УДК 512.624.2

ПЕРВООБРАЗНЫЕ МНОГОЧЛЕНЫ НАД КОНЕЧНЫМИ ПОЛЯМИ

Д. Ф. Базылев
заведующий кафедрой геометрии, топологии и методики преподавания математики механико-математического факультета, кандидат физико-математических наук
Белорусский государственный университет

В работе рассматривается обобщение для многочленов над конечными полями понятия первообразного корня в модулярной арифметике. Получены условия, которые обеспечивают существование или отсутствие первообразных многочленов. Ряд свойств сохраняется в сравнении со свойствами первообразных корней. Но имеются также и существенные отличия, которые приведены в статье. Эти результаты могут быть использованы при построении криптографических систем с открытым ключом.

Ключевые слова: многочлены над конечными полями, первообразные элементы, криптографические системы.

Введение

Возросший в последнее время интерес к криптографии обусловлен необходимостью обеспечения конфиденциальности переданной информации. Один из первых и самых распространенных подходов основан на использовании криптосистемы RSA [1]. Позднее появились модификации этого алгоритма. Например, алгоритм, основанный на теории эллиптических кривых [2]. При анализе криптоустойчивости таких алгоритмов используют, например, тест Соловея – Штрассена [3, с. 149] или тест Рабина – Миллера [4, с. 152].

Эти алгоритмы и тесты используют свойства первообразных корней в модулярной арифметике. В работе [5] предлагается обобщение функции Эйлера для многочленов над конечными полями и излагаются некоторые свойства этой функции. Поэтому для построения алгоритмов, использующих многочлены над конечными полями, необходимо описать свойства первообразных элементов в этом множестве.

Основная часть

Пусть F_p – конечное поле, состоящее из p элементов, $g(x)$ – многочлен положительной степени над полем F_p. Обозначим через $\varphi(g)$ количество всех ненулевых многочленов над F_p, которые взаимно просты с многочленом $g(x)$ и степени которых меньше степени многочлена $g(x)$. Множество этих многочленов обозначим $U_g = \{g_1(x), g_2(x),..., g_{\varphi(g)}(x)\}$ и назовем базой многочле-

нов для многочлена $g(x)$. Если же $g(x)$ – многочлен нулевой степени над полем F_p, то будем считать $\varphi(g)=1$. Введем следующее обозначение: $\widetilde{g}=p^{\deg(g)}$, где $g(x)\in F_p[x]$. Справедливы следующие утверждения:

1) пусть $f(x),\ g(x)\in F_p[x],\ \deg(g)>0,\ НОД(f;g)=1,$

тогда $f^{\varphi(g)}\equiv 1 \pmod{g}$.

2) пусть $g(x)=\prod_{i=1}^{k} g_i^{m_i}(x)$ – каноническое разложение многочлена $g(x)$ на степени неприводимых над F_p многочленов $g_1(x),...,\ g_k(x)$, тогда $\varphi(g)=\widetilde{g}\prod_{i=1}^{k}\left(1-\frac{1}{\widetilde{g}_i}\right)$.

Эти свойства являются обобщением формулы Эйлера и формулы для вычисления функции Эйлера [6].

В настоящей работе мы рассмотрим обобщение понятия первообразного корня в модулярной арифметике, а также соответствующие свойства.

Определение. *Пусть* $f(x),\ g(x)\in F_p[x],\ \deg(g)>0,\ НОД(f;g)=1$. *Наименьшее натуральное число n такое, что* $f^n\equiv 1 \pmod{g}$, *называется показателем многочлена* $f(x)$ *по модулю многочлена* $g(x)$ *и обозначается* $n=P_g(f)$.

Так как $f^{\varphi(g)}\equiv 1 \pmod{g}$, то $P_g(f)$ всегда существует.

Сформулируем некоторые свойства показателей.

Теорема 1. *Пусть* $n=P_g(f)$, *тогда справедливы следующие утверждения.*

1) Многочлены $1=f^0, f^1,..., f^{n-1}$ *попарно не сравнимы по модулю* g.

2) $f^{k_1}\equiv f^{k_2} \pmod{g}$ *тогда и только тогда, когда* $k_1\equiv k_2 \pmod{n}$. *В частности,* $f^k\equiv 1 \pmod{g}$ *тогда и только тогда, когда* $k\equiv 0 \pmod{n}$.

3) $\varphi(g)\equiv 0 \pmod{n}$.

4) Если $P_g(f)=ab$ *для некоторых* $a,b\in N$, *то* $P_g(f^a)=b$.

5) Если $НОД(P_g(f_1);\ P_g(f_2))=1$, *то* $P_g(f_1f_2)=P_g(f_1)P_g(f_2)$.

6) Если $НОД(f_1f_2;g)=1,\ f_1\equiv f_2 \pmod{g}$, *то* $P_g(f_1)=P_g(f_2)$.

Доказательство. 1) Предположим, что $f^{k_1}\equiv f^{k_2} \pmod{g}$ для некоторых $0\le k_1<k_2<n$, тогда $f^{k_1}(f^{k_2-k_1}-1)\equiv 0 \pmod{g}$, значит, $f^{k_2-k_1}\equiv 1 \pmod{g}$, поскольку $НОД(f^{k_1};g)=1$. Так как $0<k_2-k_1<n$, $n=P_g(f)$, то получено противоречие. Что и требовалось доказать.

2) Пусть $k_1 = nq_1 + r_1$, $k_2 = nq_2 + r_2$, $0 \le r_1 < n$, $0 \le r_2 < n$.

Так как $f^n \equiv 1 \pmod{g}$, то $f^{k_1} \equiv (f^n)^{q_1} f^{r_1} \equiv f^{r_1} \pmod{g}$.

Аналогично получаем $f^{k_2} \equiv f^{r_2} \pmod{g}$.

Имеем $f^{k_1} \equiv f^{k_2} \pmod{g} \Leftrightarrow f^{r_1} \equiv f^{r_2} \pmod{g} \Leftrightarrow r_1 = r_2 \Leftrightarrow$
$k_1 - nq_1 = k_2 - nq_2 \Leftrightarrow k_1 - k_2 = n(q_1 - q_2) \Leftrightarrow k_1 \equiv k_2 \pmod{n}$.

В частности, $f^k \equiv 1 \pmod{g} \Leftrightarrow f^k \equiv f^0 \pmod{g} \Leftrightarrow k \equiv 0 \pmod{n}$.

3) Так как $f^{\varphi(g)} \equiv 1 \pmod{g}$, то, согласно свойству 2), получаем требуемое.

4) Пусть $k = P_g(f^a)$, тогда $f^{ak} \equiv (f^a)^k \equiv 1 \pmod{g}$, следовательно, $ak \equiv 0 \pmod{ab}$, поскольку $P_g(f) = ab$. Значит, $k \equiv 0 \pmod{b}$. Так как $P_g(f) = ab$, то $(f^a)^b \equiv f^{ab} \equiv 1 \pmod{g}$, следовательно, $b \equiv 0 \pmod{k}$, поскольку $P_g(f^a) = k$. Так как $k \equiv 0 \pmod{b}$, $b \equiv 0 \pmod{k}$, то $k = b$.

5) Пусть $k = P_g(f_1 f_2)$, $a = P_g(f_1)$, $b = P_g(f_2)$,

тогда $(f_1 f_2)^k \equiv 1 \pmod{g}$, $f_1^a \equiv 1 \pmod{g}$, $f_2^b \equiv 1 \pmod{g}$, следовательно, $f_1^{kb} \equiv f_1^{kb} (f_2^b)^k \equiv ((f_1 f_2)^k)^b \equiv 1 \pmod{g}$, значит, $kb \equiv 0 \pmod{a}$. Учитывая $\text{НОД}(a;b) = 1$, получаем $k \equiv 0 \pmod{a}$. Аналогично устанавливаем $k \equiv 0 \pmod{b}$. Так как $k \equiv 0 \pmod{a}$, $k \equiv 0 \pmod{b}$, $\text{НОД}(a;b) = 1$, то $k \equiv 0 \pmod{ab}$. Так как $(f_1 f_2)^{ab} \equiv (f_1^a)^b (f_2^b)^a \equiv 1 \pmod{g}$, то $ab \equiv 0 \pmod{k}$. Следовательно, $k = ab$.

6) Пусть $a = P_g(f_1)$, $b = P_g(f_2)$, тогда $f_1^a \equiv 1 \pmod{g}$, $f_2^b \equiv 1 \pmod{g}$. Так как $f_1 \equiv f_2 \pmod{g}$, то $f_1^b \equiv f_2^b \equiv 1 \pmod{g}$, следовательно, $b \equiv 0 \pmod{a}$. Аналогично получаем $a \equiv 0 \pmod{b}$. Следовательно, $a = b$.

Теорема доказана.

Определение. Если $P_g(f) = \varphi(g)$, то многочлен $f(x)$ называется первообразным многочленом по модулю $g(x)$.

Теорема 2. *Пусть многочлен $g(x)$ неприводим над F_p, тогда существует первообразный многочлен по модулю $g(x)$.*

Доказательство. Вначале проверим справедливость следующей леммы.

Лемма. Пусть $K = F_p[x]$, $a_i(x) \in K$,

$G(y) = a_k(x) y^k + \ldots + a_1(x) y + a_0(x) \in K[y]$, $g(x) \in K$, U_g – база неприводимых многочленов для многочлена $g(x)$. Если сравнение $G(y) \equiv 0 \pmod{g}$ имеет более k различных решений, принадлежащих множеству U_g, то $a_i(x) \equiv 0 \pmod{g}$ для любого $i = 1, \ldots, k$.

Доказательство леммы. Пусть $g_1(x),\ g_2(x),\ ...,\ g_{k+1}(x) \in U_g$ являются различными решениями сравнения $G(y) \equiv 0 \pmod{g}$,

т. е. $G(g_i(x)) \equiv 0 \pmod{g}$ для $i = 1,2,...,\ k+1$. Разделим многочлен $G(y)$ на многочлен $(y - g_1(x)) \cdot (y - g_2(x)) \cdot ... \cdot (y - g_k(x))$ с остатком:

$G(y) = c_k(x) \cdot (y - g_1(x)) \cdot (y - g_2(x)) \cdot ... \cdot (y - g_k(x)) + r_k(y),$

где $c_k(x) = a_k(x),\ \deg(r_k) < k$ или $r_k(y) = 0$. Разделим многочлен $r_k(y)$ на $(y - g_1(x)) \cdot (y - g_2(x)) \cdot ... \cdot (y - g_{k-1}(x))$ с остатком:

$r_k(y) = c_{k-1}(x) \cdot (y - g_1(x)) \cdot (y - g_2(x)) \cdot ... \cdot (y - g_k(x)) + r_{k-1}(y),$

где $c_{k-1}(x) \in F_p[x],\ \deg(r_{k-1}) < k-1$ или $r_{k-1}(y) = 0$.

И так далее продолжаем этот процесс. В результате получаем $G(y) = c_k(x) \cdot (y - g_1(x)) \cdot ... \cdot (y - g_k(x)) + c_{k-1}(x) \cdot (y - g_1(x)) \cdot ... \cdot (y - g_{k-1}(x)) + ...$ $+ c_1(x) \cdot (y - g_1(x)) + c_0(x)$, где $c_i(x) \in F_p[x]$. Так как $G(g_1(x)) \equiv 0 \pmod{g}$, то $c_0(x) \equiv 0 \pmod{g}$. Так как $G(g_2(x)) \equiv 0 \pmod{g}$, то $c_1(x) \cdot (g_2(x) - g_1(x)) + c_0(x) \equiv 0 \pmod{g}$. Так как $g_1(x),\ g_2(x) \in U_g$, то $g_2(x) - g_1(x)$ не делится на $g(x)$. Учитывая $c_0(x) \equiv 0 \pmod{g}$, получаем $c_1(x) \equiv 0 \pmod{g}$. И так далее, рассматривая $G(g_3(x)),\ ...,\ G(g_{k+1}(x))$, получаем $c_2(x) \equiv ... \equiv c_k(x) \equiv 0 \pmod{g}$.

Так как $G(y) = a_k(x)y^k + ... + a_1(x)y + a_0(x),$

$G(y) = c_k(x) \cdot (y - g_1(x)) \cdot ... \cdot (y - g_k(x)) + + c_{k-1}(x) \cdot (y - g_1(x)) \cdot ... \cdot (y - g_{k-1}(x)) + ...$ $+ c_1(x) \cdot (y - g_1(x)) + c_0(x)$, то каждый многочлен $a_i(x)$ является линейной комбинацией многочленов $c_1(x),\ ...,\ c_k(x)$. Учитывая $c_i(x) \equiv 0 \pmod{g}$ для любого *i*, получаем $a_i(x) \equiv 0 \pmod{g}$ для любого *i*.

Лемма доказана.

Перейдем к доказательству теоремы.

Рассмотрим случай $p = 2,\ \deg(g) = 1$. Тогда $g(x) = x$ или $g(x) = x + 1$. Следовательно, $U_g = \{1\}$ – база неприводимых многочленов по модулю $g(x)$, $\varphi(g) = |U_g| = 1$. Если $g(x) = x$, то многочлен $f(x) = x + 1$ является первообразным многочленом по модулю $g(x)$, поскольку $f^1 \equiv 1 \pmod{g}$. Если $g(x) = x + 1$, то многочлен $f(x) = x$ является первообразным многочленом по модулю $g(x)$, поскольку $f^1 \equiv 1 \pmod{g}$.

Пусть теперь $p \geq 3$ или $\deg(g) \geq 2$.

Пусть $U_g = \{g_1(x),\ g_2(x),\ ...,\ g_{\varphi(g)}(x)\}$; $a_1, a_2, ..., a_{\varphi(g)}$ – показатели многочленов $g_1(x),\ g_2(x),\ ...,\ g_{\varphi(g)}(x)$ по модулю $g(x)$; $a = \text{НОК}(a_1, a_2, ..., a_{\varphi(g)})$.

Покажем, что $a > 1$. Действительно, если $p \geq 3$, то $2 \in U_g$, причем показатель многочлена 2 не равен 1 по модулю $g(x)$. Следовательно, в этом случае $a > 1$. Если же $\deg(g) \geq 2$, то $x \in U_g$, причем показатель многочлена 2 не равен 1 по модулю $g(x)$. Действительно, если $x \notin U_g$, то НОД $(x; g(x)) \neq 1$, значит, $g(x) \equiv 0 \pmod{x}$, что невозможно, поскольку $g(x)$ неприводим и $\deg(g) \geq 2$. Следовательно, и в этом случае $a > 1$.

Пусть $a = q_1^{c_1} q_2^{c_2} \ldots q_k^{c_k}$ – каноническое разложение числа a, тогда среди чисел $a_1, a_2, \ldots, a_{\varphi(g)}$ найдется число b, делящееся на $q_1^{c_1}$, т. е. $b = b_1 q_1^{c_1}$. Пусть b_1 – показатель некоторого многочлена $z_1(x) \in U_g$ по модулю $g(x)$, тогда $q_1^{c_1}$ – показатель многочлена $t_1(x) = (z_1(x))^{b_1}$ по модулю $g(x)$. Аналогично находим многочлены $t_2(x), t_3(x), \ldots, t_k(x)$, показатели которых равны $q_2^{c_2}, q_3^{c_3}, \ldots, q_k^{c_k}$. Следовательно, $q_1^{c_1} q_2^{c_2} \ldots q_k^{c_k}$ – показатель многочлена $T(x) = t_1(x) t_2(x) \ldots t_k(x)$ по модулю $g(x)$, т. е. $a = P_g(T)$.

Так как $g_i \in U_g$, то НОД$(g_i; g) = 1$, следовательно, $g_i^{\varphi(g)} \equiv 1 \pmod{g}$ для любого i, значит, $\varphi(g) \equiv 0 \pmod{a_i}$, поскольку $a_i = P_g(g_i)$. Поэтому $\varphi(g) \equiv 0 \pmod{a}$, поскольку $a = \text{НОК}(a_1, a_2, \ldots, a_{\varphi(g)})$. Значит, $\varphi(g) \geq a$.

Так как $g_i^{a_i} \equiv 1 \pmod{g}$, $a \equiv 0 \pmod{a_i}$, то $g_i^{a} \equiv 1 \pmod{g}$ для любого i. Пусть $G(y) = y^a - 1$, тогда $g_1(x), g_2(x), \ldots, g_{\varphi(g)}(x)$ являются решениями сравнения $G(y) \equiv 0 \pmod{g}$. Так как не все коэффициенты многочлена $G(y)$ делятся на многочлен $g(x)$, то, согласно предыдущей лемме, $\deg(G) \geq \varphi(g)$, т. е. $a \geq \varphi(g)$.

Так как $\varphi(g) \geq a$, $a \geq \varphi(g)$, то $a = \varphi(g)$. Итак, $\varphi(g) = a = P_g(T)$.

Теорема доказана.

Теорема 3. *Пусть* $g(x) = \prod_{i=1}^{k} g_i^{m_i}(x)$ – *разложение многочлена* $g(x)$ *на степени неприводимых над* F_p *многочленов* $g_1, g_2, \ldots, g_k$. *Если* $k \geq 2$ *и* $p \geq 3$, *то не существует первообразного многочлена по модулю* $g(x)$.

Доказательство. Предположим, что существует первообразный многочлен $f(x)$ по модулю $g(x)$, тогда НОД$(f; g) = 1$. Так как $g(x) = \prod_{i=1}^{k} g_i^{m_i}(x)$, то $\varphi(g) = \prod_{i=1}^{k} \left(\widetilde{g}_i^{m_i - 1} \cdot (\widetilde{g}_i - 1)\right)$, причем $\widetilde{g}_i - 1 \equiv p^{\deg(g_i)} - 1 \equiv 0 \pmod{p-1}$. Пусть $w = \text{НОК}\left(\widetilde{g}_1^{m_1 - 1} \cdot (\widetilde{g}_1 - 1); \ldots; \widetilde{g}_k^{m_k - 1} \cdot (\widetilde{g}_k - 1)\right)$. Так как $\widetilde{g}_i - 1 \equiv 0 \pmod{p-1}$

для любого i, то $w \le \dfrac{\prod_{i=1}^{k}\left(\widetilde{g}_i^{\,m_i-1}\cdot(\widetilde{g}_i-1)\right)}{p-1} = \dfrac{\varphi(g)}{p-1} < \varphi(g)$, т. е. $w < \varphi(g)$.

Так как НОД$(f; g) = 1$, то НОД$(f; g_i^{m_i}) = 1$, следовательно, $f^{\varphi(g_i^{m_i})} \equiv 1 \pmod{g_i^{m_i}}$. Так как $\varphi(g_i^{m_i}) = \widetilde{g}_i^{\,m_i}(\widetilde{g}_i - 1)$, то $w \equiv 0 \pmod{\varphi(g_i^{m_i})}$, следовательно, $f^{w} \equiv 1 \pmod{g_i^{m_i}}$ для любого i, значит, $f^{w} \equiv 1 \pmod{g}$. Учитывая $\varphi(g) = P_g(f)$, получаем $w \equiv 0 \pmod{\varphi(g)}$, что невозможно, поскольку $w < \varphi(g)$.

Теорема доказана.

Теорема 4. *Пусть* $g(x) = \prod_{i=1}^{k} g_i^{m_i}(x)$ – *разложение многочлена* $g(x)$ *на степени неприводимых над* F_2 *многочленов* $g_1, g_2, ..., g_k$ *и* $k \ge 2$, *тогда справедливы следующие утверждения:*

1) если $m_1 \ge 2, m_2 \ge 2$, *то не существует первообразного многочлена по модулю* g;

2) если НОД$(\deg(g_1); \deg(g_2)) \ge 2$, *то не существует первообразного многочлена по модулю* g.

Доказательство. Пусть $f(x)$ – первообразный многочлен по модулю $g(x)$. Как и в предыдущей теореме обозначим через $w = \text{НОК}\left(\widetilde{g}_1^{\,m_1-1}\cdot(\widetilde{g}_1-1); ...; \widetilde{g}_k^{\,m_k-1}\cdot(\widetilde{g}_k-1)\right)$. Аналогично получаем $w \equiv 0 \pmod{\varphi(g)}$, где $\varphi(g) = \prod_{i=1}^{k}\left(\widetilde{g}_i^{\,m_i-1}\cdot(\widetilde{g}_i-1)\right)$.

Пусть $m_1 \ge 2, m_2 \ge 2$, тогда $\widetilde{g}_1^{\,m_1-1} \equiv \left(2^{\deg(g_1)}\right)^{m_1-1} \equiv 0 \pmod 2$.

Аналогично получаем $\widetilde{g}_2^{\,m_2-1} \equiv 0 \pmod 2$. Следовательно, $w \le \dfrac{1}{2}\prod_{i=1}^{k}\left(\widetilde{g}_i^{\,m_i-1}\cdot(\widetilde{g}_i-1)\right) = \dfrac{\varphi(g)}{2} < \varphi(g)$, что невозможно, поскольку $w \equiv 0 \pmod{\varphi(g)}$.

Пусть $d = \text{НОД}(\deg(g_1); \deg(g_2)) \ge 2$,

тогда $\widetilde{g}_1 - 1 \equiv 2^{\deg(g_1)} - 1 \equiv 0 \pmod{2^d - 1}$. Аналогично получаем $\widetilde{g}_2 - 1 \equiv 2^{\deg(g_2)} - 1 \equiv 0 \pmod{2^d - 1}$, причем $2^d - 1 \ge 3$. Следовательно, $w \le \dfrac{1}{2^d-1}\prod_{i=1}^{k}\left(\widetilde{g}_i^{\,m_i-1}\cdot(\widetilde{g}_i-1)\right) = \dfrac{\varphi(g)}{2^d-1} < \varphi(g)$, что невозможно, поскольку $w \equiv 0 \pmod{\varphi(g)}$.

Теорема доказана.

Теорема 5. *Пусть* $f(x),\ g(x) \in F_p[x],\quad \deg(g) > 0,\quad НОД(f;g) = 1,$ $\varphi(g) = \prod_{i=1}^{m} q_i^{a_i}$ *– каноническое разложение числа* $\varphi(g)$. *Многочлен* $f(x)$ *является первообразным многочленом по модулю* $g(x)$ *тогда и только тогда, когда* $f^{\frac{\varphi(g)}{q_i}} \neq 1 \pmod{g}$ *для* $i = 1, 2, ..., m$.

Доказательство. Необходимость очевидна, поскольку $\varphi(g)$ – наименьший показатель многочлена $f(x)$ по модулю $g(x)$.

Докажем достаточность. Пусть $d = P_g(f)$, тогда $\varphi(g) \equiv 0 \pmod{d}$, следовательно, $\varphi(g) \geq d$. Предположим, что $\varphi(g) \neq d$, тогда $\varphi(g) > d$. Пусть q – простой делитель числа $\frac{\varphi(g)}{d}$, т. е. $\frac{\varphi(g)}{d} = qx$ для некоторого $x \in N$, тогда $\frac{\varphi(g)}{q} = dx$, причем q – простой делитель числа $\varphi(g)$. Следовательно, $f^{\frac{\varphi(g)}{q}} \equiv (f^d)^x \equiv 1^x \equiv 1 \pmod{g}$, что противоречит условию. Значит, $\varphi(g) = d$.

Теорема доказана.

Следующий пример показывает, что существование первообразного многочлена зависит от выбора поля F_p, а именно, если мы будем рассматривать один и тот же многочлен $g(x)$ над разными полями F_p, то в одном случае будет существовать первообразный многочлен по модулю $g(x)$, а в другом случае – нет.

Пример 1. Пусть $g(x) = x \in F_p[x]$, p – простое число, $n \in N$. Первообразный многочлен по модулю $g^n(x)$ существует тогда и только тогда, когда $n = 1$ или $n = 2$, или $\{n = 3;\ p = 2\}$.

Доказательство. 1) Покажем, что если a – первообразный корень по модулю p, то a – первообразный многочлен по модулю $g(x)$. Так как $g(x) = x$, то $\varphi(g) = \widetilde{g} - 1 = p^{\deg(g)} - 1 = = p - 1$. Так как $a^{p-1} = 1$ в F_p, $a^k \neq 1$ для любого k $(0 < k < p-1)$ в F_p, то $a^{p-1} \equiv 1 \pmod{g}$, причем $p - 1$ является наименьшим показателем. Следовательно, $\varphi(g) = p - 1 = P_g(a)$.

2) Покажем, что если a – первообразный корень по модулю p, то $x + a$ является первообразным многочленом по модулю g^2. Так как $g(x) = x$, то $\widetilde{g} = p^{\deg(g)} = p$, следовательно, $\varphi(g^2) = (\widetilde{g})^2\left(1 - \frac{1}{\widetilde{g}}\right) = p^2 - p$. Так как $a^{p-1} = 1$ в F_p, то $a \neq 0$, следовательно, $НОД(x + a;\ x^2) = 1$, значит,

$(x+a)^{\varphi(g^2)} \equiv 1 \pmod{g^2}$. Предположим, что существует натуральное число k такое, что $(x+a)^k \equiv 1 \pmod{x^2}$, причем $k < \varphi(g^2) = p^2 - p$. Тогда $a^k + ka^{k-1}x \equiv 1 \pmod{x^2}$, следовательно, $a^k = 1, ka^{k-1} = 0$ в F_p, т. е. $a^k = 1, k = 0$ в F_p. Значит, $k \equiv 0 \pmod{p-1}, k \equiv 0 \pmod{p}$, т. е. $k \equiv 0 \pmod{p^2 - p}$, что невозможно, поскольку $0 < k < p^2 - p$.

3) Покажем, что если $p = 2$, то $x+1$ является первообразным многочленом по модулю g^3. Так как $g(x) = x$, то $\widetilde{g} = 2^{\deg(g)} = 2$, следовательно, $\varphi(g^3) = (\widetilde{g})^3\left(1 - \frac{1}{\widetilde{g}}\right) = 4$. Кроме того, несложно проверить, что при $k = 1, 2, 3$ сравнение $(x+1)^k \equiv 1 \pmod{x^3}$ не выполняется.

4) Покажем, что если $\{n = 3;\ p \geq 3\}$ или $n \geq 4$, то не существует первообразного многочлена по модулю g^n. Предположим, что существует первообразный многочлен $f(x)$ по модулю $g^n(x)$. Пусть $r(x)-$ остаток при делении многочлена $f(x)$ на многочлен $g^n(x)$, тогда $r(x)-$ также первообразный многочлен по модулю g^n, $r(x) = a_{n-1}x^{n-1} + ... + a_1x + a_0$, причем НОД $(r; g^n) = 1$. Так как НОД$(r; g^n) = (r; x^n) = 1$, то $a_0 \neq 0$ в F_p, следовательно, $a_0^{p-1} = 1$ в F_p. Так как $g(x) = x$, то $\widetilde{g} = p^{\deg(g)} = p$, следовательно, $\varphi(g^n) = (\widetilde{g})^n\left(1 - \frac{1}{\widetilde{g}}\right) = p^{n-1}(p-1)$. Так как $\{n = 3;\ p \geq 3\}$ или $n \geq 4$, то $p^{n-2} \geq n$. Следовательно, $(r(x))^{p^{n-2}} \equiv (a_{n-1}x^{n-1} + ... + a_1x + a_0)^{p^{n-2}} \equiv$

$\equiv a_{n-1}^{p^{n-2}}(x^{n-1})^{p^{n-2}} + ... + a_1^{p^{n-2}}x^{p^{n-2}} + a_0^{p^{n-2}} \equiv a_0^{p^{n-2}} \pmod{x^n}$,

значит, $(r(x))^{p^{n-2}(p-1)} \equiv \left(a_0^{p^{n-2}}\right)^{p-1} \equiv$ $\equiv (a_0^{p-1})^{p^{n-2}} \equiv 1^{p^{n-2}} \equiv 1 \pmod{x^n}$, что невозможно, поскольку $p^{n-2}(p-1) < p^{n-1}(p-1) = \varphi(g^n)$.

Что и требовалось доказать.

Как видим из предыдущего примера, первообразный многочлен по модулю x^3 существует тогда и только тогда, когда $x^3 \in F_2[x]$.

Следующий пример показывает, что первообразные многочлены существуют не только по модулю примарной степени или произведения двух примарных степеней неприводимых многочленов. Тем самым мы обнаруживаем существенное отличие от модулярной арифметики, поскольку первообразные корни по модулю m существуют только при $m = 2, 4, p^k, 2p^k$.

Пример 2. Пусть $g_1(x) = x, g_2(x) = x+1, g_3(x) = x^2 + x + 1-$ неприводимые над полем F_2 взаимно простые многочлены, тогда существует первообразный многочлен по модулю $g_1g_2g_3$.

Доказательство. Покажем, что многочлен $f(x) = x^3 + x + 1$ является первообразным многочленом по модулю $g_1 g_2 g_3$. Так как $g_1(x)$, $g_2(x)$, $g_3(x)$ – неприводимые над F_2 многочлены, то $\varphi(g_1 g_2 g_3) = (\widetilde{g}_1 \widetilde{g}_2 \widetilde{g}_3)\left(1 - \frac{1}{\widetilde{g}_1}\right)\left(1 - \frac{1}{\widetilde{g}_2}\right)\left(1 - \frac{1}{\widetilde{g}_3}\right) = 3,$ поскольку $\widetilde{g}_1 = 2^{\deg(g_1)} = 2,\ \widetilde{g}_2 = 2^{\deg(g_2)} = 2,\ \widetilde{g}_3 = 2^{\deg(g_3)} = 4.$ Так как многочлен $f(x)$ не делится на неприводимые многочлены $g_1(x)$, $g_2(x)$, $g_3(x)$, то НОД $(f; g_1 g_2 g_3) = 1,$ следовательно, $f^{\varphi(g_1 g_2 g_3)} \equiv 1 \pmod{g_1 g_2 g_3}$, т. е. $f^3 \equiv 1 \pmod{g_1 g_2 g_3}$. Кроме того, несложно проверить, что при $k = 1, 2$ сравнение $f^k \equiv 1 \pmod{g_1 g_2 g_3}$ не выполняется.

Что и требовалось доказать.

Заключение

Таким образом, получены свойства первообразных многочленов над полем F_p. Это показывает преемственность в изучении первообразных корней в модулярной арифметике и в теории многочленов над конечными полями. Для одного и того же многочлена *f(x)* может существовать первообразный многочлен по модулю *f(x)* над одним конечным полем, но при этом не существовать первообразного многочлена по модулю *f(x*) над другим конечным полем. Кроме того, первообразные многочлены могут существовать по модулю произведения более двух примарных степеней различных неприводимых многочленов, в то время как, в модулярной арифметике первообразные корни могут существовать по модулю произведения не более двух примарных степеней различных простых чисел. Факт такого научно-теоретического дуализма объясняет возрастающую значимость конечных полей в криптографии указывает на важность изучения свойств многочленов над конечными полями.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Rivest, R. A method for obtaining digital signatures and public-key cryptosystems / R. Rivest, A. Shamir, L. Adleman // Communications of the ACM. – 1978. – Vol. 21. – P. 120–126.

2. ***Болотов, А. А.*** Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы / А. А. Болотов, С. Б. Гашков, А. Б. Фролов, А. А. Часовских. – М. : КомКнига, 2006. – 328 с.

3. ***Коблиц, Н.*** Курс теории чисел и криптографии / Н. Коблиц. – М. : ТВП, 2001. – 254 с.

4. ***Глухов, М. М.*** Введение в теоретико-числовые методы криптографии / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. – СПб. : Лань, 2011. – 400 с.

5. ***Базылев, Д. Ф.*** О некоторых криптографических свойствах функции Эйлера для многочленов над конечным полем / Д. Ф. Базылев // Сб. науч. ст. Воен. акад. Респ. Беларусь. – 2019. – № 37. – С. 44–49.

6. ***Бухштаб, А. А.*** Теория чисел / А. А. Бухштаб. – М. : Государственное учебно-педагогическое издательство Министерства просвещения РСФСР, 1960. – 375 с.

Поступила в редакцию 01.06.2025 г.
Контакты: bazylev@bsu.by (Базылев Дмитрий Федорович)

Bazyleu D. F. **PRIMITIVE POLYNOMIALS OVER FINITE FIELDS**

The paper considers a generalization to the case of polynomials over finite fields of the notion of a primitive root in modular arithmetic. The conditions that ensure the existence or absence of primitive polynomials are obtained. A number of properties are preserved in comparison with the properties of primitive roots. But there are also significant differences which are given in the article. The results can be used in the construction of cryptographic systems with a public key.

Keywords: polynomials over finite fields, primitive elements, cryptographic systems.