УДК 512.541

ПОПОВ Иван Николаевич*, кандидат физико-математических наук, доцент кафедры математики института математики, информационных и космических технологий Северного (Арктического) федерального университета имени М.В. Ломоносова. Автор 36 научных публикаций*

СЛОЖЕНИЕ ⊕ НА МНОЖЕСТВЕ НЕОТРИЦАТЕЛЬНЫХ ЦЕЛЫХ ЧИСЕЛ

В работе рассматривается пример абелевой группы, с неотрицательными целыми числами в качестве элементов, и операцией, которая основывается на представлении натурального числа в виде суммы степеней фиксированного числа. Показывается, что построенная группа содержит подгруппы конечного и бесконечного порядков. Используя графическое представление линейных отображений конечных подгрупп группы, предлагается способ нахождения их подгрупп.

Ключевые слова: *группа, подгруппу, конечные группы, порядок группы, порядок элемента группы, отображения групп на себя.*

Разнообразие примеров групп очень велико. Изучались и продолжаются изучаться числовые группы, симметрическая группа (группа подстановок), матричные группы и так далее в различных направлениях (например, описание строения и свойств группы и ее подгрупп, особых элементов группы). В источниках [1] и [2] изложены классические вопросы теории групп.

Множество неотрицательных чисел обозначим символом N_0. Символом a обозначим натуральное число, большее 1. Остаток от деления числа $x \in N_0$ на число a обозначим символом $\mathrm{mod}_a(x)$.

Определим множества Z_a следующим образом:

$$Z_a = \{0;1;\ldots;a-1\}.$$

Любое натуральное число x можно представить в виде суммы степеней числа a следующего вида:

$$x = x_n a^n + x_{n-1}a^{n-1} + \ldots + x_2 a^2 + x_1 a^1 + x_0 a^0,$$

где $x_n, x_{n-1}, \ldots, x_2, x_1, x_0 \in Z_a$, $n \in N_0$, $x_n \neq 0$.

Числа $x_n, x_{n-1}, \ldots, x_2, x_1, x_0$ есть остатки в последовательном делении чисел на число a:

© Попов И.Н., 2013

$x = aq_1 + x_0$, $q_1 = aq_2 + x_1$, $q_2 = aq_3 + x_2$, …, $q_{n-1} = aq_n + x_{n-1}$,

где $q_0, q_1, q_2, \ldots, q_{n-1}, q_n$ – натуральные числа. При этом $x_n = q_n$. Числа $x_n, x_{n-1}, \ldots, x_2, x_1, x_0$ назовем коэффициентами представления числа x.

Определим сложение $\underset{a}{\oplus}$ на множестве N_0 следующим образом.

Пусть x, y – натуральные числа и имеют следующие представления:

$$x = x_n a^n + x_{n-1}a^{n-1} + \ldots + x_2 a^2 + x_1 a^1 + x_0 a^0,$$

$$y = y_n a^n + y_{n-1}a^{n-1} + \ldots + y_2 a^2 + y_1 a^1 + y_0 a^0,$$

где числа $x_n, x_{n-1}, \ldots, x_2, x_1, x_0$, также как и числа $y_n, y_{n-1}, \ldots, y_2, y_1, y_0$, из множества Z_a, и хотя бы одно из чисел x_n или y_n не равно 0. Обозначим:

$z_n = \mathrm{mod}_a(x_n + y_n)$, $z_{n-1} = \mathrm{mod}_a(x_{n-1} + y_{n-1})$, ..., $z_0 = \mathrm{mod}_a(x_0 + y_0)$.

Суммой $x \underset{a}{\oplus} y$ назовем число z, имеющее представление

$$z = z_n a^n + z_{n-1}a^{n-1} + \ldots + z_2 a^2 + z_1 a^1 + z_0 a^0.$$

Будем считать, что для любого числа $x \in N_0$ справедливы равенства:

$$x \underset{a}{\oplus} 0 = 0 \underset{a}{\oplus} x = x.$$

В частности $0 \underset{a}{\oplus} 0 = 0$.

Пример. Пусть $a = 3$. Так как

$31 = 3^3 + 3^1 + 3^0$ и $17 = 3^2 + 2\cdot 3^1 + 2\cdot 3^0$,

то

$$31 \underset{3}{\oplus} 17 = (1\cdot 3^3 + 0\cdot 3^2 + 1\cdot 3^1 + 1\cdot 3^0) \underset{3}{\oplus} (0\cdot 3^3 + 1\cdot 3^2 + 2\cdot 3^1 + 2\cdot 3^0) =$$
$$= 1\cdot 3^3 + 1\cdot 3^2 + 0\cdot 3^1 + 0\cdot 3^0 = 3^3 + 3^2 = 36$$

Итак, $31 \underset{3}{\oplus} 17 = 36$. ■

Пример. Справедливы равенства:

$45 \underset{5}{\oplus} 16 = 36$, $45 \underset{7}{\oplus} 16 = 12$, $45 \underset{10}{\oplus} 16 = 51$. ■

Группа (N_0;⊕)

Теорема. Сложение $\underset{a}{\oplus}$ на множестве N_0 обладает свойствами алгебраичности, коммутативности и ассоциативности.

Теорема. Для любого числа $x \in N_0$ найдется число $y \in N_0$ такое, что $x \underset{a}{\oplus} y = y \underset{a}{\oplus} x = 0$.

Доказательство

Если $x = 0$, то и $y = 0$, так как по определению $0 \underset{a}{\oplus} 0 = 0$.

Пусть $x \neq 0$ и

$$x = x_n a^n + x_{n-1}a^{n-1} + \ldots + x_1 a^1 + x_0 a^0,$$

где $x_n, x_{n-1}, \ldots, x_1, x_0 \in Z_a$ и $x_n \neq 0$.

Определим числа $y_n, y_{n-1}, \ldots, y_1, y_0 \in N_0$ следующим образом.

Пусть $i \in \{0;1;\ldots;n\}$. Если $x_i = 0$, то будем считать, что $y_i = 0$; если $0 < x_i < a$, $y_i = a - x_i$. Тогда $y_i \in Z_a$ для любого $i \in \{0;1;\ldots;n\}$.

Определим число y следующим образом:

$$y = y_n a^n + y_{n-1}a^{n-1} + \ldots + y_1 a^1 + y_0 a^0.$$

Так как $x_i + y_i = 0$ или $x_i + y_i = a$, то $\mathrm{mod}_a(x_i + y_i) = 0$ для любого $i \in \{0;1;\ldots;n\}$. Следовательно, $x \underset{a}{\oplus} y = y \underset{a}{\oplus} x = 0$. ■

Для числа $x \in N_0$ число $y \in N_0$ такое, что $x \underset{a}{\oplus} y = y \underset{a}{\oplus} x = 0$, назовем противоположным относительно сложения $\underset{a}{\oplus}$.

Пример. Пусть $a=3$. Справедливо равенство

$11=3^2+2\cdot 3^0=1\cdot 3^2+0\cdot 3^1+2\cdot 3^0$.

Тогда число

$2\cdot 3^2+0\cdot 3^1+1\cdot 3^0=19$

обладает тем свойством, что

$11\underset{3}{\oplus}19=19\underset{3}{\oplus}11=0$. ■

Пример. Справедливы равенства:

$17\underset{3}{\oplus}22=0$, $11\underset{5}{\oplus}19=0$, $23\underset{7}{\oplus}33=0$. ■

Теорема. $(N_0;\oplus)$ – абелева группа.

Нейтральным элементом группы $(N_0;\oplus)$ является число 0.

Теорема. Для любого числа $x\in N_0$ справедливо равенство:

$$\underbrace{x\underset{a}{\oplus}x\underset{a}{\oplus}\ldots\underset{a}{\oplus}x}_{a\ \text{слагаемых}}=0.$$

Доказательство

Если $x=0$, то равенство справедливо.

Пусть $x\neq 0$ и

$$x=x_na^n+\ldots+x_ka^k+\ldots+x_0a^0,$$

где $x_n,\ldots,x_k,\ldots,x_0\in Z_a$ и $x_n\neq 0$.

При вычислении сумм $x\underset{a}{\oplus}x$, $x\underset{a}{\oplus}x\underset{a}{\oplus}x$, …, $\underbrace{x\underset{a}{\oplus}x\underset{a}{\oplus}\ldots\underset{a}{\oplus}x}_{a\ \text{слагаемых}}$ коэффициент при степени a^k соответственно равняется:

$$\mathrm{mod}_a(x_k+x_k)=\mathrm{mod}_a(2x_k),$$

$$\mathrm{mod}_a(\mathrm{mod}_a(2x_k)+x_k)=\mathrm{mod}_a(3x_k),$$

…

$$\mathrm{mod}_a(\mathrm{mod}_a((a-1)x_k)+x_k)=\mathrm{mod}_a(ax_k)=0.$$

Итак, в сумме $\underbrace{x\underset{a}{\oplus}x\underset{a}{\oplus}\ldots\underset{a}{\oplus}x}_{a\ \text{слагаемых}}$ коэффициент при степени a^k равняется 0. Это верно для любого числа $k\in\{0;1;\ldots;n\}$. Поэтому

$$\underbrace{x\underset{a}{\oplus}x\underset{a}{\oplus}\ldots\underset{a}{\oplus}x}_{a\ \text{слагаемых}}=0.\ ■$$

Очевидно, что для любого $x\in N_0$ и любого натурального числа c такого, что $c\,\vdots\,a$ (делящегося нацело на число a), справедливо равенство:

$$\underbrace{x\underset{a}{\oplus}x\underset{a}{\oplus}\ldots\underset{a}{\oplus}x}_{c\ \text{слагаемых}}=0.$$

Заметим, что равенство для $x\in N_0$

$$\underbrace{x\underset{a}{\oplus}x\underset{a}{\oplus}\ldots\underset{a}{\oplus}x}_{b\ \text{слагаемых}}=0$$

может выполняться и для натуральных чисел b, меньших a. Порядок элемента x (то есть такое наименьшее натуральное число b, для которого выполняется указанное выше равенство) обозначим символом $\mathrm{ord}_a(x)$. Будем считать, что

$\mathrm{ord}_a(0)=1.$

Очевидно, что если $x\neq 0$, то $\mathrm{ord}_a(x)\neq 1$. Отметим, что порядок числа x зависит от выбора числа a.

Теорема. В группе $(N_0;\oplus)$ каждый элемент имеет конечный порядок.

Пример. Справедливо: $6\underset{4}{\oplus}6\underset{4}{\oplus}6=8\underset{4}{\oplus}6=14$,

$6\underset{4}{\oplus}6=8$,

$6\underset{4}{\oplus}6\underset{4}{\oplus}6\underset{4}{\oplus}6=14\underset{4}{\oplus}6=0,$

$10\underset{4}{\oplus}10=0.$

Поэтому $\mathrm{ord}_4(6)=4$, $\mathrm{ord}_4(10)=2$.

Также справедливо: $10\underset{6}{\oplus}10\underset{6}{\oplus}10=14\underset{6}{\oplus}10=18,$ $10\underset{6}{\oplus}10=14,$

$10\underset{6}{\oplus}10\underset{6}{\oplus}10\underset{6}{\oplus}10=18\underset{6}{\oplus}10=28,$

$10\underset{6}{\oplus}10\underset{6}{\oplus}10\underset{6}{\oplus}10\underset{6}{\oplus}10=28\underset{6}{\oplus}10=32,$

$10\underset{6}{\oplus}10\underset{6}{\oplus}10\underset{6}{\oplus}10\underset{6}{\oplus}10\underset{6}{\oplus}10=32\underset{6}{\oplus}10=0.$

Поэтому $\mathrm{ord}_6(10)=6$. ■

Теорема. Для чисел x и $y=\underbrace{x\underset{a}{\oplus}x\underset{a}{\oplus}\ldots\underset{a}{\oplus}x}_{(\mathrm{ord}_a(x)-1)\text{ слагаемых}}$ из множества N_0 справедливы равенства:

$x\oplus y=y\oplus x=0$.

Из теоремы следует, что в группе $(N_0;\underset{a}{\oplus})$ для числа x противоположным относительно сложения $\underset{a}{\oplus}$ является число $\underbrace{x\underset{a}{\oplus}x\underset{a}{\oplus}\ldots\underset{a}{\oplus}x}_{(\mathrm{ord}_a(x)-1)\text{ слагаемых}}$.

Теорема. Для любого числа $x\in N_0$ справедливо:

$a\,\vdots\,\mathrm{ord}_a(x)$.

Доказательство

Обозначим: $c=\mathrm{ord}_a(x)$. Тогда $c\in N$.

Если $x=0$, то утверждение справедливо, так как $\mathrm{ord}_a(0)=1$.

Пусть $x\neq 0$. Предположим, что a не делится нацело на число c. Тогда разделим a на c с остатком: $a=cq+r$, где $q,r\in N_0$ и $0<r<c$. Так как

$$\underbrace{x\underset{a}{\oplus}x\underset{a}{\oplus}\ldots\underset{a}{\oplus}x}_{a\text{ слагаемых}}=0,$$

то справедливо равенство:

$$\underbrace{(x\underset{a}{\oplus}x\underset{a}{\oplus}\ldots\underset{a}{\oplus}x)}_{r\text{ слагаемых}}\underset{a}{\oplus}\underbrace{(x\underset{a}{\oplus}x\underset{a}{\oplus}\ldots\underset{a}{\oplus}x)}_{cq\text{ слагаемых}}=0,$$

откуда

$$\underbrace{(x\underset{a}{\oplus}x\underset{a}{\oplus}\ldots\underset{a}{\oplus}x)}_{r\text{ слагаемых}}=0,$$

где $0<r<c$, что противоречит тому, что c – порядок числа x. Пришли к противоречию. Значит, $a\,\vdots\,c$. ■

Следствие. Пусть a – простое натуральное число. Для любого $x\in N$ справедливо равенство: $\mathrm{ord}_a(x)=a$.

Введем обозначения. Пусть $x,y\in N_0$. Наибольший общий делитель чисел x и y обозначим символом $(x;y)$, наименьшее общее кратное – символом $[x;y]$.

Теорема. Пусть натуральное число x имеет представление

$$x=x_{i_1}a^{i_1}+x_{i_2}a^{i_2}+\ldots+x_{i_k}a^{i_k},$$

где $x_{i_1},x_{i_2},\ldots,x_{i_k}$ – ненулевые числа из множества Z_a, $i_1,i_2,\ldots,i_k$ – попарно различные числа из множества N_0, $k\in N$. Тогда порядок элемента x вычисляется по формуле:

$$\mathrm{ord}_a(x)=\left[\frac{a}{(a;x_{i_1})};\frac{a}{(a;x_{i_2})};\ldots;\frac{a}{(a;x_{i_k})}\right].$$

Доказательство

Число $q_1=\dfrac{a}{(a;x_{i_1})}$ есть такое наименьшее натуральное число, что число $x_{i_1}q_1$ делится нацело на число a. Аналогичными свойствами обладают числа $q_2 = \frac{a}{(a;x_{i_2})}$, …, $q_n = \frac{a}{(a;x_{i_k})}$.

По определению $[q_1;q_2;\ldots;q_n]$ – наименьшее натуральное число, которое делится на все числа $q_1;q_2;\ldots;q_n$. По определению порядка числа x получаем, что $\mathrm{ord}_a(x) = [q_1;q_2;\ldots;q_n]$. ■

Пример. Пусть $a = 12$. Число 872 имеет представление: $872 = 6\cdot 12^2 + 8\cdot 12^0$.

Здесь $x_2 = 6$, $x_0 = 8$. Тогда справедливо:

$$\mathrm{ord}_{12}(872) = \left[\frac{12}{(12;6)};\frac{12}{(12;8)}\right] = \left[\frac{12}{6};\frac{12}{4}\right] = [2;3] = 6\ . \quad ■$$

Пример. Найдем в группе $(N_0;\underset{12}{\oplus})$ противоположное относительно сложения $\underset{12}{\oplus}$ число для числа 872.

Так как $\mathrm{ord}_{12}(872) = 6$, то число, противоположное для 872, равно

$$\underbrace{872\underset{12}{\oplus}872\underset{12}{\oplus}872\underset{12}{\oplus}872\underset{12}{\oplus}872}_{5\ \text{слагаемых}} = 868\cdot \ ■$$

Подгруппы группа $(N_0;\oplus)$

Покажем, что в группе $(N_0;\underset{a}{\oplus})$ существуют конечные и бесконечные подгруппы.

Рассмотрим вопрос о наличии конечных подгрупп в группе $(N_0;\oplus)$, отличных от нулевой группы $(\{0\};\oplus)$.

Пусть $m \in N_0$. Введем в рассмотрение множество:

$P_m = \{0;1;\ldots;m\} \subset N_0$.

Теорема. Пусть m – натуральное число, большее 1. Сложение $\underset{a}{\oplus}$ является алгебраической операцией на множестве P_m тогда и только тогда, когда $m = a^n - 1$ для некоторого натурального числа n.

Доказательство

Докажем необходимость.

Предположим, что $m \neq a^n - 1$ ни для какого натурального числа n. Тогда в представлении

$m = m_k a^k + \ldots + m_0 a^0$,

где $k \in N$, $m_k,\ldots,m_0 \in N_0$, $m_k \neq 0$, найдется такой коэффициент m_i, $0 \le i \le k$, что $0 \le m_i < a-1$ (откуда $1 \le m_i + 1 \le a-1$). Отметим, что при этом $m_i a^i \in P_m$.

По условию $\underset{a}{\oplus}$ – алгебраическая операция на множестве P_m. Поэтому должно выполняться: $a^i \underset{a}{\oplus} m \in P_m$. С другой стороны,

$$a^i \underset{a}{\oplus} m = a^i \underset{a}{\oplus}(m_k a^k + \ldots + m_i a^i + \ldots + m_0 a^0) =$$

$$= m_k a^k + \ldots + (m_i + 1)a^i + \ldots + m_0 a^0 > m,$$

значит, $a^i \underset{a}{\oplus} m \notin P_m$. Пришли к противоречию.

Итак, все коэффициенты $m_k,\ldots,m_0$ равны $a-1$. Тогда

$$m = (a-1)\cdot a^k + (a-1)\cdot a^{k-1} + \ldots + (a-1)\cdot a^1 + (a-1)\cdot a^0 =$$

$$= (a-1)\cdot(a^k + a^{k-1} + \ldots + a^1 + a^0) = (a-1)\cdot\frac{a^{k+1}-1}{a-1} = a^{k+1} - 1.$$

Обозначая $n = k+1$, получаем, что $m = a^n - 1$ для некоторого натурального числа n.

Докажем достаточность.

Пусть $m = a^n - 1$, где $n \in N$.

Если $x, y \in P_m$, то $x \le a^n - 1$ и $y \le a^n - 1$, значит, наибольший показатель степени числа a, входящий в представление числа x или числа y, не превосходит $n-1$, то есть

$x = x_{n-1}a^{n-1} + \ldots + x_0 a^0$ и $x = y_{n-1}a^{n-1} + \ldots + y_0 a^0$

где $x_{n-1},\ldots,x_0,y_{n-1},\ldots,y_0 \in N_0$ (при этом необязательно, что $x_{n-1} \neq 0$ и $y_{n-1} \neq 0$). Тогда

$$x \underset{a}{\oplus} y \le (a-1)\cdot a^{n-1} + \ldots + (a-1)\cdot a^0 = m.$$

Поэтому $x \underset{a}{\oplus} y \in P_m$, значит, $\underset{a}{\oplus}$ является алгебраической операцией на множестве P_m. ■

Теорема. Пусть m – натуральное число, большее 1. $(P_m; \underset{a}{\oplus})$ является группой тогда и только тогда, когда $m = a^n - 1$ для некоторого неотрицательного целого числа n.

Получили, что группы $(P_{a^n-1}; \underset{a}{\oplus})$ являются конечными подгруппами группы $(N_0; \underset{a}{\oplus})$ для любого натурального числа n. При этом порядок группы (то есть количество элементов в группе) $(P_{a^n-1}; \underset{a}{\oplus})$ равен a^n.

Рассмотрим вопрос о существовании бесконечных подгрупп в группе $(N_0; \oplus)$.

Выберем k попарно различных чисел $i_1, \ldots, i_k$ из множества N_0. Обозначим символом $\overline{\{i_1, \ldots, i_k\}}_a$ множество всех чисел из множества N_0, в представлении которых в виде суммы степеней числа a с неотрицательными целыми показателями при степенях $a^{i_1}, \ldots, a^{i_k}$ коэффициенты равны 0. Очевидно, что $\overline{\{i_1, \ldots, i_k\}}_a$ – бесконечное множество и $0 \in \overline{\{i_1, \ldots, i_k\}}_a$.

Пример. Пусть $a = 3$. Множество $\overline{\{0\}}_3$ состоит из чисел вида:

$$x_n \cdot 3^n + \ldots + x_1 \cdot 3^1 + 0 \cdot 3^0 = x_n \cdot 3^n + \ldots + x_1 \cdot 3^1,$$

где n – натуральное число, $x_n, \ldots, x_1 \in N_0$. ■

Теорема. Пусть $k \in N$ и $i_1, \ldots, i_k$ – попарно различных чисел из множества N_0. Тогда $(\overline{\{i_1, \ldots, i_k\}}_a; \underset{a}{\oplus})$ – бесконечная подгруппа группы $(N_0; \underset{a}{\oplus})$.

Линейные отображения $y = x \oplus c$ на группе N_0 и ее подгруппах

Рассмотрим на плоскости с введенной прямоугольной системой координат целочисленную решетку, как множество точек, координаты которых есть целые числа.

Зафиксируем число $c \in N_0$. На целочисленной решетке можем изобразить множество точек $(x; y)$, где значения x и y связаны равенством:

$$y = x \underset{a}{\oplus} c,$$

где $x \in N_0$.

Рассмотрим свойства отображения группы P_{a^n-1} на себя, заданного равенством $y = x \underset{a}{\oplus} c$, где $x, y \in P_{a^n-1}$, для натурального числа n и фиксированного числа $c \in P_{a^n-1}$. Учитывая, что P_{a^n-1} – группа, то отображение $y = x \underset{a}{\oplus} c$ на этой группе является биективным.

Очевидно, что $y = x \underset{a}{\oplus} 0 = x$.

Отображения $f(x)$ и $g(x)$ на группе P_{a^n-1} назовем взаимно обратными, если $f(g(x)) = g(f(x)) = x$ для любого $x \in P_{a^n-1}$.

Теорема. Пусть $c, d \in P_{a^n-1}$. Отображения $y = x \underset{a}{\oplus} c$ и $y = x \underset{a}{\oplus} d$ являются взаимно обратными на группе P_{a^n-1} тогда и только тогда, когда $c \underset{a}{\oplus} d = 0$.

Доказательство

Обозначим: $f(x) = x \underset{a}{\oplus} c$ и $g(x) = x \underset{a}{\oplus} d$.

Вычислим $f(g(x))$. Получаем:

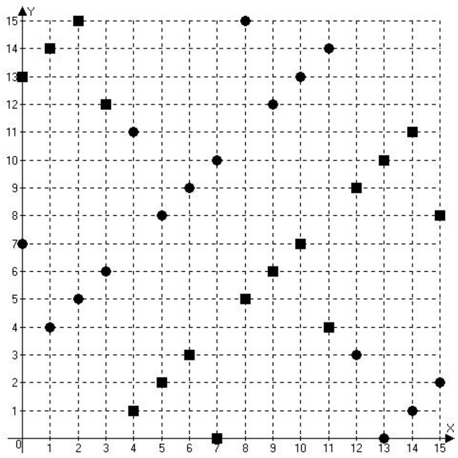
$$f(g(x)) = (x \underset{a}{\oplus} d) \underset{a}{\oplus} c = x \underset{a}{\oplus} (d \underset{a}{\oplus} c) = x \underset{a}{\oplus} 0 = x.$$

Аналогично получаем, что $g(f(x)) = x$. Следовательно, отображения $f(x)$ и $g(x)$ являются взаимно обратными на группе P_{a^n-1}.

Обратно, если $f(g(x)) = g(f(x)) = x$ для любого $x \in P_{a^n-1}$, то $x \underset{a}{\oplus} (d \underset{a}{\oplus} c) = x$. Учитывая, что P_{a^n-1} – группа, то из последнего равенства получаем, что $c \underset{a}{\oplus} d = 0$. ■

Графики взаимно обратных отображений на плоскости симметричны относительно прямой линии $y = x$. Это в полной мере относится и к графикам отображений $y = x \underset{a}{\oplus} c$ и $y = x \underset{a}{\oplus} d$ в случаи выполнения равенства $c \underset{a}{\oplus} d = 0$.

Пример. В группе $(P_{15}; \underset{4}{\oplus})$ справедливо равенство: $7 \underset{4}{\oplus} 13 = 0$. Тогда отображения $y = x \underset{4}{\oplus} 7$ и $y = x \underset{4}{\oplus} 13$ являются взаимно обратными. Графики этих отображений имеют вид:



Здесь: ● – график отображения $y = x \underset{4}{\oplus} 7$; ■ – график отображения $y = x \underset{4}{\oplus} 13$. Видим, что рисунок, полученный из графиков этих отображений, симметричен относительно прямой $y = x$. ■

Любой подгруппе H группы $P_{a^n - 1}$ можно сопоставить рисунок, состоящий из графиков отображений $y = x \underset{a}{\oplus} c$ для всех $c \in H$ на целочисленной решетке, который назовем графическим представлением группы H или рисунком группы H и обозначим $\mathrm{Pic}(H)$. В частности, $\mathrm{Pic}(P_{a^n - 1})$ – квадрат размерности $a^n \times a^n$ (рассматриваются в этом квадрате только точки с целочисленными координатами), $\mathrm{Pic}(\{0\})$ состоит из одной точки $(0;0)$.

Заметим, что для любой подгруппы H группы $P_{a^n - 1}$ точка $(0;0)$ является элементом $\mathrm{Pic}(H)$.

Теорема. Рисунок $\mathrm{Pic}(H)$ любой подгруппы H группы $P_{a^n - 1}$ симметричен относительно прямой $y = x$.

Доказательство

Пусть $c \in H$. Противоположное число d относительно сложения $\underset{a}{\oplus}$ для числа c также принадлежит группе H. Тогда графики отображений $y = x \underset{a}{\oplus} c$ и $y = x \underset{a}{\oplus} d$ для любого $x \in H$ симметричны относительно прямой $y = x$. ■

Один из вопросов изучения группы касается описания всех ее подгрупп. Для выделения подгрупп группы $(P_{a^n - 1}; \underset{a}{\oplus})$ можно поступить следующим образом.

В квадрате $\{0;\ldots;a^n - 1\} \times \{0;\ldots;a^n - 1\}$ на целочисленной решетке генерируется рисунок, состоящий из точек с абсциссами $x_1, \ldots, x_k$, где $k \in N$. Если рисунок не удовлетворяет одному из условий

1) является симметричным относительно прямой линии $y = x$;

2) число k является делителем числа a^n;

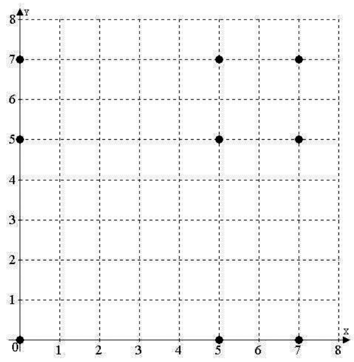
3) содержит точку $(0;0)$,

то данный рисунок не соответствует ни одной из подгрупп группы $(P_{a^n - 1}; \underset{a}{\oplus})$. В противном случае методом перебора определяем, является ли множество чисел $x_1, \ldots, x_k$ группой относительно сложения $\underset{a}{\oplus}$.

Если на подгруппе H группы $P_{a^n - 1}$ заданы два отображения $y = x \underset{a}{\oplus} c$ и $y = x \underset{a}{\oplus} d$, где $c, d \in H$, то графики этих отображений не пересекаются. Каждый график отображения на группе H состоит из $|H|$ точек, где $|H|$ – мощность (порядок) группы H. Отсюда получаем, что $\mathrm{Pic}(H)$ состоит из $|H|^2$ точек. При этом $a^n \vdots |H|$.

Пример. Рисунком группы $(P_8; \underset{3}{\oplus})$ является квадрат $\{0;\ldots;8\} \times \{0;\ldots;8\}$ на целочисленной решетке.

Пусть дан рисунок из 9 точек (0;0), (0;5), (0;7), (5;0), (5;5), (5;7), (7;0), (7;5), (7;7):



Абсциссы точек равны числам 0, 5 и 7, количество которых есть делитель числа 9, являющегося порядком группы $(P_8;\underset{3}{\oplus})$. Рисунок является симметричным относительно прямой линии $y = x$.

Легко проверить, множество $H = \{0;5;7\}$ является группой относительно операции сложения $\underset{3}{\oplus}$. Итак, $H = \{0;5;7\}$ – подгруппа группы $(P_8;\underset{3}{\oplus})$ и данный рисунок является $\mathrm{Pic}(H)$. ■

Список литературы

1. *Каргополов М.И., Мерзляков Ю.И.* Основы теории групп. М., 1982.
2. *Курош А.Г.* Теория групп. М., 1967.

References

1. Kargopolov M.I., Merzlyakov Yu.I. *Osnovy teorii grupp* [Fundamentals of the Group Theory]. Moscow, 1982.
2. Kurosh A.G. *Teoriya grupp* [Group Theory]. Moscow, 1967.

Popov Ivan Nikolaevich

Institute of Mathematics, Information and Space Technologies,
Northern (Arctic) Federal University named
after M.V. Lomonosov (Arkhangelsk, Russia)

ADDITION ⊕ ON THE SET OF NONNEGATIVE INTEGERS

The paper considers an example of Abelian group with nonnegative integers as elements and an operation that is based on representation of a natural number as a sum of the degrees of a fixed number. It is shown that the constructed group contains subgroups of finite and infinite order. Using a graphical representation of linear mappings of finite subgroups of the group, we suggest a way of finding their subgroups.

***Keywords**: group, subgroup, finite group, order of group, order of element of group, mapping of groups to themselves.*

Контактная информация
Попов Иван Николаевич
Адрес: 163002, г. Архангельск, наб. Северной Двины, д. 17
e-mail: only-for-you-pi@mail.ru

Рецензент – *Попов В.Н.*, доктор физико-математических наук, доцент, заведующий кафедрой математики института математики, информационных и космических технологий Северного (Арктического) федерального университета им. М.В. Ломоносова