## §10. Формула обернення Мебіуса

1. Нехай $n = p_1^{e_1} \dots p_m^{e_m}$. Застосовуючи рівність $n = \sum_{d|n} \varphi(d) \Leftrightarrow id = \varphi \circ 1$, звідси

$$\varphi = \varphi \circ \mathbb{1} = \varphi \circ (1 \circ \mu) = (\varphi \circ 1) \circ \mu = id \circ \mu$$

$$\Leftrightarrow \quad \varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}.$$

Використовуємо означення функції Мебіуса

$$\mu(n) = \begin{cases} 1, & n = 1; \\ 0, & n \text{ не вільне від квадратів}; \\ (-1)^\ell, & n = p_1 \cdot \dots \cdot p_\ell. \end{cases}$$

Маємо:

$$\varphi(n) = \sum_{\substack{d|n \\ k^2 \nmid d \ \forall k>1}} \mu(d) \frac{n}{d} = \sum_{\substack{d|p_2^{e_2} \dots p_m^{e_m} \\ k^2 \nmid d \ \forall k>1}} \Big[ \overbrace{\mu(p_1 d)}^{-\mu(d)} \frac{n}{p_1 d} + \mu(d) \frac{n}{d} \Big] =$$

$$= p_1^{e_1} \varphi(p_2^{e_2} \dots p_m^{e_m}) - p_1^{e_1 - 1} \varphi(p_2^{e_2} \dots p_m^{e_m}) =$$

$$= (p_1^{e_1} - p_1^{e_1 - 1}) \varphi(p_2^{e_2} \dots p_m^{e_m}) = p_1^{e_1} \left(1 - \frac{1}{p_1}\right) \varphi\left(\frac{n}{p_1^{e_1}}\right) =$$

$$= \dots = p_1^{e_1} \left(1 - \frac{1}{p_1}\right) \cdot \dots \cdot p_m^{e_m} \left(1 - \frac{1}{p_m}\right) \varphi(1) = n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right).$$

Відповідь: $\varphi(n) = n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right)$.

2. i) Припустимо, $(m, n) = 1$ та $d | mn$. Доведемо, що $d$ єдиним чином можна представити у вигляді добутку

$d = d_1 d_2$, таким числом, що $d_1 | m$ та $d_2 | n$.

▷ Розкладемо $m$ та $n$ на множники:

$$m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}; \quad n = q_1^{\beta_1} \cdot \ldots \cdot q_e^{\beta_e},$$

при чому серед $\{p_i\}$ та $\{q_j\}$ немає спільних простих чисел, бо $(m, n) = 1$.

$$d | mn \Rightarrow d = p_1^{\gamma_1} \cdot \ldots \cdot p_k^{\gamma_k} \cdot q_1^{\delta_1} \cdot \ldots \cdot q_e^{\gamma_e},$$

при чому $\gamma_i \leq \alpha_i$; $\delta_j \leq \beta_j$. Але тоді

$$d_1 = p_1^{\gamma_1} \cdot \ldots \cdot p_k^{\gamma_k} | m; \quad d_2 = q_1^{\delta_1} \cdot \ldots \cdot q_e^{\delta_e} | n; \quad d_1 d_2 = d$$

– єдині $d_1$ та $d_2$, які задовольняють $d_1 | m$; $d_2 | n$ та $d_1 d_2 = d$, адже $(d_1, n) = (m, d_2) = 1$, тобто $d_1$ та $n$ і $d_2$ та $m$ попарно не мають спільних множників. ◁

Припустимо тепер, що $f(n)$ – мультиплікативна функція, тобто

$$\forall n \in \mathbb{N} \; \forall m \in \mathbb{N} \left( (n, m) = 1 \Rightarrow f(mn) = f(m) f(n) \right).$$

Нехай $g(n) = \sum_{d | n} f(d)$, тоді якщо $(m, n) = 1$ маємо:

$$g(mn) = \sum_{d | mn} f(d) = \sum_{d_1 | m} \sum_{d_2 | n} f(d_1 d_2) =$$

$$= \left[ (d_1, d_2) = 1 \right] = \sum_{d_1 | m} \sum_{d_2 | n} f(d_1) f(d_2) =$$

$$= \left( \sum_{d_1 | m} f(d_1) \right) \left( \sum_{d_2 | n} f(d_2) \right) = g(m) g(n),$$

тобто $g$ — мультиплікативна функція, що й треба було довести. ∎

ii) Покажемо, що функція Мебіуса $\mu$ мультиплікативна. Припустимо, $(m,n)=1$. Якщо хоча б одне з чисел $m$ або $n$ не є вільним від квадратів, то $\mu(mn)=\mu(m)\mu(n)=0$ — рівність $\mu(mn)=\mu(m)\mu(n)$ виконується. Якщо $m$ та $n$ вільні від квадратів, без обмеження загальності, розклавши їх на прості множники,

$$m=p_1\cdots p_k; \qquad n=q_1\cdots q_\ell,$$

при чому $p_i\neq q_j$, адже $(m,n)=1$. Тоді

$$\mu(mn)=(-1)^{k+\ell}=(-1)^k(-1)^\ell=\mu(m)\mu(n).$$

Отже, $\forall m\in\mathbb{N}\ \forall n\in\mathbb{N}\left((m,n)=1\Rightarrow\mu(mn)=\mu(m)\mu(n)\right)$, що й треба було довести.

Користуючись результатом п. (i), маємо: для $(m,n)=1$,

$$\varphi(mn)=\sum_{d\mid mn}\mu(d)\frac{mn}{d}=\sum_{d_1\mid m}\sum_{d_2\mid n}\mu(d_1d_2)\frac{mn}{d_1d_2}=$$

$$=\left[(d_1,d_2)=1\right]=\left(\sum_{d_1\mid m}\mu(d_1)\frac{m}{d_1}\right)\left(\sum_{d_2\mid n}\mu(d_2)\frac{n}{d_2}\right)=$$

$=\varphi(m)\varphi(n)$, тобто $\varphi$ — мультиплікативна функція. ∎

## § 11. Скінченні поля

**3.** Нехай $K$ — довільне поле; $1 \le l \le m$.

i) Доведемо, що многочлен $x^l - 1 \in K[x]$ ділить $x^m - 1 \in K[x]$ тоді і тільки тоді, коли $l \mid m$.

$\Rightarrow$ Нехай $l \mid m$, тобто $m = kl$. Тоді

$$x^m - 1 = (x^l)^k - 1 = (x^l - 1)\left((x^l)^{k-1} + (x^l)^{k-2} + \ldots + 1\right),$$

тобто $x^l - 1 \mid x^m - 1$. ■

$\Leftarrow$ Нехай $x^l - 1 \mid x^m - 1$, $m = ql + r$, $0 \le r < l$. Тоді $x^l - 1 \mid (x^m - 1) - (x^{ql} - 1) = x^m - x^{ql} = x^{ql}(x^r - 1)$. Оскільки $K[x] \in$ ООФ та $(x^l - 1, x) = 1$, то $x^l - 1 \mid x^r - 1$, звідси $r = 0$ (адже інакше $\deg(x^l - 1) > \deg(x^r - 1)$, суперечність). Отже, $m = ql$, тобто $l \mid m$. ■

ii) Якщо $l \mid m$, то $\forall a \in \mathbb{N}$, $a > 1$:

$$a^m - 1 = (a^l - 1)\left((a^l)^{k-1} + (a^l)^{k-2} + \ldots + a^l + 1\right),$$

тобто $a^l - 1 \mid a^m - 1$.

Доведемо, що $a^l - 1 \mid a^m - 1 \Rightarrow l \mid m$.

Нехай $m = ql + r$, $0 \le r < l$. Тоді

$$a^l - 1 \mid (a^m - 1) - (a^{ql} - 1) = a^m - a^{ql} = a^{ql}(a^r - 1).$$

Оскільки $\mathbb{Z} \in$ ООФ та $(a^l - 1, a) = 1$, то $a^l - 1 \mid a^r - 1$. Але $a^l > a^r$, адже $l > r$ та $a > 1$, звідси $a^r - 1 = 0 \Leftrightarrow r = 0$.

Отже, $m = ql$, тобто $l \mid m$. ■