УДК 512.547.25

Ю. В. Петечук (Ужгородський національний університет)

ФОРМУЛИ ПОЛІНОМІВ ДІЛЕННЯ КРУГА НАД КІЛЬЦЯМИ

The formulas of polynomials of the division of the circle $\Phi_n(x)$, $n \geq 1$ are studied in the article. Polynomials of the division of the circle are determined by the equality $x^n - 1 = \prod\limits_{d|n} \Phi_d(x)$, $n \geq 1$. The formula of existing of the polynomial of the division of the circle $\Phi_{nm}(x)$ for any natural (not necessarily mutually prime) numbers m and n.

В даній роботі продовжують вивчатися формули поліномів ділення круга $\Phi_n(x)$, $n \geq 1$. Поліноми ділення круга визначаються рівністю $x^n - 1 = \prod\limits_{d|n} \Phi_d(x)$, $n \geq 1$. Знайдено формулу полінома ділення круга $\Phi_{nm}(x)$ для будь-яких натуральних (не обов'язково взаємно простих) чисел m і n.

Поліноми ділення круга визначаються рівністю $x^n - 1 = \prod\limits_{d|n} \Phi_d(x)$, $n \geq 1$ над полем комплексних чисел і за індукцією знаходяться над кільцем цілих чисел за правилом

$$x - 1 = \Phi_1(x), \;\; \Phi_n(x) = \frac{x^n - 1}{\prod\limits_{\substack{d|n \\ d \neq n}} \Phi_d(x)}.$$

Тому $\Phi_n(x)$ є строго унітарними (нормалізованими) многочленами (старші коефіцієнти яких дорівнюють одиниці) над кільцем цілих чисел.

Про окремі властивості поліномів ділення круга можна знайти інформацію в [1–8]. У даній статті досліджуються властивості поліномів ділення круга, які можуть бути використані як в теорії чисел, так і в теорії зображень груп.

1. Функція і перетворення Мьобіуса. Функція θ із множини натуральних чисел N в деяке комутативне кільце з 1 називається мультиплікативною, якщо $\theta(1) = 1$ і $\theta(ab) = \theta(a)\theta(b)$ для будь-яких взаємно простих натуральних чисел a і b.

Значення добутку мультиплікативних функцій задається як добуток значень функцій на множині натуральних чисел. Зрозуміло, що добуток мультиплікативних функцій є мультиплікативною функцією.

Якщо $n = p_1^{n_1} \cdots p_k^{n_k}$, $n > 1$ – канонічний розклад натурального числа n в добуток степенів простих чисел $p_1, \ldots, p_k$ і θ – мультиплікативна функція, то

$$\sum_{d|n} \theta(d) = \left(1 + \theta(p_1) + \cdots + \theta\left(p_1^{n_1}\right)\right) \cdots \left(1 + \theta(p_k) + \cdots + \theta\left(p_k^{n_k}\right)\right).$$

Функція $\mu\colon N \longrightarrow Z$ називається функцією Мьобіуса, якщо $\mu(1)=1$, $\mu(n)=(-1)^k$, якщо n – добуток k простих різних чисел і $\mu(n) = 0$ в решті випадків.

Очевидно, що μ і $\theta\mu$ – мультиплікативні функції. Тому

$$\sum_{d|n} \theta(d)\mu(d) = \left(1 - \theta(p_1)\right) \cdots \left(1 - \theta(p_k)\right).$$

Зокрема, якщо $\theta(n) = 1$ для всіх $n \in N$, то при $n > 1$ має місце рівність $\sum_{d|n} \mu(d) = 0$. Тому

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) = \begin{cases} 0, & n \neq 1, \\ 1, & n = 1. \end{cases}$$

Легко бачити, що якщо d пробігає всі дільники числа n, які діляться на t, то $\frac{d}{t}$ пробігає всі дільники числа $\frac{n}{t}$. Тому

$$\sum_{\frac{d}{t} \mid \frac{n}{t}} \mu\left(\frac{n}{d}\right) = \sum_{\frac{d}{t} \mid \frac{n}{t}} \mu\left(\frac{n}{t} \mid \frac{d}{t} \right) = \begin{cases} 0, & n \neq t, \\ 1, & n = t. \end{cases}$$

Нехай f, g – функції із N в деяке комутативне кільце. Тоді має місце формула мультиплікативного перетворення Мьобіуса

$$g(n) = \prod_{d|n} f(d) \Leftrightarrow f(n) = \prod_{d|n} g(d)^{\mu\left(\frac{n}{d}\right)}.$$

Отже,

$$x^n - 1 = \prod_{d|n} \Phi_(d)(x) \Leftrightarrow \Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu\left(\frac{n}{d}\right)}.$$

Підкреслимо, що рівність, при якій многочлен дорівнює відношенню многочленів у кільці $Z[x]$ означає, що при діленні "кутиком" чисельника на знаменник залишок від ділення дорівнює нулю.

2. Базові формули

Лема 1. *Нехай $n = p^l m$, де p – просте число, $(p, m) = 1$, $l \geq 1$, $m \geq 1$. Тоді $\Phi_n(x) = \frac{\Phi_m\left(x^{p^l}\right)}{\Phi_m\left(x^{p^{l-1}}\right)}$.*

Доведення. За вищедоведеною формулою

$$\Phi_n(x) = \prod_{i=1}^{l} \left(\prod_{d|m} \left(x^{p^i d} - 1\right)^{\mu\left(\frac{n}{p^i d}\right)} \right), \ \Phi_m(x) = \prod_{d|m} \left(\left(x^d - 1\right)^{\mu\left(\frac{m}{d}\right)} \right),$$

де $0 \leq i \leq l$, а d пробігає всі дільники числа m.

Із мультиплікативності функції μ і взаємної простоти чисел p і $\frac{m}{d}$ випливає, що має місце рівність

$$\left(x^{p^i d} - 1\right)^{\mu\left(\frac{n}{p^i d}\right)} = \begin{cases} 1, & 0 \leq i \leq l-2, \\ \left(x^{p^{l-1} d} - 1\right)^{-\mu\left(\frac{m}{d}\right)}, & i = l-1, \\ \left(x^{p^l d} - 1\right)^{\mu\left(\frac{m}{d}\right)}, & i = l. \end{cases}$$

Це означає, що

$$\Phi_n(x) = \prod_{d|m} \frac{\left(x^{p^l d} - 1\right)^{\mu\left(\frac{m}{d}\right)}}{\left(x^{p^{l-1} d} - 1\right)^{\mu\left(\frac{m}{d}\right)}} = \frac{\Phi_m\left(x^{p^l}\right)}{\Phi_m\left(x^{p^{l-1}}\right)}.$$

Якщо $m = 1$, то $\Phi_{p^l}(x) = \frac{x^{p^l}-1}{x^{p^{l-1}}-1}$.

Зокрема, $\Phi_p(x) = \frac{x^p-1}{x-1}$. Тому $\Phi_{p^l}(x) = \Phi_p\left(x^{p^{l-1}}\right)$.

Підкреслимо, що $\Phi_{pn}(x) = \frac{\Phi_n(x^p)}{\Phi_n(x)}$, якщо p не ділить n.

Лема 2. *Нехай n – натуральне число, p – просте число, яке ділить n. Тоді $\Phi_{pn}(x) = \Phi_n(x^p)$.*

Доведення. Нехай $n = p^l m$, де $l \geq 1$, $(p, m) = 1$. Тоді за лемою 1

$$\Phi_{np}(x) = \frac{\Phi_m\left(x^{p^{l+1}}\right)}{\Phi_m\left(x^{p^l}\right)} = \frac{\Phi_m\left((x^p)^{p^l}\right)}{\Phi_m\left((x^p)^{p^{l-1}}\right)} = \Phi_n(x^p).$$

Лема 3. *Нехай n – натуральне число і k – натуральне число, всі прості дільники якого зустрічаються серед дільників числа n. Тоді $\Phi_{kn}(x) = \Phi_n(x^k)$.*

Доведення. Нехай p – простий дільник n. За лемою 2

$$\Phi_{p^l n}(x) = \cdots = \Phi_n\left(x^{p^l}\right)$$

для будь-якого $t \geq 0$. Скориставшись отриманою рівністю для всіх простих дільників числа k, отримуємо твердження леми 3.

З леми 2 також випливає рівність

$$\Phi_n(x) = \Phi_{\frac{n}{p}}(x^p) = \cdots = \Phi_{\frac{n}{p^{l-1}}}\left(x^{p^{l-1}}\right), \quad \text{де } n = p^l m, l \geq 1, (p, m) = 1.$$

Тому, якщо $n = p_1^{n_1} \cdots p_k^{n_k}$, де $n_i \geq 1$, $1 \leq i \leq k$, то

$$\Phi_n(x) = \Phi_{p_1 \ldots p_k}\left(x^{p_l^{n_1-1} \cdots p_k^{n_k-1}}\right).$$

Наслідок 1. *Нехай m і n – довільні натуральні числа. Тоді має місце рівність*

$$\Phi_{mn}(x) = \Phi_{\text{НСК}(m,n)}\left(x^{\text{НСД}(m,n)}\right),$$

де НСК(m, n) – найменше спільне кратне, а НСД(m, n) – найбільший спільний дільник чисел m і n.

Доведення. Як відомо, $mn = \text{НСК}(m, n) \cdot \text{НСД}(m, n)$ і НСД(m, n) ділить НСК(m, n). Тому, згідно з лемою 3, має місце формула наслідку 1.

3. Спеціальні формули

Лема 4. *Нехай n – непарне число, $n > 1$. Тоді $\Phi_n(x)\Phi_n(-x) = \Phi_n(x^2)$.*

Доведення. Нехай $n = p^l m$, де p – непарне просте число, $l \geq 1$, а m – непарне число. Якщо $m = 1$, то

$$\Phi_n(x) = \Phi_{p^l}(x) = \Phi_p\left(x^{p^{l-1}}\right) = \frac{x^n - 1}{x - 1} \text{ і } \Phi_n(-x) = \frac{x^n + 1}{x + 1}.$$

Тому $\Phi_n(x)\Phi_n(-x) = \frac{x^{2n}-1}{x^2-1} = \Phi_n(x^2)$.

При $m > 1$ з індуктивних міркувань можна вважати, що

$$\Phi_m(x)\Phi_m(-x) = \Phi_m(x^2).$$

Тому

$$\Phi_n(x)\Phi_n(-x) = \frac{\Phi_m\left(x^{p^l}\right)}{\Phi_m\left(x^{p^{l-1}}\right)} \cdot \frac{\Phi_m\left(-x^{p^l}\right)}{\Phi_m\left(-x^{p^{l-1}}\right)} = \frac{\Phi_m\left(x^{2p^l}\right)}{\Phi_m\left(x^{2p^{l-1}}\right)} = \Phi_n(x^2).$$

З леми 4 випливає, що для непарного числа $n > 1$

$$\Phi_{2^l n}(x) = \frac{\Phi_n\left(x^{2^l}\right)}{\Phi_n\left(x^{2^{l-1}}\right)} = \Phi_n\left(-x^{2^{l-1}}\right).$$

Зокрема, $\Phi_{2n}(x) = \Phi_n(-x)$, якщо n – непарне число, $n > 1$.
Відмітимо, що при $n = 1$,

$$\Phi_{2^l n}(x) = \Phi_2\left(x^{2^{l-1}}\right) = 1 + x^{2^{l-1}} = -\Phi_n\left(-x^{2^{l-1}}\right).$$

4. Основний випадок

Теорема 1. *Нехай m і n – взаємно прості натуральні числа. Тоді*

$$\Phi_{mn}(x) = \prod_{d|n} \Phi_m\left(x^d\right)^{\mu\left(\frac{n}{d}\right)}.$$

Доведення. Нехай $n = p^l n_1$, де $l \geq 1$, $(p, n_1) = 1$, p – просте число. Доведення проведемо індукцією за числом різних простих дільників числа n. Якщо $n_1 = 1$, то теорема 1 випливає з леми 1. Нехай для $n_1 > 1$ теорема 1 вже доведена. Тому

$$\Phi_{mn_1}(x) = \prod_{d_1|n_1} \Phi_m\left(x^{d_1}\right)^{\mu\left(\frac{n_1}{d_1}\right)}.$$

В такому разі має місце рівність

$$\Phi_{mn}(x) = \Phi_{p^l mn_1}(x) = \frac{\Phi_{mn_1}\left(x^{p^l}\right)}{\Phi_{mn_1}\left(x^{p^{l-1}}\right)} = \prod_{d_1|n_1}\left(\frac{\Phi_m\left(x^{p^l d_1}\right)}{\Phi_m\left(x^{p^{l-1}d_1}\right)}\right)^{\mu\left(\frac{n_1}{d_1}\right)}.$$

Нехай $d = p^t d_1$ – дільник n, а d_1 – дільник n_1. Ясно, що

$$\mu\left(\frac{n}{d}\right) = \mu(p^{l-t})\mu\left(\frac{n_1}{d_1}\right).$$

Тому

$$\mu\left(\frac{n}{d}\right) = \begin{cases} 0, & t \leq l-2, \\ -\mu\left(\frac{n_1}{d_1}\right), & t = l-1, \\ \mu\left(\frac{n_1}{d_1}\right), & t = l. \end{cases}$$

Це означає, що

$$\prod_{d|n}\Phi_m\left(x^d\right)^{\mu\left(\frac{n}{d}\right)}=\prod_{d_1|n_1}\Phi_m\left(x^{p^l d_1}\right)^{\mu\left(\frac{n_1}{d_1}\right)}\Phi_m\left(x^{p^{l-1}d_1}\right)^{-\mu\left(\frac{n_1}{d_1}\right)}=\prod_{d_1|n_1}\left(\frac{\Phi_m\left(x^{p^l d_1}\right)}{\Phi_m\left(x^{p^{l-1}d_1}\right)}\right)^{\mu\left(\frac{n_1}{d_1}\right)}.$$

Оскільки праві частини рівностей рівні, то ліві частини рівностей також рівні. Тим самим теорема 1 доведена.

Лема 5. *Нехай m і n – довільні натуральні числа і n_0 – найбільший дільник n, який взаємно простий з m і всі прості дільники числа $\frac{n}{n_0}$ зустрічаються серед дільників mn_0.*

Тоді має місце рівність $\Phi_{mn}(x)=\prod\limits_{d|n_0}\Phi_m\left(x^{\frac{nd}{n_0}}\right)^{\mu\left(\frac{n_0}{d}\right)}$.

Доведення. За лемою 3

$$\Phi_{mn}(x)=\Phi_{mn_0\frac{n}{n_0}}(x)=\Phi_{mn_0}\left(x^{\frac{n}{n_0}}\right).$$

Оскільки $(m,n_0)=1$, то за теоремою 1

$$\Phi_{mn_0}(x)=\prod_{d|n_0}\Phi_m(x^d)^{\mu\left(\frac{n_0}{d}\right)}.$$

Тому має місце рівність

$$\Phi_{mn}(x)=\Phi_{mn_0}\left(x^{\frac{n}{n_0}}\right)=\prod_{d|n_0}\Phi_m\left(x^{\frac{n}{n_0}d}\right)^{\mu\left(\frac{n_0}{d}\right)}.$$

Наслідок 2. *Нехай n – довільне натуральне число, p – просте число, $(p,n)=1$, $l\geq 1$. Тоді*

$$\Phi_{p^l n}(x)=\prod_{d|n}\Phi_{p^i}\left(x^{p^{l-i}d}\right)^{\mu\left(\frac{n}{d}\right)},\ \ 1\leq i\leq l.$$

Доведення. Нехай $m=p^i$, $1\leq i\leq l$. Оскільки $n_0=n$ – найбільший дільник числа $p^{l-i}n$, який взаємно простий з m, такий що всі прості дільники числа p^{l-i} зустрічаються серед дільників числа m, то за лемою 5

$$\Phi_{p^l n}(x)=\prod_{d|n}\Phi_{p^i}\left(x^{p^{l-i}d}\right)^{\mu\left(\frac{n}{d}\right)}.$$

Зокрема, при $i=1$ отримуємо формулу

$$\Phi_{p^l n}(x)=\prod_{d|n}\Phi_p\left(x^{p^{l-1}d}\right)^{\mu\left(\frac{n}{d}\right)}.$$

1. Петечук Ю. В. Поліноми ділення круга // Науковий вісник Ужгород ун-ту. Сер. матем і інформ. – 2013. – Вип. 24, № 2. – С. 145–169.

2. Кострикин А. Н. Введение в алгебру. Часть 3. Основные структуры алгебры. – М.: Физ.-мат.лит., 2000. – 271 с.
3. Винберг Э. Б. Курс алгебры. – 2-е изд. испр. и доп. – М.: Факториал. Пресс., 2001. – 544 с.
4. Дроботенко В. С., Рудько В. П. Елементи теорії кілець. – Ужгород: Ужгород. нац. ун-т, 2004. – 128 с.
5. Дрозд Ю. А., Кириченко В. В. Конечномерные алгебры. – Киев: Вища школа, 1980. – 192 с.
6. Гудивок П. М., Рудько В. П., Бовді В. А. Кристалографічні групи. – Ужгород: Ужгород. нац. ун-т, 2006. – 173 с.
7. Кэртис Ч., Райнер И. Теория представлений конечных групп и ассоциативных алгебр.– М.: Наука, 1969. – 668 с.
8. Постников М. М. Введение в теорию алгебраических чисел. – М.: Наука, 1982. – 240 с.

Одержано 12.11.2014