УЧЕНЫЕ ЗАПИСКИ КАЗАНСКОГО УНИВЕРСИТЕТА.
СЕРИЯ ФИЗИКО-МАТЕМАТИЧЕСКИЕ НАУКИ

2021, Т. 163, кн. 3–4 ISSN 2541-7746 (Print)
С. 304–348 ISSN 2500-2198 (Online)

ОБЗОРНАЯ СТАТЬЯ

УДК 51(091)+512.622 doi: 10.26907/2541-7746.2021.3-4.304-348

МЕТОД ФАНЬЯНО РЕШЕНИЯ АЛГЕБРАИЧЕСКИХ УРАВНЕНИЙ: ИСТОРИЧЕСКИЙ ОБЗОР И ЕГО РАЗВИТИЕ

А.Н. Абызов

Казанский (Приволжский) федеральный университет, г. Казань, 420008, Россия

Аннотация

Статья является обзорно-методической: дан исторический обзор результатов, связанных с использованием алгебраических тождеств при решении алгебраических уравнений, в частности, рассмотрены работы Ф. Дюлорана, Г.В. Лейбница и Фаньяно. Изучены связи между тригонометрическими тождествами, известными линейными рекуррентными последовательностями и теми видами алгебраических тождеств, которые тесно связаны с известными семействами алгебраических уравнений, разрешимых в радикалах.

Ключевые слова: алгебраические уравнения, последовательности Люка, групповые определители

Введение

В 1750 г. был издан в двух томах трактат графа Джулио Карло де Тоски ди Фаньяно «Математические произведения». Во втором томе этого трактата была опубликована работа [1], в которой Фаньяно предложил единообразный метод решений алгебраических уравнений вплоть до четвертой степени. Этот метод, который в настоящей статье мы будем называть методом Фаньяно, основывается на сопоставлении алгебраических уравнений с тождествами, возникающими при представлениях выражения вида $(a_1+\dots+a_m)^n$ через меньшие степени $a_1+\dots+a_m$. Результаты из работы [1] в историко-математической литературе почти не рассматриваются. Единственное известное нам упоминание о методе решения алгебраических уравнений, предложенном Фаньяно, содержится в книге Г. Вилейтнера «История математики от Декарта до середины XIX столетия» [2, с. 45]. Отметим, что Ф. Дюлораном в его «Математических примерах»(1667) [3] и, согласно [4, с. 227], в рукописи Г.В. Лейбница "De Bisectione Laterum" («О делении сторон пополам»), датированной 1675 г., аналогичным способом были решены алгебраические уравнения, связанные с формулой косинуса n-кратного угла.

Настоящая работа посвящена обзору результатов, связанных с использованием некоторых видов алгебраических тождеств при решении ряда семейств алгебраических уравнений, разрешимых в радикалах. Рассмотрены различные связи этих тождеств с линейными рекуррентными последовательностями и тригонометрическими тождествами. Исторический обзор, посвященный использованию метода Фаньяно при решении алгебраических уравнений, изложен в первом параграфе. Второй параграф посвящен алгебраическим уравнениям, разрешимых в радикалах, тесно связанных с многочленами Чебышева, решение которых в радикалах основано на использовании тождества Куммера, являющегося частным случаем тождества Жирара – Варинга. С помощью тождества Куммера получены новые доказательства некоторых результатов из работ [5–7]. Приведены также два коротких доказательства закона взаимности, в которых используются тождества, рассмотренные во втором параграфе. В третьем параграфе изучены семейства алгебраических уравнений, часть из которых является расширением на произвольные натуральные степени алгебраических уравнений, рассмотренных в работах [8, 9]. В четвертом и пятом параграфах изучены связи тождеств, рассмотренных в предыдущих параграфах, с известными числовыми линейными рекуррентными последовательностями. Изучены также арифметические свойства таких последовательностей, приведены новые доказательства некоторых известных утверждений. В заключительном параграфе устанавливается связь между тождествами, рассмотренными в настоящей работе, и групповыми определителями.

1. Метод Фаньяно. Исторический обзор

При решении кубического уравнения

$$x^3 = nx^2 + px + q \tag{1}$$

Фаньяно [1, с. 387] воспользовался тождеством

$$(a+b+c)^3 = 3c(a+b+c)^2 + (3ab - 3c^2)(a+b+c) + a^3 + b^3 + c^3 - 3abc. \tag{2}$$

Сопоставляя это тождество с уравнением (1), Фаньяно заметил, что если в качестве $a,\ b,\ c$ выбрать числа, удовлетворяющие равенствам

$$3c = n, \quad 3ab - 3c^2 = p, \quad a^3 + b^3 + c^3 - 3abc = q, \tag{3}$$

то число $a+b+c$ является решением уравнения (1). Из равенств (3) следует, что $c = n/3$ и числа $a^3,\ b^3$ являются корнями многочлена второй степени

$$x^2 - \left(\frac{2n^3}{27} + \frac{pn}{3} + q\right)x + \left(\frac{p}{3} + \frac{n^2}{9}\right)^3 = 0. \tag{4}$$

Решение уравнения (1) Фаньяно [1, с. 394] записал в виде

$$x = \frac{n}{3} + a + \frac{1}{a}\left(\frac{p}{3} + \frac{n^2}{9}\right),$$

где a^3 – корень уравнения (4). Отметим, что в 1863 г. была опубликована работа Иоганна Августа Грунерта [10], в которой был независимо воспроизведен метод Фаньяно решения кубического уравнения, основанный на тождестве (2).

Выделим частный случай тождества (2), когда $c = 0$. В этом случае формула Кардано решения неполного кубического уравнения

$$x^3 = px + q \tag{5}$$

следует из сопоставления этого уравнения с тождеством

$$(a+b)^3 = 3ab(a+b) + a^3 + b^3. \tag{6}$$

Впервые такой способ решения неполного кубического уравнения, по-видимому, был предложен Ф. Дюлораном в его «Математических примерах» (1667) [3, с. 224–225]. Аналогичным способом Ф. Дюлораном также были решены некоторые алгебраические уравнения более высоких степеней, некоторые из которых будут приведены ниже. В современной литературе описанный способ решения уравнения (5) встречается. Например, в недавней работе [11] этот способ приписывается

Р. Соломону, известному специалисту по теории конечных групп. Соломон привел его в своем учебнике по абстрактной алгебре [12].

Решение общего уравнения четвертой степени

$$x^4 = nx^3 + px^2 + qx + r$$

с помощью стандартной подстановки $y = x - n/4$ Фаньяно сводит к решению неполного уравнения четвертой степени

$$y^4 = Py^2 + Qy + R. \tag{7}$$

При решении уравнения (7) Фаньяно воспользовался тождеством

$$(a+b+c)^4 = (2c^2+4ab)(a+b+c)^2+(4a^2c+4b^2c)(a+b+c)+a^4+b^4-c^4-2a^2b^2+4abc^2. \tag{8}$$

Из сопоставления тождества (8) и уравнения (7) следует: если в качестве a, b, c выбрать числа, для которых выполнены равенства

$$2c^2 + 4ab = P, \quad 4a^2c + 4b^2c = Q, \quad a^4 + b^4 - c^4 - 2a^2b^2 + 4abc^2 = R, \tag{9}$$

то число $a+b+c$ является решением алгебраического уравнения (7). Из последних равенств следует, что c^2 является корнем кубического уравнения

$$x^3 - \frac{P}{2}x^2 + \left(\frac{P^2}{16} + \frac{R}{4}\right)x + \frac{Q^2}{64} = 0. \tag{10}$$

Используя равенства (9), с помощью несложных преобразований Фаньяно [1, с. 396] записывает решение уравнения (7) в виде радикального выражения, зависящего от коэффициентов уравнения (7) и корня кубического уравнения (10).

В мемуаре «О решении уравнений любой степени» (1764) Леонард Эйлер предложил метод решения алгебраического уравнения степени n, основанный на представлении его корня в виде

$$x = \alpha_0 + \alpha_1 \sqrt[n]{\beta} + \alpha_2 \sqrt[n]{\beta^2} + \cdots + \alpha_{n-1} \sqrt[n]{\beta^{n-1}},$$

где α_0 – рациональное число, $\alpha_1, \ldots, \alpha_{n-1}, \beta$ – рациональны или выражаются через радикалы не выше $(n-1)$-й степени. Свой метод Эйлер применил к решению в радикалах алгебраических уравнений третьей и четвертой степеней и к некоторым интересным типам алгебраических уравнений пятой степени, а именно, им были рассмотрены следующие уравнения:

$$x^5 = 5px^3 - 5p^2x + q, \tag{11}$$

$$x^5 = 5px^2 + 5qx + \frac{q^2}{p} + \frac{p^3}{q}. \tag{12}$$

Уравнения вида (11) обычно называются уравнениями Муавра, они были изучены в ряде работ (см., например, [13, 14]). С помощью своего метода Эйлер показал, что корни уравнения (11) имеют вид

$$x = \varepsilon_5^i \sqrt[5]{\frac{1}{2}(q - \sqrt{q^2 - 4p^5})} + \varepsilon_5^{-i} \sqrt[5]{\frac{1}{2}(q + \sqrt{q^2 - 4p^5})}, \quad i = 1, 2, 3, 4, 5, \tag{13}$$

и корни уравнения (12) находятся по формуле

$$x = \varepsilon_5^i \sqrt[5]{\frac{q^2}{p}} + \varepsilon_5^{2i} \sqrt[5]{\frac{p^3}{q}}, \quad i = 1, 2, 3, 4, 5. \tag{14}$$

С подробным анализом мемуара Эйлера можно ознакомиться в работе [15].

В 1873 г. был опубликован трактат Франсуа Валлеса «Воображаемые формы в алгебре» [16], в котором методом Фаньяно были решены как алгебраические уравнения третьей и четвертой степеней, так и алгебраические уравнения пятой степени видов (11) и (12).

При решении уравнения

$$x^4 + px^2 + qx + r = 0 \tag{15}$$

Валлес [16, с. 212] воспользовался тождеством

$$\begin{multline}(a + b + c)^4 - 2(a^2 + b^2 + c^2)(a + b + c)^2 - \\ - 8abc(a + b + c) + (a^2 + b^2 + c^2)^2 - 4(a^2b^2 + a^2c^2 + b^2c^2) = 0. \tag{16}\end{multline}$$

Из предыдущего тождества следует, что если в качестве a, b, c выбрать числа, для которых выполнены равенства

$$a^2 + b^2 + c^2 = -\frac{p}{2}, \quad a^2b^2 + a^2c^2 + b^2c^2 = \frac{p^2}{16} - \frac{r}{4}, \quad abc = -\frac{q}{8},$$

то $x = a + b + c$ является решением уравнения. Таким образом, если в качестве a, b, c выбрать числа, для которых выполнено равенство $abc = -q/8$ и a^2, b^2, c^2 – корни уравнения

$$y^3 + \frac{p}{2}y^2 + \left(\frac{p^2}{16} - \frac{r}{4}\right) y - \frac{q^2}{64} = 0,$$

то решения уравнения (15) имеют вид

$$x_1 = a + b + c, \quad x_2 = a - b - c, \quad x_3 = -a - b + c, \quad x_4 = -a + b - c.$$

При решении уравнения (11) Валлес [16, с. 350] приводит тождество

$$(a + b)^5 - 5ab(a + b)^3 + 5a^2b^2(a + b) - (a^5 + b^5) = 0. \tag{17}$$

Из тождества (17) следует, что если в качестве a, b выбрать числа, удовлетворяющие равенствам

$$ab = p, \quad a^5 + b^5 = q, \tag{18}$$

то решения уравнения (11) имеют вид

$$x = \varepsilon_5^i a + \varepsilon_5^{4i} b, \quad i = 1, 2, 3, 4, 5.$$

Из равенств (18) следует, что формулы, выражающие в радикалах решения уравнения (11), имеют вид (13).

При решении уравнения (12) Валлес [16, с. 384] воспользовался тождеством

$$(a + b)^5 - 5b^2a(a + b)^2 - 5ba^3(a + b) - (a^5 + b^5) = 0. \tag{19}$$

Последнее тождество можно записать в виде

$$(a + b)^5 = 5b^2a(a + b)^2 + 5ba^3(a + b) + \frac{(ba^3)^2}{b^2a} + \frac{(b^2a)^3}{ba^3}. \tag{20}$$

Следовательно, если в качестве a, b взять числа, удовлетворяющие равенствам

$$b^2a = p, \quad ba^3 = q, \tag{21}$$

то из (20) следует, что решения уравнения (12) имеют вид

$$x = \varepsilon_5^i a + \varepsilon_5^{2i} b, \quad i = 1, 2, 3, 4, 5.$$

Из последнего равенства и равенств (21) следует формула (14), выражающая в радикалах решения уравнения (12).

Формула (17) и ее расширения на случаи степеней 7, 9 и 11 были приведены в трактате «Математические примеры» (1667) Ф. Дюлорана. Сопоставляя эти формулы с уравнением (11) и его естественными расширениями на алгебраические уравнения степеней 7 и 11, Дюлоран [3, с. 231] получил формулы корней этих уравнений. В частности, им была получена и формула (13). Найденный им способ решения алгебраических уравнений, естественно связанных с выражением многочлена $a^n + b^n$ через элементарные симметрические функции ab и $a+b$ при $n = 3, 4, 5, 7, 9$ и 11, Дюлоран проиллюстрировал на ряде примеров. Например, сравнивая тождество

$$\begin{aligned}(m+n)^9 = 9mn(m+n)^7 - 27m^2n^2(m+n)^5 + \\ + 30m^3n^3(m+n)^3 - 9m^4n^4(m+n) + n^9 + m^9 \quad (22)\end{aligned}$$

с уравнением

$$a^9 - 18a^7 + 108a^5 - 240a^3 + 144a - 48 = 0, \quad (23)$$

Дюлорен [3, с. 228] находит вещественный корень этого уравнения, равный $\sqrt[9]{32} + \sqrt[9]{16}$. В монографии [17, с. 56] отмечено, что в «Математических примерах» были впервые представлены решения алгебраических уравнений степеней выше 4 алгебраическими методами. До работы Дюлорана алгебраические уравнения степеней выше 4 также рассматривались, но, как правило, они были связаны с уравнениями деления угла на равные части и решались с помощью тригонометрических функций. В 1675–1676 гг. Г.В. Лейбниц изучал проблемы, связанные с разрешимостью алгебраических уравнений в радикалах. Как и многие ведущие математики его времени, Лейбниц был убежден в разрешимости в радикалах алгебраических уравнений произвольной степени. В сочинении «О делении сторон пополам» (1675) им были получены результаты, близкие к тем, которые приведены в «Математических примерах». Более точно, согласно [4], Лейбницем были установлены тождества вида

$$(a-b)^{2n+1} = a^{2n+1} - b^{2n+1} - \sum_{i=1}^{n} \frac{2n+1}{2n+1-2i} \binom{2n+1-i}{i} (ab)^i (a-b)^{2n+1-2i}, \quad (24)$$

$$(a-b)^{2n} = (a^n - b^n)^2 - \sum_{i=1}^{n-1} \frac{2n}{2n-i} \binom{2n-i}{i} (ab)^i (a-b)^{2(n-i)} \quad (25)$$

для $n \leq 6$ и найдено правило, которое позволяет рекуррентно получать тождества видов (24) и (25) для произвольного n. Из сопоставления соотношений (24), (25) соответственно с алгебраическим уравнением

$$r = \sum_{i=0}^{n} \frac{2n+1}{2n+1-i} \binom{2n+1-i}{i} p^i x^{2n+1-2i} \quad (26)$$

и с уравнением

$$r = \sum_{i=0}^{n-1} \frac{2n}{2n-i} \binom{2n-i}{i} p^i x^{2n-2i} \quad (27)$$

несложно получить формулы решений соответственно уравнений (26) и (27)

$$x = \sqrt[2n+1]{\frac{r}{2} + \sqrt{\frac{r^2}{4} + p^{2n+1}}} + \sqrt[2n+1]{\frac{r}{2} - \sqrt{\frac{r^2}{4} + p^{2n+1}}}, \tag{28}$$

$$x = \sqrt[n]{\sqrt{\frac{r}{4} + p^n} + \sqrt{\frac{r}{4}}} - \sqrt[n]{\sqrt{\frac{r}{4} + p^n} - \sqrt{\frac{r}{4}}}. \tag{29}$$

Как отмечено в [4, с. 227], метод нахождения формулы решения уравнений (26), (27) с помощью тождеств(24) и (25) был проиллюстрирован Лейбницем для уравнений пятых степеней.

В недавней работе [9] были найдены некоторые расширения уравнения (12) на более высокие степени, а именно: с помощью обобщенных перестановочных матриц и их определителей в этой статье были найдены формулы для корней одного семейства алгебраических уравнений степеней $5 \leq n \leq 10$. Рассматриваемые в работе [9] уравнения пятой степени совпадают с уравнениями вида (11). Для уравнений девятой степени вида

$$x^9 - AX^4 - BX^3 - \frac{27B^2}{100A}X^2 - \frac{27B^3}{1000A^2}X - \left(\frac{9B^4}{10000A^3} + \frac{10A^3}{243B}\right) = 0, \quad A \neq 0, B \neq 0,$$

в статье [9] приводится следующая формула для нахождения корней этого уравнения

$$x_m = \sqrt[9]{\frac{9B^4}{10000A^3}} \exp\left(\frac{2\pi mi}{9}\right) + \sqrt[9]{\frac{10A^3}{243B}} \exp\left(\frac{4\pi mi}{9}\right), \quad 0 \leq m \leq 8.$$

В этой работе авторами было сделано замечание о возможности получения формул, аналогичных выписанной выше, с помощью используемых ими методов для конкретных значений степеней $n \geq 11$ рассматриваемых ими типов алгебраических уравнений, но при этом, как отмечено авторами, не гарантировано получение общей формулы для произвольного n. В третьем параграфе с помощью метода Фаньяно будут рассмотрены расширения формул для решения алгебраических уравнений, рассмотренных в [9], на случай произвольного натурального числа n.

2. Уравнения Кардано и многочлены Чебышева

Формулы для решения в радикалах неполного кубического уравнения и уравнения Муавра (11) следуют из сопоставления их с тождествами (6) и (17). В этом параграфе будут рассмотрены тождество Куммера, которое является обобщением тождеств (6) и (17), и близкие к нему тождества. Будут также изучены связи этих тождеств с многочленами Чебышева, последовательностями Люка, некоторыми радикальными соотношениями, алгебраическими уравнениями, разрешимыми в радикалах, частными случаями которых являются уравнения (5) и (11), и квадратичным законом взаимности.

Пусть $a, b \in \mathbb{C}[x, y]$. Через $\{v_n(a, b)\}_{n \in \mathbb{N}_0}$ и $\{u_n(a, b)\}_{n \in \mathbb{N}_0}$ будем обозначать рекуррентные последовательности, удовлетворяющие соответственно условиям:

$$u_0(a, b) = 0, \quad u_1(a, b) = 1, \quad u_{n+1}(a, b) = au_n(a, b) - bu_{n-1}(a, b), \quad n \in \mathbb{N}, \tag{30}$$

$$v_0(a, b) = 2, \quad v_1(a, b) = a, \quad v_{n+1}(a, b) = av_n(a, b) - bv_{n-1}(a, b), \quad n \in \mathbb{N}. \tag{31}$$

В случае, когда $a, b \in \mathbb{Z}$, последовательности $\{u_n(a, b)\}_{n \in \mathbb{N}_0}$ и $\{v_n(a, b)\}_{n \in \mathbb{N}_0}$ называются последовательностями Люка. Если a и b удовлетворяют равенствам

$a = -b = 1$, то $\{u_n(a,b)\}_{n\in\mathbb{N}_0}$ и $\{v_n(a,b)\}_{n\in\mathbb{N}_0}$ являются хорошо известными числовыми последовательностями, которые соответственно называются числами Фибоначчи $\{F_n\}_{n\in\mathbb{N}_0}$ и числами Люка $\{L_n\}_{n\in\mathbb{N}_0}$. Подробный исторический обзор результатов, связанных с последовательностями Люка и их приложениями, изложен в семнадцатой главе известной монографии Л. Диксона [18].

Непосредственно проверяется, что последовательности

$$\{u_n(x+y,xy)\}_{n\in\mathbb{N}}, \quad \left\{\frac{x^n-y^n}{x-y}\right\}_{n\in\mathbb{N}} \quad \text{и}$$
$$\left\{\sum_{i=0}^{[(n-1)/2]}(-1)^i\binom{n-i-1}{i}(xy)^i(x+y)^{n-2i-1}\right\}_{n\in\mathbb{N}} \tag{32}$$

удовлетворяют одним и тем же рекуррентным соотношениям и их значения при n, равным 1 и 2, совпадают. Таким образом, для любого натурального числа n имеет место тождество

$$\frac{x^n-y^n}{x-y} = \sum_{i=0}^{[(n-1)/2]}(-1)^i\binom{n-i-1}{i}(xy)^i(x+y)^{n-2i-1}. \tag{33}$$

Аналогично, для любого натурального числа n устанавливается тождество

$$x^n+y^n = \sum_{i=0}^{[n/2]}(-1)^i\frac{n}{n-i}\binom{n-i}{i}(xy)^i(x+y)^{n-2i} = v_n(x+y,xy). \tag{34}$$

Несложно заметить, что тождества

$$(x+y)^3-3xy(x+y)-x^3-y^3=0$$

и

$$(x+y)^5-5xy(x+y)^3+5x^2y^2(x+y)-x^5-y^5=0,$$

с помощью которых методом Фаньяно решаются соответственно неполное кубическое уравнение и уравнение Муавра, являются частными случаями тождества (34). Из тождества (34) следует выполнимость для каждого $0\le i\le n-1$ равенства:

$$x^n+y^n = \sum_{i=0}^{[n/2]}(-1)^i\frac{n}{n-i}\binom{n-i}{i}(xy)^i(\varepsilon_n^i x+\varepsilon_n^{-i}y)^{n-2i}, \tag{35}$$

где ε_n – примитивный корень степени n из единицы. Таким образом, в алгебре многочленов от трех переменных $\mathbb{C}[x,y,t]$ выполнено тождество

$$\prod_{i=0}^{n-1}(t-(\varepsilon_n^i x+\varepsilon_n^{-i}y)) = \sum_{i=0}^{[n/2]}(-1)^i\frac{n}{n-i}\binom{n-i}{i}(xy)^i t^{n-2i}-(x^n+y^n). \tag{36}$$

Так как, согласно изложенному выше имеют место равенства

$$\{u_n(x,y)\}_{n\in\mathbb{N}_0} = \left\{\frac{\alpha^n-\beta^n}{\alpha-\beta}\right\}_{n\in\mathbb{N}_0}, \quad \{v_n(x,y)\}_{n\in\mathbb{N}_0} = \{\alpha^n+\beta^n\}_{n\in\mathbb{N}_0}, \tag{37}$$

где α, β – корни многочлена t^2-xt+y из некоторого расширения поля $\mathbb{C}(x,y)$, то, как показывают непосредственные вычисления, для произвольного $n\in\mathbb{N}$ имеет место соотношение

$$2u_{n+1}(x,y)-xu_n(x,y)=v_n(x,y). \tag{38}$$

Тождества (33) и (34) в литературе называются формулами Куммера (см., например, [24]). Отметим, что тождество (33) является частным случаем важного тождества Жирара – Варинга:

$$x_1^m + \cdots + x_n^m = \sum_{\substack{j_1+2j_2+\cdots+\\+nj_n=m}} (-1)^{j_2+j_4+\cdots} \frac{m(j_1+j_2+\cdots+j_n-1)!}{j_1!j_2!\cdots j_n!} \sigma_1^{j_1}\sigma_2^{j_2}\cdots\sigma_n^{j_n}, \qquad (39)$$

где $\sigma_1, \sigma_2, \ldots \sigma_n$ – элементарные симметрические функции, зависящие от переменных $x_1, \ldots, x_n$. Формула (39) была получена Альбером Жираром [19] (1629) при $m \leq 4$ и в общем случае доказана Э. Варингом [20] (1762). В современных учебных руководствах по алгебре формула Жирара – Варинга как правило отсутствует. Эту формулу и ее доказательство можно найти в учебнике А.К. Сушкевича [21]. Отметим, что достаточно ясное изложение доказательства формулы Жирара – Варинга приведено в учебнике Н.И. Лобачевского «Алгебра или вычисление конечных» [22, с. 334-335].

Тождества Куммера и близкие к ним тождества тесно связаны со многими важными и нетривиальными тригонометрическими соотношениями. Приведем вывод некоторых хорошо известных тригонометрических тождеств, основываясь на тождествах (33) и (34). Подставляя в формулу (34) вместо x и y соответственно $e^{i\alpha}$ и $e^{-i\alpha}$, несложно получить равенство

$$\cos n\alpha = \frac{1}{2} \sum_{k=0}^{[n/2]} (-1)^k \frac{n}{n-k} \binom{n-k}{k} (2\cos\alpha)^{n-2k}. \qquad (40)$$

Аналогично из соотношения (33) следует тождество

$$\frac{\sin n\alpha}{\sin\alpha} = \sum_{k=0}^{[(n-1)/2]} (-1)^k \binom{n-k-1}{k} (2\cos\alpha)^{n-2k-1}. \qquad (41)$$

Отметим, что вывод предыдущей формулы на основе соотношения (33) также содержится в книге Н.И. Лобачевского «Алгебра или вычисление конечных» [22, с. 246–247]. Пусть $n = 2m+1$ – нечетное натуральное число. Из (34) следует тождество

$$x^{2m+1} - x^{-2m-1} = \sum_{k=0}^{m} \frac{n}{m+k+1} \binom{m+k+1}{2k+1} \left(x - x^{-1}\right)^{2k+1}. \qquad (42)$$

Заметим, что

$$\frac{2^{2k}}{m+k+1} \binom{m+k+1}{2k+1} = \frac{((2m+1)^2-1)\cdots((2m+1)^2-(2k-1)^2)}{(2k+1)!}.$$

Тогда

$$\frac{x^{2m+1} - x^{-2m-1}}{2} = \\ = \sum_{k=0}^{m} \frac{(2m+1)((2m+1)^2-1)\cdots((2m+1)^2-(2k-1)^2)}{(2k+1)!} \left(\frac{x-x^{-1}}{2}\right)^{2k+1}. \qquad (43)$$

Положим в последнем равенстве $x = e^{i\alpha n}$. Таким образом, получаем соотношение

$$\sin n\alpha = \sum_{k=0}^{[n/2]} (-1)^k \frac{n(n^2-1)\cdots(n^2-(2k-1)^2)}{(2k+1)!} \sin^{2k+1}\alpha. \qquad (44)$$

Предыдущая формула была приведена Исааком Ньютоном в 1676 году в одном из писем Г.В. Лейбницу [2, с. 44]. Аналогично устанавливаются следующие тождества:

$$\frac{x^{2m+1}+x^{-2m-1}}{2}=$$
$$=\sum_{k=0}^{m}\frac{(1-(2m+1)^2)\cdots((2k-1)^2-(2m+1)^2)}{(2k+1)!}\left(\frac{x+x^{-1}}{2}\right)^{2k+1}, \quad (45)$$

$$\cos(2m+1)\alpha=\sum_{k=0}^{m}(-1)^k\,\frac{(1-(2m+1)^2)\cdots((2k-1)^2-(2m+1)^2)}{(2k+1)!}\cos^{2k+1}\alpha. \quad (46)$$

В статье «Аналитическое решение некоторых уравнений третьей, пятой, седьмой, девятой и высших следующих до бесконечности степеней в конечном виде, аналогичное правилам Кардано для кубических уравнений» [23] Авраамом де Муавром для уравнений

$$\sum_{k=0}^{n}\frac{((2n+1)^2-1)\cdots((2n+1)^2-(2k-1)^2)}{(2k+1)!}\,nx^{2k+1}=a \quad (47)$$

и

$$\sum_{k=0}^{n}\frac{(1-(2n+1)^2)\cdots((2k-1)^2-(2n+1)^2)}{(2k+1)!}\,nx^{2k+1}=a \quad (48)$$

были выписаны соответственно следующие формулы их решений:

$$x=\frac{1}{2}\left(\sqrt[2n+1]{a+\sqrt{a^2+1}}-\frac{1}{\sqrt[2n+1]{a+\sqrt{a^2+1}}}\right), \quad (49)$$

$$x=\frac{1}{2}\left(\sqrt[2n+1]{a+\sqrt{a^2-1}}+\frac{1}{\sqrt[2n+1]{a+\sqrt{a^2-1}}}\right). \quad (50)$$

Заметим, что формулы (49) и (51) непосредственно следуют из сопоставления уравнений (47), (48) соответственно с тождествами (43) и (45). Также отметим, что в случае, когда в уравнении (48) $a=\cos\alpha(2n+1)$, из (46) следует соотношение

$$\cos\alpha=\frac{1}{2}\left(\sqrt[2n+1]{\cos(2n+1)\alpha+i\sin(2n+1)\alpha}+\right.$$
$$\left.+\frac{1}{\sqrt[2n+1]{\cos(2n+1)\alpha+i\sin(2n+1)\alpha}}\right), \quad (51)$$

которое равносильно формуле Муавра

$$\cos(2m+1)\alpha+i\sin(2m+1)\alpha=(\cos\alpha+i\sin\alpha)^{2m+1}.$$

Следуя [24], назовем уравнением Кардано следующее алгебраическое уравнение:

$$\sum_{i=0}^{[n/2]}(-1)^i\,\frac{n}{n-i}\binom{n-i}{i}p^ix^{n-2i}-q=0. \quad (52)$$

Примерами уравнения Кардано являются неполное кубическое уравнение и уравнение Муавра (12).

Напомним, что многочлены Чебышева первого и второго рода определяются соответственно с помощью равенств

$$\cos \alpha n = T_n(\cos \alpha), \qquad \frac{\sin \alpha n}{\sin \alpha} = U_n(\cos \alpha). \tag{53}$$

Из (40) и (41) следуют соотношения

$$T_n(x) = \frac{1}{2} \sum_{r=0}^{[n/2]} (-1)^i \frac{n}{(n-i)} \binom{n-i}{i} (2x)^{n-2i} = \frac{1}{2}\, v_n(2x, 1), \tag{54}$$

$$U_n(x) = \sum_{r=0}^{[(n-1)/2]} (-1)^i \binom{n-i-1}{i} (2x)^{n-2i-1} = u_n(2x, 1). \tag{55}$$

С помощью многочлена Чебышева первого рода уравнение Кардано запишется следующим образом:

$$q = 2 \sqrt[n]{p}\, T_n\left(\frac{x}{2\sqrt{p}}\right). \tag{56}$$

Теорема 1. *Если p, $q \in \mathbb{C}$, то корнями уравнения*

$$\sum_{i=0}^{[n/2]} (-1)^i \frac{n}{n-i} \binom{n-i}{i} p^i x^{n-2i} - q = 0$$

являются числа

$$x = \varepsilon_n^i a + \varepsilon_n^{-i} b, \quad i = 1, 2, \ldots, n,$$

где a и b – значения соответственно $\sqrt[n]{\frac{1}{2}(q + \sqrt{q^2 - 4p^n})}$ и $\sqrt[n]{\frac{1}{2}(q - \sqrt{q^2 - 4p^n})}$, для которых выполнено равенство

$$ab = p.$$

Доказательство. Теорема непосредственно следует из равенства (36) и из сопоставления уравнения Кардано (52) с тождеством (34). □

Таким образом, согласно предыдущей теореме формула решения уравнения Кардано (52) имеет вид

$$x = \sqrt[n]{\frac{1}{2}(q + \sqrt{q^2 - 4p^n})} + \frac{p}{\sqrt[n]{\frac{1}{2}(q + \sqrt{q^2 - 4p^n})}}. \tag{57}$$

Как отмечено в предыдущем параграфе, частные случаи этой формулы были получены в работах Ф.Дюлорана, Г.В. Лейбница, Л. Эйлера и Ф. Валлеса. Формула, равносильная формуле (57), приведена в монографиях Л. Диксона [25, с. 75] и [26, с. 58]. Формула решения уравнения Кардано независимо переоткрывалась также в работах [24, 27].

Хорошо известные методы решений кубических уравнений, предложенные Франсуа Виетом, имеют естественные расширения на уравнения Кардано. В сочинении “De Aequationum Recognitione et Emendatione Tractatus Duo” (Paris, 1615) («Об анализе и усовершенствовании уравнений») Ф. Виет с помощью подстановки $x = \dfrac{p}{3y} - y$ сводит кубическое уравнение $x^3 + px + q = 0$ к уравнению $y^6 - qy^3 - \dfrac{p^3}{27} = 0$, квадратному относительно y^3. Положим в уравнении (52) $x = y + \dfrac{p}{y}$.

Тогда согласно тождеству (34) уравнение (52) сведется к уравнению $y^n + \dfrac{p^n}{y^n} = q$, квадратному относительно y^n. Таким образом, получаем выражение для корней уравнения (34), которые приведены в теореме 1. Отметим, что, согласно [4], в 1661 г. Пьер Ферма написал письмо Х. Гюйгенсу, в котором изложил аналогичный способ решения уравнений вида

$$\sum_{i=0}^{[n/2]} (-1)^i \frac{n}{n-i} \binom{n-i}{i} x^{n-2i} - q = 0, \tag{58}$$

которые являются примерами уравнений Кардано. П. Ферма решал предыдущее уравнение в случае, когда $\mid q \mid > 2$ и n нечетно. Если $\mid q \mid < 2$, то, как отмечено в [4, с. 223], полученная им формула решения этого уравнения

$$x = \sqrt[n]{\frac{1}{2}(q + \sqrt{q^2-4})} + \sqrt[n]{\frac{1}{2}(q - \sqrt{q^2-4})} \tag{59}$$

равносильна формуле

$$2\cos\frac{\alpha}{n} = \sqrt[n]{\cos\alpha + i\sin\alpha} + \sqrt[n]{\cos\alpha - i\sin\alpha},$$

которую можно рассматривать как одну их форм записи формулы Муавра. В своем сочинении “Supplementum Geometriae” (Turonis, 1593) («Дополнение геометрии») Ф. Виет показал, как с помощью тригонометрического соотношения $\cos 3\alpha = 4\cos^3\alpha - 3\cos^2\alpha$ неприводимое кубическое уравнение сводится к задаче о трисекции угла. Метод Виета решения неприводимых кубических уравнений имеет естественное расширение на вещественные уравнения (52) нечетных степеней, у которых $q^2 - 4p^n < 0$. Из теоремы 1 следует, что такие уравнения обладают n различными вещественными корнями. Положим $x = 2\sqrt{p}y$. Тогда уравнение (52) согласно (56) примет вид

$$T_n(y) = \frac{q}{2\sqrt[n]{p}}.$$

Так как $q^2 - 4p^n < 0$, то $\left|\dfrac{q}{2\sqrt[n]{p}}\right| < 1$. Тогда согласно (53) корни уравнения (52) имеют вид

$$2\sqrt{p}\cos\frac{\arccos\left(\dfrac{q}{2\sqrt[n]{p}}\right) + 2\pi k}{n}, \quad k = 1, 2, \ldots, n.$$

Пусть

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{C})$$

есть произвольная матрица. Из теоремы Гамильтона–Кэли следует, что последовательность $\{A^n\}_{n\in\mathbb{N}_0}$ удовлетворяет рекуррентному соотношению

$$A^{n+1} = \mathrm{tr}(A)A^n - \det(A)A^{n-1}, \quad n \in \mathbb{N}. \tag{60}$$

Для произвольного неотрицательного целого числа n введем обозначения: $u_n = u_n(\mathrm{tr}(A), \det(A))$ и $v_n = v_n(\mathrm{tr}(A), \det(A))$. С помощью стандартных вычислений несложно линейно выразить последовательность $\{A^n\}_{n\in\mathbb{N}_0}$ через последовательности $\{u_nE\}_{n\in\mathbb{N}_0}$ и $\{v_nE\}_{n\in\mathbb{N}_0}$, которые удовлетворяют тем же рекуррентным соотношениям, что и последовательность $\{A^n\}_{n\in\mathbb{N}_0}$:

$$\{A^n\}_{n\in\mathbb{N}_0} = \left(A - \frac{\mathrm{tr}(A)}{2}\right)\{u_nE\}_{n\in\mathbb{N}_0} + \frac{1}{2}\{v_nE\}_{n\in\mathbb{N}_0}, \tag{61}$$

где $E \in M_2(\mathbb{C})$ – единичная матрица. Таким образом, для произвольного натурального числа n имеет место равенство

$$A^n = \begin{pmatrix} \dfrac{v_n}{2} + u_n\left(a - \dfrac{\mathrm{tr}(A)}{2}\right) & bu_n \\ cu_n & \dfrac{v_n}{2} + u_n\left(d - \dfrac{\mathrm{tr}(A)}{2}\right) \end{pmatrix}. \tag{62}$$

Из равенства (38) следует, что

$$A^n = \begin{pmatrix} u_{n+1} - du_n & bu_n \\ cu_n & u_{n+1} - au_n \end{pmatrix}. \tag{63}$$

Формула (63) приведена в работе [7], в которой она доказывается с помощью метода математической индукции. Формула (62) позволяет единообразно получить ряд результатов и наблюдений, встречающихся в различных работах. Применим формулу (62) к выражению вида $(a+b\sqrt{d})^n$, где $a, b \in \mathbb{Q}$, $n \in \mathbb{N}$ и $d > 1$ – натуральное число, не являющееся квадратом. Используя матричное представление

$$\begin{pmatrix} a & bd \\ b & a \end{pmatrix}$$

для $a + b\sqrt{d}$, из формулы (62) получаем

$$(a+b\sqrt{d})^n = \frac{1}{2}\, v_n(2a, N) + bu_n(2a, N)\sqrt{d}, \tag{64}$$

где $N = a^2 - b^2 d$. Заметим, что предыдущее соотношение можно также получить из равенств (37). Из (64) следуют равенства

$$\left(\frac{1+\sqrt{5}}{2}\right)^n = \frac{1}{2}\left(v_n(1,-1) + u_n(1,-1)\sqrt{5}\right) = \frac{1}{2}\left(L_n + F_n\sqrt{5}\right), \tag{65}$$

$$\left(\frac{1-\sqrt{5}}{2}\right)^n = \frac{1}{2}\left(v_n(1,-1) - u_n(1,-1)\sqrt{5}\right) = \frac{1}{2}\left(L_n - F_n\sqrt{5}\right). \tag{66}$$

Следовательно,

$$\sqrt[n]{\frac{1}{2}(L_n + F_n\sqrt{5})} = \frac{1+\sqrt{5}}{2}, \quad \sqrt[n]{\frac{1}{2}(L_n - F_n\sqrt{5})} = (-1)^{n+1}\left(\frac{1-\sqrt{5}}{2}\right)$$

(все рассматриваемые корни являются арифметическими). Таким образом,

$$1 = \sqrt[n]{\frac{1}{2}(L_n + F_n\sqrt{5})} + (-1)^{n+1}\sqrt[n]{\frac{1}{2}(L_n - F_n\sqrt{5})}. \tag{67}$$

Числами Пелля–Люка называется последовательность $\{Q_n\}_{n\in N_0}$, удовлетворяющая условиям

$$Q_0 = 1, \quad Q_1 = 1, \quad Q_{n+1} = 2Q_n + Q_{n-1}, \quad n \in \mathbb{N}. \tag{68}$$

Хорошо известно, что последовательность подходящих дробей к вещественному числу $\sqrt{2} = [1;\overline{2}\,]$ имеет вид $\dfrac{Q_0}{P_0}, \dfrac{Q_1}{P_1}, \ldots$, где $\{P_n\}_{n\in N_0}$ – числа Пелля, которые определяются согласно условиям

$$P_0 = 0, \quad P_1 = 1, \quad P_{n+1} = 2P_n + P_{n-1}, \quad n \in \mathbb{N}. \tag{69}$$

Из условий (31) и (68) следует, что $\{2Q_n\}_{n\in N_0} = \{v_n(2,-1)\}_{n\in N_0}$. Из формулы (64) следует, что последовательность $\{v_n(2,-1)\}_{n\in N_0}$ возникает при рассмотрении выражения $(1+\sqrt{2})^n$. Действительно, имеет место равенство

$$(1+\sqrt{2})^n = \frac{1}{2}\,v_n(2,-1) + u_n(2,-1)\sqrt{2} = Q_n + P_n\sqrt{2}.$$

Таким образом,

$$\sqrt[n]{Q_n + P_n\sqrt{2}} = 1+\sqrt{2}, \quad \sqrt[n]{Q_n - P_n\sqrt{2}} = (-1)^{n+1}(1-\sqrt{2}),$$

$$2 = \sqrt[n]{Q_n + P_n\sqrt{2}} + (-1)^{n+1}\sqrt[n]{Q_n - P_n\sqrt{2}}. \tag{70}$$

Рассмотрим уравнение Пелля

$$x^2 - dy^2 = 1, \tag{71}$$

где d – натуральное число, не являющееся квадратом. Пусть (x_1, y_1) – наименьшее решение уравнения (71) в натуральных числах. Хорошо известно, что тогда все решения уравнения (71) в натуральных числах образуют последовательность $\{(x_n, y_n)\}_{n\in\mathbb{N}}$, для членов которой выполнено равенство

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n.$$

Тогда согласно (64) имеем

$$(x_1 + y_1\sqrt{d})^n = \frac{1}{2}\,v_n(2x_1, 1) + y_1 u_n(2x_1, 1)\sqrt{d} = T_n(x_1) + y_1 U_n(x_1)\sqrt{d}.$$

Таким образом, получаем следующие формулы для решения уравнения (71) в натуральных числах

$$x_n = T_n(x_1) = \frac{1}{2}\sum_{i=0}^{[n/2]}(-1)^i\,\frac{n}{(n-i)}\binom{n-i}{i}(2x_1)^{n-2i},$$

$$y_n = y_1 U_n(x_1) = y_1\sum_{i=0}^{[(n-1)/2]}(-1)^i\binom{n-i-1}{i}(2x_1)^{n-2i-1}.$$

Последняя форма записи решений в натуральных числах уравнения (71) приведена в [28, с. 69]. Рассмотрим несколько более общую ситуацию. Пусть A – двумерная алгебра с единицей над полем P нулевой характеристики. В A существует базис вида 1_A, e, где $e^2 = \alpha 1_A$ и $\alpha \in P$. Тогда с помощью рассуждений, аналогичных приведенным выше, можно показать, что для всякого элемента $a+be \in A$, $a, b \in P$, удовлетворяющего условию $a^2 - \alpha b^2 = 1$, имеет место равенство

$$(a+be)^n = T_n(a) + bU_n(a)e.$$

В случае, когда P – поле вещественных чисел и $\alpha \neq 0$, последняя формула равносильна либо обыкновенной формуле Муавра, либо формуле Муавра для двойных чисел D, которая имеет вид

$$(\mathrm{ch}(x) + \mathrm{sh}(x)e)^n = \mathrm{ch}(nx) + \mathrm{sh}(nx)e, \quad e^2 = 1_D.$$

Таким образом, формулы (51), (59), (67), (70), (64) и аналогичные им можно рассматривать как естественные аналоги классической формулы Муавра. Как было отмечено выше, формулы, близкие к формуле Муавра, которая впервые в современной форме записи была приведена Л. Эйлером в его трактате «Введение в анализ бесконечных» [29, с. 114], встречаются в работах Ф. Виета, П. Ферма, Ф. Дюлорана, Г.В. Лейбница и Муавра в связи с задачами, связанными с решениями алгебраических уравнений деления круга на равные части. При этом алгебраические методы решения этих уравнений, предложенные в работах Ф. Дюлорана и Г.В. Лейбница, основаны на сопоставлении алгебраических уравнений с тождествами, близкими к соотношению (34).

Покажем как равенства, аналогичные (67) и (70), можно также получать с помощью уравнений Кардано. Пусть $A, B \in \mathbb{R}$ и $\{v_n\}_{n\in N_0}$ – последовательность, удовлетворяющая условиям:

$$v_0 = 2, \quad v_1 = A, \quad \ldots, \quad v_{n+1} = Av_n - Bv_{n-1}, \quad n \in \mathbb{N}. \tag{72}$$

Из тождества (34) следует, что для каждого $n \in \mathbb{N}$ число A является корнем уравнения Кардано

$$\sum_{i=0}^{[n/2]} (-1)^i \, \frac{n}{n-i} \binom{n-i}{i} B^i x^{n-2i} = v_n. \tag{73}$$

Предположим, что для некоторого нечетного натурального числа $n > 1$ выполнено условие $v_n^2 - 4B^n > 0$. Из теоремы 1 следует, что в этом случае алгебраическое уравнение (73) обладает единственным вещественным корнем. Таким образом, имеет место равенство

$$A = \sqrt[n]{\frac{1}{2}(v_n + \sqrt{v_n^2 - 4B^n})} + \sqrt[n]{\frac{1}{2}(v_n - \sqrt{v_n^2 - 4B^n})}. \tag{74}$$

В последнем равенстве предполагается, что все радикалы принимают вещественные значения. Пусть α – наибольший из корней уравнения $x^2 - Ax + B = 0$. Тогда из теоремы 1 следует равенство

$$\alpha = \sqrt[n]{\frac{1}{2}(v_n + \sqrt{v_n^2 - 4B^n})}. \tag{75}$$

Если для некоторого четного натурального числа n числа v_n, $v_n^2 - 4B^n$ и B являются положительными, то аналогично получаем равенства (74) и (75). В качестве примера рассмотрим выражение $\sqrt[5]{\frac{123}{2} + \frac{55}{2}\sqrt{5}}$. Используя предыдущие обозначения, находим, что $v_5 = 123$ и из равенства $v_5^2 - 4B^5 = 5 \cdot 55^2$ получаем $B = 1$. Следовательно, выражение $\sqrt[5]{\frac{123}{2} + \frac{55}{2}\sqrt{5}} + \sqrt[5]{\frac{123}{2} - \frac{55}{2}\sqrt{5}}$ является единственным вещественным корнем уравнения $123 = x^5 - 5x^3 + 5x$. С другой стороны, 3 является корнем этого уравнения. Таким образом, $3 = \sqrt[5]{\frac{123}{2} + \frac{55}{2}\sqrt{5}} + \sqrt[5]{\frac{123}{2} - \frac{55}{2}\sqrt{5}}$. Следовательно, $\sqrt[5]{\frac{123}{2} + \frac{55}{2}\sqrt{5}}$ – наибольший из корней уравнения $x^2 - 3x + 1 = 0$. Таким образом, $\sqrt[5]{\frac{123}{2} + \frac{55}{2}\sqrt{5}} = \frac{3 + \sqrt{5}}{2}$.

В статье [30] приведены тождества, аналогичные тождествам Куммера. В этой работе были доказаны следующие тождества:

$$(x+y)^{2n+1} - x^{2n+1} - y^{2n+1} = \\ = \sum_{k=0}^{[(n-1)/3]} \frac{2n+1}{n-k} \binom{n-k}{2k+1} (xy(x+y))^{2k+1} (x^2 + xy + y^2)^{n-3k-1}, \tag{76}$$

$$(x+y)^{2n}+x^{2n}+y^{2n}=\sum_{k=0}^{[n/3]}\frac{2n}{n-k}\binom{n-k}{2k}(xy(x+y))^{2k}(x^2+xy+y^2)^{n-3k}, \quad (77)$$

$$x^{2n}+y^{2n}=\sum_{k=0}^{n}\omega_{k,n}(xy)^k(x^2+xy+y^2)^{n-k}, \quad (78)$$

где $\omega_{k,n}\sum_{i=0}^{k}(-1)^i\frac{2n}{2n-i}\binom{2n-i}{i}\binom{n-i}{k-i}$.

Приведем некоторые дополнения к этим результатам. В работе [30] формула (78) выводится с помощью несложных преобразований из формулы (34). Аналогичными преобразованиями из формулы (33) можно вывести тождество

$$\frac{x^{2n+1}-y^{2n+1}}{x-y}=\sum_{k=0}^{n}\eta_{k,n}(xy)^k(x^2+xy+y^2)^{n-k}, \quad (79)$$

где $\eta_{k,n}=\sum_{i=0}^{k}(-1)^i\binom{2n-i}{i}\binom{n-i}{k-i}$. Для каждого натурального числа n рассмотрим следующий определитель тридиагональной матрицы размера $n\times n$:

$$g_n(x,y)=\begin{vmatrix} y-x & -y & 0 & \dots & 0 & 0\\ -y & y-x & -y & \dots & 0 & 0\\ 0 & -y & y-x & \dots & 0 & 0\\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots\\ 0 & 0 & 0 & \dots & y-x & -y\\ 0 & 0 & 0 & \dots & -y & -x \end{vmatrix}. \quad (80)$$

Непосредственно проверяется, что последовательность $\{g_n(x,y)\}_{n\in\mathbb{N}}$ является рекуррентной и удовлетворяет условиям:

$$\begin{aligned} &g_1(x,y)=-x, \quad g_2(x,y)=x^2-xy-y^2,\\ &g_{n+2}(x,y)=(y-x)g_{n+1}(x,y)-y^2g_n(x,y), \quad n\in\mathbb{N}. \end{aligned} \quad (81)$$

Для каждого натурального числа n через $f_n(x,y)$ обозначим многочлен вида

$$(-1)^n\sum_{k=0}^{n}\eta_{k,n}y^kx^{n-k}.$$

Из равенства (79) следует, что

$$(-1)^n\,\frac{x^{2n+1}-y^{2n+1}}{x-y}= \\ =(-1)^n\sum_{k=0}^{n}\eta_{k,n}(xy)^k(x^2+xy+y^2)^{n-k}=f_n(x^2+xy+y^2,xy). \quad (82)$$

Так как

$$(-1)^{n+2}\,\frac{x^{2n+5}-y^{2n+5}}{x-y}= \\ =(-1)^{n+1}(-x^2-y^2)\,\frac{x^{2n+3}-y^{2n+3}}{x-y}-(-1)^nx^2y^2\,\frac{x^{2n+1}-y^{2n+1}}{x-y},$$

то согласно (82) для каждого натурального числа n имеем

$$f_{n+2}(x^2+xy+y^2,xy) = \\ = (xy-(x^2+xy+y^2))f_{n+1}(x^2+xy+y^2,xy) - x^2y^2 f_n(x^2+xy+y^2,xy).$$

Так как рациональные дроби xy, $x^2+xy+y^2 \in \mathbb{C}(x,y)$ алгебраически независимы над $\mathbb{C}$, то для каждого натурального числа n выполнено равенство

$$f_{n+2}(x,y) = (y-x)f_{n+1}(x,y) - y^2 f_n(x,y). \tag{83}$$

Поскольку $f_1(x,y) = -x$ и $f_2(x,y) = x^2 - xy - y^2$, то из условий (81) и рекуррентного соотношения (83), которому удовлетворяют члены последовательности $\{f_n(x,y)\}_{n\in\mathbb{N}}$, окончательно получаем равенства

$$\sum_{k=0}^{n} \eta_{k,n} y^k x^{n-k} = (-1)^n g_n(x,y), \tag{84}$$

$$\frac{x^{2n+1}-y^{2n+1}}{x-y} = (-1)^n g_n(x^2+xy+y^2,xy). \tag{85}$$

Иоганном Кеплером в трактате «Гармония мира» [31] было сделано интересное наблюдение, согласно которому у произвольного правильного семиугольника $A_1A_2A_3A_4A_5A_6A_7$, вписанного в единичную окружность, квадраты длин хорд A_1A_2, A_1A_3, A_1A_4 являются корнями алгебраического уравнения с целыми коэффициентами

$$x^3 - 7x^2 + 14x - 7 = 0.$$

В [6] этот факт был обобщен на случай произвольного правильного n-угольника $(n > 2)$. Было доказано утверждение, согласно которому у произвольного правильного n-угольника $A_1A_2\ldots A_n$, вписанного в единичную окружность, квадраты длин хорд $A_1A_2, \ldots, A_1A_{[(n-1)/2]+1}$, равные соответственно $4\sin^2\dfrac{\pi}{n}, \ldots, 4\sin^2\dfrac{\pi\left[\frac{n-1}{2}\right]}{n}$, являются корнями характеристического многочлена тридиагональной матрицы размера $([(n-1)/2]\times[(n-1)/2])$, которая в случае нечетного $n = 2m+1$ имеет вид

$$A_m = \begin{pmatrix} 2 & 1 & 0 & \ldots & 0 & 0 \\ 1 & 2 & 1 & \ldots & 0 & 0 \\ 0 & 1 & 2 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 2 & 1 \\ 0 & 0 & 0 & \ldots & 1 & 3 \end{pmatrix}, \tag{86}$$

а в случае четного $n = 2m+2$ имеет вид

$$B_m = \begin{pmatrix} 2 & 1 & 0 & \ldots & 0 & 0 \\ 1 & 2 & 1 & \ldots & 0 & 0 \\ 0 & 1 & 2 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 2 & 1 \\ 0 & 0 & 0 & \ldots & 1 & 2 \end{pmatrix}. \tag{87}$$

Заметим, что в случае нечетного натурального числа $n = 2m+1$ приведенное выше утверждение следует из ранее установленного тождества (85). Действительно, согласно (85) числа $1+2\cos\dfrac{2\pi i}{n}$ $(1 \le i \le m)$ являются корнями многочлена

$g_n(x,1)$. Тогда квадраты длин хорд $A_1A_2,\dots,A_1A_{m+1}$ являются корнями многочлена $g_m(3-x,1)$. При этом несложно заметить, что $(-1)^m g_m(3-x,1)=\chi_{A_m}(x)$.

Кроме того, заметим, что с помощью формул Куммера (33) и (34) для каждого натурального числа $n>2$ несложно явно выписать многочлен, корнями которого являются квадраты длин хорд $A_1A_2,\dots,A_1A_{[(n-1)/2]+1}$ правильного n-угольника $A_1A_2\dots A_n$, вписанного в единичную окружность, и тем самым явно выписать характеристические многочлены матриц A_m и B_m. Пусть $n=2m+1$, где $m\in\mathbb{N}$. Согласно (34) имеем равенство

$$\frac{x^n-x^{-n}}{x-x^{-1}}=\sum_{k=0}^{m}\frac{n}{n-k}\binom{n-k}{k}(x-x^{-1})^{2m-2k}. \tag{88}$$

В предыдущем тождестве положим $x=e^{\alpha i}$. Тогда

$$\frac{\sin n\alpha}{\sin\alpha}=\sum_{k=0}^{m}(-1)^{m-k}\frac{n}{n-k}\binom{n-k}{k}(4\sin^2\alpha)^{m-k}. \tag{89}$$

Из последнего равенства следует, что вещественные числа $\left\{4\sin^2\dfrac{\pi k}{n}\right\}_{k=1}^{m}$ являются корнями многочлена

$$\sum_{k=0}^{m}(-1)^k\,\frac{n}{n-k}\binom{n-k}{k}x^{m-k}=x^m+\sum_{k=0}^{m-1}(-1)^{m-k}\frac{n}{m-k}\binom{m+k}{2k+1}x^k. \tag{90}$$

Таким образом,

$$\chi_{A_m}(x)=x^m+\sum_{k=0}^{m-1}(-1)^{m-k}\frac{n}{m-k}\binom{m+k}{2k+1}x^k=\prod_{k=1}^{m}\left(x-4\sin^2\frac{\pi k}{n}\right). \tag{91}$$

Пусть $n=2m+2$, где $m\in\mathbb{N}$. Из (33) следует равенство

$$\frac{x^n-x^{-n}}{x^2-x^{-2}}=\sum_{k=0}^{m}\binom{n-1-k}{k}(x-x^{-1})^{2m-2k}. \tag{92}$$

В предыдущем тождестве положим $x=e^{\alpha i}$. Тогда

$$\frac{\sin n\alpha}{\sin 2\alpha}=\sum_{k=0}^{m}(-1)^{m-k}\binom{n-1-k}{k}(4\sin^2\alpha)^{m-k}. \tag{93}$$

Из последнего равенства следует, что вещественные числа $\left\{4\sin^2(\dfrac{\pi k}{n})\right\}_{k=1}^{m}$ являются корнями многочлена

$$\sum_{k=0}^{m}(-1)^k\binom{n-1-k}{k}x^{m-k}=x^m+\sum_{k=0}^{m-1}(-1)^{m-k}\binom{m+1+k}{2k+1}x^k. \tag{94}$$

Таким образом,

$$\chi_{B_m}(x)=x^m+\sum_{k=0}^{m-1}(-1)^{m-k}\binom{m+1+k}{2k+1}x^k=\prod_{k=1}^{m}\left(x-4\sin^2\frac{\pi k}{n}\right). \tag{95}$$

Равенства (91) и (95) также доказаны другим способом в работе [5]. Как отмечено авторами статьи, эти равенства сначала ими были установлены экспериментально, а затем доказаны с помощью метода математической индукции с использованием рекуррентных соотношений, которым удовлетворяют многочлены, участвующие в равенствах (91) и (95).

Равенства (91) и (95) могут быть использованы при изучении геометрических свойств правильных многоугольников. Через $d_1, \dots, d_{[(n-1)/2]}$ обозначим квадраты длин хорд $A_1A_2, \dots, A_1A_{[(n-1)/2]+1}$ правильного n-угольника $A_1A_2\dots A_n$, вписанного в единичную окружность. Пусть n – нечетно и $n = 2m+1$. Так как свободный член многочлена (91) равен $(-1)^m n$, а коэффициент при x^{m-1} равен $-n$, то приходим к равенству

$$d_1 + \dots + d_m = d_1 \cdots d_m = n. \tag{96}$$

Так как коэффициент при x у многочлена (91) равен $\dfrac{(-1)^{m-1}nm(m+1)}{6}$, то

$$\frac{1}{d_1} + \dots + \frac{1}{d_m} = \frac{d_2 \cdots d_m + d_1 d_3 \cdots d_m + \dots + d_1 \cdots d_{m-1}}{d_1 \cdots d_m} = \frac{m(m+1)}{6}.$$

Аналогично в случае, когда n четно и $n = 2(m+1)$, с помощью многочлена (95) получаем равенства

$$d_1 + \dots + d_m + 2 = d_1 \cdots d_m = \frac{n}{2}.$$

Отметим, что равенства (96) при $n = 5, 7$ приведены в [32, с. 491]. Предыдущие соотношения и равенства (96) также можно получить, используя разложение многочлена $x^n - 1$ на линейные множители.

Из определений чисел Фибоначчи и чисел Люка и из соотношений (33), (34) следует, что для произвольного натурального числа n имеют место следующие хорошо известные тождества:

$$F_n = \sum_{i=0}^{[(n-1)/2]} \binom{n-i-1}{i}, \quad L_n = \sum_{i=0}^{[n/2]} \frac{n}{n-i}\binom{n-i}{i}. \tag{97}$$

Тогда из соотношений (90), (91), (94), (95) следует, что для произвольного $n \in \mathbb{N}$ выполнены равенства

$$L_{2n+1} = \sum_{i=0}^{n} \frac{2n+1}{2n+1-i}\binom{2n+1-i}{i} = (-1)^n \chi_{A_n}(-1) = \prod_{k=1}^{n}(1+d_k),$$

$$F_{2n+2} = \sum_{i=0}^{n} \binom{2n+1-i}{i} = (-1)^n \chi_{B_n}(-1) = \prod_{k=1}^{n}(1+d_k).$$

Таким образом, для правильного n-угольника $A_1A_2\dots A_n$, $n > 2$, вписанного в единичную окружность, имеет место соотношение

$$\prod_{k=1}^{[\frac{n-1}{2}]}(1+d_k) = \begin{cases} F_n, & \text{если} \quad n \quad \text{четно}, \\ L_n, & \text{если} \quad n \quad \text{нечетно}. \end{cases} \tag{98}$$

Для того чтобы подчеркнуть важность тождеств (33), (34) и аналогичных им, приведем два коротких доказательства квадратичного закона взаимности, основанных на этих соотношениях.

Приведенное ниже утверждение непосредственно следует из леммы Гаусса [33, с. 589].

Лемма. *Для любых различных нечетных простых чисел p и q имеет место равенство*

$$\prod_{k=1}^{(p-1)/2} \frac{\varepsilon_p^{qk} - \varepsilon_p^{-qk}}{\varepsilon_p^{k} - \varepsilon_p^{-k}} = \left(\frac{q}{p}\right). \tag{99}$$

Пусть p и q – различные простые нечетные числа. Приведем доказательство закона взаимности, основанного на рассуждениях из работы Эйзенштейна [34], в которой неявно используются многочлены Чебышева второго рода и, следовательно, тождество (33). Из (33) следует соотношение

$$\frac{x^q - x^{-q}}{x - x^{-1}} = \sum_{k=0}^{(q-1)/2} (-1)^k \binom{q-k-1}{k} (x + x^{-1})^{q-1-2k} =$$
$$= \sum_{k=0}^{(q-1)/2} (-1)^k \binom{q-k-1}{k} ((x - x^{-1})^2 + 4)^{(q-1)/2-k}. \tag{100}$$

Тогда для $j = 1, \ldots, (q-1)/2$ имеет место равенство

$$\sum_{k=0}^{(q-1)/2} (-1)^k \binom{q-k-1}{k} ((\varepsilon_q^{j} - \varepsilon_q^{-j})^2 + 4)^{(q-1)/2-k} = 0. \tag{101}$$

Несложно заметить, что положительные вещественные числа $\left\{\sin \dfrac{2\pi k}{q}\right\}_{k=1}^{(q-1)/2}$ попарно различны. Следовательно, согласно равенству (101) имеем

$$\sum_{k=0}^{(q-1)/2} (-1)^k \binom{q-k-1}{k} (t+4)^{(q-1)/2-k} = \prod_{k=1}^{(q-1)/2} (t - (\varepsilon_q^{k} - \varepsilon_q^{-k})^2). \tag{102}$$

Из последнего равенства и равенства (100) следует тождество

$$\frac{x^q - x^{-q}}{x - x^{-1}} = \prod_{k=1}^{(q-1)/2} ((x - x^{-1})^2 - (\varepsilon_q^{k} - \varepsilon_q^{-k})^2). \tag{103}$$

Тогда

$$\left(\frac{q}{p}\right) = \prod_{i=1}^{(p-1)/2} \frac{\varepsilon_p^{qk} - \varepsilon_p^{-qk}}{\varepsilon_p^{k} - \varepsilon_p^{-k}} = \prod_{k=1}^{(p-1)/2} \prod_{i=1}^{(q-1)/2} ((\varepsilon_p^{k} - \varepsilon_p^{-k})^2 - (\varepsilon_q^{i} - \varepsilon_q^{-i})^2) =$$
$$= (-1)^{(p-1)/2\cdot(q-1)/2} \prod_{k=1}^{(p-1)/2} \prod_{i=1}^{(q-1)/2} \left((\varepsilon_q^{i} - \varepsilon_q^{-i})^2 - (\varepsilon_p^{k} - \varepsilon_p^{-k})^2\right) =$$
$$= (-1)^{(p-1)/2\cdot(q-1)/2} \left(\frac{p}{q}\right).$$

Приведем доказательство квадратичного закона взаимности, в котором используется тождество (34), основанное на рассуждениях из работы Ж. Лиувилля [35]. Несложно заметить, что все коэффициенты, участвующие в соотношении (34), являются целыми числами. Рассмотрим тождество (34) при $n = q$ по модулю простого числа p. В результате получим тождество следующего вида для многочленов от двух переменных a и b с коэффициентами из поля $\mathbb{F}_p$:

$$a^q + b^q = \sum_{i=0}^{[q/2]} m_i (a+b)^{q-2i} (ab)^i, \tag{104}$$

где $m_i \in \mathbb{F}_p$. Заметим, что согласно тождеству (34) имеет место равенство $m_{(q-1)/2} = (-1)^{(q-1)/2}q$. Пусть ε_q – примитивный корень из единицы степени q из некоторого расширения поля $\mathbb{F}_p$. Подставляя вместо a и b в тождество (104) соответственно $a\varepsilon_q^i$ и $b\varepsilon_q^{-i}$, где $0 \le i \le q-1$, получим соотношения вида

$$a^q + b^q = \sum_{i=0}^{[q/2]} m_i(a\varepsilon_q^i + b\varepsilon_q^{-i})^{q-2i}(ab)^i. \tag{105}$$

Таким образом, имеет место равенство

$$\prod_{i=0}^{q-1}(t - (\varepsilon_q^i a + \varepsilon_q^{-i} b)) = \sum_{i=0}^{[q/2]} m_i t^{q-2i}(ab)^i - (a^q + b^q). \tag{106}$$

Положим в последнем равенстве $a = 1,\ b = -1$. В результате получим соотношение

$$t\prod_{i=1}^{q-1}(t - (\varepsilon_q^i - \varepsilon_q^{-i})) = \sum_{i=0}^{[q/2]}(-1)^i m_i t^{q-2i}. \tag{107}$$

Сравнивая коэффициенты при первой степени t с обеих частей последнего тождества, получаем равенства

$$q = \prod_{i=1}^{q-1}(\varepsilon_q^i - \varepsilon_q^{-i}) = (-1)^{(q-1)/2}\prod_{i=1}^{(q-1)/2}(\varepsilon_q^i - \varepsilon_q^{-i})^2. \tag{108}$$

Отметим, что соотношения (103) и (108) также можно получить, используя разложения многочлена $x^q - 1$ на линейные множители. Из (108) следует, что в поле $\mathbb{F}_p$ имеют место равенства

$$\left(\frac{q}{p}\right) = q^{(p-1)/2} = (-1)^{(q-1)2\cdot(p-1)/2}\prod_{i=1}^{(q-1)/2}(\varepsilon_q^i - \varepsilon_q^{-i})^{p-1} =$$
$$= (-1)^{(q-1)2\cdot(p-1)/2}\prod_{i=1}^{(q-1)/2}\frac{\varepsilon_q^{pi} - \varepsilon_q^{-pi}}{\varepsilon_q^i - \varepsilon_q^{-i}} = (-1)^{(q-1)/2\cdot(p-1)/2}\left(\frac{p}{q}\right).$$

Заметим, что в работе Ж. Лиувилля, содержание которой воспроизведено в монографии [36], используются комплексные примитивные корни из единицы.

3. Алгебраические уравнения, близкие к уравнениям Кардано

Неполные кубические уравнения, биквадратные уравнения и уравнения Муавра являются частными случаями уравнения Кардано. В настоящем параграфе изучено семейство алгебраических уравнений, которое является расширением алгебраических уравнений вида (12) на случай произвольных степеней, и найдена формула решений уравнений из этого семейства, частным случаем которой является формула (14).

Положим в тождестве (36) $t = x,\ y = t,\ x = -y$. В результате получим соотношение

$$\prod_{i=0}^{n-1}(t - (\varepsilon_n^i x + \varepsilon_n^{2i} y)) = t^n - \sum_{i=1}^{[n/2]}\frac{n}{n-i}\binom{n-i}{i}x^{n-2i}y^i t^i - x^n + (-1)^n y^n. \tag{109}$$

Следовательно, имеет место тождество

$$(a+b)^n - a^n + (-1)^n b^n = \sum_{i=1}^{[n/2]} \frac{n}{n-i} \binom{n-i}{i} a^{n-2i} b^i (a+b)^i. \tag{110}$$

Частным случаем предыдущего тождества является соотношение (19). Рассмотрим следующее семейство алгебраических уравнений:

$$x^n = \sum_{i=1}^{[n/2]} \frac{2n+1}{n-i} \binom{n-i}{i} \frac{p^{i-1}}{q^{i-2}}\, x^i + \frac{q^2}{p} - (-1)^n \frac{p^{n-2}}{q^{n-4}}. \tag{111}$$

Из (109) следует, что если в качестве a, b выбрать числа, удовлетворяющие равенствам $a^{n-4}b^2 = p$ и $a^{n-2}b = q$, то корни уравнения (111) будут иметь вид $\varepsilon_n^i a + \varepsilon_n^{2i} b$, $i = 1, \ldots, n$. Таким образом, получаем формулу решения уравнения (111)

$$x = \varepsilon_n^i \sqrt[n]{\frac{q^2}{p}} + \varepsilon_n^{2i} \sqrt[n]{\frac{p^{n-2}}{q^{n-4}}}, \quad i = 1, \ldots, n. \tag{112}$$

Примером уравнений вида (111) являются уравнения пятой степени вида (12), впервые рассмотренные Л. Эйлером. Формула решений этих уравнений (14) является частным случаем формулы (112).

Отметим, что тождество (110) в случае, когда $n = 3$, дает еще один способ решения кубических уравнений. Действительно, рассмотрим уравнение

$$x^3 = px + q. \tag{113}$$

Из равенства

$$(a+b)^3 = 3ab(a+b) + \frac{(ab)^2}{a^2b^{-1}} + a^2b^{-1}ab$$

следует, что если в качестве m и n выбрать числа, для которых выполнены равенства

$$3m = p, \quad \frac{m^2}{n} + nm = q,$$

то решения (113) уравнения будут иметь вид

$$x = a + b,$$

где a и b – значения соответственно $\sqrt[3]{mn}$ и $\sqrt[3]{\frac{m^2}{n}}$, для которых выполнено условие $ab = m$. Таким образом, получаем формулу решения уравнения (113)

$$x = \sqrt[3]{\frac{np}{3}} + \frac{p}{3\sqrt[3]{\frac{np}{3}}}, \tag{114}$$

где n – один из корней квадратного уравнения $3px^2 - 9qx + p^2 = 0$. Если в формулу (114) вместо n подставить его выражение через p и q, то есть $\dfrac{9q + \sqrt{81q^2 - 12p^3}}{6p}$, то формула (114) преобразуется в формулу Кардано.

Из (110) следует тождество

$$(a+b)^{2n+1} - a^{2n+1} - b^{2n+1} = \sum_{i=0}^{n-1} \frac{2n+1}{n+1+i} \binom{n+1+i}{n-i} a^{2i+1} b^{n-i} (a+b)^{n-i}. \tag{115}$$

Рассмотрим следующее семейство алгебраических уравнений:

$$t^{2n+1} = \sum_{i=0}^{n-1} \frac{1}{(n+1+i)(n^2+n)^i} \binom{n+1+i}{n-i} \frac{(6q)^i}{p^{i-1}}\, t^{n-i} + \\ + \frac{p^3(n^2+n)}{6q(2n+1)^2} + \frac{(6q)^n}{p^{n-1}(n^2+n)^n(2n+1)}. \quad (116)$$

При $n = 2, 3, 4$ семейства алгебраических уравнений вида (116) были рассмотрены в работе [9]. Пусть a и b – некоторое решение системы

$$p = (2n+1)ab^n, \quad q = \frac{(n+1)n(2n+1)}{6}\, a^3 b^{n-1}.$$

Тогда имеют место равенства

$$a^{2n+1} = \frac{(6q)^n}{p^{n-1}(n^2+n)^n(2n+1)}, \quad b^{2n+1} = \frac{p^3(n^2+n)}{6q(2n+1)^2},$$

$$\frac{2n+1}{n+1+i}\binom{n+1+i}{n-i} a^{2i+1} b^{n-i} = \frac{1}{(n+1+i)(n^2+n)^i}\binom{n+1+i}{n-i}\frac{(6q)^i}{p^{i-1}},$$

и из (109) и (115) следует формула решений уравнения вида (116)

$$x_m = \sqrt[2n+1]{\frac{(6q)^n}{p^{n-1}(n^2+n)^n(2n+1)}}\, \exp\left(\frac{2\pi m i}{2n+1}\right) + \\ + \sqrt[2n+1]{\frac{p^3(n^2+n)}{6q(2n+1)^2}}\, \exp\left(\frac{4\pi m i}{2n+1}\right), \quad 0 \le m \le 2n. \quad (117)$$

В частности, при $n = 2, 3, 4$ из (117) получаем формулы решений уравнений (3), (5), (7) из [9], где также рассматриваются аналогичные семейства алгебраических уравнений степеней 6, 8 и 10. Для этих же семейств алгебраических уравнений можно найти расширение на семейство алгебраических уравнений произвольной четной степени и выписать формулу решения для этого семейства.

Пусть $tx^3 - ax - b$ – многочлен с коэффициентами из поля рациональных дробей $\mathbb{C}(a, b, t)$ от переменных a, b, t и α_1, α_2, α_3 – корни этого многочлена из некоторого алгебраического замыкания поля $\mathbb{C}(a, b, t)$. Найдем явное выражение для коэффициентов многочлена $\prod_{i=0}^{n-1}(t - a\varepsilon_n^{2i} - b\varepsilon_n^{3i}) \in \mathbb{C}(a, b)[t]$. Имеют место равенства

$$\prod_{i=0}^{n-1}(t - a\varepsilon_n^{2i} - b\varepsilon_n^{3i}) = (-1)^{n-1}\prod_{i=0}^{n-1}(t\varepsilon_n^{3i} - a\varepsilon_n^{i} - b) = \\ = (-1)^{n-1}(-1)^{3n} t^n (\alpha_1^n - 1)(\alpha_2^n - 1)(\alpha_3^n - 1) = \\ = t^n\left(-\frac{b^n}{t^n} + \alpha_1^n\alpha_2^n + \alpha_1^n\alpha_3^n + \alpha_2^n\alpha_3^n - (\alpha_1^n + \alpha_2^n + \alpha_3^n) + 1\right).$$

В предыдущих равенствах мы воспользовались тем фактом, что для произвольных элементов $a_1, \ldots, a_m$, $b_1, \ldots, b_n$ из некоторого поля P и любых ненулевых элементов $a_0, b_0 \in P$ для многочленов $f(x) = a_0(x - a_1)\cdots(x - a_m)$, $g(x) = b_0(x - b_1)\cdots(x - b_n) \in P[x]$ выполнены равенства

$$a_0^n \prod_{i=1}^{m} g(a_i) = (-1)^{mn}\, b_0^m \prod_{i=1}^{n} f(b_i) = \mathrm{Res}(f, g).$$

Так как

$$\alpha_1+\alpha_2+\alpha_3=0,$$
$$\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3=-\frac{a}{t},$$
$$\alpha_1\alpha_2\alpha_3=\frac{b}{t},$$

то согласно формуле Жирара–Варинга (39) имеем

$$\alpha_1^n+\alpha_2^n+\alpha_3^n=\sum_{2r_1+3r_2=n}(-1)^{r_1}\frac{n(r_1+r_2-1)!}{r_1!r_2!}\left(-\frac{a}{t}\right)^{r_1}\left(\frac{b}{t}\right)^{r_2}=$$
$$=\sum_{n/3\le k\le n/2}\frac{n}{k}\binom{k}{n-2k}a^{-n+3k}b^{n-2k}t^{-k}=\sum_{n/2\le k\le 2n/3}\frac{n}{n-k}\binom{n-k}{2k-n}a^{2n-3k}b^{2k-n}t^{k-n}.$$

Учитывая тот факт, что $\alpha_1\alpha_2,\ \alpha_1\alpha_3,\ \alpha_2\alpha_3$ – корни уравнения $x^3+\dfrac{a}{t}x^2-\dfrac{b^2}{t^2}=0$, аналогично получаем равенства

$$\alpha_1^n\alpha_2^n+\alpha_1^n\alpha_3^n+\alpha_2^n\alpha_3^n=\sum_{r_1+3r_2=n}\frac{n(r_1+r_2-1)!}{r_1!r_2!}\left(-\frac{a}{t}\right)^{r_1}\left(\frac{b^2}{t^2}\right)^{r_2}=$$
$$=\sum_{2n/3\le k\le n}\frac{n}{2k-n}\binom{2k-n}{n-k}\left(-\frac{a}{t}\right)^{-2n+3k}\left(\frac{b^2}{t^2}\right)^{n-k}=$$
$$=\sum_{2n/3\le k\le n}(-1)^k\,t^{-k}\frac{n}{2k-n}\binom{2k-n}{n-k}a^{-2n+3k}b^{2(n-k)}=$$
$$=\sum_{0\le i\le n/3}(-1)^{n-i}t^{i-n}\frac{n}{n-2i}\binom{n-2i}{i}a^{n-3i}b^{2i}.$$

Таким образом,

$$\prod_{i=0}^{n-1}(t-a\varepsilon_n^{2i}-b\varepsilon_n^{3i})=t^n\left(-\frac{b^n}{t^n}+\sum_{0\le i\le\frac{n}{3}}(-1)^{n-i}t^{i-n}\frac{n}{n-2i}\binom{n-2i}{i}a^{n-3i}b^{2i}-\right.$$
$$\left.-\sum_{n/2\le i\le 2n/3}\frac{n}{n-i}\binom{n-i}{2i-n}a^{2n-3i}b^{2i-n}t^{i-n}+1\right)=$$
$$=t^n-\sum_{n/2\le i\le 2n/3}\frac{n}{n-i}\binom{n-i}{2i-n}a^{2n-3i}b^{2i-n}t^i+$$
$$+\sum_{1\le i\le n/3}(-1)^{n-i}\frac{n}{n-2i}\binom{n-2i}{i}a^{n-3i}b^{2i}t^i+(-1)^na^n-b^n. \quad (118)$$

В частности, имеет место соотношение

$$(-1)^{n-1}a^n+b^n=(a+b)^n-$$
$$-\sum_{n/2\le i\le 2n/3}\frac{n}{n-i}\binom{n-i}{2i-n}a^{2n-3i}b^{2i-n}(a+b)^i+$$
$$+\sum_{1\le i\le n/3}(-1)^{n-i}\frac{n}{n-2i}\binom{n-2i}{i}a^{n-3i}b^{2i}(a+b)^i. \quad (119)$$

Рассмотрим семейство алгебраических уравнений

$$t^n - q\sum_{n/2\le i\le 2n/3}\frac{n}{n-i}\binom{n-i}{2i-n}p^i t^i + \\ + q^2p^n\sum_{1\le i\le n/3}(-1)^{n-i}\frac{n}{n-2i}\binom{n-2i}{i}p^it^i = (-1)^{n-1}q^2p^n + q^3p^{2n}. \quad (120)$$

Из тождества (119) следует, что если в качестве $a,\ b$ взять числа, удовлетворяющие соотношениям

$$a^n = q^2p^n, \quad b^n = q^3p^{2n},$$

то $x = a+b$ является решением уравнения (120). Тогда из (119) следует, что корни уравнения (120) имеют вид

$$x = \varepsilon_n^{2i}\sqrt[n]{q^2}p + \varepsilon_n^{3i}\sqrt[n]{q^3}p^2, \quad i = 1,\ldots,n.$$

Из (118) с помощью замен переменных несложно получить следующие соотношения:

$$\prod_{i=0}^{n-1}(t - a\varepsilon_n^i - b\varepsilon_n^{-2i}) = t^n - \sum_{n/2\le i\le 2n/3}\frac{n}{n-i}\binom{n-i}{2i-n}a^{2i-n}b^it^{2n-3i} + \\ + \sum_{1\le i\le n/3}(-1)^i\frac{n}{n-2i}\binom{n-2i}{i}a^{2i}b^it^{n-3i} + (-1)^nb^n - a^n, \quad (121)$$

$$\prod_{i=0}^{n-1}(t - a\varepsilon_n^i - b\varepsilon_n^{3i}) = t^n + \sum_{n/2\le i\le 2n/3}(-1)^i\frac{n}{n-i}\binom{n-i}{2i-n}a^{2n-3i}b^it^{2i-n} - \\ - \sum_{1\le i\le n/3}\frac{n}{n-2i}\binom{n-2i}{i}a^{n-3i}b^it^{2i} - a^n - b^n. \quad (122)$$

Как показано в работе [24], с помощью многочленов Чебышева и связанных с ними уравнений Кардано могут быть получены нетривиальные тригонометрические тождества. Приведем несложные примеры аналогичных приложений рассмотренных выше семейств алгебраических уравнений и связанных с ними тождеств.

Так как согласно (118) $\alpha = \varepsilon_n^2 + \varepsilon_n^3 = 2\cos\frac{\pi}{n}\left(\cos\frac{5\pi}{n} + i\sin\frac{5\pi}{n}\right)$ является корнем многочлена

$$f(t) = t^n - \sum_{n/2\le i\le 2n/3}\frac{n}{n-i}\binom{n-i}{2i-n}t^i + \sum_{1\le i\le n/3}(-1)^{n-i}\frac{n}{n-2i}\binom{n-2i}{i}t^i + (-1)^n - 1,$$

то $\mathrm{Re}(f(\alpha)) = 0$ и $\mathrm{Im}(f(\alpha)) = 0$. Таким образом,

$$\left(2\cos\frac{\pi}{n}\right)^n = \sum_{1\le i\le n/3}(-1)^{n-i}\frac{n}{n-2i}\binom{n-2i}{i}\cos\frac{5\pi i}{n}\left(2\cos\frac{\pi}{n}\right)^i - \\ - \sum_{n/2\le i\le 2n/3}\frac{n}{n-i}\binom{n-i}{2i-n}\cos\frac{5\pi i}{n}\left(2\cos\frac{\pi}{n}\right)^i + (-1)^n - 1,$$

$$\sum_{1\le i\le n/3}(-1)^{n-i}\frac{n}{n-2i}\binom{n-2i}{i}\sin\frac{5\pi i}{n}\left(2\cos\frac{\pi}{n}\right)^i=$$
$$=\sum_{n/2\le i\le 2n/3}\frac{n}{n-i}\binom{n-i}{2i-n}\sin\frac{5\pi i}{n}\left(2\cos\frac{\pi}{n}\right)^i.$$

Аналогично с помощью тождеств (121) и (122) получаются следующие соотношения:

$$\left(2\cos\frac{3\pi}{n}\right)^n=\sum_{1\le i\le n/3}(-1)^i\frac{n}{n-2i}\binom{n-2i}{i}\cos\frac{\pi(n-3i)}{n}\left(2\cos\frac{3\pi}{n}\right)^{n-3i}-$$
$$-\sum_{n/2\le i\le 2n/3}\frac{n}{n-i}\binom{n-i}{2i-n}\cos\frac{\pi(2n-3i)}{n}\left(2\cos\frac{3\pi}{n}\right)^{2n-3i}+(-1)^n-1,$$

$$\sum_{1\le i\le n/3}(-1)^i\frac{n}{n-2i}\binom{n-2i}{i}\left(2\cos\frac{3\pi}{n}\right)^{n-3i}\sin\frac{\pi(n-3i)}{n}=$$
$$=\sum_{n/2\le i\le 2n/3}\frac{n}{n-i}\binom{n-i}{2i-n}\left(2\cos\frac{3\pi}{n}\right)^{2n-3i}\sin\frac{\pi(2n-3i)}{n},$$

$$\left(2\cos\frac{2\pi}{n}\right)^n=\sum_{1\le i\le n/3}\frac{n}{n-2i}\binom{n-2i}{i}\cos\frac{8\pi i}{n}\left(2\cos\frac{2\pi}{n}\right)^{2i}-$$
$$-\sum_{n/2\le i\le 2n/3}(-1)^i\frac{n}{n-i}\binom{n-i}{2i-n}\cos\frac{4\pi(2i-n)}{n}\left(2\cos\frac{2\pi}{n}\right)^{2i-n}+2,\quad n\neq 4,$$

$$\sum_{1\le i\le n/3}\frac{n}{n-2i}\binom{n-2i}{i}\left(2\cos\frac{2\pi}{n}\right)^{2i}\sin\frac{8\pi i}{n}=$$
$$=\sum_{n/2\le i\le 2n/3}(-1)^i\frac{n}{n-i}\binom{n-i}{2i-n}\left(2\cos\frac{2\pi}{n}\right)^{2i-n}\sin\frac{4\pi(2i-n)}{n}.$$

4. Некоторые связи с известными числовыми последовательностями

Используя результаты, полученные в предыдущем параграфе, приведем некоторые тождества, связывающие тригонометрические функции с известными числовыми последовательностями.

Пусть $n=2m+1$ – нечетное натуральное число. Следующие соотношения проверяются непосредственно

$$\prod_{i=0}^{n-1}(t-(\varepsilon_n^i a+\varepsilon_n^{2i}b))=(t-(a+b))\times$$
$$\times\prod_{k=1}^{m}\left(t^2-2\left(a\cos\frac{2\pi k}{n}+b\cos\frac{4\pi k}{n}\right)t+a^2+b^2+2ab\cos\frac{2\pi k}{n}\right),\quad (123)$$

$$u_n(a+b,ab) = \frac{a^n - b^n}{a-b} = \prod_{k=1}^{m}\left(a^2+b^2-2ab\cos\frac{2\pi k}{n}\right), \tag{124}$$

$$v_n(a+b,ab) = a^n + b^n = (a+b)\prod_{k=1}^{m}\left(a^2+b^2+2ab\cos\frac{2\pi k}{n}\right). \tag{125}$$

Сравнивая коэффициенты при t с обеих частей равенства (109), с помощью соотношений (123)–(125) получаем тождества

$$-a^{n-2}bn = \frac{v_n(a+b,ab)}{a+b} + v_n(a+b,ab)\sum_{k=1}^{m}\frac{2\left(a\cos\dfrac{2\pi k}{n} + b\cos\dfrac{4\pi k}{n}\right)}{a^2+b^2+2ab\cos\dfrac{2\pi k}{n}}, \tag{126}$$

$$a^{n-2}bn = u_n(a+b,ab) + (a-b)u_n(a+b,ab)\sum_{k=1}^{m}\frac{2\left(a\cos\dfrac{2\pi k}{n} - b\cos\dfrac{4\pi k}{n}\right)}{a^2+b^2-2ab\cos\dfrac{2\pi k}{n}}. \tag{127}$$

Положим в равенствах (126) и (127) $a = \dfrac{1+\sqrt{5}}{2}$ и $b = \dfrac{1-\sqrt{5}}{2}$. Тогда с учетом соотношений (65) и (66) получаем

$$\frac{L_{n-3}+F_{n-3}\sqrt{5}}{2}n = \\ = L_n + L_n\sum_{k=1}^{m}\frac{\left(\cos\dfrac{2\pi k}{n} + cos\dfrac{4\pi k}{n}\right) + \sqrt{5}\left(\cos\dfrac{2\pi k}{n} - \cos\dfrac{4\pi k}{n}\right)}{3-2\cos\dfrac{2\pi k}{n}}, \tag{128}$$

$$-\frac{L_{n-3}+F_{n-3}\sqrt{5}}{2}n = \\ = F_n + F_n\sum_{k=1}^{m}\frac{5\left(\cos\dfrac{2\pi k}{n} + \cos\dfrac{4\pi k}{n}\right) + \sqrt{5}\left(\cos\dfrac{2\pi k}{n} - \cos\dfrac{4\pi k}{n}\right)}{3+2\cos\dfrac{2\pi k}{n}}. \tag{129}$$

Предположим, что $n \notin 5\mathbb{Z}$. Так как простой идеал (5) кольца $\mathbb{Z}$ разветвлен в $\mathbb{Q}[\sqrt{5}]$ и не разветвлен в $\mathbb{Q}[\varepsilon_n]$, то $\sqrt{5} \notin \mathbb{Q}[\varepsilon_n]$. Тогда из тождеств (128) и (129) следует, что в случае, когда $2m+1 \notin 5\mathbb{Z}$, имеют место соотношения

$$\sum_{k=1}^{m}\frac{\cos\frac{\pi k}{2m+1}\cos\dfrac{3\pi k}{2m+1}}{3-2\cos\dfrac{2\pi k}{2m+1}} = \frac{(2m+1)L_{2m-2} - 2L_{2m+1}}{4L_{2m+1}},$$

$$\sum_{k=1}^{m}\frac{\sin\dfrac{\pi k}{2m+1}\sin\dfrac{3\pi k}{2m+1}}{3-2\cos\dfrac{2\pi k}{2m+1}} = \frac{(2m+1)F_{2m-2}}{4L_{2m+1}},$$

$$\sum_{k=1}^{m}\frac{\cos\dfrac{\pi k}{2m+1}\cos\dfrac{3\pi k}{2m+1}}{3+2\cos\dfrac{2\pi k}{2m+1}} = -\frac{(2m+1)L_{2m-2} + 2F_{2m+1}}{20F_{2m+1}},$$

$$\sum_{k=1}^{m}\frac{\sin\dfrac{\pi k}{2m+1}\sin\dfrac{3\pi k}{2m+1}}{3+2\cos\dfrac{2\pi k}{2m+1}}=-\frac{(2m+1)F_{2m-2}}{4F_{2m+1}}.$$

Нам неизвестно, верны ли предыдущие тождества для произвольных нечетных чисел n.

Положим в равенстве (126) $a=b=1$. Тогда это равенство в результате несложных преобразований примет вид

$$\sum_{k=1}^{m}\frac{\cos\dfrac{3\pi k}{2m+1}}{\cos\dfrac{\pi k}{2m+1}}=-(m+1). \tag{130}$$

Из предыдущего равенства и легко проверяемого тождества $\sum\limits_{k=1}^{m}\cos\dfrac{4\pi k}{2m+1}=-\dfrac{1}{2}$ следует соотношение

$$\sum_{k=1}^{m}\frac{\cos\dfrac{5\pi k}{2m+1}}{\cos\dfrac{\pi k}{2m+1}}=m. \tag{131}$$

Из равенства

$$\sum_{k=1}^{m}\frac{\cos\dfrac{(\alpha+4)\pi k}{2m+1}}{\cos\dfrac{\pi k}{2m+1}}-\sum_{k=1}^{m}\frac{\cos\dfrac{\alpha\pi k}{2m+1}}{\cos\dfrac{\pi k}{2m+1}}=-2\sin\frac{(\alpha+1)\pi}{2}\,\frac{\sin\dfrac{(\alpha+2)\pi}{4m+2}\cos\dfrac{\pi}{4m+2}}{\sin\dfrac{(\alpha+1)\pi}{4m+2}\sin\dfrac{(\alpha+3)\pi}{4m+2}},$$

которое проверяется с помощью стандартных преобразований, и соотношений (130) и (131) следует, что для всяких натуральных чисел m и n, для которых выполнено неравенство $n\le m$, имеет место тождество

$$\sum_{k=1}^{m}\frac{\cos\dfrac{(2n+1)\pi k}{2m+1}}{\cos\dfrac{\pi k}{2m+1}}=(-1)^n\,m+\frac{(-1)^n-1}{2}.$$

Положим в равенстве (121) $n=6m+3$. Тогда имеют место равенства

$$\prod_{k=0}^{6m+2}(t-a\varepsilon_n^k-b\varepsilon_n^{-2k})=$$

$$=(t-(a+b))\prod_{k=1}^{3m+1}\left(t^2-2\left(a\cos\frac{2\pi k}{6m+3}+b\cos\frac{4\pi k}{6m+3}\right)t+a^2+b^2+2ab\cos\frac{2\pi k}{2m+1}\right)=$$

$$=t^n-\sum_{n/2\le i\le 2n/3}\frac{n}{n-i}\binom{n-i}{2i-n}a^{2i-n}b^it^{2n-3i}+$$

$$+\sum_{1\le i\le n/3}(-1)^i\frac{n}{n-2i}\binom{n-2i}{i}a^{2i}b^it^{n-3i}-b^n-a^n.$$

Сравним в последнем равенстве коэффициенты при первой степени t с обеих частей и положим

$$A=\prod_{k=1}^{3m+1}\left(a^2+b^2+2ab\cos\frac{2\pi k}{2m+1}\right).$$

Тогда

$$A+(a+b)A\sum_{k=1}^{3m+1}\frac{2\left(a\cos\dfrac{2\pi k}{6m+3}+b\cos\dfrac{4\pi k}{6m+3}\right)}{a^2+b^2+2ab\cos\dfrac{2\pi k}{2m+1}}=0,$$

$$\sum_{k=1}^{3m+1}\frac{a\cos\dfrac{2\pi k}{6m+3}+b\cos\dfrac{4\pi k}{6m+3}}{a^2+b^2+2ab\cos\dfrac{2\pi k}{2m+1}}=-\frac{1}{2(a+b)}.$$

В частности, полагая в последнем равенстве $a=b=1$, с помощью несложных преобразований получаем

$$\sum_{k=1}^{3m+1}\frac{1}{1-2\cos\dfrac{2\pi k}{6m+3}}=\frac{1}{2}.$$

Положим в тождестве (118) $t=1$. В результате получим равенство

$$\prod_{i=0}^{n-1}(1-a\varepsilon_n^{2i}-b\varepsilon_n^{3i})=P'_n(a,b)-P_n(a,b)+1-b^n, \tag{132}$$

где

$$P_n(a,b)=\sum_{n/2\le i\le 2n/3}\frac{n}{n-i}\binom{n-i}{2i-n}a^{2n-3i}b^{2i-n}, \tag{133}$$

$$P'_n(a,b)=\sum_{0\le i\le n/3}(-1)^{n-i}\,\frac{n}{n-2i}\binom{n-2i}{i}a^{n-3i}b^{2i}. \tag{134}$$

Для каждого натурального числа n имеют место равенства $P_n(a,b)=\alpha_1^n+\alpha_2^n+\alpha_3^n$ и $P'_n(a,b)=(\alpha_1\alpha_2)^n+(\alpha_1\alpha_3)^n+(\alpha_2\alpha_3)^n$, где α_1, α_2, α_3 – корни многочлена $x^3-ax-b\in\mathbb{C}(a,b)[x]$. Тогда последовательности $\{P_n(a,b)\}_{n\in\mathbb{N}}$, $\{P'_n(a,b)\}_{n\in\mathbb{N}}$ являются рекуррентными и удовлетворяют условиям

$$\begin{aligned}&P_1(a,b)=0,\quad P_2(a,b)=2a,\quad P_3(a,b)=3b,\\&P_{n+3}(a,b)=aP_{n+1}(a,b)+bP_n(a,b),\quad n\in\mathbb{N},\end{aligned} \tag{135}$$

$$\begin{aligned}&P'_1(a,b)=-a,\quad P'_2(a,b)=a^2,\quad P'_3(a,b)=-a^3+3b^2,\\&P'_{n+3}(a,b)=-aP'_{n+2}(a,b)+b^2P'_n(a,b),\quad n\in\mathbb{N}.\end{aligned} \tag{136}$$

Положим для каждого $n\in\mathbb{N}$ $P_n=P_n(1,1)$ и $P'_n=P'_n(1,1)$. В результате получим последовательности $\{P_n\}_{n\in\mathbb{N}}$, $\{P'_n\}_{n\in\mathbb{N}}$, удовлетворяющие условиям

$$P_1=0,\quad P_2=2,\quad P_3=3,\quad P_{n+3}=P_{n+1}+P_n,\quad n\in\mathbb{N}, \tag{137}$$

$$P'_1=-1,\quad P'_2=1,\quad P'_3=2,\quad P'_{n+3}=-P'_{n+2}+P'_n,\quad n\in\mathbb{N}. \tag{138}$$

Последовательность $\{P_n\}_{n\in\mathbb{N}}$ хорошо известна и называется числами Перри. Эта последовательность была впервые изучена Р. Перрином в работе [37]. Используя условия (137), числа Перри можно доопределить и для отрицательных целых чисел. При этом несложно заметить, что

$$P_{-n}=P'_n.$$

Согласно равенству (133) имеем

$$P_n = \sum_{n/2\le i\le 2n/3} \frac{n}{n-i}\binom{n-i}{2i-n} = \sum_{i=1}^{[n/2]} \frac{n}{i}\binom{i}{n-2i}, \quad n\in\mathbb{N}. \tag{139}$$

Из (132) с помощью несложных преобразований следует тождество

$$P_n - P_{-n} = \prod_{k=1}^{[n/2]}\left(1+8\cos\frac{\pi k}{n}\sin\frac{2\pi k}{n}\sin\frac{3\pi k}{n}\right), \quad n\in\mathbb{N}.$$

Аналогично из (34) и (109) следует тождество

$$L_n = \prod_{k=1}^{[n/2]}\left(1+4\sin^2\frac{2\pi k}{n}\right)+1+(-1)^n, \quad n\in\mathbb{N}. \tag{140}$$

5. Арифметика некоторых целочисленных линейных рекуррентных последовательностей

Числа Перри, Люка и Пелля–Люка обладают рядом общих арифметических свойств. Например, Р. Перрином [37] было замечено, что для любого простого числа p имеет место сравнение

$$P_p \equiv 0 \pmod p. \tag{141}$$

Комбинаторное доказательство этого сравнения приведено в статье [38]. Заметим также, что сравнение (141) непосредственно следует из формулы (139). Аналогичные сравнения имеют место для чисел Люка и Пелля–Люка. Ниже эти свойства будут рассмотрены в общей ситуации.

Пусть $f = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{Z}[x]$ – произвольный унитарный многочлен степени m и $\alpha_1,\dots,\alpha_n$ – все его корни с учетом их кратности. Через C_f будем обозначать сопровождающую матрицу к f, то есть матрицу вида

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}.$$

Хорошо известно, что характеристический многочлен матрицы C_f совпадает с f. Следовательно, для каждого натурального числа m имеет место равенство $\alpha_1^m + \dots + \alpha_n^m = tr(C_f^m)$. Если $A\in M_n(\mathbb{Z})$ и $\alpha_1,\dots,\alpha_n$ – все корни его характеристического многочлена с учетом их кратности, то $tr(A^m) = \alpha_1^m + \dots + \alpha_n^m$. Из сделанных выше замечаний и полиномиальной формулы непосредственно следует

Лемма 1. 1) *Пусть $\alpha_1,\dots,\alpha_m$ – корни унитарного многочлена $f\in\mathbb{Z}[x]$ степени m и p – простое число. Тогда имеет место сравнение*

$$\alpha_1^p + \dots + \alpha_m^p \equiv \alpha_1 + \ldots + \alpha_m \pmod p.$$

2) *Пусть A – целочисленная квадратная матрица и p – простое число. Тогда имеет место сравнение*

$$\mathrm{tr}(A^p) \equiv \mathrm{tr}(A) \pmod p. \tag{142}$$

Сравнение (142) впервые было доказано в 1839 г. в работе [39]. Оно также встречается в работе С.О. Шатуновского [40] и в последующем переоткрывалось в ряде работ [41–43].

Пусть $n_1, n_2, \ldots, n_m$ – последовательность целых неотрицательных чисел, расположенных в порядке (нестрогого) убывания, то есть $n_1 \geq n_2 \geq \cdots \geq n_m$. Через $\mu_{n_1,\ldots,n_m}(x_1, \ldots, x_n)$ обозначим симметрический многочлен вида $\sum x_1^{\alpha_1} \ldots x_n^{\alpha_n}$, где сумма берется по всем различным перестановкам $(\alpha_1 \ldots, \alpha_m)$ последовательности $(n_1, n_2, \ldots, n_m)$.

Теорема 2. *Пусть $\alpha_1, \ldots, \alpha_m$ – корни унитарного многочлена $f \in \mathbb{Z}[x]$ степени m и p – простое число. Тогда для каждых натуральных чисел n и k имеет место сравнение*

$$\alpha_1^{kp^n} + \cdots + \alpha_m^{kp^n} \equiv \alpha_1^{kp^{n-1}} + \cdots + \alpha_m^{kp^{n-1}} \pmod{p^n}. \tag{143}$$

Доказательство. Ясно, что для каждого $k \in \mathbb{N}$ числа $\alpha_1^k, \ldots, \alpha_m^k$ – корни некоторого унитарного многочлена с целыми коэффициентами. Таким образом, сравнение (143) достаточно доказать в случае, когда $k = 1$. Докажем индукцией по n. Согласно лемме (1) утверждение теоремы верно при $n = 1$. Предположим, что утверждение теоремы верно для некоторого натурального числа n. Пусть $\alpha_1, \ldots, \alpha_m$ – корни унитарного многочлена $f \in \mathbb{Z}[x]$ степени m. Тогда имеет место сравнение

$$\alpha_1^{p^n} + \cdots + \alpha_m^{p^n} \equiv \alpha_1^{p^{n-1}} + \cdots + \alpha_m^{p^{n-1}} \pmod{p^n}.$$

Тогда для некоторого натурального числа t выполнено равенство

$$\alpha_1^{p^n} + \cdots + \alpha_m^{p^n} = \alpha_1^{p^{n-1}} + \cdots + \alpha_m^{p^{n-1}} + p^n t.$$

Следовательно,

$$(\alpha_1^{p^n} + \cdots + \alpha_m^{p^n})^p \equiv (\alpha_1^{p^{n-1}} + \cdots + \alpha_m^{p^{n-1}})^p \pmod{p^{n+1}}.$$

С другой стороны, согласно полиномиальной формуле имеют место равенства

$$(\alpha_1^{p^n} + \cdots + \alpha_m^{p^n})^p = \alpha_1^{p^{n+1}} + \cdots + \alpha_m^{p^{n+1}} + \\ + \sum_{\substack{n_1+\cdots+n_m=p \\ p>n_1\geq n_2\geq\cdots\geq n_m}} \binom{p}{n_1, \ldots, n_m} \mu_{n_1,\ldots,n_m}(\alpha_1^{p^n}, \ldots, \alpha_m^{p^n})$$

$$(\alpha_1^{p^{n-1}} + \cdots + \alpha_m^{p^{n-1}})^p = \alpha_1^{p^n} + \cdots + \alpha_m^{p^n} + \\ + \sum_{\substack{n_1+\cdots+n_m=p \\ p>n_1\geq n_2\geq\cdots\geq n_m}} \binom{p}{n_1, \ldots, n_m} \mu_{n_1,\ldots,n_m}(\alpha_1^{p^{n-1}}, \ldots, \alpha_m^{p^{n-1}}).$$

Пусть $n_1, n_2, \ldots, n_m$ – последовательность целых неотрицательных чисел, для которых выполнены условия $p > n_1 \geq n_2 \geq \ldots \geq n_m$ и $p = n_1 + n_2 + \ldots + n_m$. Множество алгебраических целых чисел, которые получаются из мономов, являющихся слагаемыми многочлена $\mu_{n_1,\ldots,n_m}$, подстановкой вместо $x_1, \ldots, x_m$ соответственно $\alpha_1, \ldots, \alpha_m$, очевидно, совпадает с множеством всех корней некоторого унитарного целочисленного многочлена. Таким образом, по предположению индукции имеем

$$\mu_{n_1,\ldots,n_m}(\alpha_1^{p^n}, \ldots, \alpha_m^{p^n}) \equiv \mu_{n_1,\ldots,n_m}(\alpha_1^{p^{n-1}}, \ldots, \alpha_m^{p^{n-1}}) \pmod{p^n}.$$

Так как $\binom{p}{n_1,\ldots,n_m}$ делится на p, то

$$\sum_{\substack{n_1+\cdots+n_m=p\\ p>n_1\geq n_2\geq\cdots\geq n_m}} \binom{p}{n_1,\ldots,n_m}\mu_{n_1,\ldots,n_m}(\alpha_1^{p^n},\ldots,\alpha_m^{p^n}) \equiv$$

$$\equiv \sum_{\substack{n_1+\cdots+n_m=p\\ p>n_1\geq n_2\geq\cdots\geq n_m}} \binom{p}{n_1,\ldots,n_m}\mu_{n_1,\ldots,n_m}(\alpha_1^{p^{n-1}},\ldots,\alpha_m^{p^{n-1}}) \pmod{p^{n+1}}.$$

Таким образом, имеет место сравнение

$$\alpha_1^{p^{n+1}}+\cdots+\alpha_m^{p^{n+1}} \equiv \alpha_1^{p^n}+\cdots+\alpha_m^{p^n} \pmod{p^{n+1}}.$$

□

Данное утверждение непосредственно следует из теоремы 2:

Теорема 3. *Пусть A – целочисленная квадратная матрица и p – простое число. В этом случае для произвольных натуральных чисел n и m имеет место сравнение*

$$\mathrm{tr}(A^{mp^n}) \equiv \mathrm{tr}(A^{mp^{n-1}}) \pmod{p^n}. \tag{144}$$

При этом если свободный член характеристического многочлена матрицы A равен ±1, то предыдущее сравнение верно для произвольного целого числа m.

Следствие [44]. *Пусть A – целочисленная квадратная матрица и $m\in\mathbb{N}$. Тогда имеет место сравнение*

$$\sum_{d|m}\mu\left(\frac{m}{d}\right)\mathrm{tr}(A^d)\equiv 0 \pmod{m}. \tag{145}$$

Доказательство. Пусть $m=p_1^{n_1}\cdots p_k^{n_k}$ – разложение натурального числа m на простые сомножители. Так как для каждого $0\leq i\leq k$ и всякого натурального числа s, согласно теореме 4, имеет место сравнение $\mathrm{tr}(A^{sp_i^{n_i}})\equiv \mathrm{tr}(A^{sp_i^{n_i-1}})$ $\pmod{p_i^{n_i}}$, то сравнение

$$tr(A^{p_1^{n_1}\cdots p_k^{n_k}})+\sum_{t=1}^{k}(-1)^t\sum_{1\leq i_1<\cdots<i_t\leq k}\mathrm{tr}\left(A^{\frac{p_1^{n_1}\cdots p_k^{n_k}}{p_{i_1}\cdots p_{i_t}}}\right)\equiv 0 \pmod{p_i^{n_i}}$$

также имеет место для каждого $0\leq i\leq k$. Таким образом, имеет место сравнение (145). □

Следствие [45, теорема 14]. *Пусть p – простое число. Тогда для каждого натурального числа n и всякого целого числа m имеет место сравнение*

$$P_{mp^n}\equiv P_{mp^{n-1}} \pmod{p^n}.$$

Сравнение (145) в эквивалентной формулировке, по-видимому, впервые было доказано в работе [44]. Различные доказательства сравнений (143)–(145) в разные годы были приведены также в работах [46–51]. Исторические обзоры исследований, связанных со сравнениями(143)–(145), изложены в работах [52] и [51]. В последнее время целочисленные рекуррентные последовательности $\{a_n\}$, для которых сравнение

$$a_{mp^n}\equiv a_{mp^{n-1}} \pmod{p^n}$$

выполнено для произвольного простого числа p и любых неотрицательных целых чисел m и n, были изучены и описаны в работах [53, 54]

Теорема 4. *Пусть* $\alpha_1, \dots, \alpha_m$ *– корни унитарного многочлена* $f \in \mathbb{Z}[x]$ *степени* m *и* p *– простое число. Тогда имеют место утверждения:*

1) *если многочлен* f *по модулю* p *раскладывается на линейные множители, то для каждого неотрицательного целого числа* k *выполнено сравнение*

$$\alpha_1^{1+k} + \dots + \alpha_m^{1+k} \equiv \alpha_1^{p+k} + \dots + \alpha_m^{p+k} \pmod p;$$

2) *если дискриминант многочлена* f *несравним с нулем по модулю* p *и сравнение*

$$\alpha_1^{1+k} + \dots + \alpha_m^{1+k} \equiv \alpha_1^{p+k} + \dots + \alpha_m^{p+k} \pmod p$$

выполнено для $k = 1, \dots, m-1$, *то многочлен* f *по модулю* p *раскладывается на линейные множители.*

Доказательство. Через $\overline{f}$ обозначим многочлен, коэффициенты которого являются классами вычетов по модулю p коэффициентов многочлена $f(x)$. Пусть $\beta_1, \dots, \beta_m$ – все корни многочлена $\overline{f}$ из некоторого расширения поля $\mathbb{Z}_p$ с учетом их кратностей.

1) Так как согласно условию $\beta_1, \dots, \beta_m \in \mathbb{Z}_p$, то для каждого неотрицательного целого числа k выполнены равенства

$$\mathrm{tr}(C_{\overline{f}}^{1+k}) = \beta_1^{1+k} + \dots + \beta_m^{1+k} = \beta_1^{p+k} + \dots + \beta_m^{p+k} = \mathrm{tr}(C_{\overline{f}}^{p+k}).$$

Таким образом, для каждого неотрицательного целого числа k выполнено сравнение

$$\mathrm{tr}(C_f^{1+k}) \equiv \mathrm{tr}(C_f^{p+k}) \pmod p,$$

которое равносильно сравнению из п. 1).

2) Согласно условию для каждого $k = 1, \dots, m-1$ выполнено сравнение

$$\mathrm{tr}(C_f^{1+k}) \equiv \mathrm{tr}(C_f^{p+k}) \pmod p.$$

Следовательно, для каждого $k = 1, \dots, m-1$ выполнено равенство $\mathrm{tr}(C_{\overline{f}}^{1+k}) = \mathrm{tr}(C_{\overline{f}}^{p+k})$. Таким образом, для каждого $k = 1, \dots, m-1$ имеет место равенство

$$\beta_1^{1+k} + \dots + \beta_m^{1+k} = \beta_1^{p+k} + \dots + \beta_m^{p+k}.$$

Предположим, что все корни многочлена $\overline{f}$ отличны от нуля. Так как многочлен $\overline{f}$ согласно условию не имеет кратных корней, то определитель матрицы коэффициентов системы линейных уравнений:

$$\beta_1 x_1 + \dots + \beta_m x_m = \beta_1 + \dots + \beta_m;$$

$$\beta_1^2 x_1 + \dots + \beta_m^2 x_m = \beta_1^2 + \dots + \beta_m^2;$$

$$\dots$$

$$\beta_1^m x_1 + \dots + \beta_m^m x_m = \beta_1^m + \dots + \beta_m^m$$

отличен от нуля. Согласно лемме 1 и условию п. 2) $(\beta_1^{p-1}, \dots, \beta_m^{p-1})$ – решение этой системы. Так как выписанная выше система обладает единственным решением, то $\beta_1^{p-1} = \dots = \beta_m^{p-1} = 1$. Предположим теперь, что один из корней многочлена равен $\overline{f}$ нулю. С точностью до переобозначения можно считать, что $\beta_1 = 0$. Тогда с помощью приведенных выше рассуждений получаем равенства $\beta_2^{p-1} = \dots = \beta_m^{p-1} = 1$. Таким образом, в любом случае $\beta_i \in \mathbb{Z}_p$ для каждого i. □

Предыдущая теорема была доказана С.О. Шатуновским в работе [40]. Приведенное выше доказательство этой теоремы отлично от оригинального, данного в [40]. В литературе почти отсутствуют ссылки на [40]. Единственное упоминание о приведенном выше результате С.О. Шатуновского, которое нам удалось найти, содержится в работе Н.Г. Чеботарёва [55].

Следующее утверждение хорошо известно (см., например, [56, предложение 3.7.3]).

Лемма 2. *Пусть R – локальное кольцо и $\{e_{ij}\}_{1\leq i,j\leq n}\in M_n(R)$ – матричные единицы. Тогда для каждого ортогонального семейства примитивных идемпотентов $e_1,\dots,e_n\in M_n(R)$ существует такая обратимая матрица $C\in M_n(R)$, что $e_{ii}=C^{-1}e_iC$ для каждого $1\leq i\leq n$.*

Рассмотрим следующее дополнение к теореме Шатуновского, которое можно рассматривать как аналог теоремы Эйлера о периодичности геометрической прогрессии по примарным модулям.

Теорема 5. *Пусть $\alpha_1,\dots,\alpha_m$ – корни унитарного многочлена $f\in\mathbb{Z}[x]$ степени m и p – простое число. Если многочлен f по модулю p раскладывается на линейные множители и дискриминант многочлена f несравним с нулем по модулю p , то для каждого натурального числа n и неотрицательного целого числа k выполнено сравнение*

$$\alpha_1^{p^n+k}+\dots+\alpha_m^{p^n+k}\equiv\alpha_1^{p^{n-1}+k}+\dots+\alpha_m^{p^{n-1}+k}\pmod{p^n}.$$

При этом если свободный член многочлена f равен ±1, то предыдущее сравнение выполнено для произвольного целого числа k.

Доказательство. Для произвольного многочлена $f(x)\in\mathbb{Z}[x]$ через $\overline{f}(x)$ (соответственно, $\widetilde{f}(x)$) обозначим многочлен, коэффициенты которого являются классами вычетов по модулю p (соответственно, p^n) коэффициентов многочлена $f(x)$.

Так как согласно условию многочлен f в поле $\mathbb{Z}_p$ имеет m попарно различных корней и $\mathbb{Z}_p[C_{\overline{f}}]\cong\mathbb{Z}_p[x]/(f)$, то для некоторого семейства ортогональных примитивных идемпотентов $e_1,\dots e_m$ из алгебры $\mathbb{Z}_p[C_{\overline{f}}]$ имеют место равенства $1=e_1+$ $+\dots+e_m$ и $\mathbb{Z}_p[C_{\overline{f}}]=e_1\mathbb{Z}_p\oplus\dots\oplus e_m\mathbb{Z}_p$. Согласно [56, предложение 3.6.1], для некоторого семейства ортогональных примитивных идемпотентов $\widetilde{e_1},\dots,\widetilde{e_m}$ из алгебры $\mathbb{Z}_{p^n}[C_{\widetilde{f}}]$ имеют место равенства $1=\widetilde{e_1}+\dots+\widetilde{e_m}$. Тогда согласно лемме 2 для некоторой обратимой матрицы $C\in M_m(\mathbb{Z}_{p^n})$ для каждого $k=1,2,\dots,m$ имеет место равенство $C^{-1}\widetilde{e_k}C=e_{kk}$. Поскольку в алгебре $\mathbb{Z}_{p^n}[C^{-1}C_{\widetilde{f}}C]$ каждая матрица является линейной комбинацией матриц $E,C^{-1}C_{\widetilde{f}}C,\dots,C^{-1}C_{\widetilde{f}}^{m-1}C$ с коэффициентами из кольца $\mathbb{Z}_{p^n}$ и количество матриц из свободного $\mathbb{Z}_{p^n}$-модуля $e_{11}\mathbb{Z}_{p^n}\oplus\dots\oplus e_{mm}\mathbb{Z}_{p^n}$ равно p^{nm}, получаем равенство $\mathbb{Z}_{p^n}[C^{-1}C_{\widetilde{f}}C]=e_{11}\mathbb{Z}_{p^n}\oplus\dots\oplus e_{mm}\mathbb{Z}_{p^n}$. Таким образом, имеет место равенство $C^{-1}C_{\widetilde{f}}C=\mathrm{diag}(a_1,\dots,a_m)$, где $a_i\in\mathbb{Z}_{p^n}$ для каждого $i=1,2,\dots,m$. Тогда по теореме Эйлера для каждого неотрицательного числа k имеет место равенство

$$\mathrm{tr}(C^{-1}C_{\widetilde{f}}^{p^n+k}C)=\mathrm{tr}(C^{-1}C_{\widetilde{f}}^{p^{n-1}+k}C),$$

и, следовательно,

$$a_1^{p^n+k}+\dots+a_m^{p^n+k}=\mathrm{tr}(C_{\widetilde{f}}^{p^n+k})=\mathrm{tr}(C_{\widetilde{f}}^{p^{n-1}+k})=a_1^{p^{n-1}+k}+\dots+a_m^{p^{n-1}+k}.$$

Если свободный член многочлена f равен ±1, то для каждого $i=1,2,\dots,m$ элемент a_i обратим в $\mathbb{Z}_{p^n}$ и, следовательно, предыдущие равенства имеют место для произвольного целого числа k. □

Следующее утверждение является эквивалентной переформулировкой теорем 4 и 5.

Теорема 6. *Пусть A – целочисленная квадратная матрица порядка m и p – простое число. Тогда имеют место утверждения:*

1) *если характеристический многочлен матрицы A по модулю p раскладывается на линейные множители, то для каждого неотрицательного целого числа k выполнено сравнение*

$$\operatorname{tr}(A^{1+k}) \equiv \operatorname{tr}(A^{p+k}) \pmod p;$$

2) *если дискриминант характеристического многочлена матрицы A несравним с нулем по модулю p и сравнение*

$$\operatorname{tr}(A^{1+k}) \equiv \operatorname{tr}(A^{p+k}) \pmod p$$

выполнено для $k = 1, \ldots, m-1$, то характеристический многочлен матрицы A по модулю p раскладывается на линейные множители и сравнение

$$\operatorname{tr}(A^{p^n+k}) \equiv \operatorname{tr}(A^{p^{n-1}+k}) \pmod{p^n}$$

выполнено для всякого неотрицательного целого числа k и для каждого $n \in \mathbb{N}$. При этом если матрица A обратима в $M_m(\mathbb{Z})$, то предыдущее сравнение выполнено для произвольного целого числа k.

Приведем некоторые приложения теоремы Шатуновского и теоремы 5.

Следствие. *Пусть $\dfrac{Q_0}{P_0}, \dfrac{Q_1}{P_1}, \ldots$ – последовательность подходящих дробей к вещественному числу $\sqrt{2}$. Тогда для произвольного нечетного простого числа p следующие условия равносильны:*

1) $Q_{p+1} \equiv 3 \pmod p$;

2) *для произвольного $n \in \mathbb{N}$ и каждого неотрицательного целого числа k выполнено сравнение*

$$Q_{p^n+k} \equiv Q_{p^{n-1}+k} \pmod{p^n};$$

3) в поле $\mathbb{F}_p$ извлекается квадратный корень из 2, то есть $p \equiv \pm 1 \pmod 8$.

Доказательство. Последовательность $\{Q_n\}_{n \in N_0}$ удовлетворяет условиям (68). Следовательно, для каждого натурального числа n выполнено равенство $2Q_n = \alpha^n + \beta^n$, где α, β – корни многочлена $x^2 - 2x - 1$. Тогда эквивалентность пунктов 1), 2) и 3) непосредственно следует из теорем 4 и 5. □

Пусть a, b, $c \in \mathbb{Z}$ и α_1, α_2, α_3 – корни многочлена $x^3 - ax^2 - bx - c$. Для любого натурального числа n через $s_n(a,b,c)$ будем обозначать выражение $\alpha_1^n + \alpha_2^n + \alpha_3^n$. Следующее утверждение непосредственно следует из теоремы 4.

Следствие. *Пусть дискриминант многочлена $f = x^3 - ax^2 - bx - c$ несравним с нулем по модулю простого числа p. Тогда многочлен f по модулю p раскладывается на линейные множители в точности тогда, когда выполнены сравнения*

$$s_{p+1}(a,b,c) \equiv a^2 + 2b \pmod p,$$

$$s_{p+2}(a,b,c) \equiv a^3 + 3ab + 3c \pmod p.$$

Связи между арифметическими свойствами линейных рекуррентных целочисленных последовательностей и разложимостью целочисленных многочленов по модулям простых чисел были систематически изучены для многочленов третьей и четвертой степеней в недавней работе [57]. В частности, в ней был получен результат, аналогичный предыдущему утверждению, согласно которому если a, $b \in \mathbb{Z}$ и p не делит a^2+3b, то многочлен $f = x^3-ax^2-bx-c = 0$ по модулю p раскладывается на линейные множители в точности тогда, когда выполнено сравнение

$$s_{p+1}(a,b,c) \equiv a^2 + 2b \pmod{p}.$$

Следствие. *Для произвольного нечетного простого числа $p \neq 23$ следующие условия равносильны:*

1) $P_{p+1} \equiv 2 \pmod{p}$, $P_{p+2} \equiv 3 \pmod{p}$*;*

2) *для произвольного $n \in \mathbb{N}$ и каждого неотрицательного целого числа k выполнено сравнение*

$$P_{p^n+k} \equiv P_{p^{n-1}+k} \pmod{p^n};$$

3) *многочлен x^3-x-1 по модулю p раскладывается на линейные множители.*

Пусть $q = 2n+1$ – произвольное нечетное простое число. Через $d_1, \dots, d_n$ обозначим квадраты длин хорд $A_1A_2, \dots, A_1A_{n+1}$ правильного q-угольника $A_1A_2\dots A_q$, вписанного в единичную окружность. Ясно, что $\{d_i\}_{i=1}^n = \left\{4\sin^2\dfrac{\pi i}{q}\right\}_{i=1}^n$ и, согласно [6], $d_1, \dots, d_n$ – корни унитарного многочлена $\chi_{A_n}(x)$ с целыми коэффициентами, где A_n – матрица размера $(n\times n)$ вида (86). Используя изложенный выше материал, изучим арифметические свойства целочисленной последовательности $\{d_1^k+\dots+d_n^k\}_{k\in\mathbb{N}}$. Выясним, по модулям каких простых чисел многочлен $\chi_{A_n}(x)$ раскладывается на линейные множители. Так как $(-1)^n g_n(3-x,1) = \chi_{A_n}(x)$, где $g_n(x,y)$ – определитель вида (80), то поставленная задача равносильна аналогичному вопросу для многочленов вида $g_n(x,1)$. Пусть p – некоторое нечетное простое число. Через $\overline{g}_n(x,1)$ обозначим многочлен, коэффициенты которого являются классами вычетов по модулю p коэффициентов многочлена $g_n(x,1)$. Предположим, что $p \neq q$. Через $\overline{F}$ обозначим алгебраическое замыкание поля $\mathbb{F}_p$. Пусть $\alpha \in \overline{F}$ – корень уравнения $\overline{g}_n(x,1)$ и $\beta \in \overline{F}$ – корень уравнения $\alpha = x^2 + \dfrac{1}{x^2} + 1$. Покажем, что $\beta^{2q} = 1$. Без ограничения общности можно считать, что $\beta \neq \pm 1$. Тогда согласно равенству (85) имеем

$$\frac{\beta^{2n+1}-\beta^{-2n-1}}{\beta-\beta^{-1}} = (-1)^n\overline{g}_n((\beta^2+1+\beta^{-2}),1) = (-1)^n\overline{g}_n(\alpha,1) = 0. \tag{146}$$

Следовательно, $\beta^{2q}=1$. Предположим, что для некоторого целого числа t имеет место равенство $p = qt\pm 1$. Тогда

$$\alpha^p = \left(\beta^2+\frac{1}{\beta^2}+1\right)^p = (\beta^2)^p + \left(\frac{1}{\beta^2}\right)^p + 1 = (\beta^2)^{qt\pm1} + \left(\frac{1}{\beta^2}\right)^{qt\pm1} + 1 = \alpha.$$

Таким образом, если $p \equiv \pm 1 \pmod{q}$, то все корни многочлена $\overline{\chi}_{A_n}(x)$ принадлежат полю $\mathbb{F}_p$. Предположим, что все корни многочлена $\overline{g}_n(x,1)$ принадлежат полю $\mathbb{F}_p$. Из тождества (85) следует, что для примитивного корня степени q из единицы $\varepsilon \in \overline{F}$ имеет место равенство $\overline{g}_n(\varepsilon^2+1+\varepsilon^{-2},1) = 0$. Тогда $\varepsilon^2+1+\varepsilon^{-2} \in \mathbb{F}_p$ и, следовательно, либо поле $\mathbb{F}_p$, либо поле $\mathbb{F}_{p^2}$ содержит ε. Следовательно, p^2-1 делится на q, то есть $p \equiv \pm 1 \pmod{q}$. Так как q нечетно, то $\varepsilon' = \varepsilon^2$ также является примитивным корнем степени q из единицы. Квадратное уравнение $\varepsilon'^k + \varepsilon'^{-k} = x + x^{-1}$ для каждого $1 \le k \le n$ обладает двумя различными решениями ε'^k и ε'^{-k}. Следовательно, уравнение $\overline{g}_n(x,1) = 0$ обладает n различными решениями $\varepsilon'^k + 1 + \varepsilon'^{-k}$ $(1 \le k \le n)$.

Если $p = q$, то с помощью рассуждений, аналогичных приведенным выше, можно показать, что $\overline{g}_n(3-x,1) = -(x-3)^n$. Таким образом, из приведенных выше рассуждений и теорем 5 и 6 следует утверждение

Теорема 7. *Пусть $q = 2n+1$ – нечетное простое число. Тогда для нечетного простого числа p, отличного от q, следующие условия равносильны:*

1) *для каждого $m \in \mathbb{N}$ и для каждого $k \in \mathbb{N}_0$ имеет место сравнение*

$$\operatorname{tr}(A_n^{p^m+k}) \equiv \operatorname{tr}(A_n^{p^{m-1}+k}) \pmod{p^m};$$

2) *для каждого $m \in \mathbb{N}$ и для каждого $k \in \mathbb{N}_0$ имеет место сравнение*

$$d_1^{p^m+k} + \cdots + d_n^{p^m+k} \equiv d_1^{p^{m-1}+k} + \cdots + d_n^{p^{m-1}+k} \pmod{p^m};$$

3) *сравнение*

$$d_1^{1+k} + \cdots + d_n^{1+k} \equiv d_1^{p+k} + \cdots + d_n^{p+k} \pmod{p}$$

выполнено для $k = 1, \ldots, n-1$;

4) *многочлен $\chi_{A_n}(x)$ по модулю p раскладывается на линейные множители;*

5) $p \equiv \pm 1 \pmod{q}$.

6. Групповые определители

В настоящем параграфе будет показано, что тождества (2), (8), (16), (17), (19), (34), (110), с помощью которых в предыдущих параграфах были получены формулы решений для рассмотренных ранее семейств алгебраических уравнений, естественно связаны с характеристическими многочленами некоторых групповых матриц конечных абелевых групп.

Пусть $G = \{g_0 = e, g_1, \ldots, g_{n-1}\}$ – конечная абелева группа порядка n и $G^* = \{\chi_1, \chi_2, \ldots, \chi_n\}$ – группа ее характеров. Для каждого $\chi \in G^*$ положим $e_\chi = \dfrac{1}{n} \sum\limits_{g\in G} g\chi(g^{-1})$. Хорошо известно, что для групповой алгебры $\mathbb{C}(x_{g_0}, \ldots, x_{g_{n-1}})G$ имеет место изоморфизм

$$\mathbb{C}(x_{g_0}, \ldots, x_{g_{n-1}})G \cong \underbrace{\mathbb{C}(x_{g_0}, \ldots, x_{g_{n-1}}) \times \ldots \times \mathbb{C}(x_{g_0}, \ldots, x_{g_{n-1}})}_{n}$$

и $1 = \sum_{\chi \in G^*} e_\chi$ – разложение единицы. Несложно заметить, что для элемента $\sum\limits_{g\in G} x_g g$ матрицы регулярных представлений относительно базисов $\{g\}_{g\in G}$ и $\{e_\chi\}_{\chi\in G^*}$ равны соответственно $(x_{gh^{-1}})$ и

$$\operatorname{diag}\left(\sum_{g\in G} x_g\chi_1(g), \sum_{g\in G} x_g\chi_2(g), \ldots, \sum_{g\in G} x_g\chi_n(g)\right).$$

Таким образом, имеет место равенство

$$\det(x_{gh^{-1}}) = \prod_{\chi\in G^*}^{n} \sum_{g\in G} x_g\chi(g). \tag{147}$$

Частным случаем предыдущего тождества является известная формула для определителя циркулянта. Матрица $(x_{gh^{-1}})$ называется групповой матрицей группы G, а ее определитель называется групповым определителем группы G. Равенство (147) впервые было доказано Р. Дедекиндом в 1880 г. Обобщение равенства (147) на случай произвольной конечной группы было получено Г. Фробениусом в работе «О простых множителях группового детерминанта» (1896) [58]. В этой работе и близких к ней статьях автором были заложены основы теории характеров и теории представлений конечных групп. Групповым матрицам и групповым определителям посвящено много работ, систематическое изложение результатов приведено в монографии [59].

Через $\mathbb{Z}_n$ будем обозначать аддитивную группу кольца вычетов по модулю n. Рассмотрим частные случаи формулы (147), когда либо $G = \mathbb{Z}_3$, либо $G = \mathbb{Z}_4$. Пусть $G = \mathbb{Z}_3$. Тогда согласно формуле (147) имеем

$$\begin{vmatrix} t - x_0 & -x_1 & -x_2 \\ -x_2 & t - x_0 & -x_1 \\ -x_1 & -x_2 & t - x_0 \end{vmatrix} = \\ = (t - (x_0 + x_1 + x_2))(t - (x_0 + \varepsilon_3 x_1 + \varepsilon_3^2 x_2))(t - (x_0 + \varepsilon_3^2 x_1 + \varepsilon_3 x_2)). \quad (148)$$

Вычисляя определитель в левой части последнего равенства, получаем тождество

$$t^3 - 3x_0 t^2 - (3x_1 x_2 - 3x_0^2)t - x_0^3 - x_1^3 - x_2^3 + 3x_0 x_1 x_2 = \\ = (t - (x_0 + x_1 + x_2))(t - (x_0 + \varepsilon_3 x_1 + \varepsilon_3^2 x_2))(t - (x_0 + \varepsilon_3^2 x_1 + \varepsilon_3 x_2)),$$

непосредственным следствием которого является тождество (2). В случае, когда $G = \mathbb{Z}_4$, аналогично устанавливается формула

$$t^4 - (2x_3^2 + 4x_1 x_2)t^2 - (4x_1^2 x_3 + 4x_2^2 x_3)t + \\ + x_1^4 + x_2^4 - x_3^4 - 2x_1^2 x_2^2 + 4x_1 x_2 x_3^2 = (t - (x_1 + x_2 + x_3))(t - (ix_1 - x_2 - ix_3)) \times \\ \times (t - (-x_1 + x_2 - x_3))(t - (-ix_1 - x_2 + ix_3)). \quad (149)$$

Следствием предыдущей формулы является тождество (8), на основе которого Фаньяно решил своим способом уравнение четвертой степени. Отметим, что согласно тождеству (147) формулы (36), (109), (118), (121) и (122) дают явные выражения для определителей соответствующих циркулянтов призвольного порядка.

В работе [60] был предложен единообразный способ решения алгебраических уравнений $f(x) = 0$, степень которых не превосходит четырех, основанный на нахождении циркулянта, чей характеристический многочлен равен $f(x)$. Естественным расширением этого способа является представление заданного многочлена $f(x)$ степени n в виде характеристического многочлена матрицы вида $(a_{gh^{-1}})_{g,h\in G}$, где G – некоторая абелева группа порядка n. Тогда, согласно (147), множество всех корней многочлена $f(x)$ совпадет с множеством $\Big\{ \sum\limits_{g\in G} a_g \chi(g) \mid \chi \in G^* \Big\}$. Проиллюстрируем этот способ на примере нахождения корней многочлена четвертой степени

$$x^4 - 4px^3 + 2qx^2 - 4rx + s. \quad (150)$$

Пусть $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ и положим $x_{(0,0)} = d$, $x_{(1,0)} = a$, $x_{(0,1)} = b$, $x_{(1,1)} = c$. С помощью непосредственных вычислений можно показать, что характеристический многочлен групповой матрицы группы G равен

$$x^4 - 4dx^3 + 2(-a^2 - b^2 - c^2 + 3d^2)x^2 + (-4d^3 + (4(a^2 + b^2 + c^2))d - 8abc)x + \\ + d^4 - (2(a^2 + b^2 + c^2))d^2 + 8abcd + (a^2 + b^2 + c^2)^2 - 4a^2 b^2 - 4a^2 c^2 - 4b^2 c^2. \quad (151)$$

Из сопоставления коэффициентов при соответствующих степенях многочленов (150) и (151) следует, что если в качестве $a_0,\ a_1,\ a_2,\ a_3$ взять числа, удовлетворяющие равенствам

$$a_0 = p,$$
$$a_1^2 + a_2^2 + a_3^2 = 3p^2 - q,$$
$$a_1a_2a_3 = \frac{-qp + r + 2p^3}{2},$$
$$a_1^2a_2^2 + a_1^2a_3^2 + a_2^2a_3^2 = 3p^4 - 2p^2q + pr + \frac{q^2 - s}{4},$$

то многочлен (150) совпадет с характеристическим многочленом матрицы A, которая получается из групповой матрицы $(x_{gh^{-1}})_{g,h\in G}$ в результате замены независимых переменных $x_{(0,0)},\ x_{(1,0)},\ x_{(0,1)},\ x_{(1,1)}$ соответственно числами $a_0,\ a_1,\ a_2,\ a_3$. Таким образом, согласно (147) собственные значения матрицы A и, следовательно, корни многочлена (150) имеют вид

$$x_1 = a_0 + a_1 + a_2 + a_3, \quad x_2 = a_0 + a_1 - a_2 - a_3,$$

$$x_3 = a_0 - a_1 - a_2 + a_3, x_4 = a_0 - a_1 + a_2 - a_3,$$

где $a_1a_2a_3 = \dfrac{qp + r - 4p^3}{2}$ и $a_1^2,\ a_2^2,\ a_3^2$ – корни уравнения

$$y^3 + (q - 3p^2)y^2 + \left(3p^4 - 2p^2q + pr + \frac{q^2 - s}{4}\right)y - \left(\frac{-qp + r + 2p^3}{2}\right)^2 = 0.$$

В частности, имеет место тождество

$$\begin{gathered}(a+b+c+d)^4 - 4d(a+b+c+d)^3 + \\ + 2(-a^2 - b^2 - c^2 + 3d^2)(a+b+c+d)^2 + \\ + (-4d^3 + (4(a^2+b^2+c^2))d - 8abc)(a+b+c+d) + d^4 - (2(a^2+b^2+c^2))d^2 + \\ + 8abcd + (a^2+b^2+c^2)^2 - 4a^2b^2 - 4a^2c^2 - 4b^2c^2 = 0.\end{gathered}$$

Заметим, что в случае, когда $p = 0$, из предыдущего равенства следует тождество (16), лежащее в основе метода решения уравнения (15), предложенного Ф. Валлесом.

Благодарности. Автор выражает благодарность Д.Т. Тапкину за постоянное внимание к работе и сделанные полезные замечания.

Литература

1. *Fagnano G.C.* Soluzione di quattro problemi analitici // Fagnano G.C. Opere Matematiche: 2 t. – Milano; Roma; Napoli: Albrighi Segati, 1911. – T. 2. – 516 p.
2. *Вилейтнер Г.* История математики от Декарта до середины XIX столетия. – М.: ГИФМЛ, 1960. – 468 с.
3. *Dulaurens Fr.* Specimina Mathematica. – Paris, 1667.
4. *Schneider I.* Der Mathematiker Abraham de Moivre (1667–1754) // Archive for History of Exact Sciences. – 1968. – V. 5, No 3/4. – P. 177–317.

5. *Haukkanen P., Merikoski J., Mustonen S.* Some polynomials associated with regular polygons // Acta Univ. Sapientiae, Math. – 2014. – V. 6, No 2. – P. 178–193. – doi: 10.1515/ausm-2015-0005.

6. *Savio D.Y., Suryanarayan E.R.* Chebychev polynomials and regular polygons // Am. Math. Mon. – 1993. – V. 100, No 7. – P. 657–661. – doi: 10.1080/00029890.1993.11990466.

7. *Laughlin J.Mc.* Combinatorial identities deriving from the n-th power of a 2×2 matrix // Integers. – 2004. – V. 4. – P. 1–15.

8. *Eulero L.* De resolutione aequationum cuiusvis gradus // Novi Comment. Acad. Sci. Imp. Petropolitanae. – Petropolis, 1764. – V. 9 (1762–1763). – P. 70–98.

9. *Kaddoura I., Mourad B.* On a class of matrices generated by certain generalized permutation matrices and applications // Linear Multilinear Algebra. – 2018. – V. 67, No 10. – P. 2117–2134. – doi: doi: 10.1080/03081087.2018.1484420.

10. *Grunert J.A.* Die allgemeine Cardanische Formel // Arch. Math. Phys. – 1863. – Bd. 40. – S. 246–249.

11. *Blum-Smith B., Wood J.* Chords of an ellipse, Lucas polynomials, and Cubic Equations // Am. Math. Mon. – 2020. – V. 127, No 8. – P. 688–705. – doi: 10.1080/00029890.2020.1785253.

12. *Solomon R.* Abstract Algebra. – Belmont: Thompson Brooks/Cole, 2003. – 227 p.

13. *Spearman B.K., Williams K.S.* DeMoivre's quintic and a theorem of Galois // Far East J. Math. Sci. – 1999. – V. l. – P. 137–143.

14. *Borger R.L.* On DeMoivre's quintic // Am. Math. Mon. – 1908. – V. 15, No 10. – P. 171–174. – doi: 10.1080/00029890.1908.11997448.

15. *Майстрова А.Л.* Решение алгебраических уравнений в работах Л. Эйлера // Историко-математические исследования / Под ред. А.П. Юшкевича. – М.: Наука, 1985. – Вып. 29. – С. 189–199.

16. *Valles F.* Des formes imaginaires en algebre. – Paris: Gauthier-Villars, 1873. – 539 p.

17. *Stedall J.A.* From Cardano's Great Art to Lagrange's Reflections: Filling a Gap in the History of Algebra. – Zürich: Eur. Math. Soc., 2011. – 224 p.

18. *Dickson L.E.* History of the Theory of Numbers. – Washington: Carnegie Inst., 1919. – V. I: Divisibility and primality. – XII, 486 p.

19. *Girard A.* Invention nouvelle en l'algebre. – Amsterdam, 1629. – 72 p.

20. *Waring E.* Miscellanea analytica de aequationibus algebraicis, et curvarum proprietatibus. – Cambridge: Thurlbourn Woodyer, 1762. – 206 p.

21. *Сушкевич А.К.* Основы высшей алгебры. – М; Л.: Гостехиздат, 1941. – 460 с.

22. *Лобачевский Н.И.* Сочинения по алгебре. Алгебра или вычисление конечных. Понижение степени в двучленном уравнении, когда показатель без единицы делится на 8 // Лобачевский Н.И. Полное собрание сочинений: в 5 т. / Гл. ред. В.Ф. Каган. – М.; Л.: Гостехиздат, 1948. – Т. 4. – 472 с.

23. *De Moivre A.* Aequationum quarundam potestatis tertiae, quintae, septimae, nonae, et superiorum, ad infinitum usque pergendo, in terminis finitis, ad instar regularum pro cubicis quae vocantur Cardani resolutio analytica // Philos. Trans. – 1707. – V. 25, No 309. – P. 2368–2371.

24. *Wituła R., Słota D.* Cardano's formula, square roots, Chebyshev polynomials and radicals // J. Math. Anal. Appl. – 2010. – V. 363, No 2. – P. 639–647. – doi: 10.1016/j.jmaa.2009.09.056.

25. *Dickson L.E.* Elementary Theory of Equations. – N. Y.: Wiley, 1914. – 196 p.

26. *Dickson L.E.* Linear Groups: With an Exposition of the Galois Field Theory. – Leipzig: Teubner, 1901. – X, 312 p.

27. *Williams K.S.* A generalization of Cardan's solution of the cubic // Math. Gaz. – 1962. – V. 46, No 357. – P. 221–223.

28. *Lehmer D.H.* On the multiple solutions of the Pell equation // Ann. Math. – 1928. – V. 30, No 1/4. – P. 66–72.

29. *Эйлер Л.* Введение в анализ бесконечных: в 2 т. – М.: Физматгиз, 1961. – Т. 1. – 315 с.

30. *Wituła R., Słota D.* Cauchy, Ferrers–Jackson and Chebyshev polynomials and identities for the powers of elements of some conjugate recurrence sequences // Cent. Eur. J. Math. – 2006. – V. 4, No 3. – P. 531–546. – doi: 10.2478/s11533-006-0022-9.

31. *Kepler J.* Harmonice Mundi // Kepler J. Opera Omnia. Bd. 5. – Frankfurt: Heyder Zimmer, 1864. – S. 75–327.

32. *Kappraff J.* Beyond Measure: A Guided Tour through Nature, Myth, and Number. – River Edge, N. J.: World Sci. Publ., 2002. – XXX, 582 p.

33. *Гаусс К.Ф.* Труды по теории чисел. – М.: Изд-во АН СССР, 1959. – 980 с.

34. *Eisenstein G.* Application de l'algebre a l'arithmetique transcendante // J. Reine Angew. Math. – 1845. – T. 29. – P. 177–184. – doi: 10.1515crll.

35. *Liouville J.* Sur la loi de reciprocite dans la theorie des residus quadratiques // J. Math. Pures Appl. – 1847. – T. 12. – P. 95–96.

36. *Baumgart O., Lemmermeyer F.* The Quadratic Reciprocity Law: A Collection of Classical Proofs. – Cham; Heidelberg; N. Y.; Dordrecht; London: Birkhauser Springer, 2015. – XIV, 172 p.

37. *Perrin R.* Item 1484 // L'Intermed. Math. – 1899. – T. 6. – P. 76–77.

38. *Minton G.T.* Three approaches to a sequence problem // Math. Mag. – 2011. – V. 84, No 1. – P. 33–37. – doi: 10.4169/math.mag.84.1.033.

39. *Schönemann T.* Theorie der symmetrischen Functionen der Wurzeln einer Gleichung. Allgemeine Sätze über Congruenzen nebst einigen Anwendungen derselben // J. Reine Angew. Math. – 1839. – Bd. 19. – S. 289–308.

40. *Шатуновский С.О.* Об условиях существования n неравных корней сравнения n-й степени по простому модулю. – Казань: Тип.-лит. Имп. ун-та, 1903. – 19 с.

41. *Arnold V.I.* On the matricial version of Fermat–Euler congruences // Jpn. J. Math. – 2006. – V. 1, Art. 1. – P. 1–24. – doi: 10.1007/s11537-006-0501-6.

42. *Browder F.E.* The Lefschetz fixed point theorem and asymptotic fixed point theorems in partial differential equations and related topics // Lecture Notes in Mathematics. – V. 446. – N. Y.: Springer-Verlag, 1975. – P. 96–122.

43. *Peitgen H.O.* On the Lefschetz Number for Iterates of Continuous Mappings // Proc. Am. Math. Soc. – 1976. – V. 54, No 1. – P. 441–444. – doi: 0.1090/S0002-9939-1976-0391074-1.

44. *Janichen W.* Uber die Verallgemeinerung einer Gaussschen Formel aus der Theorie der hoheren Kongruenzen // Sitzungsber. Berlin. Math. Ges. – 1921. – Bd. 20. – S. 23–29.

45. *Adams W.W., Shanks D.* Strong primality tests that are not sufficient // Math. Comput. – 1982. – V. 39, No 159. – P. 255–300.

46. *Винберг Э.Б.* Малая теорема Ферма и ее обобщения // Матем. просвещение. Сер. 3. – 2008. – № 12. – С. 43–53.

47. *Зарелуа А.В.* О матричных аналогах малой теоремы Ферма // Матем. заметки. – 2006. – Т. 79, № 6. – С. 838–853. – doi: 10.4213/mzm2758.

48. *Jezierski J., Marzantowicz W.* Homotopy methods in topological fixed and periodic points theory // Gorniewicz L. (Ed.) Topological Fixed Point Theory and Its Applications. – Dordrecht: Springer, 2006. – V. 3. – XII, 319 p.

49. *Schur I.* Arithmetische Eigenschaften der Potenzsummen einer algebraischen Gleichung // Compos. Math. – 1937. – Bd. 4. – S. 432–444.

50. *Smyth C.J.* A coloring proof of a generalisation of Fermat's little theorem // Am. Math. Mon. – 1986. – V. 93, No 6. – P. 469–471.

51. *Steinlein H.* Fermat's little theorem and Gauss congruence: Matrix versions and cyclic permutations // Am. Math. Mon. – 2017. – V. 124, No 6. – P. 548–553.

52. *Зарелуа А.В.* О сравнениях для следов степеней некоторых матриц // Труды Матем. ин-та им. В.А. Стеклова РАН. – 2008. – Т. 263. – С. 85–105.

53. *Beukers F., Houben M.R., Straub A.* Gauss congruences for rational functions in several variables // Acta Arithmetica. – 2018. – V. 184, No 4. – P. 341–362. – doi: 10.4064/aa170614-13-7.

54. *Minton G.T.* Linear recurrence sequences satisfying congruence conditions // Proc. Am. Math. Soc. – 2014. – V. 142, No 7. – P. 2337–2352.

55. *Чеботарёв Н.Г.* Самуил Осипович Шатуновский (к 10-летию со дня смерти) // Усп. матем. наук. – 1940. – № 7. – С. 316–321.

56. *Ламбек И.* Кольца и модули. – М.: Мир, 1971. – 280 с.

57. *Sun Z.-H.* Cubic and quartic congruences modulo a prime // J. Number Theory. – 2003. – V. 102, No 1. – P. 41–89. – doi: 10.1016/S0022-314X(03)00067-2.

58. *Фробениус Г.* Теория характеров и представлений групп. – Харьков: ОНТИ, 1937. – 214 с.

59. *Johnson K.W.* Group Matrices, Group Determinants and Representation Theory: The Mathematical Legacy of Frobenius. – N. Y.: Springer Int. Publ., 2019. – 409 p. (Lecture Notes in Mathematics. V. 2233)

60. *Pen-Tung Sah A.* A uniform method of solving cubics and quartics // Am. Math. Mon. – 1945. – V. 52, No 4. – P. 202–206.

Поступила в редакцию
16.09.2021

Абызов Адель Наилевич, доктор физико математических наук, профессор кафедры алгебры и математической логики

Казанский (Приволжский) федеральный университет
ул. Кремлевская, д. 18, г. Казань, 420008, Россия
E-mail: *aabyzov@kpfu.ru*

ISSN 2541-7746 (Print)
ISSN 2500-2198 (Online)

**UCHENYE ZAPISKI KAZANSKOGO UNIVERSITETA.
SERIYA FIZIKO-MATEMATICHESKIE NAUKI
(Proceedings of Kazan University. Physics and Mathematics Series)**

2021, vol. 163, no. 3–4, pp. 304–348

REVIEW ARTICLE

doi: 10.26907/2541-7746.2021.3-4.304-348

Fagnano's Method for Solving Algebraic Equations: Its Historical Overview and Development

A.N. Abyzov

Kazan Federal University, Kazan, 420008 Russia
E-mail: *aabyzov@kpfu.ru*

Received September 16, 2021

Abstract

In 1750, Giulio Carlo Fagnano dei Toschi's treatise "Produzioni matematiche" was published in two volumes. The second volume of the treatise contains a work in which Fagnano proposed a uniform method for solving algebraic equations up to the fourth degree. Fagnano's method, as we call it in this article, is based on a comparison of algebraic equations with identities arising in the representation of an expression of the form $(a_1 + \cdots + a_m)^n$ in terms of lesser powers of $a_1 + \cdots + a_m$. Here we explore the results related to the use of certain types of algebraic identities in solving a number of families of algebraic equations that are solvable by radicals. Various connections of these identities with linear recurrent sequences and trigonometric identities are considered. A historical survey devoted to the use of Fagnano's method for solving algebraic equations is presented in section 1. Section 2 is devoted to algebraic equations that are solvable by radicals closely related to Chebyshev polynomials and whose solution by radicals is based on the use of the Kummer identity. In section 3, Fagnano's method is used to study some families of algebraic equations that are solvable by radicals. In sections 4 and 5, the connections of the identities considered in the previous sections with the well-known linear recurrent sequences are analyzed. In section 6, a connection is established between the identities covered in this article and the group determinants.

Keywords: algebraic equations, Lucas sequences, group determinants

Acknowledgments. D.T. Tapkin's continuous support during the study and helpful advice are gratefully acknowledged.

References

1. Fagnano G.C. Soluzione di quattro problemi analitici. In: Fagnano G.C. *Opere Matematiche.* T. 2. Milano, Roma, Napoli, Albrighi Segati, 1911. 516 p. (In Italian)
2. Wieleitner H. *Istoriya matematiki ot Dekarta do serediny XIX stoletiya* [History of Mathematics from Descartes to the Mid-19th Century]. Moscow, GIFML, 1960. 468 p. (In Russian)
3. Dulaurens Fr. *Specimina Mathematica.* Paris, 1667.
4. Schneider I. Der Mathematiker Abraham de Moivre (1667–1754). *Arch. Hist. Exact Sci.*, 1968, vol. 5, no. 3/4, pp. 177–317. (In German)

5. Haukkanen P., Merikoski J., Mustonen S. Some polynomials associated with regular polygons. *Acta Univ. Sapientiae. Math.*, 2014, vol. 6, no. 2, pp. 178–193. doi: 10.1515/ausm-2015-0005.

6. Savio D.Y., Suryanarayan E.R. Chebychev polynomials and regular polygons. *Am. Math. Mon.*, 1993, vol. 100, no. 7, pp. 657–661. doi: 10.1080/00029890.1993.11990466.

7. Laughlin J.Mc. Combinatorial identities deriving from the n-th power of a 2×2 matrix. *Integers*, 2004, vol. 4, pp. 1–15.

8. Eulero L. De resolutione aequationum cuiusvis gradus. *Novi Comment. Acad. Sci. Imp. Petropolitanae*. Petropolis, 1764, vol. 9 (1762–1763), pp. 70–98. (In Latin)

9. Kaddoura I., Mourad B. On a class of matrices generated by certain generalized permutation matrices and applications. *Linear Multilinear Algebra*, 2018, vol. 67, no. 10, pp. 2117–2134. doi: 10.1080/03081087.2018.1484420.

10. Grunert J.A. Die allgemeine Cardanische Formel. *Arch. Math. Phys.*, 1863, Bd. 40, S. 246–249. (In German)

11. Blum-Smith B., Wood J. Chords of an ellipse, Lucas polynomials, and cubic equations. *Am. Math. Mon.*, 2020, vol. 127, no. 8, pp. 688–705. doi: 10.1080/00029890.2020.1785253.

12. Solomon R. *Abstract Algebra*. Belmont, Thompson Brooks/Cole, 2003. 227 p.

13. Spearman B.K., Williams K.S. DeMoivre's quintic and a theorem of Galois. *Far East J. Math. Sci.*, 1999, vol. l, pp. 137–143.

14. Borger R.L. On De Moivre's quantic. *Am. Math. Mon.*, 1908, vol. 15, no. 10, pp. 171–174. doi: 10.1080/00029890.1908.11997448.

15. Maistrova A.L. Solving algebraic equations in L. Euler's works. In: *Istoriko-matematicheskie issledovaniya* [Historical and Mathematical Studies]. Yushkevich A.P. (Ed.). Moscow, Nauka, 1985, no. 29, pp. 189–199. (In Russian)

16. Valles F. *Des formes imaginaires en algebra*. Paris, Gauthier-Villars, 1873. 539 p. (In French)

17. Stedall J.A. *From Cardano's Great Art to Lagrange's Reflections: Filling a Gap in the History of Algebra*. Zürich, Eur. Math. Soc., 2011. 224 p.

18. Dickson L.E. *History of the Theory of Numbers*. Vol. I: Divisibility and primality. Washington, Carnegie Inst., 1919. XII, 486 p.

19. Girard A. *Invention nouvelle en l'algebre*. Amsterdam, 1629. 72 p.

20. Waring E. *Miscellanea analytica de aequationibus algebraicis, et curvarum proprietatibus*. Cambridge, Thurlbourn Woodyer, 1762. 206 p. (In Latin)

21. Sushkevich A.K. *Osnovy vysshei algebry* [Fundamentals of Higher Algebra]. Moscow, Leningrad, Gostekhizdat, 1941. 460 p. (In Russian)

22. Lobachevsky N.I. Essays on algebra. Algebra, or the calculus of finite quantities. Lowering the degree in a binominal equation when the exponent minus a unit is a multiple of 8. In: Lobachevsky N.I. *Polnoe sobranie sochinenii* [Complete Collection of Works]. Vol. 4. Kagan V.F. (Ed.). Moscow, Leningrad, Gostekhizdat, 1948. 472 p. (In Russian)

23. De Moivre A. Aequationum quarundam potestatis tertiae, quintae, septimae, nonae, et superiorum, ad infinitum usque pergendo, in terminis finitis, ad instar regularum pro cubicis quae vocantur Cardani resolutio analytica. *Philos. Trans.*, 1707, vol. 25, no. 309, pp. 2368–2371. (In Latin)

24. Wituła R., Słota D. Cardano's formula, square roots, Chebyshev polynomials and radicals. *J. Math. Anal. Appl.*, 2010, vol. 363, no. 2, pp. 639–647. doi: 10.1016/j.jmaa.2009.09.056.

25. Dickson L.E. *Elementary Theory of Equations*. New York, Wiley, 1914. 196 p.

26. Dickson L.E. *Linear Groups: With an Exposition of the Galois Field Theory*. Leipzig, Teubner, 1901. X, 312 p.

27. Williams K.S. A generalization of Cardan's solution of the cubic. *Math. Gaz.*, 1962, vol. 46, no. 357, pp. 221–223.

28. Lehmer D.H. On the multiple solutions of the Pell equation. *Ann. Math.*, 1928, vol. 30, no. 1/4, pp. 66–72.

29. Euler L. *Vvedenie v analiz beskonechnykh* [Introduction to Analysis of the Infinite]. Vol. 1. Moscow, Fizmatgiz, 1961. 315 p. (In Russian)

30. Wituła R., Słota D. Cauchy, Ferrers–Jackson and Chebyshev polynomials and identities for the powers of elements of some conjugate recurrence sequences. *Cent. Eur. J. Math.*, 2006, vol. 4, no. 3, pp. 531–546. doi: 10.2478/s11533-006-0022-9.

31. Kepler J. Harmonice Mundi. In: Kepler J. *Opera Omnia*. Bd. 5. Frankfurt, Heyder Zimmer, 1864, S. 75–327.

32. Kappraff J. *Beyond Measure: A Guided Tour through Nature, Myth, and Number*. River Edge, N. J., World Sci. Publ., 2002. XXX, 582 p.

33. Gauss C.F. *Trudy po teorii chisel* [Works on the Number Theory]. Moscow, Izd. Akad. Nauk SSSR, 1959. 980 p. (In Russian)

34. Eisenstein G. Application de l'algebre a l'arithmetique transcendante. *J. Reine Angew. Math.*, 1845, T. 29, pp. 177–184. doi: 10.1515crll. (In French)

35. Liouville J. Sur la loi de reciprocite dans la theorie des residus quadratiques. *J. Math. Pures Appl.*, 1847, T. 12, pp. 95–96. (In French)

36. Baumgart O., Lemmermeyer F. *The Quadratic Reciprocity Law: A Collection of Classical Proofs*. Cham, Heidelberg, New York, Dordrecht, London, Birkhauser Springer, 2015. XIV, 172 p.

37. Perrin R. Item 1484. *L'Intermed Math.*, 1899, T. 6, pp. 76–77. (In French)

38. Minton G.T. Three approaches to a sequence problem. *Math. Mag.*, 2011, vol. 84, no. 1, pp. 33–37. doi: 10.4169/math.mag.84.1.033.

39. Schönemann T. Theorie der symmetrischen Functionen der Wurzeln einer Gleichung. Allgemeine Sätze über Congruenzen nebst einigen Anwendungen derselben. *J. Reine Angew. Math.*, 1839, Bd. 19, S. 289–308. (In German)

40. Shatunovskii S.O. *Ob usloviyakh sushchestvovaniya n neravnykh kornei sravneniya n-i stepeni po prostomu modulyu* [On the Conditions for the Existence of n Unequal Roots of Congruence of n-Degree Using a Simple Module]. Kazan, Tip.-Lit. Imp. Univ., 1903. 19 p. (In Russian)

41. Arnold V.I. On the matricial version of Fermat–Euler congruences. *Jpn. J. Math.*, 2006, vol. 1, art. 1, pp. 1–24. doi: 10.1007/s11537-006-0501-6.

42. Browder F.E. The Lefschetz fixed point theorem and asymptotic fixed point theorems in partial differential equations and related topics. In: *Lecture Notes in Mathematics*. Vol. 446. New York, Springer-Verlag, 1975, pp. 96–122.

43. Peitgen H.O. On the Lefschetz number for iterates of continuous mappings. *Proc. Am. Math. Soc.*, 1976, vol. 54, no. 1, pp. 441–444. doi: 0.1090/S0002-9939-1976-0391074-1.

44. Janichen W. Uber die Verallgemeinerung einer Gaussschen Formel aus der Theorie der hoheren Kongruenzen. Sitzungsber. *Berlin. Math. Ges.*, 1921, Bd. 20, S. 23–29. (In German)

45. Adams W.W., Shanks D. Strong primality tests that are not sufficient. *Math. Comput.*, 1982, vol. 39, no. 159, pp. 255–300.

46. Vinberg E.B. Fermat's little theorem and generalizations. *Mat. Prosveshchenie. Ser. 3*, 2008, no. 12, pp. 43–53. (In Russian)

47. Zarelua A.V. On matrix analogs of Fermat's little theorem. *Math. Notes*, 2006, vol. 79, no. 6, pp. 783–796. doi: 10.1007/s11006-006-0090-y.

48. Jezierski J., Marzantowicz W. Homotopy methods in topological fixed and periodic points theory. In: Gorniewicz L. (Ed.) *Topological Fixed Point Theory and Its Applications*. Vol. 3. Dordrecht, Springer, 2006. XII, 319 p.

49. Schur I. Arithmetische Eigenschaften der Potenzsummen einer algebraischen Gleichung. *Compos. Math.*, 1937, Bd. 4, S. 432–444. (In German)

50. Smyth C.J. A coloring proof of a generalisation of Fermat's little theorem. *Am. Math. Mon.*, 1986, vol. 93, no. 6, pp. 469–471.

51. Steinlein H. Fermat's little theorem and Gauss congruence: Matrix versions and cyclic permutations. *Am. Math. Mon.*, 2017, vol. 124, no. 6, pp. 548–553.

52. Zarelua A.V. On congruences for the traces of powers of some matrices. *Proc. Steklov Inst. Math.*, 2008, vol. 263, pp. 78–98. doi: 10.1134/S008154380804007X.

53. Beukers F., Houben M.R., Straub A. Gauss congruences for rational functions in several variables. *Acta Arithmetica*, 2018, vol. 184, no. 4, pp. 341–362. doi: 10.4064/aa170614-13-7.

54. Minton G.T. Linear recurrence sequences satisfying congruence conditions. *Proc. Am. Math. Soc.*, 2014, vol. 142, no. 7, pp. 2337–2352.

55. Chebotarev N.G. Samuil Osipovich Shatunovskii (on the occasion of the 10th anniversary of his death). *Usp. Mat. Nauk*, 1940, no. 7, pp. 316–321. (In Russian)

56. Lambek J. *Kol'tsa i moduli* [Lectures on Rings and Modules]. Moscow, Mir, 1971. 280 p. (In Russian)

57. Sun Z.-H. Cubic and quartic congruences modulo a prime. *J. Number Theory*, 2003, vol. 102, no. 1, pp. 41–89. doi: 10.1016/S0022-314X(03)00067-2.

58. Frobenius G. *Teoriya kharakterov i predstavlenii* [Theory of Group Characters and Representations]. Kharkiv, ONTI, 1937. 214 p. (In Russian)

59. Johnson K.W. *Group Matrices, Group Determinants and Representation Theory: The Mathematical Legacy of Frobenius*. New York, Springer Int. Publ., 2019. 409 p. (*Lecture Notes in Mathematics*. Vol. 2233)

60. Pen-Tung Sah A. A uniform method of solving cubics and quartics. *Am. Math. Mon.*, 1945, vol. 52, no. 4, pp. 202–206.

⟨ ***Для цитирования***: *Абызов А.Н.* Метод Фаньяно решения алгебраических уравнений: исторический обзор и его развитие // Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки. – 2021. – Т. 163, кн. 3–4. – С. 304–348. – doi: 10.26907/2541-7746.2021.3-4.304-348. ⟩

⟨ ***For citation***: Abyzov A.N. Fagnano's method for solving algebraic equations: Its historical overview and development. *Uchenye Zapiski Kazanskogo Universiteta. Seriya Fiziko-Matematicheskie Nauki*, 2021, vol. 163, no. 3–4, pp. 304–348. doi: 10.26907/2541-7746.2021.3-4.304-348. (In Russian) ⟩