THE LIND-LEHMER CONSTANT FOR $\mathbb{Z}_m \times \mathbb{Z}_n^p$

Vincent Pigno  
Department of Mathematics & Statistics, University of California, Sacramento,  
California  
v Vincent Pigno@csus.edu

Chris Pinner  
Department of Mathematics, Kansas State University, Manhattan, Kansas  
pinner@math.ksu.edu

Wasin Vipismakul  
Department of Mathematics, Burapha University, Chonburi, Thailand  
wvipismakul@gmail.com

Received: 12/21/15, Accepted: 6/12/16, Published: 7/7/16

Abstract
We give bounds on the Lind-Lehmer constant for groups of the form

$$\mathbb{Z}_m \times \mathbb{Z}_n^p, \quad p \nmid m$$

that are in many cases sharp. In particular we obtain the Lind-Lehmer constant for groups of the form $\mathbb{Z}_2 \times \mathbb{Z}_p^n$, $p \geq 3$.

1. Introduction

For a polynomial $F$ in $\mathbb{Z}[x_1, \ldots, x_k]$ and a finite abelian group

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

one defines the Lind-Mahler measure [4] of $F$ with respect to $G$ by

$$M_G(F) = |P_G(F)|^{1/|G|},$$

where $P_G(F)$ is the integer

$$P_G(F) := \prod_{j_1=1}^{n_1} \cdots \prod_{j_k=1}^{n_k} F\left(e^{2\pi i j_1/n_1}, \ldots, e^{2\pi i j_k/n_k}\right).$$
That is, instead of the classical logarithmic Mahler measure
\[ \log M(F) = \int_0^1 \cdots \int_0^1 \log |F(e^{2\pi i x_1}, \ldots, e^{2\pi i x_k})| dx_1 \cdots dx_k, \]
one defines
\[ \log M_G(F) = \frac{1}{|G|} \sum_{x_1=1}^{n_1} \cdots \sum_{x_k=1}^{n_k} \log |F(e^{2\pi i x_1/n_1}, \ldots, e^{2\pi i x_k/n_k})|. \]
Mirroring the Lehmer problem for the classical measure, one can ask for the minimal positive logarithmic Lind-Mahler measure, and define a Lind-Lehmer constant for \( G \)
\[ \lambda(G) = \frac{1}{|G|} \log \mathcal{P}_G, \]
where
\[ \mathcal{P}_G = \min \left\{ \left| P_G(F) \right| : \left| P_G(F) \right| \geq 2, \ F \in \mathbb{Z}[x_1, \ldots, x_k] \right\}. \]
For cyclic groups \( G = \mathbb{Z}_m \), Kaiblinger [2] gave the bounds
\[ \min \left\{ \min_{q \mid m} q, \min_{q \mid m} q^{\alpha+1} \right\} \leq \mathcal{P}_{\mathbb{Z}_m} \leq \min \left\{ \min_{q \mid m} q, \min_{q \mid m} q^{\alpha} \right\}, \]
with equality in these upper and lower bounds when 420 \( \nmid m \) (see [5] for \( \lambda(\mathbb{Z}_m) \) when 892371480 \( \nmid m \)). Here \( p \) and \( q \) will always denote primes. Writing
\[ M_j := \{ a^{p^i-1} - tp^j : 1 \leq a < p, \ t \in \mathbb{Z} \}, \]
and
\[ M_j^* := \min \{ |b| \geq 2 : b \in M_j \}, \]
the second author showed in [1] that for \( G = \mathbb{Z}_p^n \), we have
\[ \mathcal{P}_G = M^*_n. \]
In his thesis [7, Theorem 2.1.5] the third author extended this to general \( p \)-groups
\[ G_p := \mathbb{Z}_{p^{l_1}} \times \cdots \times \mathbb{Z}_{p^{l_n}}, \quad l_1 \leq \cdots \leq l_n, \quad N = \sum_{i=1}^n l_i, \]
showing the bounds
\[ M^*_n \leq \mathcal{P}_{G_p} \leq M^*_N. \]
In this note we obtain the counterpart of (2) and (6) for \( G = \mathbb{Z}_m \times G_p, \ p \nmid m \). When \( G_p = \mathbb{Z}_p^n \) (i.e., \( N = n \)) we seem to have equality in many cases, including \( m = 2 \).
2. Results

We define

\[ M_j^-(r) := \min \{ b > 1 : b \in M_j, (b, r) \neq 1 \}, \]
\[ M_j^+(r) := \min \{ b > 1 : b \in M_j, (b, r) = 1 \}. \]

Note that \(-1 + mp^l\) is in \(M_j\) so that

\[ M_j^+(r) \leq mp^l - 1. \]  \hspace{1cm} (7)

Theorem 1. If \(G = \mathbb{Z}_m \times G_p\) with \(G_p\) as in (5) and \(p \nmid m\phi(m)\), then

\[ \min \left\{ M_1^+(m), \min_{q^a \mid m} M_1^-(q)^{\alpha + 1}, p^{B(G_p)} \right\} \leq \mathcal{P}_G \leq \min \{ M_N^+(m), M_N^{m_1} \}, \]  \hspace{1cm} (8)

where \(m_1 = \prod_{q^a \mid m, a \in M_N^*} q^a\) and

\[ B(G_p) = (l_1 + 1) + \sum_{i=1}^{n-1} (l_{i+1} - l_i + 1)p^{l_1 + \cdots + l_i}. \]  \hspace{1cm} (9)

In view of (7) we can drop the \(p^{B(G_p)}\) from the lower bound if \(m \leq p^{B(G) - n}\), and we also recover the trivial bound

\[ M_N^+(m) \leq |G| - 1 = \left| \mathcal{P}_G \left( -1 + \left( \frac{z^m - 1}{z - 1} \right) \prod_{i=1}^{n} \left( \frac{x_i^{p^{l_i}} - 1}{x_i - 1} \right) \right) \right|. \]

If \(G_p = \mathbb{Z}_p^n\) and \(M_1^+(m) \leq p^{2 + p + \cdots + p^{n-1}}\) and \(p \nmid m\phi(m)\) we have

\[ M_1^+(m) < M_1^{n^2} \implies \mathcal{P}_G = M_1^+(m). \]  \hspace{1cm} (10)

If \(G_p = \mathbb{Z}_p^n\) and \(m = 2\) we clearly have equality in our upper and lower bounds (8):

Corollary 1. If \(G = \mathbb{Z}_2 \times \mathbb{Z}_p^n\) and \(p \geq 3\), then

\[ \mathcal{P}_G = \min \{ M_n^+(2), M_n^{n-2} \}. \]

The lower bound in Theorem 1 will come from observing that if \(p \mid \mathcal{P}_G(F)\) then \(p^{B(G_p)} \mid \mathcal{P}_G(F)\), and that if \(p \nmid \mathcal{P}_G(F)\) then \(\mathcal{P}_G(F)\) must be a product of \(d(m)\) elements of \(M_n\) (which includes 1); moreover that if \(q \mid \mathcal{P}_G(F)\) and \(q^a \mid m\), then at least \((\alpha + 1)\) of them are divisible by \(q\). The upper bounds are constructive. We can drop the assumption \(p \nmid \phi(m)\) in Theorem 1 if we replace the \(M_N^n(m)\) in our upper bound by the smallest element of \(M_N\) which is coprime to \(m\) and a \(p^{n-1}\)st power mod \(m\) and add to \(m_1\) any \(q^a \mid m\), \(q \equiv 1 \mod p\), such that \(M_N^*\) is not a \(p^{n-1}\) power mod \(q\).
3. Proofs

The bound $\mathcal{P}_G \leq \mathcal{M}_p^r(m)$ follows at once from the following lemma and the observation that if $p \nmid \phi(m)$ and $(s,m) = 1$ then $s$ is a $p^{N-1}$st power mod $m$.

**Lemma 1.** Let $G = \mathbb{Z}_m \times G_p$, $p \nmid m$. If $s = a^{p^{N-1}} - tp^N$ has $(s,pm) = 1$ and is a $p^{N-1}$st power mod $m$ then there is a polynomial $F$ in $\mathbb{Z}[x_1, \ldots, x_n]$ with $P_G(F) = s$.

**Proof.** The proof is entirely constructive and similar to Lemma 2.2 of [1].

Suppose that $s \equiv a_0^{p^{N-1}} \mod m$. Since $p \nmid m$ we can find an integer $\lambda$ such that $a + p\lambda$ is a positive integer satisfying $a + p\lambda \equiv a_0 \mod m$. Hence we can write

$$s = a^{p^{N-1}} - tp^N = (a + \lambda p)^{p^{N-1}} - t_1p^N$$

for some $t_1$ which must satisfy $m \mid t_1$. Thus we can assume that $a$ is a positive integer and that $m \mid t$. Notice also that $(s,pm) = 1$ ensures that $(a, pm) = 1$.

We define $H_1(z,y), \ldots, H_{N-1}(z,y)$ in $\mathbb{Z}[z,y]$ by

$$(1 + (zy) + \cdots + (zy)^{a-1})^{p^i} = \left( \sum_{j=0}^{a-1} z^{pj} \right)^{p^{i-1}} + p^i H_i(z,y) \mod y^p - 1. \quad (11)$$

To see (11) for $i = 1$ we have

$$(1 + (zy) + \cdots + (zy)^{a-1})^p = 1 + (zy)^p + \cdots + (zy)^{p(a-1)} + pH_1(z,y)$$

$$\equiv (1 + z^p + \cdots + z^{p(a-1)}) + pH_1(z,y) \mod y^p - 1,$$

and for $i \geq 1$ successively

$$(1 + (zy) + \cdots + (zy)^{a-1})^{p^{i+1}} \equiv \left( \sum_{j=0}^{a-1} z^{pj} \right)^{p^{i-1}} + p^i H_i(z,y) \mod y^p - 1$$

$$= \left( \sum_{j=0}^{a-1} z^{pj} \right)^{p^i} + p^{i+1} H_{i+1}(z,y).$$

We define $\alpha(1), \ldots, \alpha(N)$ by $1, 1, 2, 2, \ldots, n, \ldots, n$, and $\beta(1), \ldots, \beta(N)$ by $p^{l_1-1}, p^{l_1-2}, \ldots, 1, p^{l_2-1}, \ldots, 1, \ldots, p^{l_n-1}, \ldots, 1$. Recalling the $p$th cyclotomic polynomial

$$\Phi_p(x) = 1 + x + \cdots + x^{p-1} = \frac{x^p - 1}{x - 1},$$
we take a positive integer \( r \) such that \( rp \equiv 1 \pmod{m} \) and set

\[
F(z, x_1, \ldots, x_n) = \left( 1 + \left( \frac{z x_1^{p_{i_{1}^{1}}}}{1} \right) + \cdots + \left( \frac{z x_1^{p_{i_{n}^{1}}}}{1} \right)^{a-1} \right) + \sum_{j=1}^{N-1} H_j \left( \frac{z^{x_1^{j}}}{x_1^{\beta(j+1)}} \right) \prod_{i=1}^{j} \Phi_p \left( \frac{x_1^{\beta(i)}}{x_1^{\alpha(i)}} \right) - \frac{t}{m} \left[ \frac{z^{m-1}}{z-1} \right] \prod_{i=1}^{n} \left( \frac{x_1^{p_{i_j}}-1}{x_1^{i_j}-1} \right).
\]

Suppose that \( w \) is a primitive \( p^{j_1} \)th root of unity and \( z \) is an \( m \)th root of unity which is a primitive \( j \)th root of unity. Then \( w' = w^{p_{i_{j}^{1}}} \) is a primitive \( j \)th root of unity and, since \((a, pm) = 1\) and \((m, p) = 1\), both \( zw' \) and \( (zw')^a \) are primitive \( p^j \)th roots of unity. Thus \( 1 - (zw')^a \) and \( 1 - (zw') \) have the same norm and

\[
F(z, w, \ldots) = 1 + (zw') + \cdots + (zw')^{a-1} = \frac{1 - (zw')^a}{1 - (zw')}
\]

is a unit of norm 1.

Similarly, suppose \( x_k = w \) is a primitive \( p^{k_{j}^{1}} \)th root of unity with \( 0 \leq j \leq l_k - 1 \) (with \( j \geq 1 \) if \( k = 1 \)) and \( x_i = 1 \) for any \( 1 \leq i < k \). We set \( J = l_1 + \cdots + l_k - 1 + j \). Then \( x_{\alpha(i)}^{\beta(i)} = 1 \) and \( \Phi_p \left( x_{\alpha(i)}^{\beta(i)} \right) = p \) for all \( i < J \), and \( w' = x_{\alpha(j)}^{\beta(j)} = w^{p_{i_{j}^{1}}^{l_{k}^{1}}} \) is a primitive \( j \)th root of unity and \( \Phi_p \left( x_{\alpha(j)}^{\beta(j)} \right) = 0 \). Hence

\[
F(z, 1, \ldots, 1, w, \ldots) = \sum_{j=0}^{a-1} z^j + \sum_{i=1}^{J-2} p^i H_i(z^{r_i}, 1) + p^{J-1} H_{J-1}(z^{r_{J-1}}, w')
\]

\[
= \left( \sum_{j=0}^{a-1} (z^r)^{p_j} + pH_i(z^{r_i}, 1) \right) + \sum_{i=1}^{J-2} p^i H_i(z^{r_i}, 1) + p^{J-1} H_{J-1}(z^{r_{J-1}}, w')
\]

\[
= \left( \sum_{j=0}^{a-1} (z^{r_{j}})^{p_j} \right) + \sum_{i=1}^{J-2} p^i H_i(z^{r_i}, 1) + \sum_{i=1}^{J-2} H_{J-1}(z^{r_{J-1}}, w')
\]

\[
= \left( \sum_{j=0}^{a-1} (z^{r_{j}})^{p_j} \right) + p^{J-1} H_{J-1}(z^{r_{J-1}}, w')
\]

\[
= \left( \sum_{j=0}^{a-1} (z^{r_{j}})^{p_j} \right) + \left( \frac{1 - (z^{r_{J-1}}w')^a}{1 - (z^{r_{J-1}}w')} \right)^{p^{J-1}}
\]

is again a unit of norm 1. Finally, if \( z \neq 1 \) is an \( m \)th root of unity, then

\[
F(z, 1, \ldots, 1) = \sum_{j=0}^{a-1} z^j + \sum_{i=1}^{N-1} p^i H_i(z^{r_i}, 1) = \left( \sum_{j=0}^{a-1} z^{j^{N-1}} \right)^{p^{N-1}} = \left( \frac{1 - z^{ar^{N-1}}}{1 - z^{r^{N-1}}} \right)^{p^{N-1}}
\]
is a unit of norm 1,

\[ F(1, 1, \ldots, 1) = a + \sum_{i=1}^{N-1} p^i H_i(1, 1) - tp^N = (1 + 1 + \cdots + 1)p^{N-1} - tp^N, \]

and \( P_G(F(z, x_1, \ldots, x_n)) = a p^{N-1} - tp^N. \)

We observe that if \( p \) divides a \( G_p \) measure then a high power of \( p \) divides the measure.

**Lemma 2.** Suppose that \( p^m \parallel P_{G_p}(F) \). Then \( m = 0 \) or

\[ m \geq (l_1 + 1) + \sum_{i=1}^{n-1} (l_{i+1} - l_i + 1)p^{l_1 + \cdots + l_i}. \]

(12)

We can also replace this by a more precise but less digestible bound; if \( l_1, \ldots, l_n \)
take the values \( k_1 < \cdots < k_L \) with multiplicities \( m_1, \ldots, m_L \) and \( k_0 = 0 \), then the right-hand side of (12) can be replaced by

\[ 1 + \sum_{i=0}^{L-1} \sum_{j=0}^{k_{L-i-1} - 1} m_{L-i-1}^{m_{L-i-1}} k_{L-i-1}^{m_{L-i-1}} (k_{L-i-1} + \cdots + m_{L-i-1} - 1)(k_{L-i-1} - j)^{m_{L-i-1}}. \]

(13)

Either bound (12) or (13) can be used for \( B(G_p) \) in Theorem 1. When \( G_p = \mathbb{Z}_p^n \)
both give the bound \( 2 + p + \cdots + p^{n-1} = 1 + \frac{p^n - 1}{p-1} \) used in [1]. A simpler bound on
\( B(G_p) \) is given in [7, Theorem 2.1.3].

**Proof.** Observe that if \( w_{p^j} \) denotes a primitive \( p^j \)th root of unity, then

\[ \text{Norm}_{\mathbb{Q}(w_{p})/\mathbb{Q}}F(w_{p^1}, \ldots, w_{p^n}) = \prod_{j=1}^{p} F(w_{p^1}, \ldots, w_{p^n}) \in \mathbb{Z}, \]

where

\[ s = \max\{s_1, \ldots, s_n\}, \]

and \( M_{G_p}(F) \) can be written as a product of such integer norms. Moreover, extending the \( p \)-adic absolute value to \( \mathbb{Q}(w_{p}) \), we have \( |w_{p^j} - 1|_p < 1 \) and so plainly

\[ \text{Norm}_{\mathbb{Q}(w_{p})/\mathbb{Q}}F(w_{p^1}, \ldots, w_{p^n}) \equiv F(1, \ldots, 1)^{s(p^j)} \mod p. \]

Hence if \( p \mid P_{G_p}(F) \), then \( p \mid F(1, \ldots, 1) \) and \( p \) divides all the norms. Thus the bounds (12) and (13) represent a bound on the number of integer norms that make up \( M_{G_p} \). For (12) we proceed by induction on \( n \); for \( n = 1 \) we have \( l_1 + 1 \) norms, namely the value \( F(1) \) and the norms of \( F(w_{p^j}), j = 1, \ldots, l_1 \). For \( n > 1 \) and a
primitive \( p \)th root of unity \( w_p \), with \( l_n - 1 \leq j \leq l_n \) the \( F(x_1, \ldots, x_{n-1}, w_p^j) \) produce a different norm for each choice of \( x_1, \ldots, x_{n-1}, \) giving \( (l_n-l_{n-1}+1)p^{l_n-l_{n-1}} \) norms. Discarding any terms \( F(x_1, \ldots, x_{n-1}, w_p^j) \) with \( 1 \leq j < l_{n-1} \), the remaining terms in (12) come from the \( n-1 \) variable \( \mathbb{Z}_{p^1} \times \cdots \times \mathbb{Z}_{p^{n-1}} \) measure of \( F(x_1, \ldots, x_{n-1}, 1) \).

Retaining the terms \( F(x_1, \ldots, x_{n-1}, w_p^j) \) with \( 1 \leq j < l_{n-1} \) gives (13); taking \( x_n = w_p^{k_L} \) we have the \( p^{m_1k_1} \cdots + m_{L-1}k_{L-1}+(m_L-1)k_L \) choices of the other \( x_i \). The remaining norms then have a \( k_L \) replaced by \( k_L - 1 \). When \( m_L > 1 \) one successively reduces the remaining \( k_L \) to \( k_L - 1 \) contributing \( p^{\sum_{i=1}^{L-1} m_ik_i+(m_{L-1}+m_L-2)k_L} \) for \( i = 0 \) to \( m_L - 1 \). When \( k_L - 1 > k_{L-1} \) one continues to reduce all the \( m_L \) exponents \( k_L - 1 \) until one has \( m_L + m_{L-1} \) values \( k_{L-1} \) (the \( j \) sum). One repeats (the \( l \) sum) until left with \( m_1 + \cdots + m_L \) exponents \( k_1 \) and finally the single term \( F(1, \ldots, 1) \).

**Proof of Theorem 1.** Let \( w_r \) denote a primitive \( r \)th root of unity. For the lower bound observe that we can write

\[
P_{G}(F) = P_{G_p}(F_1) = \prod_{d|m} P_{G_p}(f_d),
\]

where

\[
F_1 := \prod_{j=0}^{m} F(w_m^j, x_1, \ldots, x_n) = \prod_{d|m} f_d(x_1, \ldots, x_n)
\]

with

\[
f_d(x_1, \ldots, x_n) := \prod_{j=d}^{d} F(w_m^j, x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n].
\]

From Lemma 2 if \( p \mid P_{G_p}(f_d) \) then \( p^{|G_p|} \mid P_{G_p}(f_d) \). It was shown in [1, Lemma 2.1] for \( G_p = \mathbb{Z}_p^* \) and in [7, Theorem 2.1.2] for general \( G_p \) that if \( p \nmid P_{G_p}(f_d) \) then \( P_{G_p}(f_d) \) lies in \( M_p \). Since for a prime \( q \) and \( (l,q) = 1 \) we can write \( w_{lq} = w_l w_{q} \) with \( |w_q| - 1 \) \( q \), we have

\[
f_{lq} = f_i \mod q
\]

and

\[
P_{G_p}(f_{lq}) \equiv P_{G_p}(f_i)^{\phi(q)} \mod q.
\]

Hence if \( q^\alpha \mid \mid m \) has \( q \mid P_{G}(F) \), then \( q \mid P_{G_p}(f_{lq}) \) for some \( l \) with \( q \nmid l \) and \( 0 \leq j \leq \alpha \), and \( q \mid P_{G_p}(f_{iq}) \) for all \( 0 \leq i \leq \alpha \), and \( |P_{G_p}(f_{iq})| \geq M_{\alpha}(q) \) for all \( i \). So \( |P_{G}(F)| \geq M_{\alpha}(q)^\alpha+1 \) and the lower bound is plain.

From Lemma 1 we have \( P_{G} \leq M_N^+(m) \). For the remaining upper bound observe that if \( a \) is in \( M_{\alpha} \) and we write \( m = m_1 m_2 \), where \( m_1 = \prod_{q^\alpha \mid m} q^\alpha (m_2, a) = 1 \), then we know that for \( G_2 := \mathbb{Z}_{m_2} \times \mathbb{Z}_p^* \) there is an \( f(z, x_1, \ldots, x_k) \) with \( P_{G_2}(f) = \)
a. Hence $F(z, x_1, \ldots, x_k) = f(z^{m_1}, x_1, \ldots, x_k)$ will have $P_G(F) = P_{G_{f,k}}(f^{m_1}) = a^{m_1}$. Taking $a = M_N$ gives the bound stated. Note, taking the polynomial $F(x_1, \ldots, x_n)$ achieving $P_{G_{f,k}}$, we similarly have the trivial bound $P_G \leq P_{G_{f,k}}$. □

4. Examples

Notice that the smallest possible value of $P_{Z_2 \times Z_2}$ is 3, achievable exactly when $3^{p-1} \equiv 1 \mod p^2$. The only known such Mirimanoff primes (Wieferich primes base 3) are $p = 11$ and $p = 1006003$; see for example [3, p.150] or [6, p.347]. The two known Wieferich primes, $p = 1093$ and 3511, have $P_{Z_2 \times Z_2} = M_2(2)^2 = 4$.

The following tables give the $M_n$ and $M_n^+(m)$ for $G = Z_m \times Z_p^n$, with $3 \leq p \leq 103$, $n = 2, 3, 4$, and $m$ of the form $2^a, 3^a, 5^a, 2^a 3^b, 7^a, 2^a 5^b$ or $11^a$. For $p \nmid m \phi(m)$ we have $M_n^+(m) < M_n^2$ and $P_G = M_n^+(m)$ except for the following few unresolved cases:

<table>
<thead>
<tr>
<th>$G$</th>
<th>$P_G$</th>
<th>$G$</th>
<th>$P_G$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Z_{2^{a+3}} \times Z_{11}^\alpha, \alpha \geq 0$,</td>
<td>27 or 40</td>
<td>$Z_{32} \times Z_{11}^m$</td>
<td>27 or 40</td>
</tr>
<tr>
<td>$Z_{2^{a+3}} \times Z_{11}^\alpha, \alpha \geq 1$,</td>
<td>27, 81 or 161</td>
<td>$Z_8 \times Z_5^m$</td>
<td>324 or 437</td>
</tr>
<tr>
<td>$Z_{2^{a+3}} \times Z_{11}^\alpha, \alpha \geq 1$,</td>
<td>81 or 161</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Since 8 is a cube, the restriction $p \nmid \phi(m)$ only affects $Z_7 \times Z_4^n, n = 3, 4$ and $Z_{11} \times Z_5^n, n = 2, 3, 4$.

Table of $M_n^+$:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>8</td>
<td>7</td>
<td>8</td>
<td>18</td>
<td>3</td>
<td>3</td>
<td>35</td>
<td>28</td>
<td>28</td>
<td>14</td>
<td>115</td>
<td>18</td>
<td>51</td>
<td>19</td>
</tr>
<tr>
<td>3</td>
<td>26</td>
<td>57</td>
<td>182</td>
<td>184</td>
<td>124</td>
<td>239</td>
<td>158</td>
<td>333</td>
<td>42</td>
<td>1215</td>
<td>1215</td>
<td>691</td>
<td>172</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>80</td>
<td>182</td>
<td>1047</td>
<td>1963</td>
<td>1963</td>
<td>239</td>
<td>4260</td>
<td>2819</td>
<td>19214</td>
<td>2463</td>
<td>51344</td>
<td>51344</td>
<td>1172</td>
<td>3038</td>
</tr>
</tbody>
</table>

Table of $P_G$ for $G = Z_{2^a} \times Z_p^n, n = 2, 3, 4, p \leq 103$. In all these cases $P_G = M_n^+(2)$:
\[
\begin{array}{|c|c|c|c|c|c|c|}
\hline
 & n = 2 & n = 3 & n = 4 & n = 2 & n = 3 & n = 4 \\
\hline
p = 3 & 17 & 53 & 161 & p = 47 & 53 & 295 \\
p = 5 & 7 & 57 & 443 & p = 53 & 43 & 9283 \\
p = 7 & 19 & 19 & 1047 & p = 59 & 53 & 2511 \\
p = 11 & 3 & 161 & 1963 & p = 61 & 601 & 28743 \\
p = 13 & 19 & 239 & 239 & p = 67 & 143 & 3859 \\
p = 17 & 65 & 399 & 15541 & p = 71 & 11 & 8327 \\
p = 19 & 69 & 333 & 2819 & p = 73 & 527 & 923 \\
p = 23 & 63 & 803 & 60793 & p = 79 & 31 & 1523 \\
p = 29 & 41 & 1215 & 2463 & p = 83 & 99 & 6509 \\
p = 31 & 115 & 513 & 126279 & p = 89 & 605 & 1485 \\
p = 37 & 117 & 691 & 216739 & p = 97 & 53 & 34557 \\
p = 41 & 51 & 9325 & 20677 & p = 101 & 181 & 4943 \\
p = 43 & 19 & 3623 & 162637 & p = 103 & 43 & 26319 \\
\hline
\end{array}
\]

Table of \( M_n^3(3) \neq M_n^* \) for \( G = \mathbb{Z}_{3^n} \times \mathbb{Z}_p^n, n = 2, 3, 4, p \leq 103 \):

\[
\begin{array}{|c|c|c|c|}
\hline
 & n = 2 & n = 3 & n = 4 \\
\hline
p = 7 & 19 & p = 5 & 68 \\
p = 11 & 40 & p = 7 & 19 \\
p = 37 & 76 & p = 19 & 623 \\
p = 41 & 148 & p = 23 & 803 \\
p = 61 & 572 & p = 29 & 4850 \\
p = 73 & 368 & p = 31 & 5995 \\
p = 83 & 161 & p = 59 & 18511 \\
p = 71 & 8327 & p = 83 & 6509 \\
p = 101 & 571075 & p = 103 & 4717448 \\
\hline
\end{array}
\]

Table of \( M_n^5(5) \neq M_n^* \) for \( G = \mathbb{Z}_{5^n} \times \mathbb{Z}_p^n, n = 2, 3, 4, p \leq 103 \):

\[
\begin{array}{|c|c|c|c|}
\hline
 & n = 2 & n = 3 & n = 4 \\
\hline
p = 31 & 117 & p = 29 & 1872 \\
p = 47 & 4757 & p = 3 & 161 \\
p = 53 & 111529 & p = 17 & 15541 \\
p = 59 & 648103 & p = 59 & 111529 \\
p = 61 & 201306 & p = 67 & 201306 \\
\hline
\end{array}
\]
Table of $M_n^+(6) \neq M_n^*$, for primes such that $3 \mid M_n^+(2) \neq M_n^*$ or $2 \mid M_n^+(3) \neq M_n^*$ for $G = \mathbb{Z}_{2^n \cdot 3^k} \times \mathbb{Z}_p^n$, $n = 2, 3, 4$, $p \leq 103$:

<table>
<thead>
<tr>
<th></th>
<th>$n = 2$</th>
<th>$n = 3$</th>
<th>$n = 4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p = 11$</td>
<td>161</td>
<td>$p = 7$</td>
<td>2549</td>
</tr>
<tr>
<td>$p = 19$</td>
<td>127</td>
<td>$p = 5$</td>
<td>193</td>
</tr>
<tr>
<td>$p = 23$</td>
<td>263</td>
<td>$p = 17$</td>
<td>653</td>
</tr>
<tr>
<td>$p = 37$</td>
<td>437</td>
<td>$p = 19$</td>
<td>623</td>
</tr>
<tr>
<td>$p = 41$</td>
<td>313</td>
<td>$p = 29$</td>
<td>3103</td>
</tr>
<tr>
<td>$p = 61$</td>
<td>601</td>
<td>$p = 29$</td>
<td>10133</td>
</tr>
<tr>
<td>$p = 73$</td>
<td>527</td>
<td>$p = 31$</td>
<td>5095</td>
</tr>
<tr>
<td>$p = 83$</td>
<td>161</td>
<td>$p = 31$</td>
<td>50645</td>
</tr>
</tbody>
</table>

Table of $M_n^+(7) \neq M_n^*$ for $G = \mathbb{Z}_{7^n} \times \mathbb{Z}_p^n$, $n = 2, 3, 4$, $p \leq 103$:

<table>
<thead>
<tr>
<th></th>
<th>$n = 2$</th>
<th>$n = 3$</th>
<th>$n = 4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p = 5$</td>
<td>18</td>
<td>$p = 7$</td>
<td>443</td>
</tr>
<tr>
<td>$p = 19$</td>
<td>54</td>
<td>$p = 5$</td>
<td>803</td>
</tr>
<tr>
<td>$p = 23$</td>
<td>118</td>
<td>$p = 43$</td>
<td>3623</td>
</tr>
<tr>
<td>$p = 29$</td>
<td>41</td>
<td>$p = 89$</td>
<td>1485</td>
</tr>
</tbody>
</table>

Table of $M_n^+(10) \neq M_n^*$, for primes such that $5 \mid M_n^+(2) \neq M_n^*$ or $2 \mid M_n^+(5) \neq M_n^*$ for $G = \mathbb{Z}_{2^n \cdot 5^k} \times \mathbb{Z}_p^n$, $n = 2, 3, 4$, $p \leq 103$:

<table>
<thead>
<tr>
<th></th>
<th>$n = 2$</th>
<th>$n = 3$</th>
<th>$n = 4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p = 31$</td>
<td>117</td>
<td>$p = 29$</td>
<td>2463</td>
</tr>
<tr>
<td>$p = 89$</td>
<td>707</td>
<td>$p = 41$</td>
<td>10399</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$p = 89$</td>
<td>24833</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$p = 89$</td>
<td>7552311</td>
</tr>
</tbody>
</table>

Table of $M_n^+(11) \neq M_n^*$ for $G = \mathbb{Z}_{11^n} \times \mathbb{Z}_p^n$, $n = 2, 3, 4$, $p \leq 103$:

<table>
<thead>
<tr>
<th></th>
<th>$n = 2$</th>
<th>$n = 4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p = 61$</td>
<td>432</td>
<td>225947</td>
</tr>
<tr>
<td>$p = 67$</td>
<td>248</td>
<td>905953</td>
</tr>
<tr>
<td>$p = 71$</td>
<td>26</td>
<td>381718</td>
</tr>
<tr>
<td>$p = 83$</td>
<td>161</td>
<td></td>
</tr>
</tbody>
</table>
Similarly, fixing \( p \) we can evaluate \( \mathcal{P}_G \) for varying \( m \):

**Example 4.1.** Suppose that \( G = \mathbb{Z}_m \times \mathbb{Z}_3^2 \) with \( 3 \nmid m \). Then

\[
\mathcal{P}_G = \begin{cases} 
8 & \text{if } 2 \nmid m, \\
17 & \text{if } m = 2n, \ 17 \nmid n, \ 3 \nmid \phi(n), \\
19 & \text{if } m = 2 \cdot 17n, \ 3 \nmid \phi(n), \\
64 & \text{if } m = 2 \cdot 5 \cdot 17 \cdot 19 \cdot 37 \cdot 53n \text{ or } m = 2 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 37 \cdot 53n, \ 2 \nmid n.
\end{cases}
\]

**Example 4.2.** Suppose that \( G = \mathbb{Z}_m \times \mathbb{Z}_5^2 \) with \( 5 \nmid \phi(m) \). Then

\[
\mathcal{P}_G = \begin{cases} 
7 & \text{if } 7 \nmid m, \\
18 & \text{if } m = 7n, \ (6, n) = 1, \\
26 & \text{if } m = 3 \cdot 7n, \ (26, n) = 1, \\
32 & \text{if } m = 3 \cdot 7 \cdot 13n, \ 2 \nmid n, \\
43 & \text{if } m = 2 \cdot 7n, \ 43 \nmid n.
\end{cases}
\]

For \( m = 2 \cdot 7 \cdot 43 \) we have \( \mathcal{P}_G = 49 \) or 51. Since 32 is a fifth power we can drop the restriction \( 5 \nmid \phi(m) \) when \( m = 3 \cdot 7 \cdot 13n, \ 2 \nmid n \).

**Example 4.3.** Suppose that \( G = \mathbb{Z}_m \times \mathbb{Z}_7^2 \) with \( 7 \nmid \phi(m) \). Then

\[
\mathcal{P}_G = \begin{cases} 
18 & \text{if } (6, m) = 1, \\
19 & \text{if } m = 2n \text{ or } m = 3n, \ 19 \nmid n, \\
31 & \text{if } m = 2 \cdot 19n \text{ or } m = 3 \cdot 19n, \ 31 \nmid n, \\
50 & \text{if } m = 3 \cdot 19 \cdot 31n, \ (10, n) = 1, \\
67 & \text{if } m = 2 \cdot 19 \cdot 31n \text{ or } m = 3 \cdot 5 \cdot 19 \cdot 31n, \ 67 \nmid n, \\
68 & \text{if } m = 3 \cdot 5 \cdot 19 \cdot 31 \cdot 67n, \ (2, 17, n) = 1, \\
79 & \text{if } m = 2 \cdot 19 \cdot 31 \cdot 67n \text{ or } m = 3 \cdot 5 \cdot 17 \cdot 19 \cdot 31 \cdot 67n, \ 79 \nmid n, \\
97 & \text{if } m = 2 \cdot 19 \cdot 31 \cdot 67 \cdot 79n \text{ or } m = 3 \cdot 5 \cdot 17 \cdot 19 \cdot 31 \cdot 67 \cdot 79n, \ 97 \nmid n, \\
99 & \text{if } m = 2 \cdot 19 \cdot 31 \cdot 67 \cdot 79 \cdot 97n, \ (3, 11, n) = 1, \\
116 & \text{if } m = 3 \cdot 5 \cdot 17 \cdot 19 \cdot 31 \cdot 67 \cdot 79 \cdot 97n, \ 2 \nmid n, \\
117 & \text{if } m = 2 \cdot 11 \cdot 19 \cdot 31 \cdot 67 \cdot 79 \cdot 97n, \ (3, 13, n) = 1, \\
129 & \text{if } m = 2 \cdot 11 \cdot 13 \cdot 19 \cdot 31 \cdot 67 \cdot 79 \cdot 97n, \ 3 \nmid n, \\
197 & \text{if } m = 2 \cdot 3 \cdot 19 \cdot 31 \cdot 67 \cdot 79 \cdot 97n.
\end{cases}
\]

Since 128 is a seventh power we can drop the restriction \( 7 \nmid \phi(m) \) and obtain \( \mathcal{P}_G = 128 \) when \( m = 3 \cdot 5 \cdot 17 \cdot 19 \cdot 29 \cdot 31 \cdot 67 \cdot 79 \cdot 97n, \ 2 \nmid n \).
Acknowledgment. The second author thanks Felipe Voloch for asking whether $P_{\mathbb{Z}_2 \times \mathbb{Z}_3} = 8$ or 17.

References


