Teoria liczb
funkcje zeta, 20-23 marca

Zadanie 1. Niech $p > 3$ będzie liczbą pierwszą i niech liczby całkowite a, b będą takie, że

$$\frac{a}{b} = \sum_{i=1}^{p-1} \frac{1}{i}.$$

Pokaż, że

(a) liczba a jest podzielna przez p,

(b) liczba a jest podzielna przez p^2.

Rozwiązanie.

Zauważmy, że dla każdej liczby całkowitej k z przedziału $\{1, 2, \ldots, p-1\}$ zachodzi $\frac{1}{k} + \frac{1}{p-k} = \frac{p}{k(p-k)}$. Zatem sumę z zadania możemy zapisać

$$\sum_{k=1}^{p-1} \frac{1}{k} = \frac{1}{2} \sum_{k=1}^{p-1} \left(\frac{1}{k} + \frac{1}{p-k} \right) = p \cdot \frac{1}{2} \sum_{k=1}^{p-1} \frac{1}{k(p-k)}.$$

Sumę po prawej stronie możemy przepisać jako

$$p \cdot \frac{1}{2} \frac{1}{(p-1)!} \sum_{k=1}^{p-1} \frac{(p-1)!}{k(p-k)},$$

zatem jest ona postaci $\frac{p\ell}{2\cdot(p-1)!}$, gdzie $\ell = \sum_{k=1}^{p-1} \frac{(p-1)!}{k(p-k)}$ jest liczbą całkowitą. Stąd liczba a z zadania jest podzielna przez p. By pokazać, że liczba a jest podzielna przez p^2, należy wykazać, że podzielna przez p jest liczba

$$\ell = \sum_{k=1}^{p-1} \frac{(p-1)!}{k(p-k)} .$$

Redukujemy modulo p i otrzymujemy

$$\sum_{k=1}^{p-1} \frac{(p-1)!}{k(p-k)} \equiv (p-1)! \cdot \sum_{k=1}^{p-1} \frac{1}{k(-k)} = -(p-1)! \sum_{k=1}^{p-1} \frac{1}{k^2} \pmod{p}.$$

Pozostaje wykazać, że $\sum_{k=1}^{p-1} \frac{1}{k^2} \mod p$ jest równa zero (w tej sumie de facto wszystkie elementy są $\mod p$, w szczególności np. $\frac{1}{k^2}$ oznacza odwrotność liczby $k^2 \mod p$. Na przykład $\frac{1}{4} \mod 7$ wynosi $2 \mod 7$, bo $2 \cdot 4 \equiv 1 \pmod{7}$).

Argument jest podobny do zadania 7 z pierwszej serii zadań. Niech g będzie generatorem $\mathbb{Z}_p^*$, wtedy zbiór $\{1 \mod p, 2 \mod p, \ldots, p-1 \mod p\}$ jest równy zbiorowi $\{g \mod p, g^2 \mod p, \ldots, g^{p-1} \mod p\}$. Wynika stąd, że

$$\sum_{k=1}^{p-1} \frac{1}{k^2} \equiv \sum_{a=1}^{p-1} \frac{1}{g^{2a}} \pmod{p}$$

Z własności generatora wypisanej powyżej wynika, że najmniejszą liczbą całkowitą dodatnią taką, że $g^a \equiv 1 \pmod p$ jest $a = p-1$. Skoro $p > 3$, to $g^2 - 1 \not\equiv 0 \pmod p$. Ma więc sens element $\frac{1}{1-g^2} \mod p$ i możemy zapisać „wzór na sumę ciągu geometrycznego":

$$\sum_{a=1}^{p-1} \frac{1}{g^{2a}} \equiv \frac{1}{1-g^2} \cdot (1-g^2) \cdot \left(\sum_{a=1}^{p-1} \frac{1}{g^{2a}} \right) = \frac{1}{1-g^2} \left(\sum_{a=1}^{p-1} \frac{1}{g^{2a}} - \sum_{a=0}^{p-2} \frac{1}{g^{2a}} \right) = \frac{1}{1-g^2} \left(\frac{1}{g^{2(p-1)}} - 1 \right) \pmod p.$$

Z małego twierdzenia Fermata wynika, że $g^{p-1} \equiv 1 \pmod p$. Zatem $g^{2(p-1)} \equiv 1$, a stąd $\frac{1}{g^{2(p-1)}} - 1 \equiv \frac{1}{1} - 1 = 0 \pmod p$. To pokazuje, że suma $\sum_{k=1}^{p-1} \frac{1}{k^2}$ przystaje do zera modulo p, co kończy dowód.

Zadanie 2. Niech $\zeta^*(s) = \sum_{n \geq 1, 2 \nmid n} n^{-s}$ dla $s \in \mathbb{R}$, $s > 1$.

(a) Oblicz granicę $\lim_{s \to 1^+} \frac{\ln \zeta^*(s)}{-\ln(s-1)}$.

(b) Określamy funkcję $R(s)$ dla $s \in \mathbb{R}$, $s > 1$ poprzez

$$\ln \zeta^*(s) = \sum_{p \in \mathbb{P}, p \neq 2} p^{-s} + R(s)$$

Pokaż, że $R(s)$ jest ograniczona przy $s \to 1^+$.

Wskazówka: imituj dowody dla $\zeta(s)$ z wykładu lub wykorzystaj udowodnione tam zależności pomiędzy ζ i ζ^*.

Rozwiązanie.

Szereg $\zeta^*(s)$ jest zbieżny bezwzględnie dla $s > 1$. Zauważmy, że

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \sum_{n \geq 1, 2 \nmid n} n^{-s} + 2^{-s} \sum_{n \geq 1} n^{-s} = \zeta^*(s) + 2^{-s}\zeta(s),$$

zatem $\zeta^*(s) = (1 - 2^{-s})\,\zeta(s)$. Przejdźmy do rozwiązania zadania.
(a). Na wykładzie pokazaliśmy, że $\lim_{s \to 1^+} \frac{\ln \zeta(s)}{-\ln(s-1)} = 1$. Ponadto $\lim_{s \to 1^+} 1 - 2^{-s} = \frac{1}{2}$, zaś $\lim_{s \to 1^+} -\ln(s-1) = \infty$. Łącznie mamy

$$\lim_{s \to 1^+} \frac{\ln \zeta^*(s)}{-\ln(s-1)} = \lim_{s \to 1^+} \frac{\ln \zeta(s) + \ln(1-2^{-s})}{-\ln(s-1)} = \lim_{s \to 1^+} \frac{\ln \zeta(s)}{-\ln(s-1)} + \lim_{s \to 1^+} \frac{\ln(1-2^{-s})}{-\ln(s-1)} = 1 + 0 = 1.$$

(b). Na wykładzie pokazaliśmy, że

$$\ln \zeta(s) = \sum_{p \in \mathbb{P}} p^{-s} + R'(s),$$

gdzie $R'(s)$ jest ograniczone przez $s \to 1^+$. Pozostaje zapisać, że $\ln \zeta(s) = \ln \zeta^*(s) - \ln(1-2^{-s})$ i zauważyć, że $\ln(1-2^{-s})$ jest ograniczony przy $s \to 1^+$.

Zadanie 3. Niech $L(s, \chi) = \sum_{n \geq 1} \chi(n) n^{-s}$, gdzie $s \in \mathbb{R}$, $s > 1$ oraz

$$\chi(n) = \begin{cases} 0 & \text{gdy } n \equiv 0, 2 \pmod 4 \\ 1 & \text{gdy } n \equiv 1 \pmod 4 \\ -1 & \text{gdy } n \equiv -1 \pmod 4. \end{cases}$$

(a) Pokaż, że $1 - \frac{1}{3} < L(s, \chi) < 1$.

(b) Pokaż, że $L(s, \chi) = \prod_{p \in \mathbb{P}} \frac{1}{1-\chi(p)p^{-s}}$.

(c) Określamy funkcję $R'(s)$ dla $s \in \mathbb{R}$, $s > 1$ poprzez

$$\ln L(s, \chi) = \sum_{p \in \mathbb{P}, p \neq 2} \chi(p)p^{-s} + R'(s)$$

Pokaż, że $R'(s)$ jest ograniczona przy $s \to 1^+$.

Rozwiązanie.
(a). Dla $s > 1$ szereg $L(s, \chi)$ jest zbieżny bezwzględnie, więc możemy dokonywać różnorakich grupowań. Zauważmy, że

$$L(s, \chi) = 1 - \frac{1}{3^s} + \left(\frac{1}{5^s} - \frac{1}{7^s}\right) + \left(\frac{1}{9^s} - \frac{1}{11^s}\right) + \ldots > 1 - \frac{1}{3^s} > 1 - \frac{1}{3}.$$

Podobnie, grupowanie przesunięte o jeden wyraz daje

$$L(s, \chi) = 1 - \left(\frac{1}{3^s} - \frac{1}{5^s}\right) - \left(\frac{1}{7^s} - \frac{1}{9^s}\right) - \ldots < 1.$$

(b). Zauważmy, że dla każdych całkowitych n_1, n_2 zachodzi $\chi(n_1 n_2) = \chi(n_1)\chi(n_2)$. Dalej argumentujemy podobnie jak na wykładzie. Niech $p_1, \ldots, p_n$ będą n najmniejszymi liczbami pierwszymi. Wtedy

$$\prod_{i=1}^{n} \frac{1}{1 - \chi(p)p^{-s}} = \prod_{i=1}^{n} \sum_{m \geq 0} \chi(p^m)p^{-sm} = \sum_{n \in \mathcal{F}} \chi(n)n^{-s},$$

gdzie $\mathcal{F}$ jest zbiorem liczb całkowitych dodatnich, w których w rozkładzie na czynniki pierwsze występują tylko liczby $p_1, \ldots, p_n$. W szczególności, $\{1, 2, \ldots, p_n\} \subseteq \mathcal{F}$. Wynika stąd, że przy $n \to \infty$, prawa strona równania zbiega do $L(s, \chi)$, zaś lewa strona do $\prod_{p \in \mathbb{P}} \frac{1}{1-\chi(p)p^{-s}}$. To kończy dowód.
(c). Rozwiązanie tego podpunktu opiera się na analogicznym argumencie z wykładu dla $\zeta(s)$. Mianowicie, mamy

$$\ln L(s, \chi) = \sum_{p \in \mathbb{P}} - \ln\left(1 - \chi(p)p^{-s}\right),$$

szereg jest zbieżny bezwzględnie (bo $s > 1$). Wartość bezwzględna $\chi(p)p^{-s}$ to mniej niż jeden, zatem $\ln(1 - \chi(p)p^{-s}) = \sum_{m=1}^{\infty} (\chi(p))^m (-1)^m \frac{p^{-sm}}{m} = \sum_{m=1}^{\infty} \chi(p^m) \cdot (-1)^m \frac{p^{-sm}}{m}$. Wynika stąd, że

$$\ln L(s, \chi) = \sum_{p \in \mathbb{P}} \sum_{m=1}^{\infty} \chi(p^m) \cdot (-1)^{m+1} \frac{p^{-sm}}{m} = \sum_{p \in \mathbb{P}} \chi(p)p^{-s} + \sum_{p \in \mathbb{P}} \sum_{m=2}^{\infty} \chi(p^m) \cdot (-1)^{m+1} \frac{p^{-sm}}{m}.$$

Szereg $\sum_{p \in \mathbb{P}} \sum_{m=2}^{\infty} \chi(p^m) \cdot (-1)^{m+1} \frac{p^{-sm}}{m}$ jest ograniczony przy $s \to 1^+$, bowiem na wykładzie pokazaliśmy, że ograniczony przy $s \to 1^+$ jest nawet szereg $\sum_{p \in \mathbb{P}} \sum_{m=2}^{\infty} \frac{p^{-sm}}{m}$, którego wyrazy są dodatnie i niemniejsze od wyrazów naszego szeregu. Możemy więc położyć $R'(s) =$

$\sum_{p\in\mathbb{P}}\sum_{m=2}^{\infty}\chi(p^m)\cdot(-1)^{m+1}\frac{p^{-sm}}{m}$. Wreszcie, $\chi(2)=0$, więc sumę $\sum_{p\in\mathbb{P}}\chi(p)p^{-s}$ można obciąć do nieparzystych liczb pierwszych.

Zadanie 4. (a) Pokaż, że $\lim_{s\to 1^+}\frac{\ln\zeta^*(s)\pm\ln L(s,\chi)}{-\ln(s-1)}=1$.

(b) Pokaż, że gęstość Dirichleta zbioru liczb pierwszych p takich, że $p\equiv 1 \pmod 4$ to $1/2$. Pokaż to samo dla $p\equiv 3 \pmod 4$. Zatem oba zbiory są nieskończone.

Rozwiązanie.
(a). Z zadania 2(a) wiemy, że $\lim_{s\to 1^+}\frac{\ln\zeta^*(s)}{-\ln(s-1)}=1$, zaś z zadania 3(a) wiemy, że $\ln(1-1/3)<\ln L(s,\chi)<0$, więc $\lim_{s\to 1^+}\frac{\ln L(s,\chi)}{-\ln(s-1)}=0$. To daje granice z punktu (a).
(b). Z zadań 2(b) i 3(b) wynika, że mamy

$$\ln\zeta^*(s)+\ln L(s,\chi)=\sum_{p\in\mathbb{P},p\neq 2}(1+\chi(p))\,p^{-s}+R(s)+R'(s).$$

Zauważmy, że $1+\chi(p)=2$, jeśli $p\equiv 1 \pmod 4$ oraz $1+\chi(p)=0$, jeśli $p\equiv 3 \pmod 4$. Wynika stąd, że

$$\ln\zeta^*(s)+\ln L(s,\chi)=2\sum_{p\in\mathbb{P},p\equiv 1 \pmod 4}p^{-s}+R(s)+R'(s).$$

Wstawiając to do definicji gęstości Dirichleta, otrzymujemy

$$d(\{p\in\mathbb{P}\mid p\equiv 1 \pmod 4\}=\lim_{s\to 1^+}\frac{\frac{1}{2}\cdot(\ln\zeta^*(s)+\ln L(s,\chi)-R(s)-R'(s))}{-\ln(s-1)}=\frac{1}{2}.$$

Gęstość zbioru $\{p\in\mathbb{P}\mid p\equiv 3 \pmod 4\}$ obliczamy analogicznie, biorąc $\ln\zeta^*(s)-\ln L(s,\chi)$ i zauważając, że $1-\chi(p)=0$ jeśli $p\equiv 1 \pmod 4$, zaś 2 jeśli $p\equiv 3 \pmod 4$. To kończy rozwiązanie.