УДК: 511.6

Маданбекова Э.Э., Айбек кызы А.
ИГУ им. К.Тыныстанова,
ИГУ им. К.Тыныстанова, магистрант

ПРИМЕНЕНИЕ ТЕОРИИ ДЕЛИМОСТИ К РЕШЕНИЮ НЕОПРЕДЕЛЕННЫХ УРАВНЕНИЙ

В этой статье рассматривается применение теории делимости к решению неопределенных уравнений первой степени с двумя неизвестными.

Ключевые слова: *теории чисел, теории делимости, неопределенные уравнения, решение уравнений, теоремы, целые числа, простые числа.*

Бул макалада бөлүнүүчүлүк теориясынын эки белгисиздүү биринчи даражадагы аныкталбаган теңдеменин чыгарылышында колдонулушу каралган.

Негизги сөздөр: *сандар теориясы, бөлүнүүчүлүк теориясы, аныкталбаган теңдеме, теңдеменин чыгарылышы,теоремалар, бүтүн сан, жөнөкөй сан.*

This article is discusses the application of the theory of divisibility to the solution of indefinite simple equations with two unknown.

Key words: *number theory, divisibility theory, indefinite equations, solution of equations, theorems, integers, prime numbers.*

Решение уравнений в целых числах является одной из древнейших математических задач. Наибольшего расцвета эта область математики достигла в Древней Греции. Основным источником, дошедшим до нашего времени, является произведение Диофанта – «Арифметика». Диофант суммировал и расширил накопленный до него опыт решения неопределенных уравнений в целых числах. По некоторым данным Диофант жил до 364 года н.э. Наиболее известной, решенной Диофантом, является задача «о разложении на два квадрата». Ее эквивалентом является известная всем теорема Пифагора. Эта теорема была известна в Вавилоне, возможно ее знали и в Древнем Египте, но впервые она была доказана, в пифагорейской школе. Так называлась группа интересующихся математикой философов по имени основателя школы Пифагора (ок. 580–500 г. до н.э.).

Жизнь и деятельность Диофанта протекала в Александрии, он собирал и решал известные и придумывал новые задачи. Позднее он объединил их в большом труде под названием «Арифметика». Мы рассмотрим здесь некоторые методы решения уравнений в целых числах и способы доказательства того, что уравнение не имеет решений в целых числах. Многие из этих методов предполагают применение некоторых понятий и алгоритмов теории делимости.

Определение. Неопределенные уравнения – уравнения, содержащие более одного неизвестного.

Под одним решением неопределенного уравнения понимается совокупность значений неизвестных, которая обращает данное уравнение в верное равенство.

Пример 1. Решить в целых числах уравнение $x^5 - x^3 = y^3 \cdot p$, где y и p – простые числа.

Решение: Преобразуем уравнение $x^3 \cdot (x^5 - 1) = y^3 \cdot p$. Если имеются целые решения этого уравнения, тогда $y^3 \cdot p$ делится на x^3, так как НОД (x^3, $x^2 - 1$) = 1, но y^3 и p являются взаимно простыми числами, т.е. $НОД(y^3, p) = 1$, значит, p не делится на x^3, следовательно, y^3 делится на x^3, что возможно, если x = y, т.е. x – простое число. Тогда $x^2 - 1 = p,\ \ (x-1)(x+1) = p$, что возможно, если $x - 1 = 1,\ \ x + 1 = p$, т.е.x = 2,y = 2, p = 3. *Ответ:* x = 2, y = 2, p = 3.

Пример 2. Найти целые решения уравнения $xy = x + y$.

Решение: Преобразуем уравнение

$xy - x - y = 0,\quad x(y-1) - y + 1 = 1,\quad x(y-1) - (y-1) = 1, (x-1)(y-1) = 1$. Произведение целых чисел будет равно 1 в двух случаях, когда каждый из сомножителей равен 1, и когда каждый из сомножителей равен -1.

Получим совокупность двух систем уравнений:

(1) $\begin{cases} x-1=1, \\ y-1=1 \end{cases}$ и (2) $\begin{cases} x-1=-1, \\ y-1=-1. \end{cases}$

Решим каждую систему уравнений:

(1) $\begin{cases} x_1 = 2, \\ y_1 = 2, \end{cases}$ (2) $\begin{cases} x_2 = 0, \\ y_2 = 0. \end{cases}$

Ответ: $\begin{cases} x_1 = 2, \\ y_1 = 2, \end{cases} \begin{cases} x_2 = 0, \\ y_2 = 0. \end{cases}$

Пример 3. Найти все целые решения уравнения: $p(x+y) = xy$, где p – простое число.

Решение:

Преобразуем уравнение:

$px + py - xy = 0,\quad xy - px - py = 0,\quad xy - px - py + p^2 = p^2,$

$(p^2 - px) + (xy - py) = p^2,\quad p(p-x) + y(x-p) = p^2,\quad p(p-x) - y(p-x) = p^2,$

$(p-x)(p-y) = p^2$.

Произведение двух множителей равно целому числу p^2. Очевидно, что каждый из множителей должен быть числом целым, следовательно, получим системы уравнений, которые представляют всевозможные случаи, когда множители целые и их произведение равно p^2,

(1) $\begin{cases} p-x=1, \\ p-y=p^2, \end{cases}$ (2) $\begin{cases} p-x=p^2, \\ p-y=1, \end{cases}$ (3) $\begin{cases} p-x=p, \\ p-y=p, \end{cases}$ (4) $\begin{cases} p-x=-p, \\ p-y=-p. \end{cases}$

В результате решения систем, получаем:

(1) $\begin{cases} x_1 = p-1, \\ y_1 = p-p^2, \end{cases}$ (2) $\begin{cases} x_2 = p-p^2, \\ y_2 = p-1, \end{cases}$ (3) $\begin{cases} x_3 = 0, \\ y_3 = 0, \end{cases}$ (4) $\begin{cases} x_4 = 2p, \\ y_4 = 2p. \end{cases}$

Ответ: $\begin{cases} x_1 = p-1, \\ y_1 = p-p^2, \end{cases} \begin{cases} x_2 = p-p^2, \\ y_2 = p-1, \end{cases} \begin{cases} x_3 = 0, \\ y_3 = 0, \end{cases} \begin{cases} x_4 = 2p, \\ y_4 = 2p. \end{cases}$

Пример 4. Найти все целые решения уравнения: $xy + 3x - 5y = -3$.

Решение:

Преобразуем уравнение: $xy + 3x - 5y - 15 = -3 - 15,\quad x(y+3) - 5(y+3) = -18,$

$(y+3)(x-5) = -18,\quad (5-x)(y+3) = 18$.

Произведение двух целых сомножителей равно 18. Чтобы выяснить, каким числам могут быть равны эти сомножители, найдем все делители числа 18:

18 имеет делители: 1, 2, 3, 6, 9, 18. Если первый множитель равен первому из делителей 18, тогда второй множитель будет равен последнему – получим шесть пар решений:

(1) $\begin{cases} 5-x=1, \\ y+3=18 \end{cases}$ (2) $\begin{cases} 5-x=2, \\ y+3=9, \end{cases}$ (3) $\begin{cases} 5-x=3, \\ y+3=6, \end{cases}$

(4) $\begin{cases} 5-x=6, \\ y+3=3, \end{cases}$ (5) $\begin{cases} 5-x=9, \\ y+3=2, \end{cases}$ (6) $\begin{cases} 5-x=18, \\ y+3=1. \end{cases}$

(1) $\begin{cases} x=4, \\ y=15, \end{cases}$ (2) $\begin{cases} x=3, \\ y=6, \end{cases}$ (3) $\begin{cases} x=2, \\ y=3, \end{cases}$ (4) $\begin{cases} x=-1, \\ y=0, \end{cases}$ (5) $\begin{cases} x=-4, \\ y=-1, \end{cases}$ (6) $\begin{cases} x=-13, \\ y=-2. \end{cases}$

Ответ: $\begin{cases} x=4, \\ y=15, \end{cases} \begin{cases} x=3, \\ y=6, \end{cases} \begin{cases} x=2, \\ y=3, \end{cases} \begin{cases} x=-1, \\ y=0, \end{cases} \begin{cases} x=-4, \\ y=-1, \end{cases} \begin{cases} x=-13, \\ y=-2. \end{cases}$

Пример 5. Найти натуральные значения корней уравнения
$x^2-4xy+5y^2=169$.

Решение: Преобразуем уравнение: $x^2-4xy+4y^2+y^2=13^2$, $(x-2y)^2+y^2=13^2$.

Отсюда получаем четыре системы уравнений:

(1) $\begin{cases} (x-2y)^2=0, \\ y^2=13^2, \end{cases}$ (2) $\begin{cases} (x-2y)^2=13^2, \\ y^2=0, \end{cases}$ (3) $\begin{cases} (x-2y)^2=12^2, \\ y^2=5^2, \end{cases}$ (4) $\begin{cases} (x-2y)^2=5^2, \\ y^2=12^2. \end{cases}$

Поскольку x и y – натуральные числа, находим:

$\begin{cases} x_1=26, \\ y_1=13, \end{cases} \begin{cases} x_2=22, \\ y_2=5, \end{cases} \begin{cases} x_3=29, \\ y_3=12. \end{cases}$

Ответ: $\begin{cases} x_1=26, \\ y_1=13, \end{cases} \begin{cases} x_2=22, \\ y_2=5, \end{cases} \begin{cases} x_3=29, \\ y_3=12. \end{cases}$

Уравнения вида ax + by = c, где a, b, c – целые числа, отличные от нуля

Теорема 1. Если НОД (a; b) = d, то существуют такие целые числа x и y, что имеет место равенство $a\cdot x+b\cdot y=d$.

Это равенство называется линейной комбинацией или линейным представлением наибольшего общего делителя двух чисел через сами эти числа.

Пример. Найти линейное представление наибольшего общего делителя чисел 1232 и 1672.

Решение:

1) Применим алгоритм Евклида и найдем НОД (1232, 1672):

НОД (1232, 1672) = 88.

2) Выразим 88 последовательно через неполные частные и остатки, используя полученные равенства, начиная с конца:

$88=440-352\cdot 1=440-(1232-440\cdot 2)=440\cdot 3-1232\cdot 1=(1672-1232\cdot 1)\cdot 3-1232\cdot 1=$

$=1672\cdot 3-1232\cdot 4$, т.е. $88=1672\cdot 3+1232\cdot(-4)$.

Теорема 2. Если в уравнении ax + by = l (a, b) = 1, то уравнение имеет по крайней мере одно целое решение.

Справедливость этой теоремы следует из теоремы 1. Таким образом, чтобы найти одно целое решение уравнения ax + by = 1, если (a, b) = 1, достаточно представить число 1 в виде линейной комбинации чисел a и b.

Пример. Найти целое решение уравнения 15x + 37y = 1.

Решение:

1) Применим алгоритм Евклида и найдем НОД (15, 37):НОД (15, 37) = 1

2) Выразим 1 последовательно через неполные частные и остатки, используя полученные равенства, начиная с конца:

$1=15-7\cdot 2=15-(37-15\cdot 2)\cdot 2=15-37\cdot 2+15\cdot 4=15\cdot 5+37\cdot(-2)$,

т.е. $x_0=5$, $y_0=-2$.

Теорема 3. Если в уравнении ax + by = c (a, b) = d > 1 и c не делится на d, то уравнение *целых решений не имеет.*

Для доказательства теоремы достаточно предположить противное.

Пример. Найти целое решение уравнения 16x – 34y = 7.

Решение:

(16, 34) = 2, 7 не делится на 2, уравнение целых решений не имеет.

Теорема 4. Если в уравнении ax + by = c (a, b) = d > 1 и c делится на d, то оно равносильно уравнению $a_1x + b_1y = c_1$, в котором $(a_1, b_1) = 1$.

При доказательстве теоремы следует показать, что произвольное целое решение первого уравнения является также решением второго уравнения и обратно.

С помощью сравнений легко указать необходимые признаки правильности и достаточные признаки неправильности результатов выполнения арифметических действий сложения, вычитания и умножения целых чисел. Теория сравнений дает следующий способ проверки арифметических действий.

Выбираем некоторый модуль m и заменяем большие числа a, b, c, ..., над которыми нам надо производить действия (сложение, вычитание, умножение, возведение в степень), небольшими числами a', b', c', ..., сравнимыми с ними по модулю т. Произведя действия над a, b, c мы точно такие же действия производим над a', b', c', ... Если действия произведены правильно, то результаты этих действий над a, b, c, ... и над a', b', c', ... должны быть сравнимы по модулю m.

Если $a \equiv a'(\mathrm{mod}\ m), b \equiv b'(\mathrm{mod}\ m), \ldots$, то $a+b+\ldots \equiv a'+ b'+\ldots(\mathrm{mod}\ m), a \cdot b\ldots \equiv a'\ b'\ldots(\mathrm{mod}\ m)$.

Для проверки соотношения a/b=c представляем его в виде a=bc. Применение этого способа проверки, конечно, имеет смысл только тогда, когда нахождение таких чисел a', b', c',... может быть осуществлено легко и быстро. Для этого обычно в качестве модуля т выбирают т=9 или m=11. Каждое число, записанное в десятичной системе счисления, сравнимо с суммой его цифр по модулю 9, так что мы можем сформулировать следующий способ “проверки с помощью девятки”.

Для каждого числа вычисляется остаток от деления на 9 суммы цифр. Производя действия над числами, производят такие же действия над этими остатками. Результат рассматриваемых действий над этими остатками должен отличаться от суммы цифр искомого результата на число, кратное девяти.

Конечно, если ошибка такова, что разность между найденной и истинной величинами кратна 9, то она при этом способе проверки не будет замечена.

По модулю m = 11 каждое число, записанное в десятичной системе счисления, будет сравнимо с суммой цифр, взятых справа налево попеременно со знаками „плюс” и „минус”; поэтому мы можем сформулировать следующий способ „проверки с помощью одиннадцати”. Для каждого числа вычисляется остаток от деления на 11 суммы цифр, взятых попеременно справа налево со знаками „плюс” и „минус”. Результат рассматриваемых действий над этими остатками должен отличаться от суммы взятых попеременно со знаками „плюс” и „минус” справа налево цифр искомого результата на число, кратное 11. Если ошибка будет кратна 11, она не будет замечена при этом способе.

При сложных вычислениях имеет смысл проводить две проверки: одну с помощью модуля 9, а другую с помощью модуля 11. В этом случае ошибка не будет замечена только, если она кратна 99, что, конечно, бывает очень редко.

Примеры. Проверим правильность выполнения действий (с помощью 9 и 11):

13547 – 9862=3685

1) $13547 \equiv 1+3+5+4+7 \equiv 2(\mathrm{mod}\ 9)$

$9862 \equiv 9+8+6+2 \equiv 7(\mathrm{mod}\ 9)$

$3685 \equiv 3+6+8+5 \equiv 4(\mathrm{mod}\ 9)$

$2 - 7 \equiv 4(\mathrm{mod}\ 9)$

$-5 \equiv 4(\mathrm{mod}\ 9)$

Сравнение подтверждает, но не гарантирует правильности выполнения действий.
2) $13547 \equiv 7+(-4)+5+(-3)+1 \equiv 6 \pmod{11}$
$9862 \equiv 2+(-6)+8+(-9) \equiv 6 \pmod{11}$
$3685 \equiv 5+(-8)+6+(-3) \equiv 0 \pmod{11}$
$6-6 \equiv 0 \pmod{11}$
$0 \equiv 0 \pmod{11}$
Проверка одиннадцатью подтверждает правильность получения результата.
Пример. Проверим правильность выполнения умножение (с помощью 9 и 11):
$4371 \cdot 1243 = 5433153$
1) $4371 \equiv 4+3+7+1 \equiv 6 \pmod 9$
$1243 \equiv 1+2+4+3 \equiv 1 \pmod 9$
$5433153 \equiv 5+4+3+3+1+5+3 \equiv 6 \pmod 9$
$6 \cdot 1 \equiv 6 \pmod 9$
$6 \equiv 6 \pmod 9$
Сравнение подтверждает, но не гарантирует правильности выполнения действий.
$4371 \equiv 1+(-7)+3+(-4) \equiv -7 \pmod{11}$
$1243 \equiv 3+(-4)+2+(-1) \equiv 0 \pmod{11}$
$5433153 \equiv 3+(-5)+1+(-3)+3+(-4)+5 \equiv 0 \pmod{11}$
$-7 \cdot 0 \equiv 0 \pmod{11}$
$0 \equiv 0 \pmod{11}$
Проверка одиннадцатью подтверждает правильность получения результата.
Пример. Проверим правильность возведение степени (с помощью 9 и 11):
$1965^2 = 3761225$
$1965 \equiv 1+9+6+5 \equiv 3 \pmod 9$
$3761225 \equiv 3+7+6+1+2+2+5 \equiv 8 \pmod 9$
$3 \cdot 3 \equiv 8 \pmod 9$
$9 \equiv 8 \pmod 9$
Сравнение не подтверждает правильности выполнения действий.
$1965 \equiv 5+(-6)+9+(-1) \equiv 7 \pmod{11}$
$3761225 \equiv 5+(-2)+2+(-1)+6+(-7)+3 \equiv 6 \pmod{11}$
$7 \cdot 7 \equiv 6 \pmod{11}$
$49 \equiv 6 \pmod{11}$
Проверка одиннадцатью подтверждает неправильность получения результата.
Пример. Проверим правильность деление (с помощью 9 и 11):
$421767:3429=123$
$421767 \equiv 4+2+1+7+6+7 \equiv 0 \pmod 9$
$3429 \equiv 3+4+2+9 \equiv 0 \pmod 9$
$123 \equiv 1+2+3 \equiv 6 \pmod 9$
$0 \cdot 6 \equiv 0 \pmod 9$
$0 \equiv 0 \pmod 9$
Сравнение подтверждает, но не гарантирует правильности выполнения действий.
$421767 \equiv 7+(-6)+7+(-1)+2+(-4) \equiv 5 \pmod{11}$
$3429 \equiv 9+(-2)+4+(-3) \equiv 8 \pmod{11}$
$123 \equiv 3+(-2)+1 \equiv 2 \pmod{11}$
$8 \cdot 2 \equiv 5 \pmod{11}$
$16 \equiv 5 \pmod{11}$
Проверка одиннадцатью подтверждает правильность получения результата.

В ходе работы мы получили ответ на вопрос о разрешимости неопределенных уравнений первой степени в целых числах; научились решать такие уравнения с помощью алгоритма Евклида; решили задачу, математической моделью которой является данное уравнение; решили в целых числах разными методами неопределенное уравнение первой степени. Проведенное нами исследование методов решения неопределенных уравнений первой степени позволяет нам сделать следующие выводы:

1) во всех методах, которые мы рассмотрели используются свойства делимости чисел;

2) зная одно частное решение уравнения, можно найти общее решение уравнения.

Литература:

1. Бухштаб А.А. Теория чисел. –М.: Государственное учебно-педагогическое издательство министерства просвещения РСФСР, 1960.
2. Соловьев Ю. Неопределенные уравнения первой степени. –М.: Квант, 1992.
3. Гельфонд А.О. Решение уравнений в целых числах. Популярные лекции по математике, – М.: Гостехиздат, 1957.
4. Литвер Е.Л. Теория чисел. – М.: МГУ, 1966.