Записки научных
семинаров ПОМИ
Том 443, 2016 г.

С. А. Евдокимов

ДОКАЗАТЕЛЬСТВО КОНГРУЭНЦ-ГИПОТЕЗЫ ДЛЯ ОБОБЩЁННЫХ КОЛЕЦ

§1. Введение

В работе [1] А. Л. Смирнов сформулировал следующую гипотезу об обобщённых кольцах, введённых и изученных Н. В. Дуровым (см. [2]).

Конгруэнц-гипотеза. Пусть R – обобщённая $\mathbb{F}_{1^2}$-подалгебра кольца $\mathbb{Z}$, содержащая бинарную операцию $(a,b) \in R(2)$, где $a \neq 0$, $b \neq 0$ и НОД$\,(a,b) = 1$. Тогда найдётся такое целое $N \geqslant 1$, что $R \supset R_N$, где R_N – прообраз при эпиморфизме $\mathbb{Z} \to \mathbb{Z}/N$ образа обобщённого поля $\mathbb{F}_{1^2}$.

Дуров свёл конгруэнц-гипотезу к некоторому элементарному утверждению о подмножествах кольца $\mathbb{Z}$. В следующем параграфе мы доказываем это утверждение (теорема 2.1), доказывая тем самым и конгруэнц-гипотезу. Следует отметить, однако, что доказательства ничего не говорят о конкретном значении числа N, фигурирующего в формулировке гипотезы. Модифицируя рассуждение Дурова, мы показываем в §3, что в качестве N можно взять, например, абсолютное значение произведения чисел a и b (теорема 3.1).

В настоящей работе мы следуем обозначениям и соглашениям работ [1, 2]. В частности, с обобщённой $\mathbb{F}_{1^2}$-подалгеброй R кольца $\mathbb{Z}$ связаны множества $R(1) \subset \mathbb{Z}$ и $R(2) \subset \mathbb{Z}^2$, причём $R(1) = -R(1)$, $R(2) = -R(2)$ и

$$(R(1) \times \{0\}) \cup (\{0\} \times R(1)) \subset R(2) \subset R(1) \times R(1).$$

Если же $(a,b) \in R(2)$, то $aR(1) + bR(1) \subset R(1)$ и $aR(2) + bR(2) \subset R(2)$.

В заключение отметим, что результаты работы были получены более 6 лет назад и не предназначались для публикации. Однако интерес специалистов побудил автора изменить своё решение.

Ключевые слова: обобщённое кольцо, конгруэнц-гипотеза, бинарная операция.

§2. Ключевое утверждение

Пусть $a, b \in \mathbb{Z}$ и X – подмножество кольца $\mathbb{Z}$, удовлетворяющее следующим условиям:

(1) $a, b \in X$,
(2) $x \in X \Longrightarrow -x \in X$,
(3) $x, y \in X \Longrightarrow ax + by \in X$.

Легко видеть, что $0 = a \cdot b + b \cdot (-a) \in X$ и потому $a^i b^j \in X$ для всех $i, j \geqslant 0$ таких, что $i + j \geqslant 1$, и $a^i b^j X \subset X$ для всех $i, j \geqslant 0$. Более того,

$$x(ab)^N \in X \quad \text{для всех} \quad x \in \mathbb{Z} \quad \text{таких, что} \quad |x| \leqslant N. \tag{1}$$

(Действительно, $x(ab)^N = a \cdot (a^{N-1}b^N) + b \cdot (a \cdot (x-1)(ab)^{N-1})$ для $N, x > 0$, и мы рассуждаем по индукции.)

Теорема 2.1. *Пусть X – подмножество кольца $\mathbb{Z}$, удовлетворяющее условиям (1)–(3), где целые числа a и b отличны от нуля и взаимно просты. Тогда $1 \in X$.*

Ниже, не умаляя общности, будем считать, что $a > 0$ и $b > 0$. Докажем сначала два вспомогательных утверждения, где через m, n, k, l, x, y, z обозначены целые числа.

Лемма 2.2. *Для любого $m > 0$ существует $l > 0$ такое, что для любого $n > 0$ существуют $k > 0$ и $x \equiv 1 \pmod{a^m}$, для которых $a^{mk} + b^{nl}x = 1$.*

Доказательство. Положим $l = \varphi(a^m)$ и $k = \varphi(b^{nl})$, где φ – функция Эйлера. Тогда по теореме Эйлера $a^{mk} - 1 = -b^{nl}x$, где $x \in \mathbb{Z}$. Более того, $x \equiv 1 \pmod{a^m}$, поскольку $b^l \equiv 1 \pmod{a^m}$. □

Для натурального числа N положим $I_N = (ab)^N\mathbb{Z}$.

Лемма 2.3. *Существует натуральное N, для которого $I_N \subset X$.*

Доказательство. Положим $N = ab$. Предполагая, не умаляя общности, что $ab > 1$, докажем, используя индукцию по x, что $(ab)^N x \in X$ для всех $x > 0$ и потому для всех x. Запишем $x > 0$ в виде $x = y + abz$, где $0 \leqslant y < ab$. Тогда

$$(ab)^N x = (ab)^N y + (ab)^{N+1} z = a \cdot (b \cdot (ab)^{N-1} y) + b \cdot (a \cdot (ab)^N z).$$

Поскольку $y \leqslant N - 1$, то $(ab)^{N-1} y \in X$ в силу (1). Более того, поскольку $z < x$, то по индукционному предположению $(ab)^N z \in X$. Таким образом, $(ab)^N x \in X$. □

Доказательство теоремы 2.1. Пусть целые числа m, n, k, l и x те же, что и в лемме 2.2. Тогда $x = 1 + a^m y$, где $y \in \mathbb{Z}$, и

$$1 = a^{mk} + b^{nl} x = a^{mk} + b^{nl} + b^{nl} a^m y = a \cdot a^{mk-1} + b \cdot (a \cdot a^{m-1} b^{nl-1} y + b \cdot b^{nl-2}).$$

По лемме 2.3 найдём $N > 0$ такое, что $I_N \subset X$. Поскольку m и n могут быть выбраны сколь угодно большими, $a^{m-1} b^{nl-1} y = a^i b^j z$, где $z \in I_N$ и $i, j \geqslant 0$. Поэтому $a^{m-1} b^{nl-1} y \in X$, откуда следует, что $1 \in X$, поскольку, очевидно, $a^{mk-1}, b^{nl-2} \in X$. □

§3. Оценка числа N в конгруэнц-гипотезе

Пусть R – обобщённое кольцо, фигурирующее в формулировке конгруэнц-гипотезы. Поскольку $(a, b) \in R(2)$, то $a, b \in R(1)$ и потому $a^i, b^i \in R(1)$ для всех $i \geqslant 1$. Более того, $1 \in R(1)$, поскольку $R \supset \mathbb{F}_{1^2}$ (это следует также из теоремы 2.1, так как при $X = R(1)$ условие теоремы, очевидно, выполнено). Не умаляя общности, можно считать, что $a > 0$ и $b > 0$.

Теорема 3.1. *Кольцо R содержит кольцо R_N, где $N = ab$.*

Доказательство. Достаточно показать, что $(1, N) \in R(2)$ (см. [1, с. 239]). Положим

$$I = \{x \in \mathbb{Z} : \ (x, Nx) \in R(2)\}.$$

Поскольку $R(2) = -R(2)$ и $aR(2) + bR(2) \subset R(2)$, то $I = -I$ и $aI + bI \subset I$, соответственно. Проверим, что $a, b \in I$. Действительно,

$$(a, Na) = a(1, 0) + b(0, a^2), \quad (b, Nb) = a(0, b^2) + b(1, 0).$$

Поскольку $1, a^2, b^2 \in R(1)$, то $(1, 0), (0, a^2), (0, b^2) \in R(2)$. Отсюда следует, что $(a, Na), (b, Nb) \in R(2)$, то есть $a, b \in I$. Таким образом, множество $X = I$ удовлетворяет условию теоремы 2.1 и потому $1 \in I$, то есть $(1, N) \in R(2)$. □

Литература

1. А. Л. Смирнов, *Обобщённые подкольца арифметических колец.* — Зап. научн. семин. ПОМИ **349** (2007), 211–241.
2. N. Durov, *New approach to Arakelov geometry.* — arXiv: 0704.2030 v1 [math AG] 16 Apr 2007.

Evdokimov S.A. Proof of the congruence conjecture for generalized rings.

In 2007 A. L. Smirnov formulated an interesting conjecture on generalized rings introduced and studied by N. V. Durov. In this paper we prove the conjecture.

С.-Петербургское отделение
Математического института
им. В. А. Стеклова РАН,
наб. р. Фонтанки, д. 27,
191023 С.-Петербург, Россия
E-mail: evdokim@pdmi.ras.ru

Поступило 11 января 2016 г.