ТЕОРЕМА МИНКОВСКОГО. ПРИЛОЖЕНИЯ

записано лично Паниной Г.

Лемма 10.1. *Пусть p – нечетное простое число, $p \equiv 1(mod4)$. Тогда найдется такое $a \in \mathbb{Z}$, что $a^2 \equiv -1(modp)$.*

Доказательство. С одной стороны,
$1 \cdot 2 \cdot ... \cdot (p-1) = \underbrace{1 \cdot 2 \cdot ... \frac{p-1}{2}}_{*}(\frac{p-1}{2}+1) \cdot ... \cdot (p-2)(p-1) \equiv *^2(-1)^{\frac{p-1}{2}} \equiv$
$*^2(modp)$. С другой стороны, $1 \cdot 2 \cdot ... \cdot (p-1) = 1 \cdot 2 \cdot ... k ... k^(-1) \cdot (p-1) \equiv p-1$ (Каждое число сокращается с обратным по модулю p. Без пар остаются только 1 и $p-1$. Отсюда $*^2 = -1$. □

Задача 10.2. *Всякое простое $p \equiv 1(mod4)$ есть сумма двух квадратов целых чисел.*

Указание. Нужно взять a из леммы и рассмотреть в $\mathbb{R}^2$ решетку, порожденую базисом
$u_1 = (p, 0)$
$u_2 = (a, 1)$
В качестве C взять круг радиуса $\sqrt(2p)$ и применить теорему Минковского.

Теорема 10.3. ***Теорема Лагранжа.*** *Любое натуральное число представимо в виде суммы четырех квадратов целых чисел.*

Докажем вначале две леммы.

Лемма 10.4. *Если числа m, n – суммы четырех квадратов, то их произведение mn – тоже сумма четырех квадратов.*

Доказательство.
$(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+t^2) = (ax+by+cz+dt)^2 + (-ay+bx-ct+dz)^2 + (-az+cx-dy+bt)^2 + (-at+dx-bz+cy)^2$.
Смысл этого тождества на языке кватернионов таков: модуль произведения кватернионов равен произведению модулей. □

Лемма 10.5. *Для всякого простого p найдутся целые a и b такие, что $a^2 + b^2 \equiv -1(modp)$.*

Доказательство. Среди ненулевых вычетов по модулю p ровно половина – квадраты. Всего квадратов (включая 0), следовательно, $\frac{p+1}{2}$ штук. Пар вычетов (x, y) таких, что $x + y \equiv -1(modp)$ – столько же, причем там есть исключительная пара вида $x+x \equiv -1(mod p)$. По принципу Дирихле, либо в одной из пар оба члена – квадраты (и лемма доказана), либо в каждой паре по одному. Тогда нас спасет исключительная пара. $\square$

Задача 10.6. *Всякое простое p есть сумма четырех квадратов целых чисел. Отсюда следует теорема Лагранжа.*

Указание. Нужно взять a, b из леммы и рассмотреть в $\mathbb{R}^4$ решетку, порожденую базисом
$u_1 = (p, 0, 0, 0)$
$u_2 = (0, p, 0, 0)$
$u_3 = (a, b, 1, 0)$
$u_4 = (-b, a, 0, 1)$
В качестве C взять круг радиуса $\sqrt{(2p)}$ (его объем равен $2p^2\pi^2$) и применить теорему Минковского.

E-mail address: `marinakn@mail.ru`