**23*.** Докажите, что уравнение $x^7 + y^7 = 1998^z$ не имеет решений в натуральных числах.

**24*.** Для любого целого числа $k \neq 1$ существует бесконечно много натуральных чисел $n$, для которых число $2^{2^n} + k$ – составное. Докажите это. (Аналогичное утверждение для $k = 1$ мы доказать не умеем: существует или нет бесконечно много составных чисел вида $2^{2^n} + 1$, неизвестно.)

## Усиление теоремы Эйлера

Рассмотрим утверждение теоремы Эйлера при $n = 360$. Очевидно, $\varphi(360) = \varphi(2^3 \cdot 5 \cdot 9) = 4 \cdot 4 \cdot 6 = 96$. Значит, для любого целого числа $a$, взаимно простого с 360, выполнено сравнение

$$a^{96} \equiv 1 \pmod{360}.$$

А на самом деле верно даже сравнение

$$a^{12} \equiv 1 \pmod{360}.$$

Для доказательства достаточно применить теорему Эйлера к каждому из модулей 8, 5 и 9:

$$a^4 \equiv 1 \pmod 8,$$
$$a^4 \equiv 1 \pmod 5,$$
$$a^6 \equiv 1 \pmod 9,$$

и заключить, что $a^{12} \equiv 1$ по каждому из модулей 8, 5 и 9, а значит, и по модулю 360.

В общем виде это можно сформулировать следующим образом. Рассмотрим разложение

$$n = p_1^{m_1} p_2^{m_2} \ldots p_s^{m_s}$$

числа $n$ в произведение степеней различных простых множителей. Обозначим через $f(n)$ наименьшее общее кратное чисел $\varphi\left(p_i^{m_i}\right)$, где $i = 1, 2, \ldots, s$. (Например, $f(360) = \text{НОК}\left[\varphi\left(2^3\right), \varphi\left(3^2\right), \varphi(5)\right] = \text{НОК}[4, 6, 4] = 12$.) Тогда при любом целом $a$, взаимно простом с $n$, справедливы сравнения

$$a^{f(n)} \equiv 1 \left(\bmod p_i^{m_i}\right),$$

где $i = 1, 2, \ldots, s$; следовательно,

$$a^{f(n)} \equiv 1 \pmod n.$$

**Упражнение 25.** а) Для каких натуральных $n$ верно равенство $f(n) = \varphi(n)$?

б) Пусть $n > 4$ и $n$ не представимо ни в виде $p^m$, ни в виде $2p^m$, где $p$ – нечетное простое, $m$ – натуральное. Докажите, что невозможно так расположить все $\varphi(n)$ меньших $n$ и взаимно простых с ним натуральных чисел вдоль окружности, чтобы для любых трех стоящих подряд чисел $a$, $b$, $c$ разность $b^2 - ac$ делилась на $n$. (Другими словами, для этих $n$ нет первообразного корня, т.е. нет числа $g$, порядок которого по модулю $n$ равен $\varphi(n)$.)

### Сравнения по модулю $2^m$

Пусть $m$ – натуральное число, $m \geq 3$. Теорема Эйлера утверждает, что $a^{2^{m-1}} \equiv 1 \left(\bmod 2^m\right)$ для любого нечетного числа $a$. На самом деле верно более сильное утверждение:

$$a^{2^{m-2}} \equiv 1 \left(\bmod 2^m\right).$$

Его легко доказать по индукции.

*База* – случай $m = 3$. Число $a^2 - 1 = (a-1)(a+1)$ кратно 8, поскольку одно из соседних четных чисел $a - 1$ и $a + 1$ кратно 4.

*Переход*. Пусть утверждение верно для некоторого $m \geq 3$. Рассмотрим разложение на множители:

$$a^{2^{m-1}} - 1 = \left(a^{2^{m-2}} - 1\right)\left(a^{2^{m-2}} + 1\right).$$

Поскольку первый множитель правой части делится на $2^m$, а второй множитель четен, произведение делится на $2^{m+1}$, что и требовалось доказать.

**Упражнение 26.** Пусть $a$ нечетно, $m \geq 3$. а) Решите сравнение $x^2 \equiv a^2 \left(\bmod 2^m\right)$. б) Докажите, что сравнение $x^2 \equiv a \left(\bmod 2^m\right)$ разрешимо для тех и только тех $a$, для которых $a \equiv 1 \pmod 8$.

### Функция Кармайкла

Через $\lambda(n)$ обозначим такое наименьшее натуральное число $k$, что $a^k - 1$ кратно $n$ для любого числа $a$, взаимно простого с $n$. Функцию $\lambda$ называют *функцией Кармайкла*.

Легко понять, что для любого натурального числа $l$, не кратного $\lambda(n)$, существует такое взаимно простое с $n$ целое число $a$, что $a^l \not\equiv 1 \pmod n$. Чтобы это доказать, разделим с остатком $l$ на $\lambda(n)$. Имеем:

$$l = \lambda(n)q + r,$$

где $q$ – целое неотрицательное, $0 < r < \lambda(n)$. При этом

$$a^l = \left(a^{\lambda(n)}\right)^q \cdot a^r.$$

Поскольку $r < \lambda(n)$, хотя бы для одного взаимно простого с $n$ числа $a$ сравнение $a^r \equiv 1 \pmod n$ не выполнено. Это и требовалось доказать.

Функция Кармайкла обладает еще одним интересным свойством: $\lambda(mn) = \text{НОК}\left[\lambda(m), \lambda(n)\right]$ *для любых взаимно простых натуральных чисел $m$ и $n$*. В самом деле, если целое число $a$ взаимно просто с числами $m$ и $n$, то по определению

$$a^{\lambda(m)} \equiv 1 \pmod m,$$

$$a^{\lambda(n)} \equiv 1 \pmod n,$$

откуда для числа $k = \text{НОК}\left[\lambda(m), \lambda(n)\right]$ имеем

$$a^k \equiv 1 \pmod m,$$

$$a^k \equiv 1 \pmod n,$$

так что $a^k \equiv 1 \pmod{mn}$. Таким образом, $\lambda(mn) \leq k$.

Осталось доказать, что $\lambda(mn)$ делится как на $\lambda(m)$, так и на $\lambda(n)$. Сделаем это «от противного». Пусть, например, $l = \lambda(mn)$ не делится на $\lambda(m)$. Тогда существует такое число $b$, взаимно простое с $m$, что $b^l \not\equiv 1 \pmod m$.

Рассмотрим число $a$, для которого $a \equiv b \pmod m$ и $a$ взаимно просто с $n$.[7] Очевидно, $a^l \equiv b^l \not\equiv 1 \pmod m$, что и требовалось доказать.

[7] *Почему такое $a$ существует? Например, можно рассмотреть числа вида $b + mx$, где $x = 1, 2, \ldots, n$. Они дают разные остатки при делении на $n$. Поскольку этих чисел $n$ – столько же, сколько классов вычетов по модулю $n$, – то среди них найдется и нужное нам $a$.*