УДК 512.624
МРНТИ 27.17.27

https://doi.org/10.55452/1998-6688-2024-21-1-85-93

[1]*Турусбекова У.К.,
PhD, ORCID ID 0000-0002-0591-2143, *e-mail: umut.t@mail.ru
[2]Муратбеков М.М.,
PhD, ORCID ID 0000-0003-2197-4982, e-mail: Madimm@list.ru
[3]Алтынбек С.А.,
PhD, ORCID ID 0000-0002-8435-7773, e-mail: serik_aa@bk.ru

[1]Esil University, 010000, г. Астана, Казахстан
[2]Евразийский национальный университет им. Л.Н. Гумилева, 010008, г. Астана, Казахстан,
[3]Казахский университет технологии и бизнеса, 010000, г. Астана, Казахстан

ИССЛЕДОВАНИЕ АЛГОРИТМОВ ПОИСКА ПРИМИТИВНЫХ ЭЛЕМЕНТОВ КОНЕЧНОГО ПОЛЯ БОЛЬШОГО ПОРЯДКА

Аннотация

Одной из наиболее важных нерешенных и заведомо трудных задач в вычислительной теории конечных полей является разработка быстрого алгоритма для построения примитивных корней в конечном поле. С другой стороны, для многих приложений вместо примитивного корня достаточно элемента высокого мультипликативного порядка. Такие приложения включают, помимо прочего, криптографию, теорию кодирования, генерацию псевдослучайных чисел и комбинаторные схемы. Явные построения элементов высокого порядка обычно полагаются на методы комбинаторики, которые могут обеспечить доказуемую нижнюю границу порядка, но не вычисляют его точный порядок. Выполнение таких построений обычно основано на том, что факторизация порядка уже известна. В идеале мы должны иметь возможность получить примитивный элемент для любого конечного поля за разумное время. Однако если простая факторизация порядка группы неизвестна, этого сложно добиться. Таким образом, ставят менее амбициозную задачу – задачу построения элемента достаточно высокого порядка. В данной статье мы рассматриваем различные алгоритмы, которые находят элемент высокого порядка как для общих, так и для специальных конечных полей. Кроме того, в этой работе мы касаемся теории периодов Гаусса над конечными полями, их обобщениями и аналогами, которые, как известно, уже доказали свою полезность для ряда различных приложений.

Ключевые слова: конечное поле, примитивный элемент, простое число, простая факторизация, периоды Гаусса.

Введение

Известно, что мультипликативные группы конечных полей являются циклическими. Их мультипликативные порождающие иногда называют примитивными элементами. Важной проблемой в вычислительной теории чисел является поиск мультипликативного порождающего для конечного поля. Общеизвестно, что эта проблема сложна и все еще остается открытой. Трудность ее заключается не в недостатке примитивных элементов. В действительности, доказана следующая теорема.

Теорема 1. Пусть q – простая степень, а F_q – конечное поле, состоящее из q элементов. Число примитивных элементов в F_q, т.е. $\varphi(q-1)$, больше, чем $cq/\log\log q$, где $c > 0$ – абсолютная константа, а φ является функцией Эйлера [1, глава 1, теорема 5.1].

Функция $1/\log\log q$ является функцией от размера входных данных и очень медленно приближается к нулю по мере того, как q становится большим. Это означает, что, если выбрать случайный элемент, есть значительная вероятность получить именно примитивный элемент. Эквивалентно, если выбрать список из $(\log\log q)^{1+\varepsilon}$ множества случайных элементов, с вероятностью $1-o(1)$ в списке будет примитивный элемент. Однако очень трудно решить,

какой именно элемент будет примитивным. Единственный известный общий метод основан на следующем факте.

Предложение 2. Пусть $q-1=p_1^{e_1}p_2^{e_2}\ldots p_m^{e_m}$, где $p_1,\ldots,p_m$ – разные простые числа. Элемент α является примитивным в F_a тогда и только тогда, когда для любого p_i, где $1 \le i \le m$, выполняется неравенство $\alpha^{(q-1)/p_i} \neq 1$.

На основе этих утверждений можно построить рандомизированный алгоритм для нахождения примитивного элемента с предполагаемой временной сложностью $e^{O\left(\log^{1/3} q(\log\log q)^{2/3}\right)}$. Эта сложность равна сложности самого быстрого алгоритма общего назначения с коэффициентом $q-1$ и непрактична по мере увеличения q. Более того, нахождение примитивного элемента является крайним случаем нахождения элемента большого порядка.

На практике особенно полезны поля с небольшими характеристиками. Если характеристики полей малы, то часто поиск простой факторизации порядка является более сложной задачей, чем поиск порядка случайных простых полей. В этом контексте задачу об элементе большого порядка можно перефразировать следующим образом: для фиксированной простой степени q найти элемент в F_{q^n} с большим порядком за полиномиальное по n время. Еще одна актуальная, но при этом более простая задача: требуется найти число n, большее заданного числа N, и элемент порядка по крайней мере q^{n^c} в F_{q^n} для некоторой константы c. Логическое обоснование этого вопроса, называемого *проблемой специального конечного поля с элементами высокого порядка*, состоит в том, чтобы сначала рассмотреть вопросы, связанные со специальными конечными полями, а затем попытаться увеличить «плотность» последовательности из n, чтобы в итоге для всех расширений конечного поля можно было бы найти элементы высокого порядка. Напомним, что *плотностью последовательности* (A) по Шнирельману называется точная нижняя грань всех значений дроби $A(n)/n$, где $A(n)$ – число натуральных чисел последовательности (A), не превосходящих n. Поскольку $0 \le A(n) \le n$, получаем, что $0 \le A(n)/n \le 1$. Заметим, что от нас не требуется вычислять точный порядок элемента. Вместо этого нам нужно только предоставить доказательство того, что элемент имеет порядок, превышающий определенную границу.

Обзор литературы

Разработка быстрого алгоритма для построения примитивных элементов конечных полей является сложной задачей в вычислительной теории конечных полей. В зависимости от конкретных задач иногда достаточно изучить построения элементов высокого порядка. В своей классической работе [2] Ванг показал, что для простого конечного поля F_p наименее примитивный элемент ограничен $p^{1/4+\varepsilon}$. В работе [3] Шоуп улучшил его результат. В статье [4] показано, как построить множество мощности $O(\log^4 p)$, которое содержит по крайней мере один примитивный элемент, однако это построение основано на расширенной гипотезе Римана. В работах [5–6] показано, что в поле с простой степенью q примитивный элемент может быть найден с временной сложностью $q^{\frac{1}{4}+\varepsilon}$. В статье [7] приведен метод построения элементов в F_{q^n}, порядки которых больше любого многочлена от n, когда n становится большим. В работе [8] приводится тщательный анализ конструкции элементов высокого порядка в конечных полях, предложенной С. Гао. В статьях [9–11] представлен эффективный алгоритм, который для любого конечного поля малой характеристики находит расширение полиномиально ограниченной степени. Работы [12–14] основаны на алгоритме AKC (тест Агравала – Каяла – Саксены) тестирования простоты чисел.

Основные положения

Если известна факторизация порядка, то имеем эффективный рандомизированный алгоритм для построения примитивного элемента. Можно ли дерандомизировать алгоритм? Этот вопрос

сводится к задаче построения небольшого множества, содержащего примитивный элемент. Естественно, начинаем с небольших чисел. Определение верхней границы наименьшего примитивного элемента является интересной задачей в теории чисел. Предполагая РГР (расширенная гипотеза Римана), Ванг [2] показал, что наименьший примитивный корень в простом конечном поле F_p ограничен $O(\omega^6(p-1)\log^2 p)$, где ω – отображение, передающее положительное целое число числу его различных простых делителей. Можно доказать, что $\omega(n) = O(\log n / \log\log n)$. Шоуп [3] улучшил привязку к $\tilde{O}(\omega^4(p-1)\log^2 p)$. Здесь $\tilde{O}(f(n))$ означает $O(f(n)\log^c f(n))$ для некоторой константы c.

Следовательно, если РГР верна, можно сгенерировать множество, содержащее примитивный элемент, перечислив все числа, меньшие границы Шоупа, которая является полиномиальной в зависимости от размера входных данных. Бах [4] показывает, как при предположении истинности РГР построить множество мощности $O(\log^4 p)$, которое содержит по крайней мере один примитивный элемент. Вместо того чтобы использовать только небольшие числа, это множество состоит из более крупных элементов, которые являются произведением маленьких простых чисел.

Случай с полями малых характеристик кажется более простым. Шоуп [3] и – независимо – Шпарлински [5, теорема 2.4] показывают, что можно детерминистически построить множество размера $(np)^{O(1)}$, которое содержит по крайней мере один примитивный элемент в F_{p^n}.

Шпарлински [6] показал, что в F_q, где q – степень простого числа, примитивный элемент может быть найден с временной сложностью $q^{\frac{1}{4}+\varepsilon}$. Заметим, что наилучший детерминированный алгоритм для вычисления коэффициента N требует времени $N^{\frac{1}{4}+\varepsilon}$.

Материалы и методы

Предположим, что поле задано как $F_q[x]/(f(x))$, где $f(x)$ – неприводимый многочлен над F_q. Пусть $\alpha \equiv x \pmod{f(x)}$. Два разных многочлена могут представлять один и тот же элемент в поле. Например, $x+1$ и $1-x^3$ относятся к одному и тому же классу эквивалентности в $F_3[x]/(x^2+1)$. Тем не менее легко показать следующее.

Предложение 3. Если $f(x)$ и $g(x)$ не равны в $F_q[x]$ и их степени меньше n, то $f(\alpha) \neq g(\alpha)$.

Все построения следуют из вышеизложенной схемы. Целевой элемент β спроектирован таким образом, что мы можем найти множество U большой мощности, состоящее из целых чисел от 1 до $q^n - 1$, которое удовлетворяет следующим условиям:

1. Для любого $i \in U$, элемент β^i имеет простое представление порядка, меньшее n в $F_p[\alpha]$ (обычно мы получаем представление, используя линейность p-й степени);

2. Для любого $i, j \in U$, если $i \neq j$, то $\beta^i \neq \beta^j$. Поскольку степень β имеет представление малого порядка, мы можем перенести элемент в кольцо многочленов $F_q[x]$, где легче доказать различие двух элементов.

Если докажем эти два утверждения, то можно показать, что мощность множества U является нижней границей порядка.

Следуя этой схеме, Гао [7] представил алгоритм полиномиального времени, который для фиксированной простой степени q и целого числа n выводит элемент порядка по меньшей мере

$$n^{\frac{\log_q n}{4\log_q(2\log_q n)}-\frac{1}{2}}. \quad (1)$$

Он не доказал, что алгоритм всегда выводит такой элемент. Но такое предположение допустимо.

Для многочлена $g(x) \in F_q[x]$ определим $g^{(i)}(x)$ как i-кратную композицию функции g. Формально

$$g^{(0)}(x) = x \text{ и } g^{(i)}(x) = g^{(i-1)}(g(x)) \text{ для } i \geq 1.$$

Пусть m – наименьшая степень простого числа q, которая больше или равна n. Метод Гао проверяет, имеет ли $x^m - g(x)$ неприводимый множитель степени n для всех многочленов степени не более $2\log_q n$. Если это так, то он выводит корень такого многочлена, обозначаемого через β. Очевидно, что $F_q[\beta] = F_{q^n}$. Гао предположил, что такой многочлен $g(x)$ существует.

Рассмотрим порядок β. Обозначим степень $g(x)$ через ε. Можно показать, что

$$\beta^m = g(\beta),$$
$$\beta^{m^2} = g(\beta)^m = g(\beta^m) = g^{(2)}(\beta).$$

По индукции $\beta^{m^i} = g^{(i)}(\beta)$. Эта степень β^{m^i} растет со скоростью ε^i. Пусть

$$t = \left\lfloor \frac{\log_q n}{2\log_q \varepsilon} \right\rfloor \text{ и } U = \left\{ \sum_{i=0}^{t-1} a_i m^i \mid 0 \le a_i \le \sqrt{n} \right\}.$$

Для любого $u = \sum_{i=0}^{t-1} a_i m^i \in U$ положим, что $\beta^u = \prod_{i=0}^{t-1} g^{(i)}(\beta)^{a_i}$. Можно проверить, что многочлен $\prod_{i=0}^{t-1} g^{(i)}(x)^{a_i}$ имеет степень меньше n.

Пусть

$$u' = \sum_{i=0}^{t-1} a'_i m^i \in U.$$

Для того чтобы показать, что для любого $u \neq u' \in U$ имеет место $\beta^u \neq \beta^{u'}$, необходимо доказать неравенство

$$\prod_{i=0}^{t-1} g^{(i)}(\alpha)^{a_i} \neq \prod_{i=0}^{t-1} g^{(i)}(\alpha)^{a'_i}.$$

Это сводится к тому, чтобы показать

$$\prod_{i=0}^{t-1} g^{(i)}(x)^{a_i} \neq \prod_{i=0}^{t-1} g^{(i)}(x)^{a'_i}.$$

Это следует из утверждения о мультипликативной независимости $g^{(i)}(x)$, доказанного Гао:

Предложение 4. Предположим, что $f(x) \in F_q[x]$ не является ни одночленным, ни биномиальным вида $ax^{p^l} + b$. Тогда многочлены

$$f^{(1)}(x), f^{(2)}(x), \dots, f^{(n)}(x), \dots$$

являются мультипликативно независимыми, а именно для любых целых чисел $k_1, k_2, \dots, k_n$

$$\left(f^{(1)}(x)\right)^{k_1}\left(f^{(2)}(x)\right)^{k_2}\dots\left(f^{(n)}(x)\right)^{k_n} = 1$$

тогда и только тогда, когда $k_1 = k_2 = \dots = k_n = 0$.

Более тщательно проанализировав построение Гао, Конфлитти [8] показал, что в некоторых случаях нижняя граница для порядка β лучше, чем (1). Поскольку степень $g^{(i)}(x)$ растет экспоненциально с увеличением i, оба результата доказывают лишь незначительно суперполиномиальные нижние границы. Если поле обладает дополнительными структурами, то есть два метода, которые позволяют избежать проблемы и построить элемент порядка, большего, чем q^{n^c}, для константы c. Оба метода работают только в специальных полях.

Основываясь на свойствах периодов Гаусса, фон Цур Гатен и Шпарлински предложили алгоритм, который создает элемент субэкспоненциального порядка в некоторых специальных полях. Предположим, что $r = 2n + 1$ – простое число, не делящее q, а q – примитивный элемент в F_r. Разумеется, $r | q^{2n-1}$. Пусть ξ – примитивный r-й корень из единицы в $F_{q^{2n}}$.

Рассмотрим значение $\beta = \xi + \xi^{-1}$, также известное как период Гаусса типа (n, 2). Легко показать, что $\beta \in F_{q^n}$.

Пусть $h = \lfloor \sqrt{r} \rfloor - 1$,

$$U = \left\{ \sum_{i=1}^{h} a_i q^{s_i} \mid a_i \in \{0,1\} \right\},$$

где s_i – дискретный логарифм i по модулю r, а именно $q_i^s (mod\ r) \equiv i$. Таким образом, $|U| = 2^h$. Для $u = \sum_{i=0}^{h-1} a_i q^{s_i} \in U$, имеем

$$(\xi + \xi^{-1})^u = \prod_{i=1}^{h} \left(\xi^{q^{s_i}} + \xi^{-q^{s_i}}\right)^{a_i} = \prod_{i=1}^{h} (\xi^i + \xi^{-i})^{a_i} =$$

$$= \xi^{\sum_{i=1}^{h}(-a_i)} \prod_{i=1}^{h} (\xi^{2i} + 1)^{a_i}.$$

Пусть

$$u' = \sum_{i=0}^{h-1} a'_i q^{s_i} \in U.$$

Для любых двух $u \neq u' \in U$ докажем, что $\beta^u \neq \beta^{u'}$. Предположим, что

$$\sum_{i=1}^{h} a'_i \geq \sum_{i=1}^{h} a_i.$$

Мы должны доказать, что

$$\xi^{\sum_{i=1}^{h}(a'_i) - \sum_{i=1}^{h}(a_i)} \prod_{i=1}^{h} (\xi^{2i} + 1)^{a_i} - \prod_{i=1}^{h} (\xi^{2i} + 1)^{a'_i} \neq 0\,.$$

Степень многочлена

$$t(x) = x^{\sum_{i=1}^{h}(a'_i) - \sum_{i=1}^{h}(a_i)} \prod_{i=1}^{h} (x^{2i} + 1)^{a_i} - \prod_{i=1}^{h} (x^{2i} + 1)^{a'_i}$$

меньше $r - 1$. Поскольку минимальный многочлен от ξ над F_q имеет степень $r - 1$, необходимо доказать только, что в $F_q[x]$ многочлен $t(x)$ не является нулевым.

Если $\sum_{i=1}^{h} a_i \neq \sum_{i=1}^{h} a'_i$, это очевидно, поскольку $t(0) = -1$.

В противном случае предположим, что $\{i \mid a_i = 1\} \cap \{i \mid a'_i = 1\} = \emptyset$.

Пусть s – наименьшее i такое, что $a_i = 1$ или $a'_i = 1$. Можно проверить, что коэффициент x^s в $t(x)$ не равен нулю. На этом доказательство завершается.

Основываясь на этом аргументе, фон Цур Гатен и Шпарлински [9–11] получили следующие результаты:

Предложение 5. Пусть q – фиксированная простая степень. Для любого натурального числа N целое число $n \geq N$ с $n = O(N \log N)$ и элементом $\alpha \in F_{q^n}$ порядка не менее $2^{(2n)^{1/2}-2}$ может быть вычислено за полиномиальное по N время.

По сути, алгоритм ищет простое число r, большее чем $2N + 1$, такое, что q является примитивным элементом в F_r. Преимущество этого алгоритма в том, что полученный элемент также является нормальным элементом. Убрав это требование, докажем результат с более плотной последовательностью из n.

Предложение 6. Пусть q – фиксированная простая степень. Для любого натурального числа N целое число $n \geq N$ с $n = N + O(N/log^c N)$ и элементом $\alpha \in F_{q^n}$ порядка не менее $2^{10q^{-12}n^{1/2}-25}$ может быть вычислено за полиномиальное по N время.

Степень многочлена в ξ представлении $\xi^i \beta^{q^{s_i}}$ равна $2i$, которая линейно растет с i. Следовательно, они достигают субэкспоненциальной нижней границы $2^{o(\sqrt{n})}$. Далее рассмотрим результаты работы [12], в которой степень многочлена, представляющего β^{q^i}, фиксирована равной 1, и, следовательно, получается нижняя граница $2^{n^{1-\varepsilon}}$.

Результаты и обсуждения

Новый метод в алгоритме тестирования простоты АКС и его последующих улучшениях [13] заключается в использовании многочленов первой степени для генерации большой мультипликативной подгруппы по модулю целого числа и многочлена. Ченг [12] обнаружил связь со специальной задачей об элементах высокого порядка конечного поля и применил эту идею для получения нового решения специальной задачи об элементах высокого порядка конечного поля. Его результат показывает более плотную последовательность из n и гораздо более высокого порядка.

Рассмотрим расширение Куммера F_{q^n}, где $n \mid q-1$. Можно предположить, что $F_{q^n} = F_q[x]/(x^n - b)$, где $x^n - b$ – неприводимый многочлен над F_q. Как обычно, пусть $\alpha \equiv x (mod\ x^n - b)$. Пусть $\beta = \alpha + 1$. Рассмотрим порядок β. Получаем

$$\beta^q = (\alpha+1)^q = \alpha^q + 1 = (\alpha^n)^{\frac{q-1}{n}}\alpha + 1 = b^{\frac{q-1}{n}}\alpha + 1.$$

Обозначим $c = b^{\frac{q-1}{n}}$. Имеем

$$(\alpha+1)^{q^i} = b^{\frac{i(q-1)}{n}}\alpha + 1 = c^i\alpha + 1.$$

Пусть

$$U = \left\{ \sum_{i=1}^{n} a_i q^i \;\middle|\; \sum_{i=1}^{n} |a_i| = n-1, |\{i: a_i < 0\}| = \lfloor 0.292n \rfloor, \sum_{a_i<0} |a_i| = \lceil n/2 \rceil \right\}.$$

Имеем

$$|U| = \binom{n}{d_-}\begin{pmatrix} d & -1 \\ d_- & -1 \end{pmatrix}\begin{pmatrix} 2n-d_- & -d-2 \\ n-d_- & -1 \end{pmatrix} = \Omega(5.8^n).$$

где $d_- = \lfloor 0.292n \rfloor$ и $d = \lceil n/2 \rceil$. Пусть $u = \sum_{i=1}^{n} a_i q^i \in U$, имеем

$$\beta^u = \prod_{i=1}^{n} (c^i\alpha + 1)^{a_i} = \frac{\prod_{1\leq i\leq m, a_i\geq 0}(c^i\alpha+1)^{a_i}}{\prod_{1\leq i\leq m, a_i<0}(c^i\alpha+1)^{-a_i}}.$$

Докажем от противного, что для $u' = \sum_{i=1}^{n} a'_i q^i \in U$, если $u \neq u'$, тогда $\beta^u \neq \beta^{u'}$. Предположим, что эти два элемента равны, имеем

$$\prod_{1\leq i\leq m, a_i\geq 0} (c^i\alpha+1)^{a_i} \prod_{1\leq i\leq m, a'_i<0} (c^i\alpha+1)^{-a'_i} =$$

$$= \prod_{1\leq i\leq m, a_i<0} (c^i\alpha+1)^{-a_i} \prod_{1\leq i\leq m, a'_i\geq 0} (c^i\alpha+1)^{a'_i}.$$

Так как

$$\sum_{1\leq i\leq m, e_i\geq 0} a_i + \sum_{1\leq i\leq m, a'_i<0} (-a'_i) = \sum_{1\leq i\leq m, a_i<0} (-a_i) + \sum_{1\leq i\leq m, a'_i\geq 0} a'_i = m-1$$

получаем

$$\prod_{1\le i\le m, a_i\ge 0}(c^i x+1)^{a_i}\prod_{1\le i\le m, a_i'<0}(c^i x+1)^{-a_i'}=$$
$$=\prod_{1\le i\le m, a_i<0}(c^i x+1)^{-a_i}\prod_{1\le i\le m, a_i'\ge 0}(c^i x+1)^{a_i'}.$$

в кольце $F_q[x]$. Это противоречит единственности факторизации кольца. Использование отрицательных показателей было предложено Волохом [14].

Теперь можно обобщить результаты, вытекающие из приведенных выше рассуждений.

Теорема 2. Пусть q – фиксированная простая степень. Для достаточно большого натурального числа N можно вычислить за полиномиальное по N время целое число $n \in [N, 2qN]$ и элемент $\beta \in F_{q^n}$ с порядком больше $5.8^{n/\log_q n}$.

В этой теореме используем последовательность $q-1$, $2(q^2-1)$, …, $i(q^i-1)$, ... В следующей теореме будем использовать более плотную последовательность 2, 6, 20, …, $p(p-1)$,… где p пробегает все простые числа.

Теорема 3. Пусть q – фиксированная простая степень. Можно вычислить за полиномиальное по N время целое число $n \in [N, N + O(N^{0.77})]$ и элемент

$\beta \in F_{q^n}$ с порядком, большим $5.8^{\sqrt{n}}$.

При $n \geq \log q$ полагается, что β имеет порядок $q^{n/2}$. Эта гипотеза имеет важное значение, что рандомизированное доказательство простоты АКС имеет временную сложность $\tilde{O}(\log^3 p)$, где p – целое число.

Заключение

Поскольку задача с примитивными элементами сложна, в большинстве случаев криптографических приложений конечные поля выбираются таким образом, что известны полные разложения порядков полей на множители, следовательно, существует эффективный рандомизированный алгоритм для построения генераторов для этих полей. Таким образом, в работе мы обобщили результаты, вытекающие из приведенных выше рассуждений, и предложили алгоритмы, которые находят элемент высокого порядка как для общих, так и для специальных конечных полей.

Благодарности

Работа выполнена при поддержке Министерства науки и высшего образования Республики Казахстан в рамках проекта AP19677733 «Разработка интеллектуальной распределенной системы параллельного анализа научных текстов», за что авторы выражают огромную благодарность.

ЛИТЕРАТУРА

1 Prachar K. Primzahlverteilung, Springer, Berlin, 1957, pp. 77, doi: https://doi.org/10.2307/3608911.

2 Wang Y. On the least primitive root of a prime, Acta Math. Sinica, 9, 1959, pp. 432–441. (English translation in Sci. Sinica 10 (1961)).

3 Shoup V. Searching for primitive roots in finite fields, Math. Comp., 58, 1992, pp. 369–380.

4 Bach E. Comments on search procedures for primitive roots, Math. Comp., 66(220), 1997, pp. 1719–1727.

5 Shparlinski I.E. On finding primitive roots in finite fields, Theoret. Comput. Sci., 157, 1997, pp. 273–275.

6 Shparlinski I.E. Finite fields: Theory and computation, Kluwer Academic Publishers, Dordrecht, 1999.
7 Gao S. Elements of provable high orders in finite fields, Proc. Amer. Math. Soc., 127, 1999, pp.1615–1623.
8 Conflitti A. On elements of high order in finite fields, in: Cryptography and Computational Number Theory, Birkhauser, Basel, 2001, pp. 11–14.
9 Von zur Gathen J. and Shparlinski I. Orders of Gauss periods in finite fields, Applicable Algebra in Engineering, Comm. Comput., 9, 1999, pp.15–24.
10 Von zur Gathen J. and Shparlinski I. Constructing elements of large order in finite fields, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes: AAECC-13, Lecture Notes in Computer Science, Springer, Berlin, 1719, 1999, pp. 404–409.
11 Von zur Gathen and Shparlinski I. Gauss periods in finite fields, Proceedings of the Fifth Conference of Finite Fields and their Applications, Springer, Berlin, 1999, P. 162–177.
12 Cheng Q. Constructing finite field extensions with large order elements, ACM-SIAM Symposium on Discrete Algorithms (SODA), 2004, pp. 1123–1124, https://doi.org/10.1137/S0895480104445514.
13 Cheng Q. Primality proving via one round in ECPP and one iteration in AKS, D. Boneh (Ed.), Proceedings of the 23rd Annual International Cryptology Conference (CRYPTO), Lecture Notes in Computer Science, Santa Barbara, Springer, Berlin, 2729, 2003, pp. 338–348.
14 Voloch J.F. On some subgroups of the multiplicative group of finite rings, 2003, http://www.ma.utexas.edu/users/voloch/preprint.html.
15 Shparlinski I.E. On constructing primitive roots in finite fields with advice. IEEE Trans. Inform. Theory, 64, 2018, pp. 7132–7136.
16 Bhowmick A. and Lê T. H. On primitive elements in finite fields of low characteristic, Finite Fields Appl., 35, 2015, pp. 64–77.

[1]*Турусбекова У.К.,
PhD, ORCID ID: 0000-0002-0591-2143, *e-mail: umut.t@mail.ru
[2]Муратбеков М.М.,
PhD, ORCID ID: 0000-0003-2197-4982, e-mail: Madimm@list.ru
[3]Алтынбек С.А.,
PhD, ORCID ID: 0000-0002-8435-7773, e-mail: serik_aa@bk.ru

[1]Esil University, 010000, Астана қ., Қазақстан
[2]Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 010008, Астана қ., Қазақстан
[3]Қазақ технология және бизнес университеті, 010000, Астана қ., Қазақстан

ЖОҒАРЫ РЕТТІ АҚЫРЛЫ ӨРІСТІҢ ПРИМИТИВТІ ЭЛЕМЕНТТЕРІН ІЗДЕУ АЛГОРИТМДЕРІН ЗЕРТТЕУ

Аңдатпа

Ақырлы өрістерді есептеу теориясындағы ең маңызды шешілмеген және күрделі мәселелердің бірі ақырлы өрісте алғашқы түбірлерді құрудың жылдам алгоритмін дайындау. Екінші жағынан, көптеген қосымшалар үшін алғашқы түбірдің орнына жоғары мультипликативті ретті элемент жеткілікті. Мұндай қосымшаларға криптография, кодтау теориясы, псевдокездейсоқ сандар генерациясы және комбинаторлық схемалар кіреді, бірақ олармен шектелмейді. Жоғары ретті элементтердің айқын құрылыстары әдетте дәлелденетін төменгі реттік шекараны қамтамасыз ете алатын комбинаторика әдістеріне сүйенеді, бірақ бұл нақты ретті есептемейді. Оны орындау әдетте ретті факторизациялауды білуді білдіреді. Ең дұрысы, саналы уақыт ішінде кез келген ақырлы өріс үшін примитивті элементті ала алуымыз керек. Алайда егер топтық реттің қарапайым факторизациясы белгісіз болса, мақсатқа қалай жетуге болатыны белгісіз. Осылайша, мүмкіндігінше жоғары ретті элементті құру есебін қоямыз. Бұл мақалада жалпы немесе арнайы ақырлы өрістер үшін жоғары ретті элементті табатын әртүрлі алгоритмдер қарастырылады. Сонымен қатар ұсынылған жұмыс ақырлы өрістердегі Гаусс кезеңдерінің теориясына тағы бір үлес қосады және олардың әртүрлі қосымшалар үшін пайдалы екендігін дәлелдеген жалпылаулары мен аналогтар болады.

Тірек сөздер: ақырлы өріс, примитивті элемент, жай сан, қарапайым факторизация, Гаусс периодтары.

[1]*Turusbekova U.K.,
PhD, ORCID ID: 0000-0002-0591-2143, *e-mail: umut.t@mail.ru
[2]Muratbekov M.M.,
PhD, ORCID ID: 0000-0003-2197-4982, Madimm@list.ru
[3]Altynbek S.A.,
PhD, ORCID ID: 0000-0002-8435-7773, serik_aa@bk.ru

[1]Esil University, 010000, Astana, Kazakhstan
[2]L.N. Gumilyov Eurasian National University, 010008, Astana, Kazakhstan
[3]Kazakh University of Technology and Business, 010000, Astana, Kazakhstan

RESEARCH OF ALGORITHMS FOR SEARCHING PRIMITIVE ELEMENTS OF A FINITE FIELD OF HIGH ORDER

Abstract

One of the most important unsolved and notoriously difficult problems in computational finite field theory is the development of a fast algorithm for constructing primitive roots in a finite field. It is known that for many applications, instead of a primitive root, just an element of high multiplicative order is sufficient. Such applications include, but are not limited to, cryptography, coding theory, pseudorandom number generation, and combinatorial schemes. Explicit constructions of high-order elements usually rely on combinatory methods that can provide a provable lower bound on the order, but this does not compute the exact order. Its execution usually implies knowledge of the factorization of the order. Ideally, we should be able to get a primitive element for any finite field in a reasonable amount of time. However, if the simple factorization of the group order is unknown, it is difficult to achieve the goal. Thus, we set the task of constructing an element, probably of a high order. This article discusses various algorithms that find a high-order element for general or special finite fields. This work also represents another contribution to the theory of Gauss periods over finite fields and their generalizations and analogues, which have already proven their usefulness for a number of different applications.

Key words: finite field, primitive element, prime number, simple factorization, Gauss periods.