

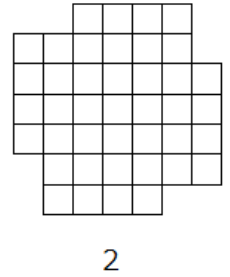
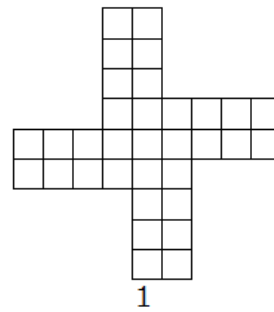
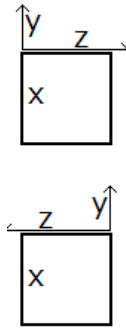
## 9 июля

1. а) Докажите, что если  $x^2 + y^2$  делится на простое число  $p = 4k + 3$ , то числа  $x$  и  $y$  делятся на  $p$ .  
б) Докажите, что в разложение на простые множители числа вида  $x^2 + y^2$  простое число  $p = 4k + 3$  обязательно входит в четной степени (возможно, нулевой).
2. Докажите, что если простое число  $p = 4k + 1$ , то существует такое  $b$ , что  $b^2 + 1 : p$ .
3. **Рождественская теорема Ферма.** Пусть простое число  $p = 4k + 1$ , и  $b$  – целое число, такое, что  $b^2 + 1 : p$ .  
а) Докажите, что найдутся пары остатков  $(x_1, y_1), (x_2, y_2)$  такие, что  $0 \leq x_i, y_i \leq [\sqrt{p}]$  и  $x_1 - by_1 \equiv x_2 - by_2 \pmod{p}$ .  
б) Докажите, что найдется пара остатков  $(x, y)$  такая, что  $0 \leq x, y \leq [\sqrt{p}]$ , и при этом  $x \equiv \pm by \pmod{p}$ .  
в) Докажите, что найдется пара остатков  $(x, y)$  такая, что  $x^2 + y^2 = p$ .
4. а) Докажите, что произведение двух натуральных чисел, представимых в виде суммы двух квадратов целых чисел, тоже является суммой квадратов двух целых чисел.  
б) **Теорема Ферма-Эйлера.** Натуральное число представимо в виде суммы двух квадратов целых чисел тогда и только тогда, когда каждый простой делитель вида  $4k + 3$  входит в его разложение в четной степени.
5. а) Пусть  $p$  – нечётное простое число. Докажите, что существует ровно  $\frac{p+1}{2}$  таких остатков  $a$ , для которых найдется  $x$  такой, что  $x^2 \equiv a \pmod{p}$ .  
б) Докажите, что найдётся четверка чисел  $a, b, c, d$  такая, что  $a^2 + b^2 + c^2 + d^2 : p$  и при этом не все числа  $a, b, c, d$  делятся на  $p$ .  
в) Пусть  $m$  – минимальное натуральное число, для которого существуют  $a, b, c, d$  такие, что  $a^2 + b^2 + c^2 + d^2 = mp$ . Докажите, что  $m \leq p - 1$ .  
г) Докажите, что если бы  $a^2 + b^2 + c^2 + d^2 = mp$  было чётным числом, то  $\frac{mp}{2}$  тоже бы являлось суммой четырёх точных квадратов целых чисел.  
д) Докажите, что найдутся такие  $x, y, z, w$ , что  $a - x \equiv b - y \equiv c - z \equiv d - w \equiv 0 \pmod{m}$  и  $x^2 + y^2 + z^2 + w^2 = mn$ , где  $0 < n \leq m - 1$ .  
е) Докажите, что произведение двух натуральных чисел, представимых в виде суммы четырёх квадратов целых чисел, является суммой квадратов четырёх целых чисел.  
ж) Докажите, что  $mp \cdot mn$  является суммой четырёх квадратов, делящихся на  $m^2$ .  
з) Докажите, что  $m = 1$ .  
и) **Теорема Лагранжа.** Докажите, что любое натуральное число представимо в виде суммы четырёх квадратов целых чисел.
6. Докажите, что числа вида  $n = 4^m(8k + 7)$  не представимы в виде суммы трёх квадратов.  
PS. **Теорема Лежандра** утверждает, что все остальные натуральные числа представимы в виде суммы трёх квадратов, но мы не будем её доказывать.

7. Еще одно доказательство рождественской теоремы Ферма.

Рассмотрим число  $p$  вида  $4k + 1$  и представим его в виде  $p = x^2 + 4yz$ , где  $x, y, z$  – натуральные числа. Такие представления существуют, например,  $p = 1^2 + 4 \cdot 1 \cdot k$ . Посчитаем общее количество таких представлений. По представлению  $(x, y, z)$  построим «мельницы» по схеме на картинке.

К квадрату со стороной  $x$  приставим прямоугольник высотой  $y$  и шириной  $z$  к левому верхнему углу (левая мельница) или к правому верхнему углу (правая мельница). Далее поворотом вокруг центра квадрата добавим еще 3 прямоугольника.



Например, мельница под номером 1 соответствует представлениям  $33 = 3^2 + 4 \cdot 3 \cdot 2$  (левая мельница для  $(3, 3, 2)$ ) и  $33 = 1^2 + 4 \cdot 4 \cdot 2$  (правая мельница для  $(1, 4, 2)$ ).

а) Каким представлениям какого  $p$  соответствует мельница 2?

б) Докажите, что если  $p$  – простое, то мельница не может соответствовать более, чем двум представлениям.

в) При простом  $p$  найдите все мельницы, которые соответствуют ровно одному представлению.

г) Докажите, что при простом  $p$  общее количество мельниц нечетно.

д) Докажите, что среди представлений найдется такое, что  $y = z$ .

е) Завершите доказательство теоремы.

$$\ddot{E} \neq E$$