

Тексты на диске O: Orders mod  $m$ , Fermat Test, Chinese Remainder Theorem, список команд в Wolfram Alpha ([www.wolframalpha.com](http://www.wolframalpha.com)).

Чтобы делать явные вычисления, используйте Wolfram Alpha.

1. Сколько умножений нужно, чтобы вычислить  $a^{100}$  и  $a^{2015}$ , где  $a > 1$ ?
2. Число Ферма — это целое число вида  $F_n = 2^{2^n} + 1$ , где  $n \geq 0$ . Число Мерсенна — это целое число вида  $M_n = 2^n - 1$ , где  $n \geq 1$ .
  - а) Докажите, что 2 является лжесвидетелем Ферма каждого числа Ферма. Подсказка: Вычислите порядок 2 по модулю  $F_n$ .
  - б) Докажите, что если  $n$  простое, то 2 является лжесвидетелем Ферма числа Мерсенна  $M_n$ . Что происходит, когда  $n$  составное? Подсказка: Вычислите порядок 2 по модулю  $M_n$ .
  - в) Докажите, что числа Ферма  $F_6, F_7, \dots, F_{10}$  составные, тестом Ферма.
3. Найти все свидетели Ферма числа 35. Подсказка: Если  $a$  свидетель Ферма нечетного составного числа  $n$ , то  $n - a$  тоже свидетель Ферма  $n$ .
4. Найти первый свидетель Ферма чисел 49141, 29341, и 216821881.
5. Если  $6k + 1$ ,  $12k + 1$ ,  $18k + 1$  и  $36k + 1$  простые для некоторого  $k \geq 1$ , то докажите, что их произведение является числом Кармайкла, по критерию Корселя (см. текст по тесту Ферма). Потом найти три примера таких  $k$ .
6. Существует ли такое число Кармайкла  $n$ , что его плотность свидетелей Ферма

$$\frac{|\{1 \leq a \leq n - 1 : a^{n-1} \not\equiv 1 \pmod n\}|}{n - 1}$$

больше, чем 50%?