УДК 735.29

КОНГРУЭНЦ-ПРОБЛЕМА МЕНИКЕ-ИХАРА

Литаврин А.В.,
научный руководитель д-р физ.-мат. наук Левчук В. М.
Сибирский федеральный университет

Если G - линейная группа и J - идеал основного кольца K (K - ассоциативно коммутативное кольцо с единицей 1), то все матрицы группы G, сравнимые с единичной матрицей по модулю идеала J образуют подгруппу в G и эту подгруппу называют конгруэнц-подгруппой уровня J. Конгруэнц-подгруппа всегда является нормальным делителем основной группы. В связи с этим встает конгруэнц-проблема: «Верно ли, что в линейной группе G любая нецентральная нормальная подгруппа содержит неединичную конгруэнц-подгруппу?»

Отметим, что конгруэнц-проблема для групп GL(k,Z) была положительно решена для k>2, а для k=2 отрицательное решение указал Меннике. См. монографии Платонова, В.П. и А.С Рапинчука «алгебраические группы и теория чисел», и Каргаполова М.И., Ю.И. Мерзлякова «Основы теории групп».

Алгебру обобщенных кватернионов A=A(x,y,z,u) над полем Q рациональных чисел с нормой $f(A) = x^2 - ny^2 - mz^2 + nmu^2$ $(n, m -$ целые числа) обозначают через H(n,m,Q).

Пусть p - простое число и Z[1/p] - расширение в Q кольца Z целых чисел с помощью элемента 1/p. В мультипликативной группе обратимых элементов алгебры H(n,m,Q) выделим подгруппу G(n,m,p) кватернионов над Z[1/p] с нормой 1. Конгруэнц-проблема Й. Меннике - И.Ихара для групп G(n,m,p) записана в 1976 году в Коуровской тетради.

Работа посвящается изучению связи диофантовых уравнения от четырех неизвестных

$$x^2 - ny^2 - mz^2 + nmu^2 = 1 \quad (1)$$

в кольце Z[1/p] описывающих обобщенные кватернионы с нормой 1 с конгруэнц-проблемой Менике-Ихара.

Решение уравнения (1) можно свести к решению диофантова уравнения

$$x^2 - Ay^2 - Bz^2 + ABu^2 = K \quad (A, B, C, K \in Z, \sqrt{A} - \textit{иррационально}, A > 0) \quad (2)$$

в кольце Z.

Для решения уравнения (2) нам потребуется рассмотреть обобщенное уравнение Пелля:

$$x^2 - ny^2 = c, \quad (3)$$

где n - натуральное число, не являющееся квадратом; c – целое число.

Уравнение (3) достаточно изучено. Все необходимые свойства уравнения (3), мы сформулируем в виде леммы 1. Если a – наименьшее натуральное число, для которого существует натуральное число b такое, что $a^2 - nb^2 = 1$, то число $q = a + \sqrt{n}b$ называется основной единицей числа n. Положим

$$M_{n,c} := \{x + \sqrt{n}y \in Z + \sqrt{n}Z | x^2 - ny^2 = c, 1 < x + \sqrt{n}y \leq q\},$$

И сформулируем лемму 1.

Лемма 1. Пусть n - натуральное число не являющееся квадратом, c - целое число не равное нулю. Тогда верны следующие утверждения.

1) Множество $M_{n,c}$ - конечно.

2) Уравнение $x^2 - ny^2 = c$ разрешимо в целых числах тогда и только тогда, когда $M_{n,c}$ - не пустое множество.

3) Всякое решение уравнения $x^2 - ny^2 = c$ в целых числах можно записать в виде $x + \sqrt{n}y = \pm wq^s$, где w из $M_{n,c}$, q – основная единица числа n и s – некоторое целое число.

Теорема 1. Пусть A,B,K - параметры, введенные выше, q - основная единица числа A , S - множество решений уравнения (2), $M_{n,c}$ - множества, введенные выше и

$$D \coloneqq \left\{\left(x + \sqrt{n}y, z + \sqrt{n}u\right)\middle|(x, y, z, u) \in S\right\},\ F_1 \coloneqq \{x^2 - ny^2 | x, y \in Z\}$$

$$.\ F_2 \coloneqq \{\frac{x^2 - Ay^2 - K}{B} | x, y \in Z, B | (x^2 - Ay^2 - K)\}$$

Тогда для любого $(x + \sqrt{n}y, z + \sqrt{n}u) \in D$ существует $t \in F_1 \cap F_2$ такое, что при любых $s, k \in Z$ и при любых $w_1 \in M_{A,1+Bt}, w_2 \in M_{A,t}$ имеют место равенства:

$$x + \sqrt{n}y = q^s w_1,\ z + \sqrt{n}u = q^k w_2.$$

Теорема 1 дает возможность исследовать арифметические свойства элементов группы G(n,m,p). Кроме того с помощью теоремы 1 можно непосредственно описывать элементы произвольной конгруэнц-подгруппы. В настоящий момент для решений конгруэнц-проблемы Менике-Ихара, ведется поиск порождающих множеств (конечных или бесконечных) для произвольной конгруэнц-подгруппы группы G(n,m,p).