УДК 511.1

Д.Исмоилов

*Инновационный евразийский университет, Павлодар*
*(E-mail: i.Dodojon@rambler.ru)*

# Многочлены деления круга, проблема Фейта-Томпсона и некоторые применения к теории делимости

В статье предложен один из способов решения гипотезы Фейта-Томпсона из теории групп. На основании арифметической трактовки многочленов деления круга доказаны некоторые утверждения относительно представления многочленов, зависящих от круговых многочленов. На основании полученных утверждений выводится ряд результатов, относящихся к теории делимости в полугруппе натуральных чисел.

*Ключевые слова:* теория групп, многочлены, теория делимости, полугруппа.

## *I О многочленах деления круга*

В этом пункте приведем определения, понятия и соотношения, необходимые для доказательства основных результатов работы.

*Определение.* Многочленом деления круга порядка $n$ называется многочлен

$$f_n(x) = (x-\varepsilon_1)(x-\varepsilon_2)...(x-\varepsilon_{\varphi(n)}), \tag{1}$$

где $\varepsilon_1, \varepsilon_2, \varepsilon_{\varphi(n)}$ — все первообразные корни степени $n$ из единицы;

$$\varepsilon_k = \exp\left(2\pi i \frac{k}{n}\right);\ k = 1,2,\cdots,n;\ k = 1,2,\cdots,n;\ (k,n) = 1, \tag{2}$$

где $\varphi(n)$ — функция Эйлера. Заметим, что $\varepsilon_k^m \neq 1$ при всех $1 \le m < n$.

Согласно определению основных симметрических многочленов $f(x) = x^n - 1$ является многочленом с комплексными коэффициентами. В действительности же коэффициенты $f(x)$ — целые числа. Вопрос разложения многочлена $f(x) = x^n - 1$ на множители в общем случае осуществляется на основании известной формулы обращения

$$f(n) = \prod_{d/n} g(d) \Leftrightarrow g(n) = \prod_{d/n} (x^d - 1)^{\mu(n/d)}, \tag{3}$$

где $\mu(n)$ — функция Мёбиуса (мультипликативный аналог формулы обращения Мёбиуса). Отсюда непосредственно выводится формула

$$x^n - 1 = \prod_{d/n} f_d(x) \Leftrightarrow f_n(x) = \prod_{d/n} (x^d - 1)^{\mu(n/d)}. \tag{4}$$

*Следствие.* Если $n$ — простое, то существует единственное разложение

$$f(x) = x^n - 1 = (x-1) f_n(x), \tag{5}$$

где

$$f_n(x) = 1 + x + x^2 + ... + x^{n-1};\ f_0(x) = 0; f_1(x) = 1. \tag{6}$$

Если же $n$ — составное, то возможны и другие разложения $f(x)$ на сомножители. Пусть $d/n$, $1 \le d \le n$, тогда имеет место разложение

$$f(x) = (x^d)^m - 1 = (x^d - 1)(x^{d(m-1)} + x^{d(m-2)} + ... + x^d + 1), \tag{7}$$

где $d$ пробегает все натуральные делители числа $n$. Как известно, число различных делителей $n$ равно $\tau(n)$, тем самым будем иметь $\tau(n)$ различных разложений $f(x) = x^n - 1$ [1]. В общем случае имеет место мультипликативная формула

$$x^n - 1 = \prod_{d/n} f_d(x);\ \ x^n - 1 = f_n(x) \cdot g_n(x), \tag{8}$$

где $g_n(x)$ — произведение многочленов $f_d(x)$ по всем собственным делителям $d$ числа $n$.

Проверка первого равенства (8) проводится следующим образом. Рассмотрим разложение с учетом следствия из основной теоремы алгебры:

$$x^n - 1 = (x - \varepsilon_0)(x - \varepsilon_1)...(x - \varepsilon_{n-1}) = \prod_{k=0}^{n-1}(x - \varepsilon_k),\ \varepsilon_0 = 1. \tag{9}$$

Далее сгруппируем все множители вида $x - \varepsilon_k$, для которых $(k,d) = 1$, т.е. по всем первообразным корням фиксированной степени *d*, *d/n*. Таким образом, получим $f_d(x)$, поскольку каждый множитель $(x - \varepsilon_k)$ входит в правой части (9) ровно в один из многочленов $f_d(x)$. Как было отмечено, если *n* — простое, то существует единственное разложение (5) с равенством (6). Теперь, согласно свойствам функции Мёбиуса, из равенства (3) следует равенство (4), так как левая часть формулы (4) представляет равенство (8), тем самым для нахождения многочленов $f_d(x)$ будем иметь вычислительную формулу

$$f_n(x) = \prod_{d/n}(x^d - 1)^{\mu(n/d)} \tag{10}$$

для выписывания явного вида многочленов деления круга при $n = p$ (где *p* — простое число), и имеют место равенства

$$P_p(q) = (q - \varepsilon_1)(q - \varepsilon_2)...(q - \varepsilon_{p-1}) = \frac{q^p - 1}{q - 1}; \tag{11}$$

$$P_q(p) = (p - \eta_1)(p - \eta_2)...(p - \eta_{q-1}) = \frac{p^q - 1}{p - 1}, \tag{12}$$

где $\varepsilon_k; \eta_r$ — соответственно первообразные корни *p*- и *q*-ой степени из единицы; *p* и *q* — различные простые числа. Теперь заметим, что многочлены (11) и (12), соответственно, являются многочленами деления круга. Каждый из них многочлен корней $p$ и $q$-ой степени из единицы соответственно, и вместе с единицей они делят единичный круг комплексной плоскости на *p* и *q* равных частей. Кроме того, каждый из этих многочленов является неприводимым над полем рациональных чисел *Q*.

Следует отметить, что многочлены деления круга сами не раскладываются дальше на множители с целыми коэффициентами [2]. Если $P_p(x)$ — многочлен деления круга ( $p$ — простое число), то известно, что

$$P_p(x) = \frac{x^p - 1}{x - 1} = 1 + x + x^2 + ... + x^{p-1}. \tag{13}$$

Корнями этого многочлена служат корни $p$-ой степени из единицы, отличные от самой единицы. Так как эти корни $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{p-1}$ (здесь значение функции Эйлера $\varphi(p) = p - 1$) вместе с единицей делят единичный круг комплексной плоскости на $p$-равных частей (величина раствора сектора деления $\theta = 2\pi/p$), то отсюда и название «многочлен деления круга». К этому многочлену не может быть непосредственно применен критерий Эйзенштейна о неприводимости над полем *Q* [3]. Пусть дан многочлен $h(x) = a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n$ с целыми коэффициентами. Если хотя бы одним способом можно подобрать простое число *p*, удовлетворяющее следующим требованиям:

1) старший коэффициент $a_0$ не делится на *p*;

2) все остальные коэффициенты делятся на *p*;

3) свободный член, делясь на p, не делится на $p^2$,

то многочлен *h* (*x*) неприводим над полем рациональных чисел *Q* [1].

В равенстве (13) произведем замену $x = y + 1$, тогда получим

$$P_p(y+1) = g(y) = \frac{(y+1)^p - 1}{(y+1) - 1} = \frac{1}{y}[y^p + C_p^1 y^{p-1} + C_p^2 y^{p-2} + ... + py] = y^{p-1} + py^{p-2} + C_p^2 \cdot y^{p-3} + ... + p.$$

Коэффициенты $C_p^k$ многочлена кратны *p* при всех $1 \le \kappa < p$, причем старший коэффициент равен 1, а свободный член не делится на $p^2$. Следовательно, многочлен *g* (*y*) неприводим и тем самым $P_p(x)$ неприводим.

*II Функция Мёбиуса и ее применение*

Пусть $\mu(n)$ — функция Мёбиуса. Определим функцию Мёбиуса следующим образом: если $n = p_1^{\alpha_1}...p_r^{\alpha_r}$ — каноническое представление числа $n$, то положим

$$\mu(n) = (-1)^r C_1^{\alpha_1}...C_1^{\alpha_r}, \tag{14}$$

где $C_m^k$ — биноминальные коэффициенты. Классическое определение отличается от равенства (14) [1]. Согласно (14) легко заметить, что

$$\mu(1) = 1, \mu(p) = -1, \mu(p^\alpha) = 0, \alpha \geq 2;$$

$$\mu(p_1 p_2 ... p_r) = (-1)^r = \begin{cases} 1, & r \text{ — четное;} \\ -1, & r \text{ — нечетное.} \end{cases}$$

Формула (14) удобна для последующих обобщений функции Мёбиуса, а именно:

$$\mu_k(n) = (-1)^r C_k^{\alpha_1}...C_k^{\alpha_r}; k = 2,3,\cdots$$

Далее, согласно первым примерам по равенству (10) (для начальных значений $n$), казалось бы, можно предположить, что коэффициенты многочленов деления круга всегда равны 0, 1, -1 (их будем называть *многочленами первого класса*). Однако существуют такие $n$, при которых коэффициенты многочленов деления круга отличны от 0, 1, -1 (их будем называть *многочленами второго класса*).

Такой пример указан в [4], для значений $n = 105$. Для полноты картины приведём этот пример. Следуя равенству (10), получим:

$$f_{105}(x) = (x-1)^{\mu(105)}(x^3-1)^{\mu(35)}(x^5-1)^{\mu(21)} \times$$
$$\times (x^7-1)^{\mu(15)}(x^{105}-1)^{\mu(1)}(x^{15}-1)^{\mu(7)}(x^{21}-1)^{\mu(5)}(x^{35}-1)^{\mu(3)}.$$

Отсюда после некоторых стандартных упрощений получим

$$f_{105}(x) = \frac{(x^{105}-1)(x^3-1)(x^5-1)(x^7-1)}{(x-1)(x^{15}-1)(x^{21}-1)(x^{35}-1)} =$$
$$= x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36} + x^{35} +$$
$$+ x^{34} + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} +$$
$$+ x^{14} + x^{13} + + x^{12} - x^9 - x^8 - 2x^7 - x^6 - x^5 + x^2 + x + 1.$$

Возникают интересные арифметические задачи:

− *определить, для каких n коэффициенты многочленов деления круга отличны от* 0, 1, -1;

− *найти следующее число n* >105, *для которого* $f_n(x)$ *является многочленом второго класса;*

− *в отрезке натурального ряда* $[n, n+m]$ *оценить количество многочленов второго класса.*

Докажем следующее утверждение (решение гипотезы Фейта-Томпсона [2]).

*Теорема 1.* При любых различных простых $p$ и $q$ многочлены $P_p(q)$ и $P_q(p)$ являются взаимно простыми.

*Доказательство.* Известно, что для функции Мёбиуса $\mu(n)$ от любого натурального числа $n$ верно равенство

$$\mu(n) = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} e^{2\pi i \frac{k}{n}} = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} \xi_k. \tag{15}$$

Многочлены (11) и (12) взаимно просты тогда и только тогда, когда у них в правых частях отсутствуют общие комплексные корни. Покажем, что все множители в произведениях (11) и (12) различны для $p \neq q$. Рассуждения будем вести от противного. Пусть некоторый первообразный корень $\varepsilon_k$ совпадает с некоторым первообразным корнем $\eta_r$, т.е. $\varepsilon_k = \eta_r$. Просуммируем обе части последнего равенства по всем целым $k = 1,2,\cdots,p-1$ и $r = 1,2,\cdots,q-1$, получим

$$\sum_{r=1}^{q-1}\sum_{k=1}^{p-1}\varepsilon_k = \sum_{k=1}^{p-1}\sum_{r=1}^{q-1}\eta_r. \tag{16}$$

Отсюда, согласно (15) и (16), получим, что простые числа $p$ и $q$ равны между собой вопреки условию нашей теоремы. Утверждение доказано, тем самым получено и доказательство гипотезы.

*Замечания:*

1. Пусть в равенствах (11) и (12) $p$ и $q$ — бесквадратные числа. Тогда, используя метод доказательства теоремы, можно установить, что если $m \neq n,$ то $(f_n(m), f_m(n)) = 1.$

2. а) Если $f_n(a) = \dfrac{a^n - 1}{a - 1}$ и $d/(a-1),$ то можно доказать, что число $(f_n(a) - n)$ также кратно $d,$ а следовательно, верна эквивалентность $d/f_n(a) \Leftrightarrow d/n$. Отсюда можно вывести

$$\text{b) } (f_n(a), a-1) = (a-1, n).$$

Доказательства утверждений пунктов α) и β) в §6 [2].

c) На основании пунктов α) и β) можно вывести еще одно доказательство гипотезы Фейта-Томпсона.

3. Пусть $\forall a \in Z_+,\ a \geq 2$ и $f_n(a,d) = \dfrac{a^n - 1}{a^d - 1},$ $d/n,$ тогда $\left( f_{\frac{n}{d}}(a), f_{\frac{m}{d}}(a) \right) = 1,\ d = (m,n) = \text{НОД}\{m,n\}.$

*III Об одном применении круговых многочленов к теории делимости*

Ниже сформулируем некоторые выводы, относящиеся к теории делимости. Имеет место

*Теорема 2.* Пусть $2 \leq g \in Z_+$ и $\forall n \in Z_+,$ и пусть последовательность многочленов $D_n(g)$ определяется равенством

$$D_n(g) = g^n + (g-1)\cdot(g-2)\cdot n - 1. \tag{17}$$

Тогда справедлива формула $D_n(g) = (g-1)^2 \cdot \left[ \sum_{k=0}^{n-1} f_k(g) + n \right].$

*Доказательство.* Очевидно, что при $n = 1$ $D_n(g) = (g-1)^2.$ Пусть $n > 1,$ тогда по формуле (5) имеем $g^n - 1 = (g-1)^2 \cdot \sum_{k=1}^{n-1} f_k(g) + (g-1)\cdot n.$ Прибавляя к обеим частям последнего равенства выражение $(g-1)\cdot(g-2)\cdot n,$ получим наше утверждение. Теорема 2 имеет многочисленные применения к теории делимости. Приведём примеры:

1) $D_n(g^m) \vdots (g^m - 1)^2 \Rightarrow D_n(g^m) \vdots [(g-1)\cdot f_m(g)]^2;$

2) $D_n(g^m) \vdots [f_m(g)]^2,\ m \in Z_+;$

3) для любых целых $m \geq 0; n \geq 1$ имеет место признак делимости $D_n(F_m) \vdots 2^{2^{m+1}},$ где $F_m = 2^{2^m} + 1$ — числа Ферма.

Рассмотрим ещё одно утверждение в связи с круговыми многочленами.

*Теорема 3.* Пусть $g - 1 \geq 0$ и $\forall n \in Z_+.$ Пусть многочлен $D_n(g;k)$ определён равенством

$$D_n(g;k) = P_n(g) \cdot \{g^n + 2\sqrt{g-1}\cdot k - 1\} + k^2;\ k \in Z.$$

Тогда справедливо равенство $D_n(g;k) = \left[ \sqrt{g-1} \cdot f_n(g) + k \right]^2.$ В частности, справедливо равенство

$$D_n(m^2+1;k) = \left[ m \cdot f_n(m^2+1) + k \right]^2.$$

*Доказательство.* В соответствии с определением $f_n(g)$ и условием $g - 1 \geq 0$ имеем: в частности, также и для $g = m^2 + 1,$

$$f_n(g) = \frac{(g^n - 1)}{g - 1} = f_n(m^2+1) = \frac{(m^2+1)^n - 1}{m^2}.$$

Следовательно, проведя стандартные преобразования, получим равенства

$$D_n(g;k) = \frac{(g^n - 1)\cdot\left[ g^n + (2\sqrt{g-1}\cdot k - 1) + (\sqrt{g-1}\cdot k)^2 \right]}{g-1} =$$

$$= \left\{ \frac{g^n + \sqrt{g-1}\cdot k - 1}{\sqrt{g-1}} \right\}^2 = \left\{ \sqrt{g-1}\cdot f_n(g) + k \right\}^2.$$

Основное утверждение доказано. В частности, для случаев $g-1=m^2$ получим

$$D_n(m^2+1;k)=\left\{\frac{(m^2+1)^n+m\cdot k-1}{m}\right\}^2=\left\{\frac{m[(m^2+1)^n-1]}{m^2}+k\right\}^2.$$

Таким образом, доказано и равенство $D_n(m^2+1;k)=[m\cdot f_n(m^2+1)+k]^2$. Очевидно, что указанный результат справедлив и для $g-1=m^{2l};\ m\in Z;\ m\neq 0;\ l\in Z_+$.

*Замечание.* Доказанное утверждение является источником многих интересных следствий, относящихся к теории делимости. К примеру:

$$D_1(m^2+1;k)=(m+k)^2\Rightarrow D_1(m^2+1;0)=m^2;\forall m\in Z_+;$$
$$D_1(m^2+1;f_n(m^2+1)-m)=[f_n(m^2+1)]^2;$$
$$D_1(1;k)=k^2;\forall k\in Z;$$
$$D_2(m^2+1;3m^2+m+1)=(m+1)^2$$

и т.д. Очевидно, что аналогичные утверждения также справедливы при $n=p$ (где $p$ — простое число), тогда $f_n(x)$ заменяется всюду на $P_p(x)$:

$$D_1(m^2+1;P_p(m^2+1)-m)=[P_p(m^2+1)]^2;$$

где $p$ — простое число. Отметим, что в равенстве $D_n(g;k)=\left[\sqrt{g-1}\cdot f_n(g)+k\right]^2$ параметры $g\geq 2$ и $k$ — произвольные числа, а это обстоятельство позволяет нам расширить круг применения полученных результатов.

*Следствия.* Пусть $\sqrt{g-1}=m=[\sqrt{p}];\ k=\{\sqrt{p}\}$, где $p$ — простое число. Тогда справедлива формула $D_1(g,k)=([\sqrt{p}]+\{\sqrt{p}\})^2=(\sqrt{p})^2=p$, где $[\alpha]$ — целая часть, а $\{\alpha\}$ — дробная часть числа $\alpha$. Или в случаях $\sqrt{g-1}=m=[\sqrt{p}];\ k=-([\sqrt{p}])^3-[\sqrt{p}]+\{\sqrt{p}\}$ справедлива другая формула:

$$D_2(g,k)=\left([\sqrt{p}]+\{\sqrt{p}\}\right)^2=(\sqrt{p})^2=p.$$

Отметим, что аналогичную теорию легко развивать для случая разности целых $a^n-b^n$:

$$a^n-b^n=(a-b)\cdot F_n(a,b);\ F_n(a,b)=\sum_{k=1}^{n}a^{n-k}\cdot b^k.$$

Для этого многочлен $x^n-1$ представим в многочлен вида $x^n-y^n$, подстановкой $x\to x/y$ и, умножая результат на $y^n$, получим равенства

$$F_n(x,y)=x^{\varphi(n)}\cdot f_n\left(x/y\right),\ x^n-y^n=\prod_{d/n}F_d(x,y);\ x^n-y^n=F_n(x,y)\cdot G_n(x,y),$$

где $G_n(x,y)$ — произведение многочленов $F_d(x,y)$ по всем собственным делителям $d$ числа $n$

$$G_n(x,y)=x^{n-\varphi(n)}\cdot g_n(x/y).$$

Можно доказать:

1) Если $a-b$ кратно $m$, то число $F_n(a,b)-n\cdot a^{n-1}$ тоже кратно $m$, задача 6.41 [5].

2) $F_n(a,b)>n$ для всех $n$, за исключением $n=6;\ a=2;\ b=1$ [1].

3) Для любого натурального числа $n>1$ существует бесконечно много простых чисел, дающих остаток 1 при делении на $n$ (частный случай теоремы Дирихле, не поддаётся пока элементарному доказательству) [5].

4) Для любого натурального числа $n>2$ и любых натуральных $a;b$, где $a>b$, число $a^n-b^n$ имеет простой делитель, больший $n$.

*Замечание.* В случае $n=2$ утверждение 4) неверно. Например, пусть $a=2^k+1;\ b=2^k-1$, тогда $a^2-b^2=2^{k+2}$.

Сформулируем две задачи, связанные с теорией делителей. Пусть $m$ и $n$ — натуральные числа, причем $n > 2$. Докажите, что $2^m + 1$ никогда не делится на число $2^n - 1$. Пусть $\delta$ — общий делитель чисел $a$ и $b$ (т.е. $a = \delta \cdot a_1$; $b = \delta \cdot b_1$), $n$ — любое целое число больше 1.

Докажите, что если $b_1$ нечетно, то общий множитель чисел $n^a + 1$; $n^b - 1$ не может быть больше двух [6]. Также можно сформулировать и доказать аналоги теоремы 2 и 3 для функции от двух переменных $D_n(a,b)$. Сформулируем один из результатов.

*Утверждение.* Пусть многочлен $D_n(a,b)$ определяется равенством

$$D_n(a,b) = a^n + b^{n-1} \cdot (a-b) \cdot (a-b-1) \cdot n - b^n.$$

Тогда для всех натуральных чисел $n$ и различных пар натуральных чисел $\{a,b\}$ имеет место критерий делимости $D_n(a,b) \vdots (a-b)^2$. На этом мы завершаем нашу статью. Читатели самостоятельно могут убедиться в полезности рассмотренных предложений.

Список литературы


1 *Виноградов И.И.* Основы теории чисел. — М.: Наука, 1981. — 176 с.
2 *Feit W., Thompson J.G.* Pacif. Tourna. Math. — 1963. — 13. — № 3 — P. 775–1029.
3 *Курош А.Г.* Курс высшей алгебры. — М.: Наука, 1965. — 432 с.
4 Задачи Санкт-Петербургской олимпиады школьников по математике. — Л., 2006. — 224 с.
5 *Гашков С.Б., Чубариков В.Н.* Арифметика, алгоритмы, сложность вычисления. — М.: Наука, 2005. — 350 с.
6 Избранные задачи: Сб. / Пер. с англ. — М.: Мир, 1977.


Д.Исмоилов

## Дөңгелекті бөлу көпмүшеліктері, Фейт-Томсон проблемасы және бөлінгіштік теориянің кейбір қолданылуы

Мақалада группалар теориясының Фейт-Томпсон ғылыми болжамын шешудің бір әдісі берілген. Дөңгелекті бөлу көпмүшеліктерінің арифметикалық түсінігі негізінде дөңгелекті көпмүшеліктерге тәуелді көпмүшеліктердің берілуіне қатысты кейбір тұжырымдар дәлелденген. Алынған тұжырымдар негізінде натурал сандардың жартылай группасында бөлінгіштік теориясына қатысты бірқатар нәтижелер енгізілген.

D.Ismoilov

## Cyclotomic polynomials, the problem of Feit-Thompson and some applications to the theory of divisibility

In this paper we propose one way of solving the conjecture of Feit-Thompson of group theory. On the basis of the arithmetic interpretation of cyclotomic polynomials prove some statements about the representation of polynomials depending on cyclotomic polynomials. On the basis of the allegations shows a number of results relating to the theory of divisibility in the semigroup of natural numbers.

References


1 Vinogradov I.I. *Fundamentals of the theory of numbers*, Moscow: Nauka, 1981, 176 p.
2 Feit W., Thompson J.G., *Pacif. Tourna. Math*., 1963, 13, 3 p. 775–1029.
3 Kurosh A.G. *Course of higher algebra*, Moscow: Nauka, 1965, 432 p.
4 *Problems of St.-Petersburg mathematical olympiad*, Leningrad: 2006, 224 p.
5 Gashkov S.B., Chubarikov V.N. *Arithmetic, algorithms, computational complexity*, Moscow: Nauka, 2005, 350 p.
6 *Selected problems. Compilation. Trans.* / Transl. from Engl., Moscow: Mir, 1977.