5| # Диофантовы уравнения

Критерий разрешимости уравнений вида $ax+by=0$ в целых числах.

Нам понадобится следующая

Теорема. Если $ax=by$ $(a,b,x,y\in\mathbb{Z})$ и $НОД(a,b)=1$, то x и y можно представить в виде $\boxed{x=bt,\ y=at}$ для некоторого $t\in\mathbb{Z}$

Док-во. Рассм. два случая.

① $b\neq 0$. По условию, $(ax)\vdots b$, $НОД(a,b)=1$, поэтому $x\vdots b$ (почему?). Т.о., $x=bt$ для некот $t\in\mathbb{Z}$. Тогда $y=\frac{ax}{b}=\frac{abt}{b}=at$.

② $b=0$. Тогда $a\neq 0$ и исходное ур-ие принимает вид $ax=0$, откуда $x=0$. Т.к. $НОД(a,b)=1$, получаем $a=\pm 1$. Полагая $t=\frac{y}{a}$, имеем $y=at$, $x=0=0\cdot t=bt$ $(t\in\mathbb{Z}$, т.к. $a=\pm 1)$

Док-но.

Диофантово уравнение – это уравнение (с одним или несколькими неизвестными), для которого требуется найти решение в целых или рациональных числах

Простейшим диофантовым уравнением явл. ур-ие $\boxed{ax+by=c}$, где $a,b,c\in\mathbb{Z}$ и хотя бы один из коэффициентов a b не равен 0. Как по коэфф. этого ур-ия определить, имеет ли оно решения в $\mathbb{Z}$ и, если имеет, то как найти все эти решения?

6) На эти вопросы отвечают след. две теоремы.

Теорема Уравнение $\boxed{ax+by=c}$, где $a,b,c\in\mathbb{Z}$ и $a\cdot b\neq 0$ имеет решения в целых числах т.и т.т., когда $\boxed{c \vdots НОД(a,b)}$

Док-во $\Rightarrow$ Пусть это ур-ие имеет целочисленные решения, и пусть $(x_0,y_0)\in\mathbb{Z}^2$ - произвольное решение. Тогда $ax_0+by_0=c$. Очевидно, что $a \vdots НОД(a,b)$ и $b \vdots НОД(a,b)$, поэтому $c=(ax_0+by_0) \vdots НОД(a,b)$.

$\Leftarrow$ Имеет место

Теорема. Если $НОД(a,b)=1$ и $(x_0,y_0)\in\mathbb{Z}^2$ - некот. решение ур-ия $ax+by=c$, то все целочисл. решения этого ур-ия имеют вид

$$\begin{cases} x = x_0 - bt \\ y = y_0 + at \end{cases} \quad (t\in\mathbb{Z} \text{ - произвольное})$$

① Непосредственной подстановкой убеждаемся, что пара $(x_0-bt,\ y_0+at)$ яв. решением $\forall t\in\mathbb{Z}$.

② Пусть теперь $(x_1,y_1)\in\mathbb{Z}^2$ - произвольное решение, т.е. $ax_1+by_1=c$. Т.к (x_0,y_0) также яв. решен., то $ax_0+by_0=c$. Отсюда $a(x_0-x_1)=b(y_1-y_0)$. Т.к. $НОД(a,b)=1$, то по теореме, указанной ранее, $x_0-x_1=bt$, $y_1-y_0=at$ для некот. $t\in\mathbb{Z}$. Т.о., $x_1=x_0-bt$, $y_1=y_0+at$, т.е. все решения (из $\mathbb{Z}^2$) имеют такой вид ▶

Т.о., если $c \vdots НОД(a,b)$, то, разделив исходное

7] уравнение $ax+by=c$ на $НОД(a,b)$, получим эквивалентное ему ур-ие $a'x+b'y=c'$, в котором $НОД(a',b')=1$, и если бы удалось найти хотя бы одно (частное) решение этого ур-ия, мы получили бы общее решение из теоремы выше.

Итак, осталось понять, как найти какое-нибудь решение ур-ия $ax+by=c$ в случае, когда $НОД(a,b)=1$. Воспользуемся для этого следствием из алгоритма Евклида: $НОД(a,b)=au+bv$ для некот. $u,v\in\mathbb{Z}$. В нашем случае имеем $1=au+bv$ для некот. $u,v\in\mathbb{Z}$ (их можно найти из док-ва следствия из алгоритма Евкл.). Тогда $a(uc)+b(vc)=c$, следовательно, пара (uc,vc) явл. (частным) решением ур-ия $ax+by=c$.

Док-но