Рубрика “Наукообразие на кружке”

Теорема. Натуральное число n представимо в виде суммы двух квадратов $\Leftrightarrow$ все его простые делители вида $4k+3$ входят в четных степенях.

Лемма 1. Пусть $p > 2$ простое число. Сравнение $x^2 \equiv -1 \pmod p$ разрешимо тогда и только тогда, когда $p = 4k+1$.

1. Пусть x – остаток по модулю p. Рассмотрим четверку чисел $x, -x, x^{-1}, -x^{-1}$. Докажите, что различные четверки не пересекаются.

2. Бывает ли так, что внутри четверки некоторые числа совпадают? В каких случаях это может произойти? Рассмотрите все варианты.

3. Посчитайте все четверки чисел по модулю p для случаев $p = 4k+1$ и $p = 4k+3$. Докажите **Лемму 1**.

   Лемма 2. Пусть $p = 4k+1$. Тогда при некоторых a и b выполняется $p = a^2+b^2$.

   Пусть $s^2 \equiv -1 \pmod p$, $M = \{0, 1, 2, \dots, [\sqrt{p}]\}$, $x, y \in M$.

4. Докажите, что количество различных пар чисел (x, y) больше p.

5. Докажите, что при некоторых x_1, y_1, x_2, y_2 выполнено $x_1 + sy_1 \equiv x_2 + sy_2$.

6. Пусть $a = x_1 - x_2$, $b = y_1 - y_2$. Докажите, что $a^2 + b^2 \equiv 0 \pmod p$.

7. Докажите, что $a^2 + b^2 = p$.

   Лемма 3. Пусть некоторые m, n представимы в виде суммы двух квадратов. Тогда их произведение $m \cdot n$ тоже представимо.

8. Рассмотрим два комплексных числа $z_1 = a_1 + ib_1$ и $z_2 = a_2 + ib_2$. Чему равно их произведение? Чему равно произведение $|z_1|^2 \cdot |z_2|^2$? Докажите **Лемму 3**.

   Лемма 4. Пусть $n = a^2 + b^2$, $p = 4k+3$, $n \,\vdots\, p$. Тогда $a \,\vdots\, p$ и $b \,\vdots\, p$.

9. Воспользуйтесь **Леммой 1** и докажите **Лемму 4**.

10. Докажите **Следствие.** Пусть $n = a^2 + b^2$, $p = 4k+3$, $n \,\vdots\, p$. Тогда $n \,\vdots\, p^2$.

11. При помощи **Лемм 2–4** докажите **Теорему**.