Малая теорема Ферма

Первое доказательство. Пусть p – простое число, число a не делится на p.

а) Докажите, что среди чисел 0, a, $2a$, $3a$, ..., $(p-1)a$ есть все остатки при делении на p. (вспомним про полную систему вычетов!)

б) Докажите, что число $a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv (p-1)! \pmod{p}$.

в) Докажите *Малую теорему Ферма.* Если a – натуральное число, не делящееся на простое число p, то $a^{p-1} \equiv 1 \pmod{p}$.

Второе доказательство – через показатели. Рассмотрим некоторое число a, не делящееся на простое число p, и выпишем остатки, которые дают степени 1, a, a^2, a^3, a^4 при делении на p.

а) Докажите, что последовательность остатков зациклится;

б) Докажите, что первый повторившийся остаток – это 1 (то есть нет предпериода)

в) Допустим, что длина периода равна k, то есть $a^k \equiv 1 \pmod{p}$. От каждого числа x нарисуем стрелочку к числу ax, и получим ориентированный граф. Докажите, что в этом графе из каждой вершины выходит только одна стрелка, и в каждую вершину входит только одна стрелка.

г) Докажите, что этот граф разбивается на циклы длиной k.

д) Докажите, что k – делитель числа $p-1$.

е) докажите *Малую теорему Ферма.* Если a – натуральное число, не делящееся на простое число p, то $a^{p-1} \equiv 1 \pmod{p}$.

Третье доказательство. Рассмотрим правильный p-угольник и будем раскрашивать его вершины в a цветов.

а) Подсчитайте общее число раскрасок.

б) Какие раскраски переходят сами в себя при повороте на угол, кратный $\frac{2\pi}{p}$?

в) Докажите, что раскраски, которые не переходят в себя при повороте на угол, кратный $\frac{2\pi}{p}$, разбиваются на группы по p штук. д) Докажите, что $a^p - a$ делится на p.

Четвертое доказательство.

Рассмотрим бином Ньютона. $(a+b)^n = \sum_{k=0}^{n} C_n^k \, a^{n-k} b^k$

а) Докажите, что при простых p C_p^k делится на p

б) Докажите, что при простых p верно, то $(a+b)^p \equiv a^p + b^p \pmod{p}$

в) Докажите, что $a^p + 1 \equiv (a+1)^p \pmod{p}$, откуда получить МТФ индукцией по a.