УДК 519.7

А.С.Цурина

ЛИНЕЙНАЯ СЛОЖНОСТЬ ШЕСТЕРИЧНЫХ БИНАРНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

В данной статье представлены результаты расчета линейной сложности шестеричных бинарных последовательностей, сформированных на основе двух и трех циклотомических классов. Линейная сложность последовательности определяется через разложение её периода на сумму квадратов целых чисел.

Ключевые слова: линейная сложность, шестеричные бинарные последовательности, циклотомические классы

Введение

Линейная сложность последовательности определяется как длина самого короткого линейного регистра сдвига с обратной связью, который может генерировать последовательность и является её важным показателем [1]. Последовательности, обладающие высокой линейной сложностью, важны для криптографических приложений. Известны алгоритмы определения минимального многочлена последовательности и её линейной сложности, например алгоритм Берлекэмпа-Месси [1]. В [2] был разработан теоретический метод вычисления линейной сложности циклотомических последовательностей, сформированных на основе классов шестеричных вычетов. Он основан на вычислении значений многочлена, соответствующего классу шестеричных вычетов. Далее, в [3] при исследовании след представления последовательностей на классах степенных вычетов линейная сложность была вычислена для любой бинарной последовательности, сформированной на классе шестеричных вычетов и его классах смежности, при нечетном числе элементов в классе.

Цель настоящей статьи заключается в завершении исследования, начатого в [2,3], то есть в определении линейной сложности любой бинарной периодической последовательности, сформированной на основе классов шестеричных вычетов. Линейная сложность последовательности будет определена через разложение периода последовательности на сумму квадратов целых чисел. Метод исследования основан на найденных в [2] соотношениях для многочлена последовательности, соответствующего классу шестеричных вычетов.

1. Основные определения

Пусть $p = 6R+1$ — простое число, где R - натуральное четное число. Обозначим через H_0 - класс вычетов 6 степени по модулю p, то есть $H_0 = \left\{q^{6t} (\mathrm{mod}\ p),\ t = \overline{0, R-1}\right\}$, здесь q - первообразный корень по модулю p [4], $k = \overline{0, d-1}$. Положим $H_s = q^s H_0$, где $s = \overline{0, d-1}$ (все действия выполняются по модулю p), тогда $H_i \cap H_j = \varnothing, i \neq j$ и порядок $|H_i| = R$.

H_s - называются классами смежности H_0 или циклотомическими классами шестого порядка, при этом справедливо разбиение $Z_p = \{0\} \cup \bigcup_{i=0}^{d-1} H_i$. Рассмотрим последовательность $X = \{x_i\}$, сформированную по следующему правилу:

$$x_i = \begin{cases} 1, & \text{если } i(\mathrm{mod}\ p) \in \bigcup_{k \in I} H_k, \\ 0, & \text{в ост. случаях.} \end{cases}, \qquad (1)$$

где I — подмножество множества индексов $\{0,1,\mathrm{K},5\}$.

Обозначим через a примитивный корень степени p из единицы в поле разложения многочлена $t^p - 1$ над полем второго порядка. Пусть $S_6(t) = \sum_{n \in H_0} t^n$, $\mathbf{S}_6(a) = \left(S_6(a),\ S_6(a^q), \mathrm{K}, S_6\left(a^{q^5}\right)\right)$ и $\mathrm{T}_X(a) = \sum_{k \in I} D^k \mathrm{S}_6(a)$, где D — оператор циклического сдвига матрицы на единицу влево. Тогда, согласно [2],

$$L = p - \frac{p-1}{6}\Delta - e,$$

где Δ - число нулей в $\mathrm{T}_X(a)$, а $e = \begin{cases} 1, & \text{если } S(1) = 0, \\ 0, & \text{в ост. случаях.} \end{cases}$

В рассматриваемом случае всегда S(1)=*0*, поэтому

$$L = p - \frac{p-1}{6}\Delta - 1. \qquad (2)$$

Далле, следующие соотношения для $p \equiv 1(\mathrm{mod}12)$, $p = A^2 + 3B^2$, $A \equiv 1(\mathrm{mod}\ 6)$ были доказаны в [5] при условии, что $ind_q\, 2 \equiv 1(\mathrm{mod}\ 3)$, то есть $B \equiv 2(\mathrm{mod}\ 3)$:

- $S_d(\alpha) = (1,0,0,0,0,0)$, если $A \equiv 1(\mathrm{mod}\ 12)$ и $B \equiv 0(\mathrm{mod}\ 12)$, например, p = 433, 601, 1801, ...
- $S_d(\alpha) = (1,1,1,0,1,1)$ если $A \equiv 7(\mathrm{mod}\ 12)$ и $B \equiv 0(\mathrm{mod}\ 12)$, например, p = 457, 1753, 1777, …
- $S_d(a) = (w,1,1,w+1,1,1)$, если $A \equiv 1(\mathrm{mod}\ 12)$ и $B \equiv 6(\mathrm{mod}\ 12)$, здесь w - корень уравнения $x^2 + x + 1$, например, p = 109, 229, 277,…
- $S_d(a) = (w,0,0,w+1,0,0)$ если $A \equiv 7(\mathrm{mod}\ 12)$ и $B \equiv 6(\mathrm{mod}\ 12)$, например, p =157, 397, 997,…
- $S_d(a) = (e, 0, e^2 + e + 1, 0, e^2, 0)$, если $A \equiv 1(\mathrm{mod}\ 12)$ и $B \equiv 8(\mathrm{mod}\ 12)$, где e - корень уравнения $f(x) = x^3 + x^2 + 1$, например, p = 193, 313, 1201, …
- $S_d(a) = (e+1, 1, e^2 + e, 1, e^2 + 1, 1)$, если $A \equiv 7(\mathrm{mod}\ 12)$ и $B \equiv 8(\mathrm{mod}\ 12)$, например, p = 241, 1153, 1249, …
- $S_d(a) = (g, g^2, g^4, g^8, g^{16}, g^{32})$, если $A \equiv 1(\mathrm{mod}\ 12)$ и $B \equiv 2(\mathrm{mod}\ 12)$, где g - корень уравнений $x^2 + ex + e^4$ или $f(x) = x^6 + x^5 + x^4 + x + 1 = (x^2 + ex + e^4)(x^2 + e^2x + e)(x^2 + e^4x + e^2)$, например, p = 13, 541, 709, …
- $S_d(a) = (g+1, g^2+1, g^4+1, g^8+1, g^{16}+1, g^{32}+1)$, если $A \equiv 7(\mathrm{mod}\ 12)$ и $B \equiv 2(\mathrm{mod}\ 12)$, где $g+1$ - корень уравнения $f(x) = x^6 + x^5 + x^4 + x^2 + 1 = (x^2 + ex + e^2)(x^2 + e^2x + e^4)(x^2 + e^4x + e)$, например, p = 37, 61, 373,…

2. Линейная сложность последовательностей на основе двух циклотомических классов

Случай, когда последовательность определена на основе одного циклотомического класса был изучен в [5], поэтому сначала рассмотрим вариант, когда последовательность формируется на основе двух циклотомических классов. Как показано в [2], линейная сложность последовательности не меняется при циклическом сдвиге номеров классов. Если I={0,3}, то (1) определяет последовательность кубических вычетов, линейная сложность которой рассмотрена в [3]. Следовательно, достаточно рассмотреть только случаи, когда I={0,1} , I={0,2}.

Теорема 1. Пусть последовательность X сформирована по (1) для I={0,1} и $p = A^2 + 3B^2$, $A \equiv 1(\mathrm{mod}\ 6)$. Тогда:

- $L = \frac{(p-1)}{3}$, если $B \equiv 0(\mathrm{mod}\ 12)$;
- $L = \frac{2(p-1)}{3}$, если $B \equiv 6(\mathrm{mod}\ 12)$;
- $L = p - 1$, если $B \not\equiv 0(\mathrm{mod}\ 6)$.

Доказательство. Рассмотрим первый случай, когда $A \equiv 1(\mathrm{mod}\ 12)$ и $B \equiv 0(\mathrm{mod}\ 12)$, тогда $S_6(a) = (1,0,0,0,0,0)$ и

$$T_X(a) = S_6(a) + DS_6(a) = (1,0,0,0,0,0) + (0,0,0,0,0,1) = (1,0,0,0,0,1).$$

Таким образом, в этом случае $\Delta = 4$ (число нулей) и утверждение теоремы следует из формулы (2).

По аналогии рассмотрим второй и последующие случаи.

Если $A \equiv 7(\mathrm{mod}\ 12)$ и $B \equiv 0(\mathrm{mod}\ 12)$,то $S_6(a) = (1,1,1,0,1,1)$ и

$T_X(a) = S_6(a) + DS_6(a) = (1,1,1,0,1,1) + (1,1,0,1,1,1) = (0,0,1,1,0,0)$, здесь, как и в первом, $\Delta = 4$. Эти случаи можно обьеденить в один, когда $B \equiv 0(\mathrm{mod}\ 12)$ и утверждении теоремы следует из (2).

Рассмотрим третий и четвертый случаи.

Если $A \equiv 1(\mathrm{mod}\ 12)$ и $B \equiv 6(\mathrm{mod}\ 12)$,то $_6(a) = (w,1,1,w+1,1,1)$ и

$T_X(a) = S_6(a) + DS_6(a) = (w,1,1,w+1,1,1) + (1,1,w+1,1,1,w) = (w+1,0,w,w,0,w+1)$, и, следовательно, $\Delta = 2$. Для четвёртого случая, когда $A \equiv 7 \pmod{12}$ и $B \equiv 6 \pmod{12}$, где $S_6(a) = (w,0,0,w+1,0,0)$ и $T_X(a) = S_6(a) + D^2 S_6(a) = (w,0,0,w+1,0,0) + (0,w+1,0,0,w,0) = (w,w+1,0,w+1,w,0)$, и число нулей, так же как и в третьем случае, в $T_X(a)$ равно $\Delta = 2$, поэтому эти два случая можно объединить в один, когда $B \equiv 6 \pmod{12}$.

Рассмотрим оставшиеся четыре случая.

Если $A \equiv 1 \pmod{12}$ и $B \equiv 8 \pmod{12}$, то $S_6(a) = (e, 0, e^2+e+1, 0, e^2, 0)$ и $T_X(a) = S_6(a) + DS_6(a) = (e,0,e^2+e+1,0,e^2,0) + (0,e^2+e+1,0,e^2,0,e) = (e,e^2+e+1,e^2+e+1,e^2,e^2,e)$, и $\Delta = 0$.

Если $A \equiv 7 \pmod{12}$ и $B \equiv 8 \pmod{12}$, то $S_6(a) = (e+1, 1, e^2+e, 1, e^2+1, 1)$ и

$T_X(a) = S_6(a) + DS_6(a) = (e+1,1,e^2+e,1,e^2+1,1) + (1,e^2+e,1,e^2+1,1,e+1) =$

$(e+1,e^2+e,e^2+e,e^2,e^2,e)$, и $\Delta = 0$.

Если $A \equiv 1 \pmod{12}$ $B \equiv 2 \pmod{12}$, то $S_6(a) = (g, g^2, g^4, g^8, g^{16}, g^{32})$ и

$T_X(a) = S_6(a) + DS_6(a) = (g,g^2,g^4,g^8,g^{16},g^{32}) + (g^2,g^4,g^8,g^{16},g^{32},g) =$

$(g^2+g, g^2+g^4, g^4+g^8, g^8+g^{16}, g^{16}+g^{32}, g^{32}+g)$, и $\Delta = 0$.

Если $A \equiv 7 \pmod{12}$ и $B \equiv 2 \pmod{12}$, то $S_6(a) = (g+1, g^2+1, g^4+1, g^8+1, g^{16}+1, g^{32}+1)$ и

$T_X(a) = S_6(a) + DS_6(a) = (g+1, g^2+1, g^4+1, g^8+1, g^{16}+1, g^{32}+1) +$

$(g^2+1, g^4+1, g^8+1, g^{16}+1, g^{32}+1, g+1) = (g^2+g, g^2+g^4, g^4+g^8, g^8+g^{16}, g^{16}+g^{32}, g^{32}+g)$, и $\Delta = 0$.

Для четырех вышеприведенных случаев видно, что число нулей в $T_X(a)$ равно $\Delta = 0$, поэтому их объединим в один при $B \not\equiv 0 \pmod{6}$ и утверждение теоремы следует из формулы (2).

Таким образом, теорема 1 доказана.

Ниже приведена таблица, поясняющая первую теорему на числовых значениях.

Таблица 1

Численные примеры для Теоремы 1.

p	*L*	*p*	*L*	*p*	*L*	*p*	*L*
433	144	457	152	109	72	157	104
601	200	1753	584	229	152	397	264
1801	600	1777	592	277	184	997	664
p	*L*	*p*	*L*	*p*	*L*	*p*	*L*
193	192	241	240	13	12	37	36
313	312	1153	1152	541	540	61	60
1201	1200	1249	1248	709	708	373	372

Результататы расчета линейной сложности по алгоритму Берлекэмпа-Месси, представленные в таблице 1, подтверждают справедливость теоремы 1.

Рассмотрим теперь последовательность для *I*={0,2}.

Теорема 2. Пусть последовательность X сформирована по (1) для *I*={0,2} и $p = A^2 + 3B^2$, $A \equiv 1 \pmod{6}$. Тогда:

- $L = \frac{(p-1)}{3}$, если $B \equiv 0 \pmod{12}$;
- $L = \frac{2(p-1)}{3}$, если $B \equiv 6 \pmod{12}$;

- $L = \dfrac{(p-1)}{2}$, если $B \equiv 8 (\mathrm{mod}\, 12)$;
- $L = p-1$, если $B \equiv 2 (\mathrm{mod}\, 12)$.

Доказательство. Рассмотрим первый случай, если $A \equiv 1 (\mathrm{mod}\, 12)$ и $B \equiv 0 (\mathrm{mod}\, 12)$, то $S_6(a) = (1,0,0,0,0,0)$ и $T_X(a) = S_6(a) + D^2 S_6(a) = (1,0,0,0,0,0) + (0,0,0,0,1,0) = (1,0,0,0,1,0)$, $\Delta = 4$.

Если $A \equiv 7 (\mathrm{mod}\, 12)$ и $B \equiv 0 (\mathrm{mod}\, 12)$, то $S_6(a) = (1,1,1,0,1,1)$ и $T_X(a) = S_6(a) + D^2 S_6(a) = (1,1,1,0,1,1) + (1,0,1,1,1,1) = (0,1,0,1,0,0)$, и в этом случае, как и в первом, $\Delta = 4$. Следовательно, для $B \equiv 0 (\mathrm{mod}\, 12)$ утверждении теоремы следует из (2).

Если $A \equiv 1 (\mathrm{mod}\, 12)$ и $B \equiv 6 (\mathrm{mod}\, 12)$, то $S_6(a) = (w,1,1,w+1,1,1)$ и $T_X(a) = S_6(a) + D^2 S_6(a) = (w,1,1,w+1,1,1) + (1,w+1,1,1,w,1) = (w+1,w,0,w,w+1,0)$, и $\Delta = 2$.

Для четвёртого случая, когда $A \equiv 7 (\mathrm{mod}\, 12)$ и $B \equiv 6 (\mathrm{mod}\, 12)$, $S_6(a) = (w,0,0,w+1,0,0)$ и $T_X(a) = S_6(a) + D^2 S_6(a) = (w,0,0,w+1,0,0) + (0,w+1,0,0,w,0) = (w,w+1,0,w+1,w,0)$, число нулей, так же как и в третьем случае, в $T_X(a)$ равно $\Delta = 2$, поэтому эти два случая можно объединить в один, когда $B \equiv 6 (\mathrm{mod}\, 12)$.

Аналогично рассматриваем оставшиеся случаи.

Если $A \equiv 1 (\mathrm{mod}\, 12)$ и $B \equiv 8 (\mathrm{mod}\, 12)$, то $S_6(a) = (e, 0, e^2+e+1, 0, e^2, 0)$ и $T_X(a) = S_6(a) + D^2 S_6(a) = (e,0,e^2+e+1,0,e^2,0) + (e^2+e+1,0,e^2,0,e,0) = (e^2+1,0,e+1,0,e^2+e,0)$, $\Delta = 3$.

Если $A \equiv 7 (\mathrm{mod}\, 12)$ и $B \equiv 8 (\mathrm{mod}\, 12)$, то $S_6(a) = (e+1, 1, e^2+e, 1, e^2+1, 1)$ и $T_X(a) = S_6(a) + D^2 S_6(a) = (e+1,1,e^2+e,1,e^2+1,1) + (e^2+e,1,e^2+1,1,e+1,1) =$
$(e^2+1,0,e+1,0,e^2+e,0)$, и $\Delta = 3$.

Пятый и шестой случаи можно объеденить в один, когда $B \equiv 8 (\mathrm{mod}\, 12)$, так как $\Delta = 3$ и утверждение теоремы следует из (2).

Если $A \equiv 1 (\mathrm{mod}\, 12)$ и $B \equiv 2 (\mathrm{mod}\, 12)$, то $S_6(a) = (g, g^2, g^4, g^8, g^{16}, g^{32})$ и $T_X(a) = S_6(a) + D^2 S_6(a) = (g,g^2,g^4,g^8,g^{16},g^{32}) + (g^4,g^8,g^{16},g^{32},g,g^2) =$
$(g+g^4, g^2+g^8, g^4+g^{16}, g^8+g^{32}, g^{16}+g, g^{32}+g^2)$, и $\Delta = 0$.

Если $A \equiv 7 (\mathrm{mod}\, 12)$ и $B \equiv 2 (\mathrm{mod}\, 12)$, то $S_6(a) = (g+1, g^2+1, g^4+1, g^8+1, g^{16}+1, g^{32}+1)$ и $T_X(a) = S_6(a) + D^2 S_6(a) = (g+1, g^2+1, g^4+1, g^8+1, g^{16}+1, g^{32}+1) +$
$(g^4+1, g^8+1, g^{16}+1, g^{32}+1, g+1, g^2+1) = (g+g^4, g^2+g^8, g^4+g^{16}, g^8+g^{32}, g^{16}+g, g^{32}+g^2)$, и $\Delta = 0$.

Седьмой и восьмой случаи тоже можно обьеденить, когда $B \equiv 2 (\mathrm{mod}\, 12)$, так как $\Delta = 0$ и утверждение теоремы следует из (2).

Теорема 2 доказана.

Ниже приведена таблица, поясняющая вторую теорему на числовых значениях.

Таблица 2

Численные примеры примеры для Теоремы 2.

p	*L*	*p*	*L*	*p*	*L*	*p*	*L*
433	144	457	152	109	72	157	104
601	200	1753	584	229	152	397	264
1801	600	1777	592	277	184	997	664
p	*L*	*p*	*L*	*p*	*L*	*p*	*L*
193	96	241	120	13	12	37	36
313	156	1153	576	541	540	61	60
1201	600	1249	624	709	708	373	372

Результататы расчета линейной сложности по алгоритму Берлекэмпа-Месси, представленные в таблице 2, подтверждают справедливость теоремы 2.

3. Линейная сложность последовательностей на основе трех циклотомических классов

Если $d = 6$ и порядок $|I| = 3$, то возможны четыре циклически независимые подмножества индексов: $I \in \{\{0,1,2\},\{0,1,3\},\{0,1,4\},\{02,4\}\}$. Вариант {0,1,4} сводится к {0,1,3} заменой q на q^{-1}. При $I = \{0,2,4\}$ получаем последовательность Лежандра, линейная сложность которой известна [6]. Таким образом, необходимо рассмотреть два варианта: *I*={0,1,2} и *I*={0,1,3}.

Теорема 3. Пусть последовательность *X* сформирована по (1) для *I*={0,1,2} . Тогда:

- $L = \dfrac{p-1}{2}$, если $B \equiv 0 (\mathrm{mod}\, 12);;$
- $L = p-1$, если $B \not\equiv 0 (\mathrm{mod}\, 12)$.

Доказательство. Рассмотрим первый случай, если $A \equiv 1 (\mathrm{mod}\, 12)$ и $B \equiv 0 (\mathrm{mod}\, 12)$, то $S_6(a) = (1,0,0,0,0,0)$ и

$$T_X(a) = S_6(a) + DS_6(a) + D^2 S_6(a) = (1,0,0,0,0,0) + (0,0,0,0,0,1) + (0,0,0,0,1,0) = (1,0,0,0,1,1).$$

Таким образом, в этом случае $\Delta = 3$.

Если $A \equiv 7 (\mathrm{mod}\, 12)$ и $B \equiv 0 (\mathrm{mod}\, 12)$, то $S_6(a) = (1,1,1,0,1,1)$ и $T_X(a) = S_6(a) + DS_6(a) + D^2 S_6(a) = (1,1,1,0,1,1) + (1,1,0,1,1,1) + (1,0,1,1,1,1) = (1,0,0,0,1,1)$, и в этом случаи, как и в первом, $\Delta = 3$, поэтому эти два случая мы обьеденим в один, когда $B \equiv 0 (\mathrm{mod}\, 12)$ и утверждении теоремы следует из (2).

Если $A \equiv 1 (\mathrm{mod}\, 12)$ и $B \equiv 6 (\mathrm{mod}\, 12)$, то $S_6(a) = (w,1,1,w+1,1,1)$ и $T_X(a) = S_6(a) + DS_6(a) + D^2 S_6(a) = (w,1,1,w+1,1,1) + (1,1,w+1,1,1,w) + (1,w+1,1,1,w,1) = (w,w+1,w+1,w+1,w,w)$, и $\Delta = 0$.

В четвертом случае, когда $A \equiv 7 (\mathrm{mod}\, 12)$ и $B \equiv 6 (\mathrm{mod}\, 12)$, где $S_6(a) = (w,0,0,w+1,0,0)$ и $T_X(a) = S_6(a) + DS_6(a) + D^2 S_6(a) = (w,0,0,w+1,0,0) + (0,0,w+1,0,0,w) + (0,w+1,0,0,w,0) = (w,w+1,w+1,w+1,w,w)$, следовательно, $\Delta = 0$.

Если $A \equiv 1 (\mathrm{mod}\, 12)$ и $B \equiv 8 (\mathrm{mod}\, 12)$, то $S_6(a) = (e, 0, e^2+e+1, 0, e^2, 0)$ и $T_X(a) = S_6(a) + DS_6(a) + D^2 S_6(a) = (e,0,e^2+e+1,0,e^2,0) + (0,e^2+e+1,0,e^2,0,e) + (e^2+e+1,0,e^2,0,e,0) = (e^2+1,e^2+e+1,e+1,e^2,e^2+e,e)$, и $\Delta = 0$.

Если $A \equiv 7 (\mathrm{mod}\, 12)$ и $B \equiv 8 (\mathrm{mod}\, 12)$, то $S_6(a) = (e+1, 1, e^2+e, 1, e^2+1, 1)$ и $T_X(a) = S_6(a) + DS_6(a) + D^2 S_6(a) = (e+1,1,e^2+e,1,e^2+1,1) + (1,e^2+e,1,e^2+1,1,e+1) + (e^2+e,1,e^2+1,1,e+1,1) = (e^2,e^2+e,e,e^2+1,e^2+e+1,e+1)$, и $\Delta = 0$.

Если $A \equiv 1 (\mathrm{mod}\, 12)$ и $B \equiv 2 (\mathrm{mod}\, 12)$, то $S_6(a) = (g, g^2, g^4, g^8, g^{16}, g^{32})$ и $T_X(a) = S_6(a) + DS_6(a) + D^2 S_6(a) = (g,g^2,g^4,g^8,g^{16},g^{32}) + (g^2,g^4,g^8,g^{16},g^{32},g) + (g^4,g^8,g^{16},g^{32},g,g^2) = (g^2+g+g^4, g^2+g^4+g^8, g^4+g^8+g^{16}, g^8+g^{16}+g^{32}, g^{16}+g^{32}+g, g^{32}+g+g^2)$, и $\Delta = 0$.

Если $A \equiv 7 (\mathrm{mod}\, 12)$ и $B \equiv 2 (\mathrm{mod}\, 12)$, то $S_6(a) = (g+1, g^2+1, g^4+1, g^8+1, g^{16}+1, g^{32}+1)$ и $T_X(a) = S_6(a) + DS_6(a) + D^2 S_6(a) = (g+1,g^2+1,g^4+1,g^8+1,g^{16}+1,g^{32}+1) + (g^2+1,g^4+1,g^8+1,g^{16}+1,g^{32}+1,g+1) + (g^4+1,g^8+1,g^{16}+1,g^{32}+1,g+1,g^2+1) = (g^2+g+g^4+1, g^2+g^4+g^8+1, g^4+g^8+g^{16}+1, g^8+g^{16}+g^{32}+1, g^{16}+g^{32}+g+1, g^{32}+g+g^2+1)$, и $\Delta = 0$.

Во всех случаях, кроме первого и второго, $\Delta = 0$. Все эти случии мы обьеденим при $B \not\equiv 0 (\mathrm{mod}\, 12)$ и утверждение теоремы следует из (2), что и тебовалось доказать.

Ниже приведена таблица, поясняющая третью теорему на числовых значениях.

Таблица 3

Численные примеры для Теоремы 3.

p	L	p	L	p	L	p	L
433	216	457	228	109	108	157	156
601	300	1753	876	229	228	397	396
1801	900	1777	888	277	276	997	996
p	L	p	L	p	L	p	L
193	192	241	240	13	12	37	36
313	312	1153	1152	541	540	61	60
1201	1200	1249	1248	709	708	373	372

Результататы расчета линейной сложности по алгоритму Берлекэмпа-Месси, представленные в таблице 3, подтверждают справедливость теоремы 3.

Рассмотрим последовательность для *I={0,1,3}.*

Теорема 4. Пусть последовательность X сформирована по (1) для *I={0,1,3}.*Тогда:

- $L = \frac{p-1}{2}$, если $B \equiv 0(\mathrm{mod}\,12)$;
- $L = \frac{2(p-1)}{3}$, если $B \equiv 6(\mathrm{mod}\,12)$;
- $L = p-1$, если $B \not\equiv 0(\mathrm{mod}\,12)$.

Доказательство. Рассмотрим первый случай, если $A \equiv 1(\mathrm{mod}\,12)$ и $B \equiv 0(\mathrm{mod}\,12)$, то $S_6(a) = (1,0,0,0,0,0)$ и

$$T_X(a) = S_6(a) + DS_6(a) + D^3S_6(a) = (1,0,0,0,0,0) + (0,0,0,0,0,1) + (0,0,0,1,0,0) = (1,0,0,1,0,1),$$

тогда $\Delta = 3$.

Если $A \equiv 7(\mathrm{mod}\,12)$ и $B \equiv 0(\mathrm{mod}\,12)$, то $S_6(a) = (1,1,1,0,1,1)$ и $T_X(a) = S_6(a) + DS_6(a) + D^3S_6(a) = (1,1,1,0,1,1) + (1,1,0,1,1,1) + (0,1,1,1,1,1) = (0,1,0,0,1,1)$, и в этом случаи, как и в первом, $\Delta = 3$, эти два случая мы обьеденим в один, когда $\mathrm{B} \equiv 0(\mathrm{mod}\,12)$ и утверждении теоремы следует из (2).

Если $A \equiv 1(\mathrm{mod}\,12)$ и $B \equiv 6(\mathrm{mod}\,12)$, то $S_6(a) = (w,1,1,w+1,1,1)$ и $T_X(a) = S_6(a) + DS_6(a) + D^3S_6(a) = (w,1,1,w+1,1,1) + (1,1,w+1,1,1,w) + (w+1,1,1,w,1,1) = (w+1,0,w,w,0,w+1)$, и $\Delta = 2$.

При $A \equiv 7(\mathrm{mod}\,12)$ и $B \equiv 6(\mathrm{mod}\,12)$, где $S_6(a) = (w,0,0,w+1,0,0)$ и $T_X(a) = S_6(a) + DS_6(a) + D^3S_6(a) = (w,0,0,w+1,0,0) + (0,0,w+1,0,0,w) + (w+1,0,0,w,0,0) = (1,0,w+1,1,0,w)$. Здесь $\Delta = 2$, поэтому этот и предыдущий случая можно обьеденить в один, когда $\mathrm{B} \equiv 6(\mathrm{mod}\,12)$.

Если $A \equiv 1(\mathrm{mod}\,12)$ и $B \equiv 8(\mathrm{mod}\,12)$, то $S_6(a) = (e, 0, e^2+e+1, 0, e^2, 0)$ и $T_X(a) = S_6(a) + DS_6(a) + D^3S_6(a) = (e,0,e^2+e+1,0,e^2,0) + (0,e^2+e+1,0,e^2,0,e) + (0,e^2,0,e,0,e^2+e+1) = (e,e+1,e^2+e+1,e^2+e,e^2,e^2+1)$, и $\Delta = 0$.

Если $A \equiv 7(\mathrm{mod}\,12)$ и $B \equiv 8(\mathrm{mod}\,12)$, то $S_6(a) = (e+1, 1, e^2+e, 1, e^2+1, 1)$ и $T_X(a) = S_6(a) + DS_6(a) + D^3S_6(a) = (e+1,1,e^2+e,1,e^2+1,1) + (1,e^2+e,1,e^2+1,1,e+1) + (1,e^2+1,1,e+1,1,e^2+e)$, и $\Delta = 0$.

Если $A \equiv 1(\mathrm{mod}\,12)$ и $B \equiv 2(\mathrm{mod}\,12)$, то $S_6(a) = \left(g, g^2, g^4, g^8, g^{16}, g^{32}\right)$ и

$T_X(a) = S_6(a) + DS_6(a) + D^3S_6(a) = \left(g, g^2, g^4, g^8, g^{16}, g^{32}\right) + \left(g^2, g^4, g^8, g^{16}, g^{32}, g\right) + \left(g^8, g^{16}, g^{32}, g, g^2, g^4\right) =$

$\left(g^2 + g + g^8, g^2 + g^4 + g^{16}, g^4 + g^8 + g^{32}, g^8 + g^{16} + g, g^{16} + g^{32} + g^2, g^{32} + g + g^4\right)$, и $\Delta = 0$.

Если $A \equiv 7(\mathrm{mod}\,12)$ и $B \equiv 2(\mathrm{mod}\,12)$, то $S_6(a) = \left(g+1, g^2+1, g^4+1, g^8+1, g^{16}+1, g^{32}+1\right)$ и

$T_X(a) = S_6(a) + DS_6(a) + D^3S_6(a) = \left(g+1, g^2+1, g^4+1, g^8+1, g^{16}+1, g^{32}+1\right)$

$+ \left(g^2+1, g^4+1, g^8+1, g^{16}+1, g^{32}+1, g+1\right) + \left(g^8+1, g^{16}+1, g^{32}+1, g+1, g^2+1, g^4+1\right) =$

$\left(g^2 + g + g^8 + 1, g^2 + g^4 + g^{16} + 1, g^4 + g^8 + g^{32} + 1, g^8 + g^{16} + g + 1, g^{16} + g^{32} + g^2 + 1, g^{32} + g + g^4 + 1\right)$, и $\Delta = 0$.

Последние случаи, с пятого по восьмой включительно, можно обьеденить в один, когда $B \not\equiv 0(\mathrm{mod}\,12)$, так как $\Delta = 0$ и утверждение теоремы следует из (2).

Теорема 4 доказана.

Ниже приведена таблица, поясняющая четвертую теорему на числовых значениях.

Таблица 4

Численные примеры для Теоремы 4.

p	*L*	*p*	*L*	*p*	*L*	*p*	*L*
433	216	457	228	109	72	157	104
601	300	1753	876	229	152	397	264
1801	900	1777	888	277	184	997	664
p	*L*	*p*	*L*	*p*	*L*	*p*	*L*
193	192	241	240	13	12	37	36
313	312	1153	1152	541	540	61	60
1201	1200	1249	1248	709	708	373	372

Результататы расчета линейной сложности по алгоритму Берлекэмпа-Месси, представленные в таблице 4, подтверждают справедливость теоремы 4.

Таким образом, значения $S_6\left(a^{q^f}\right)$, $f = \overline{0,5}$ позволили рассчитать линейную сложность шестеричной бинарной последовательности, сформулированной по (1) на основе классов шестеричных вычитов, в зависимости от разложения $p = A^2 + 3B^2$, при $B \equiv 2(\mathrm{mod}\,3)$.

Заключение

В работе было завершено исследовании, начатое в [2, 3]. Определена линейная сложность последовательностей, формируемых на основе двух и трех циклотомических классов, через разложение периода последовательности на сумму квадратов целых чисел.

1. Cusick T. W, Ding C., Renvall A. Stream Ciphers and Number Theory. Amsterdam: Elsevier, 1998. 474 p.
2. Едемский В.А. О линейной сложности двоичных последовательностей на основе классов биквадратичных и шестеричных вычетов // Дискретная математика. 2010 . Т. 22. Вып. 1 . С. 74-82.
3. Dai Z., Gong G., Song H.-Y., Ye D. Trace Representation and Linear Complexity of Binary eth Power ResidueSequences of Period p. // IEEE Trans. Inf. Theory. 2011. V. 57. P. 1530-1547.
4. Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. М.: Мир, 1987. 416 с.
5. Едемский В.А., Гантмахер В.Е. Синтез двоичных и троичных последовательностей с заданными ограничениями на их характеристики. Великий Новгород.: НовГУ, 2009. 189 с.
6. Ding C., Helleseth T., Shan W. On the linear complexity of Legendre sequences// IEEE Trans. Inform. Theory. 1998. Vol. 44. P. 1276-1278.

References

1. Cusick T. W, Ding C., Renvall A. Stream Ciphers and Number Theory. Amsterdam: Elsevier, 1998. 474 p.
2. Edemskii V.A. On the linear complexity of binary sequences on the basis of biquadratic and sextic residue classes. Discret. Math. Appl., 2010, vol. 20, no. 1, pp. 75-84.
3. Dai Z., Gong G., Song H.-Y., Ye D. Trace Representation and Linear Complexity of Binary eth Power ResidueSequences of Period p. IEEE Trans. Inf. Theory, 2011, vol. 57, pp. 1530-1547.
4. Ireland K., Rosen M. A. Classical Introduction to Modern Number Theory. Springer, Berlin, 1982. 416 p.
5. Edemskiy V.A., Gantmakher V.E. Sintez dvoichnykh i troichnykh posledovatel'nostey s zadannymi ogranicheniyami na ikh kharakteristiki. Velikiy Novgorod, NovGU, 2009. 189 p.
6. Ding C., Helleseth T., Shan W. On the linear complexity of Legendre sequences. IEEE Trans. Inform. Theory, 1998. , vol. 44, pp. 1276-1278.

Tsurina A.S. the linear complexity of sextuple binary sequences. This article presents the results of the calculation of the linear complexity of sextuple binary sequences formed on the basis of two or three cyclotomic classes. The linear complexity of the sequence is determined by the expansion of its period, the sum of squares of integers.

Keywords: linear complexity, sextuple binary sequences, cyclotomic classes.

Сведения об авторе. А.С.Цурина — студент 3 курса, Институт электронных и информационных систем НовГУ, направление «Прикладная математика и информатика», aleksandra.curina@mail.ru.

Статья публикуется впервые. Поступила в редакцию 10.12.2015.