Доказательства теоремы Ферма-Эйлера

$*$ Пусть $p \in \mathbb{P}$, $p \equiv_4 1$. $*$

!! **Теорема Ферма-Эйлера.**

p представимо в виде суммы двух квадратов, т.е. $\exists m, n \in \mathbb{N}$, т.ч. $p = m^2 + n^2$.

1. **Теорема Вильсона.** Докажите, что $(p-1)! \equiv_p -1$.

2. **Следствие из теоремы Вильсона.**

   Докажите, что найдется целое z, такое что $z^2 + 1 \,\vdots\, p$.

3. **Доказательство с помощью леммы Туэ.**

   (a) Докажите, что найдутся $x, y \in \mathbb{Z} \cap [0, \sqrt{p})$ такие, что $\left[\begin{array}{l} zx \equiv_p y \\ zx \equiv_p -y \end{array}\right.$.

   (b) Докажите, что p представимо в виде суммы двух квадратов.

4. **Доказательство методом спуска.**

   Пусть $m \in \mathbb{N}$ — наименьшее число такое, что $mp = x^2 + y^2$ (где $x, y \in \mathbb{N}$).

   (a) Докажите, что m существует и нечётно.

   (b) Предположим, что $m > 1$. Пусть $\hat{x}, \hat{y}$ — абсолютно минимальные остатки от деления x, y на m (т.е. $x \equiv_m \hat{x}$, $y \equiv_m \hat{y}$, $|\hat{x}|, |\hat{y}| < m/2$); $\hat{x}^2 + \hat{y}^2 = km$ (очевидно, $k \in \mathbb{N}$). Докажите, что kp представимо в виде суммы двух квадратов и $k < m$.

5. **Доказательство из леммы Минковского.**

   Пусть $z^2 + 1 = cp$. Рассмотрим фигуру $px^2 + 2zxy + cy^2 < t$ на декартовой координатной плоскости Oxy.

   (a) Чем является эта фигура? Какова её площадь (в зависимости от p, z, c, t)?

   (b) Докажите, что уравнение $px^2 + 2zxy + cy^2 = 1$ имеет ненулевое целочисленное решение (x, y).

   (c) Докажите, что p представимо в виде суммы двух квадратов.

6. **Доказательство из факториальности кольца гауссовых чисел.**

   (a) Докажите, что в разложении $z^2 + 1$ на произведение простых в $\mathbb{Z}[\mathrm{i}]$ нет вещественных множителей, а все невещественные множители разбиваются на пары сопряженных.

   (b) Докажите, что p представимо в виде суммы двух квадратов.

Доказательства теоремы Ферма-Эйлера

$*$ Пусть $p \in \mathbb{P}$, $p \equiv_4 1$. $*$

!! **Теорема Ферма-Эйлера.**

p представимо в виде суммы двух квадратов, т.е. $\exists m, n \in \mathbb{N}$, т.ч. $p = m^2 + n^2$.

1. **Теорема Вильсона.** Докажите, что $(p-1)! \equiv_p -1$.

2. **Следствие из теоремы Вильсона.**

   Докажите, что найдется целое z, такое что $z^2 + 1 \vdots p$.

3. **Доказательство с помощью леммы Туэ.**

   (a) Докажите, что найдутся $x, y \in \mathbb{Z} \cap [0, \sqrt{p})$ такие, что $\left[\begin{array}{c} zx \equiv_p y \\ zx \equiv_p -y \end{array}\right.$.

   (b) Докажите, что p представимо в виде суммы двух квадратов.

4. **Доказательство методом спуска.**

   Пусть $m \in \mathbb{N}$ — наименьшее число такое, что $mp = x^2 + y^2$ (где $x, y \in \mathbb{N}$).

   (a) Докажите, что m существует и нечётно.

   (b) Предположим, что $m > 1$. Пусть $\hat{x}, \hat{y}$ — абсолютно минимальные остатки от деления x, y на m (т.е. $x \equiv_m \hat{x}$, $y \equiv_m \hat{y}$, $|\hat{x}|, |\hat{y}| < m/2$); $\hat{x}^2 + \hat{y}^2 = km$ (очевидно, $k \in \mathbb{N}$). Докажите, что kp представимо в виде суммы двух квадратов и $k < m$.

5. **Доказательство из леммы Минковского.**

   Пусть $z^2 + 1 = cp$. Рассмотрим фигуру $px^2 + 2zxy + cy^2 < t$ на декартовой координатной плоскости Oxy.

   (a) Чем является эта фигура? Какова её площадь (в зависимости от p, z, c, t)?

   (b) Докажите, что уравнение $px^2 + 2zxy + cy^2 = 1$ имеет ненулевое целочисленное решение (x, y).

   (c) Докажите, что p представимо в виде суммы двух квадратов.

6. **Доказательство из факториальности кольца гауссовых чисел.**

   (a) Докажите, что в разложении $z^2 + 1$ на произведение простых в $\mathbb{Z}[\mathrm{i}]$ нет вещественных множителей, а все невещественные множители разбиваются на пары сопряженных.

   (b) Докажите, что p представимо в виде суммы двух квадратов.