ACTA ARITHMETICA
165.4 (2014)

Coefficients of a relative of cyclotomic polynomials

by

Ricky Ini Liu (Ann Arbor, MI)

1. Introduction. We define the *height* of a polynomial in $\mathbf{Z}[x]$ to be the maximum absolute value of its coefficients. It has long been known that the cyclotomic polynomials $\Phi_n(x)$ have a tendency to have small heights compared to n when n is divisible by few primes. For instance, if n is divisible by at most two odd primes, then the height of $\Phi_n(x)$ is 1 (see [8]). However, when $n = pqr$, where $p < q < r$ are odd primes, the height of $\Phi_n(x)$ is only bounded by a linear function in p (see [1]). On the other hand, Gallot and Moree [4] showed that any two adjacent coefficients of $\Phi_{pqr}(x)$ differ by at most 1, which is equivalent to saying that $(1-x)\Phi_{pqr}(x)$ has height 1. The heights of other cyclotomic polynomials and products of cyclotomic polynomials have been studied extensively elsewhere (see, for instance, [3, 5, 6, 7, 9, 11, 12]).

We generalize $\Phi_{pq}(x)$ and $(1-x)\Phi_{pqr}(x)$ by considering the polynomial

$$P_N(x) = \frac{(1-x^N)\prod_{1\le i<j\le n}(1-x^{N_{ij}})}{\prod_{i=1}^{n}(1-x^{N_i})},$$

where $N = p_1 \cdots p_n$ is a product of n distinct primes and $N_{i_1\ldots i_m} = N/(p_{i_1}\cdots p_{i_m})$. In some sense, $P_N(x)$ is a toy version of the cyclotomic polynomial in that $\Phi_N(x)$ can be written as a rational function containing in the numerator or denominator all $(1-x^{N_{i_1\cdots i_m}})$ while $P_N(x)$ contains only those for which $m \le 2$.

Let $M(n)$ be the maximum height of $P_N(x)$ when N has n distinct prime factors. Since $P_{pq}(x) = \Phi_{pq}(x)$ when $n = 2$, and $P_{pqr}(x) = (1-x)\Phi_{pqr}(x)$ when $n = 3$, it is already known that $M(2) = M(3) = 1$. We will show that $M(4) = 2$ as well as that $M(n)$ exists for all n, so that the height of $P_N(x)$ is bounded by a function in n that does not depend on the individual primes dividing N. We will also provide an explicit expression for the coefficients of $P_N(x)$ that generalizes the known expressions for the coefficients of $\Phi_{pq}(x)$,

2010 *Mathematics Subject Classification*: Primary 11C08; Secondary 11B83.
Key words and phrases: cyclotomic polynomial, height.

DOI: 10.4064/aa165-4-1

and we will exhibit polynomials $P_N(x)$ with height 1 for any n. Finally, we will show that although $M(n)$ is small when n is small, in fact $M(n)$ grows exponentially in n^2.

We begin in Section 2 with some preliminaries, including a short proof that the height of $\Phi_{pq}(x)$ is 1. In Section 3 we prove that the coefficients of $P_N(x)$ can be described in terms of the relative order of sums of residues of the form $p_j^{-1} \pmod{p_i}$, and we then use this to give an upper bound on $M(n)$. In Section 4 we explicitly and pictorially describe the coefficients of $P_N(x)$ for $n = 3$ and prove that $M(4) = 2$. In Section 5 we construct polynomials $P_N(x)$ with large height and thereby show that $M(n) = 2^{n^2/2+O(n\log n)}$. Finally, in Section 6 we construct $P_N(x)$ with height 1 for all n.

2. Preliminaries.

Let $n \geq 2$ be a positive integer, and let $N = p_1 \cdots p_n$ be the product of n distinct primes. For ease of notation throughout, we write $N_{i_1\cdots i_m} = N/(p_{i_1} \cdots p_{i_m})$ for any $i_1, \ldots, i_m \in [n]$.

Our main object of study is the following:

$$P_N(x) = \frac{(1 - x^N)\prod_{1\leq i<j\leq n}(1 - x^{N_{ij}})}{\prod_{i=1}^{n}(1 - x^{N_i})}.$$

Remark. Essentially all of the results below regarding the coefficients of $P_N(x)$ will hold even when the p_i are not distinct primes but only pairwise relatively prime positive integers greater than 1. However, we will assume that they are prime in order to simplify the statements of the results.

Proposition 2.1. *The rational function $P_N(x)$ is a polynomial with integer coefficients.*

Proof. Every root of the denominator is a primitive root of unity of degree $p_{i_1} \cdots p_{i_m}$ for some distinct $i_1, \ldots, i_m \in [n]$. Such a root appears $n - m$ times in the denominator and $1 + \binom{n-m}{2}$ times in the numerator. Since $\binom{n-m}{2} + 1 - (n - m) = \frac{1}{2}(n - m - 1)(n - m - 2) \geq 0$, $P_N(x)$ is a polynomial, and it has integer coefficients since both the numerator and denominator are monic integer polynomials (up to sign). ■

When $n = 2$ and $N = pq$, we have

$$P_{pq}(x) = \frac{(1 - x^{pq})(1 - x)}{(1 - x^p)(1 - x^q)} = \Phi_{pq}(x),$$

where Φ_{pq} is the pqth cyclotomic polynomial. Likewise, when $n = 3$ and $N = pqr$, we find that $P_{pqr}(x) = (1 - x)\Phi_{pqr}(x)$.

It is well known that Φ_{pq} has all of its coefficients at most 1 in absolute value (see, for instance, [8]), and Gallot and Moree [4] have recently shown that $(1-x)\Phi_{pqr}(x)$ also has this property. We give one proof of the result for Φ_{pq} below for illustrative purposes.

For a rational number $c = a/b$ with b relatively prime to m, we will write $[c]_m$ for the smallest nonnegative integer k such that $kb \equiv a \pmod{m}$. Note that $0 \le [c]_m \le m-1$.

We first need the following easy lemma.

Lemma 2.2. *Let p and q be distinct primes. Then*

$$(1 - x^{p[p^{-1}]_q}) + (x^{pq} - x^{q[q^{-1}]_p}) \equiv 1 - x \pmod{(1-x^p)(1-x^q)}.$$

Proof. Since $p[p^{-1}]_q + q[q^{-1}]_p = pq + 1$, the difference between the two sides is

$$x - x^{p[p^{-1}]_q} - x^{q[q^{-1}]_p} + x^{pq} = x(1 - x^{p[p^{-1}]_q - 1})(1 - x^{q[q^{-1}]_p - 1}),$$

and the two binomials are divisible by $1 - x^q$ and $1 - x^p$, respectively. ∎

We now derive an expression for $P_{pq}(x)$ that will allow us to easily extract its coefficients.

Proposition 2.3. *Modulo $1 - x^{pq}$, $P_{pq}(x)$ is congruent to the polynomial*

$$\frac{1-x^{pq}}{1-x^q}\,\frac{1-x^{p[p^{-1}]_q}}{1-x^p} + \frac{1-x^{pq}}{1-x^p}\,\frac{x^{pq}-x^{q[q^{-1}]_p}}{1-x^q}.$$

Proof. By subtracting $P_{pq}(x)$ from the above expression and dividing by $1 - x^{pq}$, we must show that

$$\frac{(1 - x^{p[p^{-1}]_q}) + (x^{pq} - x^{q[q^{-1}]_p}) - (1-x)}{(1-x^p)(1-x^q)}$$

is a polynomial. But this follows from Lemma 2.2. ∎

Let us write

$$\{a<b\} = \begin{cases} 1 & \text{if } a<b, \\ 0 & \text{otherwise} \end{cases}$$

(and similarly for other inequalities).

Proposition 2.4. *For $0 \le k < pq$, the coefficient of x^k in $P_{pq}(x)$ is*

$$\{[kp^{-1}]_q < [p^{-1}]_q\} - \{[kq^{-1}]_p \ge [q^{-1}]_p\}.$$

Proof. The first summand in Proposition 2.3 can be written as

$$(1 + x^p + x^{2p} + \cdots + x^{([p^{-1}]_q - 1)p})(1 + x^q + x^{2q} + \cdots + x^{(p-1)q}).$$

This has terms of the form x^{ap+bq}, where $0 \le a < [p^{-1}]_q$ and $0 \le b < p$. But $[(ap+bq)p^{-1}]_q = a$, so modulo $1 - x^{pq}$ these are the terms x^k, $0 \le k < pq$, such that $[kp^{-1}]_q < [p^{-1}]_q$. A similar analysis of the second summand in Proposition 2.3 (as well as the fact that $\deg P_{pq} < pq$) gives the result. ∎

One can describe Proposition 2.4 pictorially as follows. (A similar diagram can be found in [3].) Construct an array with p rows and q columns such that the entry in the $(i+1)$st row and $(j+1)$st column is $[pj+qi]_{pq}$. Then to find the coefficient of x^k, we add 1 if k lies in the first $[p^{-1}]_q$ columns and subtract 1 if it lies in the last $p-[q^{-1}]_p$ rows. (See Figure 1.) There are therefore $[p^{-1}]_q[q^{-1}]_p$ coefficients equal to 1 and $(q-[p^{-1}]_q)(p-[q^{-1}]_p) = [p^{-1}]_q[q^{-1}]_p - 1$ coefficients equal to -1.

	+	+	+				
	0	5	10	15	20	25	30
	7	12	17	22	27	32	2
	14	19	24	29	34	4	9
–	21	26	31	1	6	11	16
–	28	33	3	8	13	18	23

Fig. 1. Finding the coefficients of $P_{pq}(x) = \Phi_{pq}(x)$ when $p=5$ and $q=7$. Since $p[p^{-1}]_q + q[q^{-1}]_p \equiv 1 \pmod{pq}$, we draw lines directly to the left and above 1 in the table. To find the coefficient of x^k, find k and add the signs in the corresponding row and column. Therefore the coefficient is 1 for the exponents in the northwest region, -1 for those in the southeast region, and 0 for the other two.

Recall that the *height* of a polynomial is the maximum absolute value of its coefficients. We will write $M(n)$ for the maximum height of $P_N(x)$ over all $N = p_1\cdots p_n$. We have just seen that $M(2)=1$.

The purpose of the next section is to provide a similar description of $P_N(x)$ for larger n and thereby derive an upper bound on $M(n)$ (in particular showing that $M(n)$ exists).

3. Coefficients of $P_N(x)$.

In Section 2, we have seen that for $0 \le k < pq$, the coefficient of x^k in $P_{pq}(x)$ depends only on the relative orders of the elements in $\{[kp^{-1}]_q, [p^{-1}]_q\}$ and $\{[kq^{-1}]_p, [q^{-1}]_p\}$. In this section we will show that a similar result holds for the coefficients of $P_N(x)$ in general. We will also provide an exponential upper bound on $M(n)$. This bound will be enough to show that $M(3)=1$, and we will see in Section 5 that this bound is in fact asymptotically tight.

We first mimic the strategy of Proposition 2.3: we will write $P_N(x)$ modulo $1-x^N$ as a linear combination of $(1-x^N)/(1-x^{N_i})$. In fact, we will do so in $2^{\binom{n}{2}}$ different ways. (We remark that this approach essentially expresses $P_N(x)$ as a "coboundary" à la Question 25 of Musiker and Reiner [10].)

Proposition 3.1. *Let $S \subset [n]\times[n]$ be a set such that for all integers $1 \le i \ne j \le n$, S contains exactly one of the ordered pairs (i,j) or (j,i).*

Then modulo $1-x^N$, $P_N(x)$ *is congruent to the polynomial*

$$\sum_{i=1}^{n}\biggl(\frac{1-x^N}{1-x^{N_i}}\prod_{(i,j)\in S}\frac{1-x^{[p_i^{-1}]_{p_j}N_j}}{1-x^{N_j}} \cdot\prod_{(j,i)\in S}\frac{x^N-x^{[p_i^{-1}]_{p_j}N_j}}{1-x^{N_j}}\prod_{\substack{1\le j_1<j_2\le n\\ j_1,j_2\ne i}}(1-x^{N_{j_1j_2}})\biggr).$$

Proof. Note that the denominator of each term on the left is the same as the denominator of $P_N(x)$. Therefore it suffices to show that, modulo the denominator $\prod_{i=1}^{n}(1-x^{N_i})$,

$$\sum_{i=1}^{n}\Bigl(\prod_{(i,j)\in S}(1-x^{[p_i^{-1}]_{p_j}N_j})\prod_{(j,i)\in S}(x^N-x^{[p_i^{-1}]_{p_j}N_j})\prod_{\substack{1\le j_1<j_2\le n\\ j_1,j_2\ne i}}(1-x^{N_{j_1j_2}})\Bigr) \equiv\prod_{1\le j_1<j_2\le n}(1-x^{N_{j_1j_2}}).$$

Note that $\prod_{i=1}^{n}(1-x^{N_i})$ is the least common multiple of $(1-x^{N_{i_1\cdots i_m}})^m$ as $\{i_1,\dots,i_m\}$ ranges over nonempty subsets of $[n]$ because any root of order $N_{i_1\dots i_m}$ appears m times. Therefore it suffices to check that the congruence holds modulo each $(1-x^{N_{i_1\cdots i_m}})^m$.

Note $1-x^{N_{i_1\cdots i_m}}$ divides the ith term on the left side $(m-1)+\binom{m-1}{2}=\binom{m}{2}$ times when $i\in\{i_1,\dots,i_m\}$, and $m+\binom{m}{2}=\binom{m+1}{2}$ times otherwise. It also divides the right side $\binom{m}{2}$ times.

If $m=1$, then $1-x^{N_{i_1}}$ divides all the terms on the left except when $i=i_1$. Reducing the exponents in that term modulo N_i, it suffices to observe that

$$[p_i^{-1}]_{p_j}N_j=N_i\frac{p_i[p_i^{-1}]_{p_j}-1}{p_j}+N_{ij}\equiv N_{ij}\pmod{N_i},$$

so each factor is congruent to the corresponding factor on the right.

When $m=2$, both sides are divisible by $1-x^{N_{i_1i_2}}$, and all but the i_1th and i_2th terms on the left are divisible by its square. Let $y=x^{N_{i_1i_2}}$, and without loss of generality, assume $(i_1,i_2)\in S$. In the i_1th term, the factor corresponding to (i_1,i_2) is divisible by $1-y$, and any factor corresponding to (i_1,j) or (j,i_1) is congruent modulo $1-y$ to $1-x^{N_{i_1j}}$ by the calculation in the previous paragraph. Similarly reducing the i_2th term and ignoring the common factors on both sides, we find that it suffices to show that

$$(1-y^{p_{i_1}[p_{i_1}^{-1}]_{p_{i_2}}})+(y^{p_{i_1}p_{i_2}}-y^{p_{i_2}[p_{i_2}^{-1}]_{p_{i_1}}})\equiv 1-y\pmod{(1-y)^2}.$$

This follows from Lemma 2.2.

When $m \geq 3$, we have $\binom{m}{2} \geq m$, so both sides are divisible by $(1 - x^{N_{i_1 \cdots i_m}})^m$. ■

Using Proposition 3.1, we may now state a result similar to Proposition 2.4. Let us write $\overline{P}_N(x)$ for the reduction of $P_N(x)$ modulo $1 - x^N$ (so $\overline{P}_N(x)$ has degree less than N).

Theorem 3.2. *Let S be as in Proposition* 3.1, *and let*

$$f_i(k) = \prod_{(i,j)\in S} \{[kN_j^{-1}]_{p_j} < [p_i^{-1}]_{p_j}\} \prod_{(j,i)\in S} -\{[kN_j^{-1}]_{p_j} \geq [p_i^{-1}]_{p_j}\}.$$

The coefficient of x^k in $\overline{P}_N(x)$ is

$$\sum_{i=1}^{n} \sum_{A \subset A_i} (-1)^{|A|} f_i(k - N_A),$$

where A_i is the set consisting of two-element subsets of $[n] \setminus \{i\}$, and $N_A = \sum_{\{j_i, j_2\} \in A} N_{j_1 j_2}$. In particular, if $\deg P_N < N$, then this is also the coefficient of x^k in $P_N(x)$.

Proof. The expression

$$\frac{1 - x^N}{1 - x^{N_i}} \prod_{(i,j)\in S} \frac{1 - x^{[p_i^{-1}]_{p_j} N_j}}{1 - x^{N_j}} \prod_{(j,i)\in S} \frac{x^N - x^{[p_i^{-1}]_{p_j} N_j}}{1 - x^{N_j}}$$

is the sum of terms $\pm x^k$, where $k = \sum a_j N_j$ is such that $0 \leq a_i < p_i$, $0 \leq a_j < [p_i^{-1}]_{p_j}$ if $(i,j) \in S$, and $[p_i^{-1}]_{p_j} \leq a_j < p_j$ if $(j,i) \in S$, and the sign is given by the parity of the number of j in this last case. Note that $k \equiv a_j N_j \pmod{p_j}$, so $a_j \equiv [kN_j^{-1}]_{p_j}$. Thus the above expression modulo $1 - x^N$ is just $\sum_{k=0}^{N-1} f_i(k) x^k$. The result now follows easily from Proposition 3.1. ■

If $\overline{P}_N = P_N$, we find the following corollary.

Corollary 3.3. *If $\deg P_N < N$, then the coefficient of x^k in $P_N(x)$ for $k < N$ depends only on, for each j, the relative order of the $2^{n-1} + 1$ residues $[kN_j^{-1}]_{p_j}$ and $[\sum_{j' \in T} p_{j'}^{-1}]_{p_j}$ for all $T \subset [n] \setminus \{j\}$.*

Proof. First, observe that $f_i(k)$ depends only on the relative order of $[kN_j^{-1}]_{p_j}$, 0, and $[p_i^{-1}]_{p_j}$, for each j. For any $A \subset A_i$ as in Theorem 3.2, consider $k' = k - N_A$. We have $[N_{j_1 j_2} N_j^{-1}]_{p_j} = 0$ if $j \notin \{j_1, j_2\}$, while if instead $\{j_1, j_2\} = \{j, j'\}$, then $[N_{jj'} N_j^{-1}]_{p_j} = [p_{j'}^{-1}]_{p_j}$. Let $T_j = \{j' \mid \{j, j'\} \in A\}$. Then $k' N_j^{-1} \equiv kN_j^{-1} - \sum_{j' \in T_j} p_{j'}^{-1} \pmod{p_j}$. Thus $f_i(k')$ depends only on the relative order of $[kN_j^{-1}]_{p_j}$, $[\sum_{j'\in T_j} p_{j'}^{-1}]_{p_j}$, and $[\sum_{j'\in T_j\cup\{i\}} p_{j'}^{-1}]_{p_j}$, for each j. Considering all possible A and i and using Theorem 3.2 gives the result. ∎

In particular, these coefficients do not even depend on the specific primes p_i as long as the order of the residues is given. We will say N is *generic* if $\deg P_N < N$ and all the $[\sum_{j\in T} p_j^{-1}]_{p_i}$ are distinct for any fixed i. In this case, it follows that if we plot the integers $0 \le k < n$ at $([kN_1^{-1}]_{p_1}, \dots, [kN_n^{-1}]_{p_n})$, there exists an analogous diagram to Figure 1 with n dimensions and $2^{n(n-1)}$ regions. (The exponents k are plotted such that they increase by N_i modulo N in direction i.) In the next section we will investigate this diagram in more detail for the case $n = 3$.

The condition that $\deg P_N < N$ is fairly weak in that it holds always for small n and "most of the time" for large n.

Proposition 3.4. *If* $\sum_{i=1}^{n} 1/p_i < 2n/(n-1)$, *then* $\deg P_N < N$. *In particular, this holds if either* $n < 176$ *or every prime* p_i *is at least* $(n-1)/2$.

Proof. Let $A = \sum_{i=1}^{n} 1/p_i$. By Maclaurin's inequality,

$$1 - \frac{\deg P_N}{N} = A - \sum_{1\le i<j\le n} \frac{1}{p_i p_j} > A - \frac{n-1}{2n}A^2.$$

Thus if $A < 2n/(n-1)$, then $N > \deg P_N$.

If every prime p_i is at least $(n-1)/2$, then clearly $A < 2n/(n-1)$.

Suppose $\deg P_N \ge N$. We claim that $\deg P_{N'} \ge N'$, where N' is the product of the first n primes. It suffices to check that $A - \sum 1/(p_i p_j)$ decreases if we reduce any p_i and keep the others fixed. The coefficient of $1/p_i$ in this expression is $1 - \sum_{j\ne i} 1/p_j = 1 + 1/p_i - A$, which is negative since $A \ge 2n/(n-1) > 2 > 1 + 1/p_i$, proving the claim. Therefore it suffices to check that whenever N is the product of the first $n < 176$ primes, $\deg P_N < N$. This follows from a straightforward computer calculation. ∎

The smallest N for which $\deg P_N \ge N$ is the product of the first 176 primes, roughly 2.4182×10^{439}.

One can use Theorem 3.2 to give a bound on the largest absolute value of a coefficient of $P_N(x)$.

Corollary 3.5. *If* $\deg P_N < N$, *then every coefficient of* $P_N(x)$ *has absolute value at most* $n \cdot 2^{\binom{n-2}{2}-1}$.

Proof. Let us denote by f_i^S the function defined in Theorem 3.2 corresponding to the set S. Then since the theorem holds for all f_i^S (and the expression for the coefficients is linear in the f_i^S), it will also hold for the average $g_i = 2^{-\binom{n}{2}} \sum_S f_i^S$. Note that $|g_i(k)| = 2^{-(n-1)}$ for all k. Then

$$\Big|\sum_{i=1}^{n} \sum_{A \subset A_i} (-1)^{|A|} g_i(k - N_A)\Big| \le n \cdot 2^{|A_i|} \cdot 2^{-(n-1)} = n \cdot 2^{\binom{n-2}{2}-1}. \ \blacksquare$$

Although this bound looks rather weak, it is in fact fairly tight as we shall see in Section 5. As a special case, we can apply it when $n = 3$ to recover the result of Gallot and Moree [4].

Corollary 3.6. *We have* $M(3) = 1$. *In other words, all of the coefficients of* $(1 - x)\Phi_{pqr}(x)$ *have absolute value at most* 1.

Proof. Corollary 3.5 (along with Proposition 3.4) gives $M(3) \le 3/2$. ■

Applying Corollary 3.5 for $n = 4$ gives $M(4) \le 4$. We will show in the next section that in fact $M(4) = 2$.

We will need the following alternate descriptions of the coefficients of $P_N(x)$.

Proposition 3.7. *Let* p *be a prime not dividing* N, *and let* $a_N(k)$ *be the coefficient of* x^k *in* $P_N(x)$. *For any* $T \subset [n]$, *write* $N_T = \sum_{i\in T} N_i$. *Then*

$$a_{pN}(k) - a_{pN}(k - N) = \sum (-1)^{|T|} a_N(p^{-1}(k - N_T)),$$

where the sum ranges over all $T \subset [n]$ *for which* $k \equiv N_T \pmod{p}$ (*or, equivalently, for which* $kN^{-1} \equiv \sum_{i\in T} p_i^{-1} \pmod{p}$).

Proof. We can write

$$(1 - x^N)P_{pN}(x) = P_N(x^p) \prod_{i=1}^{n} (1 - x^{N_i}).$$

Computing the coefficient of x^k on both sides gives the result. ■

Note that if pN is generic, then the sum on the right side of Proposition 3.7 can have at most one term since the values $[\sum_{i\in T} p_i^{-1}]_p$ are all distinct.

Proposition 3.8. *Let* p *be a prime not dividing* N, *and let* $a_N(k)$ *and* N_T *be defined as in Proposition* 3.7. *If* $m_k = p^{-1}(k - N[kN^{-1}]_p)$, *then*

$$a_{pN}(k) - a_{pN}(k - pN) = \sum_{T\subset[n]} (-1)^{|T|} a_N(m_{k-N_T}).$$

Proof. Expanding the left side as the telescoping sum

$$(a_{pN}(k) - a_{pN}(k - N)) + (a_{pN}(k - N) - a_{pN}(k - 2N)) + \cdots \\ + (a_{pN}(k - (p - 1)N) - a_{pN}(k - pN))$$

and using Proposition 3.7, we see that each subset $T \subset [n]$ contributes to exactly one term $a_{pN}(k-cN)-a_{pN}(k-(c+1)N)$, where $k-cN \equiv N_T \pmod{p}$, or equivalently $c = [(k-N_T)N^{-1}]_p$. As $m_{k-N_T} = p^{-1}(k - N_T - cN)$, the result follows. ∎

We can use this to bound the growth of $M(n)$ without the restriction that $\deg P_N < N$.

Corollary 3.9. *We have* $M(n) \le 2^{n^2/2+O(n \log\log\log n)}$.

Proof. Note that it suffices to check $M(n)/M(n-1) \le 2^{n+O(\log\log\log n)}$.

We may write $a_N(k) = \sum_{i=0}^{\infty}(a_N(k-iN)-a_N(k-(i+1)N))$. By Proposition 3.8, each term on the right side is bounded by $2^{n-1}M(n-1)$. Moreover, the number of nonzero terms on the right side is bounded by

$$\left\lceil \frac{\deg P_N}{N} \right\rceil \le 1 + \frac{\deg P_N}{N} < 1 + \sum_{i=1}^{n} \frac{1}{p_i}.$$

If the p_i are in increasing order, then p_i is at least the ith smallest prime, which grows like $i \log i$. Hence $\sum_{i=1}^{n} 1/p_i = O(\log\log n)$, and the result follows. ∎

Note that this bound grows like $2^{n^2/2}$, just like the bound found in Corollary 3.5.

In a certain special case, we can simplify Proposition 3.8 to a form that will be useful later.

Proposition 3.10. *Let p be a prime not dividing $N = p_1 \cdots p_n$, and suppose that $\sum_{i=1}^{n} 1/p_i < 1$. Then for any integer k,*

$$a_{pN}(k) = \sum_{T \subset [n]} (-1)^{|T|} a_N(m'_{k-N_T})\{m'_{k-N_T} \le kp^{-1}\},$$

where $m'_k = [m_k]_N = [kp^{-1}]_N$.

Proof. By telescoping the sum in Proposition 3.8, we find that

$$a_{pN}(k) = \sum_{T \subset [n]} (-1)^{|T|} \sum_{j=0}^{\infty} a_N(m_{k-N_T} - jN).$$

By Proposition 3.4, since $\sum_{i=1}^{n} 1/p_i < 1$, $\deg P_N < N$. Thus each infinite sum has at most one nonzero term. This nonzero term must be $a_N([m_{k-N_T}]_N) = a_N(m'_{k-N_T})$, and it is present if and only if $m'_{k-N_T} \le m_{k-N_T}$. Since m_{k-N_T} was constructed to be the largest integer m such that $pm \equiv k - N_T \pmod{N}$ and $pm \le k - N_T$, and m'_{k-N_T} satisfies the first condition, we deduce that $m'_{k-N_T} \le m_{k-N_T}$ if and only if $pm'_{k-N_T} \le k - N_T$. But since both sides of this inequality are congruent modulo N, and $N_T = N\sum_{i\in T} 1/p_i < N$, we can equivalently drop the N_T on the right side, and the result follows. ∎

In other words, to find $a_{pN}(k)$, we find a number of terms of the form $\pm a_N(m)$, order them by m, and sum some initial segment of them. Moreover, note that increasing k by N only changes the initial segment and not the terms. If pN is generic, then by Proposition 3.7, the sum over any initial segment will equal $a_{pN}(k')$ for some $k' \equiv k \pmod{N}$.

Another consequence of Proposition 3.7 is that we can use it to show that many coefficients must vanish.

Proposition 3.11. *Suppose* $\deg P_N < N$ *and choose any* p_i *dividing* N. *Let* $0 < k < N_i$ *be an integer such that* $kN_i^{-1} \not\equiv [\sum_{j\in T} p_j^{-1}]_{p_i} \pmod{p_i}$ *for any* $T \subset [n] \setminus \{i\}$. *Then* $a_N(k) = 0$.

Proof. By Proposition 3.7, $a_N(k) = a_N(k - N_i) = 0$ (since the sum on the right hand side is empty and $k - N_i < 0$). ∎

Proposition 3.11 implies that a large number of the regions defined by Corollary 3.3 must yield coefficients of zero. Another way of stating Proposition 3.11 is to say that within a region corresponding to a nonzero coefficient, any two exponents adjacent in the ith direction differ by N_i (as opposed to $N - N_i$).

In the next section we will give a more explicit (and visual) description of Corollary 3.3 for the case $n = 3$.

4. The cases $n = 3$ and $n = 4$.

In this section, we will give a more explicit description of $P_N(x)$ when $n = 3$. (A similar description was found independently by Bzdęga [2].) We will then use this to show that $M(4) = 2$.

Let $N = pqr$. As per Corollary 3.3, we first need to determine the possible orders of the residues in $\{0, [p^{-1}]_r, [q^{-1}]_r, [p^{-1} + q^{-1}]_r\}$ (and the analogous sets for the other primes). Let us write $[c]_m^+ = [c]_m$ if $[c]_m \neq 0$ and $[c]_m^+ = m$ if $[c]_m = 0$.

Lemma 4.1. *Let* p, q, *and* r *be distinct primes. Then, up to permutation of* p, q, *and* r, *one of the following four possibilities holds:*

(1) $[p^{-1} + q^{-1}]_r^+ < [p^{-1}]_r \le [q^{-1}]_r$,
$[r^{-1}]_q \le [p^{-1}]_q < [p^{-1} + r^{-1}]_q^+$,
$[q^{-1}]_p \le [r^{-1}]_p < [q^{-1} + r^{-1}]_p^+$.

(2) $[p^{-1} + q^{-1}]_r^+ < [p^{-1}]_r \le [q^{-1}]_r$,
$[r^{-1}]_q \le [p^{-1}]_q < [p^{-1} + r^{-1}]_q^+$,
$[r^{-1}]_p \le [q^{-1}]_p < [q^{-1} + r^{-1}]_p^+$.

(3) *The same as* (1) *but with all inequalities reversed.*

(4) *The same as* (2) *but with all inequalities reversed.*

Proof. Note that if $([p^{-1}]_r + [q^{-1}]_r)/r$ is at most 1, then $[p^{-1} + q^{-1}]_r^+$ is greater than both $[p^{-1}]_r$ and $[q^{-1}]_r$, while if it is greater than 1, then these inequalities are reversed. Since $p[p^{-1}]_q + q[q^{-1}]_p = pq + 1$, it follows that

$$(*) \qquad \frac{1}{r}([p^{-1}]_r + [q^{-1}]_r) + \frac{1}{q}([p^{-1}]_q + [r^{-1}]_q) + \frac{1}{p}([q^{-1}]_p + [r^{-1}]_p) \\ = 3 + \frac{1}{pq} + \frac{1}{pr} + \frac{1}{qr}.$$

Thus the three terms on the left side cannot all be at most 1. Moreover, they cannot all be greater than 1, for then the left side would be at least $3 + 1/p + 1/q + 1/r$. Thus either one or two of these terms are greater than 1.

Suppose that exactly one term on the left side of $(*)$ is greater than 1, say $([p^{-1}]_r + [q^{-1}]_r)/r$. We may assume without loss of generality that $[p^{-1}]_r \le [q^{-1}]_r$. If $[r^{-1}]_q > [p^{-1}]_q$, then

$$qr + 1 = q[q^{-1}]_r + r[r^{-1}]_q > q[p^{-1}]_r + r[p^{-1}]_q,$$

so

$$1 \ge \frac{1}{r}[p^{-1}]_r + \frac{1}{q}[p^{-1}]_q = 2 + \frac{1}{pr} + \frac{1}{pq} - \frac{1}{p}([r^{-1}]_p + [q^{-1}]_p) \\ \ge 1 + \frac{1}{pr} + \frac{1}{pq} > 1,$$

which is a contradiction. It follows that $[r^{-1}]_q \le [p^{-1}]_q$, and the only possibilities are then (1) and (2).

Suppose two of the three terms on the left side of $(*)$ are greater than 1. We may assume without loss of generality that $[q^{-1}]_r \le [p^{-1}]_r < [p^{-1}+q^{-1}]_r^+$. If $[r^{-1}]_q < [p^{-1}]_q$, then

$$qr + 1 = q[q^{-1}]_r + r[r^{-1}]_q < q[p^{-1}]_r + r[p^{-1}]_q,$$

so

$$1 < \frac{1}{r}[p^{-1}]_r + \frac{1}{q}[p^{-1}]_q = 2 + \frac{1}{pr} + \frac{1}{pq} - \frac{1}{p}([r^{-1}]_p + [q^{-1}]_p) \\ \le 1 + \frac{1}{pr} + \frac{1}{pq} - \frac{1}{p} < 1,$$

which is a contradiction (since $1/r + 1/q < 1$). This yields either (3) or (4). ■

It is now a simple matter to use Theorem 3.2 to calculate the coefficients of P_{pqr}. We will assume that N is generic (all other N can be obtained by degenerating these diagrams). For any integer $0 \leq k < pqr$, let

$$h(k) = ([k(qr)^{-1}]_p, [k(pr)^{-1}]_q, [k(pq)^{-1}]_r).$$

By Theorem 3.2, the coefficient of x^k can be written as a sum of three terms depending on the projections of $h(k)$ onto the three coordinate planes. If p, q, and r satisfy the first condition of Lemma 4.1 and the set S in Theorem 3.2 is taken to be $\{(q,p),(r,p),(r,q)\}$, then we obtain Figure 2. The coefficient of x^k is then the sum of the values corresponding to each of the three projections of $h(k)$ (where $+$ represents 1 and $-$ represents -1). This allows us to explicitly compute the coefficient of x^k for each of the 64 regions as shown in Figure 2. (Note that each region is a product of three half-open intervals that contain their lower endpoints but not their upper endpoints.)

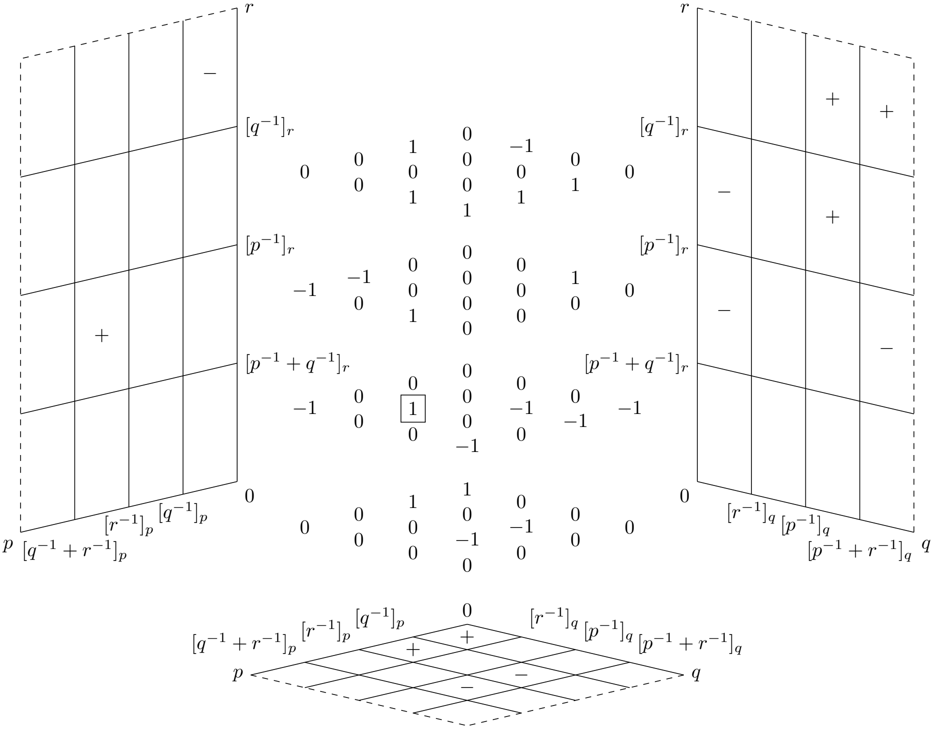

Fig. 2. Coefficients of $P_{pqr}(x)$ in case (1) of Lemma 4.1. To find the coefficient of x^k, compute $h(k) = ([k(qr)^{-1}]_p, [k(pr)^{-1}]_q, [k(pq)^{-1}]_r)$ and determine which of the 64 regions it lies in. (All intervals contain their lower endpoints but not their upper endpoints.) According to Theorem 3.2, the coefficient of x^k can be determined by summing the +'s and −'s from the three projections of its region as indicated. For instance, the coefficient of x^{71} in $P_{5\cdot 11\cdot 23}(x)$ is the boxed 1, which received a contribution of +1 from the projection along the q direction and no contributions from the other two projections.

If p, q, and r satisfy the second condition of Lemma 4.1, the resulting coefficients are given in Figure 3. The coefficients for when the third or fourth condition is satisfied are given by these same two figures if we reverse the direction of each of the axes. Note that it is evident from this that all of the coefficients of P_{pqr} are at most 1 in absolute value, so $M(3) = 1$.

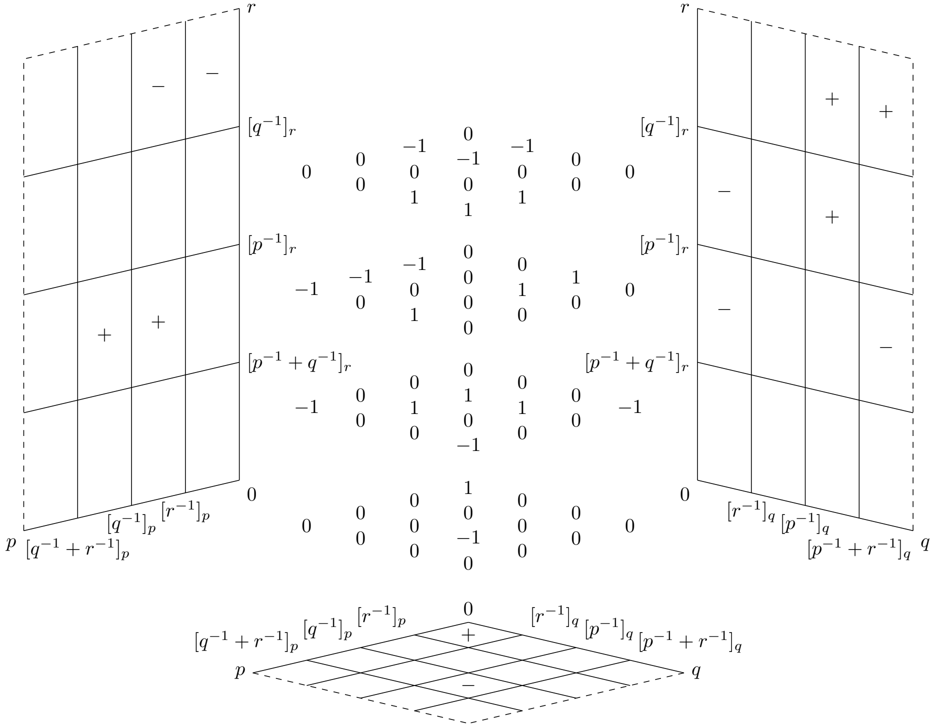

Fig. 3. Coefficients of $P_{pqr}(x)$ in case (2) of Lemma 4.1

Example. Let $p = 5$, $q = 11$, and $r = 23$. Then

$$[q^{-1}]_p = 1, \qquad [r^{-1}]_p = 2, \qquad [q^{-1}+r^{-1}]_p = 3,$$
$$[r^{-1}]_q = 1, \qquad [p^{-1}]_q = 9, \qquad [p^{-1}+r^{-1}]_q = 10,$$
$$[p^{-1}+q^{-1}]_r = 12, \qquad [p^{-1}]_r = 14, \qquad [q^{-1}]_r = 21,$$

which is part of case (1) of Lemma 4.1. To find the coefficient of x^{71}, we first calculate

$$h(71) = \big([71\cdot(11\cdot 23)^{-1}]_5, [71\cdot(5\cdot 23)^{-1}]_{11}, [71\cdot(5\cdot 11)^{-1}]_{23}\big) = (2,1,13).$$

(Indeed, $2\cdot(11\cdot 23) + 1\cdot(5\cdot 23) + 13\cdot(5\cdot 11) = 1336 \equiv 71 \pmod{5\cdot 11\cdot 23}$.) Thus the coefficient corresponds to the region from $[r^{-1}]_p$ to $[q^{-1}+r^{-1}]_p$, from $[r^{-1}]_q$ to $[p^{-1}]_q$, and from $[p^{-1}+q^{-1}]_r$ to $[p^{-1}]_r$. Then Figure 2 shows that the coefficient of x^{71} equals 1 (as indicated by the box).

We can also use these diagrams showing the coefficients of $P_{pqr}(x)$ to prove that $M(4) = 2$.

THEOREM 4.2. *We have $M(4) = 2$.*

Proof. Let p, q, r, and s be arbitrary distinct primes. Also let us assume that pqr satisfies the first condition of Lemma 4.1; the other cases are similar. For convenience, let us denote each of the 64 regions in Figure 2 by a triple of integers from 0 to 3 denoting its position in the p, q, and r directions, and let $f(xyz)$ denote the coefficient corresponding to the region xyz. For instance, 211 will refer to the region containing the coefficient of x^{71} in the example above, and so $f(211) = 1$.

Fix a residue $\bar{k}$ modulo $N = pqr$. By Proposition 3.10, the coefficients of x^k for $k \equiv \bar{k} \pmod{N}$ in $P_{Ns}(x)$ are partial sums of a signed sequence of eight coefficients of $P_N(x)$ that when plotted into the regions of Figure 2 lie at the corners of a rectangular box. Let us denote the corresponding exponents by $k_{000}, k_{001}, k_{010}, \dots, k_{111}$, and suppose that they lie in the eight (not necessarily distinct) regions $x_0y_0z_0, \dots, x_1y_1z_1$, so the corresponding signed term is $g_{abc} = (-1)^{a+b+c} f(x_a y_b z_c)$. The order in which the g_{abc} are summed is given by the order of the k_{abc}. Note that switching k_{0bc} and k_{1bc} for all b and c will only swap x_0 and x_1 and will therefore just change the sign of all the g_{abc} and not the order in which we sum them. Since this will not affect the absolute value of any partial sum, we will assume that $h(k_{000})$ is minimal in all three coordinate directions.

Note that the sum of all eight of the g_{abc} is 0 since the coefficients of x^k vanish for k sufficiently large. Then in order for a partial sum of these terms to be at least 3 in absolute value, at least six of the g_{abc} must be nonzero.

First suppose all the $x_a y_b z_c$ are distinct. Then by examining Figure 2 we see that there are only two places this can occur, namely either

$$x_a y_b z_c \in \{1,3\} \times \{0,3\} \times \{1,3\} \quad \text{or} \quad x_a y_b z_c \in \{1,3\} \times \{2,3\} \times \{1,3\}.$$

In the first case, we find

$$(g_{000}, g_{001}, g_{010}, g_{011}, g_{100}, g_{101}, g_{110}, g_{111}) = (0, -1, -1, 1, 1, 0, -1, 1).$$

In order to have a coefficient of absolute value at least 3, we must make sure that when the g_{abc} are ordered according to the k_{abc}, all the 1's come before all the -1's or vice versa. But this cannot happen: by Proposition 3.11, $k_{011} < k_{001}$ (since $f(133)$ and $f(103)$ are both nonzero) and likewise $k_{110} < k_{100}$. The second case is similar.

Therefore we may suppose that not all of the $x_a y_b z_c$ are distinct, say $x_0 = x_1$ (the other cases are similar). Then by Proposition 3.11, we have $k_{0bc} \le k_{1bc}$ if $g_{0bc} = -g_{1bc}$ is nonzero. So in order for some partial sum of the g_{abc} to have absolute value at least 3, at least three of the g_{0bc} must have the same sign. Then some $f(x_0 y_b z_c)$ must differ in sign from both $f(x_0 y_{1-b} z_c)$

and $f(x_0 y_b z_{1-c})$. But an inspection of Figure 2 shows that this cannot happen.

We have shown that $M(4) \leq 2$. Since the coefficient of x^{233} in $P_{5\cdot 7\cdot 11\cdot 13}(x)$ is -2, we must have $M(4) = 2$, as desired. ∎

Having analyzed $M(n)$ for small values of n, we will give an asymptotic bound for $M(n)$ in the next section.

5. Asymptotics of $M(n)$.

In this section, we will show that, although from the values $M(2) = M(3) = 1$ and $M(4) = 2$ it might appear that $M(n)$ grows slowly, in fact it grows exponentially in n^2. To place a lower bound on $M(n)$, we will inductively construct a polynomial $P_N(x)$ with a large coefficient by applying Proposition 3.10.

We first need to show that there exist N which yield arbitrarily large regions. Let $N = p_1 \cdots p_n$, and let $S_j(N)$ be the multiset $\{[\sum_{i\in T} p_i^{-1}]_{p_j} \mid T \subset [n] \setminus \{j\}\}$. Let us write $d(S_j(N))$ for the smallest difference between two elements of $S_j(N) \cup \{p_j\}$ (corresponding to different subsets T). Thus $d(S_j(N))$ is the smallest length of any region in the jth direction, and N is generic if $d(S_j(N)) \geq 1$ for all j. We will examine what happens when we add to p_j a multiple of N_j. Clearly this will not change $S_i(N)$ for any $i \neq j$.

Lemma 5.1. *Fix $T \subset [n] \setminus \{j\}$, and define z_T to be the fractional part of $\sum_{i\in T}(1 - [p_j^{-1}]_{p_i}/p_i)$. Then $p_j z_T + \sum_{i\in T} 1/p_i$ is an integer congruent to $\sum_{i\in T} p_i^{-1}$ modulo p_j. In particular, if $\sum_{i\in T} 1/p_i < 1$ and T is nonempty, then $[\sum_{i\in T} p_i^{-1}]^+_{p_j} = \lceil p_j z_T \rceil$.*

Proof. Since $p_i p_j + 1 = p_i[p_i^{-1}]_{p_j} + p_j[p_j^{-1}]_{p_i}$, we have

$$[p_i^{-1}]_{p_j} = p_j\left(1 - \frac{1}{p_i}[p_j^{-1}]_{p_i}\right) + \frac{1}{p_i}.$$

Summing over all i gives the result. ∎

Note that z_T only depends on the residue of p_j modulo N_j. This means that increasing p_j by some multiple of N_j will tend to keep the residues we care about in the same order while increasing the gaps in between them.

In particular, each z_T is a rational number with denominator $\prod_{i\in T} p_i$ (when written in reduced form). Hence any two z_T differ by at least $1/N_j$. Thus if $p_j > aN_j$ for some integer a, then $d(S_j(N)) \geq a$.

Lemma 5.2. *Suppose that $\sum_{i=1}^n 1/p_i < 1$ and N is generic. Then there exists $N' = p'_1 \cdots p'_n$ and a positive constant $c < 1$ such that for all j, $p'_j > p_j$, the corresponding elements of $S_j(N)$ and $S_j(N')$ are in the same order, and $\lfloor n/2\rfloor + 1 < cp'_j < d(S_j(N'))$.*

Proof. We first construct $N'' = p''_1 \cdots p''_n$ such that for all j, $p''_j > p_j$, the corresponding elements of $S_j(N)$ and $S_j(N'')$ are in the same order, and $d(S_j(N'')) \geq 3$.

Fix some j. By Lemma 5.1, the elements of $S_j(N)$—which are distinct since N is generic—are in the same order as the z_T. Moreover, if we add a multiple of N_j to any p_j to get p''_j, this does not change the values (nor the order) of the z_T. By choosing p''_j sufficiently large, which is always possible by Dirichlet's theorem on primes in arithmetic progressions, we can ensure that the difference between any two $p''_j z_T$ is at least 3 (or as large as needed). Applying this process for all j gives the result.

Now choose c to be smaller than each $1/p''_j$. Then, as above, replace each p''_j with some $p'_j > (\lfloor n/2 \rfloor + 1)/c$ by adding multiples of the products of the other primes. We claim that the resulting N' satisfies the desired properties. By the argument above, we need only check the desired inequalities. Therefore it suffices to show that $1/p''_j < d(S_j(N'))/p'_j$. Fix j, and suppose that we are replacing p''_j with p'_j. Let the smallest difference $d(S_j(N'))$ between two elements of $S_j(N') \cup \{p'_j\}$ occur between $\lceil p'_j z_T \rceil$ and $\lceil p'_j z_{T'} \rceil$. (If the difference involves p'_j, take 1 for the corresponding z_T.) Then $(d(S_j(N')) + 1)/p'_j > |z_T - z_{T'}|$. But we know from before we replaced p''_j that $|\lceil p''_j z_T \rceil - \lceil p''_j z_{T'} \rceil| \geq d(S_j(N''))$, so $|z_T - z_{T'}| > (d(S_j(N'')) - 1)/p''_j$. We find that

$$\frac{d(S_j(N'))}{p'_j} > |z_T - z_{T'}| - \frac{1}{p'_j} > \frac{d(S_j(N'')) - 1}{p''_j} - \frac{1}{p'_j} > \frac{2}{p''_j} - \frac{1}{p''_j} = \frac{1}{p''_j}. \blacksquare$$

By ensuring that $d(S_j(N'))$ is large, we are guaranteed that the regions in which the coefficients are constant are large. Recall that when we add another prime, the coefficients of the new polynomial can be written as signed sums of coefficients of the old polynomial. Therefore, having large regions will allow us to use the maximum coefficient many times in these sums, thereby generating a large coefficient in the new polynomial.

Lemma 5.3. *Let $N = p_1 \cdots p_n$ be generic with $\sum_{i=1}^{n} 1/p_i < 1$. Then there exists $N' = p'_1 \cdots p'_n$ and q prime such that $N'q$ is generic with $1/q + \sum_{i=1}^{n} 1/p'_i < 1$ and the height of $P_{N'q}(x)$ is at least $\binom{n-1}{\lfloor (n-1)/2 \rfloor}$ times the height of $P_N(x)$.*

Proof. First find N' and c as in Lemma 5.2, and let M be the coefficient of maximum absolute value in $P_{N'}(x)$. Then, by the Chinese Remainder Theorem, choose q such that $q > N'$ (which implies $\sum 1/p'_i + 1/q < 1$) and $q^{-1} \equiv \lfloor c p'_j \rfloor \pmod{p'_j}$ for all j. Since $q > N'$, $[\sum_{i \in T} p_i'^{-1}]_q$ are distinct for all $T \subset [n]$ as in the discussion following Lemma 5.1. Moreover, we have $[q^{-1}]_{p'_j} \leq c p'_j < d(S_j(N'))$, so $N'q$ is generic.

For an integer $\bar{k}$, consider the exponents $[q^{-1}(\bar{k}-\sum_{j\in T} N'_j)]_{N'}$ for $T \subset [n]$. Since

$$\Big[q^{-1}\Big(\bar{k} - \sum_{j\in T} N'_j\Big)\Big]_{N'} \equiv [q^{-1}\bar{k}]_{N'} - \sum_{j\in T}([q^{-1}]_{p'_j} N'_j) \pmod{N'},$$

these exponents will be plotted at the corners of a rectangular box with side lengths $[q^{-1}]_{p'_j}$. Since $[q^{-1}]_{p'_j} < d(S_j(N'))$, this box is smaller than the region corresponding to M, so we can find an integer $\bar{k}$ such that the coefficients of $P_{N'}(x)$ corresponding to exponents $[q^{-1}(\bar{k}-\sum_{j\in T} N'_j)]_{N'}$ are all equal to M. (In fact, we may take $\bar{k} = qk'$, where k' is the maximum exponent whose coefficient in $P_{N'}(x)$ is M.) Since $M \neq 0$, by Proposition 3.11,

$$\Big[q^{-1}\Big(\bar{k}-\sum_{j\in T} N'_j\Big)\Big]_{N'} = [q^{-1}\bar{k}]_{N'}-\sum_{j\in T}([q^{-1}]_{p'_j} N'_j) = [q^{-1}\bar{k}]_{N'}-\sum_{j\in T}(\lfloor cp'_j\rfloor N'_j).$$

Observe that

$$cN' - N'_j = (cp'_j - 1)N'_j < \lfloor cp'_j \rfloor N'_j \le cp'_j N'_j = cN'.$$

Let $s = \lfloor n/2 \rfloor$, and suppose $T_1, T_2 \subset [n]$ with $|T_1| \le s$ and $|T_2| > s$. Without loss of generality, assume p'_1 is the smallest p'_j. Then, since $cp'_1 > s+1$,

$$\begin{aligned}\sum_{j\in T_2}(\lfloor cp'_j\rfloor N'_j) &> (s+1)(cN' - N'_1) = csN' + (cp'_1 - s - 1)N'_1 \\ &> csN' \ge \sum_{j\in T_1}(\lfloor cp'_j\rfloor N'_j).\end{aligned}$$

Thus all the exponents corresponding to sets T_1 of size at most s are greater than those corresponding to sets T_2 of size at least $s+1$. Choose $k \equiv \bar{k} \pmod{N'}$ such that

$$\Big[q^{-1}\Big(\bar{k} - \sum_{j\in T_1} N'_j\Big)\Big]_{N'} > kq^{-1} > \Big[q^{-1}\Big(\bar{k} - \sum_{j\in T_2} N'_j\Big)\Big]_{N'}$$

for all T_1 and T_2. (Such a k exists because $q^{-1}N' < 1$.) But now by Proposition 3.10,

$$\begin{aligned}&a_{qN'}(k)\\ &= \sum_{T\subset[n]}(-1)^{|T|} a_{N'}\Big(\Big[q^{-1}\Big(\bar{k} - \sum_{j\in T} N'_j\Big)\Big]_{N'}\Big)\cdot\Big\{\Big[q^{-1}\Big(\bar{k} - \sum_{j\in T} N'_j\Big)\Big]_{N'} \le kq^{-1}\Big\}\\ &= \sum_{\substack{T\subset[n]\\ |T|>s}}(-1)^{|T|}M = \sum_{i=s+1}^{n}(-1)^i\binom{n}{i}M = (-1)^{s+1}\binom{n-1}{n-s-1}M.\end{aligned}$$

Thus we have found the desired coefficient with large absolute value. ■

By iterating this procedure, we can construct $P_N(x)$ with large height. We obtain the following result.

Theorem 5.4. *We have* $M(n) = 2^{n^2/2+O(n\log n)}$.

Proof. By Lemma 5.3, $M(n)$ is bounded below by $\prod_{i=1}^{n-2}\binom{i}{\lfloor i/2\rfloor}$. It is well known that $\log\binom{i}{\lfloor i/2\rfloor} = i\log 2 + O(\log i)$. Summing this over the first $n-2$ values of i gives $(\log 2)n^2/2 + O(n\log n)$, so exponentiating leads to the desired lower bound. Combining this with the upper bound from Corollary 3.9, we get the result. ∎

6. $P_N(x)$ with height 1.

While we have shown that the maximum height of a polynomial $P_N(x)$ with n distinct prime factors grows exponentially in n^2, we will now prove that the minimum height of such a polynomial is in fact 1. We first describe how to construct such an N.

Recall that if $N = p_1\cdots p_n$, then $S_j(N)$ is the multiset $\{[\sum_{i\in T} p_i^{-1}]_{p_j} \mid T \subset [n]\setminus\{j\}\}$, and $d(S_j(N))$ is the smallest difference between two elements of $S_j(N)\cup\{p_j\}$.

Lemma 6.1. *There exist primes* $p_1 < \cdots < p_n$ *satisfying the following conditions for all* u *and* v *such that* $1 \le u < v \le n$:

(a) $[p_v^{-1}]_{p_u} < d(S_u(p_1\cdots p_{v-1}))$;
(b) $p_v - [p_u^{-1}]_{p_v} < d(S_v(p_v\cdot p_1\cdots p_{u-1}))$;
(c) $\sum_{i=1}^n p_i^{-1} < 1$.

Note that conditions (a) and (b) are equivalent to specifying a particular ordering of $S_i(p_1\cdots p_n)$ for each i.

Proof of Lemma 6.1. For $n = 2$, take $p_1 < p_2$ to be any distinct primes.

Suppose that we have constructed $p_1,\dots,p_{n-1}$ satisfying the given conditions. As in Lemma 5.2, we can, in order, increase each p_i by a multiple of the others so that the orders of all the $S_i(p_1\cdots p_{n-1})$ are preserved, $d(S_i(p_1\cdots p_{n-1})) > 1$ for all i, and $p_{i+1} > 2p_i$ for $1 \le i \le n-2$.

Now let $p_n \equiv 1 \pmod{p_1\cdots p_{n-1}}$ be a prime large enough to satisfy (c). We need only check (a) and (b) when $v = n$. Condition (a) is obviously satisfied. For (b), since $p_i[p_i^{-1}]_{p_n} + p_n[p_n^{-1}]_{p_i} = p_ip_n + 1$, we have

$$p_n - [p_i^{-1}]_{p_n} = \frac{p_n[p_n^{-1}]_{p_i} - 1}{p_i} = \frac{p_n - 1}{p_i} = \lfloor p_i^{-1}p_n\rfloor.$$

Then

$$d(S_n(p_1p_n)) = \min\{\lfloor p_1^{-1}p_n\rfloor, \lfloor(1-p_1^{-1})p_n\rfloor\} = \lfloor p_1^{-1}p_n\rfloor.$$

Since

$$\lfloor p_2^{-1}p_n\rfloor \le \lfloor \tfrac{1}{2}p_1^{-1}p_n\rfloor \le \tfrac{1}{2}\lfloor p_1^{-1}p_n\rfloor,$$

we see that $d(S_n(p_1p_2p_n)) = \lfloor p_2^{-1}p_n\rfloor$. Continuing in this manner, we get

$$d(S_n(p_1p_2\dots p_ip_n)) = \lfloor p_i^{-1}p_n\rfloor < \lfloor p_{i-1}^{-1}p_n\rfloor = d(S_n(p_1p_2\dots p_{i-1}p_n))$$

for all i, as desired. ■

For the remainder of this section, we will assume that $N = p_1\cdots p_n$ as in Lemma 6.1. Note that the lemma implies that N is generic since $d(S_j(N)) > 0$ for all j. We claim that if we let $N = p_1\cdots p_n$ as in Lemma 6.1, then the height of $P_N(x)$ will be 1. The following lemma will allow us to work with the ordering of the $S_i(p_1\cdots p_n)$ more explicitly.

Let $h_i^N(k) = h_i(k) = [kN_i^{-1}]_{p_i}$, and let $x_i^N(k) = x_i(k)$ be the ith coordinate of the region containing k. In other words, $x_i(k)+1$ is the number of elements of $S_i(N)$ that are at most $h_i(k)$, so that $x_i(k)$ ranges from 0 to 2^n-1. (We will sometimes think of $h_i(k)$ as a residue modulo p_i.)

For subsets $V, W \subset [n]\setminus\{i\}$, let us write $V \prec_i h \prec_i W$ (and $V \prec_i W$) if

$$\Big[\sum_{j\in V} p_j^{-1}\Big]_{p_i} \le h < \Big[\sum_{j\in W} p_j^{-1}\Big]_{p_i}^{+}.$$

Then let $V_i^N(k) = V_i(k)$ and $W_i^N(k) = W_i(k)$ be the subsets of $[n]\setminus\{i\}$ such that for any k', $x_i(k') = x_i(k)$ if and only if $V_i(k) \prec_i h_i(k') \prec_i W_i(k)$. In other words, $V_i(k)$ and $W_i(k)$ are the subsets of $[n]\setminus\{i\}$ such that the corresponding elements of $S_i(N)$ bound the region containing k.

Lemma 6.2. *Let $N = p_1\cdots p_n$ be defined as in Lemma 6.1. For $i = n$, $n-1$, or $n-2$, the set $V_i(k)\cap\{n-2, n-1, n\}$ is determined by the residue of $x_i(k)$ modulo 4. Specifically, suppose V and W are subsets of $[n-3]$ such that $V \prec_i W$.*

(i) *If $i = n-2$, then*

$$V \prec_{n-2} V\cup\{n\} \prec_{n-2} V\cup\{n-1\} \prec_{n-2} V\cup\{n-1,n\} \prec_{n-2} W.$$

(ii) *If $i = n-1$, then*

$$V \prec_{n-1} V\cup\{n\} \prec_{n-1} W\cup\{n-2\} \prec_{n-1} W\cup\{n-2,n\} \prec_{n-1} W.$$

(iii) *If $i = n$, then*

$$V \prec_{n} W\cup\{n-2,n-1\} \prec_{n} W\cup\{n-2\} \prec_{n} W\cup\{n-1\} \prec_{n} W.$$

For instance, if $x_i(k) \equiv 0 \pmod 4$ for $i = n$, $n-1$, or $n-2$, then $V_i(k)\cap\{n-2,n-1,n\} = \emptyset$.

Proof of Lemma 6.2. This follows easily from Lemma 6.1: (i) follows from condition (a) when $(u,v) = (n-2,n-1)$ and $(n-2,n)$; (ii) follows from (b) when $(u,v) = (n-2,n-1)$ and from (a) when $(u,v) = (n-1,n)$; and (iii) follows from (b) when $(u,v) = (n-2,n)$ and $(n-1,n)$. ■

We will also need the following result (which holds for general N) in the style of Proposition 3.1.

Proposition 6.3. *Let p_i and p_j be distinct primes dividing N. Then modulo x^N-1,*

$$P_N(x) \equiv \frac{1-x^{[p_j^{-1}]_{p_i}N_i}}{1-x^{N_i}} P_{N_i}(x^{p_i}) \prod_{k\neq i,j}(1-x^{N_{ik}}) + x^{[p_j^{-1}]_{p_i}N_i} \frac{x^N - x^{[p_i^{-1}]_{p_j}N_j}}{1-x^{N_j}} P_{N_j}(x^{p_j}) \prod_{k\neq i,j}(1-x^{N_{jk}}).$$

Proof. The right side can be factored as

$$\frac{P_N(x)}{1-x^{N_{ij}}}\big((1-x^{[p_j^{-1}]_{p_i}N_i}) + x^{[p_j^{-1}]_{p_i}N_i}(x^N - x^{[p_i^{-1}]_{p_j}N_j})\big).$$

Subtracting this from the left side and multiplying by $1-x^{N_{ij}}$, we therefore need that

$$P_N(x)\big(1-x^{N_{ij}} - (1-x^{[p_j^{-1}]_{p_i}N_i}) - x^{[p_j^{-1}]_{p_i}N_i}(x^N - x^{[p_i^{-1}]_{p_j}N_j})\big)$$

is divisible by $(1-x^N)(1-x^{N_{ij}})$.

Since $[p_j^{-1}]_{p_i}N_i + [p_i^{-1}]_{p_j}N_j = N_{ij}([p_j^{-1}]_{p_i}p_j + [p_i^{-1}]_{p_j}p_i) = N + N_{ij}$, we have

$$\begin{aligned}(1-x^{[p_j^{-1}]_{p_i}N_i}) + x^{[p_j^{-1}]_{p_i}N_i}(x^N - x^{[p_i^{-1}]_{p_j}N_j}) &= x^{[p_j^{-1}]_{p_i}N_i}(x^N-1) + 1 - x^{N+N_{ij}} \\ &= (1-x^{N_{ij}}) + (x^N-1)(x^{[p_j^{-1}]_{p_i}N_i} - x^{N_{ij}}).\end{aligned}$$

Thus we just need that $P_N(x)(1-x^N)(x^{[p_j^{-1}]_{p_i}N_i} - x^{N_{ij}})$ is divisible by $(1-x^N)(1-x^{N_{ij}})$, which is clear because both exponents in the final term are divisible by N_{ij}. ∎

Let $0 \le \bar{k}_i < N_i$ be the integer such that

$$p_i\bar{k}_i + \textstyle\sum_{j\in V_i(k)} N_{ij} \equiv k \pmod{N_i}.$$

Dividing by N_j modulo p_j gives

$$h_j^{N_i}(\bar{k}_i) \equiv h_j(k) - [p_i^{-1}]_{p_j}\{j \in V_i(k)\} \pmod{p_j},$$

where $\{j \in V_i(k)\}$ equals 1 if $j \in V_i(k)$ and 0 otherwise. Then $V_j^{N_i}(\bar{k}_i)$ and $W_j^{N_i}(\bar{k}_i)$ are, as in the definition of $V_j(k)$ and $W_j(k)$, the subsets defining the interval containing $h_j(k) - [p_i^{-1}]_{p_j}\{j \in V_i(k)\}$ except that we only consider subsets not containing i.

Lemma 6.4. *Let $N = p_1\cdots p_n$ be as constructed in Lemma 6.1. Then for $0 \le k < N$,*

$$a_N(k) = (-1)^{|V_{n-1}(k)|}a_{N_{n-1}}(\bar{k}_{n-1})\{n \notin V_{n-1}(k)\} + (-1)^{|V_n(k)|}a_{N_n}(\bar{k}_n)\{n-1 \in V_n(k)\}.$$

Proof. Consider the right side of Proposition 6.3. For any $0 \le \bar{k}_i < N_i$, the product

$$\frac{1 - x^{[p_j^{-1}]_{p_i} N_i}}{1 - x^{N_i}} P_{N_i}(x^{p_i}) = \big(1 + x^{N_i} + x^{2N_i} + \cdots + x^{([p_j^{-1}]_{p_i} - 1)N_i}\big) P_{N_i}(x^{p_i})$$

contributes $a_{N_i}(\bar{k}_i)$ to the coefficient of $a_N(k)$ for $k = p_i \bar{k}_i + cN_i$ for $0 \le c < [p_j^{-1}]_{p_i}$. Considering all possible $\bar{k}_i$, the resulting values of k are exactly those for which $0 \le h_i(k) < [p_j^{-1}]_{p_i}$. Then the entire first term on the right side of Proposition 6.3 contributes, for each subset $V \subset [n] \setminus \{i, j\}$, $(-1)^{|V|} a_{N_i}(\bar{k}_i)$ to each $a_N(k)$ for which $h_i(k)$ lies in the half-open cyclic interval from $[\sum_{s \in V} p_s^{-1}]_{p_i}$ to $[\sum_{s \in V \cup \{j\}} p_s^{-1}]_{p_i}$. Now let $i = n-1$ and $j = n$. By Lemma 6.2(ii), the $a_N(k)$ that receive a contribution from this first term are those for which $n \notin V_{n-1}(k)$, and there can only be one such contribution, namely from $V = V_{n-1}(k)$. This yields the first term on the right side of the lemma's statement.

Similarly, the product

$$x^{[p_j^{-1}]_{p_i} N_i} \frac{x^N - x^{[p_i^{-1}]_{p_j} N_j}}{1 - x^{N_j}} P_{N_j}(x^{p_j})$$

contributes, for each $0 \le \bar{k}_j < N_j$, $-a_{N_j}(\bar{k})$ to those $a_N(k)$ for which

$$\begin{aligned} k &\equiv [p_j{}^{-1}]_{p_i} N_i + [p_i^{-1}]_{p_j} N_j + cN_j + p_j \bar{k}_j = p_j \bar{k}_j + N + N_{ij} + cN_j \\ &\equiv p_j \bar{k}_j + N_{ij} + cN_j \pmod{N} \end{aligned}$$

for $0 \le c < p_j - [p_i{}^{-1}]_{p_j}$. Over all $\bar{k}_j$, these are those k for which $[p_i^{-1}]_{p_j} \le h_j(k) < p_j$. Then the entire second term on the right side of Proposition 6.3 contributes, for each subset $W \subset [n] \setminus \{i, j\}$, $(-1)^{|W|+1} a_{N_j}(\bar{k}_j)$ to each $a_N(k)$ for which $h_j(k)$ lies in the half-open cyclic interval from $[\sum_{s \in W \cup \{i\}} p_s^{-1}]_{p_j}$ to $[\sum_{s \in W} p_s^{-1}]_{p_j}$. When $i = n-1$ and $j = n$, by Lemma 6.2(iii), there can again be at most one contribution to any $a_N(k)$, namely when $n-1 \in V_n(k)$ and $V_n(k) = W \cup \{n-1\}$, which yields the second term above, completing the proof. ∎

Note that this lemma implies that if $n \in V_{n-1}(k)$ and $n-1 \notin V_n(k)$, then $a_N(k) = 0$.

We can also prove a slightly different version of Lemma 6.4.

LEMMA 6.5. *Let $N = p_1 \cdots p_n$ be as constructed in Lemma 6.1. For $0 \le k < N$,*

$$\begin{aligned} a_N(k) = {} & (-1)^{|V_{n-1}(k)|} a_{N_{n-1}}([\bar{k}_{n-1} - N_{n-1,n}]_{N_{n-1}}) \{n \notin V_{n-1}(k)\} \\ & + (-1)^{|V_n(k)|} a_{N_n}([\bar{k}_n + N_{n-1,n}]_{N_n}) \{n-1 \in V_n(k)\}. \end{aligned}$$

Proof. As in Proposition 6.3,

$$P_N(x) \equiv \frac{x^N - x^{[p_j^{-1}]_{p_i} N_i}}{1 - x^{N_i}} P_{N_i}(x^{p_i}) \prod_{k \neq i,j} (1 - x^{N_{ik}})$$
$$+ x^{[p_j^{-1}]_{p_i} N_i} \frac{1 - x^{[p_i^{-1}]_{p_j} N_j}}{1 - x^{N_j}} P_{N_j}(x^{p_j}) \prod_{k \neq i,j} (1 - x^{N_{jk}})$$

modulo $x^N - 1$. Now apply the same argument as in Lemma 6.4 with $i = n$ and $j = n - 1$. ∎

(Alternatively, one can use Proposition 3.7 to compare the corresponding terms in Lemmas 6.4 and 6.5.)

We are now ready to prove the main theorem of this section.

Theorem 6.6. *Let $N = p_1 \cdots p_n$ be as constructed in Lemma* 6.1. *Then $|a_N(k)| \leq 1$ for all k.*

Proof. We proceed by induction on n, having proven the cases $n \leq 3$ previously. Note that if $p_1, \dots, p_n$ satisfy the conditions of Lemma 6.1, then so does any subset of them.

By the induction hypothesis, we may assume that none of the four terms on the right sides of Lemmas 6.4 and 6.5 vanish. In particular, this implies that $n \notin V_{n-1}(k)$, so $x_{n-1}(k)$ is even, and similarly $n - 1 \in V_n(k)$, so $x_n(k)$ is odd.

Suppose $x_n(k) \equiv 1 \pmod 4$, so that $n-2, n-1 \in V_n(k)$. We claim that $x_{n-1}(k) \equiv 2 \pmod 4$ and $x_{n-2}(k) \equiv 2 \pmod 4$. Indeed, suppose $x_{n-1}(k) \equiv 0 \pmod 4$, so that $n-2, n \notin V_{n-1}(k)$.

If $x_{n-2}(k) \equiv 0 \pmod 4$, then let $m' = [\bar{k}_n + N_{n-1,n}]_{N_n}$. Since $n-2 \in V_n(k)$ and $W_{n-2}(k)$ contains n but not $n-1$, it follows that $W_{n-2}^{N_n}(\bar{k}_n) \setminus \{n\} = W_{n-2}(k)$ does not contain $n-1$, so $n-1 \in V_{n-2}^{N_n}(\bar{k}_n) = V_{n-2}^{N_n}(m')$. Similarly, since $n-1 \in V_n(k)$ and $W_{n-1}(k)$ contains n but not $n-2$, we see that $n - 2 \in V_{n-1}^{N_n}(\bar{k}_n)$. Then since $x_{n-1}^{N_n}(m') = x_{n-1}^{N_n}(\bar{k}_n) + 1$, $n-2 \notin V_{n-1}^{N_n}(m)$. But then applying Lemma 6.4 to $a_{N_n}(m')$ implies that it equals 0, which we assumed was not the case.

Likewise, if $x_{n-2}(k) \not\equiv 0 \pmod 4$, then let $\ell = \bar{k}_{n-1}$. A similar argument to the above implies that $n-2 \notin V_n^{N_{n-1}}(\ell)$ and $n \in V_{n-2}^{N_{n-1}}(\ell)$, so that again by Lemma 6.4, $a_{N_{n-1}}(\ell) = 0$, which we assumed was not the case. It follows that if $x_n(k) \equiv 1 \pmod 4$, then $x_{n-1}(k) \equiv 2 \pmod 4$. Then we still have $n-2 \notin V_n^{N_{n-1}}(\ell)$, but now $n \in V_{n-2}^{N_{n-1}}(\ell)$ if and only if $x_{n-2}(k) \not\equiv 2 \pmod 4$. Therefore if $a_{N_{n-1}}(\ell) \neq 0$, then we must have $x_{n-2}(k) \equiv 2 \pmod 4$.

Assume then that $x_n(k) \equiv 1 \pmod 4$ and $x_{n-1}(k) \equiv x_{n-2}(k) \equiv 2 \pmod 4$, and let $m = \bar{k}_n$ and $\ell = \bar{k}_{n-1}$ so that

$$a_N(k) = (-1)^{|V_{n-1}(k)|} a_{N_{n-1}}(\ell) + (-1)^{|V_n(k)|} a_{N_n}(m).$$

From the above, $n-2 \notin V_n^{N_{n-1}}(\ell)$ and $n \notin V_{n-2}^{N_{n-1}}(\ell)$, so

$$a_{N_{n-1}}(\ell) = (-1)^{|V_{n-2}^{N_{n-1}}(\ell)|} a_{N_{n-1,n-2}}(\bar{\ell}_{n-2}),$$

where $\bar{\ell}_{n-2}$ is defined as in Lemma 6.4 applied to $a_{N_{n-1}}(\ell)$. Similarly, $n-2 \notin V_{n-1}^{N_n}(m)$ and $n-1 \notin V_{n-2}^{N_n}(m)$, so

$$a_{N_n}(m) = (-1)^{|V_{n-2}^{N_n}(m)|} a_{N_{n,n-2}}(\bar{m}_{n-2}).$$

Since $V_{n-2}^{N_{n-1}}(\ell) = V_{n-2}^{N_n}(m) = V_{n-2}(k) \cap [n-3]$, we have

$$(*) \quad \pm a_N(k) = (-1)^{|V_{n-1}(k)|} a_{N_{n-1,n-2}}(\bar{\ell}_{n-2}) + (-1)^{|V_n(k)|} a_{N_{n,n-2}}(\bar{m}_{n-2}).$$

Let $s = [\bar{k}_{n-2} - N_{n,n-2}]_{N_{n-2}}$. We claim that the right side of $(*)$ equals $-a_{N_{n-2}}(s)$, which will complete the proof in this case by the inductive hypothesis.

It is straightforward to check that $V_n^{N_{n-2}}(s) = V_n(k) \setminus \{n-2\}$ and that $V_{n-1}^{N_{n-2}}(s) = V_{n-1}(k) \setminus \{n-2\}$. Then by Lemma 6.4,

$$\begin{aligned} a_{N_{n-2}}(s) &= (-1)^{|V_{n-1}^{N_{n-2}}(s)|} a_{N_{n-1,n-2}}(\bar{s}_{n-1}) + (-1)^{|V_n^{N_{n-2}}(s)|} a_{N_{n,n-2}}(\bar{s}_n) \\ &= -\big((-1)^{|V_{n-1}(k)|} a_{N_{n-1,n-2}}(\bar{s}_{n-1}) + (-1)^{|V_n(k)|} a_{N_{n,n-2}}(\bar{s}_n)\big). \end{aligned}$$

Therefore it suffices to show that $a_{N_{n-1,n-2}}(\bar{\ell}_{n-2}) = a_{N_{n-1,n-2}}(\bar{s}_{n-1})$ and $a_{N_{n,n-2}}(\bar{m}_{n-2}) = a_{N_{n,n-2}}(\bar{s}_n)$.

For all $i \in [n] \setminus \{n-1, n-2\}$,

$$h_i^{N_{n-1,n-2}}(\bar{s}_{n-1}) = h_i^{N_{n-2}}(s) - [p_{n-1}^{-1}]_{p_i}\{i \in V_{n-1}^{N_{n-2}}(s)\}.$$

When also $i \neq n$, we have $h_i^{N_{n-2}}(s) = h_i^{N_{n-2}}(\bar{k}_{n-2})$, so since

$$V_{n-2}^{N_{n-1}}(\ell) = V_{n-2}(k) \setminus \{n-1\},$$

we get

$$\begin{aligned} h_i^{N_{n-1,n-2}}(\bar{s}_{n-1}) &= h_i^{N_{n-2}}(\bar{k}_{n-2}) - [p_{n-1}^{-1}]_{p_i}\{i \in V_{n-1}^{N_{n-2}}(s)\} \\ &= h_i^N(k) - [p_{n-2}^{-1}]_{p_i}\{i \in V_{n-2}(k)\} - [p_{n-1}^{-1}]_{p_i}\{i \in V_{n-1}^{N_{n-2}}(s)\} \\ &= h_i^N(k) - [p_{n-1}^{-1}]_{p_i}\{i \in V_{n-1}(k)\} - [p_{n-2}^{-1}]_{p_i}\{i \in V_{n-2}^{N_{n-1}}(\ell)\} \\ &= h_i^{N_{n-1}}(\ell) - [p_{n-2}^{-1}]_{p_i}\{i \in V_{n-2}^{N_{n-1}}(\ell)\} = h_i^{N_{n-1,n-2}}(\bar{\ell}_{n-2}). \end{aligned}$$

When $i = n$,

$$\begin{aligned} h_n^{N_{n-1,n-2}}(\bar{s}_{n-1}) &= h_n^{N_{n-2}}(s) = h_n^{N_{n-2}}(\bar{k}_{n-2}) - [p_{n-2}^{-1}]_{p_n} = h_n^N(k) - [p_{n-2}^{-1}]_{p_n} \\ &= h_n^{N_{n-1}}(\ell) - [p_{n-2}^{-1}]_{p_n} = h_n^{N_{n-1,n-2}}(\bar{\ell}_{n-2}) - [p_{n-2}^{-1}]_{p_n}. \end{aligned}$$

But since $x_n(k) \equiv 1 \pmod 4$, Lemma 6.2 implies that even with the shift of $[p_{n-2}^{-1}]_{p_n}$, $\bar{s}_{n-1}$ and $\bar{\ell}_{n-2}$ still lie in the same region for $N_{n-1,n-2}$, proving that $a_{N_{n-1,n-2}}(\bar{\ell}_{n-2}) = a_{N_{n-1,n-2}}(\bar{s}_{n-1})$. A similar argument gives

$$h_{n-1}^{N_{n,n-2}}(\bar{s}_n) = h_{n-1}^{N_{n,n-2}}(\bar{m}_{n-2}) - [p_{n-2}^{-1}]_{p_{n-1}} = h_{n-1}^{N}(k) - [p_{n-2}^{-1}]_{p_{n-1}} - [p_n^{-1}]_{p_{n-1}},$$

while $h_i^{N_{n,n-2}}(\bar{s}_n) = h_i^{N_{n,n-2}}(\bar{m}_{n-2})$ for $i \in [n-3]$, and Lemma 6.2 once again shows that $\bar{s}_n$ and $\bar{m}_{n-2}$ lie in the same region for $N_{n,n-2}$. This completes the proof in the case that $x_n(k) \equiv 1 \pmod 4$.

The only case remaining is when $x_n(k) \equiv 3 \pmod 4$. This follows by essentially the same argument as in the previous case: first, in order for the four terms on the right sides of Lemmas 6.4 and 6.5 not to vanish, we must have $x_{n-1}(k) \equiv x_{n-2}(k) \equiv 0 \pmod 4$. Then let $\ell' = [\bar{k}_{n-1} - N_{n-1,n}]_{N_{n-1}}$ and $m' = [\bar{k}_n + N_{n-1,n}]_{N_n}$ as in Lemma 6.5. Once again, we find that $n-2 \notin V_n^{N_{n-1}}(\ell') = V_n(k) \setminus \{n-1\}$ and $n \notin V_{n-2}^{N_{n-1}}(\ell') = V_{n-2}(k)$, so by Lemma 6.4,

$$a_{N_{n-1}}(\ell') = (-1)^{|V_{n-2}^{N_{n-1}}(\ell')|} a_{N_{n-1,n-2}}(\bar{\ell}'_{n-2}).$$

Similarly

$$a_{N_n}(m') = (-1)^{|V_{n-2}^{N_{n-2}}(m)|} a_{N_{n,n-2}}(\bar{m}'_{n-2}).$$

Then, since $V_{n-2}^{N_{n-1}}(\ell') = V_{n-2}^{N_n}(m') = V_{n-2}(k)$, we have

$$(**) \quad \begin{aligned} a_N(k) &= (-1)^{|V_{n-1}(k)|} a_{N_{n-1}}(\ell') + (-1)^{|V_n(k)|} a_{N_n}(m') \\ &= \pm\big((-1)^{|V_{n-1}(k)|} a_{N_{n-1,n-2}}(\bar{\ell}'_{n-2}) + (-1)^{|V_n(k)|} a_{N_{n,n-2}}(\bar{m}'_{n-2})\big). \end{aligned}$$

An analogous argument to the previous case now shows that the two terms on the right side of $(**)$ equal the two terms on the right side of Lemma 6.5 when applied to $a_{N_{n-2}}(\bar{k}_{n-2})$, which completes the proof by induction. ∎

Acknowledgments. The author would like to thank Victor Reiner for useful discussions and overall encouragement, as well as the anonymous referee for useful comments. This work was partially supported by NSF Postdoctoral Research Fellowship DMS 1004375.

References

[1] S. M. Beiter, *Magnitude of the coefficients of the cyclotomic polynomial $F_{pqr}(x)$*, Amer. Math. Monthly 75 (1968), 370–372.

[2] B. Bzdęga, *Jumps of ternary cyclotomic coefficients*, Acta Arith. 163 (2014), 203–213.

[3] S. Elder, *Flat cyclotomic polynomials: a new approach*, arXiv:1207.5811 (2012).

[4] Y. Gallot and P. Moree, *Neighboring ternary cyclotomic coefficients differ by at most one*, J. Ramanujan Math. Soc. 24 (2009), 235–248.

[5] Y. Gallot and P. Moree, *Ternary cyclotomic polynomials having a large coefficient*, J. Reine Angew. Math. 632 (2009), 105–125.

[6] N. Kaplan, *Flat cyclotomic polynomials of order three*, J. Number Theory 127 (2007), 118–126.

[7] N. Kaplan, *Bounds for the maximal height of divisors of $x^n - 1$*, J. Number Theory 129 (2009), 2673–2688.

[8] T. Y. Lam and K. H. Leung, *On the cyclotomic polynomial $\Phi_{pq}(X)$*, Amer. Math. Monthly 103 (1996), 562–564.

[9] P. Moree, *Inverse cyclotomic polynomials*, J. Number Theory 129 (2009), 667–680.

[10] G. Musiker and V. Reiner, *The cyclotomic polynomial topologically*, J. Reine Angew. Math. 687 (2014), 113–132.

[11] R. C. Vaughan, *Bounds for the coefficients of cyclotomic polynomials*, Michigan Math. J. 21 (1974), 289–295.

[12] J. Zhao and X. Zhang, *Coefficients of ternary cyclotomic polynomials*, J. Number Theory 130 (2010), 2223–2237.

Ricky Ini Liu
Department of Mathematics
University of Michigan
Ann Arbor, MI 48109, U.S.A.
E-mail: riliu@umich.edu

Received on 5.3.2013
and in revised form on 7.8.2014 (7363)