Формулировка

Любое простое число $p = 4k + 1$, $k \in \mathbb{N}$ представимо в виде суммы двух квадратов натуральных чисел.

Первое доказательство

1. Докажите, что для любого простого числа $p = 4k + 1$, $k \in \mathbb{N}$ найдётся q, такое что

$$q^2 + 1 \equiv 0\ (mod\ p)$$

2. **Лемма Туэ**. Пусть n — натуральное число, большее единицы. Тогда для всякого натурального a, взаимно простого с n, существуют такие натуральные x и y, не превосходящие $\sqrt{n}$, что $ay \equiv \pm x\ (mod\ n)$.
3. Докажите рождественскую теорему Ферма.

Второе доказательство (мельницы)

4. Обозначим через S множество всех решений уравнения $a^2 + 4bc = p$. Рассмотрим отображение

$$f(a,b,c) = \begin{cases} (a + 2b, c - a - b, b) & \text{если } a + b < c \\ (a - 2c, c, a + b - c) & \text{если } c < a + b \text{ и } 2c < a \\ (2c - a, a + b - c, c) & \text{если } c < a + b \text{ и } a < 2c \end{cases}$$

Проверьте, что f отображает множество S в себя и более того является инволюцией, то есть $f(f(x)) = x$.
5. Сколько существует неподвижных точек у отображения f?
6. И ещё раз докажите рождественскую теорему Ферма.

Общие мысли

7. Докажите, что натуральное число n разлагается в сумму двух квадратов, если и только если все простые делители вида $p = 4k + 3$ в разложение n входят в чётной степени. Сколько существует таких разложений?
8. Числа вида $z = a + ib$, где $a, b \in \mathbb{Z}$ называются Гауссовыми числами или просто целыми комплексными числами. Сформулируйте и докажите ОТА для целых комплексных чисел.
9. Докажите, что число $n^7 + 7$ не является точным квадратом для всех целых чисел n.