МОУ «Белозерская средняя общеобразовательная школа»

Линейные диофантовые уравнения

Работу выполнили
Ученики 7 б класса
Киселёв Евгений
Петряков Иван

2011 год

Диофант представляет одну из занимательных загадок в истории математики. Мы не знаем, кем был Диофант, точные года его жизни, нам не известны его предшественники, которые работали бы в той же области, что и он.

На могиле Диофанта есть стихотворение – загадка.

Прах Диофанта гробница покоит: дивись ей — и камень

Мудрым искусством его скажет усопшего век.

Волей богов шестую часть жизни он прожил ребенком

И половину шестой встретил с пушком на щеках.

Только минула седьмая, с подругой он обручился;

С нею пять лет проведя, сына дождался мудрец.

Только полжизни отцовской возлюбленный сын его прожил,

Отнят он был у отца ранней могилой своей.

Дважды два года родитель оплакивал тяжкое горе,

Тут и увидел предел жизни печальной своей.

Решая которую нетрудно подсчитать, что Диофант прожил 84 года. О времени жизни Диофанта мы можем судить по работам французского исследователя науки Поля Таннри, и это, вероятно, середина III в.н.э.

Диофант практиковался в нахождении решений неопределенных уравнений вида $Ax^2 + Bx + C = y^2$, $Ax^3 + Bx^2 + Cx + D = y^2$ или систем таких уравнений. Типично для Диофанта, что его интересуют только положительные целые и рациональные решения. Иррациональные решения он называет «невозможными» и тщательно подбирает коэффициенты так, чтобы получились искомые положительные, рациональные решения.

Поэтому, обычно, произвольное неопределенное уравнение (но, как правило, все-таки с целыми коэффициентами) получает титул "диофантово", если хотят подчеркнуть, что его требуется решить в целых числах.

Неопределенные уравнения 1-й степени начали рассматриваться индусскими математиками позднее, примерно с V века. Первое общее решение уравнения первой степени $ax + by = c$, где a,b,c - целые числа, встречается у индийского мудреца Брахмагупты (ок. 625 г). Поэтому, строго говоря, нет оснований называть линейные неопределенные уравнения диофантовыми. Однако, исторически все же сложилось применять термин «диофантово», к любому уравнению, решаемому в целых числах.

Для того, чтобы решить диофантово уравнение, вспомним алгоритм Евклида нахождения НОД.

Алгоритм Евклида: для того, чтобы найти НОД двух чисел a и b, нужно выполнить последовательно несколько делений с остатком:

- $a = b\,q_1 + r_1$
- $b = r_1 q_2 + r_2$
- $r_1 = r_2 q_3 + r_3$
- $r_2 = r_3 q_4 + r_4$
- ……
- $r_{n-2} = r_{n-1} q_n + r_n$
- $r_{n-1} = r_n\, q_{n+1}$

На каждом шаге предыдущий делитель делится с остатком на предыдущий остаток. Так продолжается до тех пор, пока на каком-то шаге остаток не станет равен 0. Последний ненулевой остаток r_n равен НОД(a,b).

Пусть требуется решить линейное диофантово уравнение:

$ax + by = c$,

где a , b , $c \in \mathbf{Z}$; a и b - не нули.

Попробуем порассуждать, глядя на это уравнение.

Пусть $(a , b) = d$. Тогда $a = a_1 d$; $b = b_1 d$ и уравнение выглядит так:

$a_1 d \cdot x + b_1 d \cdot y = c$, т.е. $d \cdot (a_1 x + b_1 y) = c$.

Теперь у такого уравнения имеется решение (пара целых чисел x и y) только тогда, когда $c \vdots d$. Поскольку очень хочется решать это уравнение дальше, то пусть $c \vdots d$. Поделим обе части уравнения на d , и всюду далее будем считать, что (a , b) = 1.

Пример. $7x + 12y = 43$

Включаем алгоритм Евклида:

$12 = 7 \cdot 1 + 5$
$7 = 5 \cdot 1 + 2$
$5 = 2 \cdot 2 + 1$
$2 = 1 \cdot 2$

Значит, наибольший общий делитель чисел 7 и 12 равен 1 , а его линейное выражение таково:

$1 = 5 - 2\cdot 2 = 5 - (7 - 5)\cdot 2 = (12 - 7) - (7 - (12 - 7)\cdot 2) = 12\cdot 3 + 7\cdot (-5)$,

т.е. $u = -5$, $v = 3$. Частное решение:

$x_0 = uc = (-5)\cdot 43 = -215$
$y_0 = vc = 3\cdot 43 = 129$.

$x = -215 - 12t$
$y = 129 + 7t$

Частное решение

Мы договорились, что НОД(a, b) = 1. Это означает, что найдутся такие u и v из **Z**, что $au + bv = 1$, причем эти u и v мы легко умеем находить с помощью алгоритма Евклида. Умножим теперь равенство $au + bv = 1$ на c и получим: $a(uc) + b(vc) = c$, т.е. $x_0 = uc$, $y_0 = vc$.

Общее решение

Рассмотрим несколько случаев.

Случай 1. Пусть $c = 0$, уравнение имеет вид $ax + by = 0$. Находим, что

$$x = -\frac{b}{a}y .$$

Так как x должен быть целым числом, то $y = at$, где t - произвольное целое число. Значит $x = -bt$ и решениями однородного диофантова уравнения $ax + by = 0$ являются все пары вида $\{-bt , at\}$, где $t = 0; \pm 1; \pm 2;...$

Случай 2. Пусть теперь $c \neq 0$. Этот случай закрывается следующей теоремой.

Теорема. Пусть $(a , b) = 1$, $\{x_0 , y_0\}$ - частное решение диофантова уравнения $ax + by = c$. Тогда его общее решение задается формулами:

$$\begin{cases} x = x_0 - bt \\ y = y_0 + at . \end{cases}$$

Доказательство. То, что правые части указанных в формулировке теоремы равенств действительно являются решениями, проверяется их непосредственной подстановкой в исходное уравнение. Покажем, что любое решение уравнения $ax + by = c$ имеет именно такой вид, какой указан в формулировке теоремы. Пусть $\{x_1 , y_1\}$ - какое-

нибудь решение уравнения $ax + by = c$. Тогда $ax_1 + by_1 = c$, но ведь и $ax_0 + by_0 = c$. вычтем из первого равенства второе и получим:

$a(x_1 - x_0) + b(y_1 - y_0) = 0$

- однородное уравнение. Далее, глядя на случай 1, рассмотрение которого завершилось несколькими строками выше, пишем сразу общее решение: $x_1 - x_0 = -bt$, $y_1 - y_0 = at$, откуда получаем:

$$\begin{cases} x_1 = x_0 - bt, \\ y_1 = y_0 + at. \end{cases}$$

Мы договорились, что $(a, b) = 1$. Это означает, что найдутся такие u и v из $\mathbf{Z}$, что $au + bv = 1$, причем эти u и v мы легко умеем находить с помощью алгоритма Евклида. Умножим теперь равенство $au + bv = 1$ на c и получим: $a(uc) + b(vc) = c$, т.е. $x_0 = uc$, $y_0 = vc$.