УДК 512.624.5

ПЕРИОДЫ РАЗРЯДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ЛИНЕЙНЫХ РЕКУРРЕНТ МАКСИМАЛЬНОГО ПЕРИОДА НАД КОНЕЧНЫМИ ПРОСТЫМИ ПОЛЯМИ

С. А. Кузьмин

г. Москва, Россия

Найдены периоды разрядных последовательностей, полученных из r-ичного разложения знаков линейной рекуррентной последовательности максимального периода над конечным простым полем для произвольного натурального $r \geqslant 3$.

Ключевые слова: *линейные рекурренты максимального периода, разрядные последовательности, конечные поля, простые поля, период последовательности.*

PERIODS OF DIGIT-POSITION SEQUENCES RECEIVED FROM LINEAR RECURRENT SEQUENCES OF MAXIMAL PERIOD OVER FINITE PRIME FIELDS

S. A. Kuzmin

Moscow, Russia

E-mail: kzmn_sr@mail.ru

In the paper, for any integer $r \geqslant 3$, the periods of digit-position sequences obtained from r-ary representation of elements in a linear recurrent sequence of the maximal period over prime field are computed.

Keywords: *linear recurrent sequences of maximal period, digit-position sequences, finite fields, prime fields, periods of linear recurrent sequences.*

Введение

Пусть дано поле вычетов $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$, где p — простое число, $p \geqslant 3$. Пусть также u — линейная рекуррентная последовательность (ЛРП) максимального периода (МП) над полем $\mathbb{Z}_p$ с характеристическим многочленом $g(x)$ степени m. Известно, что период линейной рекурренты u равен $T(u) = p^m - 1$ [1, с. 330].

Пусть целое число r удовлетворяет условиям $1 < r < p$. В этом случае знаки $u(i)$, $i \geqslant 0$, ЛРП u однозначно представляются в виде

$$u(i) = \sum_{t=0}^{k} u_t(i) r^t, \tag{1}$$

где $0 \leqslant u_t(i) < r$; $k = [\log_r p]$.

Для каждого $s \in \{1, \ldots, k\}$ из элементов $u_s(i)$ r-ичного разложения знаков ЛРП u образуем разрядные последовательности $u_s = (u_s(0), u_s(1), \ldots)$. Будем рассматривать их как усложнения ЛРП u.

Отметим, что в настоящее время наблюдается большой интерес к изучению p-ичных разрядных последовательностей над кольцами вычетов по модулю p^n. Это связано с тем, что данные последовательности обладают высокой линейной сложностью и

могут рассматриваться как псевдослучайные последовательности для датчиков случайных чисел. С большим количеством работ по этой тематике можно ознакомиться в [2, 3]. Следует также отметить работы зарубежных авторов [4, 5], в которых проводится анализ частотных и алгебраических свойств приведённых по модулю 2 ЛРП МП над кольцами вычетов вида $\mathbb{Z}_{p^n}$ и $\mathbb{Z}_{pq}$, где q и p — различные простые числа.

Нетрудно заметить, что так как $T(u)$ является одним из периодов ЛРП u_s, то, согласно [1, с. 320], $T(u_s)$ делит период ЛРП u.

Для $r = 2$ и для некоторых $r \geqslant 3$ А. С. Кузьминым в [6] найдены периоды ЛРП u_s, $s \in \{1, \ldots, k\}$. В настоящей работе этот результат обобщён для случая $r \geqslant 3$. Доказано, что $T(u_s) = T(u)$ для всех $r \geqslant 3$ и любого $s \in \{1, \ldots, k\}$.

1. Общие сведения

Для натурального числа r, удовлетворяющего условию $2 \leqslant r < p$, рассмотрим r-ичное разложение числа p:

$$p = a_k r^k + a_{k-1} r^{k-1} + \cdots + a_1 r + a_0,$$

где $k = [\log_r p]$; $a_i \in \{0, \ldots, r-1\}$. Выделим s-й разряд полученного разложения:

$$p = \theta + a_s r^s + a(s) r^{s+1}, \tag{2}$$

где

$$\theta = \begin{cases} \sum\limits_{t=0}^{s-1} a_t r^t, & \text{если } s \neq 0, \\ 0, & \text{если } s = 0, \end{cases} \qquad a(s) = \sum_{t=s+1}^{k} a_t r^{t-s-1},$$

рассмотрение $a(s)$ при $k = 0$ лишено смысла.

Нетрудно заметить, что для элементов θ и $a(s)$ справедливы следующие свойства.

Лемма 1. Во введённых обозначениях при $s \neq 0$ имеют место следующие соотношения:

1) $\theta \equiv p \pmod{r^s}$;
2) $0 < \theta < r^s$;
3) $\theta \not\equiv -1 \pmod{p}$;
4) $a(s) + 1 < p$.

Отметим, что, согласно работе [6], справедливы неравества $\dfrac{T(u)}{d} \leqslant T(u_s) \leqslant T(u)$, где d — наибольший общий делитель чисел появлений элементов $\omega \in \{0, \ldots, r-1\}$ в последовательности u_s на отрезке длины $T(u)$.

Воспользуемся результатом, который даёт следующая теорема.

Теорема 1 [6]. Если $a_s \geqslant 2$ и $r \geqslant 3$, то наибольший общий делитель количеств появлений элементов $\omega \in \{0, \ldots, r-1\}$ на отрезке длины $T(u)$ последовательности u_s равен единице. При этих условиях $T(u_s) = T(u)$.

Получаем, что для всех возможных значений a_s, за исключением $a_s = 0$ и $a_s = 1$, период $T(u_s)$ заведомо равен периоду исходной рекурренты.

Для нахождения периодов в двух оставшихся случаях применим следующий подход. Рассмотрим функции $\delta_s : \mathbb{Z}_p \to \mathbb{Z}_p$, $s \in \{0, \ldots, k\}$, $k = [\log_r p]$, задаваемые по правилу: $\delta_s(y) = y_s$ для всех $y \in \mathbb{Z}_p$, где y_s — s-я координата r-ичного разложения числа $y = y_0 + y_1 r + \cdots + y_k r^k$.

Тогда, согласно [7, с. 179], получаем, что для всех $s \in \{0, \ldots, k\}$ функции δ_s однозначно представимы над $\mathbb{Z}_p$ полиномами вида $C^{(s)}(x) = \sum\limits_{t=0}^{p-1} c_t^{(s)} x^t$.

Таким образом, для всех $y \in \mathbb{Z}_p$ справедливо $\delta_s(y) = C^{(s)}(y)$. Многочлены $C^{(s)}(x)$ могут быть найдены при помощи интерполяционной формулы Лагранжа, представленной, согласно [6], в виде

$$C^{(s)}(x) = \delta_s(0) - \sum_{j=0}^{p-1} \delta_s(j) x^{p-1} - \sum_{k=1}^{p-2} x^k \sum_{j=1}^{p-1} \delta_s(j) j^{p-k-1}. \tag{3}$$

Кроме того, в работе [6] доказана следующая лемма.

Лемма 2 [6]. Пусть u — ЛРП МП над полем $\mathbb{Z}_p$, $T(u) = p^m - 1$ и многочлен $h(x) = \sum\limits_{j=0}^{p-1} h_j x^j$, заданный над полем $\mathbb{Z}_p$, отличен от константы. Тогда период $T(v)$ последовательности v, знаки которой определяются равенством $v(i) = h(u(i))$, $i \geqslant 0$, равен $\sigma(p^m - 1)/(p - 1)$, где $(p - 1)/\sigma$ — наибольший общий делитель $p - 1$ и чисел $j \in \{1, 2, \ldots, p - 2\}$, для которых коэффициент h_j при x^j отличен от нуля.

Используем лемму 2 для оценки $T(u_s)$ при $a_s < 2$. Для этого установим, когда коэффициент $c_{p-2}^{(s)}$ многочлена $C^{(s)}$ отличен от 0. Вычисление коэффициента $c_{p-2}^{(s)}$ производится по той причине, что если он не сравним с нулём по модулю p, то, согласно лемме 2, период $T(u_s)$ последовательности u_s будет заведомо равен периоду $T(u)$ последовательности u при любом выборе $s \in \{0, \ldots, k\}$, независимо от других коэффициентов в выражении (3).

2. Основные результаты

Из формулы (3) непосредственно вытекает, что коэффициент при x^{p-2} в многочлене $C^{(s)}(x)$ имеет вид

$$c_{p-2}^{(s)} = -\sum_{j=0}^{p-1} j \delta_s(j). \tag{4}$$

Представим число p в виде (2), тогда суммирование в формуле (4) можно разбить на три суммы: по старшим разрядам, s-му и младшим соответственно. При этом индекс суммирования также представляется посредством r-ичного разложения с выделенным s-м разрядом.

Формула (4) для подсчёта значений $-c_{p-2}^{(s)}$ в случае $a_s = 0$ имеет вид

$$-c_{p-2}^{(s)} = \sum_{k=0}^{a(s)-1} \sum_{t=0}^{r-1} \sum_{j=0}^{r^s-1} t(kr^{s+1} + tr^s + j) + \sum_{k=a(s)}^{a(s)} \sum_{t=0}^{0} \sum_{j=0}^{\theta-1} t(kr^{s+1} + tr^s + j), \tag{5}$$

а для случая $a_s = 1$ формула (5) принимает вид

$$\begin{aligned} -c_{p-2}^{(s)} = \sum_{k=0}^{a(s)-1} \sum_{t=0}^{r-1} \sum_{j=0}^{r^s-1} t(kr^{s+1} + tr^s + j) + \sum_{k=a(s)}^{a(s)} \sum_{t=0}^{0} \sum_{j=0}^{r^s-1} t(kr^{s+1} + tr^s + j) + \\ + \sum_{k=a(s)}^{a(s)} \sum_{t=1}^{1} \sum_{j=0}^{\theta-1} t(kr^{s+1} + tr^s + j). \end{aligned} \tag{6}$$

Так как получаемые в ходе анализа формулы (6) громоздкие выражения не дают возможности определить, верно условие $-c_{p-2}^{(s)} \neq 0$ или нет, применим следующий

подход: введём вспомогательные функции δ'_s, определив их для любого $j \in \{0, \dots, p-1\}$ по правилу

$$\delta'_s(j) = \begin{cases} 1, & \text{если } \delta_s(j) \neq 0, \\ 0, & \text{если } \delta_s(j) = 0. \end{cases}$$

Таким образом произведено отождествление всех ненулевых значений функций δ_s. Функции $\delta'_s(x)$ также представимы многочленами $C'^{(s)}(x)$ над полем $\mathbb{Z}_p$, которые находятся при помощи формулы (3) с заменой $\delta_s(j)$ на $\delta'_s(j)$. При этом если $u'_s = (\delta'_s(u(0), \delta'_s(u(1)\dots)$ и $T(u'_s) = p^m - 1$, то очевидно, что $T(u_s) = p^m - 1$, так как справедливы неравенства $T(u) \geqslant T(u_s) \geqslant T(u'_s)$.

Формула (4) для случая $a_s = 0$ принимает вид

$$-c'^{(s)}_{p-2} = \sum_{k=0}^{a(s)-1} \sum_{t=1}^{r-1} \sum_{j=0}^{r^s-1} (kr^{s+1} + tr^s + j), \tag{7}$$

а для случая $a_s = 1$

$$-c'^{(s)}_{p-2} = \sum_{k=0}^{a(s)-1} \sum_{t=1}^{r-1} \sum_{j=0}^{r^s-1} (kr^{s+1} + tr^s + j) + \sum_{k=a(s)}^{a(s)} \sum_{t=1}^{1} \sum_{j=0}^{\theta-1} (kr^{s+1} + tr^s + j). \tag{8}$$

Лемма 3. Пусть для числа p выполнены условия (2). Тогда для любого $a_s \in \{0, 1\}$ коэффициент при x^{p-2} в многочлене $C'^{(s)}(x)$ отличен от нуля, за исключением случая $a_s = 0$, $\theta = r^s - 1$.

Доказательство. Рассмотрим сначала случай $a_s = 0$, то есть $p = a(s)r^{s+1} + \theta$. Вычислим $-c'^{(s)}_{p-2}$ по формуле (7):

$$-c'^{(s)}_{p-2} = \sum_{k=0}^{a(s)-1} \sum_{t=1}^{r-1} \sum_{j=0}^{r^s-1} (kr^{s+1} + tr^s + j) = a(s) \sum_{t=1}^{r-1} \sum_{j=0}^{r^s-1} \left(\frac{a(s)-1}{2} r^{s+1} + tr^s + j \right) =$$

$$= a(s)(r-1) \sum_{j=0}^{r^s-1} \left(\frac{a(s)-1}{2} r^{s+1} + \frac{r^{s+1}}{2} + j \right) =$$

$$= \frac{a(s)(r-1)r^s}{2} ((a(s)-1)r^{s+1} + r^{s+1} + r^s - 1) = \frac{a(s)(r-1)r^s}{2} (a(s)r^{s+1} + r^s - 1).$$

Выясним, когда выполняется соотношение $c'^{(s)}_{p-2}(x) \equiv 0 \pmod p$.

Заметим, что ни один из элементов, входящих в произведение $a(s)(r-1)r^s/2$, не сравним с нулем по модулю p, а следовательно, и $a(s)(r-1)r^s/2 \not\equiv 0 \pmod p$. Значит, $c'^{(s)}_{p-2}(x) \equiv 0 \pmod p$ тогда и только тогда, когда $a(s)r^{s+1} + r^s - 1 \equiv 0 \pmod p$, что возможно только при $\theta = r^s - 1$.

Теперь рассмотрим случай $a_s = 1$, то есть $p = a(s)r^{s+1} + r^s + \theta$. Из (7) и (8) следует, что к вычисленной выше сумме будет добавлено слагаемое

$$\sum_{k=a}^{a(s)} \sum_{t=1}^{1} \sum_{j=0}^{\theta-1} (kr^{s+1} + tr^s + j) = \sum_{j=0}^{\theta-1} (a(s)r^{s+1} + r^s + j) = \theta \left(a(s)r^{s+1} + r^s + (\theta - 1)/2 \right).$$

Надо выяснить, верно ли сравнение

$$\frac{a(s)(r-1)r^s}{2} (a(s)r^{s+1} + r^s - 1) + \theta(a(s)r^{s+1} + r^s + (\theta-1)/2) \equiv 0 \pmod p. \tag{9}$$

Так как $p = a(s)r^{s+1} + r^s + \theta$, то $-\theta \equiv r^{s+1} + r^s \pmod p$.

Из (9) получаем $a(s)(r-1)r^s(-\theta-1)+\theta(-1-\theta)\equiv 0 \pmod p$. Так как, согласно лемме 1, $-1-\theta\not\equiv 0 \pmod p$, то элемент $(-1-\theta)$ является обратимым в $\mathbb{Z}_p$. Последнее сравнение равносильно сравнению

$$a(s)(r-1)r^s+\theta\equiv -r^s-\theta-a(s)r^s+\theta=-a(s)r^s-r^s\equiv 0 \pmod p,$$

что выполняется тогда и только тогда, когда $1+a(s)\equiv 0 \pmod p$. В итоге получаем противоречие с видом числа p, так как, согласно лемме 1, справедливо неравенство $a(s)+1<p$, а значит, $-c'^{(s)}_{p-2}\neq 0$, что и требовалось доказать. ■

Теорема 2. Пусть $p=\theta+a_sr^s+a(s)r^{s+1}$, u — ЛРП МП над полем $\mathbb{Z}_p$, последовательности u'_t для любого $t\in\{0,\dots,k\}$, $k=[\log_r p]$, образованы из последовательностей u_t путём замены в формуле (3) всех значений $y_t=\delta_t(j)$ на

$$\delta'_t(j)=\begin{cases}1, & \text{если } \delta_t(j)\neq 0,\\ 0, & \text{если } \delta_t(j)=0.\end{cases}$$

Тогда $T(u'_s)=T(u)$ всегда, за исключением случая $a_s=0$, $\theta=r^s-1$.

Доказательство. Заметим, что лемма 2 справедлива и для многочленов $C'^{(s)}(x)$. Тогда сокращение периода ЛРП u'_s возможно, если наибольший общий делитель $p-1$ и чисел $j\in\{1,2,\dots,p-2\}$, для которых $c'^{(s)}_j\neq 0$, больше единицы. По лемме 3 коэффициент при x^{p-2} в многочлене $C'^{(s)}(x)$ отличен от нуля, и так как $(p-2,p-1)=1$, то и наибольший общий делитель всех $j\in\{1,2,\dots,p-2\}$, таких, что $c'^{(s)}_j\neq 0$, равен единице. Значит, выполняется равенство $T(u'_s)=p^m-1=T(u)$. ■

Следствие 1. В условиях теоремы 2 верно равенство $T(u_t)=T(u)$.

Доказательство следствия вытекает из двойного неравенства $T(u)\geqslant T(u_t)\geqslant T(u'_t)$ для любого $t\in\{0,\dots,k\}$, $k=[\log_r p]$.

Таким образом, остался не исследованным вопрос о равенстве нулю коэффициента при x^{p-2} в случае $\theta=r^s-1, a_s=0$, то есть в случае $p=a(s)r^{s+1}+r^s-1$.

Лемма 4. Пусть $p=a(s)r^{s+1}+r^s-1$. Тогда коэффициент при x^{p-2} в многочлене $C^{(s)}(x)$ отличен от нуля при $r\geqslant 3$.

Доказательство. Заметим, что $a(s)\neq 0$, так как иначе получим противоречие с леммой 1. Вычислим сумму (5), учитывая, что $p>r\geqslant 3$:

$$-c^{(s)}_{p-2}=\sum_{k=0}^{a(s)-1}\sum_{t=0}^{r-1}\sum_{j=0}^{r^s-1}t(kr^{s+1}+tr^s+j)+\sum_{k=a(s)}^{a(s)}\sum_{t=0}^{0}\sum_{j=0}^{\theta-1}t(kr^{s+1}+tr^s+j)=$$

$$=\sum_{t=0}^{r-1}\sum_{j=0}^{r^s-1}t\left(\frac{a(s)(a(s)-1)}{2}r^{s+1}+ta(s)r^s+a(s)j\right)=$$

$$=\sum_{j=0}^{r^s-1}\left(\frac{a(s)r(r-1)(a(s)-1)}{4}r^{s+1}+\frac{a(s)r^{s+1}(r-1)(2r-1)}{6}+\frac{a(s)r(r-1)j}{2}\right)=$$

$$=\frac{a(s)r(r-1)(a(s)-1)}{4}r^{2s+1}+\frac{a(s)(r-1)(2r-1)}{6}r^{2s+1}+\frac{a(s)(r^s-1)(r-1)r^{s+1}}{4}=$$

$$=\frac{a(s)r^{s+1}(r-1)}{12}(3r^{s+1}(a(s)-1)+2r^s(2r-1)+3(r^s-1)).$$

Так как $\dfrac{a(s)r^{s+1}(r-1)}{12}\not\equiv 0 \pmod p$, сравнение (9) эквивалентно сравнению

$$3r^{s+1}(a(s)-1)+2r^s(2r-1)+3(r^s-1)\equiv 0 \pmod p. \tag{10}$$

Раскроем в полученном выражении скобки. Учитывая сравнение

$$a(s)r^{s+1} \equiv 1 - r^s \pmod{p},$$

получаем, что выполнение сравнения (10) эквивалентно выполнению сравнения

$$3(1 - r^s) + r^{s+1} + r^s - 3 \equiv 0 \pmod{p}.$$

Следовательно, $r^{s+1} - 2r^s \equiv 0 \pmod{p}$. Поэтому $r^s(r-2) \equiv 0 \pmod{p}$, что равносильно сравнению $r - 2 \equiv 0 \pmod{p}$. Последнее не выполняется, так как $3 \leqslant r < p$.

Таким образом, коэффициент при x^{p-2} в многочлене $C^{(s)}(x)$ отличен от нуля. ■

Теорема 3. Пусть $p = a(s)r^{s+1} + r^s - 1$, $r \geqslant 3$, u — ЛРП МП над полем $\mathbb{Z}_p$, последовательности u_s образованы из последовательности u по правилу (1). Тогда $T(u_s) = T(u)$.

Доказательство. Согласно лемме 2, сокращение периода ЛРП u_t возможно, если наибольший общий делитель $p - 1$ и чисел $j \in \{1, 2, \ldots, p-2\}$, для которых $c_j^{(s)} \neq 0$, больше единицы. Согласно лемме 4, коэффициент при x^{p-2} в многочлене $C^{(s)}(x)$ отличен от нуля, и так как $(p-2, p-1) = 1$, то и наибольший общий делитель всех j, таких, что $c_j^{(s)} \neq 0$, равен единице. Значит, $T(u_t) = T(u) = p^m - 1$. ■

Замечание 1. Пусть $r = 2$. Тогда для каждого нечётного простого числа p, не являющегося числом Мерсенна, найдётся такое s, что $p = 2^s - 1 + a(s)2^{s+1}$. Для так выбранного s в работе [6] доказано, что $T(u_s) = T(u)/2$, и $T(u_t) = T(u)$ для всех $t \neq s$.

Заключение

Из следствия к теореме 2 и теоремы 3 следует, что периоды всех разрядных последовательностей u_s равны периоду последовательности u во всех случаях, за исключением $r = 2$, $\theta = r^s - 1$ и $a(s) \neq 0$.

ЛИТЕРАТУРА

1. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра. Т. 2. М.: Гелиос АРВ, 2003. 416 с.
2. Труды по дискретной математике. Т. 1. / сост. В. Н. Сачков, Ю. Н. Горчинский, А. Н. Зубков, С. В. Яблонский. М.: ТВП, 1997. 280 с.
3. Труды по дискретной математике. Т. 2. / сост. В. Н. Сачков, Ю. Н. Горчинский, А. Н. Зубков, С. В. Яблонский. М.: ТВП, 1998. 314 с.
4. *Zhu X. Y. and Qi W.-F.* On the distinctness of modular reductions of maximal length sequences modulo odd prime powers // Math. Comput. 2008. V. 77. No. 263. P. 1623–1637.
5. *Zheng Q.-X. and Qi W.-F.* A new result on the distinctness of primitive sequences over $\mathbb{Z}/(pq)$ modulo 2 // Finite Fields Their Appl. 2011. V. 17. No. 3. P. 254–274.
6. *Кузьмин А. С.* О периодах разрядов в r-ичной системе счисления знаков линейных рекуррентных последовательностей над конечными простыми полями // Безопасность информационных технологий. 1995. Вып. 4. С. 71–75.
7. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра. Т. 1. М.: Гелиос АРВ, 2003. 336 с.

REFERENCES

1. *Gluhov M. M., Elizarov V. P., Nechaev A. A.* Algebra. V. 2. Moscow, Gelios ARV Publ., 2003. 416 p. (in Russian)
2. Sachkov V. N., Gorchinskij Ju. N., Zubkov A. N., Jablonskij S. V., eds. Trudy po Diskretnoi Matematike. V. 1. Moscow, TVP Publ., 1997. 280 p. (in Russian)

3. Sachkov V. N., Gorchinskij Ju. N., Zubkov A. N., Jablonskij S. V., eds. Trudy po Diskretnoi Matematike. V. 2. Moscow, TVP Publ., 1998. 314 p. (in Russian)
4. *Zhu X. Y. and Qi W.-F.* On the distinctness of modular reductions of maximal length sequences modulo odd prime powers. Math. Comput., 2008, vol. 77, no. 263, pp. 1623–1637.
5. *Zheng Q.-X. and Qi W.-F.* A new result on the distinctness of primitive sequences over $\mathbb{Z}/(pq)$ modulo 2. Finite Fields Their Appl., 2011, vol. 17, no. 3, pp. 254–274.
6. *Kuz'min A. S.* O periodah razrjadov v r-ichnoj sisteme schislenija znakov linejnyh rekurrentnyh posledovatel'nostej nad konechnymi prostymi poljami. Bezopasnost' Informacionnyh Tehnologij, 1995, no. 4, pp. 71–75. (in Russian)
7. *Gluhov M. M., Elizarov V. P., Nechaev A. A.* Algebra. V. 1. Moscow, Gelios ARV Publ., 2003. 336 p. (in Russian)