

ВЫЧИСЛЕНИЕ СТЕПЕНИ НЕЛИНЕЙНОСТИ ФУНКЦИИ НА ЦИКЛИЧЕСКОЙ ГРУППЕ ПРИМАРНОГО ПОРЯДКА

А. В. Черемушкин

Институт криптографии, связи и информатики, г. Москва, Россия

E-mail: avc238@mail.ru

Предлагается способ вычисления степени нелинейности дискретных функций, заданных на циклической группе примарного порядка, основанный на свойствах разложения Ньютона. Найдены значения степени нелинейности для базисных функций этого разложения. Для циклических групп порядков p^2 и p^3 приводится распределение числа функций с заданным значением степени нелинейности.

Ключевые слова: дискретные функции, степень нелинейности, разложение Ньютона.

Настоящая работа является продолжением [1]. Напомним определения. Рассмотрим функции $F : G^m \rightarrow H$, где G и H — циклические группы. Для удобства будем считать, что циклические группы — это аддитивные группы колец вычетов. Всюду ниже запись $N \bmod M$ обозначает остаток от деления натурального числа N на натуральное число M , а запись (N, M) — их наибольший общий делитель. Производная по направлению $\Delta_a F$, $a \in G^m$, функции F определяется равенствами

$$\Delta_a F(x) = F(x + a) - F(x),$$

где $x \in G^m$. Степенью нелинейности функции F (обозначается $\text{dl } F$) называется минимальное натуральное число t , такое, что

$$\Delta_{a_1} \dots \Delta_{a_{t+1}} F(x) = 0$$

при всех $a_1, \dots, a_{t+1}, x \in G^m$. Если такого числа t не существует, то полагаем $\text{dl } F = \infty$. Если функция F тождественно равна нулю, то для удобства полагаем $\text{dl } F = -1$.

В работе [1] показано, что степень нелинейности у всех функций из этого множества конечна в том и только в том случае, когда $|G| = p^n$, $|H| = p^k$ при некотором простом p и натуральных $n \geq 1$ и $k \geq 1$, а также $\text{dl } F \leq m(p^n + (k-1)(p-1)p^{n-1} - 1)$ и верхняя граница степени нелинейности достигается для функций, в табличном задании которых имеется одно ненулевое значение равное 1.

Пусть D_t — множество функций со степенью нелинейности равной t :

$$D_t = \{F : \text{dl } F = t\}, \quad 1 \leq t \leq t_{\max}.$$

Из работы [1] следует, что $D_t \subseteq \text{Ker } \Delta_1^{t+1}$, в частности $D_t = \text{Ker } \Delta_1^{t+1} \setminus \text{Ker } \Delta_1^t$,

$$\text{Ker } \Delta_1^1 \subseteq \text{Ker } \Delta_1^2 \subseteq \text{Ker } \Delta_1^3 \subseteq \dots \subseteq \text{Ker } \Delta_1^{t_{\max}} \subseteq \text{Ker } \Delta_1^{t_{\max}+1}. \quad (1)$$

¹Заметим, что в формулировке [1, теорема 1] допущена неточность: в условии пропущены слова «для любой функции» степень нелинейности конечна. Следует также заметить, что свойства значений биномиальных коэффициентов по примарному модулю, приведённые в [1], могут быть выведены в качестве следствия из обобщённой теоремы Люка [2].

Если F — такая функция, что $\Delta_1^{t_{\max}} F \neq 0$, то функции $\Delta_1^{t_{\max}-t} F \neq 0$ имеют степень нелинейности t . Поэтому классы D_t при всех числах t из интервала $1 \leq t \leq t_{\max}$ не являются пустыми, и в цепочке (1) все включения являются строгими.

В данной работе рассматриваются подходы к описанию классов D_t на основе разложения Ньютона.

Пусть $n = k \geq 2$ и $m \geq 1$. Как известно, всякую функцию $F : \mathbb{Z}_{p^n}^m \rightarrow \mathbb{Z}_{p^n}$ можно представить в виде

$$F(x_1, \dots, x_m) = \sum_{i_1, \dots, i_m=0}^{n-1} h(i_1, \dots, i_m) \binom{x_1}{i_1} \cdots \binom{x_m}{i_m} \mod p^n, \quad (2)$$

где $0 \leq h(i_1, \dots, i_m) \leq p^n - 1$, $0 \leq i_1, \dots, i_m \leq p^n - 1$, и $\binom{x}{i} = \frac{x(x-1)\cdots(x-i+1)}{i!}$

при $0 < i \leq p^n - 1$ и $\binom{x}{0} = 1$.

Подсчитаем степени нелинейности для базисных функций, входящих в это разложение. Пусть

$$F_i(x) = \binom{x}{i} \mod p^n,$$

$x \in \mathbb{Z}_{p^n}$, $0 \leq i \leq p^n - 1$.

Для дальнейшего потребуются следующие простые свойства.

Свойство 1. Если $\text{dl } F > \text{dl } F'$, то $\text{dl } (F \pm F') = \text{dl } F$.

Свойство 2. Пусть $m \geq 1$ и $F : G^m \rightarrow H$, где G и H — циклические группы порядков p^n и p^k соответственно, $n \geq 2$ и $k \geq 2$. Если $k > s \geq 1$ и функция F имеет максимальную степень нелинейности $\text{dl } F = m(p^n + (k-1)(p-1)p^{n-1} - 1)$, то степень нелинейности функции $F' : G^m \rightarrow H$ вида $F'(x) = p^s F(x) \mod p^k$ не превосходит величины

$$\text{dl } F' \leq m(p^n + (k-s-1)(p-1)p^{n-1} - 1). \quad (3)$$

Действительно, в силу изоморфизма колец $p^s \mathbb{Z}_{p^k} \cong \mathbb{Z}_{p^{k-s}}$ функцию F' можно рассматривать как функцию $F' : G^m \rightarrow H'$, где H' — циклическая группа порядка p^{k-s} . Поэтому степень нелинейности функции F' не превосходит максимальной степени нелинейности для функций такого вида, которая в точности равна указанной величине. (Далее будет показано, что при $k = n$ в (3) выполняется равенство.)

Свойство 3. Функция $F_{p^n-1}(x) = \binom{x}{p^n-1} \mod p^n$ при $x \in \mathbb{Z}_{p^n}$ принимает значение 1 только при $x = p^n - 1$, а в остальных точках равна нулю. Поэтому она имеет максимальную степень нелинейности $p^n + (n-1)(p-1)p^{n-1} - 1$.

Это утверждение является прямым следствием способа доказательства теоремы 2 из [1]. Еще одним следствием этой теоремы является

Свойство 4. Пусть $m \geq 1$ и G и H — циклические группы порядков p^n и p^k соответственно, $1 \leq s < k \leq n$. Тогда функция $F : G^m \rightarrow H$ вида

$$F(x_1, \dots, x_m) = p^s \binom{x_1}{p^n-1} \cdots \binom{x_m}{p^n-1} \mod p^k$$

имеет степень нелинейности $m(p^n + (k-s-1)(p-1)p^{n-1} - 1)$.

Действительно, при $x_1 = \dots = x_m = p^n - 1$ функция F принимает значение p^s , а в остальных точках равна нулю. Если теперь функцию F рассматривать как функцию $F' : G^m \rightarrow H'$, где H' — циклическая группа порядка p^{k-s} , то она будет иметь единственное ненулевое значение равное 1. Поэтому она имеет максимальную степень нелинейности.

Лемма 1. Пусть $M \geq 2$ — натуральное число и

$$F_i(x) = \binom{x}{i} \pmod{M},$$

$x \in \mathbb{Z}_M$, $0 \leq i \leq M-1$. Тогда при $1 \leq i \leq M-1$ и $x \in \mathbb{Z}_M$ выполняется тождество

$$\Delta_1 F_i \equiv F_{i-1} - F_i(M) F_{M-1} \pmod{M}. \quad (4)$$

Доказательство. В силу целочисленного тождества

$$\Delta_1 \binom{x}{i} \equiv \binom{x}{i-1}, \quad x > i \geq 1,$$

при $0 \leq x < M-1$ имеем

$$\Delta_1 F_i(x) \equiv F_i((x+1) \pmod{M}) - F_i(x) \equiv F_i(x+1) - F_i(x) \equiv F_{i-1}(x) \pmod{M}.$$

Для $x = M-1$ получаем

$$\begin{aligned} \Delta_1 F_i(M-1) &\equiv F_i(0) - F_i(x) \equiv F_i(M) - F_i(M-1) + F_i(0) - F_i(M) \equiv \\ &\equiv F_{i-1}(M-1) - F_i(M) \pmod{M}. \end{aligned}$$

Так как функция $F_{M-1}(x)$ принимает значение 1 только при $x = M-1$, а в остальных точках равна нулю, то эти равенства можно переписать в виде (4). ■

Лемма 2. Пусть $n \geq 2$, p простое и $1 \leq i \leq p^n - 1$. Тогда значения производных функции $F_i(x) = \binom{x}{i} \pmod{p^n}$ при $1 \leq x \leq p^n - 1$ удовлетворяют равенствам

$$\Delta_1 \binom{x}{i} \equiv \begin{cases} \binom{x}{i-1} \pmod{p^n}, & \text{если } (p^n, i) = 1, \\ \binom{x}{i-1} - \binom{p^n}{i} \binom{x}{p^n-1} \pmod{p^n}, & \text{если } (p^n, i) \neq 1. \end{cases}$$

Доказательство вытекает из того факта, что $\binom{p^n}{i} \pmod{p^n} \neq 0$ только при $(p^n, i) \neq 1$ (см., например, [1, лемма 1]).

Теорема 1. Пусть $n \geq 1$ и p простое. Тогда степень нелинейности функции $F_i(x) = \binom{x}{i} \pmod{p^n}$, $1 \leq i \leq p^n - 1$, равна

$$\text{dl } F_i = \begin{cases} i + (t-1)(p-1)p^{n-1} + p^n - p^t, & \text{если } p^t \leq i \leq p^{t+1} - 1, \quad 1 \leq t \leq n-1, \\ i, & \text{если } 1 \leq i \leq p-1. \end{cases}$$

Доказательство. Определим рекурсивно семейство деревьев $D_p(n, k)$, $k = 1, 2, \dots$. При $k = 1$ дерево $D_p(n, 1)$ представляет собой цепь с вершинами, помеченными последовательно числами $0, 1, \dots, p^n - 1$, и корнем в вершине с пометкой $p^n - 1$. Если деревья при $k = 1, 2, \dots, t-1$ уже построены, то дерево $D_p(n, t)$ получается из дерева $D_p(n, 1)$ путём присоединения к каждой вершине с пометкой вида $p^s a$, $(a, p) = 1$, при $1 \leq s \leq t-1$ ребра, соединяющего эту вершину с корнем дерева $D_p(n, s)$ (см. рис. 1).

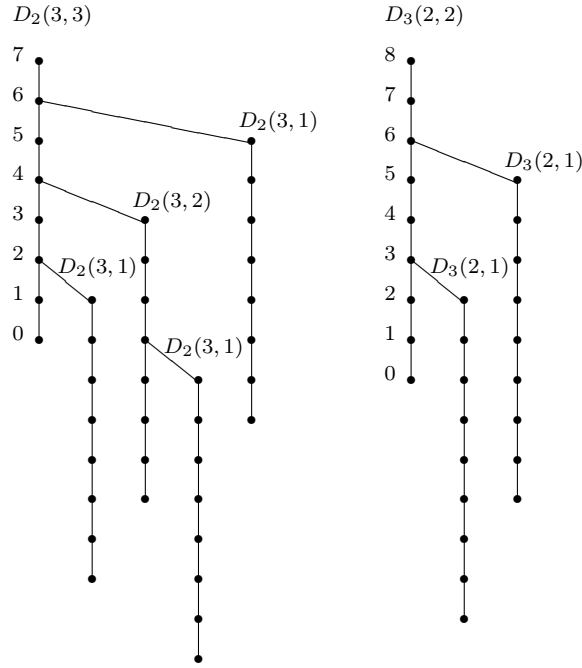


Рис. 1. Деревья $D_2(3, 3)$ и $D_3(2, 2)$

В терминах свойств этого дерева удобно интерпретировать значения степеней нелинейности. Поставим в соответствие i -й вершине исходного дерева $D_p(n, 1)$ биномиальный коэффициент $\binom{x}{i}$. Тогда переходу от вершины i к $i-1$ в дереве $D_p(n, k)$ соответствует взятие производной Δ_1 , причём точкам присоединения деревьев соответствует появление дополнительных слагаемых, возникающих в соответствии с формулой

$$\Delta_1 \binom{x}{i} \equiv \binom{x}{i-1} - \binom{p^n}{i} \binom{x}{p^n-1} \pmod{p^k}.$$

Нетрудно видеть, что степень нелинейности функции $\binom{x}{i} \pmod{p^k}$ при $x \in \mathbb{Z}_n$ равна высоте поддерева с корнем в вершине i , т. е. длине максимального пути от i -й вершины до листьев дерева $D_p(n, k)$.

Рассмотрим теперь дерево $D_p(n, n)$ и вычислим значения $\text{dl } F_i$, $1 \leq i \leq p^n - 1$. Воспользуемся индукцией по t . При $t = 0$ все значения i из интервала $0 \leq i \leq p - 1$ взаимно просты с p , $(i, p) = 1$. По лемме 2 получаем $\text{dl } F_{i-1} = \text{dl } F_i - 1$. Так как при $i = 1$ имеем $\text{dl } F_1 = 1$, то для значений i в этом интервале выполнено равенство $\text{dl } F_i = i$.

Предположим, что для значений t , меньших s , равенство выполняется. Докажем его для $t = s$. В силу лемм 5 и 6 из [1] достаточно рассмотреть случай, когда используется только производная Δ_1 , так как остальные производные могут быть выражены через неё. При $i = p^s$ имеем

$$\Delta_1 F_{p^s}(x) \equiv \Delta_1 \binom{x}{p^s} \equiv \binom{x}{p^s - 1} - \binom{p^n}{p^s} \binom{x}{p^n - 1} \pmod{p^n}.$$

В силу леммы 1 из [1] и того факта, что умножение на обратимый элемент не изменяет значения степени нелинейности функции, получаем

$$\text{dl} \left[\binom{p^n}{p^s} \binom{x}{p^n - 1} \right] = \text{dl} \left[p^{n-s} \binom{x}{p^n - 1} \right].$$

Это значение совпадает с высотой дерева $D_p(n, s)$ и в силу свойства 4 равно

$$\text{dl} \left[p^{n-s} \binom{x}{p^n - 1} \right] = p^n + (s - 1)(p - 1)p^{n-1} - 1.$$

По предположению индукции

$$\text{dl} \binom{x}{p^s - 1} = p^s - 1 + (s - 2)(p - 1)p^{n-1} + p^n - p^{s-1}.$$

Значит, по свойству 1 имеем $\text{dl} F_{p^s} = p^n + (s - 1)(p - 1)p^{n-1}$.

Рассмотрим теперь случай $p^s < i \leq p^{s+1} - 1$. В этом интервале встречаются только числа вида $i = p^r a$, $(p, a) = 1$, при $r \leq s$. В графе $D_p(n, n)$ точке $i = p^r a$ при $r \geq 1$ соответствует присоединение к дереву $D_p(n, 1)$ дерева $D_p(n, r)$. Так как все такие вершины находятся выше вершины с пометкой p^s , а высота дерева $D_p(n, r)$ не превосходит высоты дерева $D_p(n, s)$, то присоединение этих деревьев не изменит длину максимального пути от i -й вершины до листьев дерева $D_p(n, n)$, который будет проходить через вершину с пометкой p^s . Значит, $\text{dl} F_i = \text{dl} F_{p^s} + i - p^s = p^n + (s - 1)(p - 1)p^{n-1} + i - p^s$. ■

Следствие 1. Пусть $n \geq 1$, p простое. Тогда для степеней нелинейности функций $F_i(x) = \binom{x}{i} \pmod{p^n}$, $1 \leq i \leq p^n - 1$, выполняются равенства

$$\text{dl} F_i - \text{dl} F_{i-1} = \begin{cases} (p - 1)p^{n-1} + p^t - p^{t+1}, & \text{если } i = p^t, \quad 1 \leq t \leq n - 1, \\ 1, & \text{если } i \neq p^t, \quad 1 \leq t \leq n - 1. \end{cases}$$

Следствие 2. Пусть $n \geq 1$, $p \geq 2$ и разложение функции $F : \mathbb{Z}_{p^n} \rightarrow \mathbb{Z}_{p^n}$ имеет вид

$$F(x) = \sum_{i=0}^{p^n-1} a_i \binom{x}{i} \pmod{p^n}.$$

Тогда следующие условия эквивалентны:

- 1) функция F имеет максимальную степень нелинейности;
- 2) коэффициент a_{p^n-1} обратим в кольце $\mathbb{Z}_{p^n}$, т. е. $(a_{p^n-1}, p) = 1$;
- 3) сумма значений функции F является обратимым элементом в кольце $\mathbb{Z}_{p^n}$:

$$\left(\sum_{x=0}^{p^n-1} F(x) \pmod{p^n}, p \right) = 1.$$

Доказательство. Эквивалентность первого и второго условий вытекает из теоремы 1 и свойства 1. Для доказательства эквивалентности второго и третьего условий воспользуемся следующим свойством суммы биномиальных коэффициентов:

$$\sum_{i=0}^x \binom{i}{y} = \binom{x+1}{y+1},$$

справедливым при всех $x \geq y \geq 0$. Его доказательство легко проводится индукцией по x :

$$\sum_{i=0}^x \binom{i}{y} = \sum_{i=0}^{x-1} \binom{i}{y} + \binom{x}{y} = \binom{x}{y+1} + \binom{x}{y} = \binom{x+1}{y+1}.$$

С помощью этого равенства получаем

$$\sum_{i=0}^{p^n-1} \binom{x}{i} = \binom{p^n}{i+1} \equiv \begin{cases} 0 & (\text{mod } p^n), \quad 0 \leq i \leq p^n - 2, \\ 1 & (\text{mod } p^n), \quad i = p^n - 1, \end{cases}$$

откуда $\sum_{x=0}^{p^n-1} F(x) \equiv a_{p^n-1} \pmod{p^n}$. ■

Следствие 3. Пусть $m \geq 2$, $n \geq 1$, $p \geq 2$ и разложение функции $F : \mathbb{Z}_{p^n}^m \rightarrow \mathbb{Z}_{p^n}$ имеет вид (2). Тогда следующие условия эквивалентны:

1) функция F имеет максимальную степень нелинейности равную

$$\text{dl } F = m(p^n + (k-1)(p-1)p^{n-1} - 1);$$

2) коэффициент $h(p^n - 1, \dots, p^n - 1)$ обратим в кольце $\mathbb{Z}_{p^n}$, т. е.

$$(h(p^n - 1, \dots, p^n - 1), p) = 1;$$

3) сумма значений функции F является обратимым элементом в кольце $\mathbb{Z}_{p^n}$:

$$\left(\sum_{x_1, \dots, x_m} F(x_1, \dots, x_m) \pmod{p^n}, p \right) = 1.$$

Доказательство проводится полностью аналогично.

Следствие 4. Пусть $m \geq 1$ и $F : \mathbb{Z}_{p^n}^m \rightarrow \mathbb{Z}_{p^n}$, где $n \geq 2$. Если $n > s \geq 1$ и функция F имеет максимальную степень нелинейности $m(p^n + (n-1)(p-1)p^{n-1} - 1)$, то степень нелинейности функции $F' : G^m \rightarrow H$ вида $F'(x) = p^s F(x) \pmod{p^n}$ равна

$$\text{dl } F' = m(p^n + (n-s-1)(p-1)p^{n-1} - 1).$$

Доказательство. Рассмотрим разложение Ньютона функции F вида (2). В силу следствия 3 и свойства 1 можно считать, что функция F имеет в своём задании единственное ненулевое значение, причём оно должно быть взаимно просто с p . Пусть, например, $F(0) = 1$ (в противном случае можно перейти к функции $F'' = F(0)^{-1} F \pmod{p^n}$). Значит, у функции $F'(x)$ также одно ненулевое значение $F'(0) = p^s$. При гомоморфизме $\mathbb{Z}_{p^n} \rightarrow \mathbb{Z}_{p^{n-s}}$ элементу p^s соответствует элемент $1 \in \mathbb{Z}_{p^{n-s}}$. Поэтому для степени нелинейности функции $F'(x)$ в неравенстве (3) на самом деле должно стоять равенство. ■

Следствие 5. При $n \geq 1$, $p \geq 2$ число функций максимальной степени нелинейности среди функций вида $F : \mathbb{Z}_{p^n} \rightarrow \mathbb{Z}_{p^n}$ равно

$$|D_{t_{\max}}| = \varphi(p^n)p^{n(p^n-1)} = (p-1)p^{np^n-1} = \left(1 - \frac{1}{p}\right)p^{np^n}.$$

Следствие 6. При $m \geq 1$, $n \geq 1$, $p \geq 2$ число функций максимальной степени нелинейности среди функций вида $F : \mathbb{Z}_{p^m}^n \rightarrow \mathbb{Z}_{p^n}$ равно

$$|D_{t_{\max}}| = \varphi(p^n)p^{n(p^{mn}-1)} = (p-1)p^{np^{mn}-1} = \left(1 - \frac{1}{p}\right)p^{np^{mn}}.$$

Следствие 7. Пусть $n \geq 2$, $p \geq 2$. Тогда число функций степени нелинейности i при $0 \leq i \leq p-1$ среди функций вида $F : \mathbb{Z}_{p^n} \rightarrow \mathbb{Z}_{p^n}$ равно

$$|D_i| = (p^n - 1)p^{ni}.$$

Следствие 8. Пусть $n \geq 2$, $p \geq 2$. Тогда число функций степени нелинейности $t_{\max} - i$ при $1 \leq i \leq p-1$ среди функций вида $F : \mathbb{Z}_{p^n} \rightarrow \mathbb{Z}_{p^n}$ равно

$$|D_{t_{\max}-i}| = (p-1)p^{np^n-i-1}.$$

Доказательство. В силу следствия 3 при $i = 1$

$$\text{dl} \left[p \binom{x}{p^n-1} \right] = p^n + (n-2)(p-1)p^{n-1} - 1.$$

Поскольку при $n \geq 2$ выполняется неравенство

$$\text{dl} \left[p \binom{x}{p^n-1} \right] \leq p^n + (n-2)(p-1)p^{n-1} - 1 < p^n + (n-1)(p-1)p^{n-1} - 2 = \text{dl} \left(\binom{x}{p^n-2} \right),$$

то в этот класс попадают только функции, у которых в разложении Ньютона коэффициент при $\binom{x}{p^n-2}$ взаимно прост с p , а коэффициент при $\binom{x}{p^n-1}$ кратен p . Число таких функций равно

$$(p-1)p^{2(n-1)}p^{n(p^n-2)} = (p-1)p^{np^n-2}.$$

Далее для $2 \leq i \leq p-1$ можно воспользоваться индукцией. ■

Пример 1. Пусть $G = H = \mathbb{Z}_4$. Подсчитаем число функций $F : G \rightarrow H$ для каждого возможного значения степени нелинейности. Всего имеется 256 таких функций. Рассмотрим разложение Ньютона функции F

$$F(x) = a_0 + a_1 \binom{x}{1} + a_2 \binom{x}{2} + a_3 \binom{x}{3} \pmod{4}, \quad a_i \in \mathbb{Z}_4, \quad 0 \leq i \leq 3.$$

С помощью теоремы 1 и следствия 3 подсчитаем степени нелинейности функций $2^i \binom{x}{j} \pmod{2^2}$, $0 \leq i \leq 1$, $2 \leq j \leq 3$ (табл. 1):

Т а б л и ц а 1

i	$\binom{x}{2}$	$\binom{x}{3}$
0	4	5
1	2	3

Пользуясь табл. 1, найдём возможные значения коэффициентов разложения Ньютона для каждого значения степени нелинейности (табл. 2):

Т а б л и ц а 2

$\text{dl } F$	a_0	a_1	a_2	a_3	Число F
5	*	*	*	1,3	128
4	*	*	1,3	2	64
3	*	*	0,2	2	32
2	*	*	2	0	16
1	*	1-3	0	0	12
0	1-3	0	0	0	3
-1	0	0	0	0	1

П р и м е ч а н и е. Символ «*» означает, что соответствующий коэффициент может принимать любое значение из $\mathbb{Z}_4$.

Пример 2. Для $G = H = \mathbb{Z}_9$ уже будет 387 420 489 функций. Рассмотрим разложение Ньютона функции F :

$$F(x) = a_0 + a_1 \binom{x}{1} + a_2 \binom{x}{2} + \dots + a_8 \binom{x}{8} \pmod{9}, \quad a_i \in \mathbb{Z}_9.$$

С помощью теоремы 1 и следствия 3 находим степени нелинейности функций $3^i \binom{x}{j} \pmod{3^2}$, $0 \leq i \leq 1$, $2 \leq j \leq 8$ (табл. 3, см. также рис. 1):

Т а б л и ц а 3

i	$\binom{x}{2}$	$\binom{x}{3}$	$\binom{x}{4}$	$\binom{x}{5}$	$\binom{x}{6}$	$\binom{x}{7}$	$\binom{x}{8}$
0	2	9	10	11	12	13	14
1	2	3	4	5	6	7	8

Теперь выпишем возможные значения коэффициентов разложения Ньютона для каждого значения степени нелинейности (табл. 4):

Т а б л и ц а 4

dl F	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	Число F
14	*	*	*	*	*	*	*	*	$\neg 0,3,6$	258 280 326
13	*	*	*	*	*	*	*	$\neg 0,3,6$	0,3,6	86 093 442
12	*	*	*	*	*	*	$\neg 0,3,6$	0,3,6	0,3,6	28 697 814
11	*	*	*	*	*	$\neg 0,3,6$	0,3,6	0,3,6	0,3,6	9 565 938
10	*	*	*	*	$\neg 0,3,6$	0,3,6	0,3,6	0,3,6	0,3,6	3 188 646
9	*	*	*	$\neg 0,3,6$	0,3,6	0,3,6	0,3,6	0,3,6	0,3,6	1 062 882
8	*	*	*	0,3,6	0,3,6	0,3,6	0,3,6	0,3,6	3,6	354 294
7	*	*	0,3,6	0,3,6	0,3,6	0,3,6	0,3,6	3,6	0	118 098
6	*	*	0,3,6	0,3,6	0,3,6	0,3,6	3,6	0	0	39 366
5	*	*	0,3,6	0,3,6	0,3,6	3,6	0	0	0	13 122
4	*	*	0,3,6	0,3,6	3,6	0	0	0	0	4 374
3	*	*	*	3,6	0	0	0	0	0	1 458
2	*	*	1-8	0	0	0	0	0	0	648
1	*	1-8	0	0	0	0	0	0	0	72
0	1-8	0	0	0	0	0	0	0	0	8
-1	0	0	0	0	0	0	0	0	0	1

П р и м е ч а н и е. Обозначение « $\neg 0,3,6$ » использовано для множества $\{1, 2, 4, 5, 7, 8\}$.

Данный пример можно обобщить следующим образом.

Теорема 2. Пусть $p \geq 2$. Тогда число функций степени нелинейности i среди функций вида $F : G \rightarrow H$, $G = H = \mathbb{Z}_{p^2}$, равно

$$|D_i| = \begin{cases} 1, & \text{если } i = -1, \\ p^{2i}(p^2 - 1), & \text{если } 0 \leq i \leq p - 1, \\ p^{i+p}(p - 1), & \text{если } p \leq i \leq p^2 + (p - 1)p - 1. \end{cases}$$

Доказательство вытекает из табл. 5 со значениями степеней нелинейности функций $p^i \binom{x}{j} \bmod p^2$, $0 \leq i \leq 1$, $2 \leq j \leq p^2 - 1$.

Т а б л и ц а 5

i	$\binom{x}{2}$	$\dots$	$\binom{x}{p-1}$	$\binom{x}{p}$	$\binom{x}{p+1}$	$\dots$	$\binom{x}{p^2-1}$
0	2	$\dots$	$p-1$	p^2	p^2+1	$\dots$	$p^2 + (p-1)p - 1$
1	2	$\dots$	$p-1$	p	$p+1$	$\dots$	$p^2 - 1$

Пример 3. Для $G = H = \mathbb{Z}_8$ имеется 16 777 216 функций. Рассмотрим разложение Ньютона функции F :

$$F(x) = a_0 + a_1 \binom{x}{1} + a_2 \binom{x}{2} + \dots + a_7 \binom{x}{7} \bmod 8, \quad a_i \in \mathbb{Z}_8.$$

Выпишем степени нелинейности функций $2^i \binom{x}{j} \bmod 2^3$, $0 \leq i \leq 2$, $2 \leq j \leq 7$ (табл. 6, см. также рис. 1):

Т а б л и ц а 6

i	$\binom{x}{2}$	$\binom{x}{3}$	$\binom{x}{4}$	$\binom{x}{5}$	$\binom{x}{6}$	$\binom{x}{7}$
2^0	8	9	12	13	14	15
2^1	2	3	8	9	10	11
2^2	2	3	4	5	6	7

Отсюда вытекают возможные значения коэффициентов разложения Ньютона для каждого значения степени нелинейности (табл. 7):

Т а б л и ц а 7

dl F	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	Число F
15	*	*	*	*	*	*	*	1,3,5,7	8 388 608
14	*	*	*	*	*	*	1,3,5,7	0,2,4,6	4 194 304
13	*	*	*	*	*	1,3,5,7	0,2,4,6	0,2,4,6	2 097 152
12	*	*	*	*	1,3,5,7	0,2,4,6	0,2,4,6	0,2,4,6	1 048 576
11	*	*	*	*	0,2,4,6	0,2,4,6	0,2,4,6	2,6	524 288
10	*	*	*	*	0,2,4,6	0,2,4,6	2,6	0,4	262 144
9	*	*	*	*	0,2,4,6	2,6	0,4	0,4	131 072
9	*	*	*	1,3,5,7	0,2,4,6	0,4	0,4	0,4	65 536
8	*	*	*	0,2,4,6	2,6	0,4	0,4	0,4	32 768
8	*	*	1,3,5,7	0,2,4,6	0,4	0,4	0,4	0,4	16 384
7	*	*	0,2,4,6	0,2,4,6	0,4	0,4	0,4	4	8 192
6	*	*	0,2,4,6	0,2,4,6	0,4	0,4	4	0	4 096
5	*	*	0,2,4,6	0,2,4,6	0,4	4	0	0	2 048
4	*	*	0,2,4,6	0,2,4,6	4	0	0	0	1 024
3	*	*	0,2,4,6	2,4,6	0	0	0	0	768
2	*	*	2,4,6	0	0	0	0	0	192
1	*	1-7	0	0	0	0	0	0	56
0	1-7	0	0	0	0	0	0	0	7
-1	0	0	0	0	0	0	0	0	1

Этот пример также можно обобщить в виде следующей теоремы.

Теорема 3. Пусть $p \geq 2$. Тогда число функций степени нелинейности i среди функций вида $F : G \rightarrow H$, $G = H = \mathbb{Z}_{p^3}$, равно

$$|D_i| = \begin{cases} 1, & \text{если } i = -1, \\ p^{3i}(p^3 - 1), & \text{если } 0 \leq i \leq p - 1, \\ p^{2i+p}(p^2 - 1), & \text{если } p \leq i \leq p^2 - 1, \\ p^{i+p^2+p}(p - 1), & \text{если } p^2 \leq i \leq p^3 - 1, \\ p^{2i-p^3+p^2+p}(p^2 - 1), & \text{если } p^3 \leq i \leq p^3 + p^2 - p - 1, \\ p^{i+2p^2}(p - 1), & \text{если } p^3 + p^2 - p \leq i \leq p^3 + 2(p - 1)p^2 - 1. \end{cases}$$

Доказательство вытекает из табл. 8 со значениями степеней нелинейности функций $p^i \binom{x}{j} \bmod p^3$, $0 \leq i \leq 2$, $2 \leq j \leq p^3 - 1$:

Т а б л и ц а 8

i	$\binom{x}{2}$	$\dots$	$\binom{x}{p-1}$	$\binom{x}{p}$	$\dots$	$\binom{x}{p^2-1}$	$\binom{x}{p^2}$	$\dots$	$\binom{x}{p^3-1}$
0	2	$\dots$	$p-1$	p^3	$\dots$	$p^3 + p^2 - p - 1$	$p^2 + 2(p-1)p^2$	$\dots$	$p^3 + 2(p-1)p^2 - 1$
1	2	$\dots$	$p-1$	p	$\dots$	$p^2 - 1$	p^3	$\dots$	$p^3 + (p-1)p^2 - 1$
2	2	$\dots$	$p-1$	p	$\dots$	$p^2 - 1$	p^2	$\dots$	$p^3 - 1$

Теперь нетрудно выписать возможные значения коэффициентов разложения Ньютона для каждого значения степени нелинейности (табл. 9):

Т а б л и ц а 9

$\text{dl } F$	$a_0 \dots a_{p-1}$	a_p	$\dots$	a_{p^2-1}	a_{p^2}	$\dots$	a_{2p^2-p-1}	a_{2p^2-p}	$\dots$	a_{p^3-1}	Число F
$p^3 + 2(p-1)p^2 - 1$	$\dots$	$*$	$\dots$	$*$	$*$	$\dots$	$*$	$*$	$\dots$	n	$p^{3p^3-1}(p-1)$
$p^3 + 2(p-1)p^2 - 2$	$\dots$	$*$	$\dots$	$*$	$*$	$\dots$	$*$	$*$	$\dots$	p	$p^{3p^3-2}(p-1)$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$p^3 + p^2 - p$	$\dots$	$*$	$\dots$	$*$	$*$	$\dots$	$*$	n	$\dots$	p	$p^{p^3+3p^2-p}(p-1)$
$p^3 + p^2 - p - 1$	$\dots$	$*$	$\dots$	$*$	p	$\dots$	$!p$	p^2	$\dots$	p^2	$p^{p^3+3p^2-p-2}(p-1)$
$p^3 + p^2 - p - 1$	$\dots$	$*$	$\dots$	n	p	$\dots$	p^2	p^2	$\dots$	p^2	$p^{p^3+3p^2-p-3}(p-1)$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
p^3	$\dots$	$*$	$\dots$	p	$!p$	$\dots$	p^2	p^2	$\dots$	p^2	$p^{p^3+p^2+p+1}(p-1)$
p^3	$\dots$	n	$\dots$	p	p^2	$\dots$	p^2	p^2	$\dots$	p^2	$p^{p^3+p^2+p}(p-1)$
$p^3 - 1$	$\dots$	$*$	$\dots$	p	p	$\dots$	p	p^2	$\dots$	$!p^2$	$p^{p^3+p^2+p-1}(p-1)$
$p^3 - 2$	$\dots$	$*$	$\dots$	p	p	$\dots$	p	p^2	$\dots$	0	$p^{p^3-2p^2-p-2}(p-1)$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$2p^2 - p$	$\dots$	p	$\dots$	p	p	$\dots$	p	$!p^2$	$\dots$	0	$p^{4p^2-2p}(p-1)$
$2p^2 - p - 1$	$\dots$	p	$\dots$	p	p	$\dots$	$!p^2$	0	$\dots$	0	$p^{4p^2-2p-1}(p-1)$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$p^2 + 1$	$\dots$	p	$\dots$	p	p	$\dots$	0	0	$\dots$	0	$p^{2p^2+p+1}(p-1)$
p^2	$\dots$	p	$\dots$	p	$!p^2$	$\dots$	0	0	$\dots$	0	$p^{2p^2+p}(p-1)$
$p^2 - 1$	$\dots$	p	$\dots$	$p \setminus 0$	0	$\dots$	0	0	$\dots$	0	$p^{2p^2+p-2}(p^2-1)$
$p^2 - 2$	$\dots$	p	$\dots$	0	0	$\dots$	0	0	$\dots$	0	$p^{2p^2+p-4}(p^2-1)$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$p+1$	$\dots$	p	$\dots$	0	0	$\dots$	0	0	$\dots$	0	$p^{3p+2}(p^2-1)$
p	$\dots$	$p \setminus 0$	$\dots$	0	0	$\dots$	0	0	$\dots$	0	$p^{3p}(p^2-1)$
$p-1$	$\dots \neq 0$	0	$\dots$	0	0	$\dots$	0	0	$\dots$	0	$p^{3(p-1)}(p^3-1)$
$p-2$	$\dots 0$	0	$\dots$	0	0	$\dots$	0	0	$\dots$	0	$p^{3(p-2)}(p^3-1)$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
0	$\neq 0 \dots 0$	0	$\dots$	0	0	$\dots$	0	0	$\dots$	0	$p^3 - 1$
-1	$0 \dots 0$	0	$\dots$	0	0	$\dots$	0	0	$\dots$	0	1

П р и м е ч а н и е. $*$ — произвольное значение; p — кратные p ; p^2 — кратные p^2 ; $!p$ — кратные p , но не p^2 , без нуля; $!p^2$ — кратные p^2 без нуля; $p \setminus 0$ — кратные p без нуля; $\neq 0$ — произвольное значение, не равное нулю.

ЛИТЕРАТУРА

1. Черемушкин А. В. Аддитивный подход к определению степени нелинейности дискретной функции на циклической группе примарного порядка // Прикладная дискретная математика. 2013. № 2(20). С. 26–38.
2. Granville A. Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers // Organic Math. (Burnaby, BC, 1995), CMS Conf. Proc., 20, Amer. Math. Soc., Providence, RI, 1997. P. 253–276.