Теорія чисел - весняний семестр 2023 року
§10. Формула обернення Мебіуса
§11. Скінченні поля

1. Для цілого додатного числа n розгляньте множину дробів $\{\frac{1}{n}, \ldots, \frac{n-1}{n}\}$ записаних у нескоротній формі. Зауважимо, що їхні знаменники є дільниками $d|n$ і маємо

$$\left\{\frac{1}{n}, \ldots, \frac{n-1}{n}\right\} = \underset{d|n}{\cup} \left\{\frac{a}{d} : 1 \leq a \leq d, (a,d) = 1\right\}.$$

   Зокрема, функція Ейлера $\phi(n) = \#\{1 \leq a \leq n : (a,n) = 1\}$ задовольняє рівності $n = \sum_{d|n} \phi(d)$. Застосуйте формулу обернення Мебіуса щоби обчислити вираз $\phi(n)$ якщо $n = p_1^{e_1} \ldots p_m^{e_m}$ є розкладом n на прості множники.

2. Позначимо $\mathbb{N} = \mathbb{Z}_{\geq 1}$. Функцію $f : \mathbb{N} \to \mathbb{C}$ назвемо мультиплікативною якщо з $(m,n) = 1$ випливає $f(mn) = f(n)f(n)$.

   i) Якщо $f(n)$ є мультиплікативною функцією, покажіть що $g(n) = \sum_{d|n} f(d)$ також буде мультиплікативною.

   ii) Покажіть, що функція Мебіуса $\mu(n)$ є мультиплікативною. Скористайтеся (i) щоби показати, що функція Ейлера є мультиплікативною. (На лекціях ми вивели цей факт з Китайської теореми про лишки.)

3. i) Нехай K це будь-яке поле. Для цілих чисел $1 \leq \ell \leq m$ покажіть, що в $K[x]$ многочлен $x^\ell - 1$ ділить многочлен $x^m - 1$ тоді і тільки тоді коли $\ell|m$.

   ii) Нехай $a > 1$ є цілим числом. Для цілих чисел $1 \leq \ell \leq m$ покажіть, що $a^\ell - 1$ ділить $a^m - 1$ тоді і тільки тоді коли $\ell|m$.

4. Нехай F це поле з p^n елементами. Для $\alpha \in F$ покажіть, що многочлен $f_\alpha(x) = (x-\alpha)(x-\alpha^p)(x-\alpha^{p^2}) \cdots (x-\alpha^{p^{n-1}}) \in F[x]$ має коефіцієнти в $\mathbb{F}_p \subset F$. Зокрема, *слід* $Tr(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \ldots + \alpha^{p^{n-1}}$ та *норма* $N(\alpha) = \alpha \cdot \alpha^p \cdot \alpha^{p^2} \cdot \ldots \cdot \alpha^{p^{n-1}}$ є елементами $\mathbb{F}_p$.

5. Нехай позначення будуть як у попередній вправі. Покажіть, що слід

$$Tr : F \to \mathbb{F}_p$$

   є $\mathbb{F}_p$-лінійним ненульовим функціоналом, тобто:

   i) $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta)$ для всіх $\alpha, \beta \in F$,

   ii) $Tr(a\alpha) = aTr(\alpha)$ для всіх $a \in \mathbb{F}_p, \alpha \in F$,

   iii) існує $\alpha \in F$ таке що $Tr(\alpha) \neq 0$.

Зауважте, що коли $f \in \mathbb{F}_p[x]$ є таким многочленом, що $f(\alpha) = 0$, тоді $f(\alpha^{p^d}) = 0$ для всіх $d \geq 1$. Коли $f(x)$ незвідний і нормований, то степені α^{p^i}, $i = 0, \ldots, \deg(f) - 1$ будуть в точності всіма коренями f і маємо $f_\alpha(x) = f(x)^{n/deg(f)}$. Це показує аналогію між слідом та нормою для алгебраїчних чисел. Порявняйте вправи 4 та 5 відповідно з вправами 3 та 4 завдання 4 (до §5).