Принадлежность к показателю.

Пусть целое a взаимно просто с натуральным модулем m. В последовательности степеней

$$1, a, a^2, \ldots \qquad (*)$$

бесконечно много чисел, дающих конечное число остатков при делении на m. Поэтому в ней найдутся два члена, сравнимых по модулю m:

$$a^k \equiv a^\ell \pmod{m}, k > \ell.$$

Сокращая это сравнение на a^ℓ, мы получаем $a^{k-\ell} \equiv 1 \pmod{m}$, то есть некоторая степень a с натуральным показателем сравнима с $1 \bmod m$.

Определение. Наименьшее натуральное d, для которого

$$a^d \equiv 1 \pmod{m},$$

называется *показателем, к которому принадлежит a по модулю m.*

Мы будем писать $d = ord_m(a)$.

Чисто комбинаторными рассуждениями несложно убедиться, что

(i) $ord_m(a)$ – длина периода последовательности (*), и

(ii) все члены этого периода различны.

Мы докажем арифметически чаще всего используемое свойство показателя.

Предложение. Сравнение $a^k \equiv 1 \pmod{m}$ имеет место для тех и только тех натуральных k, которые кратны $d = ord_m(a)$.

Доказательство. Если $k = sd$, то $a^{sd} \equiv (a^d)^s \equiv 1 \pmod{m}$.

Наоборот, пусть $a^k \equiv 1 \pmod{m}$. Разделим k на d с остатком: $k = ds + r$, $0 \leqslant r < d$. Тогда

$$1 \equiv a^{ds+r} \equiv (a^d)^s a^r \equiv a^r \pmod{m},$$

откуда по определению показателя следует, что $r = 0$.

Из малой теоремы Ферма следует, что показатель любого вычета по простому модулю p является делителем $p - 1$. Для произвольного m показатель, к которому принадлежит вычет $\bmod m$, должен делить $\varphi(m)$.