Uniwersytet im. Adama Mickiewicza w Poznaniu
Wydział Matematyki i Informatyki

Bartłomiej Bzdęga

O wielomianach cyklotomicznych

Rozprawa doktorska
napisana pod kierunkiem
prof. dra hab.
Wojciecha Gajdy

Poznań, 2012r.

Składam serdeczne podziękowania
Panu Profesorowi Wojciechowi Gajdzie
za okazaną życzliwość i pomoc
na mojej naukowej drodze.

Moim Rodzicom

Spis treści

Wstęp

Definicja 1. Wielomian cyklotomiczny Φ_n jest najmniejszym co do stopnia, unormowanym i nierozkładalnym nad $\mathbb{Z}$ wielomianem, którego pierwiastkiem jest pierwiastek z jedności

$$\zeta_n = e^{2\pi i/n} = \cos(2\pi i/n) + i\sin(2\pi i/n).$$

Symbolem $a_n(m)$ będziemy oznaczali współczynnik przy x^m w wielomianie Φ_n.

Pierwiastkami wielomianu Φ_n są wszystkie pierwiastki pierwotne stopnia n z jedności, z czego wynika, że wielomian $x^n - 1$ rozkłada się nad $\mathbb{Z}$ na iloczyn wielomianów $\Phi_d(x)$, w którym d przebiega wszystkie dzielniki n. Zastosowanie formuły odwrotnej Möbiusa pozwala uzyskać jawny wzór na $\Phi_n(x)$. Prowadzi to do następującego, podręcznikowego, faktu.

Fakt 2. Poniższe stwierdzenia są równoważne definicji 1.

- Φ_n jest unormowanym wielomianem, którego pierwiastkami są wszystkie pierwiastki pierwotne stopnia n z jedności, tj.

$$\Phi_n(x) = \prod_{(k,n)=1,\ 0<k<n} (x - \zeta_n^k),$$

- wielomiany cyklotomiczne spełniają zależność rekurencyjną

$$\prod_{d|n} \Phi_d(x) = x^n - 1,$$

- przez μ oznaczamy funkcję Möbiusa. Wtedy

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$

Na mocy pierwszego wzoru, wielomian Φ_n ma stopień $\varphi(n)$, gdzie φ jest funkcją Eulera. Ostatni ze wzorów, uzyskany przy pomocy formuły Möbiusa, jest najbardziej użyteczny. Korzystając z niego, można wyprowadzić następującą zależność.

Fakt 3. Niech N będzie iloczynem wszystkich dzielników pierwszych n. Wtedy

$$\Phi_n(x) = \Phi_N(x^{n/N}).$$

Ponadto, dla nieparzystych n zachodzi równość $\Phi_{2n}(x) = \Phi_n(-x)$.

Wobec tego wystarczy rozpatrywać jedynie takie wielomiany Φ_n, dla których n jest iloczynem różnych liczb pierwszych nieparzystych. W tej sytuacji sensowne jest wprowadzenie pojęcia rzędu wielomianu cyklotomicznego Φ_n w następujący sposób:

Definicja 4. *Rzędem* wielomianu cyklotomicznego Φ_n nazywamy liczbę nieparzystych dzielników pierwszych n. Samą liczbę n nazywamy *indeksem* bądź numerem wielomianu cyklotomicznego Φ_n.

Im wyższy rząd, tym trudniej jest obliczyć współczynniki wielomianu cyklotomicznego. Obrazują to poniższe wzory.

Fakt 5. Niech p, q i r będą różnymi liczbami pierwszymi. Zachodzą następujące równości.

$$\begin{aligned}
\Phi_p(x) &= \sum_{m=0}^{\varphi(p)} x^m, \\
\Phi_{pq}(x) &= \sum_{m=0}^{\varphi(pq)} \Big(\chi_2(m) - \chi_2(m-1)\Big) x^m, \\
\Phi_{pqr}(x) &= \sum_{m=0}^{\varphi(pqr)} \left(\sum_{k=m-p+1}^{m} \Big(\chi_3(k) - \chi_3(k-q) - \chi_3(k-r) + \chi_3(k-q-r)\Big) \right) x^m,
\end{aligned}$$

gdzie

$$\chi_2(m) = \begin{cases} 1, & \text{gdy } m = ap + bq, \\ 0, & \text{w przeciwnym razie,} \end{cases} \quad \chi_3(m) = \begin{cases} 1, & \text{gdy } m = aqr + brp + cpq, \\ 0, & \text{w przeciwnym razie,} \end{cases}$$

dla pewnych liczb całkowitych $a, b, c \geqslant 0$.

Pierwszy z tych wzorów jest bardzo łatwy do otrzymania. Drugi uzyskała Beiter [8], a trzeci Bloom [15].

Spośród własności współczynników wielomianów cyklotomicznych najbardziej intensywnie są badane te, które wymieniamy w poniższej definicji.

Definicja 6. Niech $P(x) = \sum_m a_m x^m \in \mathbb{R}[x]$ będzie dowolnym wielomianem. Następujące wartości

$$H(P) = \max_m |a_m|, \quad W(P) = \sum_m |a_m|, \quad L(P) = \sum_{m:\, a_m \neq 0} 1$$

nazywamy odpowiednio *wysokością*, *szerokością* i *długością* wielomianu P. Inaczej rzecz ujmując, jest to odpowiednio największy moduł współczynnika wielomianu P, suma modułów współczynników wielomianu P oraz liczba niezerowych współczynników tego wielomianu.

W pracach poświęconych wielomianom cyklotomicznym przyjęły się następujące oznaczenia, którym pozostaniemy wierni w niniejszej rozprawie.

$$A_n = H(\Phi_n), \quad S_n = W(\Phi_n), \quad \theta_n = L(\Phi_n).$$

Nad szacowaniem A_n, S_n oraz θ_n pracowali: Bachman [1, 2, 3, 4, 5, 6], Bateman [13, 14], Beiter [8, 9, 10, 11, 12], Erdös [24, 25, 26, 27, 28], Maier [38, 40, 41, 42, 43, 44], Moree [6, 23, 30, 31, 32, 49, 50], Pomerance [14, 51], Vaughan [14, 48, 53] i wielu innych.

Zasadniczą częścią niniejszej rozprawy doktorskiej będzie oszacowanie wszystkich trzech powyższych parametrów dla wielomianów cyklotomicznych rzędu 3. Wykażemy również istnienie wielomianów cyklotomicznych rzędu 2 o bardzo małej długości. Ponadto podamy nowe oszacowanie wartości A_n dla wielomianów cyklotomicznych dowolnego, ustalonego rzędu.

W rozdziale 1 udowodnimy następujące twierdzenie.

Twierdzenie 7 (Bzdęga [18], 2012)**.** *Niech $\varepsilon > 0$. Przez $B_\varepsilon(M)$ oznaczamy zbiór wielomianów cyklotomicznych Φ_n rzędu 2, dla których $n < M$ oraz $\theta_n < n^{1/2+\varepsilon}$. Wtedy*

$$\lim_{M\to\infty} \frac{\log(\#B_\varepsilon(M))}{\log M} = \frac{1}{2} + \varepsilon.$$

W szczególności, dla dowolnego $\varepsilon > 0$ istnieje nieskończenie wielomianów Φ_n rzędu 2, dla których $\theta_n < n^{1/2+\varepsilon}$.

Dość łatwo wykazać, że wykładnika $1/2$ w nierówności $\theta_n < n^{1/2+\varepsilon}$ nie można zmniejszyć. Tym samym uzyskany przez nas wynik jest najlepszy z możliwych.

Rozdział 2 poświęcony jest wielomianom cyklotomicznym rzędu 3. Niech liczby $p < q < r$ będą pierwsze i większe od 2. Wprowadzamy następujące oznaczenia:

$$\alpha = \min\{q^{-1}(p), r^{-1}(p), p - q^{-1}(p), p - r^{-1}(p)\},$$

$$\beta = (\alpha qr)^{-1}(p), \quad \beta^* = \min\{\beta, p - \beta\},$$

gdzie $a^{-1}(b) \in \{1, 2, \dots b-1\}$ spełnia kongruencję $aa^{-1}(b) \equiv 1 \pmod b$, lub innymi słowy, reprezentuje odwrotność a modulo b.

Twierdzenie 8 (Bzdęga [16], 2010)**.** *Zachodzi nierówność $A_{pqr} \leqslant \min\{2\alpha+\beta^*, p-\beta^*\}$.*

Twierdzenie 9 (Bzdęga [19], 2012)**.** *Niech ε_3 będzie najmniejszą liczbą dodatnią, dla której nierówność $A_{pqr} \leqslant \varepsilon_3 p$ zachodzi przy dowolnych liczbach pierwszych p, q, r. Wtedy $S_{pqr} \leqslant \frac{1}{2}p^2qr\varepsilon_3(2-\varepsilon_3)$.*

W obecnej chwili wiadomo, że $\frac{2}{3} \leqslant \varepsilon_3 \leqslant \frac{3}{4}$. Przypuszczenie $\varepsilon_3 = \frac{2}{3}$ znane jest jako poprawiona hipoteza Beiter, o której szerzej opowiemy w rozdziale 2.

Gallot i Moree oraz niezależnie autor niniejszej rozprawy wykazali następującą własność współczynników wielomianów cyklotomicznych rzędu 3.

Twierdzenie 10 (Gallot i Moree [31], 2009; Bzdęga [16], 2010)**.** *Każde dwa sąsiednie współczynniki wielomianu Φ_{pqr} różnią się o co najwyżej* 1*.*

W niniejszej rozprawie pójdziemy jeszcze o krok dalej, szacując liczbę tych m, dla których $a_{pqr}(m) = a_{pqr}(m-1)+1$. Liczbę tą oznaczamy przez J_{pqr}.

Twierdzenie 11 (Bzdęga [21])**.** *Dla wszystkich $n = pqr$ mamy $J_n = \Omega(n^{1/3})$.*

Dokładny wzór na liczbę J_{pqr} zaprezentujemy dalej, w Twierdzeniu 2.32, gdyż wymaga on wcześniejszego wprowadzenia kilku bardziej skomplikowanych definicji. Wykażemy również, że jeśli zachodzi hipoteza H Schinzla, to wykładnika $1/3$ nie można zwiększyć. Poniżej zamieszczamy bezpośredni wniosek z Twierdzenia 11.

Twierdzenie 12 (Bzdęga [21])**.** *Dla wszystkich $n = pqr$ zachodzi $\theta_n = \Omega(n^{1/3})$.*

Rozdział 3 poświęcony jest wielomianom cyklotomicznym wyższych rzędów. Dla $n = p_1p_2\ldots p_k$, gdzie $p_1 < p_2 < \ldots < p_k$, określamy

$$M_n = \prod_{j=1}^{k-2} p_j^{2^{k-j-1}-1}.$$

Udowodnimy następujące twierdzenie.

Twierdzenie 13 (Bzdęga [19], 2012)**.** *Zachodzi nierówność*

$$(A_n/M_n)^{2^{-k}} < C + o_k(1),$$

gdzie C jest pewną stałą mniejszą od 1*, a $o_k(1) \to 0$ dla $k \to \infty$.*

Zastosujemy twierdzenie 13 do poprawienia istniejących oszacowań w problemach pokrewnych. Udowodnimy także jego prawdziwość w szerszej klasie wielomianów włączania-wyłączania, oraz że oszacowanie w tej klasie jest optymalne z dokładnością do stałej C.

Rozdział 1

Wielomiany rzędu 2

Po wyznaczeniu pierwszych kilkudziesięciu wielomianów cyklotomicznych, stwierdzamy, że ich współczynniki należą do zbioru $\{-1, 0, 1\}$. Wbrew temu, co początkowo przypuszczano, nie jest to prawdą dla wszystkich Φ_n. Dla przykładu $A_{105} = 2$ i jest to przykład z najniższym możliwym indeksem. Odpowiedź na pytanie dlaczego tak się dzieje, daje poniższe twierdzenie.

Twierdzenie 1.1 (Migotti [45], 1883)**.** *Dla liczb pierwszych $p \neq q$ mamy $A_{pq} = 1$.*

Wystarczy je teraz połączyć z faktem 3 i zauważyć, że najmniejszą liczbą posiadającą trzy różne nieparzyste dzielniki pierwsze jest 105.

Jeśli współczynniki Φ_{pq} mogą przyjmować tylko trzy różne wartości, naturalne jest poszukiwanie kryterium, które pozwalałoby rozstrzygnąć, kiedy przyjmują one konkretną wartość. Problem ten rozwiązała Beiter.

Twierdzenie 1.2 (Beiter [8], 1960)**.** *Współczynnik przy x^m w wielomianie Φ_{pq} jest równy*

$$a_{pq}(m) = \chi_2(m) - \chi_2(m-1),$$

gdzie $\chi_2(m)$ przyjmuje wartość 1 jeśli $m = ap + bq$ dla pewnych całkowitych $a, b \geqslant 0$, natomiast w przeciwnym wypadku przyjmuje wartość 0.

Mając do dyspozycji tak proste kryterium, można dość łatwo policzyć, ile spośród współczynników wielomianu Φ_{pq} przyjmuje niezerową wartość.

Twierdzenie 1.3 (Carlitz [22], 1966)**.** *Liczba θ_{pq} niezerowych współczynników Φ_{pq} wynosi $2p^{-1}(q)q^{-1}(p) - 1$.*

W tej sytuacji znamy już $A_{pq} = 1$ oraz $S_{pq} = \theta_{pq}$ z powyższego twierdzenia. Pozostaje jednak pytanie, jak duże jest θ_n w porównaniu z n, dla $n = pq$. Najważniejsze

jest tu oszacowanie dolne, gdyż górne jest proste do uzyskania. Wynosi ono $(pq-1)/2$ [15] i jest osiągalne dla bliźniaczych liczb pierwszych p i q [14]. Ogólnie, statystyczna wielkość θ_{pq} to pq pomnożone przez pewną dodatnią stałą.

Niech $x = q^{-1}(p)/p$. Na mocy twierdzenia 1.3 oraz łatwej do udowodnienia równości $pp^{-1}(q) + qq^{-1}(p) = pq + 1$ uzyskujemy

$$\theta_{pq} = 2q^{-1}(p) \cdot \frac{pq + 1 - qq^{-1}(p)}{p} - 1 \geqslant 2pqx(1-x) - 1 \geqslant \frac{2q(p-1)}{p} - 1 \geqslant q,$$

gdyż $p, q > 2$. Analogicznie $\theta_{pq} \geqslant p$, stąd $\theta_{pq} \geqslant (pq)^{1/2}$. Naturalne jest pytanie, jak bardzo można się zbliżyć do $1/2$. Częściową odpowiedź podał H.W.Lenstra.

Twierdzenie 1.4 (H.W.Lenstra [39], 1979)**.** *Dla dowolnego $\varepsilon > 0$ nierówność $\theta_n < n^{8/13+\varepsilon}$ zachodzi dla nieskończenie wielu $n = pq$.*

W następnym podrozdziale wzmocnimy to twierdzenie, zmieniając $8/13$ na najlepszą możliwą stałą $1/2$.

1.1. Wielomiany o małej długości

W tym podrozdziale udowodnimy twierdzenie 7. Głównym narzędziem będzie tu następujący wynik.

Twierdzenie 1.5 (Hildebrand [33], 1985)**.** *Niech $P(m)$ oznacza największy dzielnik pierwszy liczby naturalnej $m \geqslant 2$. Zbiór*

$$\left\{m \in \mathbb{N} :\ m^\alpha < P(m) < m^\beta,\ (m+1)^\alpha < P(m+1) < (m+1)^\beta\right\}$$

ma dodatnią dolną gęstość naturalną dla dowolnych $0 \leqslant \alpha < \beta \leqslant 1$.

Dowód twierdzenia 7. Oznaczmy przez $Q_\varepsilon(m_0, M)$ zbiór liczb naturalnych z przedziału (m_0, M), dla których $P(m) > m^{1-\varepsilon}$ oraz $P(m+1) > (m+1)^{1-\varepsilon}$. Idea naszego dowodu polega na określeniu następujących funkcji:

$$\begin{array}{ccccc} Q_{\varepsilon_2}(m_0, M^{1/2+\varepsilon'}) \setminus Q_{\varepsilon_1} & \xrightarrow{f} & B_\varepsilon(M) \setminus [1, n_0] & \xrightarrow{g} & Q_{\varepsilon_3}(1, M^{1/2+\varepsilon}) \\ m & \overset{f}{\longmapsto} & P(m)P(m+1) & & \\ & & pq & \overset{g}{\longmapsto} & \min\{pp^{-1}(q), qq^{-1}(p)\} - 1, \end{array}$$

gdzie $\varepsilon' < \varepsilon$, natomiast ε_1, ε_2 $(\varepsilon_1 < \varepsilon_2)$, ε_3 oraz m_0, n_0 zależą tylko od ε i ε', a ponadto przeciwobraz każdej wartości funkcji f i g jest zbiorem skończonym, o liczbie elementów ograniczonej przez stałą T, zależną również tylko od ε i ε'.

Jeśli dla dowolnych $0 < \varepsilon' < \varepsilon < 1/2$ znajdziemy stałe ε_1, ε_2, ε_3 i m_0, n_0 dla których funkcje f i g są dobrze określone oraz spełniają opisany wcześniej warunek związany z przeciwobrazami, to na mocy twierdzenia 1.5 dowód będzie zakończony. Istotnie, wtedy

$$\lim_{M\to\infty} \frac{\log(\#B_\varepsilon(M))}{\log M} \leqslant \lim_{M\to\infty} \frac{\log(T\#Q_{\varepsilon_3}(1, M^{1/2+\varepsilon}))}{\log M} = \frac{1}{2} + \varepsilon,$$
$$\lim_{M\to\infty} \frac{\log(\#B_\varepsilon(M))}{\log M} \geqslant \lim_{M\to\infty} \frac{\log(\#(Q_{\varepsilon_2}(m_0, M^{1/2+\varepsilon'}) \setminus Q_{\varepsilon_1})/T)}{\log M} = \frac{1}{2} + \varepsilon',$$

a liczba ε' może być dowolnie blisko ε.

Wybierzmy tak stałe ε_1, ε_2, ε_3, aby spełniały warunki

$$\frac{\varepsilon'}{1/2+\varepsilon'} < \varepsilon_1 < \varepsilon_2 < \frac{\varepsilon}{1/2+\varepsilon} \quad \text{i} \quad \frac{2\varepsilon}{1/2+\varepsilon} < \varepsilon_3 < 1.$$

Niech $m_0 > n_0$ będą na tyle duże, aby dla $m, n > m_0$ zachodziły nierówności:

$$(m+1)^{\varepsilon_2} < m^{1-\varepsilon_2}, \quad 2n^{1/(2-2\varepsilon_2)} < n^{1/2+\varepsilon}, \quad m^{1-\varepsilon_1}(m+1)^{1-\varepsilon_1} < m^{1/(1/2+\varepsilon')}$$

oraz dla $n > n_0$ i $m > n_0^{1/2-\varepsilon} - 1$ – nierówności

$$n/3 > n^{3/4+\varepsilon/2} \quad \text{i} \quad m^{\frac{1/2-\varepsilon}{1/2+\varepsilon}} > (m+1)^{1-\varepsilon_3}.$$

Niech ponadto $T = \max\{2, (1-\varepsilon_3)^{-2}\}$.

Rozważmy najpierw funkcję f. Niech $p = P(m)$, $q = P(m+1)$ oraz $n = pq = f(m)$, gdzie $m \in Q_{\varepsilon_2}(m_0, M^{1/2+\varepsilon'}) \setminus Q_{\varepsilon_1}$. Wtedy

$$(m+1)/q < (m+1)^{\varepsilon_2} < m^{1-\varepsilon_2} < p,$$

zatem $qq^{-1}(p) = m+1$. Zaobserwujmy, że

$$n = f(m) > m^{2-2\varepsilon_2} > m > m_0 > n_0.$$

Korzystając z faktu $n > m > m_0$, uzyskujemy

$$f(m) < m^{1-\varepsilon_1}(m+1)^{1-\varepsilon_1} < m^{1/(1/2+\varepsilon')} < M,$$
$$\theta_n < 2qq^{-1}(p) = 2m+2 < 2n^{1/(2-2\varepsilon_2)} < n^{1/2+\varepsilon},$$

więc funkcja f jest dobrze określona.

Jeśli $P(m') = p$ oraz $P(m'+1) = q$, to $m' = m + kpq$ dla pewnego dodatniego całkowitego k i wtedy $m' \geqslant m + n > n = f(m')$, co prowadzi do sprzeczności

z uzyskaną wcześniej nierównością $f(m) > m$. Stąd przeciwobraz $f^{-1}(n)$ jest najwyżej dwupunktowy (drugi punkt mógłby powstać z zamiany q z p).

Kolej na funkcję g. Niech $n = pq \in B_\varepsilon(N) \setminus [1, n_0]$. Odnotujmy następujące fakty:

$$\begin{aligned} pp^{-1}(q) + qq^{-1}(p) &= pq + 1 = n + 1, \\ (pp^{-1}(q))(qq^{-1}(p)) &= np^{-1}(q)q^{-1}(p) < \frac{2}{3}n\theta_n < \frac{2}{3}n^{3/2+\varepsilon}. \end{aligned}$$

Załóżmy bez straty ogólności, że $pp^{-1}(q) < qq^{-1}(p)$. Wtedy

$$m = g(n) = \min\{pp^{-1}(q), qq^{-1}(p)\} - 1 = pp^{-1}(q) - 1.$$

Jeśli $pp^{-1}(q) > n^{1/2+\varepsilon}$, to na mocy drugiej nierówności $qq^{-1}(p) < \frac{2}{3}n$, a zatem na mocy pierwszej z nich

$$n/3 < pp^{-1}(q) < \sqrt{(pp^{-1}(q))(qq^{-1}(p))} < n^{3/4+\varepsilon/2},$$

co jest sprzecznością, gdyż $n > n_0$. Wobec tego

$$m = g(n) = pp^{-1}(q) - 1 < n^{1/2+\varepsilon} < M^{1/2+\varepsilon}.$$

Jak wykazano wcześniej, $\theta_n > p, q$, zatem $p, q < n^{1/2+\varepsilon}$. Ponieważ $n = pq$, mamy $p, q > n^{1/2-\varepsilon}$. W takim razie

$$m = pp^{-1}(q) - 1 > n^{1/2-\varepsilon} - 1 > n_0^{1/2-\varepsilon} - 1,$$

co pozwala skorzystać z podanej wcześniej nierówności prawdziwej dla $m > n_0^{1/2-\varepsilon} - 1$. Mamy zatem

$$p, q > n^{1/2-\varepsilon} > m^{\frac{1/2-\varepsilon}{1/2+\varepsilon}} > (m+1)^{1-\varepsilon_3} > m^{1-\varepsilon_3}.$$

Stąd $m \in Q_{\varepsilon_3}(1, M^{1/2+\varepsilon})$ i funkcja g jest dobrze określona.

Pozostaje zauważyć, że element $p'q'$ przeciwobrazu $g^{-1}(m)$ spełnia następujące warunki:

$$p' \mid m, \quad q' \mid m+1, \quad p' > m^{1-\varepsilon_3}, \quad q' > (m+1)^{1-\varepsilon_3}.$$

Daje to najwyżej $(1-\varepsilon_3)^{-2}$ elementów w przeciwobrazie. □

Rozdział 2

Wielomiany rzędu 3

Pierwsze oszacowanie współczynników wielomianu Φ_{pqr} podał Bang.

Twierdzenie 2.1 (Bang [7], 1895)**.** *Zachodzi nierówność* $A_{pqr} < p$.

Ponad pół wieku później Bloom podał elegancką formułę na współczynnik przy x^m wielomianu $\Phi_{pqr}(x)$.

Twierdzenie 2.2 (Bloom [15], 1968)**.** *Niech* $\chi_3(m) = 1$, *gdy* $m = aqr + brp + cpq$ *dla pewnych całkowitych* $a, b, c \geqslant 0$, *w przeciwnym razie* $\chi_3(m) = 0$. *Wtedy*

$$a_{pqr}(m) = \sum_{k=m-p+1}^{m} \Big(\chi_3(k) - \chi_3(k-q) - \chi_3(k-r) + \chi_3(k-q-r)\Big).$$

Znana jest następująca własność wielomianów cyklotomicznych.

Fakt 2.3. Wielomian Φ_n jest palindromiczny, tj. $\Phi_n(x) = x^{\varphi(n)}\Phi_n(x^{-1})$.

Biorąc pod uwagę powyższy fakt, wystarczy szacować współczynniki przy potęgach o wykładnikach mniejszych lub równych $\varphi(n)/2$. Zauważmy, że liczba a z ostatniego twierdzenia nie może przekroczyć $\lfloor m/(qr)\rfloor$, gdy $\chi_3(m) = 1$. W takim razie mamy

Wniosek 2.4. $|a_{pqr}(m)| \leqslant 2(\lfloor m/(qr)\rfloor + 1) \leqslant 2(\lfloor \varphi(pqr)/(2qr)\rfloor + 1) = p - 1$.

Wniosek ów nie poprawia oszacowania Banga, jednak daje lepsze wyniki przy małych m, jak również przy m bliskich $\varphi(pqr)$, ze względu na palindromiczność Φ_n. Oszacowanie ogólne zostało poprawione przez Beiter.

Twierdzenie 2.5 (Beiter [10], 1968)**.** *Zachodzi nierówność* $A_{pqr} \leqslant \lceil 3p/4\rceil$.

Trzy lata później Beiter [11] i Möler [47] znaleźli niezależnie przykłady liczb p, q, r, dla których $A_{pqr} = (p+1)/2$. Beiter postawiła następującą hipotezę.

Hipoteza 2.6 (Beiter [11], 1971). *Zachodzi nierówność* $A_{pqr} \leqslant (p+1)/2$.

Przez długi czas hipoteza Beiter pozostawała nierozstrzygnięta. Dopiero niedawno Gallot i Moree znaleźli kontrprzykłady. W znacznej mierze umożliwił to rozwój techniki i możliwość dokonywania obliczeń przy pomocy komputerów.

Twierdzenie 2.7 (Gallot i Moree [30], 2009). *Dla każdego* $\varepsilon > 0$ *istnieje nieskończenie wiele trójek liczb pierwszych* (p, q, r)*, w których* p *jest dowolnie duża oraz*

$$A_{pqr} > (2/3 - \varepsilon)p.$$

Naturalnym i nadal pozostającym bez odpowiedzi pytaniem postawionym w wyżej cytowanej pracy jest to, czy następująca hipoteza jest prawdziwa.

Hipoteza 2.8 (poprawiona hipoteza Beiter, Gallot i Moree [30], 2009). *Zachodzi nierówność* $A_{pqr} \leqslant \frac{2}{3}p$.

W międzyczasie poprawione zostały oszacowania górne. Bachman podał następujące, przy takich samych oznaczaczeniach, jak w Twierdzeniu 8.

Twierdzenie 2.9 (Bachman [2], 2003). $A_{pqr} \leqslant \min\{(p-1)/2 + \alpha, p - \beta^*\} \leqslant \lfloor 3p/4 \rfloor$.

Dowodząc twierdzenia 8, poprawimy ten wynik. Można łatwo sprawdzić, że jeśli $\alpha + \beta^* < (p-1)/2$, to twierdzenie 8 daje ściśle mocniejsze oszacowanie, a w pozostałych przypadkach – takie samo. Zatem spośród wszystkich $(p-1)^2$ par reszt z dzielenia q i r przez p, dla $\frac{1}{2}(p-3)(p-5)$ par uzyskujemy ściśle lepsze oszacowanie. Asymptotycznie jest to połowa wszystkich par. Ograniczenie niezależne od reszt wynosi $\lfloor 3p/4 \rfloor$, czyli pozostaje bez zmian.

W dowodzie twierdzenia 8 i dalszych twierdzeń dotyczących wielomianów cyklotomicznych rzędu 3 będziemy korzystać z własności pewnego szczególnego ciągu, któremu poświęcony jest następny podrozdział.

2.1. Ciąg związany z Φ_{pqr}

Ustalmy liczby pierwsze p, q, r. Bloom [15], a potem Bachman [2] uzyskiwali swoje wyniki dotyczące A_{pqr} analizując własności liczb $\chi_3(m)$. Liczby te zdefiniowaliśmy przy okazji twierdzenia 2.2. Można jednak tę definicję rozszerzyć, uzyskując nieco więcej informacji. Następujący fakt jest łatwy do udowodnienia.

Fakt 2.10. Dla każdej liczby $k \in \{0, 1, \ldots, pqr - 1\}$ istnieje dokładnie jedna trójka (a_k, b_k, c_k) spełniająca kongruencję

$$k \equiv a_k qr + b_k rp + c_k pq \pmod{pqr},$$

przy czym $a_k \in \{0, 1, \ldots, p-1\}$, $b_k \in \{0, 1, \ldots q-1\}$, $c_k \in \{0, 1, \ldots, r-1\}$.

Definicja 2.11. *Ciągiem związanym z wielomianem* Φ_{pqr} nazywamy ciąg liczb F_k spełniających warunek

$$k + F_k pqr = a_k qr + b_k rp + c_k pq,$$

gdzie a_k, b_k i c_k określone są w fakcie 2.10.

Jest jasne, że $\chi_3(k) = 1$ wtedy i tylko wtedy, gdy $F_k = 0$. Natomiast jeśli $\chi_3(k) = 0$, to F_k może przyjmować dwie różne wartości, w zależności od k. Mówi o tym następujący lemat.

Lemat 2.12. *Dla* $-(qr + rp + pq) < k < pqr$ *zachodzi* $F_k \in \{0, 1, 2\}$. *Jeśli* $F_k = 0$, *to* $a_k \leqslant \lfloor k/(qr) \rfloor$. *Jeśli* $F_k = 2$, *to* $a_k \geqslant \lceil (k + rp + pq)/(qr) \rceil$.

Dowód. Pierwszą część dowodzimy w jednej linii:

$$0 \leqslant a_k qr + b_k rp + c_k pq < (p-1)qr + (q-1)rp + (r-1)pq + qr + rp + pq = 3pqr.$$

Jeśli $F_k = 0$, to $k = a_k qr + b_k rp + c_k pq$, z czego natychmiast wynika, że $a_k \leqslant \lfloor k/(qr) \rfloor$. Jeżeli natomiast $F_k = 2$, to

$$k + 2pqr = a_k qr + b_k rp + c_k pq \leqslant a_k qr + (q-1)rp + (r-1)pq,$$

skąd wynika, że $a_k qr \geqslant k + rp + pq$. □

Kolejne lematy odkrywają dalsze własności ciągu (F_k).

Lemat 2.13.

$$F_k - F_{k-q} = \begin{cases} 1, & \text{gdy } a_k < r^{-1}(p) \text{ i } c_k < p^{-1}(r), \\ -1, & \text{gdy } a_k \geqslant r^{-1}(p) \text{ i } c_k \geqslant p^{-1}(r), \\ 0, & \text{w przeciwnym razie.} \end{cases}$$

Dowód. Z łatwego do zaobserwowania faktu $a_k qr \equiv k \pmod{p}$ oraz dwóch analogicznych dla b_k i c_k wynikają następujące kongruencje:

$$a_{k-q} \equiv a_k - r^{-1}(p) \pmod{p}, \quad c_{k-q} \equiv c_k - p^{-1}(r) \pmod{r},$$

a ponadto, że $b_k = b_{k-q}$. W takim razie

$$a_k - a_{k-q} = \begin{cases} r^{-1}(p) - p, & \text{gdy } a_k < r^{-1}(p), \\ r^{-1}(p), & \text{gdy } a_k \geqslant r^{-1}(p), \end{cases}$$

$$c_k - c_{k-q} = \begin{cases} p^{-1}(r) - r, & \text{gdy } c_k < p^{-1}(r), \\ p^{-1}(r), & \text{gdy } c_k \geqslant p^{-1}(r). \end{cases}$$

Niech $[P]$ oznacza wartość logiczną wyrażenia P. Wtedy

$$\begin{aligned} F_k - F_{k-q} &= \frac{a_k - a_{k-q}}{p} + \frac{a_k - a_{k-q}}{q} + \frac{a_k - a_{k-q}}{r} - \frac{1}{pr} \\ &= \frac{r^{-1}(p)}{p} + \frac{p^{-1}(r)}{r} - \frac{1}{pr} - [a_k < r^{-1}(p)] - [c_k < p^{-1}(r)] \\ &= 1 - [a_k < r^{-1}(p)] - [c_k < p^{-1}(r)], \end{aligned}$$

co kończy dowód. □

Definicja 2.14. Określamy następujące zbiory

$$\begin{aligned} \mathcal{A}_0^p &= \{0, 1, \ldots, p-1\} \cap \Big[0,\ q^{-1}(p) + r^{-1}(p) - p\Big), \\ \mathcal{A}_1^p &= \{0, 1, \ldots, p-1\} \cap \Big[q^{-1}(p) + r^{-1}(p) - p,\ \min\{q^{-1}(p), r^{-1}(p)\}\Big), \\ \mathcal{A}_2^p &= \{0, 1, \ldots, p-1\} \cap \Big[\min\{q^{-1}(p), r^{-1}(p)\},\ \max\{q^{-1}(p), r^{-1}(p)\}\Big), \\ \mathcal{A}_3^p &= \{0, 1, \ldots, p-1\} \cap \Big[\max\{q^{-1}(p), r^{-1}(p)\},\ q^{-1}(p) + r^{-1}(p)\Big), \\ \mathcal{A}_4^p &= \{0, 1, \ldots, p-1\} \cap \Big[q^{-1}(p) + r^{-1}(p),\ p\Big). \end{aligned}$$

Analogicznie definiujemy zbiory $\mathcal{A}_j^q$ oraz $\mathcal{A}_j^r$ dla $j = 0, 1, 2, 3, 4$.

Lemat 2.15.

$$F_k - F_{k-q} - F_{k-r} + F_{k-q-r} = \begin{cases} -1, & \textit{gdy } a_k \in \mathcal{A}_1^p, \\ 1, & \textit{gdy } a_k \in \mathcal{A}_3^p, \\ 0, & \textit{w przeciwnym razie.} \end{cases}$$

Dowód. Na mocy lematu 2.13 otrzymujemy

$$\begin{aligned} F_k - F_{k-q} &= 1 - [a_k < r^{-1}(p)] - [c_k < p^{-1}(r)], \\ F_{k-r} - F_{k-q-r} &= 1 - [a_{k-r} < r^{-1}(p)] - [c_{k-r} < p^{-1}(r)]. \end{aligned}$$

Korzystając z powyższych równości oraz z faktu, że $a_{k-r} \equiv a_k - q^{-1}(p) \pmod p$ i $c_{k-r} = c_k$, mamy

$$\begin{aligned} F_k - F_{k-q} - F_{k-r} + F_{k-q-r} &= [a_{k-r} < r^{-1}(p)] - [a_k < r^{-1}(p)] \\ &= [a_k < q^{-1}(p) + r^{-1}(p) - p] - [a_k < q^{-1}(p)] \\ &\quad - [a_k < r^{-1}(p)] + [a_k < q^{-1}(p) + r^{-1}(p)]. \end{aligned}$$

Teraz łatwo sprawdzić, że lemat zachodzi. □

Lemat 2.16.

$$F_m - F_{m-p} - F_{m-q} - F_{m-r} + F_{m-q-r} + F_{m-r-p} + F_{m-p-q} - F_{m-p-q-r} = 0.$$

Dowód. Na mocy lematu 2.15, wartość wyrażenia $F_k - F_{k-q} - F_{k-r} + F_{k-q-r}$ zależy jedynie od reszty z dzielenia k przez p. Z tego natychmiast wynika teza. □

Uwaga 2.17. Każdy z lematów 2.12, 2.13, 2.15 posiada swoje symetryczne wersje, powstałe przez dokonanie odpowiednich permutacji (p, q, r) i (a_k, b_k, c_k).

Definicja 2.18. Przyjmijmy następujące oznaczenia:

$$\delta_{qr} = \begin{cases} 1, & \text{gdy } q^{-1}(p) < r^{-1}(p), \\ 0, & \text{w przeciwnym razie,} \end{cases} \qquad \delta_{rq} = \begin{cases} 1, & \text{gdy } r^{-1}(p) < q^{-1}(p), \\ 0, & \text{w przeciwnym razie.} \end{cases}$$

Analogicznie określamy δ_{rp}, δ_{pr}, δ_{pq} i δ_{pq}.

Kolejny lemat pozwala wyznaczyć wartości ósemek

$$\operatorname{oct}(m) = (F_m, F_{m-p}, F_{m-q}, F_{m-r}, F_{m-q-r}, F_{m-r-p}, F_{m-p-q}, F_{m-p-q-r})$$

w zależności od przynależności trójki (a_m, b_m, c_m) do jednego ze zbiorów postaci $\mathcal{A}^p_{j_1} \times \mathcal{A}^q_{j_2} \times \mathcal{A}^r_{j_3}$.

Lemat 2.19. *W tabeli 2.1 znajdują się wszystkie możliwe wartości wyżej określonych ósemek oct(m), z dokładnością do dodania do wszystkich ośmiu elementów oct(m) pewnej liczby całkowitej. Zapis $j_1j_2j_3$ oznacza w skrócie $(a_m, b_m, c_m) \in \mathcal{A}^p_{j_1} \times \mathcal{A}^q_{j_2} \times \mathcal{A}^r_{j_3}$. Ponadto trzecia kolumna zawiera wartości*

$$V(m) = N_0(F_m, F_{m-q-r}, F_{m-r-p}, F_{m-p-q}) - N_0(F_{m-p}, F_{m-q}, F_{m-r}, F_{m-p-q-r}),$$

gdzie $N_0(\boldsymbol{a})$ oznacza liczbę zer w ciągu $(\boldsymbol{a})$.

Dowód powyższego lematu będzie ciągnął się niemal do końca bieżącego podrozdziału. W pierwszej kolejności udowodnimy fakt pomocniczy 2.20, dzięki któremu będziemy mogli obliczyć oct(m) dla 10 przypadków, a pozostałe uzyskamy z nich przy jego pomocy. Następnie przedstawimy zasadniczą część dowodu. W dalszej uwadze 2.21 uzasadniamy, że w tabeli są wszystkie możliwe przypadki za wyjątkiem (000) i (444), a lemat 2.22 odpowiada na pytanie, dlaczego te przypadki zostały pominięte.

Będziemy pisać w skrócie $\operatorname{oct}(m) \sim (\ldots)$, jeśli zachodzi równość z dokładnością do dodania do wszystkich elementów $(\ldots)$ pewnej liczby całkowitej.

Tabela 2.1: Wartości $\mathrm{oct}(m)$ w zależności od (a_m, b_m, c_m).

	$\mathrm{oct}(m)$	$V(m)$
001	$(0,1,1,1,1,2,2,2)$	1
002	$(0,\delta_{pq},\delta_{qp},1,1+\delta_{qp},1+\delta_{pq},1,2)$	0
003	$(0,0,0,1,1,1,1,2)$	-1
004	$(0,0,0,1,1,1,0,1)$	0
011	$(0,1,1,1,2,1,1,1)$	1
012	$(0,\delta_{pq},\delta_{qp},1,1+\delta_{qp},\delta_{pq},1,1)$	δ_{qp}
013	$(0,0,0,1,1,0,1,1)$	0
014	$(0,0,0,1,1,0,0,0)$	0
022	$(0,\delta_{pq}+\delta_{pr}-1,\delta_{qp},\delta_{rp},\delta_{qp}+\delta_{rp},\delta_{pq},\delta_{pr},1)$	0
023	$(1,\delta_{pr},1,1+\delta_{pr},1+\delta_{pr},1,1+\delta_{pr},2)$	$-\delta_{rp}$
024	$(1,\delta_{pr},1,1+\delta_{pr},1+\delta_{pr},1,\delta_{pr},1)$	0
033	$(1,0,1,1,1,1,1,2)$	-1
034	$(1,0,1,1,1,1,0,1)$	0
044	$(1,0,1,1,1,0,0,0)$	0
111	$(0,1,1,1,1,1,1,0)$	0
112	$(0,\delta_{pq},\delta_{qp},1,\delta_{qp},\delta_{pq},1,0)$	0
113	$(0,0,0,1,0,0,1,0)$	0
114	$(1,1,1,2,1,1,1,0)$	-1
122	$(1,\delta_{pq}+\delta_{pr},1+\delta_{qp},1+\delta_{rp},\delta_{qp}+\delta_{rp},1+\delta_{pq},1+\delta_{pr},1)$	$\delta_{pq}\delta_{pr}-\delta_{qp}\delta_{rp}$
123	$(1,\delta_{pr},1,1+\delta_{rp},\delta_{rp},1,1+\delta_{pr},1)$	$\delta_{pr}-\delta_{rp}$
124	$(1,\delta_{pr},1,1+\delta_{rp},\delta_{rp},1,\delta_{pr},0)$	$-\delta_{rp}$
133	$(1,0,1,1,0,1,1,1)$	0
134	$(1,0,1,1,0,1,0,0)$	0
144	$(2,1,2,2,1,1,1,0)$	-1
222	$(1,\delta_{pq}+\delta_{pr},\delta_{qr}+\delta_{qp},\delta_{rp}+\delta_{rq},\delta_{qp}+\delta_{rp},\delta_{rq}+\delta_{pq},\delta_{pr}+\delta_{qr},1)$	0
223	$(1,\delta_{pr},\delta_{qr},\delta_{rp}+\delta_{rq},\delta_{rp},\delta_{rq},\delta_{pr}+\delta_{qr},1)$	$\delta_{pr}\delta_{qr}-\delta_{rp}\delta_{rq}$
224	$(1,\delta_{pr},\delta_{qr},\delta_{rp}+\delta_{rq},\delta_{rp},\delta_{rq},\delta_{pr}+\delta_{qr}-1,0)$	0
233	$(1,0,\delta_{qr},\delta_{rq},0,\delta_{rq},\delta_{qr},1)$	0
234	$(2,1,1+\delta_{qr},1+\delta_{rq},1,1+\delta_{rq},\delta_{qr},1)$	δ_{rq}
244	$(2,1,1+\delta_{qr},1+\delta_{rq},1,\delta_{rq},\delta_{qr},0)$	0
333	$(1,0,0,0,0,0,0,1)$	0
334	$(2,1,1,1,1,1,0,1)$	1
344	$(2,1,1,1,1,0,0,0)$	1

Fakt 2.20. Niech $(a_m, b_m, c_m) \in \mathcal{A}^p_{j_1} \times \mathcal{A}^q_{j_2} \times \mathcal{A}^r_3$ i $(a_{m'}, b_{m'}, c_{m'}) \in \mathcal{A}^p_{j_1} \times \mathcal{A}^q_{j_2} \times \mathcal{A}^r_4$. Wtedy

$$\mathrm{oct}(m') \sim (F_m, F_{m-p}, F_{m-q}, F_{m-r}, F_{m-q-r}, F_{m-r-p}, F_{m-p-q}+1, F_{m-p-q-r}+1),$$

Podobnie, jeśli $m \in \mathcal{A}^p_1 \times \mathcal{A}^q_{j_2} \times \mathcal{A}^r_{j_3}$ oraz $m' \in \mathcal{A}^p_0 \times \mathcal{A}^q_{j_2} \times \mathcal{A}^r_{j_3}$, to

$$\mathrm{oct}(m') \sim (F_m, F_{m-p}, F_{m-q}, F_{m-r}, F_{m-q-r}-1, F_{m-r-p}, F_{m-p-q}, F_{m-p-q-r}-1).$$

Dowód. Zajmiemy się pierwszą sytuacją. Z lematu 2.13 i jego symetrycznych wersji wynika, że:

$$F_m - F_{m-p} = F_{m'} - F_{m'-p}, \quad F_m - F_{m-q} = F_{m'} - F_{m'-q}, \quad F_m - F_{m-r} = F_{m'} - F_{m'-r}.$$

Następnie, na mocy lematu 2.15 oraz jego symetrycznej wersji, widzimy, że

$$F_m - F_{m-q-r} = F_{m'} - F_{m'-q-r} \quad \text{i} \quad F_m - F_{m-r-p} = F_{m'} - F_{m'-r-p}.$$

Jeszcze raz korzystamy z symetrycznej wersji lematu 2.15, otrzymując równości

$$F_m - F_{m-p} - F_{m-q} + F_{m-p-q} = F_{m-r} - F_{m-r-p} - F_{m-q-r} + F_{m-p-q-r} = 1,$$
$$F_{m'} - F_{m'-p} - F_{m'-q} + F_{m'-p-q} = F_{m'-r} - F_{m'-r-p} - F_{m'-q-r} + F_{m'-p-q-r} = 0,$$

z których wynika teza. Dla drugiej sytuacji rozumowanie jest analogiczne. □

Dowód lematu 2.19. Rozważmy najpierw te 10 przypadków z tabeli 2.1, w których nie występuje ani $\mathcal{A}^p_0$, ani $\mathcal{A}^r_4$. Rozumowanie jest proste, problemem jest tylko wykonanie go dziesięć razy. W każdym wierszu tabeli 2.1 wartość F_m została ustalona, ponieważ podajemy $\mathrm{oct}(m)$ jedynie z dokładnością do przesunięcia o liczbę całkowitą. Następnie, korzystając z lematu 2.13 i jego symetrycznych wersji, podajemy wartości F_{m-p}, F_{m-q}, F_{m-r}. Kolejnym krokiem jest wykorzystanie lematu 2.15 i jego symetrycznych wersji, w celu obliczenia F_{m-q-r}, F_{m-r-p}, F_{m-p-q}. Na koniec używamy lematu 2.16, aby policzyć $F_{m-p-q-r}$.

Zakładamy przy tym, że $\delta_{pq} + \delta_{qp} = 1$, gdyż jeśli obie te liczby są zerami, to zbiór $\mathcal{A}^r_2$ jest pusty, a ponieważ występuje on zawsze jako czynnik iloczynu kartezjańskiego w przypadkach, w których pojawiają się δ_{pq} lub δ_{qp}, nie ma znaczenia, co wtedy otrzymamy, bowiem jest to otrzymane dla zbioru pustego.

Teraz możemy skorzystać z faktu 2.20, aby policzyć $\mathrm{oct}(m)$ dla pozostałych 23 wierszy tabeli 2.1, uzupełniając tym samym całkowicie drugą kolumnę.

Zostały nam tylko obliczenia $V(m)$. W tych wierszach, w których nie występują wyrażenia postaci δ_{pq}, jest to natychmiastowe. Wszystkie 15 pozostałych przypadków trzeba po prostu przeliczyć. Nie robimy tego kolejno według wierszy, tylko od najprostszych przypadków do najtrudniejszych.

(002) Nie ma tu znaczenia, która z liczb δ_{pq}, δ_{qp} jest równa 1, przyjmijmy więc, że pierwsza z nich. Wtedy $\mathrm{oct}(m) = (0, 1, 0, 1, 1, 2, 1, 2)$ i $V(m) = 0$.

(244) Przypadek w pełni analogiczny do poprzedniego, z elementami $\mathrm{oct}(m)$ wpisanymi w przeciwnym porządku, co daje znów $V(m) = 0$.

(112) Również wartość δ_{pq} nie ma znaczenia i dla $\delta_{pq} = 1$ otrzymujemy $\mathrm{oct}(m) \sim (0, 1, 0, 1, 0, 1, 1, 0)$ i $V(m) = 0$.

(233) Podobnie jak poprzednio, wartość δ_{qr} nie ma wpływu na $V(m)$ i możemy przyjąć $\delta_{qr} = 1$. Wtedy $\mathrm{oct}(m) \sim (1, 0, 1, 0, 0, 0, 1, 1)$ i $V(m) = 0$.

(012) Dla $\delta_{pq} = 1$ mamy $\mathrm{oct}(m) \sim (0, 1, 0, 1, 1, 1, 1, 1)$ i $V(m) = 0$, natomiast dla $\delta_{qp} = 1$ otrzymujemy $\mathrm{oct}(m) = (0, 0, 1, 1, 2, 0, 1, 1)$ i $V(m) = 1$. Stąd, niezależnie od wartości δ_{qp}, zachodzi $V(m) = \delta_{qp}$.

(234) Dla $\delta_{qr} = 1$ otrzymujemy $\mathrm{oct}(m) \sim (2, 1, 2, 1, 1, 1, 1, 1)$ i $V(m) = 0$, a dla $\delta_{rq} = 1$ mamy $\mathrm{oct}(m) = (2, 1, 1, 2, 1, 2, 0, 1)$ i $V(m) = 1$. W takim razie $V(m) = \delta_{rq}$.

(024) W zależności od wartości δ_{pr}, otrzymujemy $\mathrm{oct}(m) \sim (1, 0, 1, 1, 1, 1, 0, 1)$, bądź $\mathrm{oct}(m) \sim (1, 1, 1, 2, 2, 1, 1, 1)$. W obu przypadkach $V(m) = 0$.

(123) Jeśli $\delta_{rp} = 1$, to $\mathrm{oct}(m) = (1, 0, 1, 2, 1, 1, 1, 1)$ i $V(m) = -1$. Jeśli $\delta_{pr} = 1$, to $\mathrm{oct}(m) = (1, 1, 1, 1, 0, 1, 2, 1)$ i $V(m) = 1$. Zatem $V(m) = \delta_{pr} - \delta_{rp}$.

(023) Dla $\delta_{rp} = 1$ zachodzi $\mathrm{oct}(m) = (1, 0, 1, 1, 1, 1, 1, 2)$ i $V(m) = -1$, a dla $\delta_{pr} = 1$ mamy $\mathrm{oct}(m) \sim (1, 1, 1, 2, 2, 1, 2, 2)$ i $V(m) = 0$. Wobec tego $V(m) = -\delta_{rp}$.

(124) Jeżeli $\delta_{rp} = 1$, to $\mathrm{oct}(m) = (1, 0, 1, 2, 1, 1, 0, 0)$ i $V(m) = -1$. Gdy $\delta_{pr} = 1$, mamy $\mathrm{oct}(m) \sim (1, 1, 1, 2, 2, 1, 1, 1)$ i $V(m) = 0$. Zatem $V(m) = -\delta_{rp}$.

(022) Zauważmy, że w tym przypadku nie może być $\delta_{pq} = \delta_{pr} = 0$, ponieważ wtedy $F_{m-q-r} = F_{m-p} + 3$, sprzeczność z lematem 2.12. Jeśli $\delta_{pq} = \delta_{pr} = 1$, to $\mathrm{oct}(m) \sim (0, 1, 0, 0, 0, 1, 1, 1)$ i $V(m) = 0$. Pozostał przypadek, w którym dokładnie jedna z liczb δ_{pq}, δ_{pr} jest równa 1. Załóżmy, że jest to δ_{pq}, gdyż nie ma to wpływu na wartość $V(m)$. Otrzymujemy wtedy $\mathrm{oct}(m) \sim (0, 0, 0, 1, 1, 1, 0, 1)$ i $V(m) = 0$.

(224) Przypadek analogiczny do poprzedniego, ze zmianą kolejności w $\mathrm{oct}(m)$.

(122) Zachodzą następujące równości

$$\mathrm{oct}(m) \sim \begin{cases} (1,2,1,1,0,2,2,1) & \text{dla } \delta_{pq} = \delta_{pr} = 1, \\ (1,0,2,2,2,1,1,1) & \text{dla } \delta_{qp} = \delta_{rp} = 1, \\ (1,1,1,2,1,2,1,1) & \text{dla } \delta_{pq} = \delta_{rp} = 1, \\ (1,1,2,1,1,1,2,1) & \text{dla } \delta_{qp} = \delta_{pr} = 1, \end{cases}$$

z których łatwo wydedukować $V(m) = \delta_{pq}\delta_{pr} - \delta_{qp}\delta_{rp}$.

(223) Podobnie jak poprzednio, z równości

$$\mathrm{oct}(m) \sim \begin{cases} (1,1,1,0,0,0,2,1) & \text{dla } \delta_{pr} = \delta_{qr} = 1, \\ (1,0,0,2,1,1,0,1) & \text{dla } \delta_{rp} = \delta_{rq} = 1, \\ (1,1,0,1,0,1,1,1) & \text{dla } \delta_{pr} = \delta_{rq} = 1, \\ (1,0,1,1,1,0,1,1) & \text{dla } \delta_{rp} = \delta_{qr} = 1, \end{cases}$$

wnioskujemy, że $V(m) = \delta_{pr}\delta_{qr} - \delta_{rp}\delta_{rq}$.

(222) Obliczamy następujące równości

$$\mathrm{oct}(m) \sim \begin{cases} (1,1,1,1,1,1,1,1) & \text{dla } \delta_{pq} = \delta_{qr} = \delta_{rp} = 1, \\ (1,2,1,0,0,1,2,1) & \text{dla } \delta_{pq} = \delta_{qr} = \delta_{pr} = 1. \end{cases}$$

W powyższych dwóch przypadkach $V(m) = 0$. Pozostałe uzyskujemy dzięki symetrii i zachodzi w nich taka sama równość.

Weryfikacja wszystkich przypadków została zakończona i lemat jest dowiedziony. □

Uwaga 2.21. W kolejnych wierszach tabeli 2.1 wypisaliśmy trójki $(j_1 j_2 j_3)$, którym odpowiadają kolejne liczby $\overline{j_1 j_2 j_3}$ zapisane w piątkowym systemie pozycyjnym i uporządkowane rosnąco. Trójki (000) i (444) oraz te trójki, które powstały z wcześniejszych poprzez zmianę kolejności cyfr, zostały pominięte.

Wobec tego z lematu 2.19 można otrzymać wszystkie możliwe przypadki. Wystarczy dokonać odpowiedniej permutacji (p, q, r) oraz odpowiadającej jej permutacji (j_1, j_2, j_3).

Ostatni lemat, który udowodnimy w tym podrozdziale, nie dotyczy bezpośrednio liczb F_k. Uzasadnia on jednak, dlaczego w tabeli 2.2 nie ma zbioru $\mathcal{A}_0^p \times \mathcal{A}_0^q \times \mathcal{A}_0^r$, ani $\mathcal{A}_4^p \times \mathcal{A}_4^q \times \mathcal{A}_4^r$. Wynika bowiem z niego, że te iloczyny kartezjańskie są zbiorami pustymi.

Lemat 2.22. *Jedno z poniższych wyrażeń*

$$[q^{-1}(p) + r^{-1}(p) > p], \quad [r^{-1}(q) + p^{-1}(q) > q], \quad [p^{-1}(r) + q^{-1}(r) > r]$$

ma inną wartość logiczną niż pozostałe dwa.

Dowód. Sumując stronami równość

$$\frac{q^{-1}(p)}{p} + \frac{p^{-1}(q)}{q} = 1 + \frac{1}{pq}$$

z dwiema analogicznymi, otrzymamy

$$\frac{q^{-1}(p) + r^{-1}(p)}{p} + \frac{r^{-1}(q) + p^{-1}(q)}{q} + \frac{p^{-1}(r) + q^{-1}(r)}{r} = 3 + \frac{1}{qr} + \frac{1}{rp} + \frac{1}{pq}.$$

Teraz już widać, że teza zachodzi. □

Z definicji 2.14 wynika, że zbiór $\mathcal{A}_0^p$ jest niepusty dla $q^{-1}(p) + r^{-1}(p) > p$, a zbiór $\mathcal{A}_4^p$ jest niepusty dla $q^{-1}(p) + r^{-1}(p) < p$, analogicznie dla $\mathcal{A}^q$ i $\mathcal{A}^r$. Zatem na mocy powyższego lematu

$$\mathcal{A}_0^p \times \mathcal{A}_0^q \times \mathcal{A}_0^r = \mathcal{A}_4^p \times \mathcal{A}_4^q \times \mathcal{A}_4^r = \emptyset.$$

2.2. Szacowanie współczynników

W tym podrozdziale udowodnimy twierdzenia 8 oraz 9. Dla potrzeb dowodu będziemy zakładać, że $p < q, r$ i $q^{-1}(p) \leqslant r^{-1}(p)$. Będziemy też używać oznaczeń α, β oraz β^*, które zostały zdefiniowane przed sformułowaniem twierdzenia 8.

Niech ponadto $N_0(\mathbf{a})$ oznacza liczbę zer w danym ciągu $(\mathbf{a})$, N_1 oznacza liczbę jedynek, itd. W szczególności przyjmijmy

$$N_0^+(m) = N_0(F_m, F_{m-1}, \ldots, F_{m-p+1}, F_{m-q-r}, F_{m-q-r-1}, \ldots, F_{m-p-q-r+1}),$$
$$N_0^-(m) = N_0(F_{m-q}, F_{m-q-1}, \ldots, F_{m-p-q+1}, F_{m-r}, F_{m-r-1}, \ldots, F_{m-r-p-1}),$$

oraz analogicznie $N_1^+(m)$, $N_1^-(m)$, $N_2^+(m)$ i $N_2^-(m)$. Następujący lemat jest nieznacznym rozszerzeniem twierdzenia 2.2.

Lemat 2.23. *Zachodzą następujące równości:*

$$a_{pqr}(m) = N_0^+(m) - N_0^-(m) = N_2^+(m) - N_2^-(m) = -\frac{1}{2}\Big(N_1^+(m) - N_1^-(m)\Big),$$

dla $0 \leqslant m < pqr$.

Dowód. Będziemy pisać w skrócie N_0^+ zamiast $N_0^+(m)$. Pierwsza równość natychmiast wynika z twierdzenia 2.2. W oczywisty sposób zachodzi

$$N_0^+ + N_1^+ + N_2^+ = N_0^- + N_1^- + N_2^- = 2p.$$

Ponieważ istnieje naturalna bijekcja pomiędzy zbiorami $\{m, m-1, \ldots, m-p+1\}$ i $\{a_m, a_{m-1}, \ldots, a_{m-p+1}\}$, korzystając z lematu 2.15, otrzymujemy

$$\sum_{j=0}^{2} j(N_j^+ - N_j^-) = \sum_{k=m-p+1}^{m} (F_k - F_{k-q} - F_{k-r} + F_{k-q-r}) = \#\mathcal{A}_3^p - \#\mathcal{A}_1^p = 0.$$

Niech $x_j = N_j^+ - N_j^-$ dla $j = 1, 2, 3$. Otrzymaliśmy następujący układ równań

$$\begin{cases} x_0 + x_1 + x_2 = 0, \\ x_1 + 2x_2 = 0, \end{cases}$$

którego rozwiązaniem jest $x_0 = -\frac{1}{2}x_1 = x_2$, a to, na mocy okazanej wcześnej równości $a_{pqr}(m) = x_0$, kończy dowód. □

Do dowodu twierdzenia 8 wystarczy nam tylko pierwsza z równości w powyższym lemacie, natomiast pozostałe będą użyteczne w innych dowodach. Wobec tego potrzebujemy zlokalizować te czwórki $Q_k = (F_k, F_{k-q}, F_{k-r}, F_{k-p-q-r})$, w których $N_0(F_k, F_{k-q-r}) \neq N_0(F_{k-q}, F_{k-r})$. Pozostałe bowiem nie wpływają na wartość wyrażenia $N_0^+(m) - N_0^-(m)$.

W tabeli 2.2 wypisano wszystkie możliwe takie czwórki. Innych nie ma, czego łatwo dowieść, korzystając z lematów 2.12, 2.13 i 2.15. W tabeli znajdują się również wartości

$$f(k) = F_k - F_{k-p} - F_{k-q} + F_{k-q-r} \quad \text{oraz} \quad v(k) = N_0(F_k, F_{k-q-r}) - N_0(F_{k-q}, F_{k-r}).$$

Będą one użyteczne w dowodzie.

Tabela 2.2: Czwórki Q_k.

Lp.	Q_k	$f(k)$	$v(k)$
1	$(0,0,1,0)$, $(0,1,0,0)$, $(0,1,1,1)$, $(1,1,1,0)$	-1	1
2	$(0,0,0,1)$, $(1,0,0,0)$, $(1,0,1,1)$, $(1,1,0,1)$	1	-1
3a	$(0,1,1,2)$	0	1
3b	$(2,1,1,0)$	0	1
4	$(1,0,2,1)$, $(1,2,0,1)$	0	-1

Dowód twierdzenia 8. Oznaczmy przez C_ℓ liczbę tych $k \in \{m, m-1, \ldots, m-p+1\}$, dla których czwórka Q_k znajduje się w wierszu $\ell \in \{1, 2, 3a, 3b, 4\}$ tabeli 2.2. Oszacujemy z góry liczby C_1, C_2, $C_3 = C_{3a} + C_{3b}$, C_4. Zamiast wyznaczać ilość liczb k,

będziemy wyznaczać ilość liczb a_k, ze względu na wspomnianą w dowodzie lematu 2.23 bijekcję. Dla przejrzystości zapisu przyjmijmy $q' = q^{-1}(p)$ i $r' = r^{-1}(p)$. Wprowadźmy też dodatkowe oznaczenie $\gamma = \lfloor m/qr \rfloor + 1$.

Na mocy lematu 2.15 zachodzą następujące nierówności

$$C_1 \leqslant \mathcal{A}_1^p = \alpha, \quad C_2 \leqslant \mathcal{A}_3^p = \alpha.$$

Pozostałe przypadki są nieco bardziej skomplikowane.

Jeśli $Q_k = (0, 1, 1, 2)$, to na mocy lematu 2.13 mamy $a_k < m$, więc z lematu 2.15 wynika, że $a_k \in \mathcal{A}_0^p$. Podobnie dochodzimy do wniosku, że jeśli $Q_k = (2, 1, 1, 0)$, to $a_k \in \mathcal{A}_4^p$.

W przypadku (3a) mamy $q' + r' > p$ oraz $a_k < \gamma$ i $a_k - q' - r' + 2p = a_{k-q-r} \geqslant \gamma$, co daje

$$\max\{0, \gamma + q' + r' - 2p\} \leqslant a_k < \min\{\gamma, q' + r' - p\}.$$

W konsekwencji

$$\begin{aligned} C_{3a} &\leqslant \min\{\gamma, q' + r' - p\} - \max\{0, \gamma + q' + r' - 2p\} \\ &= \min\{\gamma, p - \gamma, q' + r' - p, 2p - q' - r'\} \\ &\leqslant \min\{q' + r' - p, 2p - q' - r'\} = \min\{\alpha + \beta, p - \alpha - \beta\}, \end{aligned}$$

gdzie skorzystaliśmy z łatwego do wykazania faktu, że jeśli $q' + r' > p$, to $\alpha = p - q'$ i $\beta = p - r'$.

W przypadku (3b) mamy $q' + r' < p$, przy czym zachodzą nierówności $a_k \geqslant \gamma$ oraz $a_k - q' - r' = a_{k-q-r} < \gamma$, z których wnioskujemy, że

$$\max\{\gamma, q' + r'\} \leqslant a_k < \min\{p, \gamma + q' + r'\}.$$

Zatem

$$\begin{aligned} C_{3b} &\leqslant \min\{p, \gamma + q' + r'\} - \max\{\gamma, q' + r'\} = \min\{\gamma, p - \gamma, q' + r', p - q' - r'\} \\ &\leqslant \min\{q' + r', p - q' - r'\} = \min\{\alpha + \beta, p - \alpha - \beta\}, \end{aligned}$$

gdzie skorzystaliśmy z faktu, że dla $q' + r' < p$ zachodzi $\alpha = q'$ oraz $\beta = r'$.

Przypadki (3a) i (3b) wykluczają się wzajemnie, stąd $C_3 = \min\{\alpha + \beta, p - \alpha - \beta\}$. W szczególności wzór pozostaje prawdziwy dla $q' + r' = p$.

W przypadku (4), na mocy lematów 2.13 i 2.15, zachodzi $a_k \in \mathcal{A}_2^p$, więc $q' \leqslant a_k < r'$. Z tych samych lematów wnioskujemy, że $F_{k-r} = 0$, zatem $Q_k = (1, 2, 0, 1)$. Z lematu 2.13 wynikają nierówności $a_k - q' = a_{k-r} < \gamma$ oraz $a_k - r' + p = a_{k-q} \geqslant \gamma$. Wobec tego

$$\max\{r' + \gamma - p, q'\} \leqslant a_k < \min\{q' + \gamma, r'\},$$

z czego otrzymujemy

$$\begin{aligned} C_k &\leqslant \min\{q'+\gamma, r'\} - \max\{r'+\gamma-p, q'\} = \min\{\gamma, p-\gamma, p-r'+q', r'-q'\} \\ &\leqslant \min\{p-r'+q', r'-q'\} = \min\{\beta-\alpha, p+\alpha-\beta\}. \end{aligned}$$

Z tabeli 2.2 wynika, że

$$-(C_1+C_3) \leqslant a_k \leqslant C_2+C_4.$$

W takim razie

$$\begin{aligned} A_{pqr} &\leqslant \max\Big\{ \min\{2\alpha+\beta, p-\beta\}, \min\{\beta, p+2\alpha-\beta\}\Big\} \\ &= \begin{cases} \max\Big\{\min\{2\alpha+\beta^*, p-\beta^*\}, \beta^*\Big\}, & \text{dla } \beta < p/2, \\ \max\Big\{\beta^*, \min\{p-\beta^*, 2\alpha+\beta^*\}\Big\}, & \text{dla } \beta > p/2 \end{cases} \\ &= \min\{2\alpha+\beta^*, p-\beta^*\}. \end{aligned}$$

Otrzymany wynik nie zależy od kierunku nierówności $q' \leqslant r'$, zatem możemy już opuścić to założenie, kończąc tym samym dowód. □

Podajemy tu kilka wniosków twierdzenia 8. Pierwszy z nich wymaga twierdzenia 9, które teraz udowodnimy.

Dowód twierdzenia 9. Na mocy faktu 2.3 oraz wniosku 2.4 mamy

$$|a_{pqr}(m)| = |a_{pqr}(\varphi(pqr)-m)| \leqslant 2(\lfloor m/qr \rfloor + 1).$$

Stąd

$$\begin{aligned} S_{pqr} &\leqslant 2 \sum_{k=0}^{\varphi(pqr)/2} \min\{A_{pqr}, 2(\lfloor m/qr \rfloor + 1)\} \\ &\leqslant A_{pqr}(\varphi(pqr)+2-2\lfloor A_{pqr}/2 \rfloor qr) + 2qr \sum_{a=0}^{\lfloor A_{pqr}/2 \rfloor - 1} (2a+2) \\ &= A_{pqr}(p-1)(q-1)(r-1) + 2A_{pqr} - 2\lfloor A_{pqr}/2 \rfloor A_{pqr} qr \\ &\quad + 2\lfloor A_{pqr}/2 \rfloor (2\lfloor A_{pqr}/2 \rfloor + 1) qr \\ &< A_{pqr}(2p - A_{pqr})qr/2, \end{aligned}$$

co kończy dowód. □

Teraz zastosujemy twierdzenie 8. Otrzymujemy

$$\begin{aligned} 2S_{pqr}/(qr) &= \min\{2\alpha+\beta^*, p-\beta^*\}\max\{2p-2\alpha-\beta^*, p+\beta^*\} \\ &= \min\left\{(2\alpha+\beta^*)(p+\beta^*), (p-\beta^*)(2p-2\alpha-\beta^*)\right\} \\ &= \beta^*(2\alpha+\beta^*-p)+2p\min\{\beta^*, p-\alpha-\beta^*\}, \end{aligned}$$

co ostatecznie daje

$$S_{pqr} \leqslant pqr\min\{\beta^*, p-\alpha-\beta^*\}+\frac{1}{2}qr\beta^*(2\alpha+\beta^*-p).$$

Na specjalną uwagę zasługuje pewna klasa wielomianów, którą definiujemy niżej.

Definicja 2.24. Wielomian $P \in \mathbb{Z}[x]$ nazywamy *płaskim*, jeśli $H(P) = 1$.

Wiadomo, że każdy wielomian cyklotomiczny rzędu 0, 1 lub 2 jest płaski. Bachman [4] jako pierwszy znalazł nieskończoną rodzinę płaskich wielomianów cyklotomicznych rzędu 3. Jego wynik wzmocnił później Kaplan.

Twierdzenie 2.25 (Kaplan [35], 2007)**.** *Jeśli* $r \equiv \pm 1 \pmod{pq}$*, to wielomian* Φ_{pqr} *jest płaski.*

Choć twierdzenie 8 nie pozwala w bezpośredni sposób odkryć nowych nieskończonych rodzin płaskich wielomianów cyklotomicznych rzędu 3, dostarcza ono rodziny wielomianów *prawie płaskich*, czyli takich, w których p może być dowolne, natomiast A_{pqr} nie przekracza pewnej ustalonej liczby.

Wniosek 2.26. *Niech* $p > 12$ *oraz*

$$p = 2d_2 \pm 1 = 3d_3 \pm 1 = 4d_4 \pm 1 = 6d_6 \pm 1$$

(znaki $\pm$ *nie muszą sobie odpowiadać). Dodatkowo połóżmy* $d_1 = 1$*. Jeśli zachodzą kongruencje* $q \equiv \pm d_{j_1} \pmod{p}$ *oraz* $r \equiv \pm d_{j_2} \pmod{p}$*, to*

$$A_{pqr} \leqslant j_1 + j_2 + \min\{j_1, j_2\} \leqslant 18.$$

Dowód. Wystarczy zauważyć, że $\alpha = \min\{j_1, j_2\}$ oraz $\beta^* = \max\{j_1, j_2\}$ i zastosować twierdzenie 8. □

Z twierdzenia 8 wynika rónież, że dla ustalonego p poprawiona hipoteza Beiter statystycznie zachodzi w przynajmniej $25 + O(1/p)$ przypadkach na 27. Innymi słowy, jeżeli określić

$$D_{\mathrm{HB}}(p) = \liminf_{n\to\infty} \frac{\#\{(q,r) : p < q < r < n, A_{pqr} \leqslant 2p/3\}}{\#\{(q,r) : p < q < r < n\}},$$

to prawdziwa jest następująca nierówność.

Wniosek 2.27. $D_{HB}(p) \geqslant 25/27 + O(1/p)$.

Dowód. Niech $a(j_1, j_2) = \min\{2\alpha+\beta^*, p-\beta^*\}$, gdzie α i β^* są takie, jak w twierdzeniu 8, dla wielomianu Φ_{pqr} spełniającego warunki $q^{-1}(p) = j_1$ oraz $r^{-1}(p) = j_2$. Korzystając z twierdzenia Dirichleta o liczbach pierwszych w postępach arytmetycznych oraz twierdzenia 8, otrzymujemy

$$\begin{aligned} D_{\mathrm{HB}}(p) &\geqslant \lim_{n\to\infty} \frac{\sum_{a(j_1,j_2)\leqslant 2p/3} \#\{(q,r) : p<q<r<n, (q,r) \equiv (j_1^{-1}, j_2^{-1}) \pmod p\}}{\#\{(q,r) : p<q<r<n\}} \\ &= \lim_{n\to\infty} \frac{\frac{n^2}{2(p-1)^2\log^2 n}\sum_{a(j_1,j_2)\leqslant 2p/3} 1}{n^2/(2\log^2 n)} = (p-1)^{-2} \sum_{a(j_1,j_2)\leqslant 2p/3} 1, \end{aligned}$$

gdzie sumowanie przebiega po wszystkich parach (j_1, j_2) niezerowych reszt modulo p. W takim razie

$$\begin{aligned} D_{\mathrm{HB}}(p) &\geqslant 8(p-1)^{-2} \left(\sum_{1\leqslant\alpha\leqslant\beta^*\leqslant(p-1)/2} \sum_{\min\{2\alpha+\beta^*, p-\beta^*\}\leqslant 2p/3} + O(p) \right) \\ &= p^{-2} \left(\sum_{\beta^*=1}^{p-1/2} \sum_{\alpha=1}^{\beta^*} 1 - \sum_{\beta^*=\lfloor 2p/9\rfloor+1}^{\lceil p/3\rceil-1} \sum_{\alpha=\lfloor p/3-\beta^*/2\rfloor+1}^{\beta^*} 1 \right) + O(1/p) \\ &= 8(1/8 - 1/108) + O(1/p) = 25/27 + O(1/p), \end{aligned}$$

co dowodzi postulowanej nierówności. □

2.3. Sąsiednie współczynniki

Na początku zaprezentujemy alternatywny, łatwiejszy dowód twierdzenia 10, oparty na lematach 2.12, 2.13, 2.15, 2.16 oraz 2.23. W tym celu podajemy wzór na różnicę pomiędzy kolejnymi współczynnikami Φ_{pqr}. Stosujemy w nim ponownie oznaczenia N_0, N_1 i N_2 zdefiniowane przed sformułowaniem lematu 2.23. Niech także

$$\begin{aligned} \mathcal{F}^+(m) &= (F_m, F_{m-q-r}, F_{m-r-p}, F_{m-p-q}) \\ \mathcal{F}^-(m) &= (F_{m-p}, F_{m-q}, F_{m-r}, F_{m-p-q-r}). \end{aligned}$$

O ile nie doprowadzi to do nieporozumienia, będziemy pisać w skrócie $\mathcal{F}^+ = \mathcal{F}^+(m)$ oraz $\mathcal{F}^- = \mathcal{F}^-(m)$.

Lemat 2.28. *Dla $0 \leqslant m < pqr$ zachodzą równości:*

$$\begin{aligned} a_{pqr}(m) - a_{pqr}(m-1) &= N_0(\mathcal{F}^+) - N_0(\mathcal{F}^-) \\ &= N_2(\mathcal{F}^+) - N_2(\mathcal{F}^-) \\ &= -\frac{1}{2}\Big(N_1(\mathcal{F}^+) - N_1(\mathcal{F}^-)\Big). \end{aligned}$$

Dowód. Jest to bezpośredni wniosek z lematu 2.23. □

Dowód twierdzenia 10. Rozważmy zbiór

$$\Big\{F_m, F_{m-p}, F_{m-q}, F_{m-r}, F_{m-q-r}, F_{m-r-p}, F_{m-p-q}, F_{m-p-q-r}\Big\}$$

jako graf, w którym krawędzie odpowiadają zbiorom $\{F_{j_1}, F_{j_2}\}$, spełniającym warunek $|j_1 - j_2| \in \{p, q, r\}$. Na mocy ostatniej równości w lemacie 2.28 wnioskujemy, że $|a_{pqr}(m) - a_{pqr}(m-1)| \leqslant 2$. Załóżmy, że zachodzi tu równość i spróbujmy uzyskać sprzeczność. Mamy $\mathcal{F}^+ = (1,1,1,1)$ albo $\mathcal{F}^- = (1,1,1,1)$. Znów na mocy lematu 2.28, w tym spośród ciągów $\mathcal{F}^+$, $\mathcal{F}^-$, który jest różny od $(1,1,1,1)$, występują dwa zera, obydwa na jednym 4-cyklu $(F_{j_1}, F_{j_2}, F_{j_3}, F_{j_4})$. Cykl ten spełnia równość

$$\Big|(F_{j_1} - F_{j_3}) - (F_{j_2} - F_{j_4})\Big| = 2,$$

która zaprzecza lematowi 2.15. □

Uwaga 2.29. W powyższym dowodzie nie korzystamy z lematu 2.19, choć łatwo zaobserwować, że $V(m) = a_{pqr}(m) - a_{pqr}(m-1)$ oraz żadna z liczb $V(m)$ z tabeli 2.1 nie przekracza 1 co do bezwzględnej wartości.

Dowód twierdzenia 10 nie wymaga lematu 2.19, natomiast konieczne będzie wykorzystanie go w celu obliczenia

$$J_{pqr} = \#\{m : a_{pqr}(m) = a_{pqr}(m-1) + 1\}.$$

Wyprowadzimy dokładny wzór na J_{pqr}, w zależności od p, q, r i liczb α i β zdefiniowanych przed sformułowaniem twierdzenia 8. Tym razem dodamy im indeksy, przyjmując $\alpha_p = \alpha$, $\beta_p = \beta$ oraz definiując analogicznie

$$\alpha_q = \min\{r^{-1}(q), p^{-1}(q), q - r^{-1}(q), q - p^{-1}(q)\}, \quad \beta_q = (\alpha_q rp)^{-1}(q),$$

podobnie definiujemy α_r i β_r.

Przed przeprowadzeniem dowodu warto przypomnieć liczbę elementów każdego ze zbiorów $\mathcal{A}_0^p, \mathcal{A}_1^p, \ldots, \mathcal{A}_4^p$.

Fakt 2.30. Zachodzą równości

$$\#\mathcal{A}_1^p = \#\mathcal{A}_3^p = \alpha_p, \quad \#\mathcal{A}_2^p = \beta_p - \alpha_p, \quad \#\mathcal{A}_0^p + \#\mathcal{A}_4^p = p - \alpha_p - \beta_p,$$

oraz analogiczne dla q i r.

Potrzebujemy jeszcze paru dodatkowych oznaczeń, dla uproszczenia zapisu. Niech

$$\sum_{\text{cycl}} f(p,q,r) = f(p,q,r) + f(r,p,q) + f(q,r,p),$$
$$\sum_{\text{perm}} f(p,q,r) = f(p,q,r) + f(r,p,q) + f(q,r,p) + f(r,q,p) + f(p,r,q) + f(q,p,r).$$

Definicja 2.31. Wprowadzamy następujące stałe, zależne od p, q i r.

$$R = \sum_{\text{cycl}} \delta'_p \alpha_p (q - \alpha_q - \beta_q)(r - \alpha_r - \beta_r),$$
$$S = \sum_{\text{cycl}} \delta_p \alpha_p (\beta_q - \alpha_q)(\beta_r - \alpha_r),$$
$$T = \sum_{\text{perm}} \delta_{qr} (\beta_p - \alpha_p)(\alpha_q \# \mathcal{A}_0^r + \alpha_r \# \mathcal{A}_4^q),$$

gdzie $\delta_p = 1$, gdy zachodzą nierówności

$$\begin{cases} p^{-1}(q) & < & r^{-1}(q), \\ p^{-1}(r) & < & q^{-1}(r), \end{cases} \quad \text{lub} \quad \begin{cases} p^{-1}(q) & > & r^{-1}(q), \\ p^{-1}(r) & > & q^{-1}(r), \end{cases}$$

w przeciwnym razie $\delta_p = 0$. Ponadto $\delta'_p = 1$, gdy pierwsze wyrażenie z lematu 2.22 ma inną wartość logiczną niż pozostałe, w przeciwnym razie $\delta'_p = 0$. Analogicznie określamy δ_q, δ_r oraz δ'_q, δ'_r.

Twierdzenie 2.32. *Zachodzi równość*

$$J_{pqr} = \sum_{cycl} \alpha_p \alpha_q (r - 2\alpha_r) + R + S + T,$$

gdzie R, S i T określone są w definicji 2.31.

Dowód. Dla skrócenia zapisu przyjmijmy oznaczenia

$$\sigma^{\text{perm}}_{j_1 j_2 j_3} = \sum_{\text{perm}} \#\mathcal{A}^p_{j_1} \#\mathcal{A}^q_{j_2} \#\mathcal{A}^r_{j_3},$$
$$\sigma^{\text{perm}}_{j_1 j_2 j_3}(f(p,q,r)) = \sum_{\text{perm}} f(p,q,r) \#\mathcal{A}^p_{j_1} \#\mathcal{A}^q_{j_2} \#\mathcal{A}^r_{j_3},$$

analogicznie $\sigma^{\text{cycl}}_{j_1 j_2 j_3}$ dla sumowania po cyklach. Będziemy się posługiwać lematem 2.19, tabelą 2.1, uwagą 2.21 oraz faktem 2.30. Otrzymujemy

$$\begin{aligned} J_{pqr} = {} & \sigma^{\text{cycl}}_{001} + \sigma^{\text{cycl}}_{011} + \sigma^{\text{cycl}}_{334} + \sigma^{\text{cycl}}_{344} + \sigma^{\text{perm}}_{123}(\delta_{pr}) \\ & + \sigma^{\text{perm}}_{012}(\delta_{qp}) + \sigma^{\text{perm}}_{234}(\delta_{rq}) + \sigma^{\text{cycl}}_{122}(\delta_{pq}\delta_{pr}) + \sigma^{\text{cycl}}_{223}(\delta_{pr}\delta_{qr}). \end{aligned}$$

Obliczymy wartość tego wyrażenia w kilku krokach:

$$\sigma^{\mathrm{cycl}}_{001} + \sigma^{\mathrm{cycl}}_{344} = \sigma^{\mathrm{cycl}}_{100} + \sigma^{\mathrm{cycl}}_{344} = \sum_{\mathrm{cycl}} \alpha_p \Big(\#\mathcal{A}^q_0 \#\mathcal{A}^r_0 + \#\mathcal{A}^q_4 \#\mathcal{A}^r_4 \Big) = R,$$
$$\sigma^{\mathrm{cycl}}_{011} + \sigma^{\mathrm{cycl}}_{334} = \sigma^{\mathrm{cycl}}_{011} + \sigma^{\mathrm{cycl}}_{411} = \sum_{\mathrm{cycl}} (p - \alpha_p - \beta_p)\alpha_q \alpha_r.$$

Przechodzimy teraz do sum zawierających wyrażenia postaci δ_{pq}. Poniższe równości pozostają prawdziwe, bowiem jeśli $\delta_{pr} + \delta_{rp} \neq 1$, to zbiór $\mathcal{A}^q_2$ jest pusty.

$$\sigma^{\mathrm{perm}}_{123}(\delta_{pr}) = \sigma^{\mathrm{cycl}}_{123}(\delta_{pr}) + \sigma^{\mathrm{cycl}}_{321}(\delta_{rp}) = \sum_{\mathrm{cycl}} \alpha_p \alpha_q (\beta_r - \alpha_r),$$
$$\sigma^{\mathrm{perm}}_{012}(\delta_{qp}) + \sigma^{\mathrm{perm}}_{234}(\delta_{rq}) = \sigma^{\mathrm{perm}}_{210}(\delta_{qr}) + \sigma^{\mathrm{perm}}_{243}(\delta_{qr}) = T,$$
$$\sigma^{\mathrm{cycl}}_{122}(\delta_{pq}\delta_{pr}) + \sigma^{\mathrm{cycl}}_{223}(\delta_{pr}\delta_{qr}) = \sigma^{\mathrm{cycl}}_{122}(\delta_{pq}\delta_{pr}) + \sigma^{\mathrm{cycl}}_{322}(\delta_{rp}\delta_{qp}) = S.$$

Sumując otrzymane wyniki, dostajemy tezę. □

Bezpośrednim wnioskiem z dowiedzionego powyżej twierdzenia jest twierdzenie 11. Poniżej przeprowadzamy jego dowód.

Dowód twierdzenia 11. Skorzystamy z faktu, że $ab \geqslant a + b - 1$ dla liczb całkowitych $a, b > 0$. Na mocy twierdzenia 2.32 mamy

$$\begin{aligned} J_{pqr} &\geqslant \sum_{\mathrm{cycl}} \alpha_p \alpha_q (r - 2\alpha_r) = \frac{1}{2} \sum_{\mathrm{cycl}} \alpha_p \Big(\alpha_q (r - 2\alpha_r) + (q - 2\alpha_q)\alpha_r \Big) \\ &\geqslant \frac{1}{2} \sum_{\mathrm{cycl}} \Big(\alpha_q + (r - 2\alpha_r) - 1 + (q - 2\alpha_q) + \alpha_r - 1 \Big) \\ &= \frac{1}{2} \sum_{\mathrm{cycl}} (q - \alpha_q - 1 + r - \alpha_r - 1) \geqslant \frac{1}{2} \sum_{\mathrm{cycl}} \Big((q-1)/2 + (r-1)/2 \Big) \\ &= (p-1)/2 + (q-1)/2 + (r-1)/2 > (p+q+r)/3 > \sqrt[3]{pqr}, \end{aligned}$$

gdzie w ostatnim kroku skorzystaliśmy z nierówności między średnią arytmetyczną i geometryczną. □

Pod pewnymi, dość mocnymi założeniami, możemy uzasadnić, że stałej $1/3$ nie można w tym twierdzeniu zmniejszyć. Przypomnijmy, że $P(m)$ oznacza największy dzielnik pierwszy m. Liczbę pierwszą q nazywamy liczbą Sophie Germain, jeżeli liczba $2q + 1$ również jest pierwsza.

Twierdzenie 2.33. *Niech $\varepsilon > 0$. Załóżmy, że istnieje nieskończenie wiele liczb pierwszych q Sophie Germain, spełniających warunek $P(q+1) > q^{1-\varepsilon}$. Wtedy istnieje nieskończenie wiele liczb $n = pqr$, dla których $J_n = O(n^{1/(3-\varepsilon)})$.*

Dowód. Przyjmijmy $p = P(q+1)$, $q = tp-1$, gdzie $3 \leqslant t < q^{\varepsilon}$ oraz $r = 2q+1 = 2tp-1$. Wtedy

$$\begin{array}{lll} q^{-1}(p) = p-1, & r^{-1}(q) = 1, & p^{-1}(r) = 2t, \\ r^{-1}(p) = p-1, & p^{-1}(q) = t, & q^{-1}(r) = 2tp-3, \\ \alpha_p = 1, & \alpha_q = 1, & \alpha_r = 2, \\ \beta_p = 1, & \beta_q = t, & \beta_r = 2tp-2t-1, \\ \mathcal{A}_4^p = \emptyset, & \mathcal{A}_0^q = \emptyset, & \mathcal{A}_4^r = \emptyset, \end{array}$$

a ponadto $\delta_{rp} = \delta_{pq} = \delta'_q = 1$ oraz wszystkie pozostałe delty z twierdzenia 2.32 wynoszą 0. Obliczmy wszystkie parametry, które występują w tym twierdzeniu:

$$\sum_{\text{cycl}} \alpha_p\alpha_q(r-2\alpha_r) = (2tp-5) + 2(tp-3) + 2(p-2) < 6q,$$

$$R = (p-\alpha_p-\beta_p)\alpha_q(r-\alpha_r-\beta_r) = (p-2)(2t-2) < 2q.$$

Ponieważ $\delta_p = \delta_q = \delta_r = 0$, otrzymujemy $S = 0$. Pozostaje jeszcze do obliczenia

$$T = (\beta_q-\alpha_q)(\alpha_r\#\mathcal{A}_0^p + \alpha_p\#\mathcal{A}_4^r) + (\beta_r-\alpha_r)(\alpha_p\#\mathcal{A}_0^q + \alpha_q\#\mathcal{A}_4^p) = (t-1)2(p-2) < 2q.$$

Na mocy twierdzenia 2.32, $J_{pqr} < 10q$. Ponadto $pqr > q^{3-\varepsilon}$, co kończy dowód. □

Nasze założenie wynika z hipotezy H Schinzla. Można wziąć na przykład $q = 6p-1$ oraz $r = 12p-1$.

Do udowodnienia pozostało nam jeszcze oszacowanie liczby θ_n niezerowych współczynników wielomianu Φ_n, dla $n = pqr$.

Dowód twierdzenia 12. Liczba skoków współczynników Φ_{pqr}, czyli liczba tych m, dla których $|a_{pqr}(m) - a_{pqr}(m-1)| = 1$, wynosi $2J_{pqr}$, ponieważ wielomian Φ_{pqr} jest palindromiczny. Połowa liczby skoków szacuje od dołu liczbę nieparzystych współczynników, które są oczywiście niezerowe. W takim razie $\theta_{pqr} \geqslant J_{pqr}$, co po zastosowaniu twierdzenia 11 kończy dowód. □

Rozdział 3

Wielomiany wyższych rzędów

Pierwsze zasługujące na uwagę oszacowanie liczby A_n w przypadku ogólnym podał Bateman.

Twierdzenie 3.1 (Bateman [13], 1949)**.** *Zachodzi nierówność* $A_n \leqslant n^{d(n)/2}$*, gdzie* $d(n)$ *oznacza liczbę dzielników* n*.*

Stosując wykazaną przez Wigerta nierówność $d(n) \leqslant 2^{(1+o(1))\log n/\log\log n}$, w tej samej pracy Bateman udowadnia następujący wniosek.

Wniosek 3.2. $\log\log A_n \leqslant (\log 2 + o(1))\log n/\log\log n$*.*

Erdös [25] przypuszczał, że stałej $\log 2$ nie można zmniejszyć. Po 26 latach udowodnił to Vaughan [53].

Na uwagę zasługują także poniższe oszacowania Maiera.

Twierdzenie 3.3 (Maier [41, 42], 1993 – 1996)**.** *Dla dowolnych funkcji* $\varepsilon, E : \mathbb{N} \to \mathbb{R}$*, spełniających warunek* $\varepsilon(n) \to 0$ *i* $E(n) \to \infty$ *przy* $n \to \infty$*, nierówność*

$$n^{\varepsilon(n)} < A_n < n^{E(n)}$$

zachodzi w zbiorze liczb n *o gęstości naturalnej* 1*.*

Chcielibyśmy znaleźć oszacowanie zależne od dzielników pierwszych n. Dla wielomianów cyklotomicznych rzędu 4 wygląda ono następująco.

Twierdzenie 3.4 (Bloom [15], 1968)**.** $A_{pqrs} \leqslant p(p-1)(pq-1)$*.*

Jak widać, wynik nie zależy od liczb pierwszych r i s, podobnie jak oszacowanie $A_{pqr} \leqslant \frac{3}{4}p$ nie zależy od q i r. Nie są to wyjątki, o czym świadczy następujące twierdzenie.

Twierdzenie 3.5 (Flesh i Schmidt [29], 1968; Justin [34], 1969)**.** *Liczba $A_{p_1p_2\ldots p_k}$ może być oszacowana z góry przez funkcję liczb $p_1, p_2, \ldots, p_{k-2}$.*

Möller podał następujące oszacowanie, bazując na zależności rekurencyjnej, którą uzyskał Justin w wyżej cytowanej pracy.

Twierdzenie 3.6 (Möller [47], 1971)**.** *Zachodzi nierówność*

$$A_{p_1p_2\ldots p_k} \leqslant (p_{k-2}p_{k-3})^3(p_{k-4}p_{k-5})^7(p_{k-6}p_{k-7})^{15}\ldots.$$

Wynik ten został kilka lat później poprawiony. Niech $n = p_1p_2\ldots p_k$, gdzie $p_1 < p_2 < \ldots < p_k$, oraz niech

$$M_n = \prod_{j=1}^{k-2} p_j^{2^{k-j-1}-1}.$$

Twierdzenie 3.7 (Bateman, Pomerance i Vaughan [14], 1981)**.** $A_n \leqslant M_n$.

W niniejszej rozprawie doktorskiej nieznacznie poprawimy ten wynik. Udowodnimy, że prawą stronę można pomnożyć przez $(C + o_k(1))^{2^k}$, gdzie $C < 1$, k jest rzędem wielomianu cyklotomicznego Φ_n, natomiast $o_k(1) \to 0$ dla $k \to \infty$. Jest to równoważne twierdzeniu 13, którego dowód podajemy w następnym podrozdziale.

3.1. Szacowanie współczynników

W bieżącym podrozdziale przyjmujemy $n = p_1\ldots p_k$. Kluczem do dowodu twierdzenia 13 jest następująca zależność rekurencyjna.

Lemat 3.8. *Dla różnych liczb pierwszych $p_1, \ldots, p_k$ mamy*

$$\Phi_{p_1\ldots p_k}(x) = f(x)\cdot\prod_{j=1}^{k-2} P_j(x),$$

gdzie

$$P_j = \prod_{i=j+2}^{k} \Phi_{p_1\ldots p_j}(x^{p_{j+2}\ldots p_k/p_i})$$

oraz f jest szeregiem formalnym, określonym równaniem

$$f(x) = (1-x^{p_1\ldots p_k})\cdot\frac{\prod_{i=2}^{k}(1-x^{p_2\ldots p_k/p_i})}{\prod_{i=1}^{k}(1-x^{p_1\ldots p_k/p_i})}.$$

Dowód. Przeprowadzimy dowód przez indukcję ze względu na k. Dla $k < 5$ lemat zachodzi, co udowodnił Bloom [15]. Wprowadźmy następujące oznaczenia:

$$\widetilde{P}_j(x) = \prod_{i=j+2}^{k} \Phi_{p_2 \dots p_j}(x^{p_{j+2} \dots p_k / p_i})$$

oraz

$$\widetilde{f}(x) = (1 - x^{p_2 \dots p_k}) \cdot \frac{\prod_{i=3}^{k}(1 - x^{p_3 \dots p_k / p_i})}{\prod_{i=2}^{k}(1 - x^{p_2 \dots p_k / p_i})}.$$

Znany jest fakt, że $\Phi_{np}(x) = \Phi_n(x^p)/\Phi_n(x)$ dla liczb pierwszych p nie dzielących n. Wobec tego, oraz powyższej równości, mamy

$$\Phi_{p_1 \dots p_k}(x) = \frac{\Phi_{p_2 \dots p_k}(x^{p_1})}{\Phi_{p_2 \dots p_k}(x)} \quad \text{oraz} \quad P_j(x) = \frac{\widetilde{P}_j(x^{p_1})}{\widetilde{P}_j(x)}.$$

Na mocy założenia indukcyjnego otrzymujemy

$$\Phi_{p_2 \dots p_k} = \widetilde{f}(x) \cdot \prod_{j=2}^{k-2} \widetilde{P}_j(x).$$

Podstawiając to do otrzymanych wcześniej wzorów, uzyskujemy równość

$$\Phi_{p_1 \dots p_k}(x) = \frac{\widetilde{f}(x^{p_1}) \cdot \prod_{j=2}^{k-2} \widetilde{P}_j(x^{p_1})}{\widetilde{f}(x) \cdot \prod_{j=2}^{k-2} \widetilde{P}_j(x)} = \frac{\widetilde{f}(x^{p_1})}{\widetilde{f}(x) P_1(x)} \cdot \prod_{j=1}^{k-2} P_j(x).$$

Ostatecznie

$$\frac{\widetilde{f}(x^{p_1})}{\widetilde{f}(x)} = P_1(x)(1 - x^{p_1 \dots p_k}) \cdot \frac{\prod_{i=2}^{k}(1 - x^{p_2 \dots p_k / p_i})}{\prod_{i=1}^{k}(1 - x^{p_1 \dots p_k / p_i})} = P_1(x) f(x),$$

co kończy dowód. □

Aby efektywnie wykorzystać lemat 3.8, będziemy potrzebowali ograniczenia na współczynniki f. W celu ich uzyskania, użyjemy twierdzenia Spernera, które cytujemy poniżej.

Twierdzenie 3.9 (Sperner [52], 1928)**.** *Spośród wszystkich podzbiorów zbioru m-elementowego można wybrać najwyżej $\binom{m}{\lfloor m/2 \rfloor}$, z których żaden nie jest zawarty w innym.*

Dla uproszczenia zapisu przyjmijmy $b_m = \binom{m}{\lfloor m/2 \rfloor}$.

Lemat 3.10. *Współczynniki przy potęgach o wykładniku mniejszym niż n określonego w lemacie 3.8 szeregu f nie przekraczają b_{k-2} co do bezwzględnej wartości.*

Dowód. Niech $f(x) = \sum_m d_m x^m$. Bezpośrednio z definicji f otrzymujemy

$$f(x) \equiv \left(\prod_{i=2}^{k}(1 - x^{p_2 \ldots p_k/p_i})\right) \sum_{\alpha_1,\ldots,\alpha_k \geqslant 0} x^{\alpha_1 n/p_1 + \ldots + \alpha_k n/p_k} \pmod{x^n}.$$

Określmy następujący zbiór $\Lambda \subset \mathbb{R}^{k-1}$ oraz funkcję $s : \Lambda \to \{-1, 1\}$.

$$\Lambda = \Big\{\lambda = (\lambda_2, \ldots, \lambda_k) : \lambda_i \in \{0, 1\} \text{ dla } i = 2, \ldots, k\Big\}, \quad s(\lambda) = (-1)^{\lambda_2 + \ldots + \lambda_k}.$$

Na mocy wcześniejszej kongruencji, mamy

$$d_m = \sum_{\lambda \in \Lambda} s(\lambda)\chi(m - \langle \lambda, v/p_1 \rangle),$$

gdzie $\langle \cdot, \cdot \rangle$ oznacza iloczyn skalarny w $\mathbb{R}^{k-1}$, $v = (n/p_2, \ldots, n/p_k)$ oraz

$$\chi(m) = \begin{cases} 1, & \text{gdy } m = \alpha_1 n/p_1 + \ldots + \alpha_k n/p_k \text{ dla pewnych } \alpha_1, \ldots, \alpha_k \geqslant 0, \\ 0, & \text{w przeciwnym przypadku.} \end{cases}$$

Dla $j = 2, 3, \ldots, k$ oraz $t \in \{0, 1\}$ określamy liczbę całkowitą nieujemną $\alpha_j(t) < p_j$, spełniającą kongruencję

$$\alpha_j(t) \equiv \frac{p_j}{n} m - \frac{t}{p_1} \pmod{p_j}.$$

Niech $\alpha = (\alpha_i(\lambda_i))_{i=2}^k$. Na mocy twierdzenia chińskiego o resztach, dla każdego $\lambda \in \Lambda$ zachodzi kongruencja

$$m - \langle \lambda, v/p_1 \rangle \equiv \beta(\lambda) n/p_1 + \langle \alpha(\lambda), v \rangle \pmod{n},$$

gdzie $\beta(\lambda) \in \{0, 1, \ldots, q_1 - 1\}$. Wobec powyższego, następujące fakty są sobie równoważne:

- $\chi(m - \langle \lambda, v/p_1 \rangle) = 1$,
- $\langle \lambda, v/p_1 \rangle + \langle \alpha(\lambda), v \rangle \leqslant m$,
- $\langle \lambda, v/p_1 \rangle + \langle \alpha(\lambda) - \alpha(\mathbf{0}), v \rangle \leqslant m - \langle \alpha(\mathbf{0}), v \rangle$,

gdzie $\mathbf{0}$ oznacza wektor zerowy w $\mathbb{R}^{k-1}$. W takim razie

$$\langle \alpha(\lambda) - \alpha(\mathbf{0}), v \rangle = \sum_{i=2}^{k} (\alpha_i(\lambda_i) - \alpha_i(0)) v_i = \sum_{i=2}^{k} (\alpha_i(1) - \alpha_i(0)) v_i \lambda_i = \langle \lambda, w \rangle,$$

gdzie $w = ((\alpha_i(1) - \alpha_i(0))v_i)_{i=2}^k$. Wobec tego $\chi(m - \langle \lambda, v/p_1 \rangle) = 1$ wtedy i tylko wtedy, gdy $\langle \lambda, u \rangle \leqslant D$, gdzie $u = v/p_1 + w$ i $D = m - \langle \alpha(\mathbf{0}), v \rangle$. Ostatecznie otrzymujemy

$$d_m = \sum_{\lambda \in \Lambda,\ \langle \lambda, u \rangle \leqslant D} s(\lambda),$$

przy czym ani liczba D, ani wektor u nie zależy od λ.

Bez straty ogólności możemy założyć, że $0 \leqslant u_k \leqslant u_2, \ldots, u_{k-1}$.

Istnieje naturalna bijekcja S pomiędzy zbiorem Λ a rodziną wszystkich podzbiorów zbioru $\{2, 3, \ldots, k\}$. Jest ona określona wzorem

$$S_\lambda = \{i \in \{2, \ldots, k\} : \lambda_i = 1\}.$$

Nazwijmy $\lambda = (\lambda_2, \ldots, \lambda_{k-1}, 0)$ maksymalną, gdy $\langle \lambda, u \rangle \leqslant D$ i dla każdego $\lambda' = (\lambda'_2, \ldots, \lambda'_{k-1}, 0)$ spełniającego inkluzję $S_\lambda \subset S_{\lambda'}$ zachodzi nierówność $\langle \lambda', u \rangle > D$. Dla wszystkich

$$\lambda^0 = (\lambda_2, \ldots, \lambda_{k-1}, 0) \quad \text{i} \quad \lambda^1 = (\lambda_2, \ldots, \lambda_{k-1}, 1)$$

zachodzą następujące zależności:

- Jeśli λ^0 nie jest maksymalna i $\langle \lambda^0, u \rangle \leqslant D$, to $\langle \lambda^1, u \rangle \leqslant D$.
- Jeśli $\langle \lambda^1, u \rangle \leqslant D$, to $\langle \lambda^0, u \rangle \leqslant D$.
- $s(\lambda^0) + s(\lambda^1) = 0$.

Stąd oraz na mocy uzyskanego wcześniej wzoru na d_m wnioskujemy, że

$$|d_m| \leqslant \#\{\lambda \in \Lambda \ :\ \lambda \text{ jest maksymalna}\}.$$

Pozostaje już tylko zauważyć, że gdy weźmiemy wszystkie maksymalne λ, to żaden ze zbiorów S_λ nie będzie zawarty w innym zbiorze tego typu. Są to ponadto podzbiory zbioru $\{2, 3, \ldots, k-1\}$, z czego po zastosowaniu twierdzenia 3.9 wynika teza. □

Po takim przygotowaniu możemy rozpocząć dowód twierdzenia 13. Będziemy stosować oznaczenia H i S z definicji 6, a także A_n i S_n oraz M_n określone przed sformułowaniem twierdzenia 13. Ponadto przez f^* oznaczymy wielomian stopnia mniejszego niż n, spełniający kongruencję $f^* \equiv f \pmod{x^n}$. Wprowadzamy jeszcze dodatkowo następujące stałe:

$$d = \sup_{p,q,r} \frac{S_{pqr}}{p^2 qr}, \quad \varrho = \prod_{j=0}^{\infty} \left(\frac{2j+5}{2j+6} \right)^{4^{-j}}, \quad C = \left(\frac{3}{4} \epsilon_3^{1/2} d \varrho^{1/8} \right)^{1/32}.$$

Dla tak zdefiniowanej stałej C przeprowadzimy dowód. Stosując fakt $\varepsilon_3 \leqslant \frac{3}{4}$ oraz twierdzenie 9, uzyskujemy po bezpośrednich obliczeniach $C < 0.9627$. Jeśli ponadto zachodzi poprawiona hipoteza Beiter, czyli $\varepsilon_3 = \frac{2}{3}$, to $C < 0.9594$.

Dowód twierdzenia 13. Niech

$$\varepsilon_j = \sup_{p_1,\ldots,p_j} \frac{A_{p_1\ldots p_j}}{M_{p_1\ldots p_j}}.$$

Zachodzi nierówność

$$S_{p_1\ldots p_j} \leqslant (\deg(\Phi_{p_1\ldots p_j})+1)A_{p_1\ldots p_j} \leqslant \varepsilon_j \cdot p_j \cdot p_1^{2^{j-2}} p_2^{2^{j-3}} \ldots p_{j-2}^2 p_{j-1}.$$

W takim razie

$$S(P_j) \leqslant (S_{p_1\ldots p_j})^{k-j-1} = \varepsilon_j^{k-j-1} \left(p_j \cdot p_1^{2^{j-2}} p_2^{2^{j-3}} \ldots p_{j-2}^2 p_{j-1}\right)^{k-j-1}.$$

Dodatkowo $S_{p_1} = p_1$, $S_{p_1p_2} < p_1p_2/2$ oraz $S_{p_1p_2p_3} \leqslant d \cdot p_1^2 p_2 p_3$. Stosując powyższe fakty oraz lematy 3.8 i 3.10, otrzymujemy dla $k \geqslant 5$

$$\begin{aligned} A_{p_1\ldots p_k} &\leqslant H(f^*) \prod_{j=1}^{k-2} S(P_j) \leqslant b_{k-2} \cdot p_1^{k-2} \cdot (p_1p_2/2)^{k-3} \cdot (dp_1^2p_2p_3)^{k-4} \cdot \prod_{j=4}^{k-2} S(P_j) \\ &\leqslant \frac{b_{k-2}d^{k-4}}{2^{k-3}} \cdot \prod_{j=4}^{k-2} \varepsilon_j^{k-j-1} \cdot \prod_{j=1}^{k-2} \left(p_j \cdot p_1^{2^{j-2}} p_2^{2^{j-3}} \ldots p_{j-2}^2 p_{j-1}\right)^{k-j-1} \\ &= \frac{b_{k-2}d^{k-4}}{2^{k-3}} \cdot \prod_{j=4}^{k-2} \varepsilon_j^{k-j-1} \cdot M_{p_1\ldots p_k}. \end{aligned}$$

Ostatnia równość wynika z faktu, że dla $t = 1, 2, \ldots, k-2$ liczba p_t występuje w iloczynie $\prod_{j=1}^{k-2}(p_j \cdot p_1^{2^{j-2}} p_2^{2^{j-3}} \ldots p_{j-2}^2 p_{j-1})^{k-j-1}$ w potędze

$$k-t-1+\sum_{j=t+1}^{k-2} 2^{j-t-1}(k-j-1) = k-t-1+\sum_{i=1}^{k-t-2}(2^i-1) = 2^{k-t-1}-1.$$

Udowodniliśmy zatem, że

$$\varepsilon_k \leqslant \frac{b_{k-2}d^{k-4}}{2^{k-3}} \cdot \prod_{j=4}^{k-2} \varepsilon_j^{k-j-1}.$$

Zdefiniujmy ciąg $(e_k)_{k=1}^{\infty}$ za pomocą rekurencji powstałej z powyższej nierówności dla $k \geqslant 5$ przez zamianę ε na e i znaku nierówności na znak równości, z warunkami początkowymi

$$e_1 = e_2 = 1, \quad e_3 = e_4 = \varepsilon_3.$$

Z nierówności $A_{pqrs} \leqslant A_{pqr}S_{pq}S_pS_1$, udowodnionej w [14] wynika, że $\varepsilon_4 \leqslant \varepsilon_3$. Zatem $\varepsilon_k \leqslant e_k$ dla wszystkich $k \geqslant 1$.

Spróbujmy wyznaczyć wzór na e_k. Dla $k = 5$ i $k = 6$ otrzymujemy

$$e_5 = \frac{3}{4}d, \quad e_6 = \frac{3}{4}\varepsilon_3 d^2,$$

natomiast dla $k \geqslant 7$ mamy

$$\frac{e_k/e_{k-1}}{e_{k-1}/e_{k-2}} = \frac{\frac{db_{k-2}}{2b_{k-3}} \cdot e_4 \dots e_{k-2}}{\frac{db_{k-3}}{2b_{k-4}} \cdot e_4 \dots e_{k-3}} = e_{k-2} \cdot \frac{b_{k-2}b_{k-4}}{b_{k-3}^2},$$

co daje znacznie prostszą postać rekurencyjną

$$e_k = e_{k-1}^2 \cdot \frac{b_{k-2}b_{k-4}}{b_{k-3}^2}.$$

Rozwijając ją, otrzymujemy

$$e_k = e_6^{2^{k-6}} \cdot \prod_{j=7}^{k} \left(\frac{b_{j-2}b_{j-4}}{b_{j-3}^2} \right)^{2^{k-j}}.$$

Prosty rachunek pozwala stwierdzić, że

$$\frac{b_{j-2}b_{j-4}}{b_{j-3}^2} = \begin{cases} \frac{j-2}{j-1} & \text{dla nieparzystych } j, \\ \frac{j-2}{j-3} & \text{dla parzystych } j. \end{cases}$$

Wobec tego

$$e_k^{2^{8-k}} = e_6^4 \cdot \left(\frac{5}{6}\right)^2 \cdot \left(\frac{6}{5}\right) \cdot \left(\frac{7}{8}\right)^{1/2} \cdot \left(\frac{8}{7}\right)^{1/4} \cdot \ldots = e_6^4 \varrho + o_k(1).$$

To kończy dowód. □

Uwaga 3.11. Istnieje taka stała $c > 0$, że dla $C < c$ twierdzenie 13 nie zachodzi. Niech p_j będzie j-tą nieparzystą liczbą pierwszą. Wtedy

$$1 \leqslant A_{p_1 \dots p_k} \leqslant (C + o(1))^{2^k} M_n,$$

zatem

$$C + o_k(1) \geqslant M_n^{-2^k} = \prod_{j=1}^{\infty} p_j^{-2^{3-j}} + o_k(1).$$

Na mocy twierdzenia o liczbach pierwszych, powyższy iloczyn jest zbieżny do pewnej dodatniej stałej c.

3.2. Wnioski z oszacowania

Jako pierwszy wniosek podajemy nierówności analogiczne do $A_{pqr} < \frac{3}{4}p$, sformułowane dla większej liczby czynników pierwszych.

Wniosek 3.12. *Zachodzą następujące szacowania:*

$$A_{pqrs} \leqslant \frac{3}{4}p^3q, \quad A_{pqrst} \leqslant \frac{45}{128}p^7q^3r, \quad A_{pqrstu} \leqslant \frac{2025}{16384}p^{15}q^7r^3s.$$

Jeżeli założyć, że poprawiona hipoteza Beiter jest prawdziwa, to:

$$A_{pqrs} \leqslant \frac{2}{3}p^3q, \quad A_{pqrst} \leqslant \frac{1}{3}p^7q^3r, \quad A_{pqrstu} \leqslant \frac{7}{81}p^{15}q^7r^3s.$$

Moree [49] rozpatrywał odwrotne wielomiany cyklotomiczne, które definiujemy poniżej.

Definicja 3.13. Wielomian Ψ_n^* spełniający zależność

$$\Psi_n^*(x)\Phi_n(x) = 1 - x^n$$

nazywamy n-tym odwrotnym wielomianem cyklotomicznym. Określamy także szereg formalny

$$\Psi_n(x) = 1/\Phi_n(x) = \sum_m c_n(m)x^m,$$

którego współczynniki są powtarzającymi się okresowo współczynnikami Ψ_n^*, o okresie n. Niech ponadto

$$C_n = H(\Psi_n^*)$$

będzie wysokością wielomianu Ψ_n^*.

Stosując twierdzenie 13, możemy udowodnić następujące, analogiczne twierdzenie dla odwrotnych wielomianów cyklotomicznych.

Twierdzenie 3.14. *Zachodzi nierówność* $(C_n/M_n)^{2^{-k}} \leqslant C + o_k(1)$*, gdzie* C *jest taką samą stałą jak w twierdzeniu 13.*

Dowód. Analogicznie jak w dowodzie twierdzenia 13, wprowadzamy oznaczenie

$$\varepsilon_j^* = \sup_{p_1,\ldots,p_j} \frac{C_{p_1\ldots p_j}}{M_{p_1\ldots p_j}}.$$

Niech p będzie liczbą pierwszą nie dzielącą n. Na mocy łatwej do otrzymania tożsamości $\Psi_{np}(x) = \Psi_n(x^p)\Phi_n(x)$ mamy

$$c_{np}(m) = \prod_{j=0}^{\lfloor m/p \rfloor} c_n(j)a_n(m - jp).$$

Zauważmy, że $a_n(t) = 0$ dla $t \notin \{0, \ldots, \varphi(n)\}$, zatem dla $k \geqslant 2$

$$C_{p_1\ldots p_k} \leqslant \left(\left\lfloor \frac{\varphi(p_1\ldots p_{k-1})}{p_k} \right\rfloor + 1\right) A_{p_1\ldots p_{k-1}}C_{p_1\ldots p_{k-1}} \leqslant p_1\ldots p_{k-2} \cdot A_{p_1\ldots p_{k-1}}C_{p_1\ldots p_{k-1}}.$$

Wobec tego

$$C_{p_1\dots p_k} \leqslant C_{p_1p_2} \prod_{j=2}^{k-1} (p_1 \dots p_{j-1} \cdot A_{p_1\dots p_j}) \leqslant \varepsilon_2 \dots \varepsilon_{k-1} M_n$$

i stąd dla $k \geqslant 6$

$$\varepsilon_k^* \leqslant \varepsilon_2 \dots \varepsilon_{k-1} \leqslant e_3 \dots e_{k-1} = \frac{2e_3 b_{k-3}}{d b_{k-2}} e_k = \left(\frac{e_3}{d} + o_k(1)\right) e_k,$$

gdzie stała d oraz liczby ε_j, e_j i b_j są takie same, jak w dowodzie twierdzenia 13.

Aby zakończyć dowód, wystarczy zastosować dowiedziony przy okazji twierdzenia 13 fakt, że $e_k^{2^{-k}} \to C$ dla $k \to \infty$. □

Dokonując bezpośrednich obliczeń, otrzymujemy następujące oszacowania.

Wniosek 3.15. *Zachodzą nierówności:*

$$C_{pqrs} \leqslant \frac{3}{4} p^3 q, \quad C_{pqrst} \leqslant \frac{9}{16} p^7 q^3 r, \quad C_{pqrstu} \leqslant \frac{405}{2048} p^{15} q^7 r^3 s.$$

Jeśli dodatkowo założyć prawdziwość poprawionej hipotezy Beiter, to:

$$C_{pqrs} \leqslant \frac{2}{3} p^3 q, \quad C_{pqrst} \leqslant \frac{4}{9} p^7 q^3 r, \quad C_{pqrstu} \leqslant \frac{4}{27} p^{15} q^7 r^3 s.$$

Wielomiany $\Phi_n(x)$ oraz $\Psi_n^*(x)$ są dzielnikami wielomianu $1 - x^n$. Pomerance i Ryan [51] zaproponowali badanie największej możliwej wysokości dzielnika $1 - x^n$, czyli liczby

$$B_n = \max_{P(x) | (1-x^n)} H(P).$$

Uzyskali przy tym, dla n będącego iloczynem k różnych nieparzystych liczb pierwszych, następujący wynik.

Twierdzenie 3.16 (Pomerance i Ryan [51], 2007)**.** *Zachodzi nierówność* $B_n < n^{2^k + 3^k/2}$.

W rzeczywistości udowodnili oni bardziej ogólne oszacowanie, prawdziwe dla dowolnego n, którego konsekwencją jest fakt, że

$$\log\log B_n < (\log 3 + o(1)) \log n / \log\log n.$$

W tej samej pracy autorzy udowodnili, że stałej $\log 3$ nie można zmniejszyć. Twierdzenie 3.16 potrafimy wzmocnić dla n będących iloczynem k różnych liczb pierwszych.

Twierdzenie 3.17. *Zachodzi nierówność* $(B_n / n^{(3^k-1)/(2k)-1})^{3^{-k}} < C + o_k(1)$.

Dowód. Wielomiany cyklotomiczne są nierozkładalne nad $\mathbb{Z}$, więc na mocy faktu 2 każdy dzielnik $x^n - 1$ jest postaci $\prod_{d\in D} \Phi_d(x)$, gdzie D jest podzbiorem zbioru dzielników n. Wobec tego

$$B_n \leqslant A_n \prod_{d|n,\, d<n} S_d \leqslant \frac{2}{n} \prod_{d|n} dA_d \leqslant \frac{2}{n} \left(\prod_{d|n} d\right) \left(\prod_{d|n} \varepsilon_{\omega(d)}\right) \left(\prod_{d|n} M_d\right),$$

Gdzie $\omega(d)$ jest liczbą dzielników pierwszych d. Łatwo sprawdzić, że

$$\frac{1}{n} \prod_{d|n} d = n^{2^{k-1}-1},$$

$$\prod_{d|n} M_n(d) \leqslant \prod_{\omega=1}^{k} \left(\left((\sqrt[k]{n})^{\omega} \right)^{2^{\omega-1}/\omega - 1} \right)^{\binom{k}{\omega}} = n^{\frac{1}{k}\sum_{\omega=1}^{k} \binom{k}{\omega}(2^{\omega-1}-\omega)} = n^{(3^k-1)/(2k) - 2^{k-1}}.$$

Niech $\xi_\omega = \max\{2^{-\omega} \log \varepsilon_\omega - \log C, 0\}$. Wtedy

$$\log \left(2 \prod_{d|n} \varepsilon_{\omega(d)} \right) = (1 + o_k(1)) \sum_{\omega=0}^{k} \binom{k}{\omega} \log \varepsilon_\omega \leqslant 3^k \log C + \sum_{\omega=0}^{k} \binom{k}{\omega} 2^\omega \xi_\omega.$$

Pozostaje do udowodnienia, że wartość ostatniej sumy wynosi $o(3^k)$. Niech $\xi'_\omega = \sup\{\xi_\omega, \xi_{\omega+1}, \ldots\}$. Na mocy twierdzenia 13, dla $\omega \to \infty$ mamy $\xi_\omega \to 0$ i w takim razie również $\xi'_\omega \to 0$. Zatem

$$\sum_{\omega=0}^{k} \binom{k}{\omega} 2^\omega \xi_\omega \leqslant \xi'_0 \sum_{\omega=0}^{\lfloor \log k \rfloor} \binom{k}{\omega} 2^\omega + \xi'_{\lceil \log k \rceil} \sum_{\omega=0}^{k} \binom{k}{\omega} 2^\omega = O(2^{\log k} e^{\log^2 k} \log k) + o(3^k) = o(3^k),$$

co kończy dowód. □

Na koniec udowodnimy następujące przypuszczenie.

Hipoteza 3.18 (Bateman, Pomerance i Vaughan [14], 1981)**.** *Zachodzi nierówność*

$$A_n \leqslant \varphi(n)^{k^{-1}2^{k-1}-1},$$

gdzie k jest liczbą dzielników pierwszych n.

Podany przez nas dowód nie korzysta z twierdzenia 13, wystarczy bowiem oszacowanie $A_n < M_n$, uzyskane przez autorów powyższej hipotezy.

Dowód. Wykażemy, że $M_n \leqslant \varphi(n)^{k^{-1}2^{k-1}-1}$. Jest to prawda dla $k = 1, 2$, ponieważ $M_1 = M_2 = 1$. Przeprowadzimy dowód przez indukcję ze względu na k.

Niech $p_1 < \ldots < p_k$. Wtedy dla $k \geqslant 3$ zachodzą nierówności

$$\begin{aligned} M_n &\leqslant p_1^{2^{k-2}-1} \cdot \varphi(p_2 \ldots p_k)^{2^{k-2}/(k-1)-1} \\ &= \left(\frac{p_1}{p_1-1}\right)^{\frac{2^{k-1}}{k}-1} \cdot \left(\frac{p_1^{k-1}}{\varphi(p_2 \ldots p_k)}\right)^{\frac{2^{k-2}}{k-1}-\frac{2^{k-1}}{k(k-1)}} \cdot (\varphi(p_1 \ldots p_k))^{\frac{2^{k-1}}{k}-1} \\ &\leqslant \left(\frac{p_1}{p_1-1}\right)^{\frac{2^{k-1}}{k}-1} \cdot \left(\frac{p_1}{p_1+1}\right)^{2^{k-2}-\frac{2^{k-1}}{k}} \cdot (\varphi(p_1 \ldots p_k))^{\frac{2^{k-1}}{k}-1}. \end{aligned}$$

Ponieważ

$$\left(\frac{p_1}{p_1-1}\right)\left(\frac{p_1}{p_1+1}\right)^2 < 1 \quad \text{oraz} \quad \frac{2^{k-2}-\frac{2^{k-1}}{k}}{\frac{2^{k-1}}{k}-1} \geqslant 2 \quad \text{dla } k \geqslant 3,$$

dowód hipotezy jest zakończony. □

3.3. Wielomiany włączania-wyłączania

Oszacowanie z twierdzenia 13 oraz wynik, który przedstawimy w niniejszym podrozdziale, upoważaniają do postawienia następującej hipotezy.

Hipoteza 3.19. *Istnieje takie $c > 0$, że dla każdego $k \geqslant 1$, dla dowolnie dużych N znajdziemy liczby pierwsze $p_1, \ldots, p_k > N$, spełniające warunek*

$$(A_{p_1 \ldots p_k}/M_{p_1 \ldots p_k})^{2^{-k}} > c + o_k(1).$$

Potrafimy udowodnić tę hipotezę dla wielomianów włączania-wyłączania, zdefiniowanych przez Bachmana [5]. Jest to klasa nieznacznie uogólniająca wielomiany cyklotomiczne.

Definicja 3.20. Wielomianem włączania-wyłączania nazywamy wielomian postaci

$$Q_{\{q_1,q_2,\ldots,q_k\}} = \frac{(1-x^m) \cdot \prod_{1 \leqslant j_1 < j_2 \leqslant k}(1-x^{m/(q_{j_1}q_{j_2})}) \cdot \ldots}{\prod_{1 \leqslant j_1 \leqslant k}(1-x^{m/q_{j_1}}) \cdot \prod_{1 \leqslant j_1 < j_2 < j_3 \leqslant k}(1-x^{m/(q_{j_1}q_{j_2}q_{j_3})}) \cdot \ldots},$$

gdzie $m = q_1 q_2 \ldots q_k$ oraz liczby $q_1, q_2, \ldots, q_k$ są parami względnie pierwsze.

W przypadku gdy $q_1, q_2, \ldots, q_k$ są liczbami pierwszymi, zachodzi równość $\Phi_{q_1 q_2 \ldots q_k} = Q_{\{q_1,q_2,\ldots,q_k\}}$.

Ze względu na podobieństwo powyższej definicji oraz ostatniej równości z faktu 2, wielomiany włączania-wyłączania posiadają dużo cech wielomianów cyklotomicznych. Dla przykładu, jeśli q jest liczbą względnie pierwszą z każdym elementem zbioru ρ, to

$$Q_{\rho \cup \{q\}} = \frac{Q_\rho(x^q)}{Q_\rho(x)},$$

co wynika bezpośrednio z definicji wielomianu Q_ρ. Jest to własność analogiczna do $\Phi_{np}(x) = \Phi_n(x^p)/\Phi_n(x)$ dla $p \nmid n$. We wszystkich oszacowaniach w rozdziale 3 korzystaliśmy tylko z powyższego wzoru, natomiast nie wykorzystaliśmy nigdzie faktu, że $p_1, p_2, \ldots, p_k$ są pierwsze.

Dla uproszczenia zapisu przyjmijmy $\rho = \{q_1, q_2, \ldots, q_k\}$, $m = q_1 q_2 \ldots q_k$ oraz $q_1 < q_2 < \ldots < q_k$. Niech także

$$A_\rho = H(Q_\rho) \quad \text{i} \quad M_\rho = \prod_{j=1}^{k-2} q_j^{2^{k-j-1}-1}.$$

Na mocy powyższych rozważań zachodzi następujące twierdzenie.

Twierdzenie 3.21. *Dla C takiego jak w twierdzeniu 13 mamy*

$$(A_\rho/M_\rho)^{2^{-k}} < C + o_k(1).$$

Poniżej udowadniamy obustronną wersję powyższego twierdzenia dla wielomianów włączania-wyłączania.

Twierdzenie 3.22. *Granica*

$$\hat{c} = \lim_{k\to\infty} \lim_{N\to\infty} \sup_{q_1>N} (A_\rho/M_\rho)^{2^{-k}}$$

istnieje i jest dodatnia.

Dowód. Istnienie oraz fakt, że $\hat{c} \leqslant C < 0.9627$ wynika z twierdzenia 3.21. Pozostaje wskazać dla każdego k zbiory $\rho = \{q_1, q_2, \ldots, q_k\}$ o elementach większych od dowolnego N całkowitego dodatniego, spełniające warunek $(A_\rho/M_\rho)^{2^{-k}} > c + o_k(1)$, gdzie c jest pewną dodatnią stałą.

Bateman, Pomerance i Vaughan ([14], lemat 5, str. 188) udowodnili, że jeśli $p_1, p_2, \ldots, p_k$ są liczbami pierwszymi, z których każda daje resztę $2r+1$ lub $2r-1$ z dzielenia przez $4r$, to $A_{p_1\ldots p_k} \geqslant (4r/\pi)^{2^{k-1}}/(p_1 \ldots p_k)$. Idea dowodu polegała na znalezieniu liczby zespolonej z o module 1, dla której wartość $|\Phi_{p_1 p_2 \ldots p_k}(z)|$ jest duża oraz wykorzystaniu łatwej do zaobserwowania nierówności, prawdziwej dla dowolnego wielomianu P o stopniu mniejszym niż n:

$$|P(z)| \leqslant W(P) \leqslant nH(P).$$

W dowodzie korzystano jedynie z formuły $\Phi_n(x) = \prod_{d|n}(1-x^d)^{\mu(n/d)}$, zatem wystarcza założenie, że $p_1, \ldots, p_k$ są parami względnie pierwsze i możemy rozpatrywać wielomiany włączania-wyłączania.

Niech $r = Nk!$ oraz $q_j = (4j-2)r+1$ dla $j = 1, 2, \ldots, k$. Stosując algorytm Euklidesa, przekonujemy się, że

$$(q_{j_1}, q_{j_2}) = \Big((4j_1-2)r+1, (4j_2-2)r+1\Big) = \Big(4(j_1-j_2)r, (4j_2-2)r+1\Big) = 1,$$

gdyż $4(j_1-j_2)r$ posiada wyłącznie dzielniki pierwsze mniejsze od k lub dzielące N, a $(4j_2-2)r+1$ takowych nie ma. Wykorzystując wspomniany wcześniej wynik, otrzymujemy

$$\begin{aligned}(A_\rho/M_\rho)^{2^{-k}} &> \frac{2}{\sqrt{\pi}} \left(\frac{r^{2^{k-1}}/m}{\prod_{j=1}^{k-2} q_j^{2^{k-j-1}-1}} \right)^{2^{-k}} = \frac{2}{\sqrt{\pi}} \left(\frac{r^{2^{k-1}}/q_k}{\prod_{j=1}^{k-1} q_j^{2^{k-j-1}}} \right)^{2^{-k}} \\ &= \frac{2}{\sqrt{\pi}} \left(\frac{r}{q_k} \prod_{j=1}^{k-1} \left(\frac{r}{q_j} \right)^{2^{k-j-1}} \right)^{2^{-k}} = \frac{2}{\sqrt{\pi}} \prod_{j=1}^{\infty} (4j-2)^{-2^{-j-1}} + o_k(1),\end{aligned}$$

co kończy dowód, gdyż ostatni iloczyn jest zbieżny. Obliczenia wykonane przez komputer wskazują, że jego wartość przemnożona przez $2/\sqrt{\pi}$ nieznacznie przewyższa 0.5495. Wobec tego zachodzi nierówność $c > 0.5495$ i ostatecznie $c \leqslant \hat{c} \leqslant C$. □

Różnice pomiędzy wielomianami cyklotomicznymi a wielomianami włączania-wyłączania mogą wynikać z bardzo subtelnych własności liczb pierwszych. Jest to ciekawy temat do dalszych badań.

Bibliografia

[1] G.Bachman, *On the coefficients of cyclotomic polynomials*, Mem. Amer. Math. Soc. **510** (1993).

[2] G.Bachman, *On the coefficients of ternary cyclotomic polynomials*, J. Number Theory **100** (2003), 104–116.

[3] G.Bachman, *Ternary cyclotomic polynomials with an optimally large set of coefficients*, Proc. Amer. Math. Soc. **132** (2004), 1943–1950.

[4] G.Bachman, *Flat cyclotomic polynomials of order three*, Bull. London Math. Soc. **38** (2006), 53–60.

[5] G.Bachman, *On ternary inclusion – exclusion polynomials*, Integers **10** (2010), 623–638.

[6] G.Bachman, P.Moree *On a class of ternary inclusion – exclusion polynomials*, ArXiv:1006.0522.

[7] A.S.Bang, *Om Ligningen* $\Phi_n(x) = 0$, Nyt Tidsskr. for Math., Afdeling B, **6** (1895), 6–12.

[8] M.Beiter, *Coefficients in the cyclotomic polynomial for numbers with at most three distinct odd primes in their factorization*, The catolic university of America Press, Washington (1960).

[9] M.Beiter, *The midterm coefficient of the cyclotomic polynomial* $F_{pq}(X)$, Amer. Math. Monthly **71** (1964), 769–770.

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

[11] M.Beiter, *Magnitude of the coefficients of the cyclotomic polynomial* F_{pqr}, II, Duke Math. J. **38** (1971), 591–594.

[12] M.Beiter, *Coefficients of the cyclotomic polynomial* $F_{3qr}(x)$, Fibonacci Quart., **16** (1978), 302–306.

[13] P.T.Bateman, *Note on the coefficients of cyclotomic polynomial*, Bull. Amer. Math. Soc., **55** (1949), 1180–1181.

[14] P.T. Bateman, C. Pomerance, R.C. Vaughan, *On the size of the coefficients of cyclotomic polynomials*, Coll. Math. Soc. J. Bolyai **34** (1981), 171–202.

[15] D.M.Bloom, *On the coefficients of the cyclotomic polynomials*, Amer. Math. Monthly **75** (1968), 370—372.

[16] B.Bzdęga, *Bounds on ternary cyclotomic coefficients*, Acta Arith., **144** (2010), 5–16.

[17] B.Bzdęga, *O wielomianach cyklotomicznych*, Praca Magisterska, Uniwersytet im. Adama Mickiewicza, Poznań, 2010.

[18] B.Bzdęga, *Sparse binary cyclotomic polynomials*, J. Number Theory **132** (2012), 410–413.

[19] B.Bzdęga, *On the height of cyclotomic polynomials*, Acta Arith. **152** (2012), 349–359.

[20] B.Bzdęga, *Inclusion-exclusion polynomials with large coefficients* (3str.), arXiv:1202.0257[math.NT], preprint (2012).

[21] B.Bzdęga, *Jumps of ternary cyclotomic coefficients* (10str.), preprint (2012).

[22] L.Carlitz, *The number of terms in the cyclotomic polynomial* $F_{pq}(x)$, Amer. Math. Monthly **73** (1966), 979–981.

[23] A.Decker, P.Moree *Coefficients convexity of divisors of* x^n-1, ArXiv:1010.3938.

[24] P.Erdös, *On the coefficients of the cyclotomic polynomials*, Bull. Amer. Math. Soc. **52** (1946), 179–181.

[25] P.Erdös, *On the coefficients of the cyclotomic polynomials*, Portugal. Math. **8** (1949), 63–71.

[26] P.Erdös, *On the coefficients of the cyclotomic polynomials*, Comment. Math. Univ. St. Pauli, **23** (1974/75), 121–126.

[27] P.Erdös, *On the growth of the cyclotomic polynomial in the interval* $(0,1)$, Proc. Glassgow Math. Assoc. **3** (1957), 102–104.

[28] P.Erdös, R.C.Vaughan, *Bounds for the* $r-th$ *coefficients of cyclotomic polynomials*, J. London Math. Soc. **8** (1974), 393–401.

[29] V.Flesh, E.Schmidt, *Über Perioden in den Koeffizienten der Kreisteilungspolynome* $F_{np}(x)$, Math. Z. **106** (1968), 267–272.

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

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

[32] Y.Gallot, P.Moree, R.Wilms, *The family of ternary cyclotomic polynomials with one free prime*, ArXiv:1110.4590[math.NT], preprint.

[33] A.Hildebrand, *On a conjecture of Balog*, Proc. Amer. Math. Soc. **95** (1985), 517–523.

[34] J.Justin, *Bornes des coefficients du polynôme cyclotomique et de cetains autres polynômes*, C.R. Acad. Sci. Paris **268** (1969), 995–997.

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

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

[37] N.Kaplan, *Flat cyclotomic polynomial of order four and higher*, Integers **10** (2010), 357–363.

[38] S.Konyagin, H.Maier, E.Wirsing, *Cyclotomic polynomials with many primes dividing their orders*, Periodica Math. Hungar. **49** (2004), 99–106.

[39] H.W.Lenstra, *Vanishing sums of roots of unity*, Proceedings, Bicentennial Congress Wiskundig Genootschap, Vrije Univ., Amsterdam (1978), Part II (1979), 249–268.

[40] H.Maier, *The coefficients of cyclotomic polynomials*, Analytic number theory, Proceedings of a conference in honor of Paul Bateman (ed. by B.C. Berndt, H.G. Diamond, H. Halberstam and A.J. Hildebrand), 1990, 349–366.

[41] H.Maier, *Cyclotomic polynomials with large coefficients*, Acta Arith. **64** (1993), 227–235.

[42] H.Maier, *The size of the coefficients of cyclotomic polynomials*, Analytic number theory, Proceedings of a conference in honor of Heini Halberstam (ed. by .C. Berndt, H.G. Diamond, and A.J. Hildebrand) Vol. 2, 1996, 633–639.

[43] H.Meier, *Cyclotomic polynomials whose orders contain many prime factors*, Periodica Math. Hungar. **43** (2001), 155–164.

[44] H.Maier, *Anatomy of integers and cyclotomic polynomials*, CRM Proc. and Lecture Notes **46** (2008), 89–95.

[45] A.Migotti, *Aur Theorie der Kreisteilungsgleichung*, Z. B. der Math.-Naturwiss, Classe der Kaiserlichen Akademie der Wissenschaften, Wien, **87** (1883), 7–14.

[46] H.Möller, *Über die $i-$ten Koeffizienten der Kreisteilungspolynome*, Math. Ann. **188** (1970), 26–38.

[47] H.Möller, *Über die Koeffizienten des $n-$ten Kreisteilungspolynome*, Math. Z. **119** (1971), 33–40.

[48] H.L.Montgomery, R.C.Vaughan, *The order of magnitude of the mth coefficients of cyclotomic polynomials*, Glasgow Math. J. **27** (1985) 143–159.

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

[50] P.Moree, E.Rosu, *Non-Beiter cyclotomic polynomials with an optimally large set of coefficients*, ArXiv:1111.6800[Math.NT], preprint.

[51] C.Pomerance, N.C.Ryan, *Maximal height of divisors of $x^n - 1$*, Illinois J. Math. **51** (2007), 597–604.

[52] E.Sperner, *Ein Satz über Untermengen einer endlichen Menge*, Mathematische Zeitschrift **27** (1928), 544–548.

[53] R.C.Vaughan, *Bounds for the coefficients of cyclotomic polynomials*, Michigan Math. J. **21** (1975), 289–295.