0 Введение

1. Диофант, Ферма и метод бесконечного спуска

„Арифметика" Диофант III н.э.

Перевод на арабский X в., на латинский XVII в.

Экземпляр Ферма содержал 48 замечаний

издан сыном Ферма: зам. 2 к задаче 8

из книги II „представить квадрат в виде суммы двух квадратов"

„Удивительное док-во"...

Упр 1 $x^2+y^2=z^2$ имеет примитивное решение в нат числах ($\neq 0$ целых)

$\Longleftrightarrow$: $\exists$ вз. простые числа $p>q\geq 0$ разной четности, что $z=p^2+q^2$ (и $x=2pq$, $y=p^2-q^2$ или наоборот)

Лемма 1 $vw=u^2 \Longleftrightarrow \exists\, a,b : v=a^2\ w=b^2$.
и $(v,w)=1$

"Д-во Ферма": методом беск. спуска.

Пред. что сущ-ет нетр. число v: (1) $vw=u^2$, $(v,w)=1$ и v неявл-ся кв. Мы покажем, что $\exists\, v'<v$ удовл. этим же условиям...

$\exists$ простое $p \mid v \Rightarrow p \mid u \Rightarrow p^2 \mid vw \Rightarrow p^2 \mid v$
$\Rightarrow v'p^2=v \Rightarrow \boxed{v'w=(u')^2}$ ↯

Т. 1 (Ферма) Ур-е $x^4+y^4=z^2$ не имеет решения в целых ненул. числах.

Д-во: $x^4+y^4=z^2$ можно считать, что x, y, z вз. прост. $\Rightarrow (x^2, y^2, z)$ – прим. пиф. тройка $\Rightarrow \exists\, p > q$ вз. пр. и разной чёт.:

$x^2=2pq \quad y^2=p^2-q^2 \quad z=p^2+q^2 \quad \Rightarrow$

(p, y, q) – прим. пиф. тройка, в частности, q нечётно и p чётно $\Rightarrow \exists\, a, b$ в.з. пр. разной чёт., т.ч. $p=2ab$ $y=a^2-b^2$, $q=a^2+b^2$

$\Rightarrow x^2=2pq=4ab(a^2+b^2)$ – полный квадрат $\Rightarrow$

т.к. a, b и a^2+b^2 вз. прост., то a, b и $a^2+b^2=z$ тоже полные кв-ты. Пусть $X^2=a$ $Y^2=b$ $\Rightarrow$

$$X^4+Y^4=a^2+b^2=z^2=p<p^2+q^2=z^2=x^4+y^4$$

Противоречие в силу м. б. спуска.

<u>Упр 2</u> Д-ть, а) $x^4-y^4=z^2$ не разрешимо в целых неотр. числах

б) площадь (рац.) прямоугольного тр-ка $\neq$ площади квадрата, т.е. система

$$\begin{cases} x^2+y^2=z^2 \\ xy=2u^2 \end{cases}$$

не разр. в целых неотр. числах

(2) Что нужно помнить из алгебры:

Кольцо, ком. кольцо с 1, R, R^* — обр. эл-ты кольца,

подкольцо

идеал и фактор-кольцо

Модуль M над кольцом R — аб. группа:

$a(x+y) = ax + ay$ $\forall a, b \in R$ $x, y \in M$

$(a+b)x = ax + bx$

$(ab)x = a(bx)$

$1 \cdot x = x$ [кольцо-модуль над собой]

подмодуль. —

Точный модуль $\mathrm{Ann}\, M = 0$

$\forall a \in R$ $\exists x \in M$: $ax \neq 0$.

x_0

$S \subseteq R$ подкольцо, пор. S

идеал, порожд. $S = \langle a_i r_i + r_i a_i \rangle$

$a_i \in R \quad r_i \in S$

главный идеал $= \langle a \rangle$

модуль, порожд. $\langle S \rangle$ ....

Нётеровость модуля, кольца

(1) всякий подмодуль (идеал) к.п.

(2) всякая возр. цепочка подм. (идеалов) обрывается.

Факты о нётеровых кольцах:

фактор-кольцо нёт. кольца нётерово

Делимость идеалы и области целостности:

Пусть R — область целостности.

Отн-е делимости $a \mid b \iff \exists\, c : ac = b$

$a \sim b \iff a \mid b$ и $b \mid a$ „ассоциированы"

Обратимый это $a \mid 1$, т.е. $\exists\, c : ac = 1$.

„единица"

$a \sim b \iff \exists$ обр. $c : a = cb$ (почему?)

необр. и ненул.

$\forall a$ <u>неприводим</u>, если $a = bc \Rightarrow$ либо b, либо c обратим.

необр. и ненул.

$\forall a$ <u>прост</u>, если $a \mid bc \Rightarrow a \mid b$ или $a \mid c$.

Лемма 1 R - обл. целостн. a - прост. $\Rightarrow$ a - неприв.

Д-во: $a = bc$ для $b, c \in R$. Т.к. a прост., то $a | b$ или $a | c$. Пусть $a | b \Rightarrow$
$\Rightarrow a = adc \Rightarrow a(1 - dc) = 0 \underset{R\text{-целост.}}{\Rightarrow} 1 = dc$
$\Rightarrow c$ обратим. $\Rightarrow a$ неприводим.

„Язык идеалов" $a | b \Rightarrow (a) \supseteq (b)$,
причём $a \sim b \Leftrightarrow (a) = (b)$.

Лемма 2 R - нёт. обл. целостности $\Rightarrow$ каждый необр. эл-т $(\neq 0)$ представим в виде пр-я неприводимых

Упр 3 Д-ть лемму 2

Опр 1. Обл. целостн. R наз-ся факториальным кольцом, если в нем каждый необр. ненулев. эл-т представим в виде пр-я неприв. эл-тов и это представление единств. с точн. до перестановки сомн-лей и умн-ия на обр. эл-т. (до ассоц).

Теорема 1. Обл. целостности R, допуск. разл. в неприв. факториальна $\Leftrightarrow$ любой неприв. эл-т прост.

Д-во: $\Rightarrow$) p – неприв. эл-т. Предп., что $p \mid ab$, т.е. $pc = ab$. Разложим на неприв. a, b и c. Имеем $p u_1 p_1 \ldots p_k = u_2 p'_1 \ldots p'_l \, u_3 q_1 \ldots q_m$. Из факт. $\Rightarrow$ $p \sim p'_i$ или $p \sim q_j$

$\Rightarrow$ $p \mid a$ или $p \mid b$

$\Leftarrow$) пусть $u_1 p_1 \ldots p_k = u_2 q_1 \ldots q_t$, где u_1, u_2 – обр.

$p_1 \ldots p_k$ и $q_1 \ldots q_t$ – неприв. Тогда $p_1 \sim q_i$, т.е.

$q_i = u p_1$. „Сократим" на p_1 получим по инд. единств. разложения. $\blacksquare$

Опр. Целост. R – кольцо гл. идеалов (PID), если любой идеал – главный, т.е. $I = \langle a \rangle$).

<u>Упр 4</u> Д-ть, что PID всегда факториально.

<u>Упр 5</u> Показать, что $R = \mathbb{Z}[\sqrt{-5}]$ нётерово не факториальное кольцо (<u>Указ</u> 2 – <u>неприв. в</u> R, но $2 \nmid 1 \pm \sqrt{-5}$, хотя $2 \mid 6 = (1+\sqrt{-5})(1-\sqrt{-5})$)