Лекція 4

ФОРМУЛА ВКЛЮЧЕНЬ-ВИКЛЮЧЕНЬ У ТЕОРІЇ ЧИСЕЛ

Нехай $a_1, \dots, a_m$ деякі взаємно прості натуральні числа. Нехай $n \geq 1$ — також натуральне число. Позначимо через $N(i)$ кількість натуральних чисел $k \leq n$, які діляться на a_i (мають властивість ділитися на a_i). Аналогічно, $N(i,j)$, $i \neq j$, — це кількість натуральних чисел $k \leq n$, які діляться на a_i та a_j (мають властивість ділитися на a_i та a_j). Для будь-якого $1 \leq k \leq m$ таким же чином можна означити $N(i_1, \dots, i_k)$ (індекси $i_1, \dots, i_k$ всі різні) як кількість тих натуральних чисел $k \leq n$, які діляться на $a_{i_1}, \dots, a_{i_k}$ (мають властивість ділитися на $a_{i_1}, \dots, a_{i_k}$). Позначимо через M кількість тих натуральних чисел $k \leq n$, які діляться принаймні на одне з чисел $a_1, \dots, a_m$.

Приклад 1. Нехай $m = 2$. З формули (3.6) випливає, що $M = N(1) + N(2) - N(1,2)$. Неважко зрозуміти, що $N(1) = [n/a_1]$, $N(2) = [n/a_2]$, $N(1,2) = [n/a_1a_2]$ ($[x]$ — ціла частина дійчного числа x). Якщо L — це кількість тих натуральних чисел $k \leq n$, які не діляться на жодне з чисел a_1 та a_2, то

$$L = n - \left[\frac{n}{a_1}\right] - \left[\frac{n}{a_2}\right] + \left[\frac{n}{a_1 a_2}\right]. \tag{1}$$

[0]Printed from the file `[discretka_L=03.tex]` on 25.7.2013

Теорема 1. *Нехай $m \geq 3$, а $a_1, \dots, a_m$ — взаємно прості натуральні числа. Позначимо через L кількість тих натуральних чисел $k \leq n$, які не діляться на жодне з чисел $a_1, \dots, a_m$. Тоді*

$$L = n - \left(S_1 - S_2 + \cdots + (-1)^{m-1} S_m\right), \tag{2}$$

де

$$S_1 = \sum_{i=1}^{m} \left[\frac{n}{a_i}\right], \qquad S_m = \left[\frac{n}{a_1 \dots a_m}\right],$$

$$S_k = \sum_{\substack{1 \leq i_1, \dots, i_k \leq n \\ i_1, \dots, i_k \text{ всі різні}}} \left[\frac{n}{a_{i_1} \dots a_{i_k}}\right], \qquad 2 \leq k \leq m-1.$$

Доведення теореми 1. Нехай $C = \{k : k \leq n\}$. Розглянемо властивості $v_i = \{$число $k \in C$ ділиться на $a_i\}$. Тоді $N(i) = [n/a_i]$, $N(i,j) = [n/a_i a_j]$ і так далі. Тому (2) випливає з формули (3.6). $\square$

1. Функція Ойлера

Функція Ойлера $\varphi(a)$ натурального аргументу a означається як кількість натуральних чисел $k \leq a$, які є взаємно простими з a. Для невеликих a значення функції Ойлера легко обчислити: $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$.

Зауваження 1. Якщо p просте число, то $\varphi(p) = p - 1$.

Теорема 2. *Нехай* $a = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ *— канонічне представлення числа* a *через степені простих чисел, причому* $\alpha_1 > 0, \dots, \alpha_m > 0$. *Тоді*

$$\varphi(a) = a\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_m}\right).$$

Доведення теореми 2. Спочатку розглянемо випадок $m = 2$, тобто $a = p_1^{\alpha_1} p_2^{\alpha_2}$ для $\alpha_1 > 0$, $\alpha_2 > 0$. Формула (1) у цьому випадку має вигляд:

$$\begin{aligned}\varphi(a) &= a - \left[\frac{a}{p_1}\right] - \left[\frac{a}{p_1}\right] + \left[\frac{a}{p_1 p_2}\right] \stackrel{?}{=} a - \frac{a}{p_1} - \frac{a}{p_1} + \frac{a}{p_1 p_2} \\ &= a\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right).\end{aligned}$$

У загальному випадку

$$\begin{aligned}&\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_m}\right) \\ &\quad = 1 - \sum_{i=1}^{m} \frac{1}{p_i} + \sum_{\substack{1 \le i,j \le m \\ i \ne j}} \frac{1}{p_i p_j} + \dots + (-1)^m \frac{1}{p_1 \dots p_m}.\end{aligned}$$

Домноживши обидві частини на a, отримуємо твердження теореми. $\square$

2. Мультиплікативнивні функції

Функція f натурального аргументу називається *мультиплікативною*, якщо

(i) існує a_0, для якого $f(a_0) \neq 0$;
(ii) $f(ab) = f(a)f(b)$ для всіх взаємно простих a та b.

Наприклад, функція $f(a) = a^s$ є мультиплікативною для будь-якого s.

Лема 1. *$f(1) = 1$ для будь-якої мультиплікативної функції f.*

Доведення леми 1. Якщо a_0 — це число, для якого $f(a_0) \neq 0$, то на підставі мультиплікативності маємо $f(a_0) = f(1 \cdot a_0) = f(1)f(a_0)$, тобто $f(1) = 1$. $\square$

Лема 2. *Якщо f_1 та f_2 мультиплікативні функції, то $f = f_1 f_2$ також мультиплікативна.*

Теорема 3. *Функція Ойлера є мультиплікативною. Іншими словами, $\varphi(ab) = \varphi(a)\varphi(b)$ для всіх взаємно простих a та b.*

Доведення. Дійсно, $f(1) = f_1(1)f_2(1) = 1$. Крім цього, $f(ab) = f_1(ab)f_2(ab) = f_1(a)f_1(b)f_2(a)f_2(b) = f(a)f(b)$ для взаємно простих чисел a та b. $\square$

Доведення теореми 3. Умова (i) очевидно виконана. Нехай a та b взаємно прості. Запишемо їхні канонічні розклади:

$$a = p_1^{\alpha_1} \dots p_m^{\alpha_m}, \qquad b = q_1^{\beta_1} \dots q_n^{\beta_n}.$$

Зауважимо, що множини $\{p_1, \dots, p_m\}$ та $\{q_1, \dots, q_n\}$ не перетинаються, оскільки a та b взаємно прості. Тому на підставі теореми 2

$$\begin{aligned}\varphi(ab) &= ab\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_m}\right)\left(1-\frac{1}{q_1}\right)\dots\left(1-\frac{1}{q_n}\right)\\ &= a\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_m}\right)\times b\left(1-\frac{1}{q_1}\right)\dots\left(1-\frac{1}{q_n}\right)\\ &= \varphi(a)\varphi(b).\end{aligned}$$

□

Відзначимо одну з важливих властивостей мультиплікативних функцій, що стосується підрахунку суми

$$\sum_{d|a} f(d),$$

яка поширена на всі дільники числа a (включаючи 1 і саме a). Важливими прикладами таких сум є кількість дільників числа a (випадок $f(x) = 1$ для всіх x) та сума дільників числа a (випадок $f(x) = x$ для всіх x).

Теорема 4. *Нехай $a = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ — канонічний розклад числа a. Тоді для будь-якої мультиплікативної функції f*

$$\sum_{d|a} f(d) = \prod_{i=1}^{m} \left\{1 + f(p_i) + \dots + f\left(p_i^{\alpha_i}\right)\right\}. \tag{3}$$

Сума в лівій частині рівності (3) *поширена на всі дільники числа a* (*включаючи* 1 *і саме a*).

Доведення теореми 4. Кожен дільник d числа a має вигляд $p_1^{\beta_1} \dots p_m^{\beta_m}$ для будь-яких $0 \le \beta_1 \le \alpha_1, \dots, 0 \le \beta_m \le \alpha_m$. На підставі мультиплікативності

$$f\left(p_1^{\beta_1} \dots p_m^{\beta_m}\right) \overset{?}{=} f\left(p_1^{\beta_1}\right) \dots f\left(p_m^{\beta_m}\right).$$

Тому

$$\sum_{d|a} f(d) = \sum_{\beta_1=0}^{\alpha_1} \cdots \sum_{\beta_m=0}^{\alpha_m} f\left(p_1^{\beta_1} \dots p_m^{\beta_m}\right)$$
$$\stackrel{?}{=} \sum_{\beta_1=0}^{\alpha_1} \cdots \sum_{\beta_m=0}^{\alpha_m} f\left(p_1^{\beta_1}\right) \dots f\left(p_m^{\beta_m}\right)$$
$$\stackrel{?}{=} \prod_{i=1}^{m} \left\{f(1) + f(p_i) + \cdots + f\left(p_i^{\alpha_i}\right)\right\}.$$

Теорема доведена, оскільки $f(1) = 1$ згідно до леми 1. $\square$

Наслідок 1. $\sum_{d|a} \varphi(d) = a$.

Доведення наслідку 1. Нехай $a = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ — канонічний розклад числа a. Тоді згідно з теоремою 4

$$\sum_{d|a} \varphi(d) = \prod_{i=1}^{m} \left\{\varphi(1) + \varphi(p_i) + \varphi\left(p_i^2\right) + \cdots + \varphi\left(p_i^{\alpha_i}\right)\right\}.$$

Оскільки

$$\varphi\left(p_i^k\right) = p_i^k - p_i^{k-1}, \qquad k \geq 1,$$

то $\varphi(1) + \varphi(p_i) + \varphi\left(p_i^2\right) + \cdots + \varphi\left(p_i^{\alpha_i}\right) = p_i^{\alpha_i}$ і тому

$$\sum_{d|a} \varphi(d) = \prod_{i=1}^{m} p_i^{\alpha_i} = a.$$

$\square$

3. Функція Мебиуса

Функцією Мебіуса називається функція μ натурального аргументу, яка для аргументу $a = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ з $\alpha_1 > 0, \dots, \alpha_m > 0$, визначається наступним чином: $\mu(1) = 1$,

$$\mu(a) = \begin{cases} (-1)^m, & \alpha_1 = \dots = \alpha_m = 1, \\ 0, & \text{в іншому випадку.} \end{cases}$$

Зауважимо, що $\mu(a) = 0$ тоді і тільки тоді, коли a ділиться на квадрат деякого числа.

Лема 3. *Функція Мебіуса є мультиплікативною.*

Доведення. Нехай $a = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ та $b = q_1^{\beta_1} \dots q_n^{\beta_n}$ взаємно прості, тобто множини $\{p_1, \dots, p_m\}$ та $\{q_1, \dots, q_n\}$ не перетинаються. Тому ab ділиться на квадрат простого числа тоді і тільки тоді, коли або a, або b ділиться на квадрат простого числа. В цьому випадку $\mu(ab) = 0$ та $\mu(a)\mu(b) = 0$, тобто $\mu(ab) = \mu(a)\mu(b)$. В іншому випадку $\mu(a) = (-1)^m$, $\mu(b) = (-1)^n$, та $\mu(ab) = (-1)^{m+n}$, тобто $\mu(ab) = \mu(a)\mu(b)$. $\square$

Теорема 5. *Нехай f — деяка мультиплікативна функція. Тоді для $a > 1$, $a = p_1^{\alpha_1} \dots p_m^{\alpha_m}$,*

$$\sum_{d|a} \mu(d) f(d) = (1 - f(p_1)) \dots (1 - f(p_m)).$$

Доведення теореми 5. Покладемо $f_1 = \mu f$. Тоді $f_1(p) \stackrel{?}{=} -f(p)$ та $f_1(p^s) \stackrel{?}{=} 0$ для $s > 1$, якщо p — просте число. З лем 2 та 3 випливає, що f_1 є мультиплікативною функцією. Тепер запишемо (3) для f_1, це і доводить теорему. $\square$

В П Р А В И

Вправа 1. Довести, що $\lim_{a\to\infty}\varphi(a)=\infty$.

Вказівка. Нехай $a=p_1^{\alpha_1}\dots p_m^{\alpha_m}$. Якщо $a>N^{N^2}$, то

$$\max\left\{m,\ \max_{1\le i\le m}\alpha_i,\ \max_{1\le i\le m}p_i\right\}>N.$$

Вправа 2. Обчислити $\sum_{d|1024}\varphi(d)$.

Вправа 3. Позначимо через $S(a)$ суму дільників числа a. Довести, що

$$S(a)=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\dots\frac{p_m^{\alpha_m+1}-1}{p_m-1}.$$

Вказівка. Записати (3) для $f(a)=a$; потім підрахувати суми геометричних прогресій.

Вправа 4. Знайти $S(720)$.

Вправа 5. Позначимо через $\tau(a)$ кількість дільників числа a. Довести, що

$$\tau(a)=(\alpha_1+1)\dots(\alpha_m+1).$$

Вказівка. Записати (3) для $f(a)=1$.

Вправа 6. Знайти $\tau(720)$.

Вправа 7. Довести, що $\sum_{d|a}\mu(d)=0$ для $a>1$.

Вказівка. Застосувати теоерему 5 для $f(a)=1$.

Вправа 8. Довести, що для $a>1$

$$\varphi(a)=a\sum_{d|a}\frac{\mu(d)}{d}.$$

Вказівка. Застосувати теорему 5 для $f(a)=\frac{1}{a}$; скористатись теоремою 2.