Теория чисел. Малая теорема Ферма. 10 июля.

1т. а) Пусть $a, b \in \mathbb{Z}$ и $p \in \mathbb{P}$. Докажите, что $(a+b)^p \equiv a^p + b^p \pmod{p}$.

б) Выведите отсюда по индукции *малую теорему Ферма*: если $p \in \mathbb{P}, a \in \mathbb{Z}$ и a не делится на p, то $a^{p-1} \equiv 1 \pmod{p}$.

2т. Пусть $a \in \mathbb{Z}, p \in \mathbb{P}$ и a не делится на p. Рассмотрим следующий ориентированный граф: вершины графа — числа от 1 до $p-1$; из числа x ведет ориентированное ребро висло y, если $ax \equiv y \pmod{p}$.

а) Докажите, что этот граф является объединением нескольких циклов одинаковой длины.

б) Выведите из этого малую теорему Ферма.

3т. Возьмём натуральное число a, которое не делится на простое число p.

а) Докажите, что среди остатков $a, 2a, 3a, \ldots (p-1)a$ есть все ненулевые остатки по модулю p.

б) Перемножив всё это, выведите отсюда малую теорему Ферма.

4. Пусть p и q — различные простые числа. Докажите, что $p^q + q^p \equiv p + q \,(mod\, pq)$.

5. Какой остаток даёт число $42^{42^{42}}$ при делении на 2017?

6. Дано простое число p. Докажите, что $2^{2^p} - 4$ делится на $2^p - 1$.

7. Докажите, что если $a^{15} - 1$ делится на 29, то и $a - 1$ делится на 29.

8. Какие остатки может давать число a^{50} при делении на 101?

Кировская ЛМШ 2016 год *7 класс. Группа ПРОФИ*

Теория чисел. Малая теорема Ферма. 10 июля.

1т. а) Пусть $a, b \in \mathbb{Z}$ и $p \in \mathbb{P}$. Докажите, что $(a+b)^p \equiv a^p + b^p \pmod{p}$.

б) Выведите отсюда по индукции *малую теорему Ферма*: если $p \in \mathbb{P}, a \in \mathbb{Z}$ и a не делится на p, то $a^{p-1} \equiv 1 \pmod{p}$.

2т. Пусть $a \in \mathbb{Z}, p \in \mathbb{P}$ и a не делится на p. Рассмотрим следующий ориентированный граф: вершины графа — числа от 1 до $p-1$; из числа x ведет ориентированное ребро висло y, если $ax \equiv y \pmod{p}$.

а) Докажите, что этот граф является объединением нескольких циклов одинаковой длины.

б) Выведите из этого малую теорему Ферма.

3т. Возьмём натуральное число a, которое не делится на простое число p.

а) Докажите, что среди остатков $a, 2a, 3a, \ldots (p-1)a$ есть все ненулевые остатки по модулю p.

б) Перемножив всё это, выведите отсюда малую теорему Ферма.

4. Пусть p и q — различные простые числа. Докажите, что $p^q + q^p \equiv p + q \,(mod\, pq)$.

5. Какой остаток даёт число $42^{42^{42}}$ при делении на 2017?

6. Дано простое число p. Докажите, что $2^{2^p} - 4$ делится на $2^p - 1$.

7. Докажите, что если $a^{15} - 1$ делится на 29, то и $a - 1$ делится на 29.

8. Какие остатки может давать число a^{50} при делении на 101?