DOI: 10.18372/2410-7840.24.16860
УДК 512.624

ФАКТОРИЗАЦИЯ СТЕПЕНИ СФЕНИЧЕСКИХ ПОЛИНОМОВ

Анатолий Белецкий, Арсен Ковальчук

К сфеническим будем относить полиномы, образуемые произведением трёх (не обязательно различных) простых неприводимых полиномов с априори неизвестными степенями. Основная задача исследования состоит в разработке эффективного алгоритма факторизации степени сфенических полиномов, доставляющего минимум вычислительной сложности. Рассмотрены различные варианты решения проблемы факторизации в зависимости от соотношений степени и периода цикла этих полиномов. Период цикла сфенического полинома определён как параметр, равный числу неповторяющихся вычетов, вычисляемых на линейно-логарифмической шкале группы, образуемой полиномом. Предлагаемый алгоритм является инвариантным к характеристикам полей Галуа, порождаемых сомножителями сфенических полиномов. Корректность результатов исследования подтверждается многочисленными числовыми примерами.
Ключевые слова: *неприводимые полиномы, сфенические полиномы, сложность алгоритма факторизации.*

ВВЕДЕНИЕ

Термин *сфенический полином* (пока ещё, пожалуй, не используемый в математике) образован наподобие термина *сфеническое число*. По определению [1] сфеническим является натуральное число, которое можно представить в виде произведения *трёх различных* простых чисел. Сфенические числа *свободны от квадратов* [2], потому что простые множители в разложении числа должны быть разными.

Понятие сфенического полинома (СП) несколько шире понятия сфенического числа.

Определение 1. Сфеническим будем называть полином, который можно представить в виде произведения трёх неприводимых над полем $GF(p)$ полиномов, совсем *не обязательно различных*.

Из предлагаемого определения следует, что в сфенических полиномах одинаковыми могут как два, так и три элемента разложения полинома. Снятие в СП ограничений, характерных для сфенических чисел, расширяет область их возможных приложений. СП принадлежат подмножеству *составных полиномов*.

В данной работе в качестве объекта исследования выступают полиномы f_n степени n от одной переменной над полем Галуа характеристики $p \geq 2$. Для записи полинома будем применять *векторную форму* – совокупностью коэффициентов α_k полинома, полагая

$$f_n = \alpha_n \alpha_{n-1} \ldots \alpha_k \ldots \alpha_1 \alpha_0 .$$

Одним из важнейших вопросов, связанных с полиномами f_n, является вопрос о типе разложения (факторизации) полинома.

Определение 2. Под *типом разложения* составного полинома f_n будем понимать [3] количество k и степени n_i, $i = \overline{1, k}$, неприводимых полиномов $f_{n_1}, f_{n_2}, \ldots, f_{n_k}$ (возможно повторяющихся), произведение которых над $GF(p)$ образует заданный полином f_n степени $n = \sum_{i=1}^{k} n_i$.

В теории чисел натуральное число называется *k-почти простым*, если оно имеет k простых множителей [4]. Аналогично полином f_n назовём k-почти простым, если он образован произведением k простых (неприводимых) полиномов, причем их перемножение, восстанавливающее f_n, осуществляется над полем $GF(p)$. Для k-почти простых полиномов степени n введём обозначение $f_n^{[k]}$. Таким образом, полином f_n является простым тогда и только тогда, когда он

1-почти простой, и *полупростым* [5], когда он 2-почти простой. Проблема факторизации полупростых полиномов $f_n^{[2]}$ подробно рассмотрена в [6].

Основная задача данной статьи состоит в разработке эффективных алгоритмов разложения степени n сфенических полиномов $f_n^{[3]}$ от одной переменной над полями Галуа произвольных характеристик p. К эффективным будем относить алгоритмы факторизации степени полиномов $f_n^{[3]}$, обеспечивающие минимум сложности вычислений.

К числу возможных приложений результатов исследований можно отнести теорию факторизации целых чисел [7], в том числе факторизацию с помощью полиномов [8], криптографию [9], алгебраическую теорию модулярных вычислений [10, 11] и пр.

1. МАТЕМАТИЧЕСКИЕ ОСНОВЫ

Пусть $f_n^{[3]}$ – полином, образованный произведением над $GF(p)$ трёх, совсем не обязательно различных, неприводимых полиномов (НП) с априори неизвестными степенями x, y и z такими, что

$$f_n^{[3]} = f_x \overset{p}{\otimes} f_y \overset{p}{\otimes} f_z . \qquad (1)$$

Тем самым решаемая задача сводится к определению степеней НП, совместно порождающих сфенический полином $f_n^{[3]}$. Математическую основу факторизации степени полиномов $f_n^{[3]}$ составляют результаты, полученные ранее в [6, 12], краткое изложение которых (с учётом специфики СП) приводится ниже.

В классическом варианте для определения трёх неизвестных переменных x, y и z необходимо составить систему трёх уравнений, каждое из которых функционально зависит от этих переменных. В качестве первого уравнения, в соответствии с (1), примем

$$x + y + z = n . \qquad (2)$$

Второе уравнение может быть получено на основании параметра, введенного в работах [6, 12], и названного *периодом цикла* (Cord – cycle order) составного полинома $f_n^{[k]}$. Приведём определение этого параметра.

Определение 3. Периодом цикла $\mathrm{Cord}(f_n^{[k]})$ произвольного k-почти простого полинома будем называть число неповторяющихся вычетов S, вычисляемых на *линейно-логарифмической шкале группы*, порождаемой полиномом $f_n^{[k]}$.

Перейдём к пояснению термина «линейно-логарифмическая шкала группы». С этой целью нам потребуется привлечь дополнительно ещё два параметра: порядок НП f_n, который обозначается $\mathrm{ord}(f_n)$, и порядок составного полинома – $\mathrm{ord}(f_n^{[k]})$. Согласно теореме 6.11, [8], порядок полинома $f_n^{[k]}$ определяется выражением

$$\mathrm{ord}(f_n^{[k]}) = \mathrm{HOK}(\mathrm{ord}(f_{x1}), \mathrm{ord}(f_{x2}), \ldots, \mathrm{ord}(f_{xl}), \ldots, \mathrm{ord}(f_{xk})), \quad n = \sum_{i=1}^{k} x_i \qquad (3)$$

В (3) обозначения несколько отличаются от принятых в оригинале, но эквивалентны им.

Порядок P_{pr} примитивного над $GF(p)$ полинома f_n вычисляется по формуле $P_{pr} = \mathrm{ord}(f_n) = p^n - 1$. Если f_n не является примитивным, то его порядок P_{ir} принадлежит подмножеству нетривиальных делителей P_{pr}. В условиях априорной неопределённости относительно параметров x, y и z возможно единственным вариантом оценки $\mathrm{ord}(f_n^{[3]})$ является последовательное возведение в степень образующего элемента θ, называемого генератором мультипликативной группы $GF^*(p^n)$, порождаемой полиномом $f_n^{[3]}$. К наиболее простому способу вычисления порядка СП $f_n^{[3]}$ приходим в том случае, когда в качестве генератора группы выбран элемент $\theta = 10$. При этом вне зависимости от характеристики p поля $GF(p^n)$ формирование очередного элемента g_{k+1} группы $GF^*(p^n)$ сводится к сдвигу на один разряд влево предыдущего элемента g_k с последующим приведением g_{k+1} (при необходимости) к остатку по модулю $f_n^{[3]}$.

Совершенно очевидно, что даже при небольших значениях параметров x, y и z, не превышающих нескольких десятков, оценка порядков СП $f_n^{[3]}$ наталкивается на возможно непреодолимые препятствия, связанные с необходимостью выполнения вычислений огромного объёма. Для преодоления «кошмара больших чисел» воспользуемся методом замены «линейной шкалы» при определении $\mathrm{ord}(f_n^{[3]})$ на «линейно-логарифмическую шкалу». Суть метода состоит в следующем.

Перефразируем классическую лемму 2.3 [13], не меняя её смысла, таким образом.

Лемма 1. Для каждого ненулевого элемента $\alpha > 1$ поля $GF(p^n)$, порождаемого НП f_n, соблюдается равенство $\alpha^{p^n-1} (\mathrm{mod}\, f_n) = 1$.

Из леммы 1 вытекает

Следствие 1. Произвольные неприводимые над полем $GF(p)$ полиномы f_n (как примитивные, так и простые, т.е. не являющиеся примитивными) поддерживают сравнение

$$1(0)^{[p^n-1]} \equiv 1 (\mathrm{mod}\, f_n), \qquad (4)$$

где $(a)^{[m]} = \underbrace{aa\ldots aa}_{m \text{ раз}}$.

Сравнение (4) выполняется в том и только в том случае, если $f_n -$ НП. Соотношение (4) удобно использовать в качестве одного из критериев неприводимости тестируемых полиномов. Критерий неприводимости (4) необходимый, но недля всех степеней n полиномов f_n достаточный [12].

Числа в некоторой позиционной системе счисления, которые записываются как единица с последующими нулями, как в (4), называются *круглыми числами* [14].

Сформулируем далее две важнейшие формальные спецификации [6].

Определение 4. Последовательность натуральных чисел $k = 0, 1, 2, ..., p^n - 1$, являющихся показателями степени образующего элемента θ мультипликативной группы максимального порядка (МПГМП):

$$GF^*(p^n) = \left\{\theta^0, \theta^1, \ldots, \theta^k, ..., \theta^{p^n-1}\right\} (\mathrm{mod}\, f_n),$$

назовём *линейной шкалой* группы.

Определение 5. Последовательность натуральных чисел $r = 1, 2, ..., n$, являющихся показателями степени характеристики p группы $GF^*(p^n)$ в элементе $t_{r,p} = p^r - 1$, назовём *логарифмической шкалой* группы.

Сведём числовые параметры r и $t_{r,2}$ в табл. 1.

Таблица 1

Вспомогательные параметры МПГМП над $GF(2)$

r	1	2	3	4	5	6	7	8	…
$t_{r,2}$	1	3	7	15	31	63	127	255	…

«Завяжем» параметры из табл. 1 с характеристиками так называемой *реперной лестницы* (рис. 1), состоящей из совокупности параллельных прямых линий (*ступенек лестницы*).

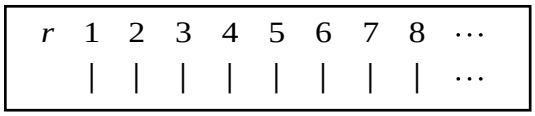

Рис. 1. Реперная лестница

В табл. 1 приняты такие обозначения: r – номер ступеньки реперной лестницы; $t_{r,2}$ – степень двоичного полинома CV_r, назовём его *координатным вектором* (Coordinate Vector), левый разряд которого равен 1, а остальные заполнены нулями, т.е.

$$CV_r = \underset{t_{r,2}}{100...0}. \qquad (5)$$

Термин «координатный вектор» в (5) есть ничто иное, как упоминавшийся выше термин «круглое число». Однако здесь и далее мы будем именовать его «координатным вектором», полагая такое название более подходящим по контексту.

Метки $t_{r,2}$, будучи равномерно расставленными по индексу r на некоторой оси, как раз и образуют упомянутую выше «линейно-логарифмическую шкалу группы». Параметр $t_{r,2}$ представляет собой *порядок* (длину) нулевого вектора полинома CV_r, число нулевых разрядов которого определяется формулой $t_{r,2} = 2^r - 1$.

Представим реперную лестницу (рис. 1), соответствующую полиному f_n, в виде вектора $1^{[n]} = \underbrace{11\ldots1}_{n \text{ бит}}$. Каждая $r-$я единица в $1^{[n]}$ символизирует координатный вектор CV_r, вычисляемый на $r-$й ступеньке реперной лестницы. Закон изменения порядка $t_{r,2}$ нулевых разрядов двоичного вектора CV_r можно легко установить, анализируя данные нижней строки табл. 1. А именно

$$t_{r,2} = 2 \cdot t_{r-1,2} + 1, \quad t_0 = 0, \quad r = \overline{1,n}. \tag{6}$$

Пусть $\boldsymbol{S}_r = Res(CV_r)_{f_n}$ означает вычет координатного вектора CV_r по модулю полинома f_n. Соотношение (6) составляет *фундаментальную основу* алгоритма факторизации полупростых полиномов [6], который сводится к последовательности простых рекуррентных вычислений

$$\boldsymbol{S}_r = Res(\boldsymbol{S}_{r-1} \cdot s_k)_{f_n}, \; s_r = \boldsymbol{S}_{r-1}0,$$

$$\boldsymbol{S}_0 = 1, \; r = \overline{1,n},$$

или иначе (для полиномов f_n над полем $GF(2)$)

$$\boldsymbol{S}_r = Res(\boldsymbol{S}_{r-1}^2 0)_{f_n}, \; \boldsymbol{S}_0 = 1, \; r = \overline{1,n}. \tag{7}$$

При достижении индексом r последней $n-$й ступеньки реперной лестницы если окажется, что $\boldsymbol{S}_n = 1$, то это будет означать выполнение условий сравнения (4). Последовательность вычетов $\boldsymbol{S}_r$ на ступеньках реперной сетки, формируемых произвольным полиномом f_n, будем называть *последовательностью $\boldsymbol{S}-$вычетов*.

Для пояснения введенного ранее понятия «период цикла полинома» обратимся к числовым примерам. С этой целью сопоставим последовательности $\boldsymbol{S}-$вычетов, образуемых двумя полиномами, принадлежащими разным подклассам. В качестве первого полинома выберем двоичный ПрП шестой степени $f_6^{(1)} = 1000011$, а второго – ПНП $f_6^{(2)} = 1001001$. Выполнив расчёты по формуле (7), получим:

Таблица 2

Последовательность $\boldsymbol{S}-$вычетов, порождаемая ПрП $f_6^{(1)}$

$\boldsymbol{S}_1 = 10;$	$\boldsymbol{S}_4 = 101000;$
$\boldsymbol{S}_2 = 1000;$	$\boldsymbol{S}_5 = 100101;$
$\boldsymbol{S}_3 = 110;$	$\boldsymbol{S}_6 = \boldsymbol{1}.$

Таблица 3

Последовательность $\boldsymbol{S}-$вычетов, порождаемая ПНП $f_6^{(2)}$

$\boldsymbol{S}_1 = 10;$	$\boldsymbol{S}_4 = 1001;$
$\boldsymbol{S}_2 = 1000;$	$\boldsymbol{S}_5 = 10000;$
$\boldsymbol{S}_3 = 10010;$	$\boldsymbol{S}_6 = \boldsymbol{1}.$

Как следует из табл. 2 и 3 *периоды циклов* полиномов $f_6^{(1)}$ и $f_6^{(2)}$ совпадают со степенью НП, т.е. $\mathrm{Cord}(f_6^{(1)}) = \mathrm{Cord}(f_6^{(2)}) = 6$, тогда как $\mathrm{ord}(f_6^{(1)}) = 63$ и $\mathrm{ord}(f_6^{(2)}) = 9$ различны и определяют *порядки* этих же полиномов.

А теперь обратимся к НП над полями $GF(p)$, $p > 2$. Составим табл. 4, подобную табл. 1, но для характеристики $p = 3$.

Таблица 4

Вспомогательные параметры МПГМП для варианта $GF(3)$

r	1	2	3	4	5	6	7	8	…
$t_{r,3}$	1	8	26	80	242	728	2186	65600	…

Из сопоставления данных табл. 1 и 4, приходим к таким обобщённым соотношениям для степени $t_{r,p}$ и вычета $\boldsymbol{S}_{r,p}$ координатного вектора CV_r

$$t_{r,p} = p \cdot t_{r-1,p} + (p-1), \quad t_{0,p} = 0,$$

$$r = \overline{1,n};$$

$$\boldsymbol{S}_{r,p} = Res(\boldsymbol{S}_{r-1,p}^{\,p} \underbrace{0\ldots0}_{p-1})_{f_n}, \; \boldsymbol{S}_{0,p} = 1, \; r = \overline{1,n}. \tag{8}$$

Таблица 5

Последовательность S – вычетов, порождаемая ПНП $f_6^{(3)}$

$S_1 = 10000;$	$S_4 = 414114;$
$S_2 = 40240;$	$S_5 = 130222;$
$S_3 = 302403;$	$S_6 = \mathbf{1}.$

Как и в предыдущих вариантах НП $f_6^{(1)}$ и $f_6^{(2)}$ для полинома $f_6^{(3)}$ имеем $\mathrm{Cord}(f_6^{(3)}) = 6$, тогда как $\mathrm{ord}(f_6^{(3)}) = 3906$, значение которого получено по результатам компьютерных расчётов.

На основании рассмотренных примеров может быть сформулирована

Аксиома 1. Период цикла как простых, так и примитивных полиномов f_n над полем $GF(p)$ инвариантен к характеристике поля и совпадает со степенью полинома, то есть $\mathrm{Cord}(f_n) = n$.

Аксиома 1 даёт возможность без потери общности в последующих числовых вычислениях ограничиваться рассмотрением лишь полиномов над полями $GF(2)$.

2. АЛГОРИТМ ФАКТОРИЗАЦИИ СФЕНИЧЕСКИХ ПОЛИНОМОВ

Выражение для *периода цикла* составных полиномов $\mathrm{Cord}(f_n^{[k]})$ подобно (3), которым определяется *порядок* $\mathrm{ord}(f_n^{[k]})$ этих же полиномов. В частности, для сфенических полиномов:

$$\mathrm{Cord}(f_n^{[3]}) = \mathrm{НОК}(\mathrm{Cord}(f_x), \mathrm{Cord}(f_y), \mathrm{Cord}(f_z)). \quad (9)$$

Объединяя формулы (2) и (9), с учётом аксиомы 1, приходим для СП к системе двух уравнений относительно трёх неизвестных:

$$\begin{aligned} x + y + z &= n, \\ \mathrm{НОК}(x, y, z) &= C, \end{aligned} \quad (10)$$

где для краткости обозначено $C = \mathrm{Cord}(f_n^{[3]})$.

Уравнения (10) образуют несовместимую систему, которая, на первый взгляд, представляется априори неразрешимой. Но всё не так плохо, как кажется. Проблема становится преодолимой, если привлечь для её решения как отношение между параметрами n и C, так и подмножество нетривиальных делителей (НТД) периода цикла C СП $f_n^{[3]}$.

В самом деле, если, например, окажется, что $C = n/3$, то это будет означать, что всё три полинома, образующие СП, являются полиномами степени $n/3$. С другой стороны, если C равен квадрату натурального числа, то решение системы уравнений (10) таково: $x = \sqrt{C}$; $z = C$; $y = n - (x + z)$. Полный набор решений системы (10) представлен структурно-логической схемой на рис. 2.

Переходим к анализу способов преодоления несовместимости системы уравнений (10). Обратим внимание на следующий факт. Предположим, что двоичный СП образован произведением над $GF(2)$ трёх неприводимых полиномов, априори неизвестные степени которых $x = 3$, $y = 4$ и $z = 6$.

Период цикла C такого СП определяется выражением $C = \mathrm{НОК}(x, y, z) = \mathrm{НОК}(3, 4, 6) = 12$. Выпишем совокупность НТД C, равную $\{2, 3, 4, 6\}$. Из данного примера следует, что все неизвестные степени полинома $f_n^{[3]}$ содержатся в подмножестве C нетривиальных делителей периода цикла полинома. Отмеченная взаимосвязь между степенями сомножителей СП и НТД периодов циклов $f_n^{[3]}$ совсем не обязательно в полном объеме соблюдается для всех сфенических полиномов и их периодов циклов.

И тем не менее, она оказывается весьма полезной при решении задачи факторизации степеней в общем случае k – почти простых полиномов.

Обратимся к упоминавшемуся ранее примеру, которым предполагается, что все три компоненты СП являются полиномами степени $n/3$.

При этом возможны такие варианты для совокупности НП f_x, f_y и f_z. В первом варианте будем полагать, что все полиномы различны.

Пусть $f_x = 1010111$, $f_y = 1100111$ и $f_z = 1101101$, которым отвечает сфенический полином $f_{18}^{[3]} = 1001110000101011001$. В соответствии с (7) получим:

Таблица 6

Последовательность $\boldsymbol{S}-$вычетов, порождаемая первым вариантом СП $f_{18}^{[3]}$

$\boldsymbol{S}_1=10;$	$\boldsymbol{S}_4=1000000000000000;$
$\boldsymbol{S}_2=1000;$	$\boldsymbol{S}_5=11111010101001010;$
$\boldsymbol{S}_3=10000000;$	$\boldsymbol{S}_6=\mathbf{1}.$

Пусть $\boldsymbol{Sk}-$старший вычет последовательности (в таблицах выделен жирным шрифтом). Если $\boldsymbol{Sk}=1$, то это означает, что все компоненты СП различны и совсем не обязательно должны иметь одинаковые степени (как в табл. 6).

Подкрепим данный вывод примером. Пусть $f_x=111,\ f_y=1101$ и $f_z=10011.$

Тогда $f_9^{[3]}=1001010101,\ C=12$, а $\boldsymbol{S}-$вычеты сведены в табл. 7.

Во втором варианте будем считать, что два их трёх НП являются одинаковыми.

Пусть $f_x=f_y=1100111$ и $f_z=1101101$, т.е. $C=6,\ f_{18}^{[3]}=1110110001100001001.$

Таблица 7

Последовательность $\boldsymbol{S}-$вычетов, порождаемая СП $f_9^{[3]}=1001010101$

$\boldsymbol{S}_1=10;$	$\boldsymbol{S}_7=110010110;$
$\boldsymbol{S}_2=1000;$	$\boldsymbol{S}_8=110011100;$
$\boldsymbol{S}_3=10000000;$	$\boldsymbol{S}_9=100010100;$
$\boldsymbol{S}_4=100010111;$	$\boldsymbol{S}_{10}=10000011;$
$\boldsymbol{S}_5=10001001;$	$\boldsymbol{S}_{11}=100011101;$
$\boldsymbol{S}_6=110010101;$	$\boldsymbol{S}_{12}=\mathbf{1}.$

Тогда имеем:

Таблица 8

Последовательность $\boldsymbol{S}-$вычетов, порождаемая вторым вариантом СП $f_{18}^{[3]}$

$\boldsymbol{S}_1=10;$	$\boldsymbol{S}_5=100101100011011100;$
$\boldsymbol{S}_2=1000;$	$\boldsymbol{S}_6=10110100111010010;$
$\boldsymbol{S}_3=10000000;$	$\boldsymbol{S}_7=\mathbf{10}.$
$\boldsymbol{S}_4=1000000000000000;$	

К подобному результату (по значению $\boldsymbol{Sk}$) приходим и в том случае, когда степень полинома f_z отлична от степени полиномов $f_x,\ f_y$.

В самом деле, пусть $f_x=f_y=1011$ и $f_z=11001.$ Тогда $f_{10}^{[3]}=11000111101,$ $C=12$, а последовательность $\boldsymbol{S}-$вычетов представлена в табл. 9. Обратим внимание на то, что последовательности $\boldsymbol{S}-$вычетов в табл. 8 и 9 заканчиваются значением $\boldsymbol{Sk}=10$.

Таблица 9

Последовательность $\boldsymbol{S}-$вычетов, порождаемая СП $f_{10}^{[3]}=11000111101$

$\boldsymbol{S}_1=10;$	$\boldsymbol{S}_7=1100111110;$
$\boldsymbol{S}_2=1000;$	$\boldsymbol{S}_8=101011001;$
$\boldsymbol{S}_3=10000000;$	$\boldsymbol{S}_9=1110111100;$
$\boldsymbol{S}_4=100010110;$	$\boldsymbol{S}_{10}=1000111;$
$\boldsymbol{S}_5=1001101;$	$\boldsymbol{S}_{11}=1101110001;$
$\boldsymbol{S}_6=1111111001;$	$\boldsymbol{S}_{12}=1010101000;$
	$\boldsymbol{S}_{13}=\mathbf{10}.$

И, наконец, третьим вариантом предполагается, что все три сомножителя СП одинаковы. Пусть $f_x=f_y=f_z=1101101$. Следовательно, СП $f_{18}^{[3]}=1110111100111111101$ и $C=6$, а последовательность $\boldsymbol{S}-$вычетов показана в табл. 10.

Таблица 10

Последовательность $\boldsymbol{S}-$вычетов, порождаемая третьим вариантом СП $f_{18}^{[3]}$

$\boldsymbol{S}_1=10;$	$\boldsymbol{S}_5=1110111100111110110;$
$\boldsymbol{S}_2=1000;$	$\boldsymbol{S}_6=1110111100011111110;$
$\boldsymbol{S}_3=10000000;$	$\boldsymbol{S}_7=1100111100111111110;$
$\boldsymbol{S}_4=1000000000000000;$	$\boldsymbol{S}_8=\mathbf{1000}.$

Таким образом, согласно данным табл. 6-10, значение старшего вычета $\boldsymbol{Sk}$ может играть роль *индикатора качества* состава компонент СП. А именно, если $\boldsymbol{Sk}=1$, то это означает, что все сомножители сфенического полинома различны, если $\boldsymbol{Sk}=10$, то это означает, что два из трёх сомножителей СП одинаковые и, наконец, если $\boldsymbol{Sk}=1000$, то это означает, что одинаковыми являются все три сомножителя СП.

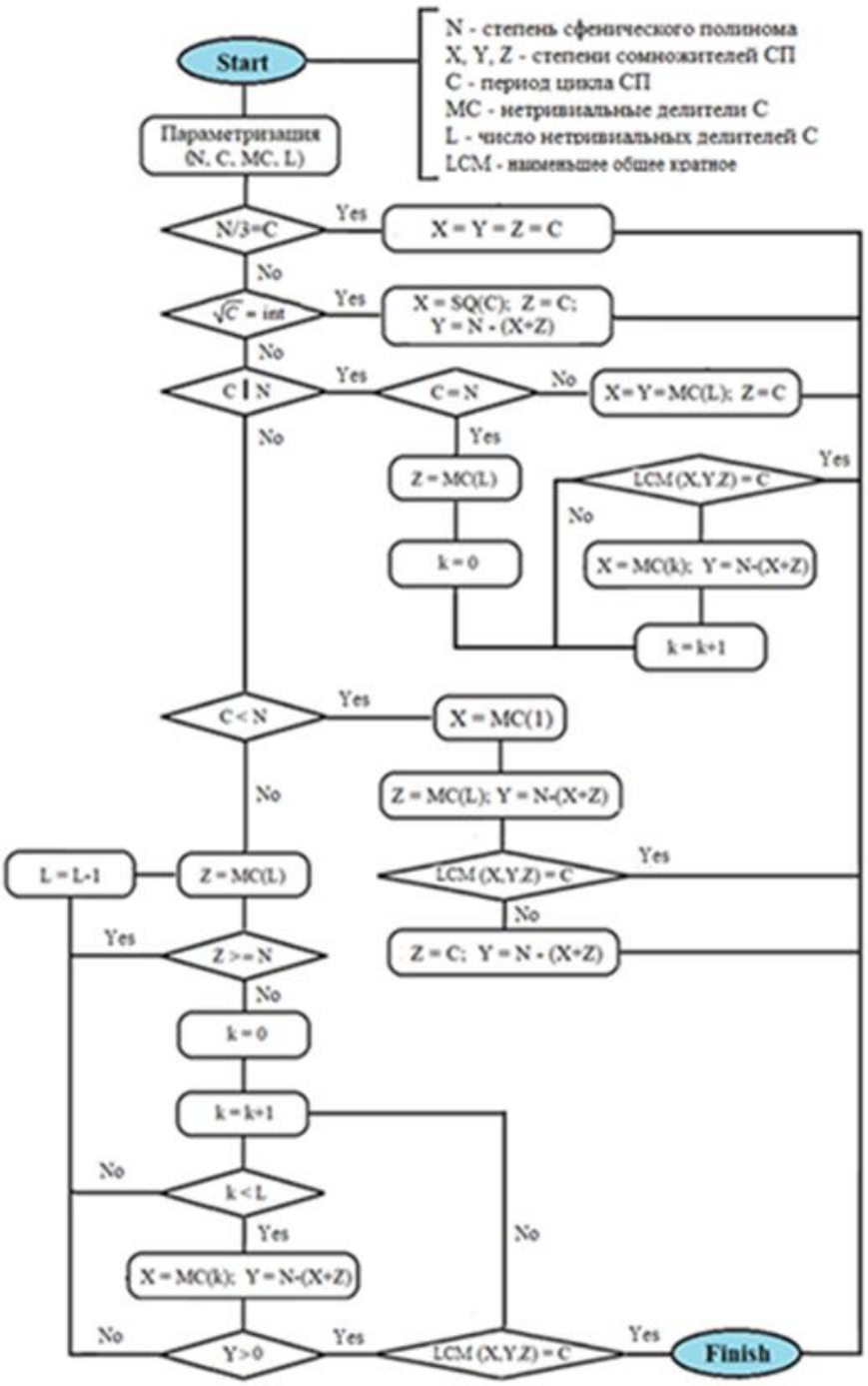

Рис. 2 Блок-схема алгоритма факторизации степени сфенических полиномов

Рассмотрим ситуацию, при которой $\sqrt{C}$ является целым числом. Такое условие, накладываемое на период цикла СП, дает возможность определить минимальную $x=\sqrt{C}$ и максимальную $z=C$ степени сомножителей f_x и f_z. Для степени y остается возможность выбора одного из альтернативных решений, которыми являются $y=x$ или $y=z$. Оба этих значения y сохраняют C. Рассмотрим пример. Пусть $x=y=3$ и $z=9$, то есть $n=15$ и $C=9$.

Выберем такими сомножители СП: $f_x=f_y=1011$, $f_z=1010110111$ и, тем самым, получим $f_{15}^{[3]}=1010010110101011$. Приходим к последовательности $\boldsymbol{S}$ – вычетов, представленную в табл. 11.

Поскольку $n=16$, $C=8$ и $MC=\{2,4\}$, $L=2$, то $x=y=MC(2)=4$, а $z=C=8$. Так как $\boldsymbol{S}k=10$, то это означает, что полиномы f_x и f_y одинаковые.

Таблица 11

Последовательность $\boldsymbol{S}-$вычетов, порождаемая $f_{15}^{[3]}=1010010110101011$

$\boldsymbol{S}_1=10;$	$\boldsymbol{S}_6=101010101011110;$
$\boldsymbol{S}_2=1000;$	$\boldsymbol{S}_7=110010101100101;$
$\boldsymbol{S}_3=10000000;$	$\boldsymbol{S}_8=110001111011000;$
$\boldsymbol{S}_4=10010110101011;$	$\boldsymbol{S}_9=110110101000111;$
$\boldsymbol{S}_5=1101110000101;$	$\boldsymbol{S}_{10}=\boldsymbol{10}.$

Естественно, если полиномы f_x и f_y разные, но их степени одинаковые, то в последовательности $\boldsymbol{S}-$вычетов параметр $\boldsymbol{S}k=1$.

А теперь обратимся к анализу алгоритма разложения степени n СП на множители при условии, что период цикла C полинома $f_n^{[3]}$ такой, что $C\,|\,n$. К наиболее простому решению приходим, когда $C\neq n$. В этом случае эмпирически установлено, что $C=n/2$, причём $x=y=MC(L)$, $z=C$, где *MC* и L – подмножество и число НТД периода цикла C. Рассмотрим пример. Пусть $f_{16}^{[3]}=10001100001101001$. Составим (табл. 12) последовательность $\boldsymbol{S}-$вычетов

Таблица 12

Последовательность $\boldsymbol{S}-$вычетов, порождаемая СП $f_{16}^{[3]}=10001100001101001$

$\boldsymbol{S}_1=10;$	$\boldsymbol{S}_5=11010111100011;$
$\boldsymbol{S}_2=1000;$	$\boldsymbol{S}_6=110100111000000;$
$\boldsymbol{S}_3=10000000;$	$\boldsymbol{S}_7=111110000001001;$
$\boldsymbol{S}_4=1000000000000000;$	$\boldsymbol{S}_8=1010000010100000$
	$\boldsymbol{S}_9=\boldsymbol{10}.$

В качестве таковых для рассмотренного примера были выбраны полиномы $f_x=f_y$ четвёртой степени 10011, а f_z – НП восьмой степени 100011101. Если бы полиномы f_x и f_y были разными, например такими $f_x=10011$ и $f_y=11001$, которые совместно с f_z формируют СП $f_{16}^{[3]}=11010101000111111$, то старшим в последовательности (см. табл. 13) становится вычет $\boldsymbol{S}_8=\boldsymbol{S}k=1$.

Таблица 13

Последовательность $\boldsymbol{S}-$вычетов, порождаемая СП $f_{16}^{[3]}=11010101000111111$

$\boldsymbol{S}_1=10;$	$\boldsymbol{S}_5=100100100100110;$
$\boldsymbol{S}_2=1000;$	$\boldsymbol{S}_6=1011010110100100;$
$\boldsymbol{S}_3=10000000;$	$\boldsymbol{S}_7=111110000001001;$
$\boldsymbol{S}_4=1000000000000000;$	$\boldsymbol{S}_8=\boldsymbol{1}.$

На этом завершим анализ алгоритмов факторизации степени сфенических полиномов, полагая, что структурно-логическая схема, представленная на рис. 2, в полной мере содержит все необходимые сведения, поясняющие технологию факторизации.

Естественным направлением дальнейших исследований является обобщение полученных результатов с целью решения проблемы факторизации степени $k-$почти простых полиномов, порядок k которых превышает 3.

ВЫВОДЫ

Основным результатом исследования является разработка эффективного алгоритма факторизации степени n сфенических полиномов $f_n^{[3]}$, образуемых произведением трёх неприводимых полиномов над полем Галуа произвольной характеристики. Из трёх уравнений, функционально зависящих от неизвестных степеней сомножителей сфенических полиномов, в явной форме удается представить только два уравнения. Одно из них тривиальное и сводится к тому, что сумма неизвестных степеней сомножителей полинома $f_n^{[3]}$ равна априори заданной степени n этого полинома. Второе уравнение опирается на вычисляемый на основании $f_n^{[3]}$ параметр, названный периодом цикла C сфенического полинома, равный наименьшему общему кратному степеней сомножителей $f_n^{[3]}$. Преодоление проблемы несовместимости системы двух уравнений относительно трёх неизвестных осуществляется благодаря тому, что вычисляемые степени сомножителей сфенических полиномов или совпадают с нетривиальными делителями C, или функционально связаны с ними.

Рассмотрены различные варианты решения проблемы факторизации степеней сфенических полиномов в зависимости от соотношений параметров n и C этих полиномов.

Сокращение объёма вычислений достигается за счёт перехода от линейной шкалы при определении периода цикла C полинома $f_n^{[3]}$ к логарифмической. Предлагаемый алгоритм факторизации является инвариантным к характеристике поля, порождаемого сомножителями сфенического полинома.

ЛИТЕРАТУРА

[1] Сфеническое число. Wikipedia [online], Available at: https://dic.academic.ru/dic.nsf/ ruwiki/1644009.

[2] Сфеническое число. Wikipedia [online], Available at: https://wikisko.ru/wiki/Sphenic_number.

[3] Шпаринский И.Е. О некоторых вопросах теории конечных полей, УМН, 46:1(277) (1991). — С. 165-200. Wikipedia [online], Available at: www.mathnet.ru/links/c42de5a12c7ae9608284aece3963a1fa/rm4570.pdf.

[4] Gerald Tenenbaum. Introduction to Analytic and Probabilistic Number Theory. Cambridge University Press, (2004). ISBN 978-0-521-41261-2

[5] Полупростое число. Wikipedia [online], Available at: https://wiki5.ru/wiki/Semiprime.

[6] Anatoly Beletsky. Factorization of the Degree of Semisimple Polynomials of one Variable over the Galois Fields of Arbitrary Characteristics. *WSEAS Transactions on Mathematics*. Vol. 21, 2022, Art. 23, p.p. 160-172. DOI: 10.37394/23206.2022.21.23.

[7] Ишмухаметов Ш.Т. Методы факторизации натуральных чисел. – Казань: Казанский ун-т. 2011. – 190 с.

[8] Bach E., Shallit J. Factoring with cyclotomic polynomials. – Math. Comp. 1989. v.52(185), p. 201–219.

[9] Schneier B., Applied cryptography, Second Edition: Protocols, Algorithms, and Source Code in C+. John Wiley & Sons, New York (1996).

[10] Chervyakov N.I., Kolyada A.A., Lyakhov P.A. Modular arithmetic and its applications in Infocommunication technologies. – M.: Fizmatlit, 2017. – 400 p.

[11] Henri Cohen. A course in computational algebraic number theory. Berlin, Springer, 1996. – 545 p.

[12] Anatoly Beletsky. An Effective Algorithm for the Synthesis of Irreducible Polynomials over a Galois Fields of Arbitrary Characteristics. *WSEAS Transactions on Mathematics*. VOL 20, 2021. – pp. 508-519. DOI: 10.37394/23206.2021.20.54.

[13] Lidl R., Niederreiter H. Finite Fields. Cambridge University Press (1996).

[14] Круглые числа. Wikipedia [online], Available at: https://dic.academic.ru/dic.nsf/ruwiki/ 180635.

ФАКТОРИЗАЦІЯ СТУПЕНЯ СФЕНІЧНИХ ПОЛІНОМІВ

До сфенічних будемо відносити поліноми, що утворені добутком трьох (не обов'язково різних) простих поліномів з апріорі невідомими ступенями. Основне завдання дослідження полягає у розробці ефективного алгоритму факторизації ступеня сфенічних поліномів, що забезпечує мінімум обчислювальної складності. Розглянуто різні варіанти вирішення проблеми факторизації залежно від співвідношень ступеня та періоду циклу цих поліномів. Період циклу сфенічного полінома визначений як параметр, якій дорівнює числу відрахувань, що не повторюються, та обчислений на лінійно-логарифмічній шкалі групи відрахувань за модулем сфенічного поліному. Пропонований алгоритм інваріантний до характеристик полів Галуа, що породжуються співмножниками сфенічних поліномів. Коректність результатів дослідження підтверджується численними прикладами.

Ключові слова: незвідні поліноми, сфенічні поліноми, складність алгоритму факторизації.

FACTORIZATION OF THE DEGREE OF SPHENIC POLYNOMES

By sphenic polynomials, we mean polynomials formed by the product of three (not necessarily different) irreducible polynomials with a priori unknown degree. The study's main goal is to develop an effective algorithm for factorizing degrees of sphenic polynomials with minimal computational complexity. Different solutions to the problem of factorization degrees of sphenic polynomials depending on the ratio degree of the cycle period of these polynomials consider. The sphenic polynomial cycle period defines as a parameter equal to the number of non-repeating subtractions computed on
the linear-logarithmic scale of the group formed by the sphenic polynomial. The proposed algorithm is invariant to the characteristics of the Galois fields generated by the multipliers of sphenic polynomials. Numerous numerical examples confirm the correctness of the results. Directions for further research outlines.

Key words*:* irreducible polynomials, sphenic polynomials, modulo comparability.

Білецький Анатолій Якович, доктор технічних наук, професор, заслужений діяч науки і техніки України, лауреат Державної премії України в галузі науки і техніки, професор кафедри електроніки, робототехніки та технологій моніторингу и Інтернету речей Національного авіаційного університету.