

Сумма двух квадратов

9 июля

1. Решите в целых числах уравнение $x_1^4 + x_2^4 + \dots + x_7^4 = 100000000000002024$.
2. Каково наибольшее количество подряд идущих натуральных чисел, ни одно из которых нельзя представить в виде ab^2 , где a и b взаимнопросты, $b > 1$?

Определение. Пусть p — простое число, x — ненулевой остаток. Множество $\{x, 2x, 3x, \dots, (p-1)x\}$ образует *полную систему вычетов*, т.е. каждый остаток встречается в ней ровно один раз. Остаток y , такой что $xy \equiv 1 \pmod{p}$, называется *обратным к x* и обозначается x^{-1} .

3. Пусть p — нечётное простое число. Для ненулевого остатка x рассмотрим множество $M_x = \{x, -x, x^{-1}, -x^{-1}\}$.
 - (а) Докажите, что любые два таких множества не пересекаются, либо совпадают.
 - (б) Докажите, что все множества, кроме, быть может, двух, состоят ровно из четырёх элементов.
 - (в) Сделайте вывод, что уравнение $x^2 \equiv -1 \pmod{p}$ имеет решение в том и только том случае, если $p \equiv 1 \pmod{4}$.
4. (а) Пусть p — простое число вида $4k + 3$. Докажите, что если сумма квадратов натуральных чисел $a^2 + b^2$ делится на p^{2m-1} , то a и b делятся на p^m .
 - (б) Докажите, что существует бесконечно много натуральных чисел, которые дают остаток 1 по модулю 4, но не представимы в виде суммы двух квадратов.
5. Докажите, что простых чисел вида (а) $4k + 1$; (б) $4k + 3$ бесконечно много.
6. Докажите, что если a и b — натуральные и $2^a \equiv 2^b \pmod{101}$, то $a \equiv b \pmod{100}$.

Теорема(Критерий Эйлера). Уравнение $x^2 \equiv a \pmod{p}$ имеет решение в том и только том случае, если $a^{(p-1)/2} \equiv 1 \pmod{p}$.

7. (а) Пусть t — количество чётных чисел, больших $p/2$, но меньших p . Докажите, что

$$2 \cdot 4 \cdot \dots \cdot (p-1) \equiv (-1)^t \cdot 1 \cdot 2 \cdot \dots \cdot \left(\frac{p-1}{2}\right).$$

- (б) Пользуясь критерием Эйлера, установите, для каких p имеют решения уравнения $x^2 \equiv -1$, $x^2 \equiv 2$, $x^2 \equiv -2$. Результаты запишите в таблицу:

	$8k + 1$	$8k + 3$	$8k + 5$	$8k + 7$
-1				
2				
-2				

8. Докажите, что простых чисел вида $8k + 3$, $8k + 5$ и $8k + 7$ бесконечно много.

Сумма двух квадратов

9 июля

1. Решите в целых числах уравнение $x_1^4 + x_2^4 + \dots + x_7^4 = 100000000000002024$.
2. Каково наибольшее количество подряд идущих натуральных чисел, ни одно из которых нельзя представить в виде ab^2 , где a и b взаимнопросты, $b > 1$?

Определение. Пусть p — простое число, x — ненулевой остаток. Множество $\{x, 2x, 3x, \dots, (p-1)x\}$ образует *полную систему вычетов*, т.е. каждый остаток встречается в ней ровно один раз. Остаток y , такой что $xy \equiv 1 \pmod{p}$, называется *обратным к x* и обозначается x^{-1} .

3. Пусть p — нечётное простое число. Для ненулевого остатка x рассмотрим множество $M_x = \{x, -x, x^{-1}, -x^{-1}\}$.
 - (а) Докажите, что любые два таких множества не пересекаются, либо совпадают.
 - (б) Докажите, что все множества, кроме, быть может, двух, состоят ровно из четырёх элементов.
 - (в) Сделайте вывод, что уравнение $x^2 \equiv -1 \pmod{p}$ имеет решение в том и только том случае, если $p \equiv 1 \pmod{4}$.
4. (а) Пусть p — простое число вида $4k + 3$. Докажите, что если сумма квадратов натуральных чисел $a^2 + b^2$ делится на p^{2m-1} , то a и b делятся на p^m .
 - (б) Докажите, что существует бесконечно много натуральных чисел, которые дают остаток 1 по модулю 4, но не представимы в виде суммы двух квадратов.
5. Докажите, что простых чисел вида (а) $4k + 1$; (б) $4k + 3$ бесконечно много.
6. Докажите, что если a и b — натуральные и $2^a \equiv 2^b \pmod{101}$, то $a \equiv b \pmod{100}$.

Теорема(Критерий Эйлера). Уравнение $x^2 \equiv a \pmod{p}$ имеет решение в том и только том случае, если $a^{(p-1)/2} \equiv 1 \pmod{p}$.

7. (а) Пусть t — количество чётных чисел, больших $p/2$, но меньших p . Докажите, что

$$2 \cdot 4 \cdot \dots \cdot (p-1) \equiv (-1)^t \cdot 1 \cdot 2 \cdot \dots \cdot \left(\frac{p-1}{2}\right).$$

- (б) Пользуясь критерием Эйлера, установите, для каких p имеют решения уравнения $x^2 \equiv -1$, $x^2 \equiv 2$, $x^2 \equiv -2$. Результаты запишите в таблицу:

	$8k + 1$	$8k + 3$	$8k + 5$	$8k + 7$
-1				
2				
-2				

8. Докажите, что простых чисел вида $8k + 3$, $8k + 5$ и $8k + 7$ бесконечно много.