(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 задачек

Издан сыном Ферма: Зам. 2 к задаче 8

из книги II, предлагает квадрат в виде

суммы двух квадратов"

"Удивительное док-во"...

Ур-е $x^n+y^n=z^n$. Что такое примитивное решение?

Упр 1 Ур-е $x^2+y^2=z^2$ имеет примитивное (т.е. НОД$(x,y)=1$) решение в целых числах

$\Leftrightarrow$ $\exists$ вз. пр-ое числа $p>q>0$ разной четности, т.ч. $z=p^2+q^2$ (и $x=2pq$, $y=p^2-q^2$ или наоборот)

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

Док-во Ферма методом бесконечного спуска:

Пред. что сущ-ет число v: (1) $vw=u^2$, $(v,w)=1$ и v наим. кв-том. Мы докажем, что $\exists v'<v$ удов. тем же условиям, что даст нам противоречие.

$\exists$ простое $p \mid v \Rightarrow p \mid u \Rightarrow p^2 \mid vw \underset{(v,w)=1}{\Rightarrow} p^2 \mid v \Rightarrow$

$\exists v'$: $v=v'p^2$, $v'<v$ и v' не квадрат $\Rightarrow v' \cdot w=(u')^2$, противор-

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

1-ВО: $x^4+y^4=z^2$ можно считать, что x, y, z вз. прост. $\Rightarrow (x^2, y^2, z)$ – примит. пифагорова тройка $\Rightarrow \exists\, p > q$ вз. пр. и разной четности:

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

(y, q, p) – примит. пифагорова тройка, в частности, p нечетно и q четно $\Rightarrow \exists\, a, b$ взаимно простые разной четности, т.ч. $q=2ab \quad y=a^2-b^2, \quad p=a^2+b^2$

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

Т.к. a, b и a^2+b^2 вз. просты, то a, b и a^2+b^2 — тоже полные кв-ты. Пусть $X^2=a$, $Y^2=b$ =>

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

Противоречие по методу бесконечного спуска.

<u>Следствие</u> Если $x^n+y^n=z^n$ не имеет решений для всех нечетных простых n, то оно не имеет реш. $\forall n\geq 3$.

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

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

$$\begin{cases} x^2+y^2=z^2 \\ \frac{1}{2}xy=u^2 \end{cases}$$

не разр. в целых неотр. числах.

2. Квадратичный закон взаимности Гаусса

Опр 1 Пусть $a, m \in \mathbb{Z}^*$ и $(a,m)=1$. Число a НЗ-сч квадратичным вычетом по модулю m, если разрешимо сравнение $x^2 \equiv a \pmod m$, и квадр. невычетом в противном случае.

Пример По модулю 7 $(\pm 1)^2, (\pm 2)^2, (\pm 3)^2$ сравнимы соот-но с 1, 4 и 2 $\Rightarrow$ 2 – кв. вычет по mod 7, а 3 – кв.

Несложно понять, что $\forall$ простого случая, когда m – простое.

Предл 1 Пусть $m = 2^k p_1^{k_1} \cdots p_s^{k_s}$ — разл. на простые и $(a, m) = 1$.
a — квадр. вычет mod m $\Leftrightarrow$ а) $x^2 \equiv a \pmod{p_i}$
$\forall i = 1..s$ и б) $a \equiv 1 \pmod 4$ $k = 2$
$a \equiv 1 \pmod 8$ $k \geq 3$.

Упр 3 Δ-п предл. 1.
Сравнение $x^2 \equiv a \pmod p$ удобно описывать в $\mathbb{F}_p$.

Предл 2 Для нечетного простого числа p имеется
мн-во $(\mathbb{F}_q^*)^2$ всех ненул. кв-тов поля $\mathbb{F}_q$ — это ядро гом-зма $x \mapsto x^{(q-1)/2}$ из $\mathbb{F}_q^*$ на $\{\pm 1\}$. В частности, $|\mathbb{F}_q^* : (\mathbb{F}_q^*)^2| = 2$.

Δ-во: Пусть $\mathbb{F} = \mathbb{F}_q$ и $\overline{\mathbb{F}}$ — ее алг. замк.

$\forall x \in F^* \ \exists y \in \overline{F} : y^2 = x$. Тогда $y^{q-1} = x^{\frac{q-1}{2}} = \pm 1$, т.к. $x^{q-1} = 1$ по т-ме Лагранжа. Эл-т x - кв-т поля F $\Leftrightarrow$ $y \in F$, т.е $y^{q-1} = 1$. Поэтому $(F^*)^2$ — ядро гом-зма $x \mapsto x^{\frac{q-1}{2}}$. ▨

Упр 4 Доказать, что при $p=2$, любой эл-т $\mathbb{F}_q$ — квадрат.

Опр 2 Пусть $p \neq 2$ - простое и $x \in \mathbb{F}_p^*$. Символ Лежандра $\left(\frac{x}{p}\right) = x^{(p-1)/2} \in \{\pm 1\}$. Положим $\left(\frac{0}{p}\right) = 0$ и $\forall x \in \mathbb{Z}$ $\left(\frac{x}{p}\right) = \left(\frac{\overline{x}}{p}\right)$, где $\overline{x}$ - образ x в $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

(Лежандр и Дирихле д-ли т. Ферма для $n=5$)

Предл 3 (Св-ва символа Лежандра) Пусть p – нечет. прост.

1) $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$

2) $\left(\frac{1}{p}\right) = 1$

3) $\left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)}$, $\varepsilon(p) = p \overset{(2)}{=} \frac{p-1}{2}$ ← Критерий Эйлера (т. нужна для $n=3$)

$\varepsilon(n) = \begin{cases} 0, & n \equiv 1 \pmod 4 \\ 1, & n \equiv -1 \pmod 4 \end{cases}$

4) $\left(\frac{2}{p}\right) = (-1)^{\omega(p)}$, $\omega(p) = \frac{p^2-1}{8}$ (2)

$\omega(n) = \begin{cases} 0, & n \equiv \pm 1 \pmod 8 \\ 1, & n \equiv \pm 5 \pmod 8. \end{cases}$

Δ-во: $1|x \mapsto \left(\frac{x}{p}\right)$ – гом-зм.

2 и 3) очевидно из $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$

Δ сказан 4)

Пусть $\alpha \in \overline{\mathbb{F}}_p$ — прим. корень 8-ой степени из 1.

Тогда $\alpha^4 = -1 \Rightarrow \alpha^2 + \alpha^{-2} = 0 \Rightarrow (\alpha + \alpha^{-1})^2 = 2$.

Обозн: $y = \alpha + \alpha^{-1}$. Имеем $y^p = \alpha^p + \alpha^{-p}$ и $y^{p-1} = \left(\frac{2}{p}\right)$.

Если $p \equiv \pm 1 \ (8) \Rightarrow y^p = y \Rightarrow y^{p-1} = 1 = \left(\frac{2}{p}\right)$

Если $p \equiv \pm 5 \ (8) \Rightarrow y^p = \alpha^5 + \alpha^{-5} = -(\alpha + \alpha^{-1}) = -y \Rightarrow$

$y^{p-1} = -1 = \left(\frac{2}{p}\right)$ $\quad \left[\alpha + \alpha^3 + \alpha^5 + \alpha^7 = 0\right]$ ∎

Теорема 1 (Гаусс, 1801) Пусть p и ℓ — разл. простые числа.

Тогда $\left(\frac{\ell}{p}\right)\left(\frac{p}{\ell}\right) = (-1)^{\frac{\ell-1}{2} \cdot \frac{p-1}{2}} = (-1)^{\varepsilon(\ell)\varepsilon(p)}$.

Квадр. закон вз-сти: p и ℓ одновр. вычеты $\Leftrightarrow$ p или $\ell \equiv 1 \ (4)$

Эйлер 1783, Лежандр 1785.... $\quad$ (p − вч $\Leftrightarrow$ ℓ невыч) $\Leftrightarrow$ $p, \ell \equiv -1 \ (4)$.

Д-во: $w \in \overline{\mathbb{F}_p}$ – прим. корень ℓ-ой ст. из 1 в алг. замк. поле $\mathbb{F}_p$.

Если $x \in \mathbb{F}_\ell$, то w^x однозн. определена, т.к. $w^\ell = 1$.

Поэтому корректно опр-но "сумма Гаусса":

$$y = \sum_{x \in \mathbb{F}_\ell} \left(\frac{x}{\ell}\right) w^x \qquad (*)$$

Лемма 1 $y^2 = (-1)^{\varepsilon(\ell)} \ell$ $\quad \varepsilon(\ell) = (\ell-1)/2$

$\ell = \overline{\ell}$ – образ ℓ в $\mathbb{F}_p$.

Д-во: $y^2 = \sum_{t,z \in \mathbb{F}_\ell} \left(\frac{tz}{\ell}\right) w^{t+z} \underset{u=t+z}{=} \sum_{u \in \mathbb{F}_\ell} w^u \left(\sum_{t \in \mathbb{F}_\ell} \left(\frac{t(u-t)}{\ell}\right)\right)$.

Если $t \neq 0$, то $\left(\frac{t(u-t)}{\ell}\right) = \left(\frac{-t^2}{\ell}\right)\left(\frac{1-ut^{-1}}{\ell}\right) =$

$= (-1)^{\varepsilon(\ell)} \left(\frac{1-ut^{-1}}{\ell}\right) \Rightarrow (-1)^{\varepsilon(\ell)} y^2 = \sum_{u \in \mathbb{F}_\ell} C_u w^u$, где

$$C_u = \sum_{t \in \mathbb{F}_\ell^*} \left(\frac{1-ut^{-1}}{\ell}\right).$$

Если $u = 0$, то $C_u = \sum_{t \in \mathbb{F}_\ell^*} \left(\frac{1}{\ell}\right) = \ell - 1$.

Если $u \neq 0$, то $s = 1 - ut^{-1}$ пробегает все $\mathbb{F}_\ell \setminus \{1\} \Rightarrow$

$$C_u = \sum_{s \in \mathbb{F}_\ell} \left(\frac{s}{\ell}\right) - \left(\frac{1}{\ell}\right) = -\left(\frac{1}{\ell}\right) = -1, \text{ т.к. } |\mathbb{F}_\ell^* : (\mathbb{F}_\ell^*)^2| = 2.$$

Поэтому $\sum_{u \in \mathbb{F}_\ell} C_u w^u = (\ell - 1) - \sum_{u \in \mathbb{F}_\ell^*} w^u = \ell$ ▣

т.к. $\sum_{u \in \mathbb{F}_\ell} w^u = 0$!

Лемма 2 $y^{p-1} = \left(\frac{p}{\ell}\right)$.

Δ-во: т.к. $\operatorname{char} \mathbb{F}_p = p \Rightarrow y^p = \sum_{x \in \mathbb{F}_\ell} \left(\frac{x}{\ell}\right) w^{xp} =$

$$\sum_{z \in \mathbb{F}_\ell} \left(\frac{zp^{-1}}{\ell}\right) w^z = \left(\frac{p^{-1}}{\ell}\right) \sum_{z \in \mathbb{F}_\ell} \left(\frac{z}{\ell}\right) w^z = \left(\frac{p^{-1}}{\ell}\right) y = \left(\frac{p}{\ell}\right) y$$ ▣

Чтобы закончить д-во теоремы, осталось заметить:

$$\left(\frac{p}{e}\right) \underset{\uparrow 1.2}{=} y^{\frac{p-1}{2}} = \left(y^2\right)^{\frac{p-1}{2}} \underset{\text{л.1+ опр. с. Лежандра}}{=} \left(\frac{(-1)^{\varepsilon(e)} e}{p}\right) = \left(\frac{e}{p}\right)\left(\frac{(-1)^{\varepsilon(e)}}{p}\right)$$

$$= \left(\frac{e}{p}\right)(-1)^{\varepsilon(p)\varepsilon(e)}$$

Пример $\left(\frac{29}{43}\right) \underset{\varepsilon(29)=0}{=} \left(\frac{43}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) \underset{\omega(29)=1}{=} -\left(\frac{7}{29}\right) =$

$$= -\left(\frac{29}{7}\right) = -\left(\frac{1}{7}\right) = -1.$$

Упр 5 При каких простых p мн-н t^2+2 неприводим над $\mathbb{F}_p$?