

## Малая теорема Ферма

**Формулировки.** Пусть  $a \in \mathbb{Z}$ ,  $p$  – простое.

1. Если  $(a, p) = 1$ , то  $a^{p-1} \equiv 1 \pmod{p}$ .
2.  $a^p \equiv a \pmod{p}$ .

*Замечание.* Эти две формулировки эквивалентны, если  $(a, p) = 1$ .

**Доказательство 1:** хороводы (ожерелья, карусели).

1. Сколько способов одеть пятерых (одинаковых) близнецов, вставших в шеренгу, в футболки чёрного и белого цветов?
2. Сколько способов сделать это для пяти близнецов, стоящих в хороводе?
3. Угадайте ответ на аналогичную задачу для 7 близнецов и 3 цветов; для  $p$  близнецов (где  $p$  простое) и  $a$  цветов.
4. Как из полученного результата следует малая теорема Ферма?
5. Работает ли такое рассуждение для составного  $p$ ? Если нет, то где оно ломается?

**Доказательство 2:** перемножение остатков. Пусть  $(a, p) = 1$ .

1. Докажите, что числа  $0 \cdot a, 1 \cdot a, \dots, (p-1) \cdot a$  различны по модулю  $p$ .
2. Докажите, что  $(1 \cdot a) \cdot \dots \cdot ((p-1) \cdot a) \equiv (p-1)! \pmod{p}$ .
3. Докажите, что  $a^{p-1} \equiv 1 \pmod{p}$ .

**Доказательство 3:** бином и индукция.

1. Докажите, что  $(a + b)^p \equiv a^p + b^p \pmod{p}$ .
2. Докажите, используя индукцию, что  $a^p \equiv a \pmod{p}$ .

1. Посчитайте остаток от деления числа  $8^{900}$  на 29.
2. Докажите, что  $17^{120} - 1$  делится на 143.
3. Докажите, что одно из чисел  $n^{51} - 1$ ,  $n^{51} + 1$  обязательно делится на 103, если  $n$  не делится на 103.
4. Известно, что сумма 64-ых степеней шести чисел делится на 17. Докажите, что произведение этих шести чисел делится на  $17^6$ .
5. Докажите, что при любом простом  $p > 5$  число  $\underbrace{1 \dots 1}_{p-1}$  кратно  $p$ .
6. Пусть  $p$  — простое число, большее пяти. Докажите, что число  $\underbrace{11 \dots 1}_p \underbrace{22 \dots 2}_p \dots \underbrace{99 \dots 9}_p - 123456789$  делится на  $p$ .