Теорема 12.4. Многочлен $p_k(x)$ степени k принимает целые значения при $x = 1, q, q^2, \ldots, q^k$ тогда и только тогда, когда

$$p_k(x) = c_k f_k(x) + c_{k-1} f_{k-1}(x) + \ldots + c_1 f_1(x) + c_0, \tag{3}$$

где $c_0, c_1, \ldots, c_k$ — целые числа. В частности, такой многочлен принимает целые значения при всех $x = q^n$ $(n \in \mathbb{N})$.

Доказательство. Многочлены $f_0, f_1, \ldots, f_k$ образуют базис линейного пространства многочленов степени не выше k, поэтому равенство (3) выполняется при некоторых $c_0, c_1, \ldots, c_k \in \mathbb{C}$. Нужно лишь проверить, что $c_0, \ldots, c_k \in \mathbb{Z}$. Формулы (2) показывают, что

$$\begin{aligned}
p_k(1) &= c_0,\\
p_k(q) &= c_1 + c_0,\\
p_k(q^2) &= c_2 + c_1 f_1(q^2) + c_0,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
p_k(q^k) &= c_k + c_{k-1} f_{k-1}(q^k) + \ldots + c_1 f_1(q^k) + c_0.
\end{aligned}$$

Поэтому последовательно получаем

$$c_0 \in \mathbb{Z} \Rightarrow c_1 \in \mathbb{Z} \Rightarrow \ldots \Rightarrow c_k \in \mathbb{Z}. \qquad \square$$

Если целая аналитическая функция принимает целые значения в точках $1, q, q^2, \ldots$ и при этом растет не слишком быстро, то эта функция — многочлен. Точную формулировку и доказательство этого утверждения можно найти в книге [Ге2], с. 186–188.

13. Круговые многочлены

13.1. Основные свойства круговых многочленов

Многочлен $\Phi_n(x) = \prod(x - \varepsilon_k)$, где $\varepsilon_1, \ldots, \varepsilon_{\varphi(n)}$ — примитивные корни степени n из единицы, называют *круговым многочленом*, или *многочленом деления круга* порядка n. Например, $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$, $\Phi_3(x) = x^2 + x + 1$, $\Phi_4(x) = x^2 + 1$.

При $n > 2$ в число первообразных корней (из единицы) степени n не входит ± 1. В таком случае первообразные корни разбиваются на пары комплексно сопряженных чисел. Поэтому при $n > 2$ степень многочлена Φ_n четна.

Непосредственно из определения кругового многочлена видно, что

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

Теорема 13.1. Пусть $n > 1$ — нечетное число. Тогда

$$\Phi_{2n}(x) = \Phi_n(-x).$$

Доказательство. Если $\varepsilon_1, \ldots, \varepsilon_{\varphi(n)}$ — первообразные корни степени n, то $-\varepsilon_1, \ldots, -\varepsilon_{\varphi(n)}$ — первообразные корни степени $2n$. Таким образом,

$$\begin{aligned}
\Phi_n(-x) &= (-x - \varepsilon_1) \cdot \ldots \cdot (-x - \varepsilon_{\varphi(n)}),\\
\Phi_{2n}(x) &= (x + \varepsilon_1) \cdot \ldots \cdot (x + \varepsilon_{\varphi(n)}).
\end{aligned}$$

Остается заметить, что степень многочлена Φ_n четна. $\square$

13.2. Формула обращения Мёбиуса

Соотношение

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

позволяет получить явное выражение для $\Phi_n(x)$ через $x^d - 1$, где d пробегает делители n. Для этого имеется достаточно общая конструкция, основанная на *функции Мёбиуса*

$$\mu(n) = \begin{cases} 1 & \text{при } n = 1;\\ (-1)^k & \text{при } n = p_1 \ldots p_k;\\ 0 & \text{при } n = p^2 m. \end{cases}$$

Теорема 13.2 (Мёбиус). Если $F(n) = \sum\limits_{d|n} f(d)$, то

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

Доказательство. Прежде всего проверим, что при всех $n > 1$ выполняется соотношение $\sum\limits_{d|n} \mu(d) = 0$. Пусть $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$. Тогда

$$\sum_{d|n} \mu(d) = \sum_{d|p_1 \ldots p_k} \mu(d) = 1 - \binom{k}{1} + \binom{k}{2} + \ldots + (-1)^k = (1-1)^k = 0.$$

Ясно, что

$$\sum_{ab=n} F(a)\mu(b) = \sum_{d_1 d_2 b=n} f(d_1)\mu(b) = \sum_{d_1|n}\left(f(d_1)\sum_{d_2 b=n/d_1}\mu(b)\right).$$

Пусть $n/d_1 = m$. Тогда

$$\sum_{d_2 b=m}\mu(b) = \sum_{b|m}\mu(b) = \begin{cases} 1 & \text{при } n = d_1; \\ 0 & \text{при } n \neq d_1. \end{cases}$$

Поэтому

$$\sum_{d_1|n}\left(f(d_1)\sum_{d_2 b=n/d_1}\mu(b)\right) = f(n).$$ □

Следствие. Если $F(n) = \prod\limits_{d|n} f(d)$, то

$$f(n) = \prod_{d|n} F(n/d)^{\mu(d)} = \prod_{d|n} F(d)^{\mu(n/d)}.$$

Для круговых многочленов формула обращения Мёбиуса дает выражение

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

Теорема 13.3. Коэффициенты многочлена $\Phi_n(x)$ — целые числа.

Доказательство. Сгруппируем в произведении $\prod_{d|n}(x^d-1)^{\mu(n/d)}$ отдельно множители с $\mu = 1$ и множители с $\mu = -1$. В результате получим $\Phi_n(x) = P(x)/Q(x)$, где P и Q — многочлены с целыми коэффициентами и со старшим коэффициентом 1. Алгоритм деления многочленов показывает, что Φ_n — многочлен с рациональными коэффициентами. Поэтому существует такое целое m, что многочлен $m\Phi_n$ имеет целые коэффициенты, причем их наибольший общий делитель равен 1. Согласно лемме Гаусса наибольший общий делитель коэффициентов многочлена $mP = (m\Phi_n)Q$ равен произведению наибольших общих делителей коэффициентов многочленов $m\Phi_n$ и Q, т. е. он равен 1. С другой стороны, наибольший общий делитель коэффициентов многочлена mP равен m. Поэтому $m = \pm 1$, т. е. коэффициенты многочлена Φ_n — целые числа. □

13.3. Неприводимость круговых многочленов

В предыдущем параграфе мы показали, что коэффициенты многочлена $\Phi_n(x)$ — целые числа.

Теорема 13.4. Многочлен Φ_n неприводим над $\mathbb{Z}$.

Доказательство. Предположим, что $\Phi_n = fg$, где f и g — многочлены с целыми коэффициентами. Пусть ε — корень многочлена Φ_n. Можно считать, что $f(\varepsilon) = 0$ и многочлен f неприводим. Пусть p — простое число, взаимно простое с n. Тогда ε^p — корень многочлена Φ_n. Мы хотим доказать, что ε^p — корень многочлена f. Предположим, что ε^p не является корнем многочлена f. Тогда можно считать, что $\Phi_n = fgh$, где f и g — неприводимые многочлены со старшим коэффициентом 1 и $f(\varepsilon) = 0$, $g(\varepsilon^p) = 0$.

Многочлен $x^n - 1$ и неприводимый многочлен $f(x)$ имеют общий корень ε, поэтому $x^n - 1$ делится на $f(x)$. Аналогично $x^n - 1$ делится на $g(x)$. А так как многочлены f и g взаимно просты, то $x^n - 1$ делится на их произведение. Следовательно, дискриминант D многочлена $x^n - 1$ делится на результант $R(f, g)$ (см. теорему 3.4 на с. 34). Легко проверить, что $D = \pm n^n$ (см. пример 3.1 на с. 35). Чтобы прийти к противоречию, достаточно показать, что $R(f, g)$ делится на p.

Лемма. Если p — простое число и $f(x)$ — многочлен с целыми коэффициентами, то $\bigl(f(x)\bigr)^p \equiv f(x^p) \pmod{p}$.

Доказательство. Пусть $f(x) = a_n x^n + \ldots + a_1 x + a_0$. Тогда

$$\bigl(f(x)\bigr)^p = \sum_{k_0+\ldots+k_n=p} \frac{p!}{k_0! \cdot \ldots \cdot k_n!}(a_n x^n)^{k_n} \cdot \ldots \cdot (a_0)^{k_0}.$$

Число $p!/(k_0! \cdot \ldots \cdot k_n!)$ не делится на p лишь в том случае, когда одно из чисел $k_0, \ldots, k_n$ равно p. Следовательно,

$$\bigl(f(x)\bigr)^p \equiv (a_n x)^p + \ldots + (a_0)^p \pmod{p}.$$

Воспользовавшись тем, что $a^p \equiv a \pmod{p}$ при всех a, получим требуемое. □

Пусть $y_1 = \varepsilon^p$, y_2, $\ldots$, y_k — корни многочлена g. Согласно лемме $f(\varepsilon^p) \equiv \bigl(f(\varepsilon)\bigr)^p \equiv 0 \pmod{p}$, т. е. $f(y_1) = p\psi(y_1)$, где ψ — многочлен с целыми коэффициентами. Многочлен $f - p\psi$ и неприводимый многочлен g имеют общий корень y_1, поэтому $f - p\psi$ делится на g, а значит, $f(y_i) - p\psi(y_i) = 0$ при всех i. Следовательно,

$$R(f, g) = \pm f(y_1) \cdot \ldots \cdot f(y_k) = \pm p^k \psi(y_1) \cdot \ldots \cdot \psi(y_k).$$

Выражение $\psi(y_1) \cdot \ldots \cdot \psi(y_k)$ представляет собой симметрический многочлен с целыми коэффициентами от корней многочлена g. Таким образом, это выражение — целое число, т. е. $R(f, g)$ делится на p^k.

Итак, если Φ_n делится на неприводимый многочлен f и ε — корень f, то для любого простого числа p, взаимно простого с n, число ε^p тоже будет корнем многочлена f. Теперь уже легко показать, что все корни многочлена Φ_n являются корнями многочлена f, т. е. $f = \pm\Phi_n$. В самом деле, любой корень ω многочлена Φ_n имеет вид ε^m, где $(m, n) = 1$. Запишем m в виде $m = p_1 \cdot \ldots \cdot p_s$, где $p_1, \ldots, p_s$ — простые числа, среди которых могут быть совпадающие. Из условия $(m, n) = 1$ следует, что $(p_i, n) = 1$ при всех i. Поэтому $\varepsilon^{p_1}, \varepsilon^{p_1 p_2}, \ldots, \varepsilon^{p_1 \ldots p_s} = \omega$ — корни многочлена f. □

13.4. Выражение Φ_{mn} через Φ_n

Круговой многочлен $\Phi_{mn}(x)$ во многих случаях можно выразить через $\Phi_n(x)$. Мы ограничимся случаем, когда $m = p$ — простое число.

Теорема 13.5. Пусть p — простое число. Тогда

$$\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p) & \text{при } (n, p) = p; \\ \Phi_n(x^p)/\Phi_n(x) & \text{при } (n, p) = 1. \end{cases}$$

Доказательство. Рассмотрим сначала случай, когда n делится на p. Если ε — примитивный корень степени pn, то $\omega = \varepsilon^p$ — примитивный корень степени n. При этом корню ω соответствуют корни $\varepsilon_1, \ldots, \varepsilon_p$ так, что $(x - \varepsilon_1) \cdot \ldots \cdot (x - \varepsilon_p) = x^p - \omega$. Следовательно,

$$\Phi_{pn}(x) = \prod_{\varepsilon}(x - \varepsilon) = \prod_{\omega = \varepsilon^p}(x^p - \omega) = \Phi_n(x^p).$$

Рассмотрим теперь случай, когда n не делится на p. В этом случае делители pn состоят из делителей n и их произведений на p. Поэтому

$$\Phi_{pn}(x) = \prod_{d|pn}(x^d - 1)^{\mu(pn/d)} = \prod_{d|n}(x^d - 1)^{\mu(pn/d)} \prod_{d|n}(x^{dp} - 1)^{\mu(n/d)}.$$

А так как $\mu(pn/d) = -\mu(n/d)$, то

$$\Phi_{pn}(x) = \prod_{d|n}(x^d - 1)^{-\mu(n/d)} \prod_{d|n}(x^{dp} - 1)^{\mu(n/d)} = \left(\Phi_n(x)\right)^{-1}\Phi_n(x^p). \quad \square$$

Воспользовавшись теоремой 13.5, можно вычислить $\Phi_n(\pm 1)$. Начнем с вычисления $\Phi_n(1)$. Если n делится на p, то согласно теореме 13.5 $\Phi_n(1) = \Phi_{n/p}(1)$. Таким образом, если $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ и $m = p_1 \cdot \ldots \cdot p_k$, то $\Phi_n(1) = \Phi_m(1)$. Остается вычислить $\Phi_m(1)$. Если $m = p$ — простое число, то $\Phi_p(1) = p$. Если же $m = p_1 \cdot \ldots \cdot p_k$, где $k > 1$, то положим $p = p_1$ и $n = m/p$. Согласно теореме 13.5 $\Phi_m(1) = \Phi_n(1)/\Phi_n(1) = 1$.

Итак, если $n > 1$, то

$$\Phi_n(1) = \begin{cases} p & \text{при } n = p^\lambda; \\ 1 & \text{при } n \neq p^\lambda. \end{cases}$$

Вычислим теперь $\Phi_n(-1)$. Возможны следующие варианты.

1) $n > 1$ — нечетное число. Тогда $\Phi_n(-1) = \Phi_{2n}(1) = 1$.

2) $n = 2^k$. Тогда $\Phi_n(x) = (x^n - 1)/(x^{n/2} - 1) = (x^{n/2} + 1)$. Поэтому $\Phi_n(-1) = 0$ при $n = 2$ и $\Phi_n(-1) = 2$ при $n = 2^k$, где $k > 1$.

3) $n = 2m$, где $m > 1$ — нечетное число. В этом случае $\Phi_n(-1) = \Phi_m(1)$. Таким образом, $\Phi_n(-1) = p$, если $m = p^\alpha$, и $\Phi_n(-1) = p$, если в m входит более одного простого делителя.

4) $n = 2^k m$, где $k > 1$ и $m > 1$ — нечетное число. Пусть $m = p_1^{\alpha_1} \cdot \ldots \cdot p_t^{\alpha_t}$. Тогда $\Phi_n(x) = \Phi_{2r}(x^s)$, где $r = p_1 \cdot \ldots \cdot p_t$ и $s = 2^{k-1}p_1^{\alpha_1 - 1} \cdot \ldots \cdot p_t^{\alpha_t - 1}$. Поэтому $\Phi_n(-1) = \Phi_{2r}(1) = 1$.

13.5. Дискриминант кругового многочлена

Представим круговой многочлен $\Phi_n(x)$ в виде

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

Если ε — корень многочлена Φ_n, то

$$\Phi_n'(\varepsilon) = n\varepsilon^{n-1}\prod_{d|n,\, d \neq n}(\varepsilon^d - 1)^{\mu(n/d)}.$$

Поэтому модуль дискриминанта многочлена Φ_n равен

$$\prod_{\varepsilon}\left|\Phi_n'(\varepsilon)\right| = n^{\varphi(n)} \prod_{d|n,\, d\neq n} \prod_{\varepsilon} |1-\varepsilon^d|^{\mu(n/d)}.$$

Ясно, что ε^d — примитивный корень степени n/d, т. е.

$$\prod_{\varepsilon}(1-\varepsilon^d) = \left(\Phi_{n/d}(1)\right)^{\varphi(n)/\varphi(n/d)},$$

поскольку отношение $\deg\Phi_n$ к $\deg\Phi_{n/d}$ равно $\varphi(n)/\varphi(n/d)$.

Значение многочлена $\Phi_{n/d}(x)$ при $x=1$ может быть отлично от 1 лишь в том случае, когда $n/d = p^\lambda$. С другой стороны, $\mu(n/d)\neq 0$ лишь в том случае, когда n/d не делится на квадрат простого числа. Поэтому остаются лишь те значения d, для которых n/d — простое число. Итак,

$$\prod_{\varepsilon}\left|\Phi_n'(\varepsilon)\right| = n^{\varphi(n)}\left(\prod_{p|n} p^{\frac{\varphi(n)}{p-1}}\right)^{-1}.$$

Остается определить знак дискриминанта многочлена Φ_n. Воспользуемся для этого тем, что у многочлена Φ_n нет вещественных корней, а его степень равна $\varphi(n)$. В таком случае знак дискриминанта должен быть равен $(-1)^{\varphi(n)/2}$ (см. теорему 3.5 на с. 34).

13.6. Результант пары круговых многочленов

Начнем с того, что вычислим результант $R(\Phi_n, x^m-1)$. Многочлен x^m-1 делится на $\Phi_1 = x-1$, поэтому $R(\Phi_1, x^m-1)=0$. Предположим, что $n\geqslant 2$. Пусть $d=(n,m)$, $n_1=n/d$, $\xi_1,\xi_2,\ldots$ — первообразные корни степени n, $\eta_1,\eta_2,\ldots$ — первообразные корни степени n_1. Тогда

$$\begin{aligned}R(\Phi_n, x^m-1) &= \prod(\xi_i^m-1) = \prod(1-\xi_i^m) = \\ &= \left(\prod(1-\eta_i)\right)^{\varphi(n)/\varphi(n_1)} = \left(\Phi_{n_1}(1)\right)^{\varphi(n)/\varphi(n_1)}.\end{aligned}$$

Если $n_1=1$, т. е. если m делится на n, то $\Phi_{n_1}(1)=0$, поэтому $R(\Phi_n, x^m-1)=0$. Если же $n_1\neq 1$, то $\Phi_{n_1}(1)=p$ при $n_1=p^\lambda$ и $\Phi_{n_1}(1)=1$ при $n_1\neq p^\lambda$.

Переходя к вычислению $R(\Phi_n,\Phi_m)$, заметим, что это — целое число, являющееся делителем как числа $R(\Phi_n, x^m-1)$, так и числа $R(\Phi_m, x^n-1)$. В самом деле, $x^m-1=\Phi_m(x)f(x)$, где $f(x)$ — многочлен с целыми коэффициентами, поэтому

$$R(\Phi_n, x^m-1) = R(\Phi_n, \Phi_m f) = R(\Phi_n,\Phi_m)R(\Phi_n, f).$$

Кроме того, если $n>m>1$, то

$$R(\Phi_m,\Phi_n) = (-1)^{\varphi(m)\varphi(n)}R(\Phi_n,\Phi_m) = R(\Phi_n,\Phi_m)$$

и $R(\Phi_m,\Phi_n)>0$. Последнее свойство можно доказать, например, так. Ясно, что

$$0\neq R(\Phi_n, x^m-1) = \prod_{d|m} R(\Phi_n,\Phi_d),$$

поэтому

$$R(\Phi_n,\Phi_m) = \prod_{d|m} R(\Phi_n, x^d-1)^{\mu(m/d)} > 0.$$

Если m не делится на n и n не делится на m, то числа m/d и n/d, где $d=(m,n)$, не равны 1 и взаимно просты. Поэтому числа $R(\Phi_n, x^m-1)$ и $R(\Phi_m, x^n-1)$ взаимно просты, а значит, $R(\Phi_n,\Phi_m)=1$.

Пусть теперь для определенности m делится на n. Если $m=n$, то $R(\Phi_n,\Phi_m)=0$. Если $m/n\neq p^\lambda$, то $R(\Phi_m, x^n-1)=1$, поэтому $R(\Phi_n,\Phi_m)=1$. Остается рассмотреть случай $m/n=p^\lambda$. Ясно, что

$$R(\Phi_n,\Phi_m) = \prod_{\delta|n} R(\Phi_m, x^\delta-1)^{\mu(n/\delta)}.$$

В правой части все множители равны 1, за исключением тех, для которых $m/\delta = p^a$.

Если $(n,p)=1$, то неединичный множитель возникает лишь при $\delta = n$. В этом случае

$$R(\Phi_n,\Phi_m) = R(\Phi_m, x^n-1) = p^{\varphi(m)/\varphi(m/n)} = p^{\varphi(n)}.$$

Если n делится на p, то неединичные множители возникают лишь при $\delta=n$ и при $\delta=n/p$. В этом случае

$$R(\Phi_n,\Phi_m) = \frac{R(\Phi_m, x^n-1)}{R(\Phi_m, x^{n/p}-1)} = p^a,$$

где

$$a = \frac{\varphi(m)}{\varphi(m/n)} - \frac{\varphi(m)}{\varphi(mp/n)} = \varphi(m)\left(\frac{1}{p^{\lambda-1}(p-1)} - \frac{1}{p^{\lambda}(p-1)}\right) = \frac{\varphi(m)}{p^{\lambda}} = \varphi(n).$$

Итак, если $m \geqslant n$, то

$$R(\Phi_n, \Phi_m) = \begin{cases} 0 & \text{при } m = n; \\ p^{\varphi(n)} & \text{при } m = np^{\lambda}; \\ 1 & \text{в остальных случаях.} \end{cases}$$

13.7. Коэффициенты круговых многочленов

Примеры многочленов $\Phi_n(x)$ при малых n показывают, что их коэффициенты равны 0 и ± 1. Но в работе [Suz] доказано, что любое целое число служит коэффициентом некоторого кругового многочлена. Это доказательство основано на следующем вспомогательном утверждении.

Лемма. Для любого натурального $t \geqslant 3$ существуют такие простые числа $p_1 < p_2 < \ldots < p_t$, что $p_1 + p_2 > p_t$.

Доказательство. Фиксируем $t \geqslant 3$. Предположим, что для любого набора простых чисел $p_1 < p_2 < \ldots < p_t$ выполняется неравенство $p_1 + p_2 \leqslant p_t$. В таком случае $2p_1 < p_t$, поэтому между 2^{k-1} и 2^k заключено менее t простых чисел. Это означает, что $\pi(2^k) < kt$ (здесь $\pi(s)$ — количество простых чисел между 1 и s).

Согласно теореме Чебышева (см. [ГНШ], [Дэ] или [Ч]) $\pi(x) > cx/\ln x$, где c — положительная константа. Поэтому $c2^k/\ln 2^k < kt$, т. е. $c2^k < k^2 t \ln 2$. При достаточно больших k это неравенство выполняться не будет. □

Пусть $t \geqslant 3$ — нечетное целое число. Выберем простые числа $p_1 < p_2 < \ldots < p_t$ так, что $p_1 + p_2 > p_t$. Положим $p = p_t$. Рассмотрим многочлен $\Phi_n(x)$ по модулю x^{p+1}. При нечетном t

$$\Phi_{p_1\ldots p_t} = \frac{(x^{p_1}-1)\cdot\ldots\cdot(x^{p_t}-1)}{x-1} \cdot \frac{\prod(x^{p_ip_jp_k}-1)}{\prod(x^{p_ip_j}-1)} \cdot \ldots$$

Но $x^{p_ip_j} \equiv 0 \pmod{x^{p+1}}$, $x^{p_ip_jp_k} \equiv 0 \pmod{x^{p+1}}$ и т. д. Поэтому

$$\Phi_{p_1\ldots p_t} \equiv \pm\frac{(1-x^{p_1})\cdot\ldots\cdot(1-x^{p_t})}{1-x} \pmod{x^{p+1}}.$$

Равенство $\Phi_{p_1\ldots p_t}(0) = 1$ позволяет выбрать знак плюс. Из неравенства $p_i + p_j \geqslant p_1 + p_2 > p_t = p$ следует, что

$$(1-x^{p_1})\cdot\ldots\cdot(1-x^{p_t}) \equiv (1 - x^{p_1} - \ldots - x^{p_t}) \pmod{x^{p+1}}.$$

Ясно также, что $(1-x)^{-1} \equiv (1 + x + \ldots + x^p) \pmod{x^{p+1}}$. Поэтому

$$\Phi_{p_1\ldots p_t} \equiv (1 + x + \ldots + x^p)(1 - x^{p_1} - \ldots - x^{p_t}) \pmod{x^{p+1}}.$$

Среди мономов $x^{p_i}, x^{p_i+1}, \ldots, x^{p_i+p}$ моном x^p встречается при всех i, а мономы x^{p-1} и x^{p-2} встречаются при всех $i \neq t$. Поэтому коэффициент при x^p у многочлена $\Phi_{p_1\ldots p_t}$ равен $-t+1$, а коэффициент при x^{p-2} равен $-(t-1)+1 = -t+2$.

Когда t пробегает все нечетные числа начиная с 3, числа $-t+1$ и $-t+2$ пробегают все отрицательные числа.

Чтобы получить в качестве коэффициентов круговых многочленов все положительные числа, рассмотрим многочлен $\Phi_{2p_1\ldots p_t}$, где $p_1 \geqslant 3$ и $p_1 + p_2 > p_t$. Число $n = p_1\cdot\ldots\cdot p_t$ нечетно, поэтому $\Phi_{2n}(x) = \Phi_n(-x)$. Это означает, что у многочленов Φ_{2n} и Φ_n коэффициенты как при x^p, так и при x^{p-2} отличаются знаком, т. е. у многочлена $\Phi_{2p_1\ldots p_t}$ коэффициенты при x^p и x^{p-2} равны $t-1$ и $t-2$, соответственно.

13.8. Теорема Веддерберна

Одним из наиболее интересных приложений круговых многочленов является доказательство теоремы Веддерберна о коммутативности конечного тела. Такое доказательство предложил Витт [Wt].

Телом называют кольцо, в котором уравнения $ax = b$ и $xa = b$ однозначно разрешимы при всех $a \neq 0$.

Теорема 13.6 (Веддерберн). Конечное ассоциативное тело R коммутативно, т. е. является полем.

Доказательство. Пусть e_1 и e_2 — решения уравнений $ax = a$ и $xa = a$, соответственно. Тогда $ae_1a = a^2 = ae_2a$, поэтому $ae_1 = ae_2$ и $e_1 = e_2 = e$. Покажем, что $be = b$ для любого b. В самом деле, пусть $xa = b$. Тогда $be = xae = xa = b$. Аналогично $eb = b$.

Таким образом, тело R содержит единицу 1. Рассмотрим поле F_p, порожденное элементом $1 \in R$. Тело R является линейным пространством над полем F_p. Пусть r — размерность этого пространства. Тогда R состоит из p^r элементов. Пусть Z — центр тела R, т. е. множество тех элементов R, которые коммутируют со всеми элементами R. Ясно, что Z — поле, содержащее F_p. Поэтому Z состоит из $q = p^s$ элементов. Тело R является также и линейным пространством над полем Z. Если размерность R над Z равна t, то R состоит из q^t элементов. Таким образом, $p^r = q^t = p^{st}$. Мы хотим доказать, что $R = Z$, т. е. $t = 1$.

Для любого элемента $x \in R$ рассмотрим его нормализатор $N_x = \{y \in R \,|\, xy = yx\}$. Ясно, что N_x — подтело в R, содержащее Z. С одной стороны, тело N_x является линейным пространством над полем Z, поэтому N_x состоит из q^d элементов. С другой стороны, тело R является линейным пространством над телом N_x, поэтому $q^t = (q^d)^k = q^{dk}$, т. е. $d \,|\, t$.

В мультипликативной группе R^* для каждого элемента x рассмотрим его орбиту $O_x = \{yxy^{-1} \,|\, y \in R^*\}$. Ясно, что O_x состоит из

$$|O_x| = |R^*|/|N_x^*| = (q^t - 1)/(q^d - 1)$$

элементов. Орбиты разных элементов либо совпадают, либо не пересекаются, поэтому R^* разбивается на орбиты, причем орбита любого элемента Z^* состоит из одного элемента. Следовательно,

$$q^t - 1 = q - 1 + \sum (q^t - 1)/(q^d - 1), \qquad (1)$$

где суммирование ведется по некоторым делителям d числа t. При этом $d < t$ (равенство $d = t$ соответствует тому, что $x \in Z^*$; такие элементы выделены в качестве первого слагаемого).

С помощью кругового многочлена $\Phi_t(x)$ мы покажем, что равенство (1) возможно лишь при $t = 1$. Многочлен $x^t - 1$ делится нацело на $\Phi_t(x)$. Более того, если $d \,|\, t$ и $d < t$, то многочлен $(x^t - 1)/(x^d - 1)$ тоже делится нацело на $\Phi_t(x)$, так как в этом случае многочлены $x^d - 1$ и $\Phi_t(x)$ не имеют общих корней. В частности, числа $q^t - 1$ и $(q^t - 1)/(q^d - 1)$ делятся на $\Phi_t(q)$. Соотношение (1) показывает, что тогда $q - 1$ делится на $\Phi_t(q)$. С другой стороны, $|\Phi_t(q)| = \prod |q - \varepsilon_i| > q - 1$, так как $|\varepsilon_i| = 1$ и $\varepsilon_i \neq 1$. □

13.9. Многочлены, неприводимые по модулю p

С помощью формулы обращения Мёбиуса можно получить выражение для числа неприводимых многочленов степени n со старшим коэффициентом 1 над полем $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Докажем сначала следующее утверждение.

Теорема 13.7. Пусть $F_d(x)$ — произведение всех неприводимых многочленов степени d со старшим коэффициентом 1 над полем $\mathbb{F}_p$. Тогда

$$x^{p^n} - x = \prod_{d|n} F_d(x).$$

Доказательство. Многочлен $x^{p^n} - x$ взаимно прост со своей производной $p^n x^{p^n - 1} - 1 = -1$, поэтому у него нет кратных корней. Таким образом, достаточно доказать, что если $f(x)$ — неприводимый многочлен степени d со старшим коэффициентом 1, то $f(x)$ делит $x^{p^n} - x$ тогда и только тогда, когда d делит n.

Пусть α — корень многочлена f и $K = \mathbb{F}_p(\alpha)$ — расширение степени d поля $\mathbb{F}_p$. Оно состоит из p^d элементов и все его элементы удовлетворяют уравнению $x^{p^d} - x = 0$. В самом деле, мультипликативная группа поля $\mathbb{F}_p$ имеет порядок $p^d - 1$, поэтому любой ненулевой элемент $x \in \mathbb{F}_p$ удовлетворяет уравнению $x^{p^d - 1} = 1$.

Лемма. а) Над произвольным полем многочлен $x^n - 1$ делит $x^m - 1$ тогда и только тогда, когда n делит m.

б) Если $a \geqslant 2$ — натуральное число, то $a^n - 1$ делит $a^m - 1$ тогда и только тогда, когда n делит m.

Доказательство. а) Пусть $m = qn + r$, где $0 \leqslant r < n$. Тогда

$$\frac{x^m - 1}{x^n - 1} = x^r \frac{x^{qn} - 1}{x^n - 1} + \frac{x^r - 1}{x^n - 1}.$$

Многочлен $x^{qn} - 1$ делится на $x^n - 1$. Поэтому $x^m - 1$ делится на $x^n - 1$ тогда и только тогда, когда $x^r - 1$ делится на $x^n - 1$. Но $r < n$, поэтому $x^r - 1$ делится на $x^n - 1$ лишь при $r = 0$.

б) Доказывается аналогично. □

Предположим сначала, что d делит n. Тогда $p^d - 1$ делит $p^n - 1$, а значит, $x^{p^d} - x$ делит $x^{p^n} - x$. Корень α неприводимого многочлена $f(x)$ является также и корнем уравнения $x^{p^d} = x$, поэтому $f(x)$ делит $x^{p^d} - x$.

Предположим теперь, что $f(x)$ делит $x^{p^n} - x$. Тогда $\alpha^{p^n} - \alpha = 0$. Если $b_1\alpha^{d-1} + b_2\alpha^{d-2} + \ldots + b_d$ — произвольный элемент поля K, то

$$(b_1\alpha^{d-1} + \ldots + b_d)^p = b_1(\alpha^{p^n})^{d-1} + \ldots + b_d = b_1\alpha^{d-1} + \ldots + b_d.$$

Поэтому любой элемент поля K удовлетворяет уравнению $x^{p^n} = x$, т. е. $x^{p^n} - x$ делится на $x^{p^d} - x$. Следовательно, n делится на d. □

Пусть N_d — число неприводимых многочленов степени d со старшим коэффициентом 1 над полем $\mathbb{F}_p$. Тогда степень многочлена F_d равна dN_d, поэтому

$$p^n = \sum_{d|n} dN_d.$$

Применив формулу обращения Мёбиуса, получим

$$N_n = \frac{1}{n}\sum_{d|n} \mu(n/d)p^d.$$

В частности, $N_n \neq 0$, так как сумма $\sum\limits_{d|n} \mu(n/d)p^d$ имеет вид $p^{d_1} \pm \pm p^{d_2} \pm \ldots \pm p^{d_k}$, где числа d_i попарно различны.

14. Многочлены Чебышева

14.1. Определение и основные свойства

Многочлены Чебышева $T_n(x)$ являются одним из наиболее замечательных семейств многочленов. Они часто встречаются во многих областях математики, от теории аппроксимации до теории чисел и топологии трехмерных многообразий. Мы обсудим некоторые наиболее простые, но весьма важные свойства многочленов Чебышева.

Определение многочленов Чебышева основано на том, что $\cos n\varphi$ полиномиально выражается через $\cos\varphi$, т. е. существует такой многочлен $T_n(x)$, что $T_n(x) = \cos n\varphi$ при $x = \cos\varphi$. В самом деле, формула

$$\cos(n+1)\varphi + \cos(n-1)\varphi = 2\cos\varphi\cos n\varphi$$

показывает, что многочлены $T_n(x)$, определенные рекуррентным соотношением

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x)$$

и начальными условиями $T_0(x) = 1$ и $T_1(x) = x$, обладают нужным свойством. Эти многочлены $T_n(x)$ называют *многочленами Чебышева*.

Непосредственно из того, что $T_n(x) = \cos n\varphi$ при $x = \cos\varphi$, следует, что $|T_n(x)| \leqslant 1$ при $x \leqslant 1$. А из рекуррентного соотношения следует, что $T_n(x) = 2^{n-1}x^n + a_1x^{n-1} + \ldots + a_n$, где $a_1, \ldots, a_n$ — целые числа.

Наиболее важное свойство многочленов Чебышева было обнаружено самим Чебышевым. Оно заключается в следующем.

Теорема 14.1. Пусть $P_n(x) = x^n + \ldots$ — многочлен степени n со старшим коэффициентом 1, причем $|P_n(x)| \leqslant \frac{1}{2^{n-1}}$ при $|x| \leqslant 1$. Тогда $P_n(x) = \frac{1}{2^{n-1}}T_n(x)$. (Иными словами, многочлен $\frac{1}{2^{n-1}}T_n(x)$ — наименее уклоняющийся от нуля на интервале $[-1, 1]$ многочлен степени n со старшим коэффициентом 1.)

Доказательство. Мы воспользуемся лишь одним свойством многочлена $T_n(x) = 2^{n-1}x^n + \ldots$, а именно тем, что $T_n\big(\cos(k\pi/n)\big) = \cos k\pi = (-1)^k$ при $k = 0, 1, \ldots, n$. Рассмотрим многочлен $Q(x) = \frac{1}{2^{n-1}}T_n(x) - P_n(x)$. Его степень не превосходит $n-1$, поскольку старшие члены многочленов $\frac{1}{2^{n-1}}T_n(x)$ и $P_n(x)$ равны. Из того, что $|P_n(x)| \leqslant \frac{1}{2^{n-1}}$ при $|x| \leqslant 1$, следует, что в точке $x_k = \cos(k\pi/n)$ знак числа $Q(x_k)$ совпада-

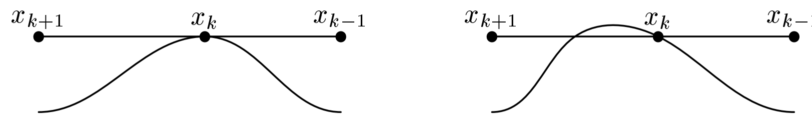

Рис. 5

ет со знаком числа $T_n(x_k)$. Таким образом, в концах каждого отрезка $[x_{k+1}, x_k]$ многочлен $Q(x)$ принимает значения разного знака, поэтому у многочлена $Q(x)$ на этом отрезке есть корень. Чуть более аккуратные рассуждения нужны в том случае, когда $Q(x_k) = 0$. В этом случае либо x_k — двукратный корень, либо внутри одного из отрезков $[x_{k+1}, x_k]$ и $[x_k, x_{k-1}]$ есть еще один корень. Это следует из того, что в точках x_{k+1} и x_{k-1} многочлен $Q(x)$ принимает значения одного знака (рис. 5).

Количество отрезков $[x_{k+1}, x_k]$ равно n, поэтому многочлен $Q(x)$ имеет по крайней мере n корней. Для многочлена степени не более $n-1$ это означает, что он тождественно равен нулю, т. е. $P_n(x) = \frac{1}{2^{n-1}}T_n(x)$. □

Если $z = \cos\varphi + i\sin\varphi$, то $z + z^{-1} = 2\cos\varphi$ и $z^n + z^{-n} = 2\cos n\varphi$.