Алевтина Юрьевна Васильева — асс., Балтийский федеральный университет им. И. Канта, Калининград.
E-mail: vasilyeva.alevtina@gmail.com

**About the authors**

Prof. Leonid Zinin — I. Kant Baltic Federal University, Kaliningrad.
E-mail: leonid.zinin@gmail.com

Alexandr Sharamet — ass., I. Kant Baltic Federal University, Kaliningrad.
E-mail: alexsharamet@gmail.com



Alevtina Vasileva — ass., I. Kant Baltic Federal University, Kaliningrad.
E-mail: vasilyeva.alevtina@gmail.com

УДК 512.62

*С. И. Алешников, М. В. Алешникова, А. А. Горбачёв*

# ОБ ОДНОМ АЛГОРИТМЕ ВЫЧИСЛЕНИЯ ОБРАТНЫХ ЭЛЕМЕНТОВ В КОНЕЧНЫХ ПОЛЯХ

*В работе предложены два алгоритма вычисления обратных элементов в конечном поле $\mathbf{F}_{q^n}$, где $q$ — степень простого числа. Они получены путем обобщения алгоритма Вонга для поля $\mathbf{F}_{2^n}$ с использованием главной идеи быстрого алгоритма вычисления обратного элемента в поле $\mathbf{F}_{2^n}$.*

*In work are two algorithms of calculation of inverses in a finite field $\mathbf{F}_{q^n}$ developed, where $q$ is power of the prime number. They are received by generalisation of algorithm of Wong for a field $\mathbf{F}_{2^n}$ with use of the main idea for fast algorithm of calculation of inverses in the field $\mathbf{F}_{2^n}$.*

**Ключевые слова:** конечное поле, умножение, инверсия, нормальный базис, циклический сдвиг, алгоритм, быстрый алгоритм.

**Key words:** finite field, multiplication, inversion, normal basis, cyclic shift, algorithm, fast algorithm.

## Введение

В криптосистемах с открытым ключом на эллиптических и гиперэллиптических кривых, в криптосистемах на основе идентификационных данных, использующих спаривания Вейля и Тэйта и их модификации, используются конечные поля большого порядка. В то же время наиболее трудоемкая операция — вычисление обратных элементов. Вопросам ускорения вычислений посвящена огромная литература.


*Вестник Балтийского федерального университета им. И. Канта. Сер.: Физико-математические и технические науки. 2017. № 2. С. 34–40.*

Так, список литературы в [2] состоит из 3084 источников. Большое число вычислительных алгоритмов в конечных полях представлено в [1]. Информация по структуре конечных полей содержится в [4; 5].

В работе [3] изложены два алгоритма.

1. Алгоритм Вонга для вычисления обратных элементов в поле $\mathbf{F}_{2^n}$ с использованием нормального базиса и циклического сдвига. Он требует выполнения $n-2$ операций умножения в поле и $n-1$ циклических сдвигов.

2. Быстрый алгоритм для вычисления обратных элементов в поле $\mathbf{F}_{2^n}$, $(n=2^r+1)$, также использующий нормальный базис и циклический сдвиг. Требует выполнения $M = r$ операций умножения.



Целью этой работы стало обобщение названных алгоритмов, а именно разработка алгоритма вычисления обратного элемента в поле $\mathbf{F}_{q^n}$. В работе получена обобщенная формула для нахождения обратного элемента и, опираясь на алгоритм Вонга, представлен обобщенный алгоритм для поля $\mathbf{F}_{q^n}$. Представлен также быстрый алгоритм для поля $\mathbf{F}_{2^n}$.

## 1. Обобщенный алгоритм Вонга

Напомним, что нормальным базисом поля $\mathbf{F}_{q^n}$ над $\mathbf{F}_q$ называется базис вида $a, a^q, a^{q^2}, \ldots, a^{q^{n-1}}$, где $a \in \mathbf{F}_{q^n}$, $a \neq 0$. Разложение элемента $x \in \mathbf{F}_{q^n}$ по этому базису записываем в виде

$$x = x_0 a + x_1 a^q + \ldots x_{n-1} a^{q^{n-1}} = [x_0, x_1, \ldots, x_{n-1}].$$

Тогда элемент $x^{q^k}$ вычисляется с помощью $k$ циклических сдвигов, т. е.

$$x^{q^k} = [x_{n-k}, x_{n-k+1}, \ldots, x_{n-1}, x_0, \ldots, x_{n-k-1}].$$

Если натуральное $n$ записано в виде

$$n = 2^{k_1} + 2^{k_2} + \ldots + 2^{k_s},$$

где $k_1 > k_2 > \ldots > k_s$, то вес Хэмминга $H_w(n)$ числа $n$ есть количество индексов $i$, $1 \leqslant i \leqslant s$, для которых $k_i$ встречаются в предыдущем разложении.

Так как для любого $x \in \mathbf{F}_{q^n}$ выполняется $x^{q^n} = x$, то

$$x^{-1} = x^{q^n - 2}. \qquad (1)$$

Рассмотрим степень $q^n - 2$. Имеем

$$\begin{aligned} q^n - 2 &= (q^n - q) + (q-2) = q(q^{n-1} - 1) + (q-2) = \\ &= q(q-1)(1 + q + q^2 + \ldots + q^{n-2}) + (q-2) = \\ &= (q-1)(q + q^2 + q^3 + \ldots + q^{n-1}) + (q-2). \end{aligned}$$

Следовательно,

$$x^{-1} = x^{(q-1)(q+q^2+q^3+\ldots+q^{n-1})+(q-2)} = (x^{q-1})^{q+q^2+q^3+\ldots+q^{n-1}} \cdot x^{q-2}.$$

Таким образом, обратный элемент $x^{-1}$ вычисляется как

$$x^{-1} = (x^{q-1})^q \cdot (x^{q-1})^{q^2} \cdot (x^{q-1})^{q^3} \cdot \ldots \cdot (x^{q-1})^{q^{n-1}} \cdot (x^{q-2}).$$

Например, при $q = 2$ обратный элемент $x^{-1}$ в поле $\mathbf{F}_{2^n}$ вычисляется как

$$x^{-1} = x^2 \cdot x^{2^2} \cdot x^{2^3} \cdot \ldots \cdot x^{2^{n-1}}.$$

Например, при $q = 3$ обратный элемент $x^{-1}$ в поле $\mathbf{F}_{3^n}$ вычисляется как

$$x^{-1} = (x^2)^3 \cdot (x^2)^{3^2} \cdot (x^2)^{3^3} \cdot \ldots \cdot (x^2)^{3^{n-1}} \cdot x.$$

Например, при $q = 5$ обратный элемент $x^{-1}$ в поле $\mathbf{F}_{5^n}$ вычисляется как

$$x^{-1} = (x^4)^5 \cdot (x^4)^{5^2} \cdot (x^4)^{5^3} \cdot \ldots \cdot (x^4)^{5^{n-1}} \cdot x^3.$$

Имеем следующий алгоритм вычисления $x^{-1}$ в поле $\mathbf{F}_{q^n}$.

**Алгоритм 1.**

| | | |
|---|---|---|
| Шаг 1. | $g := x^{q-2}$ | ($q$ – 3 умножений) |
| Шаг 2. | $y_1 := g \cdot x$ | (1 умножение) |
| Шаг 3. | $y := y_1$ | |
| Шаг 4. | for $k$ :=1 to $n$ – 2 do | |
| Шаг 5. | begin | |
| Шаг 6. | $z := y^q$ | (1 циклический сдвиг) |
| Шаг 7. | $y := z \cdot y_1$ | (1 умножение) |
| Шаг 8. | end | |
| Щаг 9. | $y := y^q$ | (1 циклический сдвиг) |
| Шаг 10. | $y := y \cdot g$ | (1 умножение) |
| Шаг 11. | write $y$ | |

Таким образом, алгоритм требует $q + n - 3$ операций умножения в поле $\mathbf{F}_{q^n}$ и $n - 1$ циклических сдвигов над $\mathbf{F}_q$, $n > 2$.

Алгоритм Вонга является частным случаем предыдущего алгоритма для $q = 2$. В этом алгоритме для вычисления $x^{-1}$ требуется $n - 2$ операции умножения в поле $\mathbf{F}_{2^n}$ и $n - 1$ циклических сдвигов.

**Пример 1.** Вычисление обратного $x^{-1}$ в поле $\mathbf{F}_{3^8}$ по формуле (1), а именно $x^{-1} = x^{3^8-2} = x^{6559}$ требует 6558 операций умножения. Использование предыдущего алгоритма требует $q + n - 3 = 8$ операций умножения и $n - 1 = 7$ циклических сдвигов.

Таким образом, выигрыш в числе операций в полях большого порядка весьма существенный.

## 2. Быстрый алгоритм вычисления инверсии

**Предложение 1.** *Пусть* $x$ *– ненулевой элемент поля* $\mathbf{F}_{2^n}$ $(n = 2^r + 1)$. *Тогда существует алгоритм вычисления обратного элемента* $x^{-1}$, *требующий числа умножений*

$$M = \log_2(n-1) = r$$

*и числа циклических сдвигов*

$$S = n - 1 = 2^r.$$



Соответствующий алгоритм имеет такой вид.

**Алгоритм 2.**

Шаг 1. $y := x$
Шаг 2. for $k := 0$ to $r - 1$ do
Шаг 3. begin
Шаг 4. $\quad z := y^{2^{2^k}}$ $\quad$ ($2^k$ циклических сдвигов)
Шаг 5. $\quad y := z \cdot y$ $\quad$ (1 умножение)
Шаг 6. end
Шаг 7. $y := y^2$ $\quad$ (1 циклический сдвиг)
Шаг 8. write $y$

**Пример 2.** Вычисление обратного $x^{-1}$ в поле $\mathbf{F}_{2^9}$ по формуле (1), а именно $x^{-1} = x^{2^9 - 2} = x^{510}$ требует 509 операций умножения. Использование предыдущего алгоритма требует $M = \log_2(n-1) = \log_2 8 = 3$ операции умножения и $n - 1 = 8$ циклических сдвигов.

Следующее предложение является обобщением предыдущего.

**Предложение 2.** *Пусть* $x$ *– ненулевой элемент поля* $\mathbf{F}_{2^n}$. *Тогда существует алгоритм вычисления обратного элемента* $x^{-1}$, *требующий числа умножений*

$$M = [\log_2(n-1)] + H_w(n-1) - 1 \leqslant 2 \cdot [\log_2(n-1)],$$

*где* $[x]$ *– целая часть числа* $x$, *и числа циклических сдвигов*

$$S = n - 1.$$

Соответствующий алгоритм для быстрого вычисления обратного $x^{-1}$ в поле $\mathbf{F}_{2^n}$ имеет следующий вид.

**Алгоритм 3.**

Шаг 1. $y := x$
Шаг 2. for $k := 0$ to $k_1 - 1$ do
Шаг 3. begin
Шаг 4. $\quad z := y^{2^{2^k}}$ $\quad$ ($2^k$ циклических сдвигов)
Шаг 5. $\quad y := z \cdot y$ $\quad$ (1 умножение)

Шаг 6. $y[k] := y$
Шаг 7. end
Шаг 8. for $i := 2$ to $s$ do
Шаг 9. begin
Шаг 10. $z := y^{2^{2^{k_i}}}$ ($2^{k_i}$ циклических сдвигов)
Шаг 11. if $k_i = 0$ then $y := z \cdot x$
else $y := z \cdot y[k_i - 1]$ (1 умножение)
Шаг 12. end
Шаг 13. $y := y^2$ (1 циклический сдвиг)
Шаг 14. write $y$



**Пример 3.** Вычисление обратного $x^{-1}$ в поле $\mathbf{F}_{2^{12}}$ по формуле (1), а именно $x^{-1} = x^{2^{12}-2} = x^{4094}$ требует 4093 операций умножения. Использование предыдущего алгоритма требует

$$M = [\log_2(12-1)] + H_w(12-1) - 1 = 3 + 3 - 1 = 5$$

операций умножения и

$$S = 12 - 1 = 11$$

циклических сдвигов.

Следующее предложение обобщает быстрый алгоритм вычисления $x^{-1}$ для произвольного $q$.

**Предложение 3.** *Пусть $x$ – ненулевой элемент поля $\mathbf{F}_{q^n}$. Тогда существует алгоритм вычисления обратного элемента $x^{-1}$, требующий числа умножений*

$$M = [\log_2(n-1)] + H_w(n-1) + H_w(q-2)$$

*и числа циклических сдвигов*

$$S = n - 1.$$

*Запишем алгоритм для быстрого вычисления обратного $x^{-1}$ в поле $\mathbf{F}_{q^n}$. Пусть*

$$n - 1 = \sum_{s=1}^{t} 2^{k_s}\ , \text{ где } \ k_1 > k_2 > \ldots > k_t.$$

$$q - 2 = \sum_{s=1}^{j} 2^{p_s}\ , \text{ где } \ p_1 > p_2 > \ldots > p_t.$$

*Тогда $H_w(n-1) = t$.*

**Алгоритм 4.**

Шаг 1. $z := x$
Шаг 2. for $k := 0$ to $k_1 - 1$ do
Шаг 3. begin
Шаг 4. $l := z^{q^{2^k}}$ ($2^k$ циклических сдвигов)
Шаг 5. $z := z \cdot l$ (1 умножение)
Шаг 6. $z[k] := z$

Шаг 7. end
Шаг 8. for $i := 2$ to $t$ do
Шаг 9. begin
Шаг 10. $l := y^{q^{2^{k_i}}}$ ($2^{k_i}$ циклических сдвигов)
Шаг 11. if $k_i = 0$ then $z := z \cdot x$
else $z := l \cdot z[k_i - 1]$ (1 умножение)
Шаг 12. end
Шаг 13. $z := z^q$ (1 циклический сдвиг)
Шаг 14. $y := z \cdot x$ (1 умножение)
Шаг 15. $g := y$
Шаг 16. $y := y^{2^{p_1}}$
Шаг 17. for $k := 2$ to $j$ do
Шаг 18. begin
Шаг 19. $r := g^{2^{p_k}}$
Шаг 20. $y := y \cdot r$ (1 умножение)
Шаг 21. end
Шаг 22. $x^* := y \cdot z$ (1 умножение)
Шаг 23. write $x^*$



**Пример 4.** Вычисление обратного $x^{-1}$ в поле $\mathbf{F}_{9^8}$ по формуле (1), а именно $x^{-1} = x^{9^8-2} = x^{43046719}$ требует 43 046 718 операций умножения. Использование предыдущего алгоритма требует

$$M = [\log_2(8-1)] + H_w(8-1) + H_w(9-2) = 2 + 3 + 3 = 8$$

операций умножения и

$$S = 8 - 1 = 7$$

циклических сдвигов.

Заметим, что в силу определений выполняется неравенство

$$H_w(n-1) \leqslant [\log_2(n-1)] + 1.$$

Тогда число умножений в алгоритме 4 оценивается так:

$$\begin{aligned} M_4 &= [\log_2(n-1)] + H_w(n-1) + H_w(q-2) \leqslant \\ &\leqslant [\log_2(n-1)] + [\log_2(n-1)] + H_w(q-2) + 1 \leqslant \\ &\leqslant 2 \cdot [\log_2(n-1)] + q - 2 + 1 \leqslant n - 2 + q - 1 = n + q - 3 = M_1, \end{aligned}$$

начиная с $n = 6$. Поэтому алгоритм 4 более быстрый, чем алгоритм 1.

### Список литературы

1. *Handbook* of elliptic and hyperelliptic curve cryptography / Scientific editors, Henry Cohen & Gerhard Frey. Chapman & Hall/CRC, 2006.
2. *Handbook* of finite Fields / Scientific editors, Gary L. Mullen, Daniel Panario. CRC Press, Taylor & Francis Group, 2013.
3. *Itoh T., Tsujii S.* A fast algorithm for computing multiplicative inverses in $GF(2^m)$ using normal bases, Inform. and Comput. 1988. Vol. 78. P. 171—177.

4. *Jungnickel D*. Finite fields: Structure and Arithmetics. Mannheim ; Leipzig ; Wien ; Zürich, 1993.

5. *Lidl R*., *Niederreiter H*. Finite fields (Second edition). Cambridge University Press, 1997.

**Об авторах**

Сергей Иванович Алешников — канд. техн. наук, доц., Балтийский федеральный университет им. И. Канта, Калининград.
E-mail: elliptec@mail.ru

Марина Валерьевна Алешникова — ст. преп., Балтийский федеральный университет им. И. Канта, Калининград.
E-mail: aleshnikova_m_v@mail.ru

Андрей Александрович Горбачёв — канд. техн. наук, доц., Калининградский государственный технический университет.
E-mail: terjer@mail.ru

**About the authors**

Dr Sergey Aleshnikov, ass. prof., I. Kant Baltic Federal University, Kaliningrad.
E-mail: elliptec@mail.ru

Marina Aleshnikova, head teacher, I. Kant Baltic Federal University, Kaliningrad.
E-mail: aleshnikova_m_v@mail.ru

Dr Andrey Gorbachev, ass. prof., Kaliningrad State Technical University.
E-mail: terjer@mail.ru



УДК 511

***С. И. Алешников, М. В. Алешникова, А. А. Горбачёв***

# ЭЛЕМЕНТАРНОЕ РЕШЕНИЕ ОДНОГО КУБИЧЕСКОГО ДИОФАНТОВА УРАВНЕНИЯ

*Представлен элементарный подход к решению кубического диофантова уравнения $y^2 = x^3 - 2^{2s}$, зависящего от одного натурального параметра s. Получено полное решение для всех значений s.*

*An elementary approach to solving of the cubic Diophantine equations $y^2 = x^3 - 2^{2s}$, depending on one natural parameter s is presented. The full solving for all values s is received.*

**Ключевые слова:** диофантово уравнение, квадратичное поле, число классов, уравнение Пелля, делимость, целые гауссовы числа, фундаментальная единица.

**Key words:** Diophantine equation, quadratic field, class number, Pell equation, divisibility, Gaussian integers, fundamental unit.