Пусть n – произвольное целое число большее 1. Пусть s – степень вхождения двойки в $n-1$, $2m+1$ – наибольший нечетный делитель $n-1$, то есть $n-1=2^s(2m+1)$.

Свидетелем простоты числа n называется такое a из $\{2, 3, \dots, n-2\}$, что

$$\left[\begin{array}{l} \quad a^{2m+1} \equiv 1\ (mod\ n) \\ \exists\ t < s: a^{2^t(2m+1)} \equiv -1 (mod\ n) \end{array}\right.$$

Теорема

Для любого простого p верно, что у 5p не больше четырех свидетелей простоты.

Доказательство:

Пусть $5p-1=2^s(2m+1)$

Пусть есть свидетель простоты – a

Тогда верна следующая совокупность

$$\left[\begin{array}{l} \quad a^{2m+1} \equiv 1\ (mod\ 5p)\ (1) \\ \exists\ t < s: a^{2^t(2m+1)} \equiv -1 (mod\ 5p)\ (2) \end{array}\right.$$

Отдельно рассмотрим случай p = 5.

$2m+1=3, s=3.$

$\varphi(25)=20$(функция Эйлера)$=>a^{20}\equiv 1\ mod(25)$(т. Эйлера)

Если $a^3\equiv 1\ (mod\ 25)$ и $a^{20}\equiv 1\ mod(25)$, то $a^{\text{НОД}(20,\ 3)}\equiv 1\ mod(25) => a\equiv 1\ mod(25)$ – противоречие ($a\in\{2,3,\dots,23\}$)

Если $\exists\ t<3: a^{3*2^t}\equiv -1(mod\ 25)$

При t = 0:

$a^3\equiv -1(mod\ 25)$

$a^{20}=(a^3)^6\times a^2\equiv(-1)^6\times a^2=a^2\equiv 1\ mod(25)$(т. Эйлера).

Получаем, что $a^3\equiv -1(mod\ 25)$ и $a^2\equiv 1(mod\ 25)$=>$a\equiv -1(mod\ 25)$ – противоречие ($a\in\{2,3,\dots,23\}$)

$$a\in\emptyset$$

При t = 1

$$a^6\equiv -1(mod\ 25)$$

$a^{20} = (a^6)^3 \times a^2 \equiv (-1)^3 \times a^2 = -a^2 \equiv 1\, mod(25)$(т. Эйлера) $=> a \equiv \pm 2\, mod(5) => a \in \{3, 7, 8, 12, 13, 17, 18, 22\}$. Проверим каждое из этих чисел $3^2 \equiv 22^2 \equiv 9\ (mod\ 25)$, $7^2 \equiv 18^2 \equiv -1\ (mod\ 25)$, $8^2 \equiv 17^2 \equiv 14\ (mod\ 25)$, $12^2 \equiv 13^2 \equiv 19\ (mod\ 25)$. Подходят только 2 решения: a = 7 и a = 18

$$a \in \{7, \quad 18\}$$

При t = 2

$a^{12} \equiv -1(mod\ 25) => a^{24} \equiv 1(mod\ 25)$ и $a^{20} \equiv 1\, mod(25)$(т. Эйлера) $=> a^4 \equiv 1(mod\ 25)$

Найдем такие a перебором.

$2^4 \equiv 23^4 \equiv 16\ (mod\ 25)$; $3^4 \equiv 22^4 \equiv 6\ (mod\ 25)$; $4^4 \equiv 21^4 \equiv 6\ (mod\ 25)$; $5^4 \equiv 10^4 \equiv 15^4 \equiv 20^4 \equiv 0\ (mod\ 25)$; $6^4 \equiv 19^4 \equiv 21\ (mod\ 25)$; $7^4 \equiv 18^4 \equiv 1\ (mod\ 25)$; $8^4 \equiv 17^4 \equiv 21\ (mod\ 25)$; $9^4 \equiv 16^4 \equiv 11\ (mod\ 25)$; $11^4 \equiv 14^4 \equiv 16\ (mod\ 25)$; $12^4 \equiv 13^4 \equiv 11\ (mod\ 25)$.

Таким образом, подходят только 2 решения: a = 7 и a = 18

При p = 5 a $\in \{7, 18\}$ => в этом случае теорема верна.

Если p $\neq 5$

Лемма 1

Для любого простого $p \neq 5$ *и любого* a *из* $\{2, 3, \dots, 5p-2\}$ *верно, что* a^{2m+1} не сравнимо с 1 $(mod\ 5p)$, *где* $2m+1$ – *наибольший нечетный делитель 5p – 1.*

Доказательство:

Пусть s – степень вхождения двойки в 5p – 1.

Предположим противное: существуют такое простое $p \neq 5$ и такое a из $\{2, 3, \dots, 5p-2\}$, что $a^{2m+1} \equiv 1\ (mod\ 5p)$

По Малой теореме Ферма $a^4 \equiv 1\ (mod\ 5)$ и $a^{p-1} \equiv 1\ (mod\ p)$.

$a^{2m+1} \equiv 1\ (mod\ p)$ и $a^{p-1} \equiv 1\ (mod\ p)$, следовательно, $a^{\text{НОД}(2m+1,\ p-1)} \equiv 1(mod\ p)$.

$a^{2m+1} \equiv 1\ (mod\ 5)$ и $a^4 \equiv 1\ (mod\ 5)$, следовательно, $a^{\text{НОД}(2m+1,\ 4\ )} \equiv 1(mod\ 5)$.

$$\text{НОД}(2m+1, p-1) = \text{НОД}\left(\frac{5p-1}{2^s}, p-1\right) = \frac{\text{НОД}(5p-1, p-1)}{2^i}$$
$$= \frac{\text{НОД}(5p-5(p-1)-1, p-1)}{2^i} = \frac{\text{НОД}(4,\ p-1)}{2^i} = 1$$

i = min(s, $deg_2(p-1)$, т.к. НОД$(2m+1, p-1)$ не делится 2.

$\text{НОД}(2m+1,\ \ 4\ ) = 1$ (НОД нечетного и степени двойки)

$a \equiv 1(mod\ p), a \equiv 1(mod\ 5),$ следовательно, $a \equiv 1(mod\ 5p) -$ противоречие $(a \in \{2, 3, \dots, 5p-2\})$

Лемма доказана

По Лемме 1 условие (1) не может выполняться, значит, выполняется условие (2): $\exists\ t < s$: $a^{2^t(2m+1)} \equiv -1(mod\ 5p)$.

Для p возможны 2 варианта остатков при делении на 4 (1 и 3).

<u>Лемма 2</u>

Для любого простого $p \neq 5$ *и любого* a *из* $\{2, 3, \dots, 5p-2\}$ *верно, что* a^{2m+1} не сравнимо с $-1(mod\ 5p)$, *где* $2m+1$ *наибольший нечетный делитель 5p – 1.*

Доказательство:

Предположим обратное:

$\exists\ a, p$: $a^{2m+1} \equiv -1(mod\ 5p) => a^{2(2m+1)} \equiv 1(mod\ 5p)$

По Малой теореме Ферма $a^4 \equiv 1\ (mod\ 5)$ и $a^{p-1} \equiv 1\ (mod\ p)$

$a^{2(2m+1)} \equiv 1\ (mod\ p)$ и $a^{p-1} \equiv 1\ (mod\ p)$, следовательно, $a^{\text{НОД}(2(2m+1),\ p-1\ )} \equiv 1(mod\ p)$.

$a^{2(2m+1)} \equiv 1\ (mod\ 5)$ и $a^4 \equiv 1\ (mod\ 5)$, следовательно, $a^{\text{НОД}(2(2m+1),\ 4\ )} \equiv 1(mod\ 5)$

$$\text{НОД}(2(2m+1),\ \ p-1\ ) = 2\text{НОД}(2m+1,\ \ p-1\ ) = 2$$

$$НОД(2(2m+1),\ \ 4\ ) = 2НОД(2m+1,\ \ 4\ ) = 2$$

$a^2 \equiv 1\ (mod\ 5)$ и $a^2 \equiv 1\ (mod\ p)$, следовательно, $a^2 \equiv 1\ (mod\ 5p)$.

$a^{(2m+1)} = (a^2)^m \times a \equiv a \equiv -1(mod\ 5p) -$ противоречие $(a \in \{2, 3, \dots, 5p-2\})$

Лемма доказана

Если $p \equiv 3\ (mod\ 4)$, $\left(\frac{-1}{p}\right) = -1$ => t = 0, тогда

$a^{(2m+1)} \equiv -1(mod\ 5p)$ – противоречие (Лемма 2)

Тогда p сравнимо с 1 по модулю 4.

Представим p в следующем виде: $p = 4k + 1$

$a^{2^t(2m+1)} \equiv -1(mod\ 5p), t < s \rightarrow a^{5p-1} \equiv 1(mod\ 5p)$

$5p - 1 = 5(4k+1) - 1 = 20k + 4$

$a^{20k+4} \equiv 1(mod\ 5p)$

По Малой теореме Ферма $a^{4k} \equiv 1(mod\ p)$ и $a^4 \equiv 1(mod\ 5)$

$a^{20k+4} \equiv 1(mod\ p)$ и $a^{4k} \equiv 1(mod\ p)$ => $a^4 \equiv 1(mod\ p)$

$a^4 \equiv 1(mod\ p)$ и $a^4 \equiv 1(mod\ 5)$, следовательно, $a^4 \equiv 1(mod\ 5p)$

Сравнение $a^4 \equiv 1\ (mod\ p)$ имеет ровно 2 решения для a^2 по модулю p.

$a^2 \equiv 1\ (mod\ p)$

$a^2 \equiv -1\ (mod\ p)$

Каждое из сравнений для a^2 имеет ровно 2 решения относительно a.

$a^2 \equiv 1\ (mod\ p)$

$a \equiv 1\ (mod\ p)$

$a \equiv -1\ (mod\ p)$

Пусть $\pm r$ – решения $a^2 \equiv -1\ (mod\ p)$ относительно a.

$a \equiv r\ (mod\ p)$

$a \equiv -r\ (mod\ p)$

- Решение $a \equiv 1\ (mod\ p)$ не подходит, т.к. $a^{2^t(2m+1)} \equiv -1(mod\ 5p)$

- При $a \equiv -1\ (mod\ p)$, $a^{2^t(2m+1)} \equiv -1(mod\ 5p)$. Это верно только при $t = 0$. Тогда $a^{(2m+1)} \equiv -1(mod\ 5p)$ – противоречие (Лемма 2).
- При $a \equiv \pm r\ (mod\ p)$ получается не больше 10 вариантов для a:

$a = r$

$a = p \pm r$

$a = 2p \pm r$

$a = 3p \pm r$

$a = 4p \pm r$

$a = 5p - r$

Заметим, что а не может быть сравнимо с 0 и ± 1 по модулю 5.

$a^{2^t(2m+1)} \equiv -1(mod\ 5) -$ отсюда очевидно, что а не может быть сравнимо с 0 и 1 по модулю 5. Если а сравнимо с -1, тогда *t=0* => $a^{(2m+1)} \equiv -1(mod\ 5p) -$ противоречие (Лемма 2).

В группе из 5 чисел $\{r,\ p + r, 2p + r, 3p + r, 4p + r\}$ 5 различных остатков от деления на 5 и в группе $\{p - r,\ 2p - r, 3p - r, 4p - r, 5p - r\}$ тоже 5 различных остатков, тогда в данном наборе из 10 чисел каждый остаток от деления на 5 присутствует ровно 2 раза. Тогда, из предложенных 10 вариантов для а найдутся 2 сравнимых с 1, 2 сравнимых с -1 и 2 сравнимых с 0 по модулю 5, а такие не подходят. Т.о. вариантов для а остается не больше 4.

Ч.т.д.