

УДК 511.17, 512.624  
DOI 10.46698/m2155-1449-8044-d

## О ПРИМЕНЕНИЯХ КОНЕЧНЫХ ПОЛЕЙ К ФУНКЦИИ ЭЙЛЕРА

У. М. Пачев<sup>1</sup>, А. А. Токбаева<sup>1</sup>

<sup>1</sup> Кабардино-Балкарский государственный университет им. Х. М. Бербекова,  
Россия, 360004, Нальчик, ул. Чернышевского, 173  
E-mail: urusbi@rambler.ru, tok2506@mail.ru

*70-летию В. А. Койбаева посвящается*

**Аннотация.** Работа относится к применениям конечных полей к функции Эйлера из теории чисел. С помощью понятия нормированного неприводимого многочлена заданной степени над конечным полем  $F_q$  получен некоторый аналог известного соотношения Гаусса  $\sum_{d|n} \varphi(d) = n$ . Здесь  $\varphi(k)$  — арифметическая функция Эйлера, значение которой равно количеству чисел ряда  $1, 2, \dots, k$ , взаимно простых с числом  $k$ . Для формулировки и доказательства аналога этого соотношения используется ряд понятий и предварительных результатов из теории многочленов над конечным полем  $F_q$  из  $q$  элементов. Именно к ним относятся понятия нормированного неприводимого многочлена от одной переменной над полем  $F_q$  и  $n$ -кругового многочлена  $Q_n(x)$  над любым полем ненулевой характеристики. Кроме того, существенно используется также понятие порядка многочлена  $f(x) \in F_q[x]$ , согласно которому наименьшее натуральное число  $e$ , для которого многочлен  $f(x)$  делит  $x^e - 1$  в кольце  $F_q[x]$  есть порядок многочлена  $f(x)$ . При этом на явной формуле  $n$ -кругового многочлена  $Q_n(x)$ , а также на вспомогательном результате для числа нормированных неприводимых многочленов  $f(x) \in F_q[x]$  степени  $m$  и заданного порядка  $e$  основаны доказательства основных новых результатов. Основными из них являются формула для числа  $N_q(n)$  нормированных неприводимых многочленов степени  $n$ , а также аналог соотношения Гаусса для функции Эйлера.

**Ключевые слова:** конечное поле, нормированный неприводимый многочлен, порядок многочлена,  $n$ -круговой многочлен, функция Эйлера.

**AMS Subject Classification:** 11T55.

**Образец цитирования:** Пачев У. М., Токбаева А. А. О применениях конечных полей к функции Эйлера // Владикавк. мат. журн.—2025.—Т. 27, вып. 3.—С. 120–126. DOI: 10.46698/m2155-1449-8044-d.

## Введение

Конечные поля более целенаправленно стали изучаться в начале XIX века. Но еще до этого с разными подходами (см. [1, 2]) основы теории конечных полей были заложены в работах Гаусса и Галуа. (см. [1–3]).

Вслед за этим введением изложены вспомогательные результаты: леммы 1–5. Из них в лемме 1 дается явная формула для  $n$ -кругового многочлена  $Q_n(x)$  над полем  $K$  ненулевой характеристики, при этом такой многочлен задается формулой

$$Q_n(x) = \prod_{\substack{s=1, \\ (s,n)=1}}^n (x - \xi^s),$$

где  $\xi$  — первообразный корень  $n$ -й степени из единицы над полем  $K$ , причем  $\deg Q_n(x) = \varphi(n)$ , где  $\varphi(n)$  — функция Эйлера.

В лемме 2 дается формула для произведения  $J(q, n; x)$  всех нормированных неприводимых многочленов  $F_q[x]$ .

Леммы 3–5 непосредственно используются в доказательствах теорем 1 и 2, являющихся основными результатами нашей работы.

Из них в теореме 1 дается новая формула для числа  $N_q(n)$  нормированных неприводимых многочленов степени  $n$  над конечным полем  $F_q$ .

Возникает вопрос: существует ли какой-нибудь аналог известного соотношения Гаусса для функции Эйлера из теории чисел, но с меньшим числом слагаемых?

Положительный ответ на такой вопрос дает теорема 2, в ходе доказательства которой получен также новый вывод формулы для  $N_q(n)$  (другой способ см. в [4, 5]).

## 1. Вспомогательные результаты о многочленах над конечным полем

Основные понятия, относящиеся к многочленам над конечным полем даны во введении. Поэтому сразу переходим к изложению вспомогательных средств, используемых в доказательствах основных результатов.

**Лемма 1** (о явной формуле  $n$ -кругового многочлена). Для поля  $K$  характеристики  $p > 0$  и натурального  $n$ , не делящегося на  $p$ ,  $n$ -круговой многочлен задается формулой

$$Q_n(x) = \prod_{d|n} (x^d - 1)^{\mu\left(\frac{n}{d}\right)} = \prod_{d|n} (x^d - 1)^{\mu(d)},$$

где  $\mu$  — функция Мебиуса.

◁ Доказательство см. в [6], где оно основано на разложении

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

с последующим применением к этому равенству мультипликативного варианта формулы обращения Мебиуса. ▷

**Лемма 2.** Произведение  $J(q, n; x)$  всех нормированных неприводимых многочленов степени  $n$  из кольца многочленов  $F_q[x]$  задается формулой

$$J(q, n; x) = \prod_{d|n} (x^{q^d} - x)^{\mu\left(\frac{n}{d}\right)} = \prod_{d|n} (x^{q^{\frac{n}{d}}} - x),$$

где  $\mu$  — функция Мебиуса.

◁ Доказательство см. в [6]. ▷

Полезно и следующее представление для  $J(q, n; x)$  в разложенном виде через круговые многочлены.

**Лемма 3.** Для натурального числа  $n > 1$  имеет место формула

$$J(q, n; x) = \prod_{m|q^n-1} Q_m(x),$$

где  $Q_m(x)$  —  $m$ -круговой многочлен над полем  $F_q$  и произведение берется по всем натуральным делителям  $m$  числа  $q^n - 1$ , для которых  $n$  является показателем, которому принадлежит число  $q$  по модулю  $m$ .

◁ Доказательство см. в [6]. ▷

**Лемма 4.** Для произведения  $J(q, n; x)$  всех нормированных неприводимых многочленов степени  $n$  из кольца многочленов  $F_q[x]$  справедливо соотношение

$$J(q, n; x) \prod_{\substack{d|n, \\ \mu(d)=-1}} \left(x^{q^{\frac{n}{d}}} - x\right) = \prod_{\substack{d|n, \\ \mu(d)=1}} \left(x^{q^{\frac{n}{d}}} - x\right),$$

где  $\mu$  — функция Мебиуса.

◁ В силу леммы 2 имеем

$$J(q, n; x) = \prod_{\substack{d|n, \\ \mu(d)=-1}} \left(x^{q^{\frac{n}{d}}} - x\right)^{-1} \prod_{\substack{d|n, \\ \mu(d)=1}} \left(x^{q^{\frac{n}{d}}} - x\right).$$

Умножая теперь обе части этого равенства на произведение  $\prod \left(x^{q^{\frac{n}{d}}} - x\right)$ , получаем

$$J(q, n; x) \cdot \prod_{\substack{d|n, \\ \mu(d)=-1}} \left(x^{q^{\frac{n}{d}}} - x\right)^{-1} = \prod_{\substack{d|n, \\ \mu(d)=1}} \left(x^{q^{\frac{n}{d}}} - x\right). \triangleright$$

**Лемма 5.** Число нормированных неприводимых многочленов из  $F_q[x]$  степени  $m$  и порядка  $e$  равно  $\frac{\varphi(e)}{m}$ , если  $e \geq 2$ , а  $m$  — показатель, которому принадлежит число  $q$  по модулю  $e$ , равно 2, если  $m = e = 1$ , и равно нулю во всех остальных случаях.

◁ Доказательство см. в [6]. ▷

Отметим, что к данной части нашей работы имеют некоторое отношение публикации [7–13], в частности, в [7] доказано асимптотическое разложение для числа  $N_q(n)$  нормированных неприводимых многочленов степени  $n$  над полем  $F_q$ .

## 2. Доказательства основных результатов

В этой части нашей работы решается вопрос, поставленный в конце введения, относительно существования аналога соотношению Гаусса для функции Эйлера.

**Теорема 1.** Число  $N_q(n)$  неприводимых нормированных многочленов степени  $n$  в кольце  $F_q[x]$  определяется формулой

$$N_q(n) = \sum_{\substack{e|q^n-1, \\ q^m \not\equiv 1 \pmod{e}, \\ 1 \leq m < n}} \frac{\varphi(e)}{n},$$

где суммирование проводится по тем числам  $e$ , для которых  $q^m \not\equiv 1 \pmod{e}$  при  $1 \leq m < n$ ;  $\varphi$  — функция Эйлера.

◁ Так как все нормированные неприводимые многочлены степени  $n$  над полем  $F_q$  можно разбить на группы многочленов с заданным порядком  $e$ , то, применяя к каждой такой группе лемму 3 и затем суммируя по всем возможным значениям  $e$ , получим

$$N_q(n) = \sum_{\substack{e|q^n-1, \\ q^m \not\equiv 1 \pmod{e}, \\ 1 \leq m \leq n}} \frac{\varphi(e)}{n},$$

где  $q^m \not\equiv 1 \pmod{e}$  при  $1 \leq m \leq n$ . ▷

**Теорема 2.** Пусть  $q$  — степень простого числа;  $n$  — показатель, которому число  $q$  принадлежит по модулю  $e$ . Тогда имеет место соотношение

$$\sum_{\substack{e|q^n-1, \\ q^m \not\equiv 1 \pmod{e}, \\ 1 \leq m \leq n}} \varphi(e) = \sum_{d|n} \mu(d)q^{\frac{n}{d}},$$

где  $\varphi$  — функция Эйлера;  $\mu$  — функция Мебиуса; суммирование в левой части проводится по тем числам  $e$ , по которым число  $q$  принадлежит показателю  $n$  по модулю  $e$ .

◁ Воспользуемся леммой 3, согласно которой  $J(q, n; x) = \prod_{\substack{m|q^n-1, \\ q^s \not\equiv 1 \pmod{e}, \\ 1 \leq s \leq n}} Q_m(x)$ , где

$Q_m(x)$  —  $m$ -круговой многочлен над полем  $F_q$ , при этом произведение берется по всем натуральным делителям  $m$  числа  $q^n - 1$ . Применяя к обеим частям этого соотношения  $\deg$ , будем иметь

$$\deg J(q, n; x) = \deg \prod_{m|q^n-1} Q_m(x).$$

Воспользуемся еще леммой 4, согласно которой

$$J(q, n; x) \prod_{\substack{d|n, \\ \mu(d)=-1}} \left(x^{q^{\frac{n}{d}}} - x\right) = \prod_{\substack{d|n, \\ \mu(d)=1}} \left(x^{q^{\frac{n}{d}}} - x\right).$$

Переходя в этом равенстве к степеням, будем иметь

$$\deg J(q, n; x) + \sum_{\substack{d|n, \\ \mu(d)=-1}} \deg \left(x^{q^{\frac{n}{d}}} - x\right) = \sum_{\substack{d|n, \\ \mu(d)=1}} \deg \left(x^{q^{\frac{n}{d}}} - x\right).$$

Отсюда непосредственно следует

$$\begin{aligned} \deg J(q, n; x) &= \sum_{\substack{d|n, \\ \mu(d)=-1}} \deg \left(x^{q^{\frac{n}{d}}} - x\right) - \sum_{\substack{d|n, \\ \mu(d)=1}} \deg \left(x^{q^{\frac{n}{d}}} - x\right) \\ &= \sum_{\substack{d|n, \\ \mu(d)=1}} q^{\frac{n}{d}} - \sum_{\substack{d|n, \\ \mu(d)=-1}} q^{\frac{n}{d}} = \sum_{\substack{d|n, \\ \mu(d)=1}} \mu(d)q^{\frac{n}{d}} + \sum_{\substack{d|n, \\ \mu(d)=-1}} \mu(d)q^{\frac{n}{d}} = \sum_{d|n} \mu(d)q^{\frac{n}{d}}. \end{aligned} \tag{1}$$

Теперь вычисляем также  $\deg I(q, n; x)$  по лемме 3. Имеем

$$\deg I(q, n; x) = \deg \prod_{\substack{m|q^n-1, \\ q^s \not\equiv 1 \pmod{e}, \\ 1 \leq s \leq n}} Q_m(x) = \sum_{\substack{m|q^n-1, \\ q^s \not\equiv 1 \pmod{e}, \\ 1 \leq s \leq n}} \deg Q_m(x) = \sum_{\substack{m|q^n-1, \\ q^s \not\equiv 1 \pmod{e}, \\ 1 \leq s \leq n}} \varphi(m). \tag{2}$$

Теперь из (1) и (2) следует утверждение теоремы 2. ▷

Приведем пример к результату теоремы 2 в случае  $q = 3$ ,  $n = 4$ . Сначала находим  $\sum_{d|4} \mu(d) \cdot 3^{\frac{4}{d}} = \mu(1) \cdot 3^4 + \mu(2) \cdot 3^2 + \mu(4) \cdot 3 = 72$ . Теперь вычисляем

$$\sum_{\substack{e|3^4-1, \\ q^m \not\equiv 1 \pmod{e}, \\ 1 \leq m < n}} \varphi(e),$$

где суммирование проводится по делителям числа 80, по которым число 3 будет принадлежать показателю 4 по модулю  $e$ .

Определяем числа  $e$ , для которых  $\frac{e}{80}$  и  $3^m \not\equiv 1 \pmod{e}$  при  $1 \leq m \leq 4$ .

Из всех делителей 80 нашим условиям будут удовлетворять только следующие числа:  $e_1 = 5$ ,  $e_2 = 10$ ,  $e_3 = 16$ ,  $e_4 = 20$ ,  $e_5 = 40$ ,  $e_6 = 80$ . Тогда

$$\sum_{\substack{e|3^4-1, \\ q^m \not\equiv 1 \pmod{e}, \\ 1 \leq m \leq n}} \varphi(e) = \varphi(5) + \varphi(10) + \varphi(16) + \varphi(20) + \varphi(40) + \varphi(80) = 72.$$

Значит, для обеих сумм получаем равные значения.

Сравним полученное значение с соотношением Гаусса для функции Эйлера. Имеем

$$\sum_{d|80} \varphi(d) = 80.$$

Значит,

$$\sum_{d|80} \varphi(d) - \sum_{\substack{d|80, \\ q^m \not\equiv 1 \pmod{e}, \\ 1 \leq m \leq n}} \varphi(d) = 8,$$

но при этом во второй сумме меньше слагаемых, чем в первой сумме.

Завершая изложение нашей работы, отметим еще, что имеются также некоторые приложения теории конечных полей к криптографии (см. [4, 15, 13]).

### Литература

1. Гаусс К. Ф. Труды по теории чисел.—М.: Изд-во АН СССР, 1959.—987 с.
2. Галуа Э. Из теории чисел. Сочинения.—М.—Л.: ОНТИ, 1936.—342 с.
3. Пачев У. М. Избранные главы теории чисел.—Нальчик: Изд-во М. и В. Котляровых, 2016.—186 с.
4. Минеев М. П., Чубариков В. Н. Лекции по арифметическим вопросам криптографии.—М.: Изд-во «Луч», 2014.—224 с.
5. Степанов С. А. Сравнения.—М.: Изд-во «Знание», 1975.
6. Лидл Р., Нидеррайтер Г. Конечные поля. Т. 1.—М.: «Мир», 1988.—486 с.
7. Ленской Д. Н. К арифметике многочленов над конечным полем // Волжский матем. сб. Тр. матем. кафедр пед. ин-тов Поволжья.—1966.—Вып. 4.—С. 155–159.
8. Fredman M. L. Congruence formulas obtained by counting irreducible // Pacific J. Math.—1970.—Vol. 35, № 3.—P. 613–624. DOI: 10.2140/pjm.1970.35.613.
9. Степанов С. А. О числе неприводимых в  $F_q[x]$  многочленов специального вида // Успехи мат. наук.—1985.—Т. 40, вып. 4(244)—С. 199–200.
10. Carlitz L. The arithmetic of polynomials in a Galois field // Proc. Nat. Acad. Sci.—1931.—Vol. 17, № 2.—P. 120–122. DOI: 10.1073/pnas.17.2.120.
11. Williams K. S. Polynomials with irreducible factors of specified degree // Canada. Math. Bull.—1969.—Vol. 12, № 2.—P. 221–223. DOI: 10.4153/CMB-1969-026-2.
12. Пачев У. М., Кодзоков А. Х., Машезова А. М. Об оценках числа нормированных неприводимых многочленов заданной степени над конечным полем // Алгебра и динамические системы. Тез. докл. Междунар. конф., посвящ. 110-летию со дня рождения С. Н. Черникова.—Нальчик, 2022.—С. 100–101.
13. Carlitz L. Some theorems on irreducible polynomials over a finite field // J. Reine Angew. Math.—1967.—Vol. 227.—P. 212–220.

14. Levine J., Brawley J. V. Involutory commutants with some applications to algebraic cryptographic // J. Reine Angew. Math.—1966.—Vol. 224.—P. 20–43.
15. Levine J., Brawley J. V. Some cryptographic applications of permutation polynomials // Cryptologia.—1977.—Vol. 1.—P. 76–92. DOI: 10.1080/0161-117791832814.

*Статья поступила 28 апреля 2025 г.*

ПАЧЕВ УРУСБИ МУХАМЕДОВИЧ  
Кабардино-Балкарский государственный университет  
им. Х. М. Бербекова,  
главный научный сотрудник, профессор кафедры  
алгебры и дифференциальных уравнений  
РОССИЯ, 360004, Нальчик, ул. Чернышевского, 173  
E-mail: [urusbi@rambler.ru](mailto:urusbi@rambler.ru)  
<https://orcid.org/0009-0002-8362-6174>

ТОКБАЕВА АЛЬБИНА АНИУАРОВНА  
Кабардино-Балкарский государственный университет  
им. Х. М. Бербекова,  
доцент кафедры алгебры и дифференциальных уравнений  
РОССИЯ, 360004, Нальчик, ул. Чернышевского, 173  
E-mail: [tok2506@mail.ru](mailto:tok2506@mail.ru)  
<https://orcid.org/0009-0007-4926-4452>

*Vladikavkaz Mathematical Journal*  
2025, Volume 27, Issue 3, P. 120–126

## ON APPLICATIONS OF FINITE FIELDS TO THE EULER FUNCTION

Pachev, U. M.<sup>1</sup> and Tokbaeva, A. A.<sup>1</sup>

<sup>1</sup>Kabardino-Balkarian State University,  
173 Chernyshevsky St., Nalchik 360004, Russia  
E-mail: [urusbi@rambler.ru](mailto:urusbi@rambler.ru), [tok2506@mail.ru](mailto:tok2506@mail.ru)

**Abstract.** The manuscript is devoted to applications of finite fields to the Euler function from number theory. Using the concept of a normalized irreducible polynomial of a given degree over a finite field  $F_q$ , we obtain an analogue of the well known Gauss relation  $\sum_{d|n} \varphi(d) = n$ . Here  $\varphi(k)$  is the Euler arithmetic function such that its value is equal to the number of integers  $1, 2, \dots, k$  relatively prime to  $k$ . In order to formulate and prove an analogue of this relation we use concepts and preliminary results from the polynomial theory over a finite field  $F_q$  of  $q$  elements. In particular, we apply the concepts of a normalized irreducible polynomial of one variable over the field  $F_q$  and  $n$ -circle polynomial  $Q_n(x)$  over any field of nonzero characteristic. In addition, we use the concept of the order of a polynomial  $f(x) \in F_q[x]$  such that if the polynomial  $f(x)$  divides  $x^e - 1$  in the ring  $F_q[x]$ , then the minimal natural number  $e$  is the order of the polynomial  $f(x)$ . The proof of the main new results is based on the explicit formula for the  $n$ -circle polynomial  $Q_n(x)$  and on the auxiliary result for the number of normalized irreducible polynomials  $f(x) \in F_q[x]$  degree  $m$  and given order  $e$ . We obtain the formula for  $N_q(n)$  of normalized irreducible polynomials degree  $n$  and an analogue of the Gauss relation for the Euler function.

**Keywords:** finite field, normed irreducible polynomial, polynomial order,  $n$ -cyclotomic polynomial, Euler function.

**AMS Subject Classification:** 11T55.

**For citation:** Pachev, U. M. and Tokbaeva, A. A. On Applications of Finite Fields to the Euler Function, *Vladikavkaz Math. J.*, 2025, vol. 27, no. 3, pp. 120–126 (in Russian). DOI: 10.46698/m2155-1449-8044-d.

## References

1. Gauss, K. F. *Works on Number Theory*, Moscow, Publishing House the USSR Academy of Sciences, 1959, 987 p. (in Russian).
2. Galois, E. *From the Theory of Numbers. Works*, Moscow, Leningrad, ONTI, 1936, pp. 35–47 (in Russian).
3. Pachev, U. M. *Selected Chapters of Number Theory*, Nalchik, «M. and V. Kotlyarov», 2016, 186 p. (in Russian).
4. Mineev, M. P. and Chubarikov, V. N. *Lectures on Arithmetic Issues of Cryptography*, Moscow, 2014, 224 p. (in Russian).
5. Stepanov, S. A. *Congruences*, Publishing house «Knowledge», Moscow, 1975 (in Russian).
6. Lidl, R. and Niederreiter, H. *Finite Fields. Vol. 1*, Cambridge University Press, 1983.
7. Lenskoy, D. N. On the Arithmetic of Polynomials Over a Finite Field, *Volzhsky Mat. Sb., Kuibishev. Works of Mathematical Departments of Pedagogical Institutes of the Volga Region, issue 4*, 1966, pp. 155–159 (in Russian).
8. Fredman, M. L. Congruence Formulas Obtained by Counting Irreducible, *Pacific Journal of Mathematics*, 1970, vol. 35, no. 3, pp. 613–624. DOI: 10.2140/pjm.1970.35.613.
9. Stepanov, S. A. On the Number of Irreducible Polynomials in  $F_q[x]$  of Special Form, *Russian Mathematical Surveys*, 1985, vol. 40, no. 4, pp. 219–220. DOI: 10.1070/RM1985v04n04ABEH003656.
10. Carlitz, L. The Arithmetic of Polynomials in a Galois Field, *Proceedings of the National Academy of Sciences*, 1931, vol. 17, no. 2, pp. 120–122. DOI: 10.1073/pnas.17.2.120.
11. Willams, K. S. Polynomials with Irreducible Factors of Specified Degree, *Canadian Mathematical Bulletin*, 1969, vol. 12, no. 2, pp. 221–223. DOI: 10.4153/CMB-1969-026-2.
12. Pachev, U. M., Kodzokov, A. Kh. and Mashezova, A. M. On Estimates on the Number of Normalized Irreducible Polynomials of a Given Degree Over a Finite Field, *Algebra and Dynamical System. Abstracts of Reports of the International Conference Dedicated to the 110-th Anniversary of the Birth of S. N. Chernikov*, Nalchik, 2022, pp. 100–101.
13. Carlitz, L. Some Theorems on Irreducible Polynomials Over a Finite Field, *Journal für die reine und angewandte Mathematik*, 1967, vol. 227, pp. 212–220.
14. Levine, J. and Brawley, J. V. Involutory Commutants with Some Applications to Algebraic Cryptography, *Journal für die Reine und Angewandte Mathematik*, 1966, vol. 224, pp. 20–43.
15. Levine, J. and Brawley, J. V. Some Cryptographic Applications of Permutation Polynomials, *Cryptologia*, 1977, vol. 1, pp. 76–92. DOI: 10.1080/0161-117791832814.

Received April 28, 2025

URUSBI M. PACHEV  
 Kabardino-Balkarian State University,  
 173 Chernyshevsky St., Nalchik 360004, Russia,  
 Professor of the Department of Algebra  
 and Differential Equations  
 E-mail: [urusbi@rambler.ru](mailto:urusbi@rambler.ru)  
<https://orcid.org/0009-0002-8362-6174>

ALBINA A. TOKBAEVA  
 Kabardino-Balkarian State University,  
 173 Chernyshevsky St., Nalchik 360004, Russia,  
 Associate Professor of the Department of Algebra  
 and Differential Equations  
 E-mail: [tok2506@mail.ru](mailto:tok2506@mail.ru)  
<https://orcid.org/0009-0007-4926-4452>