

# 1 Множество простых чисел, являющихся делителями значений кругового многочлена в целых точках.

## 1.1 Некоторые тождества круговых многочленов.

Здесь и далее:  $\Phi_n$  —  $n$ -ый круговой многочлен,  $\varepsilon_n$  — примитивный корень степени  $n$  из 1.

**1.1.1** Пусть  $p$  — простое число. Тогда:

- а) если  $p \mid n$ , то  $\Phi_n(x^p) = \Phi_{np}(x)$
- б) если  $p \nmid n$ , то  $\Phi_n(x^p) = \Phi_{np}(x)\Phi_n(x)$

Доказательство: а) Многочлены слева и справа имеют одинаковую степень ( $p\varphi(n)$  слева и  $\varphi(np)$  справа) и одинаковый коэффициент при старшей степени, и при этом у многочлена справа нет кратных корней, а значит, достаточно проверить, что каждый его корень является корнем многочлена слева. Корни многочлена справа —  $e^{\frac{2\pi d}{np}i}$ ,  $(d, np) = 1$ .  $\left(e^{\frac{2\pi d}{np}i}\right)^p = e^{\frac{2\pi d}{n}i} = \varepsilon_n^d$ ,  $(n, d) = 1$ , а это является корнем  $\Phi_n(x)$ .

б) Многочлены слева и справа имеют одинаковую степень ( $p\varphi(n)$  слева и  $\varphi(np) + \varphi(n) = (p-1)\varphi(n) + \varphi(n) = p\varphi(n)$  справа) и одинаковый коэффициент при старшей степени, и при этом у многочлена справа нет кратных корней, а значит, достаточно проверить, что каждый его корень является корнем многочлена слева. Корни многочлена справа —  $e^{\frac{2\pi d}{np}i}$ ,  $(d, np) = 1$  или  $e^{\frac{2\pi d}{n}i}$ ,  $(d, n) = 1$ .  $\left(e^{\frac{2\pi d}{np}i}\right)^p = e^{\frac{2\pi d}{n}i} = \varepsilon_n^d$ ,  $(n, d) = 1$ ,  $\left(e^{\frac{2\pi d}{n}i}\right)^p = e^{\frac{2\pi dp}{n}i} = \varepsilon_n^{dp}$ ,  $(n, dp) = 1$ , и они все являются корнями  $\Phi_n(x)$ .

**1.1.2.**  $x^n - 1 = \Phi_n(x)q(x)$ , где  $(x^d - 1) \mid q(x)$  для всех  $d \mid n$ ,  $d < n$ .

Доказательство: пусть  $k \mid n$ ,  $k < n$ .  $x^n - 1 = \prod_{d \mid n} \Phi_d(x) = \Phi_n(x) \cdot \left(\prod_{d \mid k} \Phi_d(x)\right) \cdot \left(\prod_{d \mid n, d \nmid k, d < n} \Phi_d(x)\right) = \Phi_n(x) \cdot (x^k - 1) \cdot \left(\prod_{d \mid n, d \nmid k, d < n} \Phi_d(x)\right)$

**1.1.3.**  $\Phi(0) = \pm 1$ .

Доказательство: Докажем по индукции.

База:  $\Phi_1(0) = 0 - 1 = -1$

Переход: Пусть для  $n < n_0$  это верно, рассмотрим для  $n = n_0$ .  $0^{n_0} - 1 = \prod_{d \mid n_0} \Phi_d(0) = \Phi_{n_0}(0) \cdot (\pm 1)$ ,

следовательно,  $\Phi_{n_0}(0) = \pm 1$ .

## 1.2 Некоторые свойства круговых (и не только) многочленов в $\mathbb{Z}_p[x]$ .

Здесь все рассуждения про многочлены происходят в  $\mathbb{Z}_p[x]$ .

**1.2.1.**  $(f(x))^p = f(x^p)$ .

Доказательство: Пусть  $f(x) = a_n x^n + f_1(x)$ . По биному Ньютона  $(a_n x^n + f_1(x))^p = (a_n x^n)^p + (f_1(x))^p = a_n (x^p)^n + (f_1(x))^p$ . Повторяя аналогичные рассуждения, получаем искомое.

**1.2.2.** Пусть  $f$  — многочлен в  $\mathbb{Z}_p[x]$ . Тогда многочлены  $f$  и  $f'$  не взаимнопросты тогда и только тогда, когда существует непостоянный многочлен  $g$  такой, что  $g^2 \mid f$ .

Доказательство: (1) Пусть  $g^2 \mid f$ . Тогда  $f = g^2 h$ , значит,  $f' = g^2 h' + 2g g' h$ , следовательно,  $g \mid f'$ .

(2) Пусть  $g \mid f, f'$ ;  $g$  неприводим,  $f = gh$ . Тогда  $f' = gh' + g'h$ , значит,  $g \mid g'h$ . Если  $g \mid h$ , то  $g^2 \mid f$ . Пусть тогда  $g \nmid h$ . Если  $\deg g' > 0$ , то  $\deg g' < \deg g$ , следовательно,  $g \nmid g'$ . Значит,  $\deg g' = 0$ , а это происходит тогда и только тогда, когда все степени  $x$  в  $g(x)$  кратны  $p$ , т.е.  $g(x) = r(x^p)$ . По (1.2.1)  $g(x) = (r(x))^p$ . Но  $g(x)$  был неприводимым. Противоречие.

**1.2.3.** Пусть  $p$  — простое и  $m, n$  — различные не равные 1 натуральные числа, не делящиеся на  $p$ . Тогда  $\Phi_m(x)$  и  $\Phi_n(x)$  взаимнопросты в  $\mathbb{Z}_p[x]$ .

Доказательство: Пусть  $g(x) = \text{НОД}(\Phi_m(x), \Phi_n(x))$ ,  $\deg g > 0$ . Тогда  $g^2(x) \mid \Phi_m(x) \cdot \Phi_n(x) \mid (x^{mn} - 1)$ . По (1.2.2)  $g(x) \mid (x^{mn} - 1)'$ .  $(x^{mn} - 1)' = mn x^{mn-1}$ .  $p \nmid mn$ , значит,  $mn x^{mn-1} \not\equiv 0$ , следовательно,  $g(x) = x^\alpha$ , значит,  $x^\alpha \mid \Phi_n(x)$ , следовательно,  $\Phi_n(0) \equiv 0 \pmod{p}$ . Но по (1.1.3)  $\Phi_n(0) \equiv \pm 1 \pmod{p}$ . Противоречие.

### 1.3 Завершение.

Обозначим за  $P(f)$  множество простых чисел, являющихся делителями значений  $f$  в целых точках.  $ord_p(n)$  – показатель числа  $n$  по модулю  $p$ .

**1.3.1.** Пусть  $p$  – простое и  $m, n$  – различные не равные 1 натуральные числа, не делящиеся на  $p$ . Тогда не существует таких натуральных  $k$ , что  $\Phi_n(k) \equiv \Phi_m(k) \equiv 0 \pmod{p}$ .

Доказательство: Пусть это не так. Тогда у  $\Phi_n, \Phi_m$  как у многочленов в  $\mathbb{Z}_p[x]$  есть общий корень. Противоречие с (1.2.3).

**1.3.2.** Пусть  $p \in P(\Phi_n)$ . Тогда либо  $p \mid n$ , либо  $p \equiv 1 \pmod{n}$ .

Доказательство: Пусть  $p \nmid n$ . По (1.1.2) представим  $x^n - 1 = \Phi_n(x)q(x)$ . Пусть  $p \mid \Phi_n(x_0)$ .  $p \mid (x_0^n - 1)$ , значит,  $ord_p(x_0) \mid n$ .

Случай 1:  $ord_p(x_0) = a < n$ .  $a \mid n$ , значит, по (1.1.2)  $(x^a - 1) \mid q(x)$ , следовательно,  $p \mid q(x_0)$ , значит,  $\exists k \mid n$ :  $p \mid \Phi_k(x_0)$ . Но  $p \nmid n$ ,  $p \nmid k$ , и по (1.3.1) получаем противоречие.

Случай 2:  $ord_p(x_0) = n$ . Тогда  $n \mid p - 1$ , а значит,  $p \equiv 1 \pmod{n}$ .

**1.3.3.** Пусть  $m$  – целое число, не делящееся на нечётное простое  $p$ , и пусть  $d = ord_p(m)$ . Тогда при любом  $i = 0, 1, 2, \dots$  число  $p$  делит  $\Phi_{n_i}(m)$ , где  $n_i = dp^i$ .

Доказательство: По (1.1.2) представим  $x^d - 1 = \Phi_d(x)q(x)$ .

Пусть  $p \mid q(m)$ . Тогда  $\exists k \mid d$ ,  $k < d$ :  $p \mid \Phi_k(m)$ . Значит, поскольку  $\Phi_k(x) \mid x^k - 1$ ,  $m^k - 1 \equiv 0 \pmod{p}$ . Но  $k < d = ord_p(m)$ . Противоречие. Значит,  $p \mid \Phi_d(m)$ .

$ord_p(m) \mid p - 1$ , следовательно,  $d < p$ , значит,  $p \nmid d$ .

Дальнейшее докажем по индукции.

База:

Рассмотрим многочлен  $\Phi_d(x^p)$  как многочлен в  $\mathbb{Z}_p[x]$ . По (1.2.1)  $\Phi_d(x^p) = (\Phi_d(x))^p$ . По (1.1.16)  $(\Phi_d(x))^p \equiv \Phi_{dp}(x)$ .  $\Phi_{dp}(m) \equiv (\Phi_d(m))^{p-1} \equiv 0 \pmod{p}$ .

Переход:

Пусть  $p \mid \Phi_{dp^\alpha}(m)$ . По (1.1.1a)  $\Phi_{dp^{\alpha+1}}(m) \equiv \Phi_{dp^\alpha}(m^p) \equiv \Phi_{dp^\alpha}(m) \equiv 0 \pmod{p}$ , что и требовалось доказать.

**1.3.4.**  $P(\Phi_n)$  состоит из таких  $p$ , что либо  $p = nk + 1$ , либо  $p \mid n$  и если  $n = p^\alpha m$ ,  $p \nmid m$ , то  $p \equiv 1 \pmod{m}$ .

Доказательство: По (1.3.2) есть 2 случая:

1)  $p \equiv 1 \pmod{n}$ . Пусть  $p = nk + 1$ . Пусть  $a$  – первообразный корень по модулю  $p$ .  $ord_p(a^k) = n$ , а значит, по (1.3.3)  $\Phi_n(a^k) \equiv 0 \pmod{p}$ , значит, все такие  $p$  подходят.

2) Пусть  $p \mid n$ ,  $p \mid \Phi_n(a)$ ,  $n = p^\alpha m$ ,  $p \nmid m$ . Проведем серию рассуждений, пользуясь (1.1.1):

$$0 \equiv \Phi_{p^\alpha m}(a) = \Phi_{p^{\alpha-1}m}(a^p) \equiv \Phi_{p^{\alpha-1}m}(a) \pmod{p}$$

$$0 \equiv \Phi_{p^{\alpha-1}m}(a) = \Phi_{p^{\alpha-2}m}(a^p) \equiv \Phi_{p^{\alpha-2}m}(a) \pmod{p}$$

...

$$0 \equiv \Phi_{p^2m}(a) = \Phi_{pm}(a^p) \equiv \Phi_{pm}(a) \pmod{p}$$

$$0 \equiv \Phi_{pm}(a) \cdot \Phi_m(a) = \Phi_m(a^p) \equiv \Phi_m(a) \pmod{p}$$

Значит,  $p \in P(\Phi_m)$ . По (1.3.2)  $p \equiv 1 \pmod{m}$  (по предположения  $p \nmid m$ ).

Теперь пусть  $q \mid n$  – простое, такое, что если  $n = q^\beta m_1$ ,  $q \nmid m_1$ , то  $q \equiv 1 \pmod{m_1}$ .

Пусть  $q = m_1 k_1 + 1$  и пусть  $b$  – первообразный корень по модулю  $q$ . Тогда  $ord_q(b^{k_1}) = m_1$ , а значит, по (1.3.3)  $q \mid \Phi_{q^\beta m_1}(b^{k_1})$ . Значит, все такие  $q$  подходят, что и требовалось доказать.

## 2 Бесконечность множества простых чисел вида $4k + 1$ , являющихся делителями значений многочлена $f \in \mathbb{Z}[x]$ в целых точках.

### Лемма

Пусть  $a, b \in \mathbb{Z}$ ,  $a > b > 0$ ,  $a^2 + b^2 = c$ . Тогда найдётся простое число вида  $4k + 1$  такое, что  $p \mid c$ .

Доказательство: Будем считать, что  $a, b, c$  взаимнопросты в совокупности (иначе разделим  $a$  и  $b$  на их наибольший общий делитель).

Пусть  $c$  не делится на простые вида  $4k + 1$ .

Пусть  $c$  делится на простое  $q$  вида  $4k + 3$ .  $q \nmid b$  (иначе  $q \mid a$  и противоречие с взаимной простотой), а значит,  $\left(\frac{a}{b}\right)^2 \equiv -1 \pmod{q}$ . Но  $-1$  — не квадратичный вычет по модулю простых вида  $4k + 3$ . Противоречие.

Значит,  $c = 2^k$ . Причём  $c = a^2 + b^2 > 2^2 + 1^2 = 5$ , значит,  $k > 1$ , значит,  $4 \mid c$ . Но, поскольку  $a$  и  $b$  нечётны (иначе противоречие с взаимной простотой),  $a^2 + b^2 \equiv 1 + 1 \equiv 2 \not\equiv 0 \pmod{4}$ . Противоречие. Лемма доказана.

### Найдем одно такое число.

Без ограничения общности будем считать, что старший коэффициент  $f$  больше 0.

Пусть  $a \in \mathbb{Z}$ . Пусть  $f(a + i) = v_a + w_a i$ ,  $f(a - i) = v_a - w_a i$ ,  $v_a, w_a \in \mathbb{R}$ . Поскольку

$$f(a + i) = f(a) + f'(a)i - \frac{f''(a)}{2}i^2 - \frac{f'''(a)}{6}i^3 + \frac{f^{(4)}(a)}{24}i^4 + \dots$$

имеем

$$v_a = f(a) - \frac{f''(a)}{2} + \frac{f^{(4)}(a)}{24} + \dots$$

и

$$w_a = f'(a) - \frac{f'''(a)}{6} + \frac{f^{(5)}(a)}{120} - \dots$$

$v_a$  и  $w_a$  — многочлены степень  $\deg f$  и  $\deg f - 1$  с целыми коэффициентами и со старшим коэффициентом, большим 0, соответственно, а значит,  $v_a, w_a \in \mathbb{Z}$  и, начиная с некоторого  $a$ ,  $v_a > w_a > 0$ . Рассмотрим любое такое  $a$ . Пусть  $s = v_a^2 + w_a^2$ . По лемме у  $s$  будет простой делитель  $p = 4k + 1$ . Пусть  $r$  такое, что  $r^2 \equiv -1 \pmod{p}$ .

Теперь докажем, что  $f(x) = h_a(x) \cdot ((x - a)^2 + 1) + w_a(x - a) + v_a$ . Достаточно проверить  $x = a + i$  и  $x = a - i$ :

$$f(a + i) = h_a(a + i) \cdot 0 + w_a i + v_a = v_a + w_a i$$

$$f(a - i) = h_a(a - i) \cdot 0 - w_a i + v_a = v_a - w_a i$$

Также, поскольку  $v_a, w_a \in \mathbb{Z}$  и старший коэффициент у  $(x - a)^2 + 1$  равен 1,  $h_a \in \mathbb{Z}[x]$ .

Теперь есть 2 случая:

1)  $p \mid v_a$ ,  $p \mid w_a$ . Тогда  $f(a + r) \equiv h_a(a + r) \cdot (r^2 + 1) \equiv 0 \pmod{p}$ .

2)  $p \nmid v_a$ ,  $p \nmid w_a$ . Тогда  $\left(\frac{v_a}{w_a}\right)^2 \equiv -1 \pmod{p}$ , значит,  $\frac{v_a}{w_a} \equiv \mp r \pmod{p}$ , следовательно,  $p \mid (\pm w_a r + v_a)$ . Подставляя в разложение  $f$ , получаем:

$$f(a \pm r) = h_a(a \pm r) \cdot (r^2 + 1) \pm w_a r + v_a \equiv 0 \pmod{p}$$

Итак, одно простое число вида  $4k + 1$  найдено.

**Теперь докажем, что если есть одно такое число  $p$ , то таких чисел бесконечно много.**

Пусть  $p \mid f(m)$ . Если  $f(m) = 0$ , то  $f(m)$  делится на любое простое число, поэтому будем считать, что степень вхождения  $p$  в  $f(m)$  равна  $\alpha \neq \infty$ .

Рассмотрим  $f_1(x) = \frac{f(m+p^{\alpha+1})}{p^\alpha}$ .

$$f_1(x) = \frac{1}{p^\alpha} \left( f(m) + \frac{f'(m)}{1!} \cdot p^{\alpha+1}x + \frac{f''(m)}{2!} \cdot p^{2\alpha+2}x + \dots \right)$$

Значит,  $f_1(x) \in \mathbb{Z}[x]$ , и при этом  $\forall n \in \mathbb{Z}: p \nmid f_1(n)$ . Применим предыдущие рассуждения к  $f_1$  и найдём для него отличное от  $p$  простое вида  $4k+1$ , и оно же будет делителем значения  $f$  в некоторой целой точке. Далее образуем  $f_2$  из  $f_1$  и т.д. Таким образом мы найдём сколь угодно много простых чисел вида  $4k+1$ , являющихся делителями значений  $f$  в целых точках, что и требовалось доказать.