, \dots, \varepsilon_{t-1} \le 1} A(\varepsilon_1, \dots, \varepsilon_{t-1})\, x_1^{\varepsilon_1} \cdots x_{t-1}^{\varepsilon_{t-1}}.$$

Thus

$$\gamma_j \equiv 1 \bmod 2^{s+k-t+1}$$

(with this trivially holding if $k \le t - 1$), and

$$|M_G(F)| \ge (2^{s+k+1-t} - 1)^t.$$

For $t = 1$ this gives

$$|M_G(F)| \ge 2^{s+k} - 1 = |G| - 1,$$

and for $t \ge 2$

$$|M_G(F)| \ge 2^{t(s+k+1/2-t)} \ge 2^{2s+2k-3} \ge 2^{s+k}. \qquad \square$$

4. Proof of Theorem 1.2

Using $\Phi_j(x)$ to denote the j-th cyclotomic polynomial and recalling, see [Apostol 1970; Lehmer 1930], that for $j > k$ the resultant satisfies $|\mathrm{Res}(\Phi_j, \Phi_k)| = q^{\varphi(k)}$ if $j = kq^\alpha$ for some prime q and 1 otherwise,

we see that

$$M_{\mathbb{Z}_2\times\mathbb{Z}_{2^n}}(1+y+y^2) = M_{\mathbb{Z}_{2^n}}(\Phi_3(y))^2 = \left(\prod_{j=0}^{n}|\mathrm{Res}(\Phi_3,\Phi_{2^j})|\right)^2 = 9.$$

Let $G = \mathbb{Z}_2 \times \mathbb{Z}_{2^n}$. Reducing mod x^2-1, we can write our $F(x,y)$ in $\mathbb{Z}[x,y]$ in the form

$$F(x,y) = A_0(y^2) + xA_1(y^2) + yA_2(y^2) + xyA_3(y^2).$$

Plainly,

$$M_G(F(x,y)) = M_{\mathbb{Z}_{2^n}}(F(1,y))M_{\mathbb{Z}_{2^n}}(F(-1,y)),$$

where each of these measures is a product of $n+1$ integers,

$$M_{\mathbb{Z}_{2^n}}(f(y)) = \prod_{j=0}^{n} N_j(f), \quad N_j(f) := \mathrm{Res}(f,\Phi_{2^j}),$$

that is,

$$N_0(f) = f(1), \quad N_1(f) = f(-1), \quad N_2(f) = f(i)f(-i) = |f(i)|^2,$$

and, writing $w_j := e^{2\pi i/2^j}$, for any $j = 3,\dots,n$, we have

$$N_j(f) = \prod_{\substack{k=1\\ k \text{ odd}}}^{2^j} f(w_j^k) = \prod_{\substack{k=1\\ k \text{ odd}}}^{2^{j-1}} f(w_j^k)f(-w_j^k) = |R_j(f)|^2,$$

where

$$R_j(f) := \prod_{\substack{k=1\\ k\equiv 1 \bmod 4}}^{2^{j-1}} f(w_j^k)f(-w_j^k) \in \mathbb{Z}[i], \quad 3 \le j \le n.$$

Note $N_j(f)$ and $R_j(f)$ represent the norms of $f(w_j^k)$ from $\mathbb{Q}(w_j)$ to $\mathbb{Q}$ and $\mathbb{Q}(i)$ respectively, and since they are algebraic integers they will be in $\mathbb{Z}$ and $\mathbb{Z}[i]$, respectively.

Since $|1-w_j|_2 = 2^{-1/\varphi(2^j)}$, for all $j = 3,\dots,n$ we have $N_j(F(\pm 1,y)) \equiv F(1,1)^{2^{j-1}} \bmod 2$, and if $M_G(F) < 2^{2n+2}$ we can assume $F(1,1)$ and all the $N_j(F(\pm 1,y))$ are odd. Note that for all the $j \ge 2$ we have

$$N_j(F(\pm 1,y)) = |a+ib|^2 = a^2+b^2 \equiv 1 \bmod 4.$$

If $|M_G(F)| < 9$ then $|M_{\mathbb{Z}_{2^n}}(F(1,y))|$ or $|M_{\mathbb{Z}_{2^n}}(F(-1,y))|$ must be 1. Replacing x with $-x$ as necessary we assume that

$$1 < |M_{\mathbb{Z}_{2^n}}(F(1,y))| < 9, \quad |M_{\mathbb{Z}_{2^n}}(F(-1,y))| = 1.$$

Since

$$F(1,1) = A_0(1) + A_1(1) + A_2(1) + A_3(1)$$

is odd, we can assume that at least one of the $A_i(1)$ is odd. Replacing F by xF or yF or xyF and reducing by x^2-1 as necessary, we may assume that $A_0(1)$ is odd. Replacing y by $-y$ and F by $-F$ as necessary, we may further assume that $|F(1,1)| \ge |F(1,-1)|$ and $F(1,1) > 0$.

Since

$$F(1,-1) = A_0(1) + A_1(1) - A_2(1) - A_3(1),$$
$$F(-1,1) = A_0(1) - A_1(1) + A_2(1) - A_3(1),$$
$$F(-1,-1) = A_0(1) - A_1(1) - A_2(1) + A_3(1),$$

we have

$$A_0(1) = \tfrac{1}{4}\big(F(1,1) + F(1,-1) + F(-1,1) + F(-1,-1)\big),$$
$$A_1(1) = \tfrac{1}{4}\big(F(1,1) + F(1,-1) - F(-1,1) - F(-1,-1)\big),$$
$$A_2(1) = \tfrac{1}{4}\big(F(1,1) - F(1,-1) + F(-1,1) - F(-1,-1)\big),$$
$$A_3(1) = \tfrac{1}{4}\big(F(1,1) - F(1,-1) - F(-1,1) + F(-1,-1)\big).$$

Observe that

$$F(1,w_j^k)F(1,-w_j^k) = \big(A_0(w_j^{2k}) + A_1(w_j^{2k})\big)^2 - w_j^{2k}\big(A_2(w_j^{2k}) + A_3(w_j^{2k})\big)^2$$

and

$$F(-1,w_j^k)F(-1,-w_j^k) = \big(A_0(w_j^{2k}) - A_1(w_j^{2k})\big)^2 - w_j^{2k}\big(A_2(w_j^{2k}) - A_3(w_j^{2k})\big)^2$$

differ by

$$4\big(A_0(w_j^{2k})A_1(w_j^{2k}) - w_j^{2k}A_2(w_j^{2k})A_3(w_j^{2k})\big) \in 4\mathbb{Z}[w_{j-1}].$$

Hence $R_j(F(1,y))$ and $R_j(F(-1,y))$ differ by an element of $4\mathbb{Z}[w_{j-1}]$ and, since both are in $\mathbb{Z}[i]$, we conclude that

$$R_j(F(1,y)) - R_j(F(-1,y)) \in 4\mathbb{Z}[i].$$

Since $N_j(F(-1,y)) = 1$, we have $R_j(F(-1,y)) = \pm 1$ or $\pm i$, and either $R_j(F(1,y)) = R_j(F(-1,y))$ and $N_j(F(1,y)) = 1$, or $N_j(F(1,y)) \geq (4-1)^2 = 9$.

Thus if $|M_G(F)| < 9$ then we must have $N_j(F(1,y)) = N_j(F(-1,y)) = 1$ for $j = 3,\dots,n$ and $M_G(F) = M_{\mathbb{Z}_2\times\mathbb{Z}_4}(F)$. By Theorem 1.1 and Lemma 1.3, we have $|M_{\mathbb{Z}_2\times\mathbb{Z}_4}(F)| \geq 7$ and $M_{\mathbb{Z}_2\times\mathbb{Z}_4}(F) \equiv 1 \bmod 4$, and so

$$M_G(F) = M_{\mathbb{Z}_2\times\mathbb{Z}_4}(F) = -7.$$

Since $N_j(f) \equiv 1 \bmod 4$ for $j \geq 2$ we must have $|F(1,1)F(1,-1)| = 7$ and $N_2(F(1,y)) = 1$ and

$$F(1,1) = 7, \quad F(1,-1), \quad F(-1,\pm 1) = \pm 1, \quad F(\pm 1,\pm i) = \pm 1 \text{ or } \pm i,$$

with $R_j(F(1,y)) = R_j(F(-1,y)) = \pm 1$ or $\pm i$ for $j = 3,\dots,n$.

We have

$$A_0(1) = \tfrac{1}{4}\big(F(1,1) + F(1,-1) + F(-1,1) + F(-1,-1)\big) = \tfrac{1}{4}(7 \pm 1 \pm 1 \pm 1)$$

and, since $A_0(1)$ is odd, we must have $F(1,-1) = F(-1,\pm 1) = -1$ and $A_0(1) = 1$ and $A_1(1) = A_2(1) = A_3(1) = 2$. Hence

$$F(x,y) = 1 + 2x + 2y + 2xy + (y^2-1)\big(B_0(y^2) + xB_1(y^2) + yB_2(y^2) + xyB_3(y^2)\big).$$

Thus

$$F(1,i) = 3 + 4i - 2\big(B_0(-1) + B_1(-1) + iB_2(-1) + iB_3(-1)\big),$$
$$F(-1,i) = -1 - 2\big(B_0(-1) - B_1(-1) + iB_2(-1) - iB_3(-1)\big),$$

and since $F(\pm 1, i)$ are units with odd real part and difference in $4\mathbb{Z}[i]$ they must both be 1 or -1. By replacing F by $y^2 F$ as necessary, we may assume $F(\pm 1, i) = -1$. Solving, we obtain $B_0(-1) = B_1(-1) = B_2(-1) = B_3(-1) = 1$ and

$$F(x, y) = -1 + (1+x)(1+y)(1+y^2) + (y^4-1)\big(C_0(y^2) + xC_1(y^2) + yC_2(y^2) + xyC_3(y^2)\big).$$

Therefore

$$F(1, w_3)F(1, -w_3) = (1 + 2i - 2C_0(i) - 2C_1(i))^2 - 4i(1 + i - C_2(i) - C_3(i))^2$$

and

$$F(-1, w_3)F(-1, -w_3) = (-1 - 2C_0(i) + 2C_1(i))^2 - 4i(C_2(i) - C_3(i))^2.$$

Since both are units and are members of $1 + 4\mathbb{Z}[i]$, these must both equal 1. However, their difference

$$4\big((i - 2C_0(i))(1 + i - 2C_1(i)) - i(1 + i - 2C_3(i))(1 + i - 2C_2(i))\big) \in 4(1 + i + 2\mathbb{Z}[i])$$

is not zero. □

References

[Apostol 1970] T. M. Apostol, "Resultants of cyclotomic polynomials", *Proc. Amer. Math. Soc.* **24** (1970), 457–462. MR Zbl

[Conrad 1998] K. Conrad, "The origin of representation theory", *Enseign. Math.* (2) **44**:3-4 (1998), 361–392. MR Zbl

[Dedekind 1968] R. Dedekind, *Gesammelte mathematische Werke, II*, Chelsea, New York, 1968. MR

[DeSilva and Pinner 2014] D. DeSilva and C. Pinner, "The Lind Lehmer constant for $\mathbb{Z}_p^n$", *Proc. Amer. Math. Soc.* **142**:6 (2014), 1935–1941. MR Zbl

[Kaiblinger 2010] N. Kaiblinger, "On the Lehmer constant of finite cyclic groups", *Acta Arith.* **142**:1 (2010), 79–84. MR Zbl

[Lang 1978] S. Lang, *Cyclotomic fields*, Graduate Texts in Mathematics **59**, Springer, 1978. MR Zbl

[Lehmer 1930] E. T. Lehmer, "A numerical function applied to cyclotomy", *Bull. Amer. Math. Soc.* **36**:4 (1930), 291–298. MR Zbl

[Lehmer 1933] D. H. Lehmer, "Factorization of certain cyclotomic functions", *Ann. of Math.* (2) **34**:3 (1933), 461–479. MR Zbl

[Lind 2005] D. Lind, "Lehmer's problem for compact abelian groups", *Proc. Amer. Math. Soc.* **133**:5 (2005), 1411–1416. MR Zbl

[Pigno and Pinner 2014] V. Pigno and C. Pinner, "The Lind–Lehmer constant for cyclic groups of order less than 892,371,480", *Ramanujan J.* **33**:2 (2014), 295–300. MR Zbl

[Vipismakul 2013] W. Vipismakul, *The stabilizer of the group determinant and bounds for Lehmer's conjecture on finite abelian groups*, Ph.D. thesis, University of Texas at Austin, 2013, available at http://hdl.handle.net/2152/21685.

Received 21 Jun 2018.

MICHAEL J. MOSSINGHOFF:
mimossinghoff@davidson.edu
Department of Mathematics & Computer Science, Davidson College, Davidson, NC, United States

VINCENT PIGNO:
vincent.pigno@csus.edu
Department of Mathematics & Statistics, California State University, Sacramento, CA, United States

CHRISTOPHER PINNER:
pinner@math.ksu.edu
Department of Mathematics, Kansas State University, Manhattan, KS, United States

Moscow Journal of Combinatorics and Number Theory

msp.org/moscow

See inside back cover or msp.org/moscow for submission instructions.

The subscription price for 2019 is US $310/year for the electronic version, and $365/year (+$20, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Moscow Journal of Combinatorics and Number Theory (ISSN 2640-7361 electronic, 2220-5438 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

MJCNT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY
mathematical sciences publishers
nonprofit scientific publishing
http://msp.org/

Moscow Journal of Combinatorics and Number Theory
vol. 8 no. 2 2019