# Многочлены деления круга

## Содержание



## 1 Простые свойства многочленов деления круга

### 1.1 Определение круговых многочленов

Рассмотрим примитивные комплексные корни из единицы. Так как $w_k = w_1^k$ будет являтся примитивным корнем тогда и только тогда, когда $(k, n) = 1$ то всего примитивных корней будет $\varphi(n)$. Обозначим их $\varepsilon_1, \ldots, \varepsilon_{\varphi(n)}$.

**Определение 1.** *Многочлен деления круга порядка $n$ определяется следующей формулой:*

$$\Phi_n(z) \overset{def}{=} (z-\varepsilon_1)(z-\varepsilon_2)\ldots\left(z-\varepsilon_{\varphi(n)}\right).$$

### 1.2 Свойства

Заметим, что при всех $n \geq 3$ многочлен не имеет действительных корней. Первое наблюдение является весьма тривиальным.

**Свойство 1.** *Для многочленов деления круга имеет место тождество:*

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

Немедленным следствием из этого свойства является тождество Гауса. Действительно, приравнивая степени многочленов слева и справа получаем

$$\sum_{d|n} \varphi(d) = n.$$

Сейчас мы докажем простое свойтсво многочленов деление круга, которое сразу же усилим.

**Свойство 2.** *При любом натуральном значении $n$ многочлен деления круга $n$-го порядка является многочленом с вещественными коэффициентами.*

*Доказательство.* Вспомним, что если $w_k$ – решения уравнения $w^n = 1$ то $\overline{w_k} = w_{n-k}$. Рассмотрим примитивный $\varepsilon_j$. Это означает, что $(j, n) = 1$, поэтому $(n - j, n) = 1$, откуда $\overline{\varepsilon_j}$ также является примитивным корнем. Поэтому все примитивные корни распадаються на пары сопряженных, причем каждый корень находится ровно в одной такой паре. Поэтому после открытия скобок и приведения подобных слагаемых получим многочлен с вещественными коэффициентами. □

**Свойство 3.** *При любом натуральном значении $n$: $\Phi(x) \in \mathbb{Z}[x]$ причем являются унитарными.*

*Доказательство.* Докажем это при помощи метода математической индукции. Для $n = 1$ очевидно.

Пусть для всех $k < n$ многочлен $\Phi_k(x)$ является многочленом с целыми коэффициентами.

Сделаем переход. По свойству 1 имеем, что:

$$x^n - 1 = \prod_{d|n} \Phi_d(x) = \Phi_n(x)Q(x).$$

Поэтому

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

Но $Q(x)$ – унитарный многочлен с целыми коэффициентами, причем он является делителем $x^n - 1$. Поэтому получаем, что их частное является унитарным многочленом с целыми коэффициентами. □

На самом деле при доказательстве этого свойства мы получили рекурсивную формулу для многочленов деления круга:

**Свойство 4.** *Многочлен деления круга $\Phi_n(x)$ удовлетворяет следующему рекуррентному соотношению:*

$$\Phi_n(x) = \frac{x^n - 1}{\prod\limits_{\substack{d|n \\ d<n}} \Phi_d(x)}$$

**Свойство 5.** *Многочлены деления круга являються возвратными в смысле коэффициентов. Другими словами, если*

$$\Phi_n(x) = \sum_{j=0}^{\varphi(n)} c_j x^j.$$

*То для коэффициентов справедлива формула $c_k = c_{\phi(n)-k}$.*

*Доказательство.* Для начала докажем лемму о многочленах с возвратными коэффициентами.

**Лемма.** *Если $P$ и $Q$ многочлены с возвратными коэффициентами, то их произведение $PQ$ также является таковым.*

*Доказательство.* Пусть $P(x) = a_p x^p + \cdots + a_0$ и $Q(x) = b_q x^q + \cdots + b_0$. Тогда условие возвратности можно записать следующим образом:

$$P(x) = x^p P(1/x).$$

Действительно $x^p P(1/x)$ – многочлен $P$ з коэффициентами записаными в обратном порядке:

$$x^p \cdot \left(\frac{a_p}{x^p} + \frac{a_{p-1}}{x^{p-1}} + \cdots + a_0\right) = a_0 x^p + \cdots + a_{p-1} + a_p.$$

Из того, что $P$ и $Q$ – многочлены с возвратными коэффициентами имеем $P(x) = x^p P(1/x)$ и $Q(x) = x^q Q(1/x)$. Пусть $R(x) := P(x)Q(x)$. Тогда:

$$R(x) = P(x)Q(x) = x^{p+q} P(1/x)Q(1/x) = x^{p+q} R(1/x)$$

Осталось заметить, что $\deg R = \deg P + \deg Q = p + q$. Получили условие возвратности коэффициентов для многочлена $R$. □

Теперь разобъём многочлен деления круга на пары сопряженных корней, таким образом, как мы это делали при доказательстве свойства 2.

$$\Phi_n(x) = \prod_{(\varepsilon, \overline{\varepsilon})} (x - \varepsilon)(x - \overline{\varepsilon}) = \prod_{(\varepsilon, \overline{\varepsilon})} (x^2 - (\varepsilon + \overline{\varepsilon})x + 1).$$

Но заметим, что последняя скобка является квадратным трехчленом с возвратными коэффициентами. Поэтому индуктивное применение леммы заканчивает доказательство. □

### 1.3 Явные значения круговых многочленов при некоторых значений $n$

Ниже приведена таблица значений круговых многочленов для $n = \overline{1, 10}$.

| $n$ | $\Phi_n(x)$ |
|---|---|
| 1 | $x - 1$ |
| 2 | $x + 1$ |
| 3 | $x^2 + x + 1$ |
| 4 | $x^2 + 1$ |
| 5 | $x^4 + x^3 + x^2 + x + 1$ |
| 6 | $x^2 - x + 1$ |
| 7 | $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ |
| 8 | $x^4 + 1$ |
| 9 | $x^6 + x^3 + 1$ |
| 10 | $x^4 - x^3 + x^2 - x + 1$ |

Внимательно изучив данную таблицу можно заметить, что $\Phi_p(x) = x^{p-1} + \cdots + 1$, что в действительности является правдой. Доказать это утверджение не составляет труда, в частности, если заметить, что для простого числа $p$ примитивными корнями являються все корни из единицы кроме тривиального.

Также может показатся, что все коэффициенты преднадлежат множеству $\{-1, 0, 1\}$, но в общем это не так. Контрпримером является 105-й круговой многочлен:

$$\Phi_{105}(x) = x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - \cdots + 1$$

## 2 Связь многочленов деления круга и функции Мёбиуса

### 2.1 Основное свойство

Сейчас будет доказано очень полезное утверждение.

**Свойство 6.** *Для круговых многочленов можна выписать явную формулу:*

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

Автору известно два доказательства данной теоремы: комбинаторное и теоретико-числовое.

*Доказательство.* Для начала приведем теоретико-числовое доказательство при помощи формулы обращения Мёбиуса. Формула обращения Мёбиуса. Пусть $f(n) = \sum_{d|n} g(d)$. Тогда справедлива формула:

$$g(n) = \sum_{d|n} \mu(d) f(n/d)$$

*Доказательство.* Запишем следующую цепочку сумм:

$$\sum_{d|n} \mu(d) f(n/d) = \sum_{d|n} \left[\mu(d) \sum_{x|\frac{n}{d}} g(x)\right] = \sum_{\substack{d|n \\ x|\frac{n}{d}}} \mu(d) g(x) =$$

$$\sum_{dx|n} \mu(d) g(x) = \sum_{dx|n} \mu(x) g(d) =$$

$$\sum_{d|n} \left[g(d) \sum_{x|\frac{n}{d}} \mu(x)\right] = \sum_{d|n} g(d)[n/d = 1] = g(n).$$

В конце использована нотация Айверсона. □

Следствие. Пусть $t(n) = \prod_{d|n} g(d)$. Тогда:

$$g(n) = \prod_{n|d} t(n/d)^{\mu(d)}.$$

*Доказательство.* Сделаем замену $g^*(x) := \ln g(x)$. Тогда

$$f^*(x) = \sum_{d|n} g^*(x) = \sum_{d|n} \ln g(x) = \ln \prod_{d|n} g(x).$$

Применим формулу обращения Мёбиуса для $f^*, g^*$.

$$g^*(n) = \sum_{d|n} \mu(d) f^*(n/d)$$

Приравняем $e$ возведенное в одинаковые степени:

$$g(n) = e^{\sum\limits_{d|n} \mu(d) f^*(n/d)} = \prod_{n|d} \left(e^{f^*(n/d)}\right)^{\mu(d)} = \prod_{n|d} \left(\prod_{x|\frac{n}{d}} g(x)\right)^{\mu(d)}.$$

□

Пусть $g(n) = \Phi_n(x)$. Тогда по свойству 1:

$$t(n) = x^n - 1 = \prod_{d|n} \Phi_n(x).$$

Теперь применим следствие из формулы обращения:

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

□

Следующее доказательство является комбинаторным. В частности, оно использует метод включений-исключений.

*Доказательство.* TODO. □

## 2.2 Вокруг основного свойства

На самом деле теперь можна передоказать свойство 3 при помощи свойства 6:

*Доказательство.* Если перегруппировать множители поставив сначала множители в которых $\mu(n/d) = 1$, а потом $\mu(n/d) = -1$ получим, что $\Phi_n(x) = P(x)/Q(x)$ для некоторых многочленов $P(x)$ и $Q(x)$ – унитарных, с целыми коэффициентами откуда $\Phi_n(x) \in \mathbb{Q}[x]$ и существует целое число $t$ такое, что $t\Phi_n(x) \in \mathbb{Z}[x]$, причем содержанием многочлена $t\Phi_n(x)$ будет единица. Но с другой стороны: $Q(x)t\Phi_n(x) = tP(x)$, поэтому применяя лемму Гауса о содержании многочленов получаем: $d(Q(x)t\Phi_n(x)) = d(tP(x))$, то есть, $d(Q(x)) = td(P(x))$. Но пользуясь унитарностю немедленно получаем $t = 1$ что и доказывает свойство. □

Докажем несколько свойств.

**Свойство 7.** *Для любого натурального числа $n$ и его делителя $d$ выполнено:*

$$\Phi_n(x) \;\Big|\; \frac{x^n - 1}{x^d - 1}.$$

*Доказательство.* Все делители числа $n$ можна разделить на два класса: делители числа $d$ и делители $n$ не являющимися делителями $d$. Тогда воспользуемся свойством 1:

$$x^n - 1 = \prod_{j|n} \Phi_j(x) = \prod_{j|d} \Phi_j(x) \cdot \prod_{\substack{j|n \\ j \nmid n}} \Phi_j(x) = (x^k - 1)\Phi_n(x)Q(x) \implies$$

$$Q(x)\Phi_n(x) = \frac{x^n - 1}{x^k - 1}.$$

Но $Q(x)$ – произведение нескольких унитарных многочленов с целыми коэффициентами, откуда следует искомое свойство. □

**Свойство 8.** *Для круговых многочленов справделива формула:*

$$\Phi_{pn}(x) = \frac{\Phi_n(x^p)}{\Phi_n(x)},$$

*если $p$ является простым числом взаимнопростым з $n$.*

*Доказательство.* Запишем следующее равенство пользуясь свойством 6:

$$\Phi_{pn}(x) = \prod_{d|pn} \left(x^d - 1\right)^{\mu\left(\frac{pn}{d}\right)} = \prod_{d|n} \left(x^d - 1\right)^{\mu\left(\frac{pn}{d}\right)} \cdot \prod_{d|n} \left(x^{pd} - 1\right)^{\mu\left(\frac{n}{d}\right)} =$$

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

□

# 3 Неприводимость многочленов деления круга

Основная цель данного раздела – доказать неприводимость круговых многочленов. Заметим, что лемма Гауса показывает равносильность приводимости над $\mathbb{Q}$ и $\mathbb{Z}$, поэтому доказывать будем приводимость над $\mathbb{Q}$.

## 3.1 Простое доказательство для простых значений $n$

### 3.1.1 Критерий Эйзенштейна

**Теорема 1** (Критерий Эйзенштейна)**.** *Пусть*

$$P(x) = c_n x^n + \cdots + c_0$$

*является многочленом с целыми коэффициентами. Тогда если существует простое число $p$ такое, что*

*1. $c_n$ не делиться на $p$,*

*2. $c_0, \ldots, c_{n-1}$ делятся на $p$,*

*3. $c_0$ не делиться на $p^2$,*

*то многочлен является неприводимым над полем рациональных чисел $\mathbb{Q}$.*

Доказательство теоремы является прямым следствием леммы Гауса о содержании многочленов.

### 3.1.2 Доказательство

Перепишем многочлен деления круга следующим образом:

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = \frac{((x-1)+1)^p}{x-1} - \frac{1}{x-1} =$$

$$\frac{1 + \sum_{k=1}^{p} \binom{p}{k}(x-1)^k}{x-1} - \frac{1}{x-1} = \sum_{k=1}^{p} \binom{p}{k} (x-1)^{k-1}.$$

Пусть $y = x - 1$. Рассмотрим многочлен

$$\Phi_p(y) = \sum_{k=1}^{p} \binom{p}{k} y^{k-1} = \binom{p}{1} + \binom{p}{2} y + \cdots + \binom{p}{p} y^{p-1}.$$

Проверим критерий Эйзенштейна:

1. $c_{p-1} = 1$, что не делиться на $p$;

2. $c_k = \binom{p}{k}$ – делится на $p$;

3. $c_0 = p$ – не делиться на $p^2$.

Поэтому многочлен неприводим над $\mathbb{Q}$.

# 4 Применения круговых многочленов

## 4.1 Теория чисел

### 4.1.1 Частный случай теоремы Дирихле

Докажем частный случай теоремы Дирихле.

Теорема Дирихле. Существует бесконечно много простых чисел $p$ таких, что $p \equiv l \pmod k$, где $l, k > 0$ являються взаимнопростыми числами.

Докажем данную теорему в случае $l = 1$.

**Теорема 2.** *Для любого натурального числа $n > 1$ и любого натурального числа $M$ существует простое число $p > M$ такое, что $p \equiv 1 \pmod 1$.*

*Доказательство.* Введем многочлен $G_n(x)$:

$$G_n(x) := \frac{x^n - 1}{\Phi_n(x)} = \prod_{\substack{d|n \\ d<n}} \Phi_d(x).$$

Докажем следующую лемму.

**Лемма.** *Пусть $a$ – натуральное число, а $p$ – простое число, такое, что $p \mid a^n - 1$ и $p \nmid G_n(a)$. Тогда $(p-1) \vdots n$.*

*Доказательство.* Ясно, что достаточно доказать, что $n$ является покзаателем числа $n$ по модулю $p$. Тогда $n$ будет делить $(p-1)$, а это и нужно доказать.

Пусть $k$ является показателем числа $n$ по модулю $p$. Тогда имеем, что $k$ является общим делителем $p-1$ и $n$ ($a^{p-1} \equiv 1$, $a^n \equiv 1$). Докажем, что $n = k$.

Предположим обратное, то есть, что $k < n$. В таком случае $G_n(x) \vdots x^k - 1$. Это легко понять если обратить внимание на корни $G_n(x)$ и $x^k - 1$. Поэтому их частное будем многочленом с целыми коэффициентами, то есть

$$\frac{G_n(x)}{x^k - 1} \in \mathbb{Z}[x] \implies \frac{G_n(a)}{a^k - 1} \in \mathbb{Z}.$$

Но так как $k$ является показателем, то $a^k - 1$ делиться на $p$, но тогда и $G_n(a)$ делиться на $p$, что противоречит условию. Поэтому $n = k$ и лемма доказана. □

Теперь докажем, что для любого натурального числа $M$ существует простое число $p > M$, такое, что $(p-1) \vdots n$. Выберем число $a$ кратное $M!$. Тогда, очевидно, $\gcd(a^n - 1, M!) = 1$, поэтому любой простой делитель $a^n - 1$ будет превышать число $M$. Выберем какой-нибудь такой делитель $p$. Для того, чтобы обеспечить тот факт факт, что $p \mid \Phi_n(a)$ и $p \nmid G_n(a)$ достаточно потребовать взаимную простоту $\Phi_n(a)$ и $G_n(a)$ как чисел.

Заметим, что данные многочлены взаимнопросты в смысле многочленов, так как они не имеют общий корней ($\Phi_n(x)$ имеет своими корнями только первообразные, а $G_n(x)$ – только не первообразные). Отсюда следует существование линейного разложения НОД данных многочленов:

$$U_1(x)\Phi_n(x) + V_1(x)G_n(x) = 1$$

причем $U_1(x)$ и $V_1(x)$ являются многочленами с рациональными коэффициентами. Умножим данное тождество на общий знаменатель и получим:

$$U(x)\Phi_n(x) + V(x)G_n(x) = N \implies U(a)\Phi_n(a) + V(a)G_n(a) = N.$$

для некоторого числа $N$, причем $U(x), V(x) \in \mathbb{Z}[x]$. Теперь предположим, что $\Phi_n(a)$ и $G_n(a)$ не взаимнопросты как числа, то есть:

$$\gcd(\Phi_n(a), G_n(a)) = d > 1 \implies N \vdots d.$$

TODO

□